Acronis

acronis.com

Cyber Protection

24.03

사용자 안내서

수정 버전: 2024-04-10

목차

Cyber Protection 시작하기 **19**
계정 활성화 19
비밀번호 요구 사항 19
2단계 인증 19
개인 정보 보호 설정 21
Cyber Protection 서비스 액세스 21
소프트웨어 요구 사항 22
지원되는 웹 브라우저 22
지원되는 운영 체제 및 환경 23
지원되는 Microsoft SQL Server 버전 29
지원되는 Microsoft Exchange Server 버전 29
지원되는 Microsoft SharePoint 버전 29
지원되는 Oracle 데이터베이스 버전 30
지원되는 SAP HANA 버전 30
지원되는 MySQL 버전 30
지원되는 MariaDB 버전 30
지원되는 가상화 플랫폼 30
암호화 소프트웨어와의 호환성 39
Dell EMC Data Domain 스토리지와의 호환성 40
운영 체제별 지원되는 보호 기능 41
지원되는 운영 체제 및 버전 42
지원되는 파일 시스템 50
논리 볼륨에서 지원되는 작업 53
백업 53
복구 53
Cyber Protection 에이전트 설치 및 디플로이 **55**
준비 55
1단계 55
2단계 55
3단계 55
4단계 55
5단계 56
6단계 57
필요한 에이전트 57
에이전트 기반 백업 및 비에이전트 백업 61

© Acronis International GmbH, 2003-2024

필요한 백업 유형 확인 61
에이전트의 시스템 요구 사항 62
Linux 패키지 64
필요한 패키지가 이미 설치되어 있습니까? 65
리포지토리에서 패키지 설치 66
수동으로 패키지 설치 67
프록시 서버 설정 구성 68
Protection 에이전트 설치 72
Protection 에이전트 다운로드 72
Windows에서 Protection 에이전트 설치 72
Linux에서 Protection 에이전트 설치 74
macOS에서 Protection 에이전트 설치 76
Connect 에이전트에 필요한 시스템 권한 부여 77
Windows 머신에서 로그온 계정 변경 79
컴퍼넌트의 동적 설치 및 설치 제거 80
무인 설치 또는 제거 81
Windows에서 무인 설치 또는 제거 81
예 82
예 83
예 83
예 91
예 92
예 92
Linux에서 무인 설치 또는 제거 97
macOS에 무인 설치 및 제거 103
수동으로 워크로드 등록 및 등록 해제 110
특수 문자 또는 공백이 포함된 비밀번호 114
워크로드 등록 변경 115
머신 자동 검색 115
사전 요구 사항 115
자동 검색의 작동 방식 116
에이전트 원격 설치의 작동 방식 118
자동 검색 및 수동 검색 수행 118
검색된 머신 관리 123
문제 해결 124
Agent for VMware(가상 어플라이언스) 배포 125
시작하기 전에 125

© Acronis International GmbH, 2003-2024

OVF 템플릿 디플로이 126
가상 어플라이언스 구성 126
Agent for Scale Computing HC3(가상 어플라이언스) 배포 중 129
시작하기 전에 129
QCOW2 템플릿 디플로이 130
가상 어플라이언스 구성 131
Agent for Scale Computing HC3 – 필요한 역할 133
Agent for Virtuozzo Hybrid Infrastructure(가상 어플라이언스) 디플로이 134
시작하기 전에 134
Virtuozzo Hybrid Infrastructure의 네트워크 구성 135
Virtuozzo Hybrid Infrastructure의 사용자 계정 구성 135
QCOW2 템플릿 디플로이 138
가상 어플라이언스 구성 139
Agent for oVirt(가상 어플라이언스) 디플로이 중 142
시작하기 전에 142
OVA 템플릿 디플로이 143
가상 어플라이언스 구성 144
Agent for oVirt – 필요한 역할과 포트 147
Agent for Synology 디플로이 147
시작하기 전에 147
설정 프로그램을 다운로드합니다. 148
Agent for Synology 설치 149
Agent for Synology 업데이트 153
그룹 정책을 통해 에이전트 배포 156
사전 요구 사항 156
등록 토큰 생성 156
변환 파일 생성 및 설치 패키지 추출 159
그룹 정책 객체 설정 159
가상 어플라이언스에 대한 SSH 연결 160
보안 셸 데몬 시작 160
가상 어플라이언스에서 루트 암호 설정 161
SSH 클라이언트를 통해 가상 어플라이언스 액세스 161
에이전트 업데이트 162
에이전트 수동 업데이트 162
자동으로 에이전트 업데이트 164
BitLocker로 보호된 워크로드에서 에이전트 업데이트 166
에이전트의 무단 설치 제거 또는 변경의 방지 166

© Acronis International GmbH, 2003-2024

에이전트 제거 ... 167
보호 설정 ... 169
컴퓨넌트에 대한 자동 업데이트 ... 169
스케줄별로 Cyber Protection 정의 업데이트 ... 170
필요에 따라 Cyber Protection 정의 업데이트 ... 171
캐시 스토리지 ... 171
머신의 서비스 할당량 변경 ... 171
사용자 환경에 설치된 Cyber Protection 서비스 ... 172
Windows에 설치되는 서비스 ... 172
macOS에 설치되는 서비스 ... 173
에이전트 로그 파일 저장 ... 173
사이트 간 OpenVPN - 추가 정보 ... 173
온프레미스 관리 서버용 라이센스 관리 ... 182
보호 방법과 대상 정의 ... 183
관리 탭 ... 183
계획 상태 ... 183
보호 계획 ... 183
클라우드 애플리케이션의 백업 계획 ... 184
백업 스캔 계획 ... 184
오프호스트 데이터 처리 ... 185
VM 하트비트 ... 192
스크린샷 유효성 검사 ... 192
중간 스냅샷 ... 199
보호 계획 및 모듈 ... 199
보호 계획 생성 ... 200
보호 계획이 있는 작업 ... 201
계획 충돌 해결 ... 205
기본 보호 계획 ... 206
호스팅 제어판 통합용 개별 보호 계획 ... 211
머신별 #CyberFit Score ... 211
작동법 ... 212
#CyberFit Score 스캔 실행 중 ... 215
Cyber Scripting ... 217
사전 요구 사항 ... 217
제한 사항 ... 217
지원되는 플랫폼 ... 217
사용자 역할 및 Cyber Scripting 권한 ... 218

© Acronis International GmbH, 2003-2024

스크립트 ... 220
스크립트 저장소 ... 229
스크립팅 계획 ... 229
스크립트 빠른 실행 ... 238
협업 및 커뮤니케이션 애플리케이션 보호 ... 239
현재 보호 수준 이해 ... 240
모니터링 ... 240
개요 대시보드 ... 240
활동 대시보드 ... 241
경보 대시보드 ... 241
경보 유형 ... 242
경보 위젯 ... 259
Cyber Protection ... 260
보호 상태 ... 260
EDR(엔드포인트 탐지 및 대응) 위젯 ... 261
머신별 #CyberFit Score ... 265
디스크 상태 모니터링 ... 266
데이터 보호 맵 ... 270
취약성 평가 위젯 ... 271
패치 설치 위젯 ... 272
백업 스캔 세부 정보 ... 274
최근 영향 받은 항목 ... 274
클라우드 애플리케이션 ... 275
소프트웨어 인벤토리 위젯 ... 276
하드웨어 인벤토리 위젯 ... 277
원격 세션 위젯 ... 278
스마트 보호 ... 278
활동 탭 ... 285
Cyber Protect 모니터 ... 286
Cyber Protect Monitor에서 프록시 서버 설정 구성 ... 287
보고 ... 287
보고서 관련 작업 ... 288
위젯 유형에 따라 보고된 데이터 ... 290
Cyber Protect 콘솔에서 워크로드 관리 ... 293
Cyber Protect 콘솔 ... 293
Cyber Protect 콘솔의 새로운 기능 ... 294
파트너 관리자로 Cyber Protect 콘솔 사용 ... 294

© Acronis International GmbH, 2003-2024

사전 요구 사항 ... 298
워크로드 ... 301
Cyber Protect 콘솔에 워크로드 추가 ... 303
Cyber Protect 콘솔에서 워크로드 제거 ... 307
장치 그룹 ... 311
기본 제공 그룹 및 사용자 지정 그룹 ... 311
정적 그룹과 동적 그룹 ... 312
클라우드 간 그룹과 클라우드 간 그룹이 아닌 그룹 ... 312
정적 그룹 생성 ... 313
정적 그룹에 워크로드 추가 ... 314
동적 그룹 생성 ... 315
동적 그룹 편집 ... 329
그룹 삭제 ... 330
그룹에 계획 적용 ... 330
그룹에서 계획 철회 ... 331
장치 제어 모듈 사용 ... 332
장치 제어 사용 ... 334
액세스 설정 ... 341
장치 유형 허용 목록 ... 346
USB 장치 허용 목록 ... 347
액세스 제어에서 프로세스 제외 ... 351
장치 제어 경보 ... 353
관리 대상 워크로드에서 데이터 소거 ... 356
CyberApp 워크로드 ... 357
집계된 워크로드 ... 357
CyberApp 워크로드 사용 ... 357
집계된 워크로드 사용 ... 358
마지막으로 로그인한 사용자 찾기 ... 359
워크로드와 파일의 백업 및 복구 관리 ... 361
백업 ... 361
보호 계획 치트 시트 ... 363
백업할 데이터 선택 ... 365
전체 머신 선택 ... 365
디스크 또는 볼륨 선택 ... 366
파일 또는 폴더 선택 ... 369
시스템 상태 선택 ... 371
ESXi 구성 선택 ... 372

© Acronis International GmbH, 2003-2024

지속적인 데이터 보호(CDP) 372
작동법 373
지원되는 데이터 소스 374
지원되는 대상 375
CDP 백업 구성 375
목적지 선택 376
고급 스토리지 옵션 377
Secure Zone 정보 378
백업 스케줄 381
백업 구성표 381
백업 유형 383
스케줄에 따라 백업 실행 383
수동으로 백업 실행 395
보관 규칙 396
중요 팁 397
백업 구성표에 따른 보존 규칙 397
보존 규칙 구성 399
복제 400
사용 예제 400
지원되는 위치 401
암호화 402
보호 계획에서 암호화 구성 402
머신 속성으로 암호화 설정 403
공증 405
공증 사용 방법 405
작동법 405
기본 백업 옵션 405
백업 옵션 406
백업 옵션의 사용 가능성 406
경보 409
백업 통합 409
백업 파일 이름 410
백업 형식 414
백업 유효성 검사 415
CBT(Changed Block Tracking) 416
클러스터 백업 모드 416
압축 수준 417

© Acronis International GmbH, 2003-2024

오류 처리 ... 418
빠른 증분/차등 백업 ... 419
파일 필터(포함/제외) ... 419
파일 수준 백업 스냅샷 ... 421
포렌직 데이터 ... 421
로그 자르기 ... 430
LVM 스냅샷 촬영 ... 430
마운트 포인트 ... 431
다중 볼륨 스냅샷 ... 431
원클릭 복구 ... 432
성능 및 백업 할당 시간 ... 436
실제 데이터 전달 ... 440
사전/사후 명령어 ... 441
데이터 캡처 전/후 명령 ... 443
일정 예약 ... 445
섹터 단위 백업 ... 446
분할 ... 446
작업 실패 처리 ... 446
작업 시작 조건 ... 447
VSS(Volume Shadow Copy Service) ... 447
가상 머신용 VSS(Volume Shadow Copy Service) ... 449
주간 백업 ... 451
Windows 이벤트 로그 ... 451
복구 ... 451
복구 치트 시트 ... 451
안전 복구 ... 453
머신 복구 ... 454
드라이버 준비 ... 463
부트 가능한 환경에서 드라이버에 대한 액세스 확인 ... 464
자동 드라이버 검색 ... 464
설치할 대용량 스토리지 드라이버 ... 464
파일 복구 ... 466
시스템 상태 복구 ... 472
ESXi 구성 복구 ... 472
복구 옵션 ... 473
백업 관련 작업 ... 480
백업 스토리지 탭 ... 480

© Acronis International GmbH, 2003-2024

백업에서 볼륨 마운트 ... 482
백업 유효성 검사 ... 484
백업 내보내기 ... 484
백업 삭제 ... 485
병목 현상 감지 방식 파악 ... 487
퍼블릭 클라우드에 워크로드 백업 ... 491
Microsoft Azure에서 백업 위치 정의 ... 492
Amazon S3에서 백업 위치 정의 ... 494
Wasabi에서 백업 위치 정의 ... 496
퍼블릭 클라우드 백업 위치 확인 및 업데이트 ... 497
퍼블릭 클라우드 계정 액세스 관리 ... 498
Microsoft 애플리케이션 보호 ... 509
Microsoft SQL Server 및 Microsoft Exchange Server 보호 ... 509
Microsoft SharePoint 보호 ... 509
도메인 컨트롤러 보호 ... 509
애플리케이션 복구 ... 510
사전 요구 사항 ... 510
데이터베이스 백업 ... 512
Aware 인식→인지 ... 518
사서함 백업 ... 520
SQL 데이터베이스 복구 ... 522
Exchange 데이터베이스 복구 ... 529
Exchange 사서함 및 사서함 항목 복구 ... 532
SQL Server 또는 Exchange Server 액세스 자격 증명 변경 ... 537
모바일 장치 보호 ... 538
지원되는 모바일 장치 ... 538
백업할 수 있는 항목 ... 538
알아야 할 사항 ... 538
Cyber Protect 앱 다운로드 방법 ... 539
데이터 백업 시작 방법 ... 539
데이터를 모바일 장치로 복구하는 방법 ... 540
Cyber Protect 콘솔을 통해 데이터를 검토하는 방법 ... 540
Hosted Exchange 데이터 보호 ... 541
어떤 항목을 백업할 수 있습니까? ... 541
복구할 수 있는 항목은 무엇입니까? ... 542
Exchange Online 사서함 선택 ... 542
사서함 및 사서함 항목 복구 ... 543

© Acronis International GmbH, 2003-2024

Microsoft 365 데이터 보호 545
Microsoft 365 데이터를 백업하는 이유? 545
클라우드 에이전트 및 로컬 에이전트 545
필수 사용자 권한 547
제한 사항 548
Microsoft 365 시트 라이센스 보고서 549
로깅 549
로컬로 설치한 Agent for Office 365 사용 549
클라우드 Agent for Microsoft 365 사용 553
Google Workspace 데이터 보호 582
Google Workspace 데이터 보호의 의미 583
필수 사용자 권한 583
백업 스케줄 정보 583
제한 사항 584
로깅 584
Google Workspace 조직 추가하기 584
개인용 Google 클라우드 프로젝트 생성 585
Google Workspace 리소스 검색 588
Google Workspace 백업의 빈도 설정 589
Gmail 데이터 보호 589
Google Drive 파일 보호 593
Shared Drive 파일 보호 597
공증 600
클라우드 간 백업에서 검색 601
전체 텍스트 검색 602
검색 인덱스 602
검색 인덱스의 크기 확인 603
인덱스 업데이트, 다시 구축 또는 삭제 603
암호화된 백업에서 향상된 검색 활성화 604
기존 계획에서 향상된 검색을 활성화하거나 비활성화하기 605
Gmail 백업에 대한 전체 텍스트 검색 비활성화 605
Oracle 데이터베이스 보호 606
SAP HANA 보호 606
MySQL 및 MariaDB 데이터 보호 606
애플리케이션 인식 백업 구성 607
애플리케이션 인식 백업에서 데이터 복구 608
웹사이트 및 호스팅 서버 보호 612

© Acronis International GmbH, 2003-2024

웹 사이트 보호 612
웹 호스팅 서버 보호 615
가상 머신을 사용한 특수 작업 616
백업에서 가상 머신 실행(즉시 복원) 616
VMware vSphere에서 작업 620
클러스터 Hyper-V 머신 백업 638
동시 백업되는 가상 머신의 총 수를 제한합니다. 638
머신 이주 640
Microsoft Azure 및 Amazon EC2 가상 머신 643
운영 체제 복구용으로 부트 가능한 미디어 생성 643
사용자 정의 부트 가능한 미디어 대 이미 생성된 부트 가능한 미디어 644
Linux 기반 부트 가능한 미디어 대 WinPE/WinRE 기반 부트 가능한 미디어 644
실제 부트 가능한 미디어 생성 645
Bootable Media Builder 645
클라우드 스토리지에서 복구 649
네트워크 공유에서 복구 649
스크립트 파일 650
autostart.json의 구조 651
최상위 객체 651
변수 객체 651
컨트롤 유형 652
부트 가능한 미디어에서 부팅한 머신에 연결 659
부트 가능한 미디어를 사용한 로컬 작업 659
부트 가능한 미디어를 사용한 원격 작업 660
Startup Recovery Manager 663
재해 복구 구현 666
Cyber Disaster Recovery Cloud 정보 666
주요 기능 666
소프트웨어 요구 사항 666
지원되는 운영 체제 666
지원되는 가상화 플랫폼 667
제한 사항 668
Cyber Disaster Recovery Cloud 평가판 버전 669
Geo-redundant Cloud Storage 사용 시의 제한 사항 669
암호화 소프트웨어와의 재해 복구 호환성 669
컴퓨팅 포인트 670
재해 복구 기능 설정 671

© Acronis International GmbH, 2003-2024

재해 복구 보호 계획 생성 671
복구 서버 기본 매개변수 편집 672
클라우드 네트워크 인프라 674
연결 설정 674
네트워킹 개념 674
최초 연결 구성 685
사전 요구 사항 687
네트워크 관리 693
사전 요구 사항 708
복구 서버 설정 708
복구 서버 생성 708
장애 조치 작동 방식 711
장애 복구 작동 방식 718
사전 요구 사항 721
사전 요구 사항 725
암호화된 백업 관련 작업 728
Microsoft Azure 가상 머신 관련 작업 729
기본 서버 설정 729
기본 서버 생성 729
기본 서버 관련 작업 732
클라우드 서버 관리 732
클라우드 서버용 방화벽 규칙 733
클라우드 서버용 방화벽 규칙 설정 734
클라우드 방화벽 활동 확인 736
클라우드 서버 백업 737
조정(작동 실행서) 737
실행서를 사용하는 이유는 무엇인가요? 737
작동 실행서 생성 738
작동 실행서 관련 작업 741
안티바이러스 및 안티맬웨어 보호 구성 743
지원되는 플랫폼 743
플랫폼별로 지원되는 기능 744
안티바이러스 및 안티맬웨어 보호 기능 746
안티맬웨어 기능 746
스캐닝 유형 747
안티바이러스 및 맬웨어 방지 기능 설정 748
Cyber Backup Standard Edition의 Active Protection 762

© Acronis International GmbH, 2003-2024

Cyber Backup Standard의 Active Protection 설정 ... 762
URL 필터링 ... 769
작동법 ... 769
URL 필터링 구성 작업 흐름 ... 771
URL 필터링 설정 ... 771
설명 ... 776
Microsoft Defender 안티바이러스 및 Microsoft Security Essentials ... 777
스캔 예약 ... 777
기본 작업 ... 778
실시간 보호 ... 778
Advanced ... 779
제외 ... 779
방화벽 관리 ... 780
격리 ... 781
파일은 어떻게 격리 폴더로 이동합니까? ... 781
격리된 파일 관리 ... 781
머신의 격리 위치 ... 782
셀프 서비스 사용자 정의 폴더 온디맨드 ... 782
기업 허용 목록 ... 782
허용 목록에 자동 추가 ... 783
허용 목록에 수동 추가 ... 783
허용 목록에 격리된 파일 추가 ... 783
허용 목록 설정 ... 783
허용 목록의 항목 관련 상세 정보 확인 ... 784
백업 맬웨어 방지 스캔 ... 784
제한 사항 ... 785
고급 보호 기능 사용 ... 786
Advanced Data Loss Prevention ... 787
데이터 플로우 정책 및 정책 규칙 생성 ... 788
보호 계획에서 Advanced Data Loss Prevention 활성화 ... 796
대상 자동 감지 ... 799
민감한 데이터 정의 ... 800
데이터 손실 방지 이벤트 ... 805
개요 대시보드의 Advanced Data Loss Prevention 위젯 ... 806
사용자 정의 민감도 카테고리 ... 807
조직 매핑 ... 809
알려진 문제 및 제한 사항 ... 812

© Acronis International GmbH, 2003-2024

EDR(Endpoint Detection and Response) 812
EDR(Endpoint Detection and Response)이 필요한 이유 813
EDR(Endpoint Detection and Response) 기능 활성화 815
EDR(Endpoint Detection and Response) 사용 방법 817
현재 완화되지 않은 인시던트 확인 820
인시던트의 범위와 영향 파악 821
공격 단계로 이동하는 방법 829
EDR(Endpoint Detection and Response)을 위한 모니터링 모드 활성화 860
EDR(Endpoint Detection and Response)이 정상 작동 중인지 테스트하는 방법 862
취약성 평가 및 패치 관리 864
취약성 평가 864
지원되는 Microsoft 및 서드 파티 제품 864
지원되는 Apple 및 서드 파티 제품 866
지원되는 Linux 제품 867
취약성 평가 설정 867
Windows 머신 취약성 평가 869
Linux 머신 취약성 평가 869
macOS 장치의 취약성 평가 870
발견된 취약성 관리 870
패치 관리 872
패치 관리 워크플로우 872
보호 계획의 패치 관리 설정 873
사용 가능한 패치 목록 확인 877
자동 패치 승인 880
수동으로 패치 승인 883
요청 시 패치 설치 884
소프트웨어 및 하드웨어 인벤토리 관리 886
소프트웨어 인벤토리 886
소프트웨어 인벤토리 스캐닝 활성화 886
수동으로 소프트웨어 인벤토리 스캔 실행 887
소프트웨어 인벤토리 찾아보기 887
단일 장치의 소프트웨어 인벤토리 보기 889
하드웨어 인벤토리 890
하드웨어 인벤토리 스캐닝 활성화 890
수동으로 하드웨어 인벤토리 스캔 실행 891
하드웨어 인벤토리 찾아보기 891
단일 장치의 하드웨어 보기 893

© Acronis International GmbH, 2003-2024

원격 데스크탑 또는 원격 지원을 위해 워크로드에 연결 895
지원되는 원격 데스크탑 및 지원 기능 896
지원되는 플랫폼 899
원격 연결 프로토콜 900
NEAR 900
RDP 901
Apple 화면 공유 901
원격 사운드 리디렉션 901
원격 데스크탑 또는 원격 지원을 위한 원격 워크로드로의 연결 902
원격 관리 계획 903
원격 관리 계획 생성 903
원격 관리 계획에 워크로드 추가 910
원격 관리 계획에서 워크로드 제거 911
기존 원격 관리 계획을 사용하여 추가 작업 수행 911
원격 관리 계획과의 호환성 문제 913
원격 관리 계획과의 호환성 문제 해결 914
워크로드 자격 증명 915
자격 증명 추가 915
워크로드에 자격 증명 할당 916
자격 증명 삭제 916
워크로드에서 자격 증명 할당 해제 917
관리 대상 워크로드 사용 917
RDP 설정 구성 917
원격 데스크탑 또는 원격 지원을 위해 관리 대상 워크로드에 연결 918
웹 클라이언트를 통해 관리 대상 워크로드에 연결 920
파일 전송 921
관리 대상 워크로드에서 제어 작업 수행 921
스크린샷 전송을 통해 워크로드 모니터링 923
동시에 여러 관리 대상 워크로드 관찰 924
비관리 대상 워크로드 사용 925
Acronis 빠른 지원을 통해 관리 대상 워크로드에 연결 925
IP 주소를 통해 비관리 대상 워크로드에 연결 926
Acronis 빠른 지원을 통한 파일 전송 926
뷰어 창에서 도구 모음 사용 927
원격 세션 녹화 및 재생 929
Connect 클라이언트 설정 구성 930
원격 데스크탑 Notifier 931

© Acronis International GmbH, 2003-2024

워크로드의 상태와 성능 모니터링 933
모니터링 계획 933
모니터링 유형 933
이상 현상 기반 모니터링 933
모니터링용으로 지원되는 플랫폼 934
구성 가능한 모니터 934
디스크 공간 모니터의 설정 937
CPU 온도 모니터의 설정 939
GPU 온도 모니터의 설정 940
하드웨어 변경 모니터의 설정 942
CPU 사용량 모니터의 설정 942
메모리 사용량 모니터의 설정 944
디스크 전송 속도 모니터의 설정 945
네트워크 사용량 모니터의 설정 948
프로세스별 CPU 사용량 모니터의 설정 950
프로세스별 메모리 사용량 모니터의 설정 951
프로세스별 디스크 전송 속도 모니터의 설정 951
프로세스별 네트워크 사용량 모니터의 설정 952
Windows 서비스 상태 모니터의 설정 954
프로세스 상태 모니터의 설정 954
설치된 소프트웨어 모니터의 설정 955
마지막 시스템 다시 시작 모니터의 설정 955
Windows 이벤트 로그 모니터의 설정 956
파일 및 폴더 크기 모니터의 설정 957
Windows 업데이트 상태 모니터의 설정 958
방화벽 상태 모니터의 설정 958
실패한 로그인 모니터의 설정 958
안티맬웨어 소프트웨어 상태 모니터의 설정 959
자동 실행 기능 상태 모니터의 설정 960
사용자 정의 모니터의 설정 961
모니터링 계획 962
모니터링 계획 생성 962
모니터링 계획에 워크로드 추가 964
모니터링 계획 해지 965
자동 대응 조치 구성 965
모니터링 계획 관련 추가 작업 967
모니터링 계획의 호환성 문제 969

© Acronis International GmbH, 2003-2024

모니터링 계획의 호환성 문제 해결 ... 970
머신 러닝 모델 재설정 ... 971
모니터링 경보 ... 971
모니터링 경보 구성 ... 971
모니터링 경보 변수 ... 972
수동 대응 조치 ... 975
워크로드에 대한 모니터링 경보 보기 ... 977
모니터링 경보의 경보 로그 확인 ... 977
이메일 알림 정책 구성 ... 978
모니터 데이터 보기 ... 979
모니터 위젯 ... 980
추가 Cyber Protection 도구 ... **982**
규제 준수 모드 ... 982
제한 사항 ... 982
지원되지 않는 기능 ... 982
암호화 비밀번호 설정 ... 982
암호화 비밀번호 변경 ... 983
규제 준수 모드로 설정된 테넌트의 백업 복구 ... 983
변경 불가 스토리지 ... 984
변경 불가능 스토리지 모드 ... 984
지원되는 스토리지 및 에이전트 ... 984
변경 불가능 스토리지 활성화 ... 985
변경 불가능 스토리지 비활성화 ... 986
변경 불가 스토리지에서 삭제된 백업 액세스 ... 986
지역 중복 스토리지 ... 986
지역 중복 스토리지 활성화 및 비활성화 ... 987
지역 간 복제 상태 ... 987
제한 사항 ... 988
용어 설명 ... **989**
색인 ... **993**

© Acronis International GmbH, 2003-2024

Cyber Protection 시작하기

계정 활성화

관리자가 사용자를 위해 계정을 생성한 경우 사용자의 이메일 주소로 이메일 메시지가 전송됩니다. 이 메시지에는 다음과 같은 정보가 포함되어 있습니다.

- **사용자 로그인.** 로그인하는 데 사용하는 사용자 이름입니다. 사용자 로그인 정보는 계정 활성화 페이지에도 표시됩니다.
- **계정 활성화** 버튼. 이 버튼을 클릭하여 계정의 비밀번호를 설정합니다. 비밀번호의 길이는 9자 이상이어야 합니다. 비밀번호에 대한 자세한 내용은 "비밀번호 요구 사항"(19페이지) 항목을 참조하십시오.

관리자가 2단계 인증을 활성화한 경우 계정에 2단계 인증을 설정하라는 메시지가 표시됩니다. 자세한 내용은 "2단계 인증"(19페이지) 항목을 참조하십시오.

비밀번호 요구 사항

사용자 계정의 비밀번호는 9자 이상이어야 합니다. 또한 비밀번호의 복잡성이 확인되고 다음 범주 중 하나로 분류됩니다.

- 약함
- 중간
- 강함

약한 비밀번호는 9자 이상이어도 저장할 수 없습니다. 사용자 이름, 로그인, 사용자 이메일 또는 사용자 계정이 속한 테넌트의 이름이 포함된 비밀번호는 항상 약한 비밀번호로 간주됩니다. 대부분의 일반적인 비밀번호는 약한 비밀번호로 간주됩니다.

비밀번호를 강화하려면 문자를 더 추가하십시오. 숫자, 대문자와 소문자, 특수 문자 등 다양한 유형의 문자를 사용하는 것은 필수는 아니지만 짧아도 더 강력한 비밀번호가 될 수 있습니다.

2단계 인증

2FA(2단계 인증) 사용 시에는 계정을 무단 액세스로부터 더욱 철저하게 보호할 수 있습니다. 2FA(2단계 인증)가 설정되어 있으면 Cyber Protect 콘솔에 로그인할 때 암호(첫 번째 요소) 및 일회성 코드(두 번째 요소)를 입력해야 합니다. 일회성 코드는 휴대폰이나 갖고 있는 다른 장치에 설치되어 있어야 하는 특별한 애플리케이션을 통해 생성됩니다. 다른 사람이 사용자의 로그인 및 암호를 알게 된다고 해도 두 번째 요소 생성 장치에 접근할 수 없다면 계정 로그인은 불가능합니다.

계정에 대한 2단계 인증을 설정하려면

관리자가 조직에서 2FA를 활성화했다면 개별 사용자는 본인 계정에서 2FA(2단계 인증)를 설정해야 합니다. Cyber Protect 콘솔에 로그인되어 있는 상태에서 관리자가 2FA(2단계 인증)를 활성화하는 경우에는 현재 세션 만료 시에 2FA를 설정해야 합니다.

사전 요구 사항

© Acronis International GmbH, 2003-2024

- 관리자가 조직을 대상으로 2단계 인증을 활성화해야 합니다.

계정에 대한 2단계 인증을 설정하려면

1. 모바일 장치에 인증 프로그램 앱을 설치합니다.
   인증 프로그램 앱의 예는 다음과 같습니다.
   - Twilio Authy
   - Microsoft Authenticator
   - Google Authenticator
2. 인증 프로그램 앱을 사용하여 QR 코드를 스캔한 후 인증 프로그램 앱에 표시된 6자리 코드를 **2단계 인증 설정** 창에 입력합니다.
3. **다음**을 클릭합니다.
   2FA(2단계 인증) 장치를 분실하거나 인증 프로그램 앱을 설치 제거하는 경우 계정 액세스를 복원하는 지침이 표시됩니다.
4. PDF 파일을 저장하거나 인쇄합니다.

   참고
   PDF 파일을 안전한 곳에 저장하거나 나중에 참조할 수 있도록 인쇄하십시오. 이렇게 하면 계정 액세스를 가장 쉽게 복원할 수 있습니다.

5. Cyber Protect 콘솔 로그인 페이지로 돌아가 생성된 코드를 입력합니다.
   일회성 코드는 30초 동안 유효합니다. 30초가 넘어가면 다음에 생성된 코드를 사용하십시오.

다음에 로그인할 때는 **이 브라우저 신뢰...** 확인란을 선택할 수 있습니다. 이렇게 하면 해당 머신에서 동일 브라우저를 사용하는 후속 로그인 시 코드를 입력하지 않아도 됩니다.

참고
이 확인란은 선택을 취소한 상태로 유지하는 것이 좋습니다. 이 확인란을 선택하면 계정에 액세스할 때 2FA(2단계 인증)를 사용하지 않게 됩니다.

새 장치에서 2FA(2단계 인증)를 복원하려면

이전에 설정한 모바일 인증 앱에 액세스할 수 있는 경우

1. 새 장치에 인증 프로그램 앱을 설치합니다.
2. 장치에서 2FA(2단계 인증)를 구성할 때 저장했던 PDF 파일을 사용합니다. 이 파일에는 Acronis 계정에 인증 프로그램 앱을 다시 연결하려면 인증 프로그램 앱에서 입력해야 하는 32자리 코드가 포함되어 있습니다.

   중요
   해당 코드가 작동하지 않으면 인증 프로그램 모바일 앱의 시간이 장치와 동기화되어 있는지 확인합니다.

   설정 시에 PDF 파일을 저장하지 않은 경우:

a. **2FA(2단계 인증) 재설정**을 클릭하고 모바일 인증 프로그램 앱에 표시된 일회성 암호를 입력합니다.

© Acronis International GmbH, 2003-2024

b. 화면에 나타나는 지침을 따릅니다.

이전에 설정한 모바일 인증 프로그램 앱에 액세스할 수 없는 경우

1. 새 모바일 장치를 가져옵니다.
2. 저장해 둔 PDF 파일을 사용하여 새 장치를 연결합니다. 이 파일의 기본 이름은 `cyberprotect-2fa-backupcode.pdf`입니다.
3. 백업에서 계정 액세스를 복원합니다. 모바일 앱에서 백업이 지원되는지 확인합니다.
4. 앱이 지원하는 경우 다른 모바일 장치에서 동일 계정으로 앱을 엽니다.

개인 정보 보호 설정

개인 정보 보호 설정을 사용하면 개인 정보 수집, 사용 및 공개 동의 여부를 선택할 수 있습니다.

Cyber Protect Cloud을(를) 사용 중인 국가와 서비스를 제공하는 Cyber Protect Cloud 데이터 센터에 따라 Cyber Protect Cloud을(를) 처음 시작할 때 Cyber Protect Cloud에서 Google Analytics를 사용하는 데 동의하는지 여부를 확인하라는 메시지가 표시될 수 있습니다.

Google Analytics 사용에 동의하면 Acronis에서 가명화된 데이터를 수집하여 사용자의 행동을 더욱 정확하게 파악할 수 있으며 Cyber Protect Cloud의 사용자 환경을 개선할 수 있습니다.

Cyber Protect Cloud을(를) 처음 시작할 때 Google Analytics를 활성화했거나 활성화를 거부했더라도 나중에 언제든지 해당 결정을 변경할 수 있습니다.

Google Analytics를 활성화하거나 비활성화하려면

1. Cyber Protect 콘솔에서 **계정 관리**를 클릭합니다.
2. 오른쪽 위에 있는 계정 아이콘을 클릭합니다.
3. **내 개인 정보 보호 설정**을 선택합니다. **내 개인 정보 보호 설정** 창이 표시됩니다.
4. **Google Analytics 데이터 수집** 섹션에서 다음 버튼 중 하나를 클릭합니다.
   - Google Analytics를 활성화하려면 **켜기**를 클릭합니다.
   - Google Analytics를 비활성화하려면 **끄기**를 클릭합니다.

쿠키 삭제 방법 섹션의 설정을 사용하면 브라우저에서 직접 쿠키를 제어하고 관리할 수 있습니다.

참고
Google Analytics 섹션이 표시되지 않으면 해당 국가에서는 Google Analytics가 사용되지 않는 것입니다.

평가 기간 동안 처음 표시되는 **제품 내 온보딩 및 대화식 도움말** 섹션에서 향후 프로그램의 새 기능 및 개선 기능 관련 정보를 더 이상 수신하지 않거나 계속 수신하도록 설정할 수 있습니다. 이 기능은 기본적으로 활성화되어 있지만 토글을 **끄기**로 전환하여 비활성화할 수 있습니다.

Cyber Protection 서비스 액세스

계정을 활성화한 후 Cyber Protect 콘솔에 로그인하거나 관리 포털을 통해 Cyber Protection 서비스에 액세스할 수 있습니다.

Cyber Protect 콘솔에 로그인하려면

© Acronis International GmbH, 2003-2024

1. Cyber Protection 서비스 로그인 페이지로 이동합니다.
2. 로그인 정보를 입력하고 **다음**을 클릭합니다.
3. 비밀번호 정보를 입력하고 **다음**을 클릭합니다.
4. [Cyber Protect Cloud 서비스를 둘 이상 사용하는 경우] **사이버 보호**를 클릭합니다.
   Cyber Protection 서비스에만 액세스할 수 있는 사용자는 바로 Cyber Protect 콘솔에 로그인합니다.

   Cyber Protection 이외의 서비스에도 액세스할 수 있는 경우 오른쪽 위의 아이콘을 사용하여 서비스를 전환할 수 있습니다. 또한 관리자는 이 아이콘을 이용하여 관리 포털을 전환할 수 있습니다.

Cyber Protect 콘솔의 시간 초과 기간은 활성 세션에 대해 24시간, 유휴 세션에 대해 1시간입니다.

오른쪽 위의 계정 아이콘을 클릭하여 웹 인터페이스 언어를 변경할 수 있습니다.

관리 포털을 통해 Cyber Protect 콘솔에 액세스하려면

1. 관리 포털에서 **모니터링** > **사용**으로 이동합니다.
2. **Cyber Protect**에서 **보호**를 선택하고 **서비스 관리**를 클릭합니다.
   또는 **클라이언트**에서 고객을 선택하고 **서비스 관리**를 클릭합니다.

그러면 Cyber Protect 콘솔로 리디렉션됩니다.

중요
관리 모드가 **셀프 서비스**인 고객의 서비스는 관리할 수 없습니다. 고객 관리자만 고객 모드를 **서비스 제공업체가 관리**로 변경한 후 서비스를 관리할 수 있습니다.

패스워드를 재설정하려면

1. Cyber Protection 서비스 로그인 페이지로 이동합니다.
2. 로그인 정보를 입력하고 **다음**을 클릭합니다.
3. **패스워드를 잊으셨습니까?**를 클릭합니다.
4. **전송**을 클릭해 추가 지침을 진행하는 것을 확인합니다.
5. 수신한 이메일에 기재된 지침을 따릅니다.
6. 새 패스워드를 설정합니다.

소프트웨어 요구 사항

지원되는 웹 브라우저

Cyber Protect 콘솔은 TLS 1.2 프로토콜을 사용하며 다음 웹 브라우저를 지원합니다:

- Google Chrome 29 이상 버전
- Mozilla Firefox 23 이상 버전
- Opera 16 이상 버전

© Acronis International GmbH, 2003-2024

- Microsoft Edge 25 이상 버전
- macOS 및 iOS 운영 체제에서 실행되는 Safari 8 이상

다른 웹 브라우저(다른 운영 체제에서 실행 중인 Safari 포함)에서는 사용자 인터페이스가 제대로 표시되지 않거나 일부 기능을 사용하지 못할 수 있습니다.

지원되는 운영 체제 및 환경

Agent for Windows

이 에이전트에는 바이러스 백신 및 맬웨어 방지와 URL 필터링용 컴퍼넌트가 포함되어 있습니다. 운영 체제별로 지원되는 기능에 대한 자세한 내용은 "운영 체제별 지원되는 보호 기능"(41페이지)을(를) 참조하십시오.

- Windows XP Professional SP1(x64), SP2(x64), SP3(x86)
- Windows Server 2003 SP1/2003 R2 이상 – Standard 및 Enterprise 에디션(x86, x64)
- Windows Small Business Server 2003/2003 R2
- Windows Server 2008, Windows Server 2008 SP2* – Standard, Enterprise, Datacenter, Foundation 및 Web 버전(x86, x64)
- Windows Small Business Server 2008, Windows Small Business Server 2008 SP2*
- Windows 7 – 모든 버전

참고

Windows 7에서 Cyber Protection을(를) 사용하려면 Protection 에이전트를 설치하기 전에 Microsoft의 다음 업데이트를 설치해야 합니다.

- Windows 7 ESU(확장 보안 업데이트)
- KB4474419
- KB4490628

필요한 업데이트에 대한 자세한 내용은 이 지식 베이스 문서를 참조하십시오.

- Windows Server 2008 R2* - Standard, Enterprise, Datacenter, Foundation 및 Web 에디션
- Windows Home Server 2011*
- Windows MultiPoint Server 2010*/2011*/2012
- Windows Small Business Server 2011* - 모든 에디션
- Windows 8/8.1 – Windows RT 버전을 제외한 모든 버전(x86, x64)
- Windows Server 2012/2012 R2 – 모든 버전
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows 10 – Home, Pro, Education, Enterprise, IoT Enterprise 및 LTSC(이전 LTSB) 에디션
- Windows Server 2016 – Nano Server를 제외한 모든 설치 옵션
- Windows Server 2019 – Nano Server를 제외한 모든 설치 옵션
- Windows 11 – 모든 버전
- Windows Server 2022 – Nano Server를 제외한 모든 설치 옵션

© Acronis International GmbH, 2003-2024

참고

* 이 버전의 Windows에서 Cyber Protection을(를) 사용하려면 Protection 에이전트를 설치하기 전에 Microsoft(KB4474419)의 SHA2 코드 서명 지원 업데이트를 설치해야 합니다.

SHA2 코드 서명 지원 업데이트와 관련된 문제는 이 기술 자료 문서를 참조하십시오.

Agent for SQL, Agent for Active Directory, Agent for Exchange(데이터베이스 백업 및 애플리케이션 인식 백업용)

이러한 각각의 에이전트는 위에 나열된 모든 운영 체제와 각 애플리케이션의 지원 버전을 실행하는 머신에 설치할 수 있습니다.

Data Loss Prevention용 에이전트

장치 제어

- Microsoft Windows 7 서비스 팩 1 이상
- Microsoft Windows Server 2008 R2 이상
- macOS 10.15 (Catalina)
- macOS 11.2.3(Big Sur)
- macOS 12 (Monterey)
- macOS 13 (Ventura)

참고

MacOS용 데이터 손실 방지 에이전트는 x64 프로세서만 지원합니다. Apple 실리콘 ARM 기반 프로세서는 지원되지 않습니다.

데이터 손실 방지

- Microsoft Windows 7 서비스 팩 1 이상
- Microsoft Windows Server 2008 R2 이상

참고

데이터 손실 방지 에이젠트는 Mac 에이전트의 필수적인 부분이기 때문에 비지원 macOS 시스템 상에 설치될 수 있습니다. 이 경우 컴퓨터에 데이터 손실 방지 에이전트가 설치되어 있다는 사실이 Cyber Protect 콘솔을 통해 표시되지만, 장치 제어 및 데이터 손실 방지 기능은 작동하지 않습니다. 장치 제어 기능은 데이터 손실 방지 에이전트가 지원하는 macOS 시스템 상에서만 작동합니다.

Agent for Advanced Data Loss Prevention

- Microsoft Windows 7 서비스 팩 1 이상
- Microsoft Windows Server 2008 R2 이상

© Acronis International GmbH, 2003-2024

Agent for File Sync & Share

지원되는 운영 체제 목록은 Cyber Files Cloud 사용자 안내서를 참조하십시오.

Agent for Exchange(사서함 백업용)

- Windows Server 2008 – Standard, Enterprise, Datacenter, Foundation 및 Web 버전(x86, x64)
- Windows Small Business Server 2008
- Windows 7 – 모든 버전
- Windows Server 2008 R2 – Standard, Enterprise, Datacenter, Foundation 및 Web 버전
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – 모든 버전
- Windows 8/8.1 – Windows RT 버전을 제외한 모든 버전(x86, x64)
- Windows Server 2012/2012 R2 – 모든 버전
- Windows Storage Server 2008/2008 R2/2012/2012 R2
- Windows 10 – Home, Pro, Education 및 Enterprise 버전
- Windows Server 2016 – Nano Server를 제외한 모든 설치 옵션
- Windows Server 2019 – Nano Server를 제외한 모든 설치 옵션
- Windows 11 – 모든 버전
- Windows Server 2022 – Nano Server를 제외한 모든 설치 옵션

Agent for Microsoft 365

- Windows Server 2008 – Standard, Enterprise, Datacenter, Foundation 및 Web 버전(x64 전용)
- Windows Small Business Server 2008
- Windows Server 2008 R2 – Standard, Enterprise, Datacenter, Foundation 및 Web 에디션
- Windows Home Server 2011
- Windows Small Business Server 2011 – 모든 버전
- Windows 8/8.1 – Windows RT 버전을 제외한 모든 버전(x64 전용)
- Windows Server 2012/2012 R2 – 모든 버전
- Windows Storage Server 2008/2008 R2/2012/2012 R2/2016(x64 전용)
- Windows 10 – Home, Pro, Education 및 Enterprise 버전(x64 전용)
- Windows Server 2016 – Nano Server를 제외한 모든 설치 옵션(x64 전용)
- Windows Server 2019 – Nano Server를 제외한 모든 설치 옵션(x64 전용)
- Windows 11 – 모든 버전
- Windows Server 2022 – Nano Server를 제외한 모든 설치 옵션

Agent for Oracle

- Windows Server 2008R2 – Standard, Enterprise, Datacenter 및 Web 버전(x86, x64)
- Windows Server 2012R2 – Standard, Enterprise, Datacenter 및 Web 버전(x86, x64)
- Linux – Agent for Linux가 지원하는 커널 및 배포(아래 나열)

© Acronis International GmbH, 2003-2024

Agent for MySQL/MariaDB

- Linux – Agent for Linux가 지원하는 커널 및 배포(아래 나열)

Agent for Linux

이 에이전트에는 바이러스 백신 및 맬웨어 방지와 URL 필터링용 컴퍼넌트가 포함되어 있습니다. 운영 체제별로 지원되는 기능에 대한 자세한 내용은 "운영 체제별 지원되는 보호 기능"(41페이지)을(를) 참조하십시오.

테스트가 완료된 Linux 배포판 및 커널 버전은 다음과 같습니다. 그러나 사용 중인 Linux 배포판이나 커널 버전이 아래 목록에 없더라도 Linux 운영 체제의 특성상 모든 필수 시나리오에서 해당 배포판이나 버전이 정상 작동할 수도 있습니다.

사용 중인 Linux 배포판 및 커널 버전 조합과 함께 Cyber Protection 사용 시 문제가 발생하면 지원팀에 추가 조사를 요청하십시오.

커널이 2.6.9~5.19 버전이고 glibc가 2.3.4 이상 버전인 Linux(다음 x86 및 x86_64 배포판 포함):

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04, 22.10, 23.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 37, 38
- SUSE Linux Enterprise Server 10, 11, 12, 15

중요
USE Linux Enterprise Server 12 및 SUSE Linux Enterprise Server 15에서는 Btrfs가 포함된 구성이 지원되지 않습니다.

- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10, 11
- CentOS 5.x, 6.x, 7.x, 8.x*
- CentOS Stream 8*, 9*
- Oracle Linux 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2* – Unbreakable Enterprise Kernel 및 Red Hat Compatible Kernel 모두

참고
보안 부팅이 활성화된 Oracle Linux 8.6 이상 버전에 보호 에이전트를 설치하려면 커널 모듈에 수동으로 서명을 해야 합니다.커널 모듈에 서명을 하는 방법에 대한 자세한 내용은 이 기술 자료 문서를 참조하십시오.

- CloudLinux 5.x, 6.x, 7.x, 8.x*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.x*,9.0*, 9.1*, 9.2*

© Acronis International GmbH, 2003-2024

- Rocky Linux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- ALT Linux 7.0

  * 버전 8.4부터는 커널 4.18에서 5.19까지만 지원됩니다.

Agent for Mac

이 에이전트에는 바이러스 백신 및 맬웨어 방지와 URL 필터링용 컴퍼넌트가 포함되어 있습니다. 운영 체제별로 지원되는 기능에 대한 자세한 내용은 "운영 체제별 지원되는 보호 기능"(41페이지)을(를) 참조하십시오.

x64 및 ARM 아키텍처(Apple M1, M2 등의 Apple 실리콘 프로세서에 사용됨)가 모두 지원됩니다.

참고
Intel 기반 Mac의 디스크 수준 백업을 Apple 실리콘 프로세서를 사용하는 Mac에 복구할 수는 없으며, 그 반대 방향의 복구도 불가능합니다. 파일과 폴더를 복구할 수 있습니다.

- macOS High Sierra 10.13
- macOS Mojave 10.14
- macOS Catalina 10.15
- macOS Big Sur 11
- macOS Monterey 12
- macOS Ventura 13
- macOS Sonoma 14

중요
Cyber Protect Cloud의 C23.07 이상 버전에서는 OS X Yosemite 10.10, OS X El Capitan 10.11, macOS Sierra 10.12 운영 체제가 지원되지 않습니다.

Cyber Protect Cloud의 모든 기능을 사용하고 호환성을 유지하려면 운영 체제를 지원되는 버전으로 업그레이드하는 것이 좋습니다.

Agent for VMware(가상 어플라이언스)

이 에이전트는 ESXi 호스트에서 실행되는 가상 어플라이언스로 제공됩니다.

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0

Agent for VMware(Windows)

이 에이전트는 Agent for Windows에 대해 위에 나열된 모든 운영 체제에서 실행할 수 있도록 Windows 애플리케이션으로 제공됩니다. 단, 다음과 같은 예외가 적용됩니다.

- 32비트 운영 체제는 지원되지 않습니다.
- Windows XP, Windows Server 2003/2003 R2, Windows Small Business Server 2003/2003 R2는 지원되지 않습니다.

© Acronis International GmbH, 2003-2024

Agent for Hyper-V

- Windows Server 2008 with Hyper-V role(x64 전용), Server Core 설치 모드 포함
- Windows Server 2008 R2 with Hyper-V role, Server Core 설치 모드 포함
- Microsoft Hyper-V Server 2008/2008 R2
- Windows Server 2012/2012 R2 with Hyper-V role, Server Core 설치 모드 포함
- Microsoft Hyper-V Server 2012/2012 R2
- Windows 8, 8.1 with Hyper-V(x64 전용)
- Windows 10 – Pro, Education 및 Enterprise 버전(Hyper-V 포함)
- Windows Server 2016 with Hyper-V role – Nano Server를 제외한 모든 설치 옵션
- Microsoft Hyper-V Server 2016
- Windows Server 2019 with Hyper-V role – Nano Server를 제외한 모든 설치 옵션
- Microsoft Hyper-V Server 2019
- Windows Server 2022 – Nano Server를 제외한 모든 설치 옵션

Agent for Virtuozzo

- Virtuozzo 6.0.10, 6.0.11, 6.0.12, 7.0.13, 7.0.14
- Virtuozzo Hybrid Server 7.5

Agent for Virtuozzo Hybrid Infrastructure

Virtuozzo Hybrid Infrastructure 3.5, 4.0, 4.5, 4.6, 4.7, 5.0, 5.1, 5.2, 5.3, 5.4, 6.0

Agent for Scale Computing HC3

Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3

Agent for oVirt

Red Hat Virtualization 4.2, 4.3, 4.4, 4.5

Agent for Synology

DiskStation Manager 6.2.x, 7.x

Agent for Synology는 x86_64 프로세서가 장착된 NAS 장치만 지원합니다. ARM 프로세서는 지원되지 않습니다.

Cyber Protect 모니터

- Windows 7 이상
- Windows Server 2008 R2 이상
- Agent for Mac에서 지원하는 모든 macOS 버전

© Acronis International GmbH, 2003-2024

지원되는 Microsoft SQL Server 버전

- Microsoft SQL Server 2022
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

상기한 SQL Server 버전의 SQL Server Express 버전도 지원됩니다.

참고
Microsoft SQL 백업은 NTFS, REFS, FAT32 파일 시스템에서 실행되는 데이터베이스에서만 지원됩니다. ExFat는 지원되지 않습니다.

지원되는 Microsoft Exchange Server 버전

- Microsoft Exchange Server 2019 – 모든 버전.
- Microsoft Exchange Server 2016 – 모든 버전.
- Microsoft Exchange Server 2013 – 모든 버전, CU1(누적 업데이트 1) 이상
- Microsoft Exchange Server 2010 – 모든 버전, 모든 서비스 팩. 사서함 백업 및 데이터베이스 백업에서 개별 복구는 SP1(서비스 팩 1)부터 지원됩니다.
- Microsoft Exchange Server 2007 – 모든 버전, 모든 서비스 팩. 사서함 백업 및 데이터베이스 백업에서 개별 복구는 지원되지 않습니다.

지원되는 Microsoft SharePoint 버전

Cyber Protection에서는 다음 Microsoft SharePoint 버전을 지원합니다.

- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1
- Microsoft SharePoint Foundation 2010 SP1
- Microsoft Office SharePoint Server 2007 SP2*
- Microsoft Windows SharePoint Services 3.0 SP2*

*이러한 버전으로 SharePoint Explorer를 사용하려면 데이터베이스를 연결할 SharePoint 복구 팜이 필요합니다.

데이터를 추출한 곳에서 가져온 백업이나 데이터베이스는 SharePoint Explorer가 설치된 곳과 동일한 버전의 SharePoint에서 생성된 것이어야 합니다.

© Acronis International GmbH, 2003-2024

지원되는 Oracle 데이터베이스 버전

- Oracle 데이터베이스 버전 11g, 모든 버전
- Oracle 데이터베이스 버전 12c, 모든 버전
- Oracle 데이터베이스 버전 19c, 모든 버전
- Oracle 데이터베이스 버전 21c, 모든 버전

단일 인스턴스 구성만 지원됩니다.

지원되는 SAP HANA 버전

실제 머신 또는 VMware ESXi 가상 머신에서 실행되는 RHEL 7.6에 HANA 2.0 SPS 03이 설치되었습니다.

SAP HANA는 스토리지 스냅샷을 사용한 멀티네턴트 데이터베이스 컨테이너의 복구를 지원하지 않으므로 이 솔루션은 하나의 테넌트 데이터베이스만 있는 SAP HANA 컨테이너를 지원합니다.

지원되는 MySQL 버전

- 5.5.x – Community Server, Enterprise, Standard, Classic 에디션
- 5.6.x – Community Server, Enterprise, Standard, Classic 에디션
- 5.7.x – Community Server, Enterprise, Standard, Classic 에디션
- 8.0.x – Community Server, Enterprise, Standard, Classic 에디션

지원되는 MariaDB 버전

- 10.0.x
- 10.1.x
- 10.2.x
- 10.3.x
- 10.4.x
- 10.5.x
- 10.6.x
- 10.7.x

지원되는 가상화 플랫폼

다음 표에는 다양한 가상화 플랫폼이 지원되는 방법이 요약되어 있습니다.

에이전트 기반 백업과 에이전트 없는 백업 간의 차이점에 대한 자세한 내용은 "에이전트 기반 백업 및 비에이전트 백업"(61페이지) 항목을 참조하십시오.

© Acronis International GmbH, 2003-2024

참고

아래에 나와 있지 않은 가상화 플랫폼이나 버전을 사용하더라도 모든 필수 시나리오에서 **에이전트 기반 백업(게스트 OS 내의 백업)** 방법이 정상 작동할 수 있습니다. 에이전트 기반 백업 시에 문제가 발생하면 지원 팀에 추가 조사를 요청하십시오.

VMware

플랫폼	비에이전트 백업 (하이퍼바이저 수준에서 백업)	에이전트 기반 백업 (게스트 OS 내에서 백업)
VMware vSphere 버전: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0 **VMware vSphere 버전:** VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	지원 **장치** > **추가** > **가상화 호스트** > **VMware ESXi** > **Windows에 설치할 에이전트** 또는 **장치** > **추가** > **가상화 호스트** > **VMware ESXi** > **가상 어플라이언스(OVF)**	지원 **장치** > **추가** > **워크스테이션** 또는 **서버** > **Windows** 또는 **Linux**
VMware vSphere Hypervisor(Free ESXi)**	지원되지 않음	지원 **장치** > **추가** > **워크스테이션** 또는 **서버** > **Windows** 또는 **Linux**
VMware Server(VMware Virtual 서버) VMware Workstation VMware ACE VMware Player	지원되지 않음	지원 **장치** > **추가** > **워크스테이션** 또는 **서버** > **Windows** 또는 **Linux**

* 이러한 버전의 경우 vSphere 5.0 이상에서 가상 디스크의 HotAdd 전송이 지원됩니다.버전 4.1에서는 백업 실행 속도가 느릴 수 있습니다.

** 이 제품은 RCLI(Remote Command Line Interface)에 대한 액세스가 읽기 전용 모드로 제한되기 때문에 vSphere Hypervisor에 대해 하이퍼바이저 수준의 백업은 지원되지 않습니다. 에이전트는 시리얼 키를 입력하지 않은 상태로 vSphere Hypervisor 평가 기간 동안 작동합니다. 시리얼 키를 입력하면 에이전트가 작동을 멈춥니다.

© Acronis International GmbH, 2003-2024

참고
Cyber Protect Cloud에서는 지원되는 vSphere 주 버전 내의 모든 업데이트가 공식적으로 지원됩니다.

예를 들어 업데이트 미지원이 특별히 명시된 경우가 아니면 vSphere 8.0 지원에는 해당 버전 내의 모든 업데이트가 지원 대상으로 포함됩니다. 즉, 원래 출시된 vSphere 8.0과 함께 vSphere 8.0 업데이트 1도 지원됩니다.

특정 VMware vSphere 버전이 지원되는 경우에는 해당 버전의 vSAN도 지원됩니다. 예를 들어 vSphere 8.0이 지원되면 vSAN 8.0도 지원됩니다.

제한 사항

- **내결함성 머신**
  Agent for VMware는 VMware vSphere 6.0 이상에서 내결함성이 활성화된 경우에만 내결함성 머신을 백업합니다.이전 vSphere 버전에서 업그레이드한 경우 각 머신에 대해 내결함성을 비활성화하고 활성화하기에 충분합니다. 이전 버전의 vSphere를 사용하는 경우 게스트 운영 체제에 에이전트를 설치하십시오.
- **독립형 디스크 및 RDM**
  Agent for VMware는 물리적 호환성 모드 또는 독립형 디스크에서 RDM(Raw Device Mapping) 디스크를 백업하지 않습니다. 에이전트는 이러한 디스크를 건너뛰며 로그에 경고를 추가합니다. 실제 호환성 모드의 독립형 디스크와 RDM을 보호 계획에서 제외하면 경고를 방지할 수 있습니다. 이러한 디스크 또는 이러한 디스크의 데이터를 백업하려면 게스트 운영 체제에 에이전트를 설치합니다.
- **게스트 iSCSI 연결**
  Agent for VMware는 게스트 운영 체제 내에서 작동하는 iSCSI 시작자에 의해 연결된 LUN 볼륨을 백업하지 않습니다. ESXi 하이퍼바이저는 이러한 볼륨을 인식하지 않으므로 해당 볼륨은 하이퍼바이저 수준 스냅샷에 포함되지 않으며 경고 없이 백업에서 제외됩니다. 이러한 볼륨 또는 이러한 볼륨의 데이터를 백업하려면 게스트 운영 체제에 에이전트를 설치합니다.
- **암호화된 가상 머신**(VMware vSphere 6.5에서 소개)
  - 암호화된 가상 머신을 암호화하지 않은 상태로 백업할 수 있습니다. 암호화가 반드시 필요한 경우 보호 계획을 생성할 때 백업 암호화를 활성화합니다.
  - 복구된 가상 머신은 항상 암호 해제됩니다. 복구가 완료된 후에는 수동으로 암호화를 활성화할 수 있습니다.
  - 암호화된 가상 머신을 백업하는 경우 Agent for VMware이 실행 중인 가상 머신도 암호화하는 것이 좋습니다. 그렇지 않으면 암호화된 머신의 작업이 예상보다 느려질 수 있습니다. VSphere Web Client를 사용하여 에이전트의 머신에 **VM 암호화 정책**을 적용하십시오.
  - 에이전트에 대해 SAN 전송 모드를 구성하더라도 암호화된 가상 머신은 LAN을 통해 백업됩니다. VMware가 암호화된 가상 디스크 백업에 SAN 전송을 지원하지 않기 때문에 에이전트가 NBD 전송으로 폴백합니다.
- **보안 부팅**
  - VMware 가상 머신: (VMware vSphere 6.5에 도입됨) 가상 머신이 새 가상 머신으로 복구되면 **보안 부팅**은 비활성화됩니다. 복구가 완료된 후에는 수동으로 이 옵션을 활성화할 수 있습니

© Acronis International GmbH, 2003-2024

다. 이 제한은 VMware에 적용됩니다.
  - Hyper-V 가상 머신: 모든 GEN2 VM의 경우, 가상 머신이 새 가상 머신이나 다른 기존 가상 머신으로 복구되면 보안 부팅은 비활성화됩니다.
- **ESXi 구성 백업**은 VMware vSphere 7.0에 대해 지원되지 않습니다.
- **논리 볼륨이 있는 머신에서 지원되는 작업**

  Windows의 LDM(동적 디스크), Linux의 LVM과 같은 논리 볼륨이 포함된 워크로드의 백업 및 복구가 지원되며 몇 가지 제한이 적용됩니다. 해당 제한에 대한 자세한 내용은 "논리 볼륨에서 지원되는 작업"(53페이지) 항목을 참조하십시오.

Microsoft

플랫폼	비에이전트 백업 (하이퍼바이저 수준에서 백업)	에이전트 기반 백업 (게스트 OS 내에서 백업)
Windows Server 2008(x64) with Hyper-V Windows Server 2008 R2(Hyper-V 사용) Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2 (Hyper-V 사용) Microsoft Hyper-V Server 2012/2012 R2 Windows 8, 8.1(x64)(Hyper-V 사용) Windows 10(Hyper-V 사용) Windows Server 2016(Hyper-V 사용) – Nano Server를 제외한 모든 설치 옵션 Microsoft Hyper-V Server 2016 Windows Server 2019(Hyper-V 사용) – Nano Server를 제외한 모든 설치 옵션 Microsoft Hyper-V Server 2019 Windows Server 2022(Hyper-V 사용) – Nano Server를 제외한 모든 설치 옵션	지원 **장치** > **추가** > **가상화 호스트** > **Hyper-V**	지원 **장치** > **추가** > **워크스테이션** 또는 **서버** > **Windows** 또는 **Linux**
Microsoft Virtual PC 2004, 2007 Windows Virtual PC	지원되지 않음	지원 **장치** > **추가** > **워크스테이션** 또는 **서버** > **Windows** 또는 **Linux**

© Acronis International GmbH, 2003-2024

플랫폼	비에이전트 백업 (하이퍼바이저 수준에서 백업)	에이전트 기반 백업 (게스트 OS 내에서 백업)
Microsoft Virtual Server 2005	지원되지 않음	지원 **장치** > **추가** > **워크스테이션** 또는 **서버** > **Windows** 또는 **Linux**

참고
S2D(Storage Spaces Direct)를 사용하는 하이퍼 컨버지드 클러스터에서 실행 중인 Hyper-V 가상 머신이 지원됩니다. Storage Spaces Direct는 백업 스토리지로도 지원됩니다.

제한 사항

- **패스스루 디스크**
  Agent for Hyper-V는 패스스루 디스크를 백업하지 않습니다. 백업 동안 에이전트는 이러한 디스크를 건너뛰며 로그에 경고를 추가합니다. 보호 계획에서 패스스루 디스크를 제외하면 경고를 방지할 수 있습니다. 이러한 디스크 또는 이러한 디스크의 데이터를 백업하려면 게스트 운영 체제에 에이전트를 설치합니다.
- **Hyper-V 게스트 클러스터링**
  Agent for Hyper-V는 Windows Server 장애 조치 클러스터의 노드인 Hyper-V 가상 머신의 백업을 지원하지 않습니다. 호스트 수준의 VSS 스냅샷은 클러스터로부터 외부 쿼럼(quorum) 디스크를 일시적으로 분리할 수도 있습니다. 이러한 머신을 백업하려면 게스트 운영 체제에 에이전트를 설치하십시오.
- **게스트 iSCSI 연결**
  Agent for Hyper-V는 게스트 운영 체제 내에서 작동하는 iSCSI 시작자에 의해 연결된 LUN 볼륨을 백업하지 않습니다. Hyper-V 하이퍼바이저는 이러한 볼륨을 인식하지 않으므로 해당 볼륨은 하이퍼바이저 수준 스냅샷에 포함되지 않으며 경고 없이 백업에서 제외됩니다. 이러한 볼륨 또는 이러한 볼륨의 데이터를 백업하려면 게스트 운영 체제에 에이전트를 설치합니다.
- **보안 부팅**
  모든 GEN2 VM의 경우, 가상 머신이 새 가상 머신이나 다른 기존 가상 머신으로 복구되면 보안 부팅은 비활성화됩니다.
- **논리 볼륨이 있는 머신에서 지원되는 작업**
  Windows의 LDM(동적 디스크), Linux의 LVM과 같은 논리 볼륨이 포함된 워크로드의 백업 및 복구가 지원되며 몇 가지 제한이 적용됩니다. 해당 제한에 대한 자세한 내용은 "논리 볼륨에서 지원되는 작업"(53페이지) 항목을 참조하십시오.
- **앰퍼샌드 기호가 있는 VHD/VHDX 파일 이름**
  원래 Hyper-V 2012 R2 이하 버전으로 생성했던 레거시 가상 머신(버전 5.0)의 VHD/VHDX 파일 이름에 앰퍼샌드 기호(&)가 포함되어 있으면 Windows Server 2016 이상을 실행 중인 Hyper-V 호스트에서 이러한 가상 머신을 백업할 수 없습니다.
  이러한 머신을 백업하려면 Hyper-V Manager에서 해당 가상 디스크를 가상 머신에서 분리하고, 앰퍼샌드 기호를 제거하여 VHD/VHDX 파일 이름을 편집한 후 가상 머신에 디스크를 다시 연결합니다.

© Acronis International GmbH, 2003-2024

- **Microsoft WMI 하위 시스템에 대한 종속성**
  비에이전트 백업의 Hyper-V 가상 머신은 Microsoft WMI 하위 시스템, 특히 `Msvm_VirtualSystemManagementService` 클래스에 따라 달라집니다. WMI 쿼리에 실패하는 경우 백업도 실패할 것입니다. `Msvm_VirtualSystemManagementService` 클래스에 대한 자세한 정보는 Microsoft 설명서를 참조하십시오.

Scale Computing

플랫폼	비에이전트 백업 (하이퍼바이저 수준에서 백업)	에이전트 기반 백업 (게스트 OS 내에서 백업)
Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3	지원 **장치** > **추가** > **가상화 호스트** > **Scale Computing HC3**	지원 **장치** > **추가** > **워크스테이션** 또는 **서버** > **Windows** 또는 **Linux**

제한 사항

논리 볼륨이 있는 머신에서 지원되는 작업

Windows의 LDM(동적 디스크), Linux의 LVM과 같은 논리 볼륨이 포함된 워크로드의 백업 및 복구가 지원되며 몇 가지 제한이 적용됩니다. 해당 제한에 대한 자세한 내용은 "논리 볼륨에서 지원되는 작업"(53페이지) 항목을 참조하십시오.

Citrix

플랫폼	비에이전트 백업 (하이퍼바이저 수준에서 백업)	에이전트 기반 백업 (게스트 OS 내에서 백업)
Citrix XenServer/Citrix Hypervisor 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 8.0, 8.1, 8.2	지원되지 않음	완전 가상화된(즉, HVM) 게스트에서만 지원됩니다. 반가상화된(즉, PV) 게스트는 지원되지 않음. **장치** > **추가** > **가상화 호스트** > **Citrix XenServer** > **Windows** 또는 **Linux**

Red Hat 및 Linux

플랫폼	비에이전트 백업 (하이퍼바이저 수준에서 백업)	에이전트 기반 백업 (게스트 OS 내에서 백업)
Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 Red Hat Virtualization (RHV) 4.0, 4.1	지원되지 않음	지원 **장치** > **추가** > **워크스테이션** 또는 **서버** > **Windows** 또는 **Linux**

© Acronis International GmbH, 2003-2024

플랫폼	비에이전트 백업 (하이퍼바이저 수준에서 백업)	에이전트 기반 백업 (게스트 OS 내에서 백업)
Red Hat Virtualization(oVirt를 통해 관리됨) 4.2, 4.3, 4.4, 4.5	지원 **장치** > **추가** > **가상화 호스트** > **Red Hat Virtualization(oVirt)**	지원 **장치** > **추가** > **워크스테이션** 또는 **서버** > **Windows** 또는 **Linux**
커널 기반 가상 머신(KVM)	지원되지 않음	지원 **장치** > **추가** > **KVM** > **Windows** 또는 **Linux**
커널 기반 가상 머신(KVM)은 Red Hat Enterprise Linux 7.6, 7.7 또는 CentOS 7.6, 7.7에서 실행되는 oVirt 4.3에 의해 관리됩니다	지원 **장치** > **추가** > **가상화 호스트** > **Red Hat Virtualization(oVirt)**	지원 **장치** > **추가** > **워크스테이션** 또는 **서버** > **Windows** 또는 **Linux**
커널 기반 가상 머신(KVM)은 Red Hat Enterprise Linux 8.x 또는 CentOS Stream 8.x에서 실행되는 oVirt 4.4에 의해 관리됩니다	지원 **장치** > **추가** > **가상화 호스트** > **Red Hat Virtualization(oVirt)**	지원 **장치** > **추가** > **워크스테이션** 또는 **서버** > **Windows** 또는 **Linux**
커널 기반 가상 머신(KVM)은 Red Hat Enterprise Linux 8.x 또는 CentOS Stream 8.x에서 실행되는 oVirt 4.5에 의해 관리됩니다.	지원 **장치** > **추가** > **가상화 호스트** > **Red Hat Virtualization(oVirt)**	지원 **장치** > **추가** > **워크스테이션** 또는 **서버** > **Windows** 또는 **Linux**

제한 사항

논리 볼륨이 있는 머신에서 지원되는 작업

Windows의 LDM(동적 디스크), Linux의 LVM과 같은 논리 볼륨이 포함된 워크로드의 백업 및 복구가 지원되며 몇 가지 제한이 적용됩니다. 해당 제한에 대한 자세한 내용은 "논리 볼륨에서 지원되는 작업"(53페이지) 항목을 참조하십시오.

Parallels

플랫폼	비에이전트 백업 (하이퍼바이저 수준에서 백업)	에이전트 기반 백업 (게스트 OS 내에서 백업)
Parallels Workstation	지원되지 않음	지원 **장치** > **추가** > **워크스테이션** 또는 **서버** > **Windows** 또는 **Linux**
Parallels Server 4 Bare Metal	지원되지 않음	지원 **장치** > **추가** > **워크스테이션** 또는 **서버** > **Windows** 또는 **Linux**

© Acronis International GmbH, 2003-2024

Oracle

플랫폼	비에이전트 백업 (하이퍼바이저 수준에서 백업)	에이전트 기반 백업 (게스트 OS 내에서 백업)
Oracle Virtualization Manager (oVirt 기반)* 4.3	지원 **장치** > **추가** > **가상화 호스트** > **Red Hat Virtualization(oVirt)**	지원 **장치** > **추가** > **워크스테이션** 또는 **서버** > **Windows** 또는 **Linux**
Oracle VM Server 3.0, 3.3, 3.4	지원되지 않음	완전 가상화된(즉, HVM) 게스트에서만 지원됩니다. 반가상화된(즉, PV) 게스트는 지원되지 않음. **장치** > **추가** > **가상화 호스트** > **Oracle** > **Windows** 또는 **Linux**
Oracle VM VirtualBox 4.x	지원되지 않음	지원 **장치** > **추가** > **가상화 호스트** > **Oracle** > **Windows** 또는 **Linux**

*Oracle Virtualization Manager는 Agent for oVirt에서 지원합니다.

제한 사항

논리 볼륨이 있는 머신에서 지원되는 작업

Windows의 LDM(동적 디스크), Linux의 LVM과 같은 논리 볼륨이 포함된 워크로드의 백업 및 복구가 지원되며 몇 가지 제한이 적용됩니다. 해당 제한에 대한 자세한 내용은 "논리 볼륨에서 지원되는 작업"(53페이지) 항목을 참조하십시오.

Nutanix

플랫폼	비에이전트 백업 (하이퍼바이저 수준에서 백업)	에이전트 기반 백업 (게스트 OS 내에서 백업)
Nutanix Acropolis Hypervisor (AHV) 20160925.x ~ 20180425.x	지원되지 않음	지원 **장치** > **추가** > **가상화 호스트** > **Nutanix AHV** > **Windows** 또는 **Linux**

© Acronis International GmbH, 2003-2024

Virtuozzo

플랫폼	비에이전트 백업 (하이퍼바이저 수준에서 백업)	에이전트 기반 백업 (게스트 OS 내에서 백업)
Virtuozzo 6.0.10, 6.0.11, 6.0.12	지원 **장치** > **추가** > **가상화 호스트** > **Virtuozzo**	가상 머신에서만 지원됩니다. 컨테이너는 지원되지 않음. **장치** > **추가** > **워크스테이션** 또는 **서버** > **Windows** 또는 **Linux**
Virtuozzo 7.0.13, 7.0.14	Ploop 컨테이너에서만 지원됩니다. 가상 머신은 지원되지 않음. **장치** > **추가** > **가상화 호스트** > **Virtuozzo**	가상 머신에서만 지원됩니다. 컨테이너는 지원되지 않음. **장치** > **추가** > **워크스테이션** 또는 **서버** > **Windows** 또는 **Linux**
Virtuozzo Hybrid Server 7.5	지원 **장치** > **추가** > **가상화 호스트** > **Virtuozzo**	가상 머신에서만 지원됩니다. 컨테이너는 지원되지 않음. **장치** > **추가** > **워크스테이션** 또는 **서버** > **Windows** 또는 **Linux**

제한 사항

논리 볼륨이 있는 머신에서 지원되는 작업

Windows의 LDM(동적 디스크), Linux의 LVM과 같은 논리 볼륨이 포함된 워크로드의 백업 및 복구가 지원되며 몇 가지 제한이 적용됩니다. 해당 제한에 대한 자세한 내용은 "논리 볼륨에서 지원되는 작업"(53페이지) 항목을 참조하십시오.

Virtuozzo Hybrid Infrastructure

플랫폼	비에이전트 백업 (하이퍼바이저 수준에서 백업)	에이전트 기반 백업 (게스트 OS 내에서 백업)
Virtuozzo Hybrid Infrastructure 3.5, 4.5, 4.6, 4.7, 5.0, 5.1, 5.2, 5.3, 5.4, 6.0	지원 **장치** > **추가** > **가상화 호스트** > **Virtuozzo Hybrid Infrastructure**	지원 **장치** > **추가** > **워크스테이션** 또는 **서버** > **Windows** 또는 **Linux**

제한 사항

- **외부 iSCSI 스토리지에 디스크가 있는 VM의 비에이전트 백업**
  VHI 클러스터에 연결된 외부 iSCSI 볼륨에 VM 디스크가 있으면 Virtuozzo Hybrid Infrastructure에서 VM을 백업할 수 없습니다.
- **논리 볼륨이 있는 머신에서 지원되는 작업**

© Acronis International GmbH, 2003-2024

Windows의 LDM(동적 디스크), Linux의 LVM과 같은 논리 볼륨이 포함된 워크로드의 백업 및 복구가 지원되며 몇 가지 제한이 적용됩니다. 해당 제한에 대한 자세한 내용은 "논리 볼륨에서 지원되는 작업"(53페이지) 항목을 참조하십시오.

Amazon

플랫폼	비에이전트 백업 (하이퍼바이저 수준에서 백업)	에이전트 기반 백업 (게스트 OS 내에서 백업)
Amazon EC2 인스턴스	지원되지 않음	지원 **장치** > **추가** > **워크스테이션** 또는 **서버** > **Windows** 또는 **Linux**

Microsoft Azure

플랫폼	비에이전트 백업 (하이퍼바이저 수준에서 백업)	에이전트 기반 백업 (게스트 OS 내에서 백업)
Azure 가상 머신	지원되지 않음	지원 **장치** > **추가** > **워크스테이션** 또는 **서버** > **Windows** 또는 **Linux**

암호화 소프트웨어와의 호환성

파일 수준 암호화 소프트웨어에서 암호화한 데이터를 백업하고 복구하는 작업에는 제한이 없습니다.

디스크 수준 암호화 소프트웨어는 데이터를 즉시 암호화하므로 백업에 포함된 데이터가 암호화되지 않습니다. 디스크 수준 암호화 소프트웨어는 종종 시스템 영역(부트 레코드, 파티션 테이블 또는 파일 시스템 테이블)을 수정합니다. 이러한 요소는 복구된 시스템이 Secure Zone을 부팅하고 액세스할 수 있는 기능인 디스크 수준 백업 및 복구에 영향을 줍니다.

다음 디스크 수준 암호화 소프트웨어에서 암호화한 데이터를 백업할 수 있습니다.

- Microsoft BitLocker Drive Encryption
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption

안정적인 디스크 수준 복구를 수행하려면 공통 규칙과 소프트웨어 특정 권장 사항을 따릅니다.

공통 설치 규칙

보호 에이전트를 설치하기 전에 암호화 소프트웨어를 설치하는 것이 좋습니다.

© Acronis International GmbH, 2003-2024

Secure Zone 사용 방법

Secure Zone은 디스크 수준 암호화로 암호화해서는 안 됩니다. Secure Zone의 유일한 사용 방법은 다음과 같습니다.

1. 암호화 소프트웨어를 설치한 다음 에이전트를 설치합니다.
2. Secure Zone을 생성합니다.
3. 디스크 또는 그 볼륨을 암호화할 때 Secure Zone을 제외합니다.

공통 백업 규칙

운영 체제에서 디스크 수준 백업을 수행할 수 있습니다.

소프트웨어별 복구 절차

Microsoft BitLocker Drive Encryption

BitLocker로 암호화된 시스템을 복구하려면

1. 부트 가능한 미디어에서 부팅합니다.
2. 시스템을 복구합니다. 복구된 데이터는 암호화되지 않습니다.
3. 복구된 시스템을 재부팅합니다.
4. BitLocker를 켭니다.

멀티 파티션 디스크의 파티션을 하나만 복구해야 하는 경우에는 운영 체제에서 이 작업을 수행합니다. 부트 가능한 미디어에서 복구하면 Windows에서 복구된 파티션을 감지할 수 없습니다.

McAfee Endpoint Encryption 및 PGP Whole Disk Encryption

부트 가능한 미디어만 사용해서 암호화된 시스템 파티션을 복구할 수 있습니다.

복구된 시스템이 부팅에 실패하면 다음의 Microsoft 기술 자료 문서의 설명에 따라 마스터 부트 레코드를 다시 빌드합니다. https://support.microsoft.com/kb/2622803

Dell EMC Data Domain 스토리지와의 호환성

Dell EMC Data Domain 장치를 백업 스토리지로 사용할 수 있습니다.

이 스토리지를 사용할 때는 **항상 전체**와 같이 정기적으로 전체 백업을 생성하는 백업 구성표를 사용하는 것을 권장합니다. 사용 가능한 백업 구성표에 대해 자세히 알아보려면 "백업 구성표"(381페이지)을(를) 참조하십시오.

보관 잠금(거버넌스 모드)이 지원됩니다. 보관 잠금이 활성화된 경우, 이 스토리지를 백업 대상으로 사용하는 보호 에이전트가 있는 머신에 `AR_RETENTION_LOCK_SUPPORT` 환경 변수를 추가해야 합니다.

© Acronis International GmbH, 2003-2024

참고
보존 잠금이 활성화되어 있는 Dell EMC Data Domain 스토리지는 Agent for Mac에서 지원되지 않습니다.

AR_RETENTION_LOCK_SUPPORT 환경 변수 추가 방법

Windows

1. 보호 에이전트가 설치된 머신에 관리자로 로그인합니다.
2. **제어판**에서 **시스템 및 보안** > **시스템** > **고급 시스템 설정**으로 이동합니다.
3. **고급 탭**에서 **환경 변수**를 클릭합니다.
4. **시스템 변수** 패널에서 **새로 만들기**를 클릭합니다.
5. **새 시스템 변수** 창에서 다음과 같이 새 변수를 추가합니다.
   - 변수 이름: AR_RETENTION_LOCK_SUPPORT
   - 변수 값: 1
6. **확인**을 클릭합니다.
7. **환경 변수** 창에서 **확인**을 클릭합니다.
8. 머신을 다시 시작합니다.

Linux

1. 보호 에이전트가 설치된 머신에 관리자로 로그인합니다.
2. /sbin 디렉토리로 이동한 후 편집을 위해 acronis_mms 파일을 엽니다.
3. export LD_LIBRARY_PATH 줄 위에 다음 줄을 추가합니다.

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. acronis_mms 파일을 저장합니다.
5. 머신을 다시 시작합니다.

가상 어플라이언스에서

1. 가상 어플라이언스에 관리자로 로그인합니다.
2. /bin 디렉토리로 이동한 후 편집을 위해 autostart 파일을 엽니다.
3. export LD_LIBRARY_PATH 줄 아래에 다음 줄을 추가합니다.

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. autostart 파일을 저장합니다.
5. 가상 어플라이언스 머신을 다시 시작합니다.

운영 체제별 지원되는 보호 기능

이 항목에는 Cyber Protect Cloud의 보호 기능 관련 정보가 포함되어 있습니다. 백업 및 복구 기능 관련 정보는 제공되지 않습니다.

© Acronis International GmbH, 2003-2024

보호 기능은 보호 에이전트가 설치된 머신에서만 지원됩니다. 예를 들어 Agent for Hyper-V, Agent for VMware, Agent for Virtuozzo Hybrid Infrastructure, Agent for Scale Computing, Agent for oVirt 등의 비에이전트 모드에서 백업되는 가상 머신에는 보호 기능을 사용할 수 없습니다.

일부 기능을 사용하려면 적용되는 라이센스 모델에 따라 추가 라이센스가 필요할 수 있습니다.

지원되는 운영 체제 및 버전

Windows

특정 기능 세트에 대한 별도의 언급이 없으면 다음 Windows 버전이 지원됩니다.

- Windows 7 서비스 팩 1 이상 버전
- Windows Server 2008 R2 서비스 팩 1 이상

참고
Windows 7에서는 보호 에이전트를 설치하기 전에 Microsoft의 다음 업데이트를 설치해야 합니다.

- Windows 7 ESU(확장 보안 업데이트)
- KB4474419
- KB4490628

필요한 업데이트에 대한 자세한 내용은 이 지식 베이스 문서를 참조하십시오.

Linux

지원되는 Linux 배포판과 해당 버전은 기능 세트에 따라 다릅니다. 각 표의 맨 아래에 지원되는 배포판과 버전이 나와 있습니다.

macOS

지원되는 macOS 버전은 기능 세트에 따라 다릅니다. 각 표의 맨 아래에 지원되는 버전이 나와 있습니다.

기능 세트	Windows	Linux	macOS
기본 보호 계획			
원격 작업자	예	아니요	아니요
사무실 작업자(타사 바이러스 백신)	예	아니요	아니요
사무실 작업자(Cyber Protect 안티바이러스)	예	아니요	아니요
Cyber Protect Essentials(Cyber Protect Essentials 버전 전용)	예	아니요	아니요
지원되는 Windows 버전은 "지원되는 운영 체제 및 버전"(42페이지) 항목을 참조하십시오.			

© Acronis International GmbH, 2003-2024

기능 세트	Windows	Linux	macOS
포렌직 백업			
메모리 덤프 수집	예	아니요	아니요
실행 중인 프로세스의 스냅샷	예	아니요	아니요
로컬 이미지 포렌직 백업의 공증	예	아니요	아니요
클라우드 이미지 포렌직 백업의 공증	예	아니요	아니요
지원되는 Windows 버전은 "지원되는 운영 체제 및 버전"(42페이지) 항목을 참조하십시오.			

기능	Windows	Linux	macOS
지속적인 데이터 보호(CDP)			
파일 및 폴더 CDP	예	아니요	아니요
애플리케이션 추적을 통한 변경된 파일 CDP	예	아니요	아니요
지원되는 Windows 버전은 "지원되는 운영 체제 및 버전"(42페이지) 항목을 참조하십시오.			

기능 세트	Windows	Linux	macOS
자동 검색 및 원격 설치			
네트워크 기반 검색	예	아니요	아니요
Active Directory 기반 검색	예	아니요	아니요
템플릿 기반 검색(파일에서 머신 가져오기)	예	아니요	아니요
수동 장치 추가	예	아니요	아니요
지원되는 Windows 버전은 "지원되는 운영 체제 및 버전"(42페이지) 항목을 참조하십시오.			

기능 세트	Windows	Linux	macOS
Active Protection			
프로세스 주입 감지	예	아니요	아니요
로컬 캐시에서 영향을 받는 파일 자동 복구	예	예	예
Acronis 백업 파일의 자체 보호	예	아니요	아니요
Acronis 소프트웨어 자체 보호	예	아니요	예 (Active

© Acronis International GmbH, 2003-2024

기능 세트	Windows	Linux	macOS
Active Protection			
			Protection 및 안티맬웨어 컴퍼넌트만 해당)
신뢰할 수 있는/차단된 프로세스 관리	예	아니요	예
프로세스/폴더 제외	예	예	예
프로세스 동작 기반(AI 기반) 랜섬웨어 감지	예	예	예
프로세스 동작 기반 크립토마이닝 프로세스 감지됨	예	아니요	아니요
외장 드라이브 보호(HDD, 플래시 드라이브, SD 카드)	예	아니요	예
네트워크 폴더 보호	예	예	예
서버측 보호	예	아니요	아니요
Zoom, Cisco Webex, Citrix Workspace 및 Microsoft Teams 보호	예	아니요	아니요
지원되는 운영 체제 및 해당 버전에 대한 자세한 내용은 "지원되는 플랫폼"(743페이지) 항목을 참조하십시오.			

기능 세트	Windows	Linux	macOS
바이러스 백신 및 맬웨어 방지 기능			
완전 통합 Active Protection 기능	예	아니요	아니요
실시간 안티맬웨어 보호	예	예(고급 맬웨어 방지 팩 사용)	예(고급 맬웨어 방지 팩 사용)
로컬 서명 기반 감지 기능이 포함된 고급 실시간 안티맬웨어 보호	예	예	예
이식 가능 파일에 대한 고정 분석	예	아니요	예*
온디맨드 맬웨어 방지 스캔	예	예**	예
네트워크 폴더 보호	예	예	아니요
서버측 보호	예	아니요	아니요

© Acronis International GmbH, 2003-2024

기능 세트	Windows	Linux	macOS
바이러스 백신 및 맬웨어 방지 기능			
아카이브 파일 스캔	예	아니요	예
이동식 드라이브 스캔	예	아니요	예
새로운 파일 및 변경된 파일만 스캔	예	아니요	예
파일/폴더 제외	예	예	예***
프로세스 제외	예	아니요	예
동작 분석 엔진	예	아니요	예
악용 방지	예	아니요	아니요
격리	예	예	예
격리 자동 정리	예	예	예
URL 필터링(http/https)	예	아니요	아니요
기업 전반 허용 목록	예	아니요	예
방화벽 관리****	예	아니요	아니요
Microsoft Defender 안티바이러스 관리*****	예	아니요	아니요
Microsoft Security Essentials 관리	예	아니요	아니요
Windows 보안 센터를 통한 바이러스 백신 및 맬웨어 방지 기능 등록 및 관리	예	아니요	아니요
지원되는 운영 체제 및 해당 버전에 대한 자세한 내용은 "지원되는 플랫폼"(743페이지) 항목을 참조하십시오.			

* 이식 가능 파일에 대한 고정 분석은 macOS의 예약된 스캔에 대해서만 지원됩니다.

** Linux의 온디맨드 스캔에서는 시작 조건이 지원되지 않습니다.

*** 파일/폴더 제외는 macOS의 실시간 보호 또는 예약된 스캔에 의해 스캔되지 않을 파일 및 폴더를 지정할 때에만 지원됩니다.

**** 방화벽 관리는 Windows 8 이상에서 지원됩니다. Windows Server는 지원되지 않습니다.

***** Microsoft Defender 안티바이러스 관리는 Windows 8.1 이상에서 지원됩니다.

© Acronis International GmbH, 2003-2024

기능 세트	Windows	Linux	macOS
취약성 평가			
운영 체제 및 해당 기본 애플리케이션 취약성 평가	예	예******	예
서드 파티 애플리케이션 취약성 평가	예	아니요	예
지원되는 운영 체제 및 해당 버전에 대한 자세한 내용은 "지원되는 Microsoft 및 서드 파티 제품"(864페이지), "지원되는 Linux 제품"(867페이지) 및 "지원되는 Apple 및 서드 파티 제품"(866페이지) 항목을 참조하십시오.			

****** 취약점 평가는 특정 배포판에 대한 공식 보안 자문 제공 여부에 따라 달라집니다(예: https://lists.centos.org/pipermail/centos-announce, https://lists.centos.org/pipermail/centos-cr-announce 등).

기능 세트	Windows	Linux	macOS
패치 관리			
패치 자동 승인	예	아니요	아니요
패치 자동 설치	예	아니요	아니요
패치 테스트	예	아니요	아니요
수동 패치 설치	예	아니요	아니요
패치 예약	예	아니요	아니요
장애 안전 패치: 보호 계획의 일부로 패치 설치 전 머신 백업	예	아니요	아니요
백업이 실행 중인 경우 머신 재부팅 취소	예	아니요	아니요
지원되는 Windows 버전은 "지원되는 운영 체제 및 버전"(42페이지) 항목을 참조하십시오.			

기능	Windows	Linux	macOS
데이터 보호 맵			
중요 파일의 조정 가능한 정의	예	아니요	아니요
보호되지 않은 파일을 찾기 위한 머신 스캔	예	아니요	아니요
보호되지 않은 위치 개요	예	아니요	아니요
데이터 보호 맵 위젯에서 보호 작업을 시작하는 기능(**모든 파일 보호** 작업)	예	아니요	아니요
지원되는 Windows 버전은 "지원되는 운영 체제 및 버전"(42페이지) 항목을 참조하십시오.			

© Acronis International GmbH, 2003-2024

기능 세트	Windows	Linux	macOS
디스크 상태			
AI 기반 HDD 및 SDD 상태 제어	예	아니요	아니요
지원되는 Windows 버전은 "지원되는 운영 체제 및 버전"(42페이지) 항목을 참조하십시오.			

기능	Windows	Linux	macOS
Acronis 사이버 보호 작업 센터(CPOC) 경보에 기반한 스마트 보호 계획			
위협 피드	예	아니요	아니요
수정 마법사	예	아니요	아니요
지원되는 Windows 버전은 "지원되는 운영 체제 및 버전"(42페이지) 항목을 참조하십시오.			

기능 세트	Windows	Linux	macOS
백업 스캔			
백업 계획에 포함된 이미지 백업의 맬웨어 방지 스캔	예	아니요	아니요
클라우드에서 맬웨어에 대한 이미지 백업 스캔	예	아니요	아니요
암호화된 백업의 맬웨어 스캔	예	아니요	아니요
지원되는 Windows 버전은 "지원되는 운영 체제 및 버전"(42페이지) 항목을 참조하십시오.			

기능 세트	Windows	Linux	macOS
안전 복구			
복구 프로세스 중 바이러스 백신 및 맬웨어 방지 기능을 사용한 맬웨어 방지 스캔	예	아니요	아니요
암호화된 백업의 안전 복구	예	아니요	아니요
지원되는 Windows 버전은 "지원되는 운영 체제 및 버전"(42페이지) 항목을 참조하십시오.			

기능 세트	Windows	Linux	macOS
원격 데스크톱 연결			
NEAR를 통한 연결	예	예	예
RDP를 통한 연결	예	아니요	아니요
Apple 화면 공유를 통한 연결	아니요	아니요	예

© Acronis International GmbH, 2003-2024

기능 세트	Windows	Linux	macOS
원격 데스크톱 연결			
웹 클라이언트를 통한 연결	예	아니요	아니요
빠른 지원을 통한 연결	예	예	예
원격 지원	예	예	예
파일 전송	예	예	예
스크린샷 전송	예	예	예
지원되는 운영 체제 및 해당 버전에 대한 자세한 내용은 "지원되는 플랫폼"(899페이지) 항목을 참조하십시오.			

기능 세트	Windows	Linux	macOS
#CyberFit 점수			
#CyberFit Score 상태	예	아니요	아니요
#CyberFit Score 독립형 도구	예	아니요	아니요
#CyberFit Score 권장 사항	예	아니요	아니요
지원되는 Windows 버전은 "지원되는 운영 체제 및 버전"(42페이지) 항목을 참조하십시오.			

기능 세트	Windows	Linux	macOS
데이터 손실 방지			
장치 제어	예	아니요	macOS 10.15 이상 또는 macOS 11.2.3 이상을 실행 중이며 Intel 프로세서가 장착된 Mac에서 지원됩니다. Apple M1/M2 등의 ARM 기반 Apple

© Acronis International GmbH, 2003-2024

기능 세트	Windows	Linux	macOS
데이터 손실 방지			
			실리콘 프로세서에서는 지원되지 않습니다.
Advanced Data Loss Prevention	예	아니요	아니요
지원되는 Windows 버전은 "지원되는 운영 체제 및 버전"(42페이지) 항목을 참조하십시오.			

기능 세트	Windows	Linux	macOS
관리 옵션			
Cyber Protect 버전 승급을 위한 업셀 시나리오	예	예	예
웹 기반 중앙 집중식 및 원격 관리 콘솔	예	예	예
지원되는 운영 체제 및 버전: 플랫폼에 관계없이 지원됩니다.			

기능 세트	Windows	Linux	macOS
보호 옵션			
원격 지우기	예	아니요	아니요
Windows 10 이상을 지원합니다.			

기능 세트	Windows	Linux	macOS
Cyber Protect 모니터			
Cyber Protect 앱	예	아니요	예
Zoom 보호 상태	예	아니요	아니요
Cisco Webex 보호 상태	예	아니요	아니요
Citrix Workspace 보호 상태	예	아니요	아니요
Microsoft Teams 보호 상태	예	아니요	아니요
지원되는 Windows 버전은 "지원되는 운영 체제 및 버전"(42페이지) 항목을 참조하십시오. macOS에서는 Agent for Mac을 설치할 수 있는 모든 버전에서 Cyber Protect Monitor가 지원됩니다. 자세한 내용은 "Agent for Mac"(27페이지)을(를) 참조하십시오.			

© Acronis International GmbH, 2003-2024

기능 세트	Windows	Linux	macOS
소프트웨어 인벤토리			
소프트웨어 인벤토리 스캐닝	예	아니요	예
소프트웨어 인벤토리 모니터링	예	아니요	예
지원되는 Windows 버전은 "지원되는 운영 체제 및 버전"(42페이지) 항목을 참조하십시오. macOS의 경우 버전 10.13.x – 13.x에서 소프트웨어 인벤토리가 지원됩니다.			

기능 세트	Windows	Linux	macOS
하드웨어 인벤토리			
하드웨어 인벤토리 검색	예	아니요	예
하드웨어 인벤토리 모니터링	예	아니요	예
지원되는 Windows 버전은 "지원되는 운영 체제 및 버전"(42페이지) 항목을 참조하십시오. macOS의 경우 버전 10.13.x – 13.x에서 하드웨어 인벤토리가 지원됩니다.			

지원되는 파일 시스템

보호 에이전트는 에이전트가 설치된 운영 체제에서 액세스 가능한 모든 파일 시스템을 백업할 수 있습니다. 예를 들어 Agent for Windows는 Windows에 해당 드라이버가 설치되어 있으면 ext4 파일 시스템을 백업하고 복구할 수 있습니다.

다음 표에는 백업 및 복구할 수 있는 파일 시스템이 요약되어 있습니다(부트 가능한 미디어는 복구만 지원). 에이전트 및 부트 가능한 미디어 모두에 제한 사항이 적용됩니다.

파일 시스템	지원			제한 사항
	에이전트	Windows 및 Linux용 부트 가능한 미디어	Ma용 부트 가능한 미디어	
FAT16/32	모든 에이전트	+	+	제한 없음
NTFS	모든 에이전트	+	+	
ext2/ext3/ext4	모든 에이전트	+	-	
HFS+	Agent for	-	+	

© Acronis International GmbH, 2003-2024

파일 시스템	지원			제한 사항
	에이전트	Windows 및 Linux용 부트 가능한 미디어	Ma용 부트 가능한 미디어	
	Mac			
APFS	Agent for Mac	-	+	• macOS High Sierra 10.13으로 시작 지원 • 원본 이외 머신 또는 베어 메탈로 복구할 때에는 디스크 구성을 수동으로 재생성해야 합니다.
JFS	Agent for Linux	+	-	• 파일 필터(포함/제외)는 지원되지 않습니다. • 빠른 증분/차등 백업을 활성화할 수 없음
ReiserFS3	Agent for Linux	+	-	
ReiserFS4	Agent for Linux	+	-	• 파일 필터(포함/제외)는 지원되지 않습니다. • 빠른 증분/차등 백업을 활성화할 수 없음 • 복구 도중 볼륨 크기를 조정할 수 없음
ReFS	모든 에이전트	+	+	• 파일 필터(포함/제외)는 지원되지 않습니다. • 빠른 증분/차등 백업을 활성화할 수 없음 • 복구 도중 볼륨 크기를 조정할 수 없음 • ReFS 백업에서 파일을 복구할 때는 해당 백업의 내용만 복구되며 ACL(액세스 제어 목록) 및 대체 스트림은 복구되지 않습니다. 스파스 파일은 일반 파일로 복구됩니다.
XFS	모든 에이전트	+	+	• 파일 필터(포함/제외)는 지원되지 않습니다. • 빠른 증분/차등 백업을 활성화할 수 없음 • 복구 도중 볼륨 크기를 조정

© Acronis International GmbH, 2003-2024

파일 시스템	지원			제한 사항
	에이전트	Windows 및 Linux용 부트 가능한 미디어	Ma용 부트 가능한 미디어	
				할 수 없음 • XFS 파일 시스템에서는 빠른 증분 백업 모드는 지원되지 않습니다. XFS 볼륨을 클라우드에서 증분 및 차등 백업하면 이와 비슷하게 빠른 증분 모드를 사용하는 ext4 백업과 비교했을 때 현저히 느릴 수 있습니다.
Linux swap	Agent for Linux	+	-	제한 없음
exFAT	모든 에이전트	+ 백업이 exFAT에 *저장되어 있을 경우* 부트 가능한 미디어를 복구에 사용할 수 없습니다	+	• 디스크/볼륨 백업만 지원 • 파일 필터(포함/제외)는 지원되지 않습니다. • 개별 파일은 백업에서 복구 불가

인식되지 않는 또는 지원되지 않는 파일 시스템이 있는 드라이브를 백업할 때에는 소프트웨어가 섹터 단위 모드로 자동 전환됩니다(예: Btrfs). 다음과 같은 모든 파일 시스템에서 섹터 단위 백업이 가능합니다.

- 블록 기반
- 단일 디스크에 걸쳐 있음
- 표준 MBR/GPT 파티셔닝 구성표가 있음

파일 시스템이 이 요구 사항을 충족하지 않는 경우 백업이 실패합니다.

데이터 중복 제거

Windows Server 2012 이상에서는 NTFS 볼륨에 대해 데이터 중복 제거 기능을 사용할 수 있습니다. 데이터 중복 제거는 볼륨 파일의 중복된 부분을 한 번만 저장함으로써 볼륨에서 사용 공간을 줄입니다.

디스크 레벨에서 제한 없이 데이터 중복 제거가 활성화된 볼륨을 백업하고 복구할 수 있습니다. Acronis VSS 공급자를 사용할 경우를 제외하고 파일 수준 백업이 지원됩니다. 디스크 백업에서 파

© Acronis International GmbH, 2003-2024

일을 복구하려면 백업에서 가상 머신을 실행하거나 Windows Server 2012 이상을 실행 중인 머신에서 백업을 마운트한 다음 마운트된 볼륨에서 파일을 복사합니다.

Windows Server의 데이터 중복 제거 기능은 Acronis Backup 중복 제거 기능과 관련이 없습니다.

논리 볼륨에서 지원되는 작업

Windows의 LDM(동적 디스크), Linux의 LVM과 같은 논리 볼륨이 포함된 워크로드의 백업 및 복구가 지원되며 다음 제한이 적용됩니다.

백업

에이전트 기반 백업은 워크로드에 설치된 보호 에이전트나 부팅 가능한 미디어에 의해 생성된 백업입니다.

에이전트 없는 백업은 가상 머신에서만 사용할 수 있습니다. 환경 내의 모든 가상 머신을 백업 및 복구할 수 있는 에이전트가 하이퍼바이저 수준에서 에이전트 없는 백업을 수행합니다. 보호되는 가상 머신에는 개별 에이전트가 설치되지 않습니다.

에이전트 기반 백업과 에이전트 없는 백업 간의 차이점에 대한 자세한 내용은 "에이전트 기반 백업 및 비에이전트 백업"(61페이지) 항목을 참조하십시오.

에이전트 기반 백업	비에이전트 백업
• 논리 볼륨은 볼륨별로 백업됩니다. • 파일 필터(포함/제외)가 지원됩니다.	• 논리 볼륨이 탐지된 디스크는 섹터 단위(RAW) 모드로 백업됩니다. 이 경우 디스크의 파티션 구조가 분석되지 않으며 볼륨 이미지가 별도로 저장되지 않습니다. • 개별 LDM 또는 LVM 볼륨은 백업 소스로 선택(직접 선택 또는 정책 규칙을 사용하여 선택)할 수 없습니다. 보호 계획의 **백업할 항목** 섹션에서는 **전체 머신**만 선택할 수 있습니다. • 파일 필터(포함/제외)는 지원되지 않으며 포함이나 제외는 구성하더라도 모두 무시됩니다.

복구

에이전트 기반 복구는 워크로드에 설치된 에이전트나 부팅 가능한 미디어에 의해 수행되는 복구입니다.

에이전트 없는 복구에서는 가상 머신만 대상으로 지원됩니다. 환경 내의 모든 가상 머신을 백업 및 복구할 수 있는 에이전트가 하이퍼바이저 수준에서 에이전트 없는 복구를 수행합니다. 백업이 복구되는 대상 머신을 수동으로 생성할 필요는 없습니다.

	에이전트 기반 백업	에이전트 없는 백업
에이전트 기반 복구	• 볼륨별 복구가 가능합니다. • 파일 및 폴더 복구가 가능합니다.	• 볼륨별 복구를 사용할 수 없습니다. • 파일 및 폴더 복구가 가능합니다.

© Acronis International GmbH, 2003-2024

	에이전트 기반 백업	에이전트 없는 백업
비에이전트 복구	• 머신 마이그레이션(P2V, V2P, V2V)은 지원되지 않습니다. 에이전트 기반 백업에서 데이터를 복구하려면 부팅 가능한 미디어를 사용해야 합니다. • **VM으로 실행** 작업은 지원되지 않습니다. • 파일 및 폴더 복구가 가능합니다.	• 볼륨별 복구를 사용할 수 없습니다. • 전체 머신 복구가 가능합니다. • 파일 및 폴더 복구가 가능합니다. • **VM으로 실행** 작업이 지원됩니다. 가상 머신을 부팅 가능하도록 설정하려는 경우에는 부팅 순서를 변경해야 할 수도 있습니다. 자세한 내용은 이 기술 자료 문서를 참조하십시오. • 다음 유형의 가상 머신으로 변환할 수 있습니다. ◦ VMware ESXi ◦ Microsoft Hyper-V ◦ Scale Computing HC3

© Acronis International GmbH, 2003-2024

Cyber Protection 에이전트 설치 및 디플로이

준비

1단계

백업하려는 항목에 따라 에이전트를 선택합니다. 선택 가능한 항목에 대한 자세한 내용은 필요한 에이전트를 참조하십시오.

2단계

에이전트를 설치하기 위해 하드 드라이브에 여유 공간이 있는 것을 확인하십시오. 공간 요구 사항 관련 상세 정보는 "에이전트의 시스템 요구 사항"(62페이지)의 내용을 참조하십시오.

3단계

설치 프로그램을 다운로드합니다. 다운로드 링크를 찾으려면 **모든 장치** > **추가**를 클릭합니다.

장치 추가 페이지는 Windows에 설치된 각 에이전트에 대한 웹 인스톨러를 제공합니다. 웹 인스톨러는 인터넷에서 주 설치 프로그램을 다운로드하여 임시 파일에 저장하는 작은 실행 파일입니다. 이 파일은 설치 후 즉시 삭제됩니다.

설치 프로그램을 로컬에 저장하려면 **장치 추가** 페이지 맨 아래에 있는 링크를 사용하여 Windows에 설치하는 데 필요한 모든 에이전트가 포함된 패키지를 다운로드합니다. 32비트 및 64비트 패키지를 둘 다 다운로드할 수 있습니다. 이 패키지에서는 설치할 컴퍼넌트 목록을 사용자 정의할 수 있습니다. 또한 이 패키지는 예를 들어 그룹 정책을 통해 무인 설치를 가능하게 합니다. 이 고급 시나리오는 "그룹 정책을 통해 에이전트 배포"(156페이지)에 설명되어 있습니다.

Agent for Microsoft 365 설치 프로그램을 다운로드하려면 오른쪽 위에 있는 계정 아이콘을 클릭하고 **다운로드** > **Agent for Microsoft 365**를 클릭합니다.

Linux 및 macOS에 설치는 일반적인 설치 프로그램에서 수행됩니다.

머신을 Cyber Protection 서비스에 등록하려면 모든 설정 프로그램에 인터넷 연결이 필요합니다. 인터넷에 연결되어 있지 않으면 설치에 실패합니다.

4단계

Cyber Protect 기능을 사용하려면 Microsoft Visual C++ 2017 Redistributable이 필요합니다. 에이전트를 설치하기 전에 Microsoft Visual C++ 2017 Redistributable이 머신에 존재하는지 확인하고, 없는 경우 설치합니다. Microsoft Visual C++ 설치 후에는 다시 시작해야 할 수 있습니다. Microsoft Visual C++ Redistributable 패키지는 https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows에서 찾을 수 있습니다.

© Acronis International GmbH, 2003-2024

5단계

방화벽 및 네트워크 보안 시스템(프록시 서버 등)의 기타 컴포넌트가 다음 TCP 포트를 통한 아웃바운드 연결을 허용하는지 확인합니다.

- 포트 **443** 및 **8443**

  이러한 포트는 Cyber Protect 콘솔에 액세스하고, 에이전트를 등록하고, 인증서 및 사용자 권한을 다운로드하고, 클라우드 스토리지에서 파일을 다운로드하는 데 사용됩니다.
- **7770 – 7800** 범위의 포트

  에이전트에서는 이러한 포트를 사용하여 관리 서버와 통신합니다.
- 포트 **44445** 및 **55556**

  에이전트에서는 백업 및 복구 중 데이터 전송에 이러한 포트를 사용합니다.

네트워크에서 프록시 서버가 활성화되어 있으면 "프록시 서버 설정 구성"(68페이지)을(를) 참조해 보호 에이전트를 실행하는 각 머신에서 프록시 서버 설정을 구성해야 하는지 파악합니다.

클라우드에서 에이전트를 관리하는데 필요한 최소 인터넷 연결 속도는 1Mbit/s입니다(클라우드 백업에 인정되는 데이터 전송 속도와 혼동해서는 안 됩니다). ADSL과 같은 저대역폭 연결 기술을 사용할 경우에는 이 점을 고려합니다.

TCP 포트는 VMware 가상 머신을 백업하고 복제하는 데 필요합니다.

- 포트 **443**

  Agent for VMware(Windows 및 가상 어플라이언스 모두 해당)는 ESXi 호스트/vCenter 서버의 이 포트에 연결되어 백업 및 복구, VM 복제 작업 도중 VSphere에서 VM을 생성하고 업데이트하고 삭제하는 등의 VM 관리 작업을 수행합니다.
- 포트 **902**

  Agent for VMware(Windows 및 가상 어플라이언스 모두 해당)는 ESXi 호스트의 이 포트에 연결되어 백업, 복구, VM 복제 작업 도중 VM 디스크에서 데이크를 읽고 쓸 수 있도록 NFC 연결을 구축합니다.
- 포트 **3333**

  Agent for VMware(가상 어플라이언스)가 VM 복제 대상인 ESXi 호스트/클러스터에서 구동 중인 경우 VM 복제 트래픽은 포트 **902**의 ESXi 호스트로 직접 전달되지 않습니다. 그 대신 해당 트래픽은 소스인 Agent for VMware에서 대상 ESXi 호스트/클러스터에 위치한 Agent for VMware(가상 어플라이언스)에 있는 TCP 포트 **3333**으로 전달됩니다.

  원본 VM 디스크에서 데이터를 읽는 소스 Agent for VMware는 이외 어디에든 존재할 수 있으며 가상 어플라이언스 또는 Windows 유형일 수 있습니다.

  대상 Agent for VMware(가상 어플라이언스)에서 VM 복제 데이터를 허용하도록 담당하는 서비스는 "복제본 디스크 서버"라고 불립니다.이러한 서비스는 복제본 시딩을 비롯해 VM 복제 작업 도중의 트래픽 압축과 중복 제거 등 WAN 최적화 기술을 담당합니다(초기 복제본 시딩 참조). 대상 ESXi 호스트에서 구동 중인 Agent for VMware(가상 어플라이언스)가 없는 경우 이러한 서비스를 사용할 수 없으며, 이로 인해 복제본 시딩 시나리오도 지원되지 않습니다.

© Acronis International GmbH, 2003-2024

다운로더 컴퍼넌트에 필요한 포트

다운로더 컴퍼넌트는 업데이트를 컴퓨터에 제공하고 다른 다운로더 인스턴스에 배포합니다. 이 컴퍼넌트는 에이전트 모드에서 실행될 수 있습니다. 그러면 컴퓨터가 다운로더 에이전트로 작동합니다. 다운로더 에이전트는 인터넷에서 업데이트를 다운로드하며 다른 컴퓨터로의 업데이트 배포 소스로 사용됩니다. 다운로더가 작동하려면 다음 포트가 필요합니다.

- TCP 및 UDP(수신) 포트 **6888**
  BitTorrent 프로토콜에서 토렌트 피어 투 피어 업데이트에 사용됩니다.
- UDP 포트 **6771**
  로컬 피어 검색 포트로 사용됩니다. 피어 투 피어 업데이트에서도 사용됩니다.
- TCP 포트 **18018**
  Updater 및 UpdaterAgent 모드에서 작동하는 업데이터 간의 통신에 사용됩니다.
- TCP 포트 **18019**
  Updater 및 Protection 에이전트 간의 통신에 사용되는 로컬 포트입니다.

6단계

Protection 에이전트를 설치하려는 머신에서 다음 로컬 포트를 다른 프로세스가 사용하지 않는지 확인합니다.

- 127.0.0.1:**9999**
- 127.0.0.1:**43234**
- 127.0.0.1:**9850**

참고
방화벽에서 해당 로컬 포트를 열 필요가 없습니다.

Protection 에이전트가 사용하는 포트 변경

Protection 에이전트가 필요로 하는 일부 포트를 환경 내 다른 애플리케이션이 사용 중일 수 있습니다. 충돌을 피하려면 다음 파일을 수정하여 Protection 에이전트가 사용하는 기본 포트를 변경하면 됩니다.

- Linux: `/opt/Acronis/etc/aakore.yaml`
- Windows: `\ProgramData\Acronis\Agent\etc\aakore.yaml`

필요한 에이전트

백업하려는 항목에 따라 에이전트를 선택합니다. 아래의 표는 결정에 도움이 되는 정보를 요약해서 보여줍니다.

Windows에서 Agent for Exchange, Agent for SQL, Agent for Active Directory, Agent for Oracle을 설치하려면 Agent for Windows도 설치되어 있어야 합니다. 따라서, 예를 들어 Agent for SQL을 설치한 경우 이 에이전트가 설치된 전체 머신을 백업할 수 있습니다.

© Acronis International GmbH, 2003-2024

Agent for VMware(Windows) 및 Agent for Hyper-V를 설치할 때는 Agent for Windows도 설치하는 것이 좋습니다.

Linux에 Agent for Oracle, Agent for MySQL/MariaDB 및 Agent for Virtuozzo를 설치하려면 Agent for Linux(64비트)도 설치되어 있어야 합니다. 이러한 에이전트는 Agent for Linux(64비트) 설치 파일에 번들로 포함되어 있습니다.

백업 대상	설치할 에이전트	에이전트 설치 위치
실제 머신		
Windows를 실행 중인 실제 머신	Agent for Windows	백업되는 머신
Linux를 실행 중인 실제 머신	Agent for Linux	
macOS를 실행 중인 실제 머신	Agent for Mac	
데이터베이스		
SQL 데이터베이스	Agent for SQL	Microsoft SQL Server 실행 중인 머신
MySQL 데이터베이스	Agent for MySQL/MariaDB (Agent for Linux(64비트) 설치 파일에 번들로 포함되어 있음)	MySQL Server 실행하는 머신에서.
MariaDB 데이터베이스	Agent for MySQL/MariaDB (Agent for Linux(64비트) 설치 파일에 번들로 포함되어 있음)	MariaDB Server 실행하는 머신에서.
Exchange 데이터베이스	Agent for Exchange	Microsoft Exchange Server의 사서함 역할을 실행 중인 머신*
Oracle 데이터베이스	Agent for Oracle (Linux에서 Agent for Linux(64비트) 설치 파일에 번들로 포함되어 있음)	Oracle 데이터베이스를 실행 중인 머신.

© Acronis International GmbH, 2003-2024

클라우드 간 워크로드		
Microsoft 365 사서함 (클라우드 에이전트 또는 로컬 에이전트)	클라우드 에이전트 (설치 불필요)	이 기능은 데이터 센터에 디플로이한 클라우드 에이전트에서 사용 가능합니다. 자세한 내용은 "클라우드 Agent for Microsoft 365 사용"(553페이지)을(를) 참조하십시오.
	Agent for Office 365	인터넷에 연결된 Windows 머신 자세한 내용은 "로컬로 설치한 Agent for Office 365 사용"(549페이지)을(를) 참조하십시오.
Microsoft 365 OneDrive 파일 및 SharePoint Online 사이트	클라우드 에이전트 (설치 불필요)	이 기능은 데이터 센터에 디플로이한 클라우드 에이전트에서 사용 가능합니다. 자세한 내용은 "클라우드 Agent for Microsoft 365 사용"(553페이지)을(를) 참조하십시오.
Google Workspace Gmail 사서함, Google Drive 파일 및 Shared Drive 파일	클라우드 에이전트 (설치 불필요)	이 기능은 데이터 센터에 디플로이한 클라우드 에이전트에서 사용 가능합니다. 자세한 내용은 "Google Workspace 데이터 보호"(582페이지)을(를) 참조하십시오.
Active Directory		
Active Directory 도메인 서비스를 실행 중인 머신	Agent for Active Directory	도메인 컨트롤러.

© Acronis International GmbH, 2003-2024

가상 머신		
VMware ESXi 가상 머신	Agent for VMware (Windows)	vCenter Server 및 가상 머신 스토리지에 네트워크를 통해 액세스할 수 있는 Windows 머신**
	Agent for VMware (가상 어플라이언스)	ESXi 호스트
Hyper-V 가상 머신	Agent for Hyper-V	Hyper-V 호스트
Scale Computing HC3 가상 머신	Agent for Scale Computing HC3 (가상 어플라이언스)	Scale Computing HC3 호스트
Red Hat Virtualization 가상 머신(oVirt를 통해 관리됨)	Agent for oVirt(가상 어플라이언스)	Red Hat Virtualization 호스트.
Virtuozzo 가상 머신 및 컨테이너***	Agent for Virtuozzo (Agent for Linux(64비트) 설치 파일에 번들로 포함되어 있음)	Virtuozzo 호스트
Virtuozzo Hybrid Infrastructure 가상 머신	Agent for Virtuozzo Hybrid Infrastructure(가상 어플라이언스)	Virtuozzo Hybrid Infrastructure 호스트.
Amazon EC2에서 호스팅되는 가상 머신	실제 머신에 대해 동일****	백업되는 머신
Windows Azure에서 호스팅되는 가상 머신		
Citrix XenServer 가상 머신		
Red Hat Virtualization (RHV/RHEV), not managed by oVirt		
oVirt가 관리하지 않는 커널 기반 가상 머신(KVM)		
oVirt가 관리하지 않는 Oracle 가상 머신		
Nutanix AHV 가상 머신		

© Acronis International GmbH, 2003-2024

oVirt가 관리하는 Red Hat Virtualization(RHV/RHEV)	Agent for oVirt(가상 어플라이언스)	가상화 호스트.
oVirt가 관리하는 커널 기반 가상 머신(KVM)		
oVirt가 관리하는 Oracle 가상 머신		
모바일 장치		
Android를 실행하는 모바일 장치	Android용 모바일 앱	백업되는 모바일 장치
iOS를 실행하는 모바일 장치	iOS용 모바일 앱	

*설치 과정에서 Agent for Exchange는 구동될 머신에 여유 공간이 충분한지 확인합니다. 개별 복구 시 일시적으로 가장 규모가 큰 Exchange 데이터베이스의 15%에 해당하는 여유 공간이 필요하므로 그만큼을 확보해 두어야 합니다.

**ESXi에서 SAN 연결 스토리지를 사용하는 경우 동일한 SAN에 연결된 머신에 에이전트를 설치합니다. 에이전트는 ESXi 호스트 및 LAN을 통해서가 아니라 스토리지에서 가상 머신을 직접 백업합니다. 자세한 지침은 "Agent for VMware - LAN 프리 백업"(626페이지) 항목을 참조하십시오.

***Virtuozzo 7의 경우 Ploop 컨테이너만 지원됩니다. 가상 머신은 지원되지 않습니다.

****외부 에이전트에서 가상 머신을 백업하는 경우 가상 머신은 가상으로 간주됩니다. 에이전트가 게스트 시스템에 설치되어 있는 경우 백업 및 복구 작업은 실제 머신과 동일합니다. 하지만 Cyber Protection가 CPUID 지침을 사용하여 가상 머신을 식별할 수 있는 경우, 가상 머신 서비스 할당이 여기에 할당됩니다. CPU 제조사 ID를 덮어쓰는 다른 선택지나 직접 변경을 사용하는 경우에는 실제 머신에 대한 서비스 할당만을 할당할 수 있습니다.

에이전트 기반 백업 및 비에이전트 백업

에이전트 기반 백업을 수행하려면 보호되는 각 머신에 보호 에이전트를 설치해야 합니다. 에이전트 기반 백업은 모든 실제 머신과 가상 머신에서 지원됩니다. 필요한 에이전트 및 해당 에이전트를 설치해야 하는 위치에 대한 자세한 내용은 "필요한 에이전트"(57페이지) 항목을 참조하십시오.

에이전트 없는 백업은 일부 가상화 플랫폼에서 지원되며 실제 머신에서는 사용할 수 없습니다. 에이전트 없는 백업 수행 시에는 가상 환경의 전용 머신에 보호 에이전트를 하나만 설치하면 됩니다. 해당 에이전트는 이 환경의 기타 모든 가상 머신을 백업합니다. 가상화 플랫폼별로 지원되는 백업 유형에 대한 자세한 내용은 "지원되는 가상화 플랫폼"(30페이지) 항목을 참조하십시오.

가상 어플라이언스를 사용할 수 있는 가상화 플랫폼도 있습니다. VA(가상 어플라이언스)는 보호 에이전트가 설치되어 있는 이미 생성된 가상 머신입니다. 가상 어플라이언스는 .ovf, .ova, .qcow 등의 하이퍼바이저별 형식으로 제공됩니다.

필요한 백업 유형 확인

다음과 같은 경우에는 에이전트 기반 백업을 수행하는 것이 좋습니다.

© Acronis International GmbH, 2003-2024

- 안티바이러스 및 안티맬웨어, 패치 관리, 원격 데스크탑 연결 등의 추가 보호 기능이 필요한 경우. 이러한 기능에 대한 자세한 내용은 "운영 체제별 지원되는 보호 기능"(41페이지) 항목을 참조하십시오.
- 테넌트 수준의 개별 가상 머신이 필요한 경우. 테넌트 내 사용자에게 자신의 백업 액세스 권한만 제공하려는 등의 경우 이러한 가상 머신이 필요할 수 있습니다.
- 게스트 운영 체제로 복구할 수 있는 파일 수준 백업이 필요한 경우

다음과 같은 경우에는 에이전트 없는 백업을 수행하는 것이 좋습니다.

- 백업만 필요한 경우(추가 보호 기능 불필요)
- 간편한 관리 방법이 필요한 경우. 에이전트 없는 백업 사용 시에는 에이전트를 하나만 설치하고 구성하면 여러 가상 머신을 백업할 수 있습니다.
- 리소스 사용량을 최소화해야 하는 경우. 에이전트 없는 백업 사용 시에는 전용 에이전트 하나만 있으면 되므로 환경 내의 각 가상 머신에 여러 에이전트를 설치하는 방식에 비해 CPU 및 RAM 사용량이 감소합니다.
- LAN을 사용하지 않는 백업 등의 특정 백업 설정을 사용해야 하는 경우. 이 기능에 대한 자세한 내용은 "Agent for VMware - LAN 프리 백업"(626페이지) 항목을 참조하십시오.
- 구성 오버헤드를 줄여야 하는 경우. 전용 에이전트는 게스트 운영 체제에 관계없이 하이퍼바이저 수준에서 가상 머신을 백업합니다.

에이전트의 시스템 요구 사항

에이전트	설치에 필요한 디스크 공간
Agent for Windows	1.2GB
Agent for Linux	2GB
Agent for Mac	1GB
Agent for SQL 및 Agent for Windows	1.2GB
Agent for Exchange 및 Agent for Windows	1.3GB
Data Loss Prevention용 에이전트	500MB
Agent for Microsoft 365	500MB
Agent for Active Directory 및 Agent for Windows	2GB
Agent for VMware 및 Windows용 에이전트	1.5GB
Agent for Hyper-V 및 Windows용 에이전트	1.5GB
Agent for Virtuozzo 및 Linux용 에이전트	1GB

© Acronis International GmbH, 2003-2024

Agent for Virtuozzo Hybrid Infrastructure	700MB
Agent for Oracle 및 Agent for Windows	2.2GB
Agent for Oracle 및 Linux용 에이전트	2GB
Agent for MySQL/MariaDB 및 Linux용 에이전트	2GB

백업 삭제를 비롯한 백업 작업을 수행하려면 백업 크기 1TB당 약 1GB의 RAM이 필요합니다. 에이전트에서 처리하는 데이터의 양 및 유형에 따라 메모리 사용량은 달라질 수 있습니다.

참고
초대형 백업 세트(4TB 이상)로 백업할 때는 RAM 사용량이 늘어날 수 있습니다.

x64 시스템에서는 재부팅 작업을 포함한 부트 가능한 미디어 또는 디스크 복구 작업에 최소한 2GB 메모리가 필요합니다.

CET 기술을 지원하는 11세대 Intel Core 또는 AMD Ryzen 7 등의 최신 프로세서를 사용하는 워크로드에서는 충돌을 방지하기 위해 데이터 손실 방지 에이전트의 일부 기능이 비활성화됩니다. 이러한 CPU가 장착된 시스템의 장치 제어 및 Advanced DLP 기능 사용 가능 여부가 아래 표에 나와 있습니다.

기능	장치 제어	Advanced DLP
로컬 채널		
이동식 스토리지	해당 없음	예
암호화된 이동식 스토리지	예	해당 없음
프린터	해당 없음	아니요
리디렉션 매핑 드라이브	해당 없음	예
리디렉션 클립보드	해당 없음	아니요
네트워크 통신		
SMTP 이메일	해당 없음	예
Microsoft Outlook(MAPI)	해당 없음	예
IBM 메모	해당 없음	아니요
웹 메일	해당 없음	예
인스턴트 메시징(ICQ)	해당 없음	아니요
인스턴트 메시징(Viber)	해당 없음	아니요
인스턴트 메시징(IRC, Jabber, Skype, Viber)	해당 없음	예

© Acronis International GmbH, 2003-2024

파일 공유 서비스	해당 없음	예
소셜 네트워크	해당 없음	예
로컬 네트워크 파일 공유(SMB)	해당 없음	예
웹 액세스(HTTP/HTTPS)	해당 없음	예
파일 전송(FTP/FTPS)	해당 없음	예
데이터 전송 허용 목록 작성		
장치 유형 허용 목록	해당 없음	예
네트워크 통신 허용 목록	해당 없음	예
원격 호스트에 대한 허용 목록	해당 없음	예
애플리케이션에 대한 허용 목록	해당 없음	예
주변 장치		
이동식 스토리지	예	예
암호화된 이동식 스토리지	예	예
프린터	아니요	아니요
MTP 연결 모바일 장치	아니요	아니요
Bluetooth 어댑터	예	예
광학 드라이브	예	예
플로피 드라이브	예	예
Windows 클립보드	아니요	아니요
스크린샷 캡처	아니요	아니요
리디렉션 매핑 드라이브	예	예
리디렉션 클립보드	아니요	아니요
Cyber Protect Agent 자체 보호		
일반 최종 사용자로부터 보호	예	예
로컬 시스템 관리자로부터 보호	예	예

Linux 패키지

Linux 커널에 필요한 모듈을 추가하려면 설치 프로그램에 다음과 같은 Linux 패키지가 필요합니다.

© Acronis International GmbH, 2003-2024

- 커널 헤더 또는 소스가 있는 패키지. 패키지 버전은 커널 버전과 일치해야 합니다.
- GCC(GNU 컴파일러 모음) 컴파일러 시스템. GCC 버전은 커널이 컴파일된 버전이어야 합니다.
- Make 도구.
- Perl 해석기.
- 4.15에서 시작하여 CONFIG_UNWINDER_ORC=y로 구성되는 커널 구축을 위한 `libelf-dev`, `libelf-devel` 또는 `elfutils-libelf-devel` 라이브러리.Fedora28과 같은 일부 배포에 대해서는 커널 헤더와 별도로 설치해야 합니다.

이러한 패키지의 이름은 Linux 배포판에 따라 다릅니다.

Red Hat Enterprise Linux, CentOS, Fedora인 경우 일반적으로 설치 프로그램이 패키지를 설치합니다. 다른 배포판인 경우 패키지가 설치되어 있지 않거나 필요한 버전이 없는 경우 패키지를 설치해야 합니다.

필요한 패키지가 이미 설치되어 있습니까?

패키지가 이미 설치되어 있는지 알아보려면 다음 단계를 수행합니다.

1. 커널 버전과 필요한 GCC 버전을 알아보려면 다음 명령을 실행합니다.

   ```
   cat /proc/version
   ```

   이 명령은 다음과 비슷한 행을 반환합니다. `Linux 버전 2.6.35.6 및 gcc 버전 4.5.1`
2. Make 도구와 GCC 컴파일러가 설치되어 있는지 확인하려면 다음 명령을 실행합니다.

   ```
   make -v
   gcc -v
   ```

   gcc의 경우 명령을 통해 반환되는 버전은 1단계의 `gcc version`과 동일해야 합니다. **make**의 경우 명령이 실행되는지 확인합니다.
3. 커널 모듈 빌드를 위한 올바른 패키지 버전이 설치되어 있는지 알아봅니다.
   - Red Hat Enterprise Linux, CentOS, Fedora의 경우 다음 명령을 실행합니다.

     ```
     yum list installed | grep kernel-devel
     ```

   - Ubuntu의 경우 다음 명령을 실행합니다.

     ```
     dpkg --get-selections | grep linux-headers
     dpkg --get-selections | grep linux-image
     ```

   두 경우 모두 패키지 버전이 1단계의 `Linux` 버전과 동일해야 합니다.
4. Perl 해석기가 설치되었는지 알아보려면 다음 명령을 입력합니다.

   ```
   perl --version
   ```

   Perl 버전에 대한 정보가 보인다면 해석기가 설치되어 잇는 것입니다.
5. Red Hat Enterprise Linux, CentOS, Fedora의 경우 다음 명령을 실행하여 `elfutils-libelf-devel`이 설치되었는지 확인합니다.

© Acronis International GmbH, 2003-2024

```
yum list installed | grep kernel-devel
```

라이브러리 버전에 대한 정보가 보인다면 라이브러리가 설치되어 있는 것입니다.

리포지토리에서 패키지 설치

다음 표에는 다양한 Linux 배포판에 필수 패키지를 설치하는 방법이 나와 있습니다.

Linux 배포판	패키지 이름	설치 방법
Red Hat Enterprise Linux	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	설치 프로그램이 Red Hat 서브스크립션을 사용하여 패키지를 자동으로 다운로드, 설치합니다.
	perl	다음 명령을 실행합니다. `yum install perl`
CentOS Fedora	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	설치 프로그램이 패키지를 자동으로 다운로드, 설치합니다.
	perl	다음 명령을 실행합니다. `yum install perl`

Ubuntu
Debian
	linux-headers
	linux-image
	gcc
	make
	perl
		다음 명령 실행:
		`sudo apt-get update`
		`sudo apt-get install linux-headers-$(uname -r)`
		`sudo apt-get install linux-image-$(uname -r)`
		`sudo apt-get install gcc-<package version>`
		`sudo apt-get install make`
		`sudo apt-get install perl`

SUSE Linux
OpenSUSE
	kernel-source
	gcc
	make
	perl
		`sudo zypper install kernel-source`
		`sudo zypper install gcc`
		`sudo zypper install make`
		`sudo zypper install perl`

패키지는 배포판 저장소에서 다운로드, 설치됩니다.

다른 Linux 배포판은 필수 패키지의 정확한 이름과 설치 방법에 대한 배포판 문서를 참조하십시오.

© Acronis International GmbH, 2003-2024

수동으로 패키지 설치

다음과 같은 경우 패키지를 **수동으로** 설치해야 합니다.

- 머신에 활성 Red Hat 서브스크립션 또는 인터넷 연결이 없는 경우.
- 설치 프로그램이 커널 버전에 해당하는 **kernel-devel** 또는 **gcc** 버전을 찾을 수 없습니다. 사용 가능한 **kernel-devel**이 기존 커널보다 최신인 경우 커널을 업데이트하거나 일치하는 **kernel-devel** 버전을 수동으로 설치해야 합니다.
- 필수 패키지가 로컬 네트워크에 있고 자동 검색 및 다운로드에 시간을 할애하지 않으려는 경우.

로컬 네트워크 또는 신뢰할 수 있는 타사 웹 사이트에서 패키지를 다운로드하여 다음과 같이 설치합니다.

- Red Hat Enterprise Linux, CentOS, Fedora의 경우 루트 사용자로 다음 명령을 실행합니다.

```
rpm -ivh PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
```

- Ubuntu의 경우 다음 명령을 실행합니다.

```
sudo dpkg -i PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
```

예: Fedora 14에서 수동으로 패키지 설치

Fedora 14 또는 32비트 머신의 경우 다음 단계에 따라 필수 패키지를 설치합니다.

1. 커널 버전과 필요한 GCC 버전을 확인하려면 다음 명령을 실행합니다.

   ```
   cat /proc/version
   ```

   이 명령의 출력에는 다음이 포함됩니다.

   ```
   Linux version 2.6.35.6-45.fc14.i686
   gcc version 4.5.1
   ```

2. 커널 버전에 해당하는 **kernel-devel**과 **gcc** 패키지를 가져옵니다.

   ```
   kernel-devel-2.6.35.6-45.fc14.i686.rpm
   gcc-4.5.1-4.fc14.i686.rpm
   ```

3. Fedora 14용 **make** 패키지를 가져옵니다.

   ```
   make-3.82-3.fc14.i686
   ```

4. 다음 명령을 루트 사용자로 실행하여 패키지를 설치합니다.

   ```
   rpm -ivh kernel-devel-2.6.35.6-45.fc14.i686.rpm
   rpm -ivh gcc-4.5.1.fc14.i686.rpm
   rpm -ivh make-3.82-3.fc14.i686
   ```


© Acronis International GmbH, 2003-2024

이 모든 패키지를 단일 rpm 명령으로 지정할 수 있습니다. 이러한 패키지를 설치하려면 종속성 해결을 위해 추가 패키지를 설치해야 합니다.

프록시 서버 설정 구성

보호 에이전트는 HTTP/HTTPS 프록시 서버를 통해 데이터를 전송할 수 있습니다. 서버는 HTTP 트래픽을 스캔하거나 방해하지 않고 HTTP 터널을 통과해야 합니다. 중간자 프록시는 지원되지 않습니다.

설치 중에 에이전트가 클라우드에 등록되기 때문에 에이전트를 설치하는 동안이나 사전에 프록시 서버 설정을 구성해야 합니다.

Windows용

제어판 > **인터넷 옵션** > **연결**에 프록시 서버가 구성되어 있는 경우에는 설치 프로그램이 레지스트리에서 프록시 서버 설정을 읽어와 자동으로 사용합니다.

다음 작업을 수행하려는 경우 이 절차를 사용합니다.

- 에이전트 설치 전에 프록시 설정 구성.
- 에이전트 설치 후에 프록시 설정 업데이트.

에이전트 설치 중에 프록시 설정을 구성하려면 "Windows에서 Protection 에이전트 설치"(72페이지) 항목을 참조하십시오.

참고

머신에 http-proxy.yaml 파일이 없을 때만 이 절차가 진행됩니다. 머신에 http-proxy.yaml 파일이 있으면 해당 파일의 프록시 설정을 업데이트해야 합니다. 이 파일의 설정이 aakore.yaml 파일의 설정을 재정의하기 때문입니다.

Cyber Protection Monitor를 사용하여 프록시 서버 설정을 구성하면 %programdata%\Acronis\Agent\var\aakore\http-proxy.yaml 파일이 생성됩니다. 자세한 내용은 "Cyber Protect Monitor에서 프록시 서버 설정 구성"(287페이지)을(를) 참조하십시오.

http-proxy.yaml 파일을 열려면 Windows의 관리자 그룹 멤버여야 합니다.

프록시 설정을 구성하려면

1. 새 텍스트 문서를 생성해 텍스트 편집기(예: 메모장)에서 엽니다.
2. 다음 라인을 복사하여 파일에 붙여넣습니다.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Global\HttpProxy]
"Enabled"=dword:00000001
"Host"="proxy.company.com"
"Port"=dword:000001bb
"Login"="proxy_login"
"Password"="proxy_password"
```


© Acronis International GmbH, 2003-2024

3. proxy.company.com을 프록시 서버 호스트 이름/IP 주소로 대체하고 000001bb는 포트 번호의 16진수 값으로 대체합니다. 예를 들어, 000001bb는 포트 443입니다.
4. 프록시 서버에 인증이 필요하다면 proxy_login과 proxy_password를 프록시 서버 자격 증명으로 대체합니다. 그렇지 않은 경우, 파일에서 이 라인을 삭제합니다.
5. 이 문서를 proxy.reg로 저장합니다.
6. 이 파일을 관리자로 실행합니다.
7. Windows 레지스트리를 편집할 것인지 확인합니다.
8. 이 워크로드에 에이전트가 아직 설치되어 있지 않으면 지금 설치합니다. 워크로드에 에이전트가 이미 설치되어 있으면 다음 단계를 계속 진행합니다.
9. 텍스트 편집기에서 %programdata%\Acronis\Agent\etc\aakore.yaml 파일을 엽니다.
   이 파일을 열려면 Windows의 관리자 그룹 멤버여야 합니다.
10. **env** 섹션을 찾거나 생성한 후 다음 라인을 추가합니다.

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

11. proxy_login과 proxy_password는 프록시 서버 자격 증명으로, proxy_address:port는 프록시 서버의 주소와 포트 번호로 대체합니다.
12. **시작** 메뉴에서 **실행**을 클릭한 다음 **cmd**를 입력하고 **확인**을 클릭합니다.
13. 다음 명령을 실행하여 aakore 서비스를 다시 시작합니다.

```
net stop aakore
net start aakore
```

14. 다음 명령을 실행하여 에이전트를 다시 시작합니다.

```
net stop mms
net start mms
```

macOS의 경우

다음 작업을 수행하려는 경우 이 절차를 사용합니다.

- 에이전트 설치 전에 프록시 설정 구성.
- 에이전트 설치 후에 프록시 설정 업데이트.

에이전트 설치 중에 프록시 설정을 구성하려면 "macOS에서 Protection 에이전트 설치"(76페이지) 항목을 참조하십시오.

프록시 설정을 구성하려면

1. /Library/Application Support/Acronis/Registry/Global.config 파일을 생성한 후 Text Edit 등의 텍스트 편집기에서 엽니다.
2. 다음 라인을 복사하여 파일에 붙여넣습니다.

```
<?xml version="1.0" ?>
<registry name="Global">
```


© Acronis International GmbH, 2003-2024

```
    <key name="HttpProxy">
        <value name="Enabled" type="Tdword">"1"</value>
        <value name="Host" type="TString">"proxy.company.com"</value>
        <value name="Port" type="Tdword">"443"</value>
        <value name="Login" type="TString">"proxy_login"</value>
        <value name="Password" type="TString">"proxy_password"</value>
    </key>
</registry>
```

3. proxy.company.com을 프록시 서버 호스트 이름/IP 주소로 대체하고 443은 포트 번호의 10진수 값으로 대체합니다.
4. 프록시 서버에 인증이 필요하다면 proxy_login과 proxy_password를 프록시 서버 자격 증명으로 대체합니다. 그렇지 않은 경우, 파일에서 이 라인을 삭제합니다.
5. 파일을 저장합니다.
6. 이 워크로드에 에이전트가 아직 설치되어 있지 않으면 지금 설치합니다. 워크로드에 에이전트가 이미 설치되어 있으면 다음 단계를 계속 진행합니다.
7. 텍스트 편집기에서 /Library/Application Support/Acronis/Agent/etc/aakore.yaml 파일을 엽니다.
8. **env** 섹션을 찾거나 생성한 후 다음 라인을 추가합니다.

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

9. proxy_login과 proxy_password는 프록시 서버 자격 증명으로, proxy_address:port는 프록시 서버의 주소와 포트 번호로 대체합니다.
10. **애플리케이션** > **유틸리티** > **터미널**로 이동합니다.
11. 다음 명령을 실행하여 aakore 서비스를 다시 시작합니다.

```
sudo launchctl stop aakore
sudo launchctl start aakore
```

12. 다음 명령을 실행하여 에이전트를 다시 시작합니다.

```
sudo launchctl stop acronis_mms
sudo launchctl start acronis_mms
```

Linux용

--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN --http-proxy-password=PASSWORD 매개변수를 사용하여 설치 파일을 실행합니다. 보호 에이전트 설치 후에 프록시 설정을 업데이트하려면 다음 절차를 진행합니다.

프록시 설정을 구성하려면

1. 텍스트 편집기에서 /etc/Acronis/Global.config 파일을 엽니다.
2. 다음 중 하나를 수행하십시오.

© Acronis International GmbH, 2003-2024

- 에이전트 설치 중에 프록시 설정을 지정한 경우 다음 섹션을 찾습니다.

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

- 에이전트 설치 중에 프록시 설정을 지정하지 않은 경우 다음 라인을 복사하여 파일에서 `<registry name="Global">...</registry>` 태그 사이에 붙여넣습니다.

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

3. `ADDRESS`를 프록시 서버 호스트 이름/IP 주소로 대체하고 `PORT`는 포트 번호의 10진수 값으로 대체합니다.
4. 프록시 서버에 인증이 필요하다면 `LOGIN` 및 `PASSWORD`를 프록시 서버 자격 증명으로 대체합니다. 그렇지 않은 경우, 파일에서 이 라인을 삭제합니다.
5. 파일을 저장합니다.
6. 텍스트 편집기에서 `/opt/acronis/etc/aakore.yaml` 파일을 엽니다.
7. **env** 섹션을 찾거나 생성한 후, 다음 행을 추가합니다.

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

8. `proxy_login`과 `proxy_password`는 프록시 서버 자격 증명으로, `proxy_address:port`는 프록시 서버의 주소와 포트 번호로 대체합니다.
9. 다음 명령을 실행하여 aakore 서비스를 다시 시작합니다.

```
sudo service aakore restart
```

10. 아무 디렉토리에서나 다음 명령을 실행하여 에이전트를 다시 시작합니다.

```
sudo service acronis_mms restart
```

부트 가능한 미디어

부트 가능한 미디어에서 작업할 때 프록시 서버를 통해 클라우드 스토리지에 액세스해야 할 수 있습니다. 프록시 서버 설정을 구성하려면 **도구** > **프록시 서버**를 클릭한 다음 프록시 서버 호스트 이름/IP 주소, 포트 및 자격 증명을 구성합니다.

© Acronis International GmbH, 2003-2024

Protection 에이전트 설치

"지원되는 운영 체제 및 환경"에 나열된 운영 체제를 실행하는 머신에서 에이전트를 설치할 수 있습니다. Cyber Protect 기능을 지원하는 운영 체제는 "운영 체제별 지원되는 Cyber Protect 기능"에 나열되어 있습니다.

Protection 에이전트 다운로드

에이전트를 설치하기 전 Cyber Protect 콘솔에서 설치 파일을 다운로드해야 합니다.

보호할 워크로드를 추가하는 동시에 에이전트를 다운로드하는 방법

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 우측 상단의 **장치 추가**를 클릭합니다.
3. **장치 추가** 패널에서 **채널 해제** 드롭 다운 메뉴에서 에이전트 버전을 선택합니다.
   - **이전 릴리스** - 이전 릴리스의 에이전트 버전을 다운로드합니다.
   - **현재** - 가장 최신 에이전트 버전을 다운로드합니다.
4. 추가하는 워크로드의 운영 체제에 해당하는 에이전트를 선택합니다.
   다른 이름으로 저장 대화창이 열립니다.
5. [Apple 실리콘(Apple M1 등) 프로세서 Mac 한정] **취소**를 클릭합니다. **Mac 추가** 패널이 열리면 **ARM 인스톨러 다운로드** 링크를 클릭합니다.
6. 에이전트 설치 프로그램 파일을 저장할 위치를 선택하고 **저장**을 클릭합니다.

추후 사용을 위한 에이전트 다운로드

1. Cyber Protect 콘솔 우측 상단에서 **사용자** 아이콘을 클릭합니다.
2. **다운로드**를 클릭합니다.
3. **다운로드** 대화창의 **채널 해제** 드롭 다운 메뉴에서 에이전트 버전을 선택합니다.
   - **이전 릴리스** - 이전 릴리스의 에이전트 버전을 다운로드합니다.
   - **현재** - 가장 최신 에이전트 버전을 다운로드합니다.
4. 사용 가능한 인스톨러 목록을 스크롤하여 필요한 에이전트 인스톨러를 찾은 다음, 행 끝에 있는 다운로드 아이콘을 클릭합니다.
   다른 이름으로 저장 대화창이 열립니다.
5. 에이전트 설치 프로그램 파일을 저장할 위치를 선택하고 **저장**을 클릭합니다.

Windows에서 Protection 에이전트 설치

사전 요구 사항

보호할 예정인 워크로드에 필요한 에이전트를 다운로드합니다. "Protection 에이전트 다운로드" (72페이지)을(를) 참조하십시오.

Agent for Windows를 설치하는 방법

1. 머신이 인터넷에 연결되어 있는지 확인합니다.
2. 관리자로 로그온한 다음 인스톨러를 시작합니다.

© Acronis International GmbH, 2003-2024

3. [선택 사항] **설치 설정 사용자 정의**를 클릭하고 원하는 대로 적절하게 변경합니다.
   - 설치할 컴포넌트를 변경하려면(예: Cyber Protection 모니터 또는 명령줄 도구의 설치를 비활성화하거나 맬웨어 방지 보호 에이전트 또는 URL 필터링 에이전트 설치).

     참고
     Windows 머신에서는 맬웨어 방지 보호 기능을 사용하려면 맬웨어 방지 보호 에이전트를 설치해야 하며, URL 필터링 기능을 사용하려면 URL 필터링 에이전트를 설치해야 합니다. 보호 계획에서 **안티바이러스 및 맬웨어 방지 보호** 및/또는 **URL 필터링** 모듈이 활성화되어 있으면 이러한 에이전트가 보호 대상 워크로드에 자동 설치됩니다.

   - Cyber Protection 서비스에서 워크로드 등록 방법 변경 **서비스 콘솔 사용**(기본값)에서 **자격 증명 사용** 또는 **등록 토큰 사용**으로 전환할 수 있습니다.
   - 설치 경로 변경.
   - 에이전트 서비스가 실행될 사용자 계정을 변경하기 위해. 자세한 내용은 "Windows 머신에서 로그온 계정 변경"(79페이지)을(를) 참조하십시오.
   - 프록시 서버 호스트 이름/IP 주소, 포트 및 자격 증명을 확인 또는 변경. Windows에서 프록시 서버가 사용하도록 설정되어 있는 경우 자동으로 감지되어 사용됩니다.
4. **설치**를 클릭합니다.
5. [Agent for VMware를 설치하는 경우에만 해당] 가상 머신을 백업 및 복구할 vCenter Server 또는 독립형 ESXi 호스트용 주소 및 액세스 자격 증명을 지정한 다음 **완료**를 클릭합니다.
   관리자 역할이 할당된 기존 계정을 사용하는 대신 vCenter Server 또는 ESXi 호스트 액세스 전용 계정을 사용하는 것이 좋습니다. 전용 계정에 필요한 권한에 대해 자세히 알아보려면 "Agent for VMware - 필수 권한"(635페이지) 항목을 참조하십시오.
6. [도메인 컨트롤러에 설치하는 경우에만 해당] 에이전트 서비스를 실행할 사용자 계정을 지한 다음 **완료**를 클릭합니다. 보안상의 이유로 설치 프로그램은 도메인 컨트롤러에서 새 계정을 자동으로 생성하지 않습니다.

   참고
   지정한 사용자 계정에 서비스로 로그온 권한이 부여되어 있어야 합니다. 이 계정이 이미 도메인 컨트롤러에 사용 중인 계정이어야 프로필 폴더가 해당 머신에서 생성될 수 있습니다.

   읽기 전용 도메인 컨트롤러에 에이전트를 설치하는 방법에 대한 자세한 내용은 이 기술 자료 문서를 참조하십시오.
7. 3단계에서 **서비스 콘솔 사용**이라는 기본 등록 방법을 유지한 경우 등록 화면이 나타날 때까지 기다린 후 다음 단계를 진행합니다. 그러지 않으면 추가 작업은 필요하지 않습니다.
8. 다음 중 하나를 수행하십시오.
   - 회사 관리자 계정으로 로그인하는 경우 회사의 워크로드를 등록합니다.
     a. **워크로드 등록**을 클릭합니다.
     b. 열려 있는 브라우저 창에서 Cyber Protect 콘솔에 로그인하고 등록 상세정보를 검토합니다.
     c. **계정 등록** 목록에서 워크로드를 등록할 사용자 계정을 선택합니다.
     d. **코드 확인**을 클릭하고 **등록 확인**을 클릭합니다.

© Acronis International GmbH, 2003-2024

- 파트너 관리자 계정으로 로그인하는 경우 고객의 워크로드를 등록합니다.
  a. **워크로드 등록**을 클릭합니다.
  b. 열려 있는 브라우저 창에서 Cyber Protect 콘솔에 로그인하고 등록 상세정보를 검토합니다.
  c. **계정 등록** 목록에서 워크로드를 등록할 고객의 사용자 계정을 선택합니다.
  d. **코드 확인**을 클릭하고 **등록 확인**을 클릭합니다.
- **등록 정보 표시**를 클릭합니다. 설치 프로그램에 등록 링크와 등록 코드가 표시됩니다. 현재 머신에서 워크로드 등록을 완료할 수 없으면 여기에 나와 있는 등록 링크와 코드를 복사하여 다른 머신에서 등록 단계를 진행하십시오. 이 경우 등록 양식에 등록 코드를 입력해야 할 수 있습니다. 등록 코드는 1시간 동안 유효합니다.

  또는, **모든 장치** > **추가**를 클릭하고 **코드를 통한 등록**으로 스크롤을 내린 다음 **등록**을 클릭해 등록 양식에 액세스할 수 있습니다.

  참고
  등록을 확인할 때까지 설정 프로그램을 종료하지 마십시오. 등록을 다시 시작하려면 설정 프로그램을 다시 시작한 다음, 설치 과정을 반복합니다.

  그러면 Cyber Protect 콘솔에 로그인하는 데 사용된 계정에 워크로드가 할당됩니다.
- 명령줄을 사용하여 수동으로 워크로드를 등록합니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 "수동으로 워크로드 등록 및 등록 해제"(110페이지)을(를) 참조하십시오.

9. [테넌트가 규제 준수 모드인 계정에 등록된 에이전트의 경우] 암호화 암호를 설정합니다.

Linux에서 Protection 에이전트 설치

준비

- 보호할 예정인 머신에 에이전트를 다운로드 합니다. "Protection 에이전트 다운로드"(72페이지)을(를) 참조하십시오.
- 필요한 Linux 패키지가 머신에 설치되어 있는지 확인하십시오.
- SUSE Linux에서 에이전트를 설치할 때는 sudo가 아닌 su -를 사용해야 합니다. 이 옵션을 사용하지 않으면 Cyber Protect 콘솔을 통해 에이전트 등록을 시도할 때 다음 오류가 발생합니다. 웹 브라우저를 시작하지 못했습니다. 사용 가능한 디스플레이가 없습니다.

  SUSE 등의 일부 Linux 배포판에서는 sudo 사용 시에 DISPLAY 변수가 전달되지 않으므로 인스톨러가 GUI(그래픽 사용자 인터페이스)에서 브라우저를 열 수 없습니다.

설치

Agent for Linux를 설치하려면 2GB 이상의 디스크 여유 공간이 필요합니다.

Agent for Linux를 설치하려면

1. 머신이 인터넷에 연결되어 있는지 확인합니다.
2. 루트 사용자로 설치 파일이 있는 디렉토리로 이동하여 파일을 실행 가능하도록 설정한 후에 실행합니다.

© Acronis International GmbH, 2003-2024

```
chmod +x <installation file name>
```

```
./<installation file name>
```

네트워크에 프록시 서버가 활성화되어 있으면 설치 파일을 실행할 때 서버 호스트 이름/IP 주소 및 포트를 `--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN --http-proxy-password=PASSWORD` 형식으로 지정합니다.

Cyber Protection 서비스에서 머신을 등록하는 기본 방법을 변경하려면 다음 매개 변수 중 하나로 설치 파일을 실행하십시오.

- `--register-with-credentials` – 설치하는 동안 사용자 이름과 비밀번호를 묻기 위해
- `--token=STRING` – 등록 토큰을 사용하기 위해
- `--skip-registration` – 등록을 생략하기 위해

3. 설치할 에이전트의 확인란을 선택합니다. 다음 에이전트를 선택할 수 있습니다.
   - Agent for Linux
   - Agent for Virtuozzo
   - Agent for Oracle
   - Agent for MySQL/MariaDB

   Agent for Virtuozzo, Agent for Oracle 및 Agent for MySQL/MariaDB를 사용하려면 Agent for Linux(64비트)도 설치해야 합니다.
4. 2단계에서 기본 등록 방법을 유지한 경우 다음 단계를 진행합니다. 그렇지 않으면 Cyber Protection 서비스에 대한 사용자 이름과 비밀번호를 입력하거나 토큰을 사용하여 머신이 등록될 때까지 기다리십시오.
5. 다음 중 하나를 수행하십시오.
   - 회사 관리자 계정으로 로그인하는 경우 회사의 워크로드를 등록합니다.
     a. **워크로드 등록**을 클릭합니다.
     b. 열려 있는 브라우저 창에서 Cyber Protect 콘솔에 로그인하고 등록 상세정보를 검토합니다.
     c. **계정 등록** 목록에서 워크로드를 등록할 사용자 계정을 선택합니다.
     d. **코드 확인**을 클릭하고 **등록 확인**을 클릭합니다.
   - 파트너 관리자 계정으로 로그인하는 경우 고객의 워크로드를 등록합니다.
     a. **워크로드 등록**을 클릭합니다.
     b. 열려 있는 브라우저 창에서 Cyber Protect 콘솔에 로그인하고 등록 상세정보를 검토합니다.
     c. **계정 등록** 목록에서 워크로드를 등록할 고객의 사용자 계정을 선택합니다.
     d. **코드 확인**을 클릭하고 **등록 확인**을 클릭합니다.
   - **등록 정보 표시**를 클릭합니다. 설치 프로그램에 등록 링크와 등록 코드가 표시됩니다. 현재 머신에서 워크로드 등록을 완료할 수 없으면 여기에 나와 있는 등록 링크와 코드를 복사하여 다른 머신에서 등록 단계를 진행하십시오. 이 경우 등록 양식에 등록 코드를 입력해야 할 수 있습니다. 등록 코드는 1시간 동안 유효합니다.

© Acronis International GmbH, 2003-2024

또는, **모든 장치** > **추가**를 클릭하고 **코드를 통한 등록**으로 스크롤을 내린 다음 **등록**을 클릭해 등록 양식에 액세스할 수 있습니다.

참고
등록을 확인할 때까지 설정 프로그램을 종료하지 마십시오. 등록을 다시 시작하려면 설정 프로그램을 다시 시작한 다음, 설치 과정을 반복합니다.

그러면 Cyber Protect 콘솔에 로그인하는 데 사용된 계정에 워크로드가 할당됩니다.

- 명령줄을 사용하여 수동으로 워크로드를 등록합니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 "수동으로 워크로드 등록 및 등록 해제"(110페이지)을(를) 참조하십시오.

6. [테넌트가 규제 준수 모드인 계정에 등록된 에이전트의 경우] 암호화 암호를 설정합니다.
7. UEFI 보안 부팅이 머신에서 활성화되어 있는 경우에는 설치 후에 시스템을 다시 시작해야 한다는 메시지가 표시됩니다. 어느 비밀번호(루트 사용자의 비밀번호 또는 "acronis")를 사용해야 하는지 잘 기억해 두십시오.

참고
설치 시에는 커널 모듈 서명에 사용되는 새 키가 생성됩니다. 머신을 다시 시작하여 MOK (Machine Owner Key) 목록에 이 새 키를 등록해야 합니다. 새 키를 등록하지 않으면 에이전트가 작동하지 않습니다. 에이전트 설치 후 UEFI 보안 부팅을 활성화하는 경우에는 에이전트를 다시 설치해야 합니다.

8. 설치가 완료되면 다음 중 하나를 수행하십시오.
   - 이전 단계에서 시스템을 다시 시작하라는 메시지가 표시된 경우 **다시 시작**을 클릭합니다. 시스템 다시 시작 중에 MOK(Machine Owner Key) 관리를 선택하고, **MOK 등록**을 선택한 다음, 이전 단계에서 권장된 비밀번호를 사용하여 키를 등록합니다.
   - 그렇지 않은 경우, **종료**를 클릭합니다.

문제 해결 정보가 다음 파일에 제공됩니다: `/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL`

macOS에서 Protection 에이전트 설치

사전 요구 사항

보호할 예정인 워크로드에 필요한 에이전트를 다운로드합니다. "Protection 에이전트 다운로드"(72페이지)을(를) 참조하십시오.

Mac(x64 또는 ARM64)에 에이전트를 설치하는 방법

1. 머신이 인터넷에 연결되어 있는지 확인합니다.
2. 설치 파일(.dmg)을 두 번 클릭합니다.
3. 운영 체제가 설치 디스크 이미지를 마운트하는 동안 기다립니다.
4. **설치**를 두 번 클릭합니다.
5. 네트워크에서 프록시 서버가 사용하도록 설정되어 있는 경우 메뉴 표시줄에서 **보호 에이전트**, **프록시 서버 설정**을 차례로 클릭한 다음 프록시 서버 호스트 이름/IP 주소, 포트 및 자격 증명을 지정합니다.

© Acronis International GmbH, 2003-2024

6. 메시지가 표시되면 관리자 자격 증명을 제공합니다.
7. **계속**을 클릭합니다.
8. 등록 화면이 나타날 때까지 기다립니다.
9. 다음 중 하나를 수행하십시오.
   - 회사 관리자 계정으로 로그인하는 경우 회사의 워크로드를 등록합니다.
     a. **워크로드 등록**을 클릭합니다.
     b. 열려 있는 브라우저 창에서 Cyber Protect 콘솔에 로그인하고 등록 상세정보를 검토합니다.
     c. **계정 등록** 목록에서 워크로드를 등록할 사용자 계정을 선택합니다.
     d. **코드 확인**을 클릭하고 **등록 확인**을 클릭합니다.
   - 파트너 관리자 계정으로 로그인하는 경우 고객의 워크로드를 등록합니다.
     a. **워크로드 등록**을 클릭합니다.
     b. 열려 있는 브라우저 창에서 Cyber Protect 콘솔에 로그인하고 등록 상세정보를 검토합니다.
     c. **계정 등록** 목록에서 워크로드를 등록할 고객의 사용자 계정을 선택합니다.
     d. **코드 확인**을 클릭하고 **등록 확인**을 클릭합니다.
   - **등록 정보 표시**를 클릭합니다. 설치 프로그램에 등록 링크와 등록 코드가 표시됩니다. 현재 머신에서 워크로드 등록을 완료할 수 없으면 여기에 나와 있는 등록 링크와 코드를 복사하여 다른 머신에서 등록 단계를 진행하십시오. 이 경우 등록 양식에 등록 코드를 입력해야 할 수 있습니다. 등록 코드는 1시간 동안 유효합니다.
     또는, **모든 장치** > **추가**를 클릭하고 **코드를 통한 등록**으로 스크롤을 내린 다음 **등록**을 클릭해 등록 양식에 액세스할 수 있습니다.

     참고
     등록을 확인할 때까지 설정 프로그램을 종료하지 마십시오. 등록을 다시 시작하려면 설정 프로그램을 다시 시작한 다음, 설치 과정을 반복합니다.

     그러면 Cyber Protect 콘솔에 로그인하는 데 사용된 계정에 워크로드가 할당됩니다.
   - 명령줄을 사용하여 수동으로 워크로드를 등록합니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 "수동으로 워크로드 등록 및 등록 해제"(110페이지)을(를) 참조하십시오.
10. [테넌트가 규제 준수 모드인 계정에 등록된 에이전트의 경우] 암호화 암호를 설정합니다.
11. macOS 버전이 Mojave 10.14.x 이상인 경우, 보호 에이전트에 대한 전체 디스크 액세스 권한을 부여하여 백업 작업을 활성화합니다.
    관련 지침은 Cyber Protection 에이전트에 '전체 디스크 액세스' 권한 부여(64657)를 참조하십시오.
12. 원격 데스크탑 기능을 사용하려면 Connect 에이전트에 필요한 시스템 권한을 부여합니다. 자세한 내용은 "Connect 에이전트에 필요한 시스템 권한 부여"(77페이지)을(를) 참조하십시오.

Connect 에이전트에 필요한 시스템 권한 부여

전체 디스크 액세스 권한과 함께 macOS 워크로드의 원격 데스크탑 기능에서 모든 기능을 활성화하려면 Connect 에이전트에 다음 권한을 부여해야 합니다.

© Acronis International GmbH, 2003-2024

- 화면 녹화 - NEAR를 통한 macOS 워크로드의 화면 녹화를 활성화합니다. 이 권한을 부여할 때까지는 모든 원격 제어 연결이 거부됩니다.
- 접근성 - NEAR를 통한 제어 모드의 원격 연결을 활성화합니다.
- 마이크 - NEAR를 통한 원격 macOS 워크로드에서 로컬 워크로드로의 사운드 리디렉션을 활성화합니다. 사운드 리디렉션 기능을 활성화하려면 워크로드에 사운드 캡처 드라이버를 설치해야 합니다. 자세한 내용은 "원격 사운드 리디렉션"(901페이지)을(를) 참조하십시오.
- 자동화 - 휴지통 비우기 작업을 활성화합니다.

macOS 워크로드에서 에이전트를 시작하고 나면 에이전트에 이러한 권한이 있는지를 확인하며, 필요한 경우 권한 부여를 요청하는 메시지가 표시됩니다.

화면 녹화 권한을 부여하려면

1. Cyber Protect 에이전트에 **필요한 시스템 권한 부여** 대화 상자에서 **시스템 권한 설정**을 클릭합니다.
2. **시스템 권한** 대화 상자에서 **화면 녹화 권한 요청**을 클릭합니다.
3. **시스템 기본 설정 열기**를 클릭합니다.
4. **Connect 에이전트**를 선택합니다.

워크로드에 원격으로 액세스하려고 하는데 에이전트에 권한이 없으면 화면 녹화 권한 요청 대화 상자가 표시됩니다. 로컬 사용자만 해당 대화 상자에서 대답을 선택할 수 있습니다.

접근성 권한을 부여하려면

1. Cyber Protect 에이전트에 **필요한 시스템 권한 부여** 대화 상자에서 **시스템 권한 설정**을 클릭합니다.
2. **시스템 권한** 대화 상자에서 **접근성 권한 요청**을 클릭합니다.
3. **시스템 기본 설정 열기**를 클릭합니다.
4. 창 왼쪽 아래에서 자물쇠 아이콘을 클릭하면 잠금이 해제된 아이콘으로 변경됩니다. 변경을 하려면 관리자 암호를 입력하라는 메시지가 표시됩니다.
5. **Connect 에이전트**를 선택합니다.

마이크 권한을 부여하려면

1. Connect 에이전트에 **필요한 시스템 권한 부여** 대화 상자에서 **시스템 권한 설정**을 클릭합니다.
2. **시스템 권한** 대화 상자에서 **마이크 권한 요청**을 클릭합니다.
3. **확인**을 클릭합니다.

참고
에이전트가 제공된 권한을 활용하여 워크로드의 사운드를 리디렉션할 수 있도록 하려면 macOS 워크로드에 사운드 캡처 드라이버도 설치해야 합니다. 자세한 내용은 "원격 사운드 리디렉션"(901페이지)을(를) 참조하십시오.

자동화 권한을 부여하려면

1. Connect 에이전트에 **필요한 시스템 권한 부여** 대화 상자에서 **시스템 권한 설정**을 클릭합니다.
2. **시스템 권한** 대화 상자에서 **자동화 권한 요청**을 클릭합니다.

© Acronis International GmbH, 2003-2024

Windows 머신에서 로그온 계정 변경

컴퍼넌트 선택 화면에서 **에이전트 서비스를 위한 로그온 계정**을 지정해 서비스를 실행할 계정을 정의합니다. 다음 중 하나를 선택합니다.

- **서비스 사용자 계정 사용**(에이전트 서비스용 기본값)

  서비스 사용자 계정은 서비스를 실행하는 데 사용되는 Windows 시스템 계정입니다. 이 설정의 이점은 도메인 보안 정책이 이 계정의 사용자 권한에 영향을 미치지 않는다는 점입니다. 기본적으로 에이전트는 **로컬 시스템** 계정 하에서 실행됩니다.
- **새 계정 생성**

  계정 이름은 해당 에이전트에 대해 Agent User로 지정됩니다.
- **다음 계정 사용**

  도메인 컨트롤러에 에이전트를 설치하는 경우 시스템에 각 에이전트의 기존 계정(또는 동일한 계정)을 지정하라는 메시지가 표시됩니다. 보안상의 이유로 시스템은 도메인 컨트롤러에서 새 계정을 자동으로 생성하지 않습니다.

  도메인 컨트롤러에서 설치 프로그램을 실행할 때 지정한 사용자 계정에 서비스로 로그온 권한이 부여되어 있어야 합니다. 이 계정이 이미 도메인 컨트롤러에 사용 중인 계정이어야 프로필 폴더가 해당 머신에서 생성될 수 있습니다.

  읽기 전용 도메인 컨트롤러에 에이전트를 설치하는 방법에 대한 자세한 내용은 이 기술 자료 문서를 참조하십시오.

새 계정 생성 또는 **다음 계정 사용** 옵션을 선택하는 경우 도메인 보안 정책이 관련 계정의 권한에 영향을 미치지 않는지 확인하십시오. 설치 중 계정에 할당되어 있는 사용자 권한이 박탈되는 경우 컴퍼넌트가 올바로 작동하지 않거나 아예 작동하지 않을 수 있습니다.

로그온 계정에 필요한 권한

보호 에이전트는 Windows 머신에서 관리 대상 머신 서비스(MMS)로 실행됩니다. 에이전트가 실행되는 계정에는 해당 에이전트가 올바르게 작동할 수 있는 특정 권한이 있어야 합니다. 따라서 MMS 사용자에게는 다음과 같은 권한이 할당되어야 합니다.

1. **백업 작업자** 및 **관리자** 그룹에 포함됨. 도메인 컨트롤러에서 사용자는 **도메인 관리자** 그룹에 포함되어 있어야 합니다.
2. **전체 제어** 권한이 `%PROGRAMDATA%\Acronis`(Windows XP 및 Server 2003, `%ALLUSERSPROFILE%\Application Data\Acronis`) 폴더 및 해당 하위 폴더에 대해 부여됩니다.
3. 다음 키 중 특정 레지스트리 키에 대해 **전체 제어** 권한이 부여됩니다. `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`.
4. 다음의 사용자 권한이 할당됨:
   - 서비스로 로그온
   - 프로세스에 대한 메모리 할당량 조정
   - 프로세스 수준 토큰 교체
   - 펌웨어 환경 값 수정

© Acronis International GmbH, 2003-2024

사용자 권한 할당 방법

아래 지침에 따라 사용자 권한을 할당하십시오(이 예시에서는 **서비스로 로그온** 사용자 권한을 사용하며, 다른 사용자 권한에 대한 단계와 동일합니다).

1. 관리자 권한이 있는 계정을 사용해 컴퓨터에서 로그온합니다.
2. **제어판**에서 **관리 도구**를 열고(또는 Win+R을 클릭하고 **control admintools**를 입력한 후 엔터를 누르고) **로컬 보안 정책**을 엽니다.
3. **로컬 정책**을 확장하고 **사용자 권한 할당**을 클릭합니다.
4. 오른쪽 창에서 **서비스로 로그온**을 마우스 오른쪽으로 클릭하고 **속성**을 선택합니다.
5. **사용자 또는 그룹 추가...** 버튼을 클릭하여 새 사용자를 추가합니다.
6. **사용자, 컴퓨터, 서비스 계정 또는 그룹 선택** 창에서 입력하려는 사용자를 찾아 **확인**을 클릭합니다.
7. **서비스로 로그온 속성**에서 **확인**을 클릭하여 변경 사항을 저장합니다.

중요
서비스로 로그온 사용자 권한에 추가한 사용자가 **로컬 보안 정책**의 **서비스로 로그온 거부** 정책에 포함되어 있지 않은지 확인하십시오.

설치가 완료된 후에는 수동으로 로그온 계정을 변경하지 않는 것이 좋습니다.

컴퍼넌트의 동적 설치 및 설치 제거

에이전트 버전 15.0.26986(2021년 5월 릴리스) 이상으로 보호되는 Windows 워크로드의 경우 다음 컴포넌트가 동적으로 설치됩니다. 즉, 보호 계획에 필요한 경우에만 설치됩니다.

- URL 필터링 에이전트 - URL 필터링 기능이 정상 작동하려면 필요한 에이전트입니다.
- 맬웨어 방지 보호 에이전트 – 맬웨어 방지 보호 기능을 작동하는 데 필요합니다.
- 데이터 손실 방지 에이전트 - 장치 제어 기능을 작동하는 데 필요합니다.

기본적으로 이러한 컴퍼넌트는 설치되지 않았습니다. 다음 모듈 중 하나가 활성화된 계획에 의해 워크로드가 보호되면 각 컴퍼넌트가 자동으로 설치됩니다.

- 안티바이러스 및 안티맬웨어 보호 기능
- URL 필터링
- 장치 제어

마찬가지로, 보호 계획에서 맬웨어 방지 보호, URL 필터링 또는 장치 제어 기능이 더 이상 필요하지 않은 경우 각 컴퍼넌트가 자동으로 제거됩니다.

컴퍼넌트의 동적 설치 또는 설치 제거는 보호 계획을 변경한 후 최대 10분이 걸립니다. 그러나 다음 작동 중 무엇이라도 실행되고 있다면 동적 설치 또는 설치 제거는 이 작동이 완료된 후에 시작됩니다.

- 백업
- 복구

© Acronis International GmbH, 2003-2024

- 백업 복제
- 가상 머신 복제
- 복제본 테스트
- 백업에서 가상 머신 실행(종료 포함)
- 재해 복구 장애 조치
- 재해 복구 장애 복구
- 스크립트 실행(사이버 스크립트 작성 기능의 경우)
- 패치 설치
- ESXi 구성 백업

무인 설치 또는 제거

Windows에서 무인 설치 또는 제거

Windows에서는 다음과 같은 방식으로 무인 설치 또는 설치 제거를 수행할 수 있습니다.

- 설치 프로그램의 EXE 파일 사용(명령줄에서 설치 매개변수 지정).
- 설치 프로그램에서 추출한 MSI 파일 사용(다음 방식 중 하나로 설치 매개변수 지정)
  - MST 파일
  - 명령줄에서 직접

EXE 파일을 통한 무인 설치 및 설치 제거

이 유형의 무인 설치를 수행할 때는 설치 프로그램을 다운로드한 후 필요한 설치 매개변수를 지정하여 명령줄에서 해당 프로그램을 시작합니다. 사용할 수 있는 매개변수를 확인하려면 "무인 설치(EXE)용 매개변수"(83페이지) 항목을 참조하십시오.

설치 패키지, MSI 및 MST 파일을 미리 추출할 필요는 없습니다.

에이전트와 컴포넌트 설치 및 설치 제거(EXE)

EXE 파일을 사용하여 무인 설치를 수행하려면 명령줄에서 설치 매개변수를 지정하여 설치 프로그램을 실행합니다.

설치 프로그램을 다운로드하려면 Cyber Protect 콘솔의 오른쪽 상단에 있는 계정 아이콘을 클릭하고 **다운로드**를 클릭합니다. **장치 추가** 창에서도 다운로드 링크를 사용할 수 있습니다.

에이전트와 컴포넌트를 설치하려면

1. 관리자로 명령줄 인터페이스를 시작하고 설치 프로그램의 EXE 파일이 있는 위치로 이동합니다.
2. 설치 프로그램을 시작하고 설치 매개변수를 지정하려면 다음 명령을 실행합니다.

   ```
   <file path>/<EXE file><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
   ```

   각 매개변수는 공백으로 구분하고, 매개변수의 값은 쉼표(공백 없음)로 구분합니다. 예:

© Acronis International GmbH, 2003-2024

```
C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
components=agentForWindows,agentForSql,commandLine --install-dir="C:\Program
Files\BackupClient" --reg-address=https://eu2-cloud.company.com --reg-token=34F6-
8C39-4A5C --quiet
```

사용 가능한 매개변수와 해당 값을 확인하려면 "무인 설치(EXE)용 매개변수"(83페이지) 항목을 참조하십시오.

예

- Agent for Windows, 맬웨어 방지 에이전트, URL 필터링 에이전트, 명령줄 도구 및 Cyber Protect 모니터 설치. 사용자 이름과 암호를 사용하여 Cyber Protection 서비스에서 워크로드 등록.

```
C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
components=agentForWindows,agentForAmp,commandLine,trayMonitor --install-
dir="C:\Program Files\BackupClient" --agent-account=system --reg-
address=https://cloud.company.com --reg-login=johndoe --reg-password=johnspassword
```

- Agent for Windows, 명령줄 도구, Cyber Protect Monitor 설치. Windows에서 에이전트 서비스용 새 로그온 계정 생성. 토큰을 사용하여 Cyber Protection 서비스에서 워크로드 등록.

```
C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
components=agentForWindows,commandLine,trayMonitor --install-dir="C:\Program
Files\BackupClient" --agent-account=new --reg-address=https://eu2-cloud.company.com -
-reg-token=34F6-8C39-4A5C
```

- Agent for Windows, 명령줄 도구, Agent for Oracle, Cyber Protect 모니터 설치. 사용자 이름과 비밀번호를 사용하여 Cyber Protection 서비스에서 머신 등록.

```
C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
components=agentForWindows,commandLine,agentForOracle,trayMonitor --install-
dir="C:\Program Files\BackupClient" --language=en --agent-account=system --reg-
address=https://cloud.company.com --reg-login=johndoe --reg-password=johnspassword
```

- Agent for Windows, 명령줄 도구, Cyber Protect Monitor 설치. 사용자 인터페이스 언어를 독일어로 설정. 토큰을 사용하여 Cyber Protection 서비스에서 머신 등록. HTTP 프록시 설정.

```
C:\Users\Administrator\Downloads\AgentForWindows_web.exe --add-
components=agentForWindows,commandLine,agentForOracle,trayMonitor --install-
dir="C:\Program Files\BackupClient"--language=de --agent-account=system --reg-
address=https://eu2-cloud.company.com --reg-token=34F6-8C39-4A5C --http-proxy-
address=https://my-proxy.company.com:80 --http-proxy-login=tomsmith --http-proxy-
password=tomspassword
```

설치된 컴포넌트를 제거하려면

1. 관리자로 명령줄 인터페이스를 시작하고 `%ProgramFiles%\BackupClient\RemoteInstall`로 이동합니다.
2. 다음 명령을 실행합니다.

© Acronis International GmbH, 2003-2024

```
web_installer.exe --remove-components=<value 1>,<value 2> --quiet
```

사용 가능한 매개변수와 해당 값을 확인하려면 "무인 설치(EXE)용 매개변수"(83페이지) 항목을 참조하십시오.

예

- Cyber Protect Monitor 설치 제거.

```
C:\Program Files\BackupClient\RemoteInstall\web_installer.exe --remove-
components=trayMonitor --quiet
```

에이전트 설치를 제거하려면

1. 관리자로 명령줄 인터페이스를 시작하고 %Program Files%\Common Files\Acronis\BackupAndRecovery로 이동합니다.
2. 다음 명령을 실행합니다.

```
Uninstaller.exe --quiet --delete-all-settings
```

사용 가능한 매개변수와 해당 값을 확인하려면 "무인 설치(EXE)용 매개변수"(83페이지) 항목을 참조하십시오.

예

- Agent for Windows 및 모든 컴포넌트 설치 제거. 모든 로그, 작업 및 구성 설정 삭제.

```
C:\Program Files\Common Files\Acronis\BackupAndRecovery\Uninstaller.exe --quiet --
delete-all-settings
```

- 암호로 보호된 Agent for Windows 및 모든 컴포넌트 설치 제거. 모든 로그, 작업 및 구성 설정 삭제.

```
C:\Program Files\Common Files\Acronis\BackupAndRecovery\Uninstaller.exe --anti-
tamper-password=<password> --quiet --delete-all-settings
```

무인 설치(EXE)용 매개변수

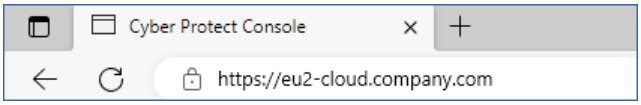
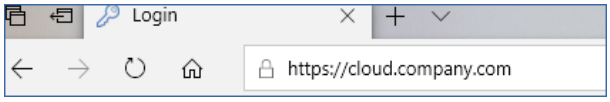
아래 표에는 EXE 파일을 통한 무인 설치용 매개변수가 요약되어 있습니다.

매개변수	설명
일반 매개변수	
--add-components=<component1,component2,...,componentN>	설치될 컴퍼넌트. 사용 가능한 컴포넌트의 전체 목록은 "무인 설치용 컴포넌트(EXE)"(88페이지) 항목을 참조하십시오. 여러 컴포넌트를 지정할 때는 각 컴포넌트를 쉼표로 구

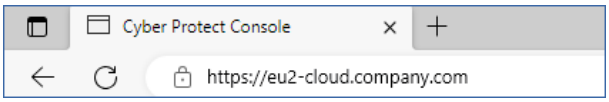
© Acronis International GmbH, 2003-2024

매개변수	설명
	분합니다. 쉼표 앞뒤에 공백을 추가하면 안 됩니다. 이미 설치되어 있는 컴포넌트를 지정하면 설치 프로그램 버전과 설치되어 있는 컴포넌트 버전에 따라 해당 컴포넌트가 복구되거나 업데이트됩니다. 이 매개변수를 지정하지 않으면 설치를 수행하는 머신에 따라 기본 컴포넌트 세트가 설치됩니다. 예를 들어 Agent for SQL은 MS SQL Server를 실행하는 머신에만 설치됩니다.
`--install-dir=<경로>`	선택한 컴포넌트를 설치할 폴더입니다. 지정한 폴더가 없는 경우에는 새로 생성됩니다. 이 매개변수를 지정하지 않으면 기본 폴더가 사용됩니다. `C:\Program Files\BackupClient`입니다.
`--log-dir=<경로>`	설치 로그를 저장할 폴더입니다. 이 매개변수를 지정하지 않으면 기본 폴더인 `%ProgramData%\Acronis\InstallationLogs`가 사용됩니다.
`--language=<코드>`	제품 언어. en, bn, bg, cs, da, de, es, fr, ko, id, it, hi, hu, ms, nl, ja, nb, pl, pt, pt_BR, ru, fi, sr, sv, th, tr, vi, zh, zh_TW 값을 사용할 수 있습니다. 이 매개변수를 지정하지 않는 경우 설치를 수행하는 머신의 시스템 언어가 상기 나열된 언어 중 하나라면 시스템 언어가 사용됩니다. 그 외의 모든 경우에는 값이 en으로 설정됩니다.
`--quiet`	그래픽 사용자 인터페이스를 표시하지 않고 설치 프로그램을 실행하려면 이 매개변수를 사용합니다. 이 매개변수는 `--register-only` 매개변수와 함께 사용하면 안 됩니다.
`--help`	명령줄에서 사용할 수 있는 모든 매개변수 및 해당 설명의 목록을 확인하려면 이 매개변수를 사용합니다.
`--fss-onboarding-auto-start`	무인 설치 이후 온보딩 마법사를 표시하려면 이 매개변수와 `--quiet` 매개변수를 함께 사용합니다.
등록 매개변수	
`--registration={skip | by-credentials | by-token | device-flow}`	설치 후 에이전트 등록 방법을 선택하려면 이 매개변수를 사용합니다. 등록을 건너뛰려면 `skip`을 지정합니다. `--register-only` 매개변수를 사용하면 에이전트를 나중에 등록할 수 있

© Acronis International GmbH, 2003-2024

매개변수	설명
	습니다. 자격 증명을 사용하여 에이전트를 등록하려면 `by-credentials`를 지정한 후 `--reg-login` 및 `--reg-password` 매개변수를 사용합니다. `--reg-login` 및 `--reg-password` 매개변수만 사용할 수도 있습니다. 이 경우 `--registration=by-credentials`는 원하는 경우에만 지정하면 됩니다. 등록 토큰을 사용하여 에이전트를 등록하려면 `by-token`을 지정한 후 `--reg-token` 매개변수를 사용합니다. `--reg-token` 매개변수만 사용할 수도 있습니다. 이 경우 `--registration=by-token`은 원하는 경우에만 지정하면 됩니다. OAuth 2.0 프로토콜을 사용하여 에이전트를 등록하려면 `device-flow`를 지정합니다. 이 경우 설치가 완료되면 등록 페이지가 자동으로 열립니다. `--registration=device-flow` 사용 시에는 정확한 데이터센터 주소를 `--reg-address` 매개변수의 값으로 지정합니다. 이 주소는 Cyber Protection 서비스에 **로그인하고 나면** 표시되는 URL입니다. 예를 들어 `https://eu2-cloud.company.com`을 지정할 수 있습니다.  `--registration=device-flow`는 `--quiet` 매개변수와 함께 사용하면 안 됩니다.
`--reg-address=<url>`	Cyber Protection 서비스의 URL입니다. 이 매개변수는 `--reg-login` 및 `--reg-password` 매개변수와 함께 사용할 수도 있고 `--reg-token` 매개변수와 함께 사용할 수도 있습니다. • 이 매개변수를 `--reg-login` 및 `--reg-password` 매개변수와 함께 사용할 때는 Cyber Protection 서비스에 **로그인**하는 데 사용하는 주소를 지정합니다. 예를 들어 `https://cloud.company.com`을 지정할 수 있습니다.  • 이 매개변수를 `--reg-token` 매개변수와 함께 사용할 때는 정확한 데이터센터 주소를 지정합니다. 이 주소는 Cyber Protection 서비스에 **로그인하고 나면** 표시되는 URL입니다. 예: `https://eu2-cloud.company.com`.

© Acronis International GmbH, 2003-2024

매개변수	설명
	 https://cloud.company.com과 --reg-token 매개변수를 함께 사용하면 안 됩니다.
--reg-login=<로그인> --reg-password=<암호>	Cyber Protection 서비스에서 에이전트를 등록할 계정의 자격 증명입니다. 파트너 관리자 계정은 사용할 수 없습니다. 이러한 매개변수를 사용할 때는 원하는 경우에만 --registration 매개변수를 지정하면 됩니다. 이러한 매개변수와 --reg-token 매개변수를 함께 사용하면 안 됩니다.
--reg-token=<토큰>	등록 토큰입니다. 등록 토큰은 하이픈에 의해 세 부분으로 구분된 12자리 문자열입니다. 토큰 생성 방법에 대한 자세한 내용은 "등록 토큰 생성"(156페이지) 항목을 참조하십시오. 이 매개변수를 사용할 때는 원하는 경우에만 --registration 매개변수를 지정하면 됩니다. 이 매개변수는 --reg-login 및 --reg-password 매개변수와 함께 사용하면 안 됩니다.
--register-only	설치를 건너뛰고 OAuth 2.0 프로토콜을 사용하여 에이전트를 등록하려면 이 매개변수를 사용합니다(device-flow). 이 경우 설치가 완료되면 등록 페이지가 자동으로 열립니다. --register-only는 --quiet 매개 변수와 함께 사용하면 안 됩니다.
에이전트 서비스용 로그온 계정	
--agent-account={system | new | custom} 또는 --agent-account-login=<로그인> --agent-account-password=<암호>	에이전트 서비스가 실행될 로그온 계정을 지정하려면 이 매개변수를 사용합니다. 로그온 계정에 대한 자세한 내용은 "Windows 머신에서 로그온 계정 변경"(79페이지) 항목을 참조하십시오. **로컬 시스템** 계정을 사용하려면 --agent-account=system을 지정하거나 명령에서 --agent-account 매개변수를 사용하지 않습니다. 자동으로 생성되는 새 로그온 계정인 **Acronis Agent User**에서 에이전트 서비스가 실행되도록 하려면 new를 지정합니다.

© Acronis International GmbH, 2003-2024

매개변수	설명
	에이전트 서비스가 기존 계정에서 실행되도록 하려면 --agent-account-login 및 --agent-account-password 매개변수를 사용하여 계정 자격 증명을 지정합니다. 이 경우에는 필요시에만 --agent-account=custom 매개변수를 지정하면 됩니다.
vCenter/ESXi 매개변수	
--esxi-address=<호스트>	vCenter Server 또는 ESXi 호스트의 호스트 이름 또는 IP 주소입니다. Agent for VMware를 설치할 때 이 매개변수를 사용합니다.
--esxi-login=<로그인> --esxi-password=<암호>	vCenter Server 또는 ESXi 호스트의 액세스 자격 증명입니다. Agent for VMware를 설치할 때 이러한 매개변수를 사용합니다.
프록시 매개변수	
--http-proxy={none | system | custom}	클라우드 스토리지로의 백업과 클라우드 스토리지에서의 복구에 사용할 HTTP 프록시 서버를 지정하려면 이 매개변수를 사용합니다. 프록시 서버 연결을 비활성화하는 경우에는 --http-proxy=none을 지정합니다. 시스템 전체에서 프록시 서버를 사용하려면 --http-proxy=system을 지정하거나 명령에서 --http-proxy 매개변수를 사용하지 않습니다. 다른 프록시 서버를 사용하려면 --http-proxy-address, --http-proxy-login 및 --http-proxy-password 매개변수를 사용하여 프록시 서버 주소와 자격 증명을 지정합니다. 이 경우에는 필요 시에만 --http-proxy=custom 매개변수를 지정하면 됩니다.
--http-proxy-address=<호스트>:<포트>	사용자 정의 HTTP 프록시 서버의 호스트 이름이나 IP 및 포트입니다.
--http-proxy-login=<로그인>	사용자 정의 HTTP 프록시 서버의 로그인.
--http-proxy-password=<암호>	사용자 정의 HTTP 프록시 서버의 비밀번호.
제거 매개변수	
--remove-components=<component1,component2,...,componentN>	설치 제거할 컴포넌트입니다. 사용 가능한 컴포넌트의 전체 목록은 "무인 설치용 컴포넌트(EXE)"(88페이지) 항목을 참조하십시오.

© Acronis International GmbH, 2003-2024

매개변수	설명
	여러 컴포넌트를 지정할 때는 각 컴포넌트를 쉼표로 구분합니다. 쉼표 앞뒤에 공백을 추가하면 안 됩니다. **중요** 이 매개변수 사용 시에는 컴포넌트만 설치 제거할 수 있습니다. 제품을 완전히 설치 제거하려면 Windows 제어판 > 프로그램 및 기능으로 이동하여 제품을 선택한 후 **설치 제거**를 클릭합니다.
`--delete-all-settings`	`--remove-components` 매개변수를 사용하여 모든 제품 로그, 작업 및 구성 설정을 삭제할 때 이 매개변수(선택 사항)를 사용합니다.
`--anti-tamper-password=<암호>`	비밀번호로 보호되는 Agent for Windows를 설치 제거하거나 컴퍼넌트를 변경하기 위해 필요한 비밀번호입니다.

무인 설치용 컴포넌트(EXE)

아래 표에는 EXE 파일을 통한 무인 설치에 사용할 수 있는 컴포넌트가 요약되어 있습니다. 값 이름을 사용하여 `--add-components` 매개변수의 값을 지정합니다.

자세한 내용은 "무인 설치(EXE)용 매개변수"(83페이지)"무인 설치(MSI)용 매개변수"(92페이지) 항목을 참조하십시오.

값 이름	컴퍼넌트 설명
`agentForWindows`	Agent for Windows
`agentForSas`	Agent for Files Sync & Share
`agentForAd`	Agent for Active Directory
`agentForAmp`	맬웨어 방지 보호 에이전트 및 URL 필터링 에이전트
`agentForDlp`	Data Loss Prevention용 에이전트
`agentForEsx`	Agent for VMware(Windows)
`agentForExchange`	Agent for Exchange
`agentForHyperV`	Agent for Hyper-V
`agentForOffice365`	Agent for Office 365
`agentForOracle`	Agent for Oracle
`agentForSql`	Agent for SQL

© Acronis International GmbH, 2003-2024

값 이름	컴퍼넌트 설명
commandLine	명령줄 도구
mediaBuilder	Bootable Media Builder
trayMonitor	Cyber Protect 모니터
all	모든 컴포넌트가 포함되는 값입니다.
allAgents	모든 에이전트가 포함되는 값입니다.

MSI 파일을 통한 무인 설치 및 설치 제거

이 유형의 무인 설치를 수행할 때는 Windows Installer(Msiexec 프로그램)를 사용합니다. 설치 프로그램의 그래픽 사용자 인터페이스를 사용하여 설치 패키지와 MSI 파일을 미리 추출합니다.

MSI 파일을 사용하여 컴포넌트를 설치할 때는 MST 변환 파일을 사용하여 설치 매개변수를 사용자 정의할 수 있습니다. MSI 및 MST 파일 조합을 사용하는 방법에 대한 자세한 내용은 "에이전트 및 컴포넌트 설치(MSI 및 MST 조합)"(90페이지) 항목을 참조하십시오. Active Directory 도메인에서 이 설치 방법을 사용하면 Windows 그룹 정책을 통해 보호 에이전트를 설치할 수 있습니다. 자세한 내용은 "그룹 정책을 통해 에이전트 배포"(156페이지)을(를) 참조하십시오.

명령줄에서 설치 매개변수를 수동으로 지정해도 됩니다. 이 경우에는 MST 파일을 사용하지 않아도 됩니다. 자세한 내용은 "예"(91페이지)을(를) 참조하십시오.

MSI, MST 및 CAB 파일 추출

설치 프로그램의 그래픽 사용자 인터페이스를 실행하면 설치 패키지와 함께 MSI, MST 및 CAB 파일을 추출할 수 있습니다.

MSI, MST 및 CAB 파일을 추출하려면

1. 설치 프로그램의 그래픽 사용자 인터페이스를 실행한 후 **무인 설치를 위해 .mst 및 .msi 파일 생성**을 클릭합니다.
2. **설치 대상**에서 설치할 컴포넌트를 선택하고 **완료**를 누릅니다.
   해당 컴포넌트용 설치 패키지가 설치 프로그램에서 CAB 파일로 추출됩니다.
3. **등록 설정**에서 **자격 증명 사용** 또는 **등록 토큰 사용**을 선택합니다. 선택에 따라 자격 증명 또는 등록 토큰을 지정한 다음 **완료**를 클릭합니다.
   등록 토큰을 생성하는 방법에 대한 자세한 내용은 "등록 토큰 생성"(156페이지) 항목을 참조하십시오.
4. [도메인 컨트롤러에 설치하는 경우에만 해당] **에이전트 서비스용 로그온 계정**에서 **다음 계정 사용**을 선택합니다. 에이전트 서비스를 실행할 사용자 계정을 지정한 다음 **완료**를 클릭합니다.
   보안상의 이유로 설치 프로그램은 도메인 컨트롤러에서 새 계정을 자동으로 생성하지 않습니다.

© Acronis International GmbH, 2003-2024

참고
지정한 사용자 계정에 서비스로 로그온 권한이 부여되어 있어야 합니다. 이 계정이 이미 도메인 컨트롤러에 사용 중인 계정이어야 프로필 폴더가 해당 머신에서 생성될 수 있습니다.

읽기 전용 도메인 컨트롤러에 에이전트를 설치하는 방법에 대한 자세한 내용은 이 기술 자료 문서를 참조하십시오.

5. MST 파일에 추가될 기타 설치 설정을 검토하거나 수정한 다음 **진행**을 클릭합니다.
6. MSI, MST 및 CAB 파일을 추출할 폴더를 선택하고 **생성**을 클릭합니다.

에이전트 및 컴포넌트 설치(MSI 및 MST 조합)

MSI 파일의 설치 설정을 사용자 정의하려면 MST 파일을 사용합니다. Windows 그룹 정책을 통해 여러 머신에 에이전트를 설치할 때 MSI 및 MST 조합을 사용합니다. 자세한 내용은 "그룹 정책을 통해 에이전트 배포"(156페이지)을(를) 참조하십시오.

MSI 및 MST 파일을 사용하여 컴포넌트를 설치하려면

1. "MSI, MST 및 CAB 파일 추출"(89페이지)의 설명에 따라 MSI 및 MST 파일을 추출합니다.
2. 컴포넌트를 설치하려는 머신의 명령줄 인터페이스에서 다음 명령을 실행합니다.

```
msiexec /i <MSI file> TRANSFORMS=<MST file>
```

예:

```
msiexec /i BackupClient64.msi TRANSFORMS=BackupClient64.msi.mst
```

에이전트와 컴포넌트 설치 및 설치 제거(MSI 및 직접 선택)

MSI 파일을 실행하고 설치할 컴포넌트를 수동으로 선택한 후 명령줄에서 컴포넌트의 설치 매개변수를 지정합니다. 이 경우에는 MST 파일을 사용하지 않아도 됩니다.

에이전트와 컴포넌트를 설치하려면

1. "MSI, MST 및 CAB 파일 추출"(89페이지)의 설명에 따라 MSI 파일 및 설치 패키지(CAB 파일)를 추출합니다.
   이 설치 방법을 사용할 때는 MSI 및 CAB 파일만 있으면 됩니다. MST 파일은 필요하지 않습니다.
2. 머신의 명령줄 인터페이스에서 다음 명령을 실행합니다.

```
msiexec /i <MSI file><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

각 매개변수는 공백으로 구분하고, 매개변수의 값은 쉼표(공백 없음)로 구분합니다. 예:

```
msiexec.exe /i BackupClient64.msi
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REGISTRATION_ADDRESS=https://eu2-
cloud.company.com REGISTRATION_TOKEN=34F6-8C39-4A5C
```


© Acronis International GmbH, 2003-2024

사용 가능한 매개변수와 해당 값을 확인하려면 "무인 설치(MSI)용 매개변수"(92페이지) 항목을 참조하십시오.

예

- Agent for Windows, 맬웨어 방지 에이전트, URL 필터링 에이전트, 명령줄 도구 및 Cyber Protect 모니터 설치. 사용자 이름과 암호를 사용하여 Cyber Protection 서비스에서 워크로드 등록.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,AmpAgentFeature,CommandLineTool,Tray
Monitor TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_USE_
SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com REGISTRATION_
LOGIN=johndoe REGISTRATION_PASSWORD=johnspassword
```

- Agent for Windows, 명령줄 도구, Cyber Protect Monitor 설치. Windows에서 에이전트 서비스용 새 로그온 계정 생성. 토큰을 사용하여 Cyber Protection 서비스에서 워크로드 등록.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_CREATE_NEW_
ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com REGISTRATION_TOKEN=34F6-
8C39-4A5C
```

- Agent for Windows, 명령줄 도구, Agent for Oracle, Cyber Protect 모니터 설치. 사용자 이름과 base64로 암호화된 비밀번호를 사용하여 Cyber Protection 서비스에서 머신 등록. 특수 문자나 공백이 포함된 암호는 인코딩해야 할 수도 있습니다. 암호 인코딩 방법에 대한 자세한 내용은 "특수 문자 또는 공백이 포함된 비밀번호"(114페이지) 항목을 참조하십시오.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,OracleAgentFeature,T
rayMonitor TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_
LANGUAGE=en MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com
REGISTRATION_LOGIN=johndoe REGISTRATION_PASSWORD_ENCODED=am9obnNwYXNzd29yZA==
```

- Agent for Windows, 명령줄 도구, Cyber Protect Monitor 설치. 토큰을 사용하여 Cyber Protection 서비스에서 머신 등록. HTTP 프록시 설정.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_LANGUAGE=en
MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com
REGISTRATION_TOKEN=34F6-8C39-4A5C HTTP_PROXY_ADDRESS=https://my-proxy.company.com
HTTP_PROXY_PORT=80 HTTP_PROXY_LOGIN=tomsmith HTTP_PROXY_PASSWORD=tomspassword
```

설치된 컴포넌트를 제거하려면

1. "MSI, MST 및 CAB 파일 추출"(89페이지)의 설명에 따라 MSI 파일 및 설치 패키지(CAB 파일)를 추출합니다.

   이 설치 방법을 사용할 때는 MSI 및 CAB 파일만 있으면 됩니다. MST 파일은 필요하지 않습니다.
2. 머신의 명령줄 인터페이스에서 다음 명령을 실행합니다.

© Acronis International GmbH, 2003-2024

```
msiexec /i <MSI file><REMOVE>=<value 1>,<value 2> REBOOT=ReallySuppress /qn
```

사용 가능한 매개변수와 해당 값을 확인하려면 "무인 설치(MSI)용 매개변수"(92페이지) 항목을 참조하십시오.

예

- Cyber Protect 모니터 제거.

```
msiexec.exe /i BackupClient64.msi /l*v uninstall_log.txt REMOVE=TrayMonitor
REBOOT=ReallySuppress /qn
```

에이전트 설치를 제거하려면

1. "MSI, MST 및 CAB 파일 추출"(89페이지)의 설명에 따라 MSI 파일 및 설치 패키지(CAB 파일)를 추출합니다.

   이 설치 방법을 사용할 때는 MSI 및 CAB 파일만 있으면 됩니다. MST 파일은 필요하지 않습니다.
2. 머신의 명령줄 인터페이스에서 다음 명령을 실행합니다.

```
msiexec /x <MSI file> /l*v uninstall_log.txt DELETE_ALL_SETTINGS=1
REBOOT=ReallySuppress /qn
```

사용 가능한 매개변수와 해당 값을 확인하려면 "무인 설치(MSI)용 매개변수"(92페이지) 항목을 참조하십시오.

예

- Agent for Windows 및 모든 컴포넌트 설치 제거. 모든 로그, 작업 및 구성 설정 삭제.

```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt DELETE_ALL_SETTINGS=1
REBOOT=ReallySuppress /qn
```

- 암호로 보호된 Agent for Windows 및 모든 컴포넌트 설치 제거. 모든 로그, 작업 및 구성 설정 삭제.

```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt ANTI_TAMPER_
PASSWORD=<password> DELETE_ALL_SETTINGS=1 REBOOT=ReallySuppress /qn
```

무인 설치(MSI)용 매개변수

아래 표에는 MSI 파일 사용 시의 무인 설치용 매개변수가 요약되어 있습니다.

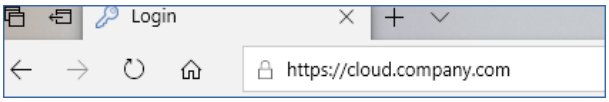
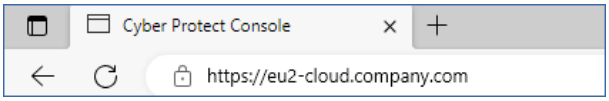
추가 `msiexec` 매개변수를 사용할 수도 있습니다. 예를 들어 GUI 요소가 표시되지 않도록 하려면 `/qn`을 사용합니다. `msiexec` 매개변수에 대해 자세히 알아보려면 Microsoft 설명서를 참조하십시오.

매개변수	설명
일반 매개변수	

© Acronis International GmbH, 2003-2024

매개변수	설명
ADDLOCAL= <component1,component2,...,componentN>	설치될 컴퍼넌트. 사용 가능한 컴포넌트의 전체 목록은 "무인 설치용 컴포넌트(MSI)"(96페이지) 항목을 참조하십시오. 여러 컴포넌트를 지정할 때는 각 컴포넌트를 쉼표로 구분합니다. 쉼표 앞뒤에 공백을 추가하면 안 됩니다. **참고** 설치할 모든 컴포넌트용 설치 파일을 추출해야 합니다. 설치 파일 추출 방법에 대한 자세한 내용은 "MSI, MST 및 CAB 파일 추출"(89페이지) 항목을 참조하십시오.
TARGETDIR=<경로>	선택한 컴포넌트를 설치할 폴더입니다. 지정한 폴더가 없는 경우에는 새로 생성됩니다. 이 매개변수를 지정하지 않으면 기본 폴더가 사용됩니다. C:\Program Files\BackupClient입니다.
REBOOT=ReallySuppress	머신을 다시 시작하지 않고 컴포넌트를 설치하려면 이 매개변수를 지정합니다.
/l*v <로그 파일>	자세한 정보 표시 로그를 저장하려면 이 매개변수를 지정합니다. 설치 문제를 조사해야 하는 경우 이 로그가 필요합니다.
CURRENT_LANGUAGE=<언어 ID>	제품 언어. en, bn, bg, cs, da, de, es, fr, ko, id, it, hi, hu, ms, nl, ja, nb, pl, pt, pt_BR, ru, fi, sr, sv, th, tr, vi, zh, zh_TW 값을 사용할 수 있습니다. 이 매개변수를 지정하지 않는 경우 설치를 수행하는 머신의 시스템 언어가 상기 나열된 언어 중 하나라면 시스템 언어가 사용됩니다. 그 외의 모든 경우에는 값이 en으로 설정됩니다.
SKIP_SHA2_KB_CHECK={0,1}	Microsoft의 SHA2 코드 서명 지원 업데이트(KB4474419)가 머신에 설치되어 있는지 확인하려면 이 매개변수를 사용합니다. 검사는 이 업데이트가 필요한 운영 체제에서만 실행됩니다. 현재 사용 중인 운영 체제에 이 업데이트가 필요한지 확인하려면 "지원되는 운영 체제 및 환경"(23페이지) 항목을 참조하십시오. 검사를 건너뛰려면 값을 1로 설정하여 이 매개변수를 사용합니다. 매개변수를 지정하지 않거나 매개변수 값을 0으로 설정했는데 머신에 SHA2 코드 서명 지원 업데이트가 설치되어 있지 않으면 설치는 실패합니다.
FSS_ONBOARDING_AUTO_START={0,1}	무인 설치 이후 온보딩 마법사를 표시하려면 값을 1로

© Acronis International GmbH, 2003-2024

매개변수	설명
	설정하여 이 매개변수를 사용합니다. 이 매개변수를 지정하지 않거나 매개변수 값을 0으로 설정하면 온보딩 마법사가 표시되지 않습니다.
등록 매개변수	
REGISTRATION_ADDRESS	Cyber Protection 서비스의 URL입니다. 이 매개변수는 REGISTRATION_LOGIN 및 REGISTRATION_PASSWORD 매개변수와 함께 사용할 수도 있고 REGISTRATION_TOKEN과 함께 사용할 수도 있습니다. • 이 매개변수를 REGISTRATION_LOGIN 및 REGISTRATION_PASSWORD 매개변수와 함께 사용할 때는 Cyber Protection 서비스에 **로그인**하는 데 사용하는 주소를 지정합니다. 예: https://cloud.company.com:  • 이 매개변수를 REGISTRATION_TOKEN 매개변수와 함께 사용할 때는 정확한 데이터센터 주소를 지정합니다. 이 주소는 Cyber Protection 서비스에 **로그인하고 나면** 표시되는 URL입니다. 예: https://eu2-cloud.company.com.  https://cloud.company.com과 REGISTRATION_TOKEN 매개변수를 함께 사용하면 안 됩니다.
REGISTRATION_LOGIN REGISTRATION_PASSWORD	Cyber Protection 서비스에서 에이전트를 등록할 계정의 자격 증명입니다. 파트너 관리자 계정은 사용할 수 없습니다. 이러한 매개변수와 REGISTRATION_TOKEN 매개변수를 함께 사용하면 안 됩니다.
REGISTRATION_PASSWORD_ENCODED	Cyber Protection 서비스에서 에이전트를 등록할 계정의 base64로 암호화된 암호입니다. 암호 암호화 방법에 대한 자세한 내용은 "특수 문자 또는 공백이 포함된 비밀번호"(114페이지) 항목을 참조하십시오.
REGISTRATION_TOKEN	등록 토큰입니다. 등록 토큰은 하이픈에 의해 세 부분으로 구분된 12자리 문자열입니다. 토큰 생성 방법에 대한 자세한 내용은 "등록 토큰 생성"(156페이지) 항목을 참조하십시오. 이 매개변수는 REGISTRATION_LOGIN 및 REGISTRATION_PASSWORD 매개변수와 함께 사용하면 안 됩니다.

© Acronis International GmbH, 2003-2024

매개변수	설명
REGISTRATION_REQUIRED={0,1}	등록 실패 시에 수행되는 작업을 선택하려면 이 매개변수를 사용합니다. 값을 1로 설정해도 설치가 실패합니다. 값을 0으로 설정하거나 매개변수를 지정하지 않으면 등록이 실패해도 설치는 정상적으로 완료됩니다.
에이전트 서비스용 로그온 계정	
MMS_USE_SYSTEM_ACCOUNT={0,1}	서비스가 **Local System** 로그온 계정으로 실행되도록 하려면 값을 1로 설정하여 이 매개변수를 사용합니다. 로그온 계정에 대한 자세한 내용은 "Windows 머신에서 로그온 계정 변경"(79페이지) 항목을 참조하십시오.
MMS_CREATE_NEW_ACCOUNT={0,1}	자동으로 생성되는 새 로그온 계정인 **Acronis Agent User**에서 에이전트 서비스가 실행되도록 하려면 값을 1로 설정하여 이 매개변수를 사용합니다.
MMS_SERVICE_USERNAME=<사용자 이름> MMS_SERVICE_PASSWORD=<암호>	에이전트 서비스를 실행할 기존 로그온 계정을 지정하려면 이러한 매개변수를 사용합니다.
vCenter/ESXi 매개변수	
SET_ESX_SERVER={0,1}	Agent for VMware를 설치할 때 이 매개변수를 사용합니다. 값을 0으로 설정하면 Agent for VMware가 vCenter Server 또는 ESXi 호스트에 연결되지 않습니다. 값을 1로 설정하는 경우에는 ESX_HOST, EXI_USER, ESX_PASSWORD 매개변수를 지정합니다.
ESX_HOST=<호스트 이름>	vCenter Server 또는 ESXi 호스트의 호스트 이름 또는 IP 주소입니다.
ESX_USER=<사용자 이름> ESX_PASSWORD=<암호>	vCenter Server 또는 ESXi 호스트의 액세스 자격 증명입니다.
프록시 매개변수	
HTTP_PROXY_ADDRESS=<IP 주소> HTTP_PROXY_PORT=<포트>	에이전트가 사용할 HTTP 프록시 서버를 지정하려면 이러한 매개변수를 사용합니다. 프록시 서버를 사용하지 않는 경우에는 이러한 매개변수를 지정하지 않습니다.
HTTP_PROXY_LOGIN=<로그인> HTTP_PROXY_암호=<암호>	HTTP 프록시 서버의 자격 증명. 프록시 서버에 인증이 필요한 경우 이러한 매개변수를 사용합니다.

© Acronis International GmbH, 2003-2024

매개변수	설명
제거 매개변수	
REMOVE={<구성 요소 목록>|ALL}	설치 제거할 컴포넌트입니다. 여러 컴포넌트를 지정할 때는 각 컴포넌트를 쉼표로 구분합니다. 쉼표 앞뒤에 공백을 추가하면 안 됩니다. 모든 제품 컴포넌트를 제거하려면 값을 ALL로 설정합니다.
DELETE_ALL_SETTINGS={0, 1}	모든 제품 로그, 작업 및 구성 설정을 삭제하려면 값을 1로 설정합니다. REMOVE 매개변수를 사용할 때 이 매개변수(선택 사항)를 사용합니다.
ANTI_TAMPER_PASSWORD=<암호>	비밀번호로 보호되는 Agent for Windows를 설치 제거하거나 컴퍼넌트를 변경하기 위해 필요한 비밀번호입니다.

무인 설치용 컴포넌트(MSI)

아래 표에는 MSI 파일을 통한 무인 설치에 사용할 수 있는 컴포넌트가 요약되어 있습니다. 값 이름을 사용하여 ADDLOCAL 매개변수의 값을 지정합니다. 자세한 내용은 "무인 설치(MSI)용 매개변수"(92 페이지)을(를) 참조하십시오.

값 이름	컴퍼넌트 설명	다음 항목과 함께 설치	비트
AgentFeature	에이전트용 핵심 컴퍼넌트		32비트/64비트
MmsMspComponents	백업용 핵심 컴퍼넌트	AgentFeature	32비트/64비트
BackupAndRecoveryAgent	Agent for Windows	MmsMspComponents	32비트/64비트
AmpAgentFeature	Agent for Antimalware protection	BackupAndRecoveryAgent	32비트/64비트
UrlFilteringAgentFeature	Agent for URL Filtering	BackupAndRecoveryAgent	32비트/64비트
DlpAgentFeature	Data Loss Prevention용 에	BackupAndRecoveryAgent	32비트/64비

© Acronis International GmbH, 2003-2024

	이전트		트
SasAgentFeature	Agent for File Sync & Share	TrayMonitor	32비트/64비트
ArxAgentFeature	Agent for Exchange	MmsMspComponents	32비트/64비트
ArsAgentFeature	Agent for SQL	BackupAndRecoveryAgent	32비트/64비트
ARADAgentFeature	Agent for Active Directory	BackupAndRecoveryAgent	32비트/64비트
ArxOnlineAgentFeature	Agent for Microsoft 365	MmsMspComponents	32비트/64비트
OracleAgentFeature	Agent for Oracle	BackupAndRecoveryAgent	32비트/64비트
AcronisESXSupport	Agent for VMware ESX(i) (Windows)	BackupAndRecoveryAgent	64비트
HyperVAgent	Agent for Hyper-V	BackupAndRecoveryAgent	32비트/64비트
CommandLineTool	명령줄 도구		32비트/64비트
TrayMonitor	Cyber Protect 모니터	AgentFeature	32비트/64비트
BackupAndRecoveryBootableComponents	Bootable Media Builder		32비트/64비트

Linux에서 무인 설치 또는 제거

이 섹션에서는 Linux를 실행하는 머신에서 명령줄을 사용하여 보호 에이전트를 무인 모드로 설치 또는 제거하는 방법에 대해 설명합니다.

에이전트를 설치하려면

© Acronis International GmbH, 2003-2024

1. 터미널을 엽니다.

2. 다음 중 하나를 수행하십시오.

- 명령줄에서 매개변수를 지정하여 설치를 시작하려면 다음 명령을 실행합니다.

  ```
  <package name> -a <parameter 1> ... <parameter N>
  ```

  여기서, <package name>은 설치 패키지(.i686 또는 .x86_64 파일)의 이름입니다. 사용 가능한 모든 매개변수와 해당 값은 "무인 설치 또는 제거 매개변수"(99페이지) 항목에 설명되어 있습니다.
- 별도의 텍스트 파일에서 지정된 매개변수를 사용해 설치를 시작하려면 다음 명령을 실행합니다.

  ```
  <package name> -a --options-file=<path to the file>
  ```

  명령줄에 민감한 정보를 입력하지 않으려는 경우 이 방식이 유용할 수 있습니다. 이 경우, 별도의 텍스트 파일에서 구성 설정을 지정하고 사용자만 액세스할 수 있는지 확인할 수 있습니다. 다음과 같이 새 행에 각 매개변수와 해당 매개변수의 값을 차례로 입력합니다.

  ```
  --rain=https://cloud.company.com
  --login=johndoe
  --password=johnspassword
  --auto
  ```

  또는

  ```
  -C
  https://cloud.company.com
  -g
  johndoe
  -w
  johnspassword
  -a
  --language
  en
  ```

  명령줄과 텍스트 파일 모두에 동일한 매개변수가 지정된 경우 명령줄 값이 우선합니다.

3. UEFI 보안 부팅이 머신에서 활성화되어 있는 경우에는 설치 후에 시스템을 다시 시작해야 한다는 메시지가 표시됩니다. 사용해야 하는 암호(루트 사용자의 암호 또는 "acronis")를 잘 기억해 두십시오. 시스템 다시 시작 중에 MOK(Machine Owner Key) 관리를 선택하고, **MOK 등록**을 선택한 다음, 권장 비밀번호를 사용하여 키를 등록합니다.

에이전트 설치 후 UEFI 보안 부팅을 활성화하는 경우에는 3단계를 포함하는 설치를 반복하십시오. 그렇지 않으면 백업에 실패하게 됩니다.

에이전트 설치를 제거하려면

1. 터미널을 엽니다.
2. 다음 중 하나를 수행하십시오.

© Acronis International GmbH, 2003-2024

- 에이전트를 설치 제거하고 로그, 작업, 구성 설정까지 모두 제거하려면 다음 명령을 실행합니다.

  ```
  /usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall -a
  ```

- 에이전트는 설치 제거하되 ID는 그대로 유지하려는 경우(예: 나중에 에이전트를 설치하려는 경우) 다음 명령을 실행합니다.

  ```
  /usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall -a --no-purge
  ```

- 설치 파일을 사용하여 에이전트를 설치 제거하려면 다음 명령을 실행합니다.

  ```
  <package name> -a -u
  ```

  여기서, <package name>은 설치 패키지(.i686 또는 .x86_64 파일)의 이름입니다. 사용 가능한 모든 매개변수와 해당 값은 "무인 설치 또는 제거 매개변수"(99페이지) 항목에 설명되어 있습니다.

  참고
  설치 패키지가 설치된 에이전트와 같은 버전이며 /usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall이 손상되었거나 액세스 불가능한 상태일 때만 이 명령을 사용하십시오.

무인 설치 또는 제거 매개변수

이 섹션에서는 Linux에서 무인 설치 또는 제거 중 사용되는 매개변수에 대해 설명합니다.

무인 설치의 최소 구성에는 -a 및 등록 매개변수(예: --login 및 --password 매개변수; --rain 및 --token 매개변수)가 포함됩니다. 더 많은 매개변수를 사용하여 설치를 사용자 정의할 수 있습니다.

설치 매개변수

기본 매개변수

{-i |--id=}<구성 요소 목록>

설치될 컴퍼넌트는 쉼표로 구분되고 공백 문자가 없습니다. .x86_64 설치 패키지에서는 다음 컴퍼넌트를 사용할 수 있습니다.

구성 요소	컴퍼넌트 설명
BackupAndRecoveryAgent	Agent for Linux
AgentForPCS	Agent for Virtuozzo
OracleAgentFeature	Agent for Oracle
MySQLAgentFeature	Agent for MySQL/MariaDB

이 매개변수가 없으면 위의 모든 컴퍼넌트가 설치됩니다.

© Acronis International GmbH, 2003-2024

Agent for Virtuozzo, Agent for Oracle 및 Agent for MySQL/MariaDB를 사용하려면 Agent for Linux도 설치해야 합니다.

.i686 설치 패키지는 BackupAndRecoveryAgent만 포함합니다.

`{-a|--auto}`

설치 및 등록 프로세스는 추가 사용자 상호 작용 없이 완료됩니다. 이 매개변수를 사용할 때 `--token` 매개변수를 사용하거나 `--login` 및 `--password` 매개변수를 사용하여 Cyber Protection 서비스에서 에이전트를 등록할 계정을 지정해야 합니다.

`{-t|--strict}`

이 매개변수를 지정하면 설치 중 발생하는 모든 경고가 설치 실패로 이어집니다. 이 매개변수가 없으면 경고가 발생하더라도 설치가 성공적으로 완료됩니다.

`{-n|--nodeps}`

설치 중에 필요한 Linux 패키지가 없으면 무시됩니다.

`{-d|--debug}`

자세한 정보 표시 모드로 설치 로그를 작성합니다.

`--options-file=<위치>`

명령줄 대신 텍스트 파일에서 설치 매개변수를 읽습니다.

`--language=<언어 ID>`

제품 언어. 사용 가능한 값은 다음과 같습니다. `en, bg, cs, da, de, es, fr, hu, id, it, ja, ko, ms, nb, nl, pl, pt, pt_BR, ru, fi, sr, sv, tr, zh, zh_TW`.
이 매개변수가 지정되지 않으면 제품 언어는 시스템 언어로 정의됩니다. 단, 해당 언어가 위 목록에 포함되어 있어야 합니다. 그렇지 않으면 제품 언어는 영어로 설정됩니다(en).

등록 매개변수

다음 매개변수 중 하나를 지정합니다.

- `{-g|--login=}`<사용자 이름> 및 `{-w|--password=}`<비밀번호>

  Cyber Protection 서비스에서 에이전트를 등록할 계정의 자격 증명. 파트너 관리자 계정은 사용할 수 없습니다.

- `--token=`<토큰>

  등록 토큰은 12자로 이루어져 있으며 하이픈에 의해 세 개의 세그먼트로 구분됩니다. "그룹 정책을 통해 에이전트 디플로이"에 설명되어 있는 대로 Cyber Protect 콘솔에서 토큰을 생성할 수 있습니다.

  `--token` 매개변수는 `--login, --password` 및 `--register-with-credentials` 매개변수와 함께 사용할 수 없습니다.

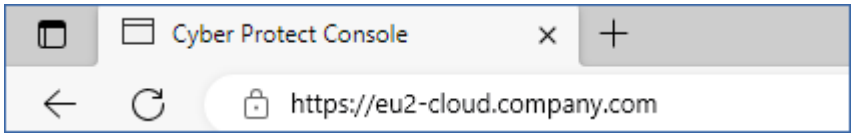
  - `{-C|--rain=}`<서비스 주소>

    Cyber Protection 서비스의 URL입니다.

© Acronis International GmbH, 2003-2024

인스톨러가 기본적으로 올바른 주소(Cyber Protection 서비스에 **로그인하기 위해** 사용하는 주소)를 사용하므로, 등록을 위해 `--login` 및 `--password` 매개변수를 사용할 때 명시적으로 이 매개변수를 포함할 필요는 없습니다. 예:

하지만 `--token` 매개변수와 함께 `{-C|--rain=}` 사용 시 정확한 데이터센터 주소를 지정해야 합니다. 이는 Cyber Protection 서비스에 **로그인하면** 표시되는 URL입니다. 예:



- `--register-with-credentials`

  이 매개변수가 지정되면 인스톨러의 그래픽 인터페이스가 시작됩니다. 등록을 완료하려면 Cyber Protection 서비스에서 에이전트를 등록할 계정의 사용자 이름과 비밀번호를 입력합니다. 파트너 관리자 계정은 사용할 수 없습니다.

- `--skip-registration`

  에이전트를 설치해야 하지만 나중에 Cyber Protection 서비스에서 등록할 예정인 경우 이 매개변수를 사용하십시오. 작업의 수행 방법에 대한 자세한 내용은 "수동으로 머신 등록"을 참조하십시오.

추가 매개변수

`--http-proxy-host=<IP 주소>` and `--http-proxy-port=<포트>`

에이전트가 클라우드에 백업하고 여기에서 복구할 때, 그리고 관리 서버에 연결할 때 사용하는 HTTP 프록시 서버. 이 매개변수가 없으면 프록시 서버가 사용되지 않습니다.

`--http-proxy-login=<로그인>` and `--http-proxy-password=<비밀번호>`

HTTP 프록시 서버의 자격 증명. 서버에 인증이 필요한 경우 이 매개변수를 사용합니다.

`--tmp-dir=<위치>`

설치 중 임시 파일을 저장할 폴더를 지정합니다. 기본 폴더는 **/var/tmp**입니다.

`{-s|--disable-native-shared}`

이미 시스템에 존재하더라도 설치 중에는 재배포 가능한 라이브러리가 사용됩니다.

`--skip-prereq-check`

snapapi 모듈의 컴파일을 위해 필요한 패키지가 이미 설치되어 있는지는 확인하지 않습니다.

`--force-weak-snapapi`

인스톨러는 snapapi 모듈을 컴파일하지 않습니다. 그 대신 Linux 커널과 정확하게 일치하지 않을 수 있는 이미 생성된 모듈을 사용합니다. 이 옵션은 사용하지 않는 것이 좋습니다.

© Acronis International GmbH, 2003-2024

`--skip-svc-start`

설치 후 서비스가 자동으로 시작되지 않습니다. 대부분의 경우, 이 매개변수는 `--skip-registration` 매개변수와 함께 사용됩니다.

정보 매개변수

`{-?|--help}`

매개변수 설명이 표시됩니다.

`--usage`

명령의 용도에 대한 간략한 설명이 표시됩니다.

`{-v|--version}`

설치 패키지 버전을 표시합니다.

`--product-info`

제품 이름 및 설치 패키지 버전을 표시합니다.

`--snapapi-list`

이미 생성된 사용 가능 snapapi 모듈을 표시합니다.

`--components-list`

인스톨러 컴퍼넌트를 표시합니다.

레거시 기능에 대한 매개변수

이러한 매개변수는 레거시 컴퍼넌트 agent.exe와 관련이 있습니다.

`{-e|--ssl=}<경로>`

SSL 통신을 위한 사용자 정의 인증서 파일의 경로를 지정합니다.

`{-p|--port=}<포트>`

agent.exe가 연결을 수신하는 포트를 지정합니다. 기본 포트는 9876입니다.

제거 매개변수

`{-u|--uninstall}`

제품을 제거합니다.

`--purge`

제품을 제거하고 제품의 로그, 작업 및 구성 설정을 제거합니다. `--purge` 매개변수를 사용할 때 `--uninstall` 매개변수를 명시적으로 지정할 필요가 없습니다.

© Acronis International GmbH, 2003-2024

예

- Agent for Linux를 등록하지 않고 설치.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent -a --skip-registration
```

- Agent for Linux, Agent for Virtuozzo 및 Agent for Oracle을 설치하고 자격 증명을 사용하여 등록.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --login=johndoe --password=johnspassword
```

- Agent for Oracle 및 Agent for Linux를 설치하고 등록 토큰을 사용하여 등록.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent,OracleAgentFeature -a --rain=https://eu2-cloud.company.com --token=34F6-8C39-4A5C
```

- 별도의 텍스트 파일에 구성 설정을 포함하여 Agent for Linux, Agent for Virtuozzo 및 Agent for Oracle 설치.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --options-file=/home/mydirectory/configuration_file
```

- Agent for Linux, Agent for Virtuozzo 및 Agent for Oracle을 제거하고 모든 로그, 작업 및 구성 설정 제거.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --purge
```

macOS에 무인 설치 및 제거

이 섹션에서는 macOS를 실행 중인 머신에서 명령줄을 사용하여 Protection 에이전트를 무인 모드로 설치, 등록 및 설치 제거하는 방법에 대해 설명합니다.

필요한 권한

mac 워크로드에서 무인 설치를 시작하기 전에 개인 정보 보호 기본 설정 정책 컨트롤을 수정하여 워크로드의 macOS에서 앱 액세스와 커널 및 시스템 확장을 허용해야 합니다. 그래야 Cyber Protection 에이전트를 설치할 수 있습니다. "macOS의 무인 설치에 필요한 권한"(105페이지) 항목을 참조하십시오.

PPPC 페이로드를 디플로이한 후에 아래 절차를 진행할 수 있습니다.

설치 파일(.dmg)을 다운로드하려면

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. **추가**를 선택한 뒤, **Mac**을 클릭합니다.

에이전트를 설치하려면

© Acronis International GmbH, 2003-2024

1. 터미널을 엽니다.
2. 설치 파일(.dmg)을 마운트할 임시 디렉토리를 생성합니다.

   ```
   mkdir <dmg_root>
   ```

   여기에서 <dmg_root>는 직접 정하는 이름입니다.
3. .dmg 파일을 마운트합니다.

   ```
   hdiutil attach <dmg_file> -mountpoint <dmg_root>
   ```

   여기에서 <dmg_file>은 설치 파일의 이름입니다. 예: **Cyber_Protection_Agent_for_MAC_x64.dmg**.
4. 인스톨러를 실행합니다.
   - CyberProtect_AgentForMac_x64.dmg, CyberProtect_AgentForMac_arm64.dmg 등의 Mac용 정식 인스톨러를 사용하는 경우 다음 명령을 실행합니다.

     ```
     sudo installer -pkg <dmg_root>/Install.pkg -target LocalSystem
     ```

     참고
     File Sync & Share의 자동 온보딩을 활성화해야 하는 경우에는 다음 명령을 대신 실행합니다. 이 옵션을 사용할 때는 관리자 암호를 입력하라는 메시지가 표시됩니다.

     ```
     open <dmg_root>/Install.app --args --unattended --fss-onboarding-auto-start
     ```

   - CyberProtect_AgentForMac_web.dmg 등의 Mac용 범용 인스톨러를 사용하는 경우 다음 명령을 실행합니다.

     ```
     sudo <dmg_root>/Install.app/Contents/MacOS/cyber_installer -a
     ```
5. 설치 파일(.dmg)을 분리합니다.

   ```
   hdiutil detach <dmg_root>
   ```

예

```
mkdir mydirectory
```

```
hdiutil attach /Users/JohnDoe/Cyber_Protection_Agent_for_MAC_x64.dmg -mountpoint
mydirectory
```

```
sudo installer -pkg mydirectory/Install.pkg -target LocalSystem
```

```
hdiutil detach mydirectory
```

에이전트 설치를 제거하려면

© Acronis International GmbH, 2003-2024

1. 터미널을 엽니다.
2. 다음 중 하나를 수행하십시오.
   - 에이전트를 설치 제거하려면 다음 명령을 실행합니다.

     ```
     sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
     Uninstall.app/Contents/MacOS/AgentUninstall /confirm
     ```

   - 에이전트를 설치 제거하고 로그, 작업, 구성 설정까지 모두 제거하려면 다음 명령을 실행합니다.

     ```
     sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
     Uninstall.app/Contents/MacOS/AgentUninstall /confirm /purge
     ```

macOS의 무인 설치에 필요한 권한

mac 워크로드에서 무인 설치를 시작하기 전에 개인 정보 보호 기본 설정 정책 컨트롤을 수정하여 워크로드의 macOS에서 앱 액세스와 커널 및 시스템 확장을 허용해야 합니다. 그래야 Cyber Protection 에이전트를 설치할 수 있습니다. 이 경우 워크로드의 그래픽 사용자 인터페이스에서 기본 설정을 구성하거나 사용자 정의 PPPC 페이로드를 디플로이하면 됩니다. 필요한 권한은 다음과 같습니다.

macOS 11(Big Sur) 이상의 요구 사항

탭	섹션	필드	값

© Acronis International GmbH, 2003-2024

개인 정보 보호 기본 설정 정책 컨트롤	앱 액세스	식별자	com.acronis.backup

© Acronis International GmbH, 2003-2024

		식별자 유형	번들 ID
		코드 요구사항	identifier "com.acronis.backup" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = ZU2TV78AA6
		앱 또는 서비스	SystemPolicyAllFiles
		액세스	허용
	앱 액세스	식별자	com.acronis.backup.aakore
		식별자 유형	번들 ID
		코드 요구사항	identifier "com.acronis.backup.aakore" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = ZU2TV78AA6
		앱 또는 서비스	SystemPolicyAllFiles
		액세스	허용
	앱 액세스	식별됨	com.acronis.backup.activeprotection
		식별자 유형	번들 ID
		코드 요구사항	identifier "com.acronis.backup.activeprotection" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		앱 또는 서비스	SystemPolicyAllFiles
		액세스	허용

© Acronis International GmbH, 2003-2024

	앱 액세스	식별자	cyber-protect-service
		식별자 유형	번들 ID
		코드 요구 사항	`identifier "cyber-protect-service" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6`
		앱 또는 서비스	SystemPolicyAllFiles
		액세스	허용
시스템 확장		사용자가 시스템 확장을 승인할 수 있음	활성화됨
	허용되는 팀 ID 및 시스템 확장	표시 이름	Acronis Cyber Protection 에이전트 시스템 확장
		시스템 확장 유형	허용되는 팀 식별자
		팀 식별자	ZU2TV78AA6

***macOS 11** 이전 버전의 요구 사항*

탭	섹션	필드	값

© Acronis International GmbH, 2003-2024

개인 정보 보호 기본 설정 정책 컨트롤	앱 액세스	식별자	com.acronis.backup
		식별자 유형	번들 ID
		코드 요구 사항	identifier "com.acronis.backup" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		앱 또는 서비스	SystemPolicyAllFiles
		액세스	허용
	앱 액세스	식별자	com.acronis.backup.aakore
		식별자 유형	번들 ID
		코드 요구 사항	identifier "com.acronis.backup.aakore" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		앱 또는 서비스	SystemPolicyAllFiles
		액세스	허용
	앱 액세스	식별됨	com.acronis.backup.activeprotection
		식별자 유형	번들 ID
		코드 요구 사항	identifier "com.acronis.backup.activeprotection" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		앱 또는 서비스	SystemPolicyAllFiles
		액세스	허용
	앱 액세스	식별자	cyber-protect-service
		식별자 유형	번들 ID
		코드 요구 사항	identifier "cyber-protect-service" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = ZU2TV78AA6
		앱 또는 서비스	SystemPolicyAllFiles
		액세스	허용
승인된 커널 확		사용자가 커널 확장을 승인할	활성화됨

© Acronis International GmbH, 2003-2024

장		수 있음	
		표준 사용자가 레거시 커널 확장(macOS 11 이하)을 승인할 수 있음	활성화됨
	승인된 팀 ID 및 커널 확장	승인된 팀 ID - 표시 이름	Acronis Cyber Protection 에이전트 커널 확장
		팀 ID	ZU2TV78AA6
		커널 확장 번들 ID	• com.acronis.systeminterceptors • com.acronis.ngscan • com.acronis.notifyframework
시스템 확장		사용자가 시스템 확장을 승인할 수 있음	활성화됨
	허용되는 팀 ID 및 시스템 확장	표시 이름	Acronis Cyber Protection 에이전트 시스템 확장
		시스템 확장 유형	허용되는 팀 식별자
		팀 식별자	ZU2TV78AA6

수동으로 워크로드 등록 및 등록 해제

워크로드는 보호 에이전트를 설치하면 Cyber Protection 서비스에 자동 등록됩니다. 보호 에이전트를 설치 제거하면 워크로드가 자동으로 등록 해제되며 Cyber Protect 콘솔에 표시되지 않습니다.

명령줄 인터페이스를 사용하여 수동으로 워크로드를 등록할 수도 있습니다. 예를 들어 자동 등록이 실패하거나 새 테넌트 또는 새 사용자 계정으로 워크로드를 이동하려는 경우에 수동 등록을 사용해야 할 수 있습니다.

사용자 이름과 암호를 사용하여 워크로드를 등록하려면

Windows

명령줄에서 다음 명령을 실행합니다.

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> -u <user name> -p <password>
```

예:

```
"C:\ProgramFiles\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -p johnspassword
```


© Acronis International GmbH, 2003-2024

Linux

명령줄에서 다음 명령을 실행합니다.

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a <service address> -u <user name> -p <password>
```

예:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a https://cloud.company.com -u johndoe -p johnspassword
```

macOS

명령줄에서 다음 명령을 실행합니다.

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a <service address> -u <user name> -p <password>
```

예:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a https://cloud.company.com -u johndoe -p johnspassword
```

참고
워크로드를 등록할 계정의 사용자 이름과 암호를 사용합니다. 파트너 관리자 계정은 사용할 수 없습니다.

서비스 주소는 Cyber Protection 서비스에 **로그인**하기 위해 사용하는 URL입니다. 예:
`https://cloud.company.com`

중요
암호에 특수 문자나 공백이 포함되어 있다면 "특수 문자 또는 공백이 포함된 비밀번호"(114페이지) 항목을 참조하십시오.

중요
macOS 10.14 이상을 사용 중인 경우 보호 에이전트에 전체 디스크 액세스 권한을 부여합니다. 이렇게 하려면 **애플리케이션** >**유틸리티**로 이동한 다음 **Cyber Protect 에이전트 지원**을 실행하십시오. 그런 다음 애플리케이션 창의 지침을 따릅니다.

등록 토큰을 사용하여 워크로드를 등록하려면

Windows

명령줄에서 다음 명령을 실행합니다.

© Acronis International GmbH, 2003-2024

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> --token <registration token>
```

예:

```
"C:\ProgramFiles\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://au1-cloud.company.com --token 3B4C-E967-4FBD
```

Linux

명령줄에서 다음 명령을 실행합니다.

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a <service
address> --token <registration token>
```

예:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://eu2-cloud.company.com --token 34F6-8C39-4A5C
```

macOS

명령줄에서 다음 명령을 실행합니다.

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a <service address> --token <registration token>
```

예:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a https://us5-cloud.company.com --token 9DBF-3DA9-4DAB
```

중요
macOS 10.14 이상을 사용 중인 경우 보호 에이전트에 전체 디스크 액세스 권한을 부여합니다. 이렇게 하려면 **애플리케이션 >유틸리티**로 이동한 다음 **Cyber Protect 에이전트 지원**을 실행하십시오. 그런 다음 애플리케이션 창의 지침을 따릅니다.

가상 어플라이언스

1. 가상 어플라이언스의 콘솔에서 Ctrl+Shift+F2를 눌러 명령줄 인터페이스를 엽니다.
2. 명령 프롬프트에서 다음 명령을 실행합니다.

   ```
   register_agent -o register -t cloud -a <service address> --token <registration token>
   ```

   예:

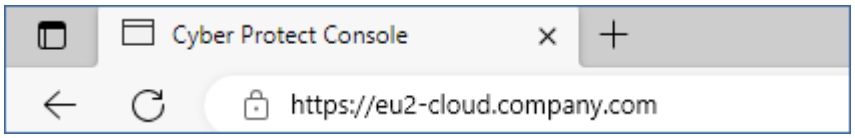
© Acronis International GmbH, 2003-2024

```
register_agent -o register -t cloud -a https://eu2-cloud.company.com --token 34F6-8C39-4A5C
```

3. 어플라이언스의 그래픽 인터페이스로 돌아가려면 Alt+F1을 누릅니다.

참고

등록 토큰을 사용할 때는 정확한 데이터 센터 주소를 지정해야 합니다. 이 주소는 Cyber Protection 서비스에 **로그인하고 나면** 표시되는 URL입니다. 예: `https://eu2-cloud.company.com`.



여기서 `https://cloud.company.com`을 사용하지 마십시오.

등록 토큰은 12자로 이루어져 있으며 하이픈에 의해 세 개의 세그먼트로 구분됩니다. 생성 방법에 대한 자세한 내용은 "등록 토큰 생성"(156페이지) 항목을 참조하십시오.

워크로드를 등록 해제하려면

Windows

명령줄에서 다음 명령을 실행합니다.

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o unregister
```

예:

```
"C:\ProgramFiles\BackupClient\RegisterAgentTool\register_agent.exe" -o unregister
```

Linux

명령줄에서 다음 명령을 실행합니다.

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

macOS

명령줄에서 다음 명령을 실행합니다.

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

가상 어플라이언스

1. 가상 어플라이언스의 콘솔에서 Ctrl+Shift+F2를 눌러 명령줄 인터페이스를 엽니다.
2. 명령 프롬프트에서 다음 명령을 실행합니다.

© Acronis International GmbH, 2003-2024

```
register_agent -o unregister
```

3. 어플라이언스의 그래픽 인터페이스로 돌아가려면 Alt+F1을 누릅니다.

다른 테넌트로 워크로드 이동

다른 테넌트로 워크로드를 이동하는 작업은 기본적으로 지원되지 않습니다. 워크로드를 등록 해제한 후 다른 테넌트에 등록하는 방식을 사용할 수는 있습니다. 그러면 해당 워크로드에 적용되어 있는 모든 보호 계획이 해지되며 해당 워크로드는 원래 테넌트의 클라우드 스토리지에 있는 백업에 액세스할 수 없게 됩니다.

워크로드를 새 테넌트나 새 사용자 계정에 등록하는 방법에 대한 자세한 내용은 "워크로드 등록 변경"(115페이지) 항목을 참조하십시오.

특수 문자 또는 공백이 포함된 비밀번호

패스워드에 특수 문자나 공백이 포함된 경우, 명령줄에 입력할 때 처음과 끝에 인용 부호를 포함하십시오.

예를 들어 Windows에서 다음 명령을 실행합니다.

명령 템플릿:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> -u <user name> -p <"password">
```

명령 예:

```
"C:\ProgramFiles\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -p "johns password"
```

이 명령이 정상적으로 실행되지 않으면 https://www.base64encode.org/에서 암호를 base64 형식으로 인코딩합니다.그런 다음 명령줄에서 -b 또는 --base64 매개변수를 사용하여 인코딩된 암호를 지정합니다.

예를 들어 Windows에서 다음 명령을 실행합니다.

명령 템플릿:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a <service address> -u <user name> -b -p <encoded password>
```

명령 예:

```
"C:\ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t
cloud -a https://cloud.company.com -u johndoe -b -p am9obnNwYXNzd29yZA==
```


© Acronis International GmbH, 2003-2024

워크로드 등록 변경

워크로드를 새 테넌트나 새 사용자 계정에 등록하는 방식으로 현재 등록을 변경할 수 있습니다.

중요
워크로드의 등록을 변경하면 해당 워크로드에 적용되어 있는 모든 보호 계획이 해지됩니다. 워크로드를 계속 보호하려면 해당 워크로드에 새 보호 계획을 적용합니다.

새 테넌트에 등록하는 워크로드는 원래 테넌트의 클라우드 스토리지에 있는 백업에 액세스할 수 없게 됩니다. 클라우드 스토리지 이외의 위치에 있는 백업에는 계속 액세스할 수 있습니다.

명령줄이나 GUI 인스톨러를 사용하여 워크로드 등록을 변경할 수 있습니다. 명령줄 사용 시에는 에이전트를 설치 제거하지 않아도 됩니다.

워크로드의 등록을 변경하려면

명령줄 사용

1. "워크로드를 등록 해제하려면"(113페이지) 항목의 설명대로 보호 에이전트 등록을 해제합니다.
2. "사용자 이름과 암호를 사용하여 워크로드를 등록하려면"(110페이지) 또는 "등록 토큰을 사용하여 워크로드를 등록하려면"(111페이지) 항목의 설명대로 새 테넌트나 새 사용자 계정에 보호 에이전트를 등록합니다.

GUI 인스톨러 사용

1. 보호 에이전트를 설치 제거합니다.
2. 보호 에이전트를 설치한 후 새 테넌트나 새 사용자 계정에 등록합니다.

에이전트 설치 및 등록 방법에 대한 자세한 내용은 "Protection 에이전트 설치"(72페이지) 항목을 참조하십시오.

머신 자동 검색

자동 검색을 사용하면 다음을 수행할 수 있습니다.

- Active Directory 도메인이나 로컬 네트워크의 머신을 감지하여 해당 머신을 등록하고 보호 에이전트를 설치하는 과정을 자동화할 수 있습니다.
- 여러 머신에서 보호 에이전트를 설치하고 업데이트할 수 있습니다.
- Active Directory와의 동기화를 사용하여, 대규모 Active Directory 도메인에서 머신을 관리하고 리소스를 프로비저닝하는 작업을 줄일 수 있습니다.

사전 요구 사항

자동 검색을 수행하려면 Active Directory 도메인이나 로컬 네트워크에 보호 에이전트가 설치된 머신이 하나 이상 있어야 합니다. 이 에이전트는 검색 에이전트로 사용됩니다.

© Acronis International GmbH, 2003-2024

중요

Windows 머신에 설치된 에이전트만 검색 에이전트로 사용할 수 있습니다. 환경 내에 검색 에이전트가 없으면 **장치 추가** 패널에서 **여러 장치** 옵션을 사용할 수 없습니다.

에이전트 원격 설치는 Windows를 실행하는 머신에 대해서만 지원됩니다(Windows XP는 지원되지 않음). Windows Server 2012 R2를 실행하는 머신에 에이전트를 원격 설치하려면 해당 머신에 Windows 업데이트 KB2999226이 설치되어 있어야 합니다.

자동 검색의 작동 방식

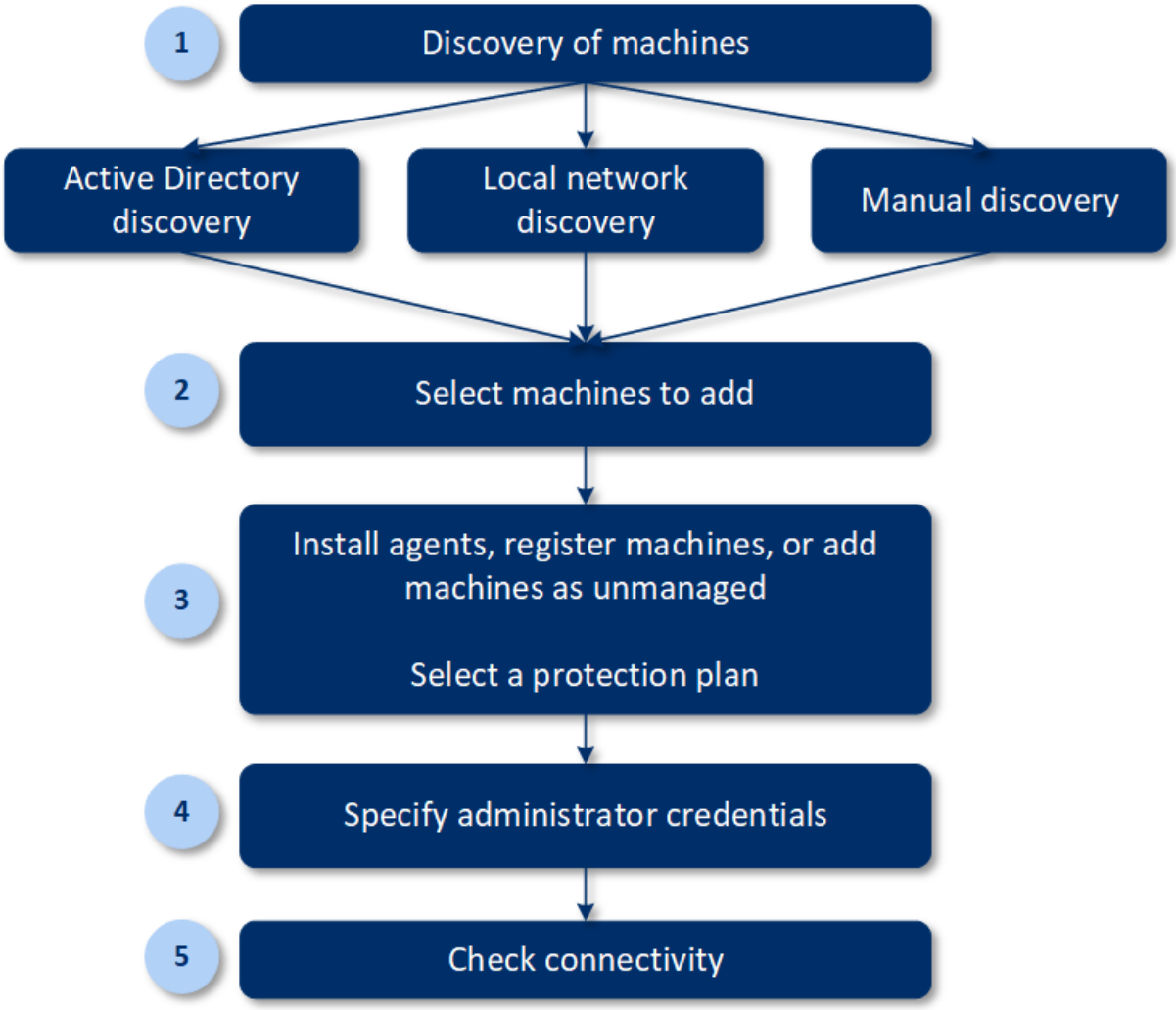
검색 에이전트는 로컬 네트워크 검색 중에 NetBIOS 검색, WSD(웹 서비스 검색) 및 ARP(주소 확인 프로토콜) 테이블을 사용하여 네트워크 내의 각 머신에 대해 다음 정보를 수집합니다.

- 이름(간단/NetBIOS 호스트 이름)
- FQDN(정규화된 도메인 이름)
- 도메인/워크그룹
- IPv4/IPv6 주소
- MAC 주소
- 운영 체제(이름/버전/제품군)
- 머신 카테고리(워크스테이션/서버/도메인 컨트롤러)

Active Directory 검색 과정에서는 검색 에이전트가 위의 목록에 나와 있는 정보 외에 머신 OU(조직 구성 단위) 관련 정보, 그리고 머신의 이름과 운영 체제 관련 세부 정보도 수집합니다. 그러나 IP 주소와 MAC 주소는 수집하지 않습니다.

아래 다이어그램에 대략적인 자동 검색 프로세스가 나와 있습니다.

© Acronis International GmbH, 2003-2024



1. 검색 방법 선택:
   - Active Directory 검색
   - 로컬 네트워크 검색
   - 수동 검색 – 머신 IP 주소 또는 호스트 이름을 사용하거나 파일에서 머신 목록 가져오기

   보호 에이전트가 설치된 머신은 Active Directory 검색이나 로컬 네트워크 검색 결과에서 제외됩니다.

   수동 검색 중에는 기존 보호 에이전트가 업데이트 및 재등록됩니다. 에이전트가 등록되어 있는 것과 같은 계정을 사용하여 자동 검색을 수행하면 에이전트는 최신 버전으로 업데이트만 됩니다. 다른 계정을 사용하여 자동 검색을 수행하면 에이전트는 최신 버전으로 업데이트되어 해당 계정이 속한 테넌트에 재등록됩니다.
2. 테넌트에 추가할 머신을 선택합니다.
3. 해당 머신을 추가할 방법을 선택합니다.
   - 보호 에이전트와 추가 컴포넌트를 머신에 설치하고 Cyber Protect 콘솔에서 등록합니다.
   - 보호 에이전트를 이미 설치한 경우에는 Cyber Protect 콘솔에서 머신을 등록합니다.
   - 보호 에이전트를 설치하지 않고 머신을 **비관리 대상 머신**으로 Cyber Protect 콘솔에 추가합니다.

© Acronis International GmbH, 2003-2024

보호 에이전트를 설치하거나 Cyber Protect 콘솔에 등록하는 머신에 기존 보호 계획을 적용할 수도 있습니다.

4. 선택한 머신의 관리자 자격 증명을 입력합니다.
5. 입력한 자격 증명을 사용하여 머신에 연결할 수 있는지 확인합니다.

Cyber Protect 콘솔에 표시되는 머신은 다음 카테고리에 속합니다.

- **검색됨** – 검색은 되었지만 보호 에이전트는 설치되지 않은 머신입니다.
- **관리 대상** – 보호 에이전트가 설치된 머신입니다.
- **보호되지 않음** – 보호 계획이 적용되어 있지 않은 머신입니다. 보호되지 않은 머신에는 보호 계획이 적용되지 않은 검색된 머신 및 관리 대상 상태의 머신이 모두 포함됩니다.
- **보호됨** – 보호 계획이 적용된 머신입니다.

에이전트 원격 설치의 작동 방식

1. 검색 에이전트가 검색 마법사에서 지정한 호스트 이름, IP 주소 및 관리자 자격 증명을 사용하여 대상 머신에 연결한 다음 해당 머신에 `web_installer.exe` 파일을 업로드합니다.
2. 대상 머신에서 `web_installer.exe` 파일이 자동 모드로 실행됩니다.
3. 웹 설치 프로그램이 클라우드에서 추가 설치 패키지를 검색한 다음 `msiexec` 명령을 통해 대상 머신에 해당 패키지를 설치합니다.
4. 설치가 완료되면 클라우드에 컴퍼넌트가 등록됩니다.

참고
에이전트 서비스를 실행하는 데 필요한 추가 권한으로 인해 도메인 컨트롤러에 대해서는 에이전트 원격 설치가 지원되지 않습니다.

자동 검색 및 수동 검색 수행

검색을 시작하기 전 사전 요구 사항이 충족되었는지 확인합니다.

참고
에이전트 서비스를 실행하는 데 필요한 추가 권한으로 인해 도메인 컨트롤러 추가에 대해서는 자동 검색이 지원되지 않습니다.

머신을 검색하려면

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. **추가**를 클릭합니다.
3. **여러 개의 장치**에서 **Windows 전용**을 클릭합니다. 검색 마법사가 열립니다.
4. [조직 단위가 있는 경우] 단위를 선택합니다. 그러면 **검색 에이전트**에서 선택한 단위 및 하위 단위와 관련된 에이전트를 선택할 수 있습니다.
5. 머신을 감지하기 위해 스캔을 수행할 검색 에이전트를 선택합니다.
6. 검색 방법 선택:
   - **Active Directory 검색**. 검색 에이전트가 설치된 머신이 Active Directory 도메인 멤버여야 합니다.

© Acronis International GmbH, 2003-2024

- **로컬 네트워크 스캔**. 선택한 검색 에이전트에서 머신을 찾지 못한 경우 다른 검색 에이전트를 선택합니다.
- **수동으로 지정 또는 파일에서 가져오기**. 추가할 머신을 수동으로 정의하거나 텍스트 파일에서 가져옵니다.

7. [Active Directory 검색 방법을 선택한 경우] 머신 검색 방법 선택:
   - **조직 단위 목록에서**. 추가될 머신 그룹을 선택합니다.
   - **LDAP 언어 쿼리에 따라**. LDAP 언어 쿼리를 사용해 머신을 선택합니다. **검색 베이스**는 검색할 곳을 정의하고, **필터**를 사용해 머신 선택의 기준을 지정합니다.
8. 선택한 검색 방법에 따라 다음 작업 중 하나를 수행합니다:

검색 방법	작업
Active Directory 검색	검색된 머신 목록에서 추가할 머신을 선택합니다.
로컬 네트워크 스캔	검색된 머신 목록에서 추가할 머신을 선택합니다.

수동으로 지정 또는 파일에서 가져오기	머신의 IP 주소 또는 호스트 이름을 직접 지정하거나 텍스트 파일의 머신 목록에서 가져옵니다. 해당 파일에는 IP 주소/호스트 이름이 한 줄에 하나씩 포함되어 있어야 합니다. 사용 가능한 파일의 예는 다음과 같습니다:
	`156.85.34.10`
	`156.85.53.32`
	`156.85.53.12`
	`EN-L00000100`
	`EN-L00000101`
	머신 주소를 수동으로 추가하거나 파일에서 가져오면, 에이전트는 추가된 머신을 핑하고 가용성을 정의하려 시도합니다.

9. 검색 후 수행해야 할 작업 선택:

옵션	설명
에이전트 설치 및 머신 등록	**컴포넌트 선택**을 클릭해 머신에 설치할 컴포넌트를 선택할 수 있습니다. 자세한 내용은 "설치할 컴퍼넌트 선택"(122페이지) 항목을 참조하십시오.
에이전트 서비스용 로그온 계정	이 설정은 **컴포넌트 선택** 화면에서 사용할 수 있습니다. 설정에 따라 서비스를 실행할 계정이 정의됩니다. 다음 옵션 중 하나를 선택할 수 있습니다: • **서비스 사용자 계정 사용**(에이전트 서비스용 기본값) 서비스 사용자 계정은 서비스를 실행하는 데 사용되는 Windows 시스템 계정입니다. 이 설정의 이점은 도메인 보안 정책이 이 계정의 사용자 권한에 영향을 미치지 않는다는 점입니다. 기본적으로 에이전트는 **로컬 시스템** 계정 하에서 실행됩니다. • **새 계정 생성** 계정 이름은 해당 에이전트에 대해 Agent User로 지정됩니다.

© Acronis International GmbH, 2003-2024

옵션	설명
	• **다음 계정 사용** 도메인 컨트롤러에 에이전트를 설치하는 경우 시스템에 각 에이전트의 기존 계정(또는 동일한 계정)을 지정하라는 메시지가 표시됩니다. 보안상의 이유로 시스템은 도메인 컨트롤러에서 새 계정을 자동으로 생성하지 않습니다. **새 계정 생성** 또는 **다음 계정 사용** 옵션을 선택하는 경우 도메인 보안 정책이 관련 계정의 권한에 영향을 미치지 않는지 확인하십시오. 설치 중 계정에 할당되어 있는 사용자 권한이 박탈되는 경우 컴포넌트가 올바로 작동하지 않거나 전혀 작동하지 않을 수 있습니다.
에이전트가 설치된 머신 등록	머신에 에이전트가 이미 설치되어 있어서 Cyber Protection에 등록만 하면 되는 경우 이 옵션을 사용합니다. 에이전트가 설치되어 있지 않은 머신은 **비관리** 머신으로 추가됩니다.
관리되지 않는 머신으로 추가	이 옵션을 선택하면 머신에 에이전트가 설치되지 않습니다. 콘솔에서 에이전트를 확인할 수 있으며 나중에 에이전트를 설치 또는 등록할 수 있습니다.
필요 시 머신 다시 시작	**에이전트 설치 및 머신 등록**을 선택하면 이 옵션이 표시됩니다. 이 옵션을 선택하면 설치를 완료하는 데 필요한 횟수만큼 머신이 다시 시작됩니다. 다음의 경우 머신을 다시 시작해야 할 수 있습니다. • 사전 요구 사항 설치가 완료되었고 설치를 계속하기 위해 다시 시작해야 하는 경우. • 설치가 완료되었지만 설치 중 일부 파일이 잠겨 다시 시작해야 하는 경우. • 설치가 완료되었지만 이전에 설치된 다른 소프트웨어에서 다시 시작을 요구하는 경우.
사용자가 로그인한 경우 다시 시작 안 함	**필요 시 머신 다시 시작**을 선택하면 이 옵션이 표시됩니다. 사용자가 시스템에 로그인한 상태에서 이 옵션을 선택하면 머신이 자동으로 다시 시작되지 않습니다. 예를 들어 설치 중에 머신을 다시 시작해야 할 때 사용자가 작업을 수행하는 중이라면 시스템이 다시 시작되지 않습니다. 사전 요구 사항은 설치되었는데 사용자가 로그인되어 있어서 머신이 다시 시작되지 않은 경우 설치를 완료하려면 머신을 다시 시작한 후 설치를 다시 시작해야 합니다. 에이전트는 설치되었는데 머신은 다시 시작되지 않았다면 머신을 다시 시작해야 합니다.
머신을 등록할 사용자	[조직에 단위가 있는 경우] 머신을 등록할 단위 또는 하위 단위가 속해 있는 사용자 계정을 선택합니다. [파트너 테넌트 수준에서 자동 검색 수행 시] 관리 대상 고객 테넌트 목록에서 트리 구조를 확장하고 머신을 등록할 사용자 계정을 선택합니다. [자동 검색을 수행하는 고객 관리자] **에이전트 설치 및 머신 등록** 또는 **에이전트가 설치된 머신 등록**을 선택한 경우에는 머신에 보호 계획을 적용하는 옵션도 사용 가능합니다. 보호 계획이 여러 개라면 사용할 계획을 선택할 수 있습니다.

10. 모든 머신에 대한 관리자 권한이 있는 사용자의 자격 증명을 지정합니다.

© Acronis International GmbH, 2003-2024

중요
에이전트의 원격 설치는 기본 제공 관리자 계정(운영 체제 설치 시 생성한 첫 번째 계정)의 자격 증명을 지정한 경우에만 아무런 준비 과정 없이 작동합니다. 사용자 정의 관리자 자격 증명을 정의하려는 경우 "원격 설치를 위해 머신 준비"(121페이지)에 설명되어 있는 대로 추가적인 수동 준비 작업을 수행해야 합니다.

11. 시스템은 모든 머신의 연결을 확인합니다. 연결되지 않는 일부 머신에 대한 자격 증명을 변경할 수 있습니다.

머신 검색이 시작되면 **모니터링** > **활동** > **머신 검색** 활동에서 해당하는 작업을 찾을 수 있습니다.

원격 설치를 위해 머신 준비

- Windows 7 이상을 실행하는 원격 머신에서 설치를 정상적으로 완료하려면 해당 머신에서 **제어판** > **폴더 옵션** > **보기** > **공유 마법사 사용** 옵션을 *비활성화*해야 합니다.
- Active Directory 도메인에 속하지 *않는* 원격 머신에 설치를 완료하려면 해당 머신에서 사용자 계정 컨트롤(UAC)을 *비활성화*해야 합니다. 비활성화에 대한 자세한 정보는 "사용자 계정 컨트롤(UAC)에 대한 요구 사항" > UAC 비활성화를 참고하십시오.
- 기본적으로, 기본 제공 관리자 계정의 자격 증명은 모든 Windows의 원격 설치에 필수입니다. 다른 관리자 계정의 자격 증명을 이용해 원격 설치를 수행하려면, 사용자 계정 컨트롤(UAC) 원격 제한 사항을 반드시 *비활성화*해야 합니다. 비활성화에 대한 자세한 정보는 "사용자 계정 컨트롤(UAC)에 대한 요구 사항" > UAC 원격 제한 사항 비활성화를 참고하십시오.
- 원격 머신에서 파일과 프린터 공유를 *활성화*해야 합니다. 이 옵션에 액세스하려면:
  - Windows 2003 Server를 실행 중인 머신: **제어판** > **Windows 방화벽** > **예외** > **파일 및 프린터 공유**로 이동합니다.
  - Windows Server 2008, Windows 7 이상을 실행 중인 머신: **제어판** > **Windows 방화벽** > **네트워크 및 공유 센터** > **고급 공유 설정 변경**으로 이동합니다.
- Cyber Protection에서는 원격 설치 시 TCP 포트 445, 25001, 43234를 사용합니다.
  포트 445는 파일 및 프린터 공유를 활성화하면 자동으로 열립니다. 포트 43234 및 25001은 Windows 방화벽에서 자동으로 열립니다. 다른 방화벽을 사용하는 경우에는 수신 및 발신 요청에 모두 이 포트 3개가 열려 있는지(예외에 추가) 확인합니다.
  원격 설치가 완료된 후에는 포트 25001이 Windows 방화벽에서 자동으로 닫힙니다. 이후 에이전트를 원격으로 업데이트하려면 포트 445 및 43234를 연 채로 두어야 합니다. 포트 25001은 각 업데이트 중에 Windows 방화벽에서 자동으로 열렸다가 닫힙니다. 다른 방화벽을 사용하는 경우 세 개 포트를 모두 연 채로 유지하십시오.

UAC(User Account Control)에 대한 요구 사항

Windows 7 이상을 실행하고 Active Directory 도메인에 속하지 않는 머신에서 중앙 집중식 관리 작업(원격 설치 포함)을 수행하려면 UAC 및 UAC 원격 제한 사항을 비활성화해야 합니다.

UAC를 비활성화하려면

운영 체제에 따라 다음 중 하나를 수행합니다.

© Acronis International GmbH, 2003-2024

- **Windows 8 이전 Windows 운영 체제:**
  제어판> 보기 기준: 작은 아이콘 > 사용자 계정> 사용자 계정 제어 설정 변경으로 이동한 후 슬라이더를 **알리지 않음**으로 이동합니다. 그런 다음 머신을 다시 시작합니다.
- **모든 Windows 운영 체제**:
  1. 레지스트리 편집기를 엽니다.
  2. 다음 레지스트리 키를 찾습니다. **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**
  3. **EnableLUA** 값은 설정을 **0**으로 변경합니다.
  4. 머신을 다시 시작합니다.

UAC 원격 제한 사항을 비활성화하는 방법

1. 레지스트리 편집기를 엽니다.
2. 다음 레지스트리 키를 찾습니다. **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
3. **LocalAccountTokenFilterPolicy** 값은 설정을 **1**로 변경합니다.
   LocalAccountTokenFilterPolicy 값이 존재하지 않는 경우 DWORD(32비트)로 생성합니다. 이 값에 대한 자세한 내용은 다음 Microsoft 문서를 참조하십시오. https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.

참고
보안상의 이유로 원격 설치와 같은 관리 작업을 마친 후에는 두 설정을 모두 원래 상태로 되돌리는 것이 좋습니다. **EnableLUA=1** 및 **LocalAccountTokenFilterPolicy = 0**

설치할 컴퍼넌트 선택

아래 표에서 필수 및 추가 컴퍼넌트에 대한 설명을 찾아볼 수 있습니다.

구성 요소	설명
필수 컴퍼넌트	
Agent for Windows	이 에이전트는 디스크, 볼륨, 파일을 백업하며 Windows 머신에 설치됩니다. 언제나 설치되는 항목으로 선택이 가능하지 않습니다.
추가 컴퍼넌트	
Data Loss Prevention 용 에이전트	이 에이전트를 사용하면 보호 계획이 적용된 머신의 로컬 및 리디렉션 주변 장치, 포트 및 클립보드에 대한 사용자의 액세스를 제한할 수 있습니다. 선택된 경우 설치됩니다.
안티맬웨어 및 URL 필터링	이 컴포넌트는 보호 계획에서 안티바이러스 및 안티맬웨어 보호 모듈과 URL 필터링 모듈을 활성화합니다. 설치하지 않기로 선택한 경우에도 머신에 대한 보호 계획에서 이러한 모듈이 활성화되어 있으면 나중에 자동으로 설치됩니다.
Agent for Hyper-V	이 에이전트는 Hyper-V 가상 머신을 백업하며, Hyper-V 호스트에 설치됩니다. 선택되었으며 머신에서 Hyper-V 역할이 감지된 경우 설치됩니다.

© Acronis International GmbH, 2003-2024

Agent for SQL	이 에이전트는 SQL Server 데이터베이스를 백업하며, Microsoft SQL Server를 실행하는 머신에 설치됩니다. 선택되었으며 머신에서 애플리케이션이 감지된 경우 설치됩니다.
Agent for Exchange	이 에이전트는 Exchange 데이터베이스를 백업하며, Microsoft Exchange Server의 사서함 역할을 실행하는 머신에 설치됩니다. 선택되었으며 머신에서 애플리케이션이 감지된 경우 설치됩니다.
Agent for Active Directory	이 에이전트는 Active Directory 도메인 서비스의 데이터를 백업하며, 도메인 컨트롤러에 설치됩니다. 선택되었으며 머신에서 애플리케이션이 감지된 경우 설치됩니다.
Agent for VMware (Windows)	이 에이전트는 VMware 가상 머신을 백업하며, vCenter Server에 대한 네트워크 액세스가 있는 Windows 머신에 설치됩니다. 선택된 경우 설치됩니다.
Agent for Microsoft 365	이 에이전트는 Microsoft 365 사서함을 로컬 대상에 백업하며, Windows 머신에 설치됩니다. 선택된 경우 설치됩니다.
Agent for Oracle	이 에이전트는 Oracle 데이터베이스를 백업하며, Oracle 데이터베이스를 실행하는 머신에 설치됩니다. 선택된 경우 설치됩니다.
Cyber Protection 모니터	이 컴퍼넌트는 사용자가 알림 영역에서 실행 중인 작업의 실행을 모니터링할 수 있게 지원하며, Windows 머신에 설치됩니다. 선택된 경우 설치됩니다. Windows 7 서비스 팩 1 이상 및 Windows Server 2008 R2 서비스 팩 1 이상에서 지원됩니다.

검색된 머신 관리

검색 프로세스를 수행하고 나면 검색된 머신을 모두 **장치** > **관리되지 않는 머신**에서 찾을 수 있습니다.

이 섹션은 사용한 검색 방법에 따라 하위 섹션으로 나누어져 있습니다. 머신 매개변수의 전체 목록은 아래 표시됩니다(검색 방법에 따라 다를 수 있음).

이름	설명
이름	머신의 이름입니다. 머신의 이름을 찾을 수 없는 경우 IP 주소가 표시됩니다.
IP 주소	머신의 IP 주소입니다.
검색 유형	머신을 감지하는 데 사용된 검색 방법입니다.
조직 단위	머신이 속한 Active Directory 내 조직 단위입니다. 이 열은 **관리되지 않는 머신** > **Active Directory**에서 머신 목록을 보는 경우 표시됩니다.
운영 체제	머신에 설치된 운영 체제입니다.

© Acronis International GmbH, 2003-2024

예외 섹션에는 검색 프로세스에서 건너뛰어야 할 머신을 추가할 수 있습니다. 검색하지 않아도 될 특정 머신이 있다면 이 목록에 추가하면 됩니다.

머신을 **예외**에 추가하려면 목록에서 해당 머신을 선택한 다음 **예외에 추가**를 클릭합니다. 머신을 **예외**에서 제거하려면 **관리되지 않는 머신** > **예외**로 이동한 다음 해당 머신을 선택하고 **예외에서 제거**를 클릭합니다.

보호 에이전트를 설치하고 검색된 머신 배치를 Cyber Protection에 등록하려면 목록에서 이를 선택한 다음, **설치 및 등록**을 클릭합니다. 보호 계획을 머신 배치에 할당할 수 있게 해주는 마법사가 열립니다.

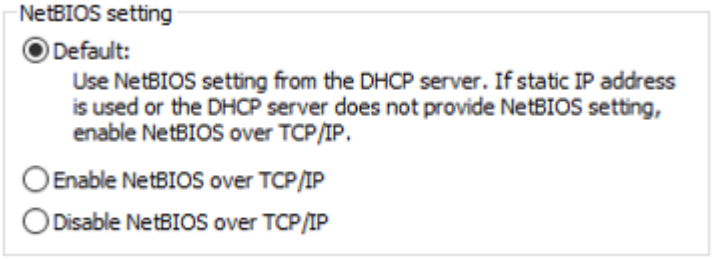
보호 에이전트를 머신에 설치하고 나면 해당 머신이 **장치** > **에이전트가 있는 머신** 섹션에 표시됩니다.

보호 상태를 확인하려면 **모니터링** > **개요**로 이동해 보호 상태 위젯 또는 검색된 머신 위젯을 추가합니다.

문제 해결

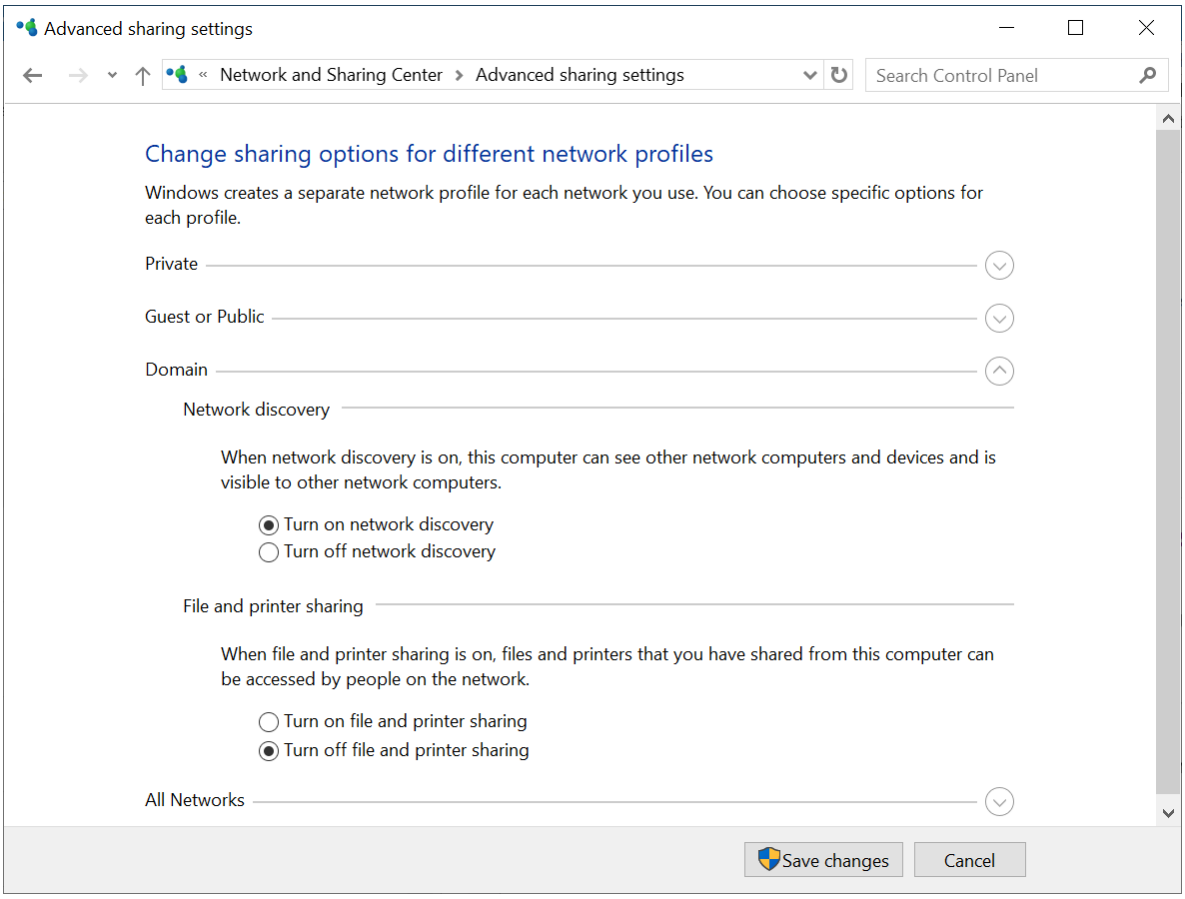
자동 검색 기능에 문제가 있다면 다음을 확인합니다.

- TCP/IP 상에서 NetBIOS 사용이 활성화되어 있거나 기본값으로 설정되어 있는지 확인합니다.



- "제어판\네트워크 및 공유 센터\고급 공유 설정"에서 네트워크 검색을 켭니다.

© Acronis International GmbH, 2003-2024



- 검색을 수행하는 머신과 검색될 머신에서 Function Discovery Provider Host 서비스가 구동되고 있는지 확인합니다.
- 검색될 머신에서 Function Discovery Resource Publication 서비스가 구동되고 있는지 확인합니다.

Agent for VMware(가상 어플라이언스) 배포

시작하기 전에

에이전트에 대한 시스템 요구사항

가상 어플라이언스는 기본값으로 대다수 작업에 최적의 상태로 실행되는 RAM 4GB, 2vCPU가 할당됩니다.

백업 성능을 개선하고 RAM 메모리 부족으로 인한 오류를 방지하려면 리소스가 더 많이 필요할 때 이러한 리소스를 RAM 16GB, vCPU 4개로 늘리는 것이 좋습니다. 예를 들어 백업 트래픽의 양이 초당 100MB를 초과할 것으로 예상되거나(예: 10기가비트 네트워크) 대용량 하드 드라이브(500GB 이상)를 사용하는 여러 가상 머신을 동시에 백업해야 한다면 할당된 리소스를 늘립니다.

어플라이언스 자체 가상 디스크가 차지하는 공간은 6GB 이하입니다. 씩 또는 씬 디스크 포맷은 문제가 되지 않습니다. 어플라이언스 성능에 영향을 주지 않습니다.

© Acronis International GmbH, 2003-2024

필요한 에이전트 수는?

가상 어플라이언스 한 대는 전체 vSphere 환경을 보호할 수 있지만, vSphere당(또는 클러스터가 없을 경우 호스트당) 가상 어플라이언스를 한 대 디플로이하는 것이 모범 사례입니다. 이 어플라이언스는 HotAdd 전송을 사용하여 백업된 디스크에 연결할 수 있고, 따라서 백업 트래픽이 하나의 로컬 디스크에서 다른 디스크로 향하기 때문에 이는 신속한 백업을 보장합니다.

동일한 vCenter Server 에 연결되거나 다른 ESXi 호스트에 연결되는 경우 가상 어플라이언스와 Agent for VMware (Windows)를 동시에 사용하는 것이 일반적입니다. 한 에이전트가 ESXi에 직접 연결되고 다른 에이전트가 이 ESXi를 관리하는 vCenter Server에 연결되는 사례를 피합니다.

에이전트가 여러 개이면 로컬 연결 스토리지를 사용하지 않는 것이 좋습니다. 가령 가상 어플라이언스에 추가한 가상 디스크에 백업을 저장하는 등의 방식은 사용하지 않는 것이 좋습니다. 추가 고려 사항은 "로컬로 연결된 스토리지 사용"(629페이지) 항목을 참조하십시오.

에이전트 자동 DRS 비활성화

가상 어플라이언스가 vSphere 클러스터에 디플로이되면 자동 vMotion을 비활성화해야 합니다. 클러스터 DRS 설정에서 개별 가상 머신 자동화 수준을 활성화하고, **비활성화**할 가상 어플라이언스에 대한 **자동화 수준**을 설정합니다.

OVF 템플릿 디플로이

1. **모든 장치** > **추가** > **VMware ESXi** > **가상 어플라이언스(OVF)**를 클릭합니다.
   .Zip 아카이브가 귀하의 머신에 다운로드됩니다.
2. .zip 아카이브의 압축을 풉니다. 폴더에는 .ovf 파일 한 개와 .vmdk 파일 두 개가 포함되어 있습니다.
3. vSphere Client를 실행하는 머신에서 이러한 파일에 액세스 가능한지 확인하십시오.
4. vSphere Client를 시작하고 vCenter Server에 로그온합니다.
5. OVF 템플릿을 디플로이합니다.
   - 스토리지를 구성할 때 존재하는 경우에는 공유 데이터 저장소를 선택합니다. 씩 또는 씬 디스크 포맷은 어플라이언스 성능에 영향을 주지 않기 때문에 문제가 되지 않습니다.
   - 네트워크 연결을 구성할 때는 에이전트 자체가 클라우드에 적절히 등록될 수 있도록 인터넷 연결이 가능한 네트워크를 선택해야 합니다.

가상 어플라이언스 구성

가상 어플라이언스를 디플로이한 후에는 해당 어플라이언스가 vCenter Server나 ESXi 호스트 및 Cyber Protection 서비스에 액세스할 수 있도록 어플라이언스를 구성해야 합니다.

가상 어플라이언스을 구성하려면

1. vSphere Client에서 가상 어플라이언스의 콘솔을 엽니다.
2. 네트워크 연결이 구성되어 있는지 확인합니다.
   연결은 동적 호스트 구성 프로토콜(DHCP)을 통해 자동 구성됩니다.

© Acronis International GmbH, 2003-2024

기본 구성을 변경하려면 **에이전트 옵션**의 **eth0** 필드에서 **변경**을 클릭한 후 네트워크 설정을 지정합니다.

3. vCenter Server 또는 ESXi 호스트에 가상 어플라이언스를 연결합니다.
   a. **에이전트 옵션**의 **vCenter/ESX(i)** 필드에서 **변경**을 클릭한 후 다음 항목을 지정합니다.
      - [vCenter Server를 사용하는 경우] vCenter Server 이름 또는 IP 주소.
      - [vCenter Server를 사용하지 않는 경우] 가상 머신을 백업 및 복구할 ESXi 호스트의 이름 또는 IP 주소. 백업을 더욱 빠르게 생성하려는 경우 같은 호스트에 가상 어플라이언스를 디플로이합니다.
      - 어플라이언스가 vCenter Server 또는 ESXi 호스트에 연결하는 데 필요한 자격 증명.
        관리자 역할이 할당된 기존 계정을 사용하는 대신 vCenter Server 또는 ESXi 호스트 액세스 전용 계정을 사용하는 것이 좋습니다. 전용 계정에 필요한 권한에 대해 자세히 알아보려면 "Agent for VMware - 필수 권한"(635페이지) 항목을 참조하십시오.
   b. **연결 확인**을 클릭하여 설정이 올바른지 확인합니다.
   c. **확인**을 클릭합니다.
4. 다음 방법 중 하나를 사용하여 어플라이언스를 Cyber Protection 서비스에 등록합니다.
   - [2단계 인증 미사용 테넌트에만 해당] 그래픽 인터페이스에서 어플라이언스를 등록합니다.
     a. **에이전트 옵션**의 **관리 서버**에서 **변경**을 클릭합니다.
     b. **서버 이름/IP** 필드에서 **클라우드**를 선택합니다.
        Cyber Protection 서비스 주소가 표시됩니다. 별도의 지시가 없는 한, 이 주소는 변경하지 마십시오.
     c. **사용자 이름** 및 **암호** 필드에서 Cyber Protection 서비스의 계정 자격 증명을 지정합니다. 가상 어플라이언스 및 해당 어플라이언스가 관리하는 가상 머신이 이 계정에 등록됩니다.
     d. **확인**을 클릭합니다.
   - 명령줄 인터페이스에서 어플라이언스를 등록합니다.

     참고
     이 방법을 사용할 때는 등록 토큰이 필요합니다. 토큰 생성 방법에 대한 자세한 내용은 "등록 토큰 생성"(156페이지) 항목을 참조하십시오.

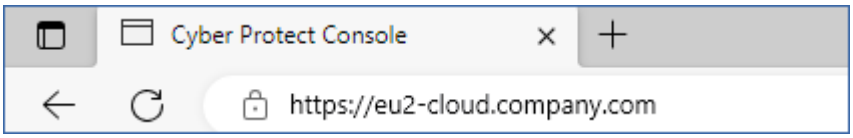
     a. Ctrl+Shift+F2를 눌러 명령줄 인터페이스를 엽니다.
     b. 다음 명령을 실행합니다.

```
register_agent -o register -t cloud -a <service address> --token <registration
token>
```


© Acronis International GmbH, 2003-2024

참고

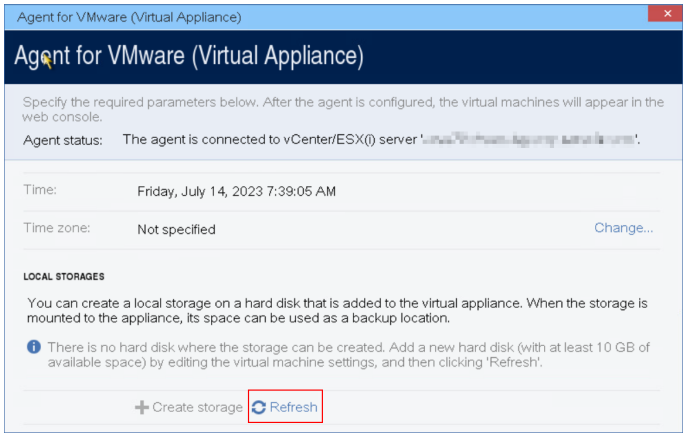
등록 토큰을 사용할 때는 정확한 데이터 센터 주소를 지정해야 합니다. 이 주소는 Cyber Protect 콘솔에 **로그인하고 나면** 표시되는 URL입니다. 예: `https://eu2-cloud.company.com`.



여기서 `https://cloud.company.com`을 사용하지 마십시오.

c. 어플라이언스의 그래픽 인터페이스로 돌아가려면 Alt+F1을 누릅니다.

5. [선택 사항] 로컬 스토리지를 추가합니다.
   a. vSphere Client에서 가상 어플라이언스에 가상 디스크를 연결합니다. 가상 디스크에는 10GB 이상의 여유 공간이 있어야 합니다.
   b. 어플라이언스의 그래픽 사용자 인터페이스에서 **새로 고침**을 클릭합니다.



   스토리지 생성 버튼이 활성화됩니다.
   c. **스토리지 생성**을 클릭합니다.
   d. 스토리지의 레이블을 지정하고 **확인**을 클릭합니다.
   e. **예**를 클릭하여 선택을 확인합니다.

6. [프록시 서버가 네트워크에서 활성화되어 있는 경우] 프록시 서버를 구성합니다.
   a. Ctrl+Shift+F2를 눌러 명령줄 인터페이스를 엽니다.
   b. 텍스트 편집기에서 **/etc/Acronis/Global.config** 파일을 엽니다.
   c. 다음 중 하나를 수행하십시오.
      - 에이전트 설치 중에 프록시 설정을 지정한 경우 다음 섹션을 참조하십시오.

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```


© Acronis International GmbH, 2003-2024

- 그렇지 않으면 위의 행을 복사하고 파일에서 `<registry name="Global">...</registry>` 태그 사이에 붙여넣습니다.

d. `ADDRESS`를 프록시 서버 호스트 이름/IP 주소로 대체하고 `PORT`는 포트 번호의 10진수 값으로 대체합니다.

e. 프록시 서버에 인증이 필요하다면 `LOGIN` 및 `PASSWORD`를 프록시 서버 자격 증명으로 대체합니다. 그렇지 않은 경우, 파일에서 이 라인을 삭제합니다.

f. 파일을 저장합니다.

g. 텍스트 편집기에서 **/opt/acronis/etc/aakore.yaml** 파일을 엽니다.

h. **env** 섹션을 찾거나 생성한 후, 다음 행을 추가합니다.

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

i. `proxy_login`과 `proxy_password`는 프록시 서버 자격 증명으로, `proxy_address:port`는 프록시 서버의 주소와 포트 번호로 대체합니다.

j. `reboot` 명령을 실행합니다.

참고

프록시를 통해 디플로이된 가상 어플라이언스를 업데이트하려면 어플라이언스의 `config.yaml` 파일(`/opt/acronis/etc/va-updater/config.yaml`)을 편집합니다. 즉, 해당 파일 맨 아래에 다음 줄을 추가한 후 환경에 적합한 값을 입력합니다.

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

예:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Agent for Scale Computing HC3(가상 어플라이언스) 배포 중

시작하기 전에

이 어플라이언스는 Scale Computing HC3 클러스터에 디플로이하는 미리 구성된 가상 머신입니다. 클러스터의 모든 가상 머신에 대한 사이버 보호를 관리할 수 있게 해주는 보호 에이전트를 포함합니다.

에이전트에 대한 시스템 요구사항

기본적으로 에이전트가 설치된 가상 머신은 vCPU 2개와 4GiB RAM을 사용합니다. 대다수 작업에는 이러한 설정을 사용하면 충분합니다. 하지만 Scale Computing HC3 웹 인터페이스에서 가상 머신을 편집하여 해당 설정을 변경할 수 있습니다.

© Acronis International GmbH, 2003-2024

백업 성능을 개선하고 RAM 메모리 부족으로 인한 오류를 방지하려면 리소스가 더 많이 필요할 때 이러한 리소스를 RAM 8GiB, vCPU 4개로 늘리는 것이 좋습니다. 예를 들어 백업 트래픽의 양이 초당 100MB를 초과할 것으로 예상되거나(예: 10기가바이트 네트워크) 대용량 하드 드라이브(500GB 이상)를 사용하는 여러 가상 머신을 동시에 백업해야 한다면 할당된 리소스를 늘립니다.

어플라이언스 가상 디스크의 크기는 약 9GB입니다.

필요한 에이전트 수는?

한 개의 에이전트가 전체 클러스터를 보호할 수 있습니다. 그러나 백업 트래픽 대역폭 로드를 분배해야 할 경우 한 클러스터에 여러 개의 에이전트를 보유할 수 있습니다.

한 클러스터에 여러 개의 에이전트가 있을 경우 가상 머신은 자동으로 에이전트 사이에 동등하게 분배되기 때문에 각 에이전트는 비슷한 수의 머신을 관리하게 됩니다.

에이전트 간 로드 불균형이 20%에 도달하면 자동 재분배가 수행됩니다. 머신이나 에이전트를 추가하거나 제거하면 자동 재분배가 수행될 수 있습니다. 예를 들어, 처리량 문제로 에이전트가 더 필요하다고 판단하여 클러스터에 추가 가상 어플라이언스를 디플로이할 수 있습니다. 관리 서버는 새 에이전트에 가장 적합한 머신을 할당합니다. 이전 에이전트의 로드는 감소합니다. 관리 서버에서 에이전트를 제거하는 경우 에이전트에 할당된 머신은 나머지 에이전트에 재분배됩니다. 그러나 에이전트가 손상되거나 Scale Computing HC3 클러스터에서 수동으로 삭제된 경우에는 수행되지 않습니다. Cyber Protect 콘솔에서 해당 에이전트를 제거한 후에만 재분배가 시작됩니다.

특정 머신을 관리하는 에이전트를 확인하려면

1. Cyber Protect 콘솔에서 **장치**를 클릭하고 **Scame Computing**을 선택합니다.
2. 표 오른쪽 위의 기어 아이콘을 클릭하고 **시스템** 아래에서 **에이전트** 확인란을 선택합니다.
3. 표시되는 열에서 에이전트의 이름을 확인합니다.

QCOW2 템플릿 디플로이

1. Cyber Protection 계정에 로그인합니다.
2. **장치** > **모든 장치** > **추가** > **Scale Computing HC3**을 클릭합니다.
   .Zip 아카이브가 귀하의 머신에 다운로드됩니다.
3. Zip 아카이브의 압축을 풀고 **ScaleAppliance** 폴더에 .qcow2 파일과 .xml 파일을 저장합니다.
4. 네트워크 공유에 **ScaleAppliance** 폴더를 업로드하고 Scale Computing HC3 클러스터가 해당 폴더에 액세스할 수 있는지 확인합니다.
5. **VM 생성/편집** 역할이 할당된 관리자로 Scale Computing HC3 클러스터에 로그인합니다. Scale Computing HC3 가상 머신을 사용하는 작업에 필요한 역할에 대한 자세한 내용은 "Agent for Scale Computing HC3 – 필요한 역할"(133페이지)을(를) 참조하십시오.
6. Scale Computing HC3 웹 인터페이스에서 **ScaleAppliance** 폴더의 가상 머신 템플릿을 가져옵니다.
   a. **HC3 VM 가져오기** 아이콘을 클릭합니다.
   b. **HC3 VM 가져오기** 창에서 다음 항목을 지정합니다.
      - 새 가상 머신의 이름.
      - **ScaleAppliance** 폴더가 있는 네트워크 공유.

© Acronis International GmbH, 2003-2024

- 이 네트워크 공유에 액세스하는 데 필요한 사용자 이름 및 비밀번호.
- [선택 사항] 새 가상 머신의 도메인 태그.
- 네트워크 공유의 **ScaleAppliance** 폴더 경로.

c. **가져오기**를 클릭합니다.

디플로이가 완료되면, 가상 어플라이언스를 구성해야 합니다. 가상 어플라이언스를 구성하는 방법에 대한 자세한 내용은 "가상 어플라이언스 구성"(131페이지)을(를) 참조하십시오.

참고
클러스터에 가상 어플라이언스가 여러 개 필요한 경우 위 단계를 반복하여 가상 어플라이언스를 추가로 디플로이하십시오. Scale Computing HC3 웹 인터페이스에서 **VM 복제** 옵션을 사용하여 기존 가상 어플라이언스를 복제하지 마십시오.

가상 어플라이언스 구성

가상 어플라이언스를 디플로이한 뒤 어플라이언스가 보호해야 하는 Scale Computing HC3 클러스터와 Cyber Protection 서비스에 모두 연결할 수 있도록 어플라이언스를 구성해야 합니다.

가상 어플라이언스을 구성하려면

1. Scale Computing HC3 계정에 로그인합니다.
2. 구성할 가상 어플라이언스를 선택하고 **콘솔** 아이콘을 클릭합니다.
3. **eth0** 필드에서 어플라이언스의 네트워크 인터페이스를 구성합니다.
   자동으로 할당된 DHCP 주소(있는 경우)가 가상 머신이 사용하는 네트워크 내에서 유효한지 확인하거나 수동으로 할당하십시오. 어플라이언스가 사용하는 네트워크의 수에 따라 한 개 이상의 인터페이스를 구성해야 할 수 있습니다.
4. **Scale Computing** 필드에서 **변경**을 클릭하여 Scale Computing HC3 클러스터 주소 및 해당 주소에 액세스하는 데 필요한 자격 증명을 지정합니다.
   a. **서버 이름/IP** 필드에 클러스터의 DNS이름 또는 IP주소를 입력합니다.
   b. **사용자 이름** 및 **비밀번호** 필드에는 Scale Computing HC3 관리자 계정의 자격 증명을 입력합니다.
      이 계정에 Scale Computing HC3 가상 머신 작업에 필요한 역할이 할당되어 있는지 확인합니다. 이러한 역할에 대한 자세한 내용은 "Agent for Scale Computing HC3 – 필요한 역할"(133페이지)을(를) 참조하십시오.
   c. **연결 확인**을 클릭하여 설정이 올바른지 확인합니다.
   d. **확인**을 클릭합니다.
5. 다음 방법 중 하나를 사용하여 어플라이언스를 Cyber Protection 서비스에 등록합니다.
   - [2단계 인증 미사용 테넌트에만 해당] 그래픽 인터페이스에서 어플라이언스를 등록합니다.
     a. **에이전트 옵션**의 **관리 서버**에서 **변경**을 클릭합니다.
     b. **서버 이름/IP** 필드에서 **클라우드**를 선택합니다.
        Cyber Protection 서비스 주소가 표시됩니다. 별도의 지시가 없는 한, 이 주소는 변경하지 마십시오.

© Acronis International GmbH, 2003-2024

c. **사용자 이름** 및 **암호** 필드에서 Cyber Protection 서비스의 계정 자격 증명을 지정합니다. 가상 어플라이언스 및 해당 어플라이언스가 관리하는 가상 머신이 이 계정에 등록됩니다.

d. **확인**을 클릭합니다.

- 명령줄 인터페이스에서 어플라이언스를 등록합니다.

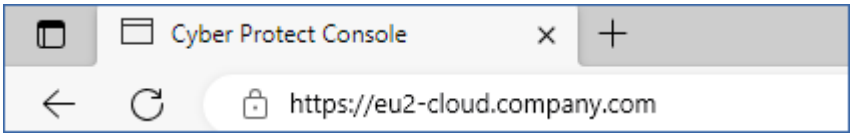
참고
이 방법을 사용할 때는 등록 토큰이 필요합니다. 토큰 생성 방법에 대한 자세한 내용은 "등록 토큰 생성"(156페이지) 항목을 참조하십시오.

a. Ctrl+Shift+F2를 눌러 명령줄 인터페이스를 엽니다.

b. 다음 명령을 실행합니다.

```
register_agent -o register -t cloud -a <service address> --token <registration token>
```

참고
등록 토큰을 사용할 때는 정확한 데이터 센터 주소를 지정해야 합니다. 이 주소는 Cyber Protect 콘솔에 **로그인하고 나면** 표시되는 URL입니다. 예: `https://eu2-cloud.company.com`.



여기서 `https://cloud.company.com`을 사용하지 마십시오.

c. 어플라이언스의 그래픽 인터페이스로 돌아가려면 Alt+F1을 누릅니다.

6. [선택 사항] **이름** 필드에서 **변경**을 클릭하여 가상 어플라이언스의 기본 이름인 **localhost**를 편집합니다. 이 이름은 Cyber Protect 콘솔에 표시됩니다.
7. [선택 사항] **시간** 필드에서 **변경**을 클릭하고 예정된 작업이 적절한 시간에 실행될 수 있도록 사용자 지역의 시간대를 선택합니다.
8. [프록시 서버가 네트워크에서 활성화되어 있는 경우] 프록시 서버를 구성합니다.
   a. Ctrl+Shift+F2를 눌러 명령줄 인터페이스를 엽니다.
   b. 텍스트 편집기에서 **/etc/Acronis/Global.config** 파일을 엽니다.
   c. 다음 중 하나를 수행하십시오.
      - 에이전트 설치 중에 프록시 설정을 지정한 경우 다음 섹션을 참조하십시오.

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```


© Acronis International GmbH, 2003-2024

- 그렇지 않으면 위의 행을 복사하고 파일에서 `<registry name="Global">...</registry>` 태그 사이에 붙여넣습니다.

d. `ADDRESS`를 프록시 서버 호스트 이름/IP 주소로 대체하고 `PORT`는 포트 번호의 10진수 값으로 대체합니다.

e. 프록시 서버에 인증이 필요하다면 `LOGIN` 및 `PASSWORD`를 프록시 서버 자격 증명으로 대체합니다. 그렇지 않은 경우, 파일에서 이 라인을 삭제합니다.

f. 파일을 저장합니다.

g. 텍스트 편집기에서 **/opt/acronis/etc/aakore.yaml** 파일을 엽니다.

h. **env** 섹션을 찾거나 생성한 후, 다음 행을 추가합니다.

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

i. `proxy_login`과 `proxy_password`는 프록시 서버 자격 증명으로, `proxy_address:port`는 프록시 서버의 주소와 포트 번호로 대체합니다.

j. `reboot` 명령을 실행합니다.

참고

프록시를 통해 디플로이된 가상 어플라이언스를 업데이트하려면 어플라이언스의 `config.yaml` 파일(`/opt/acronis/etc/va-updater/config.yaml`)을 편집합니다. 즉, 해당 파일 맨 아래에 다음 줄을 추가한 후 환경에 적합한 값을 입력합니다.

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

예:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Scale Computing HC3 클러스터의 가상 머신을 보호하려면

1. Cyber Protection 계정에 로그인합니다.
2. **장치** > **Scale Computing HC3** > <사용자 클러스터>로 이동하거나 **장치** > **모든 장치**에서 머신을 확인할 수 있습니다.
3. 머신을 선택하고 보호 계획을 적용합니다.

Agent for Scale Computing HC3 – 필요한 역할

이 섹션은 Scale Computing HC3 가상 머신 작업에 필요한 역할에 대해 설명합니다.

작업	역할
가상 머신을 백업합니다	백업 VM 생성/편집 VM 삭제

© Acronis International GmbH, 2003-2024

기존 가상 머신으로 복구	백업 VM 생성/편집 VM 전원 제어 VM 삭제 클러스터 설정
새 가상 머신으로 복구	백업 VM 생성/편집 VM 전원 제어 VM 삭제 클러스터 설정

Agent for Virtuozzo Hybrid Infrastructure(가상 어플라이언스) 디플로이

시작하기 전에

이 어플라이언스는 Virtuozzo Hybrid Infrastructure에 디플로이하는 미리 구성된 가상 머신입니다. Virtuozzo Hybrid Infrastructure 클러스터의 모든 가상 머신에 대한 사이버 보호를 관리할 수 있게 해주는 보호 에이전트를 포함합니다.

참고
가상 머신용 VSS(Volume Shadow Copy Service) 백업 옵션이 활성화된 백업이 정상적으로 실행되고 애플리케이션 일관성 상태에서 데이터를 캡처하도록 하려면 보호된 가상 머신에 Virtuozzo Guest Tools가 설치되어 있으며 최신 상태인지 확인합니다.

에이전트에 대한 시스템 요구사항

가상 어플라이언스를 디플로이할 때 미리 정의된 여러 vCPU 및 RAM(방식) 조합 중에 선택할 수 있습니다. 자신만의 방식을 생성할 수도 있습니다.

vCPU 2개 및 RAM 4GB(중간 방식)가 대다수 작업에 최적의 상태로 실행되는 조합입니다. 백업 성능을 개선하고 RAM 메모리 부족으로 인한 오류를 방지하려면 리소스가 더 많이 필요할 때 이러한 리소스를 RAM 8GB, vCPU 4개로 늘리는 것이 좋습니다. 예를 들어 백업 트래픽의 양이 초당 100MB를 초과할 것으로 예상되거나(예: 10기가바이트 네트워크) 대용량 하드 드라이브(500GB 이상)를 사용하는 여러 가상 머신을 동시에 백업해야 한다면 할당된 리소스를 늘립니다.

필요한 에이전트 수는?

한 개의 에이전트가 전체 클러스터를 보호할 수 있습니다. 그러나 백업 트래픽 대역폭 로드를 분배해야 할 경우 한 클러스터에 여러 개의 에이전트를 보유할 수 있습니다.

© Acronis International GmbH, 2003-2024

한 클러스터에 여러 개의 에이전트가 있을 경우 가상 머신은 자동으로 에이전트 사이에 동등하게 분배되기 때문에 각 에이전트는 비슷한 수의 머신을 관리하게 됩니다.

에이전트 간 로드 불균형이 20%에 도달하면 자동 재분배가 수행됩니다. 머신이나 에이전트를 추가하거나 제거하면 자동 재분배가 수행될 수 있습니다. 예를 들어, 처리량 문제로 에이전트가 더 필요하다고 판단하여 클러스터에 추가 가상 어플라이언스를 디플로이할 수 있습니다. 관리 서버는 새 에이전트에 가장 적합한 머신을 할당합니다. 이전 에이전트의 로드는 감소합니다. 관리 서버에서 에이전트를 제거하는 경우 에이전트에 할당된 머신은 나머지 에이전트에 재분배됩니다. 그러나 에이전트가 손상되거나 Virtuozzo Hybrid Infrastructure 노드에서 수동으로 삭제된 경우에는 수행되지 않습니다. Cyber Protection 웹 인터페이스에서 해당 에이전트를 제거한 후에만 재분배가 시작됩니다.

특정 머신을 관리하는 에이전트를 확인하려면

1. Cyber Protect 콘솔에서 **장치**를 클릭하고 **Virtuozzo Hybrid Infrastructure**를 선택합니다.
2. 표 오른쪽 위의 기어 아이콘을 클릭하고 **시스템** 아래에서 **에이전트** 확인란을 선택합니다.
3. 표시되는 열에서 에이전트의 이름을 확인합니다.

제한 사항

- Virtuozzo Hybrid Infrastructure 어플라이언스는 원격으로 디플로이될 수 없습니다.
- 가상 머신의 애플리케이션 인식 백업은 지원되지 않습니다.

Virtuozzo Hybrid Infrastructure의 네트워크 구성

가상 어플라이언스를 디플로이하고 구성하기 전에 Virtuozzo Hybrid Infrastructure의 네트워크를 구성해야 합니다.

Virtuozzo Hybrid Infrastructure(가상 어플라이언스)용 Agent의 네트워크 요구조건

- 가상 어플라이언스는 2개의 네트워크 어댑터를 필요로 합니다.
- 가상 어플라이언스는 반드시 다음과 같은 네트워크 트래픽 유형으로 Virtuozzo 네트워크에 연결되어야 합니다:
  - Compute API
  - VM Backup
  - ABGW Public
  - VM Public

네트워크 구성에 관한 자세한 정보는 Virtuozzo 문서의 컴퓨팅 클러스터 요구 조건을 참조하십시오.

Virtuozzo Hybrid Infrastructure의 사용자 계정 구성

가상 어플라이언스를 구성하려면 Virtuozzo Hybrid Infrastructure 사용자 계정이 필요합니다. 이 계정에는 **기본** 도메인에 대한 **관리자** 역할이 있어야 합니다. 사용자에 대한 자세한 정보는 Virtuozzo Hybrid Infrastructure 문서의 관리자 패널 사용자 관리를 참조하십시오. 이 계정에 **기본** 도메인의 모든 프로젝트에 대한 액세스 권한을 부여했는지 확인하십시오.

© Acronis International GmbH, 2003-2024

기본 도메인의 모든 프로젝트에 대한 액세스 권한을 부여하려면

1. 시스템 관리자용 환경 파일을 생성합니다. 이 파일을 생성하려면 OpenStack 명령줄 인터페이스를 통해 Virtuozzo Hybrid Infrastructure 클러스터에서 다음 스크립트를 실행합니다. 이 인터페이스에 연결하는 방법에 대한 자세한 내용은 Virtuozzo Hybrid Infrastructure 문서의 OpenStack 명령줄 인터페이스에 연결을 참조하십시오.

   ```
   su - vstoradmin
   kolla-ansible post-deploy
   exit
   ```

2. 환경 파일을 사용하여 추가 OpenStack 명령 실행 권한을 부여합니다.

   ```
   . /etc/kolla/admin-openrc.sh
   ```

3. 다음 명령 실행:

   ```
   openstack --insecure user set --project admin --project-domain Default --domain
   Default <username>
   openstack --insecure role add --domain Default --user <username> --user-domain
   Default compute --inherited
   ```

   여기에서 <사용자 이름>은 **기본** 도메인에서 **관리자** 역할을 가진 Virtuozzo Hybrid Infrastructure 계정입니다. 가상 어플라이언스는 이 계정을 사용하여 **기본** 도메인에 있는 모든 하위 프로젝트의 가상 머신을 백업하고 복원합니다.

예

```
su - vstoradmin
kolla-ansible post-deploy
exit
. /etc/kolla/admin-openrc.sh
openstack --insecure user set --project admin --project-domain Default --domain Default
johndoe
openstack --insecure role add --domain Default --user johndoe --user-domain Default
compute --inherited
```

기본 도메인 외의 도메인에 있는 가상 머신의 백업을 관리하려면 다음 명령도 실행합니다.

다른 도메인의 모든 프로젝트에 대한 액세스 권한을 부여하려면

```
openstack --insecure role add --domain <domain name> --inherited --user <username> --
user-domain Default admin
```

여기에서 <도메인 이름>은 <사용자 이름> 계정이 액세스 권한을 가지고 있는 프로젝트에 대한 도메인입니다.

© Acronis International GmbH, 2003-2024

예

```
openstack --insecure role add --domain MyNewDomain --inherited --user johndoe --user-
domain Default admin
```

프로젝트 액세스 권한이 부여되고 나면 계정에 할당된 역할을 확인합니다.

할당된 역할을 확인하려면

```
openstack --insecure role assignment list --user <username> --names
```

여기에서 <사용자 이름>은 Virtuozzo Hybrid Infrastructure 계정입니다.

예

```
openstack --insecure role assignment list --user johndoe --names -c Role -c User -c
Project -c Domain
+--------------+-----------------+---------+-------------+
| Role         | User            | Project | Domain      |
+--------------+-----------------+---------+-------------+
| admin        | johndoe@Default |         | MyNewDomain |
| compute      | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
+--------------+-----------------+---------+-------------+
```

이 예제에서는 `-c Role`, `-c User`, `-c Project`, `-c Domain` 옵션을 사용하여 페이지에 맞도록 명령 출력을 요약합니다.

모든 프로젝트의 계정에 할당된 유효 역할을 확인하려면 다음 명령도 실행합니다.

모든 프로젝트의 유효 역할을 확인하려면

```
openstack --insecure role assignment list --user <username> --names --effective
```

여기에서 <사용자 이름>은 Virtuozzo Hybrid Infrastructure 계정입니다.

예

```
openstack --insecure role assignment list --user johndoe --names --effective  -c Role -c
User -c Project -c Domain
+--------------+-----------------+-----------------+---------+
| Role         | User            | Project         | Domain  |
+--------------+-----------------+-----------------+---------+
| domain_admin | johndoe@Default |                 | Default |
| compute      | johndoe@Default | admin@Default   |         |
| compute      | johndoe@Default | service@Default |         |
| domain_admin | johndoe@Default | admin@Default   |         |
```


© Acronis International GmbH, 2003-2024

```
| domain_admin | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | service@Default |         |
| member       | johndoe@Default | service@Default |         |
| reader       | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | admin@Default   |         |
| member       | johndoe@Default | admin@Default   |         |
| reader       | johndoe@Default | admin@Default   |         |
| project_user | johndoe@Default |                 | Default |
| member       | johndoe@Default |                 | Default |
| reader       | johndoe@Default |                 | Default |
+--------------+-----------------+-----------------+---------+
```

이 예제에서는 `-c Role`, `-c User`, `-c Project`, `-c Domain` 옵션을 사용하여 페이지에 맞도록 명령 출력을 요약합니다.

QCOW2 템플릿 디플로이

1. Cyber Protection 계정에 로그인합니다.
2. **장치** > **모든 장치** > **추가** > **Virtuozzo Hybrid Infrastructure**를 클릭합니다.
   .Zip 아카이브가 귀하의 머신에 다운로드됩니다.
3. .zip 아카이브의 압축을 풉니다. .qcow2 이미지 파일이 포함되어 있습니다.
4. Virtuozzo Hybrid Infrastructure 계정에 로그인합니다.
5. .qcow2 이미지 파일을 다음과 같이 Virtuozzo Hybrid Infrastructure 컴퓨팅 클러스터에 추가합니다.
   - **컴퓨팅** > **가상 머신** > **이미지** 탭에서 **이미지 추가**를 클릭합니다.
   - **이미지 추가** 창에서 **찾아보기**를 클릭한 다음, .qcow2 파일을 선택합니다.
   - 이미지 이름을 특정하고, **Generic Linux OS** 유형을 선택한 다음 **추가**를 클릭합니다.
6. **컴퓨팅** > **가상 머신** > **가상 머신** 탭에서 **가상 머신 생성**을 클릭합니다. 새 창이 열리면 다음 매개변수를 특정해야 합니다.
   - 새 가상 머신의 이름.
   - **다음에서 디플로이**에서 **이미지**를 선택합니다.
   - **이미지** 창에서 어플라이언스의 .qcow2 이미지 파일을 선택한 다음 **완료**를 클릭합니다.
   - **볼륨** 창에서 볼륨을 추가할 필요 없습니다. 시스템 디스크에 대해 자동으로 추가되는 볼륨으로 충분합니다.
   - **선호 방식** 창에서 원하는 vCPU 및 RAM의 조합을 선택한 다음 **완료**를 클릭합니다. 일반적으로 2vCPU 및 4GiB RAM이면 충분합니다.
   - **네트워크 인터페이스** 창에서 **추가**를 클릭하고 *공용* 유형의 가상 네트워크를 선택한 다음 **추가**를 클릭합니다. 추가한 네트워크는 **네트워크 인터페이스** 목록에 표시됩니다.
     한 개 이상의 물리적 네트워크 환경을 사용하여 한 개 이상의 공용 유형 가상 네트워크를 사용할 경우, 이 단계를 반복하여 필요한 가상 네트워크를 선택하십시오.
7. **완료**를 클릭합니다.
8. 앞서 이용했던 **가상 머신 생성** 창에서 **디플로이**를 클릭해 가상 머신을 생성하고 부팅합니다.

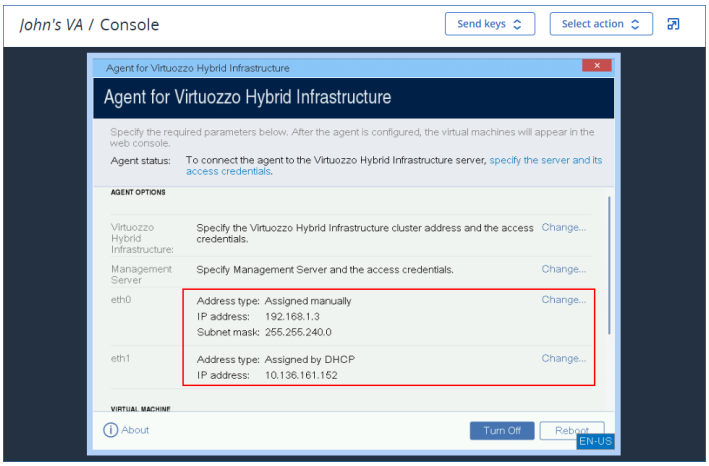
© Acronis International GmbH, 2003-2024

가상 어플라이언스 구성

Agent for Virtuozzo Hybrid Infrastructure(가상 어플라이언스)를 디플로이한 뒤 가상 어플라이언스가 보호해야 하는 Virtuozzo Hybrid Infrastructure 클러스터와 Cyber Protection 클라우드 서비스에 모두 연결할 수 있도록 가상 어플라이언스를 구성해야 합니다.

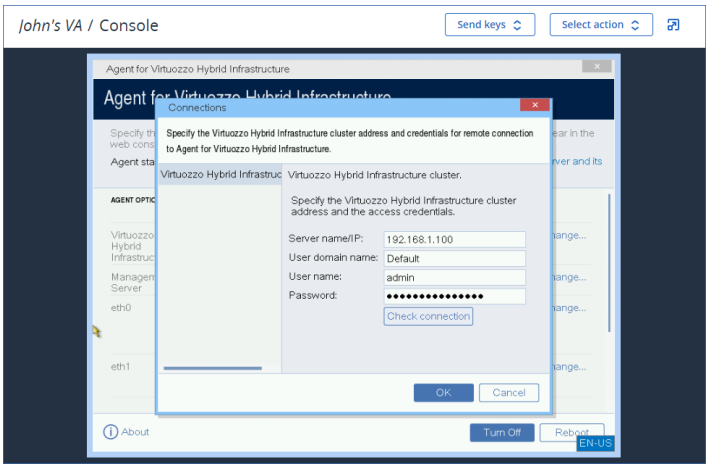
가상 어플라이언스을 구성하려면

1. Virtuozzo Hybrid Infrastructure 계정에 로그인합니다.
2. **컴퓨팅** > **가상 머신** > **가상 머신** 탭에서 생성한 머신을 선택합니다. 그런 다음 **콘솔**을 클릭합니다.
3. 어플라이언스의 네트워크 인터페이스를 구성합니다. 어플라이언스가 사용하는 가상 네트워크의 수에 따라 한 개 이상의 인터페이스를 구상해야 할 수 있습니다. 자동으로 할당된 DHCP 주소(있는 경우)가 가상 머신이 사용하는 네트워크 내에서 유효한지 확인하거나 수동으로 할당하십시오.



4. Virtuozzo 클러스터 주소 및 자격 증명을 지정하십시오.
   - Virtuozzo Hybrid Infrastructure 클러스터의 DNS 이름 또는 IP 주소. 클러스터의 관리 노드 주소입니다. 기본 포트 5000이 자동으로 설정됩니다. 다른 포트를 사용할 경우 수동으로 지정해야 합니다.
   - **사용자 도메인 이름** 필드에 Virtuozzo Hybrid Infrastructure의 도메인을 지정합니다. 예: **기본**.
     도메인 이름은 대/소문자를 구분합니다.
   - 여기에서 **사용자 이름** 및 **패스워드** 필드에는 지정된 도메인에서 **관리자** 역할을 가진 Virtuozzo Hybrid Infrastructure 사용자 계정의 자격 증명을 입력합니다. 사용자, 역할 및 도메인에 대한 자세한 내용은 Virtuozzo Hybrid Infrastructure의 사용자 계정 구성을 참조하십시오.

© Acronis International GmbH, 2003-2024



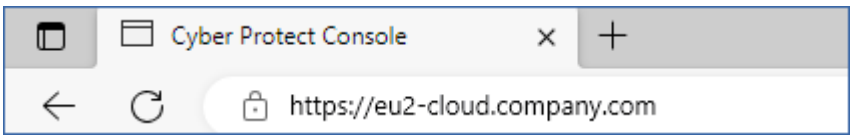
5. 다음 방법 중 하나를 사용하여 어플라이언스를 Cyber Protection 서비스에 등록합니다.
   - [2단계 인증 미사용 테넌트에만 해당] 그래픽 인터페이스에서 어플라이언스를 등록합니다.
     a. **에이전트 옵션**의 **관리 서버**에서 **변경**을 클릭합니다.
     b. **서버 이름/IP** 필드에서 **클라우드**를 선택합니다.
        Cyber Protection 서비스 주소가 표시됩니다. 별도의 지시가 없는 한, 이 주소는 변경하지 마십시오.
     c. **사용자 이름** 및 **암호** 필드에서 Cyber Protection 서비스의 계정 자격 증명을 지정합니다. 가상 어플라이언스 및 해당 어플라이언스가 관리하는 가상 머신이 이 계정에 등록됩니다.
     d. **확인**을 클릭합니다.
   - 명령줄 인터페이스에서 어플라이언스를 등록합니다.

     참고
     이 방법을 사용할 때는 등록 토큰이 필요합니다. 토큰 생성 방법에 대한 자세한 내용은 "등록 토큰 생성"(156페이지) 항목을 참조하십시오.

     a. Ctrl+Shift+F2를 눌러 명령줄 인터페이스를 엽니다.
     b. 다음 명령을 실행합니다.

     ```
     register_agent -o register -t cloud -a <service address> --token <registration token>
     ```

     참고
     등록 토큰을 사용할 때는 정확한 데이터 센터 주소를 지정해야 합니다. 이 주소는 Cyber Protect 콘솔에 **로그인하고 나면** 표시되는 URL입니다. 예: `https://eu2-cloud.company.com`.

© Acronis International GmbH, 2003-2024

여기서 `https://cloud.company.com`을 사용하지 마십시오.

c. 어플라이언스의 그래픽 인터페이스로 돌아가려면 Alt+F1을 누릅니다.

6. [프록시 서버가 네트워크에서 활성화되어 있는 경우] 프록시 서버를 구성합니다.
   a. Ctrl+Shift+F2를 눌러 명령줄 인터페이스를 엽니다.
   b. 텍스트 편집기에서 **/etc/Acronis/Global.config** 파일을 엽니다.
   c. 다음 중 하나를 수행하십시오.
      - 에이전트 설치 중에 프록시 설정을 지정한 경우 다음 섹션을 참조하십시오.

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

      - 그렇지 않으면 위의 행을 복사하고 파일에서 `<registry name="Global">...</registry>` 태그 사이에 붙여넣습니다.
   d. `ADDRESS`를 프록시 서버 호스트 이름/IP 주소로 대체하고 `PORT`는 포트 번호의 10진수 값으로 대체합니다.
   e. 프록시 서버에 인증이 필요하다면 `LOGIN` 및 `PASSWORD`를 프록시 서버 자격 증명으로 대체합니다. 그렇지 않은 경우, 파일에서 이 라인을 삭제합니다.
   f. 파일을 저장합니다.
   g. 텍스트 편집기에서 **/opt/acronis/etc/aakore.yaml** 파일을 엽니다.
   h. **env** 섹션을 찾거나 생성한 후, 다음 행을 추가합니다.

```
env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
```

   i. `proxy_login`과 `proxy_password`는 프록시 서버 자격 증명으로, `proxy_address:port`는 프록시 서버의 주소와 포트 번호로 대체합니다.
   j. `reboot` 명령을 실행합니다.

참고

프록시를 통해 디플로이된 가상 어플라이언스를 업데이트하려면 어플라이언스의 `config.yaml` 파일(`/opt/acronis/etc/va-updater/config.yaml`)을 편집합니다. 즉, 해당 파일 맨 아래에 다음 줄을 추가한 후 환경에 적합한 값을 입력합니다.

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

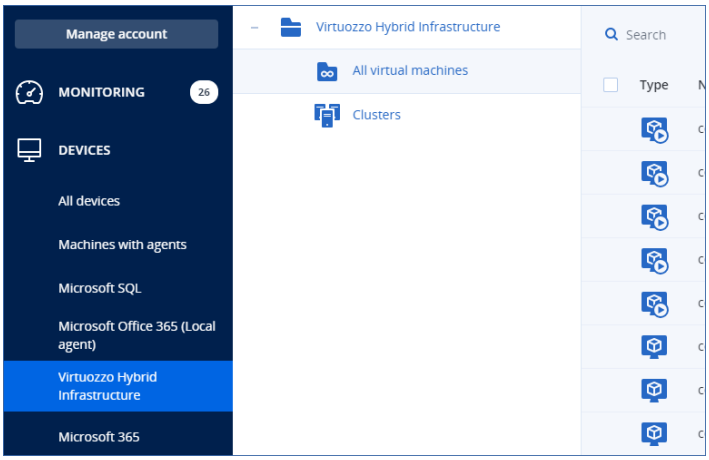
예:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```


© Acronis International GmbH, 2003-2024

***Virtuozzo Hybrid Infrastructure*리드 인프라 클러스터의 가상 머신을 보호하려면**

1. Cyber Protection 계정에 로그인합니다.
2. **장치** > **Virtuozo 하이브리드 인프라** > <사용자 클러스터> > **기본 프로젝트** > **관리자**로 이동하거나 **장치** > **모든 장치**에서 머신을 확인할 수 있습니다.
3. 머신을 선택하고 보호 계획을 적용합니다.



Agent for oVirt(가상 어플라이언스) 디플로이 중

시작하기 전에

이 어플라이언스는 Red Hat Virtualization/oVirt 데이터 센터에 디플로이하는 미리 구성된 가상 머신입니다. 이 어플라이언스는 데이터 센터의 모든 가상 머신에 대한 사이버 보호를 관리할 수 있게 해주는 보호 에이전트를 포함합니다.

에이전트에 대한 시스템 요구사항

기본적으로 에이전트가 설치된 가상 머신은 vCPU 2개와 4GiB RAM을 사용합니다. 대다수 작업에는 이러한 설정을 사용하면 충분합니다. 하지만 Red Hat Virtualization/oVirt 관리 포털에서 해당 설정을 편집할 수 있습니다.

백업 성능을 개선하고 RAM 메모리 부족으로 인한 오류를 방지하려면 리소스가 더 많이 필요할 때 이러한 리소스를 RAM 8GiB, vCPU 4개로 늘리는 것이 좋습니다. 예를 들어 백업 트래픽의 양이 초당 100MB를 초과할 것으로 예상되거나(예: 10기가바이트 네트워크) 대용량 하드 드라이브(500GB 이상)를 사용하는 여러 가상 머신을 동시에 백업해야 한다면 할당된 리소스를 늘립니다.

어플라이언스 가상 디스크의 크기는 8GiB입니다.

필요한 에이전트 수는?

한 개의 에이전트가 전체 데이터 센터를 보호할 수 있습니다. 그러나 백업 트래픽 대역폭 로드를 분배해야 할 경우 한 데이터 센터에 여러 개의 에이전트를 보유할 수 있습니다.

한 데이터 센터에 여러 개의 에이전트가 있을 경우 가상 머신은 자동으로 에이전트 사이에 분배되기 때문에 각 에이전트는 비슷한 수의 머신을 관리하게 됩니다.

© Acronis International GmbH, 2003-2024

에이전트 간 로드 불균형이 20%에 도달하면 자동 재분배가 수행됩니다. 머신이나 에이전트를 추가하거나 제거하면 자동 재분배가 수행될 수 있습니다. 예를 들어, 처리량 문제로 에이전트가 더 필요하다고 판단하여 데이터 센터에 추가 가상 어플라이언스를 디플로이할 수 있습니다. 관리 서버는 새 에이전트에 가장 적합한 머신을 할당합니다. 이전 에이전트의 로드는 감소합니다. 에이전트를 제거하는 경우 에이전트에 할당된 머신은 나머지 에이전트에 재분배됩니다. 그러나 에이전트가 손상되거나 Red Hat Virtualization/oVirt 관리 포털에서 수동으로 삭제된 경우에는 재분배가 수행되지 않습니다. Cyber Protect 콘솔에서 해당 에이전트를 제거한 후에만 재분배가 시작됩니다.

특정 머신을 관리하는 에이전트를 확인하려면

1. Cyber Protect 콘솔에서 **장치**를 클릭하고 **oVirt**를 선택합니다.
2. 표 오른쪽 위의 기어 아이콘을 클릭하고 **시스템** 아래에서 **에이전트** 확인란을 선택합니다.
3. 표시되는 열에서 에이전트의 이름을 확인합니다.

제한 사항

다음 작업은 Red Hat Virtualization/oVirt 가상 머신에서 지원되지 않습니다.

- Aware 인식→인지
- 백업에서 가상 머신 실행
- 가상 머신 복제
- 변경된 블록 추적

OVA 템플릿 디플로이

1. Cyber Protection 계정에 로그인합니다.
2. **장치** > **모든 장치** > **추가** > **Red Hat Virtualization(oVirt)**을 클릭합니다.
   .Zip 아카이브가 귀하의 머신에 다운로드됩니다.
3. .zip 아카이브의 압축을 풉니다. .ova 파일 하나가 포함되어 있습니다.
4. 보호할 Red Hat Virtualization/oVirt 데이터 센터의 호스트에 .ova 파일을 업로드합니다.
5. Red Hat Virtualization/oVirt 관리 포털에 관리자로 로그인합니다. 가상 머신을 사용하는 작업에 필요한 역할에 대한 자세한 내용은 "Agent for oVirt – 필요한 역할과 포트"(147페이지)을(를) 참조하십시오.
6. 탐색 메뉴에서 **컴퓨팅** > **가상 머신**을 선택합니다.
7. 기본 테이블 위에서 세로 말줄임표 아이콘 을 클릭하고 **가져오기**를 클릭합니다.
8. **가상 머신 가져오기** 창에서 다음을 수행합니다.
   a. **데이터 센터**에서 보호할 데이터 센터를 선택합니다.
   b. **소스**에서 **가상 어플라이언스(OVA)**를 선택합니다.
   c. **호스트**에서 .ova 파일을 업로드한 호스트를 선택합니다.
   d. **파일 경로**에서 .ova 파일이 포함된 디렉토리의 경로를 지정합니다.
   e. **로드**를 클릭합니다.
      .ova 파일의 oVirt 가상 어플라이언스 템플릿이 **소스의 가상 머신** 패널에 표시됩니다.

© Acronis International GmbH, 2003-2024

이 패널에 템플릿이 표시되지 않으면 파일의 올바른 경로를 지정했고 파일이 손상되지 않았으며 호스트에 연결할 수 있는지 확인하십시오.

f. **소스의 가상 머신**에서 oVirt 가상 어플라이언스 템플릿을 선택하고 오른쪽 화살표를 클릭합니다.

가져올 가상 머신 패널에 템플릿이 나타납니다.

g. **다음**을 클릭합니다.

9. 새 창에서 어플라이언스 이름을 클릭하고 다음 설정을 구성합니다.
   - **네트워크 인터페이스** 탭에서 네트워크 인터페이스를 구성합니다.
   - [선택 사항] **일반** 탭에서 에이전트를 포함한 가상 머신의 기본 이름을 변경합니다.

디플로이가 완료되었습니다. 다음으로는 가상 어플라이언스을 구성해야 합니다. 가상 어플라이언스를 구성하는 방법에 대한 자세한 내용은 "가상 어플라이언스 구성"(144페이지)을(를) 참조하십시오.

참고

데이터 센터에 가상 어플라이언스가 여러 개 필요한 경우 위 단계를 반복하여 가상 어플라이언스를 추가로 디플로이하십시오. Red Hat Virtualization/oVirt 관리 포털에서 **VM 복제** 옵션을 사용하여 기존 가상 어플라이언스를 복제하지 마십시오.

동적 그룹 백업에서 가상 어플라이언스를 제외하려면 Cyber Protect 콘솔의 가상 머신 목록에서도 해당 어플라이언스를 제외해야 합니다. 가상 어플라이언스를 제외하려면 Red Hat Virtualization/oVirt 관리 포털에서 에이전트가 포함된 가상 머신을 선택하고 `acronis_virtual_appliance` 태그를 해당 가상 머신에 할당합니다.

가상 어플라이언스 구성

가상 어플라이언스를 디플로이한 뒤 어플라이언스가 oVirt 엔진 및 Cyber Protection 서비스에 모두 연결할 수 있도록 어플라이언스를 구성해야 합니다.

가상 어플라이언스을 구성하려면

1. Red Hat Virtualization/oVirt 관리 포털에 로그인합니다.
2. 구성할 가상 어플라이언스를 선택하고 **콘솔** 아이콘을 클릭합니다.
3. **eth0** 필드에서 어플라이언스의 네트워크 인터페이스를 구성합니다.

   자동으로 할당된 DHCP 주소(있는 경우)가 가상 머신이 사용하는 네트워크 내에서 유효한지 확인하거나 수동으로 할당하십시오. 어플라이언스가 사용하는 네트워크의 수에 따라 한 개 이상의 인터페이스를 구성해야 할 수 있습니다.
4. **oVirt** 필드에서 **변경**을 클릭하여 oVirt 엔진 주소 및 해당 주소에 액세스하는 데 필요한 자격 증명을 지정합니다.

   a. **서버 이름/IP** 필드에 엔진의 DNS이름 또는 IP주소를 입력합니다.

   b. **사용자 이름** 및 **비밀번호** 필드에는 이 엔진용 관리자 자격 증명을 입력합니다.

   이 관리자 계정에 Red Hat Virtualization/oVirt 가상 머신을 사용한 작업에 필요한 역할이 할당되어 있는지 확인합니다. 이러한 역할에 대한 자세한 내용은 "Agent for oVirt – 필요한 역할과 포트"(147페이지)을(를) 참조하십시오.

© Acronis International GmbH, 2003-2024

Keycloak이 oVirt 엔진(oVirt 4.5.1의 기본값)을 위한 SSO(Single-Sign-On) 제공자인 경우, 사용자 이름 지정 시 Keycloak 형식을 사용하십시오. 예를 들어, 기본 관리자 계정을 `admin@internal`이 아닌 `admin@ovirt@internalsso`로 지정해야 합니다.

c. [선택 사항] **연결 확인**을 클릭하여 입력한 자격 증명이 올바른지 확인합니다.

d. **확인**을 클릭합니다.

5. 다음 방법 중 하나를 사용하여 어플라이언스를 Cyber Protection 서비스에 등록합니다.

- [2단계 인증 미사용 테넌트에만 해당] 그래픽 인터페이스에서 어플라이언스를 등록합니다.

  a. **에이전트 옵션**의 **관리 서버**에서 **변경**을 클릭합니다.

  b. **서버 이름/IP** 필드에서 **클라우드**를 선택합니다.

  Cyber Protection 서비스 주소가 표시됩니다. 별도의 지시가 없는 한, 이 주소는 변경하지 마십시오.

  c. **사용자 이름** 및 **암호** 필드에서 Cyber Protection 서비스의 계정 자격 증명을 지정합니다. 가상 어플라이언스 및 해당 어플라이언스가 관리하는 가상 머신이 이 계정에 등록됩니다.

  d. **확인**을 클릭합니다.

- 명령줄 인터페이스에서 어플라이언스를 등록합니다.

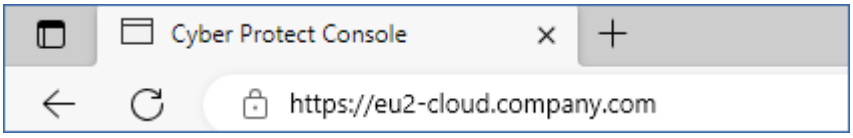
  참고
  이 방법을 사용할 때는 등록 토큰이 필요합니다. 토큰 생성 방법에 대한 자세한 내용은 "등록 토큰 생성"(156페이지) 항목을 참조하십시오.

  a. Ctrl+Shift+F2를 눌러 명령줄 인터페이스를 엽니다.

  b. 다음 명령을 실행합니다.

  ```
  register_agent -o register -t cloud -a <service address> --token <registration token>
  ```

  참고
  등록 토큰을 사용할 때는 정확한 데이터 센터 주소를 지정해야 합니다. 이 주소는 Cyber Protect 콘솔에 **로그인하고 나면** 표시되는 URL입니다. 예: `https://eu2-cloud.company.com`.

  여기서 `https://cloud.company.com`을 사용하지 마십시오.

  c. 어플라이언스의 그래픽 인터페이스로 돌아가려면 Alt+F1을 누릅니다.

6. [선택 사항] **이름** 필드에서 **변경**을 클릭하여 가상 어플라이언스의 기본 이름인 **localhost**를 편집합니다. 이 이름은 Cyber Protect 콘솔에 표시됩니다.
7. [선택 사항] **시간** 필드에서 **변경**을 클릭하고 예정된 작업이 적절한 시간에 실행될 수 있도록 사용자 지역의 시간대를 선택합니다.
8. [선택 사항] [프록시 서버가 네트워크에서 활성화되어 있는 경우] 프록시 서버를 구성합니다.

© Acronis International GmbH, 2003-2024

a. Ctrl+Shift+F2를 눌러 명령줄 인터페이스를 엽니다.
b. 텍스트 편집기에서 **/etc/Acronis/Global.config** 파일을 엽니다.
c. 다음 중 하나를 수행하십시오.
   - 에이전트 설치 중에 프록시 설정을 지정한 경우 다음 섹션을 참조하십시오.

     ```
     <key name="HttpProxy">
         <value name="Enabled" type="Tdword">"1"</value>
         <value name="Host" type="TString">"ADDRESS"</value>
         <value name="Port" type="Tdword">"PORT"</value>
         <value name="Login" type="TString">"LOGIN"</value>
         <value name="Password" type="TString">"PASSWORD"</value>
     </key>
     ```

   - 그렇지 않으면 위의 행을 복사하고 파일에서 `<registry name="Global">...</registry>` 태그 사이에 붙여넣습니다.
d. ADDRESS를 프록시 서버 호스트 이름/IP 주소로 대체하고 PORT는 포트 번호의 10진수 값으로 대체합니다.
e. 프록시 서버에 인증이 필요하다면 LOGIN 및 PASSWORD를 프록시 서버 자격 증명으로 대체합니다. 그렇지 않은 경우, 파일에서 이 라인을 삭제합니다.
f. 파일을 저장합니다.
g. 텍스트 편집기에서 **/opt/acronis/etc/aakore.yaml** 파일을 엽니다.
h. **env** 섹션을 찾거나 생성한 후, 다음 행을 추가합니다.

   ```
   env:
       http-proxy: proxy_login:proxy_password@proxy_address:port
       https-proxy: proxy_login:proxy_password@proxy_address:port
   ```

i. proxy_login과 proxy_password는 프록시 서버 자격 증명으로, proxy_address:port는 프록시 서버의 주소와 포트 번호로 대체합니다.
j. reboot 명령을 실행합니다.

참고
프록시를 통해 디플로이된 가상 어플라이언스를 업데이트하려면 어플라이언스의 config.yaml 파일(/opt/acronis/etc/va-updater/config.yaml)을 편집합니다. 즉, 해당 파일 맨 아래에 다음 줄을 추가한 후 환경에 적합한 값을 입력합니다.

```
httpProxy: http://<proxy_login>:<proxy_password>@<proxy_address>:<port>
```

예:

```
httpProxy: http://mylogin:mypassword@192.168.2.300:8080
```

Red Hat Virtualization/oVirt 데이터 센터의 가상 머신을 보호하려면

1. Cyber Protection 계정에 로그인합니다.
2. **장치** > **oVirt** > <사용자 클러스터>로 이동하거나 **장치** > **모든 장치**에서 머신을 확인할 수 있습

© Acronis International GmbH, 2003-2024

니다.

3. 머신을 선택하고 보호 계획을 적용합니다.

Agent for oVirt – 필요한 역할과 포트

필요한 역할

Agent for oVirt 디플로이 및 작동 시에는 다음 역할이 할당된 관리자 계정이 필요합니다.

oVirt/Red Hat Virtualization 4.2 및 4.3/Oracle Virtualization Manager 4.3

- DiskCreator
- UserVmManager
- TagManager
- UserVmRunTimeManager
- VmCreator

oVirt/Red Hat Virtualization 4.4, 4.5

- SuperUser

필요한 포트

Agent for oVirt는 가상 어플라이언스를 구성할 때 지정하는 URL을 사용하여 oVirt 엔진에 연결합니다. 일반적으로 엔진 URL의 형식은 `https://ovirt.company.com`입니다. 이 경우에는 HTTPS 프로토콜과 포트 443이 사용됩니다.

기본값이 아닌 oVirt 설정을 사용하는 경우에는 다른 포트가 필요할 수 있습니다. URL 형식을 분석하면 정확한 포트를 확인할 수 있습니다. 예:

oVirt 엔진 URL	포트	프로토콜
`https://ovirt.company.com/`	443	HTTPS
`http://ovirt.company.com/`	80	HTTP
`https://ovirt.company.com:1234/`	1234	HTTPS

백업이 HotAdd 모드에서 수행되므로 디스크 읽기/쓰기 작업에는 추가 포트가 필요하지 않습니다.

Agent for Synology 디플로이

시작하기 전에

Agent for Synology를 사용하면 Synology NAS 장치에서/장치에 파일과 폴더를 백업할 수 있습니다. 이 경우 공유, 폴더, 파일에 적용되어 있는 NAS 관련 속성과 액세스 권한이 보존됩니다.

© Acronis International GmbH, 2003-2024

Agent for Synology는 NAS 장치에서 실행됩니다. 그러므로 백업 복제, 유효성 검사, 정리와 같은 오프 호스트 데이터 처리 작업에 장치의 리소스를 사용할 수 있습니다. 이러한 작업에 대해 자세히 알아보려면 "오프호스트 데이터 처리"(185페이지) 항목을 참조하십시오.

참고
Agent for Synology는 x86_64 프로세서가 장착된 NAS 장치만 지원합니다. ARM 프로세서는 지원되지 않습니다.

NAS 장치의 원래 위치나 새 위치, 그리고 해당 장치를 통해 액세스할 수 있는 네트워크 폴더에 백업을 복구할 수 있습니다. 클라우드 스토리지의 백업을 Agent for Synology가 설치되어 있는 원래 장치와는 다른 NAS 장치에 복구할 수도 있습니다.

아래 표에는 사용 가능한 백업 소스와 대상이 요약되어 있습니다.

백업 대상	백업할 항목 (백업 소스)	백업 위치 (백업 목적지)
파일/폴더	로컬 폴더*	클라우드 스토리지
		로컬 폴더*
	네트워크 폴더(SMB)**	네트워크 폴더(SMB)**
		NFS 폴더

* NAS 장치에 연결되어 있는 USB 드라이브가 포함됩니다.

참고
암호화된 폴더는 지원되지 않습니다. 이러한 폴더는 Cyber Protection 그래픽 사용자 인터페이스에서 표시되지 않습니다.

** SMB 프로토콜을 통해 백업 소스나 백업 목적지로 외부 네트워크 공유를 사용하는 방식은 Synology DiskStation Manager 6.2.3 이상에서 실행 중인 에이전트에서만 사용 가능합니다.Synology NAS 자체에서 호스트되는 데이터(호스팅된 네트워크 공유 포함)는 제한 없이 백업할 수 있습니다.

제한 사항

- Agent for Synology는 x86_64 프로세서가 장착된 NAS 장치만 지원합니다. ARM 프로세서는 지원되지 않습니다.
- 백업된 암호화 공유는 암호화되지 않은 공유로 복구됩니다.
- **파일 압축** 옵션이 활성화되어 있는 백업된 공유는 이 옵션이 비활성화된 상태로 복구됩니다.
- Agent for Synology가 생성한 백업만 Synology NAS 장치로 복구할 수 있습니다.

설정 프로그램을 다운로드합니다.

Agent for Synology의 설치 프로그램은 SPK 파일로 제공됩니다.

© Acronis International GmbH, 2003-2024

Agent for Synology 7.x

설정 프로그램을 다운로드하려면

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 오른쪽 위에서 **추가**를 클릭합니다.
3. **NAS(네트워크 연결된 스토리지)** 아래에서 **Synology**를 클릭합니다.
   머신에 설정 프로그램이 다운로드됩니다.

Agent for Synology 6.x

설정 프로그램을 다운로드하려면

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 오른쪽 위에서 **추가**를 클릭합니다.
3. **NAS(네트워크 연결된 스토리지)** 아래에서 **Synology**를 클릭합니다.
   머신에 Agent for Synology 7.x 설치 프로그램이 다운로드됩니다.
   다운로드 프로세스를 중지하거나 다운로드된 파일을 무시해도 됩니다.
4. **Agent for Synology 6.x 다운로드**를 클릭합니다.
   머신에 Agent for Synology 6.x 설치 프로그램이 다운로드됩니다.

Agent for Synology 설치

Agent for Synology를 설치하려면 Synology DiskStation Manager에서 SPK 파일을 실행합니다.

참고
Agent for Synology는 x86_64 프로세서가 장착된 NAS 장치만 지원합니다. ARM 프로세서는 지원되지 않습니다.

Agent for Synology 7.x

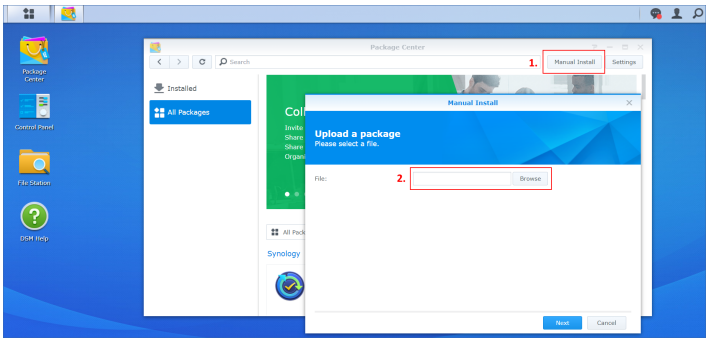
사전 요구 사항

- NAS 장치에서 DiskStation Manager 7.x를 실행합니다.
- NAS 장치의 **administrators** 그룹 멤버입니다.
- 에이전트를 설치하려는 NAS 볼륨의 여유 공간이 200MB 이상입니다.
- 머신에서 SSH 클라이언트를 사용할 수 있어야 합니다. 이 문서에서는 Putty를 예로 사용합니다.

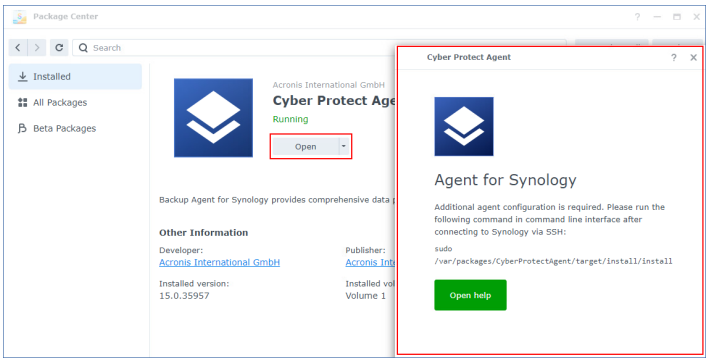
Agent for Synology를 설치하려면

1. Synology DiskStation Manager에 로그인합니다.
2. **Package Center**를 엽니다.
3. **수동 설치**를 클릭한 다음 **찾아보기**를 클릭합니다.

© Acronis International GmbH, 2003-2024



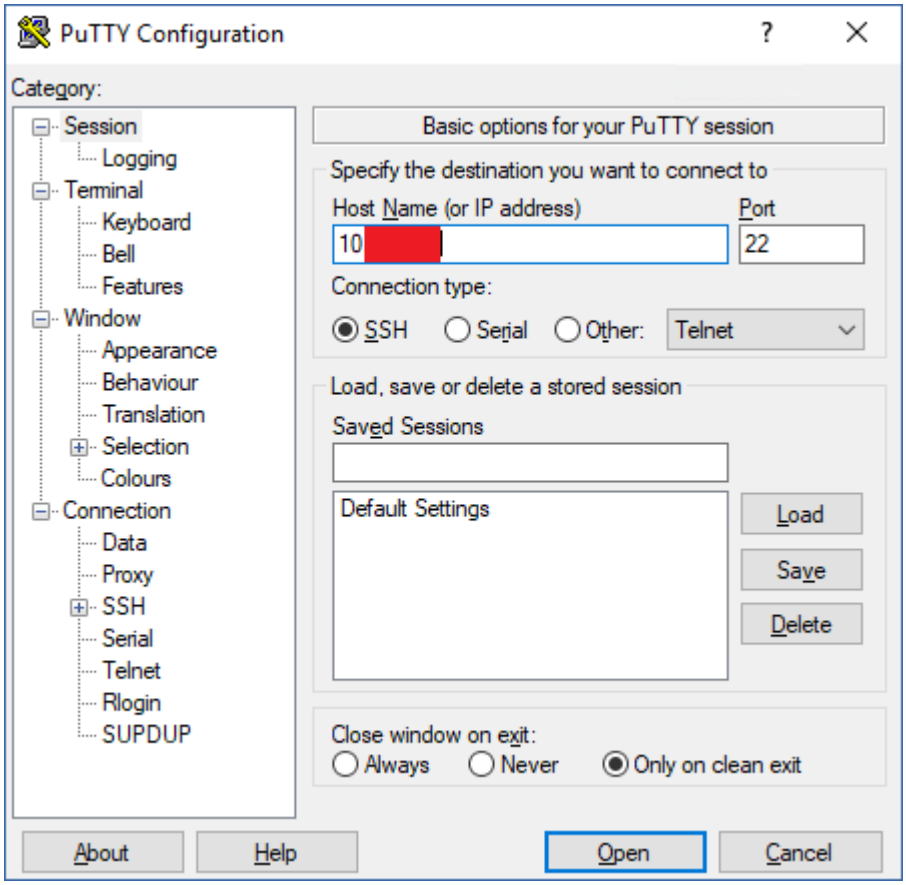
4. Cyber Protect 콘솔에서 다운로드한 SPK 파일을 선택하고 **다음**을 클릭합니다.
   서드 파티 소프트웨어 패키지가 설치된다는 경고가 표시됩니다. 이 메시지는 표준 설치 절차의 일환으로 표시되는 메시지입니다.
5. 패키지 설치를 확인하려면 **동의**를 클릭합니다.
6. 에이전트를 설치할 볼륨을 선택하고 **다음**을 클릭합니다.
7. 설정을 확인하고 **완료**를 클릭합니다.
8. Synology DiskStation Manager **Package Center**에서 Cyber Protect Agent for Synology를 열고 다음 화면이 표시되는지 확인합니다.



9. Synology DiskStation Manager **제어판**에서 **터미널 및 SNMP**로 이동한 후 NAS 장치에 대한 SSH 액세스를 활성화합니다.
10. SSH 클라이언트(이 예에서는 Putty)를 사용하여 NAS 장치에서 `install` 스크립트를 실행합니다. 이 스크립트는 DSM 7.0 이상에 대한 루트 액세스 권한(에이전트를 구성하려면 필요한 권한)을 활성화합니다.

© Acronis International GmbH, 2003-2024

a. Putty를 시작하고 Synology NAS 장치의 IP 주소 또는 호스트 이름을 지정합니다.



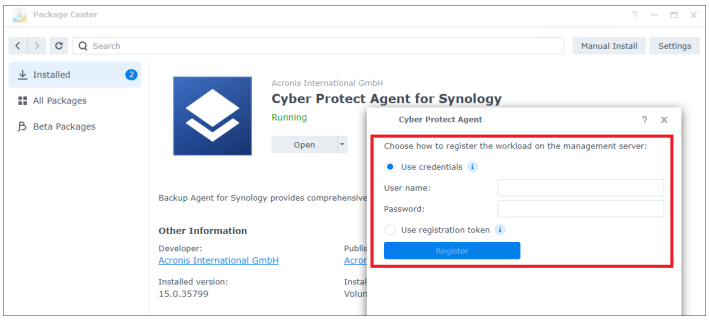
b. **열기**를 클릭하고 Synology DSM 관리자로 로그인합니다.

c. 다음 명령을 실행합니다.

```
sudo /var/packages/CyberProtectAgent/target/install/install
```

스크립트가 시작된 후 Cyber Protection 서비스가 초기화될 때까지 15초 동안 기다립니다.

11. Synology DiskStation Manager **제어판**에서 **터미널 및 SNMP**로 이동한 후 NAS 장치에 대한 SSH 액세스를 비활성화합니다. SSH 액세스는 더 이상 필요하지 않습니다.
12. Synology DiskStation Manager **Package Center**에서 Cyber Protect Agent for Synology를 엽니다.
13. 등록 방법을 선택합니다.



- [자격 증명을 사용하여 에이전트를 등록하는 방법]
  - **사용자 이름** 및 **암호** 필드에서 에이전트가 등록될 계정의 자격 증명을 지정합니다. 이 계정은 파트너 관리자 계정이 될 수 없습니다.

© Acronis International GmbH, 2003-2024

- [등록 토큰을 사용하여 에이전트를 등록하는 방법]
  - **등록 주소**에서 정확한 데이터 센터 주소를 지정합니다. 정확한 데이터 센터 주소는 Cyber Protect 콘솔에 로그인 한 후에 보이는 URL입니다. 예: `https://us5-cloud.acronis.com`.

    참고
    데이터 센터 주소가 없는 URL 형식은 사용하면 안 됩니다. 예를 들어 `https://cloud.acronis.com`은 사용할 수 없습니다.

  - **토큰** 필드에서 등록 토큰을 지정합니다.
    등록 토큰을 생성하는 방법에 대한 자세한 내용은 "등록 토큰 생성"(156페이지) 항목을 참조하십시오.

14. **등록**을 클릭합니다.

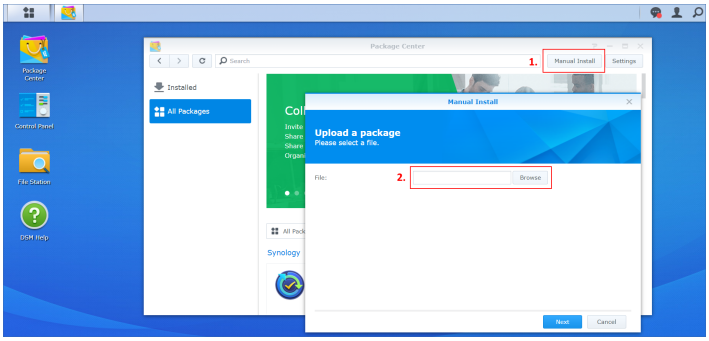
Agent for Synology 6.x

사전 요구 사항

- NAS 장치에서 DiskStation Manager 6.2.x를 실행합니다.
- NAS 장치의 **administrators** 그룹 멤버입니다.
- 에이전트를 설치하려는 NAS 볼륨의 여유 공간이 200MB 이상입니다.

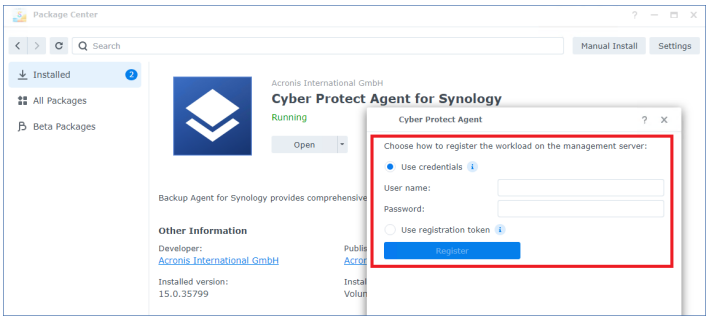
Agent for Synology를 설치하려면

1. Synology DiskStation Manager에 로그인합니다.
2. **Package Center**를 엽니다.
3. **수동 설치**를 클릭한 다음 **찾아보기**를 클릭합니다.



4. Cyber Protect 콘솔에서 다운로드한 SPK 파일을 선택하고 **다음**을 클릭합니다.
   디지털 서명이 없는 패키지가 설치된다는 경고가 표시됩니다. 이 메시지는 표준 설치 절차의 일환으로 표시되는 메시지입니다.
5. 패키지 설치를 확인하려면 **예**를 클릭합니다.
6. 에이전트를 설치할 볼륨을 선택하고 **다음**을 클릭합니다.
7. 설정을 확인하고 **적용**을 클릭합니다.
8. Synology DiskStation Manager **Package Center**에서 Cyber Protect Agent for Synology를 엽니다.
9. 등록 방법을 선택합니다.

© Acronis International GmbH, 2003-2024



- [자격 증명을 사용하여 에이전트를 등록하는 방법]
  - **사용자 이름** 및 **암호** 필드에서 에이전트가 등록될 계정의 자격 증명을 지정합니다. 이 계정은 파트너 관리자 계정이 될 수 없습니다.
- [등록 토큰을 사용하여 에이전트를 등록하는 방법]
  - **등록 주소**에서 정확한 데이터 센터 주소를 지정합니다. 정확한 데이터 센터 주소는 Cyber Protect 콘솔에 로그인 한 후에 보이는 URL입니다. 예: `https://us5-cloud.acronis.com`.

    참고
    데이터 센터 주소가 없는 URL 형식은 사용하면 안 됩니다. 예를 들어 `https://cloud.acronis.com`은 사용할 수 없습니다.

  - **토큰** 필드에서 등록 토큰을 지정합니다.
    등록 토큰을 생성하는 방법에 대한 자세한 내용은 "등록 토큰 생성"(156페이지) 항목을 참조하십시오.

10. **등록**을 클릭합니다.

등록이 완료되면 Cyber Protect 콘솔의 **장치** > **NAS(네트워크 연결 스토리지)** 탭에 Synology NAS 장치가 표시됩니다.

NAS 장치에서 데이터를 백업하려면 보호 계획을 적용합니다.

Agent for Synology 업데이트

Agent for Synology 6.x를 최신 버전의 Agent for Synology 6.x로 업데이트할 수 있습니다. 마찬가지로 Agent for Synology 7.x를 최신 버전의 Agent for Synology 7.x로 업데이트할 수 있습니다.

에이전트를 업데이트하려면 Synology DiskStation Manager에서 최신 버전의 설치 프로그램을 실행합니다. 에이전트의 원래 등록과 해당 설정, 그리고 보호된 워크로드에 적용되어 있는 계획은 보존됩니다.

참고
Cyber Protect 콘솔에서 에이전트를 업데이트할 수는 없습니다.

Agent for Synology 6.x를 Agent for Synology 7.x로 업그레이드하는 방법은 이전 버전 에이전트를 설치 제거한 후에 최신 버전 에이전트를 설치하는 것뿐입니다. 이 경우에는 모든 보호 계획이 해지되므로 보호 계획을 수동으로 다시 적용해야 합니다.

Agent for Synology 7.x

© Acronis International GmbH, 2003-2024

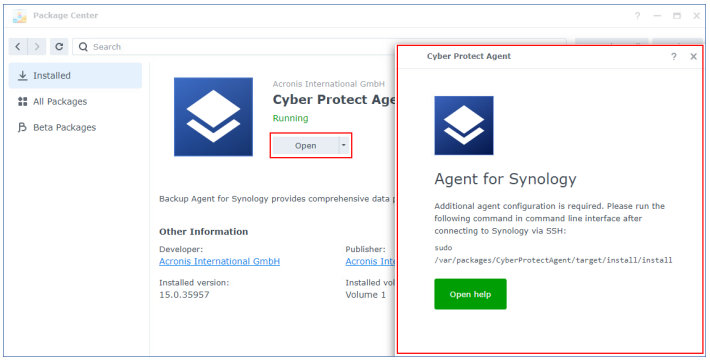
사전 요구 사항

- NAS 장치의 **administrators** 그룹 멤버입니다.
- 에이전트를 설치하려는 NAS 볼륨의 여유 공간이 200MB 이상입니다.
- 머신에서 SSH 클라이언트를 사용할 수 있어야 합니다. 이 문서에서는 Putty를 예로 사용합니다.

***Agent for Synology*를 업데이트하려면**

1. DiskStation Manager에서 **Package Center**를 엽니다.
2. **수동 설치**를 클릭한 다음 **찾아보기**를 클릭합니다.
3. Cyber Protect 콘솔에서 다운로드한 Agent for Synology 7.x용 최신 SPK 파일을 선택하고 **다음**을 클릭합니다.

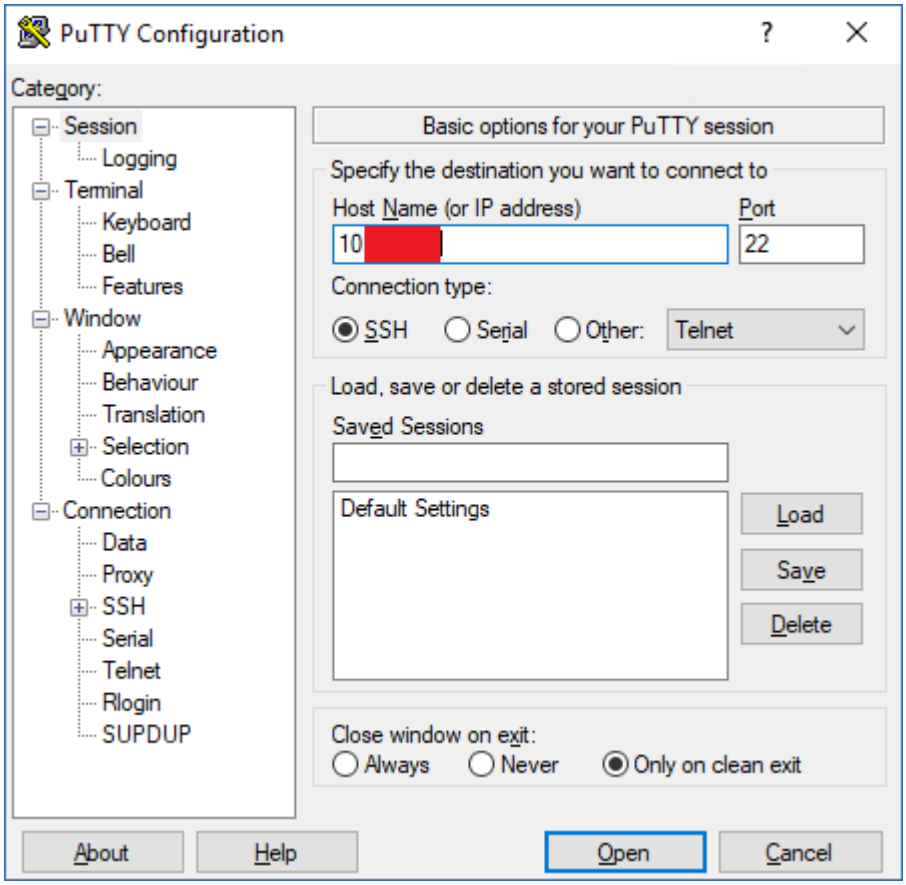
   서드 파티 소프트웨어 패키지가 설치된다는 경고가 표시됩니다. 이 메시지는 표준 설치 절차의 일환으로 표시되는 메시지입니다.
4. 패키지 설치를 확인하려면 **동의**를 클릭합니다.
5. 설정을 확인하고 **완료**를 클릭합니다.
6. Synology DiskStation Manager **Package Center**에서 Cyber Protect Agent for Synology를 열고 다음 화면이 표시되는지 확인합니다.



7. Synology DiskStation Manager **제어판**에서 **터미널 및 SNMP**로 이동한 후 NAS 장치에 대한 SSH 액세스를 활성화합니다.
8. SSH 클라이언트(이 예에서는 Putty)를 사용하여 NAS 장치에서 `install` 스크립트를 실행합니다. 이 스크립트는 DSM 7.0 이상에 대한 루트 액세스 권한(에이전트를 구성하려면 필요한 권한)을 활성화합니다.

© Acronis International GmbH, 2003-2024

a. Putty를 시작하고 Synology NAS 장치의 IP 주소 또는 호스트 이름을 지정합니다.



b. **열기**를 클릭하고 Synology DSM 관리자로 로그인합니다.

c. 다음 명령을 실행합니다.

```
sudo /var/packages/CyberProtectAgent/target/install/install
```

9. Synology DiskStation Manager **제어판**에서 **터미널 및 SNMP**로 이동한 후 NAS 장치에 대한 SSH 액세스를 비활성화합니다. SSH 액세스는 더 이상 필요하지 않습니다.

Agent for Synology 6.x

사전 요구 사항

- NAS 장치의 **administrators** 그룹 멤버입니다.
- 에이전트를 설치하려는 NAS 볼륨의 여유 공간이 200MB 이상입니다.

Agent for Synology를 업데이트하려면

1. DiskStation Manager에서 **Package Center**를 엽니다.
2. **수동 설치**를 클릭한 다음 **찾아보기**를 클릭합니다.
3. Cyber Protect 콘솔에서 다운로드한 Agent for Synology 6.x용 최신 SPK 파일을 선택하고 **다음**을 클릭합니다.

   디지털 서명이 없는 패키지가 설치된다는 경고가 표시됩니다. 이 메시지는 표준 설치 절차의 일환으로 표시되는 메시지입니다.

© Acronis International GmbH, 2003-2024

4. 패키지 설치를 확인하려면 **예**를 클릭합니다.
5. 설정을 확인하고 **적용**을 클릭합니다.

그룹 정책을 통해 에이전트 배포

Windows 그룹 정책을 사용하여 Active Directory 도메인의 멤버인 머신에 Agent for Windows를 중앙에서 설치(또는 디플로이)할 수 있습니다.

이 섹션에서는 전체 도메인 또는 도메인의 조직 단위에서 머신에 에이전트를 배포하도록 그룹 정책 개체를 설정하는 방법에 대해 알아봅니다.

머신이 도메인에 로그온할 때마다 결과적인 그룹 정책 개체는 에이전트가 설치 및 등록되어 있는지 확인합니다.

사전 요구 사항

- Active Directory 도메인에 Microsoft Windows Server 2003 이상에서 실행 중인 도메인 컨트롤러가 포함되어 있어야 합니다.
- 이 도메인 내 **도메인 관리자** 그룹의 멤버여야 합니다.
- **Windows용 모든 에이전트** 설치 프로그램을 다운로드했습니다.
  설치 프로그램을 다운로드하려면 Cyber Protect 콘솔의 오른쪽 상단에 있는 계정 아이콘을 클릭하고 **다운로드**를 클릭합니다. **장치 추가** 창에서도 다운로드 링크를 사용할 수 있습니다.

그룹 정책을 통해 에이전트를 디플로이하려면

1. "등록 토큰 생성"(156페이지)의 설명대로 등록 토큰을 생성합니다.
2. "변환 파일 생성 및 설치 패키지 추출"(159페이지)의 설명대로 .mst 파일, .msi 파일 및 .cab 파일을 생성합니다.
3. "그룹 정책 객체 설정"(159페이지)의 설명대로 그룹 정책 객체를 설정합니다.

등록 토큰 생성

등록 토큰은 Cyber Protect 콘솔에 사용자 자격 증명을 저장하지 않고 에이전트 설치 프로그램에 사용자 ID를 전달합니다. 따라서 사용자는 로그인하지 않고도 계정에 머신을 원하는 수만큼 등록하거나 워크로드에 보호 계획을 적용할 수 있습니다.

참고
보호 계획은 머신 등록 중에 자동 적용되지 않으며 별도의 작업을 수행하여 적용해야 합니다.

토큰은 보안상 일정 기간 동안만 사용할 수 있습니다. 토큰을 사용할 수 있는 기간은 조정 가능합니다. 토큰의 기본 수명은 3일입니다.

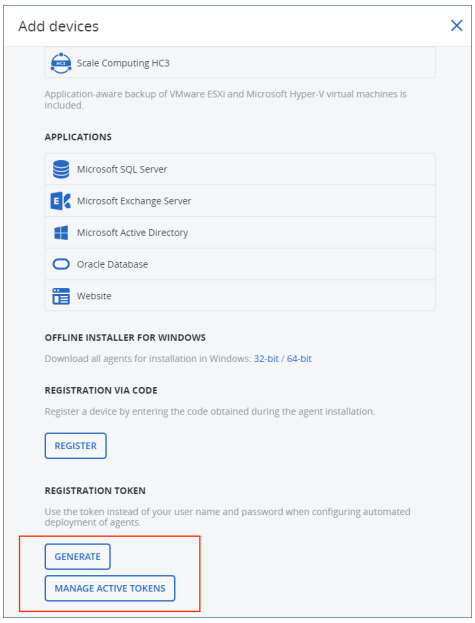
사용자는 본인 계정용으로만 등록 토큰을 생성할 수 있습니다. 관리자는 관리 대상 테넌트의 모든 사용자 계정용으로 등록 토큰을 생성할 수 있습니다.

등록 토큰을 생성하려면

사용자

© Acronis International GmbH, 2003-2024

1. Cyber Protect 콘솔에 로그인합니다.
2. **장치** > **모든 장치** > **추가**를 클릭합니다.
   장치 추가 창이 오른쪽에 열립니다.
3. **등록 토큰**으로 스크롤을 내린 다음 **생성**을 클릭합니다.



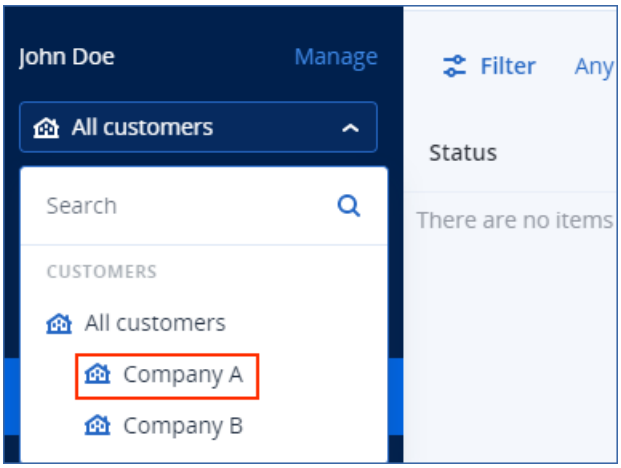
4. 토큰 수명을 지정합니다.
5. **토큰 생성**을 클릭합니다.
6. **복사**를 클릭하여 장치 클립보드에 토큰을 복사하거나 토큰을 수동으로 작성합니다.

관리자

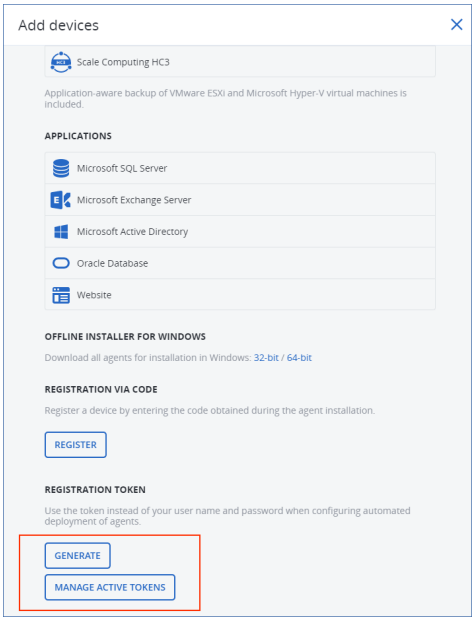
1. Cyber Protect 콘솔에 관리자로 로그인합니다.
   관리 포털에 이미 로그인한 경우 **모니터링** > **사용**으로 이동한 후 **보호** 탭에서 **서비스 관리**를 클릭하여 Cyber Protect 콘솔로 이동할 수 있습니다.

   [고객 테넌트를 관리하는 파트너 관리자의 경우] Cyber Protect 콘솔에서 토큰을 생성할 사용자가 속해 있는 테넌트를 선택합니다. **모든 고객** 수준에서는 토큰을 생성할 수 없습니다.

© Acronis International GmbH, 2003-2024



2. **장치**에서 **모든 장치** > **추가**를 클릭합니다.
   장치 추가 창이 오른쪽에 열립니다.
3. **등록 토큰**으로 스크롤을 내린 다음 **생성**을 클릭합니다.



4. 토큰 수명을 지정합니다.
5. 토큰을 생성할 사용자를 선택합니다.

> **참고**
> 토큰 사용 시에는 여기서 선택하는 사용자 계정에 워크로드가 등록됩니다.

6. [선택 사항] 토큰 사용자가 추가된 워크로드에서 보호 계획을 적용 및 해지할 수 있도록 하려면 드롭다운 목록에서 계획을 선택합니다.
   이렇게 하려면 추가된 워크로드에서 보호 계획을 적용하거나 해지할 스크립트를 실행해야 합니다. 이 기술 자료 문서에서 자세한 정보를 확인하십시오.
7. **토큰 생성**을 클릭합니다.
8. **복사**를 클릭하여 장치 클립보드에 토큰을 복사하거나 토큰을 수동으로 작성합니다.

등록 토큰을 확인하거나 삭제하려면

© Acronis International GmbH, 2003-2024

1. Cyber Protect 콘솔에 로그인합니다.
2. **장치** > **모든 장치** > **추가**를 클릭합니다.
3. 아래쪽의 **등록 토큰**으로 스크롤한 다음 **활성 토큰 관리**를 클릭합니다.
   테넌트용으로 생성된 활성 토큰 목록이 오른쪽에 열립니다.

   참고
   보안상 **토큰** 열에는 토큰 값의 첫 2자만 표시됩니다.

4. [토큰을 삭제하려면] 토큰을 선택하고 **삭제**를 클릭합니다.

변환 파일 생성 및 설치 패키지 추출

Windows 그룹 정책을 통해 보호 에이전트를 디플로이하려면 변환 파일(.mst)과 설치 패키지(.msi 및 .cab 파일)가 필요합니다.

참고
아래 절차에서는 기본 등록 옵션인 토큰을 통한 등록을 사용합니다. 등록 토큰을 생성하는 방법을 알아보려면 "등록 토큰 생성"(156페이지) 항목을 참조하십시오.

.msi 파일을 생성하고 설치 패키지(.msi 및 .cab 파일)를 추출하려면

1. Active Directory 도메인에 속해 있는 임의의 머신에서 관리자로 로그인합니다.
2. 설치 패키지를 저장할 공유 폴더를 생성합니다. 도메인 사용자가 공유 폴더에 액세스할 수 있는지 확인합니다. 예를 들어, 기본 공유 설정을 **모든 사람**으로 남겨둘 수 있습니다.
3. 에이전트 설치 프로그램을 실행합니다.
4. **무인 설치를 위해 .mst 및 .msi 파일 생성**을 클릭합니다.
5. **설치 대상**에서 설치에 포함할 컴포넌트를 선택하고 **완료**를 클릭합니다.
6. **등록 설정**에서 **지정**을 클릭하고 등록 토큰을 입력한 후 **완료**를 클릭합니다.
   등록 방법을 **등록 토큰 사용**(기본값)에서 **자격 증명 사용** 또는 **등록 건너뛰기**로 변경할 수 있습니다. **등록 건너뛰기** 옵션을 선택하면 나중에 워크로드를 수동으로 등록할 것이라고 가정합니다.
7. .mst 파일에 추가될 설치 설정을 검토하거나 수정한 다음 **진행**을 클릭합니다.
8. **파일 저장 위치**에서 생성한 공유 폴더의 경로를 지정합니다.
9. **생성**을 클릭합니다.

그러면 .mst 파일, .msi 파일 및 .cab 파일이 생성되어 지정한 공유 폴더에 복사됩니다.

다음으로는 Windows 그룹 정책 객체를 설정합니다. 이 작업을 수행하는 방법을 알아보려면 "그룹 정책 객체 설정"(159페이지) 항목을 참조하십시오.

그룹 정책 객체 설정

이 절차에서는 "변환 파일 생성 및 설치 패키지 추출"(159페이지)에서 생성한 설치 패키지를 사용하여 GPO(그룹 정책 객체)를 설정합니다. 해당 GPO는 도메인의 머신에 에이전트를 디플로이합니다.

© Acronis International GmbH, 2003-2024

그룹 정책 객체를 설정하려면

1. 도메인 관리자로 도메인 컨트롤러에 로그인합니다.
   도메인에 도메인 컨트롤러가 여러 개 있으면 아무 도메인 컨트롤러에나 도메인 관리자로 로그인합니다.
2. [조직 단위에서 에이전트를 배포하는 경우] 에이전트를 디플로이할 조직 단위가 도메인에 있는지 확인합니다.
3. Windows **시작** 메뉴에서 **관리 도구**를 가리키고 **그룹 정책 관리**(Windows Server 2003의 경우 **Active Directory 사용자 및 컴퓨터**)를 클릭합니다.
4. [Windows Server 2008 이상 버전의 경우] 도메인 또는 조직 단위의 이름을 마우스 오른쪽 버튼으로 클릭한 다음 **이 도메인에서 GPO를 만들어 여기에 연결**을 클릭합니다.
5. [Windows Server 2003의 경우] 도메인 또는 조직 단위의 이름을 마우스 오른쪽 버튼으로 클릭한 다음 **등록 정보**를 클릭합니다. 대화 상자에서 **그룹 정책** 탭을 클릭한 다음 **새로 만들기**를 클릭합니다.
6. 새 그룹 정책 개체의 이름을 **Agent for Windows**라고 지정합니다.
7. 편집을 위해 **Agent for Windows** 그룹 정책 객체를 엽니다.
   - [Windows Server 2008 이상 버전의 경우] **그룹 정책 개체**에서 그룹 정책 개체를 마우스 오른쪽 버튼으로 클릭하고 **편집**을 클릭합니다.
   - [Windows Server 2003의 경우] 그룹 정책 개체를 클릭한 다음 **편집**을 클릭합니다.
8. 그룹 정책 객체 편집기 스냅인에서 **컴퓨터 구성**을 확장합니다.
9. [Windows Server 2012 이상 버전의 경우] **정책** > **소프트웨어 설정**을 확장합니다.
10. [Windows Server 2003 및 Windows Server 2008의 경우] **소프트웨어 설정**을 확장합니다.
11. **소프트웨어 설치**를 마우스 오른쪽 버튼으로 클릭하고 **새로 만들기**를 가리킨 후 **패키지**를 클릭합니다.
12. 생성한 공유 폴더에서 에이전트의 .msi 설치 패키지를 선택한 다음 **열기**를 클릭합니다.
13. **소프트웨어 배포** 대화 상자에서 **고급**을 클릭한 다음 **확인**을 클릭합니다.
14. **수정** 탭에서 **추가**를 클릭한 다음 생성한 공유 폴더의 .mst 파일을 선택합니다.
15. **확인**을 클릭하여 **소프트웨어 배포** 대화 상자를 닫습니다.

가상 어플라이언스에 대한 SSH 연결

유지보수 작업을 위해 가상 어플라이언스에 원격 액세스하는 경우 SSH(Secure Socket Shell) 연결을 사용하십시오.

보안 셸 데몬 시작

가상 어플라이언스에 SSH 연결을 허용하려면 어플라이언스에서 보안 셸 데몬(sshd)을 시작합니다.

보안 셸 데몬을 시작하는 방법

© Acronis International GmbH, 2003-2024

1. 하이퍼바이저 소프트웨어에서 가상 어플라이언스의 콘솔을 엽니다.
2. 어플라이언스의 그래픽 사용자 인터페이스에서 CTRL+SHIFT+F2를 눌러 명령줄 인터페이스를 엽니다.
3. 다음 명령을 실행합니다.

   ```
   /bin/sshd
   ```

4. [어플라이언스에 처음 연결 시에만 해당] 루트 사용자의 암호를 설정합니다.
   암호를 설정하는 방법을 알아보려면 "가상 어플라이언스에서 루트 암호 설정"(161페이지)을(를) 참조하십시오.

참고
SSH 연결을 사용하지 않을 때는 보안 셸 데몬을 중지하는 것을 권장합니다.

가상 어플라이언스에서 루트 암호 설정

처음으로 가상 어플라이언스에 SSH 연결을 설정하기 전에 어플라이언스의 루트 암호를 설정해야 합니다.

루트 암호를 설정하는 방법

1. 하이퍼바이저 소프트웨어에서 가상 어플라이언스의 콘솔을 엽니다.
2. 어플라이언스의 그래픽 사용자 인터페이스에서 CTRL+SHIFT+F2를 눌러 명령줄 인터페이스를 엽니다.
3. 다음 명령을 실행합니다.

   ```
   passwd
   ```

4. 암호를 지정한 다음 Enter를 누릅니다.
   암호는 최소 9개의 문자를 포함해야 하며 복잡성 점수가 3점 이상이어야 합니다. 복잡성 점수는 자동으로 계산됩니다. 더 높은 점수를 얻으려면 특수 기호, 대문자 및 소문자 기호, 숫자의 조합을 사용하면 됩니다.
5. 암호를 확인한 다음 Enter를 누릅니다.

SSH 클라이언트를 통해 가상 어플라이언스 액세스

사전 요구 사항

- 원격 머신에는 SSH 클라이언트가 있어야 합니다. 아래 절차는 WinSCP 클라이언트를 예로 사용합니다. 단계를 적절히 조정하면 어떤 SSH 클라이언트든 사용할 수 있습니다.
- 가상 어플라이언스에서 보안 셸 데몬(sshd)을 시작해야 합니다. 자세한 정보는 "보안 셸 데몬 시작"(160페이지)을(를) 참조하십시오.

WinSCP를 통해 가상 어플라이언스에 액세스하는 방법

1. 원격 머신에서 WinSCP를 엽니다.
2. **세션** > **새 세션**을 클릭합니다.

© Acronis International GmbH, 2003-2024

3. **파일 프로토콜**에서 **SCP**를 선택합니다.
4. **호스트 이름**에서 가상 어플라이언스의 IP 주소를 지정합니다.
5. **사용자 이름**과 **암호**에서, 루트와 루트 사용자의 암호를 지정합니다.
6. **로그인**을 클릭합니다.

가상 어플라이언스에 있는 모든 디렉토리의 목록이 표시됩니다.

에이전트 업데이트

Cyber Protect 콘솔을 사용하거나 설치 파일을 다운로드 및 실행하여 모든 에이전트를 수동으로 업데이트할 수 있습니다.

다음 에이전트의 경우 자동 업데이트를 구성할 수 있습니다.

- Agent for Windows
- Agent for Linux
- Agent for Mac
- Cyber Files Cloud Agent for File Sync & Share

에이전트를 자동으로 업데이트하거나 Cyber Protect 콘솔을 사용하여 수동으로 업데이트하려면 다음 위치에 4.2GB의 여유 공간이 필요합니다.

- Linux - 루트 디렉토리
- Windows - 에이전트가 설치된 볼륨

macOS에서 에이전트를 업데이트하려면 루트 디렉토리에 5GB의 여유 공간이 필요합니다.

참고
[Agent for VMware, Agent for Scale Computing, Agent for Virtuozzo Hybrid Infrastructure, Agent for RHV(oVirt)를 비롯하여 가상 에이전트 형식으로 제공되는 모든 에이전트의 경우]

프록시로 보호되는 가상 어플라이언스의 자동 또는 수동 업데이트를 수행하려면 다음과 같이 각 어플라이언스에서 프록시 서버를 구성해야 합니다.

`/opt/acronis/etc/va-updater/config.yaml` 파일 맨 끝에 다음 줄을 추가하고 환경에 해당하는 값을 입력합니다.

```
httpProxy: http://proxy_login:proxy_password@proxy_address:port
```

에이전트 수동 업데이트

Cyber Protect 콘솔을 사용하거나 설치 파일을 다운로드 및 실행하여 에이전트를 업데이트할 수 있습니다.

다음 버전의 가상 어플라이언스는 Cyber Protect 콘솔을 통해서만 업데이트해야 합니다.

- Agent for VMware(가상 어플라이언스): 버전 12.5.23094 이상
- Agent for Virtuozzo Hybrid Infrastructure(가상 어플라이언스): 버전 12.5.23094 이상

다음 버전의 에이전트도 Cyber Protect 콘솔을 사용하여 업데이트할 수 있습니다.

© Acronis International GmbH, 2003-2024

- Agent for Windows, Agent for VMware(Windows), Agent for Hyper-V: 버전 12.5.21670 이상.
- Agent for Linux: 버전 12.5.23094 이상
- 기타 에이전트: 버전 12.5.23094 이상

에이전트 버전을 확인하려면 Cyber Protect 콘솔에서 머신을 선택한 다음 **상세 정보**를 클릭합니다.

이러한 에이전트의 이전 에이전트 버전을 업데이트하려면 최신 버전을 수동으로 다운로드하여 설치합니다. 다운로드 링크를 찾으려면 **모든 장치** > **추가**를 클릭합니다.

사전 요구 사항

Windows 머신에서 Cyber Protect 기능을 사용하려면 Microsoft Visual C++ 2017 Redistributable이 필요합니다. 에이전트를 업데이트하기 전에 머신에 설치되어 있는지 확인하고, 없는 경우 설치합니다. 설치 후에는 다시 시작해야 할 수 있습니다. Microsoft Visual C++ Redistributable 패키지는 Microsoft 웹 사이트 https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows에서 찾을 수 있습니다.

Cyber Protect 콘솔을 사용하여 에이전트를 업데이트하려면

1. **설정** > **에이전트**를 클릭합니다.
   소프트웨어에 머신 목록이 표시됩니다. 에이전트 버전이 오래된 머신에는 오렌지색 느낌표가 표시됩니다.
2. 에이전트를 업데이트하려는 머신을 선택합니다. 머신이 온라인 상태여야 합니다.
3. **에이전트 업데이트**를 클릭합니다.

참고
업데이트 중에는 진행 중인 모든 백업 작업에 실패하게 됩니다.

버전 12.5.23094 미만의 Agent for VMware(가상 어플라이언스)를 업데이트하려면

1. **설정** > **에이전트** > 업데이트하려는 에이전트 > **상세 정보**를 클릭한 다음, **할당된 가상 머신** 섹션을 검토합니다. 업데이트 후에 이 설정을 재입력해야 합니다.
   a. **자동 할당** 스위치의 위치를 기록해 둡니다.
   b. 에이전트에 수동으로 할당된 가상 머신을 알아보려면 **할당됨:** 링크를 클릭합니다. 소프트웨어에 할당된 가상 머신 목록이 표시됩니다. **Agent** 열에 표시된 에이전트 이름 뒤에 (M)이 있는 머신을 기록해 둡니다.
2. "에이전트 제거"의 설명대로 Agent for VMware(가상 어플라이언스)를 제거합니다. 에이전트를 다시 설치할 계획이 있더라도, 5단계에서 **설정** > **에이전트**로 이동해 에이전트를 삭제합니다.
3. "OVF 템플릿 디플로이"의 설명대로 Agent for VMware(가상 어플라이언스)를 디플로이합니다.
4. "가상 어플라이언스 구성"의 설명대로 Agent for VMware(가상 어플라이언스)를 구성합니다.
   로컬 연결된 스토리지를 복원하려는 경우, 7단계에서 다음을 수행하십시오.
   a. 로컬 스토리지를 포함하고 있는 디스크를 가상 어플라이언스에 추가합니다.
   b. **새로 고침** > **스토리지 생성** > **마운트**를 클릭합니다.

© Acronis International GmbH, 2003-2024

c. 소프트웨어는 디스크의 원래 **문자**와 **라벨**을 표시합니다. 이를 변경하지 마십시오.
d. **확인**을 클릭합니다.
5. **설정** > **에이전트** > 업데이트하려는 에이전트 > **상세 정보**를 클릭한 다음, 1단계에서 기록한 설정을 재구성합니다. 일부 가상 머신이 에이전트에 수동으로 할당된 경우, "가상 머신 결합"에 설명된 대로 재할당합니다.

   에이전트 구성이 완료되면, 이전 에이전트에 적용되어 있던 보호 계획이 자동으로 새 에이전트에 다시 적용됩니다.
6. 애플리케이션 인식 백업이 활성화된 계획에는 게스트 OS 자격 증명 재입력이 필요합니다. 이러한 계획을 편집하고 자격 증명을 재입력하십시오.
7. ESXi 구성을 백업하는 계획인 경우 "루트" 패스워드 재입력이 필요합니다. 이러한 계획을 편집하고 패스워드를 재입력하십시오.

머신에서 사이버 보호 정의를 업데이트하려면

1. **설정** > **에이전트**를 클릭합니다.
2. 사이버 보호 정의를 업데이트할 머신을 선택한 다음 **정의 업데이트**를 클릭합니다. 머신이 온라인 상태여야 합니다.

에이전트에 업데이터 역할을 할당하려면

1. **설정** > **에이전트**를 클릭합니다.
2. 업데이터 역할을 할당할 머신을 선택하고 **상세 정보**를 클릭한 다음 **사이버 보호 정의** 섹션에서 **이 에이전트를 다운로드해 패치 및 업데이트 배포**를 활성화합니다.

참고
업데이터 역할이 할당되어 있는 에이전트는 Windows 서드 파티 제품용 패치만 다운로드하여 배포할 수 있습니다. Microsoft 제품의 경우에는 업데이트 에이전트가 패치 배포를 지원하지 않습니다.

에이전트에서 캐시된 데이터를 지우려면

1. **설정** > **에이전트**를 클릭합니다.
2. 캐시된 데이터(오래된 업데이트 파일 및 패치 관리 데이터)를 지우려는 머신을 선택하고 **캐시 지우기**를 클릭합니다.

자동으로 에이전트 업데이트

여러 워크로드를 쉽게 관리하기 위해 Agent for Windows, Agent for Linux 및 Agent for Mac에 대한 자동 업데이트를 구성할 수 있습니다. 에이전트 버전 15.0.26986(2021년 5월 릴리스) 이상인 경우 자동 업데이트를 사용할 수 있습니다.기존 에이전트는 먼저 최신 버전으로 수동 업데이트해야 합니다.

자동 업데이트는 다음 운영 체제를 실행하는 머신에서 지원됩니다.

- Windows XP SP 3 이상
- Red Hat Enterprise Linux 6 이상, CentOS 6 이상
- OS X 10.9 Mavericks 이상

© Acronis International GmbH, 2003-2024

자동 업데이트 설정은 데이터 센터 수준에서 사전 구성됩니다. 회사 관리자는 회사 또는 부서의 모든 머신 또는 개별 머신에 대해 이러한 설정을 사용자 정의할 수 있습니다. 사용자 정의 설정이 적용되지 않으면 상위 수준의 설정이 다음 순서로 사용됩니다.

1. Cyber Protection 데이터 센터
2. 회사(고객 테넌트)
3. 단위
4. 머신

예를 들어, 부서 관리자는 부서의 모든 머신에 대해 사용자 정의 자동 업데이트 설정을 구성할 수 있으며, 이는 회사 수준의 머신에 적용된 설정과 다를 수도 있습니다. 관리자는 부서에 있는 하나 이상의 개별 머신에 대해 각기 다른 설정을 구성할 수 있으며, 이 경우 부서 설정과 회사 설정이 모두 적용되지 않습니다.

자동 업데이트를 활성화한 후 다음 옵션을 구성할 수 있습니다.

- **업데이트 채널**
  업데이트 채널은 사용할 에이전트 버전(가장 최신 버전 또는 이전 릴리스의 최신 버전)을 정의합니다.
- **유지보수 기간**
  유지보수 기간은 업데이트가 설치될 수 있는 시기를 정의합니다. 유지보수 기간이 비활성화되어 있으면 언제든지 업데이트를 실행할 수 있습니다.
  활성화된 유지보수 기간 내에서도 에이전트가 다음 작업을 실행하는 동안에는 업데이트가 설치되지 않습니다.
  - 백업
  - 복구
  - 백업 복제
  - 가상 머신 복제
  - 복제본 테스트
  - 백업에서 가상 머신 실행(종료 포함)
  - 재해 복구 장애 조치
  - 재해 복구 장애 복구
  - 스크립트 실행(사이버 스크립트 작성 기능의 경우)
  - 패치 설치
  - ESXi 구성 백업

자동 업데이트 설정을 사용자 정의하려면

1. Cyber Protect 콘솔에서 **설정** > **에이전트**로 이동합니다.
2. 설정의 범위를 선택합니다.
   - 모든 머신의 설정을 변경하려면 기본 **에이전트 업데이트 설정 편집**을 클릭합니다.
   - 특정 머신의 설정을 변경하려면 원하는 머신을 선택한 다음 **에이전트 업데이트 설정**을 클릭합니다.
3. 필요에 따라 설정을 구성한 다음 **적용**을 클릭합니다.

사용자 정의 자동 업데이트 설정을 제거하려면

© Acronis International GmbH, 2003-2024

1. Cyber Protect 콘솔에서 **설정** > **에이전트**로 이동합니다.
2. 설정의 범위를 선택합니다.
   - 모든 머신의 사용자 정의 설정을 제거하려면 **기본 에이전트 업데이트 설정 편집**을 클릭합니다.
   - 특정 머신의 사용자 정의 설정을 제거하려면 원하는 머신을 선택한 다음 **에이전트 업데이트 설정**을 클릭합니다.
3. **기본 설정으로 재설정**을 클릭한 다음 **적용**을 클릭합니다.

자동 업데이트 상태를 확인하려면

1. Cyber Protect 콘솔에서 **설정** > **에이전트**로 이동합니다.
2. 표 오른쪽 위의 기어 아이콘을 클릭한 다음 **자동 업데이트** 확인란을 선택했는지 확인합니다.
3. **자동 업데이트** 열에 표시된 상태를 확인합니다.

BitLocker로 보호된 워크로드에서 에이전트 업데이트

에이전트 업데이트로 인해 Startup Recovery Manager가 변경되는 경우 BitLocker와 Startup Recovery Manager가 모두 활성화되어 있는 워크로드에서 BitLocker가 정상 작동하지 않습니다. 이 경우에는 워크로드를 다시 시작한 후 BitLocker 복구 키를 입력해야 합니다. 이 문제를 완화하려면 에이전트를 업데이트하기 전에 BitLocker를 일시 중단하거나 비활성화하십시오.

영향을 받는 에이전트 버전:

- 23.12.36943, 2023년 12월 출시됨

또한 보호 에이전트의 릴리스 노트에서 업데이트가 Startup Recovery Manager에 변화를 도입하는지 확인할 수 있습니다.

BitLocker와 Startup Recovery Manager가 활성화되어 있는 워크로드에서 에이전트를 업데이트하려면

1. 에이전트를 업데이트하려는 워크로드에서 BitLocker를 일시 중단하거나 비활성화합니다.
2. 에이전트를 업데이트합니다.
3. 워크로드를 다시 시작합니다.
4. BitLocker를 활성화합니다.

에이전트의 무단 설치 제거 또는 변경의 방지

보호 계획에서 **패스워드 보호** 설정을 활성화하여 Agent for Windows를 무단 설치 제거 또는 변경으로부터 보호할 수 있습니다. 이 설정은 **자체 보호** 설정을 활성화한 경우에만 사용할 수 있습니다.

패스워드 보호를 활성화하려면

1. 보호 계획에서, **안티바이러스&안티맬웨어 보호 기능**모듈(Cyber Backup 버전의 경우 **Active Protection**)을 확대하십시오.

© Acronis International GmbH, 2003-2024

2. **자체 보호**를 클릭한 뒤 **자체 보호** 스위치가 활성화된 것을 확인하십시오.
3. **패스워드 보호** 스위치를 활성화하십시오.
4. 열린 창에서, 보호된 Agent for Windows의 컴퍼넌트를 설치 제거하거나 변경하기 위해 필요한 비밀번호를 복사하십시오.

   이 비밀번호는 고유하며 따라서 이 창을 닫은 뒤에는 복구할 수 없습니다. 이 비밀번호를 잃어버리거나 잊는 경우, 보호 계획을 편집하여 새 비밀번호를 생성할 수 있습니다.
5. **닫기**를 클릭합니다.
6. **자체 보호** 창에서 **완료**를 클릭합니다.
7. 보호 계획을 저장합니다.

이 보호 계획이 적용된 머신에서 패스워드 보호가 활성화될 것입니다. 패스워드 보호는 Agent for Windows 버전 *15.0.25821* 이상에서만 사용 가능합니다.머신이 온라인 상태여야 합니다.

macOS를 실행 중인 머신에 패스워드 보호가 활성화된 경우에도 보호 계획을 적용할 수 있지만, 보호가 제공되지는 않습니다. Linux를 실행 중인 머신에는 보호 계획을 적용할 수 없습니다.

또한, 패스워드 보호가 활성화된 동일한 Windows 머신에 두 개 이상의 보호 계획을 적용할 수 없습니다. 발생할 수 있는 충돌을 해결하는 방법에 관하여는 계획 충돌 해결을 참조하십시오.

기존 보호 계획에서 비밀번호 계획을 변경하려면

1. 보호 계획에서, **안티바이러스&안티맬웨어 보호 기능** 모듈(Cyber Backup 버전의 경우 **Active Protection**)을 확대하십시오.
2. **자체 보호**를 클릭합니다.
3. **새 비밀번호 생성**을 클릭합니다.
4. 열린 창에서, 보호된 Agent for Windows의 컴퍼넌트를 설치 제거하거나 변경하기 위해 필요한 비밀번호를 복사하십시오.

   이 비밀번호는 고유하며 따라서 이 창을 닫은 뒤에는 복구할 수 없습니다. 이 비밀번호를 잃어버리거나 잊는 경우, 보호 계획을 편집하여 새 비밀번호를 생성할 수 있습니다.
5. **닫기**를 클릭합니다.
6. **자체 보호** 창에서 **완료**를 클릭합니다.
7. 보호 계획을 저장합니다.

에이전트 제거

워크로드에서 에이전트 설치를 제거하면 해당 워크로드가 Cyber Protect 콘솔에서 자동으로 제거됩니다. 네트워크 문제 등으로 인해 에이전트 설치 제거 후에도 워크로드가 계속 표시된다면 콘솔에서 해당 워크로드를 수동으로 제거하십시오. 이 작업을 수행하는 방법에 대한 자세한 내용은 "Cyber Protect 콘솔에서 워크로드 제거"(307페이지) 항목을 참조하십시오.

참고
에이전트를 설치 제거해도 계획이나 백업이 삭제되지는 않습니다.

에이전트 설치를 제거하려면

Windows

© Acronis International GmbH, 2003-2024

1. 에이전트가 설치된 머신에 관리자로 로그인합니다.
2. **제어판**에서 **프로그램 및 기능**(Windows XP의 경우 **프로그램 추가 또는 제거**)으로 이동합니다.
3. **Acronis Cyber Protect**을(를) 마우스 오른쪽 버튼으로 클릭하고 **설치 제거**를 선택합니다.
4. [암호로 보호되는 에이전트] 에이전트를 설치 제거하기 위해 필요한 암호를 지정하고, **다음**을 클릭합니다.
5. [선택 사항] **로그 및 구성 설정 제거** 확인란을 선택합니다.
   에이전트를 다시 설치할 계획이라면 이 확인란의 선택을 해제합니다. 이 확인란을 선택하고 에이전트를 다시 설치하면 Cyber Protect 콘솔에서 이 워크로드가 중복 표시될 수 있으며 이전 백업이 워크로드와 연결되지 않을 수도 있습니다.
6. **설치 제거**를 클릭합니다.

Linux

1. 에이전트가 설치되어 있는 머신에서 루트 사용자로 `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall`을 실행합니다.
2. [선택 사항] **모든 제품 추적 정리(제품 로그, 작업, 볼트 및 구성 설정 제거)** 확인란을 선택합니다.
   에이전트를 다시 설치할 계획이라면 이 확인란의 선택을 해제합니다. 이 확인란을 선택하고 에이전트를 다시 설치하면 Cyber Protect 콘솔에서 이 워크로드가 중복 표시될 수 있으며 이전 백업이 워크로드와 연결되지 않을 수도 있습니다.
3. 결정을 확인합니다.

macOS

1. 에이전트가 설치되어 있는 머신에서 설치 .dmg 파일을 두 번 클릭합니다.
2. 운영 체제가 설치 디스크 이미지를 마운트할 때까지 기다립니다.
3. 이미지 내에서 **설치 제거**를 두 번 클릭합니다.
4. 메시지가 표시되면 관리자 자격 증명을 제공합니다.
5. 결정을 확인합니다.

Agent for Windows와 번들로 제공되는 컴포넌트를 설치 제거하려면

Agent for Windows를 설치 제거하지 않고도 Cyber Protect Monitor, Agent for Data Loss Prevention, 부트 가능한 미디어 제작기 등 Agent for Windows와 번들로 제공되는 개별 컴포넌트를 설치 제거할 수 있습니다.

1. 에이전트가 설치된 머신에 관리자로 로그인합니다.
2. 설치 프로그램을 실행하고 **설치된 컴포넌트 수정**을 클릭합니다.
3. 설치 제거할 컴포넌트 옆에 있는 확인란을 선택 취소하고 **완료**를 클릭합니다.

Agent for VMware(가상 어플라이언스)를 제거하려면

1. vSphere Client를 사용하여 vCenter Server에 로그인합니다.
2. [가상 어플라이언스의 전원이 켜져 있는 경우] 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **전원** > **전원 끄기**를 클릭합니다. 결정을 확인합니다.

© Acronis International GmbH, 2003-2024

3. [가상 어플라이언스가 가상 디스크에서 로컬 연결 스토리지를 사용하며 해당 디스크의 데이터를 보존하려는 경우] 가상 어플라이언스에서 가상 스토리지를 제거합니다.
   a. 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭한 다음 **설정 편집**을 클릭합니다.
   b. 스토리지가 있는 디스크를 선택한 다음 **제거**를 클릭합니다.
   c. **제거 옵션**에서 **가상 머신에서 제거**를 클릭합니다.
   d. **확인**을 클릭합니다.

   결과적으로 디스크는 데이터 저장소에 남아 있습니다. 다른 가상 어플라이언스에 디스크를 연결할 수 있습니다.
4. 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭한 다음 **디스크에서 삭제**를 클릭합니다. 결정을 확인합니다.
5. [선택 사항] [해당 어플라이언스를 다시 사용하지 않으려는 경우] Cyber Protect 콘솔에서 **백업 스토리지** > **위치**로 이동한 후 로컬 연결 스토리지에 해당하는 위치를 삭제합니다.

보호 설정

Cyber Protection에 대한 일반 보호 설정을 구성하려면 Cyber Protect 콘솔에서 **설정** > **보호**로 이동합니다.

컴퍼넌트에 대한 자동 업데이트

기본적으로 모든 에이전트는 인터넷에 연결하여 업데이트를 다운로드할 수 있습니다.

관리자는 환경에서 에이전트를 하나 또는 여러 개 선택한 다음 업데이터 역할을 할당하는 방식으로 네트워크 대역폭 트래픽을 최소화할 수 있습니다. 그러면 전용 에이전트가 인터넷에 연결하여 업데이트를 다운로드합니다. 기타 모든 에이전트는 피어 투 피어 기술을 사용하여 전용 업데이터 에이전트에 연결한 다음 해당 에이전트에서 업데이트를 다운로드합니다.

업데이터 역할이 지정되지 않은 에이전트는 환경 내에 전용 업데이터 에이전트가 없거나 약 5분 동안 전용 업데이트 에이전트 연결을 설정할 수 없으면 인터넷에 연결합니다.

업데이터 에이전트는 안티바이러스 및 맬웨어 방지 보호, 취약점 평가 및 패치 관리용으로 업데이트와 패치를 배포합니다. 하지만 에이전트 버전 업데이트는 배포 대상에 포함되지 않습니다.

참고
업데이터 역할이 할당되어 있는 에이전트는 Windows 서드 파티 제품용 패치만 다운로드하여 배포할 수 있습니다. Microsoft 제품의 경우에는 업데이트 에이전트가 패치 배포를 지원하지 않습니다.

에이전트에 업데이터 역할을 할당하기 전에 에이전트가 실행되는 머신의 성능이 업데이트 역할을 수행하기에 충분하고, 머신의 고속 인터넷 연결 상태가 안정적이며, 디스크 공간이 충분한지 확인하십시오.

업데이트 역할용으로 머신을 준비하려면

© Acronis International GmbH, 2003-2024

1. 업데이터 역할을 활성화할 에이전트 머신에서 다음 방화벽 규칙을 적용합니다.
   - 인바운드(들어옴) "updater_incoming_tcp_ports": 모든 방화벽 프로필(공개, 비공개, 도메인)에 대해 TCP 포트 18018 및 6888로의 연결을 허용합니다.
   - 인바운드(들어옴) "updater_incoming_udp_ports": 모든 방화벽 프로필(공개, 비공개, 도메인)에 대해 UDP 포트 6888로의 연결을 허용합니다.
2. Acronis Agent Core Service를 다시 시작합니다.
3. 방화벽 서비스를 다시 시작합니다.

잉러한 규칙을 적용하지 않고 방화벽을 활성화하면 피어 에이전트가 클라우드에서 업데이트를 다운로드합니다.

보호 에이전트에 업데이터 역할을 할당하려면

1. Cyber Protect 콘솔에서 **설정** > **에이전트**로 이동합니다.
2. 업데이터 역할을 할당할 에이전트가 있는 머신을 선택합니다.
3. **세부정보**를 클릭하고 **이 에이전트를 다운로드해 패치 및 업데이트 배포** 스위치를 활성화합니다.

피어 투 피어 업데이트의 작동 방식은 다음과 같습니다.

1. 업데이터 역할이 지정된 에이전트는 스케줄별로 서비스 제공자가 제공한 인덱스 파일을 확인하여 핵심 컴퍼넌트를 업데이트합니다.
2. 업데이터 역할이 지정된 에이전트는 다운로드를 시작하고 모든 에이전트에 업데이트를 분산합니다.

환경 내의 여러 에이전트에 업데이터 역할을 할당할 수 있습니다. 그러면 업데이터 역할이 할당된 에이전트 하나가 오프라인 상태로 전환되는 경우 해당 역할의 다른 에이전트가 정의 업데이트 소스로 작동할 수 있습니다.

스케줄별로 Cyber Protection 정의 업데이트

스케줄 탭에서 다음 각 컴퍼넌트에 대한 Cyber Protection 정의 자동 업데이트 스케줄을 설정할 수 있습니다.

- 맬웨어 방지
- 취약성 평가
- 패치 관리

정의 업데이트 설정을 변경하려면 **설정** > **보호** > **보호 정의 업데이트** > **스케줄**로 이동합니다.

예약 유형:

- **일일** – 정의를 업데이트할 요일을 정합니다.
  시작 시간 – 정의를 업데이트할 시간을 선택합니다.
- **매시간** – 업데이트를 위한 보다 상세한 시간별 스케줄을 정의합니다.
  매번 실행 – 업데이트 주기를 정의합니다.
  시작 ...종료 – 업데이트를 위한 특정 시간 범위를 정의합니다.

© Acronis International GmbH, 2003-2024

필요에 따라 Cyber Protection 정의 업데이트

필요에 따라 특정 머신에 대한 Cyber Protection 정의를 업데이트하려면

1. Cyber Protect 콘솔에서 **설정** > **에이전트**로 이동합니다.
2. 보호 정의를 업데이트할 머신을 선택한 다음 **정의 업데이트**를 클릭합니다.

캐시 스토리지

캐시된 데이터 위치는 다음과 같습니다.

- Windows 머신: `C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache`
- Linux 머신: `/opt/acronis/var/atp-downloader/Cache`
- macOS 머신: `/Library/Application Support/Acronis/Agent/var/atp-downloader/Cache`

캐시 스토리지 설정을 변경하려면 **설정** > **보호** > **보호 정의 업데이트** > **캐시 스토리지**로 이동합니다.

오래된 업데이트 파일 및 패치 관리 데이터에서 캐시된 데이터를 제거할 기간을 지정합니다.

에이전트에 대한 최대 캐시 스토리지(GB):

- **업데이터 역할** – 업데이터 역할이 있는 머신의 캐시에 대한 스토리지 크기를 정의합니다.
- **기타 역할** – 다른 머신의 캐시에 대한 스토리지 크기를 정의합니다.

참고
Acronis가 소프트웨어를 개선하는 데 활용할 수 있도록 Cyber Protection에서는 감지된 맬웨어 샘플을 추가 분석용으로 수집합니다. 언제든지 **보호** 탭에서 **맬웨어 샘플을 수집하여 CPOC에 업로드** 토글을 비활성화하여 이 설정을 변경할 수 있습니다.

머신의 서비스 할당량 변경

서비스 할당량은 보호 계획이 처음으로 머신에 적용될 때 자동으로 할당됩니다.

보호되는 시스템, 시스템의 운영 체제, 필요한 보호 수준 및 사용 가능한 할당량에 따라 가장 적절한 할당량이 할당됩니다. 조직에서 가장 적절한 할당량을 사용할 수 없다면 두 번째로 적합한 할당량이 할당됩니다. 예를 들어 가장 적절한 할당량인 **웹 호스팅 서버**를 사용할 수 없다면 **서버** 할당량이 할당됩니다.

할당량 할당의 예는 다음과 같습니다.

- Windows Server 또는 Linux 서버 운영 체제(예: Ubuntu Server)를 실행하는 실제 머신에는 **서버** 할당량이 할당됩니다.
- Windows 또는 Linux 데스크탑 운영 체제(예: Ubuntu Desktop)를 실행하는 실제 머신에는 **워크스테이션** 할당량이 할당됩니다.
- Hyper-V 역할이 활성화된 Windows 10을 실행하는 실제 머신에는 **워크스테이션** 할당량이 할당됩니다.

© Acronis International GmbH, 2003-2024

- 가상 데스크탑 인프라에서 실행되며 게스트 운영 체제 내에 보호 에이전트(예: Agent for Windows)가 설치되어 있는 데스크탑 머신에는 **가상 머신** 할당량이 할당됩니다. **가상 머신** 할당량을 사용할 수 없는 경우 이 머신 유형은 **워크스테이션** 할당량을 사용할 수도 있습니다.
- 가상 데스크탑 인프라에서 실행되며 에이전트 없는 모드에서 백업(예: Agent for VMware 또는 Agent for Hyper-V를 통해 백업)되는 데스크탑 머신에는 **가상 머신** 할당량이 할당됩니다.
- Hyper-V 또는 vSphere 서버에는 **서버**할당량이 할당됩니다.
- cPanel 또는 Plesk가 설치된 서버에는 **웹 호스팅 서버** 할당량이 할당됩니다. 웹 호스팅 서버 할당량을 사용할 수 없는 경우 이 서버는 웹 서버가 실행되는 머신 유형에 따라 **가상 머신** 또는 **서버** 할당량을 사용할 수도 있습니다.
- 애플리케이션 인식 백업을 수행하려면 워크스테이션에서도 **서버** 할당량이 필요합니다.

나중에 원래 할당을 수동으로 변경할 수 있습니다. 예를 들어, 좀 더 고급 보호 계획을 동일한 머신에 적용하려면 머신의 서비스 할당량을 업그레이드해야 할 수 있습니다. 이 보호 계획에 필요한 기능을 현재 할당된 서비스 할당량이 지원하지 않는 경우 보호 계획은 실패합니다.

원래 할당량이 할당된 후 더 적절한 할당량을 구매할 경우 서비스 할당량을 변경할 수도 있습니다. **워크스테이션** 할당량이 가상 머신에 할당된 경우를 예로 들 수 있습니다. 이 경우에는 **가상 머신** 할당량을 구매한 후 원래 **워크스테이션** 할당량 대신 수동으로 이 머신에 할당할 수 있습니다.

현재 할당되어 있는 서비스 할당량을 해제한 후 다른 머신에 해당 할당량을 할당할 수도 있습니다.

개별 머신 또는 머신 그룹의 서비스 할당량을 변경할 수 있습니다.

개별 머신의 서비스 할당량을 변경하려면

1. Cyber Protect 콘솔에서 **장치**로 이동합니다.
2. 원하는 머신을 선택한 다음, **상세 정보**를 클릭합니다.
3. **서비스 할당량** 섹션에서 **변경**을 클릭합니다.
4. **할당량 변경** 창에서 원하는 서비스 할당량을 선택하거나 **할당량 없음**을 선택한 다음 **변경**을 클릭합니다.

머신 그룹의 서비스 할당량을 변경하려면

1. Cyber Protect 콘솔에서 **장치**로 이동합니다.
2. 2개 이상의 머신을 선택한 다음 **할당량 지정**을 클릭합니다.
3. **할당량 변경** 창에서 원하는 서비스 할당량을 선택하거나 **할당량 없음**을 선택한 다음 **변경**을 클릭합니다.

사용자 환경에 설치된 Cyber Protection 서비스

Cyber Protection은 사용되는 Cyber Protection 옵션에 따라 다음의 서비스를 일부 또는 전부 설치합니다.

Windows에 설치되는 서비스

서비스 이름	용도

© Acronis International GmbH, 2003-2024

Acronis Managed Machine Service	백업, 복구, 복제, 보관, 유효성 검사 기능 제공
Acronis Scheduler2 Service	특정 이벤트에서 예약된 작업 실행
Acronis Active Protection Service	랜섬웨어 방어 기능 제공
Acronis Cyber Protection Service	맬웨어 방지 기능 제공

macOS에 설치되는 서비스

서비스 이름 및 위치	용도
/Library/LaunchDaemons/com.acronis.aakore.plist	에이전트와 관리 대상 컴퍼넌트 간의 통신 서비스 제공
/Library/LaunchDaemons/com.acronis.cyber-protect-service.plist	맬웨어 감지 기능 제공
/Library/LaunchDaemons/com.acronis.mms.plist	백업 및 복구 기능 제공
/Library/LaunchDaemons/com.acronis.schedule.plist	예약된 작업 실행

에이전트 로그 파일 저장

에이전트 로그를 .zip 파일로 저장할 수 있습니다. 불확실한 이유 때문에 백업에 실패한 경우 기술 지원 담당자가 문제를 파악하는 데 이 파일이 도움이 됩니다.

기본적으로 로그의 정보는 최근 3일에 최적화되어 있으나 이 기간을 변경할 수 있습니다.

에이전트 로그를 수집하는 방법

1. 다음 중 하나를 수행하십시오.
   - **장치**에서 로그를 수집하려는 머신을 선택한 다음 **활동**을 클릭합니다.
   - **설정** > **에이전트**에서 로그를 수집하려는 머신을 선택한 다음 **세부 정보**를 클릭합니다.
2. [선택 사항] 시스템 정보가 포함되는 기본 기간을 변경하려면 **시스템 정보 수집** 버튼 옆의 화살표를 클릭한 다음 기간을 선택합니다.
3. **시스템 정보 수집**을 클릭합니다.
4. 웹 브라우저에서 메시지가 표시되면 파일을 저장할 위치를 지정합니다.

사이트 간 OpenVPN - 추가 정보

복구 서버를 생성할 때는 **운영 네트워크 내의 서버 IP 주소**와 서버의 **테스트 IP 주소**를 구성합니다.

장애 조치(클라우드에서 가상 머신 실행)를 수행하고 가상 머신에 로그인하여 서버의 IP 주소를 확인하면 **운영 네트워크 내의 서버 IP 주소**가 표시됩니다.

테스트 장애 조치를 수행할 때는 **테스트 IP 주소**를 통해서만 테스트 서버에 연결할 수 있습니다. 테스트 IP 주소는 복구 서버의 구성에만 표시됩니다.

© Acronis International GmbH, 2003-2024

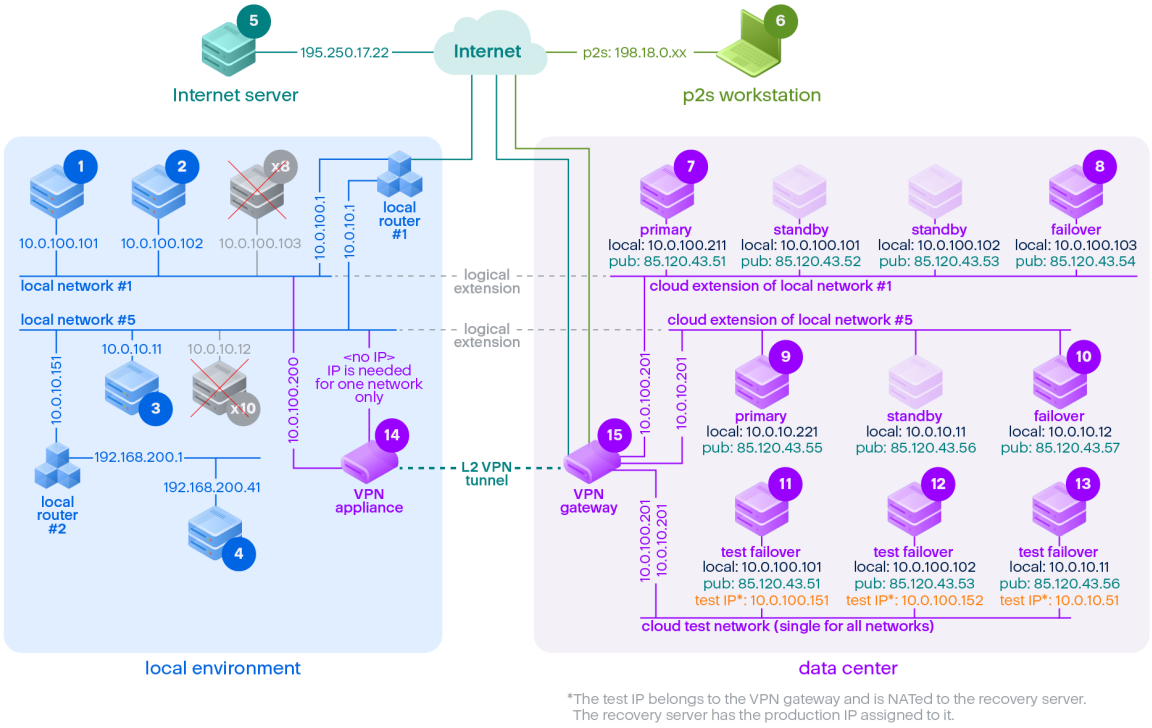
로컬 사이트에서 테스트 서버에 연결하려면 **테스트 IP 주소**를 사용해야 합니다.

참고

서버의 네트워크 구성에는 항상 **운영 네트워크 내의 서버 IP 주소**가 표시됩니다. 테스트 서버는 운영 서버의 표시 방식을 미러링하기 때문입니다. 테스트 서버가 운영 서버의 표시 방식을 미러링하는 이유는, 테스트 IP 주소는 테스트 서버가 아니라 VPN 게이트웨이에 속하는 주소이며 NAT를 사용하여 운영 IP 주소로 변환되기 때문입니다.

아래 다이어그램에 사이트 간 OpenVPN 구성의 예가 나와 있습니다. 네트워크 인프라가 정상 상태이면 로컬 환경의 일부 서버는 장애 조치를 통해 클라우드에 복구됩니다.

1. 다이어그램에 나와 있는 예에서는 고객이
   a. VPN 어플라이언스(14)를 구성한 다음 전용 클라우드 VPN 서버(15)에 연결하여 재해 복구를 활성화했습니다.
   b. 그리고 재해 복구를 통해 일부 로컬 서버(1, 2, 3, x8, x10)를 보호합니다.
      서버 4 등 로컬 사이트의 일부 서버는 VPN 어플라이언스에 연결되지 않은 네트워크에 연결되어 있습니다. 이러한 서버는 재해 복구를 통해 보호되지 않습니다.
2. 다른 네트워크에 연결된 일부 서버(1, 2, 3, 4)는 로컬 사이트에서 작동합니다.
3. 테스트 장애 조치(11, 12, 13)를 실행하여 보호된 서버(1, 2, 3)를 테스트하는 중입니다.
4. 로컬 사이트의 일부 서버(x8, x10)는 사용할 수 없는 상태입니다. 장애 조치를 수행하고 나면 클라우드에서 이러한 서버(8, 10)를 사용할 수 있게 됩니다.
5. 다른 네트워크에 연결된 일부 기본 서버(7, 9)는 클라우드 환경에서 사용 가능합니다.
6. (5)는 공용 IP주소를 사용하는 인터넷의 서버입니다.
7. (6)은 지점 및 사이트 간 VPN 연결(p2s)을 사용하여 클라우드에 연결하는 워크스테이션입니다.



© Acronis International GmbH, 2003-2024

이 예에서는 **시작:** 행의 서버에서 **종료:** 열의 서버로 다음과 같은 연결을 설정할 수 있습니다(예: "ping").

	종료:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
시작:		로컬	로컬	로컬	로컬	인터넷	p2s	기본	장애조치	기본	장애조치	테스트장애조치	테스트장애조치	테스트장애조치	VPN 어플라이언스	VPN 서버
1	로컬		직접	로컬라우터 1 을통한연결	로컬라우터 2 를통한연결	로컬라우터 1 을통한연결및인터넷	아니오	터널을통한연결: 로컬 로컬라우터 1 을통한연결및인터넷: 공용	터널을통한연결: 로컬 로컬라우터 1 을통한연결및인터넷: 공용	터널을통한연결: 로컬 로컬라우터 1 을통한연결및인터넷: 공용	터널을통한연결: 로컬 로컬라우터 1 을통한연결및인터넷: 공용	터널을통한연결: NAT (VPN 서버) 로컬라우터 1 을통한연결및인터넷: 공용	터널을통한연결: NAT (VPN 서버) 로컬라우터 1 을통한연결및인터넷: 공용	로컬라우터 1 을통한연결및터널: NAT (VPN 서버) 로컬라우터 1 을통한연결및인터넷: 공	직접	아니오

© Acronis International GmbH, 2003-2024

	종료:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
														용		
2	로컬	직접		로컬 라우터 1 을 통한 연결	로컬 라우터 2 를 통한 연결	로컬 라우터 1 을 통한 연결 및 인터넷	아니오	터널을 통한 연결: 로컬 로컬 라우터 1 을 통한 연결 및 인터넷: 공용	터널을 통한 연결: 로컬 로컬 라우터 1 을 통한 연결 및 인터넷: 공용	터널을 통한 연결: 로컬 로컬 라우터 1 을 통한 연결 및 인터넷: 공용	터널을 통한 연결: 로컬 로컬 라우터 1 을 통한 연결 및 인터넷: 공용	터널을 통한 연결: NAT (VPN 서버) 로컬 라우터 1 을 통한 연결 및 인터넷: 공용	터널을 통한 연결: NAT (VPN 서버) 로컬 라우터 1 을 통한 연결 및 인터넷: 공용	로컬 라우터 1 을 통한 연결 및 터널: NAT (VPN 서버) 로컬 라우터 1 을 통한 연결 및 인터넷: 공용	직접	아니오
3	로컬	로컬 라우터 1 을 통	로컬 라우터 1 을 통		로컬 라우터 2 를 통	로컬 라우터 1 을 통한	아니오	터널을 통한 연결: 로	터널을 통한 연결: 로	터널을 통한 연결: 로	터널을 통한 연결: 로	터널을 통한 연결: NAT	터널을 통한 연결: NAT	로컬 라우터 1 을 통한	로컬 라우터를 통한	아니오

© Acronis International GmbH, 2003-2024

	종료:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		한 연결	한 연결		한 연결	연결 및 인터넷		컬 로컬 라우터 1 을 통한 연결 및 인터넷: 공용	컬 로컬 라우터 1 을 통한 연결 및 인터넷: 공용	컬 로컬 라우터 1 을 통한 연결 및 인터넷: 공용	컬 로컬 라우터 1 을 통한 연결 및 인터넷: 공용	(VPN 서버) 로컬 라우터 1 을 통한 연결 및 인터넷: 공용	(VPN 서버) 로컬 라우터 1 을 통한 연결 및 인터넷: 공용	연결 및 터널: NAT (VPN 서버) 로컬 라우터 1 을 통한 연결 및 인터넷: 공용	연결	
4	로컬	로컬 라우터 2 와 라우터 1 을 통한 연결	로컬 라우터 2 와 라우터 1 을 통한 연결	로컬 라우터 2 를 통한 연결		로컬 라우터 2 와 라우터 1 을 통한 연결 및 인터넷	아니오	로컬 라우터 2 를 통한 연결 및 터널: 로컬 로컬	로컬 라우터 2 를 통한 연결 및 터널: 로컬 로컬	로컬 라우터 2 를 통한 연결 및 터널: 로컬 로컬	로컬 라우터 2 를 통한 연결 및 터널: 로컬 로컬	터널을 통한 연결: NAT (VPN 서버) 로컬 라우터 2 와	터널을 통한 연결: NAT (VPN 서버) 로컬 라우터 2 와	터널을 통한 연결: NAT (VPN 서버) 로컬 라우터 2 와	로컬 라우터 2 를 통한 연결	아니오

© Acronis International GmbH, 2003-2024

	종료:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								라우터 2 와 로컬 라우터 1 을 통한 연결 및 인터넷: 공용	라우터 2 와 로컬 라우터 1 을 통한 연결 및 인터넷: 공용	라우터 2 와 로컬 라우터 1 을 통한 연결 및 인터넷: 공용	라우터 2 와 로컬 라우터 1 을 통한 연결 및 인터넷: 공용	라우터 1 을 통한 연결 및 인터넷: 공용	라우터 1 을 통한 연결 및 인터넷: 공용	라우터 1 을 통한 연결 및 인터넷: 공용		
5	인터넷	아니오	아니오	아니오	아니오		해당 없음	인터넷을 통한 연결: 공용	인터넷을 통한 연결: 공용	인터넷을 통한 연결: 공용	인터넷을 통한 연결: 공용	인터넷을 통한 연결: 공용	인터넷을 통한 연결: 공용	인터넷을 통한 연결: 공용	아니오	아니오
6	p2s	아니오	아니오	아니오	아니오	인터넷을 통한 연결		p2s VPN (VPN 서버) 를 통한 연결: 로컬	p2s VPN (VPN 서버) 를 통한 연결: 로컬	p2s VPN (VPN 서버) 를 통한 연결: 로컬	p2s VPN (VPN 서버) 를 통한 연결: 로컬	p2s VPN - NAT (VPN 서버) 를 통한 연결	p2s VPN - NAT (VPN 서버) 를 통한 연결	p2s VPN - NAT (VPN 서버) 를 통한 연결	아니오	아니오

© Acronis International GmbH, 2003-2024

	종료:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								인터넷을 통한 연결: 공용	인터넷을 통한 연결: 공용	인터넷을 통한 연결: 공용	인터넷을 통한 연결: 공용	인터넷을 통한 연결: 공용	인터넷을 통한 연결: 공용	인터넷을 통한 연결: 공용		
7	기본	터널을 통한 연결	터널을 통한 연결	터널 및 로컬 라우터 1을 통한 연결	터널 및 로컬 라우터 1/2를 통한 연결	인터넷을 통한 연결 (VPN 서버를 통해 연결)	아니오		클라우드에서 직접: 로컬	터널 및 로컬 라우터 1을 통한 연결: 로컬	터널 및 로컬 라우터 1을 통한 연결: 로컬	VPN 서버를 통한 연결: NAT	VPN 서버를 통한 연결: NAT	터널 및 로컬 라우터 1을 통한 연결: NAT	아니오	DHCP 및 DNS 프로토콜 전용
8	장애 조치	터널을 통한 연결	터널을 통한 연결	터널 및 로컬 라우터 1을 통한 연결	터널 및 로컬 라우터 1/2를 통한 연결	인터넷을 통한 연결 (VPN 서버를 통해 연결)	아니오	클라우드에서 직접: 로컬		터널 및 로컬 라우터 1을 통한 연결: 로컬	터널 및 로컬 라우터 1을 통한 연결: 로컬	VPN 서버를 통한 연결: NAT	VPN 서버를 통한 연결: NAT	터널 및 로컬 라우터 1을 통한 연결: NAT	아니오	DHCP 및 DNS 프로토콜 전용

© Acronis International GmbH, 2003-2024

	종료:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
9	기본	터널 및 로컬 라우터 1을 통한 연결	터널 및 로컬 라우터 1을 통한 연결	터널을 통한 연결	터널을 통한 연결	인터넷을 통한 연결 (VPN 서버를 통해 연결)	아니오	터널 및 로컬 라우터 1을 통한 연결: 로컬	터널 및 로컬 라우터 1을 통한 연결: 로컬		클라우드에서 직접: 로컬	터널 및 로컬 라우터 1을 통한 연결: NAT	터널 및 로컬 라우터 1을 통한 연결: NAT	VPN 서버를 통한 연결: NAT	아니오	DHCP 및 DNS 프로토콜 전용
10	장애 조치	터널 및 로컬 라우터 1을 통한 연결	터널 및 로컬 라우터 1을 통한 연결	터널을 통한 연결	터널을 통한 연결	인터넷을 통한 연결 (VPN 서버를 통해 연결)	아니오	터널 및 로컬 라우터 1을 통한 연결: 로컬	터널 및 로컬 라우터 1을 통한 연결: 로컬	클라우드에서 직접: 로컬		터널 및 로컬 라우터 1을 통한 연결: NAT	터널 및 로컬 라우터 1을 통한 연결: NAT	VPN 서버를 통한 연결: NAT	아니오	DHCP 및 DNS 프로토콜 전용
11	테스트 장애 조치	아니오	아니오	아니오	아니오	인터넷을 통한 연결 (VPN 서버	아니오	아니오	아니오	아니오	아니오		클라우드에서 직접: 로컬	VPN 서버를 통한 연결: 로컬 (라	아니오	DHCP 및 DNS 프로토콜 전용

© Acronis International GmbH, 2003-2024

	종료:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
						를 통해 연결)								우팅)		
12	테스트 장애 조치	아니오	아니오	아니오	아니오	인터넷을 통한 연결 (VPN 서버를 통해 연결)	아니오	아니오	아니오	아니오	아니오	클라우드에서 직접: 로컬		VPN 서버를 통한 연결: 로컬 (라우팅)	아니오	DHCP 및 DNS 프로토콜 전용
13	테스트 장애 조치	아니오	아니오	아니오	아니오	인터넷을 통한 연결 (VPN 서버를 통해 연결)	아니오	아니오	아니오	아니오	아니오	VPN 서버를 통한 연결: 로컬 (라우팅)	VPN 서버를 통한 연결: 로컬 (라우팅)		아니오	DHCP 및 DNS 프로토콜 전용
14	VPN 어플라	직접	직접	로컬 라우터	로컬 라우터	인터넷 (로컬	아니오	아니오	아니오	아니오	아니오	아니오	아니오	아니오		아니오

© Acronis International GmbH, 2003-2024

	종료:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	이언스			1을 통한 연결	2를 통한 연결	라우터 1)을 통한 연결										
15	VPN 서버	아니오	아니오	아니오	아니오	아니오	아니오	아니오	아니오	아니오	아니오	아니오	아니오	아니오	아니오	

온프레미스 관리 서버용 라이센스 관리

온프레미스 관리 서버를 활성화하거나 해당 서버에 라이센스를 할당하는 방법과 관련된 자세한 내용은 Cyber Protect 사용자 안내서의 라이센스 섹션을 참조하십시오.

© Acronis International GmbH, 2003-2024

보호 방법과 대상 정의

관리 탭

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

생성한 모든 계획은 **콘솔의** 관리Cyber Protect 탭에서 사용할 수 있습니다.

다음 섹션을 사용할 수 있습니다.

- 보호 계획
- 원격 관리 계획
- 스크립팅 계획
- 모니터링 계획
- 스크립트 저장소
- 클라우드 애플리케이션 백업
- 백업 스캔
- 백업 복제
- 유효성 검사
- 정리
- VM으로 변환
- VM 복제

계획 상태

보호 계획 및 VM 복제 계획의 경우 상태 바가 다음과 같은 색상으로 구분된 상태를 보여줍니다.

- 확인(녹색)
- 경고(주황색)
- 오류(진한 주황색)
- 중요(빨간색)
- 계획 실행 중(파란색)
- 계획 비활성화됨(회색)

계획이 적용된 모든 워크로드에 대한 계획 상태에 대한 세부 정보를 보려면 상태 바를 클릭하십시오.

특정 상태를 클릭하여 이 상태를 가진 모든 워크로드의 목록을 확인합니다.

보호 계획

관리 > **보호 계획** 탭에서 기존 보호 계획에 대한 정보를 보고, 작업을 수행하고, 새 계획을 생성할 수 있습니다.

© Acronis International GmbH, 2003-2024

보호 계획에 대한 자세한 내용은 "보호 계획 및 모듈"(199페이지) 항목을 참조하십시오.

클라우드 애플리케이션의 백업 계획

관리 > **클라우드 애플리케이션 백업** 탭에는 클라우드 간 백업 계획이 표시됩니다. 이 계획은 클라우드에서 실행되고 클라우드 스토리지를 백업 위치로 사용하는 에이전트를 통해 클라우드에서 실행 중인 애플리케이션을 백업합니다.

이 섹션에서는 다음 작업을 수행할 수 있습니다.

- 백업 계획 생성, 확인, 실행, 중지, 편집 및 삭제
- 각 백업 계획에 관련된 활동 확인
- 각 백업 계획에 관련된 경보 확인

클라우드 애플리케이션 백업에 대한 자세한 내용은 다음을 참조하십시오.

- Microsoft 365 데이터 보호
- Google Workspace 데이터 보호

클라우드 간 백업을 수동으로 실행

Cyber Protection 서비스 중단을 방지하기 위해 수동 클라우드 간 백업 실행 수는 Microsoft 365 또는 GS uite 조직별로 1시간에 10개로 제한됩니다. 이 수를 초과하면 허용되는 실행 수가 시간당 1개로 재설정되고, 그 이후 시간당 총 10개 실행에 도달할 때까지 시간당 하나씩 추가 실행이 가능해집니다(예: 시간 1, 10개 실행; 시간 2, 1개 실행; 시간 3, 2개 실행).

장치 그룹(사서함, 드라이브, 사이트)에 적용된 백업 계획 또는 10개가 넘는 장치가 포함된 백업 계획은 수동으로 실행할 수 없습니다.

백업 스캔 계획

맬웨어(랜섬웨어 포함) 대비 백업을 스캔하려면 백업 스캔 계획을 생성하십시오.

중요
일부 워크로드 및 백업 스토리지에는 백업 스캔 계획이 지원되지 않습니다. 자세한 내용은 "제한 사항"(785페이지)을(를) 참조하십시오.

백업 스캔 계획을 생성하려면

1. Cyber Protect 콘솔에서 **관리** > **백업 스캔**으로 이동합니다.
2. **계획 생성**을 클릭합니다.
3. 계획의 이름과 다음 매개변수를 지정합니다.
   - **스캔 유형**:
     - **클라우드** – 이 옵션은 변경할 수 없습니다. 자동 선택된 클라우드 에이전트가 백업 스캔을 수행합니다.
   - **스캔할 백업**:

© Acronis International GmbH, 2003-2024

    - **위치** – 스캔하려는 백업 집합이 있는 위치를 선택합니다.
    - **백업** – 스캔하려는 백업 집합을 선택합니다.
- **다음에 대한 스캔**:
    - **맬웨어** – 이 옵션은 변경할 수 없습니다. 스캔에서는 선택한 백업 집합에서 맬웨어(랜섬웨어 포함)를 확인합니다.
- **암호화** - 암호화된 백업 집합을 스캔하려는 경우 암호화 비밀번호를 지정합니다. 위치나 여러 백업 집합을 선택했는데 지정한 비밀번호가 백업 집합과 일치하지 않으면 경보가 생성됩니다.
- **스케줄** – 이 옵션은 변경할 수 없습니다. 클라우드 스토리지에서 스캔이 자동으로 시작됩니다.

4. **생성**을 클릭합니다.

그러면 백업 스캔 계획이 생성되며, 클라우드 에이전트가 지정한 위치나 백업 집합에서 맬웨어를 스캔합니다.

오프호스트 데이터 처리

참고
이 기능은 Advanced Backup 팩 내에서 **Advanced Backup – 서버** 또는 **Advanced Backup – NAS** 할당량이 활성화되어 있는 고객 테넌트에서 사용 가능합니다.

복제, 유효성 검사 및 정리는 보통 백업을 수행하는 보호 에이전트에 의해 수행됩니다. 이로 인해 에이전트가 실행되는 머신에는 백업 과정이 완료된 후에도 추가 로드가 발생합니다. 머신의 로드를 줄이려면 오프 호스트 데이터 보호 계획을 생성하면 됩니다. 즉, 복제, 유효성 검사, 정리 및 가상 머신으로 변환을 위한 별도의 계획을 생성할 수 있습니다.

오프 호스트 데이터 보호 계획을 통해 다음을 수행할 수 있습니다.

- 백업 및 오프 호스트 데이터 보호 작업용 다른 에이전트 선택
- 네트워크 대역폭 소비를 최소화하도록 오프 호스트 데이터 처리 작업을 사용량이 많지 않은 시간으로 예약
- 오프 호스트 데이터 처리용 전용 에이전트를 설치하고 싶지 않은 경우 오프 호스트 데이터 처리 작업을 영업 시간 이후에 예약

참고
오프 호스트 데이터 처리 계획은 보호 에이전트가 설치된 머신의 시간 설정(시간대 포함)에 따라 실행됩니다. 가상 어플라이언스(예: Agent for VMware 또는 Agent for Scale Computing HC3)의 경우 에이전트의 그래픽 사용자 인터페이스에서 시간대를 구정할 수 있습니다.

백업 복제

참고
이 기능은 Advanced Backup 팩 내에서 **Advanced Backup – 서버** 또는 **Advanced Backup – NAS** 할당량이 활성화되어 있는 고객 테넌트에서 사용 가능합니다.

© Acronis International GmbH, 2003-2024

백업 복제에서는 다른 위치에 백업을 복사합니다. 오프 호스트 데이터 처리 작업인 백업 복제는 백업 복제 계획에서 구성됩니다.

보호 계획에 백업 복제를 포함할 수도 있습니다. 이 옵션에 대한 자세한 내용은 "복제"(400페이지) 항목을 참조하십시오.

백업 복제 계획 생성

오프 호스트 데이터 처리 작업으로 백업을 복제하려는 경우 백업 복제 계획을 생성합니다.

백업 복제 계획 생성 방법

1. Cyber Protect 콘솔에서 **관리** > **백업 복제**를 클릭합니다.
2. **계획 생성**을 클릭합니다.
3. **에이전트**에서 복제를 수행할 에이전트를 선택합니다.
   소스 위치와 복제 위치에 모두 액세스할 수 있는 어떤 에이전트나 선택할 수 있습니다.
4. **복제할 항목**에서 복제할 아카이브나 백업 위치를 선택합니다.
   아카이브와 위치 간을 전환하려면 오른쪽 위에 있는 **위치 / 백업** 스위치를 사용합니다.
   암호화된 아카이브 여러 개를 선택하는 경우에는 아카이브의 암호화 비밀번호가 동일해야 합니다. 다른 암호화 비밀번호를 사용하는 아카이브의 경우 개별 계획을 생성합니다.
5. **대상**에서 복제 위치를 지정합니다.
6. **복제 방법**에서 복제할 백업(복구 지점이라고도 함)을 선택합니다.
   다음 옵션을 사용할 수 있습니다.
   - **모든 백업**
   - **전체 백업만**
   - **마지막 백업만**

   이러한 옵션에 대한 자세한 내용은 "복제 대상"(187페이지) 항목을 참조하십시오.
7. **스케줄**에서 복제 스케줄을 구성합니다.
   백업 복제 계획 스케줄을 구성할 때는 백업 복제를 시작할 때의 원래 위치에서 마지막으로 복제된 백업을 계속 사용할 수 있는지 확인합니다. 예를 들어 이 백업이 보존 규칙에 의해 삭제되어 원래 위치에서 사용할 수 없는 상태라면 전체 아카이브가 전체 백업으로 복제됩니다. 그러면 복제 시간이 매우 오래 걸릴 수 있으며 스토리지 공간도 추가로 사용됩니다.
8. **보존 규칙**에서 대상 위치의 보존 규칙을 지정합니다.
   다음 옵션을 사용할 수 있습니다.
   - **백업 수별**
   - **백업 기간별**(월별, 주간, 일간, 매시간 백업용으로 각기 별도의 설정 사용 가능)
   - **백업의 총 크기 기준**
   - **백업 무기한 보관**

   참고
   이 옵션을 선택하면 스토리지 사용량이 많아집니다. 불필요한 백업은 수동으로 삭제해야 합니다.

© Acronis International GmbH, 2003-2024

9. [**복제할 항목**에서 암호화된 아카이브를 선택한 경우] **백업 비밀번호** 스위치를 활성화하고 암호화 비밀번호를 입력합니다.
10. [선택 사항] 계획 옵션을 수정하려면 기어 아이콘을 클릭하고 옵션을 필요한 대로 구성합니다.
11. **생성**을 클릭합니다.

복제 대상

참고
전체 위치 복제, 백업 세트의 모든 백업 복제 등 일부 복제 작업은 시간이 매우 오래 걸릴 수도 있습니다.

개별 백업 세트나 전체 백업 위치를 복제할 수 있습니다. 백업 위치를 복제하면 해당 위치의 모든 백업 세트가 복제됩니다.

백업 세트는 백업(복구 지점이라고도 함)으로 구성됩니다. 복제할 백업을 선택해야 합니다.

다음 옵션을 사용할 수 있습니다.

- **모든 백업**
  복제 계획을 실행할 때마다 백업 세트의 모든 백업이 복제됩니다.
- **전체 백업만**
  백업 세트의 전체 백업만 복제됩니다.
- **마지막 백업만**
  백업 유형(전체, 차등, 증분)에 관계없이 백업 세트의 최신 백업만 복제됩니다.

필요에 따라 적절한 옵션과 사용하려는 백업 구성표를 선택합니다. 예를 들어 **항상 증분(단일 파일)** 백업 구성표를 사용하며 최신 증분 백업만 복제하려는 경우 백업 복제 계획에서 **마지막 백업만**을 선택합니다.

각 백업 구성표 사용 시에 복제되는 백업이 아래 표에 요약되어 있습니다.

	항상 증분(단일 파일)	**항상 전체**	**매주 전체, 매일 증분**	**매월 전체, 매주 차등, 매일 증분(GFS)**
모든 백업	백업 세트의 모든 백업	백업 세트의 모든 백업	백업 세트의 모든 백업	백업 세트의 모든 백업
전체 백업만	첫 번째 백업(전체 백업)만	모든 백업	매주 백업 하나*	매월 백업 하나*
마지막 백업만	백업 세트의 최신 백업만*	백업 세트의 최신 백업만*	백업 유형에 관계없이 백업 세트의 최신 백업만*	백업 유형에 관계없이 백업 세트의 최신 백업만*

*백업 복제 계획 스케줄을 구성할 때는 백업 복제를 시작할 때의 원래 위치에서 마지막으로 복제된 백업을 계속 사용할 수 있는지 확인합니다. 예를 들어 이 백업이 보존 규칙에 의해 삭제되어 원래 위치에서 사용할 수 없는 상태라면 전체 아카이브가 전체 백업으로 복제됩니다. 그러면 복제 시간이 매우 오래 걸릴 수 있으며 스토리지 공간도 추가로 사용됩니다.

© Acronis International GmbH, 2003-2024

지원되는 위치

다음 표에는 백업 복제 계획에서 지원되는 백업 위치가 요약되어 있습니다.

위치:	소스로 지원됨	대상으로 지원됨
클라우드 스토리지	+	+
로컬 폴더	+	+
네트워크 폴더	+	+
퍼블릭 클라우드	+	+
NFS 폴더	–	–
Secure Zone	–	–

유효성 검사

참고
이 기능은 Advanced Backup 팩 내에서 **Advanced Backup – 서버** 또는 **Advanced Backup – NAS** 할당량이 활성화되어 있는 고객 테넌트에서 사용 가능합니다.

백업의 유효성을 검사하면 해당 백업의 데이터 복구 가능 여부를 확인할 수 있습니다.

오프 호스트 데이터 처리 작업으로 백업 유효성을 검사하려는 경우 유효성 검사 계획을 생성합니다. 유효성 검사 계획 생성 방법에 대한 자세한 내용은 "유효성 검사 계획 생성"(189페이지) 항목을 참조하십시오.

사용할 수 있는 유효성 검사 방법은 다음과 같습니다.

- 체크섬 확인
- 가상 머신으로 실행
  - VM 하트비트
  - 스크린샷 유효성 검사

이러한 방법 중 하나 이상을 선택할 수 있습니다. 방법을 여러 개 선택하면 모든 유효성 검사 방법에 해당하는 작업이 연속으로 실행됩니다. 유효성 검사 방법에 대한 자세한 내용은 "VM 하트비트"(192페이지) 항목을 참조하십시오.

백업 세트나 백업 위치의 유효성을 검사할 수 있습니다. 백업 위치의 유효성 검사에서는 해당 위치 내의 모든 백업 세트 유효성을 검사합니다.

지원되는 위치

지원되는 백업 위치와 유효성 검사 방법이 다음 표에 나와 있습니다.

© Acronis International GmbH, 2003-2024

참고
퍼블릭 클라우드 백업에는 유효성 검사 옵션을 사용할 수 없습니다. 퍼블릭 클라우드에서 전체 아카이브를 읽으면 비용이 너무 많이 발생하기 때문입니다.

위치:	체크섬 확인	가상 머신으로 실행	
		VM 하트비트	스크린샷 유효성 검사
클라우드 스토리지	+	+	+
로컬 폴더	+	+	+
네트워크 폴더	+	+	+
NFS 폴더	–	–	–
Secure Zone	–	–	–

유효성 검사 상태

유효성 검사가 정상적으로 완료되면 녹색 점과 **유효성 검사**됨 레이블이 백업에 표시됩니다.

유효성 검사가 실패하면 백업에 빨간색 점이 표시됩니다. 사용한 유효성 검사 방법 중 하나라도 실패하면 유효성 검사는 실패합니다. 유효성 검사 계획을 잘못 구성하여 유효성 검사가 실패하는 경우도 있습니다. 잘못된 호스트의 가상 머신에 **VM 하트비트** 방법을 사용하는 경우를 예로 들 수 있습니다.

새 유효성 검사 작업을 수행할 때마다 백업의 유효성 검사 상태가 업데이트됩니다. 각 유효성 검사 방법의 상태는 별도로 업데이트됩니다. 따라서 유효성 검사 방법 중 하나가 실패한 백업의 유효성 검사는 같은 유효성 검사 방법이 성공할 때까지 실패로 표시됩니다. 실패한 방법을 사용하지 않은 최신 유효성 검사 작업이 정상적으로 완료된 경우에도 마찬가지입니다.

유효성 검사 상태 확인 방법에 대한 자세한 내용은 "백업의 유효성 검사 상태 확인"(194페이지) 항목을 참조하십시오.

유효성 검사 계획 생성

오프 호스트 데이터 처리 작업으로 백업 세트 유효성을 검사하려는 경우 유효성 검사 계획을 생성합니다.

유효성 검사 계획 생성 방법

1. Cyber Protect 콘솔에서 **관리** > **유효성 검사**를 클릭합니다.
2. **계획 생성**을 클릭합니다.
   새 유효성 검사 계획용 템플릿이 열립니다.
3. [선택 사항] 계획 이름을 수정하려면 기본 이름을 클릭합니다.

© Acronis International GmbH, 2003-2024

4. **에이전트**에서 유효성 검사를 수행할 에이전트를 선택하고 **확인**을 클릭합니다.
   백업에서 가상 머신을 실행하여 유효성 검사를 수행하려면 Agent for VMware 또는 Agent for Hyper-V가 설치된 머신을 선택하십시오. 그 외의 경우에는 백업 위치에 액세스할 수 있는 머신을 선택합니다.
5. **유효성 검사할 항목**에서 유효성을 검사할 백업 세트를 선택합니다.
   a. 오른쪽 위에서 **위치** 또는 **백업**을 클릭하여 계획의 범위(개별 백업 세트 또는 전체 위치)를 선택합니다.
      선택한 백업이 암호화되어 있는 경우 모든 백업이 같은 암호화 비밀번호를 사용해야 합니다. 다른 암호화 비밀번호를 사용하는 백업의 경우 개별 계획을 생성합니다.
   b. **추가**를 클릭합니다.
   c. 유효성 검사 계획의 범위에 따라 여러 위치나 위치 하나와 백업 세트를 선택하고 **완료**를 클릭합니다.
   d. **완료**를 클릭합니다.
6. **유효성 검사 대상**에서 유효성을 검사할 선택한 백업 세트 내의 백업(복구 지점이라고도 함)을 선택합니다. 다음 옵션을 사용할 수 있습니다.
   - **모든 백업**
   - **마지막 백업만**
7. **유효성 검사 방법**에서 유효성 검사 방법을 선택합니다.
   다음 옵션 중 하나를 선택하거나 둘 다 선택할 수 있습니다.
   - **체크섬 확인**
   - **가상 머신으로 실행**

   방법에 대한 자세한 내용은 "VM 하트비트"(192페이지) 항목을 참조하십시오.
8. [**체크섬 확인**을 선택한 경우] **완료**를 클릭합니다.
9. [**가상 머신으로 실행**을 선택한 경우] 해당 방법의 설정을 구성합니다.
   a. **대상 머신**에서 가상 머신 유형(ESXi 또는 Hyper-V), 호스트 및 머신 이름 템플릿을 선택한 후 **확인**을 클릭합니다.
      기본 이름은 **[머신 이름]_validate**입니다.
   b. **데이터 저장소**(ESXi의 경우) 또는 **경로**(Hyper-V의 경우)에서 가상 머신의 데이터 저장소를 선택합니다.
   c. **가상 머신으로 실행**에서 제공되는 유효성 검사 방법 중 하나를 선택하거나 둘 다 선택합니다.
      - **VM 하트비트**
      - **스크린샷 유효성 검사**
   d. [선택 사항] **VM 설정**을 클릭하여 가상 머신의 메모리 크기 및 네트워크 연결을 변경합니다.
      기본적으로 가상 머신은 네트워크에 연결되지 않으며 가상 머신 메모리 크기는 원래 머신의 메모리 크기와 동일합니다.
   e. **완료**를 클릭합니다.
10. [선택 사항] 유효성 검사 계획 템플릿에서 **예약**을 클릭한 다음 템플릿을 구성합니다.
11. [**유효성 검사할 항목**에서 선택한 백업 세트가 암호화되어 있는 경우] **백업 비밀번호** 스위치를 활성화하고 암호화 비밀번호를 입력합니다.

© Acronis International GmbH, 2003-2024

12. [선택 사항] 계획 옵션을 수정하려면 기어 아이콘을 클릭합니다.
13. **생성**을 클릭합니다.

그러면 유효성 검사 계획이 준비되며 구성한 스케줄에 따라 실행됩니다. 계획을 즉시 실행하려면 **관리** > **유효성 검사**에서 해당 계획을 선택하고 **지금 실행**을 클릭합니다.

계획이 시작되고 나면 Cyber Protect 콘솔의 **모니터링** > **작업**에서 실행 중인 작업을 확인하고 작업 세부 정보로 드릴다운할 수 있습니다.

유효성 검사 계획에는 백업이 여러 개 포함될 수 있으며, 여러 유효성 검사 계획에서 백업 하나의 유효성을 검사할 수도 있습니다.

참고
모든 백업은 단일 유효성 검사 작업에 의해 순차적으로 하나씩 처리됩니다.

지정된 에이전트에서는 한 번에 하나의 유효성 검사 작업만 실행할 수 있습니다. 다양한 에이전트에 의해 실행되는 경우 여러 유효성 검사 작업을 동시에 실행할 수 있습니다(예: 두 개의 동시 작업은 두 개의 에이전트를 필요로 하며, 세 개의 작업은 세 개의 에이전트를 필요로 함).

아래 표에 유효성 검사 작업의 가능한 상태가 요약되어 있습니다.

작업 결과	백업이 하나 포함된 계획	백업이 여러 개 포함된 계획
성공	모든 유효성 검사 방법 성공	모든 백업에서 모든 유효성 검사 방법 성공
경고와 함께 성공	해당 없음	백업 하나 이상에서 유효성 검사 방법 하나 이상 실패
실패	유효성 검사 방법 하나 이상 실패	모든 백업에서 유효성 검사 방법 하나 이상 실패

유효성 검사 방법

유효성 검사 계획에서 사용할 수 있는 유효성 검사 방법은 다음과 같습니다.

- 체크섬 확인
- 가상 머신으로 실행
  - VM 하트비트
  - 스크린샷 유효성 검사

체크섬 확인

체크섬 확인을 통한 유효성 검사는 백업에서 복구할 수 있는 모든 데이터 블록의 체크섬을 계산한 다음 해당 데이터 블록의 원래 체크섬(백업 프로세스 중에 작성된 체크섬)과 비교합니다. 유일한 예외는 클라우드 스토리지에 위치한 파일 수준 백업의 유효성 검사입니다. 백업에 저장되어 있는 메타데이터의 일관성 확인을 통해 이러한 백업의 유효성을 검사합니다.

체크섬 확인을 통한 유효성 검사는 크기가 작은 증분 또는 차등 백업의 경우에도 시간이 걸리는 프로세스입니다. 유효성 검사 작업에서는 특정 백업에 실제로 포함되어 있는 데이터뿐 아니라 복구

© Acronis International GmbH, 2003-2024

해야 하는 모든 데이터를 확인하기 때문입니다. 즉, 이전 백업의 유효성도 검사해야 할 수 있습니다.

체크섬 확인을 통한 유효성 검사가 정상적으로 완료되면 데이터를 복구할 수 있는 가능성이 높은 것입니다. 하지만 이 방법을 통한 유효성 검사를 진행하더라도 복구 프로세스에 영향을 미치는 모든 요소를 확인하지는 않습니다.

운영 체제를 백업하는 경우에는 다음의 추가 작업 중 몇 가지를 사용하는 것이 좋습니다.

- 부트 가능한 미디어 예비 하드 드라이브로의 복구를 테스트합니다.
- ESXi 또는 Hyper-V 환경에 있는 백업에서 가상 머신을 실행합니다.
- **가상 머신으로 실행** 유효성 검사 방법이 활성화되어 있는 유효성 검사 계획을 실행합니다.

가상 머신으로 실행

이 방법은 운영 체제가 포함된 디스크 수준 백업에만 적용됩니다. 이 방법을 사용하려면 ESXi 또는 Hyper-V 호스트와 이 호스트를 관리하는 보호 에이전트(Agent for VMware 또는 Agent for Hyper-V)가 필요합니다.

가상 머신으로 실행 유효성 검사 방법을 사용할 수 있는 변형은 다음과 같습니다.

- VM 하트비트
- 스크린샷 유효성 검사

변형 중 하나 이상을 선택해야 합니다.

VM 하트비트

이 유효성 검사 방법을 사용하는 경우 에이전트가 백업에서 가상 머신을 실행하고 VMware Tools 또는 Hyper-V Integration Service에 연결한 후에 하트비트 응답을 확인하여 운영 체제가 성공적으로 시작되었는지 확인합니다. 연결에 실패하는 경우 에이전트는 2분마다 한 번씩, 총 5회까지 연결을 시도합니다. 시도가 모두 실패하는 경우 유효성 검사에 실패합니다.

유효성 검사 계획 및 유효성을 검사한 백업의 수에 관계없이 유효성 검사를 수행하는 에이전트는 한 번에 가상 머신 한 대를 실행합니다. 유효성 검사 결과가 정상으로 나오는 즉시 에이전트는 해당 가상 머신을 삭제하고 다음 머신을 실행합니다.

참고
이 방법은 ESXi 호스트에서 백업을 가상 머신으로 실행하여 VMware 가상 머신의 백업 유효성을 검사할 때, 그리고 Hyper-V 호스트에서 백업을 가상 머신으로 실행하여 Hyper-V 가상 머신의 백업 유효성을 검사할 때만 사용해야 합니다.

스크린샷 유효성 검사

이 유효성 검사 방법을 사용하는 경우 에이전트가 백업에서 가상 머신을 실행하며 가상 머신이 부팅되는 동안 스크린샷이 생성됩니다. 그러면 머신 인텔리전스(MI) 모듈이 스크린샷을 확인하여 로그인 화면이 있으면 백업을 유효성 검사가 완료된 항목으로 표시합니다.

© Acronis International GmbH, 2003-2024

스크린샷은 복구 지점에 연결되며 유효성 검사일로부터 1년 동안 Cyber Protect 콘솔에서 다운로드할 수 있습니다. 스크린샷을 확인하는 자세한 방법은 "백업의 유효성 검사 상태 확인"(194페이지) 항목을 참조하십시오.

사용자 계정에서 알림이 활성화되어 있으면 스크린샷이 연결된 백업의 유효성 검사 상태 관련 이메일이 수신됩니다. 알림에 대한 자세한 내용은 사용자를 위한 알림 설정 변경을 참조하십시오.

스크린샷 유효성 검사는 에이전트 버전 15.0.30971(2022년 11월에 출시됨) 이상에서 지원됩니다.

참고
스크린샷 유효성 검사는 GUI 기반 로그인 화면을 사용하는 Windows 및 Linux 시스템 백업에 가장 적합합니다. 이 방법은 콘솔 로그인 화면을 사용하는 Linux 시스템용으로 최적화된 방법이 아닙니다.

VM 하트비트 및 스크린샷 유효성 검사의 시간 초과 값 변경

백업을 가상 머신으로 실행하여 유효성을 검사할 때는 가상 머신을 부팅하는 시점과 하트비트 요청을 전송하거나 스크린샷을 생성하는 시점 사이의 시간 초과를 구성할 수 있습니다.

기본 기간은 다음과 같습니다.

- 1분 - 로컬 폴더 또는 네트워크 공유에 저장된 백업
- 5분 - 클라우드에 저장된 백업

Agent for VMware 또는 Agent for Hyper-V의 구성 파일을 편집하여 이 기간을 변경할 수 있습니다.

시간 초과 값을 변경하려면

1. 편집을 위해 구성 파일을 엽니다. 이 파일의 위치는 다음과 같습니다.
   - Windows에서 실행 중인 Agent for VMware 또는 Agent for Hyper-V: `C:\Program Files\BackupClient\BackupAndRecovery\settings.config`
   - Agent for VMware(가상 어플라이언스): `/bin/mms_settings.config`
     가상 어플라이언스에서 구성 파일에 액세스하는 방법에 대한 자세한 정보는 "가상 어플라이언스에 대한 SSH 연결"(160페이지)을(를) 참조하십시오.
2. <validation>으로 이동한 후 로컬 백업과 클라우드 백업의 값을 필요한 대로 변경합니다.

```
<validation>
<run_vm>
<initial_timeout_minutes>
<local_backups>1</local_backups>
<cloud_backups>5</cloud_backups>
</initial_timeout_minutes>
</run_vm>
</validation>
```

3. 구성 파일을 저장합니다.
4. 에이전트를 다시 시작합니다.
   - [Windows에서 실행 중인 Agent for VMware 또는 Agent for Hyper-V] 명령 프롬프트에서 다음 명령을 실행합니다.

© Acronis International GmbH, 2003-2024

```
net stop mms
```

```
net start mms
```

- [Agent for VMware(가상 어플라이언스)] 에이전트가 설치되어 있는 가상 머신을 다시 시작합니다.

오류 발생 시 재시도 횟수 구성

유효성 검사 성공률을 최대한 높이기 위해 종료 시 오류가 발생하는 유효성 검사 작업의 자동 재시도를 구성할 수 있습니다.

자동 재시도를 구성하려면

1. 유효성 검사 계획을 생성할 때 기어 아이콘을 클릭합니다.
2. **옵션** 창에서 **오류 처리**를 선택합니다.
3. **오류 발생 시 재시도** 아래에서 **예**를 클릭합니다.
4. **시도 횟수**에서 오류 발생 시의 최대 재시도 횟수를 구성합니다.
   유효성 검사 작업은 정상적으로 완료되거나 최대 재시도 횟수에 도달할 때까지 다시 실행됩니다.
5. **시도 간격**에서 두 연속 재시도 간의 제한 시간을 구성합니다.
6. **완료**를 클릭합니다.

백업의 유효성 검사 상태 확인

장치 탭이나 **백업 스토리지** 탭에서 백업의 유효성 검사 상태를 확인할 수 있습니다.

각 유효성 검사 방법의 상태를 확인하고 스크린샷 유효성 검사 방법을 통해 생성된 스크린샷을 다운로드할 수도 있습니다.

상태의 작동 방식에 대한 자세한 내용은 "유효성 검사 상태"(189페이지) 항목을 참조하십시오.

백업의 유효성 검사 상태 확인 방법

장치

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 백업 유효성 검사 상태를 확인하려는 워크로드를 선택하고 **복구**를 클릭합니다.
3. [사용 가능한 백업 위치가 두 개 이상인 경우] 백업 위치를 선택합니다.
4. 상태를 확인할 백업을 선택합니다.

백업 스토리지

1. Cyber Protect 콘솔에서 **백업 스토리지**로 이동합니다.
2. 백업 세트가 저장되어 있는 위치를 선택합니다.
3. 백업 세트를 선택하고 **백업 표시**를 클릭합니다.
4. 유효성 검사 상태를 확인할 백업을 선택합니다.

© Acronis International GmbH, 2003-2024

정리

정리는 보관 규칙에 따라 오래된 백업을 삭제하는 작업입니다. 이 작업은 에이전트 및 워크로드에만 적용되며 클라우드 간 백업(수동으로만 삭제 가능)에는 적용되지 않습니다.

참고
이 기능은 Advanced Backup 팩 내에서 **Advanced Backup – 서버** 또는 **Advanced Backup – NAS** 할당량이 활성화되어 있는 고객 테넌트에서 사용 가능합니다.

지원되는 위치

정리 계획은 NFS 폴더 및 Secure Zone을(를) 제외한 모든 백업 위치를 지원합니다.

정리 계획을 만들려면

1. Cyber Protect 콘솔에서 **관리** > **정리**를 클릭합니다.
2. **계획 생성**을 클릭합니다.
3. **에이전트**에서 정리를 수행할 에이전트를 선택합니다.
   백업 위치에 액세스할 수 있는 모든 에이전트를 선택할 수 있습니다.
4. **정리할 항목**에서 정리할 아카이브나 백업 위치를 선택합니다.
   아카이브와 위치 간을 전환하려면 오른쪽 위에 있는 **위치 / 백업** 스위치를 사용합니다.
   암호화된 아카이브 여러 개를 선택하는 경우에는 아카이브의 암호화 비밀번호가 동일해야 합니다. 다른 암호화 비밀번호를 사용하는 아카이브의 경우 개별 계획을 생성합니다.
5. **스케줄**에서 정리 스케줄을 구성합니다.
6. **보존 규칙**에서 보존 규칙을 지정합니다.
   다음 옵션을 사용할 수 있습니다.
   - **백업 수별**
   - **백업 기간별**(월별, 주간, 일간, 매시간 백업용으로 각기 별도의 설정 사용 가능)
   - **백업의 총 크기 기준**
7. [**복제할 항목**에서 암호화된 아카이브를 선택한 경우] **백업 비밀번호** 스위치를 활성화하고 암호화 비밀번호를 입력합니다.
8. [선택 사항] 계획 옵션을 수정하려면 기어 아이콘을 클릭하고 옵션을 필요한 대로 구성합니다.
9. **생성**을 클릭합니다.

가상 머신으로 전환

가상 머신으로 변환은 디스크 수준 백업에만 사용할 수 있습니다. 백업에 시스템 볼륨과 운영 체제를 시작하는 데 필요한 모든 정보가 포함되어 있는 경우 결과 가상 머신이 자체적으로 시작될 수 있습니다. 그렇지 않으면 가상 디스크를 다른 가상 머신에 추가해도 됩니다.

참고
기본 Scale Computing VM 복제 기능을 통해 복제된 VM은 백업할 수 없습니다.

© Acronis International GmbH, 2003-2024

가상 머신으로 전환을 위한 별도의 계획을 생성하고, 이 계획을 수동으로 또는 스케줄에 따라 실행할 수 있습니다.

전제조건과 제한 사항에 관한 자세한 내용은 "변환에 대해서 알아야 할 사항"(197페이지)을(를) 참조하십시오.

참고
이 기능은 Advanced Backup 팩 내에서 **Advanced Backup – 서버** 또는 **Advanced Backup – NAS** 할당량이 활성화되어 있는 고객 테넌트에서 사용 가능합니다.

가상 머신으로 전환을 위한 계획 생성

1. **관리** > **VM으로 변환**을 클릭합니다.
2. **계획 생성**을 클릭합니다.
   소프트웨어에 새 계획 템플릿이 표시됩니다.
3. [선택 사항] 계획 이름을 수정하려면 기본 이름을 클릭합니다.
4. **변환 대상**에서 대상 가상 머신의 유형을 선택합니다. **다음 중 하나를 선택할 수 있습니다.**
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **Scale Computing HC3**
   - **VMware Workstation**
   - **VHDX 파일**

   참고
   스토리지 공간을 절약하기 위해 VHDX 파일이나 VMware Workstation으로 변환할 때마다 대상 위치에서 이전 변환 시 생성된 VHDX/VMDK 파일을 덮어씁니다.

5. 다음 중 하나를 수행하십시오.
   - [VMware ESXi, Hyper-V 및 Scale Computing HC3] **호스트**를 클릭하고 대상 호스트를 선택한 후 새 머신 이름 템플릿을 지정합니다.
   - [기타 가상 머신 유형] **경로**에서 가상 머신 파일 및 파일 이름 템플릿을 저장할 위치를 지정합니다.

   기본 이름은 **[머신 이름]_converted**입니다.
6. **에이전트**를 클릭하고 변환을 수행할 에이전트를 선택합니다.
7. **변환할 항목**을 클릭한 다음 이 계획에서 가상 머신으로 변환할 백업을 선택합니다.
   오른쪽 위에 있는 **위치 / 백업** 스위치를 사용하여 백업 선택과 전체 위치 선택 간에 전환할 수 있습니다.
   선택한 백업이 암호화되어 있는 경우 모든 백업이 같은 암호화 비밀번호를 사용해야 합니다. 다른 암호화 비밀번호를 사용하는 백업의 경우 개별 계획을 생성합니다.
8. [VMware ESXi 및 Hyper-V에만 해당] ESXi의 경우 **데이터 저장소** 또는 Hyper-V의 경우 **경로**를 클릭한 다음 가상 머신의 데이터 저장소(스토리지)를 선택합니다.
9. [VMware ESXi 및 Hyper-V에만 해당됨] 디스크 프로비저닝 모드를 선택합니다. 기본 설정은 **씬**(VMware ESXi) 및 **동적 확장**(Hyper-V)입니다.

© Acronis International GmbH, 2003-2024

10. [선택 사항] [VMware ESXi, Hyper-V 및 Scale Computing HC3] **VM 설정**을 클릭해 메모리 크기, 프로세서 수 또는 가상 머신의 네트워크 연결을 수정합니다.
11. [선택 사항] **스케줄**을 클릭하고 스케줄을 변경합니다.
12. **변환할 항목**에서 선택한 백업이 암호화되면 **백업 비밀번호** 스위치를 활성화하고 암호화 비밀번호를 입력합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
13. [선택 사항] 계획 옵션을 수정하려면 기어 아이콘을 클릭합니다.
14. **생성**을 클릭합니다.

변환에 대해서 알아야 할 사항

지원되는 가상 머신 유형

가상 머신으로의 백업 변환은 백업을 생성한 같은 에이전트나 다른 에이전트를 통해 수행할 수 있습니다.

VMware ESXi, Hyper-V 또는 Scale Computing HC3로의 변환을 수행하려면 ESXi, Hyper-V 또는 Scale Computing HC3 호스트와 이 호스트를 관리하는 보호 에이전트(Agent for VMware, Agent for Hyper-V 또는 Agent for Scale Computing HC3)가 필요합니다.

VHDX 파일로의 변환은 파일이 가상 디스크로 Hyper-V 가상 머신에 연결된다고 가정합니다.

VM으로 변환 작업을 통해 생성할 수 있는 가상 머신의 유형이 아래 표에 요약되어 있습니다. 표의 행에 변환된 가상 머신 유형이 나와 있습니다. 표의 열에는 변환을 수행하는 에이전트가 나와 있습니다.

VM 유형	Agent for VMware	Agent for Hyper-V	Agent for Windows	Agent for Linux	Agent for Mac	Agent for Scale Computing HC3	Agent for oVirt (KVM)	Agent for Virtuozzo Hybrid Infrastructure	Agent for Virtuozzo
VMware ESXi	+	–	–	–	–	–	–	–	–
Microsoft Hyper-V	–	+	–	–	–	–	–	–	–
VMware 워크스테이션	+	+	+	+	–	–	–	–	–
VHDX 파일	+	+	+	+	–	–	–	–	–

© Acronis International GmbH, 2003-2024

Scale Computing HC3	–	–	–	–	–	+	–	–	–

제한 사항

- NFS에 저장된 백업은 변환할 수 없습니다.
- Secure Zone에 저장되어 있는 백업은 같은 머신에서 실행 중인 에이전트를 통해서만 변환할 수 있습니다.
- Linux 논리 볼륨(LVM)을 포함하고 있는 백업은 Agent for VMware, Agent for Hyper-V 및 Agent for Scale Computing HC3에서 생성되었으며 같은 하이퍼바이저로 전송하는 경우에만 변환 가능합니다. 크로스 하이퍼바이저 변환이 지원되지 않습니다.
- Windows 머신의 백업을 VMware Workstation 또는 VHDX 파일로 변환할 때에는 나머지 가상 머신이 변환을 수행하는 머신으로부터 CPU 유형을 상속합니다. 결국, 해당하는 CPU 드라이버가 게스트 운영 체제에 설치됩니다. 다른 CPU 유형의 호스트에서 시작한 경우 게스트 시스템에 드라이버 오류가 표시됩니다. 이 드라이버를 수동으로 업데이트하십시오.

가상 머신으로의 정기적인 변환과 백업에서 가상 머신 실행 비교

두 가지 방법 모두 원래 머신에 장애가 발생하는 경우 몇 초 내로 가상 머신을 시작할 수 있습니다.

가상 머신으로의 정기적인 변환에서는 CPU 및 메모리 리소스를 소비합니다. 가상 머신의 파일은 데이터 저장소(스토리지)의 공간을 일정하게 점유합니다. 운영 호스트를 변환에 사용하는 경우에는 이 방법이 실용적이지 않을 수 있습니다. 하지만 가상 머신 성능은 호스트 리소스만큼으로 제한됩니다.

백업에서 가상 머신을 실행할 때는 가상 머신이 실행될 때만 리소스를 소비합니다. 데이터 저장소(스토리지) 공간은 변경 사항을 가상 디스크에 보관하는 데에만 필요합니다. 하지만 호스트가 가상 디스크에 직접 액세스하지 않고 백업에서 데이터를 읽어오는 에이전트와 통신하기 때문에 가상 머신이 더 느리게 실행됩니다. 또한 가상 머신은 일시적입니다.

가상 머신으로의 정기적인 변환 작동 방식

정기적인 변환의 작동 방식은 가상 머신 생성 위치에 따라 다릅니다.

- **▸가상 머신을 파일 세트로 저장하도록 선택하는 경우:** 변환할 때마다 가상 머신이 처음부터 다시 생성됩니다.
- **가상 머신을 가상화 서버에 생성하도록 선택하는 경우:** 증분 또는 차등 백업을 변환하는 경우 소프트웨어는 가상 머신을 다시 생성하지 않고 기존 가상 머신을 증분 업데이트합니다. 일반적으로 이러한 변환이 속도가 더 빠릅니다. 또한 변환을 수행하는 호스트의 CPU 자원과 네트워크 트래픽을 절약할 수 있습니다. 가상 머신을 업데이트할 수 없으면 소프트웨어가 처음부터 다시 생성합니다.

다음은 두 가지 경우 모두에 대한 자세한 설명입니다.

© Acronis International GmbH, 2003-2024

가상 머신을 파일 세트로 저장하도록 선택하는 경우

처음 변환의 결과로 새로운 가상 머신이 생성됩니다. 모든 후속 변환의 결과로 이 머신은 처음부터 다시 생성됩니다. 우선 기존 머신의 이름을 임시로 바꿉니다. 그러면 이전의 기존 머신 이름을 갖는 새 가상 머신이 생성됩니다. 이 작업이 성공하면 기존 머신이 삭제됩니다. 이 작업이 실패하면 새 머신이 삭제되고 기존 머신 이름으로 이전 이름이 지정됩니다. 이러한 방식으로 항상 하나의 머신으로 변환 작업을 끝낼 수 있지만 기존 머신을 유지하기 위해 변환 도중 추가 저장 공간이 필요합니다.

가상 머신을 가상 서버에 생성하도록 선택하는 경우

최초 변환 시 새 가상 머신이 생성됩니다. 이후 변환은 다음과 같이 수행됩니다.

- 마지막 변환 이후 *전체 백업*이 진행되었다면 가상 머신이 처음부터 다시 생성됩니다(이 섹션의 앞부분 참조).
- 그렇지 않은 경우에는 기존 가상 머신이 마지막 변환 이후 변경 내용을 반영하여 업데이트됩니다. 업데이트가 불가능한 경우에는(예를 들어, 아래와 같이 중간 스냅샷을 삭제한 경우) 가상 머신이 처음부터 다시 생성됩니다.

중간 스냅샷

변환된 가상 머신을 안전하게 업데이트하기 위해 소프트웨어는 해당 머신의 중간 하이퍼바이저 스냅샷을 저장합니다. 이름이 **복제본...**인 이 스냅샷은 보관해 두어야 합니다.

복제본... 스냅샷은 최신 변환의 결과를 나타냅니다.이 스냅샷으로 이동하면 머신을 해당 상태로 되돌릴 수 있습니다(예를 들어, 머신 작업을 수행한 후 머신 변경 사항을 취소하려는 경우).

변환된 Scale Computing HC3 가상 머신의 경우에는 추가 **유틸리티 스냅샷**이 생성됩니다. Cyber Protection 서비스만 해당 스냅샷을 사용합니다.

보호 계획 및 모듈

데이터를 보호하려면 보호 계획을 만든 다음 이를 워크로드에 적용해야 합니다.

보호 계획은 여러 다른 보호 모듈로 구성됩니다. 필요한 모듈을 활성화하고 설정을 구성하여 사용자의 요구 사항을 만족시키는 보호 계획을 생성합니다.

다음과 같은 모듈을 사용할 수 있습니다.

- 백업. 데이터 소스를 로컬 또는 클라우드 스토리지에 백업합니다.
- "재해 복구 구현"(666페이지). 머신의 정확한 복제본을 클라우드 사이트에서 시작하고 손상된 원본 머신에서 클라우드의 복구 서버로 워크로드를 전환합니다.
- 안티바이러스 및 안티맬웨어 보호. 기본으로 제공되는 안티맬웨어 솔루션을 사용해 워크로드를 확인합니다.
- EDR(Endpoint Detection and Response). 워크로드에서 감지되지 않은 공격을 비롯한 의심스러운 활동을 감지하며 인시던트를 생성합니다. 따라서 공격이 발생한 방식 및 공격 재발 방지 방법을 파악할 수 있습니다.

© Acronis International GmbH, 2003-2024

- URL 필터링. 악성 URL과 다운로드 가능한 콘텐츠에 대한 액세스를 차단하여 인터넷에서 발생하는 위협으로부터 머신을 보호합니다.
- Windows Defender Antivirus. Windows Defender Antivirus 설정을 관리해 환경을 보호합니다.
- Microsoft Security Essentials. Microsoft Security Essentials 설정을 관리해 환경을 보호합니다.
- 취약점 평가. Windows, Linux, macOS, Microsoft 제삼자 제품과 머신에 설치된 macOS 서드 파티 제품을 확인하고 취약점에 대해 알려줍니다.
- 패치 관리. Windows, Linux, macOS, Microsoft 서드 파티 제품과 머신에 설치된 macOS 서드 파티 제품용 패치 및 업데이트를 설치해 발견된 취약점을 해결합니다.
- 데이터 보호 맵. 중요한 파일의 보호 상태를 모니터하기 위해 데이터를 검색합니다.
- 장치 제어. 사용자가 머신에서 사용할 수 있거나 사용이 제한되는 장치를 지정합니다.
- Advanced Data Loss Prevention. 데이터 플로우 정책에 따라 주변 장치(예: 프린터 또는 이동식 스토리지) 또는 내부 및 외부 네트워크 전송을 통해 민감한 데이터가 유출되는 것을 방지합니다.

보호 계획 생성

다음과 같은 방법으로 보호 계획을 생성할 수 있습니다.

- **장치** 탭에서 보호할 워크로드를 하나 이상 선택한 후 이들에 대한 보호 계획을 생성합니다.
- **관리** > **보호 계획** 탭의 경우. 보호 계획을 생성한 후, 계획을 적용할 워크로드를 하나 이상 선택합니다.

보호 계획을 생성할 때 해당 워크로드 유형에 적용 가능한 모듈만 표시됩니다.

보호 계획을 하나 이상의 워크로드에 적용할 수 있습니다. 또한 같은 워크로드에 여러 보호 계획을 적용할 수 있습니다. 발생할 수 있는 충돌에 대한 자세한 정보는 "계획 충돌 해결"(205페이지)을(를) 참조하십시오.

보호 계획을 만들려면

장치

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 보호하려는 워크로드를 선택하고 **보호**를 클릭합니다.
3. [이미 적용된 계획이 있는 경우] **계획 추가**를 클릭합니다.
4. **계획 생성** > **보호**를 클릭합니다.
   보호 계획 패널이 열립니다.
5. [선택 사항] 보호 계획의 이름을 변경하려면 연필 아이콘을 클릭하고 새 이름을 입력하십시오.
6. [선택 사항] 계획에서 모듈을 활성화/비활성화하려면 모듈 이름 옆의 스위치를 토글합니다.
7. [선택 사항] 모듈을 구성하려면 모듈을 클릭해 확장한 후 필요에 따라 구성을 변경합니다.
8. 준비가 되면 **생성**을 클릭합니다.

참고
암호화가 적용된 보호 계획을 생성하려면 암호화 비밀번호를 지정합니다. 자세한 정보는 "암호화"(402페이지)을(를) 참조하십시오.

© Acronis International GmbH, 2003-2024

관리 > 보호 계획

1. Cyber Protect 콘솔에서 **관리** > **보호 계획**으로 이동합니다.
2. **계획 생성**을 클릭합니다.
   보호 계획에 대한 템플릿이 열립니다.
3. [선택 사항] 보호 계획의 이름을 변경하려면 연필 아이콘을 클릭하고 새 이름을 입력하십시오.
4. [선택 사항] 계획에서 모듈을 활성화/비활성화하려면 모듈 이름 옆의 스위치를 토글합니다.
5. [선택 사항] 모듈을 구성하려면 모듈을 클릭해 확장한 후 필요에 따라 구성을 변경합니다.
6. [선택 사항] 계획을 적용할 워크로드를 선택하려면 **장치 추가**를 클릭합니다.

   참고
   워크로드에 이를 적용하지 않고 계획을 생성할 수 있습니다. 계획을 편집하여 나중에 워크로드를 추가할 수 있습니다. 계획에 워크로드를 추가하는 방법에 대한 자세한 정보는 "워크로드에 보호 계획 적용"(202페이지)을(를) 참조하십시오.

7. 준비가 되면 **생성**을 클릭합니다.

   참고
   암호화가 적용된 보호 계획을 생성하려면 암호화 비밀번호를 지정합니다. 자세한 정보는 "암호화"(402페이지)을(를) 참조하십시오.

백업, **안티바이러스 및 안티맬웨어 보호**, **취약점 평가**, **패치 관리** 또는 **데이터 보호 맵** 모듈을 온디맨드 방식으로 실행하려면 **지금 실행**을 클릭합니다.

첫 번째 보호 계획 생성하기 교육 동영상을 시청하십시오.

재해 복구 모듈에 대한 자세한 정보는 "재해 복구 보호 계획 생성"(671페이지)을(를) 참조하십시오.

장치 제어 모듈에 대한 자세한 정보는 "장치 제어 모듈 사용"(332페이지)을(를) 참조하십시오.

보호 계획이 있는 작업

보호 계획을 생성한 후 다음과 같은 작업을 수행할 수 있습니다.

- 워크로드 또는 장치 그룹에 계획을 적용합니다.
- 계획 이름을 바꾸십시오.
- 계획을 편집합니다.
  계획에 포함된 모듈을 활성화/비활성화하거나 설정을 변경할 수 있습니다.
- 계획을 활성화/비활성화합니다.
  비활성화된 계획은 적용된 워크로드에서 수행되지 않습니다.
  이 작업은 이후에 동일한 계획으로 동일한 워크로드를 보호하려는 경우 편리합니다. 계획은 장치에서 해지되지 않으며, 다시 계획을 활성화하여 보호 기능을 빠르게 복원할 수 있습니다.
- 워크로드에서 계획을 해지합니다.
  해지된 계획은 더 이상 워크로드에 적용되지 않습니다.

© Acronis International GmbH, 2003-2024

이 작업은 이후에 동일한 계획으로 동일한 워크로드를 빠르게 보호할 필요가 없는 관리자에게 편리합니다. 해지된 계획이 제공하는 보호를 복원하려면 이 계획의 이름을 파악하고 사용 가능한 계획 목록에서 선택한 다음 해당 장치에 다시 적용해야 합니다.

- 계획 중지.
  이 작업을 수행하면 계획이 적용된 모든 워크로드에서 실행 중인 백업 작업이 모두 중지됩니다. 백업이 계획 스케줄에 따라 다시 시작됩니다.
  안티맬웨어 스캐닝은 이 작업의 영향을 받지 않으며 구성된 스케줄에 따라 진행됩니다.
- 계획을 복제합니다.
  기존 계획의 정확한 복제본을 생성할 수 있습니다. 새로운 계획은 어떤 워크로드에도 할당되지 않습니다.
- 계획을 내보내고 가져옵니다.
  나중에 다시 가져올 수 있는 JSON 파일 형식으로 계획을 내보낼 수 있습니다. 따라서 수동으로 새로운 계획을 생성하고 설정할 필요가 없습니다.

참고
Cyber Protection 9.0(2020년 3월 릴리스) 이상에서 생성된 보호 계획을 가져올 수 있습니다.이전 버전에서 생성된 계획은 Cyber Protection 9.0 이상과 호환되지 않습니다.

- 계획의 상세정보를 확인합니다.
- 계획과 관련된 작업과 경보를 확인합니다.
- 계획을 삭제합니다.

워크로드에 보호 계획 적용

워크로드를 보호하려면 보호 계획을 적용해야 합니다.

장치 탭에서 계획을 적용할 수 있고, **관리** > **보호 계획** 탭에서 계획을 적용할 수 있습니다.

장치

1. 보호할 워크로드를 하나 이상 선택합니다.
2. **보호**를 클릭합니다.
3. [선택한 워크로드에 이미 보호 계획이 적용되어 있는 경우] **계획 추가**를 클릭합니다.
4. 사용 가능한 보호 계획 목록이 표시됩니다.
5. 적용할 보호 계획을 선택한 후 **적용**을 클릭합니다.

관리 > 보호 계획

1. Cyber Protect 콘솔에서 **관리** > **보호 계획**으로 이동합니다.
2. 적용할 보호 계획을 선택합니다.
3. **편집**을 클릭합니다.
4. **장치 관리**를 클릭합니다.
5. **장치** 창에서 **추가**를 클릭합니다.
6. 계획을 적용할 워크로드를 선택한 후 **추가**를 클릭합니다.

© Acronis International GmbH, 2003-2024

7. **장치** 창에서 **완료**를 클릭합니다.
8. 보호 계획 패널에서 **저장**을 클릭합니다.

장치 그룹에 보호 계획을 적용하는 방법을 알아보려면 "그룹에 계획 적용"(330페이지)을(를) 참조하십시오.

보호 계획 편집

계획을 편집할 때 계획에 포함된 모듈을 활성화/비활성화하고 설정을 변경할 수 있습니다.

모든 워크로드 또는 선택한 워크로드에 적용할 보호 계획을 편집할 수 있습니다.

장치 탭에서 계획을 편집할 수 있고, **관리** > **보호 계획** 탭에서 계획을 편집할 수 있습니다.

장치

1. 계획을 적용할 워크로드를 하나 이상 선택합니다.
2. **보호**를 클릭합니다.
3. 편집할 보호 계획을 선택합니다.
4. 계획 이름 옆에 있는 말줄임표 아이콘(...)을 클릭한 후 **편집**을 클릭합니다.
5. 편집할 모듈을 클릭한 후 필요한 경우 설정을 구성합니다.
6. **저장**을 클릭합니다.
7. [계획을 적용할 워크로드를 모두 선택하지 않은 경우] 편집 범위를 선택합니다.
   - 적용되는 모든 워크로드에 대한 계획을 편집하려면 **이 보호 계획에 대한 변경 사항 적용(다른 장치에도 영향을 줌)**을 클릭합니다.
   - 선택한 워크로드에 대해서만 계획을 변경하려면 **선택한 장치에 대해서만 새 보호 계획 생성**을 클릭합니다.

     그 결과, 선택한 워크로드에서 기존 계획이 해지됩니다. 사용자가 구성한 새로운 보호 계획이 생성되고 이들 워크로드에 적용됩니다.

관리 > 보호 계획

1. Cyber Protect 콘솔에서 **관리** > **보호 계획**으로 이동합니다.
2. 편집할 보호 계획을 선택합니다.
3. **편집**을 클릭합니다.
4. 편집할 모듈을 클릭한 후 필요한 경우 설정을 구성합니다.
5. **저장**을 클릭합니다.

참고
관리 > **보호 계획** 탭에서 계획을 편집하면 해당 계획이 적용된 모든 워크로드에 영향을 미칩니다.

보호 계획 해지

계획을 해지할 때 하나 이상의 워크로드에서 계획을 제거합니다. 계획이 적용되는 다른 워크로드를 계속 보호합니다.

장치 탭에서 계획을 취소할 수 있고, **관리** > **보호 계획** 탭에서 계획을 취소할 수 있습니다.

장치

© Acronis International GmbH, 2003-2024

1. 계획을 해지할 워크로드를 선택합니다.
2. **보호**를 클릭합니다.
3. 해지할 보호 계획을 선택합니다.
4. 계획 이름 옆에 있는 말줄임표 아이콘(...)을 클릭한 후 **해지**를 클릭합니다.

관리 > 보호 계획

1. Cyber Protect 콘솔에서 **관리** > **보호 계획**으로 이동합니다.
2. 해지할 보호 계획을 선택합니다.
3. **편집**을 클릭합니다.
4. **장치 관리**를 클릭합니다.
5. **장치** 창에서 계획을 해지할 워크로드를 선택합니다.
6. **제거**를 클릭합니다.
7. **장치** 창에서 **완료**를 클릭합니다.
8. 보호 계획 템플릿에서 **저장**을 클릭합니다.

보호 계획 활성화/비활성화

활성화된 계획이 활성 상태이며, 적용되는 워크로드에서 실행됩니다. 비활성화된 계획이 비활성 상태이며, 여전히 워크로드에 적용되지만 실행되고 있지는 않습니다.

장치 탭에서 보호 계획을 활성화/비활성화하면 해당 작업은 선택한 워크로드에만 영향을 줍니다.

관리 > **보호 계획** 탭에서 보호 계획을 활성화/비활성화하면 해당 계획이 적용되는 모든 워크로드에 영향을 줍니다. 또한 여러 보호 계획을 활성화/비활성할 수 있습니다.

장치

1. 계획을 비활성화할 워크로드를 선택합니다.
2. **보호**를 클릭합니다.
3. 비활성화할 보호 계획을 선택합니다.
4. 계획 이름 옆에 있는 말줄임표 아이콘(...)을 클릭한 후 **활성화** 또는 **비활성화**를 클릭합니다.

관리 > 보호 계획

1. Cyber Protect 콘솔에서 **관리** > **보호 계획**으로 이동합니다.
2. 활성화/비활성화할 보호 계획을 하나 이상 선택합니다.
3. **편집**을 클릭합니다.
4. **활성화** 또는 **비활성화**를 클릭합니다.

참고
이 작업은 이미 대상 상태인 보호 계획에는 영향을 주지 않습니다. 예를 들어 사용자가 활성화 상태인 계획과 비활성화 상태인 계획을 모두 선택하고 **활성화**를 클릭하면 선택한 모든 계획이 활성화됩니다.

보호 계획 삭제

계획을 삭제하면 모든 워크로드에서 계획이 해지되며 Cyber Protect 콘솔에서 제거됩니다.

© Acronis International GmbH, 2003-2024

장치 탭에서 계획을 삭제할 수 있고, **관리** > **보호 계획** 탭에서 계획을 삭제할 수 있습니다.

장치

1. 삭제할 보호 계획이 적용된 워크로드를 선택합니다.
2. **보호**를 클릭합니다.
3. 삭제할 보호 계획을 선택합니다.
4. 계획 이름 옆에 있는 말줄임표 아이콘(...)을 클릭한 후 **삭제**를 클릭합니다.

관리 > 보호 계획

1. Cyber Protect 콘솔에서 **관리** > **보호 계획**으로 이동합니다.
2. 삭제할 보호 계획을 선택합니다.
3. **삭제**를 클릭합니다.
4. **계획 삭제를 확인했습니다** 확인란을 선택하여 선택 사항을 확인한 후 **삭제**를 클릭합니다.

계획 충돌 해결

하나의 워크로드에 여러 개의 보호 계획을 적용할 수 있습니다. 예를 들어 어떤 보호 계획에서는 **안티바이러스 및 안티맬웨어** 모듈만 활성화하고 구성하여 적용하고 다른 보호 계획에서는 **백업** 모듈만 활성화하고 구성하여 적용할 수 있습니다.

서로 다른 모듈을 활성화한 보호 계획을 결합시킬 수 있습니다. **백업** 모듈만 활성화된 여러 보호 계획을 결합시킬 수도 있습니다. 하지만 하나 이상의 계획에서 다른 모듈이 활성화되는 경우 충돌이 발생합니다. 계획을 적용하려면 우선 충돌을 해결해야 합니다.

기존 계획과 새 계획 사이의 충돌

새 계획과 기존 계획이 충돌하는 경우 다음 중 한 가지 방법을 사용해 충돌을 해결할 수 있습니다.

- 새 계획을 생성하고 적용한 후 새 계획과 충돌을 일으키는 기존 계획을 비활성화합니다.
- 새로운 계획을 생성하고 비활성화합니다.

개별 및 그룹 계획 사이의 충돌

개별 보호 계획이 장치 그룹에 적용된 그룹 계획과 충돌을 일으키는 경우 다음 중 한 가지 방법을 사용해 충돌을 해결할 수 있습니다.

- 장치 그룹에서 워크로드를 제거한 후 개별 보호 계획을 적용합니다.
- 기존 그룹 계획을 편집하거나 장치 그룹에 새 그룹 계획을 적용합니다.

라이센스 문제

보호 계획 모듈은 보호된 워크로드에 특정 서비스 할당량이 할당되도록 요구할 수 있습니다. 할당된 서비스 할당량이 적절하지 않은 경우, 해당 모듈이 활성화된 보호 계획을 실행하거나, 업데이트하거나, 적용할 수 없습니다.

라이선스 문제를 해결하려면 다음 중 하나를 수행합니다.

© Acronis International GmbH, 2003-2024

- 현재 할당된 서비스 할당량이 지원하지 않는 모듈을 비활성화한 다음, 보호 계획을 계속 사용합니다.
- 할당된 서비스 할당량을 수동으로 변경하십시오. 이 방법을 배우려면 "머신의 서비스 할당량 변경"(171페이지)을(를) 참조하십시오.

기본 보호 계획

기본 보호 계획은 신속한 보호를 위해 워크로드에 적용할 수 있는 사전 구성된 템플릿입니다. 기본 보호 계획을 사용할 때는 새 보호 계획을 처음부터 생성하지 않아도 됩니다.

기본 보호 계획을 처음 적용하면 템플릿이 테넌트에 복사되며, 계획의 모듈과 모듈 설정을 편집할 수 있습니다.

사용할 수 있는 기본 계획은 다음과 같습니다.

- Cyber Protect Essentials

  기본적인 보호 기능과 파일 수준 백업 기능을 제공하는 계획입니다.
- 원격 작업자

  이 계획은 원격으로 작업하는 사용자에게 최적화되어 있습니다. 자주 사용하는 작업(예: 백업, 안티맬웨어 보호, 취약점 평가), 더 엄격한 보호 작업, 그리고 최적화된 성능 및 전원 옵션을 제공합니다.
- 사무실 작업자(타사 바이러스 백신)

  이 계획은 사무실에서 작업하며 타사 안티바이러스 소프트웨어를 사용하도록 기본 설정한 사용자에게 최적화되어 있습니다. 이 계획에서는 **안티바이러스 및 안티맬웨어 보호 기능** 모듈이 비활성화됩니다.
- 사무실 작업자(Acronis 안티바이러스)

  이 계획은 사무실에서 작업하며 Acronis 안티바이러스 소프트웨어를 사용하도록 기본 설정한 사용자에게 최적화되어 있습니다.

기본 보호 계획 비교

모듈 및 옵션	기본 보호 계획			
	Cyber Protect Essentials	**원격 작업자**	**사무실 작업자(타사 바이러스 백신)**	**사무실 작업자 (Acronis 안티바이러스)**
백업	사용 가능	사용 가능	사용 가능	사용 가능
백업 대상 백업할 항목	파일/폴더 [모든 프로필 폴더]	전체 머신	전체 머신	전체 머신
지속적인 데이터 보호(CDP)	비활성화됨	활성화됨	비활성화됨	비활성화됨
백업 위치	클라우드 스토리지	클라우드 스토리지	클라우드 스토리지	클라우드 스토리지

© Acronis International GmbH, 2003-2024

모듈 및 옵션	기본 보호 계획			
	Cyber Protect Essentials	**원격 작업자**	**사무실 작업자(타사 바이러스 백신)**	**사무실 작업자 (Acronis 안티바이러스)**
예약	월요일~금요일, 오후 11시	월요일~금요일 오전 12시 추가로 활성화된 옵션 및 시작 조건: • 머신이 꺼진 경우 머신 시작 시 누락된 작업 실행 • 절전 또는 최대 절전 모드에서 깨어나 예약된 백업 시작 • 배터리 전원 절약: 배터리 사용 시에는 시작하지 않음 • 데이터 요금제 사용 시 시작하지 않음	월요일~금요일, 오후 11시	월요일~금요일, 오후 11시
백업 구성표	항상 증분	항상 증분	항상 증분	항상 증분
보관 기간	무한히 백업 보관	월간: 12개월 주간: 4주 일일: 7일	월간: 12개월 주간: 4주 일일: 7일	월간: 12개월 주간: 4주 일일: 7일
백업 옵션	기본 옵션	기본 옵션, 그리고: • 성능 및 백업 할당 시간(초록색 세트): CPU 우선 순위: 낮음 출력 속도: 50%	기본 옵션	기본 옵션
안티바이러스 및 안티맬웨어 보호 기능	사용 가능	사용 가능	사용할 수 없음	사용 가능
Active	끄기	끄기	–	끄기

© Acronis International GmbH, 2003-2024

모듈 및 옵션	기본 보호 계획			
	Cyber Protect Essentials	**원격 작업자**	**사무실 작업자(타사 바이러스 백신)**	**사무실 작업자 (Acronis 안티바이러스)**
Protection				
고급 안티맬웨어	켜기	켜기	–	켜기
네트워크 폴더 보호	켜기	켜기	–	켜기
서버측 보호	끄기	끄기	–	끄기
자체 보호	켜기	켜기	–	켜기
크립토마이닝 프로세스 감지됨	켜기	켜기	–	켜기
격리	30일 후 후에 격리된 파일 제거	30일 후 후에 격리된 파일 제거	–	30일 후 후에 격리된 파일 제거
동작 엔진	격리	격리	–	격리
악용 방지	프로세스 알림 및 중지	프로세스 알림 및 중지	–	프로세스 알림 및 중지
실시간 보호	격리	격리	–	격리
스캔 예약	빠른 스캔: 격리 일요일~토요일, 오후 2시 20분 전체 스캔: 끄기	빠른 스캔: 끄기 전체 스캔: 격리 일요일~토요일, 오후 1시 55분 추가로 활성화된 옵션 및 시작 조건: • 머신이 꺼진 경우 머신 시작 시 누락된 작업 실행 • 절전 또는 최대 절전 모드에서 깨어나 예약된 백업 시작 • 배터리 전원 절약: 배터리 사용 시에는 시작하지	–	빠른 스캔: 격리 일요일~토요일, 오후 2시 20분 전체 스캔: 끄기

© Acronis International GmbH, 2003-2024

모듈 및 옵션	기본 보호 계획			
	Cyber Protect Essentials	**원격 작업자**	**사무실 작업자(타사 바이러스 백신)**	**사무실 작업자 (Acronis 안티바이러스)**
		않음		
제외	없음	없음	–	없음
URL 필터링	사용 가능	사용 가능	사용 가능	사용 가능
악성 웹사이트 액세스	항상 사용자에게 확인	차단	항상 사용자에게 확인	항상 사용자에게 확인
필터링할 카테고리	기본 옵션	기본 옵션	기본 옵션	기본 옵션
제외	없음	없음	없음	없음
취약성 평가	사용 가능	사용 가능	사용 가능	사용 가능
취약성 평가 범위	Microsoft 제품, Windows 서드 파티 제품	Microsoft 제품, Windows 서드 파티 제품	Microsoft 제품, Windows 서드 파티 제품	Microsoft 제품, Windows 서드 파티 제품
예약	월요일, 오후 1시 15분	월요일, 오후 2시 20분	월요일, 오후 1시 15분	월요일, 오후 1시 15분
패치 관리	사용 가능	사용 가능	사용 가능	사용 가능
Microsoft 제품	모두 업데이트	모두 업데이트	모두 업데이트	모두 업데이트
Windows 서드 파티 제품	대규모 업데이트만	대규모 업데이트만	대규모 업데이트만	대규모 업데이트만
예약	월요일, 오후 3시 10분	월요일~금요일, 오후 2시 20분	월요일, 오후 3시 10분	월요일, 오후 3시 10분
업데이트 전 백업	끄기	켜기	끄기	끄기
데이터 보호 맵	사용할 수 없음	사용 가능	사용 가능	사용 가능
확장자 및 예외 규칙	–	기본 옵션 및 다음 추가 확장: **이미지** • .jpeg • .jpg • .png	기본 옵션(감지할 확장자 66개)	기본 옵션(감지할 확장자 66개)

© Acronis International GmbH, 2003-2024

모듈 및 옵션	기본 보호 계획			
	Cyber Protect Essentials	원격 작업자	사무실 작업자(타사 바이러스 백신)	사무실 작업자 (**Acronis** 안티바이러스)
		• .gif • .bmp • .ico • .wbmp • .xcf • .psd • .tiff • .dwg 오디오 및 비디오 • .avi • .mov • .mpeg • .mpg • .mkv • .wav • .aif • .aifc • .aiff • .au • .snd • .mid • .midi • .mpga • .mp3 • .oga • .flac • .opus • .spx • .ogg • .ogx • .mp4		
예약	–	월요일~금요일, 오후 3시 35분	월요일~금요일, 오후 3시 40분	월요일~금요일, 오후 3시 40분

참고

기본 보호 계획에 포함되는 모듈 수는 Cyber Protection 라이선스에 따라 다를 수 있습니다.

© Acronis International GmbH, 2003-2024

기본 보호 계획 적용

초기 기본 보호 계획은 설정을 편집할 수 없는 템플릿입니다. 기본 계획을 처음 적용하면 템플릿이 사전 구성된 보호 계획으로 테넌트에 복사되며 선택한 워크로드에서 활성화됩니다.

보호 계획은 **관리** > **보호 계획** 탭에 표시되며, 그러면 해당 탭에서 보호 계획을 관리할 수 있습니다.

기본 보호 계획을 처음으로 적용하려면

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 보호할 워크로드를 선택합니다.
3. **보호**를 클릭합니다.
4. 기본 계획 한 가지를 선택한 후 **적용**을 클릭합니다.

기본 보호 계획 편집

기본 보호 계획은 처음으로 적용한 후에 편집할 수 있습니다.

적용한 기본 보호 계획을 편집하려면

1. Cyber Protect 콘솔에서 **관리** > **보호 계획**으로 이동합니다.
2. 편집할 계획을 선택한 다음 **편집**을 클릭합니다.
3. 이 계획에 포함된 모듈을 수정하거나 그 옵션을 수정하고, **저장**을 클릭합니다.

중요
수정할 수 없는 옵션도 있습니다.

호스팅 제어판 통합용 개별 보호 계획

DirectAdmin, cPanel 또는 Plesk를 사용하는 웹 호스팅 서버에서 호스팅 제어판 통합을 활성화하면 Cyber Protection 서비스가 각 워크로드용으로 사용자 계정에 개별 보호 계획을 자동으로 생성합니다. 이 보호 계획은 보호 계획 생성을 시작한 특정 워크로드와 연결되며 해지하거나 다른 워크로드에 할당할 수는 없습니다.

개별 보호 계획 사용을 중지하려는 경우 Cyber Protect 콘솔에서 해당 계획을 삭제하면 됩니다. 개별 보호 계획은 이름 옆의 기호로 식별 가능합니다.

보호 계획이 호스팅 제어판 통합을 사용하는 여러 웹 호스팅 서버를 보호하도록 하려는 경우에는 Cyber Protect 콘솔에서 일반 보호 계획을 생성한 후 이러한 워크로드를 해당 보호 계획에 할당하면 됩니다. 그러나 여러 웹 호스팅 제어판이 공유하는 보호 계획의 수정 사항은 통합 내에서는 적용할 수 없으며 Cyber Protect 콘솔에서만 적용할 수 있습니다.

머신별 #CyberFit Score

#CyberFit Score는 머신의 보안 상태를 평가하는 보안 평가 및 점수 메커니즘을 제공합니다. IT 환경의 보안 격차와 엔드포인트에 대한 공격 가능 요소를 확인하며, 개선을 위한 권장 사항을 보고서

© Acronis International GmbH, 2003-2024

형식으로 제공합니다. 이 기능은 모든 Cyber Protect 버전에서 사용할 수 있습니다.

#CyberFit Score 기능을 지원하는 버전:

- Windows 7(첫 번째 버전) 이상 버전
- Windows Server 2008 R2 이상 버전

작동법

머신에 설치되어 있는 보호 에이전트가 머신의 보안 평가를 수행하고, #CyberFit Score를 계산합니다. 머신의 #CyberFit Score는 일정 기간마다 자동으로 다시 계산됩니다.

#CyberFit Score 책정 메커니즘

머신의 #CyberFit Score는 다음 메트릭을 기준으로 계산됩니다.

- 맬웨어 방지 기능 0-275
- 백업 보호 0-175
- 방화벽 0-175
- 가상 개인 네트워크(VPN) 0-75
- 전체 디스크 암호화 0-125
- 네트워크 보안 0-25

머신의 최대 #CyberFit Score는 850점입니다.

미터법	무엇을 평가합니까?	사용자에 대한 권장 사항	점수 책정
맬웨어 방지	에이전트가 맬웨어 방지 소프트웨어가 머신에 설치되어 있는지 확인합니다.	결과: • 맬웨어 방지 기능이 활성화되어 있습니다(+275포인트) • 맬웨어 방지 기능이 없어 시스템이 위험해질 수 있습니다(0포인트) #CyberFit Score에서 제공한 권장 사항: 보안 위험으로부터 시스템을 보호하려면 맬웨어 방지 솔루션이 설치 및 활성화되어 있어야 합니다. AV-Test 또는 AV-Comparatives 등의 웹사이트에서 권장되는 맬웨어 방지 솔루션 목록을 참고하십시오.	275 - 맬웨어 방지 소프트웨어가 머신에 설치되어 있습니다 0 - 맬웨어 방지 소프트웨어가 머신에 설치되어 있지 않습니다
백업	에이전트는 백업 솔루션이 머신에 설치되어 있는지 확인합니다.	결과: • 데이터를 보호하는 백업 솔루션이 있습니다(+175포인트) • 백업 솔루션이 없기 때문에 데이터가 위험해질 수 있습니다(0포인트) #CyberFit Score에서 제공한 권장 사항: 데이터 손실이나 랜섬웨어 공격을 방지하려면 데이	175 - 백업 솔루션이 머신에 설치되어 있습니다 0 - 백업 솔루션이 머신에 설치되어 있지 않습니다

© Acronis International GmbH, 2003-2024

		터를 정기적으로 백업하는 것이 좋습니다. 아래는 권장되는 백업 솔루션의 예입니다. • Acronis Cyber Protect / Cyber Backup / True Image • Windows Server 백업(Windows Server 2008 R2 이상)	
방화벽	에이전트가 사용자 환경에 방화벽이 지원 및 사용되고 있는지 확인합니다. 에이전트는 다음을 수행합니다. 1. Windows 방화벽 및 네트워크 보호를 통해 공용 방화벽이 사용되고 있는지 확인합니다. 2. Windows 방화벽 및 네트워크 보호를 통해 개인 방화벽이 사용되고 있는지 확인합니다. 3. Windows 공용 및 개인 방화벽이 사용되지 않고 있는 경우 타사 방화벽 솔루션/에이전트가 있는지 확인합니다.	결과: • 공개 및 개인 네트워크에 대해 방화벽이 사용 중이거나 타사 방화벽 솔루션이 있다는 것을 확인했습니다(+175포인트) • 공개 네트워크에 대해서만 방화벽이 사용되고 있습니다(+100포인트) • 개인 네트워크에 대해서만 방화벽이 사용되고 있습니다(+75포인트) • 방화벽이 사용되고 있지 않아 네트워크 연결이 안전하지 않습니다(0포인트) #CyberFit Score에서 제공한 권장 사항: 보안 보호 기능을 개선하여 시스템에 대한 악성 공격을 방어하려면 공개 네트워크와 개인 네트워크 모두에 방화벽을 활성화하는 것이 좋습니다. 보안 요구와 네트워크 아키텍처에 따라 Windows 방화벽을 설정하는 자세한 방법이 아래에 나와 있습니다. 최종 사용자/직원용 가이드: Windows Defender 방화벽을 PC에 설정하는 방법 Windows 방화벽을 PC에 설정하는 방법 시스템 관리자 및 엔지니어용 가이드: 고급 보안 기능을 갖춘 Window Defender 방화벽을 디플로이하는 방법 Windows 방화벽에서 고급 규칙을 생성하는 방법	100 - Windows 공개 방화벽이 활성화되어 있습니다 75 - Windows 개인 방화벽이 활성화되어 있습니다 175 - Windows 공개 및 개인 방화벽이 활성화되어 있습니다 또는 타사 방화벽 솔루션이 활성화되어 있습니다 0 - Windows 방화벽 및 타사 방화벽 솔루션 모두 사용하고 있지 않습니다
가상 개인 네트워크 (VPN)	에이전트가 VPN 솔루션이 머신에 설치되었는지와 VPN이 활성화 및 실행되고 있는지 확인합니다.	결과: • VPN 솔루션이 있어 공개 및 공유 네트워크에서 데이터를 안전하게 받고 보낼 수 있습니다(+75포인트) • VPN 솔루션이 없기 때문에 공개 및 공유 네트워크 연결은 안전하지 않습니다(0포인트) #CyberFit Score에서 제공한 권장 사항: 기업 네트워크 및 기밀 데이터에 액세스할 때에는 VPN을 사용하는 것이 좋습니다. 특히 카페, 도서관, 공항 등의 무료 인터넷 액세스를 이용할 때에는 VPN을 사용하여 커뮤니케이션을 안전하게 기밀로 보호	75 - VPN이 활성화 및 실행되고 있습니다 0 - VPN이 활성화되어 있지 않습니다

© Acronis International GmbH, 2003-2024

		하는 것이 중요합니다. 아래는 권장되는 VPN 솔루션의 예입니다. • Acronis Business VPN • OpenVPN • Cisco AnyConnect • NordVPN • TunnelBear • ExpressVPN • PureVPN • CyberGhost VPN • Perimeter 81 • VyprVPN • IPVanish VPN • Hotspot Shield VPN • Fortigate VPN • ZYXEL VPN • SonicWall GVPN • LANCOM VPN	
디스크 암호화	에이전트가 머신에 디스크 암호화가 활성화되어 있는지 확인합니다. 에이전트가 Windows BitLocker가 켜져있는지 확인합니다.	결과: • 전체 디스크 암호화가 활성화되어 있으며, 물리적인 부당 변경으로부터 장치가 보호되고 있습니다(+125포인트) • 일부 하드 드라이브만 암호화되어 있기 때문에 장치가 물리적인 부당 변경에 위험해질 수 있습니다(+75포인트) • 디스크 암호화가 없기 때문에 장치가 물리적인 부당 변경에 위험해질 수 있습니다(0포인트) #CyberFit Score에서 제공한 권장 사항: Windows BitLocker를 켜서 데이터 및 파일 보호를 강화하는 것이 좋습니다. 가이드: Windows에서 기기 암호화를 켜는 방법	125 - 모든 디스크가 암호화됩니다 75 - 최소 하나의 디스크가 암호화되어 있지만 암호화되지 않은 디스크도 있습니다 0 - 어느 디스크도 암호화되지 않습니다
네트워크 보안(원격 서버로 보내는 NTLM 트래픽)	에이전트가 머신이 원격 서버로 보내는 NTLM 트래픽을 제한하는지 확인합니다.	결과: • 원격 서버로 보내는 NTLM 트래픽이 거부되면 자격 증명이 보호됩니다(+25포인트) • 원격 서버로 보내는 NTLM 트래픽이 거부되지 않으면 자격 증명이 노출에 취약해질 수 있습니다(0포인트) #CyberFit Score에서 제공한 권장 사항: 보안 보호 기능을 강화하려면 원격 서버로 보내는 모든 NTLM 트래픽을 거부하는 것이 좋습니다. NTLM 설	25 - 보내는 NTLM 트래픽이 DenyAll로 설정되어 있습니다 0 - 보내는 NTLM 트래픽이 다른 값으로 설정되어 있습니다

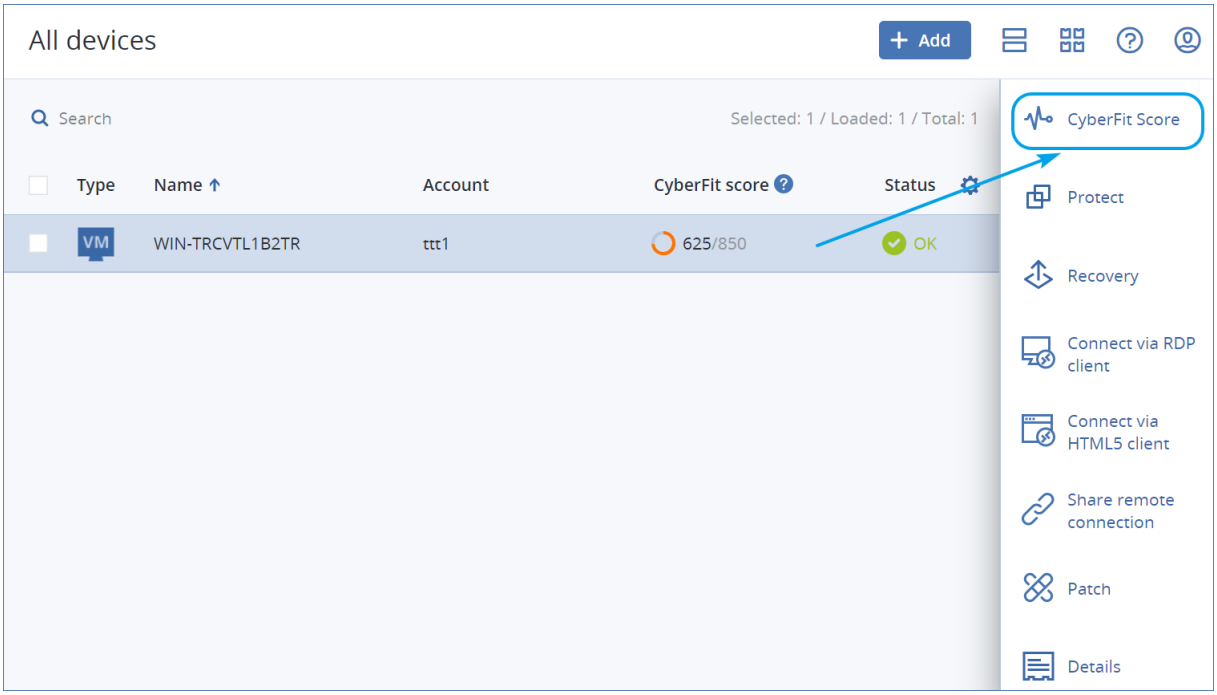
© Acronis International GmbH, 2003-2024

		정 및 예외를 변경하는 방법에 대한 정보는 아래의 링크에서 확인할 수 있습니다. 가이드: 원격 서버로 보내는 NTLM 트래픽 제한	

각 메트릭에 수여된 포인트의 합계를 기반으로 한 머신의 총 #CyberFit Score는 엔드포인트의 보호 수준을 반영하는 다음의 등급으로 구분됩니다.

- 0 - 579 - 나쁨
- 580 - 669 - 보통
- 670 - 739 - 양호
- 740 - 799 - 우수
- 800 - 850 - 최우수

머신의 #CyberFit Score는 Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동하여 확인할 수 있습니다. 장치 목록에서 **#CyberFit Score** 열을 볼 수 있습니다. 또한 #CyberFit Score 스캔을 실행하여 머신의 보안 상태를 확인할 수 있습니다.



해당하는 위젯 및 보고서에서도 #CyberFit Score 정보를 확인할 수 있습니다.

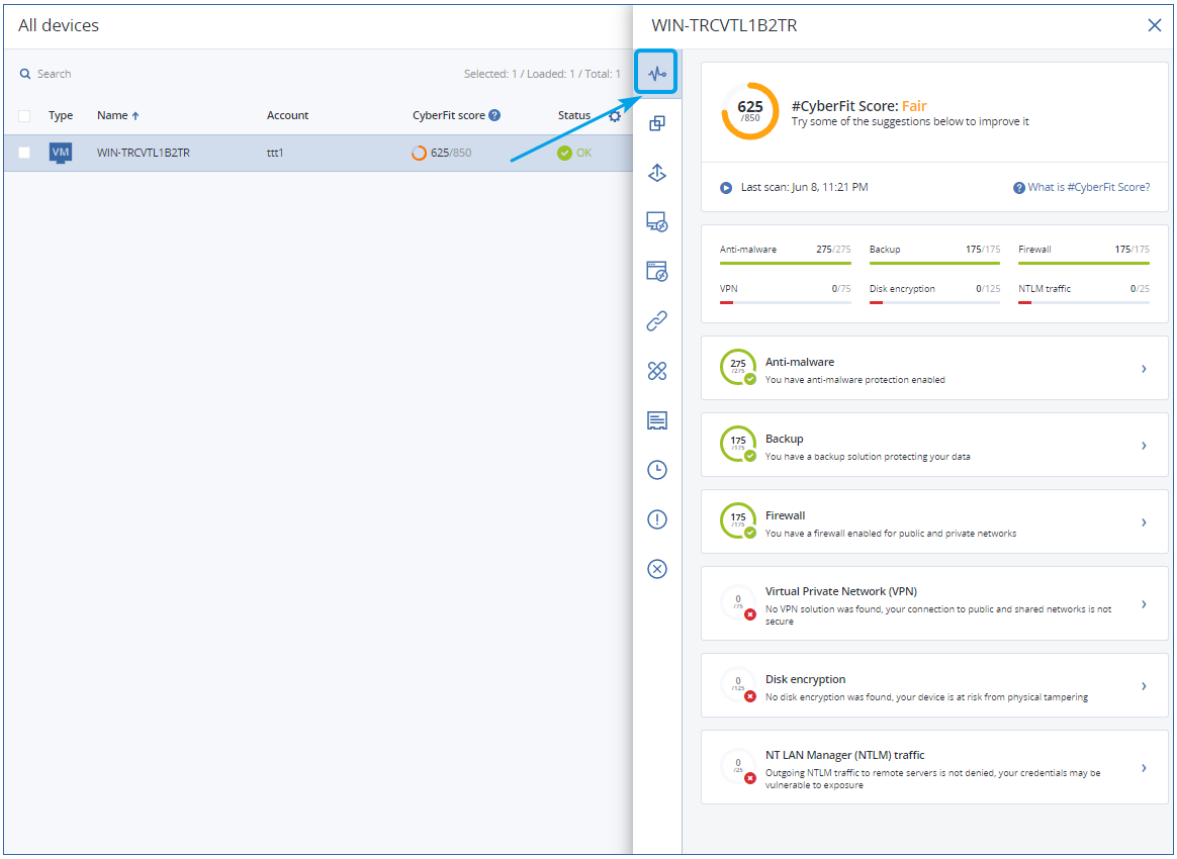
#CyberFit Score 스캔 실행 중

#CyberFit Score 스캔을 실행하려면

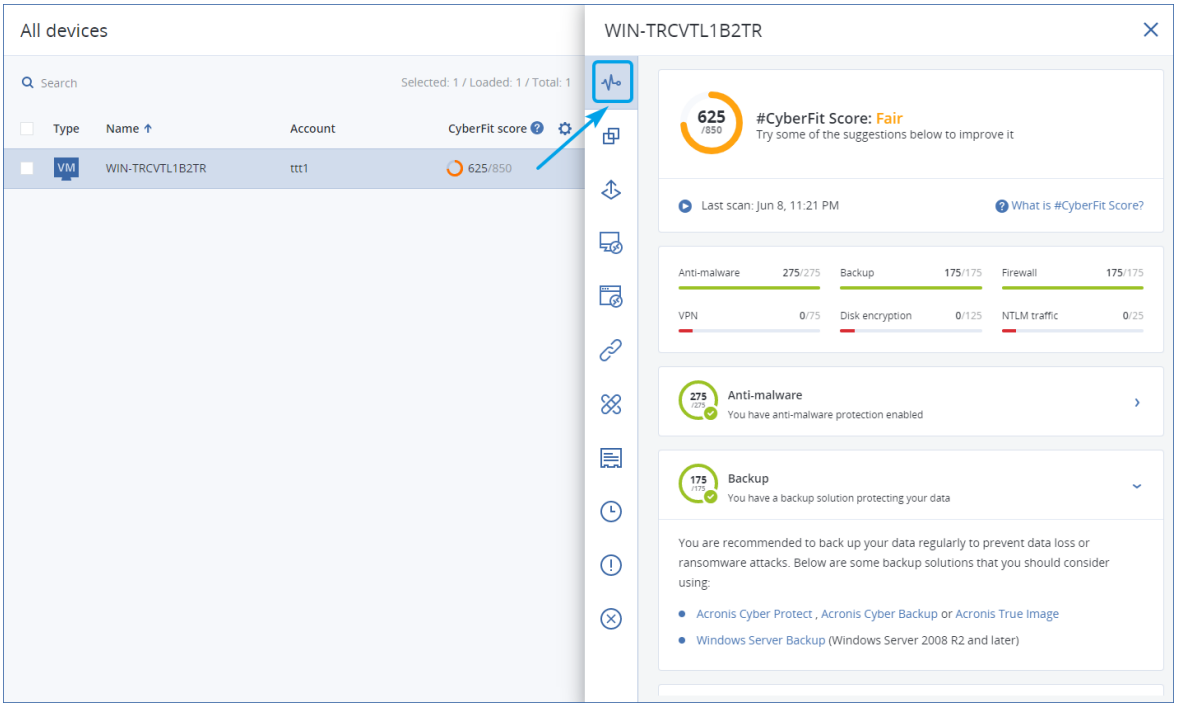
1. Cyber Protect 콘솔에서 **장치**로 이동합니다.
2. 머신을 선택한 다음 **#CyberFit Score**를 클릭합니다.
3. 이전에 머신을 스캔한 적이 없는 경우 **첫 번째 스캔 실행**을 클릭합니다.

© Acronis International GmbH, 2003-2024

4. 스캔이 완료되면 머신의 총 #CyberFit Score와 맬웨어 방지, 백업, 방화벽, VPN, 디스크 암호화 및 NT LAN Manager(NTLM) 트래픽 등 6개의 메트릭 점수를 확인할 수 있습니다.



5. 각 메트릭 점수를 올리고 보안 구성을 개선하는 방법을 확인하려면 해당 섹션을 펼치고 권장 사항을 읽어보십시오.



© Acronis International GmbH, 2003-2024

6. 권장 사항을 수행한 뒤에 총 #CyberFit Score 바로 아래에 있는 화살표 버튼을 클릭해 언제든 머신의 #CyberFit Score를 다시 계산할 수 있습니다.

Cyber Scripting

Cyber Scripting 사용 시에는 Windows 및 macOS 머신에서 스크립트를 사용하여 소프트웨어 설치, 구성 수정, 서비스 시작/중지, 계정 생성 등의 일상적인 작업을 자동화할 수 있습니다. 따라서 이러한 작업의 소요 시간 및 수동으로 해당 작업을 수행하는 경우의 오류 발생 위험성을 줄일 수 있습니다.

고객 수준의 관리자와 사용자 및 파트너 관리자(서비스 제공업체)가 Cyber Scripting을 사용할 수 있습니다. 다양한 관리 수준에 대한 자세한 내용은 "다중 테넌시 지원"(301페이지) 항목을 참조하십시오.

미리 승인을 받은 스크립트만 사용 가능 합니다. **Cyber 관리자** 역할이 할당된 관리자만 새 스크립트를 승인 및 테스트할 수 있습니다. 스크립트 상태 변경에 대한 자세한 내용은 "스크립트 상태 변경"(227페이지) 항목을 참조하십시오.

사용자 역할에 따라 스크립트 및 스크립팅 계획과 관련하여 각기 다른 작업을 수행할 수 있습니다. 역할에 대한 자세한 내용은 "사용자 역할 및 Cyber Scripting 권한"(218페이지) 항목을 참조하십시오.

사전 요구 사항

- Cyber Scripting 기능을 사용하려면 Advanced Management 팩이 필요합니다.
- 스크립트 편집, 스크립트 실행, 스크립팅 계획 생성 등 Cyber Scripting의 모든 기능을 사용하려면 계정에 대해 2단계 인증을 활성화해야 합니다.

제한 사항

- 지원되는 스크립팅 언어는 다음과 같습니다.
  - PowerShell
  - Bash
- Cyber Scripting 작업은 보호 에이전트가 설치되어 있는 대상 머신에서만 실행할 수 있습니다.

지원되는 플랫폼

Cyber Scripting은 Windows 및 macOS 워크로드에 사용 가능합니다.

다음 표에 지원되는 버전이 요약되어 있습니다.

© Acronis International GmbH, 2003-2024

운영 체제	버전
Windows	Windows 7 SP1 이상 - 모든 버전
	Windows 8/8.1 – Windows RT 버전을 제외한 모든 버전(x86, x64)
	Windows 10 - Home, Pro, Education, Enterprise, IoT Enterprise 버전
	Windows 11
	Windows Server 2008 R2 SP1 이상 – Standard, Enterprise, Datacenter, Foundation 및 Web 버전
	Windows Server 2012/2012 R2 – 모든 버전
	Windows Server 2016
	Windows Server 2019
	Windows Server 2022
	Windows Storage Server(2008 R2, 2012, 2012 R2, 2016)
macOS	macOS Mojave 10.14
	macOS Catalina 10.15
	macOS Big Sur 11
	macOS Monterey 12

사용자 역할 및 Cyber Scripting 권한

스크립트 및 스크립팅 계획에 사용할 수 있는 작업은 스크립트 상태 및 사용자의 사용자 역할에 따라 달라집니다.

관리자는 자신의 테넌트 및 하위 테넌트에서 객체를 관리할 수 있습니다. 상위 관리 수준의 객체는 보거나 액세스할 수 없습니다.

하위 관리자는 상위 관리자가 워크로드에 적용한 스크립팅 계획에 대한 읽기 전용 권한만 갖습니다.

다음 역할은 Cyber Scripting과 관련된 권한을 제공합니다.

- **회사 관리자**
  이 역할은 모든 서비스에 대한 모든 관리자 권한을 부여합니다. Cyber Scripting과 관련해서는 Cyber 관리자 역할과 동일한 권한을 부여합니다.
- **Cyber 관리자**
  이 역할은 테넌트에서 사용할 수 있는 스크립트의 승인과 **테스트 중** 상태의 스크립트를 실행할 수 있는 권한을 포함하여 전체 권한을 부여합니다.
- **관리자**

© Acronis International GmbH, 2003-2024

이 역할은 승인된 스크립트를 실행할 수 있는 권한과 승인된 스크립트를 사용하는 스크립팅 계획을 생성 및 실행할 수 있는 권한과 함께 부분 권한을 부여합니다.

- **읽기 전용 관리자**
  이 역할은 테넌트에서 사용되는 스크립트 및 보호 계획을 볼 수 있는 권한과 함께 제한된 권한을 부여합니다.
- **사용자**
  이 역할은 승인된 스크립트를 실행할 수 있는 권한과 승인된 스크립트를 사용하는 스크립팅 계획을 생성 및 실행할 수 있는 권한과 함께 부분 권한을 부여합니다. 단, 생성 및 실행할 수 있는 위치는 사용자의 머신으로 제한됩니다.

다음 표에는 사용 가능한 모든 작업(스크립트 상태 및 사용자 역할에 따라 달라짐)이 요약되어 있습니다.

역할	객체	스크립트 상태		
		초안	테스트 중	승인됨
Cyber 관리자 **회사 관리자**	스크립팅 계획	편집(계획에서 초안 스크립트 제거) 삭제 철회 비활성화 중지	생성 편집 적용 활성화 실행 삭제 철회 비활성화 중지	생성 편집 적용 활성화 실행 삭제 철회 비활성화 중지
	스크립트	생성 편집 상태 변경 복제 삭제 실행 취소	생성 편집 상태 변경 실행 복제 삭제 실행 취소	생성 편집 상태 변경 실행 복제 삭제 실행 취소
관리자 **사용자**(자신의 워크로드인 경우)	스크립팅 계획	보기 철회 비활성화 중지	보기 실행 취소	생성 편집 적용 활성화

© Acronis International GmbH, 2003-2024

				실행 삭제 철회 비활성화 중지
	스크립트	생성 편집 복제 삭제 실행 취소	보기 복제 실행 취소	실행 복제 실행 취소
읽기 전용 관리자	스크립팅 계획	보기	보기	보기
	스크립트	보기	보기	보기

스크립트

스크립트는 런타임에 해석되어 대상 머신에서 실행되는 명령어 집합입니다. 스크립트를 활용하면 반복 작업이나 복잡한 작업을 간편하게 자동화할 수 있습니다.

Cyber Scripting에서는 사전 정의된 스크립트를 실행하거나 사용자 정의 스크립트를 생성할 수 있습니다. **관리** > **스크립트 저장소**에서 사용 가능한 모든 스크립트를 확인할 수 있습니다. 사전 정의된 스크립트는 **라이브러리** 섹션에 있고 직접 생성했거나 테넌트에 복제한 스크립트는 **내 스크립트** 섹션에 있습니다.

스크립팅 계획에 포함하거나 **스크립트 빠른 실행** 작업을 수행하여 스크립트를 사용할 수 있습니다.

참고
본인의 테넌트에서 생성했거나 해당 테넌트에 복제했으며 승인된 상태의 스크립트만 사용할 수 있습니다. 스크립트 저장소에서 제거되었거나 **초안** 상태인 스크립트는 실행되지 않습니다. 스크립팅 작업의 상세 정보를 확인하거나 **모니터링** > **활동**에서 작업을 취소할 수 있습니다.

다음 표에는 상태에 따라 스크립트로 수행할 수 있는 작업이 자세히 설명되어 있습니다.

상태	가능한 작업
초안	새로 생성하는 스크립트와 저장소에 복제하는 스크립트는 **초안** 상태입니다. 이러한 스크립트는 실행하거나 스크립팅 계획에 포함할 수 없습니다.
테스트 중	**Cyber 관리자** 역할이 할당된 관리자는 이러한 스크립트를 실행하고 스크립팅 계획에 포함할 수 있습니다.

© Acronis International GmbH, 2003-2024

상태	가능한 작업
승인됨	이러한 스크립트를 실행하고 스크립팅 계획에 포함할 수 있습니다.

Cyber 관리자 역할이 할당된 관리자만 스크립트 상태를 변경하거나 승인된 스크립트를 삭제할 수 있습니다. 자세한 내용은 "스크립트 상태 변경"(227페이지) 항목을 참조하십시오.

스크립트 생성

코드를 직접 작성하여 스크립트를 생성할 수 있습니다.

스크립트를 생성하려면

1. Cyber Protect 콘솔에서 **관리** > **스크립트 저장소**로 이동합니다.
2. **내 스크립트**에서 **AI를 사용하여 스크립트 생성**을 클릭합니다.
3. 메인 창에서 스크립트 본문을 작성합니다.

중요
스크립트를 작성할 때 각 작업에 대한 종료 코드 검사를 포함합니다. 그렇지 않으면, 실패한 작업이 무시되고 **모니터링** > **활동**에서 스크립팅 활동 상태가 **성공**으로 잘못 표시될 수 있습니다.

4. 스크립트 설정을 지정합니다.

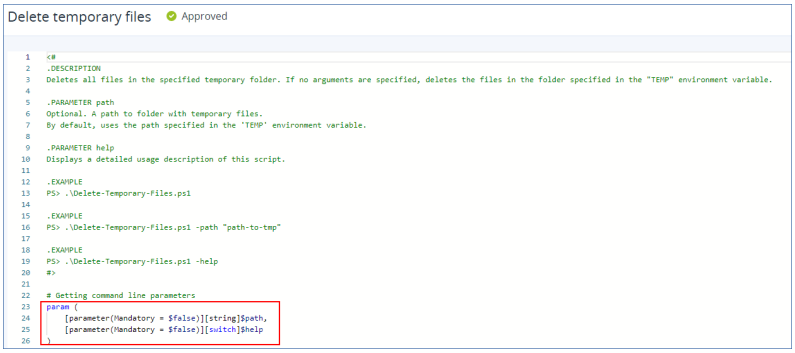
설정	설명
스크립트 이름	스크립트 이름입니다. 이 필드에는 이름이 자동으로 입력되지만 해당 값은 변경할 수 있습니다.
설명	스크립트 설명입니다. 이 설정은 원하는 경우에만 입력하면 됩니다. [AI가 생성한 스크립트의 경우] 스크립트 생성 시 필드에 내용이 자동으로 입력됩니다. AI가 제공하는 설명을 편집할 수 있습니다.
언어	스크립트 언어입니다. 사용 가능한 값은 다음과 같습니다. • **PowerShell**. 기본값입니다. • **Bash** [AI가 생성한 스크립트의 경우] 이 설정은 스크립트 생성 전에 구성됩니다.
운영 체제	스크립트를 실행할 대상 워크로드에 설치된 운영 체제입니다. 사용 가능한 값은 다음과 같습니다. • **Windows**. 기본값입니다. • **macOS** [AI가 생성한 스크립트의 경우] 이 설정은 스크립트 생성 전에 구성됩니다.
상태	스크립트 상태입니다. • **초안**. 기본값입니다. 새로 생성하는 스크립트와 저장소에 복제하는 스크립트는 **초안** 상태입니다. **초안** 스크립트는 실행하거나 스크립팅 계획에 포함할 수 없습니다. • **테스트 중**. **Cyber 관리자** 역할이 할당된 관리자만 스크립트 상태를 **테스트 중**으로 변경

© Acronis International GmbH, 2003-2024

설정	설명
	할 수 있으며 **테스트 중** 상태의 스크립트 또는 해당 스크립트가 포함된 스크립팅 계획을 실행할 수 있습니다. • **승인됨**. **승인됨** 상태의 스크립트는 실행하고 스크립팅 계획에 포함할 수 있습니다. **Cyber 관리자** 역할이 할당된 관리자만 스크립트 상태를 변경하거나 승인된 스크립트를 삭제할 수 있습니다. 자세한 내용은 "스크립트 상태 변경"(227페이지) 항목을 참조하십시오.
태그	태그는 대소문자를 구분하지 않으며 최대 32자까지 입력할 수 있습니다. 꺾쇠 괄호, 쉼표, 공백은 사용할 수 없습니다. 이 설정은 원하는 경우에만 입력하면 됩니다. [AI가 생성한 스크립트의 경우] 스크립트 생성 시 **AI로 생성됨** 태그가 자동으로 추가됩니다. 이 태그를 수동으로 삭제하거나 태그를 더 추가할 수 있습니다.

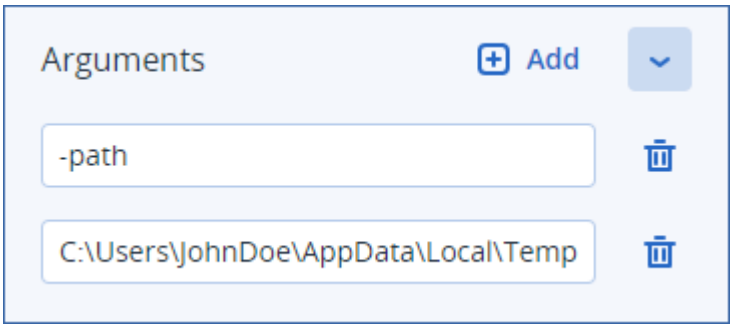
5. [자격 증명이 필요한 스크립트만 해당] 자격 증명을 지정합니다.
   단일 자격 증명(예: 토큰)또는 자격 증명 쌍(예: 사용자 이름과 비밀번호)을 사용할 수 있습니다.
6. [인수가 필요한 스크립트만 해당] 다음과 같이 인수 및 해당 값을 지정합니다.
   a. **추가**를 클릭합니다.
   b. **인수 추가** 필드에서 인수를 지정합니다.
   c. **추가**를 클릭합니다.
   d. 두 번째 필드가 표시되면 인수 값을 지정합니다.

참고
스크립트 본문에서 이미 정의한 인수만 지정할 수 있습니다.



예:

© Acronis International GmbH, 2003-2024



e. 추가해야 할 인수가 두 개 이상인 경우 위 단계를 반복합니다.

7. **저장**을 클릭합니다.

스크립트가 **초안** 상태로 저장소에 저장됩니다.

Cyber 관리자 역할이 할당된 관리자가 상태를 **승인됨**으로 변경할 때까지는 스크립트를 사용할 수 없습니다. 자세한 내용은 "스크립트 상태 변경"(227페이지) 항목을 참조하십시오.

관리하는 다른 테넌트에서 스크립트를 사용하려면 스크립트를 해당 테넌트에 복제해야 합니다. 자세한 내용은 "스크립트 복제"(225페이지) 항목을 참조하십시오.

AI(ScriptPilot)를 사용하여 스크립트 생성

참고
ScriptPilot을 사용하려면 Advanced Management 팩이 필요합니다.

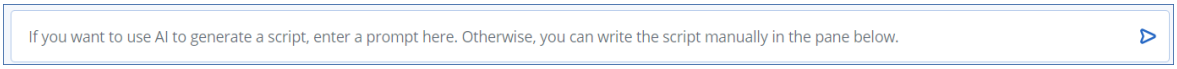
ScriptPilot에서는 AI 기능을 사용하여 프롬프트를 유용한 스크립트로 변환할 수 있으므로 스크립트 작성 시간과 작업량을 줄일 수 있습니다. AI 기능은 다음과 같은 방식으로 사용 가능합니다.

- AI에게 스크립트를 새로 생성하도록 요청하는 프롬프트를 입력합니다.
- AI에게 스크립트 본문에 입력한 코드를 검토 및 완성하도록 요청하는 프롬프트를 입력합니다. 코드가 복잡하여 직접 작성하기가 어려울 때 이 기능을 사용할 수 있습니다.

ScriptPilot은 OpenAI의 GPT-4 모델을 사용합니다. ScriptPilot을 사용하여 매월 조직용 스크립트를 100개까지 무료로 생성할 수 있습니다.

AI를 사용하여 스크립트를 생성하려면

1. Cyber Protect 콘솔에서 **관리** > **스크립트 저장소**로 이동합니다.
2. **내 스크립트**에서 **AI를 사용하여 스크립트 생성**을 클릭합니다.
3. 해당 스크립트로 수행하려는 작업에 대한 설명을 프롬프트에 입력합니다. 설명은 최대한 명확하게 자세하게 입력해야 합니다.



예:

```
I need a script that deletes Temporary files for all users (including user profiles +
Windows Temps) and disable Windows Update Service to allow the script to run
```

4. 프롬프트에서 화살표 버튼을 클릭합니다.

© Acronis International GmbH, 2003-2024

5. 확인 창에서 언어와 운영 체제를 선택하고 **생성**을 클릭합니다.
   AI가 생성한 스크립트가 메인 창에 표시됩니다. 스크립트 이름과 설명은 스크립트와 일치하도록 AI가 자동 생성합니다. 스크립트에는 **AI로 생성됨** 태그가 자동 할당됩니다.
6. AI가 생성한 스크립트를 검토하고 필요 시 수동으로 편집합니다.
7. 필요 시 스크립트 설정을 편집합니다.

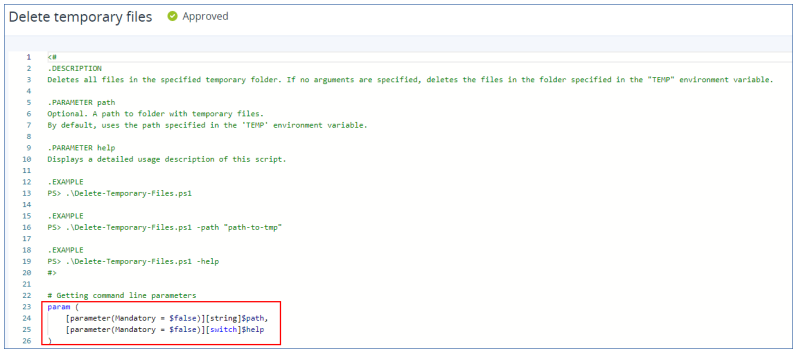
설정	설명
스크립트 이름	스크립트 이름입니다. 이 필드에는 이름이 자동으로 입력되지만 해당 값은 변경할 수 있습니다.
설명	스크립트 설명입니다. 이 설정은 원하는 경우에만 입력하면 됩니다. [AI가 생성한 스크립트의 경우] 스크립트 생성 시 필드에 내용이 자동으로 입력됩니다. AI가 제공하는 설명을 편집할 수 있습니다.
언어	스크립트 언어입니다. 사용 가능한 값은 다음과 같습니다. • **PowerShell**. 기본값입니다. • **Bash** [AI가 생성한 스크립트의 경우] 이 설정은 스크립트 생성 전에 구성됩니다.
운영 체제	스크립트를 실행할 대상 워크로드에 설치된 운영 체제입니다. 사용 가능한 값은 다음과 같습니다. • **Windows**. 기본값입니다. • **macOS** [AI가 생성한 스크립트의 경우] 이 설정은 스크립트 생성 전에 구성됩니다.
상태	스크립트 상태입니다. • **초안**. 기본값입니다. 새로 생성하는 스크립트와 저장소에 복제하는 스크립트는 **초안** 상태입니다. **초안** 스크립트는 실행하거나 스크립팅 계획에 포함할 수 없습니다. • **테스트 중**. **Cyber 관리자** 역할이 할당된 관리자만 스크립트 상태를 **테스트 중**으로 변경할 수 있으며 **테스트 중** 상태의 스크립트 또는 해당 스크립트가 포함된 스크립팅 계획을 실행할 수 있습니다. • **승인됨**. **승인됨** 상태의 스크립트는 실행하고 스크립팅 계획에 포함할 수 있습니다. **Cyber 관리자** 역할이 할당된 관리자만 스크립트 상태를 변경하거나 승인된 스크립트를 삭제할 수 있습니다. 자세한 내용은 "스크립트 상태 변경"(227페이지) 항목을 참조하십시오.
태그	태그는 대소문자를 구분하지 않으며 최대 32자까지 입력할 수 있습니다. 꺾쇠 괄호, 쉼표, 공백은 사용할 수 없습니다. 이 설정은 원하는 경우에만 입력하면 됩니다. [AI가 생성한 스크립트의 경우] 스크립트 생성 시 **AI로 생성됨** 태그가 자동으로 추가됩니다. 이 태그를 수동으로 삭제하거나 태그를 더 추가할 수 있습니다.

8. [선택 사항] [자격 증명이 필요한 스크립트만 해당] 자격 증명을 지정합니다.
   단일 자격 증명(예: 토큰)또는 자격 증명 쌍(예: 사용자 이름과 비밀번호)을 사용할 수 있습니다.
9. [인수가 필요한 스크립트만 해당] 다음과 같이 인수 및 해당 값을 지정합니다.

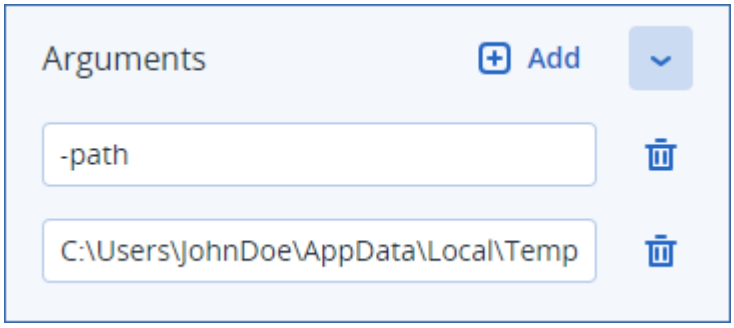
© Acronis International GmbH, 2003-2024

a. **추가**를 클릭합니다.
b. **인수 추가** 필드에서 인수를 지정합니다.
c. **추가**를 클릭합니다.
d. 두 번째 필드가 표시되면 인수 값을 지정합니다.

참고
스크립트 본문에서 이미 정의한 인수만 지정할 수 있습니다.



예:



e. 추가해야 할 인수가 두 개 이상인 경우 위 단계를 반복합니다.

10. **저장**을 클릭합니다.
스크립트가 **초안** 상태로 저장소에 저장됩니다.
Cyber 관리자 역할이 할당된 관리자가 상태를 **승인됨**으로 변경할 때까지는 스크립트를 사용할 수 없습니다. 자세한 내용은 "스크립트 상태 변경"(227페이지) 항목을 참조하십시오.
관리하는 다른 테넌트에서 스크립트를 사용하려면 스크립트를 해당 테넌트에 복제해야 합니다. 자세한 내용은 "스크립트 복제"(225페이지) 항목을 참조하십시오.

스크립트 복제

스크립트 복제는 다음과 같은 경우에 필요합니다.

- **라이브러리**의 스크립트를 사용하기 전. 이 경우에는 먼저 스크립트를 **내 스크립트** 섹션으로 복제해야 합니다.
- 상위 테넌트에서 생성한 스크립트를 하위 테넌트 또는 부서로 복제하려고 할 때.

스크립트를 복제하려면

© Acronis International GmbH, 2003-2024

1. **스크립트 저장소**에서 복제할 스크립트를 찾습니다.
2. 다음 중 하나를 수행하십시오.
   - [**내 스크립트**에서 스크립트를 복제하는 경우] 스크립트 이름 옆에 있는 말줄임표(...)를 클릭하고 **복제**를 클릭합니다.
   - [**라이브러리**에서 스크립트를 복제하는 경우] 선택한 스크립트 이름 옆의 **복제**를 클릭합니다.
3. **스크립트 복제** 팝업의 **상태** 드롭다운 목록에서 다음 스크립트 상태 중 하나를 선택합니다.
   - **초안**(기본값) - 이 상태에서는 스크립트를 즉시 실행할 수 없습니다.
   - **테스트 중** - 이 상태에서는 스크립트를 실행할 수 있습니다.
   - **승인됨** - 이 상태에서는 스크립트를 실행할 수 있습니다.
4. [관리하는 테넌트 또는 부서가 둘 이상인 경우] 스크립트를 복제할 위치를 선택합니다.

   스크립트 복제 대화 상자에는 사용자가 관리할 수 있으며 Advanced Management 팩이 적용된 테넌트만 표시됩니다.

따라서 스크립트는 사용자가 선택한 테넌트 또는 부서의 **내 스크립트** 섹션에 복제됩니다. 부서가 없는 테넌트 하나만 관리하는 경우, 스크립트가 자동으로 **내 스크립트** 섹션에 복사됩니다.

중요
스크립트를 원래 테넌트 이외의 테넌트로 복제하는 경우 스크립트에서 사용하는 자격 증명은 복사되지 않습니다.

스크립트 편집 또는 삭제

참고
사용자 역할에 따라 스크립트 및 스크립팅 계획과 관련하여 각기 다른 작업을 수행할 수 있습니다. 역할에 대한 자세한 내용은 "사용자 역할 및 Cyber Scripting 권한"(218페이지) 항목을 참조하십시오.

스크립트를 편집하려면

1. **스크립트 저장소**에서 **내 스크립트**로 이동하여 편집할 스크립트를 찾습니다.
2. 스크립트 이름 옆에 있는 말줄임표(...)를 클릭하고 **편집**을 클릭합니다.
3. 스크립트를 편집하고 **저장**을 클릭합니다.
4. [스크립팅 계획에 사용되는 스크립트를 편집하는 경우] **스크립트 저장**을 클릭하여 선택을 확인합니다.

   참고
   다음에 스크립팅 계획을 실행할 때는 스크립트의 최신 버전이 사용됩니다.

스크립트 버전

다음 스크립트 속성 중 어느 것이든 편집하면 스크립트의 새 버전이 생성됩니다.

- 스크립트 본문
- 스크립트 이름

© Acronis International GmbH, 2003-2024

- 설명
- 스크립트 언어
- 자격 증명
- 인수

그 외 다른 속성을 변경하면 편집한 내용이 현재 스크립트 버전에 추가됩니다. 버전 및 버전 비교 방법에 대해 자세히 알아보려면 "스크립트 버전 비교"(228페이지) 항목을 참조하십시오.

참고
스크립트 상태는 **상태** 필드의 값을 수정한 경우에만 업데이트됩니다. Cyber 관리자 역할이 있는 관리자만 스크립트 상태를 변경할 수 있습니다.

스크립트를 삭제하려면

1. **스크립트 저장소**에서 **내 스크립트**로 이동하여 삭제할 스크립트를 찾습니다.
2. 스크립트 이름 옆에 있는 말줄임표(...)를 클릭하고 **삭제**를 클릭합니다.
3. **삭제**를 클릭합니다.
4. [스크립팅 계획에 사용되는 스크립트를 삭제하는 경우] **스크립트 저장**을 클릭하여 선택을 확인합니다.

   참고
   삭제된 스크립트를 사용하는 스크립팅 계획은 실행되지 않습니다.

스크립트 상태 변경

새로 생성했으며 상태가 **초안**인 스크립트는 상태가 **승인됨**으로 변경될 때까지는 사용할 수 없습니다. 사용 사례에 따라 스크립트는 승인 전에 일정 기간 동안 **테스트 중** 상태로 유지될 수 있습니다.

참고
사용자 역할에 따라 스크립트 및 스크립팅 계획과 관련하여 각기 다른 작업을 수행할 수 있습니다. 역할에 대한 자세한 내용은 "사용자 역할 및 Cyber Scripting 권한"(218페이지) 항목을 참조하십시오.

사전 요구 사항

- 사용자가 **Cyber 관리자** 역할이 할당된 관리자여야 합니다.
- 해당하는 상태의 스크립트를 사용할 수 있어야 합니다.

스크립트 상태를 변경하려면

1. **스크립트 저장소**에서 **내 스크립트**로 이동합니다.
2. 스크립트 이름 옆에 있는 말줄임표(...)를 클릭하고 **편집**을 클릭합니다.
3. **상태** 드롭다운 목록에서 상태를 선택합니다.
4. **저장**을 클릭합니다.

© Acronis International GmbH, 2003-2024

5. [승인된 스크립트의 상태를 변경하는 경우] 변경 사항을 확인하려면 **스크립트 저장**을 클릭합니다.

참고
스크립트 상태가 **초안**으로 다운그레이드된 경우 해당 스크립트를 사용하는 스크립팅 계획은 실행되지 않습니다.
Cyber 관리자 역할이 할당된 관리자만 **테스트 중** 상태의 스크립트 및 해당 스크립트를 사용하는 스크립팅 계획을 실행할 수 있습니다.

스크립트 버전 비교

스크립트의 두 버전을 비교하고 이전 버전으로 되돌릴 수 있습니다. 특정 버전을 생성한 사람과 생성한 시점을 확인할 수도 있습니다.

스크립트 버전을 비교하려면

1. **스크립트 저장소**에서 **내 스크립트**로 이동하여 버전을 비교할 스크립트를 찾습니다.
2. 스크립트 이름 옆에 있는 말줄임표(...)를 클릭하고 **버전 기록**을 클릭합니다.
3. 비교할 두 버전을 선택하고 **버전 비교**를 클릭합니다.
   스크립트 본문 텍스트, 해당 인수 또는 자격 증명의 모든 변경 사항이 강조 표시됩니다.

이전 버전으로 되돌리려면

1. **스크립트 버전 비교** 창에서 **이 버전으로 되돌리기**를 클릭합니다.
2. **이전 버전으로 되돌리기** 팝업의 **상태** 드롭다운 목록에서 스크립트 상태를 선택합니다.

선택한 버전이 복원되고 버전 기록에 최신 버전으로 저장됩니다.

스크립트를 복원하려는 경우 **버전 기록** 창에서 버전을 선택한 다음 **복원** 버튼을 클릭해도 됩니다.

중요
테스트 중 또는 **승인됨** 상태인 스크립트만 실행할 수 있습니다. 자세한 내용은 "스크립트 상태 변경"(227페이지) 항목을 참조하십시오.

스크립팅 작업의 출력 다운로드

스크립팅 작업의 출력을 .zip 파일로 다운로드할 수 있습니다. .zip 파일에는 `stdout`과 `stderr`이라는 두 개의 텍스트 파일이 포함되어 있습니다. `stdout`에서는 성공적으로 완료된 스크립팅 작업의 결과를 볼 수 있습니다. `stderr` 파일에는 스크립팅 작업 중 발생한 오류에 대한 정보가 포함되어 있습니다.

출력 파일을 다운로드하려면

1. Cyber Protect 콘솔에서 **모니터링** > **활동**으로 이동합니다.
2. 출력을 다운로드할 Cyber Scripting 활동을 클릭합니다.
3. **활동 상세정보** 화면에서 **출력 다운로드**를 클릭합니다.

© Acronis International GmbH, 2003-2024

스크립트 저장소

스크립트 저장소는 **관리** 탭에서 찾을 수 있습니다. 저장소에서 이름 및 설명으로 스크립트를 검색할 수 있습니다. 필터를 사용하거나 이름 또는 상태별로 스크립트를 정렬할 수도 있습니다.

스크립트를 관리하려면 스크립트 이름 옆에 있는 말줄임표(...)를 클릭하고 원하는 작업을 선택합니다.또는 스크립트를 클릭하고 화면이 열리면 화면의 버튼을 사용합니다.

스크립트 저장소에는 다음 섹션이 있습니다.

- **내 스크립트**

  사용자 환경에서 직접 사용할 수 있는 스크립트를 찾을 수 있습니다. 사용자가 처음부터 새로 생성한 스크립트와 여기에 복제한 스크립트입니다.

  이 섹션에서 다음 기준으로 스크립트를 필터링할 수 있습니다.

  - 태그
  - 상태
  - 언어
  - 운영 체제
  - 스크립트 소유자
- **라이브러리**

  라이브러리에는 **내 스크립트** 섹션에 복제한 후 환경에서 사용할 수 있는 사전 정의된 스크립트가 있습니다. 이러한 스크립트만 검사하고 복제할 수 있습니다.

  이 섹션에서 다음 기준으로 스크립트를 필터링할 수 있습니다.

  - 태그
  - 언어
  - 운영 체제

  자세한 내용은 벤더에서 승인한 스크립트(70595)를 참조하십시오.

스크립팅 계획

스크립팅 계획을 사용하면 여러 워크로드에서 스크립트를 실행하고, 스크립트 실행을 예약하고, 추가 설정을 구성할 수 있습니다.

관리 > **스크립팅 계획**에서 생성한 스크립팅 계획 및 워크로드에 적용한 스크립팅 계획을 찾을 수 있습니다. 여기서 계획 실행 위치, 소유자 또는 상태를 확인할 수 있습니다.

클릭 가능한 막대에 스크립팅 계획에 대해 다음과 같은 색상으로 구분된 상태가 표시됩니다.

- 실행 중(파란색)
- 호환성 확인 중(진한 회색)
- 비활성화됨(밝은 회색)
- 확인(녹색)
- 심각한 경보(빨간색)

© Acronis International GmbH, 2003-2024

- 오류(주황색)
- 경고(노란색)

  상태 표시줄을 클릭하면 계획의 상태와 워크로드 수를 확인할 수 있습니다. 각 상태도 클릭할 수 있습니다.

  스크립팅 계획 탭에서 다음 작업을 수행하여 계획을 관리할 수 있습니다.

  - 실행
  - 중지
  - 편집
  - 이름 변경
  - 비활성화
  - 활성화
  - 복제
  - 내보내기. 계획 구성은 JSON 형식으로 로컬 머신에 내보내집니다.
  - 삭제

  스크립팅 계획의 가시성 및 스크립팅 계획에 사용할 수 있는 작업은 계획 소유자 및 사용자의 사용자 역할에 따라 달라집니다. 예를 들어, 회사 관리자는 워크로드에 적용된 파트너 소유 스크립팅 계획을 볼 수만 있고 계획에 대해 어떠한 작업도 수행할 수 없습니다.

  스크립팅 계획을 생성 및 관리할 수 있는 사람에 대한 자세한 내용은 "사용자 역할 및 Cyber Scripting 권한"(218페이지) 항목을 참조하십시오.

스크립팅 계획을 관리하려면

1. Cyber Protect 콘솔에서 **관리** > **스크립팅 계획**으로 이동합니다.
2. 관리할 계획을 찾은 후 계획 옆에 있는 말줄임표(...)를 클릭합니다.
3. 원하는 작업을 선택하고 화면에 나타나는 지시사항을 따릅니다.

스크립팅 계획 생성

다음과 같은 방법으로 스크립팅 계획을 생성할 수 있습니다.

- **장치** 탭에서
  워크로드를 선택한 다음 워크로드에 대한 스크립팅 계획을 생성합니다.
- **관리** > **스크립팅 계획** 탭에서
  스크립팅 계획을 생성하고 계획을 적용할 워크로드를 선택합니다.

장치 탭에서 스크립팅 계획을 생성하려면

1. Cyber Protect 콘솔에서 **장치** > **에이전트가 있는 머신**으로 이동합니다.
2. 스크립팅 계획을 적용할 워크로드 또는 장치 그룹을 선택한 다음 각각 **보호** 또는 **그룹 보호**를 클릭합니다.
3. [이미 적용된 계획이 있는 경우] **계획 추가**를 클릭합니다.
4. **계획 생성** > **스크립팅 계획**을 클릭합니다.

© Acronis International GmbH, 2003-2024

스크립팅 계획의 템플릿이 열립니다.

5. [선택 사항] 스크립팅 계획 이름을 수정하려면 연필 아이콘을 클릭합니다.
6. **스크립트 선택**을 클릭하고 사용할 스크립트를 선택한 다음 **완료**를 클릭합니다.

참고
승인된 스크립트는 **스크립트 저장소** > **내 스크립트**에서만 사용 가능합니다. **테스트 중** 상태의 스크립트는 **Cyber 관리자** 역할이 할당된 관리자만 사용할 수 있습니다. 역할에 대한 자세한 내용은 "사용자 역할 및 Cyber Scripting 권한"(218페이지) 항목을 참조하십시오.

7. 스크립팅 계획에 대한 스케줄 및 시작 조건을 구성합니다.
8. 대상 워크로드에서 스크립트를 실행할 계정을 선택합니다. 다음 옵션을 사용할 수 있습니다.
   - 시스템 계정(macOS에서는 루트 계정)
   - 현재 로그인한 계정
9. 대상 워크로드에서 스크립트를 실행할 수 있는 기간을 지정합니다.
   설정된 시간대 내에 스크립트 실행을 완료할 수 없는 경우 Cyber Scripting 작업이 실패합니다.
   지정할 수 있는 최소값은 1분이고 최대값은 1440분입니다.
10. [PowerShell 스크립트만 해당] PowerShell 실행 정책을 구성합니다.
    이 정책에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.
11. **생성**을 클릭합니다.

스크립팅 계획 탭에서 스크립팅 계획을 생성하려면

1. Cyber Protect 콘솔에서 **관리** > **스크립팅 계획**으로 이동합니다.
2. **계획 생성**을 클릭합니다.
   스크립팅 계획의 템플릿이 열립니다.
3. [선택 사항] 새 계획을 적용할 워크로드 또는 장치 그룹을 선택하려면 **워크로드 추가**를 클릭합니다.
   a. **에이전트가 있는 머신**을 선택하여 목록을 확장하고 원하는 워크로드 또는 장치 그룹을 선택합니다.
   b. **추가**를 클릭합니다.

   파트너 수준에서 장치 그룹을 생성하는 방법에 대한 자세한 내용은 "장치 탭"(296페이지) 항목을 참조하십시오.

참고
계획을 생성한 후에 워크로드 또는 장치 그룹을 선택할 수도 있습니다.

4. [선택 사항] 스크립팅 계획 이름을 수정하려면 연필 아이콘을 클릭합니다.
5. **스크립트 선택**을 클릭하고 사용할 스크립트를 선택한 다음 **완료**를 클릭합니다.

참고
승인된 스크립트는 **스크립트 저장소** > **내 스크립트**에서만 사용 가능합니다. **테스트 중** 상태의 스크립트는 **Cyber 관리자** 역할이 할당된 관리자만 사용할 수 있습니다. 역할에 대한 자세한 내용은 "사용자 역할 및 Cyber Scripting 권한"(218페이지) 항목을 참조하십시오.

© Acronis International GmbH, 2003-2024

6. 스크립팅 계획에 대한 스케줄 및 시작 조건을 구성합니다.
7. 대상 워크로드에서 스크립트를 실행할 계정을 선택합니다. 다음 옵션을 사용할 수 있습니다.
   - 시스템 계정(macOS에서는 루트 계정)
   - 현재 로그인한 계정
8. 대상 워크로드에서 스크립트를 실행할 수 있는 기간을 지정합니다.
   설정된 시간대 내에 스크립트 실행을 완료할 수 없는 경우 Cyber Scripting 작업이 실패합니다.
   지정할 수 있는 최소값은 1분이고 최대값은 1440분입니다.
9. [PowerShell 스크립트만 해당] PowerShell 실행 정책을 구성합니다.
   이 정책에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.
10. **생성**을 클릭합니다.

스케줄 및 시작 조건

예약

한 번 또는 반복적으로 실행되고, 스케줄에 따라 시작되거나 특정 이벤트에 의해 트리거되도록 스크립팅 계획을 구성할 수 있습니다.

다음 옵션을 사용할 수 있습니다.

- 한 번 실행
  이 옵션을 사용하려는 경우에는 계획이 실행될 날짜 및 시간을 구성해야 합니다.
- 시간 기준 예약
  이 옵션을 선택하면 매시간, 매일 또는 매월 실행되도록 스크립팅 계획을 예약할 수 있습니다.
  스케줄이 일시적으로만 유효하도록 하려면 **날짜 범위 내에서 실행** 확인란을 선택하고 예약된 계획이 실행될 기간을 구성합니다.
- 사용자가 시스템에 로그인할 때
  특정 사용자 또는 로그인하는 모든 사용자가 스크립팅 계획을 트리거하는지 여부를 선택할 수 있습니다.
- 사용자가 시스템에서 로그오프할 때
  특정 사용자 또는 로그오프하는 모든 사용자가 스크립팅 계획을 트리거하는지 여부를 선택할 수 있습니다.
- 시스템 시작 시
- 시스템이 중단된 경우

  참고
  이 예약 옵션은 시스템 계정으로 실행되는 스크립트에만 사용할 수 있습니다.

- 시스템이 오프라인인 경우

시작 조건

시작 조건을 사용하면 예약된 계획을 더 유연하게 사용할 수 있습니다. 조건을 여러 개 구성한 경우에는 모든 조건이 동시에 충족되어야만 계획이 시작됩니다.

© Acronis International GmbH, 2003-2024

시작 조건은 **지금 실행** 옵션을 사용하여 수동으로 계획을 실행한 경우에는 유효하지 않습니다.

조건	설명
워크로드가 온라인일 때만 실행	대상 워크로드가 인터넷에 연결되어 있을 때만 스크립트가 실행됩니다.
사용자가 유휴 상태임	이 조건은 머신에서 화면 보호기가 실행 중이거나 머신이 잠겨 있을 때 충족됩니다.
사용자 로그오프	이 조건을 사용하면 대상 워크로드의 사용자가 로그오프할 때까지 예약된 스크립팅 계획을 연기할 수 있습니다.
시간 간격에 맞춰 실행	이 조건을 사용하면 지정된 시간 간격 내에서만 스크립팅 계획이 시작될 수 있습니다. 예를 들어, 이 조건을 사용하여 **사용자 로그오프** 조건을 제한할 수 있습니다.
배터리 전원 절약	이 조건을 사용하면 배터리 부족으로 인해 스크립팅 계획이 중단되지 않도록 할 수 있습니다. 다음 옵션을 사용할 수 있습니다. • 배터리 사용 시에는 시작하지 않음 머신이 전원에 연결되어 있는 경우에만 계획이 시작됩니다. • 배터리 레벨이 다음 이상인 경우 배터리 사용 시 시작: 머신이 전원에 연결되어 있거나 배터리 수준이 지정된 값보다 높은 경우 계획이 시작됩니다.
데이터 요금제 사용 시 시작하지 않음	이 조건은 대상 워크로드가 데이터 요금제 연결을 통해 인터넷에 액세스하는 경우 계획이 시작되지 않도록 합니다.
다음과 같은 Wi-Fi 네트워크에 연결된 경우 시작하지 않음	이 조건은 대상 워크로드가 지정된 무선 네트워크 중 어느 것에든 연결되어 있는 경우 계획이 시작되지 않도록 합니다. 이 조건을 사용하려면 금지된 네트워크의 SSID를 지정해야 합니다. 이 제한 사항은 대소문자 구별 없이 이름에 하위 문자열로 지정된 이름을 포함하고 있는 모든 네트워크에 적용됩니다. 예를 들어, 네트워크 이름으로 phone을 지정하는 경우 장치가 다음 네트워크 중 어느 것에든 연결되어 있으면 백업이 시작되지 않습니다. `John's iPhone`, `phone_wifi` 또는 `my_PHONE_wifi`
장치 IP 주소 확인	이 조건은 대상 워크로드의 IP 주소 중 어느 것이든 지정된 IP 주소 범위 내이거나 밖인 경우 계획이 시작되지 않도록 합니다. 다음 옵션을 사용할 수 있습니다. • IP 범위 밖인 경우 시작 • IP 범위 내인 경우 시작 IPv4 주소만 지원됩니다.
시작 조건이 충족되지 않아도 작업 실행	이 옵션을 사용하면 다른 모든 조건에 관계없이 계획이 실행될 시간 간격을 설정할 수 있습니다. 계획은 다른 조건의 충족 또는 지정된 기간 종료 중 하나가 먼저 발생하자마자 즉시 시작됩니다. 한 번만 실행되도록 스크립팅 계획을 구성한 경우에는 이 옵션을 사용할 수 없습니다.

© Acronis International GmbH, 2003-2024

계획의 대상 워크로드 관리

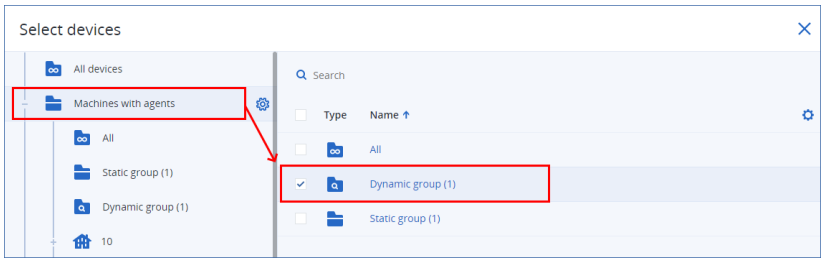
계획을 생성하는 동안 또는 나중에 스크립팅 계획을 적용할 워크로드 또는 장치 그룹을 선택할 수 있습니다.

파트너 관리자는 여러 고객의 워크로드에 동일한 계획을 적용하고 여러 고객의 워크로드가 포함된 장치 그룹을 생성할 수 있습니다. 파트너 수준에서 정적 또는 동적 장치 그룹을 생성하는 방법을 알아보려면 "장치 탭"(296페이지) 항목을 참조하십시오.

계획에 초기 워크로드를 추가하려면

1. Cyber Protect 콘솔에서 **관리** > **스크립팅 계획**으로 이동합니다.
2. 대상 워크로드를 지정할 계획의 이름을 클릭합니다.
3. **워크로드 추가**를 클릭합니다.
4. 원하는 워크로드 또는 장치 그룹을 선택하고 **추가**를 클릭합니다.

참고
장치 그룹을 선택하려면 해당 상위 수준을 클릭하고 메인 창에서 이름 옆의 확인란을 선택합니다.



5. 편집한 계획을 저장하려면 **저장**을 클릭합니다.

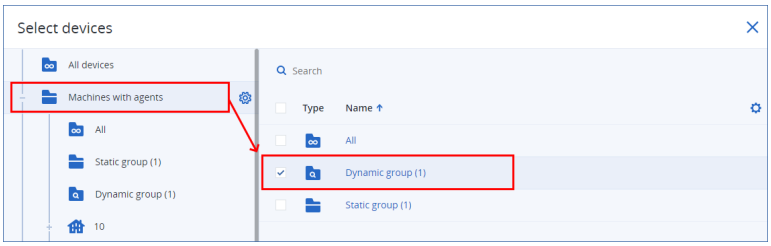
계획의 기존 워크로드를 관리하려면

1. Cyber Protect 콘솔에서 **관리** > **스크립팅 계획**으로 이동합니다.
2. 대상 워크로드를 변경할 계획의 이름을 클릭합니다.
3. **워크로드 관리**를 클릭합니다.
   장치 화면에 스크립팅 계획이 현재 적용되어 있는 워크로드가 나열됩니다. 관리하는 테넌트 또는 부서가 둘 이상인 경우 테넌트별로 워크로드가 정렬됩니다.
   - 새 워크로드 또는 장치 그룹을 추가하려면 **추가**를 클릭합니다.
     a. 원하는 워크로드 또는 장치 그룹을 선택합니다. 관리하는 모든 테넌트의 워크로드를 추가할 수 있습니다.

© Acronis International GmbH, 2003-2024

참고

장치 그룹을 선택하려면 해당 상위 수준을 클릭하고 메인 창에서 이름 옆의 확인란을 선택합니다.



b. **추가**를 클릭합니다.

- 워크로드 또는 장치 그룹을 제거하려면 해당 워크로드 또는 장치 그룹을 선택하고 **제거**를 클릭합니다.

4. **완료**를 클릭합니다.
5. 편집한 계획을 저장하려면 **저장**을 클릭합니다.

다양한 관리 수준의 계획

다음 표에는 다양한 수준의 관리자가 보고 관리할 수 있는 계획이 요약되어 있습니다.

관리자	관리 수준	계획	권한
파트너 관리자	파트너 수준	고유한 계획	전체 권한
		고객 계획(부서의 계획 포함)	전체 권한
		부서 계획	전체 권한
	고객 수준 (서비스 제공업체가 관리하는 고객의 경우)	이 고객의 워크로드에 적용된 파트너 계획	읽기 전용
		고객 계획(부서의 계획 포함)	전체 권한
		부서 계획	전체 권한
	부서 수준 (서비스 제공업체가 관리하는 고객의 경우)	이 부서의 워크로드에 적용된 파트너 계획	읽기 전용
		이 부서의 워크로드에 적용된 고객 계획	읽기 전용
		부서 계획	전체 권한

© Acronis International GmbH, 2003-2024

관리자	관리 수준	계획	권한
회사 관리자	고객 수준	이 고객 또는 부서의 워크로드에 적용된 파트너 계획	읽기 전용
		고객 계획(부서의 계획 포함)	전체 권한
		부서 계획	전체 권한
	부서 수준	이 부서의 워크로드에 적용된 파트너 계획	읽기 전용
		이 부서의 워크로드에 적용된 고객 계획	읽기 전용
		부서 계획	전체 권한
부서 관리자	부서 수준	이 부서의 워크로드에 적용된 파트너 계획	읽기 전용
		이 부서의 워크로드에 적용된 고객 계획	읽기 전용
		부서 계획	전체 권한

중요
계획의 소유자는 계획이 생성된 테넌트입니다. 따라서 파트너 관리자가 고객 테넌트 수준에서 계획을 생성한 경우 고객 테넌트가 해당 계획의 소유자입니다.

스크립팅 계획의 호환성 문제

워크로드에 스크립팅 계획을 적용하면 호환성 문제가 발생하는 경우도 있습니다. 다음과 같은 호환성 문제가 발생할 수 있습니다.

- 호환되지 않는 운영 체제 - 워크로드의 운영 체제가 지원되지 않으면 이 문제가 표시됩니다.
- 지원되지 않는 에이전트 - 워크로드의 보호 에이전트 버전이 오래되어 Cyber Scripting 기능을 지원하지 않으면 이 문제가 표시됩니다.
- 부족한 할당량 - 테넌트의 서비스 할당량이 선택한 워크로드에 할당하기에 충분하지 않으면 이 문제가 표시됩니다.

스크립팅 계획을 개별적으로 선택된 워크로드(최대 150개)에 적용하면 계획을 저장하기 전에 기존 충돌을 해결하라는 메시지가 표시됩니다. 충돌을 해결하려면 충돌의 근본 원인을 제거하거나 영향을 받는 워크로드를 계획에서 제거합니다. 자세한 내용은 "스크립팅 계획의 호환성 문제 해결"(237페이지)을(를) 참조하십시오. 충돌을 해결하지 않고 계획을 저장하면 호환되지 않는 워크로드에 대해 계획이 자동으로 비활성화되고 경보가 표시됩니다.

© Acronis International GmbH, 2003-2024

스크립팅 계획이 150개가 넘는 워크로드 또는 장치 그룹에 적용된 경우, 계획이 저장된 후 호환성이 검사됩니다. 호환되지 않는 워크로드에 대해서는 계획이 자동으로 비활성화되고 경보가 표시됩니다.

스크립팅 계획의 호환성 문제 해결

호환성 문제의 원인에 따라 각기 다른 작업을 수행하여 새 스크립팅 계획 생성 프로세스의 일부분으로 호환성 문제를 해결할 수 있습니다.

참고
계획에서 워크로드를 제거하여 호환성 문제를 해결할 때 장치 그룹에 포함된 워크로드는 제거할 수 없습니다.

호환성 문제를 해결하려면

1. **문제 검토**를 클릭합니다.
2. [호환되지 않는 운영 체제의 호환성 문제를 해결하려면]
   a. **호환되지 않는 운영 체제** 탭에서 제거할 워크로드를 선택합니다.
   b. **계획에서 워크로드 제거**를 클릭합니다.
   c. **제거**를 클릭한 다음 **닫기**를 클릭합니다.
3. [계획에서 워크로드를 제거하여 지원되지 않는 에이전트의 호환성 문제를 해결하려면]
   a. **지원되지 않는 에이전트** 탭에서 제거할 워크로드를 선택합니다.
   b. **계획에서 워크로드 제거**를 클릭합니다.
   c. **제거**를 클릭한 다음 **닫기**를 클릭합니다.
4. [에이전트 버전을 업데이트하여 지원되지 않는 에이전트의 호환성 문제를 해결하려면] **에이전트 목록으로 이동**을 클릭합니다.

   참고
   이 옵션은 고객 관리자만 사용할 수 있습니다.

5. [계획에서 워크로드를 제거하여 부족한 할당량으로 인한 호환성 문제를 해결하려면]
   a. **부족한 할당량** 탭에서 제거할 워크로드를 선택합니다.
   b. **계획에서 워크로드 제거**를 클릭합니다.
   c. **제거**를 클릭한 다음 **닫기**를 클릭합니다.
6. [테넌트의 할당량을 늘려 부족한 할당량으로 인한 호환성 문제를 해결하려면]

   참고
   이 옵션은 파트너 관리자만 사용할 수 있습니다.

   a. **부족한 할당량** 탭에서 **관리 포털로 이동**을 클릭합니다.
   b. 고객의 서비스 할당량을 늘립니다.

© Acronis International GmbH, 2003-2024

스크립트 빠른 실행

스크립트는 스크립팅 계획에 포함하지 않고 즉시 실행할 수 있습니다. 그러나 150개를 초과하는 워크로드, 오프라인 워크로드 또는 장치 그룹에서는 이 작업을 수행할 수 없습니다.

대상 워크로드에는 스크립트 빠른 실행 기능을 지원하는 서비스 할당량이 할당되어야 하며 해당 테넌트에 대해 Advanced Management 팩이 활성화되어야 합니다. 테넌트에 충분할 할당량이 있는 경우, 적절한 서비스 할당량이 자동으로 할당됩니다.

참고
승인된 스크립트는 **스크립트 저장소** > **내 스크립트**에서만 사용 가능합니다. **테스트 중** 상태의 스크립트는 **Cyber 관리자** 역할이 할당된 관리자만 사용할 수 있습니다. 역할에 대한 자세한 내용은 "사용자 역할 및 Cyber Scripting 권한"(218페이지) 항목을 참조하십시오.

다음과 같은 방법으로 빠른 실행을 시작할 수 있습니다.

- **장치** 탭에서
  하나 이상의 워크로드를 선택하고 워크로드에서 실행할 스크립트를 선택합니다.
- **관리** > **스크립트 저장소** 탭에서
  스크립트를 선택하고 하나 이상의 대상 워크로드를 선택합니다.

장치 탭에서 스크립트를 실행하려면

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 스크립트를 실행할 워크로드를 선택하고 **보호**를 클릭합니다.
3. **스크립트 빠른 실행**을 클릭합니다.
4. **스크립트 선택**을 클릭하고 사용할 스크립트를 선택한 다음 **완료**를 클릭합니다.
5. 대상 워크로드에서 스크립트를 실행할 계정을 선택합니다. 다음 옵션을 사용할 수 있습니다.
   - 시스템 계정(macOS에서는 루트 계정)
   - 현재 로그인한 계정
6. 대상 워크로드에서 스크립트를 실행할 수 있는 기간을 지정합니다.
   설정된 시간대 내에 스크립트 실행을 완료할 수 없는 경우 Cyber Script 작업이 실패합니다.
   1분에서 1440분 사이의 값을 사용할 수 있습니다.
7. [PowerShell 스크립트만 해당] PowerShell 실행 정책을 구성합니다.
   이 정책에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.
8. **지금 실행**을 클릭합니다.

스크립트 저장소 탭에서 스크립트를 실행하려면

1. Cyber Protect 콘솔에서 **관리** > **스크립트 저장소**로 이동합니다.
2. 스크립트를 실행할 워크로드를 선택하고 **보호**를 클릭합니다.
3. **워크로드 추가**를 클릭하여 대상 워크로드를 선택하고 **추가**를 클릭합니다.
4. **스크립트 선택**을 클릭하고 사용할 스크립트를 선택한 다음 **완료**를 클릭합니다.
5. 대상 워크로드에서 스크립트를 실행할 계정을 선택합니다. 다음 옵션을 사용할 수 있습니다.

© Acronis International GmbH, 2003-2024

- 시스템 계정(macOS에서는 루트 계정)
- 현재 로그인한 계정

6. 대상 워크로드에서 스크립트를 실행할 수 있는 기간을 지정합니다.
   설정된 시간대 내에 스크립트 실행을 완료할 수 없는 경우 Cyber Script 작업이 실패합니다.
   1분에서 1440분 사이의 값을 사용할 수 있습니다.
7. [PowerShell 스크립트만 해당] PowerShell 실행 정책을 구성합니다.
   이 정책에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.
8. **지금 실행**을 클릭합니다.

협업 및 커뮤니케이션 애플리케이션 보호

Zoom, Cisco Webex Meetings, Citrix Workspace, Microsoft Teams은 현재 널리 사용되고 있는 화상/웹 컨퍼런스 및 커뮤니케이션 솔루션입니다. Cyber Protection 서비스를 이용하면 공동 작업 도구를 보호할 수 있습니다.

Zoom, Cisco Webex Meetings, Citrix Workspace, Microsoft Teams에 대한 보호 구성은 비슷합니다. 아래 예에서는 Zoom 구성을 살펴보겠습니다.

Zoom 보호를 설정하려면

1. 협업 애플리케이션이 설치되어 있는 머신에 보호 에이전트를 설치합니다.
2. Cyber Protect 콘솔에 로그인하고 다음 모듈 중 하나가 활성화되어 있는 보호 계획을 적용합니다.
   - 안티바이러스 및 맬웨어 방지 기능(**Self-Protection** 및 **Active Protection** 설정이 활성화되어 있음) - Cyber Protect 버전 중 하나를 이용하는 경우.
   - **Active Protection**(**Self-Protection** 설정이 활성화되어 있음) - Cyber Backup 버전 중 하나를 이용하는 경우.
3. [선택 사항] 자동 업데이트 설치의 경우 보호 계획에서 **패치 관리** 모듈을 구성합니다.

그러면 Zoom 애플리케이션이 다음 작업을 포함하는 보호 상태에 놓이게 됩니다.

- Zoom 클라이언트 업데이트 자동 설치
- 코드 주입으로부터 Zoom 프로세스 보호
- Zoom 프로세스에 의한 의심스러운 작업 방지
- Zoom 관련 도메인이 추가되지 않도록 "호스트" 파일 보호

© Acronis International GmbH, 2003-2024

현재 보호 수준 이해

모니터링

현재 보호 수준과 관련된 중요한 정보를 제공하는 **모니터링** 탭에는 다음 대시보드가 포함되어 있습니다.

- **개요**
- **활동**
- **경보**
- **위협 피드**(자세한 내용은 "위협 피드"(278페이지) 참조)

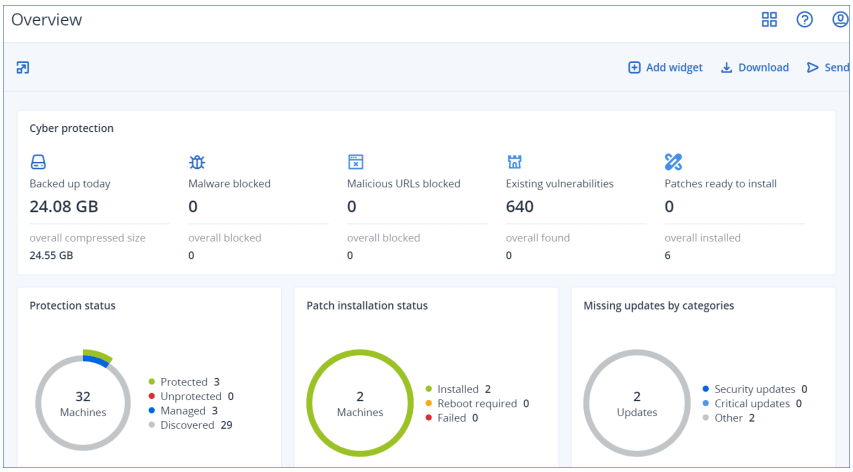
개요 대시보드

개요 대시보드는 Cyber Protection 서비스와 관련한 작업의 개요를 알려주는 사용자 정의 가능한 다양한 위젯을 제공합니다. 다른 서비스에 대한 위젯은 향후 릴리스에서 제공될 예정입니다.

위젯은 5분마다 업데이트됩니다. 위젯에는 조사할 수 있고 문제를 해결할 수 있는 클릭 가능한 요소가 있습니다. 대시보드의 현재 상태를 다운로드하거나 이메일을 통해 .pdf 및/또는 .xlsx 형식으로 보낼 수 있습니다.

표, 원 그래프, 막대형 차트, 목록, 트리형 맵으로 표시되는 여러 가지 위젯 중 선택할 수 있습니다. 서로 다른 필터를 사용하여 동일한 유형의 여러 위젯을 추가할 수 있습니다.

모니터링 > **개요** 의 **다운로드** 및 **전송** 버튼은 Cyber Protection 서비스의 Standard 에디션에서 사용할 수 없습니다.



대시보드에서 위젯을 재정렬하려면:

이름을 클릭하여 위젯을 끌어서 놓습니다.

위젯을 편집하려면:

위젯 이름 옆의 연필 아이콘을 클릭합니다. 위젯을 편집하면 이름 바꾸기, 시간 범위 변경 및 필터 및 그룹 행 설정이 가능합니다.

© Acronis International GmbH, 2003-2024

위젯을 추가하려면:

위젯 추가를 클릭한 다음, 다음 중 하나를 수행합니다.

- 추가할 위젯을 클릭합니다. 위젯이 기본 설정으로 추가됩니다.
- 추가하기 전에 위젯을 편집하려면 위젯이 선택된 상태에서 사용자 지정을 클릭합니다. 위젯을 편집한 후 **완료**를 클릭합니다.

위젯을 제거하려면:

위젯 이름 옆의 X 기호를 클릭합니다.

활동 대시보드

활동 대시보드에는 현재 및 과거 활동의 개요가 나와 있습니다. 기본적으로 보관 기간은 90일입니다.

활동 대시보드의 보기를 사용자 지정하려면 기어 아이콘을 클릭하고 확인하려는 열을 선택합니다.

활동 진행률을 실시간으로 확인하려면 **자동 새로 고침** 확인란을 선택합니다. 하지만 여러 활동을 자주 업데이트하면 관리 서버의 성능이 저하됩니다.

나열된 활동은 다음 기준으로 검색할 수 있습니다.

- **장치 이름**
  활동이 수행되는 머신입니다.
- **시작한 사람**
  활동을 시작한 계정입니다.

다음 속성을 기준으로 작업을 필터링할 수도 있습니다.

- **상태**
  예: 성공, 실패, 진행 중, 취소.
- **유형**
  예: 계획 적용, 백업 삭제, 소프트웨어 업데이트 설치.
- **시간**
  예: 최신 활동, 24시간 전부터 발생한 활동 또는 기본 보관 기간 내 특정 기간 동안의 활동.

활동에 관한 세부 사항을 자세히 확인하려면 목록에서 이 활동을 선택한 다음 **활동 세부 사항** 패널에서 **모든 속성**을 클릭합니다. 사용 가능한 속성에 대한 자세한 내용은 개발자 네트워크 포털에서 활동 및 작업 API 참고 자료를 참조하십시오.

경보 대시보드

경보 대시보드는 현재 경보가 모두 표시됩니다. 나열되는 경보는 심각 또는 오류 경보이며 대개 특정 이유로 실패한 백업 등의 작업과 관련이 있습니다.

대시보드에서 경보를 필터링하려면

© Acronis International GmbH, 2003-2024

1. **보기** 드롭다운 목록에서 다음 기준 중 하나를 선택합니다.
   - **경보 심각도**
   - **경보 카테고리**
   - **경보 유형**
   - **모니터링 유형**
   - **날짜 범위: ...에서 ...까지**
   - **워크로드**
   - **계획**
   - **고객**
2. **카테고리** 드롭다운 목록에서 **경보 카테고리**를 선택했다면 확인하려는 경보의 카테고리를 선택합니다.
3. 경보를 필터링하지 않고 모두 확인하려면 **모든 경보 유형**을 클릭합니다.

각 경보 내에서 수행할 수 있는 작업은 다음과 같습니다.

- **장치** 링크를 클릭하여 경보와 관련된 장치에 액세스합니다.
- 경보의 **문제 해결** 섹션에 나와 있는 권고 사항을 확인한 후 해당 작업을 수행해 봅니다.
- **솔루션 검색**을 클릭하여 관련 설명서 및 기술 자료 문서에 액세스합니다. **솔루션 검색** 기능 사용 시에는 사용자의 작업을 가장 효율적으로 지원하기 위해 현재 경보 상세 정보가 요청에 미리 입력됩니다.

대시보드에서 경보를 정렬하려면

경보 테이블에서 다음 열 이름 중 하나의 옆에 있는 화살표 버튼을 클릭합니다.

- **경보 심각도**
- **경보 유형**
- **생성됨**
- **경보 카테고리**
- **워크로드**
- **계획**

경보 유형

경보가 생성되는 경보 유형은 다음과 같습니다.

- 백업 경보
- 재해 복구 경보
- 안티맬웨어 보호 경보
- 라이선스 경보
- URL 필터링 경보
- EDR 경보
- 장치 제어 경보
- 시스템 경보

© Acronis International GmbH, 2003-2024

백업 경보

경보	설명	경보 해결 방법
백업에 실패	백업 실행 중에 해결 가능한 오류로 인해 백업이 실패하거나 시스템이 종료되어 백업이 중단되면 경보가 생성됩니다.	결함이 발생한 백업 작업의 로그를 확인합니다. 이렇게 하려면 워크로드를 클릭하여 선택하고 **작업**을 클릭한 후 로그에서 경고를 찾습니다. 경고 메시지를 통해 소프트웨어에 알림이 표시된 문제의 근본 원인을 확인할 수 있습니다.
백업에 성공했으나 경고가 표시됨	백업에 성공했으나 경고가 표시되면 경보가 생성됩니다.	VM으로 변환, 복제 또는 유효성 검사 계획의 로그를 확인합니다. 이러한 작업 중에 문제가 발생하면 "작업 실패" 또는 "작업을 완료했으나 경고가 표시됨" 경보가 생성됩니다.
백업이 취소됨	사용자가 백업 작업을 수동으로 취소할 때마다 경보가 생성됩니다.	지금 실행을 클릭하여 백업을 수동으로 시작할 수도 있고 백업이 다음 예약 시간에 실행될 때까지 기다릴 수도 있습니다.
백업 할당 시간이 끝나 백업이 취소됨	백업 작업이 백업 옵션에 지정된 할당 시간에 맞지 않아 누락되면 경보가 생성됩니다.	**성능 및 백업** 창에서 백업 계획의 옵션을 편집하거나 스케줄을 다시 구성합니다. 제품이 포함되어 있는 섹션을 확장하여 지침을 확인합니다.
백업 대기 중	일정이 충돌하여 백업 작업 2개가 동시에 시작될 때마다 이 경보가 생성됩니다. 이 경우에는 첫 번째 백업 작업이 완료되거나 중지될 때까지 두 번째 백업 작업이 대기됩니다.	백업이 일정에 따라 올바른 기간에 실행되는지 확인하고 가능한 경우 스케줄이 충돌하지 않도록 합니다.
백업이 응답하지 않음	실행 중인 백업이 일정 시간 동안 진행되지 않으면(백업이 동결되었을 수 있음) 경보가 생성됩니다.	백업이 잠겨 있으면 이 문제가 발생할 수 있습니다. 이 문서의 내용에 따라 필요한 문제 해결 정보를 수집합니다.
백업이 시작되지 않았음	알 수 없는 이유로 인해 예약된 백업이 시작되지 않은 경우 경보가 생성됩니다.	Acronis Backup 제품의 최신 빌드를 사용 중인지 확인합니다. • 백업 시작 시간에 에이전트 머신이 사용 가능한 상태였던 경우: 1. 백업 작업 시작 시간을 편집합니다. 2. 경보가 다시 표시되면 백업 작업을 다시 생성합니다.

© Acronis International GmbH, 2003-2024

경보	설명	경보 해결 방법
		3. 새로 생성한 백업 작업에서도 경보가 트리거되면 Acronis 지원에 문의하여 지원을 요청합니다. • 에이전트가 오프라인이었던 경우: 1. 백업이 진행되는 시간 동안 머신을 끄지 않습니다. 2. 머신을 끄지 않았다면 Acronis Managed Machine Service가 실행되고 있는지 확인합니다. 이렇게 하려면 시작-> 검색으로 이동하여 services.msc를 입력한 후 Acronis Managed Machine Service를 찾습니다. 도움이 필요하면 Acronis 지원에 문의합니다.
백업이 알 수 없는 상태임	백업 에이전트가 예약된 백업 시간에 오프라인 상태였던 경우 경보가 생성됩니다. 백업 에이전트가 온라인 상태가 되기 전까지 리소스 백업은 알 수 없는 상태가 됩니다.	1. 에이전트가 오프라인 상태인 것이 정상적인 현상인지 확인합니다(예: Management Server 네트워크 외부의 노트북에 설치되어 있는 에이전트). 2. 에이전트가 오프라인이면 안 되는 경우 Acronis Managed Machine Service가 실행되고 있는지 확인합니다. 이렇게 하려면 시작-> 검색으로 이동하여 services.msc를 입력한 후 Acronis Managed Machine Service를 찾아서 해당 상태를 확인합니다. 서비스가 중지되었으면 시작합니다.
백업이 없음	[마지막 백업 이후 경과된 기간]일보다 오랫동안 백업이 정상적으로 완료되지 않은 경우 경보가 생성됩니다.	
백업이 손상됨	유효성 검사 작업에 성공했으나 백업이 손상되었다는 메시지가 표시되면 경보가 생성됩니다.	손상된 백업 문제 해결 문서의 단계를 진행합니다. 아카이브 손상의 근본 원인 파악을 위한 도움이 필요하면 Acronis 지원에 문의합니다.
지속적인 데이터 보호 실패	지속적인 백업 보호가 실패한 경우 경보가 생성됩니다.	다음 제한 사항을 확인합니다. 1. 지속적인 데이터 보호는 NTFS 파일 시스템 및 다음 운영 체제에서만 지원됩니다.

© Acronis International GmbH, 2003-2024

경보	설명	경보 해결 방법
		• 데스크탑: Windows 7 이상 • 서버: Windows Server 2008 R2 이상 2. CDP에서는 **Acronis Secure Zone**이 대상으로 지원되지 않습니다. 3. Windows에 마운트된 NFS 폴더는 지원되지 않습니다. 4. 연속 복제는 지원되지 않습니다. 보호 계획에 위치가 두 개 있으면 첫 번째 대상에서만 CDP 슬라이스가 생성된 후 다음 백업에서 두 번째 대상으로 변경 사항이 복제됩니다. 5. 사용자가 네트워크에서 폴더에 액세스할 때와 같이 네트워크 소스에서 보호된 로컬 폴더의 변경 사항이 적용되는 경우에는 CDP에서 이러한 변경 사항이 감지되지 않습니다. 6. Excel 파일을 변경하는 등 파일을 사용 중인 경우에는 CDP에서 변경 사항이 감지되지 않습니다. CDP에서 변경 사항이 감지되도록 하려면 변경 사항을 저장한 후 파일을 닫습니다.
Hyper-V 호스트 구성이 올바르지 않음	동일한 호스트 이름의 Hyper-V 호스트에 Agent for Hyper-V가 둘 이상 설치되어 있으면 경보가 생성됩니다. 이는 동일한 계정 수준에서 지원되지 않습니다.	충돌을 피하려면 이 계정의 각기 다른 자식 단위에 이러한 Agent for Hyper-V를 등록해야 합니다.
유효성 검사 실패	백업의 유효성 검사 프로세스를 완료할 수 없으면 경보가 생성됩니다.	결함이 발생한 작업의 로그를 확인합니다. 이렇게 하려면 머신을 클릭하여 선택하고 **작업**을 클릭한 후 로그에서 경고를 찾습니다. 경고 메시지를 통해 소프트웨어에 알림이 표시된 문제의 근본 원인을 확인할 수 있습니다.
클라우드 스토리지의 백업을 새 형식으로 이동하는 데 실패함	클라우드 스토리지의 백업을 새 형식으로 마이그레이션하는 데 실패하면 경보가 생성됩니다.	Acronis Cyber Backup Advanced 아카이브를 마이그레이션하는 방법의 설명은 여기에 나와 있습니다. Acronis Cyber Backup 아카이브를 마이그레이션하는 방법의 설명은 여기에 나와 있습니다. Acronis 지원에 문의하기 전에 migrate_

© Acronis International GmbH, 2003-2024

경보	설명	경보 해결 방법
		archives 도구를 사용하여 다음 보고서를 수집하십시오. **migrate_archives.exe --account=<Acronis 계정> --password=<비밀번호> --subaccounts=All > report1.txt** **migrate_archives.exe --cmd=finishUpgrade --account=<Acronis 계정> --password=<비밀번호> > report2.txt**
암호화 비밀번호가 없음	데이터베이스 암호화 키가 잘못되었거나 손상되었거나 누락된 경우 경보가 생성됩니다.	비밀번호를 잃어버리거나 기억나지 않으면 암호화된 백업을 복구할 방법이 없습니다. 암호화 비밀번호는 보호된 장치에서 로컬로 설정해야 합니다. 보호 계획에서 암호화 비밀번호를 설정할 수는 없습니다. 자세한 내용은 암호화 비밀번호 설정을 참조하십시오.
업로드 보류 중	이 백업 계획을 위한 클라우드 아카이브로의 실제 데이터 전달이 스토리지에 업로드되지 않은 것으로 예약된 검사에서 확인되면 경보가 생성됩니다.	
백업 복구 실패	파일이나 시스템 백업 복구를 시도했는데 복구 작업이 실패하면 경보가 생성됩니다.	정확한 백업 실패 날짜를 확인한 후 마지막으로 성공한 백업을 사용하여 복구를 시도합니다.

재해 복구 경보

경보	설명	경보 해결 방법
스토리지 할당량 초과	재해 복구 스토리지의 소프트 할당량이 초과되면 경보가 생성됩니다	할당량을 늘리거나 클라우드 스토리지에서 일부 아카이브를 제거합니다.
할당량에 도달함	다음과 같은 상황에서 경보가 생성됩니다. • 클라우드 서버의 소프트 할당량 초과. • 컴퓨팅 포인트의 소프트 할당량 초과. • 공용 IP 주소의 소프트 할당	

© Acronis International GmbH, 2003-2024

경보	설명	경보 해결 방법
	량 초과.	
스토리지 할당량 초과됨	재해 복구 스토리지의 하드 할당량이 초과되면 경보가 생성됩니다. 이 스토리지는 기본 및 복구 서버에서 사용됩니다. 이 할당량 초과분에 도달한 경우 기본 및 복구 서버를 만들거나, 기존 기본 서버에 디스크를 추가/확장할 수 없습니다. 이 할당량 초과분이 초과된 경우 장애 조치를 시작하거나, 중지된 서버를 시작할 수 없습니다. 실행 중인 서버는 계속 실행됩니다.	
할당량 초과됨	다음과 같은 상황에서 경보가 생성됩니다. • 클라우드 서버의 하드 할당량 초과. • 컴퓨팅 포인트의 하드 할당량 초과. • 공용 IP 주소의 하드 할당량 초과.	장치 할당량을 추가로 구매하거나 더 이상 보호하지 않아도 되는 장치의 백업 작업을 비활성화합니다.
장애 조치 오류	장애 조치 작업을 제출한 후 시스템 문제가 발생한 경우 경보가 생성됩니다.	1. 복구 서버에서 **편집**을 클릭합니다. 자세한 내용은 복구 서버 생성을 참조하십시오. 2. 복구 서버의 CPU/RAM을 줄입니다. 3. 장애 조치를 다시 시도합니다.
테스트 장애 조치 오류	테스트 작업을 제출한 후 시스템 문제가 발생한 경우 경보가 생성됩니다.	1. 복구 서버에서 **편집**을 클릭합니다. 자세한 내용은 복구 서버 생성을 참조하십시오. 2. 복구 서버의 CPU/RAM을 줄입니다. 3. 장애 조치를 다시 시도합니다. **참고** 운영 네트워크의 IP 주소에 DHCP 서버에 구성된 것과 동일한 IP 주소가 있는지 확인합니다.
장애 복구 오류	장애 복구를 시작한 후 시스템	백업 스토리지 목록에서 잘못된 위치

© Acronis International GmbH, 2003-2024

경보	설명	경보 해결 방법
	문제가 발생한 경우 경보가 생성됩니다.	를 확인할 수 있습니다. 잘못된 위치는 사용자가 생성하지 않았으며 이름 대신 숫자로 표시되는 위치입니다(일반적으로 위치 이름은 기존 최종 사용자 이름 중 하나와 일치함). 잘못된 위치를 제거합니다. 1. Cyber Protect 콘솔에서 백업 스토리지로 이동합니다. 2. 위치를 찾은 후 x 아이콘을 클릭하여 삭제합니다. 3. 삭제를 클릭하여 선택을 확인합니다. 4. 장애 조치를 다시 시도합니다.
장애 복구 취소됨	사용자가 장애 복구를 취소한 경우 경보가 생성됩니다.	콘솔에서 경보를 수동으로 해제합니다.
VPN 연결 오류	사용자 작업과는 관계가 없는 이유로 인해 VPN 연결 오류가 발생하면 경보가 생성됩니다. VPN 어플라이언스의 상태 보고서가 오래된 상태입니다.	Acronis VPN 어플라이언스 디플로이 또는 연결 관련 문제가 발생했다면 Acronis 지원에 문의하십시오. 다음 정보를 기입한 이메일을 보내주시기 바랍니다. • 오류 메시지(표시된 경우)의 스크린샷 • Acronis VPN 어플라이언스 CLI 인터페이스의 스크린샷 • Acronis Backup Cloud 데이터 센터 및 그룹 이름.
(VPN에 연결할 수 없음) 연결 게이트웨이에 연결할 수 없음	DR 서비스가 연결 게이트웨이에 연결할 수 없으면 경보가 생성됩니다. 연결 게이트웨이의 상태 보고서가 오래된 상태입니다.	Acronis VPN 어플라이언스 디플로이 또는 연결 관련 문제가 발생했다면 Acronis 지원에 문의하십시오. 다음 정보를 기입한 이메일을 보내주시기 바랍니다. • 오류 메시지(표시된 경우)의 스크린샷 • Acronis VPN 어플라이언스 CLI 인터페이스의 스크린샷 • Acronis Backup Cloud 데이터 센터 및 그룹 이름
DR IP 재할당 필요	VPN 어플라이언스에서 네트워크 변경 사항을 감지하면 경보가 생성됩니다.	IP 주소를 재할당합니다. 자세한 내용은 IP 주소 재할당을 참조하십시오.

© Acronis International GmbH, 2003-2024

경보	설명	경보 해결 방법
연결 게이트웨이 오류	클라우드에서 VPN 서버를 디플로이하지 못한 경우 경보가 생성됩니다.	연결 확인 도구를 사용하여 연결 게이트웨이 출력에서 오류를 확인합니다. 방화벽 및 안티맬웨어 소프트웨어의 애플리케이션 제어에서 Acronis 소프트웨어를 허용합니다.
주 서버 생성 실패	오류로 인해 주 서버가 생성되지 않은 경우 경보가 생성됩니다.	
복구 서버 생성 실패	오류로 인해 복구 서버가 생성되지 않은 경우 경보가 생성됩니다.	복구 서버의 구성이 소프트웨어 요구 사항과 일치하는지 확인합니다.
주 서버 삭제	주 서버가 삭제된 경우 경보가 생성됩니다.	
서버 복구 실패	주 서버나 복구 서버를 복구하지 못한 경우 경보가 생성됩니다.	상세 정보를 확인합니다. 오류 메시지가 "내부 오류"와 같이 일반적이거나 명확하지 않은 내용이라면 **재해 복구 → 서버**로 이동하여 오류의 영향을 받은 머신을 선택하고 **작업**을 클릭합니다. 작업을 클릭하고 Ctrl 키를 누른 상태로 작업을 마우스 왼쪽 버튼으로 클릭합니다. 그러면 모든 작업 옆에 말줄임표(...) 기호가 표시됩니다. **작업 활동 정보**를 클릭하여 선택합니다.
백업에 실패	클라우드 서버(주 서버 또는 운영 장애 조치 상태의 서버)의 백업이 실패한 경우 경보가 생성됩니다.	1. 백업 위치의 연결을 확인합니다. 2. 백업 스토리지 장치(로컬 백업)를 확인합니다.
네트워크 제한 초과	최대 클라우드 네트워크 수(네트워크 5개)에 도달하면 경보가 발생합니다.	
런북 오류	런북 실행이 실패하면 경보가 생성됩니다.	제품 기능에는 아무런 영향이 없으므로 해당 경보는 무시해도 됩니다. 자세한 내용은 런북 생성을 참조하십시오.
런북 경고	런북 실행이 완료되었으나 경고가 표시되면 경보가 생성됩니다.	제품 기능에는 아무런 영향이 없으므로 해당 경보는 무시해도 됩니다. 자세한 내용은 런북 생성을 참조하십시오.

© Acronis International GmbH, 2003-2024

경보	설명	경보 해결 방법
런북 사용자 상호 작용이 필요함	런북이 사용자 상호 작용 대기 중이면 경보가 생성됩니다.	제품 기능에는 아무런 영향이 없으므로 해당 경보는 무시해도 됩니다. 자세한 내용은 런북 생성을 참조하십시오.
인터넷 트래픽 차단됨	관리자가 인터넷 트래픽을 차단한 경우 경보가 생성됩니다.	
인터넷 트래픽 차단 해제됨	관리자가 인터넷 트래픽을 차단 해제한 경우 경보가 생성됩니다.	
로컬 네트워크 겹침	동일하거나 겹치는 로컬 네트워크가 감지되면 경보가 생성됩니다.	
라이선스 전환 서버 할당량 부족	클라우드 서버 할당량이 부족하면 경보가 생성됩니다.	• 테넌트와 사용자에게 실제 서버에 사용할 수 있는 웹 호스팅 서버 할당량 또는 서버 할당량이 있는지 확인합니다. • 테넌트와 사용자에게 가상 서버에 사용할 수 있는 웹 호스팅 서버 할당량 또는 가상 머신 할당량이 있는지 확인합니다. 가상 서버는 서버 할당량을 사용할 수 없습니다.
라이선스 전환 제공 항목 부족	재해 복구 스토리지 제공 항목이 비활성화되어 있으면 경보가 생성됩니다.	자세한 내용은 재해 복구 할당량을 참조하십시오.
라이선스 전환 오류	재해 복구 업그레이드에서 오류가 발생한 경우 경보가 생성됩니다.	
라이선스 전환 컴퓨팅 포인트 부족	사용 가능한 컴퓨팅 포인트가 없으면 경보가 생성됩니다.	관리 포털에서 컴퓨팅 포인트의 하드 할당량을 확인한 후 늘립니다.
라이선스 전환 서버 제공 항목 부족	클라우드 서버 제공 항목이 비활성화되어 있으면 경보가 생성됩니다.	
정책에서 복구 서버 생성 실패	재해 복구 인프라를 설정하는 중 오류가 발생한 경우 경보가 생성됩니다.	인터넷 액세스 속성을 사용하지 않고 복구 서버를 수동으로 생성합니다. 자세한 내용은 복구 서버 생성을 참조하십시오
백업 프로세서 자동 테스트 장애 조치 재예약됨	자동 테스트 장애 조치 실행이 재예약된 경우 경보가 생성됩니다.	

© Acronis International GmbH, 2003-2024

경보	설명	경보 해결 방법
백업 프로세서 자동 테스트 장애 조치 시간 초과 도달	자동 테스트 장애 조치 작업이 만료된 경우 경보가 생성됩니다. **참고** 각 자동 테스트 장애 조치 실행에서는 비용 청구 대상 컴퓨팅 포인트가 사용됩니다.	
백업 프로세서 자동 테스트 장애 조치 전체 실패	복구 서버의 마지막으로 예약된 자동 테스트 장애 조치가 실패한 경우 경보가 생성됩니다.	1. 복구 서버의 테스트 장애 조치를 수동으로 시작합니다. 자세한 내용은 테스트 장애 조치 수행을 참조하십시오. 2. 자동 테스트 장애 조치를 수행하도록 예약한 다음 날짜까지 기다립니다
장애 복구 데이터 전송 오류	장애 복구 데이터 전송이 실패하면 경보가 생성됩니다.	
장애 복구 실패	장애 복구에서 오류가 발생하면 경보가 생성됩니다.	백업 스토리지 목록에서 잘못된 위치를 확인할 수 있습니다. 잘못된 위치는 사용자가 생성하지 않았으며 이름 대신 숫자로 표시되는 위치입니다(일반적으로 위치 이름은 기존 최종 사용자 이름 중 하나와 일치함). 잘못된 위치를 제거합니다. 1. Cyber Protection에서 백업 스토리지로 이동합니다. 2. 위치를 찾은 후 x 아이콘을 클릭하여 삭제합니다. 3. **삭제**를 클릭하여 선택을 확인합니다. 장애 조치를 다시 시도합니다.
장애 복구 확인 실패	장애 복구 확인이 실패한 경우 경보가 생성됩니다.	
장애 복구 머신 전환 준비 완료	머신을 전환할 준비가 되면 경보가 생성됩니다.	
장애 복구 전환 완료	전환이 정상적으로 완료되면 경보가 생성됩니다.	콘솔에서 경보를 수동으로 해제합니다.
장애 복구 대상 에이전트 오프라인	에이전트가 오프라인이면 경보가 생성됩니다.	

© Acronis International GmbH, 2003-2024

안티맬웨어 보호 경보

경보	설명	경보 해결 방법
의심스러운 원격 연결 작업이 감지됨	원격 연결에서 전송된 랜섬웨어가 감지되면 경보가 생성됩니다.	콘솔에서 경보를 수동으로 해제합니다.
의심스러운 작업이 감지됨	워크로드에서 랜섬웨어가 감지되면 경보가 생성됩니다.	콘솔에서 경보를 수동으로 해제합니다.하여 경보를 비활성화하십시오. Active Protection 계획에서 지정한 옵션에 따라 악성 프로세스가 중지되거나 해당 프로세스에서 적용된 변경 사항이 원래대로 돌아갈 수도 있고, 아직 아무런 작업이 수행되지 않아 이 문제를 수동으로 해결해야 할 수도 있습니다. 경보 상세 정보를 확인하여 파일을 암호화하는 프로세스와 영향을 받은 파일을 파악합니다. 파일을 암호화하는 프로세스가 제한된 프로세스로 확인되면(위양성 경보) 신뢰할 수 있는 프로세스에 이 프로세스를 추가합니다. 1. Active Protection 계획을 엽니다. 2. **편집**을 클릭하여 설정을 수정합니다. 3. **신뢰할 수 있는 프로세스**에서 랜섬웨어로 간주하지 않을 신뢰할 수 있는 프로세스를 지정합니다. 드라이브 문자로 시작하는 프로세스 실행 파일의 전체 경로를 지정합니다. 예: C:\Windows\Temp\er76s7sdkh.exe.
크립토마이닝 작업이 감지됨	워크로드에서 불법적인 크립토마이너가 감지되면 경보가 생성됩니다	콘솔에서 경보를 수동으로 해제합니다.
MBR 보호 의심스러운 작업이 감지되어 중단됨	워크로드에서 랜섬웨어가 감지되면(구체적으로는 랜섬웨어에 의해 MBR/GPT 파티션이 수정되면) 경보가 생성됩니다.	콘솔에서 경보를 수동으로 해제합니다.
지원되지 않는 네트워크 경로가 지정되었습니다	관리자가 제공한 복구 경로가 로컬 폴더 경로가 아니면 경보가 생성됩니다.	네트워크 폴더 보호의 로컬 경로(복구 경로)를 지정합니다. 콘솔에서 경보를 수동으로 해제합니다
중요 프로세스가 Active Protection 계획에 유해한 항목으로 추가되었습니다	중요 프로세스가 보호 제외 목록에 차단된 프로세스로 추가되어 있으면 경보가 생성됩니다.	콘솔에서 경보를 수동으로 해제합니다.

© Acronis International GmbH, 2003-2024

경보	설명	경보 해결 방법
Active Protection 정책을 적용하지 못했습니다	Active Protection 정책을 적용하지 못한 경우 경보가 생성됩니다.	오류 메시지에서 Active Protection 정책을 적용하지 못한 이유를 확인합니다.
Secure Zone: 인증되지 않은 작업이 감지되어 차단됨	워크로드에서 랜섬웨어가 감지되면(랜섬웨어에 의해 ASZ 파티션이 수정되면) 경보가 생성됩니다.	콘솔에서 경보를 수동으로 해제합니다.
Active Protection 서비스가 실행되지 않음	Active Protection 서비스가 작동 중단되었거나 실행되고 있지 않으면 경보가 생성됩니다.	오류 메시지에서 Active Protection 서비스가 실행되고 있지 않은 이유를 확인합니다.
Active Protection 서비스를 사용할 수 없습니다	드라이버가 호환되지 않거나 누락되어 Active Protection 서비스를 사용할 수 없으면 경보가 생성됩니다.	Windows 이벤트 로그에서 Acronis Active Protection 서비스(acronis_protection_service.exe) 작동 중단 여부를 확인합니다.
다른 보안 솔루션과의 충돌	다른 보안 솔루션과의 충돌이 감지되어 머신 '{{resourceName}}'에 대해 Active Protection을 사용할 수 없으면 경보가 발생합니다. Active Protection을 활성화하려면 충돌하는 보안 솔루션을 비활성화하거나 설치 제거하십시오.	**해결 방법 1**: Acronis 실시간 보호를 사용하려는 경우 머신에서 서드 파티 안티바이러스 솔루션을 제거합니다. **해결 방법 2**: 서드 파티 안티바이러스 솔루션을 사용하려는 경우 보호 계획에서 Acronis 실시간 보호, URL 필터링 및 Windows Defender 바이러스 백신을 비활성화합니다.
격리 작업 실패	안티맬웨어 기능이 감지된 맬웨어를 격리하지 못한 경우 경보가 생성됩니다.	오류 메시지에서 격리가 실패한 이유를 확인합니다.
악성 프로세스가 감지됨	동작 엔진이 맬웨어(프로세스 유형)를 감지하면 경보가 생성됩니다. 감지된 맬웨어는 격리된 상태입니다.	콘솔에서 경보를 수동으로 해제합니다.
악성 프로세스가 감지되었으나 격리되지 않음	동작 엔진이 맬웨어(프로세스 유형)를 감지하면 경보가 생성됩니다. 감지된 맬웨어는 격리되지 않은 상태입니다.	콘솔에서 경보를 수동으로 해제합니다.
맬웨어가 감지되어 차단됨(ODS)	예약된 스캔에서 맬웨어가 감지되면 경보가 생성됩니다. 감지된 맬웨어는 격리된 상태입니다.	콘솔에서 경보를 수동으로 해제합니다.

© Acronis International GmbH, 2003-2024

경보	설명	경보 해결 방법
맬웨어가 감지되어 차단됨(RTP)	실시간 보호에서 맬웨어가 감지되면 경보가 생성됩니다. 감지된 맬웨어는 격리된 상태입니다.	콘솔에서 경보를 수동으로 해제합니다.
백업 중 맬웨어 감지됨	백업 스캔 중에 맬웨어가 감지되면 경보가 생성됩니다.	콘솔에서 경보를 수동으로 해제합니다.
실시간 안티맬웨어 보호와 보안 제품 간에 충돌이 감지되었습니다	Windows 보안 센터에 안티맬웨어 기능을 등록하지 못한 경우 경보가 생성됩니다.	서드 파티 보안 제품을 비활성화 또는 제거하거나 보호 계획에서 실시간 안티맬웨어 보호 기능을 비활성화합니다.
Microsoft Security Essentials 모듈을 실행하지 못함	Microsoft Security Essentials 모듈을 실행하지 못한 경우 경보가 생성됩니다.	오류 메시지에서 Microsoft Security Essentials 모듈을 실행하지 못한 이유를 확인합니다.
서드 파티 안티바이러스 소프트웨어가 설치되어 있으므로 실시간 보호를 사용할 수 없습니다	서드 파티 안티바이러스에 실시간 보호 기능이 아직 활성화되어 있어 실시간 보호를 켜지 못한 경우 경보가 생성됩니다.	서드 파티 보안 제품을 비활성화 또는 제거하거나 보호 계획에서 실시간 안티맬웨어 보호 기능을 비활성화합니다.
드라이버가 호환되지 않거나 누락되어 실시간 보호를 사용할 수 없습니다	드라이버가 호환되지 않거나 누락되어 실시간 보호를 사용할 수 없으면 경보가 생성됩니다.	오류 메시지에서 Acronis가 워크로드에 드라이버를 설치하지 못한 이유를 확인합니다.
사이버 보호(또는 Active Protection) 서비스가 응답하지 않음	사이버 보호 서비스가 콘솔에서 전송된 상태 검사 ping에 응답을 하면 경보가 생성됩니다.	콘솔에서 경보를 수동으로 해제합니다.
보안 정의 업데이트 실패	보안 정의 업데이트가 실패한 경우 경보가 생성됩니다.	오류 메시지에서 보안 정의 업데이트가 실패한 이유를 확인합니다.
탬퍼 보호가 활성화됨	탬퍼 보호가 활성화되어 있어서 Microsoft Defender 설정을 변경할 수 없는 경우 경보가 생성됩니다.	Windows 워크로드에서 탬퍼 보호 설정을 비활성화합니다.
Windows Defender 모듈 실행 실패	Windows Defender 모듈 실행이 실패한 경우 경보가 생성됩니다.	오류 메시지에서 Windows Defender 모듈을 실행하지 못한 이유를 확인합니다.
Windows Defender가 제3자 안티바이러스 소프트웨어에 의해 차단되었습니다	서드 파티 안티바이러스가 머신에 설치되어 있어 Windows Defender가 차단되면 경보가 생성됩니다.	서드 파티 보안 제품을 비활성화 또는 제거합니다.

© Acronis International GmbH, 2003-2024

경보	설명	경보 해결 방법
그룹 정책 충돌	그룹 정책이 Microsoft Defender 설정을 제어하므로 설정을 변경할 수 없는 경우 경보가 생성됩니다.	Windows 워크로드에서 그룹 정책 설정을 비활성화합니다.
Microsoft Security Essentials이 맬웨어로부터 이 머신을 보호하기 위해 작업을 수행함	Microsoft Security Essentials가 맬웨어를 삭제/격리한 경우 경보가 생성됩니다.	콘솔에서 경보를 수동으로 해제합니다.
Microsoft Security Essentials이 맬웨어를 감지함	Microsoft Security Essentials가 맬웨어 또는 원치 않을 수 있는 소프트웨어를 감지한 경우 경보가 생성됩니다.	콘솔에서 경보를 수동으로 해제합니다.

라이선스 경보

경보	설명	경보 해결 방법
스토리지 할당량에 거의 도달함	정리 또는 할당량 업그레이드 후 사용량이 80% 미만으로 떨어지면 경보가 생성됩니다.	스토리지를 추가로 구매하거나 클라우드 스토리지의 공간을 확보합니다.
스토리지 할당량 초과됨	스토리지 할당량 100%를 모두 사용하면 경보가 생성됩니다.	스토리지 공간을 더 구매합니다. 구매 방법에 대한 자세한 내용은 클라우드 스토리지를 더 구매하는 방법을 참조하십시오.
워크로드 할당량에 도달함	제공 항목의 사용량이 0보다 크고 사용량이 할당량보다 많은데 사용량이 할당량과 초과분을 합한 값 이상이면 경보가 생성됩니다.	
워크로드 할당량이 초과됨	제공 항목의 사용량이 할당량과 초과분을 합한 값보다 크면 경보가 생성됩니다.	
워크로드에 백업 계획에 적용할 할당량이 없습니다(리소스에 서비스 할당량이 없음)	다음과 같은 상황에서 경보가 생성됩니다. • 할당량이 수동으로 제거됨: **장치** > **상세 정보** > **서비스 할당량**으로 이동한 후 **변경**을 클릭하고 **할당량 없음** 옵션 선택. • 관리 콘솔 제공 항목이 비활성화됨. • 제공 항목의 관리 콘솔 할당량	

© Acronis International GmbH, 2003-2024

경보	설명	경보 해결 방법
	과 초과분을 합한 값이 현재 사용량 미만으로 낮아짐.	
할당량이 지정된 워크로드를 보호할 수 없음	제공 항목이 충분하지 않으며 다음과 같은 항목이 필요한 경우 경보가 생성됩니다. • 동적 그룹. • 해당 그룹에 할당된 백업 계획. • 해당 동적 그룹에 속하는 리소스를 추가했는데 특정 특성으로 인해 이 리소스에 동일한 백업 계획을 적용할 수 없음.	
서브스크립션 라이센스가 만료됨	라이선스/유지보수 만료 경보를 확인하는 일일 검사에서 라이선스 서버에 요청을 전송했는데 라이센스가 만료되었다는 응답을 받은 경우 경보가 생성됩니다.	구독이 만료되고 나면 구독을 추가로 갱신할 때까지 복구를 제외한 모든 제품 기능이 차단됩니다. 백업된 데이터는 복구를 위해 계속 액세스 가능합니다. 새 라이선스를 구매합니다. **참고** 최근 새 구독을 구매했는데 구독이 만료되었다는 메시지가 계속 표시되면 Acronis 계정에서 새 구독을 가져와야 합니다. 이렇게 하려면 관리 콘솔에서 설정 -> 라이선스로 이동하여 오른쪽 상단 모서리에서 동기화를 클릭합니다. 그러면 구독이 동기화됩니다.
가입 라이센스가 곧 만료됨	라이선스/유지보수 만료 경보를 확인하는 일일 검사에서 라이선스 서버에 요청을 전송했는데 라이선스 만료 날짜까지 남은 기간이 30일 미만이라는 응답을 받은 경우 경보가 생성됩니다.	새 구독을 구매합니다.

URL 필터링 경보

경보	설명	경보 해결 방법
악성 URL 차단됨	URL 필터링을 통해 악성 URL이 차단되면 경보가 생성됩니다.	URL 필터링 설정을 확인합니다. URL 필터링은 URL 필터링 설정에 따라 차단되어야 하는 페이지를 차단합니다.

© Acronis International GmbH, 2003-2024

경보	설명	경보 해결 방법
악성 URL 경고가 무시됨	URL 필터링을 통해 차단된 악성 URL로 계속 이동하도록 선택한 경우 경보가 생성됩니다.	URL 필터링 설정을 확인합니다.
URL 필터링과 보안 제품 간에 충돌이 감지되었습니다	다른 보안 제품과의 충돌로 인해 URL 필터링을 활성화할 수 없으면 경보가 생성됩니다.	URL 필터링 설정을 확인합니다.
웹사이트 URL이 차단되었습니다	URL이 URL 필터링의 차단됨 카테고리에 지정되어 있는 모든 기준을 충족하면 경보가 생성됩니다.	URL 필터링 설정을 확인합니다.

EDR 경보

경보	설명	경보 해결 방법
인시던트 감지됨	인시던트가 생성되거나 기존 인시던트의 상태가 업데이트되면 경보가 생성됩니다.	이 경보에서 새 인시던트 관련 정보 또는 이전 인시던트의 업데이트 여부를 확인할 수 있습니다. 경보는 확인한 후 닫을 수 있습니다. 필요한 경우 인시던트를 열어 추가로 조사할 수 있습니다.
침해 지표(IOC) 감지됨	EDR IOC 위협 검색 서비스에서 새 침해 지표가 감지된 경우 경보가 생성됩니다.	이 경보는 하나 이상의 워크로드에서 IOC가 감지되었음을 알려 줍니다. 경보를 확인한 후 경보의 링크를 클릭하여 IOC 관련 상세 정보를 확인할 수 있습니다.
워크로드를 네트워크에서 분리하지 못했습니다	사용자가 네트워크에서 머신을 분리하는 작업을 트리거했는데 분리 작업이 실패하면 경보가 생성됩니다.	필요한 조치를 취합니다.
워크로드를 네트워크에 다시 연결하지 못했습니다	사용자가 네트워크에 머신을 다시 연결하는 작업을 트리거했는데 해당 작업이 실패한 경우 경보가 생성됩니다.	필요한 조치를 취합니다.
Windows Defender 방화벽 설정이 수정되었습니다	분리된 머신에서 방화벽의 설정이 수정된 경우 경보가 생성됩니다.	이 경보는 분리된 머신에서 방화벽 상세 정보가 수정되었음을 알려 줍니다. 이 경보는 정보 제공용이므로 확인 후 닫으면 됩니다.

© Acronis International GmbH, 2003-2024

장치 제어 경보

경보	설명	경보 해결 방법
장치 제어 및 데이터 손실 방지가 제한된 기능으로 실행됨(호환되지 않는 CPU 감지됨)	CET 기술을 지원하는 CPU가 장착된 실제 머신에서 DeviceLock 에이전트가 시작된 경우 경보가 생성됩니다.	경보가 생성되지 않도록 영향을 받은 머신에서 옵션을 비활성화합니다.
macOS Ventura에서 장치 제어 기능이 아직 지원되지 않음	실제 macOS Ventura 머신에서 DeviceLock 에이전트가 시작되었는데 해당 에이전트에 장치 제어가 포함된 보호 계획이 적용되어 있으면 경보가 생성됩니다. DeviceLock 드라이버로 인해 커널 패닉에 문제가 발생하는 버전에만 해당됩니다.	
민감한 데이터의 전송이 허용됨	민감한 내용의 전송이 허용되는 경우 경보가 생성됩니다.	
민감한 데이터의 전송이 정당화됨	민감한 내용의 전송이 정당화되는 경우 경보가 생성됩니다.	
민감한 데이터의 전송이 거부됨	민감한 내용의 전송이 차단되는 경우 경보가 생성됩니다.	
데이터 손실 방지 관찰 모드의 결과 검토	관찰 결과를 검토해야 하는 다음과 같은 상황에서 경보가 생성됩니다. • Advanced DLP 팩 라이선스가 적용되지 않음. • 워크로드 하나 이상에 적용된 보호 계획에서 관찰 모드를 활성화한 후 한 달이 지남. • 유사한 경보가 마지막으로 발생한 후 한 달이 지났으며 관찰 모드에서 특정 DLP 사용이 감지됨.	
사용자의 보안 식별자가 변경됨	알려진 사용자 이름의 SID가 업데이트되면 경보가 생성됩니다. 도메인에 속하지 않은 PC에 OS를 다시 설치하면 이러한 현상이 발생할 수 있습니다.	
주변 장치 접근이 차단됨	지원되는 장치에서 특정 작업(읽기/쓰기 작업)이 차단되면 경보가 생성됩니다.	
원격 SSL 리소스에 연결할 수 없습니다.	리소스에서 사용되는 추가 핸드셰이크 방지로 인해 원격 SSL 리소스에 대한 액세스가 차단되면 경보가 생	원격 호스트를 위한 허용 목록에 리소스를 추가하십시오.

© Acronis International GmbH, 2003-2024

경보	설명	경보 해결 방법
	성됩니다.	

시스템 경보

경보	설명	경보 해결 방법
에이전트가 오래된 버전임	에이전트 버전이 오래된 경우 경보가 생성됩니다.	에이전트 목록으로 이동하여 에이전트 업데이트를 시작합니다.
자동 업데이트 실패	에이전트 자동 업데이트가 실패한 경우 경보가 생성됩니다.	수동 업데이트를 수행해 봅니다.
새 에이전트를 설치한 후 장치를 다시 시작해야 합니다	원격 설치가 정상적으로 완료된 후 재부팅이 필요하면 경보가 생성됩니다.	워크로드를 다시 시작합니다.
작업 실패	작업이 실패한 경우 경보가 생성됩니다.	머신에서 모든 Acronis 서비스를 다시 시작합니다.
작업에 성공했으나 경고가 표시됨	작업은 정상적으로 완료되었으나 경고가 생성된 경우 경보가 생성됩니다.	
작업이 응답하지 않음	진행 중인 작업이 응답하지 않으면 경보가 생성됩니다.	
계획 배포 실패	보호 계획 디플로이먼트가 실패한 경우 경보가 생성됩니다.	
사용자 이름을 SID로 변환하지 못했습니다	스케줄 SID 변환이 실패한 경우 경보가 생성됩니다.	

경보 위젯

경보 위젯에서는 워크로드와 관련된 경보의 다음 상세정보를 확인할 수 있습니다.

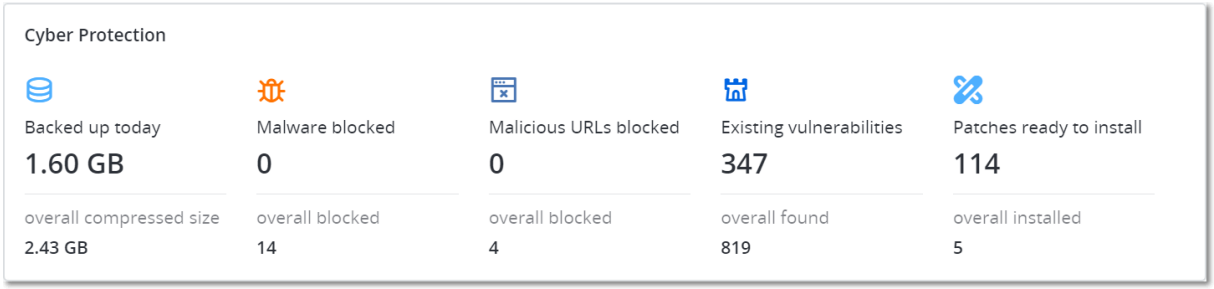
필드	설명
최신 경보 5개 위젯	최신 경보 5개가 포함된 목록이 표시됩니다.
경보 내역 요약	경보 심각도, 경보 유형 및 시간 범위를 기준으로 경보가 표시되는 그래픽 위젯입니다.
활성 경보 요약	경보 심각도와 경보 유형 및 활성 경보의 합계를 기준으로 활성 경보가 표시되는 그래픽 위젯입니다.
경보 내역	경보 내역이 표시되는 테이블 보기입니다.

© Acronis International GmbH, 2003-2024

필드	설명
활성 경보 상세정보	활성 경보가 표시되는 테이블 보기입니다.

Cyber Protection

이 위젯은 백업 크기, 차단된 맬웨어, 차단된 URL, 발견한 취약성, 설치된 패치 등의 전반적인 정보를 보여줍니다.



상단 행에는 현재 통계가 표시됩니다.

- **오늘 백업됨** – 지난 24시간에 해당하는 복구 지점의 전체 크기
- **맬웨어 차단됨** – 차단된 맬웨어에 대한 현재 활성 경보의 수
- **차단된 URL** – 차단된 URL에 대한 현재 활성 경보의 수
- **기존 취약성** – 현재 존재하는 취약성의 수
- **패치 설치 준비 완료** – 현재 설치 가능한 패치의 수

하단 행에는 전체 통계가 표시됩니다.

- 모든 백업의 압축된 크기
- 모든 머신 전반에서 차단된 맬웨어의 누적 수
- 모든 머신 전반에서 차단된 URL의 누적 수
- 모든 머신 전반에서 검색된 취약성의 누적 수
- 모든 머신 전반에서 설치된 업데이트/패치의 누적 수

보호 상태

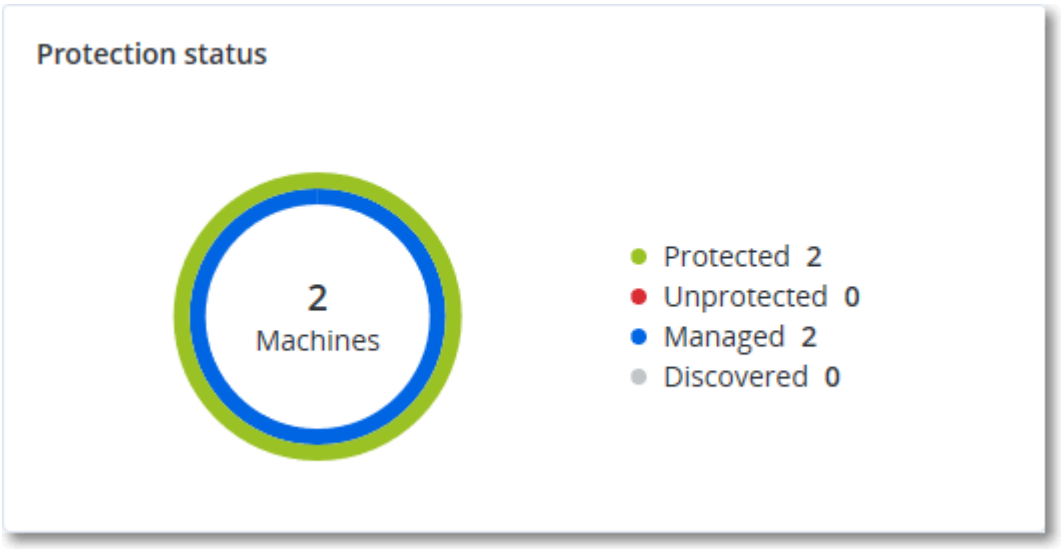
이 위젯은 모든 머신에 대한 현재 보호 상태를 표시합니다.

머신은 다음과 같은 상태일 수 있습니다.

- **보호됨** – 보호 계획이 적용되어 있는 머신입니다.
- **보호되지 않음** – 보호 계획이 적용되어 있지 않은 머신입니다. 여기에는 보호 계획이 적용되지 않은 검색된 머신 및 관리 대상 상태의 머신이 모두 포함됩니다.
- **관리 대상** – 보호 에이전트가 설치되어 있는 머신입니다.
- **검색됨** – 보호 에이전트가 설치되어 있지 않은 머신입니다.

© Acronis International GmbH, 2003-2024

머신 상태를 클릭하면 해당 상태의 머신 목록으로 리디렉션되어 자세한 정보를 확인할 수 있습니다.



검색된 머신

이 위젯은 지정한 기간 동안 검색된 머신 목록을 표시합니다.

Discovered machines

Device name ↑	IP address	OS	Organizational unit	Discovery type
Windows Server 2012 R2				
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Local Network
Windows 10 Enterprise 2016 LTSB				
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Local Network
device2	-	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory
device3	10.248.91.243	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Manual, Loc...
device4	10.248.91.125	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Local Network
device5	-	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Manual
-				
-	10.250.41.189	-	-	Manual
-	10.248.44.199	-	-	Manual

EDR(엔드포인트 탐지 및 대응) 위젯

EDR(Endpoint Detection and Response)에는 7개 위젯이 포함되어 있습니다. **개요** 대시보드에서 7개 위젯에 모두 액세스할 수 있습니다. 이러한 위젯 중 3개는 EDR 기능 내에도 기본적으로 표시됩니다("인시던트 검토"(817페이지) 참조).

사용 가능한 7개 위젯은 다음과 같습니다.

- 워크로드별 상위 인시던트 분산
- 위협 상태(EDR에 표시됨)

© Acronis International GmbH, 2003-2024

- 인시던트 심각도 이력(EDR에 표시됨)
- 보안 인시던트 MTTR
- 보안 인시던트 번다운(Burndown)
- 전술별 감지(EDR에 표시됨)
- 워크로드 네트워크 상태

워크로드별 상위 인시던트 분산

이 위젯에는 인시던트 수가 가장 많은 상위 워크로드 5개가 표시됩니다. **모두 표시**를 클릭하면 인시던트 목록으로 리디렉션됩니다. 인시던트 목록은 위젯 설정에 따라 필터링됩니다.

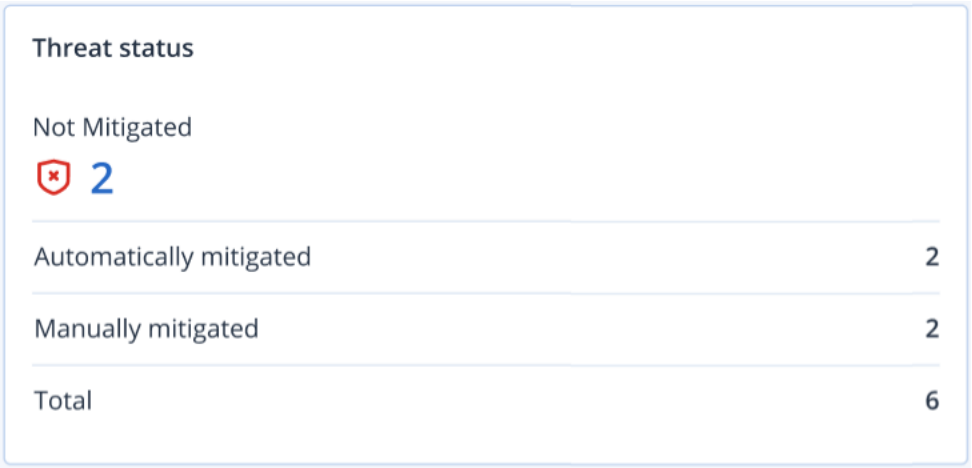
워크로드 행을 마우스로 가리키면 인시던트의 현재 조사 상태 세부 정보를 확인할 수 있습니다. 조사 상태는 **시작되지 않음**, **조사 중**, **종결됨**, **위양성** 중 하나입니다. 그런 다음 추가로 분석할 워크로드를 클릭면 위젯 설정에 따라 인시던트 목록이 새로 고쳐집니다.

위협 상태

이 위젯에는 모든 워크로드의 현재 위협 상태가 표시됩니다. 그리고 완화되지 않아 조사가 필요한 인시던트의 현재 수가 강조 표시됩니다. 그리고 수동으로 및/또는 시스템에서 자동으로 완화된 인시던트의 수도 표시됩니다.

완화되지 않음 상태인 인시던트의 수를 클릭하면 인시던트 목록이 필터링되어 완화되지 않은 인시던트가 표시됩니다.

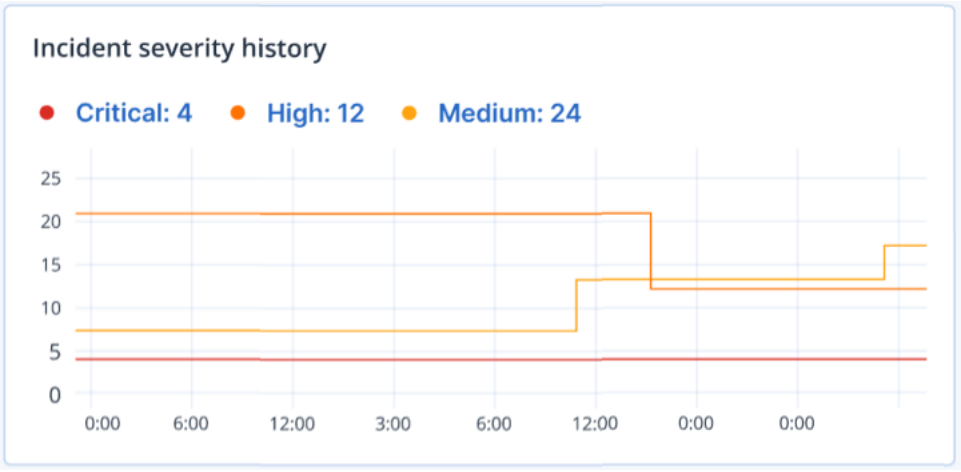
© Acronis International GmbH, 2003-2024



사건 심각도 이력

심각도별 공격 진행 과정이 표시되는 이 위젯에서는 공격 캠페인을 파악할 수 있습니다. 공격 캠페인이 급증하는 경우 조직이 공격을 받고 있는 것일 수 있습니다.

그래프를 마우스로 가리키면 지난 24시간(기본 기간) 동안 특정 지점에서 발생한 인시던트 이력의 세부 정보를 확인할 수 있습니다. 관련 인시던트 목록을 확인하려면 심각도 레벨(**심각**, **높음** 또는 **보통**)을 클릭합니다. 그러면 선택한 심각도 레벨과 일치하는 인시던트만 표시되도록 사전 필터링된 인시던트 목록으로 리디렉션됩니다.

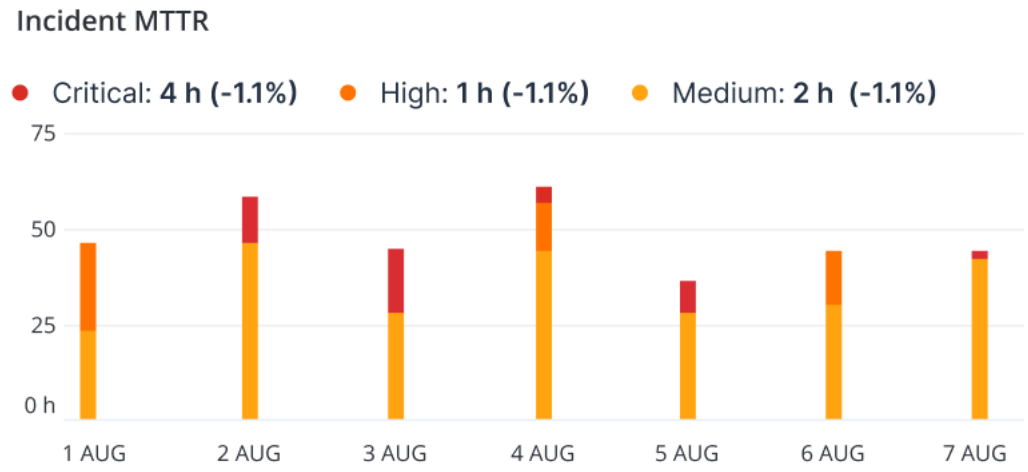


보안 인시던트 MTTR

이 위젯에는 보안 인시던트의 평균 해결 시간이 표시됩니다. MTTR은 인시던트 조사 및 해결 속도를 나타냅니다.

원하는 열을 클릭하면 심각도(**심각**, **높음**, **보통**)에 따른 인시던트 세부 정보, 그리고 각 심각도 수준의 인시던트를 해결하는 데 걸린 시간을 확인할 수 있습니다. 괄호 안에 표시되는 비율 값은 이전 기간과 비교한 증감률을 나타냅니다.

© Acronis International GmbH, 2003-2024

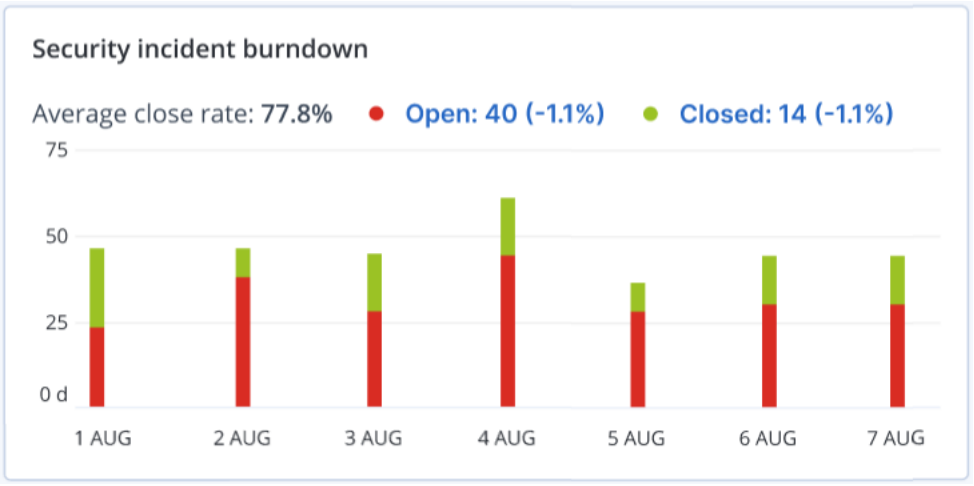


보안 인시던트 번다운(Burndown)

이 위젯에는 인시던트 종료 효율이 표시됩니다. 즉, 일정 기간 동안 종료된 인시던트 수를 기준으로 하여 측정된 미해결 인시던트 수가 표시됩니다.

원하는 열을 마우스로 가리키면 선택한 날짜의 종료된 인시던트와 미해결 인시던트 세부 정보를 확인할 수 있습니다. 미해결 값을 클릭하면 인시던트 목록이 표시되며, 해당 목록이 필터링되어 현재 미해결 상태인 인시던트(**조사 중** 또는 **시작되지 않음** 상태의 인시던트)가 표시됩니다. 종결됨 값을 클릭하면 인시던트 목록이 표시되며, 해당 목록이 필터링되어 더 이상 미해결 상태가 아닌 인시던트(**종결됨** 또는 **위양성** 상태의 인시던트)가 표시됩니다.

괄호 안에 표시되는 비율 값은 이전 기간과 비교한 증감률을 나타냅니다.



전술별 감지

이 위젯에는 선택한 기간 동안 인시던트에서 특정 공격 기술이 확인된 횟수가 표시됩니다.

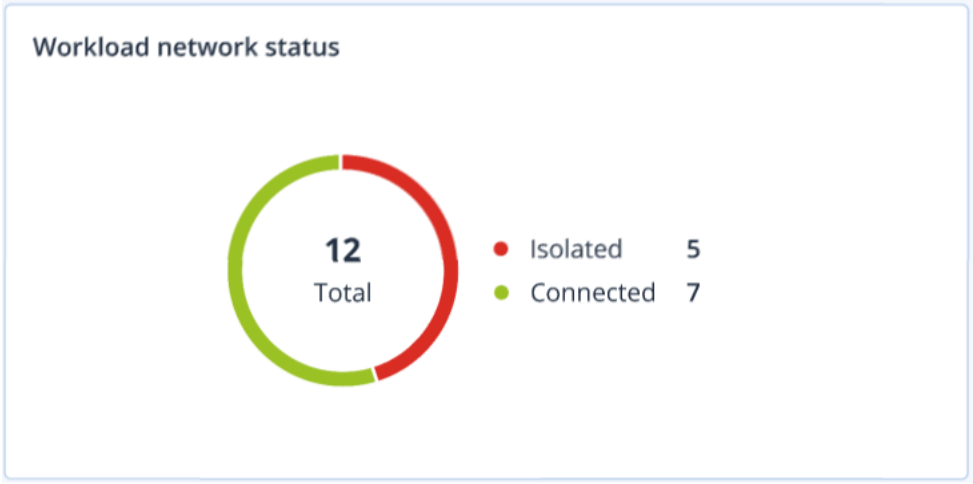
이전 기간 동안 확인된 특정 공격 기술이 많아졌는지 아니면 적어졌는지에 따라 값은 녹색이나 빨간색으로 표시됩니다. 아래 예제에서는 이전 기간 동안 권한 승격 공격과 명령 및 제어 공격 횟수가 늘어났습니다. 따라서 자격 증명 관리 방식을 분석하고 보안 수준을 높여야 할 수 있습니다.

© Acronis International GmbH, 2003-2024

워크로드 네트워크 상태

이 위젯에는 워크로드의 현재 네트워크 상태, 그리고 분리된/연결된 워크로드 수가 표시됩니다.

분리됨 값을 클릭하면 콘솔의 **워크로드** 메뉴 아래에서 에이전트가 있는 워크로드 목록을 확인할 수 있습니다. 이 목록은 분리된 워크로드가 표시되도록 필터링됩니다. 연결됨 값을 클릭하면 연결된 워크로드가 표시되도록 필터링된 에이전트가 있는 워크로드 목록을 확인할 수 있습니다.



머신별 #CyberFit Score

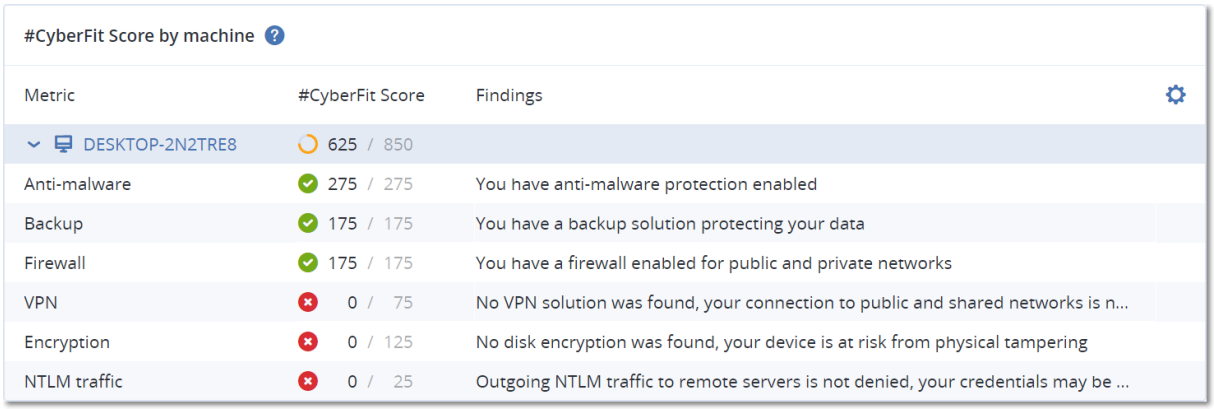
이 위젯에는 각 머신의 총 #CyberFit Score, 복합 점수 및 다음 각 평가 메트릭에 대한 결과가 표시됩니다.

- 맬웨어 방지
- 백업
- 방화벽
- VPN
- 암호화
- NTLM 트래픽

© Acronis International GmbH, 2003-2024

각 메트릭 점수를 개선하기 위한 권장사항은 보고서에서 확인할 수 있습니다.

#CyberFit Score에 대한 자세한 내용은 "머신의 #CyberFit Score"를 참고하십시오.



디스크 상태 모니터링

디스크 상태 모니터링에서는 현재 디스크 상태 관련 정보 및 상태 예측 정보를 제공합니다. 따라서 디스크 오류와 관련하여 발생할 수 있는 데이터 손실을 방지할 수 있습니다. HDD 및 SSD 디스크가 모두 지원됩니다.

제한 사항

- 디스크 상태 예측은 Windows를 실행하는 머신에 대해서만 지원됩니다.
- 실제 머신의 디스크만 모니터링됩니다. 가상 머신의 디스크는 모니터링할 수 없으며 디스크 상태 위젯에 표시되지 않습니다.
- RAID 구성은 지원되지 않습니다. 디스크 상태 위젯에는 RAID가 구현된 머신 관련 정보가 표시되지 않습니다.
- VNMe SSD는 지원되지 않습니다.

디스크 상태는 다음 중 하나로 표시됩니다.

- **정상**
  디스크 상태가 70~100% 사이입니다.
- **경고**
  디스크 상태가 30~70% 사이입니다.
- **심각**
  디스크 상태가 0~30% 사이입니다.
- **디스크 데이터 계산**
  – 현재 및 예측 디스크 상태를 계산하는 중입니다.

작동법

디스크 상태 예측 서비스는 AI 기반 예측 모델을 사용합니다.

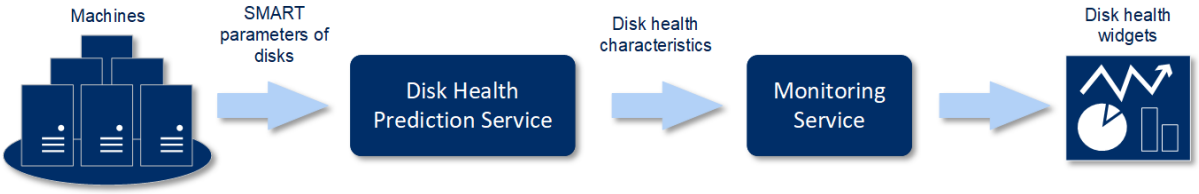
1. 보호 에이전트는 디스크의 SMART 매개변수를 수집해 해당 데이터를 디스크 상태 예측 서비스로 전달합니다.

© Acronis International GmbH, 2003-2024

- SMART 5 – 재할당된 섹터 수입니다.
- SMART 9 – 가동 시간입니다.
- SMART 187 – 수정할 수 없는 오류가 보고되었습니다.
- SMART 188 – 명령 시간이 초과되었습니다.
- SMART 197 – 현재 보류 중인 섹터 수입니다.
- SMART 198 – 수정할 수 없는 오프라인 섹터 수입니다.
- SMART 200 – 쓰기 오류 비율입니다.

2. 디스크 상태 예측 서비스는 수신한 SMART 매개변수를 처리하고, 예측하며, 다음과 같은 디스크 상태 특성을 제공합니다.
   - 디스크 현재 상태: 정상, 경고, 심각.
   - 디스크 상태 예측: 부정적, 안정적, 긍정적
   - 디스크 상태 예측 가능성을 백분율로 표시합니다.

   예측 기간은 1개월입니다.
3. 모니터링 서비스는 이러한 특성을 수신한 다음 Cyber Protect 콘솔의 디스크 상태 위젯에 관련 정보를 표시합니다.



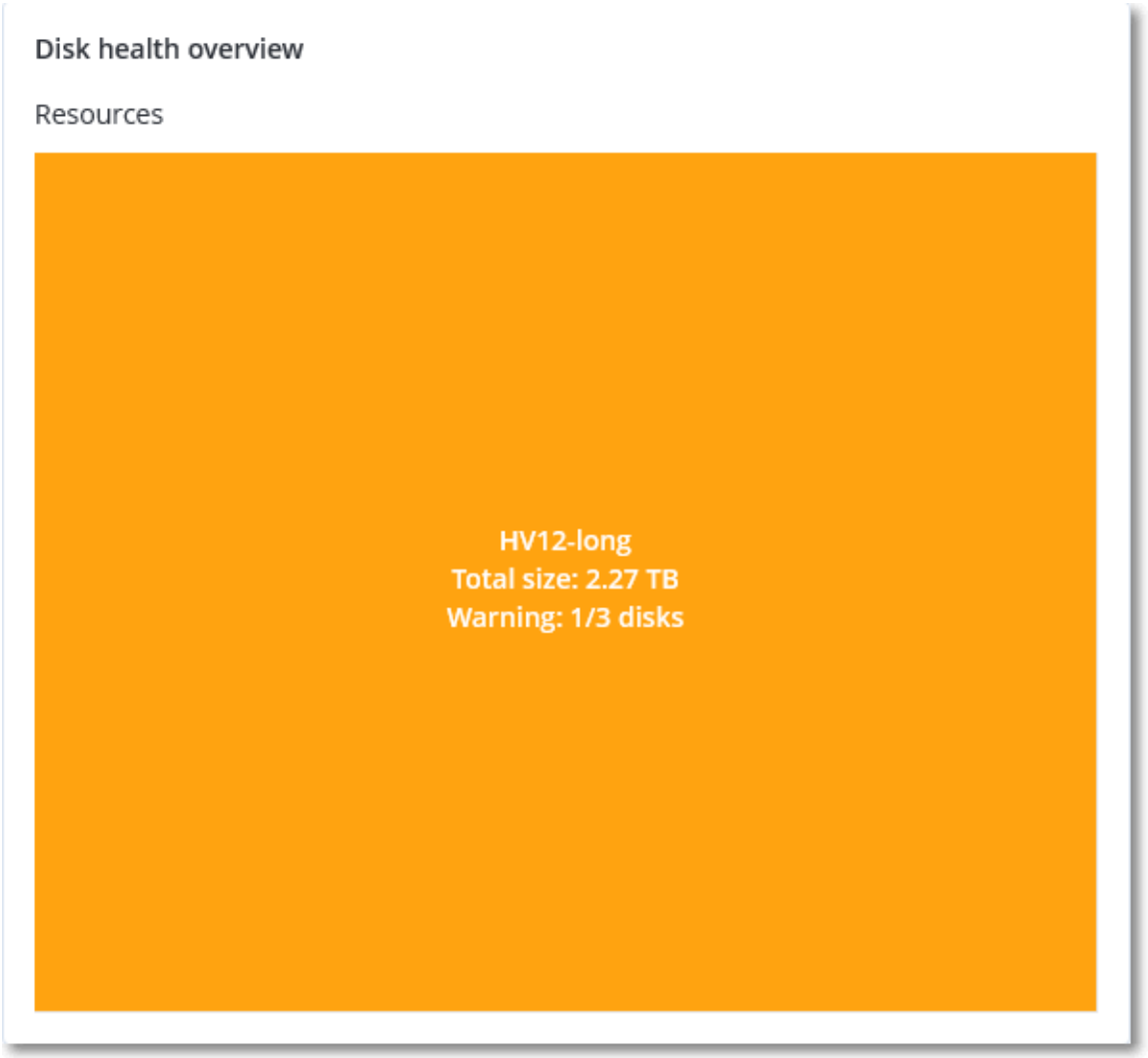
디스크 상태 위젯

디스크 상태 모니터링의 결과는 Cyber Protect 콘솔에서 사용 가능한 다음 위젯에 표시됩니다.

- **디스크 상태 개요** – 트리맵 구조의 위젯으로, 드릴다운을 통해 두 수준의 세부 정보를 전환하며 확인할 수 있습니다.
  - 머신 수준

    선택한 고객 머신별로 디스크 상태에 대한 요약 정보를 표시합니다. 가장 심각한 디스크 상태만 표시됩니다. 다른 상태는 특정 블록을 마우스로 가리켰을 때 도구 설명으로 표시됩니다. 머신 블록 크기는 머신의 총 디스크 크기에 따라 달라집니다. 머신 블록 색상은 발견된 중요 디스크 상태가 무엇인지에 따라 달라집니다.

© Acronis International GmbH, 2003-2024



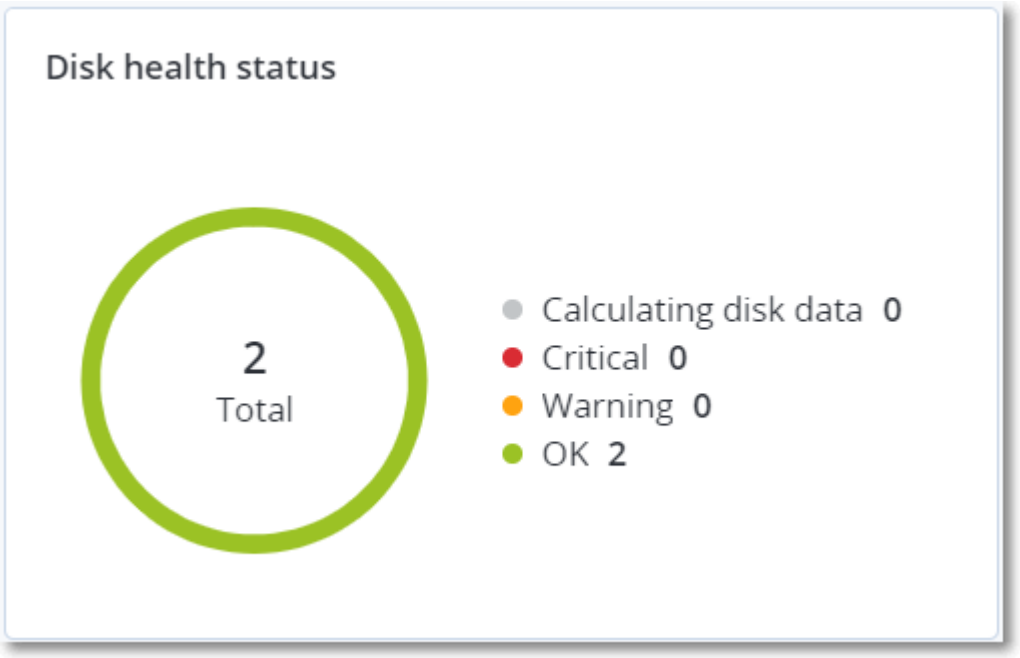
◦ 디스크 수준
선택한 머신에 있는 모든 디스크의 현재 상태를 표시합니다. 각 디스크 블록에는 다음 디스크 상태 예측 항목 중 하나와 해당 상태가 표시될 확률(비율)이 표시됩니다.

- 열화될 것으로 예측
- 안정적으로 유지될 것으로 예측

© Acronis International GmbH, 2003-2024

- 개선될 것으로 예측

- **디스크 상태** – 각 상태에 해당하는 디스크의 수를 원 그래프에 표시한 위젯입니다.



© Acronis International GmbH, 2003-2024

디스크 상태 경보

디스크 상태 확인은 30분마다 실행되고 해당 경보는 하루에 한 번 생성됩니다. 디스크 상태가 **경고**에서 **심각**으로 변경되면 항상 경보가 생성됩니다.

경보 이름	심각도	디스크 상태	설명
잠재적인 디스크 장애	경고	(30 – 70)	나중에 이 머신의 <디스크 이름> 디스크에 장애가 발생할 가능성이 높습니다. 가능한 한 빨리 이 디스크에 대한 전체 이미지 백업을 실행하고 디스크를 교체한 후, 새로운 디스크에 이미지를 복구하십시오.
디스크 장애 임박	심각	(0 – 30)	이 머신의 <디스크 이름> 디스크가 심각한 상태이며, 곧 장애가 발생할 가능성이 매우 높습니다. 추가적인 부담은 디스크 장애를 유발할 수 있으므로 현재 시점에서는 이 디스크의 이미지 백업을 수행하지 않는 것이 좋습니다. 즉시 이 디스크에서 가장 중요한 파일들을 백업한 후 디스크를 교체하십시오.

데이터 보호 맵

참고
이 기능은 Advanced Backup 팩에서 사용할 수 있습니다.

사용자는 데이터 보호 맵 기능을 통해 자신에게 중요한 모든 데이터를 발견하고 모든 중요 파일의 수, 크기, 위치, 보호 상태와 같은 자세한 정보를 확장 가능한 트리맵 보기로 확인할 수 있습니다.

각 블록 크기는 고객/머신에 속한 모든 중요 파일의 총 수/크기에 따라 달라집니다.

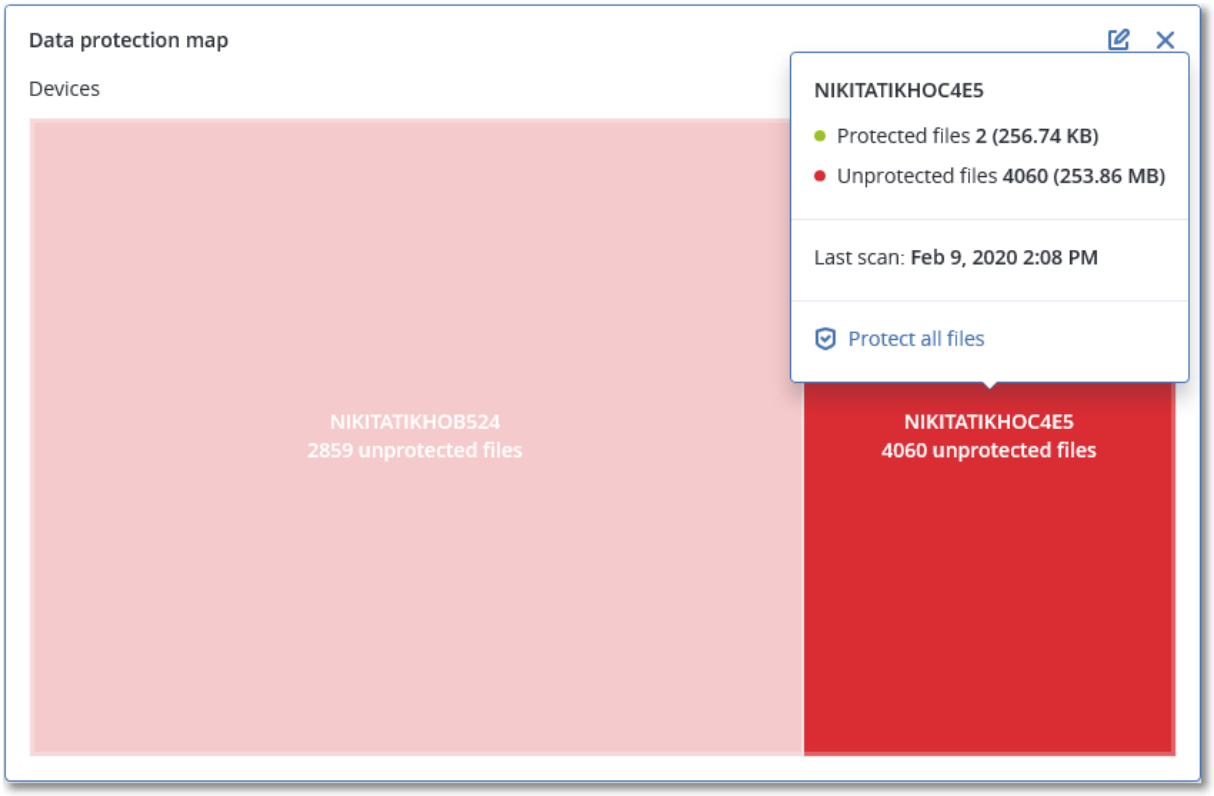
파일의 보호 상태는 다음 중 하나로 표시됩니다.

- **심각** – 선택한 머신/위치에 대해 기존 백업 설정으로 현재 또는 이후 백업되지 않도록 사용자가 지정한 확장자를 가진 파일 중 보호되지 않는 파일이 51~100%인 경우
- **낮음** – 선택한 머신/위치에 대해 기존 백업 설정으로 현재 또는 이후 백업되지 않도록 사용자가 지정한 확장자를 가진 파일 중 보호되지 않는 파일이 21~50%인 경우
- **중간** – 선택한 머신/위치에 대해 기존 백업 설정으로 현재 또는 이후 백업되지 않도록 사용자가 지정한 확장자를 가진 파일 중 보호되지 않는 파일이 1~20%인 경우
- **높음** – 선택한 머신/위치에 대해 백업되지 않도록 사용자가 지정한 확장자를 가진 모든 파일이 보호되고 있는 경우

데이터 보호 조사 결과는 머신 수준의 세부 정보를 트리맵 구조로 표시하는 데이터 보호 맵 위젯의 모니터링 대시보드에서 확인할 수 있습니다.

- 머신 수준 – 선택한 고객의 머신별로 중요한 파일의 보호 상태에 대한 요약 정보를 표시합니다.

© Acronis International GmbH, 2003-2024



보호되지 않는 파일을 보호하려면 블록을 마우스로 가리킨 다음 **모든 파일 보호**를 클릭합니다. 대화창에서 보호되지 않는 파일의 수와 해당 파일의 위치와 같은 정보를 확인할 수 있습니다. 이러한 파일을 보호하려면 **모든 파일 보호**를 클릭합니다.

상세 보고서를 CSV 형식으로 다운로드할 수도 있습니다.

취약성 평가 위젯

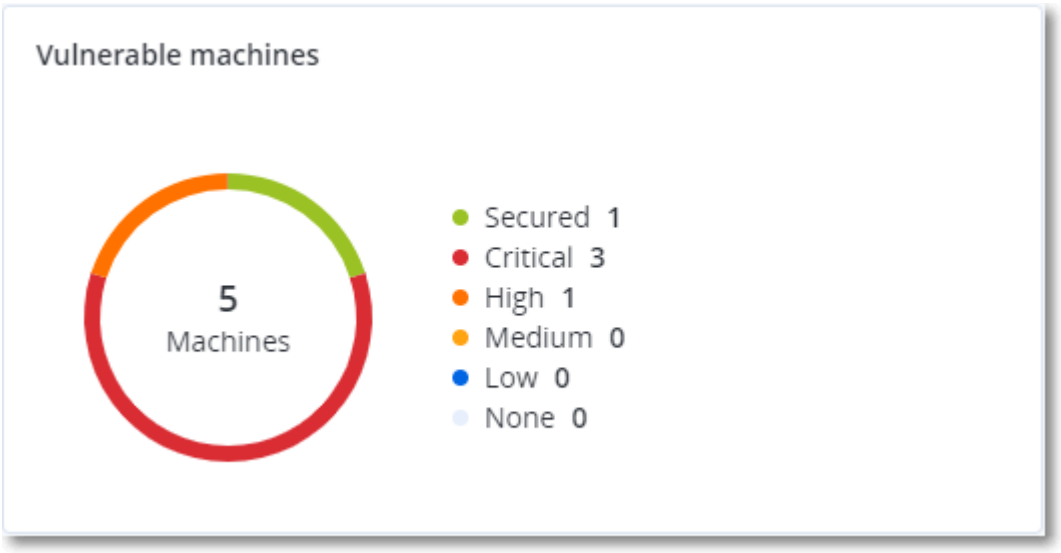
취약한 머신

이 위젯은 취약한 머신을 취약성 심각도에 따라 표시합니다.

CVSS(일반 취약성 점수 시스템) v3.0에 따라 취약성의 심각도 수준은 다음으로 나누어집니다.

- 보안됨: 발견된 취약성 없음
- 심각: 9.0 - 10.0 CVSS
- 높음: 7.0 - 8.9 CVSS
- 중간: 4.0 - 6.9 CVSS
- 낮음: 0.1 - 3.9 CVSS
- 없음: 0.0 CVSS

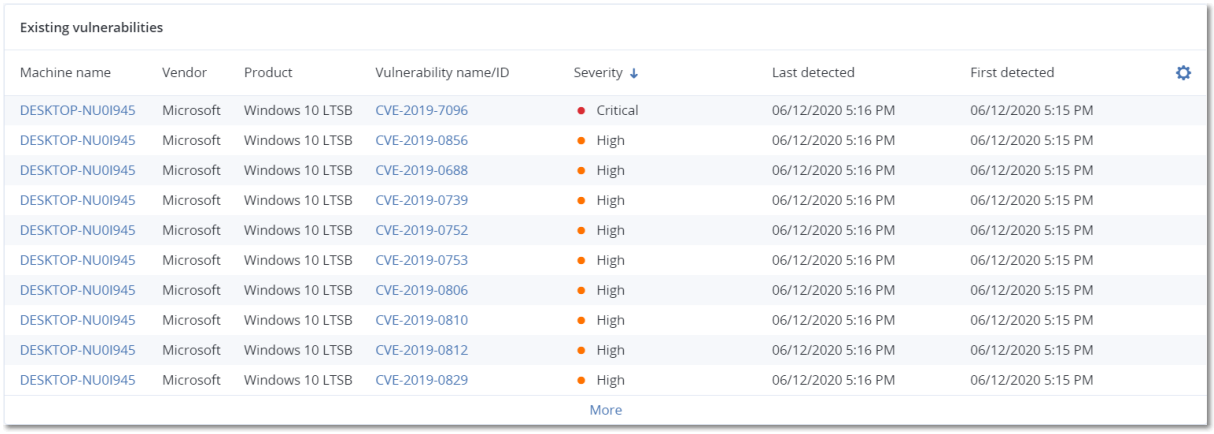
© Acronis International GmbH, 2003-2024



기존 취약성

이 위젯은 머신에 현재 존재하는 취약성을 표시합니다. **기존 취약성** 위젯에는 타임 스탬프를 보여주는 두 개의 열이 있습니다.

- **첫 번째로 감지됨** – 머신에서 처음으로 취약성이 감지된 날짜와 시간입니다.
- **마지막으로 감지됨** – 머신에서 마지막으로 취약성이 감지된 날짜와 시간입니다.



Existing vulnerabilities

Machine name	Vendor	Product	Vulnerability name/ID	Severity	Last detected	First detected
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-7096	Critical	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0856	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0688	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0739	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0752	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0753	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0806	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0810	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0812	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM
DESKTOP-NU0I945	Microsoft	Windows 10 LTSB	CVE-2019-0829	High	06/12/2020 5:16 PM	06/12/2020 5:15 PM

More

패치 설치 위젯

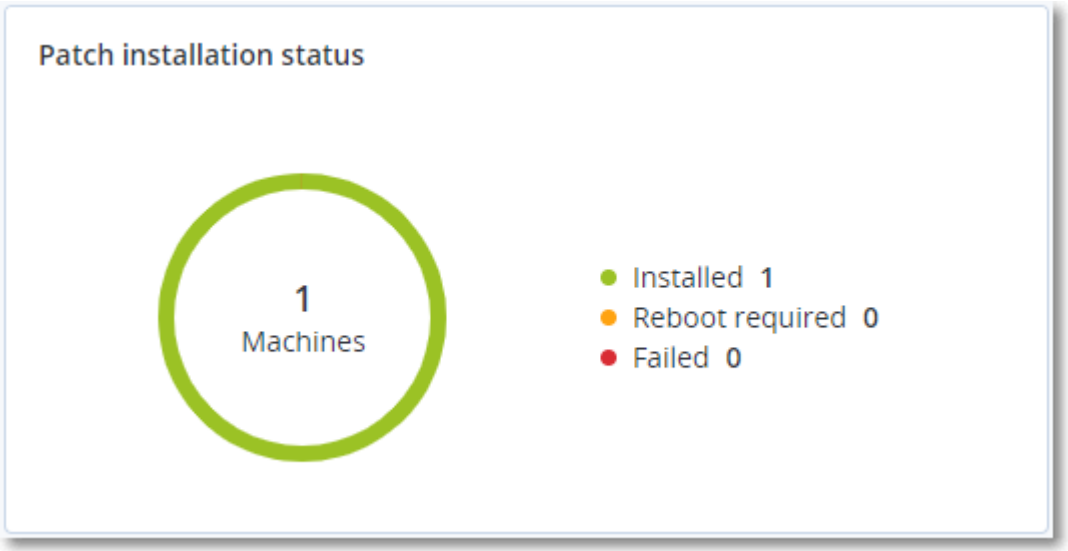
패치 설치 기능과 관련된 위젯은 4개입니다.

패치 설치 상태

이 위젯은 패치 설치 상태별로 그룹화된 머신 수를 표시합니다.

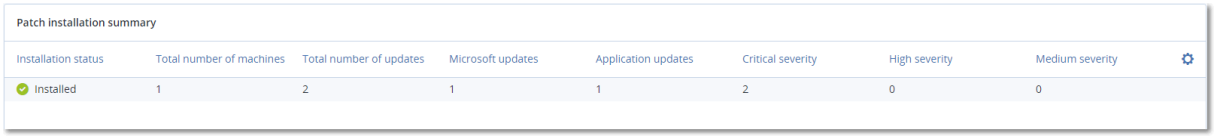
- **설치됨** – 사용 가능한 모든 패치가 머신에 설치되어 있음
- **재부팅 필요** – 패치 설치 후 재부팅이 필요한 머신
- **실패** – 머신에 패치 설치 실패

© Acronis International GmbH, 2003-2024



패치 설치 요약

이 위젯은 머신의 패치 내역을 패치 설치 상태로 요약하여 표시합니다.



패치 설치 내역

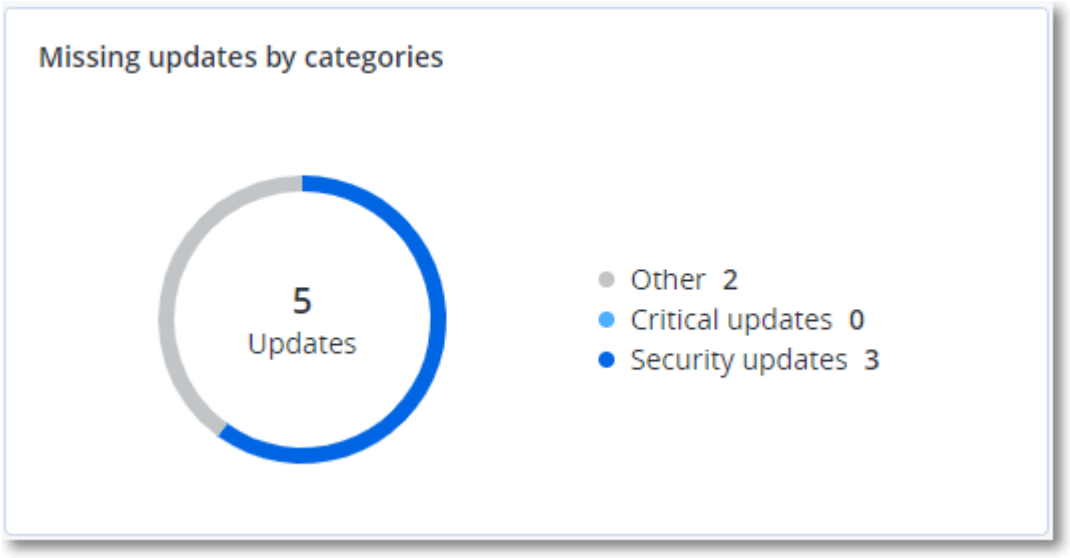
이 위젯은 머신의 패치에 대한 자세한 정보를 표시합니다.

카테고리별 누락 업데이트

이 위젯은 카테고리별 누락 업데이트의 수를 표시합니다. 다음과 같은 카테고리가 표시됩니다.

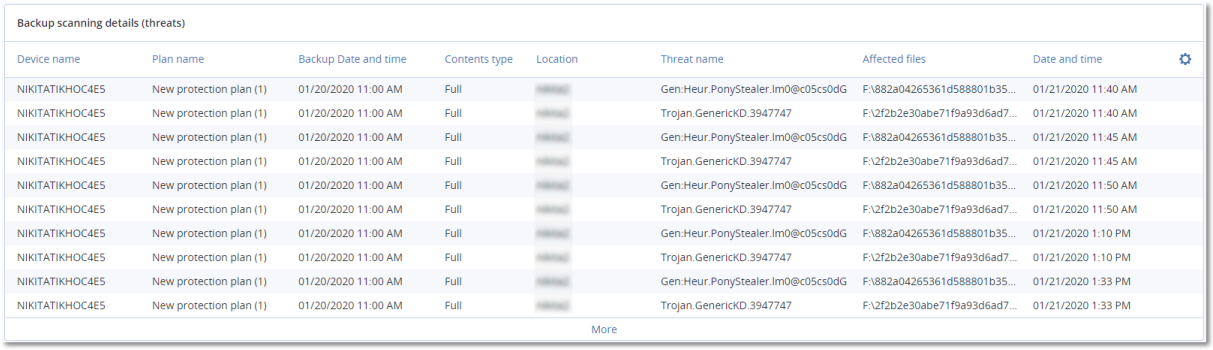
- 보안 업데이트
- 중요 업데이트
- 기타

© Acronis International GmbH, 2003-2024



백업 스캔 세부 정보

이 위젯은 백업에서 감지된 위협에 대한 자세한 정보를 표시합니다.


Backup scanning details (threats)

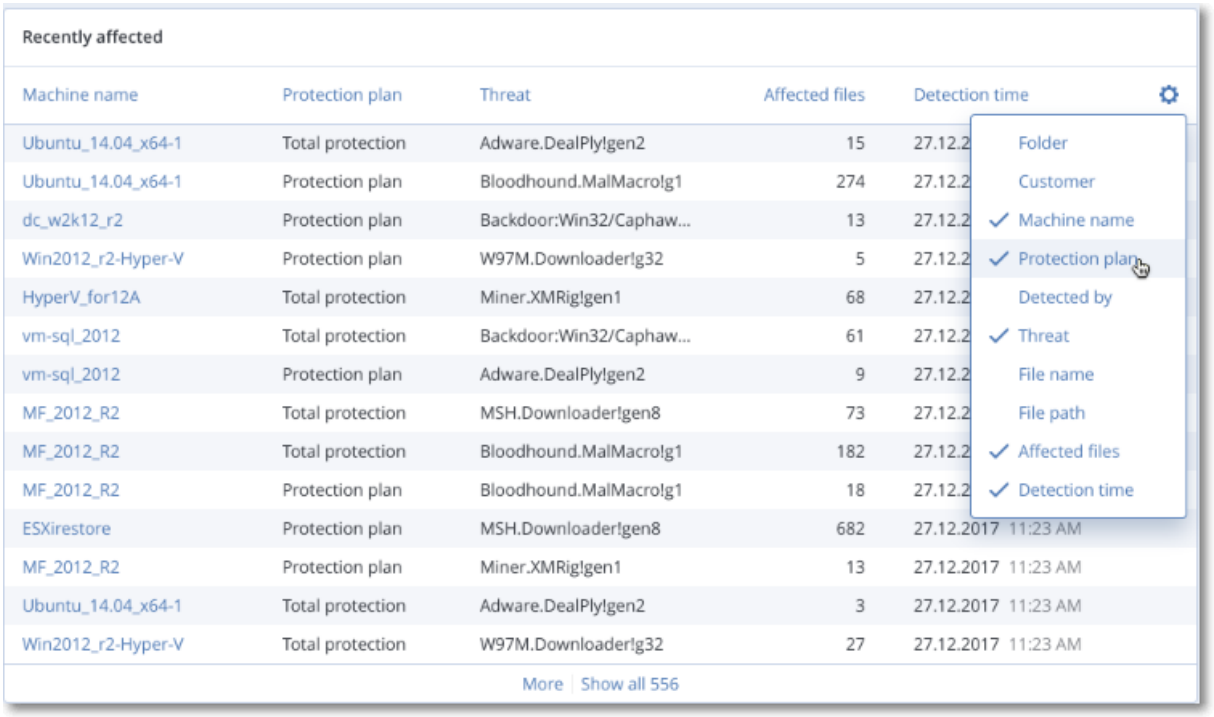
Device name	Plan name	Backup Date and time	Contents type	Location	Threat name	Affected files	Date and time
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:33 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:33 PM

More

최근 영향 받은 항목

이 위젯에는 바이러스, 맬웨어 및 랜섬웨어 같은 위협으로부터 영향을 받은 워크로드에 대한 자세한 정보가 표시됩니다. 여기서 감지된 위협, 위협이 감지된 시기 그리고 감염된 파일 수에 대한 정보를 확인할 수 있습니다.

© Acronis International GmbH, 2003-2024



최근 영향 받은 워크로드 관련 데이터 다운로드

최근 영향 받은 워크로드 관련 데이터를 다운로드하고, CSV 파일을 생성하고, 지정한 받는 사람에게 보낼 수 있습니다.

최근 영향 받은 워크로드 관련 데이터를 다운로드하려면

1. **최근 영향 받은 항목** 위젯에서 **데이터 다운로드**를 클릭합니다.
2. **기간** 필드에 데이터를 다운로드하려는 일수를 입력합니다. 입력할 수 있는 최대 일수는 200일입니다.
3. **받는 사람** 필드에 CSV 파일 다운로드 링크가 포함된 이메일을 받을 모든 사람의 이메일 주소를 입력합니다.
4. **다운로드**를 클릭합니다.

   시스템에서 지정한 기간 동안 영향을 받은 워크로드 관련 데이터가 포함된 CSV 파일을 생성하기 시작합니다. CSV 파일이 완성되면 시스템에서는 받는 사람에게 이메일을 보냅니다. 그러면 각각의 받는 사람이 CSV 파일을 다운로드할 수 있습니다.

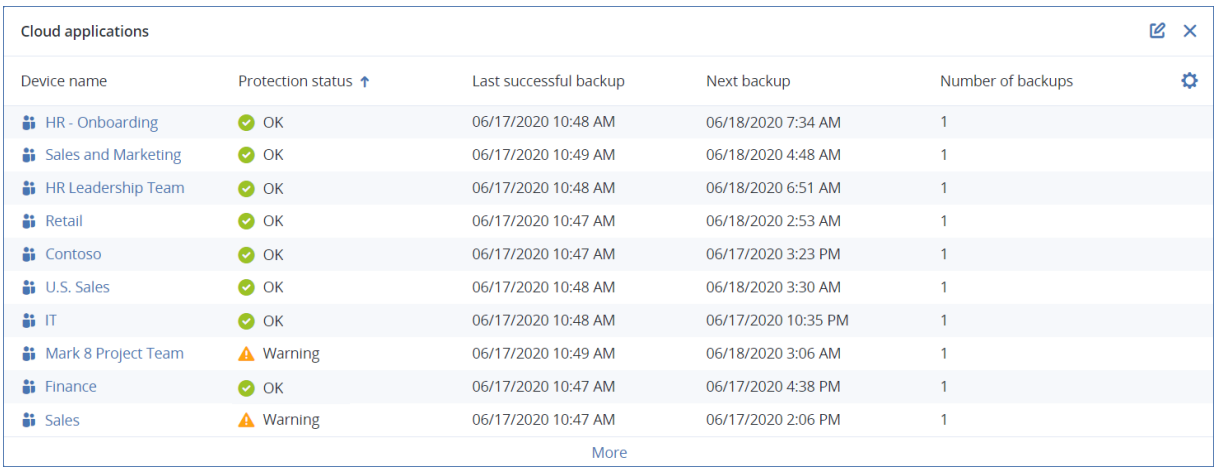
클라우드 애플리케이션

이 위젯은 클라우든 간 리소스에 대한 자세한 정보를 표시합니다.

- Microsoft 365 사용자(사서함, OneDrive)
- Microsoft 365 그룹(사서함, OneDrive)
- Microsoft 365 공용 폴더
- Microsoft 365 사이트 컬렉션
- Microsoft 365 Teams

© Acronis International GmbH, 2003-2024

- Google Workspace 사용자(Gmail, Google Drive)
- Google Workspace 공유 드라이브

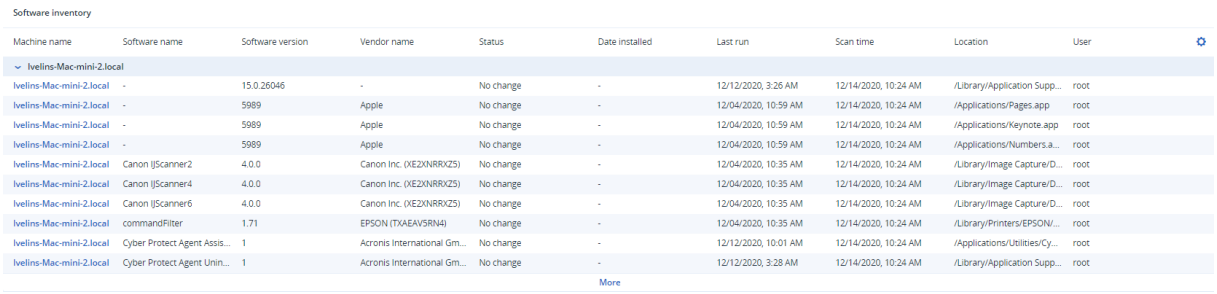


다음 위젯에서도 클라우드 간 리소스에 관한 추가 정보를 확인할 수 있습니다.

- 작업
- 활동 목록
- 최신 경보 5개
- 경보 내역
- 활성 경보 요약
- 경보 내역 요약
- 활성 경보 세부 정보
- 위치 요약

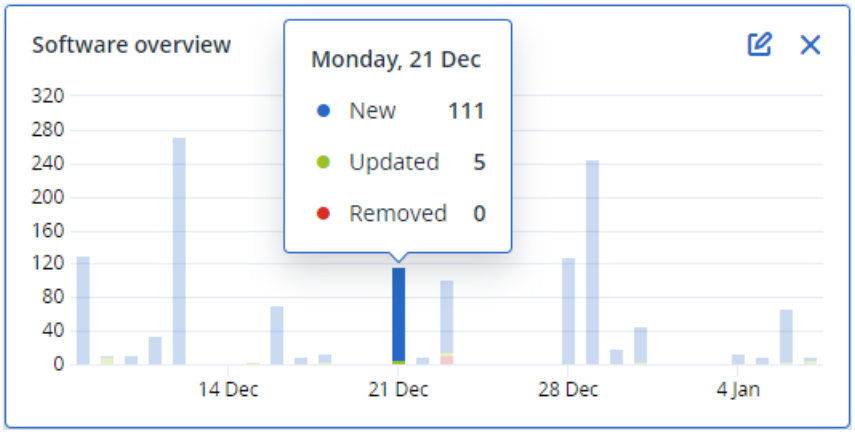
소프트웨어 인벤토리 위젯

소프트웨어 인벤토리 표 위젯은 조직의 Windows 및 macOS 장치에 설치된 모든 소프트웨어에 대한 자세한 정보를 표시합니다.



소프트웨어 개요 위젯은 조직의 Windows 및 macOS 장치에서 지정된 기간(7일, 30일 또는 현재 월) 동안 새로 설치, 업데이트 및 삭제된 애플리케이션의 수를 표시합니다.

© Acronis International GmbH, 2003-2024



차트의 특정 막대를 마우스로 가리키면 다음 정보가 포함된 툴팁이 표시됩니다.

신규 - 새로 설치된 애플리케이션의 수입니다.

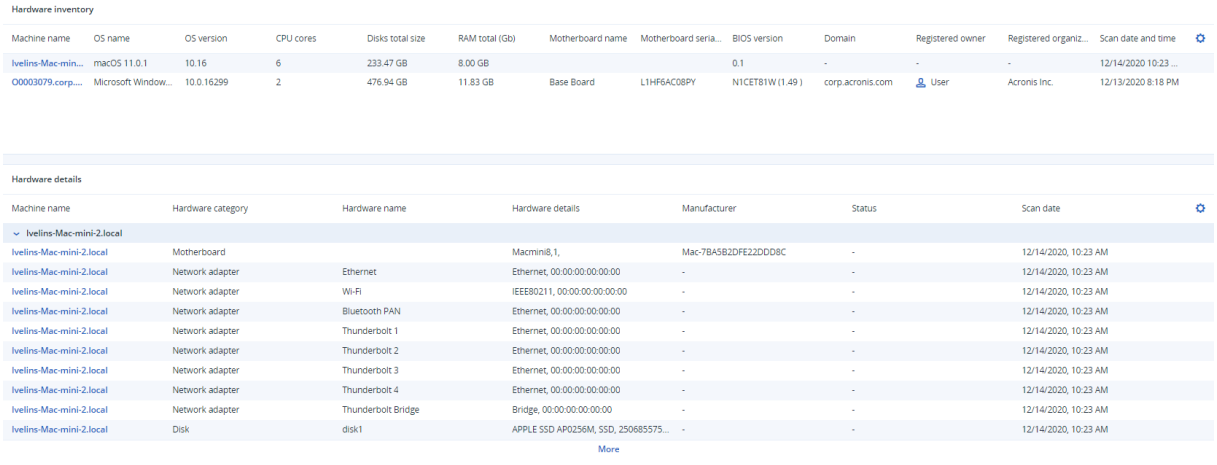
업데이트됨 - 업데이트된 애플리케이션의 수입니다.

제거됨 - 제거된 애플리케이션의 수입니다.

특정 상태를 나타내는 막대의 일부를 클릭하면 **소프트웨어 관리** -> **소프트웨어 인벤토리** 페이지로 리디렉션됩니다. 페이지의 정보는 해당하는 날짜 및 상태에 따라 필터링됩니다.

하드웨어 인벤토리 위젯

하드웨어 인벤토리 및 **하드웨어 상세 정보** 표 위젯은 조직의 물리적 및 가상 Windows 및 macOS 장치에 설치된 모든 하드웨어에 대한 정보를 표시합니다.



하드웨어 변경 표 위젯은 조직의 물리적 및 가상 Windows 및 macOS 장치에서 지정된 기간(7일, 30일 또는 현재 월) 동안 추가, 제거 및 변경된 하드웨어에 대한 정보를 표시합니다.

© Acronis International GmbH, 2003-2024

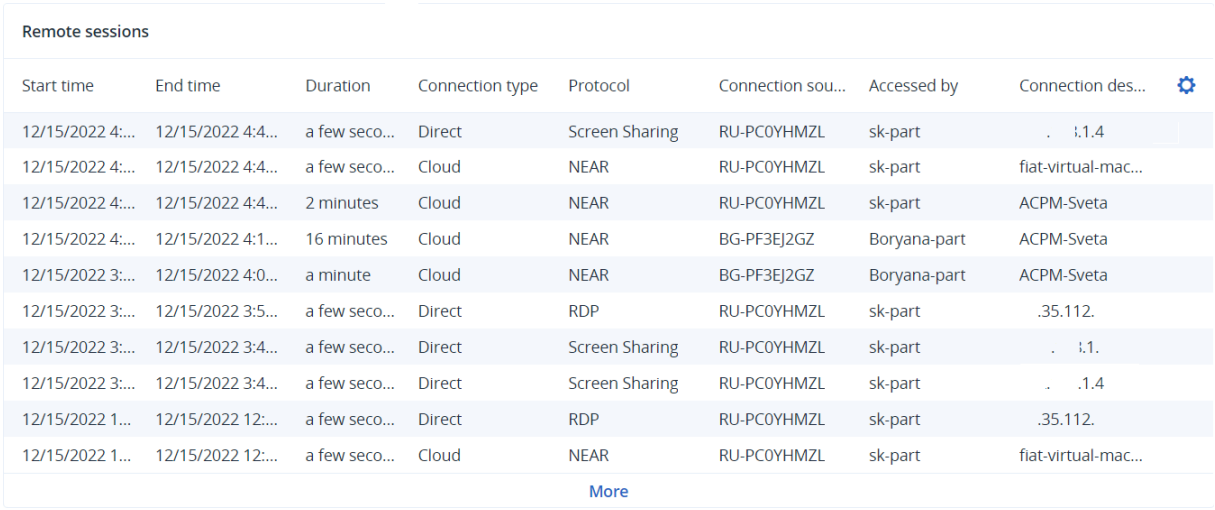
Hardware changes

Machine name	Hardware category	Status	Old value	New value	Modification date and time
DESKTOP-0FF9TTF					
DESKTOP-0FF9TTF	Network adapter	Changed	Oracle Corporation, Ethernet 802.3,...	Oracle Corporation, Ethernet 802.3, ...	01/11/2021 9:28 AM
DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor Corp., Ether...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Torronto 5C1, PF0PJB10	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), WDC WD10JP...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 802.3, 00:0...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ethernet 802.3, ...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00 GB	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows Provider V9...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM

More

원격 세션 위젯

이 위젯에는 원격 데스크탑 및 파일 전송 세션의 자세한 정보가 표시됩니다.



Remote sessions

Start time	End time	Duration	Connection type	Protocol	Connection sou...	Accessed by	Connection des...
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 4:...	12/15/2022 4:4...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...
12/15/2022 4:...	12/15/2022 4:4...	2 minutes	Cloud	NEAR	RU-PC0YHMZL	sk-part	ACPM-Sveta
12/15/2022 4:...	12/15/2022 4:1...	16 minutes	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 4:0...	a minute	Cloud	NEAR	BG-PF3EJ2GZ	Boryana-part	ACPM-Sveta
12/15/2022 3:...	12/15/2022 3:5...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.
12/15/2022 3:...	12/15/2022 3:4...	a few seco...	Direct	Screen Sharing	RU-PC0YHMZL	sk-part	. .1.4
12/15/2022 1...	12/15/2022 12:...	a few seco...	Direct	RDP	RU-PC0YHMZL	sk-part	.35.112.
12/15/2022 1...	12/15/2022 12:...	a few seco...	Cloud	NEAR	RU-PC0YHMZL	sk-part	fiat-virtual-mac...

More

스마트 보호

위협 피드

Acronis 사이버 보호 작업 센터(CPOC)에서는 관련된 지역으로만 전송되는 보안 경보를 생성합니다. 이러한 보안 경보는 맬웨어, 취약성, 자연 재해, 공공 보건을 비롯해 데이터 보호에 영향을 미칠 수 있는 글로벌 이벤트에 대한 정보를 제공합니다. 위협 피드에는 모든 잠재적인 위협이 표시되어 이를 방지할 수 있도록 해줍니다.

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

일부 보안 경보는 보안 전문가가 제공하는 특정 작업 세트를 수행하면 해결할 수 있습니다. 이후 발생할 가능성이 있지만 사용 가능한 권장 작업이 없는 위협을 알리기 위해 생성되는 보안 경보도 있습니다.

참고
맬웨어 경보는 안티맬웨어 보호용 에이전트가 설치된 머신에서만 생성됩니다.

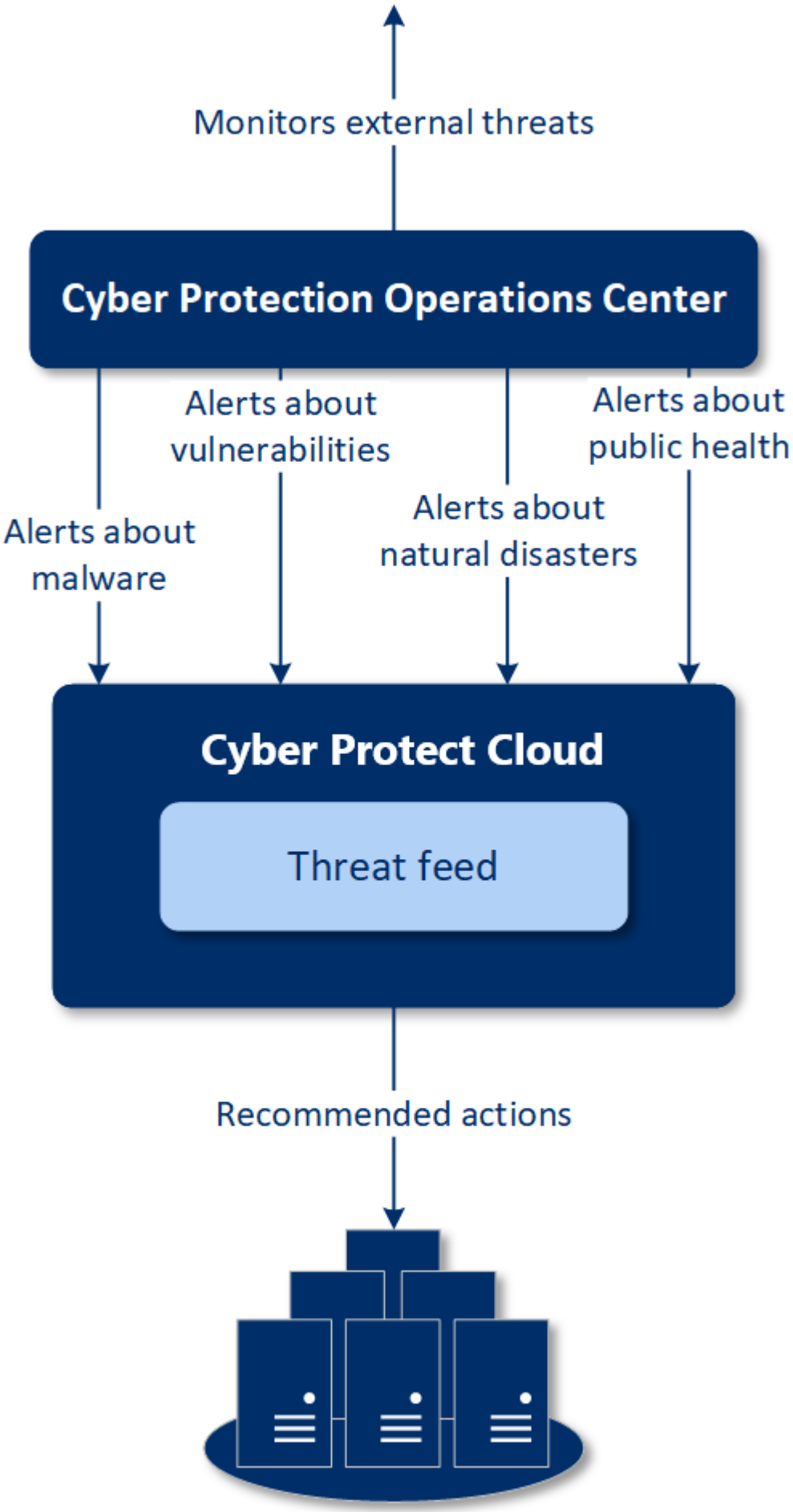
© Acronis International GmbH, 2003-2024

작동법

Acronis 사이버 보호 작업 센터는 외부 위협을 모니터링하고 맬웨어, 취약성, 자연 재해 위협, 공공 보건에 대한 경보를 생성합니다. Cyber Protect 콘솔의 **위협 피드** 섹션에서 이러한 모든 경보를 확인할 수 있습니다. 경보 유형에 따라 해당하는 권장 작업을 수행할 수 있습니다.

위협 피드의 주요 작업 흐름은 아래 다이어그램에 설명되어 있습니다.

© Acronis International GmbH, 2003-2024



© Acronis International GmbH, 2003-2024

Acronis 사이버 보호 작업 센터에서 수신한 경보에 대한 권장 작업을 실행하려면 다음을 수행하십시오.

1. Cyber Protect 콘솔에서 **모니터링** > **위협 피드**로 이동해 기존 보안 경보가 있는지 검토합니다.
2. 목록의 경보를 선택한 다음 제공된 상세 정보를 검토합니다.
3. **시작**을 클릭해 마법사를 실행합니다.
4. 수행하려는 작업과 이러한 작업이 적용될 머신을 활성화합니다. 다음 작업이 제안될 수 있습니다.
   - **취약성 평가** – 머신의 취약성 스캔
   - **패치 관리** –선택한 머신에 패치 설치
   - **맬웨어 방지 기능** – 선택한 머신에 대한 전체 스캔 실행

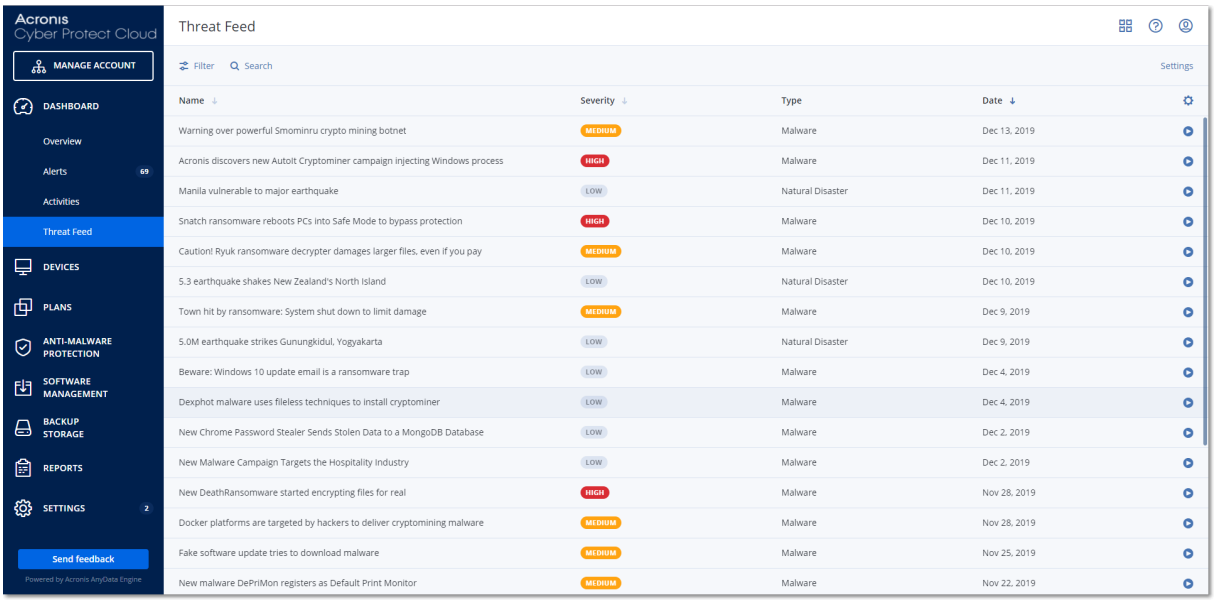
     참고
     이 작업은 안티맬웨어 보호용 에이전트가 설치된 머신에서만 사용 가능합니다.

   - **보호 또는 보호되지 않는 머신 백업** – 보호/보호되지 않는 워크로드를 백업할 수 있습니다. 워크로드의 백업이 아직 없거나(액세스 가능한 클라우드 및 로컬의 모든 위치) 기존 백업이 암호화되어 있는 경우 다음 이름 형식을 사용하여 전체 백업이 생성됩니다.

     `%workload_name%-Remediation`

     기본적으로 백업 대상은 Cyber Protect Cloud 스토리지지만 작업을 시작하기 전에 다른 위치를 구성할 수도 있습니다.

     암호화되지 않은 백업이 이미 있으면 기존 아카이브에 증분 백업이 생성됩니다.
5. **시작**을 클릭합니다.
6. **작업** 페이지에서 작업이 성공적으로 수행되었는지 확인합니다.



모든 경보 삭제

위협 피드의 자동 정리는 다음 기간 후 가능합니다.

© Acronis International GmbH, 2003-2024

- 자연 재해 – 1주
- 취약성 – 1개월
- 맬웨어 – 1개월
- 공공 보건 - 1주

데이터 보호 맵

데이터 보호 맵 기능으로 다음이 가능합니다.

- 머신에 저장된 데이터에 대한 상세한 정보(분류, 위치, 보호 상태, 기타 추가 정보)를 파악합니다.
- 데이터의 보호 여부를 감지합니다. 데이터는 백업으로 보호되어야 보호 상태로 간주됩니다(백업 모듈이 활성화된 보호 계획 사용).
- 데이터 보호를 위한 작업을 수행합니다.

작동법

1. 먼저 데이터 보호 맵 모듈이 활성화된 보호 계획을 생성합니다.
2. 계획이 수행되어 데이터의 발견 및 분석이 끝나면 데이터 보호 맵 위젯에 데이터 보호 상태가 시각적으로 표시됩니다.
3. 또한 **장치** > **데이터 보호 맵**으로 이동해 장치별로 보호되지 않는 파일에 대한 정보를 확인할 수도 있습니다.
4. 장치에서 보호되지 않는 것으로 감지된 파일을 보호하기 위한 작업을 수행할 수 있습니다.

보호되지 않는 것으로 감지된 파일 관리

보호되지 않는 것으로 감지된 중요 파일을 보호하려면 다음을 수행하십시오.

1. Cyber Protect 콘솔에서 **장치** > **데이터 보호 맵**으로 이동합니다.
   장치 목록에서 장치별로 보호되지 않는 파일의 수, 해당 파일의 크기, 마지막 데이터 검색 등과 같은 일반적인 정보를 확인할 수 있습니다.
   특정 머신의 파일을 보호하려면 말줄임표 아이콘과 **모든 파일 보호**를 차례로 클릭합니다. 백업 모듈이 활성화된 보호 계획을 생성할 수 있는 계획 목록으로 리디렉션됩니다.
   목록에서 보호되지 않는 파일이 있는 특정 장치를 삭제하려면 **다음 데이터 검색 시까지 숨김**을 클릭합니다.
2. 특정 장치에서 보호되지 않는 파일에 대한 자세한 정보를 확인하려면 해당 장치의 이름을 클릭합니다.
   확장자 및 위치별로 보호되지 않는 파일의 수를 확인할 수 있습니다. 검색 필드에 보호되지 않는 파일에 대한 정보를 알아보기 위한 확장자를 정의합니다.
3. 보호되지 않는 파일을 모두 보호하려면 **모든 파일 보호**를 클릭합니다. 백업 모듈이 활성화된 보호 계획을 생성할 수 있는 계획 목록으로 리디렉션됩니다.

보고서 형식으로 보호되지 않는 파일에 대한 정보를 받아보려면 **상세 보고서를 CSV로 다운로드**를 클릭합니다.

© Acronis International GmbH, 2003-2024

데이터 보호 맵 설정

데이터 보호 맵 모듈이 있는 보호 계획을 생성하는 방법을 알아보려면 "보호 계획 생성"을 참고하십시오.

데이터 보호 맵 모듈에 대해 다음 설정을 지정할 수 있습니다.

예약

다른 설정을 정의해 데이터 보호 맵이 수행될 작업에 따라 스케줄을 생성할 수 있습니다.

필드	설명
다음 이벤트를 사용해 작업 실행 예약	작업을 실행할 시간을 정의하는 설정입니다. 다음 값을 선택할 수 있습니다. • **시간 기준 예약** - 기본 설정입니다. 지정한 시간에 따라 작업을 실행합니다. • **사용자가 시스템에 로그인할 때** – 기본적으로 사용자가 로그인하면 작업이 트리거됩니다. 특정 사용자 계정만 작업을 트리거할 수 있도록 이 설정을 수정할 수 있습니다. • **사용자가 시스템에서 로그오프할 때** – 기본적으로 사용자가 로그오프하면 작업이 트리거됩니다. 특정 사용자 계정만 작업을 트리거할 수 있도록 이 설정을 수정할 수 있습니다. **참고** 작업은 시스템 종료 시 실행되지 않습니다. 일정 예약 구성에서 시스템 종료와 로그오프는 다른 작업입니다. • **시스템 시작 시** – 운영 체제가 시작될 때 작업을 실행합니다. • **시스템 종료 시** – 운영 체제가 종료될 때 작업을 실행합니다.
예약 유형	**다음 이벤트를 사용해 작업 실행 예약**에서 **시간 기준 예약**을 선택한 경우 이 필드가 표시됩니다. 다음 값을 선택할 수 있습니다. • **월간** – 작업을 실행할 월과 주 또는 일을 선택합니다. • **일일** - 기본 설정입니다. 작업을 실행할 요일을 선택합니다. • **매시간** – 작업을 실행할 요일, 반복 횟수, 시간 간격을 선택합니다.
시작 시간	**다음 이벤트를 사용해 작업 실행 예약**에서 **시간 기준 예약**을 선택한 경우 이 필드가 표시됩니다 작업을 실행할 정확한 시간을 선택합니다.
날짜 범위 내에서 실행	**다음 이벤트를 사용해 작업 실행 예약**에서 **시간 기준 예약**을 선택한 경우 이 필드가 표시됩니다. 구성된 스케줄이 실행될 기간의 범위를 설정합니다.
운영 체제에	**다음 이벤트를 사용해 작업 실행 예약**에서 **사용자가 시스템에 로그인할 때**

© Acronis International GmbH, 2003-2024

필드	설명
로그인할 때 작업을 시작하게 할 사용자 계정 지정	를 선택한 경우 이 필드가 표시됩니다. 다음 값을 선택할 수 있습니다. • **모든 사용자** - 어떤 사용자가 로그인하든 작업이 트리거되도록 하려는 경우 이 옵션을 사용합니다. • **다음 사용자** - 특정 사용자 계정의 로그인 시에만 작업이 트리거되도록 하려는 경우 이 옵션을 사용합니다.
운영 체제에서 로그아웃할 때 작업을 시작하게 할 사용자 계정 지정	**다음 이벤트를 사용해 작업 실행 예약**에서 **사용자가 시스템에서 로그오프할 때**를 선택한 경우 이 필드가 표시됩니다. 다음 값을 선택할 수 있습니다. • **모든 사용자** - 어떤 사용자가 로그아웃하든 작업이 트리거되도록 하려는 경우 이 옵션을 사용합니다. • **다음 사용자** - 특정 사용자 계정의 로그아웃 시에만 작업이 트리거되도록 하려는 경우 이 옵션을 사용합니다.
시작 조건	작업을 시작하기 위해 동시에 충족되어야 하는 모든 조건을 정의합니다. 맬웨어 방지 스캔용 시작 조건은 "시작 조건"에 설명되어 있는 **백업 모듈**용 시작 조건과 유사합니다. 다음과 같이 추가적인 시작 조건을 정의할 수 있습니다. • **기간 내에서 작업 시작 시간 분배** – 이 옵션을 사용하면 작업을 수행해야 하는 기간을 정의할 수 있습니다. 이 옵션을 사용해 작업 시간대를 설정하여 네트워크 병목현상을 피할 수 있습니다. 지연 시간은 시간 또는 분 단위로 지정할 수 있습니다. 예를 들어 기본 시작 시간이 오전 10시이고 지연 시간이 60분인 경우 작업은 오전 10시~오전 11시 사이에 시작됩니다. • **머신이 꺼진 경우 머신 시작 시 누락된 작업 실행** • **작업 실행 중 절전 또는 최대 절전 모드가 되는 것을 방지** – 이 옵션은 Windows를 구동 중인 머신에서만 유효합니다. • **시작 조건이 충족되지 않아도 다음 후에 작업 실행** - 다른 시작 조건에 관계없이 지정한 기간이 지나면 작업이 시작됩니다. **참고** Linux에서는 시작 조건이 지원되지 않습니다.

확장자 및 예외 규칙

확장자 탭에서 데이터 검색 시 중요하다고 간주하여 보호 여부를 확인할 파일 확장자 목록을 정의할 수 있습니다. 확장자 정의에는 다음 형식을 사용하십시오.

```
.html, .7z, .docx, .zip, .pptx, .xml
```

예외 규칙 탭에서 데이터 검색 시 보호 상태를 확인하지 않을 파일과 폴더를 정의할 수 있습니다.

- **숨겨진 파일 및 폴더** – 이 옵션을 선택하는 경우 데이터 검사 시 숨겨진 파일과 폴더를 건너뜁니다.

© Acronis International GmbH, 2003-2024

- **시스템 파일 및 폴더** – 이 옵션을 선택하는 경우 데이터 검사 시 시스템 파일과 폴더를 건너뜁니다.

활동 탭

활동 탭에는 과거 90일의 활동에 대한 개요가 나와 있습니다.

대시보드에서 작업을 필터링하려면

1. **장치 이름** 필드에서 활동이 수행되는 머신을 지정합니다.
2. **상태** 드롭다운 목록에서 상태를 선택합니다. 예: 성공, 실패, 진행 중, 취소.
3. **작업 제거** 드롭다운 목록에서 작업을 선택합니다. 예: 계획 적용, 백업 삭제, 소프트웨어 업데이트 설치.
4. **최근** 필드에서 작업 기간을 설정합니다. 예: 최신 활동, 24시간 전부터 발생한 활동 또는 과거 90일 내 특정 기간 동안의 활동.
5. 파트너 관리자로 **활동** 탭에 액세스하는 경우 관리하는 특정 고객의 활동을 필터링할 수 있습니다.

활동 탭의 보기를 사용자 정의하려면 기어 아이콘을 클릭하고 확인하려는 열을 선택합니다. 활동 진행률을 실시간으로 확인하려면 **자동 새로 고침** 확인란을 선택합니다.

실행 중인 활동을 취소하려면 활동 이름을 클릭하고 **상세정보** 화면에서 **취소**를 클릭합니다.

나열된 활동은 다음 기준으로 검색할 수 있습니다.

- 장치 이름
  활동이 수행되는 머신입니다.
- 시작한 사람
  활동을 시작한 계정입니다.

다음 속성을 기준으로 원격 데스크탑 작업을 필터링할 수 있습니다.

- 계획 생성
- 계획 적용
- 계획 철회
- 계획 삭제 중
- 원격 연결
  - RDP를 통한 클라우드 원격 데스크탑 연결
  - NEAR를 통한 클라우드 원격 데스크탑 연결
  - Apple 화면 공유를 통한 클라우드 원격 데스크탑 연결
  - 웹 클라이언트를 통한 원격 데스크탑 연결
  - 빠른 지원을 통한 원격 데스크탑 연결
  - RDP를 통한 직접 원격 데스크탑 연결
  - Apple 화면 공유를 통한 직접 원격 데스크탑 연결
  - 파일 전송
  - 빠른 지원을 통한 파일 전송

© Acronis International GmbH, 2003-2024

- 원격 작업
  - 워크로드 종료
  - 워크로드 다시 시작
  - 워크로드에서 원격 사용자 로그아웃 처리
  - 워크로드에서 사용자의 휴지통 비우기
  - 워크로드를 절전 모드로 설정

Cyber Protect 모니터

Cyber Protect 모니터에는 Agent for Windows 또는 Agent for Mac이 설치된 머신의 보호 상태 관련 정보가 표시됩니다. 사용자는 백업 암호화 및 프록시 서버 설정을 구성할 수 있습니다.

머신에 Agent for File Sync & Share를 설치하면 Cyber Protect 모니터를 통해 File Sync & Share 서비스에 액세스할 수 있습니다. 필수 온보딩 단계를 완료하면 File Sync & Share 기능에 액세스할 수 있습니다. 온보딩 단계에서는 사용자가 본인의 File Sync & Share 계정에 로그인한 후 개인 동기화 폴더를 선택합니다. Agent for File Sync & Share에 대한 자세한 내용은 Cyber Files Cloud 사용자 안내서를 참조하십시오.

중요
Cyber Protect Cyber Protection 또는 File Sync & Share 서비스에 대한 관리 권한이 없는 사용자도 모니터에 액세스할 수 있습니다.

관리 권한이 없는 사용자가 수행할 수 있는 작업이 아래 표에 요약되어 있습니다.

설치된 에이전트	사용자가 수행할 수 있는 작업	사용자가 수행할 수 없는 작업
Agent for Windows 또는 Agent for Mac	• 머신에 기본 보호 계획 추가 • 머신의 보호 상태 확인 • Active Protection 알림 수신 • 머신 백업을 임시로 일시 정지 • 프록시 서버 설정 구성 • 백업 암호화 설정 변경 **경고!** Cyber Protect 모니터에서 암호화 설정을 변경하면 보호 계획의 설정을 해당 설정으로 덮어쓰며 머신의 모든 백업에 변경된 설정이 적용됩니다. 이 작업을 수행하면 일부 보호 계획에서 오류가 발생할 수 있습니다. 자세한 내용은 "암호화"(402페이지) 항목을 참조하십시오. 비밀번호를 잃어버리거나 기억나지 않으면 암호화된 백업을 복구할 방법이 없습니다.	• 사용자 정의 보호 계획 적용 • 이미 적용된 보호 계획 관리

© Acronis International GmbH, 2003-2024

설치된 에이전트	사용자가 수행할 수 있는 작업	사용자가 수행할 수 없는 작업
Agent for Windows 및 Agent for Sync and Share Agent for Mac 및 Agent for Sync and Share	• 로컬 동기화 폴더와 File Sync & Share 계정 간에 내용 동기화 • 동기화 작업 일시 정지 • 동기화 폴더 변경 • 동기화할 수 없는 파일 유형 확인	• 동기화할 수 없는 파일 유형 편집

Cyber Protect Monitor에서 프록시 서버 설정 구성

Cyber Protect Monitor에서 프록시 서버 설정을 구성할 수 있습니다. 해당 구성은 머신에 설치하는 모든 에이전트에 적용됩니다.

프록시 서버 설정을 구성하려면

1. Cyber Protect 모니터를 열고 오른쪽 위 구석에서 기어 아이콘을 클릭합니다.
2. **설정**을 클릭한 후 **프록시**를 클릭합니다.
3. **프록시 서버 사용** 스위치를 활성화한 후 프록시 서버 주소 및 포트를 입력합니다.
4. [프록시 서버 액세스가 암호로 보호된 경우] **암호 필요** 스위치를 활성화한 후 사용자 이름 및 암호를 입력하여 프록시 서버에 액세스합니다.
5. **저장**을 클릭합니다.
   프록시 서버 설정은 `http-proxy.yaml` 파일에 저장됩니다.

보고

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

작업 보고서에는 대시보드 위젯 집합이 포함될 수 있습니다. 모든 위젯에는 회사 전체에 대한 요약 정보가 표시됩니다.

위젯 유형에 따라 보고서에는 특정 시간 범위의 데이터가 포함될 수도 있고, 보고서 찾아보기 또는 생성 시점의 데이터가 포함될 수도 있습니다. "위젯 유형에 따라 보고된 데이터"(290페이지)을(를) 참조하십시오.

모든 이력 위젯에는 같은 시간 범위의 데이터가 표시됩니다. 보고서 설정에서 이 범위를 변경할 수 있습니다.

기본 보고서를 사용하거나 사용자 정의 보고서를 생성할 수 있습니다.

XLSX(Excel) 또는 PDF 형식 보고서를 다운로드하거나 이메일로 전송할 수 있습니다.

기본 보고서 세트는 보유한 Cyber Protection 서비스 버전에 따라 달라집니다. 기본 보고서에 포함되어 있는 항목:

© Acronis International GmbH, 2003-2024

보고서 이름	설명
머신별 #CyberFit Score	각 머신의 보안 메트릭 평가 및 구성에 기반한 #CyberFit Score와 개선을 위한 권장 사항을 보여줍니다.
경보	지정된 기간 동안 발생한 경보를 표시합니다.
백업 스캔 세부 정보	백업에서 감지된 위협에 대한 자세한 정보를 표시합니다.
일일 작업	지정된 기간 동안 수행된 작업에 대한 요약 정보를 표시합니다.
데이터 보호 맵	머신에 있는 모든 중요 파일의 수, 크기, 위치, 보호 상태에 대한 자세한 정보를 표시합니다.
감지된 위협	차단된 위협, 양호한 머신 및 취약한 머신의 수를 통해 감염된 머신에 대한 자세한 정보를 표시합니다.
검색된 머신	조직 네트워크에서 발견된 모든 머신의 목록을 표시합니다.
디스크 상태 예측	HDD/SDD가 고장나게 되는 예상 시기와 현재 디스크 상태를 표시합니다.
기존 취약성	조직 OS 및 애플리케이션에 이미 존재하는 취약성의 목록을 보여줍니다. 이 보고서는 나열된 모든 제품과 관련하여 네트워크 내에서 영향을 받는 머신에 대한 상세 정보도 표시합니다.
소프트웨어 인벤토리	회사 장치에 설치된 소프트웨어에 대한 정보를 표시합니다.
하드웨어 인벤토리	회사 장치에서 사용할 수 있는 하드웨어에 대한 정보를 표시합니다.
패치 관리 요약	누락된 패치, 설치된 패치, 적용 가능한 패치의 수를 목록으로 보여줍니다. 이 보고서를 자세히 살펴보면 모든 시스템의 상세 정보 및 누락/설치된 패치 정보를 확인할 수 있습니다.
요약	지정된 기간 동안 보호되는 장치에 대한 요약 정보를 표시합니다.
주간 작업	지정된 기간 동안 수행된 작업에 대한 요약 정보를 표시합니다.
원격 세션	원격 데스크탑 및 파일 전송 세션에 대한 정보가 표시됩니다.

보고서 관련 작업

보고서를 보려면 보고서 이름을 클릭합니다.

새 보고서를 추가하려면

1. Cyber Protect 콘솔에서 **보고서**로 이동합니다.
2. 사용 가능한 보고서 목록에서 **보고서 추가**를 클릭합니다.

© Acronis International GmbH, 2003-2024

3. [사전 정의된 보고서를 추가하려는 경우] 사전 정의된 보고서 이름을 클릭합니다.
4. [사용자 정의 보고서를 추가하려는 경우] **사용자 정의**를 클릭하고 보고서에 위젯을 추가합니다.
5. [선택 사항] 위젯을 끌어서 놓아 재정렬합니다.

보고서를 편집하는 방법

1. Cyber Protect 콘솔에서 **보고서**로 이동합니다.
2. 보고서 목록에서 편집할 보고서를 선택합니다.

   수행할 수 있는 작업은 다음과 같습니다.
   - 보고서 이름 변경
   - 보고서 내 모든 위젯의 시간 범위 변경
   - 보고서 수신인 및 수신인에게 보고서를 전송할 시간 지정 사용 가능한 형식은 PDF와 XLSX입니다.

보고서를 삭제하려면

1. Cyber Protect 콘솔에서 **보고서**로 이동합니다.
2. 보고서 목록에서 삭제할 보고서를 선택합니다.
3. 말줄임표 아이콘(...)을 클릭한 후에 **삭제**를 클릭합니다.
4. **삭제**를 클릭하여 선택을 확인합니다.

보고서를 예약하는 방법

1. Cyber Protect 콘솔에서 **보고서**로 이동합니다.
2. 보고서 목록에서 예약할 보고서를 선택하고 **설정**을 클릭합니다.
3. **예약된** 스위치를 활성화합니다.
   - 수신인의 이메일 주소를 지정합니다.
   - 보고서의 형식을 선택합니다.

     참고
     PDF 파일 하나에서는 항목을 1,000개까지, XLSX 파일 하나에서는 항목을 10,000개까지 내보낼 수 있습니다. PDF 및 XLSX 파일의 타임 스탬프에는 머신의 로컬 시간이 사용됩니다.
   - 보고서의 언어를 선택합니다.
   - 일정을 구성합니다.
4. **저장**을 클릭합니다.

보고서를 다운로드하려면

1. Cyber Protect 콘솔에서 **보고서**로 이동합니다.
2. 보고서 목록에서 보고서를 선택하고 **다운로드**를 클릭합니다.
3. 보고서의 형식을 선택합니다.

보고서를 전송하려면

1. Cyber Protect 콘솔에서 **보고서**로 이동합니다.
2. 보고서 목록에서 보고서를 선택하고 **전송**을 클릭합니다.

© Acronis International GmbH, 2003-2024

3. 수신인의 이메일 주소를 지정합니다.
4. 보고서의 형식을 선택합니다.
5. **보내기**를 클릭합니다.

보고서 구조를 내보내려면

1. Cyber Protect 콘솔에서 **보고서**로 이동합니다.
2. 보고서 목록에서 보고서를 선택합니다.
3. 말줄임표 아이콘(...)을 클릭한 후에 **내보내기**를 클릭합니다.

그러면 보고서 구조가 머신에 JSON 파일로 저장됩니다.

보고서 데이터를 덤프하려면

이 옵션을 사용하면 사용자 정의 기간 동안의 모든 데이터를 필터링하지 않고 CSV 파일로 내보낸 다음 이메일 수신인에게 해당 CSV 파일을 전송할 수 있습니다.

참고
CSV 파일 하나에서 항목을 150,000개까지 내보낼 수 있습니다. CSV 파일의 타임 스탬프에는 UTC (Coordinated Universal Time)가 사용됩니다.

1. Cyber Protect 콘솔에서 **보고서**로 이동합니다.
2. 보고서 목록에서 데이터를 덤프할 보고서를 선택합니다.
3. 말줄임표 아이콘(...)을 클릭한 후에 **데이터 덤프**를 클릭합니다.
4. 수신인의 이메일 주소를 지정합니다.
5. **시간 범위**에서 데이터를 덤프할 사용자 정의 기간을 지정합니다.

   참고
   CSV 파일을 준비하는 기간이 길수록 소요 시간도 길어집니다.

6. **보내기**를 클릭합니다.

위젯 유형에 따라 보고된 데이터

대시보드의 위젯은 표시하는 데이터 범위에 따라 두 가지 유형으로 구분할 수 있습니다.

- 찾아보기 또는 보고서 생성 시점의 실제 데이터를 표시하는 위젯
- 내역 데이터를 표시하는 위젯

특정 기간의 데이터를 덤프하기 위해 보고서 설정에서 날짜 범위를 구성하면 선택한 시간 범위는 내역 데이터를 표시하는 위젯에만 적용됩니다. 찾아보기 시점의 실제 데이터를 표시하는 위젯에는 시간 범위 매개변수가 적용되지 않습니다.

다음 표에는 사용 가능한 위젯과 해당 데이터 범위가 나와 있습니다.

위젯 이름	위젯과 보고서에 표시되는 데이터
머신별 #CyberFit Score	실제

© Acronis International GmbH, 2003-2024

최신 경보 5개	실제
활성 경보 세부 정보	실제
활성 경보 요약	실제
작업	내역
활동 목록	내역
경보 내역	내역
공격 전술 통계	내역
백업 스캔 세부 정보(위협)	내역
백업 상태	내역 - **총 실행 수** 및 **성공한 실행 수** 열 실제 - 기타 모든 열
차단된 URL	실제
클라우드 애플리케이션	실제
Cyber protection	실제
데이터 보호 맵	내역
장치	실제
검색된 머신	실제
디스크 상태 개요	실제
실제 장치별 디스크 상태	실제
기존 취약성	내역
하드웨어 변경	내역
하드웨어 상세 정보	실제
하드웨어 인벤토리	실제
경보 내역 요약	내역
사건 심각도 이력	내역
위치 요약	실제
카테고리별 누락 업데이트	실제
보호되지 않음	실제
패치 설치 내역	내역
패치 설치 상태	내역

© Acronis International GmbH, 2003-2024

패치 설치 요약	내역
보호 상태	실제
최근 영향 받은 항목	내역
원격 세션	내역
보안 인시던트 번다운(Burndown)	내역
보안 인시던트 MTTR	내역
소프트웨어 인벤토리	실제
소프트웨어 개요	내역
위협 상태	실제
취약한 머신	실제
워크로드 네트워크 상태	실제

© Acronis International GmbH, 2003-2024

Cyber Protect 콘솔에서 워크로드 관리

이 섹션에서는 Cyber Protect 콘솔에서 워크로드를 관리하는 방법에 대해 설명합니다.

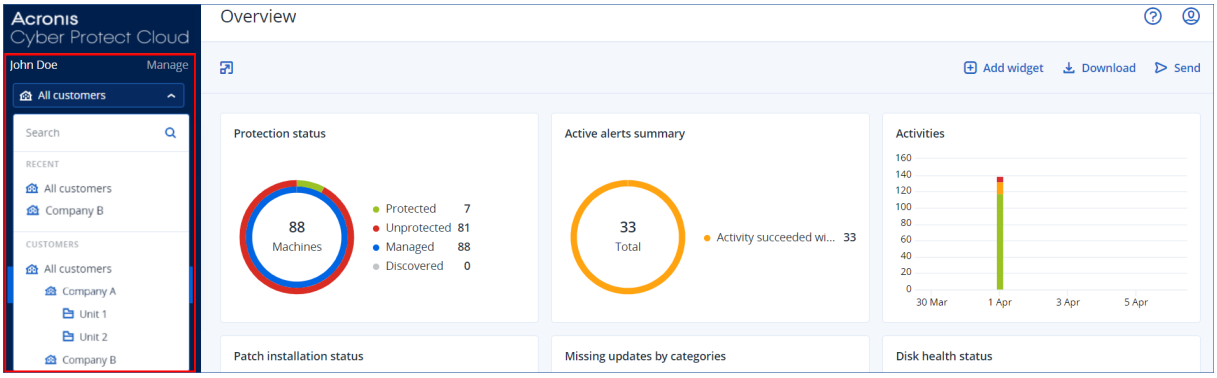
Cyber Protect 콘솔

Cyber Protect 콘솔에서 워크로드와 계획을 관리하거나, 보호 설정을 변경하거나, 보고서를 구성하거나, 백업 스토리지를 확인할 수 있습니다.

Cyber Protect 콘솔을 이용하면 File Sync & Share, 안티바이러스 및 안티맬웨어 보호, 패치 관리, 장치 제어, 취약점 평가 등의 추가 서비스나 기능에도 액세스할 수 있습니다. 이러한 서비스와 기능의 유형 및 수는 Cyber Protection 라이선스에 따라 달라집니다.

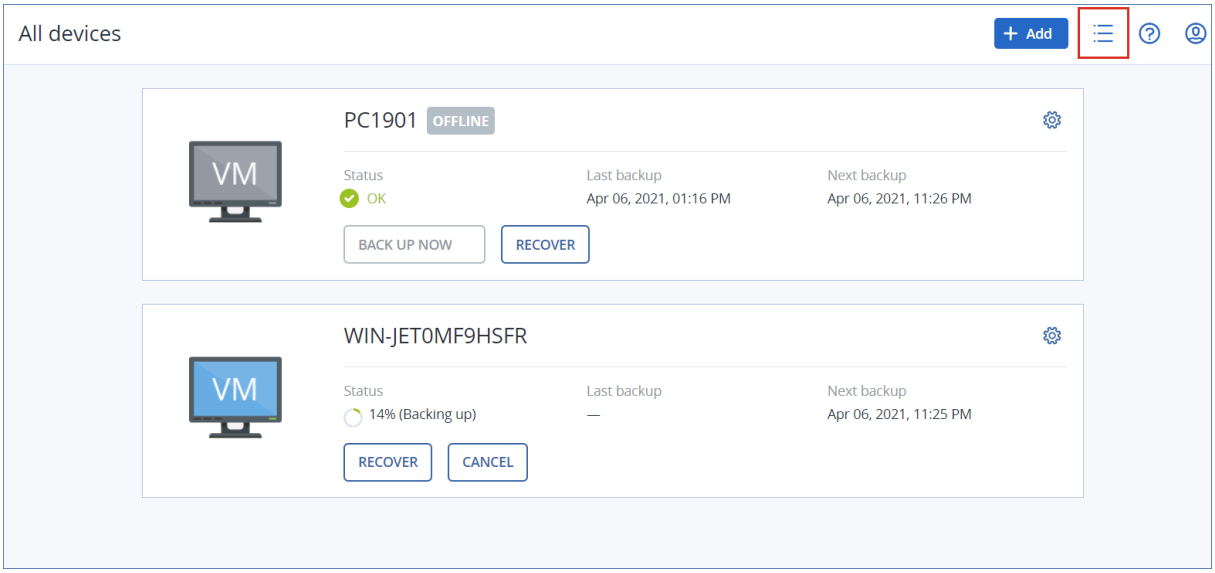
대시보드에서 보호와 관련된 가장 중요한 정보를 확인하려면 **모니터링** > **개요**로 이동합니다.

액세스 권한에 따라 테넌트의 고객 테넌트나 단위 하나 또는 여러 개에 적용되는 보호를 관리할 수 있습니다. 계층 수준을 전환하려면 탐색 메뉴의 드롭다운 목록을 사용합니다. 액세스 권한이 있는 수준만 표시됩니다. 관리 포털로 이동하려면 **관리**를 클릭합니다.



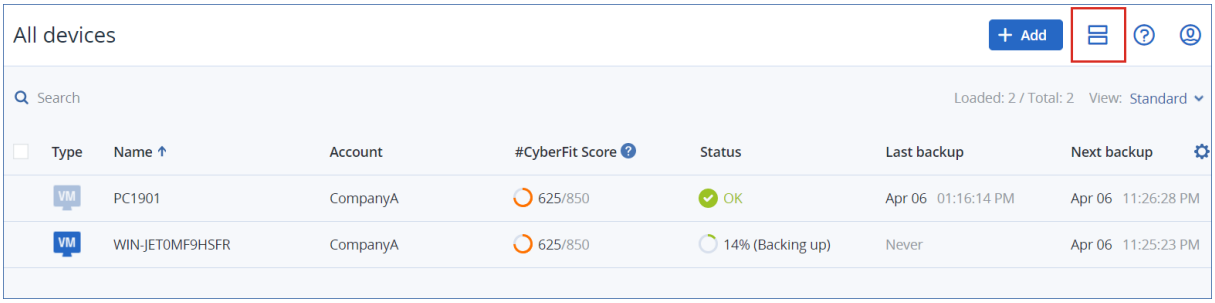
쉽게 확인 가능한 표 보기 형식의 **장치** 섹션이 제공됩니다. 이러한 보기 간에 전환하려면 오른쪽 위 구석에서 해당 아이콘을 클릭합니다.

단순 보기에는 워크로드 몇 개만 표시됩니다.



© Acronis International GmbH, 2003-2024

워크로드 수가 많아지면 테이블 보기가 자동으로 활성화됩니다.



두 보기 모두 동일한 기능 및 작업에 대한 액세스를 제공합니다. 이 문서에서는 테이블 보기에서 작업에 액세스하는 방법에 대해 설명합니다.

워크로드가 온라인 또는 오프라인 상태가 되면 Cyber Protect 콘솔에서 상태가 변경되는 데 시간이 걸립니다. 워크로드 상태는 1분마다 점검됩니다. 해당 머신에 설치된 에이전트가 데이터를 전송하지 않고 5회 연속 점검에 응답하지 않으면 워크로드가 오프라인으로 표시됩니다. 워크로드가 상태 점검에 응답하거나 데이터 전송을 시작하면 다시 온라인 상태로 표시됩니다.

Cyber Protect 콘솔의 새로운 기능

Cyber Protect Cloud의 새 기능이 제공되면 Cyber Protect 콘솔 로그인 시에 이러한 기능의 간략한 설명이 포함된 팝업 창이 표시됩니다.

기본 콘솔 창 왼쪽 아래의 **새로운 기능** 링크를 클릭하여 새 기능의 설명을 확인할 수도 있습니다.

새 기능이 없으면 **새로운 기능** 링크가 표시되지 않습니다.

파트너 관리자로 Cyber Protect 콘솔 사용

파트너 관리자는 파트너 테넌트(**모든 고객**) 수준 또는 고객 테넌트 수준에서 Cyber Protect 콘솔을 사용할 수 있습니다.

파트너 테넌트(**모든 고객**) 수준

파트너 테넌트(**모든 고객**) 수준에서는 다음 작업을 수행할 수 있습니다:

- 모든 관리 대상 고객 테넌트의 워크로드용 스크립팅 계획 관리.
  여러 고객의 워크로드에 같은 스크립팅 계획을 적용할 수 있으며 여러 고객의 워크로드로 장치 그룹을 생성할 수도 있습니다. 파트너 수준에서 정적 또는 동적 그룹을 생성하는 방법을 알아보려면 "파트너 수준에서 정적 장치 그룹 생성"(297페이지) 및 "파트너 수준에서 동적 장치 그룹 생성"(297페이지) 항목을 참조하십시오. 스크립트 및 스크립팅 계획에 대한 자세한 내용은 "Cyber Scripting"(217페이지) 항목을 참조하십시오.
- 모든 관리 대상 고객 테넌트의 워크로드용 모니터링 계획 생성.
- 모든 관리 대상 고객 테넌트의 워크로드용 원격 관리 계획 생성.
- 개별 고객의 인시던트 화면에 일일이 액세스할 필요 없이 인시던트 관리 인터페이스 하나에서 모든 고객 테넌트의 엔드포인트 탐지 및 대응(EDR) 인시던트를 확인 및 관리할 수 있습니다.
- 모든 관리 대상 고객 테넌트의 머신 자동 검색 수행.

© Acronis International GmbH, 2003-2024

고객 테넌트 수준

이 수준에서 파트너 관리자는 자신이 대리하는 회사 관리자와 동일한 권한을 갖습니다.

테넌트 수준 선택

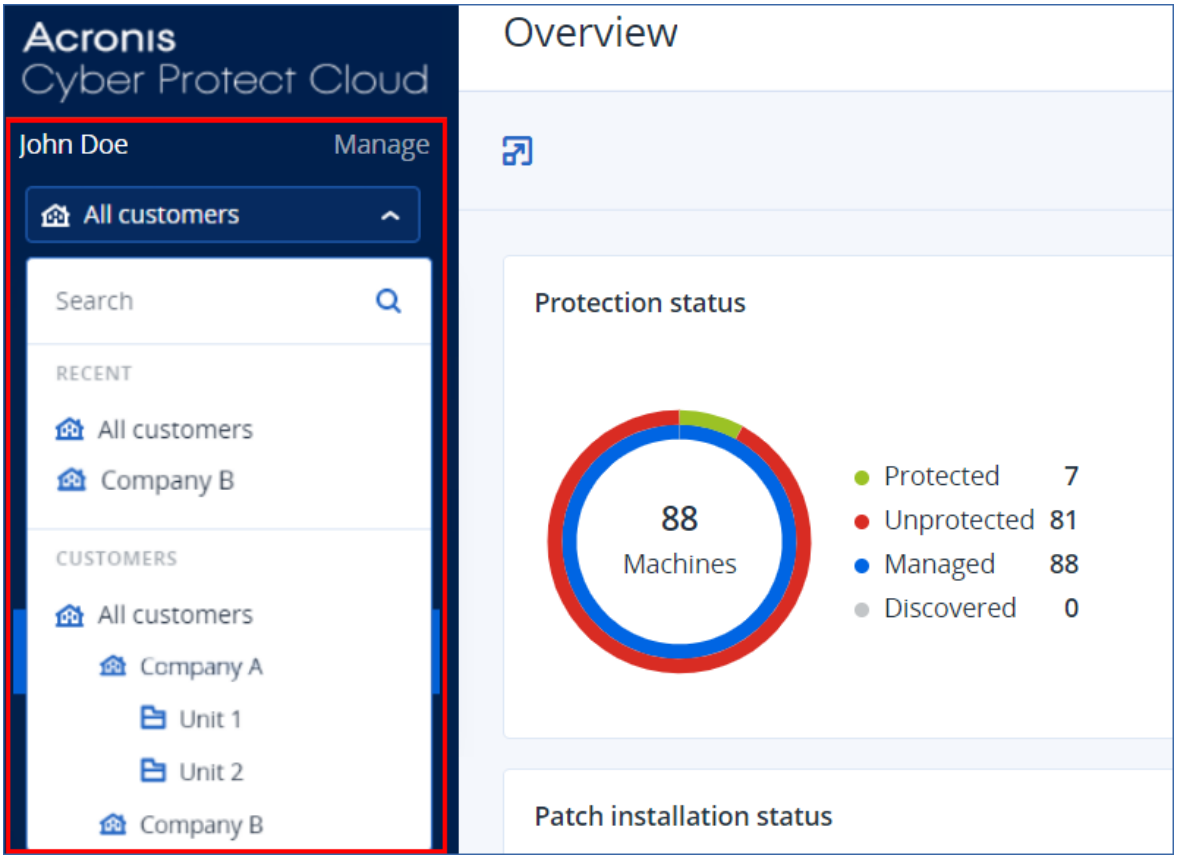
Cyber Protect 콘솔에서 작업할 테넌트 수준을 선택할 수 있습니다.

사전 요구 사항

- Cyber Protect 콘솔과 관리 포털에 모두 액세스할 수 있습니다.
- 여러 테넌트나 단위를 관리할 수 있습니다.

Cyber Protect 콘솔에서 테넌트 수준을 선택하려면

1. 왼쪽 탐색 메뉴에서 고객 테넌트 이름 옆의 화살표를 클릭합니다.
2. 다음 옵션 중 하나를 선택합니다.
   - 파트너 수준에서 작업하려면 **모든 고객**을 선택합니다.
   - 고객 또는 부서 수준에서 작업하려면 고객 또는 부서 이름을 선택합니다.



Cyber Protect 콘솔의 파트너 테넌트 수준

파트너 테넌트(**모든 고객**) 수준에서 Cyber Protect 콘솔을 사용할 때는 사용자 정의 보기를 사용할 수 있습니다.

© Acronis International GmbH, 2003-2024

경보 및 **활동** 탭은 추가 파트너 관련 파일을 제공하지만 **장치** 및 **관리** 탭에서는 파트너 관리자가 액세스할 수 있는 기능 또는 객체에만 액세스할 수 있습니다.

경보 탭

여기서 관리하는 모든 고객의 경보를 확인 및 검색하고 다음 기준에 따라 필터링할 수 있습니다.

- 장치
- 고객
- 계획

이러한 기준 각각에 대해 여러 개의 항목을 선택할 수 있습니다.

활동 탭

여기서 관리하는 모든 테넌트의 활동 또는 특정 고객 테넌트의 활동을 볼 수 있습니다.

고객, 상태, 시간 및 유형별로 활동을 필터링할 수 있습니다.

다음 활동 유형은 이 수준에서 자동으로 사전 선택되어 있습니다.

- 계획 적용
- 보호 계획 생성
- 보호 계획
- 계획 철회
- 스크립트 작성

장치 탭

에이전트가 있는 머신 탭에서는 관리하는 고객 테넌트의 모든 워크로드를 보고 하나 이상의 테넌트에서 워크로드를 선택할 수 있습니다. 다양한 테넌트의 워크로드를 포함하는 장치 그룹을 생성할 수도 있습니다.

중요

파트너(**모든 고객**) 수준에서 작업을 할 때는 몇 가지 장치 관련 작업만 수행할 수 있습니다. 예를 들어 다음 작업은 수행할 수 없습니다:

- 고객 장치에서 기존 보호 계획 확인 및 관리.
- 새 보호 계획 생성.
- 백업 복구.
- Disaster Recovery 사용.
- Cyber Protection 데스크탑 기능 액세스.

이러한 작업은 고객 수준에서 수행해야 합니다.

소프트웨어 관리 탭

고객 워크로드에 대해 소프트웨어 인벤토리 스캔이 활성화되어 있으면 소프트웨어 스캔 결과를 확인할 수 있습니다.

© Acronis International GmbH, 2003-2024

특정 고객의 워크로드 확인

파트너 관리자는 관리 대상 고객 테넌트에 속한 워크로드를 확인할 수 있습니다.

특정 고객의 워크로드를 확인하려면

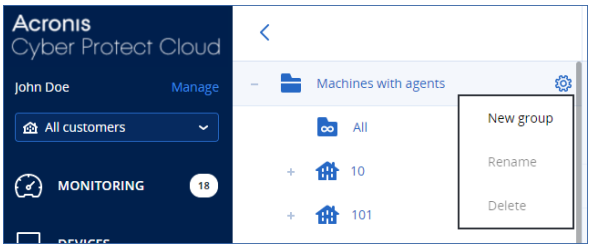
1. Cyber Protect 콘솔에서 **장치** > **에이전트가 있는 머신**으로 이동합니다.
2. 트리에서 **에이전트가 있는 머신**을 선택하여 목록을 확장합니다.
3. 확인 및 관리하려는 워크로드에 해당하는 고객의 이름을 클릭합니다.

파트너 수준에서 정적 장치 그룹 생성

파트너 (**모든 장치**) 수준에서 정적 장치 그룹을 생성할 수 있습니다.

파트너 수준에서 정적 장치 그룹을 생성하려면

1. Cyber Protect 콘솔에서 **장치** > **에이전트가 있는 머신**으로 이동합니다.
2. **에이전트가 있는 머신** 옆에 있는 기어 아이콘을 클릭한 다음 **새 그룹**을 클릭합니다.



3. 그룹 이름을 지정합니다.
4. [선택 사항] 설명을 추가합니다.
5. **확인**을 클릭합니다.

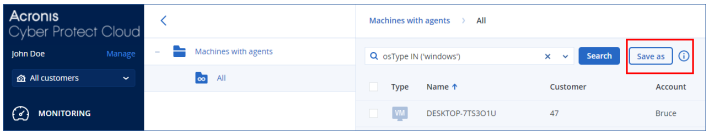
파트너 수준에서 동적 장치 그룹 생성

파트너 (**모든 장치**) 수준에서 동적 장치 그룹을 생성할 수 있습니다.

파트너 수준에서 동적 장치 그룹을 생성하려면

1. Cyber Protect 콘솔에서 **장치** > **에이전트가 있는 머신**으로 이동합니다.
2. 트리에서 **에이전트가 있는 머신**을 선택하여 목록을 확장합니다.
3. **모두**를 클릭합니다.
4. 검색 필드에 동적 장치 그룹을 생성할 기준을 지정한 다음 **검색**을 클릭합니다.

   사용 가능한 검색 조건에 대해 자세히 알아보려면 "클라우드 간 워크로드가 아닌 워크로드의 속성 검색"(318페이지) 및 "클라우드 간 워크로드의 속성 검색"(317페이지) 항목을 참조하십시오.
5. **다른 이름으로 저장**을 클릭한 다음 그룹 이름을 지정합니다.



© Acronis International GmbH, 2003-2024

6. [선택 사항] 설명을 추가합니다.
7. **확인**을 클릭합니다.

파트너 테넌트 수준에서 머신 자동 검색 수행

파트너 테넌트(**모든 고객**) 수준에서 머신 자동 검색을 수행할 수 있습니다.

사전 요구 사항

Active Directory 도메인이나 고객의 로컬 네트워크에 보호 에이전트가 설치된 머신이 하나 이상 있어야 합니다.

중요
Windows 머신에 설치된 에이전트만 검색 에이전트로 사용할 수 있습니다. 고객 환경 내에 검색 에이전트가 없으면 **장치 추가** 패널에서 **여러 장치** 옵션을 사용할 수 없습니다.

에이전트 서비스를 실행하려면 추가 권한이 필요하므로 도메인 컨트롤러 추가 시에는 자동 검색이 지원되지 않습니다.

에이전트 원격 설치는 Windows를 실행하는 머신에서만 지원됩니다(Windows XP는 지원되지 않음). Windows Server 2012 R2를 실행하는 머신에 에이전트를 원격 설치하려면 Windows 업데이트 KB2999226을 설치해야 합니다.

파트너 테넌트 수준에서 머신 자동 검색을 수행하려면

1. Cyber Protect 콘솔에서 **모든 고객**을 선택합니다.
2. **장치** > **모든 장치**로 이동합니다.
3. **추가**를 클릭합니다.
4. **여러 개의 장치**에서 **Windows 전용**을 클릭합니다. 검색 마법사가 열립니다.
5. 고객 테넌트를 선택하고 머신 탐지를 위해 스캔을 수행할 검색 에이전트를 선택합니다.
6. 검색 방법 선택:
   - **Active Directory 검색**. 검색 에이전트가 설치된 머신이 Active Directory 도메인 멤버여야 합니다.
   - **로컬 네트워크 스캔**. 선택한 검색 에이전트에서 머신을 찾지 못한 경우 다른 검색 에이전트를 선택합니다.
   - **수동으로 지정 또는 파일에서 가져오기**. 추가할 머신을 수동으로 정의하거나 텍스트 파일에서 가져옵니다.
7. [Active Directory 검색 방법을 선택한 경우] 머신 검색 방법 선택:
   - **조직 단위 목록에서**. 추가될 머신 그룹을 선택합니다.
   - **LDAP 언어 쿼리에 따라** LDAP 언어 쿼리를 사용해 머신을 선택합니다. **검색 베이스**에서 검색할 위치를 정의한 후 **필터**에서 머신 선택 기준을 지정할 수 있습니다.

© Acronis International GmbH, 2003-2024

8. 선택한 검색 방법에 따라 다음 작업 중 하나를 수행합니다:

검색 방법	작업
Active Directory 검색	검색된 머신 목록에서 추가할 머신을 선택합니다.
로컬 네트워크 스캔	검색된 머신 목록에서 추가할 머신을 선택합니다.

수동으로 지정 또는 파일에서 가져오기	머신의 IP 주소 또는 호스트 이름을 직접 지정하거나 텍스트 파일의 머신 목록에서 가져옵니다. 해당 파일에는 IP 주소/호스트 이름이 한 줄에 하나씩 포함되어 있어야 합니다. 사용 가능한 파일의 예는 다음과 같습니다:
	`156.85.34.10`
	`156.85.53.32`
	`156.85.53.12`
	`EN-L00000100`
	`EN-L00000101`
	머신 주소를 수동으로 추가하거나 파일에서 가져오면, 에이전트는 추가된 머신을 핑하고 가용성을 정의하려 시도합니다.

9. 검색 후 수행해야 할 작업 선택:

옵션	설명
에이전트 설치 및 머신 등록	**컴포넌트 선택**을 클릭해 머신에 설치할 컴포넌트를 선택할 수 있습니다. 자세한 내용은 "설치할 컴퍼넌트 선택"(122페이지) 항목을 참조하십시오.
에이전트 서비스용 로그온 계정	이 설정은 **컴포넌트 선택** 화면에서 사용할 수 있습니다. 설정에 따라 서비스를 실행할 계정이 정의됩니다. 다음 옵션 중 하나를 선택할 수 있습니다: • **서비스 사용자 계정 사용**(에이전트 서비스용 기본값) 서비스 사용자 계정은 서비스를 실행하는 데 사용되는 Windows 시스템 계정입니다. 이 설정의 이점은 도메인 보안 정책이 이 계정의 사용자 권한에 영향을 미치지 않는다는 점입니다. 기본적으로 에이전트는 **로컬 시스템** 계정 하에서 실행됩니다. • **새 계정 생성** 계정 이름은 해당 에이전트에 대해 Agent User로 지정됩니다. • **다음 계정 사용** 도메인 컨트롤러에 에이전트를 설치하는 경우 시스템에 각 에이전트의 기존 계정(또는 동일한 계정)을 지정하라는 메시지가 표시됩니다. 보안상의 이유로 시스템은 도메인 컨트롤러에서 새 계정을 자동으로 생성하지 않습니다. **새 계정 생성** 또는 **다음 계정 사용** 옵션을 선택하는 경우 도메인 보안 정책이 관련 계정의 권한에 영향을 미치지 않는지 확인하십시오. 설치 중 계정에 할당되어 있는 사용자 권한이 박탈되는 경우 컴포넌트가 올바로 작동하지 않거나 전혀 작동하지 않을 수 있습니다.

© Acronis International GmbH, 2003-2024

옵션	설명
에이전트가 설치된 머신 등록	머신에 에이전트가 이미 설치되어 있어서 Cyber Protection에 등록만 하면 되는 경우 이 옵션을 사용합니다. 에이전트가 설치되어 있지 않은 머신은 **비관리** 머신으로 추가됩니다.
관리되지 않는 머신으로 추가	이 옵션을 선택하면 머신에 에이전트가 설치되지 않습니다. 콘솔에서 에이전트를 확인할 수 있으며 나중에 에이전트를 설치 또는 등록할 수 있습니다.
필요 시 머신 다시 시작	**에이전트 설치 및 머신 등록**을 선택하면 이 옵션이 표시됩니다. 이 옵션을 선택하면 설치를 완료하는 데 필요한 횟수만큼 머신이 다시 시작됩니다. 다음의 경우 머신을 다시 시작해야 할 수 있습니다. • 사전 요구 사항 설치가 완료되었고 설치를 계속하기 위해 다시 시작해야 하는 경우. • 설치가 완료되었지만 설치 중 일부 파일이 잠겨 다시 시작해야 하는 경우. • 설치가 완료되었지만 이전에 설치된 다른 소프트웨어에서 다시 시작을 요구하는 경우.
사용자가 로그인한 경우 다시 시작 안 함	**필요 시 머신 다시 시작**을 선택하면 이 옵션이 표시됩니다. 사용자가 시스템에 로그인한 상태에서 이 옵션을 선택하면 머신이 자동으로 다시 시작되지 않습니다. 예를 들어 설치 중에 머신을 다시 시작해야 할 때 사용자가 작업을 수행하는 중이라면 시스템이 다시 시작되지 않습니다. 사전 요구 사항은 설치되었는데 사용자가 로그인되어 있어서 머신이 다시 시작되지 않은 경우 설치를 완료하려면 머신을 다시 시작한 후 설치를 다시 시작해야 합니다. 에이전트는 설치되었는데 머신은 다시 시작되지 않았다면 머신을 다시 시작해야 합니다.
머신을 등록할 사용자	[조직에 단위가 있는 경우] 머신을 등록할 단위 또는 하위 단위가 속해 있는 사용자 계정을 선택합니다. [파트너 테넌트 수준에서 자동 검색 수행 시] 관리 대상 고객 테넌트 목록에서 트리 구조를 확장하고 머신을 등록할 사용자 계정을 선택합니다. [자동 검색을 수행하는 고객 관리자] **에이전트 설치 및 머신 등록** 또는 **에이전트가 설치된 머신 등록**을 선택한 경우에는 머신에 보호 계획을 적용하는 옵션도 사용 가능합니다. 보호 계획이 여러 개라면 사용할 계획을 선택할 수 있습니다.

10. 모든 머신에 대한 관리자 권한이 있는 사용자의 자격 증명을 지정합니다.

중요
에이전트의 원격 설치는 기본 제공 관리자 계정(운영 체제 설치 시 생성한 첫 번째 계정)의 자격 증명을 지정한 경우에만 아무런 준비 과정 없이 작동합니다. 사용자 정의 관리자 자격 증명을 정의하려는 경우에는 "사전 요구 사항"(298페이지)의 설명에 따라 추가 준비 작업을 수행해야 합니다.

11. 시스템은 모든 머신의 연결을 확인합니다. 연결되지 않는 일부 머신에 대한 자격 증명을 변경할 수 있습니다.

머신 검색이 시작되고 나면 **모니터링** > **활동** > **머신 검색** 활동에서 해당하는 작업을 확인할 수 있습니다.

© Acronis International GmbH, 2003-2024

다중 테넌시 지원

Cyber Protection 서비스는 다음 수준에서의 관리를 의미하는 멀티테넌시를 지원합니다.

- [서비스 제공업체의 경우] 파트너 테넌트(**모든 고객**) 수준
  이 수준은 고객 테넌트를 관리하는 파트너 관리자만 사용할 수 있습니다.
- 고객 테넌트 수준
  이 수준은 회사 관리자가 관리합니다.
  파트너 관리자도 자신이 관리하는 고객 테넌트에서 이 수준에서 작업할 수 있습니다. 이 수준에서 파트너 관리자는 자신이 대리하는 고객 관리자와 동일한 권한을 갖습니다.
- 부서 수준
  이 수준은 부서 관리자 및 상위 고객 테넌트의 회사 관리자가 관리합니다.
  상위 고객 테넌트를 관리하는 파트너 관리자도 부서 수준에 액세스할 수 있습니다. 이 수준에서 파트너 관리자는 자신이 대리하는 고객 관리자와 동일한 권한을 갖습니다.

관리자는 자신의 테넌트 및 하위 테넌트에서 객체를 관리할 수 있습니다. 상위 관리 수준의 객체는 보거나 액세스할 수 없습니다.

예를 들어, 회사 관리자는 고객 테넌트 수준과 장치 수준 모두에서 보호 계획을 관리할 수 있습니다. 부서 관리자는 부서 수준에서 자신의 보호 계획만 관리할 수 있습니다. 고객 테넌트 수준에서 보호 계획을 관리할 수 없으며 부서 수준에서 고객 관리자가 생성한 보호 계획을 관리할 수 없습니다.

또한 파트너 관리자는 자신이 관리하는 고객 테넌트에서 스크립팅 계획을 생성하고 적용할 수 있습니다. 이러한 테넌트의 회사 관리자는 파트너 관리자가 워크로드에 적용한 스크립팅 계획에 읽기 전용으로만 액세스할 수 있습니다. 그러나 고객 관리자는 고유한 스크립팅 또는 보호 계획을 생성하고 적용할 수 있습니다.

워크로드

워크로드는 실제 머신, 가상 머신, 사서함, 데이터베이스 인스턴스 등 모든 유형의 보호되는 리소스입니다. Cyber Protect 콘솔에서 워크로드는 계획(보호 계획, 백업 계획 또는 스크립팅 계획)을 적용할 수 있는 객체로 표시됩니다.

보호 에이전트를 설치하거나 가상 어플라이언스를 디플로이해야 하는 워크로드도 있습니다. 에이전트는 그래픽 사용자 인터페이스 또는 명령줄 인터페이스(무인 설치)를 사용하여 설치할 수 있습니다. 무인 설치를 사용하면 설치 절차를 자동화할 수 있습니다. 보호 에이전트 설치 방법에 대한 자세한 내용은 "Cyber Protection 에이전트 설치 및 디플로이"(55페이지) 항목을 참조하십시오.

VA(가상 어플라이언스)는 보호 에이전트가 포함되어 있는 이미 생성된 가상 머신입니다. 가상 어플라이언스 사용 시에는 보호 에이전트를 설치하지 않고도 동일 환경 내의 다른 가상 머신을 백업할 수 있습니다(비에이전트 백업). 가상 어플라이언스는 .ovf, .ova, .qcow 등의 하이퍼바이저별 형식으로 제공됩니다. 비에이전트 백업을 지원하는 가상화 플랫폼에 대한 자세한 내용은 "지원되는 가상화 플랫폼"(30페이지) 항목을 참조하십시오.

© Acronis International GmbH, 2003-2024

중요
최소 30일에 한 번 이상 에이전트를 온라인 상태로 설정해야 합니다. 그렇지 않은 경우에는 에이전트의 계획이 해지되며 워크로드가 보호되지 않습니다.

워크로드 유형 및 각 유형용 에이전트가 아래 표에 요약되어 있습니다.

워크로드 유형	에이전트	예 (목록에 포함된 항목 이외의 기타 워크로드 유형/에이전트도 있음)
실제 머신	보호되는 모든 머신에 보호 에이전트가 설치됩니다.	워크스테이션 노트북 서버
가상 머신	가상화 플랫폼에 따라 다음 백업 방법을 사용할 수 있습니다. • 에이전트 기반 백업 - 보호되는 모든 머신에 보호 에이전트가 설치됩니다. • 비에이전트 백업 - 보호 에이전트가 하이퍼바이저 호스트 또는 전용 가상 머신에만 설치되거나 가상 어플라이언스로 디플로이됩니다. 이 에이전트는 환경 내의 모든 가상 머신을 백업합니다.	VMware 가상 머신 Hyper-V 가상 머신 oVirt가 관리하는 커널 기반 가상 머신(KVM)
Microsoft 365 Business 워크로드 Google Workspace 워크로드	이러한 워크로드는 설치하지 않아도 되는 클라우드 에이전트가 백업합니다. 클라우드 에이전트를 사용하려면 Cyber Protect 콘솔에 Microsoft 365 또는 Google Workspace 조직을 추가해야 합니다. Office 365용 로컬 에이전트도 사용 가능합니다. 이 에이전트는 별도로 설치해야 하며, Exchange Online 사서함 백업에만 사용할 수 있습니다. 로컬 에이전트와 클라우드 에이전트 간의 차이점에 대한 자세한 내용은 "Microsoft 365 데이터 보호"(545페이지) 항목을 참조하십시오. .	Microsoft 365 사서함 Microsoft 365 OneDrive Microsoft Teams SharePoint 사이트 Google 사서함 Google Drive
애플리케이션	특정 애플리케이션의 데이터는 Agent for SQL, Agent for Exchange, Agent for MySQL/MariaDB, Agent for Active Directory 등의 전용 에이전트가 백업합니다.	SQL Server 데이터베이스 MySQL/MariaDB 데이터베이스 Oracle 데이터베이스 Active Directory
모바일 장치	보호되는 장치에 모바일 앱이 설치됩니다.	Android 또는 iOS

© Acronis International GmbH, 2003-2024

워크로드 유형	에이전트	예 (목록에 포함된 항목 이외의 기타 워크로드 유형/에이전트도 있음)
		장치
웹 사이트	웹 사이트는 설치하지 않아도 되는 클라우드 에이전트가 백업합니다.	SFTP 또는 SSH 프로토콜을 통해 액세스하는 웹 사이트

필요한 에이전트와 해당 에이전트를 설치해야 하는 위치에 대한 자세한 내용은 "필요한 에이전트"(57페이지) 항목을 참조하십시오

Cyber Protect 콘솔에 워크로드 추가

워크로드 보호를 시작하려면 먼저 Cyber Protect 콘솔에 워크로드를 추가합니다.

참고
추가할 수 있는 워크로드 유형은 계정의 서비스 할당량에 따라 달라집니다. 특정 워크로드 유형이 누락된 경우에는 **장치 추가** 창에서 해당 유형이 회색으로 표시됩니다.

파트너 관리자는 관리 포털에서 필요한 서비스 할당량을 활성화할 수 있습니다. 자세한 내용은 "파트너 관리자용 정보"(307페이지) 항목을 참조하십시오.

워크로드 추가 방법

1. Cyber Protect 콘솔에 로그인합니다.
2. **장치** > **모든 장치**로 이동한 후 **추가**를 클릭합니다.
   장치 추가 창이 오른쪽에 열립니다.
3. 릴리스 채널을 선택합니다.
4. 추가할 워크로드 유형을 클릭한 후 선택한 특정 워크로드용 지침을 따릅니다.

다음 표에 워크로드 유형과 각 유형별로 수행해야 하는 작업이 요약되어 있습니다.

추가할 워크로드	수행해야 하는 작업	진행해야 하는 절차
여러 Windows 머신	사용자 환경에서 자동 검색을 수행합니다. 자동 검색을 수행하려면 Active Directory 도메인이나 로컬 네트워크에 보호 에이전트가 설치된 머신이 하나 이상 있어야 합니다. 이 에이전트는 검색 에이전트로 사용됩니다.	"자동 검색 및 수동 검색 수행"(118페이지)
Windows 워크스테이션	Agent for Windows를 설치합니다.	"Windows에서 Protection 에이전트

© Acronis International GmbH, 2003-2024

추가할 워크로드	수행해야 하는 작업	진행해야 하는 절차
Windows 서버		설치"(72페이지) 또는 "Windows에서 무인 설치 또는 제거"(81페이지)
macOS 워크스테이션	Agent for macOS를 설치합니다.	"macOS에서 Protection 에이전트 설치"(76페이지) 또는 "macOS에 무인 설치 및 제거"(103페이지)
Linux 서버	Agent for Linux를 설치합니다.	"Linux에서 Protection 에이전트 설치"(74페이지) 또는 "Linux에서 무인 설치 또는 제거"(97페이지)
모바일 장치 (iOS, Android)	모바일 앱을 설치합니다.	"모바일 장치 보호"(538페이지)
클라우드 간 워크로드		
Microsoft 365 Business	Cyber Protect 콘솔에 Microsoft 365 조직을 추가한 후 클라우드 에이전트를 사용하여 Exchange Online 사서함, OneDrive 파일, Microsoft Teams 및 SharePoint 사이트를 보호합니다. 로컬 Agent for Office 365를 설치해도 됩니다. 이 경우 Exchange Online 사서함 백업만 제공됩니다. 로컬 에이전트와 클라우드 에이전트 간의 차이점에 대한 자세한 내용은 "Microsoft 365 데이터 보호"(545페이지) 항목을 참고하십시오.	"Microsoft 365 데이터 보호"(545페이지)
Google Workspace	Cyber Protect 콘솔에 Google Workspace 조직을 추가한 후 클라우드 에이전트를 사용하여 Gmail 사서함 및 Google Drive 파일을 보호합니다.	"Google Workspace 데이터 보호"(582페이지)
가상 머신		
VMware ESXi	사용자 환경에 Agent for VMware(가상	"Agent for VMware(가상 어플라이

© Acronis International GmbH, 2003-2024

추가할 워크로드	수행해야 하는 작업	진행해야 하는 절차
	어플라이언스)를 디플로이합니다.	언스) 배포"(125페이지)
	Agent for VMware(Windows)를 설치합니다.	"Windows에서 Protection 에이전트 설치"(72페이지) 또는 "Windows에서 무인 설치 또는 제거"(81페이지)
Virtuozzo Hybrid Infrastructure	사용자 환경에 Agent for Virtuozzo Hybrid Infrastructure(가상 어플라이언스)를 디플로이합니다.	"Agent for Virtuozzo Hybrid Infrastructure(가상 어플라이언스) 디플로이"(134페이지)
Hyper-V	Agent for Hyper-V를 설치합니다.	"Windows에서 Protection 에이전트 설치"(72페이지) 또는 "Windows에서 무인 설치 또는 제거"(81페이지)
Virtuozzo	Agent for Virtuozzo를 설치합니다.	"Linux에서 Protection 에이전트 설치"(74페이지) 또는 "Linux에서 무인 설치 또는 제거"(97페이지)
KVM	Agent for Windows를 설치합니다.	"Windows에서 Protection 에이전트 설치"(72페이지) 또는 "Windows에서 무인 설치 또는 제거"(81페이지)
	Agent for Linux를 설치합니다.	"Linux에서 Protection 에이전트 설치"(74페이지) 또는 "Linux에서 무인 설치 또는 제거"(97페이지)
Red Hat Virtualization (oVirt)	사용자 환경에 Agent for oVirt(가상 어플라이언스)를 디플로이합니다.	"Agent for oVirt(가상 어플라이언스) 디플로이 중"(142페이지)
Citrix XenServer	Agent for Windows를 설치합니다.	"Windows에서 Protection 에이전트 설치"(72페이지) 또는 "Windows에서 무인 설치 또는 제

© Acronis International GmbH, 2003-2024

추가할 워크로드	수행해야 하는 작업	진행해야 하는 절차
		거"(81페이지)
	Agent for Linux를 설치합니다.	"Linux에서 Protection 에이전트 설치"(74페이지) 또는 "Linux에서 무인 설치 또는 제거"(97페이지)
Nutanix AHV	Agent for Windows를 설치합니다.	"Windows에서 Protection 에이전트 설치"(72페이지) 또는 "Windows에서 무인 설치 또는 제거"(81페이지)
	Agent for Linux를 설치합니다.	"Linux에서 Protection 에이전트 설치"(74페이지) 또는 "Linux에서 무인 설치 또는 제거"(97페이지)
Oracle VM	Agent for Windows를 설치합니다.	"Windows에서 Protection 에이전트 설치"(72페이지) 또는 "Windows에서 무인 설치 또는 제거"(81페이지)
	Agent for Linux를 설치합니다.	"Linux에서 Protection 에이전트 설치"(74페이지) 또는 "Linux에서 무인 설치 또는 제거"(97페이지)
Scale Computing HC3	사용자 환경에 Agent for Scale Computing HC3(가상 어플라이언스)를 디플로이합니다.	"Agent for Scale Computing HC3(가상 어플라이언스) 배포 중"(129페이지)
네트워크 연결 스토리지		
Synology	사용자 환경에 Agent for Synology(가상 어플라이언스)를 디플로이합니다.	"Agent for Synology 디플로이"(147페이지)
애플리케이션		

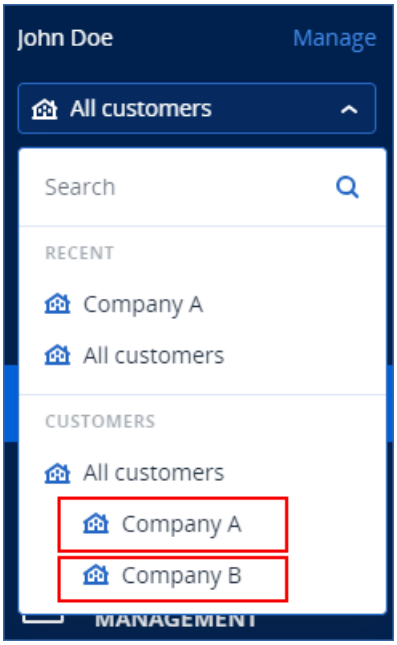
© Acronis International GmbH, 2003-2024

추가할 워크로드	수행해야 하는 작업	진행해야 하는 절차
Microsoft SQL Server	Agent for SQL을 설치합니다.	"Windows에서 Protection 에이전트 설치"(72페이지) 또는 "Windows에서 무인 설치 또는 제거"(81페이지)
Microsoft Exchange Server	Agent for Exchange를 설치합니다.	
Microsoft Active Directory	Agent for Active Directory를 설치합니다.	
Oracle 데이터베이스	Agent for Oracle을 설치합니다.	"Oracle 데이터베이스 보호"(606페이지)
웹 사이트	웹 사이트에 대한 연결을 구성합니다.	"웹사이트 및 호스팅 서버 보호"(612페이지)

사용 가능한 보호 에이전트와 해당 에이전트를 설치해야 하는 위치에 대한 자세한 내용은 "필요한 에이전트"(57페이지) 항목을 참조하십시오

파트너 관리자용 정보

- 관리 포털에서 필요한 서비스 할당량이 활성화되어 있지 않으면 **장치 추가** 창에서 워크로드 유형이 누락될 수 있습니다. 각 워크로드에 필요한 서비스 할당량에 대한 자세한 내용은 파트너 관리자 가이드에서 제공 항목 활성화 또는 비활성화를 참조하십시오.
- 파트너 관리자는 **모든 고객** 수준에서 워크로드를 추가할 수 없습니다. 워크로드를 추가하려면 개별 고객 테넌트를 선택합니다.



Cyber Protect 콘솔에서 워크로드 제거

더 이상 보호하지 않아도 되는 워크로드는 Cyber Protect 콘솔에서 제거할 수 있습니다. 제거 절차는 워크로드 유형에 따라 다릅니다.

© Acronis International GmbH, 2003-2024

보호 대상 워크로드에서 에이전트 설치를 제거할 수도 있습니다. 에이전트 설치를 제거하면 보호 대상 워크로드가 Cyber Protect 콘솔에서 자동으로 제거됩니다.

중요

Cyber Protect 콘솔에서 워크로드를 제거하면 해당 워크로드에 적용되어 있는 모든 계획이 해지됩니다. 워크로드를 제거해도 계획이나 백업이 삭제되지는 않으며 보호 에이전트 설치도 제거되지 않습니다.

다음 표에 워크로드 유형과 각 유형별로 수행해야 하는 작업이 요약되어 있습니다.

제거할 워크로드	수행해야 하는 작업	진행해야 하는 절차
실제 및 가상 머신		
보호 에이전트가 설치된 실제 머신 또는 가상 머신	1. Cyber Protect 콘솔에서 워크로드를 제거합니다. 2. [선택 사항] 보호 에이전트를 설치 제거합니다.	"Cyber Protect 콘솔에서 워크로드를 제거하는 방법"(309페이지) (보호 에이전트가 설치된 워크로드)
하이퍼바이저 수준에서 백업된 가상 머신(비에이전트 백업)	1. Cyber Protect 콘솔에서 보호 에이전트가 설치된 머신을 제거합니다. 이 에이전트가 백업하는 모든 가상 머신이 콘솔에서 자동으로 제거됩니다. 2. [선택 사항] 보호 에이전트를 설치 제거합니다.	"Cyber Protect 콘솔에서 워크로드를 제거하는 방법"(309페이지) (보호 에이전트가 설치되지 않은 워크로드)
클라우드 간 워크로드		
Microsoft 365 Business 워크로드 Google Workspace 워크로드	Cyber Protect 콘솔에서 Microsoft 365 또는 Google Workspace 조직을 삭제합니다. 해당 조직의 모든 리소스가 콘솔에서 자동으로 제거됩니다.	"Cyber Protect 콘솔에서 워크로드를 제거하는 방법"(309페이지) (클라우드 간 워크로드)
모바일 장치		

© Acronis International GmbH, 2003-2024

제거할 워크로드	수행해야 하는 작업	진행해야 하는 절차
Android 장치 iOS 장치	1. Cyber Protect 콘솔에서 모바일 장치를 제거합니다. 2. [선택 사항] 모바일 장치에서 앱을 설치 제거합니다.	"Cyber Protect 콘솔에서 워크로드를 제거하는 방법"(309페이지) (모바일 장치)
네트워크 연결 스토리지		
Synology	1. Cyber Protect 콘솔에서 워크로드를 제거합니다. 2. [선택 사항] 보호 에이전트를 설치 제거합니다.	"Cyber Protect 콘솔에서 워크로드를 제거하는 방법"(309페이지) (보호 에이전트가 설치된 워크로드)
애플리케이션		
Microsoft SQL Server Microsoft Exchange Server Microsoft Active Directory Oracle 데이터베이스	1. Cyber Protect 콘솔에서 보호 에이전트가 설치된 머신을 제거합니다. 이 에이전트가 백업하는 객체가 콘솔에서 자동으로 제거됩니다. 2. [선택 사항] 보호 에이전트를 설치 제거합니다.	"Cyber Protect 콘솔에서 워크로드를 제거하는 방법"(309페이지) (보호 에이전트가 설치되지 않은 워크로드)
웹사이트	Cyber Protect 콘솔에서 웹 사이트를 제거합니다.	"Cyber Protect 콘솔에서 워크로드를 제거하는 방법"(309페이지) (웹 사이트)

Cyber Protect 콘솔에서 워크로드를 제거하는 방법

보호 에이전트가 설치된 워크로드

이 유형의 워크로드는 직접 제거할 수 있습니다.

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 제거할 하나 이상의 워크로드 옆에 있는 확인란을 선택합니다.
3. **작업** 창에서 **삭제**를 클릭합니다.

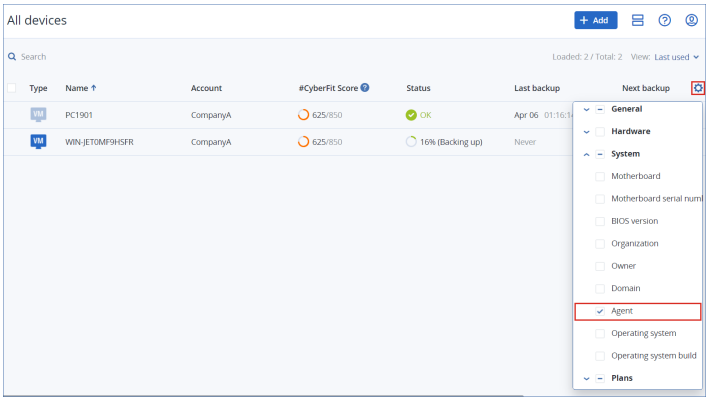
© Acronis International GmbH, 2003-2024

4. **삭제**를 클릭하여 선택을 확인합니다.
5. [선택 사항] "에이전트 제거"(167페이지)의 설명에 따라 에이전트를 설치 제거합니다.

보호 에이전트가 설치되지 않은 워크로드

이 유형의 워크로드를 제거하려면 보호 에이전트가 설치된 머신을 제거해야 합니다.

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 오른쪽 상단 모서리의 기어 아이콘을 클릭하고 **에이전트** 확인란을 선택합니다.



에이전트 열이 표시됩니다.

3. **에이전트** 열에서 보호 에이전트가 설치된 머신의 이름을 확인합니다.
4. Cyber Protect 콘솔에서 보호 에이전트가 설치된 머신 옆의 확인란을 선택합니다.
5. **작업** 창에서 **삭제**를 클릭합니다.
6. **삭제**를 클릭하여 선택을 확인합니다.
7. [선택 사항] "에이전트 제거"(167페이지)의 설명에 따라 에이전트를 설치 제거합니다.

클라우드 간 워크로드

클라우드 에이전트가 백업하는 워크로드를 제거하려면 Cyber Protect 콘솔에서 Microsoft 365 또는 Google Workspace 조직을 삭제합니다.

1. Cyber Protect 콘솔에서 **장치** > **Microsoft 365** 또는 **장치** > **Google Workspace**로 이동합니다.
2. Microsoft 365 또는 Google Workspace 조직의 이름을 클릭합니다.
3. **작업** 창에서 **그룹 삭제**를 클릭합니다.
4. **삭제**를 클릭하여 작업을 확인합니다.

모바일 장치

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 삭제할 워크로드 옆에 있는 확인란을 선택합니다.
3. **작업** 창에서 **삭제**를 클릭합니다.
4. **삭제**를 클릭하여 선택을 확인합니다.
5. [선택 사항] 모바일 장치에서 앱을 설치 제거합니다.

웹 사이트

© Acronis International GmbH, 2003-2024

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 삭제할 워크로드 옆에 있는 확인란을 선택합니다.
3. **작업** 창에서 **삭제**를 클릭합니다.
4. **삭제**를 클릭하여 선택을 확인합니다.

장치 그룹

장치 그룹에서는 그룹 계획을 사용하여 유사한 여러 워크로드를 보호할 수 있습니다. 계획은 그룹 전체에 적용되며 그룹 멤버 단위로 해지할 수는 없습니다.

워크로드 하나가 여러 그룹의 멤버가 될 수 있습니다. 장치 그룹에 포함된 워크로드도 개별 계획을 통해 보호할 수 있습니다.

장치 그룹에는 같은 유형의 워크로드만 추가할 수 있습니다. 예를 들어 **Hyper-V**에는 Hyper-V 가상 머신 그룹만 생성할 수 있습니다. **에이전트가 있는 머신**에는 에이전트가 설치되어 있는 머신 그룹만 생성할 수 있습니다.

루트 그룹인 **모든 장치**, 그리고 **에이전트가 있는 머신** > **모두**, **Microsoft 365** > 사용자 조직 > **사용자** > **모든 사용자**와 같은 기본 제공 그룹 등 **모두** 유형 그룹 내에는 장치 그룹을 생성할 수 없습니다.

기본 제공 그룹 및 사용자 지정 그룹

기본 제공 그룹

Cyber Protect 콘솔에서 등록한 워크로드는 **에이전트가 있는 머신**, **Microsoft 365**, **Hyper-V** 등 **장치** 탭의 기본 제공 루트 그룹 중 하나에 나타납니다.

등록된 워크로드 중 클라우드 간 워크로드가 아닌 모든 워크로드는 **모든 장치** 루트 그룹에도 나열됩니다. 기존 테넌트의 이름을 따서 명명된 별도의 기본 제공 루트 그룹에는 해당 테넌트의 클라우드 간 워크로드가 아닌 모든 워크로드와 모든 부서가 포함됩니다.

루트 그룹은 삭제하거나 편집할 수 없으며 루트 그룹에 계획을 적용할 수도 없습니다.

일부 루트 그룹에는 기본 제공 하위 그룹 수준이 하나 이상 포함됩니다. **에이전트가 있는 머신** > **모두**, **Microsoft 365** > 사용자 조직 > **팀** > **모든 팀**, **Google Workspace** > 사용자 조직 > **공유 드라이브** > **모든 공유 드라이브** 등을 예로 들 수 있습니다.

기본 제공 하위 그룹은 편집하거나 삭제할 수 없습니다.

사용자 정의 그룹

기본 제공 그룹의 모든 워크로드를 보호하는 방식은 불편할 수도 있습니다. 다른 보호 설정이나 보호 스케줄을 사용해야 하는 워크로드가 있을 수도 있기 때문입니다.

에이전트가 있는 머신, **Microsoft 365**, **Google Workspace**와 같은 일부 루트 그룹에서는 사용자 지정 하위 그룹을 생성할 수 있습니다. 이러한 하위 그룹은 정적 그룹일 수도 있고 동적 그룹일 수도 있습니다.

© Acronis International GmbH, 2003-2024

사용자 지정 그룹은 편집 또는 삭제하거나 이름을 변경할 수 있습니다.

정적 그룹과 동적 그룹

다음과 같은 유형의 사용자 지정 그룹을 생성할 수 있습니다.

- 정적
- 동적

정적 그룹

정적 그룹에는 수동으로 추가한 워크로드가 포함됩니다.

정적 그룹의 내용은 워크로드를 명시적으로 추가하거나 제거할 때만 변경됩니다.

예: 회사의 회계 부서용 정적 그룹을 생성한 다음 이 그룹에 회계원의 머신을 수동으로 추가합니다. 그룹 계획을 적용하면 해당 그룹의 머신이 보호됩니다. 새 회계원을 고용하는 경우 해당 회계원의 머신을 정적 그룹에 수동으로 추가해야 합니다.

동적 그룹

동적 그룹에는 특정 기준과 일치하는 워크로드가 포함됩니다. 속성(예: `osType`), 속성의 값(예: `Windows`) 및 검색 연산자(예: `IN`)가 포함된 검색 쿼리를 생성하여 이러한 기준을 미리 정의합니다.

이러한 기준을 정의하면 운영 체제가 Windows인 모든 머신용 동적 그룹 또는 이메일 주소가 `john`으로 시작하는 Microsoft 365 조직 내의 모든 사용자를 포함하는 동적 그룹을 생성할 수 있습니다.

그러면 필수 속성과 값이 포함되어 있는 모든 워크로드가 해당 그룹에 추가되며, 필수 특성이나 값이 없는 워크로드는 해당 그룹에서 자동으로 제거됩니다.

예 1: 회계 부서에 속한 머신의 호스트 이름에는 단어 accounting이 포함됩니다. 이름에 accounting이 포함된 머신을 검색한 후 검색 결과를 동적 그룹으로 저장합니다. 그런 다음 해당 그룹에 보호 계획을 적용합니다. 새 회계원을 고용하는 경우 해당 회계원의 머신 이름에는 accounting이 포함되므로 Cyber Protect 콘솔에 해당 머신을 등록하는 즉시 동적 그룹에 머신이 추가됩니다.

예 2: 회계 부서는 별도의 Active Directory 조직 단위(OU)를 만듭니다. 회계 OU를 필수 속성으로 지정한 다음 검색 결과를 동적 그룹으로 저장합니다. 그런 다음 해당 그룹에 보호 계획을 적용합니다. 새 회계원을 고용하는 경우 해당 회계원의 머신은 Active Directory OU에 추가하고 Cyber Protect 콘솔에 등록하는 즉시 동적 그룹에 추가됩니다(OU에 추가와 콘솔에 등록 중 어떤 작업을 먼저 수행하는지는 관계없음).

클라우드 간 그룹과 클라우드 간 그룹이 아닌 그룹

클라우드 간 그룹에는 클라우드 에이전트를 통해 백업되는 Microsoft 365 또는 Google Workspace 워크로드가 포함됩니다.

클라우드 간 그룹이 아닌 그룹에는 기타 모든 워크로드 유형이 포함됩니다.

장치 그룹에 지원되는 계획

다음 표에는 장치 그룹에 적용할 수 있는 계획이 요약되어 있습니다.

© Acronis International GmbH, 2003-2024

그룹	사용 가능한 계획	계획 위치
클라우드 간 워크로드 (Microsoft 365 및 Google Workspace 워크로드)	백업 계획	**관리** > **클라우드 애플리케이션 백업**
클라우드 간 워크로드가 아닌 워크로드	보호 계획	**관리** > **보호 계획**
	원격 관리 계획	**관리** > **원격 관리 계획**
	스크립팅 계획	**관리** > **스크립팅 계획**

Microsoft 365 또는 Google Workspace 사용자, OneDrive 및 Google Drive 공유, Microsoft Teams, Azure AD 그룹 등의 클라우드 리소스는 Cyber Protect 콘솔에 Microsoft 365 또는 Google Workspace 조직을 추가한 직후 콘솔에 동기화됩니다. 그 이후에 조직에서 변경하는 내용은 하루에 한 번 동기화됩니다.

변경 내용을 즉시 동기화해야 하는 경우 Cyber Protect 콘솔에서 **장치** > **Microsoft 365** 또는 **장치** > **Google Workspace**로 각각 이동하여 필요한 조직을 선택하고 **새로 고침**을 클릭합니다.

정적 그룹 생성

빈 정적 그룹을 생성한 후 해당 그룹에 워크로드를 추가할 수 있습니다.

워크로드를 선택하고 선택 항목으로 새 정적 그룹을 생성할 수도 있습니다.

루트 그룹인 **모든 장치**, 그리고 **에이전트가 있는 머신** > **모두**, **Microsoft 365** > 사용자 조직 > **사용자** > **모든 사용자**와 같은 기본 제공 그룹 등 **모두** 유형 그룹 내에는 장치 그룹을 생성할 수 없습니다.

정적 그룹을 생성하려면

주 창에서

1. **장치**를 클릭하고 정적 그룹을 생성할 워크로드가 포함된 루트 그룹을 선택합니다.
2. [선택 사항] 중첩된 그룹을 생성하려면 기존 정적 그룹으로 이동합니다.

   참고
   클라우드 간 워크로드에서는 중첩된 정적 그룹을 생성할 수 없습니다.

3. 그룹 트리 아래에서 **+ 새 정적 그룹**을 클릭하거나 **작업** 창에서 **새 정적 그룹**을 클릭합니다.
4. 새 그룹의 이름을 지정합니다.
5. [선택 사항] 그룹의 주석을 추가합니다.
6. **확인**을 클릭합니다.

그룹 트리에서

1. **장치**를 클릭하고 정적 그룹을 생성할 워크로드가 포함된 루트 그룹을 선택합니다.
2. 새 정적 그룹을 생성하려는 그룹 이름 옆의 기어 아이콘을 클릭합니다.

© Acronis International GmbH, 2003-2024

참고
클라우드 간 워크로드에서는 중첩된 정적 그룹을 생성할 수 없습니다.

3. **새 정적 그룹**을 클릭합니다.
4. 새 그룹의 이름을 지정합니다.
5. [선택 사항] 그룹의 주석을 추가합니다.
6. **확인**을 클릭합니다.

선택 항목에서

1. **장치**를 클릭하고 정적 그룹을 생성할 워크로드가 포함된 루트 그룹을 선택합니다.

참고
루트 그룹인 **모든 장치**, 그리고 **에이전트가 있는 머신** > **모두**, **Microsoft 365** > 사용자 조직 > **사용자** > **모든 사용자**와 같은 기본 제공 그룹 등 **모두** 유형 그룹 내에는 장치 그룹을 생성할 수 없습니다.

2. 새 그룹을 생성할 워크로드 옆의 확인란을 선택하고 **그룹에 추가**를 클릭합니다.
3. 폴더 트리에서 새 그룹의 상위 수준을 선택하고 **새 정적 그룹**을 클릭합니다.

참고
클라우드 간 워크로드에서는 중첩된 정적 그룹을 생성할 수 없습니다.

4. 새 그룹의 이름을 지정합니다.
5. [선택 사항] 그룹의 주석을 추가합니다.
6. **확인**을 클릭합니다.
   새 그룹이 폴더 트리에 나타납니다.
7. **완료**를 클릭합니다.

정적 그룹에 워크로드 추가

먼저 대상 그룹을 선택한 후 해당 그룹에 워크로드를 추가할 수 있습니다.

워크로드를 먼저 선택한 후 그룹에 추가할 수도 있습니다.

정적 그룹에 워크로드를 추가하려면

먼저 대상 그룹 선택

1. **장치**를 클릭하고 대상 그룹으로 이동합니다.
2. 대상 그룹을 선택하고 **장치 추가**를 클릭합니다.
3. 폴더 트리에서 필요한 워크로드가 포함된 그룹을 선택합니다.
4. 추가할 워크로드 옆의 확인란을 선택하고 **추가**를 클릭합니다.

먼저 워크로드 선택

© Acronis International GmbH, 2003-2024

1. **장치**를 클릭하고 필요한 워크로드가 포함된 루트 그룹을 선택합니다.
2. 추가할 워크로드 옆의 확인란을 선택하고 **그룹에 추가**를 클릭합니다.
3. 폴더 트리에서 대상 그룹을 선택하고 **완료**를 클릭합니다.

동적 그룹 생성

동적 그룹을 생성할 때는 검색 쿼리에서 값을 정의하는 특정 속성이 포함된 워크로드를 검색합니다. 그런 다음 검색 결과를 동적 그룹으로 저장합니다.

검색 및 동적 그룹 생성을 지원하는 속성은 클라우드 간 워크로드와 클라우드 간 워크로드가 아닌 워크로드에 따라 다릅니다. 지원되는 속성에 대한 자세한 정보는 "클라우드 간 워크로드가 아닌 워크로드의 속성 검색"(318페이지) 및 "클라우드 간 워크로드의 속성 검색"(317페이지)을(를) 참조하십시오.

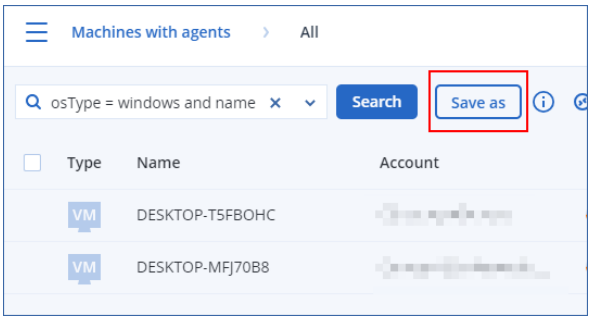
동적 그룹은 해당 루트 그룹에서 생성됩니다. 중첩된 동적 그룹은 지원되지 않습니다.

루트 그룹인 **모든 장치**, 그리고 **에이전트가 있는 머신** > **모두**, **Microsoft 365** > 사용자 조직 > **사용자** > **모든 사용자**와 같은 기본 제공 그룹 등 **모두** 유형 그룹 내에는 장치 그룹을 생성할 수 없습니다.

동적 그룹을 생성하려면

클라우드 간 워크로드가 아닌 워크로드

1. **장치**를 클릭하고 새 동적 그룹을 생성할 워크로드가 포함된 그룹을 선택합니다.
2. 지원되는 검색 속성과 연산자를 사용하여 워크로드를 검색합니다.
   단일 쿼리에서 여러 속성과 연산자를 사용할 수 있습니다. 지원되는 속성에 대한 자세한 정보는 "클라우드 간 워크로드가 아닌 워크로드의 속성 검색"(318페이지)을(를) 참조하십시오.
3. 검색 필드 옆의 **다른 이름으로 저장**을 클릭합니다.



참고
다른 이름으로 저장 버튼은 특정 레벨에서 동적 그룹을 생성할 수 없는 경우 사용할 수 없습니다. 예를 들어 루트 그룹의 **장치** > **모든 장치**에서는 사용할 수 없습니다.
다른 레벨을 선택(예: **장치** > **에이전트가 있는 머신** > **모두**)한 다음 위의 단계를 반복합니다. 이 검색을 통해 **에이전트가 있는 머신** 내에 동적 그룹을 생성할 수 있으며, **에이전트가 있는 머신** > **모두** 내에는 생성할 수 없습니다.

4. 새 그룹의 이름을 지정합니다.

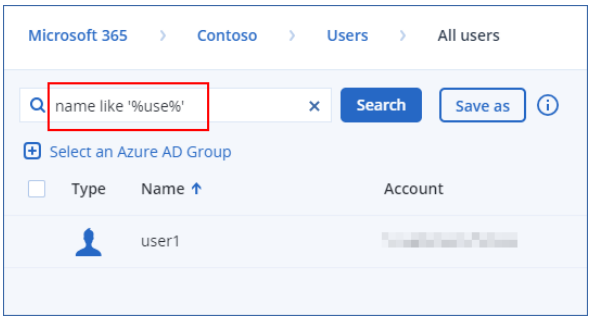
© Acronis International GmbH, 2003-2024

5. [선택 사항] **주석** 필드에 새 그룹의 설명을 추가합니다.
6. **확인**을 클릭합니다.

클라우드 간 워크로드

1. **장치**를 클릭하고 **Microsoft 365** 또는 **Google Workspace**를 선택합니다.
2. 새로운 동적 그룹을 생성하려는 워크로드가 포함된 그룹을 선택합니다(예: **사용자** > **모든 사용자**).
3. 지원되는 검색 속성과 연산자를 사용하거나 특정 Active Directory 그룹에서 Microsoft 365 사용자를 선택하여 워크로드를 검색합니다.

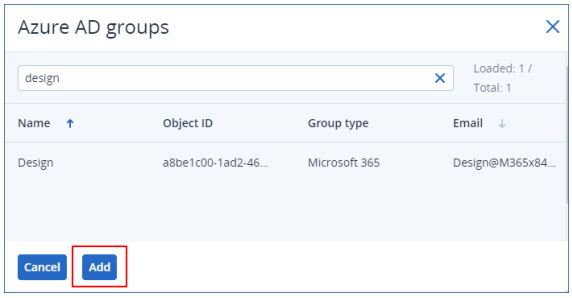
   단일 쿼리에서 여러 속성과 연산자를 사용할 수 있습니다. 지원되는 속성에 대한 자세한 정보는 "클라우드 간 워크로드의 속성 검색"(317페이지)을(를) 참조하십시오.



4. [**Microsoft 365** > **사용자**에만 해당] 특정 Active Directory 그룹에서 사용자를 선택하려면 다음을 수행합니다.
   a. **사용자** > **모든 사용자**로 이동합니다.
   b. **Azure AD 그룹 선택**을 클릭합니다.

      조직의 Active Directory 그룹 목록이 열립니다.

      이 목록에서 특정 그룹을 검색하거나 이름 또는 이메일을 기준으로 그룹을 정렬할 수 있습니다.
   c. 원하는 Active Directory 그룹을 선택하고 **추가**를 클릭합니다.

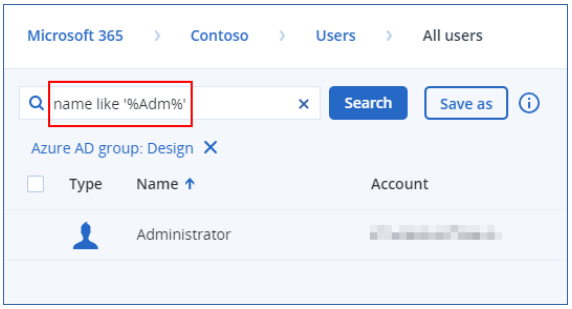


   d. [선택 사항] 선택한 Active Directory 그룹에서 특정 사용자를 포함하거나 제외하려면 지원되는 검색 속성과 연산자를 사용하여 검색 쿼리를 생성합니다.

      단일 쿼리에서 여러 속성과 연산자를 사용할 수 있습니다. 지원되는 속성에 대한 자세한 정

© Acronis International GmbH, 2003-2024

보는 "클라우드 간 워크로드의 속성 검색"(317페이지)을(를) 참조하십시오.



5. 검색 필드 옆의 **다른 이름으로 저장**을 클릭합니다.

참고
다른 이름으로 저장 버튼은 특정 레벨에서 동적 그룹을 생성할 수 없는 경우 사용할 수 없습니다. 예를 들어 **Microsoft 365** > 나의 조직 > **사용자**에서는 사용할 수 없습니다.
다른 레벨을 선택(예: **Microsoft 365** > 나의 조직 > **사용자** > **모두**)한 다음 위의 단계를 반복합니다. 이 검색을 통해 **Microsoft 365** > 나의 조직 > **사용자** > 내에 동적 그룹을 생성할 수 있으며, **사용자** > **모두** 내에서는 생성할 수 없습니다.

6. 새 그룹의 이름을 지정합니다.
7. [선택 사항] **주석** 필드에 새 그룹의 설명을 추가합니다.
8. **확인**을 클릭합니다.

클라우드 간 워크로드의 속성 검색

다음 표에는 Microsoft 365 및 Google Workspace 워크로드용 검색 쿼리에서 사용 가능한 속성이 요약되어 있습니다.

다른 워크로드 유형용 검색 쿼리에 사용할 수 있는 속성을 확인하려면 "클라우드 간 워크로드가 아닌 워크로드의 속성 검색"(318페이지) 항목을 참조하십시오.

속성	의미	사용 가능 항목	검색 쿼리 예제	그룹 생성 지원
`name`	Microsoft 365 또는 Google Workspace 워크로드의 표시 이름	모든 클라우드 간 리소스	`name = 'My Name'` `name LIKE '*nam*'`	예

`email`	Microsoft 365 사용자 또는 그룹이나 Google Workspace 사용자의 이메일 주소	Microsoft 365 > 그룹
		Microsoft 365 > 사용자
		Google Workspace > 사용자
			`email = 'my_group_email@mycompany.com'`
			`email LIKE '*@company*'`
			`email NOT LIKE '*enterprise.com'`
				예

`siteName`	Microsoft 365 그룹과 연결된 사이	Microsoft 365	`siteName = 'my_site'`	예

© Acronis International GmbH, 2003-2024

속성	의미	사용 가능 항목	검색 쿼리 예제	그룹 생성 지원
	트의 이름	> 그룹	`siteName LIKE '*company.com*support*'`	
`url`	Microsoft 365 그룹이나 SharePoint 사이트의 웹 주소	Microsoft 365 > 그룹 Microsoft 365 > 사이트 컬렉션	`url = 'https://www.mycompany.com/'` `url LIKE '*www.mycompany.com*'`	예

클라우드 간 워크로드가 아닌 워크로드의 속성 검색

다음 표에는 클라우드 간 워크로드가 아닌 워크로드용 검색 쿼리에서 사용 가능한 속성이 요약되어 있습니다.

클라우드 간 워크로드용 검색 쿼리에 사용할 수 있는 속성을 확인하려면 "클라우드 간 워크로드의 속성 검색"(317페이지) 항목을 참조하십시오.

속성	의미	검색 쿼리 예제	그룹 생성 지원
일반			
`name`	다음과 같은 워크로드 이름: • 실제 머신의 호스트 이름 • 가상 머신의 이름 • 데이터베이스 이름 • 사서함의 이메일 주소	`name = 'en-00'`	예
`id`	장치 ID. 장치 ID를 확인하려면 **장치**에서 장치를 선택하고 **상세 정보** > **모든 속성**을 클릭합니다. ID가 `id` 필드에 표시됩니다.	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	예
`resourceType`	워크로드 유형. 가능한 값: • `'machine'` • `'exchange'` • `'mssql_server'` • `'mssql_instance'`	`resourceType = 'machine'` `resourceType in ('mssql_aag_database', 'mssql_database')`	예

© Acronis International GmbH, 2003-2024

속성	의미	검색 쿼리 예제	그룹 생성 지원
	• 'mssql_database' • 'mssql_database_folder' • 'msexchange_database' • 'msexchange_storage_group' • 'msexchange_mailbox.msexchange' • 'msexchange_mailbox.office365' • 'mssql_aag_group' • 'mssql_aag_database' • 'virtual_machine.vmww' • 'virtual_machine.vmwesx' • 'virtual_host.vmwesx' • 'virtual_cluster.vmwesx' • 'virtual_appliance.vmwesx' • 'virtual_application.vmwesx' • 'virtual_resource_pool.vmwesx' • 'virtual_center.vmwesx' • 'datastore.vmwesx' • 'datastore_cluster.vmwesx' • 'virtual_network.vmwesx' • 'virtual_data_center.vmwesx' • 'virtual_machine.vmww' • 'virtual_cluster.mshyperv' • 'virtual_machine.mshyperv' • 'virtual_host.mshyperv' • 'virtual_network.mshyperv' • 'virtual_folder.mshyperv' • 'virtual_data_center.mshyperv' • 'datastore.mshyperv' • 'virtual_machine.msvs' • 'virtual_machine.parallelsw' • 'virtual_host.parallelsw' • 'virtual_cluster.parallelsw' • 'virtual_machine.rhev' • 'virtual_machine.kvm' • 'virtual_machine.xen'		

© Acronis International GmbH, 2003-2024

속성	의미	검색 쿼리 예제	그룹 생성 지원
	• 'bootable_media'		
chassis	섀시 유형. 가능한 값: • laptop • desktop • server • other • unknown	chassis = 'laptop' chassis IN ('laptop', 'desktop')	예
ip	IP 주소(물리적인 머신만 해당).	ip RANGE ('10.250.176.1','10.250.176.50')	예
comment	장치에 대한 주석. 자동이나 수동으로 지정할 수 있습니다. 기본값: • Windows를 실행하는 실제 머신의 경우 Windows의 컴퓨터 설명이 주석으로 자동 복사됩니다. 이 값은 15분마다 동기화됩니다. • 다른 장치의 경우 비어 있습니다. **참고** 주석 필드에 수동으로 추가한 텍스트가 있으면 자동 동기화는 비활성화됩니다. 동기화를 다시 활성화하려면 이 텍스트를 지웁니다. 워크로드의 자동 동기화된 주석을 새로 고치려면 **Windows 서비스**에서 Managed Machine Service를 다시 시작하거나 명령 프롬프트에서 다음 명령을 실행합니다. `net stop mms`	comment = 'important machine' comment = ''(주석 없는 모든 머신)	예

© Acronis International GmbH, 2003-2024

속성	의미	검색 쿼리 예제	그룹 생성 지원
	`net start mms` 장치 주석을 보려면 **장치**에서 해당 장치를 선택하고 **상세정보**를 클릭한 다음 **주석** 섹션을 찾습니다. 주석을 수동으로 추가하거나 변경하려면 **추가** 또는 **편집**을 클릭합니다. 보호 에이전트가 설치된 장치에는 주석 필드 2개가 있습니다. • 에이전트 주석 ◦ Windows를 실행하는 실제 머신의 경우 Windows의 컴퓨터 설명이 주석으로 자동 복사됩니다. 이 값은 15분마다 동기화됩니다. ◦ 다른 장치의 경우 비어 있습니다. **참고** 주석 필드에 수동으로 추가한 텍스트가 있으면 자동 동기화는 비활성화됩니다. 동기화를 다시 활성화하려면 이 텍스트를 지웁니다. • 장치 주석 ◦ 자동으로 지정된 에이전트 주석은 장치 주석으로 복사됩니다. 수동으로 추가한 에이전트 주석은 장치 주석으로 복사되지 않습니다. ◦ 장치 주석은 에이전트 주석으로 복사되지 않습니다. 각 장치에서는 두 주석 중 하나 이상을 지정할 수도 있고 두 주석을 모두 비워 둘 수도 있습니다. 두 주석을 모두 지정하면 장		

© Acronis International GmbH, 2003-2024

속성	의미	검색 쿼리 예제	그룹 생성 지원
	치 주석이 우선적으로 사용됩니다. 에이전트 주석을 보려면 **장치** > **에이전트**에서 에이전트가 설치된 장치를 선택하고 **세부 사항**을 클릭한 다음 **주석** 섹션을 찾습니다. 장치 주석을 보려면 **장치**에서 해당 장치를 선택하고 **상세정보**를 클릭한 다음 **주석** 섹션을 찾습니다. 주석을 수동으로 추가하거나 변경하려면 **추가** 또는 **편집**을 클릭합니다.		
`isOnline`	워크로드 가용성. 가능한 값: • `true` • `false`	`isOnline = true`	아니요
`hasAsz`	Secure Zone 가용성. 가능한 값: • `true` • `false`	`hasAsz = true`	예

`tzOffset`	UTC(협정 세계시)와의 시간대 오프셋(분).	`tzOffset = 120`
		
		`tzOffset > 120`
		
		`tzOffset < 120`
			예

CPU, 메모리, 디스크			
`cpuArch`	CPU 아키텍처. 가능한 값: • `'x64'` • `'x86'`	`cpuArch = 'x64'`	예
`cpuName`	CPU 이름.	`cpuName LIKE '%XEON%'`	예
`memorySize`	RAM 크기(메가바이트 단위).	`memorySize < 1024`	예

© Acronis International GmbH, 2003-2024

속성	의미	검색 쿼리 예제	그룹 생성 지원
diskSize	하드 드라이브 크기(기가바이트 또는 메가바이트 단위, 물리적인 머신만 해당).	diskSize < 300GB diskSize >= 3000000MB	아니요
운영 체제			
osName	운영 체제 이름.	osName LIKE '%Windows XP%'	예
osType	운영 체제 유형. 가능한 값: • 'windows' • 'linux' • 'macosx'	osType = 'windows' osType IN ('linux', 'macosx')	예
osArch	운영 체제 아키텍처. 가능한 값: • 'x64' • 'x86'	cpuArch = 'x86'	예
osProductType	운영 체제 제품 유형. 가능한 값: • 'dc' 도메인 컨트롤러를 나타냅니다. **참고** 도메인 컨트롤러 역할이 Windows 서버에 할당되어 있을 때는 osProductType이 server에서 dc로 바뀝니다. 이러한 머신은 osProductType='server'의 검색 결과에 포함되지 않습니다. • 'server' • 'workstation'	osProductType = 'server'	예
osSp	운영 체제의 서비스 팩.	osSp = 1	예
osVersionMajor	운영 체제의 주 버전.	osVersionMajor = 1	예

© Acronis International GmbH, 2003-2024

속성	의미	검색 쿼리 예제	그룹 생성 지원
osVersionMinor	운영 체제의 부 버전.	osVersionMinor > 1	예
에이전트			
agentVersion	설치된 보호 에이전트의 버전입니다.	agentVersion LIKE '12.0.*'	예
hostId	보호 에이전트의 내부 ID입니다. 보호 에이전트 ID를 확인하려면 **장치**에서 장치를 선택하고 **상세 정보** > **모든 속성**을 클릭합니다. agent 속성의 id 값을 확인합니다.	hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	예
virtualType	가상 머신 유형. 가능한 값: • 'vmwesx' VMware 가상 머신. • 'mshyperv' Hyper-V 가상 머신. • 'pcs' Virtuozzo 가상 머신. • 'hci' Virtuozzo Hybrid Infrastructure 가상 머신. • 'scale' Scale Computing HC3 가상 머신. • 'ovirt' oVirt 가상 머신	virtualType = 'vmwesx'	예
insideVm	에이전트가 포함된 가상 머신. 가능한 값: • true • false	insideVm = true	예
위치			
tenant	장치가 속한 테넌트의 이름.	tenant = 'Unit 1'	예
tenantId	장치가 속한 테넌트의 식별자. 테넌트 ID를 확인하려면 **장치**에	tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'	예

© Acronis International GmbH, 2003-2024

속성	의미	검색 쿼리 예제	그룹 생성 지원
	서 장치를 선택하고 **상세 정보** > **모든 속성**을 클릭합니다. ID가 `ownerId` 필드에 표시됩니다.		
`ou`	지정된 Active Directory 조직 단위에 속한 장치.	`ou IN ('RnD', 'Computers')`	예
상태			
`state`	장치 상태. 가능한 값: • `'idle'` • `'interactionRequired'` • `'canceling'` • `'backup'` • `'recover'` • `'install'` • `'reboot'` • `'failback'` • `'testReplica'` • `'run_from_image'` • `'finalize'` • `'failover'` • `'replicate'` • `'createAsz'` • `'deleteAsz'` • `'resizeAsz'`	`state = 'backup'`	아니요
status	보호 상태. 가능한 값: • `ok` • `warning` • `error` • `critical` • `protected` • `notProtected`	`status = 'ok'` `status IN ('error', 'warning')`	아니요
`protectedByPlan`	제공된 ID를 가진 보호 계획으로 보호되는 장치입니다. 계획 ID를 보려면 **관리** > **보호 계**	`protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	아니요

© Acronis International GmbH, 2003-2024

속성	의미	검색 쿼리 예제	그룹 생성 지원
	획에서 계획을 선택하고 **상태** 열에 있는 바를 클릭한 뒤 상태 이름을 클릭합니다. 계획 ID를 가진 새 검색이 생성됩니다.		
okByPlan	제공된 ID를 가진 보호 계획으로 보호되며 **정상** 상태인 장치입니다.	okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	아니요
errorByPlan	제공된 ID를 가진 보호 계획으로 보호되며 **오류** 상태인 장치입니다.	errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	아니요
warningByPlan	제공된 ID를 가진 보호 계획으로 보호되며 **경고** 상태인 장치입니다.	warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	아니요
runningByPlan	제공된 ID를 가진 보호 계획으로 보호되며 **실행 중** 상태인 장치입니다.	runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	아니요
interactionByPlan	제공된 ID를 가진 보호 계획으로 보호되며 **상호 작용 필요** 상태인 장치입니다.	interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	아니요
lastBackupTime*	마지막으로 성공한 백업의 날짜 및 시간. 형식은 'YYYY-MM-DD HH:MM'입니다.	lastBackupTime > '2023-03-11' lastBackupTime <= '2023-03-11 00:15' lastBackupTime is null	아니요
lastBackupTryTime*	마지막 백업 시도 시간. 형식은 'YYYY-MM-DD HH:MM'입니다.	lastBackupTryTime >= '2023-03-11'	아니요
nextBackupTime*	다음 백업 시간. 형식은 'YYYY-MM-DD HH:MM'입니다.	nextBackupTime >= '2023-08-11'	아니요
lastVAScanTime*	마지막으로 성공한 취약점 평가의 날짜 및 시간. 형식은 'YYYY-MM-DD HH:MM'입니다.	lastVAScanTime > '2023-03-11' lastVAScanTime <= '2023-03-11 00:15' lastVAScanTime is null	예
lastVAScanTryTime*	마지막 취약점 평가 시도 시간.	lastVAScanTimeTryTime >= '2022-03-	예

© Acronis International GmbH, 2003-2024

속성	의미	검색 쿼리 예제	그룹 생성 지원
	형식은 'YYYY-MM-DD HH:MM'입니다.	11'	
nextVAScanTime*	다음 취약점 평가 시간. 형식은 'YYYY-MM-DD HH:MM'입니다.	nextVAScanTime <= '2023-08-11'	예
network_status	EDR(Endpoint Detection and Response)의 네트워크 분리 상태. 가능한 값: • connected • isolated	network_status= 'connected'	예

참고

시간 및 분 값을 건너뛸 경우, 시작 시간은 YYYY-MM-DD 00:00, 종료 시간은 YYYY-MM-DD 23:59:59인 것으로 간주됩니다.예를 들어 lastBackupTime = 2023-01-20은 lastBackupTime >= 2023-01-20 00:00에서 lastBackup time <= 2023-01-20 23:59:59 사이에 생성된 모든 백업이 검색 결과에 포함된다는 의미입니다.

검색 연산자

다음 표에는 검색 쿼리에서 사용 가능한 연산자가 요약되어 있습니다.

쿼리 하나에서 여러 연산자를 사용할 수 있습니다.

연산자	지원 대상	의미	예
AND	모든 워크로드	논리적 결합 연산자	name like 'en-00' AND tenant = 'Unit 1'
OR	모든 워크로드	논리적 분리 연산자	state = 'backup' OR state = 'interactionRequired'
NOT	모든 워크로드	논리적 부정 연산자	NOT(osProductType = 'workstation')
IN (<value1>,...<valueN>)	모든 워크로드	이 연산자는 식이 값 목록의 값과 일치하는지 확인합니다.	osType IN ('windows', 'linux')

© Acronis International GmbH, 2003-2024

연산자	지원 대상	의미	예
NOT IN	모든 워크로드	IN 연산자와 반대의 연산자.	NOT osType IN ('windows', 'linux')
LIKE 'wildcard pattern'	모든 워크로드	이 연산자는 식이 와일드카드 패턴과 일치하는지 확인합니다. 다음 와일드카드 연산자를 사용할 수 있습니다. • * 또는 % 별표 및 퍼센트 기호는 0, 1 또는 여러 문자를 나타냅니다. • _ 밑줄은 단일 문자를 나타냅니다.	name LIKE 'en-00' name LIKE '*en-00' name LIKE '*en-00*' name LIKE 'en-00_'
NOT LIKE 'wildcard pattern'	모든 워크로드	LIKE 연산자와 반대의 연산자입니다. 다음 와일드카드 연산자를 사용할 수 있습니다. • * 또는 % 별표 및 퍼센트 기호는 0, 1 또는 여러 문자를 나타냅니다. • _ 밑줄은 단일 문자를 나타냅니다.	NOT name LIKE 'en-00' NOT name LIKE '*en-00' NOT name LIKE '*en-00*' NOT name LIKE 'en-00_'
RANGE (<starting_value>, <ending_value>)	모든 워크로드	이 연산자는 식이 값 범위 내에 있는지(포함)확인합니다. 영숫자 문자열을 사용하는 검색 쿼리는 ASCII 정렬 순서를 사용하지만 대/소문자를 구분하지 않습니다.	ip RANGE('10.250.176.1','10.250.176.50') name RANGE('a','d') 이 쿼리에서는 Alice, Bob, Claire 등 A, B, C로 시작하는 모든 이름을 필터링할 수 있습니다. 하지만 요구 사항을 충족하는 문자는 D 하나뿐이므로 Diana, Don 등 D 이외의 문자가 더 포함되어 있는 이름은 포함되지 않습니다. 다음 쿼리를 사용해도 같은 결과가 반환됩니다. name >= 'a' AND name <= 'd'
= 또는 ==	모든 워크로드	*같음* 연산자	osProductType = 'server'
!= 또는 <>	모든 워	*같지 않음* 연산자	id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'

© Acronis International GmbH, 2003-2024

연산자	지원 대상	의미	예
	크로드		
<	클라우드 간 워크로드가 아닌 워크로드	*보다 작음* 연산자	`memorySize < 1024`
>	클라우드 간 워크로드가 아닌 워크로드	*보다 큼* 연산자.	`diskSize > 300GB`
<=	클라우드 간 워크로드가 아닌 워크로드	*보다 작음 또는 같음* 연산자	`lastBackupTime <= '2022-03-11 00:15'`
>=	클라우드 간 워크로드가 아닌 워크로드	*보다 큼 또는 같음* 연산자	`nextBackupTime >= '2022-08-11'`

동적 그룹 편집

그룹 컨텐츠를 정의하는 검색 쿼리를 변경하면 동적 그룹을 편집할 수 있습니다.

Active Directory 기반 동적 그룹에서는 Active Directory 그룹을 변경할 수도 있습니다.

동적 그룹을 편집하려면

검색 쿼리 변경

1. **장치**를 클릭하고 편집할 동적 그룹으로 이동한 후 해당 그룹을 선택합니다.
2. 그룹 이름 옆에 있는 기어 아이콘을 클릭한 다음 **편집**을 클릭합니다. **작업** 창에서 **편집**을 클릭해도 됩니다.
3. 검색 속성이나 속성의 값 또는 검색 연산자를 수정하여 검색 쿼리를 변경한 후 **검색**을 클릭합니다.
4. 검색 필드 옆의 **저장**을 클릭합니다.

Active Directory 그룹 변경

© Acronis International GmbH, 2003-2024

참고
이 절차는 Active Directory 기반 동적 그룹에 적용됩니다. Active Directory 기반 동적 그룹은 **Microsoft 365** > **사용자**에서만 사용 가능합니다.

1. **장치**를 클릭하고 **장치** > **Microsoft 365** > 사용자 조직 > **사용자**로 이동합니다.
2. 편집할 동적 그룹을 선택합니다.
3. 그룹 이름 옆에 있는 기어 아이콘을 클릭한 다음 **편집**을 클릭합니다. **작업** 창에서 **편집**을 클릭해도 됩니다.
4. 다음 중 하나를 수행하여 그룹 컨텐츠를 변경합니다.
   - 이미 선택한 Active Directory의 이름을 클릭한 다음 열리는 목록에서 새 Active Directory 그룹을 선택하여 선택한 그룹을 변경합니다.
   - 검색 쿼리를 편집하고 **검색**을 클릭합니다.
     검색 쿼리는 현재 선택되어 있는 Active Directory 그룹에만 적용됩니다.
5. 검색 필드 옆의 **저장**을 클릭합니다.

현재 그룹을 덮어쓰지 않고 편집 내용을 저장할 수도 있습니다. 편집한 구성을 새 그룹으로 저장하려면 검색 필드 옆의 화살표 버튼을 클릭하고 **다른 이름으로 저장**을 클릭합니다.

그룹 삭제

장치 그룹을 삭제하면 해당 그룹에 적용되어 있는 모든 계획이 해지됩니다. 다른 계획이 그룹에 적용되어 있지 않으면 그룹의 워크로드는 보호되지 않습니다.

장치 그룹을 삭제하려면

1. **장치**를 클릭하고 삭제할 그룹으로 이동합니다.
2. 그룹 이름 옆에 있는 기어 아이콘을 클릭한 다음 **삭제**를 클릭합니다.
3. **삭제**를 클릭하여 선택을 확인합니다.

그룹에 계획 적용

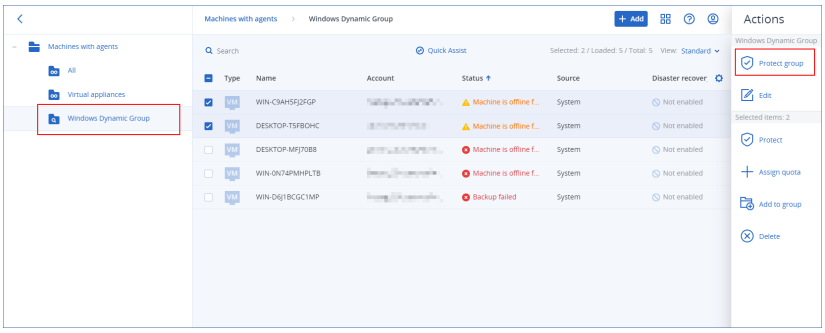
그룹을 먼저 선택한 다음 해당 그룹에 계획을 할당하는 방식으로 그룹에 계획을 적용할 수 있습니다.

편집을 위해 계획을 연 후 해당 계획에 그룹을 추가할 수도 있습니다.

그룹에 계획을 적용하려면

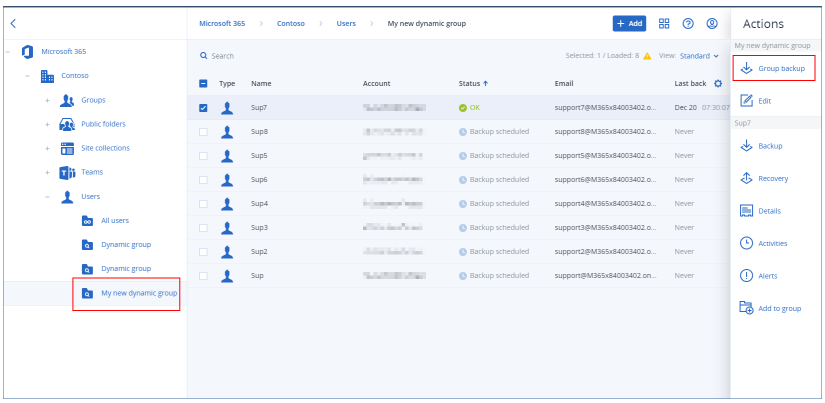
1. **장치**를 클릭하고 계획을 적용할 그룹으로 이동합니다.
2. [클라우드 간 워크로드가 아닌 워크로드의 경우] **그룹 보호**를 클릭합니다.

© Acronis International GmbH, 2003-2024



적용할 수 있는 계획 목록이 표시됩니다.

3. [클라우드 간 워크로드의 경우] **그룹 백업**을 클릭합니다.



적용할 수 있는 백업 계획 목록이 표시됩니다.

4. [기존 계획을 적용하려는 경우] 계획을 선택하고 **적용**을 클릭합니다.
5. [새 계획을 생성하려는 경우] **계획 생성**을 클릭하고 계획 유형을 선택한 후 새 계획을 생성합니다.

   사용 가능한 계획 유형과 계획 생성 방법에 대한 자세한 내용은 "장치 그룹에 지원되는 계획" (312페이지) 항목을 참조하십시오.

참고

클라우드 간 장치 그룹에 적용되는 백업 계획은 하루에 한 번 실행되도록 자동 예약됩니다. **지금 실행**을 클릭하여 이러한 계획을 필요에 따라 실행할 수는 없습니다.

그룹에서 계획 철회

그룹을 먼저 선택한 다음 해당 그룹에서 계획을 해지하는 방식으로 그룹에서 계획을 해지할 수 있습니다.

편집을 위해 계획을 연 후 해당 계획에서 그룹을 제거할 수도 있습니다.

그룹에서 계획을 해지하려면

1. **장치**를 클릭하고 계획을 해지할 그룹으로 이동합니다.
2. [클라우드 간 워크로드가 아닌 워크로드의 경우] **그룹 보호**를 클릭합니다.

   그룹에 적용된 계획 목록이 표시됩니다.
3. [클라우드 간 워크로드의 경우] **그룹 백업**을 클릭합니다.

© Acronis International GmbH, 2003-2024

그룹에 적용된 백업 계획 목록이 표시됩니다.

4. 해지할 계획을 선택합니다.
5. [클라우드 간 워크로드가 아닌 워크로드의 경우] 말줄임표 아이콘(...)을 클릭한 후에 **해지**를 클릭합니다.
6. [클라우드 간 워크로드의 경우] 기어 아이콘을 클릭한 후에 **해지**를 클릭합니다.

장치 제어 모듈 사용

장치 제어 모듈[1]은 Cyber Protection 서비스 보호 계획의 일환으로 보호되는 각 컴퓨터의 데이터 손실 방지 에이전트[2] 기능 중 일부를 활용하여 무단 액세스 및 로컬 컴퓨터 채널을 통한 데이터 전송을 감지 및 방지합니다. 이 모듈에서는 광범위한 데이터 유출 경로를 세부적으로 제어하는 기능이 제공됩니다. 예를 들어 이동식 미디어, 프린터, 가상 및 리디렉션 장치, 그리고 Windows 클립보드를 사용한 데이터 교환 등을 제어할 수 있습니다.

워크로드당 라이센스가 부여되는 Cyber Protect Essentials, Cyber Protect Standard 및 Cyber Protect Advanced Edition에서 이 모듈을 사용할 수 있습니다.

참고
Windows 머신에서 장치 제어 기능을 사용하려면 데이터 손실 방지 에이전트를 설치해야 합니다. 보호 계획에서 **장치 제어** 모듈이 활성화된 경우 보호된 워크로드를 위해 자동으로 설치됩니다.

장치 제어 모듈은 에이전트의 데이터 손실 방지[3] 기능을 활용하여 보호된 컴퓨터에서 수행하는 데이터 액세스 및 전송 작업에 상황별 제어 기능을 적용합니다. 이러한 작업으로는 사용자의 주변 장치 및 포트 액세스, 문서 인쇄, 클립보드 복사/붙여넣기 작업, 미디어 포맷 및 꺼내기 작업, 그리고 로컬에 연결된 모바일 장치와의 동기화 등이 있습니다. 데이터 손실 방지 에이전트에는 장치 제어 모듈의 모든 중앙 관리 및 관리 컴퍼넌트용 프레임워크가 포함되어 있습니다. 따라서 장치 제어 모듈을 사용하여 보호할 모든 컴퓨터에 에이전트를 설치해야 합니다. 에이전트는 보호된 컴퓨터에 적용되어 있는 보호 계획에서 수신되는 장치 제어 설정에 따라 사용자 작업을 허용, 제한 또는 거부합니다.

장치 제어 모듈은 보호되는 컴퓨터에서 직접 사용하는 장치, 보호되는 컴퓨터에서 호스팅되는 가상화 환경에서 리디렉션된 장치 등 다양한 주변 장치 액세스를 제어합니다. 이 모듈은 Microsoft

[1]장치 제어 모듈은 보호 계획의 일환으로 보호되는 각 컴퓨터의 데이터 손실 방지 에이전트 기능 중 일부를 활용하여 무단 액세스 및 로컬 컴퓨터 채널을 통한 데이터 전송을 감지 및 방지합니다. 이러한 작업으로는 사용자의 주변 장치 및 포트 액세스, 문서 인쇄, 클립보드 복사/붙여넣기 작업, 미디어 포맷 및 꺼내기 작업, 그리고 로컬에 연결된 모바일 장치와의 동기화 등이 있습니다. 장치 제어 모듈에서는 사용자가 보호된 컴퓨터에서 액세스할 수 있는 포트 및 장치 유형, 그리고 사용자가 해당 장치에서 수행할 수 있는 작업을 상황별로 자세하게 제어할 수 있습니다.
[2]기밀 데이터, 보호된 데이터 또는 중요한 데이터의 무단 사용, 전송, 저장으로부터 호스트 컴퓨터를 보호하는 데이터 손실 방지 시스템의 클라이언트 구성 요소입니다. 이 에이전트는 상황 및 내용 분석 기술을 함께 적용하고 중앙에서 관리되는 데이터 손실 방지 정책을 적용함으로써 컴퓨터를 보호합니다. Cyber Protection에서는 모든 기능을 갖춘 데이터 손실 방지 에이전트를 제공합니다. 그러나 보호된 컴퓨터의 에이전트 기능은 Cyber Protection에서 라이센스를 통해 사용 가능한 데이터 손실 방지 기능 세트로 제한됩니다. 사용 가능한 기능은 해당 컴퓨터에 적용되는 보호 계획에 따라 달라집니다.
[3]조직 내/외부의 권한이 없는 항목에 의한 실수 또는 의도적인 기밀 데이터, 보호된 데이터 또는 중요한 데이터 공개/액세스나 신뢰할 수 없는 환경으로의 해당 데이터 전송을 감지하고 방지하는 데 사용할 수 있는 통합 기술 및 조직 대책 시스템입니다.

© Acronis International GmbH, 2003-2024

Remote Desktop Server, Citrix XenDesktop/XenApp/XenServer 및 VMware Horizon에서 리디렉션된 장치를 인식합니다. 또한 VMware Workstation/Player, Oracle VM VirtualBox 또는 Windows Virtual PC에서 실행 중인 게스트 운영 체제의 클립보드와, 보호되는 컴퓨터에서 실행 중인 호스트 운영 체제의 클립보드 간 데이터 복사 작업도 제어할 수 있습니다.

장치 제어 모듈은 다음 운영 체제에서 실행되는 컴퓨터를 보호할 수 있습니다.

장치 제어

- Microsoft Windows 7 서비스 팩 1 이상
- Microsoft Windows Server 2008 R2 이상
- macOS 10.15 (Catalina)
- macOS 11.2.3(Big Sur)
- macOS 12 (Monterey)
- macOS 13 (Ventura)

참고
MacOS용 데이터 손실 방지 에이전트는 x64 프로세서만 지원합니다. Apple 실리콘 ARM 기반 프로세서는 지원되지 않습니다.

데이터 손실 방지

- Microsoft Windows 7 서비스 팩 1 이상
- Microsoft Windows Server 2008 R2 이상

참고
데이터 손실 방지 에이젠트는 Mac 에이전트의 필수적인 부분이기 때문에 비지원 macOS 시스템 상에 설치될 수 있습니다. 이 경우 컴퓨터에 데이터 손실 방지 에이전트가 설치되어 있다는 사실이 Cyber Protect 콘솔을 통해 표시되지만, 장치 제어 및 데이터 손실 방지 기능은 작동하지 않습니다. 장치 제어 기능은 데이터 손실 방지 에이전트가 지원하는 macOS 시스템 상에서만 작동합니다.

Hyper-V의 데이터 손실 방지 에이전트 사용 제한

주로 CSV(클러스터된 공유 볼륨)가 있는 Hyper-V 클러스터에서 BSOD 문제가 발생할 수 있으므로 Hyper-V 클러스터의 Hyper-V 호스트에 데이터 손실 방지 에이전트를 설치하지 마십시오.

다음과 같은 Agent for Hyper-V 버전을 사용하는 경우 데이터 손실 방지 에이전트를 수동으로 제거해야 합니다.

- 15.0.26473(C21.02)
- 15.0.26570(C21.02 HF1)
- 15.0.26653(C21.03)
- 15.0.26692(C21.03 HF1)
- 15.0.26822(C21.04)

© Acronis International GmbH, 2003-2024

데이터 손실 방지 에이전트를 제거하려면 Hyper-V 호스트에서 인스톨러를 수동으로 실행하고 데이터 손실 방지 에이전트 확인란을 지우거나 다음 명령을 실행합니다.

```
<installer_name> --remove-components=agentForDlp -quiet
```

Cyber Protect 콘솔의 보호 계획 내 **장치 제어** 섹션에서 이 모듈을 활성화하고 구성할 수 있습니다. 관련 지침은 장치 제어를 활성화하거나 비활성화하는 단계를 참조하십시오.

장치 제어 섹션에는 모듈 구성의 요약이 표시됩니다.

- 액세스 설정 - 액세스가 제한된 장치 유형 및 포트(있는 경우)의 요약이 표시됩니다. 제한된 장치 유형과 포트가 없으면 모든 장치 유형이 허용된다는 메시지가 표시됩니다. 이 요약을 클릭하면 액세스 설정을 확인하거나 변경할 수 있습니다(액세스 설정을 확인하거나 변경하는 단계 참조).
- 장치 유형 허용 목록 - 장치 액세스 제어에서 제외하면 허용되는 장치 하위 클래스(있는 경우)의 수가 표시됩니다. 해당 하위 클래스가 없으면 허용 목록이 비어 있다는 메시지가 표시됩니다. 이 요약을 클릭하면 허용되는 장치 하위 클래스 선택 항목을 확인하거나 변경할 수 있습니다(액세스 제어에서 장치 하위 클래스를 제외하는 단계 참조).
- USB 장치 허용 목록 - 장치 액세스 제어에서 제외하면 허용되는 USB 장치/모델(있는 경우)의 수가 표시됩니다. 해당 하위 클래스가 없으면 허용 목록이 비어 있다는 메시지가 표시됩니다. 이 요약을 클릭하면 허용되는 USB 장치/모델 목록을 확인하거나 변경할 수 있습니다(액세스 제어에서 개별 USB 장치를 제외하는 단계 참조).
- 제외 항목 - Windows 클립보드, 스크린샷 캡처, 프린터 및 모바일 장치를 대상으로 설정된 액세스 제어 제외 항목의 수가 표시됩니다.

장치 제어 사용

이 섹션에서는 장치 제어 모듈을 사용할 때 수행하는 기본적인 작업의 단계별 지침을 설명합니다.

© Acronis International GmbH, 2003-2024

장치 제어 활성화 또는 비활성화

보호 계획을 생성할 때 장치 제어를 활성화할 수 있습니다. 기존 보호 계획을 변경하여 장치 제어를 활성화하거나 비활성화할 수 있습니다.

장치 제어를 활성화하거나 비활성화하려면

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 다음 중 하나를 수행하여 보호 계획 패널을 엽니다.
   - 새 보호 계획을 생성하려면 보호할 머신을 선택하고 **보호**를 클릭한 다음 **계획 생성**을 클릭합니다.
   - 기존 보호 계획을 변경하려면 보호된 머신을 선택하고 **보호**를 클릭한 다음 보호 계획 이름 옆의 말줄임표(...)를 클릭하고 **편집**을 클릭합니다.
3. 보호 계획 패널에서 **장치 제어** 영역으로 이동한 다음 **장치 제어**를 활성화하거나 비활성화합니다.
4. 다음 중 하나를 수행하여 변경 사항을 적용합니다.
   - 보호 계획을 생성하는 경우 **생성**을 클릭합니다.
   - 보호 계획을 편집하는 경우 **저장**을 클릭합니다.

관리 탭에서 보호 계획 패널에 액세스할 수도 있습니다. 그러나 Cyber Protection 서비스의 모든 에디션에서 이 기능이 제공되는 것은 아닙니다.

macOS에서 장치 제어 모듈 사용 활성화

보호된 워크로드 상에 장치 제어 드라이버를 로드한 후에만 보호 계획의 장치 제어 설정이 유효합니다. 이 섹션은 macOS에서 장치 제어 모듈 사용을 활성화하기 위해 장치 제어 드라이버를 로드하는 방법에 대해 다룹니다. 이 작업은 일회성이며 엔드포인트 머신에서 관리자 권한을 필요로 합니다.

지원되는 macOS 버전:

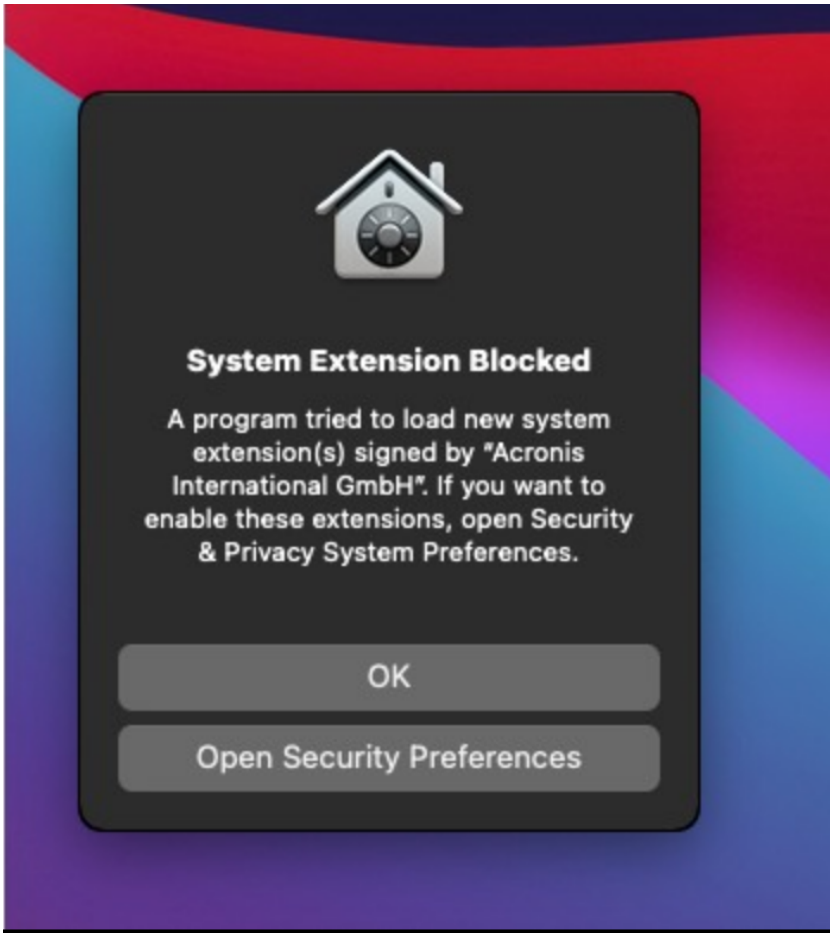
- macOS 10.15(Catalina) 이상
- macOS 11.2.3(Big Sur) 이상
- macOS 12.2(Monterey) 이상
- macOS 13.2(Ventura) 이상

macOS에서 장치 제어 모듈 사용을 활성화하는 방법

1. 보호하고자하는 머신에 Mac용 에이전트를 설치합니다.
2. 보호 계획에서 장치 제어 설정을 활성화합니다.
3. 보호 계획을 적용합니다.

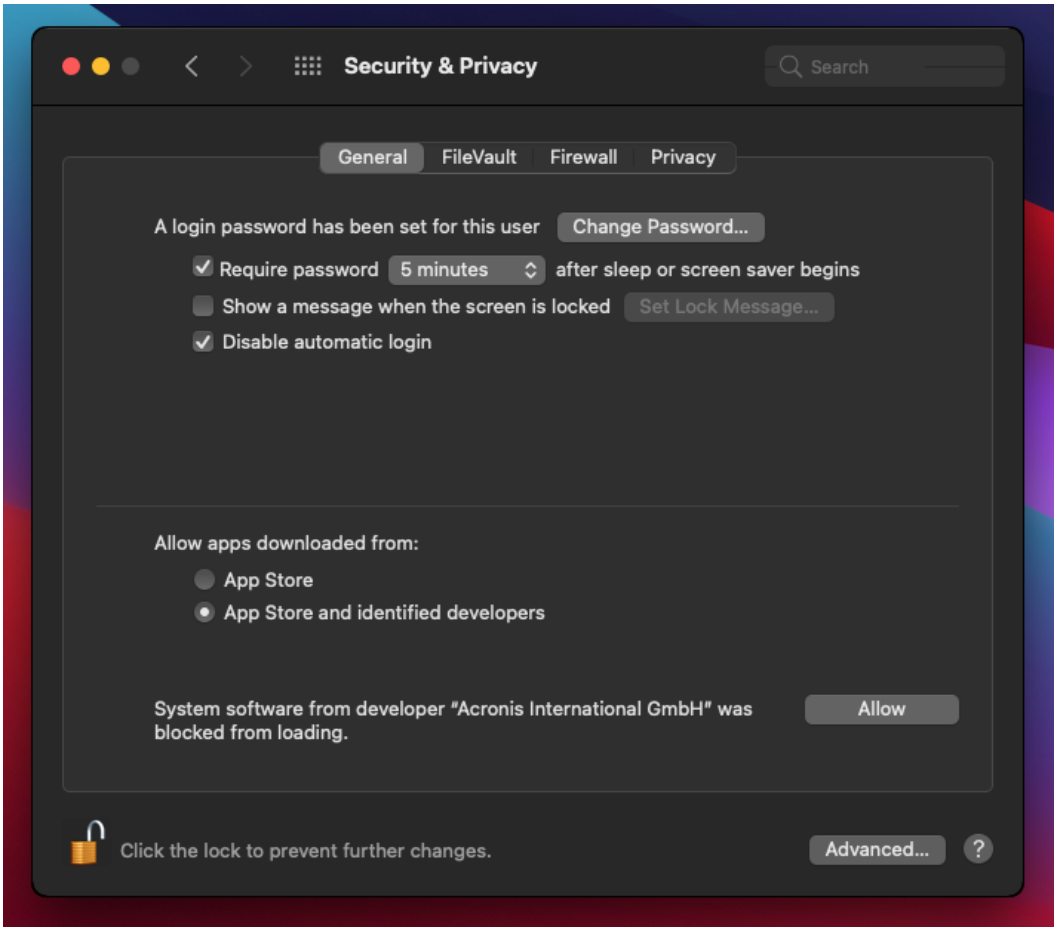
© Acronis International GmbH, 2003-2024

4. 보호된 워크로드 상에 "시스템 확장 차단됨" 경고가 표시됩니다. **보안 설정 열기**를 클릭합니다.



© Acronis International GmbH, 2003-2024

5. **보안 및 개인정보 보호** 창이 열리면 **앱 스토어 및 식별된 개발자**를 선택한 다음 **허용**을 클릭합니다.



6. 대화창이 나타나면 **다시 시작**을 선택하여 워크로드를 다시 시작한 다음 장치 제어 설정을 활성화합니다.

참고
장치 제어 설정이 비활성화된 후 다시 활성화되는 경우 이 단계를 반복하지 않아도 됩니다.

액세스 설정 확인 또는 변경

보호 계획 패널에서 장치 제어 모듈의 액세스 설정을 관리할 수 있습니다. 이렇게 하면 특정 장치 유형 액세스를 허용하거나 거부할 수 있으며 알림과 경보를 활성화하거나 비활성화할 수도 있습니다.

액세스 설정을 확인하거나 변경하려면

1. 보호 계획의 보호 계획 패널을 열고 해당 계획에서 장치 제어를 활성화합니다(장치 제어를 활성화하거나 비활성화하는 단계 참조).
2. **장치 제어** 스위치 옆의 화살표 아이콘을 클릭하여 설정을 확장한 다음 **액세스 설정** 옆의 링크를 클릭합니다.
3. 그러면 표시되는 액세스 설정 관리 페이지에서 설정을 확인하거나 적절하게 변경합니다.

© Acronis International GmbH, 2003-2024

참고
장치 제어에서 구성된 액세스 설정은 장치 제어 Advanced DLP를 모두 사용하여 워크로드를 보호하는 경우 무시될 수 있습니다. "보호 계획에서 Advanced Data Loss Prevention 활성화"(796페이지)을(를) 참조하십시오.

OS 알림 및 서비스 경보 활성화 또는 비활성화

액세스 설정을 관리할 때는 사용자가 허용되지 않는 작업 수행을 시도했음을 알려 주는 OS 알림 및 서비스 경보를 활성화하거나 비활성화할 수 있습니다.

OS 알림을 활성화 또는 비활성화하려면

1. 액세스 설정을 확인하거나 변경하는 단계를 따릅니다.
2. 액세스 설정 관리 페이지에서 **최종 사용자가 차단된 장치 유형이나 포트 사용을 시도하면 OS 알림 표시** 확인란을 선택하거나 선택을 취소합니다.

서비스 경보를 활성화 또는 비활성화하려면

1. 액세스 설정을 확인하거나 변경하는 단계를 따릅니다.
2. 액세스 설정 관리 페이지에서 원하는 장치 유형의 **경보 보이기** 확인란을 선택하거나 선택을 취소합니다.

스크린샷 캡처를 제외하고, 액세스가 제한된 장치 유형(읽기 전용 또는 액세스가 거부된 장치)의 경우에만 **경보 보이기** 확인란을 사용할 수 있습니다.

액세스 제어에서 장치 하위 클래스 제외

보호 계획 패널에서 액세스 제어에서 제외할 장치 하위 클래스를 선택할 수 있습니다. 그러면 장치 제어 액세스 설정에 관계없이 해당 장치 액세스가 허용됩니다.

액세스 제어에서 장치 하위 클래스를 제외하려면

1. 보호 계획의 보호 계획 패널을 열고 해당 계획에서 장치 제어를 활성화합니다(장치 제어를 활성화하거나 비활성화하는 단계 참조).
2. **장치 제어** 스위치 옆의 화살표 아이콘을 클릭하여 설정을 확장한 다음 **장치 제어 허용 목록** 옆의 링크를 클릭합니다.
3. 그러면 표시되는 허용 목록 관리 페이지에서 액세스 제어에서 제외할 장치 하위 클래스 선택 항목을 확인하거나 변경합니다.

액세스 제어에서 개별 USB 장치 제외

보호 계획 패널에서 액세스 제어에서 제외할 개별 USB 장치 또는 USB 장치 모델을 지정할 수 있습니다. 그러면 장치 제어 액세스 설정에 관계없이 해당 장치 액세스가 허용됩니다.

액세스 제어에서 USB 장치를 제외하려면

1. 보호 계획의 보호 계획 패널을 열고 해당 계획에서 장치 제어를 활성화합니다(장치 제어를 활성화하거나 비활성화하는 단계 참조).

© Acronis International GmbH, 2003-2024

2. **장치 제어** 스위치 옆의 화살표 아이콘을 클릭하여 설정을 확장한 다음 **USB 장치 허용 목록** 옆의 링크를 클릭합니다.
3. 그러면 표시되는 허용 목록 관리 페이지에서 **데이터베이스에서 추가**를 클릭합니다.
4. 그러면 표시되는 USB 장치 선택 페이지에서 USB 장치 데이터베이스에 등록된 장치 중에서 원하는 장치를 선택합니다.
5. **허용 목록에 추가** 버튼을 클릭합니다.

액세스 제어에서 USB 장치를 제외를 중지하려면

1. 보호 계획의 보호 계획 패널을 열고 해당 계획에서 장치 제어를 활성화합니다(장치 제어를 활성화하거나 비활성화하는 단계 참조).
2. **장치 제어** 스위치 옆의 화살표 아이콘을 클릭하여 설정을 확장한 다음 **USB 장치 허용 목록** 옆의 링크를 클릭합니다.
3. 그러면 표시되는 허용 목록 관리 페이지에서 원하는 USB 장치를 나타내는 목록 항목 끝부분의 삭제 아이콘을 클릭합니다.

USB 장치를 데이터베이스에 추가하거나 데이터베이스에서 제거

액세스 제어에서 특정 USB 장치를 제외하려면 USB 장치 데이터베이스에 해당 장치를 추가해야 합니다. 그리고 나면 해당 데이터베이스에서 장치를 선택하여 허용 목록에 추가할 수 있습니다.

장치 제어 기능이 활성화된 보호 계획에서는 다음 절차를 수행할 수 있습니다.

데이터베이스에 USB 장치를 추가하려면

1. 편집을 위해 장치에 대한 보호 계획을 엽니다.
   보호 계획 이름 옆에 있는 말줄임표(...)를 클릭한 다음 **편집**을 클릭합니다.

   참고
   장치 제어 설정에 액세스할 수 있도록 계획에서 장치 제어를 활성화해야 합니다.

2. **장치 제어** 스위치 옆의 화살표 아이콘을 클릭하여 설정을 확장한 다음 **USB 장치 허용 목록** 옆의 링크를 클릭합니다.
3. 그러면 표시되는 **USB 장치 허용 목록** 페이지에서 **데이터베이스에서 추가**를 클릭합니다.
4. 그러면 표시되는 USB 장치 데이터베이스 관리 페이지에서 **데이터베이스에 추가**를 클릭합니다.
5. **USB 장치 추가** 대화 상자가 표시되면 USB 장치가 연결된 머신을 클릭합니다.
   온라인 상태인 머신만 컴퓨터 목록에 표시됩니다.
   Data Loss Prevention용 에이전트가 설치되어 있는 머신의 경우에만 USB 장치 목록이 표시됩니다.
   USB 장치는 트리 보기에 나열됩니다. 트리 보기의 첫 번째 수준은 장치 모델을 나타냅니다. 두 번째 수준은 해당 모델의 특정 장치를 나타냅니다.
   장치 설명 옆의 파란색 아이콘은 장치가 현재 컴퓨터에 연결되어 있음을 나타냅니다. 장치가 컴퓨터에 연결되어 있지 않으면 아이콘은 회색으로 표시됩니다.
6. 데이터베이스에 추가할 USB 장치의 확인란을 선택하고 **데이터베이스에 추가**를 클릭합니다.
   선택한 USB 장치가 데이터베이스에 추가됩니다.

© Acronis International GmbH, 2003-2024

7. 보호 계획을 닫거나 저장합니다.

*컴퓨터 세부 정보 패널에서 데이터베이스에 **USB** 장치를 추가하려면*

참고
온라인 상태이며 Data Loss Prevention용 에이전트가 설치되어 있는 장치에서만 이 절차를 수행할 수 있습니다. 오프라인 상태이거나 Data Loss Prevention 에이전트가 설치되어 있지 않은 컴퓨터의 경우에는 USB 장치 목록을 확인할 수 없습니다.

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 원하는 USB 장치를 연결한 적이 없는 컴퓨터를 선택하고 오른쪽 메뉴에서 **인벤토리**를 클릭합니다.
   컴퓨터 세부 정보 패널이 열립니다.
3. 컴퓨터 세부 정보 패널에서 **USB 장치** 탭을 클릭합니다.
   선택한 컴퓨터에서 확인된 USB 장치 목록이 열립니다.
   USB 장치는 트리 보기에 나열됩니다. 트리 보기의 첫 번째 수준은 장치 모델을 나타냅니다. 두 번째 수준은 해당 모델의 특정 장치를 나타냅니다.
   장치 설명 옆의 파란색 아이콘은 장치가 현재 컴퓨터에 연결되어 있음을 나타냅니다. 장치가 컴퓨터에 연결되어 있지 않으면 아이콘은 회색으로 표시됩니다.
4. 데이터베이스에 추가할 USB 장치의 확인란을 선택하고 **데이터베이스에 추가**를 클릭합니다.

*서비스 경보에서 데이터베이스에 **USB** 장치를 추가하려면*

1. Cyber Protect 콘솔에서 **모니터링** > **경보**로 이동합니다.
2. USB 장치 액세스가 거부되었음을 알려 주는 장치 제어 경보를 찾습니다.
3. 경보 단순 보기에서 **이 USB 장치 허용**을 클릭합니다.
   그러면 액세스 제어에서 해당 USB 장치가 제외되고 추가 참조가 가능하도록 데이터베이스에 해당 장치가 추가됩니다.

*데이터베이스로 장치 목록을 가져와서 **USB** 장치를 추가하려면*

USB 장치 목록이 포함된 JSON 파일을 데이터베이스로 가져올 수 있습니다. "데이터베이스로 USB 장치 목록 가져오기"(350페이지)을(를) 참조하십시오.

*데이터베이스에서 **USB** 장치를 제거하려면*

1. 편집을 위해 장치에 대한 보호 계획을 엽니다.
   보호 계획 이름 옆에 있는 말줄임표(...)를 클릭한 다음 **편집**을 클릭합니다.

   참고
   장치 제어 설정에 액세스할 수 있도록 계획에서 장치 제어를 활성화해야 합니다.

2. **장치 제어** 스위치 옆의 화살표를 클릭하여 설정을 확장한 다음 **USB 장치 허용 목록** 행을 클릭합니다.
3. 그러면 표시되는 허용 목록 관리 페이지에서 **데이터베이스에서 추가**를 클릭합니다.
4. **데이터베이스에서 USB 장치 선택 페이지**에서 해당 장치를 나타내는 목록 항목 끝부분의 말줄임표(...)를 클릭하고 삭제를 클릭한 다음 삭제를 확인합니다.

© Acronis International GmbH, 2003-2024

USB 장치가 데이터베이스에서 삭제됩니다.

5. 보호 계획을 닫거나 저장합니다.

장치 제어 경보 확인

사용자의 특정 장치 유형 사용 시도가 거부되었음을 알려 주는 경보를 생성하도록 장치 제어 모듈을 구성할 수 있습니다(OS 알림 및 서비스 경보 활성화 또는 비활성화 참조). 이러한 경보를 확인하려면 다음 단계를 수행합니다.

장치 제어 경보를 확인하려면

1. Cyber Protect 콘솔에서 **모니터링** > **경보**로 이동합니다.
2. 상태가 "주변 장치 액세스가 차단됨"인 경보를 찾습니다.

자세한 내용은 장치 제어 경보를 참조하십시오.

액세스 설정

액세스 설정 페이지에서 특정 장치 유형 액세스를 허용하거나 거부할 수 있으며 OS 알림과 장치 제어 경보를 활성화하거나 비활성화할 수도 있습니다.

참고
장치 제어에서 구성된 액세스 설정은 장치 제어 Advanced DLP를 모두 사용하여 워크로드를 보호하는 경우 무시될 수 있습니다. "보호 계획에서 Advanced Data Loss Prevention 활성화"(796페이지)을(를) 참조하십시오.

액세스 설정에서는 사용자의 다음 장치 유형 및 포트 액세스를 제한할 수 있습니다.

- **이동식**(장치 유형별 액세스 제어) - 컴퓨터 연결용 인터페이스(USB, FireWire, PCMCIA, IDE, SATA, SCSI 등)가 있으며 운영 체제에서 이동식 스토리지 장치로 인식되는 USB 스틱, 카드 판독기, 자기 광학 드라이브 등의 디바이스입니다. 장치 제어에서는 USB, FireWire 및 PCMCIA를 통해 연결되는 모든 하드 드라이브를 이동식 장치로 분류합니다. 또한 핫 플러그 기능을 지원하며 실행 가능한 운영 체제가 설치되어 있지 않은 일부 하드 드라이브(대개 SATA 및 SCSI 드라이브)도 이동식 장치로 분류합니다.

  이동식 장치에 대한 전체 액세스 권한 또는 읽기 전용 액세스 권한을 허용하거나 액세스를 거부할 수 있습니다. 이렇게 하면 보호된 컴퓨터에서 이동식 장치의/이동식 장치로의 데이터 복사 작업을 제어할 수 있습니다. BitLocker나 FireVault(HFS+ 파일 시스템 한정)로 암호화된 장치에는 액세스 권한이 적용되지 않습니다.

  이 장치 유형은 Windows 및 macOS에서 모두 지원됩니다.
- **암호화된 이동식**(장치 유형별 액세스 제어) - BitLocker(Windows의 경우)나 FireVault(macOS의 경우) 드라이브 암호화를 사용하여 암호화한 이동식 장치입니다.

  macOS에서는 HFS+(HFS Plus나 Mac OS 확장, HFS 확장이라고도 함) 파일 시스템을 사용하는 암호화된 이동식 드라이브만 지원됩니다. APFS 파일 시스템을 사용하는 암호화된 이동식 드라이브는 이동식 장치로 취급됩니다.

  암호화된 이동식 장치에 대한 전체 액세스 권한 또는 읽기 전용 액세스 권한을 허용하거나 액세스를 거부할 수 있습니다. 이렇게 하면 보호된 컴퓨터에서 암호화된 이동식 장치의/암호화된 이

© Acronis International GmbH, 2003-2024

동식 장치로의 데이터 복사 작업을 제어할 수 있습니다. BitLocker나 FireVault(HFS+ 파일 시스템 한정)로 암호화된 장치의 경우에만 액세스 권한이 적용됩니다.

이 장치 유형은 Windows 및 macOS에서 모두 지원됩니다.

- **프린터**(장치 유형별 액세스 제어) - USB, LPT, Bluetooth 등의 컴퓨터 연결용 인터페이스가 있는 실제 프린터와 네트워크에서 컴퓨터에 액세스하는 프린터입니다.

  프린터 액세스를 허용하거나 거부할 수 있습니다. 이렇게 하면 보호된 컴퓨터에서 프린터로 문서를 인쇄하는 작업을 제어할 수 있습니다.

  참고
  프린터의 액세스 설정을 **거부**로 변경하면 프린터에 액세스하는 애플리케이션과 프로세스를 다시 시작해야 새로 구성한 액세스 설정이 적용됩니다. 액세스 설정이 올바르게 적용되었는지 확인하려면 보호된 워크로드를 다시 시작합니다.

  이 장치 유형은 Windows에서만 지원됩니다.
- **클립보드**(장치 유형별 액세스 제어) - Windows클립보드입니다.

  클립보드 액세스를 허용하거나 거부할 수 있습니다. 이렇게 하면 보호된 컴퓨터에서 Windows 클립보드를 통해 수행하는 복사 및 붙여넣기 작업을 제어할 수 있습니다.

  참고
  클립보드의 액세스 설정을 **거부**로 변경하면 클립보드에 액세스하는 애플리케이션과 프로세스를 다시 시작해야 새로 구성한 액세스 설정이 적용됩니다. 액세스 설정이 올바르게 적용되었는지 확인하려면 보호된 워크로드를 다시 시작합니다.

  이 장치 유형은 Windows에서만 지원됩니다.
- **스크린샷 캡처**(장치 유형별 액세스 제어) - 전체 화면, 활성 창 또는 화면에서 선택한 부분의 스크린샷 캡처를 활성화합니다.

  스크린샷 캡처 액세스를 허용하거나 거부할 수 있습니다. 이렇게 하면 보호된 컴퓨터에서 스크린샷 캡처를 제어할 수 있습니다.

  참고
  스크린샷 캡처의 액세스 설정을 **거부**로 변경하면 스크린샷 캡처에 액세스하는 애플리케이션과 프로세스를 다시 시작해야 새로 구성한 액세스 설정이 적용됩니다. 액세스 설정이 올바르게 적용되었는지 확인하려면 보호된 워크로드를 다시 시작합니다.

  이 장치 유형은 Windows에서만 지원됩니다.
- **모바일 장치**(장치 유형별 액세스 제어) - 미디어 전송 프로토콜(MTP)을 통해 컴퓨터와 통신하며 컴퓨터에 연결하는 데 사용되는 USB, IP, Bluetooth 등의 인터페이스가 있는 Android 기반 스마트폰 등의 장치입니다.

  모바일 장치에 대한 전체 액세스 권한 또는 읽기 전용 액세스 권한을 허용하거나 액세스를 거부할 수 있습니다. 이렇게 하면 보호된 컴퓨터에서 MTP 기반 모바일 장치의/MTP 기반 모바일 이동식 장치로의 데이터 복사 작업을 제어할 수 있습니다.

© Acronis International GmbH, 2003-2024

참고

모바일 장치의 액세스 설정을 **읽기 전용** 또는 **거부**로 변경하면 모바일 장치에 액세스하는 애플리케이션과 프로세스를 다시 시작해야 새로 구성한 액세스 설정이 적용됩니다. 액세스 설정이 올바르게 적용되었는지 확인하려면 보호된 워크로드를 다시 시작합니다.

이 장치 유형은 Windows에서만 지원됩니다.

- **Bluetooth**(장치 유형별 액세스 제어) - USB, PCMCIA 등 컴퓨터 연결용 인터페이스가 있는 외장 및 내장 Bluetooth 장치입니다. 이 설정은 해당 유형의 장치 사용 자체를 제어하며, 이러한 장치를 사용한 데이터 교환을 제어하지는 않습니다.

  Bluetooth 액세스를 허용하거나 거부할 수 있습니다. 이렇게 하면 보호된 컴퓨터에서 Bluetooth 장치 사용을 제어할 수 있습니다.

참고

macOS에서는 블루투스 액세스 권한이 블루투스 HID 장치에 적용되지 않습니다. 이러한 장치에 대한 액세스는 항상 허용되어 무선 HID 장치(마우스 및 키보드)가 iMac 및 Mac Pro 하드웨어에서 비활성화되는 것을 방지합니다.

이 장치 유형은 Windows 및 macOS에서 모두 지원됩니다.

- **광학 드라이브**(장치 유형별 액세스 제어) - IDE, SATA, USB, FireWire, PCMCIA 등 컴퓨터 연결용 인터페이스가 있는 외장 및 내장 CD/DVD/BD 드라이브(기록기 포함)입니다.

  광학 드라이브에 대한 전체 액세스 권한 또는 읽기 전용 액세스 권한을 허용하거나 액세스를 거부할 수 있습니다. 이렇게 하면 보호된 컴퓨터에서 광학 드라이브의/광학 드라이브로의 데이터 복사 작업을 제어할 수 있습니다.

  이 장치 유형은 Windows 및 macOS에서 모두 지원됩니다.

- **플로피 드라이브**(장치 유형별 액세스 제어) - USB, PCMCIA 등 컴퓨터 연결용 인터페이스가 있는 외장 및 내장 플로피 드라이브입니다. 운영 체제가 이동식 드라이브로 인식하는 플로피 드라이브 모델도 있습니다. 이러한 모델의 경우에는 장치 제어에서도 해당 드라이브를 이동식 장치로 식별합니다.

  플로피 드라이브에 대한 전체 액세스 권한 또는 읽기 전용 액세스 권한을 허용하거나 액세스를 거부할 수 있습니다. 이렇게 하면 보호된 컴퓨터에서 플로피 드라이브의/플로피 드라이브로의 데이터 복사 작업을 제어할 수 있습니다.

  이 장치 유형은 Windows에서만 지원됩니다.

- **USB**(장치 인터페이스별 액세스 제어) - USB 포트에 연결되는 모든 장치(허브 제외)입니다.

  USB 포트에 대한 전체 액세스 권한 또는 읽기 전용 액세스 권한을 허용하거나 액세스를 거부할 수 있습니다. 이렇게 하면 보호된 컴퓨터에서 USB 포트에 연결된 장치의/장치로의 데이터 복사 작업을 제어할 수 있습니다.

  이 장치 유형은 Windows 및 macOS에서 모두 지원됩니다.

- **FireWire**(장치 인터페이스별 액세스 제어) - FireWire(IEEE 1394) 포트에 연결되는 모든 장치(허브 제외)입니다.

© Acronis International GmbH, 2003-2024

FireWire 포트에 대한 전체 액세스 권한 또는 읽기 전용 액세스 권한을 허용하거나 액세스를 거부할 수 있습니다. 이렇게 하면 보호된 컴퓨터에서 FireWire 포트에 연결된 장치의/장치로의 데이터 복사 작업을 제어할 수 있습니다.

이 장치 유형은 Windows 및 macOS에서 모두 지원됩니다.

- **리디렉션 장치**(장치 인터페이스별 액세스 제어) - 가상 애플리케이션/데스크톱 세션으로 리디렉션된 클립보드, USB 장치 및 매핑된 드라이브(하드 드라이브, 이동식 드라이브 및 광학 드라이브)입니다.

  장치 제어에서는 보호된 Windows 컴퓨터에서 호스팅되는 Microsoft RDP, Citrix ICA, VMware PCoIP, Microsoft RDS의 HTML5/WebSockets 원격 프로토콜, Citrix XenDesktop, Citrix XenApp, Citrix XenServer, VMware Horizon 가상화 환경을 통해 리디렉션된 장치를 인식합니다. 또한 VMware Workstation, VMware Player, Oracle VM VirtualBox 또는 Windows Virtual PC에서 실행 중인 게스트 운영 체제의 Windows 클립보드와, 보호되는 Windows 컴퓨터에서 실행 중인 호스트 운영 체제의 클립보드 간 데이터 복사 작업도 제어할 수 있습니다.

  이 장치 유형은 Windows에서만 지원됩니다.

  다음과 같이 리디렉션 장치에 대한 액세스를 구성할 수 있습니다.

  - **매핑된 드라이브** - 전체 액세스 권한 또는 읽기 전용 액세스 권한을 허용하거나 액세스를 거부할 수 있습니다. 이렇게 하면 보호된 컴퓨터에서 호스팅되는 세션으로 리디렉션된 하드 드라이브, 이동식 드라이브 또는 광학 드라이브의/드라이브로의 데이터 복사 작업을 제어할 수 있습니다.
  - **클립보드(들어옴)** - 액세스를 허용하거나 거부할 수 있습니다. 이렇게 하면 클립보드를 통해 보호된 컴퓨터에서 호스팅되는 세션으로 데이터를 복사하는 작업을 제어할 수 있습니다.

    참고
    클립보드(들어옴)의 액세스 설정을 **거부**로 변경하면 클립보드에 액세스하는 애플리케이션과 프로세스를 다시 시작해야 새로 구성한 액세스 설정이 적용됩니다. 액세스 설정이 올바르게 적용되었는지 확인하려면 보호된 워크로드를 다시 시작합니다.

  - **클립보드(나감)** - 액세스를 허용하거나 거부할 수 있습니다. 이렇게 하면 클립보드를 통해 보호된 컴퓨터에서 호스팅되는 세션에서 데이터를 복사하는 작업을 제어할 수 있습니다.

    참고
    클립보드(나감)의 액세스 설정을 **거부**로 변경하면 클립보드에 액세스하는 애플리케이션과 프로세스를 다시 시작해야 새로 구성한 액세스 설정이 적용됩니다. 액세스 설정이 올바르게 적용되었는지 확인하려면 보호된 워크로드를 다시 시작합니다.

  - **USB 포트** - 액세스를 허용하거나 거부할 수 있습니다. 이렇게 하면 보호된 컴퓨터에서 호스팅되는 세션으로 리디렉션된 USB 포트에 연결된 장치의/장치로 데이터를 복사하는 작업을 제어할 수 있습니다.

장치 제어 설정은 모든 사용자에게 동일하게 적용됩니다. 예를 들어 이동식 장치 액세스를 거부하면 사용자가 보호된 컴퓨터에서 해당 장치의/장치로 데이터를 복사할 수 없습니다. 액세스 제어에서 개별 USB 장치를 제외하여 해당 장치 액세스를 선택적으로 허용할 수는 있습니다(장치 유형 허용 목록 및 USB 장치 허용 목록 참조).

© Acronis International GmbH, 2003-2024

장치 유형과 인터페이스로 장치 액세스를 제어하는 경우 인터페이스 수준의 액세스 거부가 우선적으로 적용됩니다. 예를 들어 USB 포트(장치 인터페이스) 액세스를 거부하면 모바일 장치(장치 유형) 액세스 허용 여부에 관계없이 USB 포트에 연결된 모바일 장치 액세스는 거부됩니다. 이러한 장치 액세스를 허용하려면 장치 인터페이스와 유형에 대해 모두 액세스를 허용해야 합니다.

참고
macOS에서 사용되는 보호 계획이 Windows에서만 지원되는 장치 유형에 대한 설정을 가지는 경우, macOS 상에서 이러한 장치 유형에 대한 설정은 무시됩니다.

중요
USB 포트에 연결된 이동식 장치, 암호화된 이동식 장치, 프린터 또는 Bluetooth 장치 액세스를 허용하면 USB 인터페이스 수준에서 설정된 액세스 거부보다 우선적으로 적용됩니다. 이러한 장치 유형 액세스를 허용하는 경우에는 USB 포트 액세스 거부 여부에 관계없이 해당 장치 액세스는 허용됩니다.

OS 알림 및 서비스 경보

최종 사용자가 보호된 컴퓨터에서 차단된 장치 유형 사용을 시도하면 최종 사용자에게 OS 알림이 표시되도록 장치 제어를 구성할 수 있습니다. 액세스 설정에서 **최종 사용자가 차단된 장치 유형이나 포트 사용을 시도하면 OS 알림 표시** 확인란을 선택하면 다음 이벤트 중 하나가 발생하는 경우 에이전트가 보호된 컴퓨터의 알림 영역에 팝업 메시지를 표시합니다.

- USB 또는 FireWire 포트에서 장치를 사용하려는 시도가 거부되는 경우. 사용자가 USB 또는 FireWire 장치를 포트에 삽입했는데 인터페이스 수준(예: USB 포트 액세스 거부 시) 또는 유형 수준(예: 이동식 장치 사용 거부 시)에서 장치 사용 시도가 거부될 때마다 이 알림이 표시됩니다. 이 알림은 사용자가 지정된 장치/드라이브에 액세스할 수 없음을 알려 줍니다.
- 특정 장치에서 파일 등의 데이터 개체를 복사하려는 시도가 거부되는 경우. 플로피 드라이브, 광학 드라이브, 이동식 장치, 암호화된 이동식 장치, 모바일 장치, 리디렉션 매핑된 드라이브, 리디렉션 클립보드(데이터 들어옴) 등의 장치에 대한 읽기 액세스가 거부되면 이 알림이 표시됩니다. 이 알림은 사용자가 지정된 장치에서 지정된 데이터 개체를 가져올 수 없음을 알려 줍니다.

  Bluetooth, FireWire 포트, USB 포트 및 리디렉션 USB 포트에 대한 읽기/쓰기 액세스 거부 시에도 읽기 거부 알림이 표시됩니다.
- 특정 장치에 파일 등의 데이터 개체를 복사하려는 시도가 거부되는 경우. 플로피 드라이브, 광학 드라이브, 이동식 장치, 암호화된 이동식 장치, 모바일 장치, 로컬 클립보드, 스크린샷 캡처, 프린터, 리디렉션 매핑된 드라이브, 리디렉션 클립보드(데이터 나감) 등의 장치에 대한 쓰기 액세스가 거부되면 이 알림이 표시됩니다. 이 알림은 사용자가 지정된 장치에 지정된 데이터 개체를 보낼 수 없음을 알려 줍니다.

사용자가 보호된 컴퓨터에서 차단된 장치 유형에 액세스하려고 하면 경보가 발생할 수 있습니다. 이러한 경보는 Cyber Protect 콘솔에 로깅됩니다. 액세스 설정에서 **경보 보이기** 확인란을 선택하면 각 장치 유형(스크린샷 캡처 제외)이나 포트에 개별적으로 경보를 활성화할 수 있습니다. 예를 들어 이동식 장치에 읽기 전용으로만 액세스할 수 있는 상태에서 해당 장치 유형에 대해 **경보 보이기** 확인란을 선택하는 경우 보호된 컴퓨터의 사용자가 이동식 장치에 데이터를 복사하려고 할 때마다 경보가 로깅됩니다. 자세한 내용은 장치 제어 경보를 참조하십시오.

OS 알림 및 서비스 경보를 활성화하거나 비활성화하는 단계도 참조하십시오.

© Acronis International GmbH, 2003-2024

장치 유형 허용 목록

장치 허용 목록 페이지에서 장치 액세스 제어에서 제외할 장치 하위 클래스를 선택할 수 있습니다. 하위 클래스를 선택하면 장치 제어 모듈의 액세스 설정에 관계없이 해당 장치 액세스가 허용됩니다.

장치 제어 모듈에서는 정의된 장치 유형 내의 특정 하위 클래스 장치에 대한 액세스를 허용하는 옵션이 제공됩니다. 이 옵션을 사용하면 해당 유형 장치의 일부 하위 클래스를 제외한 특정 유형의 모든 장치 액세스를 거부할 수 있습니다. 예를 들어 모든 USB 포트 액세스는 거부하면서 USB 키보드와 마우스 사용은 허용하려는 등의 경우 이 옵션이 유용할 수 있습니다.

장치 제어 모듈을 구성할 때 장치 액세스 제어에서 제외할 장치 하위 클래스를 지정할 수 있습니다. 장치가 제외된 하위 클래스에 속하는 경우에는 장치 유형 또는 포트 액세스 거부 여부에 관계없이 해당 장치 액세스는 허용됩니다. 장치 액세스 제어에서 다음 장치 하위 클래스를 선택적으로 제외할 수 있습니다.

- **USB HID(마우스, 키보드 등)** - 이 하위 클래스를 선택하면 USB 포트 액세스가 거부되더라도 USB 포트에 연결된 HID 장치(마우스, 키보드 등)에는 액세스할 수 있습니다. 이 항목은 기본적으로 선택되어 있으므로 USB 포트 액세스를 거부해도 키보드나 마우스는 비활성화되지 않습니다.
  Windows 및 macOS에서 모두 지원됩니다.
- **USB 및 FireWire 네트워크 카드** - 이 하위 클래스를 선택하면 USB 포트 및/또는 FireWire 포트 액세스가 거부되더라도 USB 또는 FireWire(IEEE 1394) 포트에 연결된 네트워크 카드에는 액세스할 수 있습니다.
  Windows 및 macOS에서 모두 지원됩니다.
- **USB 스캐너 및 스틸 이미지 장치** - 이 하위 클래스를 선택하면 USB 포트 액세스가 거부되더라도 USB 포트에 연결된 스캐너 및 스틸 이미지 장치에는 액세스할 수 있습니다.
  Windows에서만 지원됩니다.
- **USB 오디오 장치** - 이 하위 클래스를 선택하면 USB 포트 액세스가 거부되더라도 USB 포트에 연결된 헤드셋, 마이크 등의 오디오 장치에는 액세스할 수 있습니다.
  Windows에서만 지원됩니다.
- **USB 카메라** - 이 하위 클래스를 선택하면 USB 포트 액세스가 거부되더라도 USB 포트에 연결된 웹 카메라에는 액세스할 수 있습니다.
  Windows에서만 지원됩니다.
- **Bluetooth HID(마우스, 키보드 등)** - 이 하위 클래스를 선택하면 Bluetooth 액세스가 거부되더라도 Bluetooth를 통해 연결된 HID 장치(마우스, 키보드 등)에는 액세스할 수 있습니다.
  Windows에서만 지원됩니다.
- **애플리케이션 내 클립보드 복사/붙여넣기** - 이 하위 클래스를 선택하면 클립보드 액세스가 거부되더라도 동일한 애플리케이션 내에서 클립보드를 통해 데이터를 복사하고 붙여넣는 작업은 허용됩니다.
  Windows에서만 지원됩니다.

참고
적용되는 보호 계획에 이 설정이 구성된 경우에는 미지원 장치 하위 클래스 설정은 무시됩니다.

© Acronis International GmbH, 2003-2024

장치 유형 허용 목록을 작성할 때는 다음을 고려하십시오.

- 장치 유형 허용 목록 사용 시에는 전체 장치 하위 클래스만 허용할 수 있습니다. 같은 하위 클래스의 기타 모든 장치를 거부하면서 특정 장치 모델만 허용할 수는 없습니다. 예를 들어 USB 카메라를 장치 액세스 제어에서 제외하면 모델 및 공급 업체에 관계없이 모든 USB 카메라 사용이 허용됩니다. 개별 장치/모델을 허용하는 방법은 USB 장치 허용 목록을 참조하십시오.
- 미리 정해진 장치 하위 클래스 목록에서만 장치 유형을 선택할 수 있습니다. 허용하려는 장치가 다른 하위 클래스에 속해 있다면 장치 유형 허용 목록을 사용하여 허용할 수 없습니다. 예를 들어 USB 스마트 카드 판독기 등의 하위 클래스를 허용 목록에 추가할 수는 없습니다. USB 포트 액세스가 거부되는 상태에서 USB 스마트 카드 판독기를 허용하려는 경우에는 USB 장치 허용 목록의 지침을 따라야 합니다.
- 장치 유형 허용 목록은 표준 Windows 드라이버를 사용하는 장치에만 사용 가능합니다. 독점 드라이버를 사용하는 일부 USB 장치의 하위 클래스는 장치 제어에서 인식되지 않을 수도 있습니다. 그러므로 장치 유형 허용 목록을 사용해 이러한 USB 장치 액세스를 허용할 수는 없습니다. 이 경우에는 장치/모델별로 액세스를 허용할 수 있습니다(USB 장치 허용 목록 참조).

USB 장치 허용 목록

허용 목록을 사용하면 다른 장치 제어 설정에 관계없이 특정 USB 장치 사용을 허용할 수 있습니다. 허용 목록에 개별 장치 또는 장치 모델을 추가하여 해당 장치를 대상으로 액세스 제어를 비활성화할 수 있습니다. 예를 들어 고유 ID가 지정된 모바일 장치를 허용 목록에 추가하면 다른 USB 장치 사용은 거부되더라도 해당 특정 장치 사용은 허용할 수 있습니다.

USB 장치 허용 목록 페이지에서 장치 액세스 제어에서 제외할 개별 USB 장치 또는 USB 장치 모델을 지정할 수 있습니다. 하위 클래스를 선택하면 장치 제어 모듈의 액세스 설정에 관계없이 해당 장치 액세스가 허용됩니다.

허용 목록의 장치를 식별하는 방법은 두 가지입니다.

- 장치 모델 - 특정 모델의 모든 장치를 집합적으로 식별합니다. USB\VID_0FCE&PID_E19E와 같은 공급 업체 ID(VID) 및 제품 ID(PID)로 각 장치 모델을 식별할 수 있습니다.

  VID와 PID의 조합을 통해 특정 장치를 식별할 수 있는 것은 아니며 전체 장치 모델만 식별 가능합니다. 허용 목록에 장치 모델을 추가하면 해당 모델의 모든 장치 액세스가 허용됩니다. 예를 들어 이 방법을 통해 특정 모델의 USB 프린터 사용을 허용할 수 있습니다.
- 고유 장치 - 특정 장치를 식별합니다. USB\VID_0FCE&PID_E19E\D55E7FCA와 같은 공급 업체 ID (VID), 제품 ID(PID) 및 제품 번호로 각 고유 장치를 식별할 수 있습니다.

  모든 USB 장치에 제품 번호가 할당되는 것은 아닙니다. 생산 과정에서 제품 번호가 할당된 장치만 허용 목록에 고유 장치로 추가할 수 있습니다. 고유 제품 번호가 있는 USB 스틱 등을 예로 들 수 있습니다.

허용 목록에 추가하려는 장치는 먼저 USB 장치 데이터베이스에 추가해야 합니다. 그리고 나면 해당 데이터베이스에서 장치를 선택하여 허용 목록에 추가할 수 있습니다.

별도의 구성 페이지인 **USB 장치 허용 목록**에서 허용 목록을 관리합니다. 장치 또는 장치 모델을 나타내는 목록의 각 항목에는 다음과 같은 필드가 있습니다.

© Acronis International GmbH, 2003-2024

- **설명** - USB 장치를 연결하면 운영 체제에서 특정 설명을 할당합니다. USB 장치 데이터베이스에서 장치 설명을 수정할 수 있습니다(USB 데이터베이스 관리 페이지 참조).
- **장치 유형** - 목록 항목이 고유 장치를 나타내는 경우 '고유'가 표시되고 장치 모델을 나타내는 경우 '모델'이 표시됩니다.
- **읽기 전용** - 선택하는 경우 장치에서 데이터 수신만 허용됩니다. 장치가 읽기 전용 액세스를 지원하지 않으면 장치 액세스는 차단됩니다. 장치에 대한 전체 액세스를 허용하려면 이 확인란 선택을 취소합니다.
- **다시 초기화** - 선택하는 경우 새 사용자 로그인 시 장치가 연결 끊기/다시 연결을 시뮬레이션합니다. 마우스, 키보드 등의 일부 USB 장치는 다시 초기화해야 작동하므로 이러한 장치의 경우에는 이 확인란을 선택하는 것이 좋습니다. 또한 USB 스틱, 광학 드라이브, 외장 하드 드라이브 등의 데이터 스토리지 장치의 경우에는 이 확인란 선택을 취소하는 것이 좋습니다.
  독점 드라이버를 사용하는 일부 USB 장치의 경우 장치 제어에서 다시 초기화하지 못할 수도 있습니다. 이러한 장치 액세스 권한이 없는 경우에는 USB 장치를 USB 포트에서 제거했다가 포트에 다시 삽입해야 합니다.

참고
다시 초기화 필드는 기본적으로 숨겨집니다. 표에서 해당 열을 표시하려면 표 오른쪽 위의 기어 아이콘을 클릭하고 **다시 초기화** 확인란을 선택합니다.

참고
읽기 전용 및 **다시 초기화** 필드는 macOS에서는 지원되지 않습니다. 이는 적용되는 보호 계획에 이 필드가 구성된 경우 무시됩니다.

다음과 같이 장치/모델을 허용 목록에 추가하거나 허용 목록에서 제거할 수 있습니다.

- 목록 위의 **데이터베이스에서 추가**를 클릭하고 USB 장치 데이터베이스에 등록된 장치 중에서 원하는 장치를 선택합니다. 선택한 장치가 목록에 추가됩니다. 그러면 목록에서 장치 설정을 구성하고 변경을 확인할 수 있습니다.
- USB 장치 액세스가 거부되었음을 알리는 경보에서 **이 USB 장치 허용**을 클릭합니다(장치 제어 경보 참조). 그러면 허용 목록 및 USB 장치 데이터베이스에 장치가 추가됩니다.
- 목록 항목 끝부분의 삭제 아이콘을 클릭합니다. 그러면 개별 장치/모델이 허용 목록에서 제거됩니다.

USB 장치 데이터베이스

장치 제어 모듈이 유지보수하는 USB 장치 데이터베이스에서 장치를 선택하여 제외 목록에 추가할 수 있습니다(USB 장치 허용 목록 참조). 다음과 같은 방법으로 데이터베이스에 USB 장치를 등록할 수 있습니다.

- 제외 목록에 장치를 추가할 때 표시되는 페이지에서 장치를 추가합니다(USB 장치 데이터베이스 관리 페이지 참조).
- Cyber Protect 콘솔의 컴퓨터 인벤토리 창 USB 장치 탭에서 장치를 추가합니다(컴퓨터의 USB 장치 목록 참조).
- USB 장치 액세스 거부 경보에서 장치 액세스를 허용합니다(장치 제어 경보 참조).

USB 장치를 데이터베이스에 추가하거나 데이터베이스에서 제거하는 단계도 참조하십시오.

© Acronis International GmbH, 2003-2024

USB 장치 데이터베이스 관리 페이지

USB 장치용 허용 목록을 구성할 때는 데이터베이스에서 장치를 추가할 수 있습니다. 이 옵션을 선택하면 장치 목록이 포함된 관리 페이지가 표시됩니다. 이 페이지에는 데이터베이스에 등록된 모든 장치의 목록을 확인할 수 있습니다. 이 목록에서 허용 목록에 추가할 장치를 선택할 수 있으며 다음 작업을 수행할 수 있습니다.

데이터베이스에 장치 등록

1. 페이지 위쪽의 **데이터베이스에 추가**를 클릭합니다.
2. **USB 장치 추가** 대화 상자가 표시되면 USB 장치가 연결된 머신을 선택합니다.
   온라인 상태인 머신만 컴퓨터 목록에 표시됩니다.
   Data Loss Prevention용 에이전트가 설치되어 있는 머신의 경우에만 USB 장치 목록이 표시됩니다.
   USB 장치는 트리 보기에 나열됩니다. 트리 보기의 첫 번째 수준은 장치 모델을 나타냅니다. 두 번째 수준은 해당 모델의 특정 장치를 나타냅니다.
   장치 설명 옆의 파란색 아이콘은 장치가 현재 컴퓨터에 연결되어 있음을 나타냅니다. 장치가 컴퓨터에 연결되어 있지 않으면 아이콘은 회색으로 표시됩니다.
3. 등록할 USB 장치의 확인란을 선택하고 **데이터베이스에 추가**를 클릭합니다.

장치 설명 변경

1. **USB 장치 데이터베이스** 페이지에서 장치를 나타내는 목록 항목 끝부분의 말줄임표(...)를 클릭하고 **편집**을 클릭합니다.
2. 대화 상자가 표시되면 설명을 변경합니다.

데이터베이스에서 장치 제거

1. 장치를 나타내는 목록 항목 끝부분의 말줄임표(...)를 클릭합니다.
2. **삭제**를 클릭하고 삭제를 확인합니다.

페이지의 목록에서는 각 장치에 대한 다음 정보가 제공됩니다.

- **설명** - 장치의 판독 가능한 식별자입니다. 필요한 경우 설명을 변경할 수 있습니다.
- **장치 유형** - 목록 항목이 고유 장치를 나타내는 경우 '고유'가 표시되고 장치 모델을 나타내는 경우 '모델'이 표시됩니다. 고유 장치에는 공급 업체 ID(VID) 및 제품 ID(PID)가 포함된 제품 번호가 있어야 합니다. 반면 장치 모델은 VID와 PID 조합으로 식별할 수 있습니다.
- **공급 업체 ID, 제품 ID, 제품 번호** - 이러한 값이 조합되어 USB\VID_<공급 업체 ID>&PID_<제품 ID>\<제품 번호> 형식의 장치 ID가 생성됩니다.
- **계정** - 해당 장치가 속해 있는 테넌트를 나타냅니다. 이 테넌트에는 데이터베이스에 장치를 등록하는 데 사용한 사용자 계정이 포함되어 있습니다.

참고
이 열은 기본적으로 숨겨집니다. 표에서 해당 열을 표시하려면 표 오른쪽 위의 기어 아이콘을 클릭한 다음 **계정**을 선택합니다.

© Acronis International GmbH, 2003-2024

맨 왼쪽 열에서 허용 목록에 추가할 장치를 선택할 수 있습니다. 추가할 각 장치의 확인란을 선택하고 **허용 목록에 추가** 버튼을 클릭합니다. 모든 확인란을 선택하거나 선택을 취소하려면 열 머리글의 확인란을 클릭합니다.

장치 목록을 검색하거나 필터링할 수 있습니다.

- 페이지 위쪽의 **검색**을 클릭하고 검색 문자열을 입력합니다. 그러면 입력한 문자열과 설명이 일치하는 장치가 목록에 표시됩니다.
- **필터**를 클릭한 후 표시되는 대화 상자에서 필터를 구성 및 적용합니다. 필터를 구성할 때 선택한 유형, 공급 업체 ID, 제품 ID 및 계정과 일치하는 장치만 목록에 표시됩니다. 필터를 취소하고 모든 장치를 목록에 표시하려면 **기본값으로 재설정**을 클릭합니다.

데이터베이스의 USB 장치 목록 내보내기

데이터베이스에 추가한 USB 장치 목록을 내보낼 수 있습니다.

1. 편집을 위해 장치에 대한 보호 계획을 엽니다.
2. **장치 제어** 스위치 옆의 화살표 아이콘을 클릭하여 설정을 확장한 다음 **USB 장치 허용 목록** 행을 클릭합니다.
3. USB 장치 허용 목록 페이지에서 **데이터베이스에서 추가**를 클릭합니다.
4. 그러면 표시되는 USB 장치 데이터베이스 관리 페이지에서 **내보내기**를 클릭합니다.
   표준 찾아보기 대화 상자가 열립니다.
5. 파일을 저장할 위치를 선택하고 필요한 경우 새 파일 이름을 입력한 후에 **저장**을 클릭합니다.

USB 장치 목록이 JSON 파일로 내보내기됩니다.

내보낸 JSON 파일을 편집하여 장치를 추가하거나 제거할 수 있으며 장치 설명을 대량 변경할 수 있습니다.

데이터베이스로 USB 장치 목록 가져오기

Cyber Protect 콘솔에서 USB 장치를 추가하는 대신 USB 장치 목록을 가져올 수 있습니다. 이 목록은 JSON 형식 파일입니다.

참고
JSON 파일은 해당 파일에 설명되어 있는 장치가 없는 데이터베이스로 가져올 수 있습니다. 중복 항목을 가져올 수는 없으므로, 파일을 내보냈던 데이터베이스로 수정된 파일을 가져오려는 경우에는 먼저 데이터베이스를 지워야 합니다. USB 장치 목록을 내보내고 수정한 후에 지우지 않고 동일 데이터베이스로 해당 목록을 가져오려고 하면 가져오기가 실패합니다.

1. 편집을 위해 장치에 대한 보호 계획을 엽니다.
2. **장치 제어** 스위치 옆의 화살표 아이콘을 클릭하여 설정을 확장한 다음 **USB 장치 허용 목록** 행을 클릭합니다.
3. USB 장치 허용 목록 페이지에서 **데이터베이스에서 추가**를 클릭합니다.
4. 그러면 표시되는 USB 장치 데이터베이스 관리 페이지에서 **가져오기**를 클릭합니다.
   파일에서 USB 장치 가져오기 대화 상자가 열립니다.
5. 가져올 파일을 끌어서 놓습니다(또는 찾기).

© Acronis International GmbH, 2003-2024

Cyber Protect 콘솔이 데이터베이스에 이미 있는 중복 항목이 목록에 포함되어 있는지 확인하여 중복 항목은 건너뜁니다. 데이터베이스에 없는 USB 장치는 데이터베이스에 추가됩니다.

컴퓨터의 USB 장치 목록

Cyber Protect 콘솔의 컴퓨터 인벤토리 패널에는 **USB 장치** 탭이 있습니다. 컴퓨터가 온라인 상태이며 Data Loss Prevention용 에이전트가 설치되어 있으면 **USB 장치** 탭에는 해당 컴퓨터에 연결한 적이 있는 모든 USB 장치 목록이 표시됩니다.

USB 장치는 트리 보기에 나열됩니다. 트리 보기의 첫 번째 수준은 장치 모델을 나타냅니다. 두 번째 수준은 해당 모델의 특정 장치를 나타냅니다.

목록에서는 각 장치에 대한 다음 정보가 제공됩니다.

- **설명** - USB 장치를 연결하면 운영 체제에서 설명을 할당합니다. 이 설명을 장치의 판독 가능한 식별자로 사용할 수 있습니다.
  장치 설명 옆의 파란색 아이콘은 장치가 현재 컴퓨터에 연결되어 있음을 나타냅니다. 장치가 컴퓨터에 연결되어 있지 않으면 아이콘은 회색으로 표시됩니다.
- **장치 ID** - 운영 체제에서 장치에 할당한 식별자입니다. 이 식별자의 형식은 다음과 같습니다. USB\VID_<공급 업체 ID>&PID_<제품 ID>\<제품 번호>. 여기서 <제품 번호>는 선택 사항입니다. 예: USB\VID_0FCE&PID_ADDE\D55E7FCA(제품 번호가 있는 장치)/USB\VID_0FCE&PID_ADDE(제품 번호가 없는 장치)

USB 장치 데이터베이스에 장치를 추가하려면 원하는 장치의 확인란을 선택하고 **데이터베이스에 추가** 버튼을 클릭합니다.

액세스 제어에서 프로세스 제외

프로세스에 추가하는 후크를 통해 Windows 클립보드, 스크린샷 캡처, 프린터 및 모바일 장치 액세스를 제어합니다. 프로세스에 후크를 추가하지 않으면 이러한 장치 액세스를 제어할 수 없습니다.

참고
macOS에서는 액세스 제어에서 프로세스를 제외하는 기능이 지원되지 않습니다. 이는 적용되는 보호 계획에 제외 프로세스 목록이 구성된 경우 무시됩니다.

제외 항목 페이지에서 후크를 추가하지 않을 프로세스 목록을 지정할 수 있습니다. 이렇게 하면 해당 프로세스에는 클립보드(로컬 및 리디렉션 클립보드), 스크린샷 캡처, 프린터 및 모바일 장치 액세스 제어가 적용되지 않습니다.

프린터 액세스를 거부하는 보호 계획을 적용한 후 Microsoft Word 응용 프로그램을 시작하는 경우를 예로 들어 보겠습니다. 이 경우 해당 응용 프로그램에서 시도하는 인쇄는 차단됩니다. 그러나 제외 항목 목록에 Microsoft Word 프로세스를 추가하면 응용 프로그램에 후크가 추가되지 않습니다. 따라서 Microsoft Word에서 시도하는 인쇄는 차단되지 않습니다. 그러나 다른 응용 프로그램에서 수행하는 인쇄는 계속 차단됩니다.

제외 항목에 프로세스를 추가하려면

© Acronis International GmbH, 2003-2024

1. 편집을 위해 장치에 대한 보호 계획을 엽니다.
   보호 계획 이름 옆에 있는 말줄임표(...)를 클릭한 다음 **편집**을 클릭합니다.

   참고
   장치 제어 설정에 액세스할 수 있도록 계획에서 장치 제어를 활성화해야 합니다.

2. **장치 제어** 스위치 옆의 화살표 아이콘을 클릭하여 설정을 확장한 다음 **제외 항목** 행을 클릭합니다.
3. **제외 항목** 페이지의 **프로세스 및 폴더** 행에서 **+추가**를 클릭합니다.
4. 액세스 제어에서 제외할 프로세스를 추가합니다.
   예를 들어 `C:\Folder\subfolder\process.exe`를 추가할 수 있습니다.
   와일드카드를 사용할 수 있습니다.
   - *는 수에 관계없이 모든 문자 대신 입력할 수 있습니다.
   - 문자 하나를 와일카드로 지정하려면 ?를 사용합니다.

   예:

   ```
   C:\Folder\*
   *\Folder\SubFolder?\*
   *\process.exe
   ```
5. 확인 표시를 클릭하고 **완료**를 클릭합니다.
6. 보호 계획에서 **저장**을 클릭합니다.
7. 제외한 프로세스를 다시 시작하여 후크가 정상적으로 제거되었는지를 확인합니다.

제외된 프로세스는 장치의 액세스 설정에 관계없이 클립보드, 스크린샷 캡처, 프린터, 모바일 장치에 액세스할 수 있습니다.

제외 항목에서 프로세스를 제거하려면

편집을 위해 장치에 대한 보호 계획을 엽니다.

보호 계획 이름 옆에 있는 말줄임표(...)를 클릭한 다음 **편집**을 클릭합니다.

참고
장치 제어 설정에 액세스할 수 있도록 계획에서 장치 제어를 활성화해야 합니다.

1. **장치 제어** 스위치 옆의 화살표 아이콘을 클릭하여 설정을 확장한 다음 **제외 항목** 행을 클릭합니다.
2. **제외 항목** 페이지에서 제외 항목에서 제거할 프로세스 옆의 휴지통 아이콘을 클릭합니다.
3. **완료**를 클릭합니다.
4. 보호 계획에서 **저장**을 클릭합니다.
5. 프로세스를 다시 시작하여 후크가 정상적으로 추가되었는지를 확인합니다.

제외 항목에서 제거한 프로세스에는 보호 계획의 액세스 설정이 적용됩니다.

제외 항목에서 프로세스를 편집하려면

© Acronis International GmbH, 2003-2024

1. 편집을 위해 장치에 대한 보호 계획을 엽니다.
   보호 계획 이름 옆에 있는 말줄임표(...)를 클릭한 다음 **편집**을 클릭합니다.

   참고
   장치 제어 설정에 액세스할 수 있도록 계획에서 장치 제어를 활성화해야 합니다.

2. **장치 제어** 스위치 옆의 화살표 아이콘을 클릭하여 설정을 확장한 다음 **제외 항목** 행을 클릭합니다.
3. **제외 항목** 페이지에서 편집할 프로세스 옆의 **편집** 아이콘을 클릭합니다.
4. 변경 내용을 적용하고 확인 표시를 클릭하여 변경을 확인합니다.
5. **완료**를 클릭합니다.
6. 보호 계획에서 **저장**을 클릭합니다.
7. 편집한 프로세스를 다시 시작하여 변경 내용이 정확하게 적용되었는지 확인합니다.

장치 제어 경보

장치 제어 기능은 제어되는 장치 유형, 포트 또는 인터페이스에 대한 사용자의 액세스 시도를 추적하는 방식으로 이벤트 로그를 유지보수합니다. 특정 이벤트가 발생하면 경보가 발생할 수 있습니다. 이러한 경보는 Cyber Protect 콘솔에 로깅됩니다. 예를 들어 이동식 장치 사용을 차단하는 장치 제어 모듈을 구성할 수 있습니다. 이 경우 사용자가 이러한 장치에/장치에서 데이터 복사를 시도할 때마다 경보가 로깅됩니다.

장치 제어 모듈을 구성할 때 각 장치 유형(스크린샷 캡처는 제외)이나 포트 아래에 나열되는 대다수 항목에 대해 경보를 활성화할 수 있습니다. 경보를 활성화하면 사용자가 허용되지 않는 작업 수행을 시도할 때마다 경보가 생성됩니다. 예를 들어 이동식 장치에 읽기 전용으로만 액세스할 수 있는 상태에서 해당 장치 유형에 대해 **경보 보이기** 옵션을 선택하면 보호된 컴퓨터의 사용자가 이동식 장치에 데이터를 복사하려고 할 때마다 경보가 생성됩니다.

Cyber Protect 콘솔에서 경보를 확인하려면 **모니터링** > **경보**로 이동합니다. 콘솔에 표시되는 각 장치 제어 경보 내에서는 개별 이벤트와 관련된 다음 정보가 제공됩니다.

- **유형** - "경고"가 표시됩니다.
- **상태** - "주변 장치 액세스가 차단됨"이 표시됩니다.
- **메시지** - "'<컴퓨터 이름>'의 <장치 유형 또는 포트>' 액세스가 차단되었습니다."가 표시됩니다. 예를 들어 "'accountant-pc'의 '이동식 장치' 액세스가 차단되었습니다."와 같은 메시지가 표시될 수 있습니다.
- **날짜 및 시간** - 이벤트가 발생한 날짜 및 시간이 표시됩니다.
- **장치** - 이벤트가 발생한 컴퓨터의 이름이 표시됩니다.
- **계획 이름** - 이벤트를 발생시킨 보호 계획의 이름이 표시됩니다.
- **소스** - 이벤트와 관련된 장치 유형 또는 포트가 표시됩니다. 예를 들어 사용자의 이동식 장치 액세스 시도 거부 이벤트에서는 이 필드에 "이동식 장치"가 표시됩니다.
- **작업** - 이벤트의 원인이 된 작업이 표시됩니다. 예를 들어 사용자가 장치에 데이터를 쓰려는 시도 거부 이벤트에서는 이 필드에 "쓰기"가 표시됩니다. 자세한 내용은 작업 필드 값을 참조하십시오.

© Acronis International GmbH, 2003-2024

- **이름** - 이벤트 대상 개체의 이름이 표시됩니다. 예를 들어 사용자가 복사하려 했던 파일, 사용하려 했던 장치 등이 표시됩니다. 대상 개체를 확인할 수 없으면 아무 내용도 표시되지 않습니다.
- **정보** - 이벤트 대상 장치 관련 추가 정보가 표시됩니다. 예를 들어 USB 장치의 경우 장치 ID가 표시됩니다. 대상 장치 관련 추가 정보를 사용할 수 없으면 아무 내용도 표시되지 않습니다.
- **사용자** - 이벤트 발생의 원인이 된 사용자의 이름이 표시됩니다.
- **프로세스** - 이벤트 발생의 원인이 된 애플리케이션 실행 파일의 정규화된 경로가 표시됩니다. 경로 대신 프로세스 이름이 표시되는 경우도 있습니다. 프로세스 정보를 사용할 수 없으면 아무 내용도 표시되지 않습니다.

이동식 장치와 암호화된 이동식 장치를 비롯한 USB 장치에 적용되는 경보가 발생하는 경우 관리자는 해당 경보에서 직접 허용 목록에 장치를 추가할 수 있습니다. 그러면 장치 제어 모듈이 해당 특정 장치에 대한 액세스를 제한하지 않습니다. **이 USB 장치 허용**을 클릭하면 장치 제어 모듈 구성의 USB 장치 허용 목록에 해당 장치가 추가됩니다. 그리고 나중에 참조할 수 있도록 USB 장치 데이터베이스에도 장치가 추가됩니다.

장치 제어 경보를 확인하는 방법도 참조하십시오.

작업 필드 값

경보 **작업** 필드에는 다음 값이 포함될 수 있습니다.

- **읽기** - 장치나 포트에서 데이터를 가져옵니다.
- **쓰기** - 장치나 포트로 데이터를 보냅니다.
- **형식** - 포맷, 디스크 확인 등의 작업을 위해 장치에 직접 액세스합니다. 포트의 경우에는 해당 포트에 연결된 장치에 값이 적용됩니다.
- **꺼내기** - 시스템에서 장치를 제거하거나 장치에서 미디어를 꺼냅니다. 포트의 경우에는 해당 포트에 연결된 장치에 값이 적용됩니다.
- **인쇄** - 프린터로 문서를 보냅니다.
- **오디오 복사** - 로컬 클립보드를 통해 오디오 데이터 복사/붙여넣기를 수행합니다.
- **파일 복사** - 로컬 클립보드를 통해 파일 복사/붙여넣기를 수행합니다.
- **이미지 복사** - 로컬 클립보드를 통해 이미지 복사/붙여넣기를 수행합니다.
- **텍스트 복사** - 로컬 클립보드를 통해 텍스트 복사/붙여넣기를 수행합니다.
- **알 수 없는 내용 복사** - 로컬 클립보드를 통해 기타 데이터 복사/붙여넣기를 수행합니다.
- **RTF 데이터(이미지) 복사** - 서식 있는 텍스트 형식을 사용하여 로컬 클립보드를 통해 이미지 복사/붙여넣기를 수행합니다.
- **RTF 데이터(이미지) 복사** - 서식 있는 텍스트 형식을 사용하여 로컬 클립보드를 통해 파일 복사/붙여넣기를 수행합니다.
- **RTF 데이터(텍스트, 이미지) 복사** - 서식 있는 텍스트 형식을 사용하여 로컬 클립보드를 통해 이미지와 텍스트 복사/붙여넣기를 수행합니다.
- **RTF 데이터(텍스트, 파일) 복사** - 서식 있는 텍스트 형식을 사용하여 로컬 클립보드를 통해 파일과 텍스트 복사/붙여넣기를 수행합니다.
- **RTF 데이터(이미지, 파일) 복사** - 서식 있는 텍스트 형식을 사용하여 로컬 클립보드를 통해 파일과 이미지 복사/붙여넣기를 수행합니다.

© Acronis International GmbH, 2003-2024

- **RTF 데이터(텍스트, 이미지, 파일) 복사** - 서식 있는 텍스트 형식을 사용하여 로컬 클립보드를 통해 파일, 이미지 및 텍스트 복사/붙여넣기를 수행합니다.
- **삭제** - 이동식 장치, 모바일 장치 등의 장치에서 데이터를 삭제합니다.
- **장치 액세스** - Bluetooth 장치, USB 포트 등의 장치나 포트에 액세스합니다.
- **들어오는 오디오** - 리디렉션 클립보드를 통해 클라이언트 컴퓨터에서 호스팅된 세션으로 오디오 데이터 복사/붙여넣기를 수행합니다.
- **들어오는 파일** - 리디렉션 클립보드를 통해 클라이언트 컴퓨터에서 호스팅된 세션으로 파일 복사/붙여넣기를 수행합니다.
- **들어오는 이미지** - 리디렉션 클립보드를 통해 클라이언트 컴퓨터에서 호스팅된 세션으로 이미지 복사/붙여넣기를 수행합니다.
- **들어오는 텍스트** - 리디렉션 클립보드를 통해 클라이언트 컴퓨터에서 호스팅된 세션으로 텍스트 복사/붙여넣기를 수행합니다.
- **들어오는 알 수 없는 내용** - 리디렉션 클립보드를 통해 클라이언트 컴퓨터에서 호스팅된 세션으로 기타 데이터 복사/붙여넣기를 수행합니다.
- **들어오는 RTF 데이터(이미지)** - 서식 있는 텍스트 형식을 사용하여 리디렉션 클립보드를 통해 클라이언트 컴퓨터에서 호스팅된 세션으로 이미지 복사/붙여넣기를 수행합니다.
- **들어오는 RTF 데이터(파일)** - 서식 있는 텍스트 형식을 사용하여 리디렉션 클립보드를 통해 클라이언트 컴퓨터에서 호스팅된 세션으로 파일 복사/붙여넣기를 수행합니다.
- **들어오는 RTF 데이터(텍스트, 이미지)** - 서식 있는 텍스트 형식을 사용하여 리디렉션 클립보드를 통해 클라이언트 컴퓨터에서 호스팅된 세션으로 이미지와 텍스트 복사/붙여넣기를 수행합니다.
- **들어오는 RTF 데이터(텍스트, 파일)** - 서식 있는 텍스트 형식을 사용하여 리디렉션 클립보드를 통해 클라이언트 컴퓨터에서 호스팅된 세션으로 파일과 텍스트 복사/붙여넣기를 수행합니다.
- **들어오는 RTF 데이터(이미지, 파일)** - 서식 있는 텍스트 형식을 사용하여 리디렉션 클립보드를 통해 클라이언트 컴퓨터에서 호스팅된 세션으로 파일과 이미지 복사/붙여넣기를 수행합니다.
- **들어오는 RTF 데이터(텍스트, 이미지, 파일)** - 서식 있는 텍스트 형식을 사용하여 리디렉션 클립보드를 통해 클라이언트 컴퓨터에서 호스팅된 세션으로 이미지, 파일 및 텍스트 복사/붙여넣기를 수행합니다.
- **삽입** - USB 장치 또는 FireWire 장치를 연결합니다.
- **나가는 오디오** - 리디렉션 클립보드를 통해 호스팅된 세션에서 클라이언트 컴퓨터로 오디오 데이터 복사/붙여넣기를 수행합니다.
- **나가는 파일** - 리디렉션 클립보드를 통해 호스팅된 세션에서 클라이언트 컴퓨터로 파일 복사/붙여넣기를 수행합니다.
- **나가는 이미지** - 리디렉션 클립보드를 통해 호스팅된 세션에서 클라이언트 컴퓨터로 이미지 복사/붙여넣기를 수행합니다.
- **나가는 텍스트** - 리디렉션 클립보드를 통해 호스팅된 세션에서 클라이언트 컴퓨터로 텍스트 복사/붙여넣기를 수행합니다.
- **나가는 알 수 없는 내용** - 리디렉션 클립보드를 통해 호스팅된 세션에서 클라이언트 컴퓨터로 기타 데이터 복사/붙여넣기를 수행합니다.
- **나가는 RTF 데이터(이미지)** - 서식 있는 텍스트 형식을 사용하여 리디렉션 클립보드를 통해 호스팅된 세션에서 클라이언트 컴퓨터로 이미지 복사/붙여넣기를 수행합니다.

© Acronis International GmbH, 2003-2024

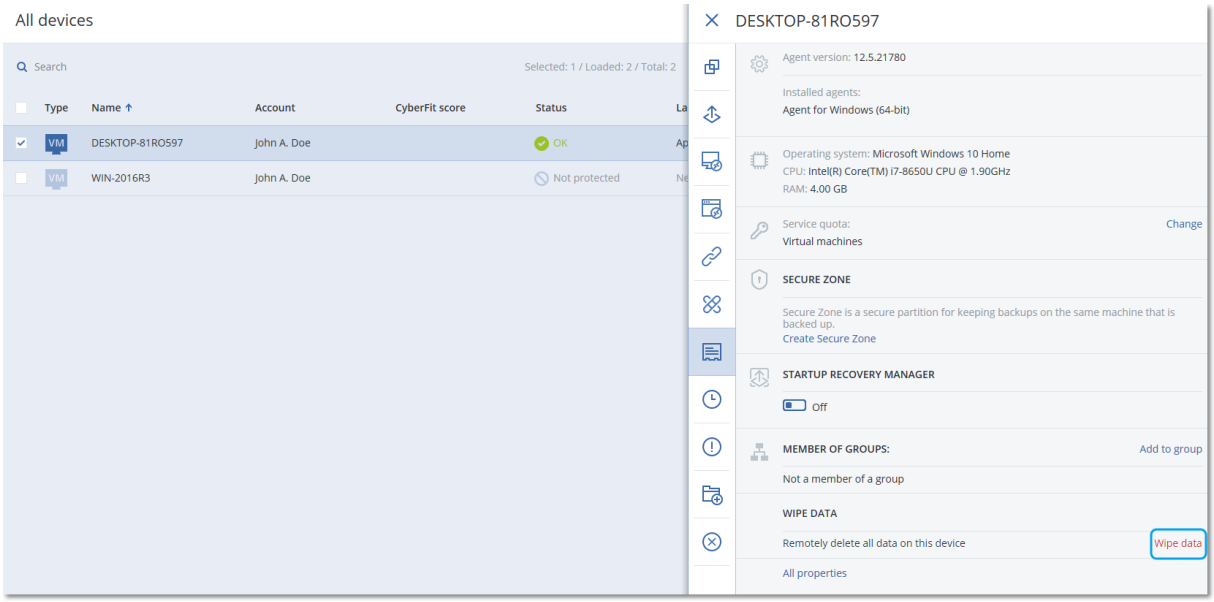
- **나가는 RTF 데이터(파일)** - 서식 있는 텍스트 형식을 사용하여 리디렉션 클립보드를 통해 호스팅된 세션에서 클라이언트 컴퓨터로 파일 복사/붙여넣기를 수행합니다.
- **나가는 RTF 데이터(텍스트, 이미지)** - 서식 있는 텍스트 형식을 사용하여 리디렉션 클립보드를 통해 호스팅된 세션에서 클라이언트 컴퓨터로 이미지와 텍스트 복사/붙여넣기를 수행합니다.
- **나가는 RTF 데이터(텍스트, 파일)** - 서식 있는 텍스트 형식을 사용하여 리디렉션 클립보드를 통해 호스팅된 세션에서 클라이언트 컴퓨터로 파일과 텍스트 복사/붙여넣기를 수행합니다.
- **나가는 RTF 데이터(이미지, 파일)** - 서식 있는 텍스트 형식을 사용하여 리디렉션 클립보드를 통해 호스팅된 세션에서 클라이언트 컴퓨터로 파일과 이미지 복사/붙여넣기를 수행합니다.
- **나가는 RTF 데이터(텍스트, 이미지, 파일)** - 서식 있는 텍스트 형식을 사용하여 리디렉션 클립보드를 통해 호스팅된 세션에서 클라이언트 컴퓨터로 이미지, 파일 및 텍스트 복사/붙여넣기를 수행합니다.
- **이름 변경** - 이동식 장치, 모바일 장치 등의 장치에서 파일 이름을 변경합니다.

관리 대상 워크로드에서 데이터 소거

참고
원격 지우기 기능은 Advanced Security 팩에서 제공됩니다.

머신을 분실 또는 도난당한 경우, Cyber Protection 서비스 관리자 및 머신 소유자는 원격 지우기를 통해 관리 대상 머신에서 데이터를 삭제할 수 있습니다. 이를 통해 민감한 정보에 대한 무단 액세스를 방지할 수 있습니다.

원격 지우기는 Windows 10 이상을 실행 중인 머신에서만 사용할 수 있습니다. 지우기 명령을 수신하려면 머신이 켜져 있고, 인터넷에 연결된 상태여야 합니다.



머신에서 데이터를 지우려면

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 데이터를 지우려는 머신을 선택합니다.

© Acronis International GmbH, 2003-2024

참고
한 번에 하나의 머신에서만 데이터를 지울 수 있습니다.

3. **상세 정보**를 클릭한 다음, **데이터 지우기**를 클릭합니다.
   선택한 머신이 오프라인이면 **데이터 지우기** 옵션에 액세스할 수 없습니다.
4. 선택 내용을 확인합니다.
5. 이 머신의 로컬 관리자의 자격 증명을 입력한 다음, **데이터 지우기**를 클릭합니다.

참고
소거 프로세스와 이 프로세스를 시작한 사람에 관한 상세 정보를 **모니터링** > **활동**에서 확인할 수 있습니다.

CyberApp 워크로드

ISV(독립 소프트웨어 공급 업체)에서 생성하는 CyberApp 워크로드는 CyberApp 통합을 활성화하고 나면 Cyber Protect 콘솔에 표시됩니다. 다음 조건이 동시에 충족되어야 합니다.

- CyberApp에서 **워크로드 및 작업** 확장 지점이 활성화되어 있어야 합니다.
- CyberApp에 **워크로드 유형**이 하나 이상 정의되어 있어야 합니다.
- ISV에서 호스트하는 커넥터 서비스가 Acronis 플랫폼에 CyberApp 워크로드를 추가했으며 업데이트했음을 확인해야 합니다.

공급 업체 포털 관련 정보와 CyberApp 생성 방법에 대한 자세한 내용은 공급 업체 포털 사용자 안내서를 참조하십시오.

집계된 워크로드

실제 워크로드에는 Cyber Protect 에이전트와 CyberApp 에이전트 하나 이상이 동시에 설치되어 있을 수도 있습니다. 이 경우 **모든 장치** 화면에 같은 워크로드가 여러 번 표시됩니다. Acronis 워크로드와 각 CyberApp 워크로드의 레코드가 별도로 표시되기 때문입니다. 공급 업체 포털이나 Cyber Protect 콘솔에서 워크로드 자동 병합을 활성화 및 구성하면 시스템이 Acronis 워크로드와 CyberApp 워크로드의 호스트 주소 및 MAC 주소를 비교한 후 표시된 모든 워크로드를 집계된 워크로드 하나로 병합합니다. Cyber Protect 콘솔에서 워크로드를 수동으로 병합하고 병합을 취소할 수도 있습니다.

CyberApp 워크로드 사용

Cyber Protect 콘솔에서 기본 제공되는 표준 작업 외에 CyberApp 워크로드가 콘솔에 표시되고 나면 사용 가능해지는 작업도 수행할 수 있습니다. 예를 들어 워크로드를 집계된 워크로드에 수동으로 병합할 수도 있고, CyberApp에 구성되어 있는 사용자 정의 작업을 수행할 수도 있습니다.

병합

© Acronis International GmbH, 2003-2024

사전 요구 사항

- 테넌트에서 여러 소스의 워크로드를 사용할 수 있어야 합니다.

CyberApp 워크로드가 하나 이상 포함된 Acronis 워크로드를 집계된 워크로드 하나로 수동 병합할 수 있습니다.

워크로드를 집계된 워크로드로 수동 병합하려면

1. **모든 장치** 화면에서 병합할 워크로드를 선택합니다.

   참고
   Acronis 워크로드와 CyberApp 워크로드 등 여러 소스의 워크로드를 선택하면 병합 작업이 표시됩니다.

2. **워크로드 병합**을 클릭합니다.

사용자 정의 작업 수행

사전 요구 사항

- 테넌트에서 **워크로드 작업**이 정의된 CyberApp 통합이 활성화되어 있어야 합니다.

CyberApp에 구성되어 있는 작업인 사용자 정의 작업은 테넌트에서 CyberApp 통합을 활성화할 때 해당 CyberApp 워크로드에 사용 가능한 상태가 됩니다.

사용자 정의 작업을 수행하려면

1. **모든 장치** 화면에서 워크로드를 클릭합니다.
2. **통합 앱 작업**을 클릭합니다.
3. 작업을 클릭합니다.

집계된 워크로드 사용

집계된 워크로드에서는 Cyber Protect 콘솔에서 기본 제공되는 표준 작업 외에도 상세 정보 확인, 소스 워크로드 병합 취소 등의 작업을 수행할 수 있으며 CyberApp에 구성된 사용자 정의 작업도 수행할 수 있습니다.

상세 정보 보기

사전 요구 사항

- 테넌트용으로 집계된 워크로드를 하나 이상 사용할 수 있어야 합니다.

집계된 워크로드 상세 정보를 확인하려면

1. **모든 장치** 화면에서 집계된 워크로드를 클릭합니다.
2. **상세정보**를 클릭합니다.
   집계된 워크로드의 상세 정보가 각 탭별로 표시됩니다. 표시된 각 워크로드의 상세 정보가 각 탭에 표시됩니다.

© Acronis International GmbH, 2003-2024

병합 취소

사전 요구 사항

- 테넌트용으로 집계된 워크로드를 하나 이상 사용할 수 있어야 합니다.

집계된 워크로드의 병합을 취소하면 장치 목록에 해당 워크로드가 더 이상 표시되지 않습니다. 대신 집계 워크로드에 병합된 각 소스 워크로드에 해당하는 개별 항목이 표시됩니다.

집계된 워크로드의 병합을 취소하려면

1. **모든 장치** 화면에서 병합을 취소할 집계된 워크로드를 클릭합니다.
2. **소스 워크로드 병합 취소**를 클릭합니다.
3. 확인 창에서 **병합 취소**를 클릭합니다.

사용자 정의 작업 수행

사전 요구 사항

- 테넌트에서 **워크로드 작업**이 정의된 CyberApp 통합이 하나 이상 활성화되어 있어야 합니다.

CyberApp에 구성되어 있는 작업인 사용자 정의 작업은 테넌트에서 CyberApp 통합을 활성화할 때 해당 CyberApp 워크로드에 사용 가능한 상태가 됩니다.

사용자 정의 작업을 수행하려면

1. **모든 장치** 화면에서 워크로드를 클릭합니다.
2. **통합 앱 작업**을 클릭합니다.
3. 사용 가능한 사용자 정의 작업에 따라 다음 중 하나를 수행합니다.
   - 집계 워크로드의 CyberApp 워크로드가 하나이면 해당 작업을 클릭합니다.
   - 집계 워크로드의 CyberApp 워크로드가 여러 개이면 CyberApp의 이름을 클릭한 후에 작업을 클릭합니다.

마지막으로 로그인한 사용자 찾기

장치를 관리하려는 관리자는 장치에 현재 로그인되어 있는 사용자와 이전에 로그인했던 사용자를 파악해야 합니다. 이 정보는 대시보드나 워크로드 상세 정보에 표시됩니다.

원격 관리 계획에서 마지막 로그인 정보 표시를 활성화하거나 비활성화할 수 있습니다.

대시보드에서:

1. **장치**를 클릭합니다. **모든 장치** 창이 표시됩니다.
2. 각 장치에 마지막으로 로그인했던 사용자의 이름이 **마지막 로그인** 열에 표시됩니다.
3. **마지막 로그인 시간** 열에는 사용자가 각 장치에 마지막으로 로그인한 시간이 표시됩니다.

장치 상세 정보에서:

1. **장치**를 클릭합니다. **모든 장치** 창이 표시됩니다.
2. 상세 정보를 확인할 장치를 클릭합니다.

© Acronis International GmbH, 2003-2024

3. **상세 정보** 아이콘을 클릭합니다. 사용자의 이름, 그리고 선택한 장치에 마지막으로 로그인한 날짜와 시간이 **마지막 사용자 로그인** 섹션에 표시됩니다.

참고
마지막 사용자 로그인 섹션에는 장치에 로그인했던 사용자가 5명까지 표시됩니다.

대시보드에서 마지막 로그인 및 마지막 로그인 시간 열을 표시하거나 숨기는 방법

1. **장치**를 클릭합니다. **모든 장치** 창이 표시됩니다.
2. 오른쪽 상단 모서리의 기어 아이콘을 클릭하고 **일반** 섹션에서 다음 작업 중 하나를 수행합니다.
   - 대시보드에서 **마지막 로그인** 및 **마지막 로그인 시간** 열을 표시하려면 해당 열을 활성화합니다.
   - 대시보드에서 **마지막 로그인** 및 **마지막 로그인 시간** 열을 숨기려면 해당 열을 비활성화합니다.

© Acronis International GmbH, 2003-2024

워크로드와 파일의 백업 및 복구 관리

백업 모듈을 통해 실제 머신 및 가상 머신, 파일과 데이터베이스를 로컬 또는 클라우드 스토리지에 백업 및 복구할 수 있습니다.

백업

백업 모듈이 활성화된 보호 계획은 지정된 데이터를 지정된 머신에서 보호하는 방법에 대한 규칙 세트입니다.

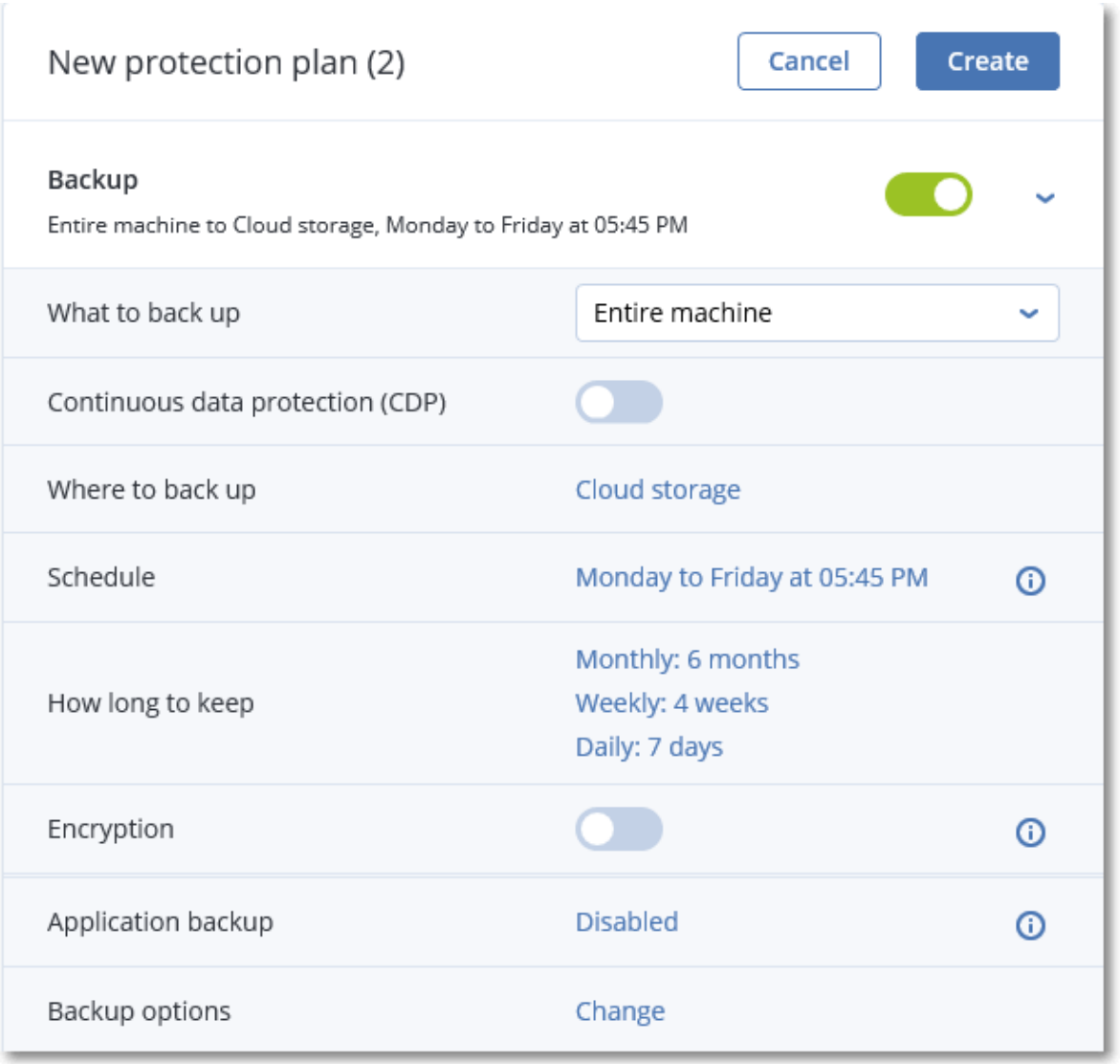
보호 계획은 생성 시 또는 이후에 여러 머신에 적용할 수 있습니다.

처음으로 백업 모듈이 활성화된 보호 계획을 생성하려면

1. 백업하려는 머신을 선택합니다.
2. **보호**를 클릭합니다.

   머신에 적용된 보호 계획이 표시됩니다. 머신에 할당된 계획이 없는 경우 적용 가능한 기본 보호 계획이 표시됩니다. 필요한 대로 설정을 조정하고, 이 계획을 적용하거나 새로운 계획을 생성할 수 있습니다.
3. 새 계획을 만들려면 **계획 생성**을 클릭합니다. **백업** 모듈을 활성화하고 설정을 언롤합니다.

© Acronis International GmbH, 2003-2024



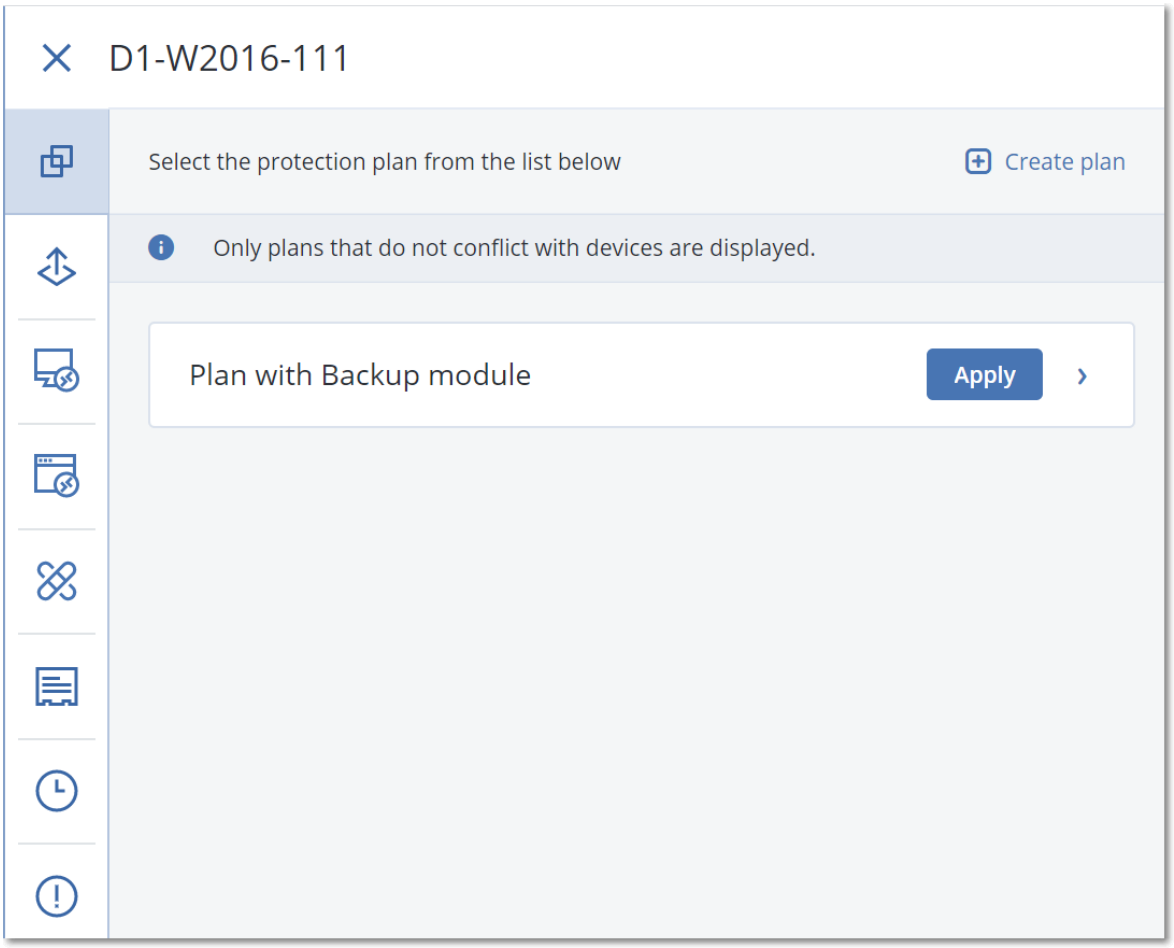
4. [선택 사항] 보호 계획 이름을 수정하려면 기본 이름을 클릭합니다.
5. [선택 사항] 백업 모듈 매개변수를 수정하려면 보호 계획 패널의 해당 섹션을 클릭합니다.
6. [선택 사항] 백업 옵션을 수정하려면 **백업 옵션** 옆에 있는 **변경**을 클릭합니다.
7. **생성**을 클릭합니다.

기존 보호 계획을 적용하려면

1. 백업하려는 머신을 선택합니다.
2. **보호**를 클릭합니다. 선택한 머신에 이미 공통 보호 계획이 적용되어 있는 경우 **계획 추가**를 클릭합니다.

   소프트웨어에 이전에 생성한 보호 계획이 표시됩니다.

© Acronis International GmbH, 2003-2024



3. 적용할 보호 계획을 선택합니다.
4. **적용**을 클릭합니다.

보호 계획 치트 시트

다음 표는 사용 가능한 보호 계획 매개변수를 요약해서 보여줍니다. 이 표를 사용하여 필요에 가장 잘 맞는 보호 계획을 생성할 수 있습니다.

백업할 대상	백업할 항목 선택 방법	백업할 위치	예약 백업 구성표	보관 기간
디스크/볼륨(실제 머신[1])	직접 선택 정책 규칙	클라우드 로컬 폴더	항상 증분 (단일 파일) 항상 전체 매주 전체, 매일 증분	백업 기간별(단일 규칙/백업 세트당) 백업 수별 백업의 총 크기 기

[1]운영 체제에 설치된 에이전트에 의해 백업된 머신.

© Acronis International GmbH, 2003-2024

	파일 필터	네트워크 폴더 NFS* Secure Zone**	매월 전체, 매주 차등, 매일 증분(GFS) 사용자 정의(F-D-I)	준*** 무기한 보관
디스크/볼륨(가상 머신[1])	정책 규칙 파일 필터	클라우드 로컬 폴더 네트워크 폴더 NFS*		
파일(실제 머신에만 해당[2])	직접 선택 정책 규칙 파일 필터	클라우드 로컬 폴더 네트워크 폴더 NFS* Secure Zone**	항상 증분(단일 파일) 항상 전체 매주 전체, 매일 증분 매월 전체, 매주 차등, 매일 증분(GFS) 사용자 정의(F-D-I)	
ESXi 구성	직접 선택	로컬 폴더 네트워크 폴더 NFS*		
웹사이트(파일 및 MySQL 데이터베이스)	직접 선택	클라우드	—	

[1]Agent for VMware 또는 Agent for Hyper-V와 같은 외부 에이전트에 의해 하이퍼바이저 수준에서 백업된 가상 머신입니다. 에이전트를 내부에 포함하고 있으며 백업 관점에서 실제 머신으로 처리되는 가상 머신입니다.
[2]운영 체제에 설치된 에이전트에 의해 백업된 머신.

© Acronis International GmbH, 2003-2024

<table>
<tr><td colspan="2">시스템 상태</td><td rowspan="3">직접 선택</td><td rowspan="3">클라우드
로컬 폴더
네트워크 폴더</td><td rowspan="3">항상 전체
매주 전체, 매일 증분
사용자 정의(F-I)
항상 증분(단일 파일) - SQL 데이터베이스에만 해당</td><td rowspan="3"></td></tr>
<tr><td colspan="2">SQL 데이터베이스</td></tr>
<tr><td colspan="2">Exchange 데이터베이스</td></tr>
<tr><td rowspan="6">Microsoft 365</td><td rowspan="2">사서함
(로컬 Agent for Microsoft 365)</td><td rowspan="2">직접 선택</td><td rowspan="2">로컬 폴더
네트워크 폴더</td><td rowspan="2">항상 증분 (단일 파일)</td></tr>
<tr><td rowspan="5">사서함
(클라우드 Agent for Microsoft 365)</td><td rowspan="5">직접 선택</td><td rowspan="5">클라우드</td><td rowspan="5">매일 백업 최대 6개</td></tr>
<tr><td>공용 폴더</td></tr>
<tr><td>Teams</td></tr>
<tr><td>OneDrive 파일</td><td>직접 선택</td></tr>
<tr><td>SharePoint 온라인 데이터</td><td>정책 규칙</td></tr>
<tr><td rowspan="3">Google Workspace</td><td>Gmail 사서함</td><td>직접 선택</td><td rowspan="3">클라우드</td><td rowspan="3">매일 백업 최대 6개</td></tr>
<tr><td>Google Drive 파일</td><td>직접 선택</td></tr>
<tr><td>Shared Drive 파일</td><td>정책 규칙</td></tr>
</table>

* NFS 공유로의 백업은 Windows에서 사용할 수 없습니다.

** Secure Zone은 Mac에서 생성할 수 없습니다.

*** **백업의 총 크기 기준** 보관 규칙은 **항상 증분(단일 파일)** 백업 구성표와 함께 사용하거나 클라우드 스토리지에 백업할 경우 사용할 수 없습니다.

백업할 데이터 선택

전체 머신 선택

전체 머신의 백업은 머신의 제거할 수 없는 모든 디스크 백업입니다. 데이터 백업에 대한 자세한 내용은 "디스크 또는 볼륨 선택"(366페이지)을(를) 참조하십시오.

© Acronis International GmbH, 2003-2024

제한 사항

- 잠금 상태의 암호화 APFS 볼륨에서는 디스크 수준 백업이 지원되지 않습니다. 전체 머신의 백업 중에는 이러한 볼륨을 건너뜁니다.
- OneDrive 루트 폴더는 백업 작업에서 기본적으로 제외됩니다. 특정 OneDrive 파일 및 폴더를 백업하도록 선택하는 경우 이러한 항목만 백업됩니다. 장치에서 사용할 수 없는 파일에는 백업 세트에서 유효하지 않은 내용이 포함됩니다.

디스크 또는 볼륨 선택

디스크 수준 백업에는 디스크 또는 볼륨의 사본이 패키지 형태로 들어 있습니다. 디스크 수준 백업에서는 개별 디스크, 볼륨, 폴더 및 파일을 복구할 수 있습니다.

보호 계획에 포함된 각 워크로드에서 백업할 디스크 또는 볼륨을 직접 선택할 수도 있고 여러 워크로드용 정책 규칙을 구성할 수도 있습니다. 또한 파일 필터를 구성하여 백업에서 특정 파일을 제외하거나 특정 파일만 백업에 포함할 수도 있습니다. 자세한 내용은 "파일 필터(포함/제외)"(419페이지)을(를) 참조하십시오.

디스크 또는 볼륨을 선택하려면

직접 선택

직접 선택은 실제 머신의 경우에만 사용할 수 있습니다.

1. **백업 대상**에서 **디스크/볼륨**을 선택합니다.
2. **백업할 항목**을 클릭합니다.
3. **백업할 항목 선택**에서 **직접**을 선택합니다.
4. 보호 계획에 포함된 각 워크로드에서 백업할 디스크 또는 볼륨 옆에 있는 확인란을 선택합니다.
5. **완료**를 클릭합니다.

정책 규칙 사용

1. **백업 대상**에서 **디스크/볼륨**을 선택합니다.
2. **백업할 항목**을 클릭합니다.
3. **백업할 항목 선택**에서 **정책 규칙 사용**을 선택합니다.
4. 사전 정의된 규칙 중 하나를 선택하거나, 자체 규칙을 입력하거나 두 가지 방법을 함께 사용합니다.

   사용 가능한 정책 규칙에 대한 자세한 내용은 "디스크 및 볼륨용 정책 규칙"(368페이지) 항목을 참조하십시오.

   정책 규칙은 보호 계획에 포함된 모든 워크로드에 적용됩니다.

   지정된 규칙 중 워크로드에 적용 가능한 규칙이 없으면 해당 워크로드의 백업은 실패합니다.
5. **완료**를 클릭합니다.

© Acronis International GmbH, 2003-2024

제한 사항

- 잠금 상태의 암호화 APFS 볼륨에서는 디스크 수준 백업이 지원되지 않습니다. 전체 머신의 백업 중에는 이러한 볼륨을 건너뜁니다.
- OneDrive 루트 폴더는 백업 작업에서 기본적으로 제외됩니다. 특정 OneDrive 파일 및 폴더를 백업하도록 선택하는 경우 이러한 항목만 백업됩니다. 장치에서 사용할 수 없는 파일에는 백업 세트에서 유효하지 않은 내용이 포함됩니다.
- ISCSI 프로토콜을 통해 실제 머신에 연결된 디스크를 백업할 수 있습니다. 그러나 iSCSI로 연결된 디스크 백업을 위해 Agent for VMware 또는 Agent for Hyper-V를 사용하는 경우에는 제한 사항이 적용됩니다. 자세한 내용은 "제한 사항"(32페이지)을(를) 참조하십시오.

디스크 또는 볼륨 백업은 어떤 항목을 저장합니까?

디스크 또는 볼륨 백업은 운영 체제 부팅에 필요한 모든 정보와 함께 디스크 또는 볼륨 **파일 시스템** 전체를 저장합니다. 해당 백업과 개별 폴더 또는 파일에서 전체 디스크 또는 볼륨을 복구할 수 있습니다.

섹터 단위(원시 모드) 백업 옵션을 활성화하면 디스크 백업 시 모든 디스크 섹터가 저장됩니다. 섹터별 백업은 알 수 없거나 지원되지 않는 파일 시스템 및 기타 독점 데이터 형식을 가진 드라이브를 백업하는 경우 사용할 수 있습니다.

Windows

볼륨 백업은 해당 속성(숨김 파일과 시스템 파일 포함), 부트 레코드, 파일 할당 테이블(FAT)(있는 경우), 마스터 부트 레코드(MBR)가 있는 하드 디스크의 루트 및 제로 트랙과는 별도로 선택된 볼륨의 다른 모든 파일과 폴더를 저장합니다.

디스크 백업은 선택된 디스크의 모든 볼륨(공급업체의 유지보수 파티션과 같은 숨겨진 볼륨 포함)과 마스터 부트 레코드가 있는 제로 트랙을 저장합니다.

다음 항목은 디스크 또는 볼륨 백업(및 파일 수준 백업)에 포함되지 *않습니다*.

- 머신이 최대 절전 모드에 진입할 때 RAM 내용을 보관하는 파일(hiberfil.sys)과 스왑 파일(pagefile.sys). 복구 후에 이 파일이 해당 위치에 0 크기로 다시 생성됩니다.
- 백업이 운영 체제에서 수행되는 경우(부트 가능한 미디어 또는 하이퍼바이저 수준의 가상 머신 백업과 다름):
  - Windows 섀도 스토리지. 해당 경로는 레지스트리 값 **VSS Default Provider**에서 결정됩니다. 이 값은 레지스트리 키 **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup**에서 찾을 수 있습니다. 따라서 Windows Vista로 시작되는 운영 체제에서는 Windows 복원 지점이 백업되지 않습니다.
  - **VSS(Volume Shadow Copy Service)** 백업 옵션이 활성화된 경우 **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** 레지스트리 키에 지정된 파일 및 폴더.

© Acronis International GmbH, 2003-2024

Linux

볼륨 백업은 해당 속성, 부트 레코드 및 파일 시스템 수퍼 블록과는 별도로 선택된 볼륨의 모든 파일과 디렉토리를 저장합니다.

디스크 백업은 마스터 부트 레코드가 있는 제로 트랙뿐 아니라 모든 디스크 볼륨을 저장합니다.

Mac

디스크 또는 볼륨 백업은 선택한 디스크 또는 볼륨의 모든 파일 및 디렉토리와 함께 볼륨 레이아웃의 설명을 저장합니다.

다음 항목은 제외됩니다.

- 파일 시스템 저널 및 Spotlight 색인과 같은 시스템 메타데이터
- 휴지통
- Time Machine 백업

실제로 Mac의 디스크와 볼륨은 파일 수준에 백업됩니다. 디스크 및 볼륨 백업에서 베어 메탈 복구가 가능하지만 섹터 단위 백업 모드를 사용할 수 없습니다.

디스크 및 볼륨용 정책 규칙

백업할 디스크 또는 볼륨을 선택할 때는 보호되는 워크로드의 운영 체제에 따라 다음 정책 규칙을 사용할 수 있습니다.

Windows

- `[All Volumes]` 사용 시에는 머신의 모든 볼륨이 선택됩니다.
- 드라이브 문자(예: `C:\`) 사용 시에는 지정된 드라이브 문자로 표시되는 볼륨이 선택됩니다.
- `[Fixed Volumes (physical machines)]` 사용 시에는 이동식 미디어를 제외한 실제 머신의 모든 볼륨이 선택됩니다. 고정된 볼륨에는 SCSI, ATAPI, ATA, SSA, SAS 및 SATA 장치와 RAID 어레이의 볼륨이 있습니다.
- `[BOOT+SYSTEM]`은 시스템 및 부트 볼륨을 선택합니다. 운영 체제를 복구할 수 있는 최소 조합입니다.
- `[Disk 1]`은 머신의 첫 번째 디스크를 선택합니다(해당 디스크의 모든 볼륨 포함). 다른 디스크를 선택하려면 해당하는 번호를 입력합니다.

Linux

- `[All Volumes]` 사용 시에는 머신에 마운트된 모든 볼륨이 선택됩니다.
- `/dev/hda1`은 첫 번째 IDE 하드 디스크에서 첫 번째 볼륨을 선택합니다.
- `/dev/sda1`은 첫 번째 SCSI 하드 디스크에서 첫 번째 볼륨을 선택합니다.
- `/dev/md1`은 첫 번째 소프트웨어 RAID 하드 디스크를 선택합니다.
- 다른 기본 볼륨을 선택하려면 `/dev/xdyN`을 지정합니다. 여기서 각 문자는 다음과 같습니다.
  - "x"는 디스크 유형에 해당합니다.
  - "y"는 디스크 번호에 해당합니다(첫 번째 디스크의 경우 a, 두 번째 디스크의 경우 b 등).

© Acronis International GmbH, 2003-2024

  - "N"은 볼륨 번호입니다.
- 논리 볼륨을 선택하려면 루트 계정에서 `ls /dev/mapper` 명령을 실행한 후에 표시되도록 그 경로를 지정합니다.

  예:

  ```
  [root@localhost ~]# ls /dev/mapper/
  control vg_1-lv1 vg_1-lv2
  ```

  이 출력은 두 가지 논리 볼륨, `lv1` 및 `lv2`를 표시하며, 이 둘은 볼륨 그룹 `vg_1`에 속합니다. 이러한 볼륨을 백업하려면 다음을 지정합니다.

  `/dev/mapper/vg_1-lv1`

  `/dev/mapper/vg-l-lv2`

macOS

- `[All Volumes]` 사용 시에는 머신에 마운트된 모든 볼륨이 선택됩니다.
- `[Disk 1]`은 머신의 첫 번째 디스크를 선택합니다(해당 디스크의 모든 볼륨 포함). 다른 디스크를 선택하려면 해당하는 번호를 지정합니다.

파일 또는 폴더 선택

특정 데이터(예: 현재 프로젝트의 파일)만 보호하려는 경우에는 파일 수준 백업을 사용합니다. 파일 수준 백업은 디스크 수준 백업보다 크기가 작으므로 스토리지 공간을 절약할 수 있습니다.

중요

파일 수준 백업에서 운영 체제를 복구할 수는 없습니다.

보호 계획에 포함된 각 워크로드에서 백업할 파일과 폴더를 직접 선택할 수도 있고 여러 워크로드용 정책 규칙을 구성할 수도 있습니다. 또한 필터를 구성하여 백업에서 특정 파일을 제외하거나 특정 파일만 백업에 포함할 수도 있습니다. 자세한 내용은 "파일 필터(포함/제외)"(419페이지)을(를) 참조하십시오.

파일 또는 폴더를 선택하려면

직접 선택

1. **백업 대상**에서 **파일/폴더**를 선택합니다.
2. **백업할 항목**에서 **지정**을 클릭합니다.
3. **백업할 항목 선택**에서 **직접**을 선택합니다.
4. 보호 계획에 포함된 각 워크로드에서 백업할 파일과 폴더를 지정합니다.
   a. **파일 및 폴더 선택**을 클릭합니다.
   b. **로컬 폴더** 또는 **네트워크 폴더**를 클릭합니다.

      선택한 머신에서 네트워크 폴더에 액세스할 수 있어야 합니다.

      소스로 **네트워크 폴더**를 선택하면 NetApp 장치 등의 NAS(Network-Attached Storage)에서 데이터를 백업할 수 있습니다. 모든 공급업체의 NAS 장치가 지원됩니다.
   c. 폴더 트리에서 필요한 파일이나 폴더로 이동합니다.

© Acronis International GmbH, 2003-2024

해당 파일이나 폴더 경로를 지정한 후 화살표 버튼을 클릭해도 됩니다.

d. [공유 폴더의 경우] 메시지가 표시되면 공유 폴더 액세스 자격 증명을 지정합니다.
익명 액세스 권한으로 폴더를 백업할 수는 없습니다.

e. 필요한 파일과 폴더를 선택합니다.

f. **완료**를 클릭합니다.

정책 규칙 사용

1. **백업 대상**에서 **파일/폴더**를 선택합니다.
2. **백업할 항목**에서 **지정**을 클릭합니다.
3. **백업할 항목 선택**에서 **정책 규칙 사용**을 선택합니다.
4. 사전 정의된 규칙 중 하나를 선택하거나, 자체 규칙을 입력하거나 두 가지 방법을 함께 사용합니다.
   사용 가능한 정책 규칙에 대한 자세한 내용은 "파일 및 폴더용 정책 규칙"(370페이지) 항목을 참조하십시오.
   정책 규칙은 보호 계획에 포함된 모든 워크로드에 적용됩니다.
   지정된 규칙 중 워크로드에 적용 가능한 규칙이 없으면 해당 워크로드의 백업은 실패합니다.
5. **완료**를 클릭합니다.

제한 사항

- 에이전트가 설치된 실제 머신이나 가상 머신을 백업(에이전트 기반 백업)할 때 파일과 폴더를 선택할 수 있습니다. 비에이전트 모드에서 백업하는 가상 머신에는 파일 수준 백업을 사용할 수 없습니다. 이러한 백업 유형 간의 차이점에 대한 자세한 내용은 "에이전트 기반 백업 및 비에이전트 백업"(61페이지) 항목을 참고하십시오.
- OneDrive 루트 폴더는 백업 작업에서 기본적으로 제외됩니다. 특정 OneDrive 파일 및 폴더를 백업하도록 선택하는 경우 이러한 항목만 백업됩니다. 장치에서 사용할 수 없는 파일에는 백업 세트에서 유효하지 않은 내용이 포함됩니다.
- iSCSI 프로토콜을 통해 실제 머신에 연결된 디스크에 있는 파일과 폴더를 백업할 수 있습니다. iSCSI로 연결된 디스크의 데이터 백업을 위해 Agent for VMware 또는 Agent for Hyper-V를 사용하는 경우에는 몇 가지 제한 사항이 적용됩니다.

파일 및 폴더용 정책 규칙

백업할 파일 또는 폴더를 선택할 때는 보호되는 워크로드의 운영 체제에 따라 다음 정책 규칙을 사용할 수 있습니다.

Windows

- 파일 또는 폴더의 전체 경로입니다. `D:\Work\Text.doc`, `C:\Windows` 등을 예로 들 수 있습니다.
- 사전 정의된 규칙:
  - `[All Files]`는 머신의 모든 볼륨에서 모든 파일을 선택합니다.
  - `[All Profiles Folder]` 사용 시에는 모든 사용자 프로필이 있는 폴더가 선택됩니다. 예를 들어 `C:\Users`, `C:\Documents and Settings` 등이 선택될 수 있습니다.
- 환경 변수:

© Acronis International GmbH, 2003-2024

- %ALLUSERSPROFILE% 사용 시에는 모든 사용자 프로필의 공통 데이터가 포함된 폴더가 선택됩니다. C:\ProgramData, C:\Documents and Settings\All Users 등을 예로 들 수 있습니다.
- %PROGRAMFILES% 사용 시에는 Program Files 폴더가 선택됩니다. C:\Program Files 등을 예로 들 수 있습니다.
- %WINDIR% 사용 시에는 Windows 폴더가 선택됩니다. C:\Windows 등을 예로 들 수 있습니다.

다른 환경 변수 또는 환경 변수와 텍스트의 조합을 사용할 수 있습니다. 예를 들어 Program Files 폴더에 있는 Java 폴더를 선택하려는 경우 %PROGRAMFILES%\Java를 지정합니다.

Linux

- 파일 또는 디렉토리에 대한 전체 경로.

  예를 들어 /home/usr/docs에 마운트된 볼륨 /dev/hda3의 file.txt 파일을 백업하려면 /dev/hda3/file.txt 또는 /home/usr/docs/file.txt를 지정합니다.
- 사전 정의된 규칙:
  - [All Profiles Folder]는 /home을 선택합니다. 모든 사용자 프로필은 기본적으로 이 폴더에 저장됩니다.
  - /home은 일반 사용자의 홈 디렉토리를 선택합니다.
  - /root는 루트 사용자의 홈 디렉토리를 선택합니다.
  - /usr는 모든 사용자 관련 프로그램의 디렉토리를 선택합니다.
  - /etc는 시스템 구성 파일의 디렉토리를 선택합니다.

macOS

- 파일 또는 디렉토리에 대한 전체 경로.

  예:
  - 사용자의 바탕 화면에 file.txt를 백업하려면 /Users/<사용자 이름>/Desktop/file.txt를 지정합니다.
  - 사용자의 바탕 화면, 문서 또는 다운로드 폴더를 백업하려면 각각 /Users/<사용자 이름>/바탕 화면, /Users/<사용자 이름>/문서 및 /Users/<사용자 이름>/다운로드를 지정합니다.
  - 이 머신에 계정이 있는 모든 사용자의 홈 폴더를 백업하려면 /Users를 지정합니다.
  - 애플리케이션이 설치된 폴더를 백업하려면 /Applications를 지정합니다.
- 사전 정의된 규칙
  - [All Profiles Folder]는 /Users를 선택합니다. 모든 사용자 프로필은 기본적으로 이 폴더에 저장됩니다.

시스템 상태 선택

참고

시스템 상태 백업은 Agent for Windows가 설치되어 있으며 Windows 7 이상을 실행 중인 머신에 대해 사용할 수 있습니다. 하이퍼바이저 수준에서 백업된 가상 머신(에이전트 없는 백업)에서는 시스템 상태 백업을 사용할 수 없습니다.

시스템 상태를 백업하려면 **백업 대상**에서 **시스템 상태**를 선택합니다.

시스템 상태 백업은 다음 파일로 구성됩니다.

© Acronis International GmbH, 2003-2024

- 작업 스케줄러 구성
- VSS 메타데이터 저장소
- 성능 카운터 구성 정보
- MSSearch 서비스
- BITS(Background Intelligent Transfer Service)
- 레지스트리
- WMI(Windows Management Instrumentation)
- 컴퍼넌트 서비스 클래스 등록 데이터베이스

ESXi 구성 선택

ESXi 호스트 구성 백업을 통해 ESXi 호스트를 베어 메탈로 복구할 수 있습니다. 복구는 부트 가능한 미디어에서 수행됩니다.

해당 호스트에서 실행 중인 가상 머신은 백업에 포함되지 않습니다. 가상 머신은 따로 백업 및 복구할 수 있습니다.

ESXi 호스트 구성의 백업에는 다음이 포함됩니다.

- 호스트의 부트로더 및 부트 뱅크 파티션.
- 호스트 상태(가상 네트워킹 및 스토리지 구성, SSL 키, 서버 네트워크 설정, 로컬 사용자 정보).
- 호스트에 설치 또는 스테이징되어 있는 확장 및 패치.
- 로그 파일.

사전 요구 사항

- SSH가 ESXi 호스트 구성의 **보안 프로필**에서 활성화되어 있어야 합니다.
- ESXi 호스트의 '루트' 계정 비밀번호를 알고 있어야 합니다.

제한 사항

- VMware ESXi 7.0 이상 버전을 실행하는 호스트에서는 ESXi 구성 백업이 지원되지 않습니다.
- ESXi 구성을 클라우드 스토리지에 백업할 수 없습니다.

ESXi 구성을 선택하려면

1. **장치** > **모든 장치**를 클릭하고 백업하려는 ESXi 호스트를 선택합니다.
2. **보호**를 클릭합니다.
3. **백업 대상**에서 **ESXi 구성**을 선택합니다.
4. **ESXi '루트' 비밀번호**에서 선택한 각 호스트의 '루트' 계정 비밀번호를 지정하거나 모든 호스트에 동일한 비밀번호를 적용합니다.

지속적인 데이터 보호(CDP)

지속적인 데이터 보호(CDP)는 고급 백업 팩의 일부입니다. 이는 중요 데이터를 변경된 직후에 백업하므로 두 예약 백업 사이의 시간에 시스템 장애가 발생하더라도 변경 내용이 손실되지 않습니다.

© Acronis International GmbH, 2003-2024

다음 데이터를 대상으로 지속적인 데이터 보호를 구성할 수 있습니다.

- 특정 위치의 파일 또는 폴더
- 특정 애플리케이션에서 수정된 파일

지속적인 데이터 보호는 NTFS 파일 시스템 및 다음 운영 체제에서만 지원됩니다.

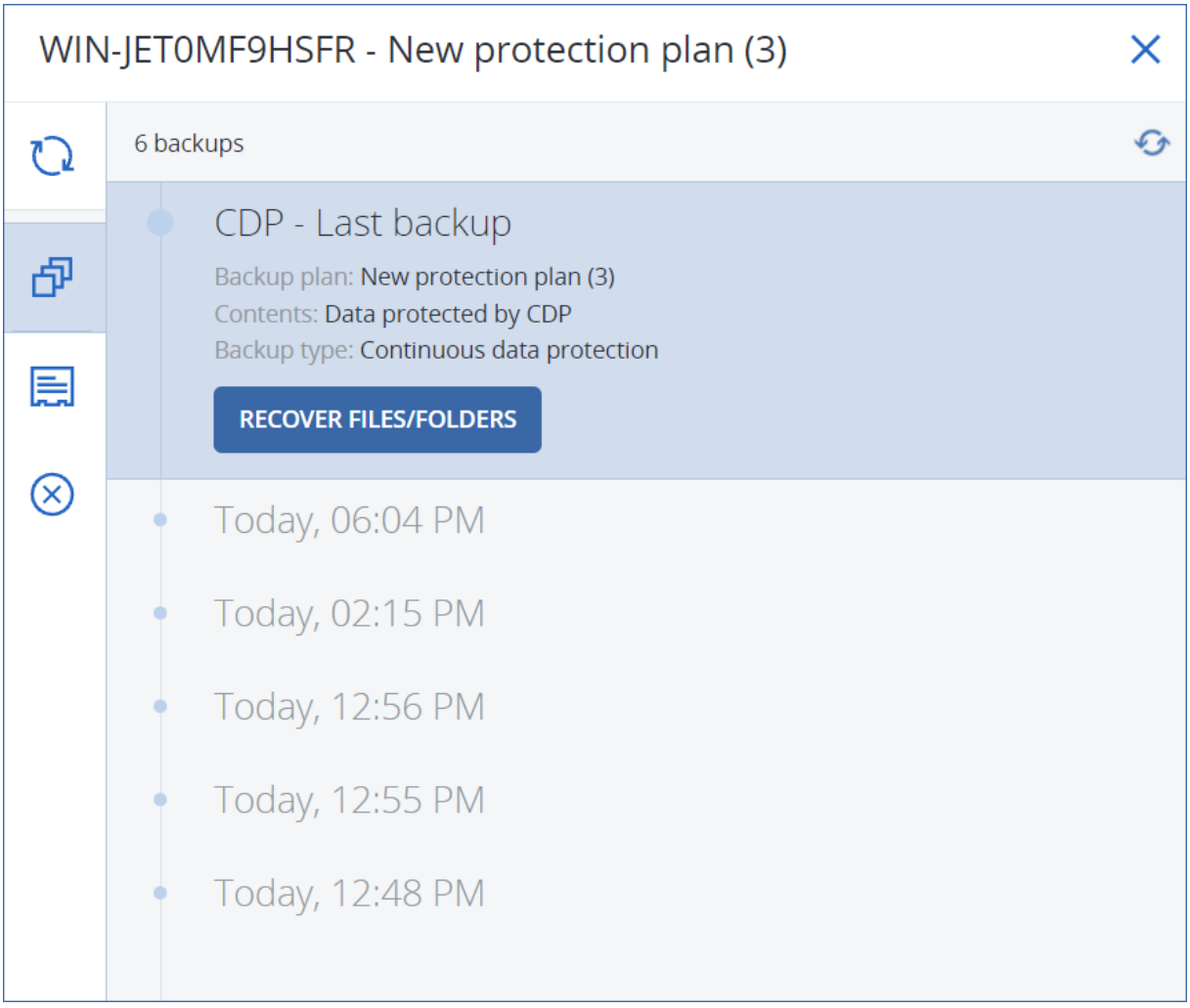
- 데스크탑: Windows 7 이상
- 서버: Windows Server 2008 R2 이상

로컬 폴더만 지원됩니다. 네트워크 폴더는 지속적인 데이터 보호용으로 선택할 수 없습니다.

지속적인 데이터 보호는 **애플리케이션 백업** 옵션과 호환되지 않습니다.

작동법

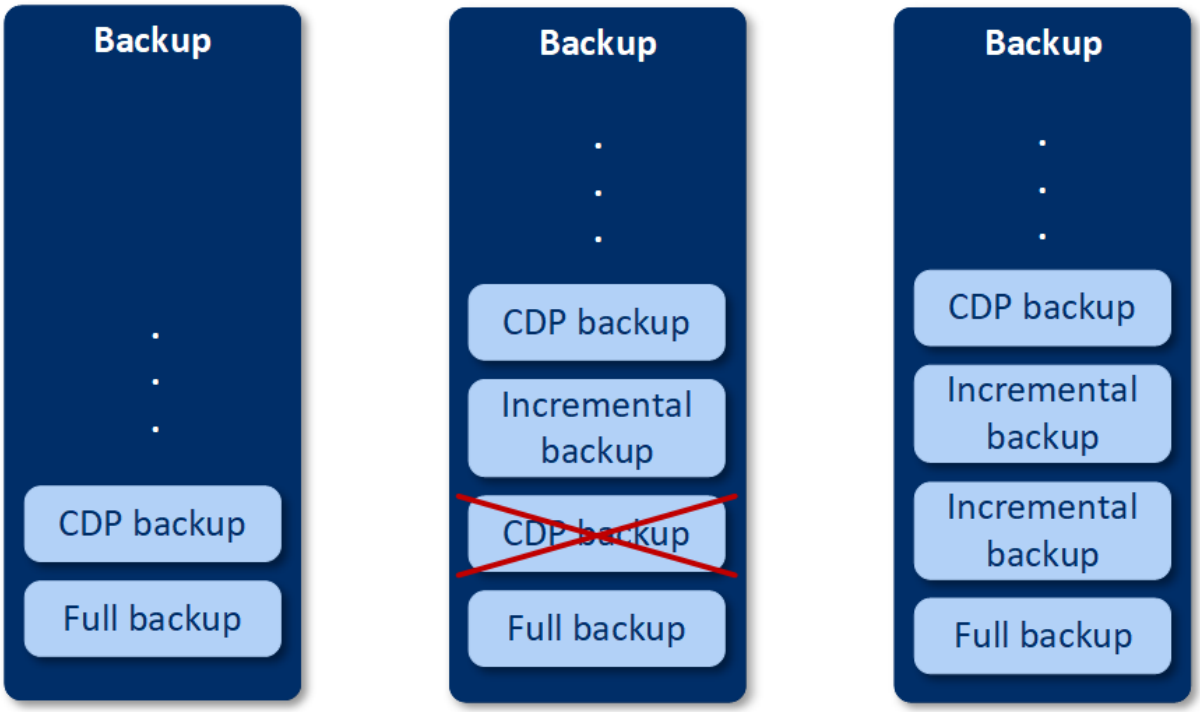
지속적인 데이터 보호에서 추적하는 파일과 폴더의 변경 내용은 특수 CDP 백업에 즉시 저장됩니다. 백업 세트에는 CDP 백업이 하나뿐이며, 항상 최신 백업이 CDP 백업으로 지정됩니다.



일반 예약 백업이 시작되면 지속적인 데이터 보호는 보류 상태로 설정됩니다. 예약 백업에 최신 데이터가 포함되기 때문입니다. 예약 백업이 완료되면 지속적인 데이터 보호가 재개되고 이전 CDP

© Acronis International GmbH, 2003-2024

백업은 삭제되며 새 CDP 백업이 생성됩니다. 이렇게 CDP 백업은 항상 백업 세트에서 최신 백업 상태를 유지하며 추적되는 파일이나 폴더의 최신 상태만 저장합니다.



일반 백업 중에 머신에서 크래시가 발생하면 머신이 다시 시작된 후에 지속적인 데이터 보호가 재개되어 정상 완료된 마지막 예약 백업을 기준으로 CDP 백업이 생성됩니다.

지속적인 데이터 보호를 사용하려면 CDP 백업 전에 일반 백업을 하나 이상 생성해야 합니다. 지속적인 데이터 보호가 포함된 보호 계획을 처음 실행하면 전체 백업이 생성되며 해당 백업에 CDP 백업이 즉시 추가되기 때문입니다. 기존 보호 계획에서 **지속적인 데이터 보호** 옵션을 활성화하면 기존 백업 세트에 CDP 백업이 추가됩니다.

참고
고급 백업 기능을 사용하도록 설정하고 선택한 머신에 다른 고급 백업 기능을 사용하지 않는 경우 **장치** 탭에서 생성한 보호 계획에 지속적인 데이터 보호가 기본적으로 설정됩니다. 선택한 머신에 지속적인 데이터 보호를 사용하는 계획이 이미 있는 경우, 새로 생성된 계획에서 해당 머신에 지속적인 데이터 보호를 사용할 수 없도록 기본 설정됩니다.
장치 그룹에 만들어진 계획에 대해 지속적인 데이터 보호가 활성화되지 않도록 기본 설정됩니다.

지원되는 데이터 소스

다음 데이터 소스를 사용하여 지속적인 데이터 보호를 구성할 수 있습니다.

- 전체 머신
- 디스크/볼륨
- 파일/폴더

© Acronis International GmbH, 2003-2024

보호 계획의 **백업 대상** 섹션에서 데이터 소스를 선택한 후 **지속적으로 보호할 항목** 섹션에서 지속적인 데이터 보호를 사용할 파일, 폴더 또는 애플리케이션을 선택합니다. 지속적인 데이터 보호를 구성하는 방법에 대한 자세한 내용은 "CDP 백업 구성"(375페이지)을(를) 참조하십시오.

지원되는 대상

다음 대상을 사용하여 지속적인 데이터 보호를 구성할 수 있습니다.

- 로컬 폴더
- 네트워크 폴더
- 클라우드 스토리지
- Acronis Cyber Infrastructure
- 스크립트에서 정의한 위치

참고
위에 나와 있는 위치만 스크립트를 통해 정의할 수 있습니다.

CDP 백업 구성

보호 계획의 **백업** 모듈에서 지속적인 데이터 보호를 구성할 수 있습니다. 보호 계획을 생성하는 방법에 대한 자세한 내용은 "보호 계획 생성"(200페이지)을(를) 참조하십시오.

지속적인 데이터 보호 설정을 구성하려면

1. 보호 계획의 **백업** 모듈에서 **지속적인 데이터 보호(CDC)** 스위치를 활성화합니다.
   이 스위치는 다음 데이터 소스에만 사용 가능합니다.
   - 전체 머신
   - 디스크/볼륨
   - 파일/폴더
2. **지속적으로 보호할 항목**에서 **애플리케이션**이나 **파일/폴더** 중 하나 또는 두 항목 모두를 대상으로 지속적인 데이터 보호를 구성합니다.
   - **애플리케이션**을 클릭하여 특정 애플리케이션이 수정하는 파일용 CDP 백업을 구성합니다.
     사전 정의된 카테고리에서 애플리케이션을 선택할 수도 있고, 다음과 같이 애플리케이션 실행 파일 경로를 지정하여 다른 애플리케이션을 추가할 수도 있습니다.
     - `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`
     - `*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE`
   - **파일/폴더**를 클릭하여 특정 위치의 파일용 CDP 백업을 구성합니다.
     선택 규칙을 사용하거나 파일과 폴더를 직접 선택하여 이러한 위치를 정의할 수 있습니다.
     - [모든 머신에 해당됨] 선택 규칙을 생성하려면 텍스트 상자를 사용합니다.
       파일의 전체 경로나 와일드카드(* 및 ?)가 포함된 경로를 사용할 수 있습니다. 별표는 0개 이상의 문자와 일치합니다. 물음표는 문자 하나와 일치합니다.

© Acronis International GmbH, 2003-2024

중요

폴더용 CDP 백업을 생성하려면 별표 와일드카드 문자를 사용하여 백업의 내용을 지정해야 합니다.

올바른 경로:`D:\Data\*`

잘못된 경로:`D:\Data\`

- [온라인 머신에 해당됨]파일 및 폴더를 직접 선택하려면
  - **다음 위치에서 탐색할 머신**에서 파일이나 폴더가 있는 머신을 선택합니다.
  - **파일 및 폴더 선택**을 클릭하여 선택한 머신을 찾습니다.

    파일이나 폴더를 직접 선택하면 선택 규칙이 생성됩니다. 여러 머신에 보호 계획을 적용했는데 선택 규칙이 그중 한 머신에 유효하지 않으면 해당 머신은 건너뜁니다.

3. 보호 계획 창에서 **생성**을 클릭합니다.

그러면 지정한 데이터가 예약 백업 간에 지속적으로 백업됩니다.

목적지 선택

백업 위치를 클릭한 후 다음 중 하나를 선택합니다.

- **클라우드 스토리지**

  클라우드 데이터 센터에 백업이 저장됩니다.
- **로컬 폴더**

  단일 머신을 선택한 경우 선택한 머신의 폴더를 찾거나 폴더 경로를 입력합니다.

  여러 머신을 선택한 경우 폴더 경로를 입력합니다. 각 선택한 실제 머신 또는 가상 머신의 에이전트가 설치된 머신에서 백업이 이 폴더에 저장됩니다. 폴더가 없는 경우에는 새로 생성됩니다.
- **네트워크 폴더**

  이 폴더는 SMB/CIFS/DFS를 통해 공유되는 폴더입니다.

  필요한 공유 폴더로 이동하거나 다음 형식으로 경로를 입력합니다.
  - SMB/CIFS 공유의 경우: `\\<호스트 이름>\<경로>\` 또는 `smb://<호스트 이름>/<경로>/`
  - DFS 공유의 경우: `\\<전체 DNS 도메인 이름>\<DFS 루트>\<경로>`

    예: `\\example.company.com\shared\files`

  그런 다음, 화살표 버튼을 클릭합니다. 메시지가 표시되면 공유 폴더에 대한 사용자 이름과 비밀번호를 지정합니다. 이 자격 증명은 폴더 이름 옆에 있는 열쇠 아이콘을 클릭하여 언제든지 변경할 수 있습니다.

  익명 액세스를 이용하여 폴더에 백업하는 작업은 지원되지 않습니다.
- **퍼블릭 클라우드**

  Advanced Backup 팩에서 제공되는 옵션입니다.

  이 옵션을 사용하면 퍼블릭 클라우드 호환 스토리지로의 직접 백업을 구성할 수 있으므로 Microsoft Azure나 기타 가상 머신을 게이트웨이로 디플로이하는 등 추가 컴포넌트를 디플로이할 필요가 없습니다. 필요에 따라 관련 퍼블릭 클라우드를 선택한 후 해당 클라우드에 연결합니다.

  자세한 내용은 "퍼블릭 클라우드에 워크로드 백업"(491페이지)을(를) 참조하십시오.

© Acronis International GmbH, 2003-2024

- **NFS 폴더**(Linux 또는 macOS를 실행하는 머신에서 사용 가능)
  Agent for Linux가 설치되어 있는 Linux 서버에 nfs-utils 패키지가 설치되어 있는지 확인합니다.
  필요한 NFS 폴더로 이동하거나 다음 형식으로 경로를 입력합니다.
  `nfs://<호스트 이름>/<내보낸 폴더>:/<하위 폴더>`
  그런 다음, 화살표 버튼을 클릭합니다.

  참고
  비밀번호로 보호되는 NFS 폴더로는 백업할 수 없습니다.

- **Secure Zone**(선택한 각 머신에 있는 경우 사용 가능)
  Secure Zone은 백업된 머신의 디스크에 있는 보안 파티션입니다. 백업 구성 전에 이 파티션을 수동으로 생성해야 합니다. Secure Zone을(를) 생성하는 방법, 장점과 제한 사항에 관한 자세한 내용은 "Secure Zone 정보"(378페이지)을(를) 참조하십시오.

고급 스토리지 옵션

참고
이 기능은 Cyber Protection 서비스의 Advanced Edition에서만 사용할 수 있습니다.

스크립트에서 정의(Windows 실행 머신에 사용 가능)

스크립트에서 정의한 폴더에 각 머신의 백업을 저장할 수 있습니다. 소프트웨어는 JScript, VBScript 또는 Python 3.5로 작성된 스크립트를 지원합니다.보호 계획을 배포하는 경우 소프트웨어는 각 머신에서 스크립트를 실행합니다. 각 머신에 대한 스크립트 출력은 로컬 또는 네트워크 폴더 경로여야 합니다. 폴더가 없는 경우에는 새로 생성됩니다(제한: Python으로 작성된 스크립트는 공유 네트워크에 폴더를 생성할 수 없습니다). **백업 스토리지** 탭에서 각 폴더가 별도의 백업 위치로 표시됩니다.

스크립트 유형에서 스크립트 유형(**JScript**, **VBScript**, 또는 **Python**)을 선택한 다음 스크립트를 가져오거나 복사하고 붙여넣습니다. 네트워크 폴더의 경우 읽기/쓰기 권한이 있는 액세스 자격 증명을 지정합니다.

예:

- 다음 JScript 스크립트는 머신의 백업 위치를 다음과 같이 `\\bkpsrv\<machine name>` 형식으로 출력합니다.

  ```
  WScript.Echo("\\\\bkpsrv\\" + WScript.CreateObject("WScript.Network").ComputerName);
  ```

  따라서 각 머신의 백업은 서버 **bkpsrv**의 이름이 동일한 폴더에 저장됩니다..
- 다음 JScript 스크립트는 스크립트가 실행되는 머신 내 폴더의 백업 위치를 출력합니다.

  ```
  WScript.Echo("C:\\Backup");
  ```

  즉, 이 머신의 백업은 해당 머신의 `C:\Backup` 폴더에 저장됩니다.

© Acronis International GmbH, 2003-2024

참고
이러한 스크립트의 위치 경로는 대/소문자를 구분합니다. 즉, C:\Backup과 C:\backup은 Cyber Protect 콘솔에서 다른 위치로 표시됩니다. 그리고 드라이브 문자에는 대문자를 사용해야 합니다.

Secure Zone 정보

Secure Zone은 백업된 머신의 디스크에 있는 보안 파티션입니다. 여기에는 이 머신의 디스크 또는 파일의 백업을 저장할 수 있습니다.

디스크에 물리적 오류가 발생하는 경우 Secure Zone에 위치한 백업이 손실될 수 있습니다. 따라서 Secure Zone이 백업을 저장하는 유일한 위치가 되면 안 됩니다. 엔터프라이즈 환경에서 Secure Zone은 일반 위치를 일시적으로 사용할 수 없거나 느리거나 사용 중인 채널을 통해 연결된 경우 백업에 사용되는 중간 위치로 여겨집니다.

Secure Zone을 사용하는 이유는 무엇일까요?

Secure Zone:

- 디스크 백업이 상주하는 동일한 디스크로 디스크를 복구할 수 있게 해줍니다.
- 소프트웨어 오작동, 바이러스 공격, 사람의 실수로부터 데이터를 보호할 수 있는 비용 효율적이면서 편리한 방법을 제공합니다.
- 데이터 백업 및 복구를 위한 별도의 미디어 또는 네트워크 연결의 필요성을 없애줍니다. 이는 로밍 사용자에게 특히 유용합니다.
- 백업 복제를 사용하는 경우 주 목적지 역할을 할 수 있습니다.

제한 사항

- Secure Zone은 Mac에서 구성할 수 없습니다.
- Secure Zone은 기본 디스크의 파티션입니다. 동적 디스크에 구성하거나 논리 볼륨(LVM으로 관리)으로 생성할 수 없습니다.
- Secure Zone은 FAT32 파일 시스템으로 포맷되어 있습니다. FAT32는 파일 크기 제한이 4GB이기 때문에 이보다 용량이 큰 백업은 Secure Zone에 저장될 때 분할됩니다. 이는 복구 절차와 속도에 영향을 주지 않습니다.

Secure Zone 생성으로 디스크가 변환되는 방식

- Secure Zone은 항상 하드 디스크 끝에 생성됩니다.
- 디스크 끝에는 할당되지 않은 공간이 없거나 부족하지만 볼륨 사이에 할당되지 않은 공간이 있는 경우 해당 볼륨이 디스크 끝으로 이동하여 할당되지 않은 공간을 보충합니다.
- 모든 할당되지 않은 공간이 수집되었지만 여전히 충분하지 않으면 소프트웨어는 사용자가 선택한 볼륨에서 여유 공간을 확보하며 이와 비례하여 볼륨 크기가 줄어듭니다.
- 하지만 볼륨에 여유 공간이 있어야 운영 체제 및 애플리케이션이 임시 파일 생성 등의 작업을 수행할 수 있습니다. 소프트웨어는 어느 한 볼륨의 여유 공간이 총 볼륨 크기의 25% 이하거나, 그

© Acronis International GmbH, 2003-2024

수준까지 떨어질 염려가 있는 경우 볼륨의 크기를 줄이지 않습니다. 디스크의 모든 볼륨에 여유 공간이 25% 이하일 때에만 소프트웨어가 볼륨의 크기를 비례적으로 계속해서 줄여나갑니다.

위 내용에 비추어 Secure Zone 크기를 최대한으로 지정하는 것은 바람직하지 않습니다. 결국 모든 볼륨에 여유 공간이 없어지면 운영 체제나 애플리케이션이 안정적으로 작동하지 못하고, 아예 시작하지 못하는 일이 생길 수도 있습니다.

중요
시스템이 현재 부팅되어 있는 볼륨을 이동하거나 크기 조정하려면 재부팅해야 합니다.

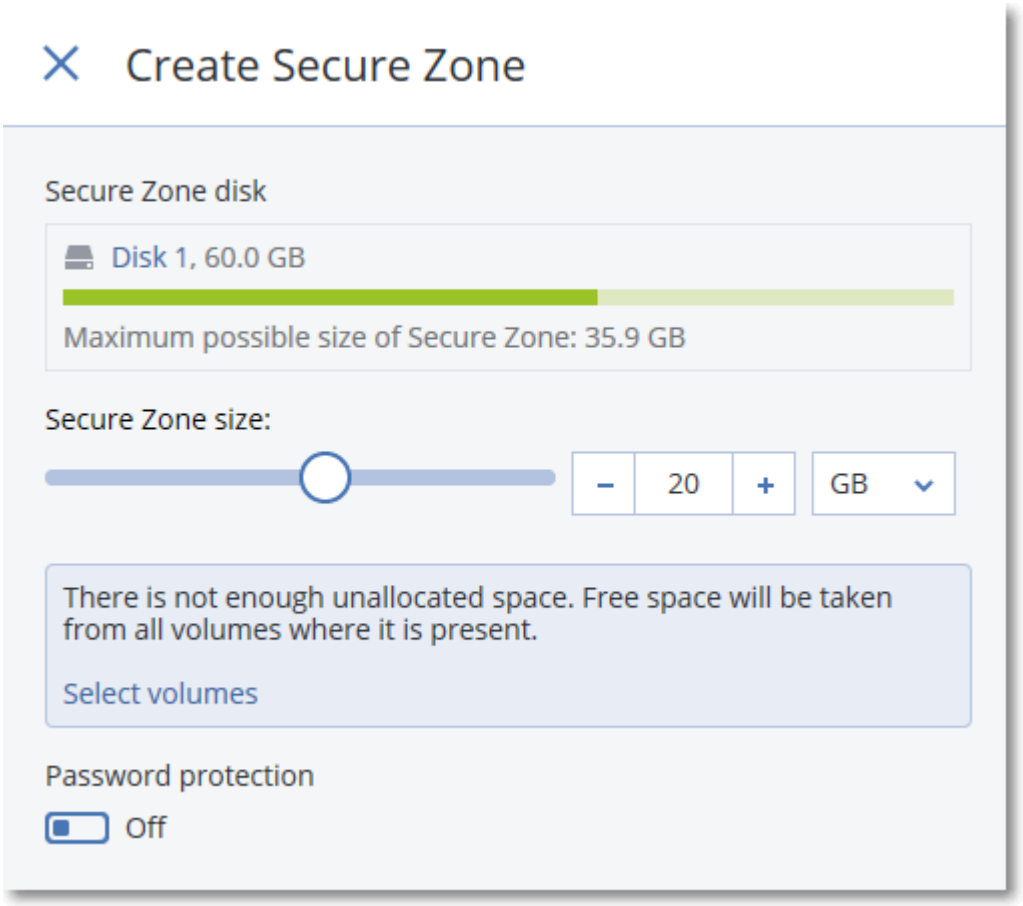
Secure Zone 생성 방법

1. Secure Zone을 생성할 머신을 선택합니다.
2. **상세정보** > **Secure Zone 생성**을 클릭합니다.
3. **Secure Zone 디스크**에서 **선택**을 클릭한 다음, 영역을 생성할 하드 디스크를 선택합니다(여러 개가 있는 경우).

   소프트웨어가 설정 가능한 Secure Zone의 최대 크기를 계산합니다.
4. Secure Zone 크기를 입력하거나 슬라이더를 끌어 최소 크기와 최대 크기 사이의 임의의 크기를 선택합니다.

   최소 크기는 하드 디스크의 구조에 따라 약 50MB 입니다. 최대 크기는 디스크의 할당되지 않은 공간에 모든 디스크 볼륨에 있는 총 여유 공간을 더한 크기와 같습니다.
5. 모든 할당되지 않은 공간이 사용자가 지정한 크기보다 부족한 경우 소프트웨어가 기존 볼륨에서 여유 공간을 확보합니다. 기본적으로 모든 볼륨이 선택되어 있습니다. 일부 볼륨을 제외하려면 **볼륨 선택**을 클릭합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.

© Acronis International GmbH, 2003-2024



6. [선택 사항] **비밀번호 보호** 스위치를 활성화하고 비밀번호를 지정합니다.
   Secure Zone에 위치한 백업에 액세스하려면 비밀번호가 필요합니다. 백업을 부트 가능한 미디어에서 수행하지 않는 한 Secure Zone으로 백업할 때는 비밀번호가 필요하지 않습니다.
7. **생성**을 클릭합니다.
   소프트웨어가 예상 파티션 레이아웃을 표시합니다. **확인**을 클릭합니다.
8. 소프트웨어가 Secure Zone을 생성할 때까지 기다립니다.

이제 보호 계획을 생성할 때 **백업할 위치**로 Secure Zone을 선택할 수 있습니다.

Secure Zone 삭제 방법

1. Secure Zone이 있는 머신을 선택합니다.
2. **상세정보**를 클릭합니다.
3. **Secure Zone** 옆에 있는 기어 아이콘을 클릭한 다음 **삭제**를 클릭합니다.
4. [선택 사항] 영역에서 사용 가능한 공간을 추가할 볼륨을 지정합니다. 기본적으로 모든 볼륨이 선택되어 있습니다.
   공간은 선택한 볼륨에 균등하게 배분됩니다. 볼륨을 선택하지 않을 경우 확보된 공간은 할당이 취소됩니다.
   시스템이 현재 부팅되어 있는 볼륨의 크기를 조정하려면 재부팅해야 합니다.
5. **삭제**를 클릭합니다.

그러면 Secure Zone과 여기에 저장된 모든 백업이 함께 삭제됩니다.

© Acronis International GmbH, 2003-2024

백업 스케줄

특정 시간에/특정 간격으로/특정 이벤트 발생 시에 백업이 자동으로 실행되도록 구성할 수 있습니다.

비클라우드 간 리소스의 예약 백업은 보호 에이전트가 설치된 워크로드의 표준 시간대 설정에 따라 실행됩니다. 예를 들어 표준 시간대 설정이 서로 다른 워크로드에 같은 보호 계획을 적용하면 백업은 각 워크로드의 로컬 표준 시간대에 따라 시작됩니다.

백업 예약 시에는 다음 작업을 수행합니다.

- 백업 구성표 선택
- 백업을 트리거하는 이벤트 선택 또는 시간 구성
- 선택적 설정 및 시작 조건 구성

백업 구성표

백업 구성표는 생성되는 백업 유형(전체, 차등, 증분) 및 백업 생성 시기를 정의하는 보호 계획 스케줄의 한 부분입니다. 사전 정의된 백업 구성표 중 하나를 선택하거나 사용자 정의 구성표를 생성할 수 있습니다.

사용 가능한 백업 구성표와 유형은 백업 위치 및 소스에 따라 다릅니다. 예를 들어 SQL 데이터, Exchange 데이터 또는 시스템 상태를 백업할 때는 차등 백업을 사용할 수 없습니다. 테이프 장치에서는 **항상 증분(단일 파일)** 구성표가 지원되지 않습니다.

백업 구성표	설명	구성 가능한 요소
항상 증분(단일 파일)	첫 번째 백업은 전체 백업이므로 시간이 많이 걸릴 수 있습니다. 후속 백업은 증분 백업이므로 첫 번째 백업보다는 속도가 훨씬 빠릅니다. 이러한 백업은 단일 파일 백업 형식[1]*을 사용합니다. 기본적으로 백업이 월요일부터 금요일까지 매일 수행됩니다. 클라우드 스토리지에 백업을 저장할 때는 이 구성표를 사용하는 것이 좋습니다. 증분 백업은 속도는 빠르고 네트워크 트래픽은 더 적기 때문입니다.	• 스케줄 유형: 매달, 매주, 일일, 매시간 • 백업 트리거: 시간 또는 이벤트 • 시작 시간 • 시작 조건 • 추가 옵션
항상 전체	백업 세트의 모든 백업이 전체 백업입니다. 기본적으로 백업이 월요일부터 금요일까지 매일	• 스케줄 유형: 매달, 매주, 일일, 매시간

[1]초기 전체 백업 및 이후 증분 백업이 단일 .tibx 파일로 저장되는 백업 형식입니다. 이 형식은 오래된 백업의 삭제가 어렵다는 주요 단점을 피하면서 증분 백업 방식의 빠른 속도를 활용합니다. 이 소프트웨어는 오래된 백업에서 사용하는 블록을 "여유"로 표시하고 이러한 블록에 새 백업을 씁니다. 이를 통해 최소한의 리소스를 사용하여 매우 빠른 정리가 가능합니다. 임의 액세스 읽기 및 쓰기가 지원되지 않는 위치로 백업할 때는 단일 파일 백업 형식을 사용할 수 없습니다.

© Acronis International GmbH, 2003-2024

백업 구성표	설명	구성 가능한 요소
	수행됩니다.	• 백업 트리거: 시간 또는 이벤트 • 시작 시간 • 시작 조건 • 추가 옵션
매주 전체, 매일 증분	전체 백업은 매주 한 번씩 생성되며 그 외의 백업은 증분으로 생성됩니다. 특정 주의 첫 번째 백업은 전체 백업이며 나머지 백업은 증분 백업입니다. 이 주기가 매주 반복 진행됩니다. 주간 전체 백업이 생성되는 요일을 선택하려면 보호 계획에서 기어 아이콘을 클릭하고 **백업 옵션** > **주간 백업**으로 이동합니다. 기본적으로 백업이 월요일부터 금요일까지 매일 수행됩니다.	• 백업 트리거: 시간 또는 이벤트 • 시작 시간 • 시작 조건 • 추가 옵션
매월 전체, 매주 차등, 매일 증분(GFS)	기본적으로 증분 백업은 월요일부터 금요일까지 매일 수행됩니다. 차등 백업은 토요일마다 수행됩니다. 전체 백업은 매월 1일에 수행됩니다. **참고** 이러한 백업 방식은 사전 정의된 사용자 정의 구성표입니다. 해당 구성표는 보호 계획에서 **사용자 정의**로 표시됩니다.	• 백업 유형별로 기존 스케줄 변경: ◦ 스케줄 유형: 매달, 매주, 일일, 매시간 ◦ 백업 트리거: 시간 또는 이벤트 ◦ 시작 시간 ◦ 시작 조건 ◦ 추가 옵션 • 백업 유형별로 새 스케줄 추가
사용자 정의	백업 유형(전체, 차등, 증분)을 선택하고 각 유형용으로 개별 스케줄을 구성해야 합니다*.	• 백업 유형별로 기존 스케줄 변경: ◦ 스케줄 유형: 매달, 매주, 일일, 매시간 ◦ 백업 트리거: 시간 또는 이벤트 ◦ 시작 시간 ◦ 시작 조건 ◦ 추가 옵션 • 백업 유형별로 새 스케줄 추가

* 보호 계획을 생성한 후에는 **항상 증분(단일 파일)**과 기타 백업 구성표 간을 전환할 수 없습니다. **항상 증분(단일 파일)**은 단일 파일 형식 구성표이고 나머지 구성표는 다중 파일 형식입니다. 형식을 전환하려면 새 보호 계획을 생성해야 합니다.

© Acronis International GmbH, 2003-2024

백업 유형

사용 가능한 백업 유형은 다음과 같습니다.

- 전체 - 전체 백업에는 모든 소스 데이터가 포함됩니다. 이 백업은 자급식 백업입니다. 즉, 데이터를 복구하기 위해 다른 백업에 액세스할 필요가 없습니다.

  참고
  보호 계획에서 생성된 첫 번째 백업은 전체 백업입니다.

- 증분 - 최신 백업의 유형(전체, 차등, 증분)에 관계없이 증분 백업에는 최신 백업 이후의 데이터 변경 사항이 저장됩니다. 데이터를 복구하려면 증분 백업이 사용하는 전체 백업 체인(초기 전체 백업까지)이 필요합니다.
- 차등 - 차등 백업에는 최신 전체 백업 이후의 데이터 변경 사항이 저장됩니다. 데이터를 복구하려면 차등 백업, 그리고 차등 백업이 사용하는 데이터가 포함된 해당 전체 백업이 모두 필요합니다.

스케줄에 따라 백업 실행

특정 시간에/특정 이벤트 발생 시에 백업을 자동으로 실행하려면 보호 계획에서 스케줄을 활성화합니다.

스케줄을 활성화하려면

1. 보호 계획에서 **백업** 모듈을 확장합니다.
2. **스케줄**을 클릭합니다.
3. 스케줄 스위치를 활성화합니다.
4. 백업 구성표를 선택합니다.
5. 필요한 대로 스케줄을 구성하고 **완료**를 클릭합니다.
   사용 가능한 예약 옵션에 대한 자세한 내용은 "시간 기준 예약"(384페이지) 및 "이벤트별 스케줄"(386페이지) 항목을 참조하십시오.
6. [선택 사항] 시작 조건이나 추가 예약 옵션을 구성합니다.
7. 보호 계획을 저장합니다.

그러면 스케줄 조건이 충족될 때마다 백업 작업이 시작됩니다.

스케줄을 비활성화하려면

1. 보호 계획에서 **백업** 모듈을 확장합니다.
2. **스케줄**을 클릭합니다.
3. 스케줄 스위치를 비활성화합니다.
4. 보호 계획을 저장합니다.

그러면 백업은 수동으로 시작해야 실행됩니다.

© Acronis International GmbH, 2003-2024

참고
스케줄을 비활성화하면 보존 규칙이 자동 적용되지 않습니다. 보관 규칙을 적용하려면 백업을 수동으로 실행합니다.

시간 기준 예약

다음 표에는 시간 기준 예약 옵션이 요약되어 있습니다. 이러한 옵션의 사용 가능 여부는 백업 구성표에 따라 달라집니다. 자세한 내용은 "백업 구성표"(381페이지)을(를) 참조하십시오.

옵션	설명	예
매달	달, 날짜 또는 요일을 선택하고 백업 시작 시간을 선택합니다.	1월 1일과 2월 3일 오전 12시에 백업을 실행합니다. 매월 1일 오전 10시에 백업을 실행합니다. 3월 1일, 3월 5일, 4월 1일, 4월 5일 오전 9시에 백업을 실행합니다. 매월 둘째/셋째 금요일 오전 11시에 백업을 실행합니다. 매월 마지막 수요일 오후 10시 30분에 백업을 실행합니다.
매주	요일을 선택하고 백업 시작 시간을 선택합니다.	월요일~금요일 오전 10시에 백업을 실행합니다. 월요일 오후 11시에 백업을 실행합니다. 화/토요일 오전 8시에 백업을 실행합니다.
매일	날짜(매일 또는 평일만)를 선택하고 백업 시작 시간을 선택합니다.	매일 오전 11시 45분에 백업을 실행합니다. 월요일~금요일 오후 9시 30분에 백업을 실행합니다.
매시간	요일을 선택하고 두 연속 백업 간의 시간 간격과 백업이 실행되는 시간 범위를 선택합니다. 간격을 분 단위로 구성할 때는 10~60분 사이의 제안 간격을 선택할 수도 있고 45분, 75분 등의 사용자 정의 간격을 지정할 수도 있습니다.	월요일~금요일 오전 8시~오후 6시에 1시간마다 백업을 실행합니다. 토/일요일 오전 1시~오후 6시에 3시간마다 백업을 실행합니다.

추가 옵션

시간을 기준으로 백업을 예약할 때는 다음의 추가 예약 옵션을 사용할 수 있습니다.

© Acronis International GmbH, 2003-2024

이러한 옵션에 액세스하려면 **스케줄** 창에서 **더 많이 표시**를 클릭합니다.

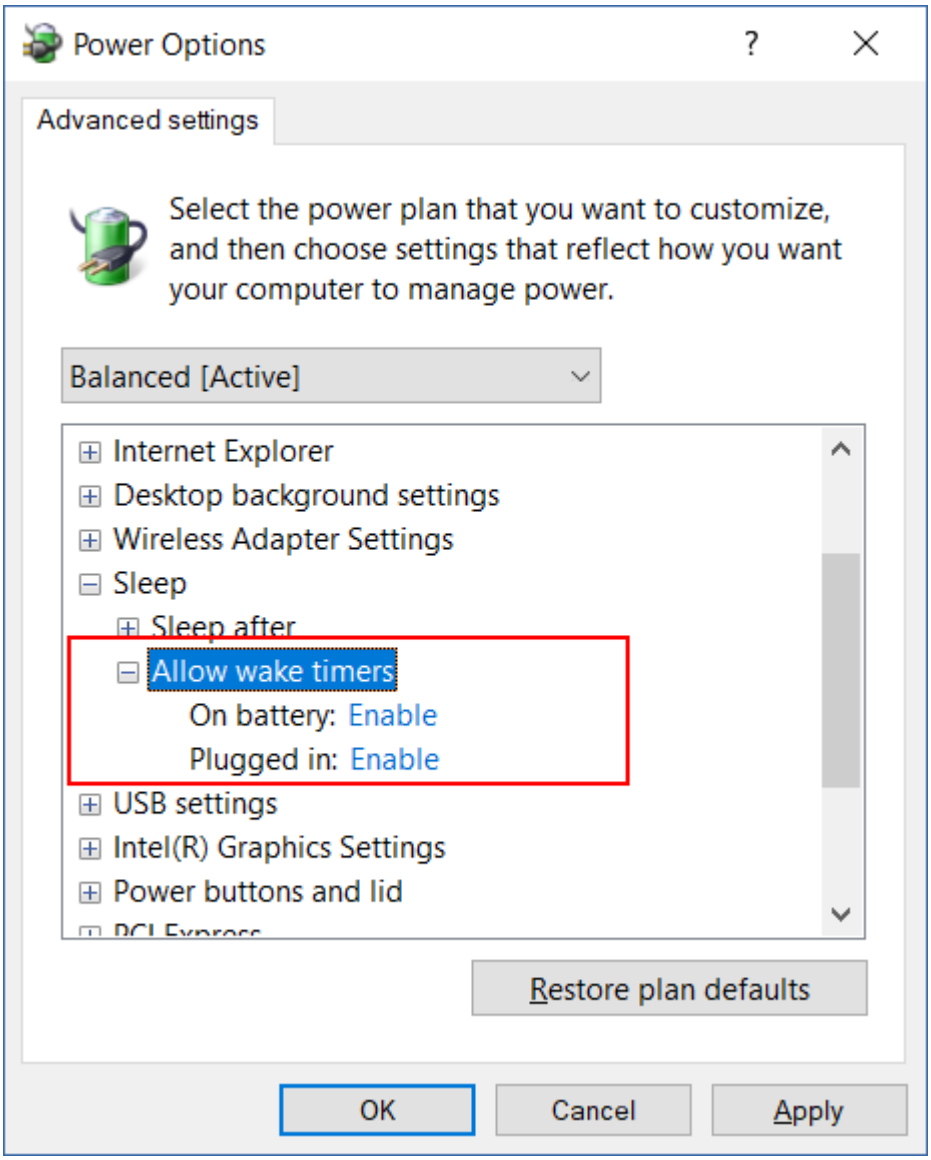
- **머신이 꺼진 경우 머신 시작 시 누락된 작업 실행**

  기본 설정: 비활성화됨.
- **백업 도중 절전 또는 최대 절전 모드가 되는 것을 방지**

  이 옵션은 Windows를 실행 중인 머신에만 적용됩니다.

  기본 설정: 활성화됨.
- **절전 또는 최대 절전 모드에서 깨어나 예약된 백업 시작**

  이 옵션은 전원 관리 옵션에서 **절전 모드 해제 타이머 허용** 옵션을 활성화한 상태로 Windows를 실행 중인 머신에만 적용됩니다.



이 옵션은 WOL(Wake-on-LAN) 기능을 사용하지 않으며 전원이 꺼진 머신에는 적용되지 않습니다.

기본 설정: 비활성화됨.

© Acronis International GmbH, 2003-2024

이벤트별 스케줄

특정 이벤트 발생 시에 실행되는 백업을 구성하려면 다음 옵션 중 하나를 선택합니다.

옵션	설명	예
마지막 백업 후 시간	마지막으로 성공한 백업 후 지정된 기간이 지나면 백업이 시작됩니다. **참고** 이전 백업 완료 방식에 따라 이 옵션이 적용되는 방식도 달라집니다. 백업이 실패하면 다음 백업은 자동으로 시작되지 않습니다. 이 경우 스케줄을 재설정하려면 백업을 수동으로 실행해야 하며 백업이 정상적으로 완료되는지 확인해야 합니다.	마지막으로 정상 완료된 백업 1일 후에 백업을 실행합니다. 마지막으로 정상 완료된 백업 4시간 후에 백업을 실행합니다.
사용자가 시스템에 로그온할 때	사용자가 머신에 로그인하면 백업이 시작됩니다. 모든 로그인이나 특정 사용자의 로그인을 대상으로 이 옵션을 구성할 수 있습니다. **참고** 임시 사용자 프로파일로 로그인하면 백업이 시작되지 않습니다.	사용자 John Doe가 로그인하면 백업을 실행합니다.
사용자가 시스템에서 로그오프할 때	사용자가 머신에서 로그오프하면 백업이 시작됩니다. 모든 로그오프나 특정 사용자의 로그오프를 대상으로 이 옵션을 구성할 수 있습니다. **참고** 임시 사용자 프로파일에서 로그오프하면 백업이 시작되지 않습니다. 머신 종료 시에는 백업이 시작되지 않습니다.	모든 사용자가 로그오프하면 백업을 실행합니다.
시스템 시작 시	보호되는 머신을 시작하면 백업이 실행됩니다.	사용자가 머신을 시작하면 백업을 실행합니다.
시스템 종료 시	보호되는 머신을 종료하면 백업이 실행됩니다.	사용자가 머신을 종료하면 백업을 실행합니다.
Windows 이벤트 로그 이벤트 시	지정한 Windows 이벤트 발생 시 백업이 실행됩니다.	유형이 오류이고 원본이 디스크인 이벤트 7이 Windows 시스템 로그에 기록되면 백업을 실행합니다.

© Acronis International GmbH, 2003-2024

이러한 옵션의 사용 가능 여부는 보호된 워크로드의 운영 체제와 백업 소스에 따라 달라집니다. Windows, Linux 및 macOS에서 사용 가능한 옵션이 아래 표에 요약되어 있습니다.

이벤트	백업 소스(백업할 대상)					
	전체 머신, 디스크/볼륨 또는 파일/폴더(실제 머신)	**전체 머신 또는 디스크/볼륨(가상 머신)**	**ESXi 구성**	**Microsoft 365 사서함**	**Exchange 데이터베이스 및 사서함**	**SQL 데이터베이스**
마지막 백업 후 시간	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
사용자가 시스템에 로그온할 때	Windows	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음
사용자가 시스템에서 로그오프할 때	Windows	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음
시스템 시작 시	Windows, Linux, macOS	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음
시스템 종료 시	Windows	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음
Windows 이벤트 로그 이벤트 시	Windows	해당 없음	해당 없음	Windows	Windows	Windows

Windows 이벤트 로그 이벤트 시

애플리케이션 로그, 보안 로그, 시스템 로그 등의 Windows 이벤트 로그에 특정 이벤트가 기록되면 백업을 자동으로 실행할 수 있습니다.

참고
Windows의 **컴퓨터 관리** > **이벤트 뷰어**에서 이벤트를 찾아 해당 속성을 확인할 수 있습니다. 보안 로그를 열려면 관리자 권한이 필요합니다.

이벤트 매개변수

Windows 이벤트 로그 이벤트 시 옵션을 구성할 때 지정해야 하는 매개변수가 아래 표에 요약되어 있습니다.

© Acronis International GmbH, 2003-2024

매개변수	설명
로그 이름	로그의 이름입니다. 표준 로그의 이름(애플리케이션, 보안 또는 시스템)을 선택하거나 다른 로그 이름을 지정합니다. 예를 들어 Microsoft Office 세션 등의 이름을 지정할 수 있습니다.
이벤트 소스	이벤트 원본은 이벤트를 야기한 프로그램이나 시스템 컴포넌트를 나타냅니다. 디스크 등을 예로 들 수 있습니다. 이벤트 원본에 지정한 텍스트 문자열이 포함되어 있으면 항상 예약 백업이 트리거됩니다. 이 옵션은 대소문자를 구분하지 않습니다. 예를 들어 `service`를 지정하면 Service Control Manager와 Time-Service 이벤트 원본 둘 다에서 백업이 트리거됩니다.
이벤트 유형	이벤트의 유형입니다. 오류, 경고, 정보, 감사 성공 또는 감사 실패를 지정합니다.
이벤트 ID	이벤트 ID를 통해 이벤트 원본 내의 특정 이벤트 종류를 식별할 수 있습니다. 예를 들어 Windows가 디스크에서 불량 블록을 발견하면 이벤트 원본이 디스크이고 이벤트 ID가 7인 오류 이벤트가 발생합니다. 반면 아직 디스크에 액세스할 수 없는 경우에는 이벤트 원본이 디스크이고 이벤트 ID가 15인 오류 이벤트가 발생합니다.

예: 하드 디스크에 불량 블록이 있는 경우의 응급 백업

하드 디스크 드라이브에서 불량 블록이 하나 이상 확인되었다면 하드 디스크 드라이브가 곧 고장 날 수도 있습니다. 그러므로 불량 블록이 감지되면 백업을 생성할 수 있습니다.

Windows가 디스크에서 불량 블록을 발견하면 이벤트 원본이 디스크이고 이벤트 번호가 7인 오류 이벤트가 시스템 로그에 기록됩니다. 보호 계획에서 다음 스케줄을 구성합니다.

- 예약: Windows 이벤트 로그 이벤트 시
- 로그 이름: 시스템
- 이벤트 소스: 디스크
- 이벤트 유형: 오류
- 이벤트 ID: 7

중요
불량 블록이 있어도 백업이 완료되도록 하려면 **백업 옵션**에서 **오류 처리**로 이동한 다음 **불량 섹터 무시** 확인란을 선택합니다.

시작 조건

특정 조건 충족 시에만 백업이 실행되도록 하려면 시작 조건을 하나 이상 구성합니다. 조건을 여러 개 구성한 경우에는 모든 조건이 동시에 충족되어야만 백업이 시작됩니다. 조건 충족 여부에 관계

© Acronis International GmbH, 2003-2024

없이 백업이 실행될 때까지의 기간을 지정할 수 있습니다. 이 백업 옵션에 대한 자세한 내용은 "작업 시작 조건"(447페이지) 항목을 참조하십시오.

백업을 수동으로 시작할 때는 시작 조건이 적용되지 않습니다.

아래 표는 Windows, Linux 및 macOS에서 다양한 데이터에 사용할 수 있는 시작 조건을 나열합니다.

시작 조건	백업 소스(백업할 대상)					
	전체 머신, 디스크/볼륨 또는 파일/폴더 (실제 머신)	**전체 머신 또는 디스크/볼륨(가상 머신)**	**ESXi 구성**	**Microsoft 365 사서함**	**Exchange 데이터베이스 및 사서함**	**SQL 데이터베이스**
사용자가 유휴 상태임	Windows	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음
백업 위치의 호스트를 사용할 수 있음	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
사용자가 로그오프함	Windows	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음
시간 간격에 맞음	Windows, Linux, macOS	Windows, Linux	해당 없음	해당 없음	해당 없음	해당 없음
배터리 전원 절약	Windows	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음
데이터 요금제 사용 시 시작하지 않음	Windows	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음
다음과 같은	Windows	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음

© Acronis International GmbH, 2003-2024

시작 조건	백업 소스(백업할 대상)					
	전체 머신, 디스크/볼륨 또는 파일/폴더 (실제 머신)	**전체 머신 또는 디스크/볼륨(가상 머신)**	**ESXi 구성**	**Microsoft 365 사서함**	**Exchange 데이터베이스 및 사서함**	**SQL 데이터베이스**
Wi-Fi 네트워크에 연결된 경우 시작하지 않음						
장치 IP 주소 확인	Windows	해당 없음	해당 없음	해당 없음	해당 없음	해당 없음

사용자가 유휴 상태임

"사용자가 유휴 상태임"라는 말은 머신에서 화면 보호기가 실행 중이거나 머신이 잠겨 있음을 의미합니다.

예

매일 오후 9시에 백업을 실행합니다. 이때 사용자가 유휴 상태인 것이 좋습니다. 사용자가 오후 11시에 작업을 수행 중이라도 백업을 실행합니다.

- 예약: **일일, 매일 실행**. 시작 시간: **오후 9시**.
- 조건: **사용자가 유휴 상태임**.
- 백업 시작 조건: **조건이 충족될 때까지 대기, 2시간 후 작업 시작**.

결과:

- 사용자가 오후 9시 전에 유휴 상태가 되더라도 백업은 오후 9시에 시작됩니다.
- 사용자가 오후 9시~11시에 유휴 상태가 되면 백업이 즉시 시작됩니다.
- 사용자가 오후 11시에 작업을 수행 중이라도 백업은 오후 11시에 시작됩니다.

백업 위치의 호스트를 사용할 수 있음

"백업 위치의 호스트를 사용할 수 있음"는 백업 위치를 호스팅하는 머신을 네트워크에서 사용할 수 있다는 의미입니다.

이 조건은 네트워크 폴더, 클라우드 스토리지 및 스토리지 노드에서 관리되는 위치에 적용됩니다.

이 조건은 위치 자체의 가용성을 포함하지 않고 호스트 가용성만 포함합니다. 예를 들어 호스트를 사용할 수 있지만 이 호스트의 네트워크 폴더가 공유되지 않거나 폴더의 자격 증명이 더 이상 유효하지 않을 경우 조건을 충족하는 것으로 간주합니다.

© Acronis International GmbH, 2003-2024

예

평일마다 오후 9시에 네트워크 폴더로의 백업을 실행합니다. 해당 시점에 유지보수 작업 등으로 인해 폴더를 호스팅하는 머신을 사용할 수 없는 경우 해당 백업을 건너뛰고 다음 평일에 예약된 백업이 시작될 때까지 기다립니다.

- 예약: **일일, 월요일~금요일 실행**. 시작 시간: **오후 9시**.
- 조건: **백업 위치의 호스트를 사용할 수 있음**
- 백업 시작 조건: **스케줄된 백업 건너뛰기**.

결과:

- 오후 9시에 호스트가 사용 가능한 상태이면 백업이 즉시 시작됩니다.
- 오후 9시에 호스트가 사용 불가능한 상태이면 백업은 다음 평일에 시작됩니다(해당일 오후 9시에 호스트가 사용 가능한 상태인 경우).
- 평일 오후 9시에 호스트를 사용할 수 없는 경우에는 백업이 시작되지 않습니다.

사용자가 로그오프함

모든 사용자가 Windows 머신에서 로그오프할 때까지 백업을 연기하려면 이 시작 조건을 사용합니다.

예

금요일마다 오후 8시에 백업을 실행합니다. 이때 모든 사용자가 로그오프하는 것이 좋습니다. 오후 11시에 아직 로그인 상태인 사용자가 있어도 백업을 실행합니다.

- 예약: **매주**, 금요일. 시작 시간: **오후 8시**.
- 조건: **사용자가 로그오프함**
- 백업 시작 조건: **조건이 충족될 때까지 대기 3시간 후 백업 시작**.

결과:

- 모든 사용자가 오후 8시에 로그오프 상태인 경우 백업이 오후 8시에 시작됩니다.
- 마지막 사용자가 오후 8시~11시 사이에 로그오프하면 백업이 즉시 시작됩니다.
- 오후 11시에 로그인 상태인 사용자가 있어도 백업은 오후 11시에 시작됩니다.

시간 간격에 맞음

백업 시작 시간을 지정된 간격으로 제한하려는 경우 이 시작 조건을 사용합니다.

예

한 회사가 동일한 NAS(네트워크 연결 스토리지)의 각기 다른 위치에 사용자 데이터와 서버를 백업합니다.

평일 업무 시간은 오전 8시에서 오후 5시까지입니다. 사용자 데이터는 오후 4시 30분부터 사용자가 로그오프하는 즉시 백업됩니다.

© Acronis International GmbH, 2003-2024

회사 서버는 매일 오후 11시에 백업됩니다. 따라서 서버 백업용 네트워크 대역폭을 확보하려면 오후 11시 전에 사용자 데이터를 백업하는 것이 좋습니다.

사용자 데이터 백업 소요 시간은 1시간 이하이므로 최신 백업 시작 시간은 오후 10시입니다. 사용자가 지정된 시간 간격 동안 아직 로그인 상태이거나 다른 시간에 로그오프하는 경우에는 사용자 데이터 백업을 건너뛰어야 합니다.

- 이벤트: **사용자가 시스템에서 로그오프할 때**. 사용자 계정 지정: **모든 사용자**.
- 조건: **오후 4시 30분**부터 **10시**까지 **시간 간격에 맞음.**
- 백업 시작 조건: **스케줄된 백업 건너뛰기**.

결과:

- 사용자가 오후 4시 30분~10시 사이에 로그오프하면 백업이 즉시 시작됩니다.
- 사용자가 그 밖의 시간에 로그오프하면 백업을 건너뜁니다.

배터리 전원 절약

머신(노트북 또는 태블릿)이 전원에 연결되어 있지 않은 경우 백업을 방지하려면 이 시작 조건을 사용합니다. 백업 시작 조건 옵션의 값에 따라 머신이 전원에 연결된 후에 건너뛴 백업이 시작될 수도 있고 시작되지 않을 수도 있습니다.

다음 옵션을 사용할 수 있습니다.

- **배터리 사용 시에는 시작하지 않음**
  머신이 전원에 연결되어 있는 경우에만 백업이 시작됩니다.
- **배터리 레벨이 다음 이상인 경우 배터리 사용 시 시작:**
  머신이 전원에 연결되어 있거나 배터리 수준이 지정된 값보다 높은 경우 백업이 시작됩니다.

예

평일마다 오후 9시에 데이터를 백업합니다. 머신이 전원에 연결되어 있지 않은 경우 백업을 건너뛰어 배터리 전력을 아끼고 머신을 전원에 연결할 때까지 기다릴 수 있습니다.

- 예약: **일일, 월요일~금요일 실행**. 시작 시간: **오후 9시**.
- 조건: **배터리 전원 절약, 배터리 사용 시에는 시작하지 않음**.
- 백업 시작 조건: **조건이 충족될 때까지 대기**.

결과:

- 오후 9시에 머신이 전원에 연결되어 있으면 백업이 즉시 시작됩니다.
- 오후 9시에 머신이 배터리에 연결되어 있으면 머신을 전원에 연결할 때 백업이 시작됩니다.

데이터 요금제 사용 시 시작하지 않음

머신이 Windows에서 데이터 요금제로 설정된 연결을 통해 인터넷에 연결되어 있는 경우 백업(로컬 디스크로의 백업 포함)을 방지하려면 이 시작 조건을 사용합니다. Windows에서의 데이터 요금제 연결에 대한 자세한 내용은 https://support.microsoft.com/en-us/help/17452/windows-metered-internet-connections-faq를 참조하십시오.

© Acronis International GmbH, 2003-2024

데이터 요금제 사용 시 시작하지 않음 조건을 활성화하면 추가 시작 조건인 **다음과 같은 Wi-Fi 네트워크에 연결된 경우 시작하지 않음**이 자동으로 활성화됩니다. 이 옵션은 모바일 핫스팟을 통한 백업을 방지하는 추가 조치입니다. android, phone, mobile, modem 같은 네트워크 이름이 기본적으로 지정됩니다.

목록에서 이러한 이름을 제거하려면 X 기호를 클릭합니다. 새 이름을 추가하려면 빈 필드에 이름을 입력합니다.

예

평일마다 오후 9시에 데이터를 백업합니다. 머신이 데이터 요금제 연결을 통해 인터넷에 연결된 경우에는 백업을 건너뛰어 네트워크 트래픽을 아끼고 다음 평일에 예약된 백업이 시작될 때까지 기다릴 수 있습니다.

- 예약: **일일, 월요일~금요일 실행**. 시작 시간: **오후 9시**.
- 조건: **데이터 요금제 사용 시 시작하지 않음**
- 백업 시작 조건: **스케줄된 백업 건너뛰기**.

결과:

- 오후 9시에 머신이 데이터 요금제 연결을 통해 인터넷에 연결되어 있지 않으면 백업이 즉시 시작됩니다.
- 오후 9시에 머신이 데이터 요금제 연결을 통해 인터넷에 연결되어 있으면 백업은 다음 평일에 시작됩니다.
- 머신이 평일 오후 9시에 항상 데이터 요금제 연결을 통해 인터넷에 연결되어 있으면 백업은 시작되지 않습니다.

다음과 같은 Wi-Fi 네트워크에 연결된 경우 시작하지 않음

머신이 지정된 무선 네트워크에 연결되어 있는 경우 백업(로컬 디스크로의 백업 포함)을 방지하려면 이 시작 조건을 사용합니다. 휴대폰 핫스팟을 통한 백업을 제한하려는 경우 등을 예로 들 수 있습니다.

SSID(서비스 세트 식별자)로도 알려진 Wi-Fi 네트워크 이름을 지정할 수 있습니다. 이 제한 사항은 지정된 이름(대소문자 미구분)이 하위 문자열로 이름에 포함되어 있는 모든 네트워크에 적용됩니다. 예를 들어 네트워크 이름으로 phone을 지정하는 경우 머신이 다음 네트워크 중 어느 것에든 연결되어 있으면 백업이 시작되지 않습니다. John's iPhone, phone_wifi 또는 my_PHONE_wifi.

데이터 요금제 사용 시 시작하지 않음 조건을 활성화하면 **다음과 같은 Wi-Fi에 연결된 경우 시작하지 않음** 시작 조건이 자동으로 활성화됩니다. android, phone, mobile, modem 같은 네트워크 이름이 기본적으로 지정됩니다.

목록에서 이러한 이름을 제거하려면 X 기호를 클릭합니다. 새 이름을 추가하려면 빈 필드에 이름을 입력합니다.

예

평일마다 오후 9시에 데이터를 백업합니다. 머신이 모바일 핫스팟을 통해 인터넷에 연결된 경우에는 백업을 건너뛰고 다음 평일에 예약된 백업이 시작될 때까지 기다릴 수 있습니다.

© Acronis International GmbH, 2003-2024

- 예약: **일일, 월요일~금요일 실행**. 시작 시간: **오후 9시**.
- 조건: **다음과 같은 네트워크에 연결된 경우 시작하지 않음, 네트워크 이름**: <핫스팟 네트워크의 SSID>.
- 백업 시작 조건: **스케줄된 백업 건너뛰기**.

결과:

- 오후 9시에 머신이 지정된 네트워크에 연결되어 있지 않으면 백업이 즉시 시작됩니다.
- 오후 9시에 머신이 지정된 네트워크에 연결되어 있으면 백업은 다음 평일에 시작됩니다.
- 머신이 평일 오후 9시에 항상 지정된 네트워크에 연결되어 있으면 백업은 시작되지 않습니다.

장치 IP 주소 확인

머신 IP 주소가 지정된 IP 주소 범위에 들거나 벗어나는 경우 백업을 방지(로컬 디스크로의 백업 포함)하려면 이 시작 조건을 사용합니다. 이렇게 하면 해외 사용자의 머신을 백업하는 등의 경우 대량의 데이터 전송 요금 발생을 방지할 수도 있고 가상 사설망(VPN) 연결을 통한 백업을 방지할 수도 있습니다.

다음 옵션을 사용할 수 있습니다.

- **IP 범위 밖인 경우 시작**
- **IP 범위 내인 경우 시작**

어느 옵션에서든 여러 범위를 지정할 수 있습니다. IPv4 주소만 지원됩니다.

예

평일마다 오후 9시에 데이터를 백업합니다. 머신이 VPN 터널을 통해 기업 네트워크에 연결된 경우에는 백업을 건너뛸 수 있습니다.

- 예약: **일일, 월요일~금요일 실행**. 시작 시간: **오후 9시**.
- 조건: **장치 IP 주소 확인, IP 범위 밖인 경우 시작, 시작**: <VPN IP 주소 범위 시작>, **끝**: <VPN IP 주소 범위 끝>.
- 백업 시작 조건: **조건이 충족될 때까지 대기**.

결과:

- 오후 9시에 머신 IP 주소가 지정된 범위 내에 있지 않으면 백업이 즉시 시작됩니다.
- 오후 9시에 머신 IP 주소가 지정된 범위 내에 있는 경우에는 해당 머신에 VPN 이외의 IP 주소가 설정되면 백업이 시작됩니다.
- 머신 IP 주소가 평일 오후 9시에 항상 지정된 범위 내에 있다면 백업이 시작되지 않습니다.

추가 예약 옵션

백업이 특정 조건 충족 시에만 실행되거나, 지정한 기간 동안만 실행되거나, 스케줄보다 지연되어 실행되도록 구성할 수 있습니다.

시작 조건을 구성하려면

© Acronis International GmbH, 2003-2024

1. 보호 계획에서 **백업** 모듈을 확장합니다.
2. **스케줄**을 클릭합니다.
3. **스케줄** 창에서 **더 많이 표시**를 클릭합니다.
4. 포함할 시작 조건 옆에 있는 확인란을 선택하고 **완료**를 클릭합니다.
   사용 가능한 시작 조건과 이러한 조건을 구성하는 방법에 대한 자세한 내용은 "시작 조건"(388 페이지) 항목을 참조하십시오.
5. 보호 계획을 저장합니다.

시간 범위를 구성하려면

1. 보호 계획에서 **백업** 모듈을 확장합니다.
2. **스케줄**을 클릭합니다.
3. **날짜 범위 내에서 계획 실행** 확인란을 선택합니다.
4. 필요에 따라 기간을 지정하고 **완료**를 클릭합니다.
5. 보호 계획을 저장합니다.

그러면 백업이 지정한 기간 동안에만 실행됩니다.

지연을 구성하려면

네트워크 위치 한 곳에 여러 워크로드를 백업할 때 네트워크에서 과도한 로드가 발생하지 않도록 짧은 지연(지연 시간은 임의로 지정됨)이 백업 옵션으로 구성됩니다. 지연을 비활성화하거나 지연 설정을 변경할 수 있습니다.

1. 보호 계획에서 **백업** 모듈을 확장합니다.
2. **백업 옵션**을 클릭하고 **일정 예약**을 선택합니다.
   각 워크로드에 대한 지연 값은 0에서 사용자가 지정하는 최대값 사이의 값으로 임의 선택됩니다. 기본적으로 최대값은 30분입니다.
   이 백업 옵션에 대한 자세한 내용은 "일정 예약"(445페이지) 항목을 참조하십시오
   각 워크로드에 대한 지연 값은 해당 워크로드에 보호 계획을 적용할 때 계산되며 최대 지연 값을 편집할 때까지 동일하게 유지됩니다.
3. 필요에 따라 기간을 지정하고 **완료**를 클릭합니다.
4. 보호 계획을 저장합니다.

수동으로 백업 실행

예약된 백업과 예약되지 않은 백업을 수동으로 실행할 수 있습니다.

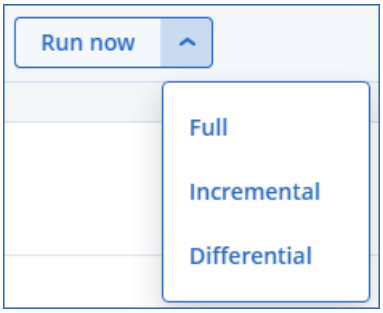
수동으로 백업을 실행하려면

1. Cyber Protect 콘솔에서 **장치**로 이동합니다.
2. 백업을 실행할 워크로드를 선택하고 **보호**를 클릭합니다.
3. 백업을 생성할 보호 계획을 선택합니다.
   워크로드에 보호 계획이 적용되어 있지 않으면 기존 계획을 적용하거나 새 계획을 생성합니다.
   보호 계획 생성 방법에 대한 자세한 내용은 "보호 계획 생성"(200페이지) 항목을 참조하십시오.
4. [기본 백업 유형을 생성하려면] 보호 계획에서 **지금 실행** 아이콘을 클릭합니다.

© Acronis International GmbH, 2003-2024

보호 계획에서 **백업** 모듈을 확장하고 **지금 실행** 버튼을 클릭해도 됩니다.

5. [특정 백업 유형을 생성하려면] 보호 계획에서 **백업** 모듈을 확장하고 **지금 실행** 버튼 옆의 화살표를 클릭한 후 백업 유형을 선택합니다.



참고
항상 증분(단일 파일), **항상 전체** 등의 한 가지 백업 방법만 사용하는 백업 구성표에서는 유형을 선택할 수 없습니다.

그러므로 백업 작업이 바로 시작됩니다. **장치** 탭의 **상태** 열에서 백업 진행 상황과 결과를 확인할 수 있습니다.

보관 규칙

오래된 백업을 자동으로 삭제하려면 보호 계획에서 백업 보존 규칙을 구성합니다.

다음 백업 속성을 기준으로 보존 규칙을 구성할 수 있습니다.

- 번호
- 기간
- 크기

사용 가능한 보존 규칙과 해당 옵션은 백업 구성표에 따라 다릅니다. 규칙은 에이전트, 워크로드 및 클라우드 간 백업에도 적용됩니다. 자세한 내용은 "백업 구성표에 따른 보존 규칙"(397페이지)을(를) 참조하십시오.

보존 규칙을 구성하면서 **무한히 백업 보관** 옵션을 선택하면 오래된 백업 자동 정리를 비활성화할 수 있습니다. 이 경우 스토리지 사용량이 늘어날 수 있으며 불필요한 이전 백업을 수동으로 삭제해야 합니다.

© Acronis International GmbH, 2003-2024

중요 팁

- 보존 규칙은 보호 계획에 포함된 요소입니다. 그러므로 계획을 해지하거나 삭제하면 해당 계획의 보존 규칙은 더 이상 적용되지 않습니다. 더 이상 필요하지 않은 백업 삭제 방법에 대한 자세한 내용은 "백업 삭제"(485페이지) 항목을 참조하십시오.
- 백업 구성표 및 백업 형식에 따라 각 백업이 개별 파일로 저장되는 경우에는 다른 증분 백업이나 차등 백업이 사용하는 백업을 삭제할 수 없습니다. 이 백업은 종속 백업에 적용된 보존 규칙에 따라 삭제됩니다. 이 구성을 사용할 때는 일부 백업의 삭제가 연기되므로 스토리지 사용량이 증가할 수 있습니다. 또한 백업의 크기, 수 또는 백업 기간이 사용자가 지정한 값을 초과할 수 있습니다. 이 동작을 변경하는 방법에 대한 자세한 내용은 "백업 통합"(409페이지) 항목을 참조하십시오.
- 기본적으로 보호 계획이 생성하는 최신 백업은 삭제되지 않습니다. 그러나 새 백업 작업을 시작하기 전에 백업을 정리하는 보존 규칙을 구성하고 유지할 백업의 수를 0으로 설정하면 최신 백업도 삭제됩니다.

경고!
백업이 하나인 백업 세트에 이 보존 규칙을 적용한 상태에서 백업 작업이 실패하면 데이터를 복구할 수 없게 됩니다. 새 백업이 생성되기 전에 기존 백업이 삭제되기 때문입니다.

백업 구성표에 따른 보존 규칙

사용 가능한 보존 규칙과 해당 설정은 보호 계획에서 사용하는 백업 구성표에 따라 다릅니다. 백업 구성표에 대한 자세한 내용은 "백업 구성표"(381페이지) 항목을 참조하십시오.

다음 표에는 사용 가능한 보존 규칙과 해당 설정이 요약되어 있습니다.

백업 구성표	예약	사용 가능한 보존 규칙 및 해당 설정
항상 증분(단일 파일)	매달 매주 매일 매시간 이벤트 트리거 백업	백업 수별 백업 기간별(월별, 주간, 일간, 매시간 백업용으로 각기 별도의 설정 사용 가능) 백업 무기한 보관
항상 전체	매달 매주 매일 매시간 이벤트 트리거 백업	백업 수별 백업 기간별(월별, 주간, 일간, 매시간 백업용으로 각기 별도의 설정 사용 가능) 백업의 총 크기 기준 백업 무기한 보관
매주 전체, 매일 증분	매일 이벤트 트리거 백업	백업 수별 백업 기간별(주간 및 일간 백업용으로 각기 별도의

© Acronis International GmbH, 2003-2024

백업 구성표	예약	사용 가능한 보존 규칙 및 해당 설정
		설정 사용 가능) 백업의 총 크기 기준 백업 무기한 보관
매월 전체, 매주 차등, 매일 증분	매달 매주 매일 매시간 이벤트 트리거 백업	백업 수별 백업 기간별(전체, 차등 및 증분 백업용으로 각기 별도의 설정 사용 가능) 백업의 총 크기 기준 백업 무기한 보관
사용자 정의	매달 매주 매일 매시간 이벤트 트리거 백업	백업 수별 백업 기간별(전체, 차등 및 증분 백업용으로 각기 별도의 설정 사용 가능) 백업의 총 크기 기준 백업 무기한 보관

매시간 구성표를 사용하는 월별 백업이 있는 이유

백업 구성표에 따라 **백업 기간별** 옵션을 구성할 수 있는 백업은

- 월별, 주간, 일간, 매시간 백업 중 하나입니다.
  시간을 기준으로 하여 사용자 정의 백업 구성표가 아닌 모든 백업 구성표에서 이러한 설정을 사용할 수 있습니다. 백업이 매시간 실행되도록 구성하더라도 이러한 모든 백업(월별, 주간, 일간, 매시간)을 사용할 수 있습니다. 아래 예를 참조하십시오.

백업	설명
매달	월별 백업은 매월 처음 생성되는 백업입니다.
매주	주간 백업은 주간 백업 옵션에서 지정하는 요일에 처음 생성되는 백업입니다. 보존 규칙 적용 시에는 이 요일이 한 주의 시작일로 간주됩니다. 해당 월의 첫 번째 백업인 주간 백업은 월별 백업으로 간주됩니다. 이 경우 주간 백업은 그 다음 주의 선택한 요일에 생성됩니다.
매일	일간 백업은 특정일에 처음 생성되며 월별 또는 주간 백업 정의에 해당되지 않는 백업입니다. 일간 백업이 월별 또는 주간 백업 정의에 해당되면 그 다음날 일간 백업이 생성됩니다.
매시간	매시간 백업은 특정 시간에 처음 생성되며 월별, 주간, 일간 백업 정의에 해당되지 않는 백업입니다. 매시간 백업이 월별, 주간, 일간 백업 정의에 해당되면 그 다음 시간에 매시간 백업이 생성됩니다.

© Acronis International GmbH, 2003-2024

- 전체, 차등 및 증분 백업.
  백업 방법을 기준으로 하여 **사용자 정의** 백업 구성표에서 이러한 설정을 사용할 수 있습니다. 사전 구성된 사용자 정의 구성표는 **매월 전체, 매주 차등, 매일 증분**입니다.

예

매시간 백업에는 기본 설정이 적용된 **항상 증분(단일 파일)** 백업 구성표를 사용합니다.

- 이 경우 백업은 시간을 기준으로 예약됩니다.
- 백업은 월~금요일 오전 8시~오후 6시에 1시간마다 실행됩니다.
- **주간 백업** 옵션 사용 시에는 백업일이 월요일로 설정됩니다.

보호 계획의 **보관 기간** 섹션에서 월별, 주간, 일간, 매시간 백업에 보존 규칙을 적용할 수 있습니다.

다음 표에는 8일의 기간 동안 생성되는 백업 유형이 요약되어 있습니다.

날짜	요일	설명
7월 1일	월요일	매월 처음 생성되는 백업은 월별 백업이므로 이 날짜에 처음 생성되는 백업이 월별 백업입니다. 이 날짜 동안 생성되는 나머지 백업은 매시간 백업입니다. 이 주에 처음 생성되는 백업은 월별 백업으로 간주됩니다. 그러므로 주간 백업은 없습니다. 그 다음 주에 처음 생성되는 백업이 주간 백업입니다.
7월 2일	화요일	이 날짜에 처음 생성되는 백업은 일간 백업이고 나머지 백업은 매시간 백업입니다.
7월 3일	수요일	이 날짜에 처음 생성되는 백업은 일간 백업이고 나머지 백업은 매시간 백업입니다.
7월 4일	목요일	이 날짜에 처음 생성되는 백업은 일간 백업이고 나머지 백업은 매시간 백업입니다.
7월 5일	금요일	이 날짜에 처음 생성되는 백업은 일간 백업이고 나머지 백업은 매시간 백업입니다.
7월 6일	토요일	이 날짜에 처음 생성되는 백업은 일간 백업이고 나머지 백업은 매시간 백업입니다.
7월 7일	일요일	이 날짜에 처음 생성되는 백업은 일간 백업이고 나머지 백업은 매시간 백업입니다.
7월 8일	월요일	이 날짜에 처음 생성되는 백업은 주간 백업이고 나머지 백업은 매시간 백업입니다.

보존 규칙 구성

보호 계획에 포함되어 있는 보존 규칙의 사용 가능 여부와 옵션은 백업 구성표에 따라 달라집니다. 자세한 내용은 "백업 구성표에 따른 보존 규칙"(397페이지)을(를) 참조하십시오.

보존 규칙을 구성하려면

© Acronis International GmbH, 2003-2024

1. 보호 계획에서 **백업** 모듈을 확장합니다.
2. **보관 개수**를 클릭합니다.
3. 다음 옵션 중 하나를 선택합니다.
   - **백업 수별**
   - **백업 기간별**

     월별, 주별, 일별 및 시간별 백업에 각기 별도의 설정을 사용할 수 있습니다. 모든 유형의 최대값은 9999입니다.

     모든 백업에 단일 설정을 사용할 수도 있습니다.
   - **백업의 총 크기 기준**

     항상 증분(단일 파일) 백업 구성표에는 이 설정을 사용할 수 없습니다.
   - **백업 무기한 보관**
4. [**백업 무기한 보관**을 선택하지 않은 경우] 선택한 옵션의 값을 구성합니다.
5. [**백업 무기한 보관**을 선택하지 않은 경우] 보존 규칙이 적용되는 경우를 선택합니다.
   - 백업 후
   - 백업 전

     Microsoft SQL Server 클러스터 또는 Microsoft Exchange Server 클러스터를 백업할 때는 이 옵션을 사용할 수 없습니다.
6. **완료**를 클릭합니다.
7. 보호 계획을 저장합니다.

복제

복제 시에는 각각의 새 백업이 복제 위치에 자동 복사됩니다. 복제 위치의 백업과 소스 위치의 백업은 서로 아무런 관계가 없습니다.

소스 위치의 마지막 백업만 복제됩니다. 그러나 네트워크 연결 문제 등으로 인해 이전 백업이 복제되지 않은 경우에는 마지막으로 정상 완료된 복제 이후 생성된 모든 백업이 복제 작업에 포함됩니다.

복제 작업이 중단되면 처리된 데이터가 다음 복제 작업에 사용됩니다.

참고
이 항목에서는 보호 계획에서 사용 가능한 복제 기능에 대해 설명합니다. 백업 복제 계획을 별도로 생성할 수도 있습니다. 자세한 내용은 "백업 복제"(185페이지)을(를) 참조하십시오.

사용 예제

- 안정적인 복구 지원

  백업을 즉시 복구용으로 온사이트에 저장하는 동시에, 주 위치에 영향을 주는 스토리지 장애나 자연 재해 발생 시에도 백업을 안전하게 보관할 수 있도록 오프사이트에도 저장할 수 있습니다.
- 클라우드 스토리지를 사용하여 자연재해로부터 데이터 보호

  데이터 변경 사항만 전송하여 클라우드 스토리지로 백업을 복제합니다.
- 최신 복구 지점만 유지

© Acronis International GmbH, 2003-2024

스토리지 비용을 절약할 수 있도록 고속 스토리지에서 오래된 백업을 삭제하는 보존 규칙을 구성합니다.

지원되는 위치

위치	소스 위치	복제 위치
로컬 폴더	+	+
네트워크 폴더	+	+
클라우드 스토리지	-	+
Secure Zone	+	–
퍼블릭 클라우드	+	+

복제를 활성화하려면

1. 보호 계획에서 **백업** 모듈을 확장하고 **위치 추가**를 클릭합니다.

   참고
   백업할 위치에서 클라우드 스토리지를 선택하면 **위치 추가** 옵션을 사용할 수 없습니다.

2. 사용 가능한 위치 목록에서 복제 위치를 선택합니다.
   보호 계획의 위치는 복제에 추가한 위치의 수에 따라서 **두 번째 위치**, **세 번째 위치**, **네 번째 위치**, 혹은 **다섯 번째 위치**로 나타납니다.
3. [선택 사항] 기어 아이콘을 클릭하여 복제 위치의 옵션을 구성합니다.
   - **성능 및 백업 할당 시간** - "성능 및 백업 할당 시간"(436페이지)에 설명된 대로 선택한 위치의 백업 할당 시간을 설정합니다. 이러한 설정에 따라 복제 성능이 정의됩니다.
   - **위치 제거** - 현재 선택한 복제 위치를 삭제합니다.
   - [클라우드 스토리지 전용] **실제 데이터 전달** - 이동 가능 스토리지 장치에 초기 백업을 저장한 다음 인터넷에서 복제하는 대신 클라우드 스토리지에 업로드할 수 있도록 배송합니다.
     이 옵션은 네트워크 연결이 느린 위치 혹은 네트워크 상으로 큰 파일 전송의 대역폭을 저장하고자 하는 경우 적합합니다. 옵션을 활성화하기 위해서 고급 Cyber Protect 서비스 할당량이 필요하지는 않지만, 전송 명령을 생성하고 트랙하기 위해서는 실제 데이터 전송 서비스 할당량이 필요합니다. "실제 데이터 전달"(440페이지)을(를) 참조하십시오.

     참고
     이 옵션은 릴리스 C21.06 이상의 Protection 에이전트 버전에서 지원됩니다.
4. [선택 사항] 복제 위치의 **보관 개수** 행에서는 "보관 규칙"(396페이지)의 설명에 따라 해당 위치의 보존 규칙을 구성합니다.
5. [선택 사항] 1~4단계를 반복하여 복제 위치를 더 추가합니다.
   최대 4개의 복제 위치(**두 번째 위치**, **세 번째 위치**, **네 번째 위치**, **다섯 번째 위치**)를 구성할 수 있습니다. **클라우드 스토리지**를 선택하는 경우에는 복제 위치를 더 추가할 수 없습니다.

© Acronis International GmbH, 2003-2024

중요
동일한 보호 계획에서 백업 및 복제를 활성화하는 경우 예약된 다음 백업 전에 복제가 완료되어야 합니다. 복제가 여전히 진행 중인 경우 예약된 백업이 시작되지 않습니다. 예를 들어, 복제를 완료하는 데 26시간이 걸리면 24시간마다 한 번씩 실행되는 예약된 백업이 시작되지 않습니다.

이러한 종속성을 방지하려면 별도의 백업 복제 계획을 사용해야 합니다. 이 특정 계획에 대한 자세한 내용은 "백업 복제"(185페이지) 항목을 참조하십시오.

암호화

GCM(Galois/Counter) 모드에서 작동하는 AES(고급 암호화 표준) 암호 알고리즘은 무작위로 생성된 256비트 키를 사용합니다. 이 암호화 키는 암호의 SHA-2(256비트) 해시를 키로 사용하여 AES-256으로 암호화됩니다. 암호 자체는 디스크나 백업 어디에도 저장되지 않으며, 암호 해시를 사용하여 암호가 검증됩니다.

이 두 가지 수준의 보안을 사용하여 백업 데이터는 무단 액세스로부터 보호되지만 분실된 암호는 복구할 수 없습니다.

참고
강력한 암호를 사용하는 AES-256 알고리즘은 양자 저항성 암호화를 제공하며, 이는 양자 컴퓨팅에 의존하는 암호 분석 공격에 대해 안전합니다.

특히 회사의 규정 준수에 따라야 하는 경우 클라우드 스토리지에 저장된 모든 백업을 암호화하는 것이 좋습니다.

다음과 같은 방법으로 암호화를 구성할 수 있습니다:

- 보호 계획에서
- 머신 속성으로, Cyber Protect 모니터 또는 명령줄 인터페이스를 사용하여

보호 계획에서 암호화 구성

보호 계획에서는 암호화가 기본적으로 활성화되며 AES-256 알고리즘이 사용됩니다.

강력한 암호 사용 시 AES-256 알고리즘을 통해 양자 저항성 암호화가 적용됩니다.

규제 준수 모드가 적용된 계정에서는 보호 계획에서 암호화를 구성할 수 없습니다. 보호되어 있는 장치에서 암호화를 구성하는 방법에 대한 자세한 내용은 "머신 속성으로 암호화 설정"(403페이지) 항목을 참조하십시오.

암호화 구성 방법

1. 보호 계획에서 **백업** 모듈을 확장합니다.
2. **암호화**에서 **암호 지정**을 클릭합니다.
3. 암호화 비밀번호를 지정한 후 확인합니다.
4. **확인**을 클릭합니다.

© Acronis International GmbH, 2003-2024

경고!
비밀번호를 잃어버리거나 기억나지 않으면 암호화된 백업을 복구할 방법이 없습니다.

보호 계획을 적용한 후에 암호화 설정을 변경할 수 없습니다. 다른 암호화 설정을 사용하려면 새로운 계획을 생성합니다.

머신 속성으로 암호화 설정

머신 속성으로 백업 암호화를 구성할 수 있습니다. 이 경우 백업 암호화는 보호 계획에서가 아니라 보호된 워크로드에서 구성됩니다. 머신 속성으로 암호화는 256비트 키(AES-256)를 사용하는 AES 알고리즘을 사용합니다.

참고
강력한 암호를 사용하는 AES-256 알고리즘은 양자 저항성 암호화를 제공하며, 이는 양자 컴퓨팅에 의존하는 암호 분석 공격에 대해 안전합니다.

머신 속성으로 암호화를 구성하는 것은 다음과 같은 방식으로 보호 계획에 영향을 미칩니다.

- **보호 계획이 이미 머신에 적용되었습니다.** 보호 계획의 암호화 설정이 다른 경우 백업에 실패합니다.
- **머신에 나중에 적용될 보호 계획입니다.** 머신에 저장된 암호화 설정은 보호 계획의 암호화 설정을 재정의합니다. 백업 모듈 설정에서 암호화가 비활성화되어 있더라도 모든 백업은 암호화됩니다.

규제 전수 모드의 계정의 경우 머신 속성으로 암호화만 사용할 수 있습니다.

동일한 vCenter Server에 연결된 Agent for VMware를 두 개 이상 가지고 있고, 머신 속성으로 암호화를 구성하는 경우, 에이전트 간 로드 밸런싱 때문에 Agent for VMware가 있는 모든 머신에서 동일한 암호화 암호를 사용해야 합니다.

다음과 같은 방식으로 머신 속성으로 암호화를 구성할 수 있습니다.

- 명령줄에서
- Cyber Protect 모니터에서(Windows 및 macOS에서 사용 가능)

암호화를 구성하는 방법

명령줄에서

1. 관리자로 로그인(Windows의 경우)하거나 루트 사용자로 로그인(Linux의 경우)합니다.
2. 명령줄에서 다음 명령을 실행합니다.
   - Windows:

     ```
     <installation_path>\PyShell\bin\acropsh.exe -m manage_creds --set-password
     <encryption_password>
     ```

     기본적으로 설치 경로는 `%ProgramFiles%\BackupClient`입니다.
   - Linux:

© Acronis International GmbH, 2003-2024

```
/usr/sbin/acropsh -m manage_creds --set-password <encryption_password>
```

- 가상 어플라이언스의 경우

```
 /./sbin/acropsh -m manage_creds --set-password <encryption_password>
```

경고!
비밀번호를 잃어버리거나 기억나지 않으면 암호화된 백업을 복구할 방법이 없습니다.

Cyber Protect 모니터에서

1. 관리자로 로그인합니다.
2. 알림 영역(Windows의 경우) 또는 메뉴 바(macOS의 경우)에서 Cyber Protect 모니터 아이콘을 클릭합니다.
3. 기어 아이콘을 클릭한 다음 **설정** > **암호화**를 클릭합니다.
4. **이 머신에 대한 암호 설정**을 선택합니다. 암호화 암호를 지정하고 확인합니다.
5. **저장**을 클릭합니다.

경고!
비밀번호를 잃어버리거나 기억나지 않으면 암호화된 백업을 복구할 방법이 없습니다.

암호화 설정을 재설정하는 방법

1. 관리자로 로그인(Windows의 경우)하거나 루트 사용자로 로그인(Linux의 경우)합니다.
2. 명령줄에서 다음 명령을 실행합니다.
   - Windows:

     ```
     <installation_path>\PyShell\bin\acropsh.exe -m manage_creds --reset
     ```

     기본적으로 설치 경로는 `%ProgramFiles%\BackupClient`입니다.
   - Linux:

     ```
     /usr/sbin/acropsh -m manage_creds --reset
     ```

   - 가상 어플라이언스의 경우

     ```
     /./sbin/acropsh -m manage_creds --reset
     ```

중요
보호 계획이 백업을 생성한 후에 머신 속성으로 암호화를 재설정하거나 암호화 암호를 변경하는 경우 그 다음 백업 작업이 실패합니다. 워크로드를 계속 백업하려면 새로운 보호 계획을 생성합니다.

© Acronis International GmbH, 2003-2024

공증

참고
이 기능은 Advanced Backup 팩에서 사용할 수 있습니다.

공증을 사용하면 파일이 신뢰할 수 있고 백업된 후 변경되지 않았음을 증명할 수 있습니다. 법적 문서 파일이나 입증된 신뢰성이 필요한 기타 파일을 보호할 때에는 공증을 활성화하는 것이 좋습니다.

공증은 파일 수준 백업에만 사용할 수 있습니다. 디지털 서명이 있는 파일은 공증이 필요하지 않기 때문에 건너뜁니다.

다음과 같은 경우 공증을 사용할 수 *없습니다*.

- 백업 형식이 **버전 11**로 설정된 경우
- 백업 목적지가 Secure Zone인 경우

공증 사용 방법

백업용으로 선택된 모든 파일(디지털 서명이 있는 파일 제외)의 공증을 활성화하려면 보호 계획을 생성할 때 **공증** 스위치를 활성화합니다.

복구를 구성할 때 공증된 파일에 특별한 아이콘이 표시되고, 이를 통해 파일 신뢰성을 확인할 수 있습니다.

작동법

백업 중에 에이전트가 백업된 파일의 해시 코드를 계산하고, 해시 트리(폴더 구조 기반)를 생성하고, 트리를 백업에 저장한 다음 해시 트리 루트를 공증 서비스로 전송합니다. 공증 서비스는 Ethereum 블록체인 데이터베이스에 해시 트리 루트를 저장하여 이 값이 변경되지 않도록 합니다.

파일 신뢰성을 확인할 때 에이전트가 파일의 해시를 계산한 다음 이를 백업 내부의 해시 트리에 저장되어 있는 해시와 비교합니다. 두 해시가 일치하지 않으면 파일이 신뢰할 수 없는 것으로 간주됩니다. 그렇지 않으면 해시 트리에 의해 파일 신뢰성이 보증됩니다.

해시 트리 자체가 손상되지 않았는지 확인하기 위해 에이전트는 해시 트리 루트를 공증 서비스로 전송합니다. 공증 서비스는 이를 블록체인 데이터베이스에 저장되어 있는 해시 트리 루트와 비교합니다. 해시가 일치하면 선택한 파일은 신뢰할 수 있는 것으로 보증됩니다. 그렇지 않으면 소프트웨어에 파일을 신뢰할 수 없다는 메시지가 표시됩니다.

기본 백업 옵션

백업 옵션의 기본값은 회사, 부서 및 사용자 수준에 존재합니다. 회사 또는 부서 내에서 부서 또는 사용자 계정이 생성될 때 회사나 부서에 설정된 기본값을 상속하게 됩니다.

© Acronis International GmbH, 2003-2024

회사 관리자, 부서 관리자, 그리고 관리자 권한이 없는 모든 사용자는 기본 옵션 값을 미리 정의된 값으로 변경할 수 있습니다. 변경이 수행된 후 해당 수준에서 생성된 모든 보호 계획에서 새 값이 기본적으로 사용됩니다.

보호 계획을 생성할 때 이 계획에만 적용되는 사용자 정의 값으로 기본값을 오버라이드할 수 있습니다.

기본 옵션 값을 변경하려면

1. 다음 중 하나를 수행하십시오.
   - 회사의 기본값을 변경하려면 Cyber Protect 콘솔에 회사 관리자로 로그인합니다.
   - 부서의 기본값을 변경하려면 Cyber Protect 콘솔에 해당 부서 관리자로 로그인합니다.
   - 자신의 기본값을 변경하려면 관리자 권한이 없는 계정을 사용해 Cyber Protect 콘솔에 로그인합니다.
2. **설정** > **시스템 설정**을 클릭합니다.
3. **기본 백업 옵션** 섹션을 확장합니다.
4. 옵션을 선택하고 필요한 변경 작업을 수행합니다.
5. **저장**을 클릭합니다.

백업 옵션

보호 계획의 백업 옵션을 수정하려면 **백업** 모듈의 **백업 옵션** 필드에서 **변경**을 클릭합니다.

백업 옵션의 사용 가능성

사용 가능한 백업 옵션은 다음에 따라 다릅니다.

- 에이전트를 운영하는 환경(Windows, Linux, macOS).
- 백업하는 데이터 유형(디스크, 파일, 가상 머신, 애플리케이션 데이터).
- 백업 목적지(클라우드 스토리지, 로컬 또는 네트워크 폴더).

다음 표는 백업 옵션의 사용 가능성을 요약해서 보여줍니다.

	디스크 수준 백업			파일 수준 백업			가상 머신			SQL 및 Exchange
	Windows	**Linux**	**macOS**	**Windows**	**Linux**	**macOS**	**ESXi**	**Hyper-V**	**Virtuozzo**	**Windows**
경보	+	+	+	+	+	+	+	+	+	+
백업 통합	+	+	+	+	+	+	+	+	+	-
백업 파일 이름	+	+	+	+	+	+	+	+	+	+
백업 형	+	+	+	+	+	+	+	+	+	+

© Acronis International GmbH, 2003-2024

식										
백업 유효성 검사	+	+	+	+	+	+	+	+	+	+
CBT (Changed Block Tracking)	+	-	-	-	-	-	+	+	-	-
클러스터 백업 모드	-	-	-	-	-	-	-	-	-	+
압축 수준	+	+	+	+	+	+	+	+	+	+
오류 처리										
오류 발생 시 재시도	+	+	+	+	+	+	+	+	+	+
처리할 동안 메시지 및 대화 상자 표시 안 함(자동 모드)	+	+	+	+	+	+	+	+	+	+
불량 섹터 무시	+	-	+	+	-	+	+	+	+	-
VM 스냅샷 생성 도중 오류가 발생하는 경우 재시도	-	-	-	-	-	-	+	+	+	-
빠른 증분/차등 백업	+	+	+	-	-	-	-	-	-	-
파일 수준 백업 스냅샷	-	-	-	+	+	+	-	-	-	-

© Acronis International GmbH, 2003-2024

파일 필터	+	+	+	+	+	+	+	+	+	-
포렌직 데이터	+	-	-	-	-	-	-	-	-	-
로그 자르기	-	-	-	-	-	-	+	+	-	SQL만 해당
LVM 스냅샷 촬영	-	+	-	-	-	-	-	-	-	-
마운트 포인트	-	-	-	+	-	-	-	-	-	-
다중 볼륨 스냅샷	+	+	-	+	+	-	-	-	-	-
원클릭 복구	+	+	-	-	-	-	-	-	-	-
성능 및 백업 할당 시간	+	+	+	+	+	+	+	+	+	+
실제 데이터 전달	+	+	+	+	+	+	+	+	+	-
사전/사후 명령어	+	+	+	+	+	+	+	+	+	+
데이터 캡처 전/후 명령	+	+	+	+	+	+	-	-	-	+
일정 예약										
기간 내에서 시작 시간 분배	+	+	+	+	+	+	+	+	+	+
동시에 실행되는 백업 수 제한	-	-	-	-	-	-	+	+	+	-
섹터 단	+	+	-	-	-	-	+	+	+	-

© Acronis International GmbH, 2003-2024

위 백업										
분할	+	+	+	+	+	+	+	+	+	+
작업 실패 처리	+	+	+	+	+	+	+	+	+	+
작업 시작 조건	+	+	-	+	+	-	+	+	+	+
VSS (Volume Shadow Copy Service)	+	-	-	+	-	-	-	+	-	+
가상 머신용 VSS (Volume Shadow Copy Service)	-	-	-	-	-	-	+	+	-	-
주간 백업	+	+	+	+	+	+	+	+	+	+
Windows 이벤트 로그	+	-	-	+	-	-	+	+	-	+

경보

지정된 기간(일) 동안 성공적인 백업이 진행되지 않음

사전 설정값이 **비활성화됨**.

이 옵션은 지정된 기간 동안 보호 계획에서 수행한 성공적인 백업이 없는 경우에 대한 경보 생성 여부를 결정합니다. 소프트웨어는 실패한 백업 외에도 스케줄에 따라 실행되지 않은 백업(누락된 백업)의 수도 계산합니다.

경보는 머신당 기준으로 생성되고 **경보** 탭에 표시됩니다.

경보가 생성된 후 백업 없이 연속으로 보낼 수 있는 일 수를 지정할 수 있습니다.

백업 통합

이 옵션은 정리 중에 백업을 통합하거나 전체 백업 체인을 삭제할지 여부를 정의합니다.

사전 설정값이 **비활성화됨**입니다.

통합은 둘 이상의 후속 백업을 단일 백업으로 결합하는 프로세스입니다.

© Acronis International GmbH, 2003-2024

이 옵션이 활성화되어 있으면 정리 중 삭제되어야 하는 백업이 다음 종속 백업(증분 또는 차등)과 통합됩니다.

그렇지 않으면 종속된 모든 백업이 삭제될 때까지 해당 백업이 보관됩니다. 이렇게 하면 시간 소모적인 통합을 피하는 데 도움은 되지만 삭제가 연기되는 백업을 저장해둘 추가 공간이 필요합니다. 백업의 수명 또는 개수가 보관 규칙에 지정되어 있는 값을 초과할 수 있습니다.

중요
통합은 단지 삭제 방법일 뿐 삭제의 대안이 아님을 유의하십시오. 이렇게 생성된 백업에는 삭제된 백업에 있었고, 보관된 증분 또는 차등 백업에 없었던 데이터는 포함되지 않습니다.

다음에 해당하는 경우 이 옵션이 적용되지 *않습니다*.

- 백업 목적지가 클라우드 스토리지입니다.
- 백업 구성표가 **항상 증분(단일 파일)**으로 설정되어 있습니다.
- 백업 형식이 **버전 12**로 설정되어 있습니다.

클라우드 스토리지에 저장된 백업과 단일 파일 백업(버전 11 및 12 형식 모두)의 경우 빠르고 간편한 통합을 위해 내부 구조가 생성되므로 항상 통합됩니다.

그러나 버전 12 형식을 사용하고 여러 백업 체인이 있는 경우(모든 체인이 별도의 .tibx 파일에 저장됨) 통합은 마지막 체인 내에서만 작동합니다. 메타 정보(~12KB)를 유지하기 위해 최소 크기로 줄어든 첫 번째 체인을 제외하고 다른 모든 체인은 전체적으로 삭제됩니다 동시 읽기 및 쓰기 작업 중 데이터 일관성을 보장하는 데 이 메타 정보가 필요합니다. 이러한 체인에 포함된 백업은 보관 규칙이 적용되는 즉시 GUI에서 사라지지만 전체 체인이 삭제될 때까지 실제로 존재합니다.

그 밖의 모든 경우에는 삭제가 연기된 백업에 GUI의 휴지통 아이콁( )이 표시됩니다. X 기호를 눌러 백업을 삭제하면 통합이 수행됩니다.

백업 파일 이름

이 옵션은 클라우드 애플리케이션 백업 계획이나 보호 계획에서 생성된 백업 파일의 이름을 정의합니다.

보호 계획에서 생성된 백업 파일의 경우에는 백업 위치를 찾아볼 때 파일 관리자에서 이러한 이름을 확인할 수 있습니다.

백업 파일이란 무엇입니까?

각 보호 계획은 사용되는 백업 구성표 및 백업 형식에 따라 백업 위치에서 하나 이상의 파일을 생성합니다. 다음 표에는 머신 또는 사서함별로 생성될 수 있는 파일이 나와 있습니다.

	항상 증분(단일 파일)	**기타 백업 구성표**
버전 11 백업 형식	TIB 파일 1개 및 XML 메타데이터 파일 1개	TIB 파일 여러 개 및 XML 메타데이터 파일 1개

© Acronis International GmbH, 2003-2024

버전 12 백업 형식	백업 체인당 TIBX 파일 1개(전체 또는 차등 백업, 이에 의존하는 증분 백업). 로컬 또는 네트워크(SMB) 폴더에 저장된 파일의 크기가 200GB를 초과할 경우, 해당 파일은 기본적으로 200GB 크기 파일로 분할됩니다.

모든 파일의 이름이 동일하고 타임 스탬프 또는 일련 번호가 추가되거나 추가되지 않습니다. 보호 계획 또는 클라우드 애플리케이션 백업 계획을 생성하거나 편집할 때 이 이름(백업 파일 이름이라고 함)을 정의할 수 있습니다.

참고
타임 스탬프는 버전 11 백업 형식의 백업 파일 이름에만 추가됩니다.

보호 계획이나 클라우드 애플리케이션 백업 계획에서 백업 파일 이름을 변경한 후에 생성하는 다음 백업은 전체 백업이 됩니다.

같은 머신의 기존 백업 파일 이름을 지정하는 경우에는 계획 스케줄에 따라 전체 백업, 증분 백업 또는 차등 백업이 생성됩니다.

참고
백업 파일(.tibx)을 원래 스토리지에서 다른 위치로 이동할 때는 파일 이름을 변경하지 마십시오. 이름을 변경한 파일은 손상된 것으로 표시되므로 해당 파일에서 데이터를 복구할 수 없게 됩니다.

클라우드 스토리지처럼 파일 관리자를 통해 이동할 수 없는 위치에 대한 백업 파일 이름을 설정할 수 있습니다. 이 경우에는 **백업 스토리지** 탭에 사용자 정의 이름이 표시됩니다.

백업 파일 이름은 어디에서 볼 수 있습니까?

보호 계획의 경우 **백업 스토리지** 탭에서 위치를 선택한 다음 백업 아카이브를 선택합니다.

- 기본 백업 파일 이름이 **상세정보** 패널에 표시됩니다.
- 기본값이 아닌 백업 파일 이름을 설정하면 해당 이름이 바로 **백업 스토리지** 탭, **이름** 열에 표시됩니다.

클라우드 애플리케이션 백업 계획의 경우 **백업 스토리지** 탭에서 위치를 선택하고, 백업 아카이브를 선택한 다음 기어 아이콘을 클릭합니다.

백업 파일 이름에 대한 제한 사항

- 백업 파일 이름은 숫자로 끝날 수 없습니다.
  기본 백업 파일 이름에는 이름이 숫자로 끝나지 않도록 문자 "A"가 추가됩니다. 사용자 정의 이름을 생성할 경우 항상 숫자로 끝나지 않는지 확인하십시오. 변수를 사용할 경우 변수는 숫자로 끝날 수 있으므로 이름은 변수로 끝나지 않아야 합니다.
- 백업 파일 이름에는 다음 기호가 포함될 수 없습니다. **()&?*$<>":\|/#**, 줄 끝(**\n**) 및 탭(**\t**).

참고
사용자가 쉽게 파악할 수 있는 백업 파일 이름을 선택합니다. 이렇게 하면 파일 관리자를 통해 백업 위치를 찾아볼 때 백업을 쉽게 구별할 수 있습니다.

© Acronis International GmbH, 2003-2024

기본 백업 파일 이름

전체 실제 머신 및 가상 머신, 디스크/볼륨, 파일/폴더, Microsoft SQL Server 데이터베이스, Microsoft Exchange Server 데이터베이스, ESXi 구성의 백업에 대한 기본 백업 파일 이름은 `[Machine Name]-[Plan ID]-[Unique ID]A`입니다.

로컬 Agent for Microsoft 365에 의해 생성되는 Exchange 사서함 백업 및 Microsoft 365 사서함 백업의 기본 이름은 `[Mailbox ID]_mailbox_[Plan ID]A`입니다.

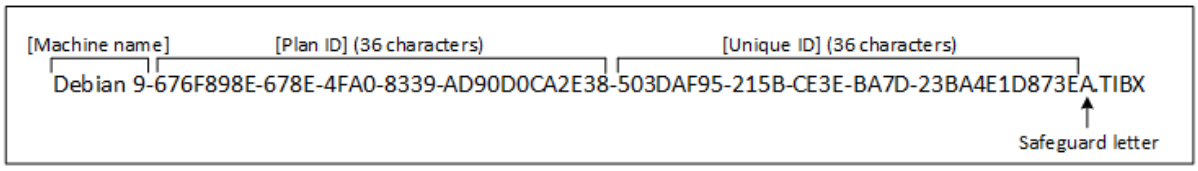
Microsoft Azure 백업의 기본 이름 앞에는 `[Mailbox ID]_` 접두사가 표시됩니다. 이 접두사는 제거할 수 없습니다.

클라우드 에이전트에 의해 생성되는 클라우드 애플리케이션 백업의 기본 이름은 `[Resource Name]_[Resource Type]_[Resource Id]_[Plan Id]A`입니다.

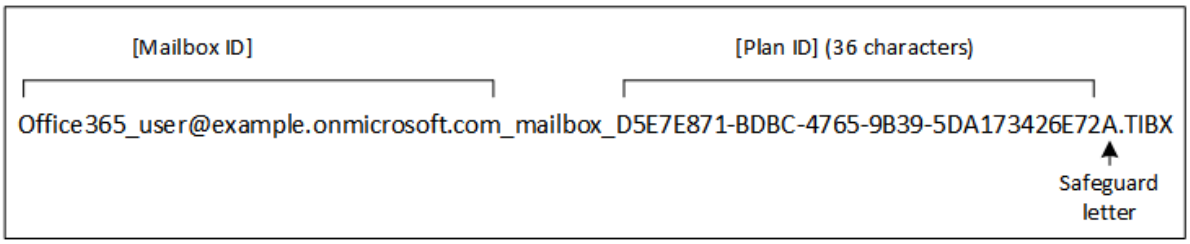
기본 이름은 다음 변수로 구성됩니다.

- `[Machine Name]`이 변수는 머신 이름으로 바뀝니다(Cyber Protect 콘솔에 표시된 동일한 이름).
- `[Plan ID]`, `[Plan Id]`이 변수는 보호 계획의 고유 식별자로 바뀝니다. 계획 이름이 바뀔 경우 이 값은 변경되지 않습니다.
- `[Unique ID]`이 변수는 선택한 머신의 고유 식별자로 바뀝니다. 머신 이름이 바뀔 경우 이 값은 변경되지 않습니다.
- `[Mailbox ID]`이 변수는 사서함 사용자의 계정 이름(UPN)으로 바뀝니다.
- `[Resource Name]`이 변수는 사용자의 계정 이름(UPN), SharePoint 사이트 URL 또는 Shared Drive 이름 등의 클라우드 데이터 소스 이름으로 바뀝니다.
- `[Resource Type]`이 변수는 `mailbox`, `O365Mailbox`, `O365PublicFolder`, `OneDrive`, `SharePoint`, `GDrive` 등의 클라우드 데이터 소스 유형으로 바뀝니다.
- `[Resource ID]`이 변수는 클라우드 데이터 소스의 고유 식별자로 바뀝니다. 클라우드 데이터 소스 이름이 바뀔 경우 이 값은 변경되지 않습니다.
- `"A"`는 이름이 숫자로 끝나지 않도록 추가되는 보호 문자입니다.

아래 다이어그램에는 기본 백업 파일 이름이 표시됩니다.



아래 다이어그램은 로컬 에이전트에 의해 수행된 Microsoft 365 사서함 백업의 기본 백업 파일 이름을 보여줍니다.



© Acronis International GmbH, 2003-2024

변수 없는 이름

백업 파일 이름을 MyBackup으로 변경하면 백업 파일이 다음 예제와 같이 표시됩니다. 두 예제에서는 모두 일일 증분 백업이 2016년 9월 13일부터 14시 40분에 스케줄되었다고 가정합니다.

항상 증분(단일 파일) 백업 구성표를 사용한 버전 12 형식의 경우:

```
MyBackup.tibx
```

기타 백업 구성표를 사용한 버전 12 형식의 경우:

```
MyBackup.tibx
MyBackup-0001.tibx
MyBackup-0002.tibx
...
```

변수 사용

기본적으로 사용되는 변수 외에 다음 변수도 사용할 수 있습니다.

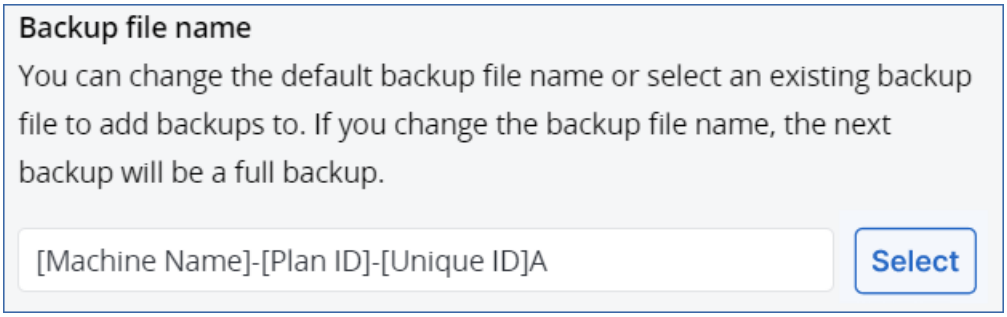
- `[Plan name]` 변수는 보호 계획의 이름으로 바뀝니다.
- `[Virtualization Server Type]` 변수는 가상 머신이 Agent for VMware에 의해 백업되는 경우에는 "vmwesx", 가상 머신이 Agent for Hyper-V에 의해 백업되는 경우 "mshyperv"로 바뀝니다.

백업할 머신 또는 사서함을 여러 개 선택할 경우 백업 파일 이름에는 `[Machine Name]`, `[Unique ID]`, `[Mailbox ID]`, `[Resource Name]` 또는 `[Resource Id]` 변수가 포함되어야 합니다.

기존 백업 아카이브에서 백업 생성하기

워크로드의 백업을 기존 백업 아카이브에 추가하도록 설정할 수 있습니다.

예를 들어 이 옵션은 보호 계획이 단일 머신에 적용되고, 이 머신을 Cyber Protect 콘솔에서 제거해야 하거나 에이전트와 구성 설정을 함께 설치 제거해야 할 때 유용할 수 있습니다. 머신을 다시 추가하거나 에이전트를 재설치한 후에는 보호 계획을 원래의 아카이브로 백업을 계속하도록 강제 적용할 수 있습니다.



기존 백업 아카이브에 워크로드의 백업을 추가하도록 설정하는 방법

클라우드 간 워크로드가 아닌 워크로드

© Acronis International GmbH, 2003-2024

1. **모든 장치** 화면에서 워크로드를 클릭한 다음 **보호**를 클릭합니다.
2. 보호 계획 설정에서 **백업** 모듈을 확장합니다.
3. **백업 옵션**을 클릭한 다음에 **변경**을 클릭합니다.
4. **파일 백업 이름** 탭에서 **선택**을 클릭합니다.
   선택 버튼은 보호 계획의 **백업할 위치** 섹션에서 선택한 위치의 백업을 표시합니다.

   참고
   선택 버튼은 생성되어 단일 워크로드에 적용된 보호 계획에 대해서만 사용할 수 있습니다.

5. 아카이브를 선택한 다음 **완료**를 클릭합니다.
6. **완료**를 클릭한 다음 **적용**을 클릭합니다.

클라우드 간 워크로드

1. **관리** > **클라우드 애플리케이션 백업** 탭에서 계획을 선택합니다.
2. **편집**을 클릭한 다음 계획의 이름 옆에 있는 기어 아이콘을 클릭합니다.
3. **파일 백업 이름** 탭에서 **선택**을 클릭합니다.

   참고
   선택 버튼은 단일 워크로드에 대해 생성되고 적용되는 백업 계획에만 사용할 수 있습니다.

4. 백업 아카이브를 선택한 다음 **완료**를 클릭합니다.
5. **완료**를 클릭한 다음 **변경 사항 저장**을 클릭합니다.

백업 형식

백업 형식 옵션은 보호 계획에서 생성된 백업의 형식을 정의합니다. 이 옵션은 이미 버전 11 백업 형식을 사용 중인 보호 계획에 대해서만 표시됩니다. 이에 해당하는 경우, 백업 형식을 버전 12로 변경할 수 있습니다. 백업 형식을 버전 12로 변경한 후에는 해당 옵션을 사용할 수 없습니다.

- **버전 11**
  하위 호환성을 위해 보존된 레거시 형식입니다.

  참고
  백업 형식 버전 11을 사용하면 데이터베이스 가용성 그룹(DAG)을 백업할 수 없습니다. DAG의 백업은 버전 12 형식에서만 지원됩니다.

- **버전 12**
  백업과 복구를 더욱 빠르게 수행할 수 있도록 Acronis Backup 12에서 도입된 백업 형식입니다. 각 백업 체인(전체 또는 차등 백업, 이에 의존하는 증분 백업)은 단일 TIBX 파일에 저장됩니다.

백업 형식 및 백업 파일

파일 관리자를 통해 찾아볼 수 있는 백업 위치(예: 로컬 또는 네트워크 폴더)의 경우 백업 형식에 따라 파일 개수와 파일 확장명이 결정됩니다. 다음 표에는 머신 또는 사서함별로 생성될 수 있는 파일이 나와 있습니다.

© Acronis International GmbH, 2003-2024

	항상 증분(단일 파일)	기타 백업 구성표
버전 11 백업 형식	TIB 파일 1개 및 XML 메타데이터 파일 1개	TIB 파일 여러 개 및 XML 메타데이터 파일 1개
버전 12 백업 형식	백업 체인당 TIBX 파일 1개(전체 또는 차등 백업, 이에 의존하는 증분 백업). 로컬 또는 네트워크(SMB) 폴더에 저장된 파일의 크기가 200GB를 초과할 경우, 해당 파일은 기본적으로 200GB 크기 파일로 분할됩니다.	

백업 형식을 버전 12(TIBX)로 변경

백업 형식을 버전 11(TIB 형식)에서 버전 12(TIBX 형식)로 변경 시:

- 다음 백업이 전체 백업으로 진행됩니다.
- 파일 관리자를 통해 찾아볼 수 있는 백업 위치(예: 로컬 또는 네트워크 폴더)에 새로운 TIBX 파일이 생성됩니다. 새로운 파일은 원래 파일과 이름이 동일하지만, 접미사 **_v12A**가 추가됩니다.
- 보관 규칙 및 복제는 새로운 백업에만 적용됩니다.
- 이전 백업은 삭제되지 않으며, **백업 스토리지** 탭에서 사용할 수 있습니다. 이전 백업은 수동으로 삭제할 수 있습니다.
- 이전 클라우드 백업은 **클라우드 스토리지** 할당량을 소비하지 않습니다.
- 이전 클라우드 백업은 수동으로 삭제할 때까지 **로컬 백업** 할당량을 소비합니다.

아카이브 내 중복 제거

버전 12의 TIBX 백업 형식은 다음과 같은 이점이 있는 아카이브 내 중복 제거를 지원합니다.

- 모든 데이터 유형에 대해 내장된 블록 수준 중복 제거를 통해 백업 크기 대폭 감소
- 하드 링크의 효율적 처리로 스토리지 중복이 없도록 보장
- 해시 기반 청크

참고
아카이브 내 중복 제거는 TIBX 형식의 모든 백업에 대해 기본적으로 활성화되어 있습니다. 백업 옵션에서 따로 활성화할 필요가 없으며, 비활성화할 수 없습니다.

여러 제품 버전 간의 백업 형식 호환성

백업 형식 호환성에 대한 자세한 내용은 여러 제품 버전(1689) 간의 백업 아카이브 호환성을 참조하십시오.

백업 유효성 검사

유효성 검사는 백업에서 데이터를 복구할 수 있는지 그 가능성을 확인하는 작업입니다. 이 옵션을 활성화하면 보호 계획에 따라 각 백업이 생성될 때마다 체크섬 확인 방법을 사용하여 백업의 유효성을 즉시 검사합니다. 이 작업은 보호 에이전트를 통해 수행됩니다.

© Acronis International GmbH, 2003-2024

사전 설정값이 **비활성화됨**.

체크섬 확인을 통한 유효성 검사에 대한 자세한 내용은 "체크섬 확인"(191페이지) 항목을 참조하십시오.

참고
서비스 제공업체에서 선택한 설정에 따라 다르지만, 클라우드 스토리지로 백업할 때는 유효성 검사를 수행하지 못할 수도 있습니다. 퍼블릭 클라우드의 백업 위치에서도 유효성 검사 기능을 사용할 수 없습니다.

CBT(Changed Block Tracking)

이 옵션은 다음 백업에 유효합니다.

- 가상 머신에 대한 디스크 수준 백업
- Windows를 실행 중인 실제 머신에 대한 디스크 수준 백업
- Microsoft SQL Server 데이터베이스 백업
- Microsoft Exchange Server 데이터베이스 백업

사전 설정값이 **활성화되었습니다**.

이 옵션은 증분 또는 차등 백업을 수행할 때 CBT(Changed Block Tracking)를 사용할지 결정합니다.

CBT 기술은 백업 프로세스를 가속화합니다. 디스크 또는 데이터베이스 콘텐츠의 변경 사항은 블록 수준에서 지속적으로 추적됩니다. 백업이 시작되면 변경 사항을 백업에 즉시 저장할 수 있습니다.

클러스터 백업 모드

참고
이 기능은 Advanced Backup 팩에서 사용할 수 있습니다.

이 옵션은 Microsoft SQL Server 및 Microsoft Exchange Server의 데이터베이스 수준 백업에 적용됩니다.

개별 노드나 개별 노드 내부 데이터베이스가 아닌 클러스터 자체(Microsoft SQL Server AAG(Always On 가용성 그룹) 또는 Microsoft Exchange Server DAG(데이터베이스 가용성 그룹))가 백업을 위해 선택된 경우에만 이 옵션이 적용됩니다. 클러스터 내부의 개별 항목을 선택하면 백업이 클러스터에서 인식되지 않고 항목의 선택한 복사본만 백업됩니다.

Microsoft SQL Server

이 옵션은 SQL Server AAG(Always On 가용성 그룹)에 대한 백업 모드를 결정합니다. 이 옵션을 사용하려면 모든 AAG 노드에 Agent for SQL이 설치되어 있어야 합니다. Always On 가용성 그룹 백업에 대한 자세한 내용은 "AAG(Always On 가용성 그룹) 보호"를 참조하십시오.

사전 설정값이 **가능한 경우 보조 복제본**입니다.

다음 중 하나를 선택할 수 있습니다.

© Acronis International GmbH, 2003-2024

- **가능한 경우 보조 복제본**
  모든 보조 복제본이 오프라인인 경우 주 복제본이 백업됩니다. 주 복제본을 백업하면 SQL Server 작업이 느려질 수 있지만 데이터가 가장 최근 상태로 백업됩니다.
- **보조 복제본**
  모든 보조 복제본이 오프라인인 경우 백업이 실패합니다. 보조 복제본 백업은 SQL Server 성능에 영향을 주지 않으며 백업 할당 시간 연장을 허용합니다. 그러나 수동 복제본은 비동기식으로 (지연) 업데이트되도록 설정되는 경우가 많으므로 최신 정보를 포함하지 않을 수 있습니다.
- **주 복제본**
  주 복제본이 오프라인인 경우 백업이 실패합니다. 주 복제본을 백업하면 SQL Server 작업이 느려질 수 있지만 데이터가 가장 최근 상태로 백업됩니다.

이 옵션의 값에 관계없이 데이터베이스 일관성을 확보하기 위해 소프트웨어에서는 백업이 시작될 때 **동기화됨** 또는 **동기화 중** 상태가 *아닌* 데이터베이스를 건너뜁니다. 모든 데이터베이스를 건너뛰면 백업이 실패합니다.

Microsoft Exchange 서버

이 옵션은 Exchange Server DAG(데이터베이스 가용성 그룹)에 대한 백업 모드를 결정합니다. 이 옵션을 사용하려면 모든 DAG 노드에 Agent for Exchange가 설치되어 있어야 합니다. 데이터베이스 가용성 그룹 백업에 대한 자세한 내용은 "DAG(데이터베이스 가용성 그룹) 보호"를 참조하십시오.

사전 설정값이 **가능한 경우 수동 복사본**입니다.

다음 중 하나를 선택할 수 있습니다.

- **가능한 경우 수동 복사본**
  모든 수동 복사본이 오프라인인 경우 활성 복사본이 백업됩니다. 활성 복사본을 백업하면 Exchange Server 작업이 느려질 수 있지만 데이터가 가장 최근 상태로 백업됩니다.
- **수동 복사본**
  모든 수동 복사본이 오프라인인 경우 백업이 실패합니다. 수동 복사본 백업은 Exchange 서버 성능에 영향을 주지 않으며 백업 할당 시간 연장을 허용합니다. 그러나 수동 사본은 비동기식으로 (지연) 업데이트되도록 설정되는 경우가 많으므로 최신 정보를 포함하지 않을 수 있습니다.
- **활성 복사본**
  활성 복사본이 오프라인인 경우 백업이 실패합니다. 활성 복사본을 백업하면 Exchange Server 작업이 느려질 수 있지만 데이터가 가장 최근 상태로 백업됩니다.

이 옵션의 값에 관계없이 데이터베이스 일관성을 확보하기 위해 소프트웨어에서는 백업이 시작될 때 **양호함** 또는 **활성** 상태가 *아닌* 데이터베이스를 건너뜁니다. 모든 데이터베이스를 건너뛰면 백업이 실패합니다.

압축 수준

참고
이 옵션은 클라우드 간 백업에는 사용할 수 없습니다. 이러한 백업에 대한 압축은 기본적으로 아래의 **보통** 수준에 해당하는 고정 수준으로 활성화되어 있습니다.

© Acronis International GmbH, 2003-2024

이 옵션은 백업 중인 데이터에 적용되는 압축 수준을 결정합니다. 사용 가능한 수준은 **없음**, **보통**, **높음**, **최대**입니다.

사전 설정값이 **보통**입니다.

압축 수준이 높아질수록 백업 처리 시간이 더 길어지지만 백업이 차지하는 공간은 줄어듭니다. 현재, **높음**과 **최대**는 비슷한 수준을 보입니다.

최적의 데이터 압축 수준은 백업 중인 데이터의 유형에 따라 달라집니다. 백업에 기본적으로 압축된 파일(예: .jpg, .pdf 또는 .mp3)이 포함되어 있으면 최대 압축 수준에서도 백업 크기가 크게 줄어들지 않습니다. 하지만 .doc 또는 .xls 같은 포맷은 압축 효과가 뛰어납니다.

오류 처리

이 옵션을 사용하여 백업 중 발생할 수 있는 오류를 어떻게 처리할지 지정할 수 있습니다.

오류 발생 시 재시도

사전 설정값이 **시도 횟수: 시도 횟수: 10. 시도 간격: 30초.**

복구 가능 오류가 발생하면 프로그램이 성공하지 못한 작업의 수행을 재시도합니다. 시간 간격과 시도 횟수를 설정할 수 있습니다. 작업 성공 또는 지정된 시도 횟수 완료 중 하나가 먼저 발생하면 시도가 즉시 중지됩니다.

예를 들어 백업 실행 중에 네트워크의 백업 대상이 사용 불가 또는 연결 불가 상태가 되면 소프트웨어가 30초마다 대상 연결을 30회까지 시도합니다. 연결 재개 또는 지정된 시도 횟수 완료 중 하나가 먼저 발생하면 시도가 중지됩니다.

그러나 백업을 시작할 때 백업 대상이 사용 불가 상태이면 대상 연결을 10회만 시도합니다.

처리하는 동안 메시지 및 대화 상자 표시 안 함(자동 모드)

사전 설정값이 **활성화됨**입니다.

자동 모드가 활성화되어 있으면 프로그램이 사용자 상호 작용이 필요한 상황을 자동으로 처리합니다(별도의 옵션으로 정의되는 불량 섹터 처리는 예외). 작업 성공 또는 지정된 시도 횟수 완료 중 하나가 먼저 발생하면 시도가 중지됩니다. 작업 로그에는 오류(있는 경우)를 포함하여 작업에 대한 자세한 정보가 기록됩니다.

불량 섹터 무시

사전 설정값이 **비활성화됨**.

이 옵션이 비활성화되어 있으면 프로그램이 불량 섹터를 발견할 때마다 백업 작업에 **상호 작용 필요** 상태가 할당됩니다. 사용 기간이 짧은 디스크에서 유효한 정보를 백업하려면 불량 섹터 무시를 활성화하십시오. 그러면 나머지 데이터는 백업되고, 생성된 디스크 백업을 다른 디스크로 마운트하여 유효한 파일을 추출할 수 있습니다.

© Acronis International GmbH, 2003-2024

참고
Linux에서는 불량 섹터를 건너뛰는 기능이 지원되지 않습니다. 온-프레미스 버전의 Cyber Protect에서 부트 가능한 미디어 제작기를 사용하여 불량 섹터가 있는 Linux 시스템을 오프라인 모드에서 백업할 수 있습니다. 온-프레미스 부트 가능한 미디어 제작기를 사용하려면 별도의 라이센스가 필요합니다. 도움이 필요하면 지원 센터로 문의하십시오.

VM 스냅샷 생성 도중 오류가 발생하는 경우 재시도

사전 설정값이: **활성화됨. 시도 횟수: 3. 시도 간격: 5분.**

가상 머신 스냅샷 생성에 실패하면 프로그램이 성공하지 못한 작업의 수행을 재시도합니다. 시간 간격과 시도 횟수를 설정할 수 있습니다. 작업 성공 또는 지정된 시도 횟수 완료 중 하나가 먼저 발생하면 시도가 중지됩니다.

빠른 증분/차등 백업

이 옵션은 증분 및 차등 디스크 수준 백업에 유효합니다.

이 옵션은 JFS, ReiserFS3, ReiserFS4, ReFS, 또는 XFS 파일 시스템으로 포맷된 볼륨에 대해 유효하지 않습니다(항상 비활성화됨).

사전 설정값이 **활성화됨**.

증분 또는 차등 백업은 데이터의 변경 내용만 캡처합니다. 백업 프로세스의 속도를 높이기 위해 프로그램이 파일 크기와 파일이 마지막으로 수정된 날짜/시간을 기준으로 파일의 변경 유무를 판별합니다. 이 기능을 비활성화하면 프로그램이 전체 파일 내용을 백업에 저장되어 있는 내용과 비교합니다.

파일 필터(포함/제외)

파일 필터를 사용하여 백업에 특정 파일 및 폴더만 포함하거나 백업에서 특정 파일 및 폴더를 제외합니다.

파일 필터는 특별히 명시되지 않은 한 전체 머신 백업, 디스크 수준 백업 및 파일 수준 백업에 사용할 수 있습니다.

파일 필터는 XFS, JFS, exFAT 및 ReiserFS4 파일 시스템에서 사용할 수 없습니다. 자세한 정보는 "지원되는 파일 시스템"(50페이지)(을)를 참조하십시오.

Agent for VMware, Agent for Hyper-V, Agent for Scale Computing 등을 통해 비에이전트 모드에서 백업된 가상 머신의 동적 디스크(LVM 또는 LDM 볼륨)에는 파일 필터가 적용되지 않습니다.

파일 필터를 사용하도록 설정하려면

1. 보호 계획에서 **백업** 모듈을 확장합니다.
2. **백업 옵션**에서 **변경**을 클릭합니다.
3. **파일 필터(포함/제외)**를 선택합니다.
4. 아래에서 설명하는 옵션 중 하나를 사용합니다.

© Acronis International GmbH, 2003-2024

포함 및 제외 필터

필터에는 포함 필터와 제외 필터의 두 가지가 있습니다.

- **다음 기준과 일치하는 파일만 포함**
  포함 필터에서 C:\File.exe를 지정하면 전체 머신 백업을 선택했더라도 이 파일만 백업됩니다.

  참고
  백업 형식이 **버전 11**이며 백업 목적지가 클라우드 스토리지가 아닌 경우에는 파일 수준 백업에서 이 필터가 지원되지 않습니다.

- **다음 기준과 일치하는 파일 제외**
  제외 필터에서 C:\File.exe를 지정하면 전체 머신 백업을 선택했더라도 백업 중 이 파일을 건너뜁니다.

두 필터를 동시에 사용할 수 있습니다. 제외 필터가 포함 필터보다 우선적으로 적용됩니다. 즉, 두 필드에서 모두 C:\File.exe를 지정하면 백업 중 이 파일을 건너뜁니다.

필터 기준

필터 기준으로는 파일 및 폴더 이름, 파일과 폴더의 전체 경로, 그리고 와일드카드 기호가 포함된 마스크를 사용할 수 있습니다.

필터 기준은 대소문자를 구분하지 않습니다. 예를 들어 C:\Temp를 지정하면 C:\TEMP와 C:\temp가 선택됩니다.

- 이름
  파일 또는 폴더의 이름을 지정합니다(예: Document.txt). 해당 이름이 포함된 모든 파일 및 폴더가 선택됩니다.
- 전체 경로
  드라이브 문자(Windows를 백업하는 경우) 또는 루트 디렉토리(Linux 또는 macOS를 백업하는 경우)로 시작하는 파일 또는 폴더의 전체 경로를 지정합니다. Windows, Linux 및 macOS에서는 C:/Temp/File.tmp와 같이 슬래시를 사용할 수 있습니다. Windows에서는 C:\Temp\File.tmp에서와 같이 기존의 백슬래시도 사용할 수 있습니다.

  중요
  백업된 머신의 운영 체제가 디스크 수준 백업 중에 올바르게 감지되지 않으면 전체 경로 파일 필터가 작동하지 않습니다. 제외 필터인 경우에는 경고가 표시됩니다. 포함 필터가 있으면 백업이 실패합니다.
  예를 들어 파일의 전체 경로를 C:\Temp\File.tmp와 같이 지정할 수 있습니다. 드라이브 문자나 루트 디렉토리를 포함하는 전체 경로 필터(예: C:\Temp\File.tmp 또는 C:\Temp*)를 지정하면 경고나 오류가 발생합니다.
  드라이브 문자나 루트 디렉토리를 사용하지 않는 필터(예: Temp* 또는 Temp\File.tmp) 또는 별표로 시작하는 필터(예: *C:\)를 지정하면 경고나 오류가 발생하지 않습니다. 하지만 백업된 머신의 운영 체제가 올바르게 감지되지 않으면 이러한 필터가 작동하지 않습니다.

© Acronis International GmbH, 2003-2024

- 마스크

  이름과 전체 경로에 사용할 수 있는 와일드카드 문자는 별표(*), 이중 별표(**), 물음표(?)입니다.

  별표(*)는 0개 이상의 문자를 나타냅니다. 예를 들어 필터 기준 **Doc*.txt**는 Doc.txt 및 Document.txt 파일과 일치합니다.

  이중 별표(**)는 슬래시 문자를 포함한 0개 이상의 문자를 나타냅니다. 예를 들어 필터 기준 ****/Docs/**.txt**는 이름이 Docs인 모든 폴더의 모든 하위 폴더에 있는 모든 .txt 파일과 일치합니다. 이중 별표(**) 와일드카드는 버전 12 형식의 백업에만 사용할 수 있습니다.

  물음표(?)는 1개의 문자만 나타냅니다. 예를 들어 **Doc?.txt**는 Doc1.txt 및 Docs.txt 파일과는 일치하지만 Doc.txt 또는 Doc11.txt 파일과는 일치하지 않습니다.

파일 수준 백업 스냅샷

이 옵션은 파일 수준 백업에 대해서만 유효합니다.

이 옵션은 파일을 하나씩 백업할지, 인스턴트 데이터 스냅샷을 생성하여 백업할지 정의합니다.

참고
네트워크 공유에 저장되어 있는 파일은 항상 하나씩 백업됩니다.

사전 설정값이

- Linux 실행 머신만 백업하기로 선택한 경우: **스냅샷을 생성하지 않습니다.**
- 그렇지 않은 경우: **가능한 경우 스냅샷을 만듭니다.**

다음 중 하나를 선택합니다.

- **가능한 경우 스냅샷을 만듭니다.**

  스냅샷 생성이 불가능한 경우에는 파일을 직접 백업합니다.
- **항상 스냅샷을 만듭니다.**

  스냅샷을 사용하면 독점적인 액세스 권한으로 열린 파일을 포함하여 모든 파일을 백업할 수 있습니다. 파일은 같은 시점에 백업됩니다. 이 요인들이 결정적으로 중요한 경우, 즉 스냅샷 없이 파일을 백업하는 것을 절대 허용할 수 없는 경우에만 이 설정을 선택하십시오. 스냅샷을 만들 수 없으면 백업이 실패합니다.
- **스냅샷을 생성하지 않습니다.**

  항상 파일을 직접 백업합니다. 독점적인 액세스 권한으로 열린 파일을 백업하려고 하면 읽기 오류가 발생합니다. 백업의 파일 시간이 일관되지 않을 수 있습니다.

포렌직 데이터

바이러스, 맬웨어, 랜섬웨어는 데이터를 훔치거나 변경하는 등 악의적 행위를 할 수 있습니다. 이들 활동에 대해 조사해야할 수 있으며, 디지털 증거가 있는 경우에만 가능합니다. 그러나 파일이나 활동 기록 등의 디지털 기록이 삭제되거나 악의적 행위가 있었던 머신이 사용 불가하게 될 수 있습니다.

포렌직 데이터 백업을 통해 조사자들이 주기적인 디스크 백업에 일반적으로 포함되지 않는 디스크 영역을 분석할 수 있습니다. **포렌직 데이터** 백업 옵션을 통해 포렌직 조사에 사용할 다음과 같

© Acronis International GmbH, 2003-2024

은 디지털 증거를 수집할 수 있습니다. 미사용 디스크 공간 스냅샷, 메모리 덤프, 실행 프로세스 스냅샷 등.

포렌직 데이터를 포함하는 백업은 자동으로 공증됩니다.

현재 **포렌직 데이터** 옵션은 다음 운영 체제를 사용하는 Windows 머신에 대한 전체 장치 백업의 경우에 한해 사용할 수 있습니다.

- Windows 8.1, Windows 10
- Windows Server 2012 R2 – Windows Server 2019

포렌직 데이터 백업은 다음 머신에서는 사용할 수 없습니다.

- VPN으로 사용자 네트워크에 연결하거나 인터넷에 직접 연결할 수 없는 머신
- BitLocker로 암호화된 디스크가 있는 머신

참고
머신에 **백업** 모듈을 활성화한 보호 계획을 적용한 이후에는 포렌직 데이터 설정을 수정할 수 없습니다. 다른 포렌직 데이터 설정을 사용하려면 새 보호 계획을 생성해야 합니다.

포렌직 데이터 백업은 다음 위치에 저장할 수 있습니다.

- 클라우드 스토리지
- 로컬 폴더

  참고
  로컬 폴더 위치는 USB를 통해 연결된 외장 하드 디스크에서만 지원됩니다.
  로컬 동적 디스크는 포렌직 백업 데이터 위치로 지원되지 않습니다.

- 네트워크 폴더

포렌직 백업 프로세스

시스템은 포렌직 백업 프로세스 중 다음 작업을 수행합니다.

1. 원시 메모리 덤프와 실행 중인 프로세스 목록을 수집합니다.
2. 머신을 부트 가능한 미디어로 자동 재부팅합니다.
3. 사용된 공간과 할당되지 않은 공간을 모두 포함하는 백업을 생성합니다.
4. 백업 디스크를 공증합니다.
5. 라이브 운영 체제로 재부팅하고 계획을 계속 실행합니다(예: 복제, 보관, 유효성 검사 등).

포렌직 데이터 컬렉션을 구성하려면

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다. 또는 **관리** 탭에서 보호 계획을 생성할 수도 있습니다.
2. 장치를 선택하고 **보호**를 클릭합니다.
3. 보호 계획에서 **백업** 모듈을 활성화합니다.
4. **백업 대상**에서 **전체 머신**을 선택합니다.
5. **백업 옵션**에서 **변경**을 클릭합니다.

© Acronis International GmbH, 2003-2024

6. **포렌직 데이터** 옵션을 찾습니다.
7. **포렌직 데이터 수집**을 활성화합니다. 시스템은 자동으로 메모리 덤프를 수집하고 실행 중인 프로세스의 스냅샷을 생성합니다.

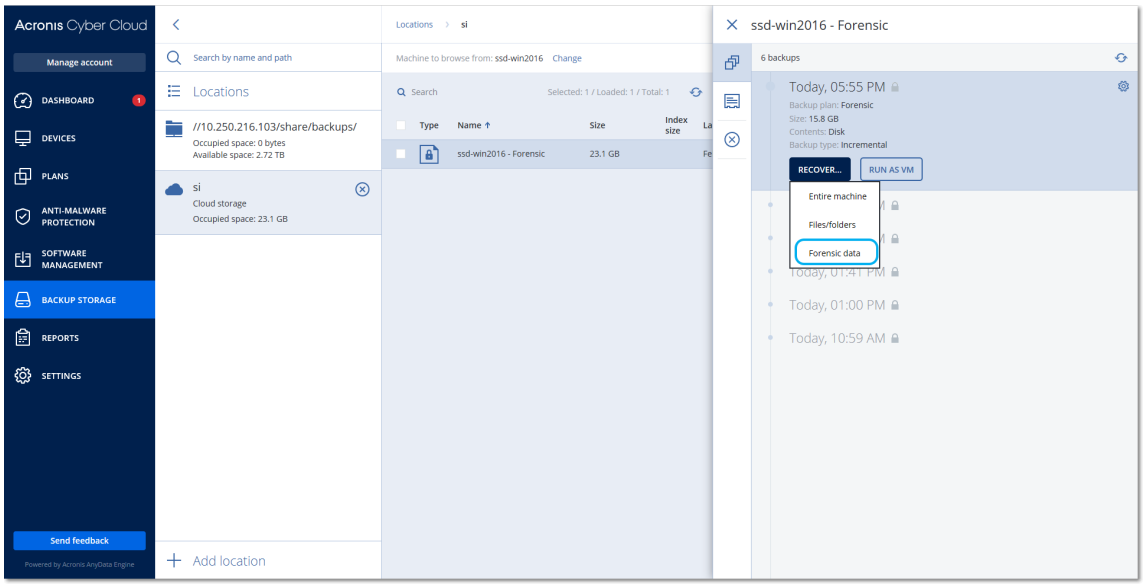
   참고
   전체 메모리 덤프에는 비밀번호와 같은 민감한 데이터가 포함될 수 있습니다.

8. 위치를 지정합니다.
9. **지금 실행**을 클릭해 즉시 포렌직 데이터를 포함하는 백업을 수행하거나 스케줄에 따라 백업이 생성될 때까지 기다립니다.
10. **모니터링** > **작업**으로 이동해 포렌직 데이터가 있는 백업이 성공적으로 생성되었는지 확인합니다.

그 결과로 백업에 포렌직 데이터가 포함되며, 해당 데이터를 받아 분석할 수 있습니다. 포렌직 데이터가 있는 백업은 표시가 되어 있으며 **포렌직 데이터가 있는 경우만** 옵션을 사용하여 **백업 스토리지** > **위치**의 여러 백업 중에서 필터링할 수 있습니다.

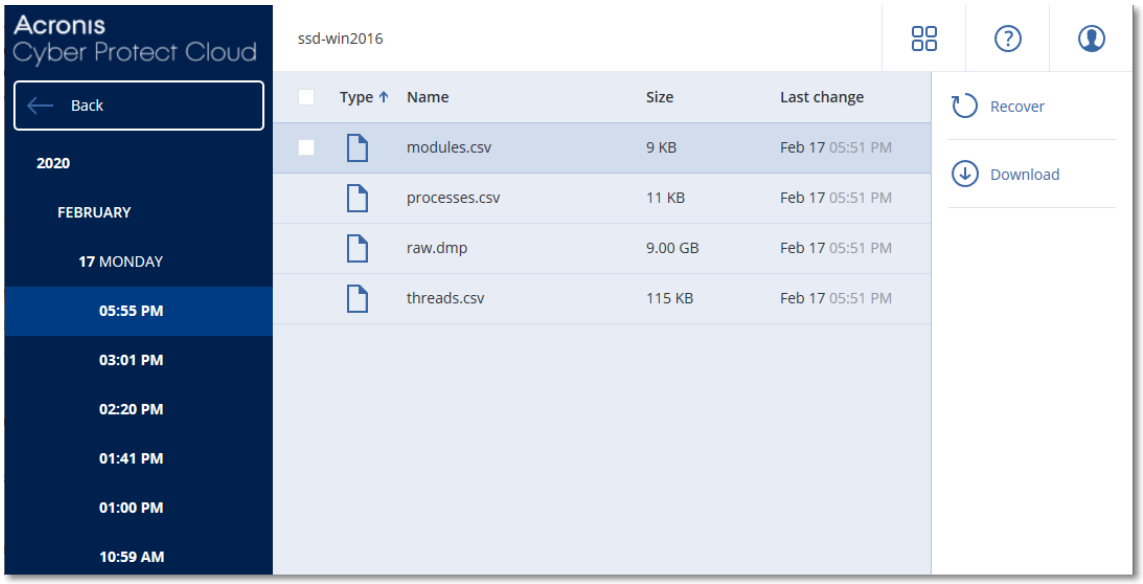
백업에서 포렌직 데이터를 가져오는 방법은?

1. Cyber Protect 콘솔에서 **백업 스토리지**로 이동해 포렌직 데이터를 포함하는 백업이 있는 위치를 선택합니다.
2. 포렌직 데이터가 있는 백업을 선택하고 **백업 표시**를 클릭합니다.
3. 포렌직 데이터가 있는 백업에 대해 **복구**를 클릭합니다.
   - 포렌직 데이터만 받으려면 **포렌직 데이터**를 클릭합니다.



시스템이 포렌직 데이터가 있는 폴더를 표시합니다. 메모리 덤프 파일 또는 다른 포렌직 파일을 선택하고 **다운로드**를 클릭합니다.

© Acronis International GmbH, 2003-2024



- 전체 포렌직 백업을 복구하려면 **전체 머신**을 클릭합니다. 시스템이 부트 모드 없이 백업을 복구합니다. 따라서 디스크가 변경되지 않았는지 확인할 수 있습니다.

여러 가지 타사 포렌직 소프트웨어로 제공된 메모리 덤프를 사용할 수 있습니다. 예를 들어, 추가 메모리 분석을 위해 https://www.volatilityfoundation.org에서 Volatility Framework를 사용할 수 있습니다.

포렌직 데이터를 포함하는 백업의 공증

포렌직 데이터가 있는 백업이 정확하게 실행된 이미지이고 손상되지 않았음을 확인하기 위해, 백업 모듈은 포렌직 데이터가 있는 백업의 공증을 제공합니다.

작동법

공증을 사용하면 포렌직 데이터가 있는 디스크가 신뢰할 수 있고 백업된 후 변경되지 않았음을 증명할 수 있습니다.

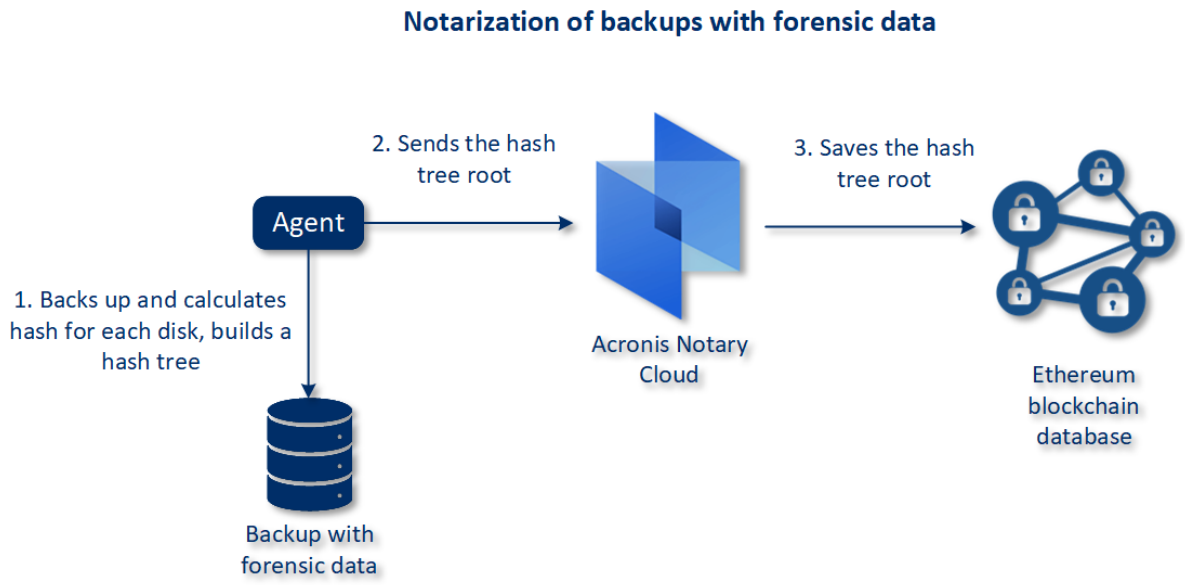
백업 중에 에이전트가 백업된 디스크의 해시 코드를 계산하고, 해시 트리를 생성하고, 트리를 백업에 저장한 다음 해시 트리 루트를 공증 서비스로 전송합니다. 공증 서비스는 Ethereum 블록체인 데이터베이스에 해시 트리 루트를 저장하여 이 값이 변경되지 않도록 합니다.

포렌직 데이터가 있는 디스크의 신뢰성을 확인할 때 에이전트가 디스크의 해시를 계산한 다음 이를 백업 내부의 해시 트리에 저장되어 있는 해시와 비교합니다. 두 해시가 일치하지 않으면 디스크가 신뢰할 수 없는 것으로 간주됩니다. 그렇지 않으면 해시 트리에 의해 디스크 신뢰성이 보증됩니다.

해시 트리 자체가 손상되지 않았는지 확인하기 위해 에이전트는 해시 트리 루트를 공증 서비스로 전송합니다. 공증 서비스는 이를 블록체인 데이터베이스에 저장되어 있는 해시 트리 루트와 비교합니다. 해시가 일치하면 선택한 디스크는 신뢰할 수 있는 것으로 보증됩니다. 그렇지 않으면 소프트웨어에 디스크를 신뢰할 수 없다는 메시지가 표시됩니다.

아래의 구성표는 포렌직 데이터를 포함하는 백업의 공증 프로세스를 간략하게 보여줍니다.

© Acronis International GmbH, 2003-2024



공증된 디스크 백업을 수동으로 검증하려면 디스크 백업에 대한 인증서를 받고 tibxread 도구를 사용하여 인증서에 나타난 확인 절차를 수행할 수 있습니다.

포렌직 데이터를 포함하는 백업에 대한 인증서 받기

콘솔에서 포렌직 데이터를 포함하는 백업에 대한 인증서를 받으려면 다음 작업을 수행합니다.

1. **백업 스토리지**로 이동하고 포렌직 데이터가 있는 백업을 선택합니다.
2. 전체 머신을 복구합니다.
3. 시스템에 **디스크 매핑** 보기가 열립니다.
4. 디스크의 **인증서 가져오기** 아이콘을 클릭합니다.
5. 시스템이 인증서를 생성하고 브라우저에서 인증서가 포함된 새 창이 열립니다. 인증서 아래에 공증된 디스크 백업의 수동 검증을 위한 지침이 표시됩니다.

백업 데이터를 받기 위한 "tibxread" 도구

Cyber Protection에서는 백업 디스크 무결성의 수동 확인을 위한 `tibxread`라는 도구를 제공합니다. 이 도구를 사용하면 백업의 데이터를 받고 특정 디스크의 해시를 계산할 수 있습니다. 도구는 자동으로 다음 컴퍼넌트와 함께 설치됩니다: Agent for Windows, Agent for Linux 및 Agent for Mac.

설치 경로: 에이전트에 포함된 폴더와 동일한 폴더(예: `C:\Program Files\BackupClient\BackupAndRecovery`).

지원되는 위치:

- 로컬 디스크
- 자격 증명 없이 액세스할 수 있는 네트워크 폴더(CIFS/SMB).
  비밀번호로 보호된 네트워크 폴더의 경우, OS 도구를 사용해 로컬 폴더에 네트워크 폴더를 마운트한 다음 로컬 폴더를 이 도구의 소스로 마운트할 수 있습니다.
- 클라우드 스토리지

© Acronis International GmbH, 2003-2024

URL, 포트 및 인증서를 제공해야 합니다. URL과 포트는 Windows 레지스트리 키 또는 Linux/Mac 머신의 구성 파일에서 가져올 수 있습니다.

Windows:

```
HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Defa
ult\<tenant_login>\FesUri
```

Linux:

```
/etc/Acronis/BackupAndRecovery.config
```

macOS:

```
/Library/Application Support/Acronis/Registry/BackupAndRecovery.config
```

인증서는 다음 위치에서 찾을 수 있습니다.

Windows:

```
%allusersprofile%\Acronis\BackupAndRecovery\OnlineBackup\Default
```

Linux:

```
/var/lib/Acronis/BackupAndRecovery/OnlineBackup/Default
```

macOS:

```
/Library/Application Support/Acronis/BackupAndRecovery/OnlineBackup/Default
```

도구에는 다음 명령이 있습니다.

- `list backups`
- `list content`
- `get content`
- `calculate hash`

list backups

백업에서 복구 지점을 나열합니다.

개요:

```
tibxread list backups --loc=URI --arc=BACKUP_NAME --raw
```

옵션

```
--loc=URI
--arc=BACKUP_NAME
--raw
```


© Acronis International GmbH, 2003-2024

```
--utc
--log=PATH
```

출력 템플릿:

```
GUID   Date   Date timestamp
----   ------ --------------
<guid> <date> <timestamp>
```

<guid> – 백업 GUID.

<date> – 백업 생성 날짜. 형식은 "DD.MM.YYYY HH24:MM:SS"입니다. 기본적으로 현지 시간대를 사용합니다(--utc 옵션을 사용해 변경할 수 있습니다).

출력 예:

```
GUID   Date   Date timestamp
----   ------ --------------
516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865
516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925
```

list content

복구 지점의 콘텐츠를 나열합니다.

개요:

```
tibxread list content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID
--raw --log=PATH
```

옵션

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--raw
--log=PATH
```

출력 템플릿:

```
Disk     Size   Notarization status
-------- ------ --------------------
<number> <size> <notarization_status>
```

<number> – 디스크 식별자.

<size> – 크기(바이트).

© Acronis International GmbH, 2003-2024

<notarization_status> – 가능한 상태: 공증 없음, 공증됨, 다음 백업.

출력 예:

```
Disk     Size   Notary status
-------- ------ --------------
1        123123465798 Notarized
2        123123465798 Notarized
```

get content

복구 지점에서 표준 출력(stdout)으로 지정된 디스크의 콘텐츠를 작성합니다.

개요:

```
tibxread get content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID -
-disk=DISK_NUMBER --raw --log=PATH --progress
```

옵션

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
--progress
```

calculate hash

SHA-2(256비트) 알고리즘을 사용하여 복구 지점에서 지정된 디스크의 해시를 계산하고 stdout으로 작성합니다.

개요:

```
tibxread calculate hash --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_
ID --disk=DISK_NUMBER --raw --log=PATH --progress
```

옵션

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
```


© Acronis International GmbH, 2003-2024

옵션 설명

옵션	설명
--arc=BACKUP_NAME	Cyber Protect 콘솔의 백업 속성에서 가져올 수 있는 백업 파일 이름입니다. 백업 파일은 확장자 .tibx로 지정되어야 합니다.
--backup=RECOVERY_POINT_ID	복구 지점 식별자
--disk=DISK_NUMBER	디스크 번호("get content" 명령의 출력으로 작성된 것과 동일)

--loc=URI	백업 위치 URI입니다. 가능한 "--loc" 옵션 형식:
	• 로컬 경로 이름(Windows)
	`c:/upload/backups`
	• 로컬 경로 이름(Linux)
	`/var/tmp`
	• SMB/CIFS
	`\\server\folder`
	• 클라우드 스토리지
	`--loc=<IP_address>:443 --cert=<path_to_certificate> [--storage_path=/1]`
	<IP_address> – Windows의 레지스트리 키에서 찾을 수 있습니다. HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<tenant_login>\FesUri
	<path_to_certificate> – Cyber Protect Cloud에 액세스하기 위한 인증서 파일의 경로. 예를 들어, Windows에서 이 인증서는 `C:\ProgramData\Acronis\BackupAndRecovery\OnlineBackup\Default\<username>.crt`에 있습니다. 여기서 <username>은 Cyber Protect Cloud에 액세스하기 위한 계정 이름입니다.

--log=PATH	지정된 경로(로컬 경로만 해당, 형식은 `--loc=URI` 매개변수와 동일)로 로그 작성을 활성화합니다. 로깅 수준은 디버그입니다.
--password=PASSWORD	백업을 위한 암호화 비밀번호입니다. 백업이 암호화되지 않은 경우 이 값을 비워두십시오.

--raw	명령 출력에서 헤더(첫 두 행)을 숨깁니다. 명령 출력 구문을 분석해야 할 때 사용됩니다.
	"`--raw`" 없는 출력 예:
	`GUID Date Date timestamp`
	`---- ------ --------------`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`

© Acronis International GmbH, 2003-2024

	"--raw" 있는 출력:
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`

--utc	날짜를 UTC로 표시합니다.

--progress	작업의 진행 상태를 표시합니다.
	예:
	`1%`
	`2%`
	`3%`
	`4%`
	`...`
	`100%`

로그 자르기

이 옵션은 Microsoft SQL Server 데이터베이스 백업, 그리고 Microsoft SQL Server 애플리케이션 백업이 활성화되어 있는 상태에서의 디스크 수준 백업에 유효합니다.

이 옵션은 성공적인 백업 후에 SQL Server 트랜잭션 로그를 자를지 결정합니다.

사전 설정값이 **활성화됨**.

이 옵션이 활성화되어 있으면 이 소프트웨어에서 생성한 백업의 시점으로만 데이터베이스를 복구할 수 있습니다. Microsoft SQL Server의 네이티브 백업 엔진을 사용하여 트랜잭션 로그를 백업하는 경우에는 이 옵션을 비활성화하십시오. 트랜잭션 로그를 복구 후에 적용할 수 있기 때문에 결국 데이터베이스를 어느 시점으로든 복구할 수 있습니다.

LVM 스냅샷 촬영

이 옵션은 실제 머신에 대해서만 유효합니다.

이 옵션은 Linux LVM(논리 볼륨 관리자)으로 관리하는 볼륨의 디스크 수준 백업에 대해 유효합니다. 해당 볼륨을 논리 볼륨이라고도 합니다.

이 옵션은 논리 볼륨의 스냅샷을 어떻게 생성할지 결정합니다. 백업 소프트웨어는 자체적으로 결정할 수도 있고, Linux LVM(논리 볼륨 관리자)을 통해 결정할 수도 있습니다.

사전 설정값이 **백업 소프트웨어 사용**.

- **백업 소프트웨어 사용**. 스냅샷 데이터는 주로 RAM에 보관됩니다. 따라서 백업 속도가 빨라지며 볼륨 그룹에 할당되지 않은 공간이 필요하지 않습니다. 그러므로 논리 볼륨 백업 시 문제가 발생하는 경우에만 사전 설정을 변경하는 것이 좋습니다.
- **LVM 사용**. 스냅샷이 볼륨 그룹의 할당되지 않은 공간에 저장됩니다. 할당되지 않은 공간이 누락되면 백업 소프트웨어가 스냅샷을 생성합니다.

© Acronis International GmbH, 2003-2024

스냅샷은 백업 작업 중에만 사용되며 백업 작업이 완료되면 자동으로 삭제됩니다. 임시 파일은 보존되지 않습니다.

마운트 포인트

이 옵션은 Windows에서 마운트된 볼륨 또는 클러스터 공유 볼륨을 포함하는 데이터 소스의 파일 수준 백업에만 유효합니다.

이 옵션은 폴더 계층 구조에서 마운트 포인트보다 상위 폴더를 백업하기 위해 선택하는 경우에만 유효합니다. (마운트 포인트는 추가 볼륨이 논리적으로 연결되는 폴더입니다.)

- 해당 폴더(상위 폴더)가 백업용으로 선택되고 **마운트 포인트** 옵션이 활성화되면 마운트된 볼륨에 있는 모든 파일이 백업에 포함됩니다. **마운트 포인트** 옵션이 비활성화되면 백업의 마운트 포인트가 비워집니다.

  상위 폴더를 복구하는 경우, **복구 시 마운트 포인트** 옵션의 활성화 또는 비활성화 여부에 따라 마운트 포인트 내용이 복구되거나 복구되지 않습니다.
- 마운트 포인트를 직접 선택하거나 마운트된 볼륨 내부의 폴더를 선택하는 경우, 선택한 폴더는 일반 폴더로 간주됩니다. 해당 폴더는 **마운트 포인트** 옵션의 상태에 관계없이 백업되고 **마운트 포인트** 옵션의 상태에 관계 없이 복구됩니다.

사전 설정값이 **비활성화됨**.

참고
파일 수준 백업으로 전체 볼륨 또는 필요한 파일을 백업하여 클러스터 공유 볼륨에 상주하는 Hyper-V 가상 머신을 백업할 수 있습니다. 가상 머신의 전원을 끄면 일관된 상태로 백업할 수 있습니다.

예

C:\Data1 폴더를 마운트된 볼륨의 마운트 포인트로 가정합니다. 볼륨에는 **Folder1** 및 **Folder2** 폴더가 포함됩니다. 파일 수준의 데이터 백업을 위한 보호 계획을 생성합니다.

볼륨 C 확인란을 선택하고 **마운트 포인트** 옵션을 활성화하면 백업의 **C:\Data1** 폴더에 **Folder1**과 **Folder2**가 포함됩니다. 백업된 데이터를 복구할 때는 복구 시 **마운트 포인트** 옵션을 올바르게 사용해야 합니다.

볼륨 C 확인란을 선택하고 **마운트 포인트** 옵션을 비활성화하면 백업의 **C:\Data1** 폴더가 비워집니다.

Data1, **Folder1** 또는 **Folder2** 폴더 확인란을 선택하면 **마운트 포인트** 옵션의 상태에 관계없이 선택한 폴더가 백업에서 일반 폴더로 포함됩니다.

다중 볼륨 스냅샷

이 옵션은 Windows 또는 Linux를 실행하는 실제 머신의 백업에 유효합니다.

이 옵션은 디스크 수준 백업에 적용됩니다. 또한, 이 옵션은 스냅샷 생성을 통해 파일 수준 백업을 수행할 때 파일 수준 백업에도 적용됩니다. ("파일 수준 백업 스냅샷" 옵션은 파일 수준 백업 중 스냅샷을 생성할지 결정합니다.)

© Acronis International GmbH, 2003-2024

이 옵션은 여러 볼륨의 스냅샷을 동시에 생성할지, 아니면 하나씩 생성할지 결정합니다.

사전 설정값이

- Windows를 실행하는 머신을 최소 하나 백업용으로 선택한 경우: **활성화됨**.
- 그렇지 않은 경우: **비활성화됨**.

이 옵션이 활성화되어 있으면 백업 중인 모든 볼륨의 스냅샷이 동시에 생성됩니다. 여러 볼륨(예: Oracle 데이터베이스)에 분산되어 있는 데이터의 백업을 시간이 일관되게 생성하려면 이 옵션을 사용하십시오.

이 옵션이 비활성화되어 있으면 볼륨의 스냅샷이 하나씩 생성됩니다. 결국, 데이터가 여러 볼륨에 분산되어 있는 경우 생성되는 백업의 시간이 일관되지 않을 수 있습니다.

원클릭 복구

참고
이 기능은 Advanced Backup 팩에서 사용할 수 있습니다.

원클릭 복구를 사용하면 Windows 또는 Linux 머신의 디스크 백업을 자동으로 복구할 수 있습니다. 이 백업은 전체 머신의 백업이거나 이 머신에서 특정 디스크 또는 볼륨의 백업일 수 있습니다.

원클릭 복구는 다음 작업을 지원합니다.

- 최신 백업에서 자동 복구
- 백업 아카이브 내의 특정 백업(복구 지점이라고도 함)에서의 복구

원클릭 복구는 다음 백업 스토리지를 지원합니다.

- Secure Zone
- 로컬 폴더
- 네트워크 폴더
- 클라우드 스토리지

중요
다음의 작업을 수행하는 경우 BitLocker 암호화를 다음 재시작까지 머신에서 일시 중지하십시오.

- Secure Zone 생성, 수정, 삭제
- Startup Recovery Manager 활성화 또는 비활성화
- [Startup Recovery Manager를 아직 활성화하지 않은 경우에만 해당됨] 보호 계획에서 원클릭 복구를 활성화한 후 첫 번째 백업 실행 이 작업을 수행하면 Startup Recovery Manager가 자동으로 활성화됩니다.
- Protection 업데이트 등의 작업을 통해 Startup Recovery Manager 업데이트

이러한 작업 중에 BitLocker 암호화가 일시 중지되지 않은 경우 머신을 재시작한 후에 Bitlocker PIN을 지정해야 합니다.

© Acronis International GmbH, 2003-2024

원클릭 복구 활성화

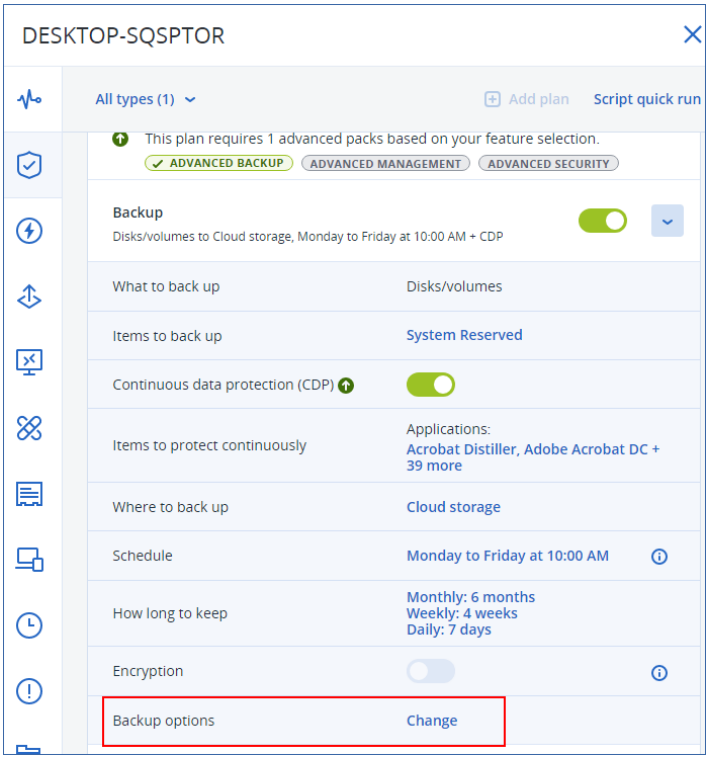
원클릭 복구는 보호 계획의 백업 옵션입니다. 계획을 생성하는 방법에 대한 자세한 정보는 "보호 계획 생성"(200페이지)을(를) 참조하십시오.

참고

원클릭 복구를 활성화하면 대상 머신에서 Startup Recovery Manager도 활성화됩니다. Startup Recovery Manager을(를) 활성화할 수 없는 경우 원클릭 복구 백업을 생성하는 백업 작업에 실패할 것입니다. Startup Recovery Manager에 대한 자세한 정보는 "Startup Recovery Manager"(663페이지)을(를) 참조하십시오.

원클릭 복구를 활성화하는 방법

1. 보호 계획에서 **백업** 모듈을 확장합니다.
2. **백업 대상**에서 **전체 머신** 또는 **디스크/볼륨**을 선택합니다.
3. [**디스크/볼륨**을 선택한 경우]. **백업할 항목**에서 백업할 디스크 또는 볼륨을 지정합니다.
4. **백업 옵션**에서 **변경**을 클릭하고 **원클릭 복구**를 선택합니다.

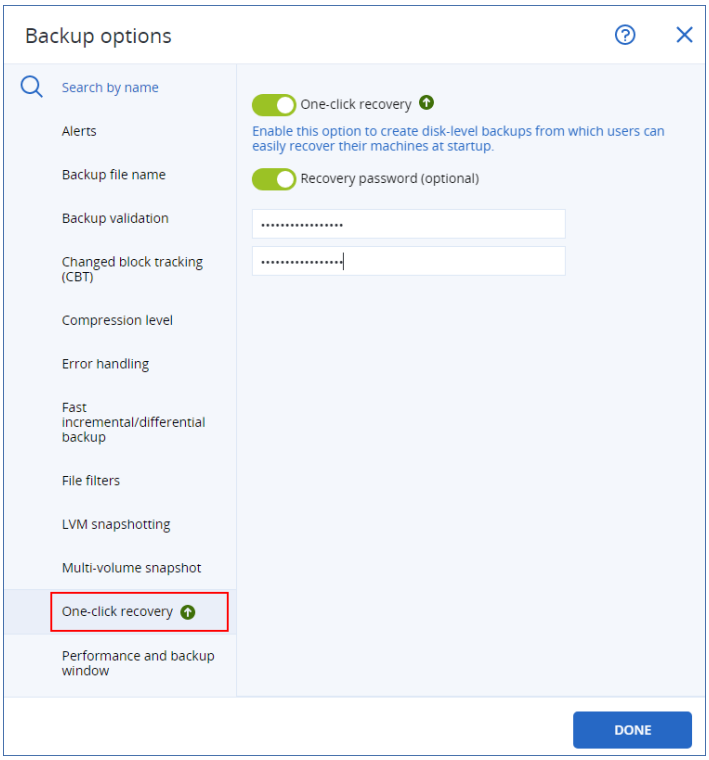


5. **원클릭 복구** 스위치를 활성화합니다.
6. [선택 사항] **복구 비밀번호** 스위치를 활성화하고 비밀번호를 지정합니다.

중요

복구 비밀번호를 지정하는 것이 좋습니다. 대상 머신에서 원클릭 복구를 수행하는 사용자가 비밀번호를 알고 있는지 확인하십시오.

© Acronis International GmbH, 2003-2024



7. **완료**를 클릭합니다.
8. 필요에 따라 보호 계획의 다른 요소를 구성한 다음 계획을 저장합니다.

보호 계획이 실행되고 백업이 생성되면 보호되는 시스템의 사용자가 원클릭 복구에 액세스할 수 있게 됩니다.

중요
보호 에이전트 업데이트 시에는 원클릭 복구 기능을 일시적으로 사용할 수 없습니다. 원클릭 복구를 다시 활성화하려면 백업을 실행합니다. 백업이 완료되면 원클릭 복구를 다시 수행할 수 있습니다.

원클릭 복구 비활성화

다음과 같은 방법으로 특정 워크로드에 대한 원클릭 복구를 비활성화 할 수 있습니다.

- 워크로드에 적용된 보호 계획에서 **원클릭 복구** 옵션을 비활성화합니다.
- **원클릭 복구** 옵션이 활성화된 보호 계획을 취소합니다.
- **원클릭 복구** 옵션이 활성화된 보호 계획을 삭제합니다.

원클릭 복구를 사용하여 머신 복구

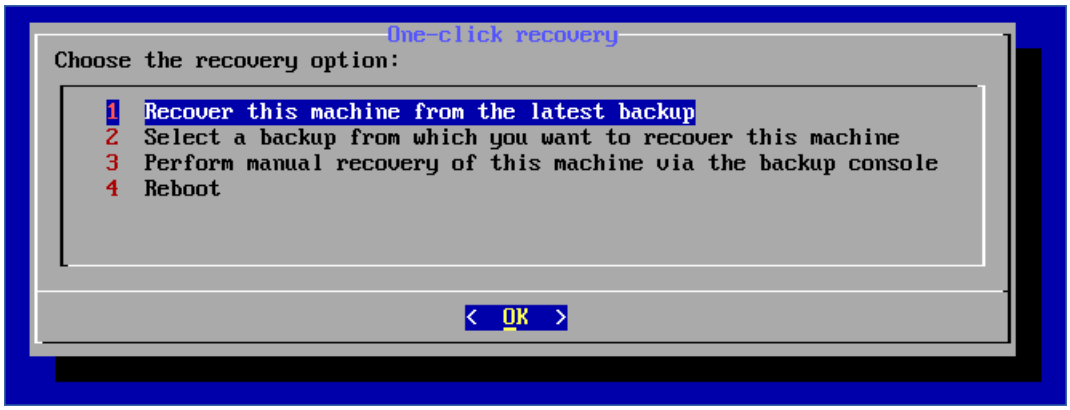
사전 요구 사항

- **원클릭 복구** 백업 옵션이 활성화된 보호 계획이 머신에 적용됩니다.
- 머신의 디스크 백업이 하나 이상 있습니다.

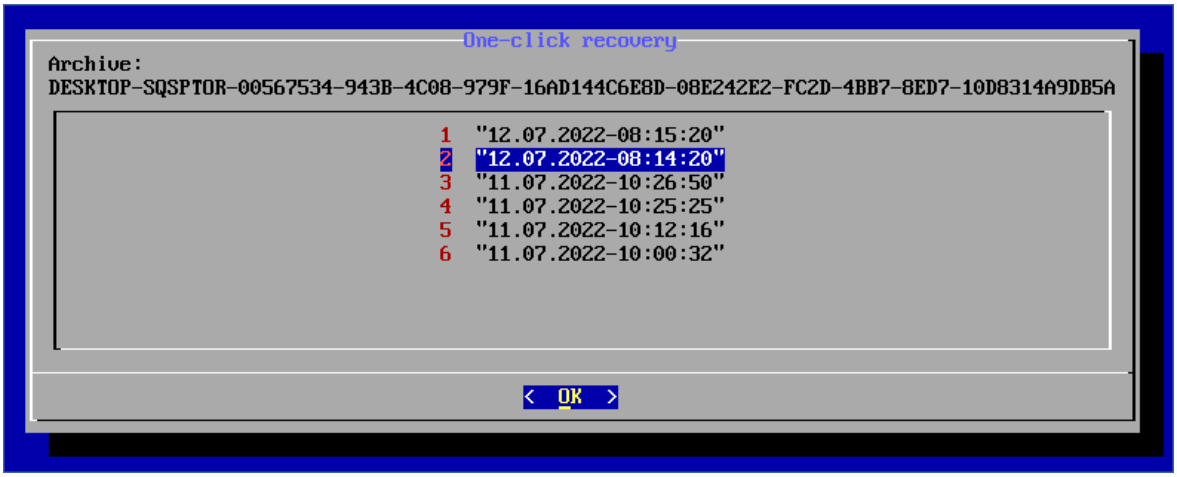
머신을 복구하려면

© Acronis International GmbH, 2003-2024

1. 복구할 머신을 재부팅합니다.
2. 재부팅 중 F11 키를 눌러 Startup Recovery Manager로 들어갑니다.
   복구 미디어 창이 열립니다.
3. **Acronis Cyber Protect**를 선택합니다.
4. [보호 계획에 복구 비밀번호가 지정된 경우] 복구 비밀번호를 입력하고 **확인**을 클릭합니다.
5. 원클릭 복구 옵션을 선택합니다.
   - 자동으로 최신 백업을 복구하려면 첫 번째 옵션을 선택하고 **확인**을 클릭합니다.
   - 백업 아카이브 내에서 다른 백업을 복구하려면 두 번째 옵션을 선택한 다음 **확인**을 클릭합니다.

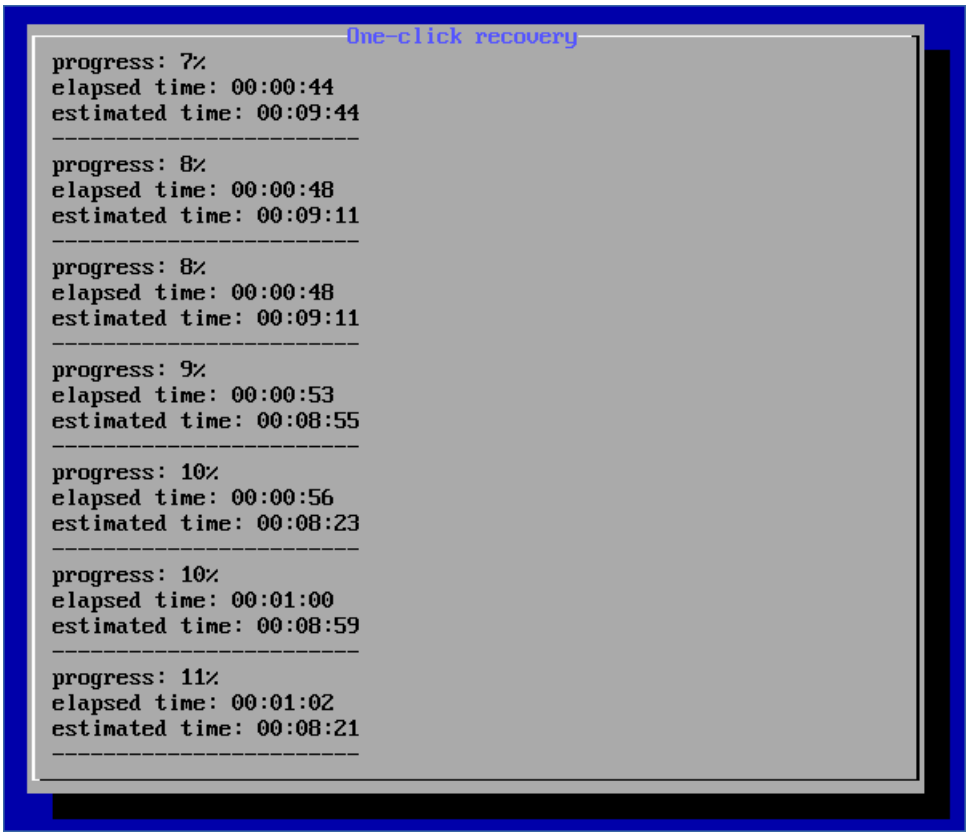


6. **예**를 클릭하여 선택을 확인합니다.
   복구 미디어 창이 열렸다가 사라집니다. 복구 미디어 창 없이 복구 절차가 계속됩니다.
7. [특정 백업을 복구하기로 선택한 경우] 복구할 백업을 선택하고 **확인**을 클릭합니다.



잠시 후 복구가 시작되고 진행률이 표시됩니다. 복구가 완료되면 머신이 재부팅됩니다.

© Acronis International GmbH, 2003-2024



성능 및 백업 할당 시간

이 옵션을 사용하면 일주일 동안의 매 시간에 대해 세 가지 백업 성능 수준(높음, 낮음, 금지됨) 중 하나를 설정할 수 있습니다. 이런 식으로 백업이 시작 및 실행될 수 있는 할당 시간을 정의할 수 있습니다. 높음 및 낮음 성능 수준은 프로세스 우선 순위와 출력 속도를 통해 구성 가능합니다.

웹사이트 백업 또는 클라우드 복구 사이트에 위치한 서버의 백업처럼 클라우드 에이전트에 의해 실행되는 백업에는 이 옵션을 사용할 수 없습니다.

이 옵션은 백업 및 백업 복제 프로세스에 대해서만 유효합니다. 보호 계획에 포함된 백업 후 명령 및 기타 작업(예: 유효성 검사)은 이 옵션과 무관하게 실행됩니다.

사전 설정값이 **비활성화됨**입니다.

이 옵션이 비활성화되면 다음 매개변수와 함께 백업이 언제든 실행될 수 있습니다(매개변수가 사전 설정 값과 다르게 변경되어도 무관):

- CPU 우선순위: **낮음**(Windows에서는 **보통 이하**)
- 출력 속도: **무제한**

이 옵션이 활성화된 경우 예약된 백업은 현재 시간에 지정된 성능 매개변수에 따라 허용되거나 차단됩니다. 백업이 차단된 시간의 시작에서 백업 프로세스는 자동으로 중지되고 경보가 생성됩니다. 예약된 백업이 차단되더라도 백업은 수동으로 시작될 수 있습니다. 이 경우 백업이 허용된 가장 최근 시간의 성능 매개변수를 사용합니다.

© Acronis International GmbH, 2003-2024

참고

복제 위치마다 성능 및 백업 할당 시간을 개별적으로 설정할 수 있습니다. 복제 위치의 설정에 액세스하려면 보호 계획에서 위치 이름 옆의 기어 아이콘을 클릭한 다음 **성능 및 백업 할당 시간**을 클릭하십시오.

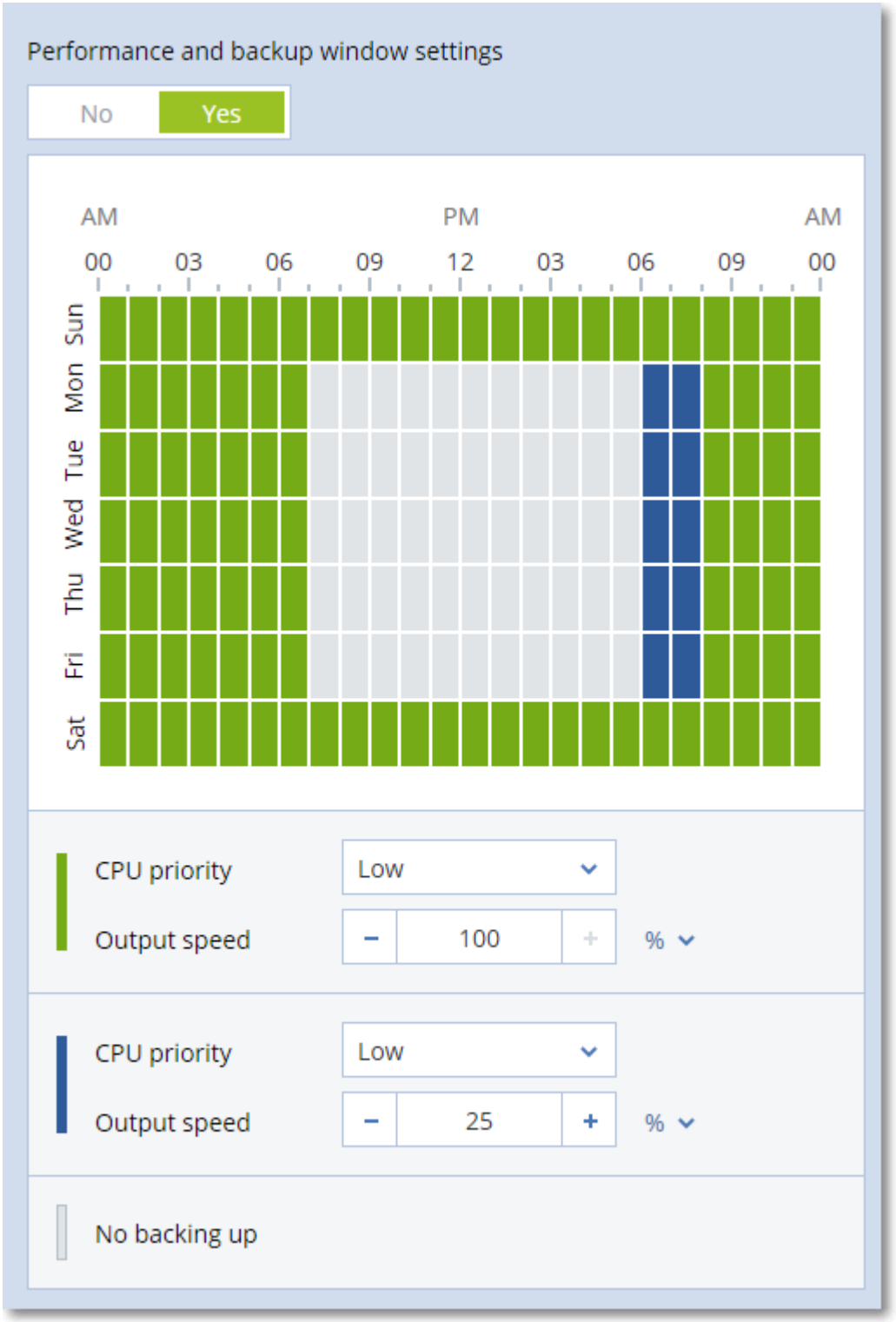
백업 할당 시간

각 직사각형이 평일 내 한 시간을 나타냅니다. 직사각형을 클릭하면 다음 상태를 순환합니다.

- **초록색:** 아래 초록색 섹션에 지정되어 있는 매개변수를 통해 백업이 허용됩니다.
- **파란색:** 아래 파란색 섹션에 지정되어 있는 매개변수를 통해 백업이 허용됩니다.
  백업 형식이 **버전 11**로 설정된 경우에는 이 상태를 사용할 수 없습니다.
- **회색:** 백업이 차단됩니다.

여러 직사각형의 상태를 동시에 변경하려면 클릭 후 드래그하면 됩니다.

© Acronis International GmbH, 2003-2024



CPU 우선 순위

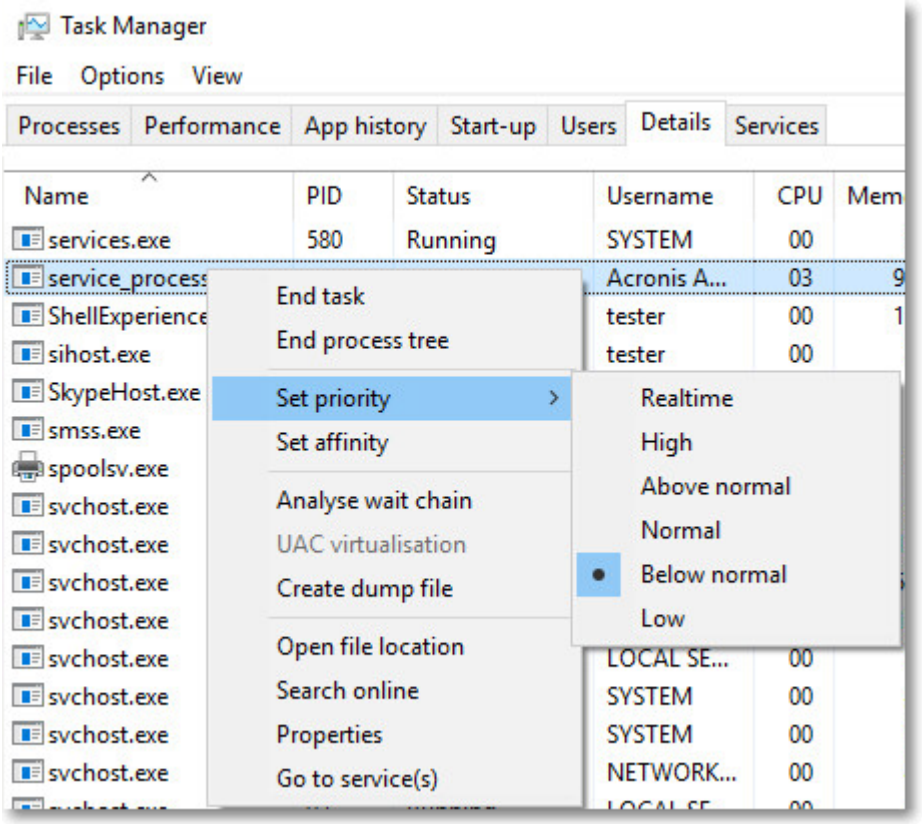
이 매개변수는 운영 체제에서 백업 프로세스의 우선 순위를 정의합니다.

사용 가능한 설정은 **낮음**, **보통**, **높음**입니다.

© Acronis International GmbH, 2003-2024

시스템에서 실행하는 프로세스의 우선 순위는 CPU와 해당 프로세스에 할당된 시스템 리소스를 결정합니다. 백업 우선순위를 낮추면 다른 애플리케이션에 더 많은 리소스를 사용할 수 있게 됩니다. 백업 우선순위를 높이면 CPU 등과 같은 더 많은 리소스를 백업 애플리케이션에 할당하도록 운영 체제에 요청하여 백업 프로세스의 속도를 높일 수 있습니다. 그러나 결과는 전체 CPU 사용량 및 디스크 입/출력 속도 또는 네트워크 트래픽 등과 같은 다른 요인에 따라 달라집니다.

이 옵션은 Windows에서는 백업 프로세스(**service_process.exe**)의 우선 순위를 설정하고, Linux 및 macOS에서는 백업 프로세스(**service_process**) 의 스케줄링 우선 순위를 설정합니다.



Windows, Linux 및 macOS의 이 설정 매핑 정보가 아래 표에 요약되어 있습니다.

Cyber Protection 우선 순위	**Windows 우선 순위**	**Linux 및 macOS 스케줄링 우선 순위**
낮음	보통보다 낮음	10
보통	보통	0
높음	높음	-10

백업 중 출력 속도

이 매개변수를 사용하여 하드 드라이브 쓰기 속도(로컬 폴더로 백업하는 경우) 또는 네트워크를 통한 백업 데이터 전송 속도(네트워크 공유 또는 클라우드 스토리지로 백업하는 경우)를 제한할 수 있습니다.

© Acronis International GmbH, 2003-2024

이 옵션이 활성화되어 있으면 다음과 같은 허용되는 최대 출력 속도를 지정할 수 있습니다.

- 대상 하드 디스크의 예상 쓰기 속도(로컬 폴더로 백업하는 경우) 또는 네트워크 연결의 예상 최고 속도(네트워크 공유 또는 클라우드 스토리지로 백업하는 경우)의 비율.
  이 설정은 에이전트가 Windows에서 실행 중인 경우에만 작동합니다.
- KB/초(모든 대상에 대해).

실제 데이터 전달

백업 또는 복제 대상이 클라우드 스토리지이고 백업 형식 이 **버전 12**로 설정되어 있으면 이 옵션을 사용할 수 있습니다.

이 옵션은 Agent for Windows, Agent for Linux, Agent for Mac, Agent for VMware, Agent for Hyper-V, 및 Agent for Virtuozzo에서 생성한 디스크 수준 백업 및 파일 백업에 효과적입니다.

이 옵션은 보호 계획에서 생성한 첫 번째 전체 백업을 실제 데이터 전달 서비스를 사용하여 하드 디스크 드라이브의 클라우드 스토리지로 보내고자 할 때 사용합니다. 이후 증분 백업은 네트워크를 통해 수행됩니다.

클라우드에 복제된 로컬 백업의 경우, 증분 백업이 계속되며 최초 백업이 클라우드 스토리지에 업로드 되기 전까지 로컬 상으로 저장됩니다. 그 후 모든 증분 변경 사항은 클라우드에 복제되고 백업 스케줄에 따라 복제가 계속됩니다.

사전 설정값이 **비활성화됨**.

실제 데이터 전달 서비스 정보

실제 데이터 전달 서비스 웹 인터페이스는 관리자가 사용할 수 있습니다.

실제 데이터 전달 서비스 및 주문 생성 도구의 사용에 대한 자세한 지침은 실제 데이터 전달 관리자 안내서를 참조하십시오. 실제 데이터 전달 서비스 웹 인터페이스에서 이 문서에 액세스하려면 물음표 아이콘을 클릭하십시오.

실제 데이터 전달 프로세스 개요

1. [클라우드 스토리지가 기본 백업 위치인 백업 전송하는 방법]
   a. 클라우드 백업으로 새로운 보호 계획을 생성합니다.
   b. **백업 옵션** 행에서 **변경**을 클릭합니다.
   c. 사용 가능한 옵션 목록에서 **실제 데이터 전달**을 클릭합니다.
   이동식 드라이브로 직접 백업하거나 로컬 또는 네트워크 폴더로 백업한 후 백업을 이동식 드라이브로 복사/이동할 수 있습니다.
2. [클라우드에 복제된 로컬 백업 전송하는 방법]

   참고
   이 옵션은 릴리스 C21.06 이상의 Protection 에이전트 버전에서 지원됩니다.

   a. 로컬 혹은 네트워크 스토리지 백업으로 새로운 보호 계획을 생성합니다.
   b. **위치 추가**를 클릭한 다음 **클라우드 스토리지**를 선택합니다.

© Acronis International GmbH, 2003-2024

c. **클라우드 스토리지** 위치 열에서 기어 휠을 클릭한 다음 **실제 데이터 전송**을 선택합니다.

3. **실제 데이터 전달 사용** 하에서 **네**를 클릭한 다음 **완료**를 클릭합니다.
   전송되는 모든 백업 파일은 암호화되어야 하므로 보호 계획에서 자동으로 암호화 옵션이 활성화됩니다.
4. **암호화** 열에서 **비밀번호 지정**을 선택한 다음 암호화에 사용할 비밀번호를 입력합니다.
5. **실제 데이터 전달** 열에서 최초 백업을 저장할 이동식 드라이브를 선택합니다.
6. **생성**을 클릭하여 보호 계획을 저장합니다.
7. 첫 번째 백업이 완료된 후 실제 데이터 전달 서비스 웹 인터페이스를 사용하여 주문 생성 도구를 다운로드하고 주문을 생성합니다.
   웹 인터페이스에 액세스하려면 관리 포털에 로그인하고 **개요** > **사용**을 클릭한 다음 **실제 데이터 전달** 아래의 **서비스 관리**를 클릭합니다.

   중요
   초기 전체 백업이 완료되면 이후의 백업은 동일한 보호 계획으로 수행해야 합니다. 다른 보호 계획에서는 매개변수와 머신이 동일하더라도 또 다른 실제 데이터 전달 사이클이 필요합니다.

8. 드라이브를 패키징하고 데이터 센터에 전달합니다.

   중요
   실제 데이터 전달 관리자 안내서에 나온 패키징 지침을 따라야 합니다.

9. 실제 데이터 전달 서비스 웹 인터페이스를 사용하여 주문 상태를 추적하십시오. 이후의 백업은 처음 백업이 클라우드 스토리지에 업로드될 때까지 실패하게 됩니다.

사전/사후 명령어

이 옵션을 사용하여 백업 절차 전과 후에 자동으로 실행될 명령을 정의할 수 있습니다.

다음 도식은 사전/사후 명령어를 언제 실행하는지 보여줍니다.

백업 전 명령	백업	백업 후 명령

사전/사후 명령어를 사용하는 방법의 예:

- 백업을 시작하기 전에 디스크에서 일부 임시 파일을 삭제합니다.
- 백업을 시작하기 전에 매번 서드 파티 안티바이러스 제품을 시작하도록 구성합니다.
- 선택적으로 백업을 다른 위치로 복사합니다. 이 옵션을 활성화하면 보호 계획에 구성되어 있는 복제가 *모든* 백업을 후속 위치로 복사하기 때문에 유용할 수 있습니다.

에이전트는 백업 후 명령을 실행한 *이후* 복제를 수행합니다.

프로그램은 대화형 명령, 즉 사용자 입력(예: "pause")이 필요한 명령을 지원하지 않습니다.

백업 전 명령

백업 프로세스가 시작되기 전에 실행할 명령/배치 파일을 지정하려면

© Acronis International GmbH, 2003-2024

1. **백업 전 명령 실행** 스위치를 활성화합니다.
2. **명령...** 필드에 명령을 입력하거나 배치 파일을 찾습니다.프로그램은 대화형 명령, 즉 사용자 입력(예: "pause")이 필요한 명령을 지원하지 않습니다.
3. **작업 디렉토리** 필드에 명령/배치 파일을 실행할 디렉토리의 경로를 지정합니다.
4. 필요한 경우 **인수** 필드에 명령 실행 인수를 지정합니다.
5. 원하는 결과에 따라 아래 표에 설명한 대로 적합한 옵션을 선택합니다.
6. **완료**를 클릭합니다.

확인란	**선택**			
명령 실행에 실패한 경우 백업 실패	선택됨	선택 해제됨	선택됨	선택 해제됨
명령 실행이 완료될 때까지 백업 안 함	선택됨	선택됨	선택 해제됨	선택 해제됨
결과				
	사전 설정 명령이 성공적으로 실행된 후에만 백업을 수행합니다. 명령 실행에 실패한 경우 백업 실패.	실행 실패 또는 성공에 상관없이 명령이 실행된 후에 백업을 수행합니다.	해당 없음	명령 실행 결과에 상관없이 명령 실행과 동시에 백업을 수행합니다.

* 이 종료 코드가 0과 같지 않다면 명령이 실패한 것으로 간주됩니다.

참고
Linux의 필수 라이브러리 버전 관련 충돌로 인해 스크립트 실행이 실패하면 스크립트에 다음 줄을 추가하여 `LD_LIBRARY_PATH` 및 `LD_PRELOAD` 환경 변수를 제외합니다.

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

백업 후 명령

백업이 완료된 후에 실행할 명령/실행 파일을 지정하려면

1. **백업 후 명령 실행** 스위치를 활성화합니다.
2. **명령...** 필드에 명령을 입력하거나 배치 파일을 찾습니다.
3. **작업 디렉토리** 필드에 명령/배치 파일을 실행할 디렉토리의 경로를 지정합니다.
4. 필요한 경우 **인수** 필드에 명령 실행 인수를 지정합니다.

© Acronis International GmbH, 2003-2024

5. 명령 실행이 반드시 성공해야 하는 경우 **명령 실행에 실패한 경우 백업 실패** 확인란을 선택합니다. 이 종료 코드가 0과 같지 않다면 명령이 실패한 것으로 간주됩니다. 명령 실행에 실패하면 백업 상태가 **오류**로 설정됩니다.

   이 확인란을 선택하지 않으면 명령 실행 결과가 백업 실패 또는 성공에 영향을 주지 않습니다. **작업** 탭을 살펴보면 명령 실행 결과를 추적할 수 있습니다.
6. **완료**를 클릭합니다.

데이터 캡처 전/후 명령

이 옵션을 사용하여 데이터 캡처(즉, 데이터 스냅샷 생성) 전과 후에 자동으로 실행될 명령을 정의할 수 있습니다. 데이터 캡처는 백업 절차 시작 시 수행됩니다.

다음 도식에 데이터 캡처 전/후 명령이 실행되는 시기가 나와 있습니다.

	<---------- 백업 ---------->				
백업 전 명령	데이터 캡처 전 명령	데이터 캡처	데이터 캡처 후 명령	백업 세트에 데이터 쓰기	백업 후 명령

다른 백업 옵션과 상호 작용

다른 백업 옵션을 통해 데이터 캡처 전/후 명령 실행을 수정할 수 있습니다.

다중 볼륨 스냅샷 옵션을 활성화하면 데이터 캡처 전/후 명령이 한 번만 실행됩니다. 모든 볼륨의 스냅샷이 동시에 생성되기 때문입니다. **다중 볼륨 스냅샷** 옵션을 비활성화하면 백업하는 모든 볼륨에서 데이터 캡처 전/후 명령이 실행됩니다. 스냅샷이 각 볼륨에서 순서대로 생성되기 때문입니다.

VSS(Volume Shadow Copy Service) 옵션을 활성화하면 데이터 캡처 전/후 명령과 Microsoft VSS 작업이 다음과 같이 실행됩니다.

데이터 캡처 전 명령 > *VSS 일시 중지* > *데이터 캡처* > *VSS 재개* > *데이터 캡처 후 명령*

데이터 캡처 전/후 명령을 사용하여 VSS와 호환되지 않는 데이터베이스 또는 애플리케이션을 일시 중지했다가 다시 시작할 수 있습니다. 데이터 캡처는 몇 초 안에 완료되기 때문에 데이터베이스 또는 애플리케이션 유휴 시간은 최소화됩니다.

데이터 캡처 전 명령

데이터 캡처 전에 실행할 명령/배치 파일을 지정하려면

1. **데이터 캡처 전 명령 실행** 스위치를 활성화합니다.
2. **명령...** 필드에 명령을 입력하거나 배치 파일을 찾습니다.프로그램은 대화형 명령, 즉 사용자 입력(예: "pause")이 필요한 명령을 지원하지 않습니다.
3. **작업 디렉토리** 필드에 명령/배치 파일을 실행할 디렉토리의 경로를 지정합니다.
4. 필요한 경우 **인수** 필드에 명령 실행 인수를 지정합니다.
5. 원하는 결과에 따라 아래 표에 설명한 대로 적합한 옵션을 선택합니다.
6. **완료**를 클릭합니다.

© Acronis International GmbH, 2003-2024

확인란	선택			
명령 실행에 실패한 경우 백업 실패	선택됨	선택 해제됨	선택됨	선택 해제됨
명령 실행이 완료될 때까지 데이터 캡처 수행 안 함	선택됨	선택됨	선택 해제됨	선택 해제됨
결과				
	사전 설정 명령이 성공적으로 실행된 후에만 데이터 캡처를 수행합니다. 명령 실행에 실패한 경우 백업 실패.	실행 실패 또는 성공에 상관없이 명령이 실행된 후에 데이터 캡처를 수행합니다.	해당 없음	명령 실행 결과에 상관없이 명령 실행과 동시에 데이터 캡처를 수행합니다.

* 이 종료 코드가 0과 같지 않다면 명령이 실패한 것으로 간주됩니다.

참고
Linux의 필수 라이브러리 버전 관련 충돌로 인해 스크립트 실행이 실패하면 스크립트에 다음 줄을 추가하여 LD_LIBRARY_PATH 및 LD_PRELOAD 환경 변수를 제외합니다.

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

데이터 캡처 후 명령

데이터 캡처가 완료된 후에 실행할 명령/배치 파일을 지정하려면

1. **데이터 캡처 후 명령 실행** 스위치를 활성화합니다.
2. **명령...** 필드에 명령을 입력하거나 배치 파일을 찾습니다.프로그램은 대화형 명령, 즉 사용자 입력(예: "pause")이 필요한 명령을 지원하지 않습니다.
3. **작업 디렉토리** 필드에 명령/배치 파일을 실행할 디렉토리의 경로를 지정합니다.
4. 필요한 경우 **인수** 필드에 명령 실행 인수를 지정합니다.
5. 원하는 결과에 따라 아래 표에 설명한 대로 적합한 옵션을 선택합니다.
6. **완료**를 클릭합니다.

확인란	선택			
명령 실행에 실패한 경우 백업 실패	선택됨	선택 해제됨	선택됨	선택 해제됨

© Acronis International GmbH, 2003-2024

명령 실행이 완료될 때까지 백업 안 함	선택됨	선택됨	선택 해제됨	선택 해제됨
결과				
	사전 설정 명령이 성공적으로 실행된 후에만 백업을 계속 진행합니다.	실행 실패 또는 성공에 상관없이 명령이 실행된 후에 백업을 계속 진행합니다.	해당 없음	명령 실행 결과에 상관없이 명령 실행과 동시에 백업을 계속 진행합니다.

* 이 종료 코드가 0과 같지 않다면 명령이 실패한 것으로 간주됩니다.

일정 예약

이 옵션은 백업을 정확히 예약한 대로 시작할지 아니면 일정 지연 시간 후에 시작할지를 정의하며 동시에 백업할 가상 머신 수도 정의합니다.

백업 스케줄 구성 방법에 대한 자세한 내용은 "스케줄에 따라 백업 실행"(383페이지) 항목을 참조하십시오.

사전 설정값이 **일정 시간 내에 백업 시작 시간을 분배합니다. 최대 지연: 30분.**

다음 중 하나를 선택합니다.

- **예약된 대로 정확하게 모든 백업 시작**
  실제 머신의 백업이 예약된 대로 정확하게 시작됩니다. 가상 머신은 하나씩 백업됩니다.
- **기간 내에서 시작 시간 분배**
  실제 머신의 백업이 예약된 시간보다 지연되어 시작됩니다. 각 머신에 대한 지연 값은 임의로 선택되며 이 값의 범위는 0에서부터 지정된 최대값까지 입니다. 여러 머신을 네트워크 위치로 백업하는 경우 과도한 네트워크 부하를 피하기 위해 이 설정을 사용할 수 있습니다. 보호 계획이 머신에 적용될 때 각 머신에 대한 지연 값이 결정되어 보호 계획을 편집하고 최대 지연 값을 변경할 때까지 동일하게 유지됩니다.
  가상 머신은 하나씩 백업됩니다.
- **다음까지 동시에 실행되는 백업 수 제한**
  하이퍼바이저 수준에서 백업된 가상 머신(비에이전트 백업)의 병렬 백업을 관리하려면 이 옵션을 사용합니다.
  이 옵션을 선택한 보호 계획은 동일한 에이전트가 동시에 작동 중인 다른 계획과 함께 실행할 수 있습니다. 이 옵션을 선택하는 경우 계획당 병렬 백업 수를 지정해야 합니다. 모든 계획에서 동시 백업되는 총 머신 수는 에이전트당 10개로 제한됩니다. 기본 제한을 변경하는 방법을 알아보려면 "동시 백업되는 가상 머신의 총 수를 제한합니다."(638페이지) 항목을 참조하십시오.
  이 옵션을 선택하지 않은 보호 계획은 백업 작업을 순차적으로 실행하여 가상 머신을 한 번에 하나씩 백업합니다.

© Acronis International GmbH, 2003-2024

섹터 단위 백업

이 옵션은 디스크 수준 백업에 대해서만 유효합니다.

이 옵션은 물리적 수준에서 디스크 또는 볼륨의 똑같은 사본을 생성할지 결정합니다.

사전 설정값이 **비활성화됨**.

이 옵션이 활성화되어 있는 경우 할당되지 않은 공간과 데이터가 없는 섹터를 포함한 디스크 또는 볼륨의 모든 섹터가 백업됩니다. 생성되는 백업은 백업 대상 디스크와 크기가 같아집니다("압축 수준" 옵션이 **없음**으로 설정되어 있는 경우). 인식되지 않는 또는 지원되지 않는 파일 시스템이 있는 드라이브를 백업할 때에는 소프트웨어가 섹터 단위 모드로 자동 전환됩니다.

참고
섹터 단위 모드에서 생성된 백업의 애플리케이션 데이터에 대한 복구를 실행하는 것이 불가능해집니다.

분할

이 옵션을 통해 대용량 백업을 더 작은 파일들로 분할하는 방법을 선택할 수 있습니다.

참고
클라우드 스토리지를 백업 위치로 사용하는 보호 계획에서는 분할을 사용할 수 없습니다.

사전 설정값이

- 백업 위치가 로컬 또는 네트워크(SMB) 폴더이고 백업 형식이 버전 12일 경우: **고정 크기 - 200GB**
  이 설정을 이용하면 백업 소프트웨어가 NTFS 파일 시스템상의 대량의 데이터를 파일 단편화로 인한 부정적인 영향 없이 작업할 수 있습니다.
- 그렇지 않은 경우: **자동**

다음 설정을 사용할 수 있습니다.

- **자동**
  백업이 파일 시스템에서 지원하는 최대 파일 크기를 초과하는 경우 분할됩니다.
- **고정 크기**
  원하는 파일 크기를 입력하거나 드롭다운 목록에서 선택합니다.

작업 실패 처리

이 옵션은 예약된 보호 계획 실행이 실패하거나 백업이 실행되는 중에 머신이 다시 시작되는 경우의 프로그램 동작을 결정합니다. 이 옵션은 보호 계획을 수동으로 시작할 때에는 적용되지 않습니다.

© Acronis International GmbH, 2003-2024

이 옵션이 활성화되어 있는 경우 프로그램이 보호 계획을 다시 실행하려고 시도합니다. 시도 횟수와 시도 간 시간 간격을 지정할 수 있습니다. 시도가 성공적으로 완료되거나 성공하기 전에 지정된 시도 횟수를 모두 수행하고 나면 프로그램이 시도를 중지합니다.

이 옵션이 활성화되어 있으면 백업이 실행되는 중에 머신이 다시 시작되더라도 백업 작업이 실패하지 않습니다. 다시 시작 후 몇 분이 지나면 백업 작업이 자동으로 계속되며 누락된 데이터가 추가되어 백업 파일이 완성됩니다. 이 사용 사례에서는 **시도 간격** 옵션이 사용되지 않습니다.

사전 설정값이 **활성화됨**.

참고
이 옵션은 포렌식 백업에는 효과가 없습니다.

작업 시작 조건

이 옵션은 Windows 및 Linux 운영 체제에서 유효합니다.

이 옵션은 작업이 시작하려고 하지만(스케줄된 시간이 되었거나 스케줄에 지정된 이벤트가 발생함) 조건(여러 개의 조건 중 하나라도)이 맞지 않는 경우 프로그램의 동작을 결정합니다. 조건에 대한 자세한 내용은 "시작 조건"(388페이지) 항목을 참조하십시오.

사전 설정값이 **스케줄의 조건이 충족될 때까지 대기합니다.**

스케줄의 조건이 충족될 때까지 대기

이 설정을 사용하면 스케줄러는 조건 모니터링을 시작하고 조건이 충족되자마자 작업을 시작합니다. 조건이 절대 충족되지 않는 경우에는 작업이 시작되지 않습니다.

조건이 너무 오랫 동안 충족되지 않고 작업을 더 지연하면 위험하게 되는 상황을 처리하기 위해서는 조건과 관계 없이 작업을 실행하게 할 시간 간격을 설정할 수 있습니다. **다음 시간 후에는 무조건 작업 실행** 확인란을 선택하고 시간 간격을 지정합니다. 작업은 조건 충족 또는 최대 시간 지연 경과 중 하나가 먼저 발생하자마자 즉시 시작됩니다.

작업 실행 건너뛰기

작업을 지연하는 것이 적합하지 않을 수도 있습니다. 예를 들어, 작업을 지정된 시간에 정확하게 실행해야 하는 경우가 있습니다. 특히 작업이 비교적 자주 발생하는 경우에는 조건이 충족되기를 기다리는 대신 작업을 건너뛰는 것이 좋습니다.

VSS(Volume Shadow Copy Service)

이 옵션은 Windows 운영 체제에만 적용됩니다.

이 옵션은 VSS(Volume Shadow Copy Service) Writer 하나 이상에 오류가 발생하더라도 백업은 성공하는지 여부, 그리고 VSS 인식 애플리케이션에 백업을 시작하라는 알림을 전송해야 하는 공급자를 정의합니다.

Volume Shadow Copy Service 사용 시에는 애플리케이션이 사용하는 모든 데이터의 상태를 일관되게 유지할 수 있습니다. 특히 백업 소프트웨어가 데이터 스냅샷을 생성하는 시점에 모든 데이터베

© Acronis International GmbH, 2003-2024

이스 트랜잭션이 완료되어 있도록 할 수 있습니다. 데이터 일관성은 또한 애플리케이션이 올바른 상태로 복구되고 복구 후 즉시 작동이 가능하도록 해줍니다.

스냅샷은 백업 작업 중에만 사용되며 백업 작업이 완료되면 자동으로 삭제됩니다. 임시 파일은 보존되지 않습니다.

데이터 캡처 전/후 명령을 사용하여 데이터가 일관된 상태로 백업되도록 할 수도 있습니다. 예를 들어 데이터베이스를 일시 중단하고 모든 캐시를 플러시하는 데이터 캡처 전 명령을 지정하여 모든 트랜잭션이 완료되도록 할 수 있습니다. 그런 후에는 스냅샷 생성 후 데이터베이스 작업을 다시 시작하도록 하는 데이터 캡처 후 명령을 지정할 수 있습니다.

참고
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot 레지스트리 키에 지정된 파일과 폴더가 백업되지 않습니다. 특히 오프라인 Outlook 데이터 파일(.ost)은 이 키의 **OutlookOST** 값에 지정되므로 백업되지 않습니다.

오류가 발생한 VSS Writer 무시

다음 중 하나를 선택합니다.

- **오류가 발생한 VSS Writer 무시**
  이 옵션을 사용하면 VSS Writer 하나 이상에 오류가 발생하더라도 백업은 정상적으로 수행할 수 있습니다.

  중요
  애플리케이션별 Writer에서 오류가 발생하면 애플리케이션 인식 백업은 항상 실패합니다. 예를 들어 SQL Server 데이터의 애플리케이션 인식 백업을 만들 때 **SqlServerWriter**가 실패하면 백업 작업도 실패합니다.

  이 옵션을 활성화하면 VSS 스냅샷 생성을 연속 3회까지 시도합니다.
  첫 번째 시도에서는 모든 VSS Writer가 필요합니다. 첫 시도가 실패하면 같은 방식으로 작업을 한 번 더 시도합니다. 두 번째 시도도 실패하면 오류가 발생한 VSS Writer가 백업 작업 범위에서 제외된 후 세 번째로 작업을 시도합니다. 세 번째 시도가 성공하면 백업이 완료되며 오류 발생 VSS Writer 관련 경고가 표시됩니다. 세 번째 시도도 실패하면 백업은 실패합니다.
- **모든 VSS Writer를 정상적으로 처리해야 함**
  VSS Writer 중 하나라도 오류가 발생하면 백업 작업도 실패합니다.

스냅샷 공급자 선택

다음 중 하나를 선택합니다.

- **자동으로 스냅샷 공급자 선택**
  하드웨어 스냅샷 공급자, 소프트웨어 스냅샷 공급자 및 Microsoft Software Shadow Copy Provider 중에서 자동으로 선택합니다.
- **Microsoft Software Shadow Copy Provider 사용**

© Acronis International GmbH, 2003-2024

애플리케이션 서버(Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint 또는 Active Directory) 백업 시 이 옵션을 선택하는 것이 좋습니다.

VSS 전체 백업 활성화

이 옵션을 활성화하면 전체/증분/차등 디스크 수준 백업이 정상적으로 완료될 때마다 Microsoft Exchange Server와 기타 VSS 인식 애플리케이션(Microsoft SQL Server는 제외)의 로그가 잘립니다.

사전 설정값이 **비활성화됨**입니다.

다음과 같은 경우 이 옵션을 비활성화 상태로 두십시오.

- Agent for Exchange 또는 서드 파티 소프트웨어를 사용하여 Exchange Server 데이터를 백업하는 경우. 이 경우 로그 잘림이 연속 트랜잭션 로그 백업을 방해하기 때문입니다.
- 서드 파티 소프트웨어를 사용하여 SQL Server 데이터를 백업하는 경우. 이 경우에는 서드 파티 소프트웨어가 "자체" 전체 백업을 위해 생성된 디스크 수준 백업을 가져가기 때문입니다. 결국, SQL Server 데이터의 다음 번 차등 백업은 실패합니다. 백업은 서드 파티 소프트웨어가 다음 번 "자체" 전체 백업을 생성할 때까지 계속 실패합니다.
- 다른 VSS 인식 애플리케이션이 머신에서 실행 중이고 어떤 이유로 해당 로그를 유지해야 하는 경우.

중요
이 옵션을 활성화하면 Microsoft SQL Server 로그가 잘리지 않습니다. 백업 후 SQL Server 로그를 자르려면 로그 자르기 백업 옵션을 활성화하십시오.

가상 머신용 VSS(Volume Shadow Copy Service)

이 옵션은 가상 머신의 정지 스냅샷을 생성할지 정의합니다.

사전 설정값이 **활성화됨**.

이 옵션이 비활성화되어 있는 경우 비정지 스냅샷이 생성됩니다. 가상 머신이 크래시 일관성 상태에서 백업됩니다.

이 옵션이 활성화되어 있으면 가상 머신에서 실행 중인 모든 VSS 인식 애플리케이션의 트랜잭션이 완료된 후에 정지 스냅샷이 생성됩니다.

"오류 처리" 옵션에 지정된 횟수만큼 재시도했는데 정지 스냅샷이 생성되지 않은 경우 애플리케이션 백업이 활성화되어 있어도 백업이 실패합니다.

"오류 처리" 옵션에 지정된 횟수만큼 재시도했는데 정지 스냅샷이 생성되지 않은 경우 애플리케이션 백업이 비활성화되어 있으면 크래시 일관성 백업이 생성됩니다. 크래시 일관성 백업을 생성하는 대신 백업이 실패하도록 설정하려면 **정지 스냅샷을 생성할 수 없으면 백업 실패 처리** 확인란을 선택합니다.

사용 가능한 설정과 각 설정 사용 시의 결과가 다음 표에 요약되어 있습니다.

© Acronis International GmbH, 2003-2024

설정	정지 스냅샷이 생성됨		정지 스냅샷이 생성되지 않음	
	애플리케이션 백업이 활성화됨	애플리케이션 백업이 비활성화됨	애플리케이션 백업이 활성화됨	애플리케이션 백업이 비활성화됨
가상 머신용 VSS (Volume Shadow Copy Service)가 활성화됨 **정지 스냅샷을 생성할 수 없으면 백업 실패 처리**가 선택되지 않음	정지 스냅샷이 생성됩니다. 애플리케이션 일관성을 보장하는 백업이 생성됩니다.	정지 스냅샷이 생성됩니다. 애플리케이션 일관성을 보장하는 백업이 생성됩니다.	백업이 실패합니다.	비정지 스냅샷이 생성됩니다. 크래시 일관성 백업이 생성됩니다.
가상 머신용 VSS (Volume Shadow Copy Service)가 활성화됨 **정지 스냅샷을 생성할 수 없으면 백업 실패 처리**가 선택됨	정지 스냅샷이 생성됩니다. 애플리케이션 일관성을 보장하는 백업이 생성됩니다.	정지 스냅샷이 생성됩니다. 애플리케이션 일관성을 보장하는 백업이 생성됩니다.	백업이 실패합니다.	백업이 실패합니다.
가상 머신용 VSS (Volume Shadow Copy Service)가 비활성화됨	비정지 스냅샷이 생성됩니다. 크래시 일관성 백업이 생성됩니다.	비정지 스냅샷이 생성됩니다. 크래시 일관성 백업이 생성됩니다.	비정지 스냅샷이 생성됩니다. 크래시 일관성 백업이 생성됩니다.	비정지 스냅샷이 생성됩니다. 크래시 일관성 백업이 생성됩니다.

가상 머신용 VSS(Volume Shadow Copy Service)를 활성화하면 백업된 가상 머신에 저장되어 있을 수 있는 정지 전 및 해제 후 스크립트도 트리거됩니다. 이러한 스크립트에 대한 자세한 내용은 "정지 전 및 해제 후 스크립트 자동 실행"(632페이지)을(를) 참조하십시오.

정지 스냅샷을 생성하기 위해 백업 소프트웨어가 VMware Tools, Hyper-V Integration Services, Virtuozzo 게스트 도구, Red Hat Virtualization 게스트 도구 또는 QEMU 게스트 도구를 사용해 가상 머신 내에서 VSS를 적용합니다.

참고

Red Hat Virtualization(oVirt) 가상 머신의 경우 Red Hat Virtualization 게스트 도구 대신 QEMU 게스트 도구를 사용하는 것이 좋습니다. 일부 Red Hat Virtualization 게스트 도구는 애플리케이션 일치 스냅샷을 지원하지 않습니다.

이 옵션은 Scale Computing HC3 가상 머신에는 영향을 주지 않습니다. 이 경우 정지는 Scale 도구가 가상 머신에 설치되었는지 여부에 따라 다릅니다.

© Acronis International GmbH, 2003-2024

주간 백업

이 옵션은 보관 규칙 및 백업 구성표에서 어떤 백업을 "주간"으로 고려할지 결정합니다. "주간" 백업은 한 주가 시작된 후 생성된 첫 번째 백업입니다.

사전 설정값이 **월요일**입니다.

Windows 이벤트 로그

이 옵션은 Windows 운영 체제에서만 유효합니다.

이 옵션은 에이전트가 Windows의 애플리케이션 이벤트 로그에 백업 작업의 이벤트를 기록해야 하는지 정의합니다(이 로그를 보려면 eventvwr.exe를 실행하거나 **제어판** > **관리 도구** > **이벤트 뷰어** 선택). 기록할 이벤트를 필터링할 수 있습니다.

사전 설정값이 **비활성화됨**.

복구

복구 치트 시트

다음 표는 사용 가능한 복구 방법을 요약해서 보여줍니다. 이 표를 사용하여 필요에 가장 잘 맞는 복구 방법을 선택할 수 있습니다.

참고
규제 준수 모드 상태인 테넌트의 경우에는 Cyber Protect 콘솔에서 백업을 복구할 수 없습니다. 이러한 백업을 복구하는 방법에 대한 자세한 내용은 "규제 준수 모드로 설정된 테넌트의 백업 복구" (983페이지) 항목을 참조하십시오.

복구 대상	복구 방법
실제 머신 (Windows 또는 Linux)	Cyber Protect 콘솔 사용 부트 가능한 미디어 사용
실제 머신 (Mac)	부트 가능한 미디어 사용
가상 머신 (VMware, Hyper-V, Red Hat Virtualization(oVirt) 또는 Scale Computing HC3)	Cyber Protect 콘솔 사용 부트 가능한 미디어 사용
가상 머신 또는 컨테이너 (Virtuozzo, Virtuozzo Hybrid Server 또는 Virtuozzo Hybrid Infrastructure)	Cyber Protect 콘솔 사용

© Acronis International GmbH, 2003-2024

ESXi 구성	부트 가능한 미디어 사용
파일/폴더	Cyber Protect 콘솔 사용 클라우드 스토리지에서 파일 다운로드 부트 가능한 미디어 사용 로컬 백업에서 파일 추출
시스템 상태	Cyber Protect 콘솔 사용
SQL 데이터베이스	Cyber Protect 콘솔 사용
Exchange 데이터베이스	Cyber Protect 콘솔 사용
Exchange 사서함	Cyber Protect 콘솔 사용
웹사이트	Cyber Protect 콘솔 사용
Microsoft 365	
사서함 (로컬 Agent for Microsoft 365)	Cyber Protect 콘솔 사용
사서함 (클라우드 Agent for Microsoft 365)	Cyber Protect 콘솔 사용
공용 폴더	Cyber Protect 콘솔 사용
OneDrive 파일	Cyber Protect 콘솔 사용
SharePoint 온라인 데이터	Cyber Protect 콘솔 사용
Google Workspace	
사서함	Cyber Protect 콘솔 사용
Google Drive 파일	Cyber Protect 콘솔 사용
Shared Drive 파일	Cyber Protect 콘솔 사용

플랫폼 간 복구

운영 체제가 포함된 디스크 백업과 전체 머신 백업에 플랫폼 간 복구를 사용할 수 있습니다.

플랫폼 간 복구는 다음과 같은 경우에 수행됩니다.

© Acronis International GmbH, 2003-2024

- 백업을 생성한 에이전트 유형과 복구하는 에이전트 유형이 다른 경우.
- 에이전트 기반 백업을 하이퍼바이저 수준에서 복구(비에이전트 복구)하거나 비에이전트 백업을 에이전트로 복구(에이전트 기반 복구)하는 경우.
- 가상 하드웨어를 비롯한 이기종 하드웨어에 백업을 복구하는 경우.

참고
플랫폼 간 복구 수행 시에는 프린터 등의 일부 주변 장치가 올바르게 복구되지 않을 수도 있습니다.

아래 표에 플랫폼 간 복구의 몇 가지 예가 나와 있습니다.

플랫폼 간 복구	
비에이전트 백업	에이전트 기반 복구
에이전트 기반 백업	비에이전트 복구
Agent for Windows를 통한 백업	Agent for VMware를 통한 복구
Agent for VMware를 통한 백업	Agent for Hyper-V를 통한 복구
VMware ESXi 가상 머신에 설치된 Agent for Windows를 통한 백업(에이전트 기반)	동일한 VMware ESXi 호스트의 Agent for VMware를 통한 복구(비에이전트 복구)
Agent for Windows를 통한 백업	이기종 하드웨어가 포함된 머신에 설치되어 있는 Agent for Windows를 통한 복구
실제 머신의 백업	가상 머신으로 복구

Mac 사용자 참고 사항

- 10.11 El Capitan으로 시작하는 특정 시스템 파일, 폴더 및 프로세스는 확장된 파일 속성 com.apple.rootless를 사용하여 보호하기 위해 플래그가 지정되어 있습니다.이 기능은 SIP(시스템 무결성 보호)라고 합니다. 보호된 파일에는 사전 설치된 애플리케이션 및 /system, /bin, /sbin, /usr의 대부분의 폴더가 포함되어 있습니다.

  보호된 파일 및 폴더는 운영 체제에서 복구되는 동안 덮어쓸 수 없습니다. 보호된 파일을 덮어써야 하는 경우 부트 가능한 미디어에서 복구를 수행합니다.
- macOS Sierra 10.12부터 자주 사용하지 않는 파일은 클라우드의 저장 기능을 통해 iCloud로 이동될 수 있습니다.이러한 파일의 작은 풋프린트가 파일 시스템에 유지됩니다. 원래 파일 대신 이러한 풋프린트가 백업됩니다.

  원래 위치로 풋프린트를 복구하면 iCloud와 동기화하여 원래 파일을 사용할 수 있게 됩니다. 다른 위치로 풋프린트를 복구하면 동기화될 수 없고 원래 파일을 사용할 수 없습니다.

안전 복구

백업에 감염된 파일이 포함되어 있더라도 맬웨어가 없는 데이터만 복구되도록 하려면 Windows 워크로드의 **전체 머신** 또는 **디스크/볼륨** 백업에서 안전 복구를 사용하십시오.

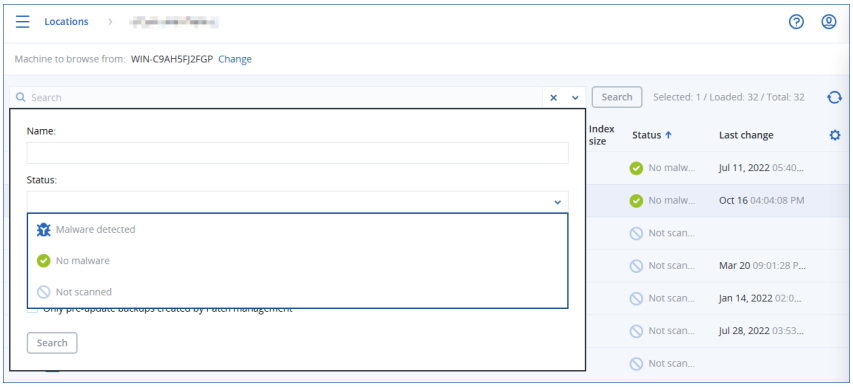
© Acronis International GmbH, 2003-2024

안전 복구 작업 중에는 백업을 자동으로 스캔하여 맬웨어 유무를 확인합니다. 그리고 나면 보호 에이전트가 대상 워크로드에 백업을 복구하고 감염된 파일을 삭제합니다. 그러므로 맬웨어가 없는 백업이 복구됩니다.

그리고 백업에 다음 상태 중 하나가 할당됩니다.

- 맬웨어 감지됨
- 맬웨어 없음
- 스캔되지 않음

상태를 사용하여 백업 아카이브를 필터링 수 있습니다.



제한 사항

- 안전 복구는 보호 에이전트가 설치된 실제 및 가상 Windows 머신에서 지원됩니다.
- 안전 복구는 **전체 머신** 또는 **디스크/볼륨** 백업에서 지원됩니다.
- NTFS 볼륨만 스캔하여 맬웨어 유무를 확인합니다. NTFS가 아닌 볼륨은 맬웨어 방지 스캔 없이 복구됩니다.
- 아카이브의 CDP(지속적인 데이터 보호) 백업에서는 안전 복구가 지원되지 않습니다. CDP 백업에서 데이터를 복구하려면 **파일/폴더** 복구 작업을 추가로 실행하십시오. CDP 백업 관련 추가 작업은 "지속적인 데이터 보호(CDP)"(372페이지) 항목을 참조하십시오.

머신 복구

실제 머신 복구

이 섹션에서는 웹 인터페이스를 사용한 실제 머신 복구에 대해 설명합니다.

다음을 복구하려는 경우에는 웹 인터페이스 대신 부트 가능한 미디어를 사용합니다.

- macOS를 실행 중인 머신
- 규제 준수 모드가 설정된 테넌트의 머신
- 베어 메탈 또는 오프라인 머신으로 임의의 운영 체제 복구
- 논리 볼륨의 구조(Linux에서는 논리 볼륨 관리자가 생성한 볼륨). 미디어를 사용하여 논리 볼륨 구조를 자동으로 재생성할 수 있습니다.

© Acronis International GmbH, 2003-2024

참고
Intel 기반 Mac의 디스크 수준 백업을 Apple 실리콘 프로세서를 사용하는 Mac에 복구할 수는 없으며, 그 반대 방향의 복구도 불가능합니다. 파일과 폴더를 복구할 수 있습니다.

복구 및 다시 시작

운영 체제 복구 및 BitLocker로 암호화된 볼륨 복구 시에는 머신을 다시 시작해야 합니다. 자동으로 머신을 다시 시작할지 머신을 **상호 작용 필요** 상태로 할당할지 선택할 수 있습니다. 복구된 운영 체제는 자동으로 온라인이 됩니다.

중요
백업된 암호화 볼륨은 암호화되지 않은 볼륨으로 복구됩니다.

BitLocker로 암호화된 볼륨을 복구하려면 같은 머신에 암호화되지 않은 볼륨이 있어야 하며, 해당 볼륨의 여유 공간이 1GB 이상이어야 합니다. 두 조건 중 하나라도 충족되지 않으면 복구는 실패합니다.

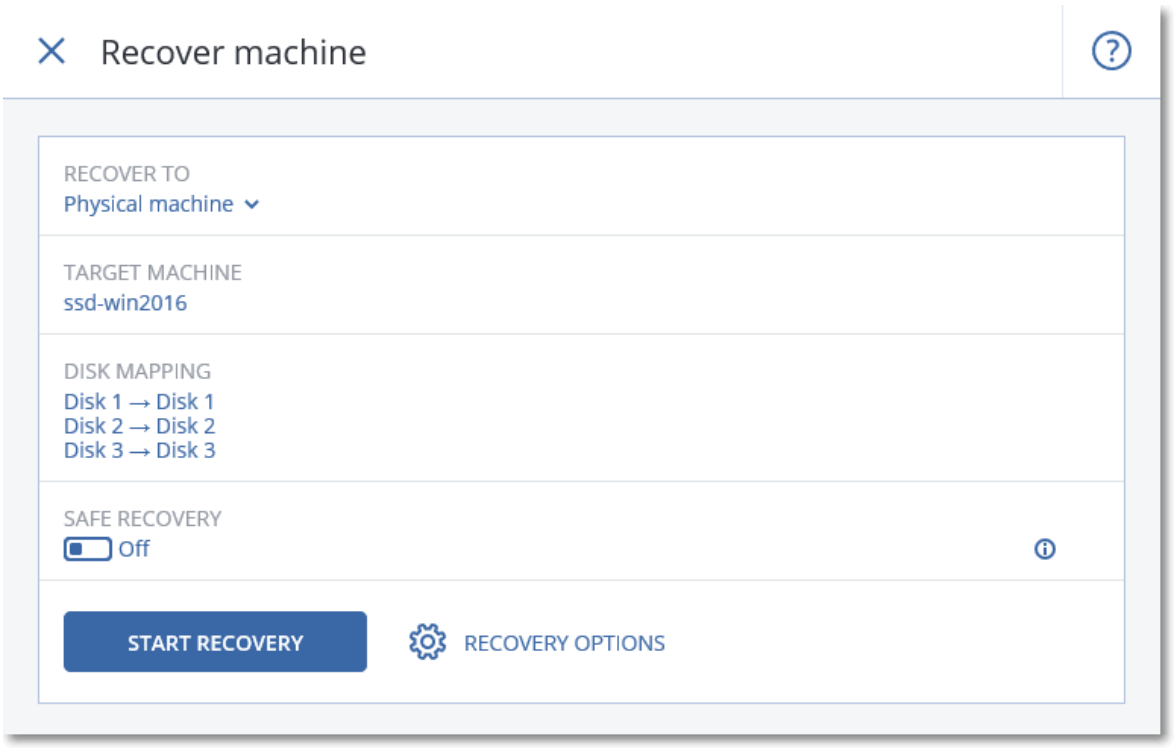
암호화된 시스템 볼륨을 복구할 때는 추가 작업을 수행할 필요가 없습니다. 암호화된 비시스템 볼륨을 복구하려면 먼저 해당 볼륨에 있는 파일을 여는 등의 방식으로 볼륨을 잠가야 합니다. 이렇게 하지 않으면 머신을 다시 시작하지 않고 복구가 계속 진행되므로 Windows에서 복구된 볼륨을 인식하지 못할 수도 있습니다.

참고
복구가 실패하고 머신이 다시 시작된 후 파티션에서 파일을 가져올 수 없음 오류가 발생하면 보안 부팅을 비활성화해 보십시오. 이 작업을 수행하는 방법을 자세히 알아보려면 Microsoft 설명서에서 보안 부팅 비활성화를 참조하십시오.

실제 머신을 복구하려면

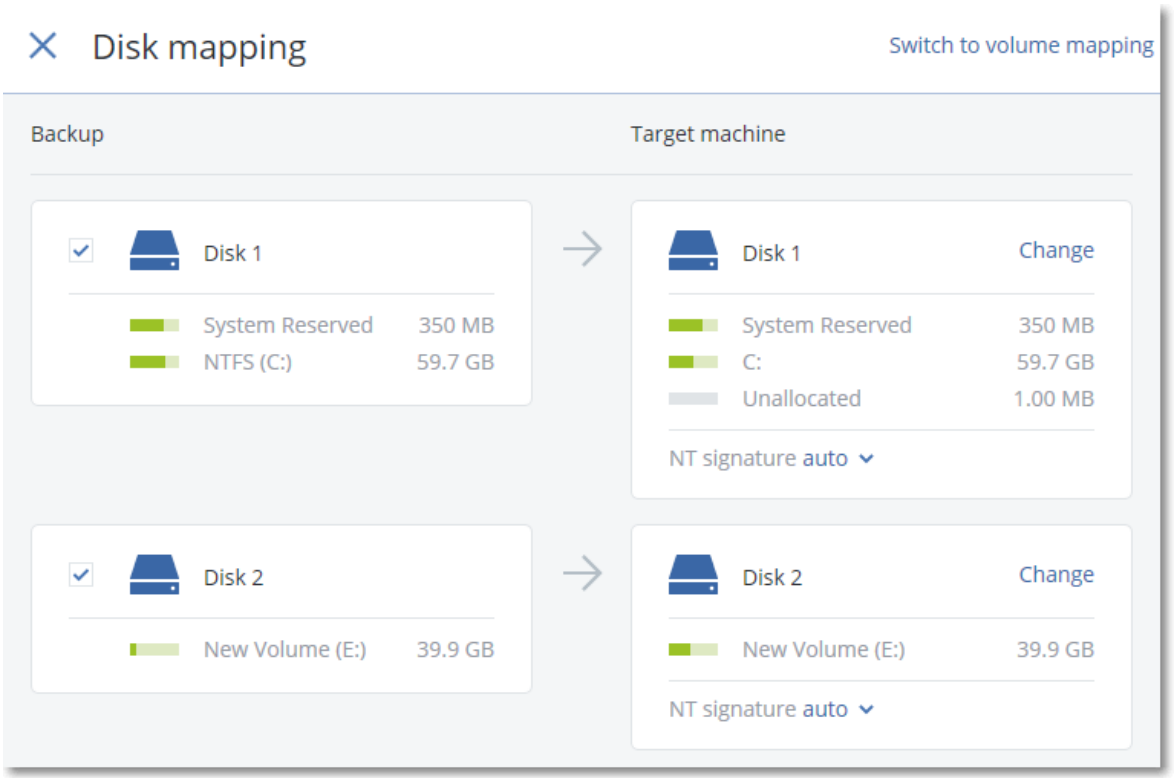
1. 백업된 머신을 선택합니다.
2. **복구**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.
   머신이 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 중 하나를 수행하십시오.
   - 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 온라인 상태인 대상 머신을 선택한 다음 복구 지점을 선택합니다.
   - 백업 스토리지 탭에서 복구 지점을 선택합니다.
   - "부트 가능한 미디어를 사용하여 디스크 복구"에서 설명하는 대로 머신을 복구합니다.
4. **복구 > 전체 머신**을 클릭합니다.
   소프트웨어가 디스크를 백업에서 대상 머신의 디스크로 자동으로 매핑합니다.
   다른 실제 머신으로 복구하려면 **대상 머신**을 클릭한 다음 온라인 상태인 대상 머신을 선택합니다.

© Acronis International GmbH, 2003-2024



5. 매핑 결과가 만족스럽지 않거나 디스크 매핑이 실패할 경우 **볼륨 매핑**을 클릭하여 디스크를 수동으로 다시 매핑합니다.

   매핑 섹션을 사용하여 복구용 개별 디스크 또는 볼륨을 선택할 수도 있습니다. 오른쪽 위에 있는 **전환...** 링크를 사용하여 디스크 복구와 볼륨 복구 간에 전환할 수 있습니다.



© Acronis International GmbH, 2003-2024

6. [보호 에이전트가 설치된 Windows 머신에서만 사용 가능] 맬웨어가 없는 데이터만 복구되도록 하려면 **안전 복구** 스위치를 활성화하십시오. 안전 복구의 작동 방식에 대한 자세한 내용은 "안전 복구"(453페이지) 항목을 참조하십시오.
7. **복구 시작**을 클릭합니다.
8. 백업된 버전으로 디스크를 덮어 쓰려는지 확인합니다. 머신을 자동으로 다시 시작할지 여부를 선택합니다.

복구 진행률이 **작업** 탭에 표시됩니다.

실제 머신에서 가상 머신으로

지원되는 하이퍼바이저 중 하나에서 실제 머신을 가상 머신으로 복구할 수 있습니다. 이 메커니즘을 통해 실제 머신을 가상 머신으로 마이그레이션할 수도 있습니다. 지원되는 P2V 마이그레이션 경로 관련 추가 정보는 "머신 마이그레이션"을 참조하십시오.

이 섹션에서는 웹 인터페이스를 사용해 실제 머신을 가상 머신으로 복구하는 방법을 설명합니다. Acronis 관리 서버에 관련 하이퍼바이저용 에이전트가 하나 이상 설치 및 등록되어 있으면 이 작업을 수행할 수 있습니다. 예를 들어 VMware ESXi로 복구하려면 Agent for VMware 하나 이상이, Hyper-V로 복구하려면 Agent for Hyper-V 하나 이상이 환경에 설치 및 등록되어 있어야 합니다.

규제 준수 모드의 테넌트에서는 웹 인터페이스를 통한 복구 기능을 사용할 수 없습니다.

참고

Hyper-V는 macOS를 지원하지 않으므로 macOS 가상 머신을 Hyper-V 호스트에 복구할 수 없습니다. macOS 가상 머신은 Mac 하드웨어에 설치된 VMware 호스트에 복구할 수 있습니다.

또한 macOS 실제 머신 백업은 가상 머신으로 복구할 수 없습니다.

실제 머신을 가상 머신처럼 복구하려면

1. 백업된 머신을 선택합니다.
2. **복구**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.

   머신이 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 중 하나를 수행하십시오.
   - 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 온라인 상태인 머신을 선택한 다음 복구 지점을 선택합니다.
   - 백업 스토리지 탭에서 복구 지점을 선택합니다.
   - "부트 가능한 미디어를 사용하여 디스크 복구"에서 설명하는 대로 머신을 복구합니다.
4. **복구** > **전체 머신**을 클릭합니다.
5. **복구 대상**에서 **가상 머신**을 선택합니다.
6. **대상 머신**을 클릭합니다.

© Acronis International GmbH, 2003-2024

a. 하이퍼바이저를 선택합니다.

참고
Acronis 관리 서버에 해당 하이퍼바이저용 에이전트가 하나 이상 설치 및 등록되어 있어야 합니다.

b. 새 머신 또는 기존 머신으로 복구할지 선택합니다. 대상 머신의 디스크 구성이 백업의 디스크 구성과 정확하게 일치할 필요가 없기 때문에 새 머신 옵션을 사용하는 것이 좋습니다.
c. 호스트를 선택하고 새 머신 이름을 지정하거나 기존 대상 머신을 선택합니다.
d. **확인**을 클릭합니다.

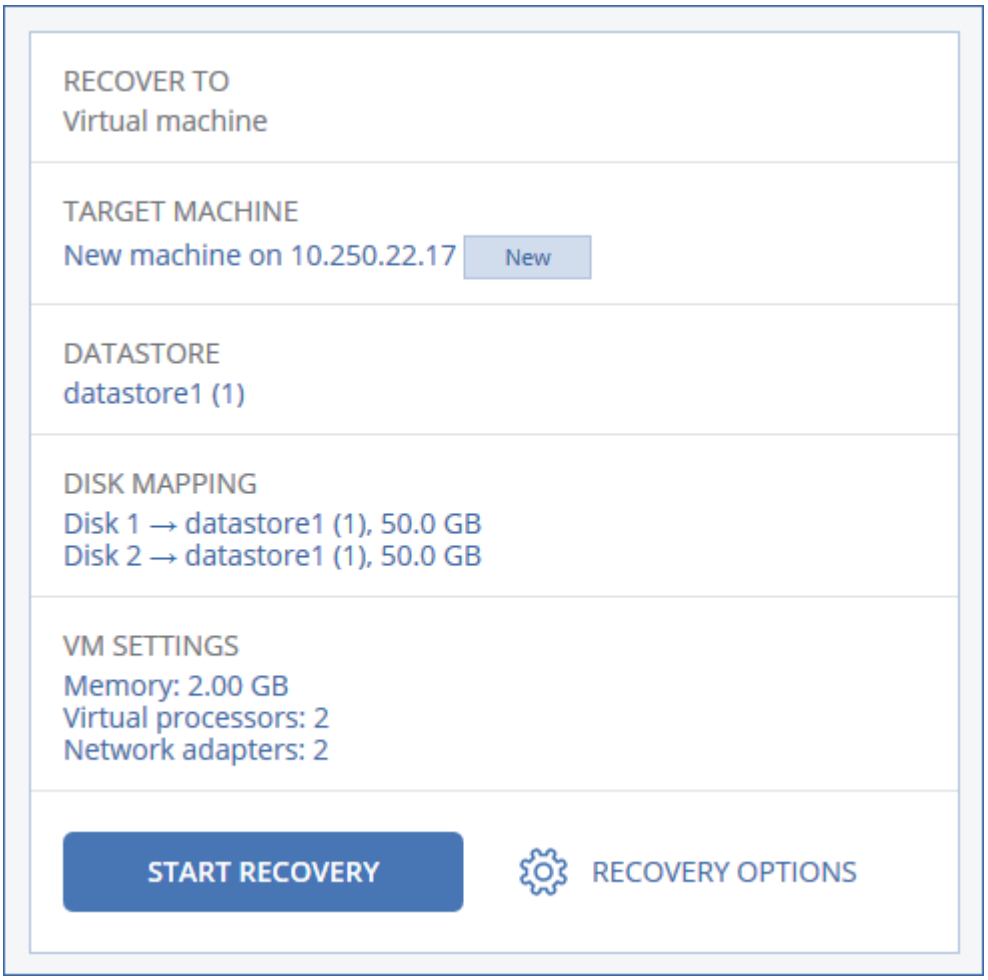
7. [Virtuozzo Hybrid Infrastructure의 경우] **VM 설정**을 클릭하여 **선호 방식**을 선택합니다. 필요한 경우 가상 머신의 메모리 크기, 프로세서 수 및 네트워크 연결을 변경할 수 있습니다.

참고
Virtuozzo Hybrid Infrastructure에서 선호 방식 선택은 필수 단계입니다.

8. [선택 사항] 추가 복구 옵션을 구성합니다.
   - [Virtuozzo Hybrid Infrastructure에서는 사용 불가] ESXi의 경우 **데이터 저장소**를, Hyper-V의 경우 **경로**를 클릭한 다음 가상 머신의 데이터 저장소(스토리지)를 선택합니다.
   - **디스크 매핑**을 클릭하여 각 가상 디스크에 대한 데이터 저장소(스토리지), 인터페이스, 프로비저닝 모드를 선택합니다. 매핑 섹션을 사용하여 복구용 개별 디스크를 선택할 수도 있습니다.

     Virtuozzo Hybrid Infrastructure의 경우, 대상 디스크의 스토리지 정책만 선택할 수 있습니다. 이 작업을 수행하려면 대상 디스크를 선택하고 변경을 클릭합니다. 날개가 열리면 기어 아이콘을 클릭하고 완료를 클릭합니다.
   - [VMware ESXi, Hyper-V 및 Red Hat Virtualization/oVirt의 경우] **VM 설정**을 클릭해 가상 머신의 메모리 크기, 프로세서 수 및 네트워크 연결을 변경합니다.

© Acronis International GmbH, 2003-2024



9. [보호 에이전트가 설치된 Windows 머신에서만 사용 가능] 맬웨어가 없는 데이터만 복구되도록 하려면 **안전 복구** 스위치를 활성화하십시오. 안전 복구의 작동 방식에 대한 자세한 내용은 "안전 복구"(453페이지) 항목을 참조하십시오.
10. **복구 시작**을 클릭합니다.
11. 기존 가상 머신으로 복구하는 경우 디스크를 덮어쓸지 확인합니다.

복구 진행률이 **작업** 탭에 표시됩니다.

가상 머신 복구

가상 머신을 백업에서 복구할 수 있습니다.

참고
규제 준수 모드 상태인 테넌트의 경우에는 Cyber Protect 콘솔에서 백업을 복구할 수 없습니다. 이러한 백업을 복구하는 방법에 대한 자세한 내용은 "규제 준수 모드로 설정된 테넌트의 백업 복구"(983페이지) 항목을 참조하십시오.

사전 요구 사항

- 이 머신으로 복구 중에는 가상 머신을 중지해야 합니다. 기본적으로 소프트웨어는 메시지를 표시하지 않고 머신을 중지합니다. 복구가 완료되면 머신을 수동으로 시작해야 합니다. VM 전원

© Acronis International GmbH, 2003-2024

관리 복구 옵션(**복구 옵션** > **VM 전원 관리** 클릭)을 사용하여 기본 동작을 변경할 수 있습니다.

절차

1. 다음 중 하나를 수행하십시오.
   - 백업된 머신을 선택하고 **복구**를 클릭한 다음 복구 지점을 선택합니다.
   - 백업 스토리지 탭에서 복구 지점을 선택합니다.
2. **복구** > **전체 머신**을 클릭합니다.
3. 실제 머신으로 복구하려면 **복구 대상**에서 **실제 머신**을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.

   대상 머신의 디스크 구성이 백업의 디스크 구성과 정확하게 일치하는 경우에만 실제 머신으로 복구가 가능합니다.

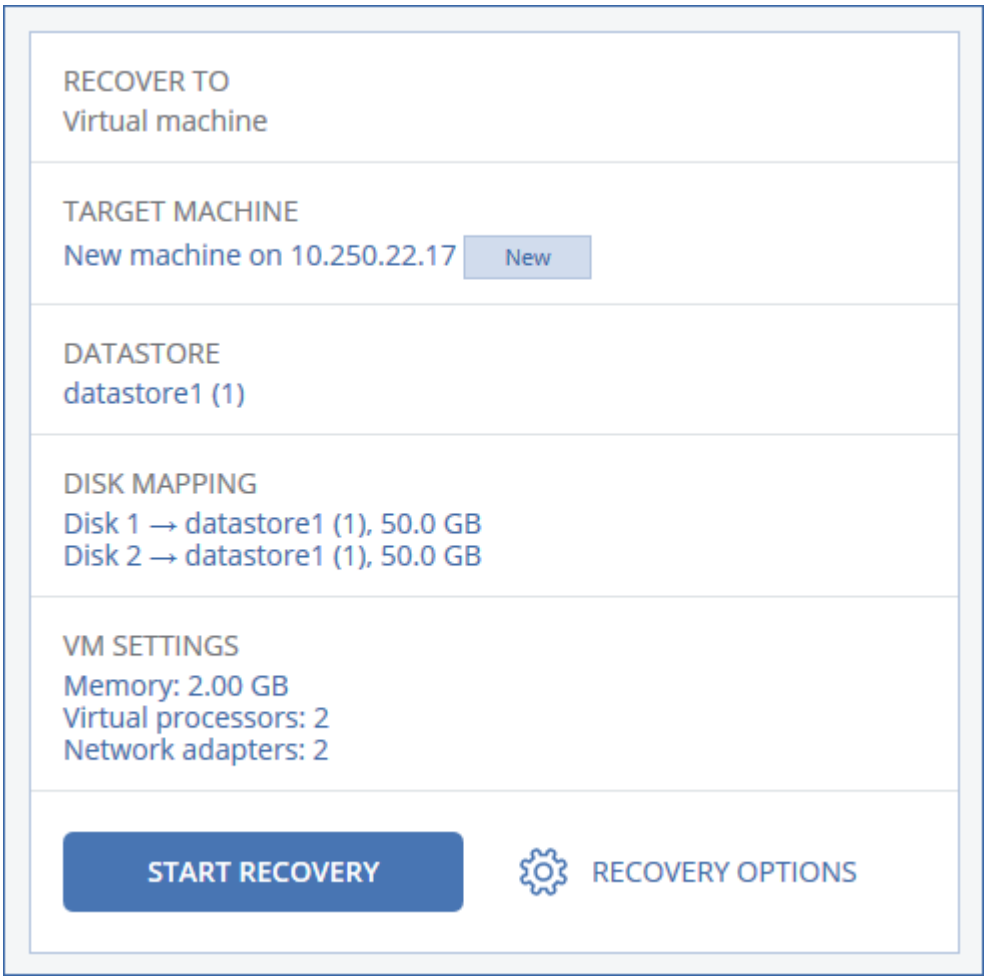
   이 경우 "실제 머신"의 4단계로 계속 진행합니다. 그렇지 않은 경우에는 부트 가능한 미디어 사용으로 V2P 마이그레이션을 수행하는 것이 좋습니다.
4. [선택 사항] 기본적으로 원래 머신이 대상 머신으로 자동으로 선택됩니다. 다른 가상 머신으로 복구하려면 **대상 머신**을 클릭한 후 다음을 수행합니다.
   a. 하이퍼바이저(**VMware ESXi**, **Hyper-V**, **Virtuozzo**, **Virtuozzo Hybrid Infrastructure**, **Scale Computing HC3** 또는 **oVirt**)를 선택합니다.

      Virtuozzo 가상 머신만 Virtuozzo로 복구할 수 있습니다. V2V 이주에 대한 자세한 내용은 "머신 이주"를 참조하십시오.
   b. 새 머신 또는 기존 머신으로 복구할지 선택합니다.
   c. 호스트를 선택하고 새 머신 이름을 지정하거나 기존 대상 머신을 선택합니다.
   d. **확인**을 클릭합니다.
5. 필요한 추가 복구 옵션을 설정합니다.
   - [선택 사항] [Virtuozzo Hybrid Infrastructure 및 Scale Computing HC3에서는 사용 불가] 가상 머신의 데이터 저장소를 선택하려면, ESXi의 경우 **데이터 저장소**를, Hyper-V 및 Virtuozzo의 경우 **경로**를, Red Hat Virtualization(oVirt)의 경우에는 **스토리지 도메인**을 클릭한 다음 가상 머신의 데이터 저장소(스토리지)를 선택합니다.
   - [선택 사항] 각 가상 디스크에 대한 데이터 저장소(스토리지), 인터페이스, 프로비저닝 모드를 보려면 **디스크 매핑**을 클릭합니다. Virtuozzo 컨테이너 또는 Virtuozzo Hybrid Infrastructure 가상 머신을 복구하는 것이 아닌 한 이 설정을 변경할 수 있습니다.

     Virtuozzo Hybrid Infrastructure의 경우, 대상 디스크의 스토리지 정책만 선택할 수 있습니다. 이 작업을 수행하려면 대상 디스크를 선택하고 **변경**을 클릭합니다. 날개가 열리면 기어 아이콘을 클릭하고 **완료**를 클릭합니다.

     매핑 섹션을 사용하여 복구용 개별 디스크를 선택할 수도 있습니다.
   - [선택 사항] [VMware ESXi, Hyper-V, Virtuozzo에 사용 가능] 가상 머신의 메모리 크기, 프로세서 수 및 네트워크 연결을 변경하려면 **VM 설정**을 클릭합니다.
   - [Virtuozzo Hybrid Infrastructure의 경우] 가상 머신의 메모리 크기 및 프로세서 수를 변경하려면 **선호 방식**을 선택합니다.

© Acronis International GmbH, 2003-2024



6. [보호 에이전트가 설치된 Windows 머신에서만 사용 가능] 맬웨어가 없는 데이터만 복구되도록 하려면 **안전 복구** 스위치를 활성화하십시오. 안전 복구의 작동 방식에 대한 자세한 내용은 "안전 복구"(453페이지) 항목을 참조하십시오.
7. **복구 시작**을 클릭합니다.
8. 기존 가상 머신으로 복구하는 경우 디스크를 덮어쓸지 확인합니다.

복구 진행률이 **작업** 탭에 표시됩니다.

부트 가능한 미디어를 사용하여 디스크 복구

부트 가능한 미디어를 생성하는 방법에 대한 자세한 내용은 "실제 부트 가능한 미디어 생성"(645페이지)을(를) 참조하십시오.

참고

Intel 기반 Mac의 디스크 수준 백업을 Apple 실리콘 프로세서를 사용하는 Mac에 복구할 수는 없으며, 그 반대 방향의 복구도 불가능합니다. 파일과 폴더를 복구할 수 있습니다.

부트 가능한 미디어를 사용하여 디스크를 복구하려면

1. 부트 가능한 미디어를 사용하여 대상 머신을 부트합니다.
2. [Mac 복구 시에만 해당] APFS 형식 디스크/볼륨을 원본 이외 머신 또는 베어 메탈로 복구하는 경우 원본 디스크 구성을 수동으로 재생성하십시오.

© Acronis International GmbH, 2003-2024

a. **디스크 유틸리티**를 클릭합니다.
b. 대상 디스크를 지우고 APFS로 포맷하십시오. 자세한 내용은 https://support.apple.com/en-us/HT208496#erasedisk를 참조하십시오.
c. 원본 디스크 구성을 재생성합니다. 자세한 내용은 https://support.apple.com/guide/disk-utility/add-erase-or-delete-apfs-volumes-dskua9e6a110/19.0/mac/10.15를 참조하십시오.
d. **디스크 유틸리티** > **디스크 유틸리티 종료**를 클릭합니다.

3. 사용 중인 미디어 유형에 따라 **이 머신을 로컬로 관리**를 클릭하거나 **부트 가능한 미디어 복구**를 두 번 클릭합니다.
4. 네트워크에서 프록시 서버가 사용하도록 설정되어 있는 경우 **도구** > **프록시 서버**를 클릭한 다음 프록시 서버 호스트 이름/IP 주소, 포트 및 자격 증명을 지정합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
5. [선택 사항] Windows나 Linux를 복구할 때는 **도구** > **Cyber Protection 서비스에서 미디어 등록**을 클릭한 후 미디어를 다운로드할 때 획득한 등록 토큰을 지정합니다. 이를 수행할 경우에는 8단계에서 설명하는 클라우드 스토리지에 액세스하기 위해 자격 증명이나 등록 코드를 입력하지 않아도 됩니다.
6. 시작 화면에서 **복구**를 클릭합니다.
7. **데이터 선택**을 클릭한 다음 **찾아보기**를 클릭합니다.
8. 백업 위치 지정:
   - 클라우드 스토리지에서 복구하려면 **클라우드 스토리지**를 선택합니다. 백업된 머신이 할당된 계정의 자격 증명을 입력합니다.

     Windows나 Linux를 복구할 때 등록 코드를 요청하여 자격 증명 대신에 사용할 수 있습니다. **등록 코드 사용** > **코드 요청**을 클릭합니다. 소프트웨어에 등록 링크와 등록 코드가 표시됩니다. 이를 복사하고 다른 머신에서 등록 절차를 수행할 수 있습니다. 등록 코드는 1시간 동안 유효합니다.
   - 로컬 또는 네트워크 폴더에서 복구하려면 **로컬 폴더** 또는 **네트워크 폴더**에서 폴더를 찾습니다.
   - Microsoft Azure, Amazon S3, Wasabi 또는 S3 호환 스토리지와 같은 퍼블릭 클라우드 스토리지의 백업 위치에서 백업을 복구하려는 경우 먼저 **Cyber Protection 서비스에 미디어 등록**을 클릭하고 웹 인터페이스를 사용하여 복구를 구성합니다. 웹 인터페이스를 통해 원격으로 미디어를 관리하는 방법에 대한 자세한 내용은 "부트 가능한 미디어를 사용한 원격 작업" (660페이지) 항목을 참조하십시오.

   확인을 클릭하여 선택 항목을 확인합니다.
9. 데이터를 복구하려는 백업을 선택합니다. 메시지가 표시되면 백업의 비밀번호를 입력합니다.
10. **백업 내용**에서 복구하려는 디스크를 선택합니다. **확인**을 클릭하여 선택 항목을 확인합니다.
11. **복구 위치**에서 선택한 디스크가 대상 디스크로 자동으로 매핑됩니다.

    매칭에 실패하거나 매핑 결과가 만족스럽지 않은 경우 디스크를 수동으로 다시 매핑할 수 있습니다.

© Acronis International GmbH, 2003-2024

참고
디스크 레이아웃을 변경하면 운영 체제 부트 가능성에 영향을 줄 수 있습니다. 확신이 없는 경우 원래 머신의 디스크 레이아웃을 사용하십시오.

12. [Linux 복구 시] 백업한 머신에 LVM(논리 볼륨)이 있고 원래 LVM 구조를 재현하려는 경우:
    a. 대상 머신 디스크의 수 및 각 디스크 용량이 원래 머신의 디스크 수 및 디스크 용량과 일치하거나 초과하는지 확인한 다음 **RAID/LVM 적용**을 클릭합니다.
    b. 볼륨 구조를 검토하고 **RAID/LVM 적용**을 클릭하여 볼륨을 생성합니다.
13. [선택 사항] 추가 설정을 지정하려면 **복구 옵션**을 클릭합니다.
14. **확인**을 클릭하여 복구를 시작합니다.

Universal Restore 사용

최신 운영 체제는 VMware 또는 Hyper-V 플랫폼을 포함한 이기종 하드웨어로 복구했을 때에도 부트 가능한 상태로 유지됩니다. 복구한 운영 체제가 부트되지 않는 경우 Universal Restore 도구를 사용해 운영 체제 시작에 핵심적인 드라이버와 모듈을 업데이트하십시오.

Universal Restore는 Windows 및 Linux에 적용할 수 있습니다.

Universal Restore를 적용하려면

1. 부트 가능한 미디어에서 머신을 부트합니다.
2. **Universal Restore 적용**을 클릭합니다.
3. 머신에 여러 운영 체제가 있는 경우 Universal Restore를 적용할 운영 체제를 선택합니다.
4. [Windows에만 해당] 추가 설정을 구성합니다.
5. **확인**을 클릭합니다.

Windows의 Universal Restore

준비

드라이버 준비

Universal Restore를 Windows 운영 체제에 적용하기 전에 새로운 HDD 컨트롤러 및 칩셋용 드라이버를 보유하고 있는지 확인하십시오. 이 드라이버는 운영 체제를 시작하는 데 필수적입니다. 하드웨어 공급업체가 제공한 CD 또는 DVD를 사용하거나 공급업체의 웹 사이트에서 드라이버를 다운로드하십시오. 드라이버 파일의 확장자가 *.inf여야 합니다. *.exe, *.cab 또는 *.zip 포맷 드라이버를 다운로드한 경우 서드 파티 애플리케이션을 사용해 추출하십시오.

가장 좋은 방법은 조직에서 사용하는 모든 하드웨어의 드라이버를 장치 유형이나 하드웨어 구성별로 분류한 단일 리포지토리에 저장하는 것입니다. 해당 리포지토리 사본을 DVD 또는 플래시 드라이브에 보관해두면 일부 드라이버를 골라 부트 가능한 미디어에 추가하고, 각 서버에 필요한 드라이버(그리고 필요한 네트워크 구성)로 사용자 지정 부트 가능한 미디어를 생성할 수 있습니다. 아니면 그냥 Universal Restore를 사용할 때마다 해당 리포지토리 경로를 지정해주면 됩니다.

© Acronis International GmbH, 2003-2024

부트 가능한 환경에서 드라이버에 대한 액세스 확인

부트 가능한 미디어에서 작업할 때 해당 드라이버를 포함한 장치에 액세스할 수 있어야 합니다. 장치를 Windows에서는 사용할 수 있지만 Linux 기반 미디어는 이를 감지할 수 없다면 WinPE 기반 미디어를 사용합니다.

Universal Restore 설정

자동 드라이버 검색

다음과 같이 HAL(Hardware Abstraction Layer), HDD 컨트롤러 드라이버 및 네트워크 어댑터 드라이버를 검색할 위치를 지정합니다.

- 드라이버가 공급업체 디스크 또는 다른 이동식 미디어에 있는 경우에는 **이동식 미디어 검색**을 켭니다.
- 드라이버가 네트워크 폴더 또는 부트 가능한 미디어에 있는 경우에는 **폴더 추가**를 클릭하여 폴더의 경로를 지정합니다.

또한, Universal Restore는 Windows 기본 드라이버 저장 폴더를 검색합니다. 그 위치는 레지스트리 값 **DevicePath**에서 정해집니다. 이 값은 레지스트리 키 **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion**에서 찾을 수 있습니다. 이 저장 폴더는 대개 WINDOWS/inf입니다.

Universal Restore는 지정한 폴더의 모든 하위 폴더에서 재귀 검색을 수행하여, 사용 가능한 모든 드라이버 중에서 가장 적합한 HAL 및 HDD 컨트롤러 드라이버를 찾아 시스템에 설치합니다. Universal Restore는 또한 네트워크 어댑터 드라이버를 검색합니다. 그다음 Universal Restore는 검색한 드라이버의 경로를 운영 체제로 전송합니다. 하드웨어에 네트워크 인터페이스 카드가 여러 개라면 Universal Restore는 모든 카드의 드라이버를 구성하려고 시도합니다.

설치할 대용량 스토리지 드라이버

다음의 경우 이 설정이 필요합니다.

- 하드웨어에 RAID(특히, NVIDIA RAID) 또는 파이버 채널 어댑터와 같은 특정 대용량 스토리지 컨트롤러가 있는 경우.
- SCSI 하드 드라이브 컨트롤러를 사용하는 가상 머신으로 시스템을 마이그레이션한 경우. 가상화 소프트웨어와 함께 묶여진 SCSI 드라이버들을 사용하거나 소프트웨어 제조사 웹 사이트에서 최신 드라이버 버전을 다운로드합니다.
- 자동 드라이버 검색으로 시스템을 부팅할 수 없는 경우.

드라이버 추가를 클릭하여 적절한 드라이버를 지정합니다. 여기에서 정의된 드라이버는 프로그램이 보다 적합한 드라이버를 찾아도 해당 경고와 함께 설치됩니다.

Universal Restore 프로세스

필수 설정을 지정한 후 **확인**을 클릭합니다.

© Acronis International GmbH, 2003-2024

Universal Restore가 지정한 위치에서 호환 가능한 드라이버를 찾지 못하는 경우 문제 장치에 관한 프롬프트가 표시됩니다. 다음 중 하나를 수행하십시오.

- 이전에 지정한 위치에 드라이버를 추가하고 **재시도**를 클릭합니다.
- 위치가 기억나지 않으면 **무시**를 클릭하고 프로세스를 계속 진행합니다. 결과가 만족스럽지 않다면 Universal Restore를 재적용합니다. 작업을 구성할 때 필요한 드라이버를 지정합니다.

Windows는 부팅되고 나면 새 하드웨어 설치를 위한 표준 절차를 시작합니다. 드라이버에 Microsoft Windows 서명이 있으면 네트워크 어댑터 드라이버가 자동으로 설치됩니다. 그렇지 않으면 Windows가 서명 없는 드라이버를 설치할지 확인을 요청합니다.

설치 후 네트워크 연결을 구성하고, 비디오 어댑터, USB 및 기타 장치에 대해 드라이버를 지정할 수 있습니다.

Linux의 Universal Restore

Universal Restore는 커널 버전이 2.6.8 이상인 Linux 운영 체제에 적용할 수 있습니다.

Universal Restore가 Linux 운영 체제에 적용되면 초기 RAM 디스크(initrd)라고 하는 임시 파일 시스템을 업데이트합니다. 이를 통해 새 하드웨어에서 운영 체제를 부팅할 수 있습니다.

Universal Restore는 새 하드웨어(장치 드라이버 포함)의 모듈을 초기 RAM 디스크에 추가합니다. 일반적으로 **/lib/modules** 디렉토리에서 필요한 모듈을 찾습니다. Universal Restore가 필요한 모듈을 찾지 못하면 모듈의 파일 이름을 로그에 기록합니다.

Universal Restore는 GRUB 부트 로더의 구성을 수정할 수 있습니다. 이러한 기능은 예를 들어, 새 머신의 볼륨 레이아웃이 원래 머신과 다른 경우 머신 부트 가능성을 확보하는 데 필요합니다.

Universal Restore는 Linux 커널은 수정하지 않습니다.

원본 초기 RAM 디스크로 되돌리기

필요한 경우 원본 초기 RAM 디스크로 되돌릴 수 있습니다.

초기 RAM 디스크는 머신에 파일로 저장됩니다. 초기 RAM 디스크를 처음 업데이트하기 전에 Universal Restore는 디스크의 사본을 동일한 디렉토리에 저장합니다. 사본의 이름은 파일 이름 뒤에 접미사 **_acronis_backup.img**가 추가됩니다. Universal Restore를 여러 번 실행해도 이 사본은 덮어쓰지 않습니다(예를 들어, 누락된 드라이버를 추가한 후).

원본 초기 RAM 디스크로 되돌리려면 다음 중 아무것이나 수행하십시오.

- 사본의 이름을 그에 따라 변경합니다. 예를 들어, 다음과 유사한 명령을 실행합니다.

  ```
  mv initrd-2.6.16.60-0.21-default_acronis_backup.img initrd-2.6.16.60-0.21-default
  ```

- GRUB 부트 로더 구성의 **initrd** 행에 사본을 지정합니다.

© Acronis International GmbH, 2003-2024

파일 복구

Cyber Protect 콘솔에서 파일 복구

참고
규제 준수 모드 상태인 테넌트의 경우에는 Cyber Protect 콘솔에서 백업을 복구할 수 없습니다. 이러한 백업을 복구하는 방법에 대한 자세한 내용은 "규제 준수 모드로 설정된 테넌트의 백업 복구"(983페이지) 항목을 참조하십시오.

1. 복구하려는 데이터가 원래 포함되어 있는 머신을 선택합니다.
2. **복구**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.
   선택한 머신이 실제 머신인데 오프라인 상태인 경우 복구 지점이 표시되지 않습니다. 다음 중 하나를 수행하십시오.
   - [권장 사항] 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 온라인 상태인 대상 머신을 선택한 다음 복구 지점을 선택합니다.
   - 백업 스토리지 탭에서 복구 지점을 선택합니다.
   - 클라우드 스토리지에서 파일을 다운로드합니다.
   - 부트 가능한 미디어를 사용합니다.
4. **복구** > **파일/폴더**를 클릭합니다.
5. 필요한 폴더를 찾거나 검색 창을 사용하여 필요한 파일 및 폴더 목록을 얻습니다.
   검색 결과는 언어와 관계없이 동일합니다.
   하나 이상의 와일드 카드 문자(* 및 ?)를 사용할 수 있습니다.와일드카드 사용에 관한 자세한 내용은 "마스크"(421페이지) 항목을 참조하십시오.

   참고
   클라우드 스토리지에 저장된 디스크 수준 백업은 검색할 수 없습니다.

6. 복구할 파일을 선택합니다.
7. 파일을 .zip 파일로 저장하려면 **다운로드**를 클릭하고 데이터를 저장할 위치를 선택한 다음 **저장**을 클릭합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
   선택 항목에 폴더가 포함되어 있거나 선택한 파일의 총 크기가 100MB를 초과하는 경우 다운로드할 수 없습니다. 클라우드에서 더 큰 용량의 데이터를 검색하려면 "클라우드 스토리지에서 파일 다운로드"(467페이지) 절차를 따르십시오.
8. **복구**를 클릭합니다.
   복구 대상에서 복구 작업의 대상을 클릭하여 선택하거나 기본 대상을 선택된 상태로 유지합니다. 기본 대상은 백업의 소스에 따라 달라집니다.
   사용 가능한 대상은 다음과 같습니다.
   - 원본 머신(보호 에이전트가 설치되어 있는 경우).
     복구하려는 파일이 원래 포함되어 있던 머신입니다.

© Acronis International GmbH, 2003-2024

- 보호 에이전트가 설치되어 있는 기타 머신 - 보호 에이전트가 설치된 실제 머신, 가상 머신, 가상화 호스트 또는 가상 어플라이언스.

  보호 에이전트가 설치된 실제 머신, 가상 머신 및 가상화 호스트로 파일을 복구할 수 있습니다. Virtuozzo 가상 머신을 제외하고는 보호 에이전트가 설치되어 있지 않은 가상 머신으로 파일을 복구할 수는 없습니다.
- Virtuozzo 컨테이너 또는 가상 머신.

  Virtuozzo 컨테이너 및 가상 머신으로 파일을 복구할 수 있습니다. 단, 이 경우에는 몇 가지 제한 사항이 적용됩니다. 해당 제한 사항에 대한 자세한 내용은 "Cyber Protect 콘솔에서 파일을 복구할 때 적용되는 제한 사항"(471페이지) 항목을 참조하십시오.

9. **경로**에서 복구 목적지를 선택합니다. 다음 중 하나를 선택합니다.
   - [원래 머신으로 복구하는 경우] 원래 위치.
   - 대상 머신의 로컬 폴더 또는 로컬에 연결된 스토리지.

     참고
     심볼 링크는 지원되지 않습니다.
   - 대상 머신에서 액세스할 수 있는 네트워크 폴더.
10. **복구 시작**을 클릭합니다.
11. 다음 파일 덮어쓰기 옵션 중 하나를 선택합니다.
    - **기존 파일 덮어쓰기**
    - **오래된 경우 기존 파일 덮어쓰기**
    - **기존 파일 덮어쓰기 안 함**

복구 진행률이 **작업** 탭에 표시됩니다.

클라우드 스토리지에서 파일 다운로드

웹 복원 콘솔에서는 클라우드 스토리지를 탐색하고, 백업의 내용을 볼 수 있으며, 백업된 파일 및 폴더를 다운로드 할 수 있습니다.

참고
고객 Cyber Protection 관리자 또는 고객 테넌트 사용자만 Web Restore 콘솔에 액세스할 수 있으며 파트너 수준 사용자 역할은 해당 콘솔에 액세스할 수 없습니다.

제한 사항

- 백업된 디스크, 볼륨 또는 전체 복구 지점을 다운로드할 수 없습니다.
- 디스크 수준 백업 검색 시 LVM, LDM 등의 논리 볼륨은 표시되지 않습니다.
- 시스템 상태, SQL 데이터베이스, 그리고 Exchange 데이터베이스의 백업을 탐색할 수 없습니다.

클라우드 스토리지에서 파일과 폴더를 다운로드하는 방법

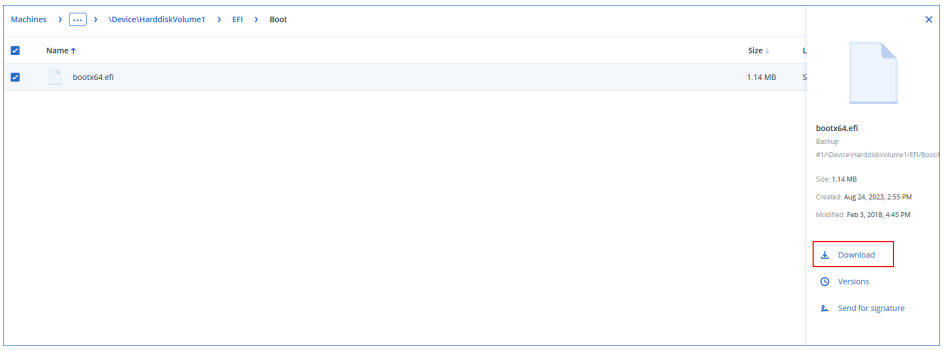
1. Cyber Protection 콘솔에서 필요한 워크로드를 선택한 다음 **복구**를 클릭합니다.
2. [여러 백업 위치가 사용 가능한 경우] 백업 위치를 선택한 다음 **더 많은 복구 방법**을 클릭합니다.
3. **파일 다운로드**를 클릭합니다.

© Acronis International GmbH, 2003-2024

4. **머신**에서 워크로드 이름을 클릭한 다음 백업 아카이브를 클릭합니다.
   백업 아카이브에는 하나 이상의 백업(복구 지점)이 포함되어 있습니다.
5. 파일이나 폴더를 다운로드하려는 백업 번호(복구 지점)를 클릭한 다음 필요한 항목으로 이동합니다.
6. 다운로드하려는 항목 옆의 확인란을 선택합니다.

참고
여러 항목을 선택하는 경우 ZIP 파일로 다운로드됩니다.

7. **다운로드**를 클릭합니다.



Notary Service를 통해 파일 신뢰성 확인

백업 중에 공증이 활성화된 경우 백업된 파일의 신뢰성을 확인할 수 있습니다.

파일 신뢰성을 확인하려면

1. "웹 인터페이스를 사용하여 파일 복구" 섹션의 1~6 단계, 또는 "클라우드 스토리지에서 파일 다운로드" 섹션의 1~5 단계에 설명된 대로 파일을 선택합니다.
2. 선택한 파일에 다음 아이콘이 표시되는지 확인합니다. 이는 파일이 공증되었음을 의미합니다.
3. 다음 중 하나를 수행하십시오.
   - **확인**을 클릭합니다.
     소프트웨어에서 파일 신뢰성을 확인하고 결과를 표시합니다.
   - **인증서 가져오기**를 클릭합니다.
     파일 공증을 확인하는 인증서가 웹 브라우저 창에서 열립니다. 이 창에는 파일 신뢰성을 수동으로 확인하는 방법도 포함되어 있습니다.

ASign으로 파일에 서명

참고
이 기능은 Advanced Backup 팩에서 사용할 수 있습니다.

ASign은 여러 사용자가 백업된 파일에 전자적으로 서명할 수 있도록 하는 서비스입니다. 이 기능은 클라우드 스토리지에 저장된 파일 수준 백업에만 사용할 수 있습니다.

© Acronis International GmbH, 2003-2024

한 번에 하나의 파일 버전에만 서명할 수 있습니다. 파일이 여러 번 백업된 경우 서명할 버전을 선택해야 하고 이 버전에만 서명이 포함됩니다.

예를 들어 다음 파일의 전자 서명에 ASign을 사용할 수 있습니다.

- 대여 또는 임대 계약
- 판매 계약
- 자산 구매 계약
- 대출 계약
- 허가서
- 금융 문서
- 보험 문서
- 책임 포기 각서
- 의료 문서
- 연구 논문
- 제품 정품 인증서
- 비공개 계약
- 제안 문서
- 기밀 유지 계약
- 독립 계약자 계약

파일 버전에 서명하려면

1. "웹 인터페이스를 사용하여 파일 복구" 섹션의 1~6 단계, 또는 "클라우드 스토리지에서 파일 다운로드" 섹션의 1~5 단계에 설명된 대로 파일을 선택합니다.
2. 왼쪽 패널에서 올바른 날짜 및 시간이 선택되었는지 확인합니다.
3. **이 파일 버전에 서명**을 클릭합니다.
4. 백업이 저장된 클라우드 스토리지 계정에 대한 비밀번호를 지정합니다. 프롬프트 창에 계정의 로그인이 표시됩니다.

   ASign 서비스 인터페이스가 웹 브라우저 창에서 열립니다.
5. 이메일 주소를 지정하여 다른 서명인을 추가합니다. 초대를 보낸 후에는 서명인을 추가하거나 제거할 수 없으므로 서명이 필요한 모든 사람이 목록에 포함되었는지 확인하십시오.
6. **서명 초대**를 클릭하여 서명인에게 초대를 보냅니다.

   각 서명인은 서명 요청이 포함된 이메일 메시지를 받습니다. 요청된 모든 서명인이 파일에 서명하면 공증 서비스를 통해 공증되고 서명됩니다.

   각 서명인이 파일에 서명하고 전체 프로세스가 완료되면 알림을 받게 됩니다. 수신한 모든 이메일 메시지에서 **세부정보 보기**를 클릭하여 ASign 웹 페이지에 액세스할 수 있습니다.
7. 프로세스가 완료되면 ASign 웹 페이지로 이동하고 **문서 가져오기**를 클릭하여 다음이 포함된 .pdf 문서를 다운로드하십시오.
   - 수집된 서명이 있는 서명 인증서 페이지.
   - 작업 내역이 있는 감사 추적 페이지: 초대가 서명인에게 전송된 시간, 서명인이 파일에 서명한 시간 등.

© Acronis International GmbH, 2003-2024

부트 가능한 미디어를 사용하여 파일 복구

부트 가능한 미디어를 생성하는 방법에 대한 자세한 내용은 "부트 가능한 미디어 생성"을 참조하십시오.

부트 가능한 미디어를 사용하여 파일을 복구하려면

1. 부트 가능한 미디어를 사용하여 대상 머신을 부트합니다.
2. 사용 중인 미디어 유형에 따라 **이 머신을 로컬로 관리**를 클릭하거나 **부트 가능한 미디어 복구**를 두 번 클릭합니다.
3. 네트워크에서 프록시 서버가 사용하도록 설정되어 있는 경우 **도구** > **프록시 서버**를 클릭한 다음 프록시 서버 호스트 이름/IP 주소, 포트 및 자격 증명을 지정합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
4. [선택 사항] Windows나 Linux를 복구할 때는 **도구** > **Cyber Protection 서비스에서 미디어 등록**을 클릭한 후 미디어를 다운로드할 때 획득한 등록 토큰을 지정합니다. 이를 수행할 경우에는 7단계에서 설명하는 클라우드 스토리지에 액세스하기 위해 자격 증명이나 등록 코드를 입력하지 않아도 됩니다.
5. 시작 화면에서 **복구**를 클릭합니다.
6. **데이터 선택**을 클릭한 다음 **찾아보기**를 클릭합니다.
7. 백업 위치 지정:
   - 클라우드 스토리지에서 복구하려면 **클라우드 스토리지**를 선택합니다. 백업된 머신이 할당된 계정의 자격 증명을 입력합니다.

     Windows나 Linux를 복구할 때 등록 코드를 요청하여 자격 증명 대신에 사용할 수 있습니다. **등록 코드 사용** > **코드 요청**을 클릭합니다. 소프트웨어에 등록 링크와 등록 코드가 표시됩니다. 이를 복사하고 다른 머신에서 등록 절차를 수행할 수 있습니다. 등록 코드는 1시간 동안 유효합니다.
   - 로컬 또는 네트워크 폴더에서 복구하려면 **로컬 폴더** 또는 **네트워크 폴더**에서 폴더를 찾습니다.
   - Microsoft Azure, Amazon S3, Wasabi 또는 S3 호환 스토리지와 같은 퍼블릭 클라우드 스토리지의 백업 위치에서 백업을 복구하려는 경우 먼저 **Cyber Protection 서비스에 미디어 등록**을 클릭하고 웹 인터페이스를 사용하여 복구를 구성합니다. 웹 인터페이스를 통해 원격으로 미디어를 관리하는 방법에 대한 자세한 내용은 "부트 가능한 미디어를 사용한 원격 작업" (660페이지) 항목을 참조하십시오.

   확인을 클릭하여 선택 항목을 확인합니다.
8. 데이터를 복구하려는 백업을 선택합니다. 메시지가 표시되면 백업의 비밀번호를 입력합니다.
9. **백업 내용**에서 **폴더/파일**을 선택합니다.
10. 복구할 데이터를 선택합니다. **확인**을 클릭하여 선택 항목을 확인합니다.
11. **복구 위치**에서 폴더를 지정합니다. 또는 새 버전의 파일 덮어쓰기를 금지하거나 복구에서 일부 파일을 제외할 수 있습니다.
12. [선택 사항] 추가 설정을 지정하려면 **복구 옵션**을 클릭합니다.
13. **확인**을 클릭하여 복구를 시작합니다.

© Acronis International GmbH, 2003-2024

로컬 백업에서 파일 추출

로컬 백업에서 파일 추출백업 내용을 찾아 필요한 파일을 추출할 수 있습니다.

요구 사항

- 이 기능은 파일 탐색기를 사용하여 Windows에서만 이용할 수 있습니다.
- 백업 파일 시스템은 다음 중 하나여야 합니다. FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS 또는 HFS+.

사전 요구 사항

- 백업을 찾아보는 머신에 보호 에이전트가 설치되어 있어야 합니다.
- 백업은 로컬 폴더 또는 네트워크 공유(SMB/CIFS)에 저장해야 합니다.

백업에서 파일을 추출하려면

1. 파일 탐색기를 사용하여 백업 위치를 찾습니다.
2. 백업 파일을 두 번 클릭합니다. 파일 이름은 다음 템플릿에 따라 지정되어 있습니다.
   `<머신 이름> - <보호 계획 GUID>`
3. 백업이 암호화되어 있는 경우 암호화 비밀번호를 입력합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
   파일 탐색기가 복구 지점을 표시합니다.
4. 복구 지점을 두 번 클릭합니다.
   파일 탐색기가 백업된 데이터를 표시합니다.
5. 필요한 폴더를 찾습니다.
6. 필요한 파일을 파일 시스템에 있는 폴더에 복사합니다.

Cyber Protect 콘솔에서 파일을 복구할 때 적용되는 제한 사항

규제 준수 모드의 테넌트

규제 준수 모드 상태인 테넌트의 경우에는 Cyber Protect 콘솔에서 백업을 복구할 수 없습니다. 이러한 백업을 복구하는 방법에 대한 자세한 내용은 "규제 준수 모드로 설정된 테넌트의 백업 복구" (983페이지) 항목을 참조하십시오.

Virtuozzo 컨테이너 또는 Virtuozzo 가상 머신으로 복구

- QEMU 게스트 에이전트는 대상 가상 머신에 설치해야 합니다.
- [컨테이너로 복구할 때만 해당됨] 컨테이너 내의 마운트 포인트를 복구 대상으로 사용할 수 없습니다. 예를 들어 컨테이너에 마운트된 NFS 공유나 두 번째 하드 디스크로 파일을 복구할 수는 없습니다.
- Windows 가상 머신으로 파일을 복구할 때 "파일 수준 보안"(477페이지) 복구 옵션이 활성화되어 있으면 아카이브 비트 속성이 복구된 파일로 설정됩니다.

© Acronis International GmbH, 2003-2024

- Windows Server 2012 이하 버전을 실행 중인 머신과 Windows 7 이하 버전을 실행 중인 머신에서는 이름에 ANSI 문자 외의 문자가 포함된 파일이 잘못된 이름으로 복구됩니다.
- Virtuozzo Hybrid Server에서 실행되는 CentOS 또는 Red Hat Enterprise Linux 가상 머신으로 파일을 복구하려는 경우에는 다음과 같이 qemu-ga 파일을 편집해야 합니다.
  - 대상 가상 머신에서 /etc/sysconfig/로 이동하여 qemu-ga 파일을 편집용으로 엽니다.
  - 다음 줄로 이동한 후 등호(=) 다음의 내용을 모두 삭제합니다.

    ```
    BLACKLIST_RPC=
    ```

  - 다음 명령을 실행하여 QEMU 게스트 에이전트를 다시 시작합니다.

    ```
    systemctl restart qemu-guest-agent
    ```

시스템 상태 복구

참고
규제 준수 모드 상태인 테넌트의 경우에는 Cyber Protect 콘솔에서 백업을 복구할 수 없습니다. 이러한 백업을 복구하는 방법에 대한 자세한 내용은 "규제 준수 모드로 설정된 테넌트의 백업 복구" (983페이지) 항목을 참조하십시오.

1. 시스템 상태를 복구하려는 머신을 선택합니다.
2. **복구**를 클릭합니다.
3. 시스템 상태 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.
4. **시스템 상태 복구**를 클릭합니다.
5. 백업된 버전으로 시스템 상태를 덮어 쓰려는지 확인합니다.

복구 진행률이 **작업** 탭에 표시됩니다.

ESXi 구성 복구

ESXi 구성을 복구하려면 Linux 기반 부트 가능한 미디어가 필요합니다. 부트 가능한 미디어를 생성하는 방법에 대한 자세한 내용은 "실제 부트 가능한 미디어 생성"(645페이지)을(를) 참조하십시오.

ESXi 구성을 원래 호스트가 아닌 호스트로 복구하는 중인데 원래 ESXi 호스트가 여전히 vCenter Server에 연결되어 있는 경우 복구 중 예기치 않은 문제를 방지하려면 이 호스트를 vCenter Server에서 연결 해제하고 제거하십시오. 원래 호스트를 복구된 호스트와 함께 유지하려면 복구가 완료된 후에 원래 호스트를 다시 추가하면 됩니다.

해당 호스트에서 실행 중인 가상 머신은 ESXi 구성 백업에 포함되지 않습니다. 가상 머신은 따로 백업 및 복구할 수 있습니다.

ESXi 구성을 복구하려면

1. 부트 가능한 미디어를 사용하여 대상 머신을 부트합니다.
2. **이 머신을 로컬로 관리**를 클릭합니다.
3. 시작 화면에서 **복구**를 클릭합니다.
4. **데이터 선택**을 클릭한 다음 **찾아보기**를 클릭합니다.

© Acronis International GmbH, 2003-2024

5. 백업 위치 지정:
   - **로컬 폴더** 또는 **네트워크 폴더**에서 폴더를 찾습니다.

   확인을 클릭하여 선택 항목을 확인합니다.
6. **표시**에서 **ESXi 구성**을 선택합니다.
7. 데이터를 복구하려는 백업을 선택합니다. 메시지가 표시되면 백업의 비밀번호를 입력합니다.
8. **확인**을 클릭합니다.
9. **새 데이터 저장소로 사용할 디스크**에서 다음을 수행합니다.
   - **ESXi 복구 대상**에서 호스트 구성을 복구할 디스크를 선택합니다. 구성을 원래 호스트로 복구하는 경우에는 원본 디스크가 자동으로 선택됩니다.
   - [선택 사항] **새 데이터 저장소로 사용**에서 새 데이터 저장소를 생성할 디스크를 선택합니다. 선택하는 디스크의 모든 데이터가 손실되므로 신중하게 선택하십시오. 기존 데이터 저장소의 가상 머신을 유지하려면 아무 데이터도 선택하지 마십시오.
10. 새 데이터 저장소로 사용할 디스크를 선택하는 경우에는 **새 데이터 저장소 생성 방법: 디스크당 하나의 데이터 저장소 생성** 또는 **선택한 모든 HDD에 하나의 데이터 저장소 생성**을 선택합니다.
11. [선택 사항] **네트워크 매핑**에서 백업에 존재하는 가상 스위치의 자동 매핑 결과를 실제 네트워크 어댑터로 변경합니다.
12. [선택 사항] 추가 설정을 지정하려면 **복구 옵션**을 클릭합니다.
13. **확인**을 클릭하여 복구를 시작합니다.

복구 옵션

복구 옵션을 수정하려면 복구를 구성할 때 **복구 옵션**을 클릭합니다.

복구 옵션의 사용 가능성

사용 가능한 복구 옵션은 다음에 따라 다릅니다.

- 복구를 수행하는 에이전트를 운영하는 환경(Windows, Linux, macOS 또는 부트 가능한 미디어).
- 복구하는 데이터 유형(디스크, 파일, 가상 머신, 애플리케이션 데이터).

다음 표는 복구 옵션의 사용 가능성을 요약해서 보여줍니다.

	디스크			파일				가상 머신	SQL 및 Exchange
	Windows	**Linux**	**부트 가능한 미디어**	**Windows**	**Linux**	**macOS**	**부트 가능한 미디어**	**ESXi, Hyper-V 및 Virtuozzo**	**Windows**
백업 유효	+	+	+	+	+	+	+	+	+

© Acronis International GmbH, 2003-2024

성 검사									
부트 모드	+	-	-	-	-	-	-	+	-
파일의 날짜 및 시간	-	-	-	+	+	+	+	-	-
오류 처리	+	+	+	+	+	+	+	+	+
파일 제외	-	-	-	+	+	+	+	-	-
파일 수준 보안	-	-	-	+	-	-	-	-	-
플래시백	+	+	+	-	-	-	-	+	-
전체 경로 복구	-	-	-	+	+	+	+	-	-
마운트 포인트	-	-	-	+	-	-	-	-	-
성능	+	+	-	+	+	+	-	+	+
사전/사후 명령어	+	+	-	+	+	+	-	+	+
SID 변경	+	-	-	-	-	-	-	-	-
VM 전원 관리	-	-	-	-	-	-	-	+	-
Windows 이벤트 로그	+	-	-	+	-	-	-	Hyper-V만 해당	+

백업 유효성 검사

이 옵션은 데이터가 백업에서 복구되기 전에 백업이 손상되지 않도록 백업의 유효성 검사를 수행할지 여부를 정의합니다. 이 작업은 보호 에이전트를 통해 수행됩니다.

사전 설정값이 **비활성화됨**.

체크섬 확인을 통한 유효성 검사에 대한 자세한 내용은 "체크섬 확인"(191페이지) 항목을 참조하십시오.

참고
서비스 제공업체에서 선택한 설정에 따라 다르지만, 클라우드 스토리지로 백업할 때는 유효성 검사를 수행하지 못할 수도 있습니다.

© Acronis International GmbH, 2003-2024

부트 모드

이 옵션은 Windows 운영 체제를 포함하고 있는 디스크 수준 백업에서 실제 머신 또는 가상 머신을 복구하는 경우에 유효합니다.

이 옵션을 사용하면 복구 후 Windows가 사용할 부트 모드(BIOS 또는 UEFI)를 선택할 수 있습니다. 원래 머신의 부트 모드가 선택한 부트 모드와 다른 경우 소프트웨어가 다음 작업을 수행합니다.

- 선택한 부트 모드에 따라 시스템 볼륨을 복구할 디스크(BIOS는 MBR, UEFI는 GPT)를 초기화합니다.
- Windows 운영 체제가 선택한 부트 모드를 사용하여 시작될 수 있도록 조정합니다.

사전 설정값이 **대상 머신에서.**

다음 중 하나를 선택할 수 있습니다.

- **대상 머신에서**
  대상 머신에서 실행 중인 에이전트가 현재 Windows가 사용 중인 부트 모드를 탐지하고, 탐지된 부트 모드에 따라 조정을 수행합니다.
  아래 나열된 제한 사항이 적용되지 않는 한 자동으로 부트 가능한 시스템으로 이어지는 가장 안전한 값입니다. 이 **부트 모드** 옵션이 부트 가능한 미디어 아래에 없기 때문에 해당 미디어의 에이전트는 항상 이 값을 선택한 것처럼 작동합니다.
- **백업된 머신에서**
  대상 머신에서 실행 중인 에이전트가 백업에서 부트 모드를 읽고, 이 부트 모드에 따라 조정을 수행합니다. 이렇게 하면 이 머신이 다른 부트 모드를 사용하는 경우에도 다른 머신의 시스템을 복구한 다음, 백업된 머신의 디스크를 교체할 수 있습니다.
- **BIOS**
  대상 머신에서 실행 중인 에이전트가 BIOS를 사용하도록 조정을 수행합니다.
- **UEFI**
  대상 머신에서 실행 중인 에이전트가 UEFI를 사용하도록 조정을 수행합니다.

설정이 변경되면 디스크 매핑 절차가 반복됩니다. 이 절차는 약간의 시간이 소요됩니다.

권장 사항

UEFI와 BIOS 간에 Windows를 전송해야 하는 경우:

- 시스템 볼륨이 위치한 전체 디스크를 복구합니다. 기존 볼륨 위에 시스템 볼륨만 복구하는 경우 에이전트가 대상 디스크를 올바로 초기화할 수 없습니다.
- BIOS는 2TB를 초과하는 디스크 공간 사용을 허용하지 않습니다.

제한 사항

- 다음에 대한 UEFI와 BIOS 간 전송은 지원되지 않습니다.
  - Windows 7 이상의 64비트 Windows 운영 체제
  - Windows Server 2008 SP1부터 64비트 Windows Server 운영 체제
- 백업이 테이프 장치에 저장되어 있는 경우에는 UEFI와 BIOS 간 전송이 지원되지 않습니다.

© Acronis International GmbH, 2003-2024

UEFI와 BIOS 간 시스템 전송이 지원되지 않으면 에이전트가 **백업된 머신에서** 설정이 선택된 것처럼 작동합니다 대상 머신이 UEFI와 BIOS를 모두 지원하는 경우에는 원본 머신에 따라 부트 모드를 수동으로 활성화해야 합니다. 그렇지 않으면 시스템이 부팅되지 않습니다.

파일의 날짜 및 시간

이 옵션은 파일을 복구할 때에만 유효합니다.

이 옵션은 백업에서 파일의 날짜 및 시간을 복구할지 또는 파일에 현재 날짜 및 시간을 할당할지 정의합니다.

이 옵션이 활성화되어 있으면 파일에 현재 날짜 및 시간이 할당됩니다.

사전 설정값이 **활성화됨**.

오류 처리

이 옵션을 사용하여 복구 중 발생할 수 있는 오류를 어떻게 처리할지 지정할 수 있습니다.

오류 발생 시 재시도

사전 설정값이 **활성화됨. 시도 횟수: 30. 시도 간격: 30초.**

복구 가능 오류가 발생하면 프로그램이 성공하지 못한 작업의 수행을 재시도합니다. 시간 간격과 시도 횟수를 설정할 수 있습니다. 작업 성공 또는 지정된 시도 횟수 완료 중 하나가 먼저 발생하면 시도가 중지됩니다.

처리할 동안 메시지 및 대화 상자 표시 안 함(자동 모드)

사전 설정값이 **비활성화됨**.

자동 모드가 활성화되어 있는 경우 가능하면 프로그램이 사용자 상호 작용이 필요한 상황을 자동으로 처리합니다. 작업 성공 또는 지정된 시도 횟수 완료 중 하나가 먼저 발생하면 시도가 중지됩니다. 작업 로그에는 오류(있는 경우)를 포함하여 작업에 대한 자세한 정보가 기록됩니다.

재부팅을 이용한 복구가 실패하는 경우 시스템 정보 저장

이 옵션은 Windows 또는 Linux를 실행하는 실제 머신으로 디스크 또는 볼륨을 복구할 때 유효합니다.

사전 설정값이 **비활성화됨**.

이 옵션이 활성화되어 있으면 로그, 시스템 정보, 크래시 덤프 파일이 저장될 로컬 디스크(대상 머신에 연결된 플래시 또는 HDD 드라이브 포함) 또는 네트워크 공유에서 폴더를 지정할 수 있습니다. 이 파일은 기술 지원 담당자가 문제를 파악하는 데 도움이 됩니다.

파일 제외

이 옵션은 파일을 복구할 때에만 유효합니다.

© Acronis International GmbH, 2003-2024

이 옵션은 복구 프로세스 중 건너뜀으로써 복구된 항목 목록에서 제외시킬 파일 및 폴더를 정의합니다.

참고
제외가 복구할 데이터 항목 선택보다 우선합니다. 예를 들어, MyFile.tmp 파일을 복구하고, 모든 .tmp 파일을 제외하기로 선택하는 경우 MyFile.tmp 파일이 복구되지 않습니다.

파일 수준 보안

이 옵션은 NTFS 형식 볼륨의 디스크 및 파일 수준 백업을 복구하는 경우에만 유효합니다.

이 옵션은 파일과 함께 파일에 대한 NTFS 권한을 복구할지 정의합니다.

사전 설정값이 **활성화됨**.

그 권한을 복구할지 아니면 파일이 복구될 대상 폴더로부터 NTFS 권한을 상속하게 할지 선택할 수 있습니다.

플래시백

이 옵션은 Mac을 제외한 실제 머신과 가상 머신에서 디스크 및 볼륨을 복구할 때 유효합니다.

이 옵션은 복구되는 디스크의 볼륨 레이아웃이 대상 디스크의 볼륨 레이아웃과 정확하게 일치할 때만 사용할 수 있습니다.

이 옵션이 활성화되어 있으면 백업에 있는 데이터와 대상 디스크 데이터 간의 차이만 복구됩니다. 이는 실제 머신 및 가상 머신의 복구를 가속화합니다. 데이터는 블록 수준에서 비교됩니다.

실제 머신을 복구할 때의 사전 설정은 **비활성화됨**.

가상 머신을 복구할 때의 사전 설정은 **활성화됨**.

전체 경로 복구

이 옵션은 파일 수준 백업에서 데이터를 복구하는 경우에만 유효합니다.

이 옵션이 활성화되어 있으면 대상 위치에서 파일의 전체 경로가 다시 생성됩니다.

사전 설정값이 **비활성화됨**.

마운트 포인트

이 옵션은 Windows의 파일 수준 백업에서 데이터를 복구하는 경우에만 유효합니다.

마운트된 볼륨에 저장되었다가 마운트 포인트 옵션이 활성화된 채로 백업된 파일 및 폴더를 복구하려면 이 옵션을 활성화합니다.

사전 설정값이 **비활성화됨**.

이 옵션은 폴더 계층에서 마운트 포인트보다 상위에 있는 폴더를 복구용으로 선택하는 경우에만 유효합니다. 마운트 포인트 내부의 폴더 또는 마운트 포인트 자체를 복구용으로 선택하는 경우에는 선택한 항목이 **마운트 포인트** 옵션 값에 상관없이 복구됩니다.

© Acronis International GmbH, 2003-2024

참고
볼륨이 복구 시점에 마운트되어 있지 않으면 데이터가 백업 당시 마운트 포인트였던 폴더로 바로 복구됩니다.

성능

이 옵션은 운영 체제에서 복구 프로세스의 우선 순위를 정의합니다.

사용 가능한 설정은 **낮음**, **보통**, **높음**입니다.

사전 설정값이 **보통**입니다.

시스템에서 실행하는 프로세스의 우선 순위는 CPU와 해당 프로세스에 할당된 시스템 리소스를 결정합니다. 복구 우선 순위를 낮추면 다른 애플리케이션용으로 추가 여유 리소스가 확보됩니다. 복구 우선 순위를 높이면 운영 체제에게 복구를 수행할 애플리케이션에 더 많은 리소스를 할당하도록 요청함으로써 복구 프로세스 속도가 빨라질 수 있습니다. 하지만 그 효과는 전체 CPU 사용량과 디스크 I/O 속도나 네트워크 트래픽 같은 기타 요인에 따라 달라집니다.

사전/사후 명령어

이 옵션을 사용하여 데이터 복구 전과 후에 자동으로 실행될 명령을 정의할 수 있습니다.

사전/사후 명령어를 사용하는 방법의 예:

- **Checkdisk** 명령을 실행하여 복구를 시작하기 전 또는 복구가 종료된 후 논리적 파일 시스템 오류, 물리적 오류 또는 불량 섹터를 찾아 수정합니다.

프로그램은 대화형 명령, 즉 사용자 입력(예: "pause")이 필요한 명령을 지원하지 않습니다.

복구로 인해 재부팅이 진행되는 경우에는 복구 후 명령이 실행되지 않습니다.

복구 전 명령

복구 프로세스가 시작되기 전에 실행할 명령/배치 파일을 지정하려면

1. **복구 전 명령 실행** 스위치를 활성화합니다.
2. **명령...** 필드에 명령을 입력하거나 배치 파일을 찾습니다.프로그램은 대화형 명령, 즉 사용자 입력(예: "pause")이 필요한 명령을 지원하지 않습니다.
3. **작업 디렉토리** 필드에 명령/배치 파일을 실행할 디렉토리의 경로를 지정합니다.
4. 필요한 경우 **인수** 필드에 명령 실행 인수를 지정합니다.
5. 원하는 결과에 따라 아래 표에 설명한 대로 적합한 옵션을 선택합니다.
6. **완료**를 클릭합니다.

확인란	**선택**			
명령 실행이 실패한 경우 복구 실패*	선택됨	선택 해제됨	선택됨	선택 해제됨

© Acronis International GmbH, 2003-2024

명령 실행이 완료될 때까지 복구 안 함	선택됨	선택됨	선택 해제됨	선택 해제됨
결과				
	사전 설정 명령이 성공적으로 실행된 후에만 복구를 수행합니다. 명령 실행이 실패한 경우 복구 실패.	실행 실패 또는 성공에 상관없이 명령이 실행된 후에 복구를 수행합니다.	해당 없음	명령 실행 결과에 상관없이 명령 실행과 동시에 복구를 수행합니다.

* 이 종료 코드가 0과 같지 않다면 명령이 실패한 것으로 간주됩니다.

복구 후 명령

복구가 완료된 후에 실행할 명령/실행 파일을 지정하려면

1. **복구 후 명령 실행** 스위치를 활성화합니다.
2. **명령...** 필드에 명령을 입력하거나 배치 파일을 찾습니다.
3. **작업 디렉토리** 필드에 명령/배치 파일을 실행할 디렉토리의 경로를 지정합니다.
4. 필요한 경우 **인수** 필드에 명령 실행 인수를 지정합니다.
5. 명령 실행이 반드시 성공해야 하는 경우 **명령 실행에 실패한 경우 복구 실패** 확인란을 선택합니다. 이 종료 코드가 0과 같지 않다면 명령이 실패한 것으로 간주됩니다. 명령 실행에 실패하면 복구 상태가 **오류**로 설정됩니다.
   이 확인란을 선택하지 않으면 명령 실행 결과가 복구 실패 또는 성공에 영향을 주지 않습니다. **작업** 탭을 살펴보면 명령 실행 결과를 추적할 수 있습니다.
6. **완료**를 클릭합니다.

참고
복구로 인해 재부팅이 진행되는 경우에는 복구 후 명령이 실행되지 않습니다.

SID 변경

이 옵션은 Windows 8.1/Windows Server 2012 R2 이전 버전을 복구할 때 효과적입니다.

이 옵션은 Agent for VMware, Agent for Hyper-V, Agent for Scale Computing HC3 또는 Agent for oVirt를 통해 가상 머신으로의 복구를 수행하는 경우 유효하지 않습니다.

사전 설정값이 **비활성화됨**.

소프트웨어는 복구된 운영 체제에 대해 고유한 보안 식별자(컴퓨터 SID)를 생성할 수 있습니다. 이 옵션은 컴퓨터 SID에 의존하는 서드 파티 소프트웨어의 운용 가능성을 보장하는 데에만 필요합니다.

Microsoft는 배포 또는 복구된 시스템에서의 SID 변경을 공식적으로 지원하지는 않습니다. 따라서 이 옵션은 사용자 책임에 따라 사용하십시오.

© Acronis International GmbH, 2003-2024

VM 전원 관리

이러한 옵션은 Agent for VMware, Agent for Hyper-V, Agent for Virtuozzo, Agent for Scale Computing HC3 또는 Agent for oVirt를 통해 가상 머신으로의 복구를 수행하는 경우에 유효합니다.

복구 시작 시 대상 가상 머신의 전원 끄기

사전 설정값이 **활성화됨**.

머신이 온라인 상태인 경우 결국 복구를 시작하자마자 머신의 전원이 자동으로 꺼지기 때문에 기존 가상 머신으로의 복구가 불가능합니다. 그러면 사용자가 머신에서 연결이 끊기게 되므로 저장되지 않은 데이터가 손실됩니다.

복구 전에 가상 머신의 전원을 수동으로 끄려면 이 옵션의 확인란을 선택 해제하십시오.

복구 완료 시 대상 가상 머신 전원 켜기

사전 설정값이 **비활성화됨**.

머신이 백업에서 다른 머신으로 복구된 후에 기존 머신의 복제본이 네트워크에 표시될 수 있습니다. 안전을 기하기 위해 필요한 예방 조치를 취한 후에 복구된 가상 머신의 전원을 수동으로 켜십시오.

Windows 이벤트 로그

이 옵션은 Windows 운영 체제에서만 유효합니다.

이 옵션은 에이전트가 Windows의 애플리케이션 이벤트 로그에 복구 작업의 이벤트를 기록해야 하는지 정의합니다(이 로그를 보려면 eventvwr.exe를 실행하거나 **제어판** > **관리 도구** > **이벤트 뷰어** 선택). 기록할 이벤트를 필터링할 수 있습니다.

사전 설정값이 **비활성화됨**.

백업 관련 작업

백업 스토리지 탭

백업 스토리지 탭에서는 오프라인 머신의 백업, Cyber Protection 서비스에 더 이상 등록되어 있지 않은 머신의 백업, Microsoft Azure와 같은 퍼블릭 클라우드로의 백업, 분리된 백업[1]을 비롯한 모든 백업에 액세스할 수 있습니다.

acrocmd를 통해 생성된 백업은 분리됨으로 플래그가 지정됩니다. 제품의 12.5 버전에서 생성된 백업도 분리됨으로 식별됩니다.

참고
분리된 백업도 비용이 부과됨을 명심하십시오.

[1]분리된 백업은 더 이상 보호 계획과 연결되어 있지 않은 백업입니다.

© Acronis International GmbH, 2003-2024

공유 위치(예: SMB 또는 NFS 공유)에 저장된 백업은 해당 위치에 대한 읽기 권한을 가진 모든 사용자에게 표시됩니다.

Windows에서는 백업 파일이 해당 상위 폴더의 액세스 권한을 상속받습니다. 따라서 이 폴더에 대한 읽기 권한을 제한하는 것이 좋습니다.

클라우드 스토리지에서 사용자는 자신의 백업에만 액세스할 수 있습니다.

관리자는 계정용 클라우드 스토리지를 선택하여 지정된 단위 또는 회사 및 해당 자식 그룹에 속한 모든 계정을 대신해 클라우드로의 백업을 볼 수 있습니다. 클라우드에서 데이터를 가져오는 데 사용할 장치를 선택하려면 **다음 위치에서 탐색할 머신** 행에서 **변경**을 클릭합니다. **백업 스토리지** 탭에는 선택한 계정에서 등록된 모든 머신의 백업이 표시됩니다.

클라우드 Agent for Microsoft 365에서 생성된 백업 및 Google Workspace 데이터 백업은 **클라우드 스토리지** 위치가 아니라 별도로 지정된 섹션 **클라우드 애플리케이션 백업**에 표시됩니다.

보호 계획에 사용된 백업 위치가 **백업 스토리지** 탭에 자동으로 추가됩니다. 백업 위치 목록에 사용자 정의 폴더(예: 분리식 USB 장치)를 추가하려면 **찾아보기**를 클릭해 폴더 경로를 지정합니다.

파일 관리자를 이용하여 일부 백업을 추가하거나 삭제하였다면, 위치 이름 옆에 있는 기어 아이콘을 클릭한 다음 **새로 고침**을 클릭합니다.

경고!
백업 파일 수동 편집을 시도하지 마십시오. 백업 파일을 수동으로 편집하면 파일이 손상되어 백업을 사용하지 못하게 될 수 있습니다. 또한 백업 파일을 수동으로 이동하는 대신 백업 복제를 사용하는 것이 좋습니다.

모든 머신이 서비스에서 삭제된 위치에 백업된 적이 있다면 **백업 스토리지** 탭에서 백업 위치가 사라집니다(클라우드 스토리지 제외). 이를 통해 이 위치에 저장된 백업에 대해서는 지불할 필요가 없어집니다. 이 위치에 백업이 발생한 순간, 해당 위치는 저장된 모든 백업과 함께 다시 추가됩니다.

백업 스토리지 탭에서 다음 조건을 사용하여 목록의 백업을 필터링할 수 있습니다.

- **포렌직 데이터가 있는 경우만** – 포렌직 데이터가 있는 백업만 표시됩니다.
- **패치 관리에 의해 생성된 업데이트 전 백업만** – 패치 설치 전 패치 관리 실행 중 생성된 백업만 표시됩니다.

백업 스토리지 탭을 사용하여 복구 지점을 선택하려면

1. **백업 스토리지** 탭에서 백업이 저장된 위치를 선택합니다.
   선택한 위치에서 사용자의 계정이 볼 수 있도록 허용된 모든 백업이 표시됩니다. 백업은 그룹으로 묶여 있습니다. 그룹 이름은 다음 템플릿에 따라 지정되어 있습니다.
   <머신 이름> - <보호 계획 이름>
2. 데이터를 복구하려는 그룹을 선택합니다.
3. [선택 사항] **다음 위치에서 탐색할 머신** 옆에 있는 **변경**을 클릭한 다음 다른 머신을 선택합니다. 일부 백업은 특정 에이전트에서만 찾을 수 있습니다. 예를 들어 Microsoft SQL Server 데이터베이스의 백업을 찾으려면 Agent for SQL을 실행 중인 머신을 선택해야 합니다.

© Acronis International GmbH, 2003-2024

중요
실제 머신 백업에서 복구하는 경우 **다음 위치에서 탐색할 머신**이 기본 목적지입니다. 복구 지점을 선택하고 **복구**를 클릭한 후에는 **대상 머신** 설정을 다시 한 번 살펴보고 특정 머신으로 복구할지 확인합니다. 복구 목적지를 변경하려면 **다음 위치에서 탐색할 머신**에서 다른 머신을 지정합니다.

4. **백업 표시**를 클릭합니다.
5. 복구 지점을 선택합니다.

백업용 위치를 추가하려면

참고
이 작업은 온라인 에이전트가 있어야 수행할 수 있습니다.

백업 스토리지 탭에서 **위치 추가**를 클릭합니다.

다음 위치 유형 중 하나에서 위치를 선택하고 **완료**를 클릭합니다.

- 로컬 폴더
- 네트워크 폴더
- Secure Zone
- NFS 폴더
- 퍼블릭 클라우드

백업에서 볼륨 마운트

디스크 수준 백업에서의 볼륨 마운트를 통해 실제 디스크인 것처럼 볼륨에 액세스할 수 있습니다.

읽기/쓰기 모드에서 볼륨 마운트를 통해 백업 내용을 수정할 수 있습니다. 즉, 파일 또는 폴더를 저장, 이동, 생성, 삭제하고 하나의 파일을 구성하는 실행 파일을 실행합니다. 이 모드에서 소프트웨어는 백업 내용의 변경 사항을 포함한 증분 백업을 생성합니다. 후속 백업의 어떤 것에도 이러한 변경 사항이 포함되지 않습니다.

요구 사항

- 이 기능은 파일 탐색기를 사용하여 Windows에서만 이용할 수 있습니다.
- Agent for Windows는 마운트 작업을 수행하는 머신에 설치되어야 합니다.
- 백업된 파일 시스템은 머신이 실행 중인 Windows 버전에서 지원해야 합니다.
- 백업은 로컬 폴더, 네트워크 공유(SMB/CIFS) 또는 Secure Zone에 저장해야 합니다.

사용 시나리오

- 데이터 공유
  마운팅된 볼륨은 네트워크에서 쉽게 공유할 수 있습니다.
- "임시 처방" 데이터베이스 복구 솔루션

© Acronis International GmbH, 2003-2024

최근 실패한 머신에서 SQL 데이터베이스를 포함하는 볼륨을 마운트합니다. 이 작업은 실패한 머신을 복구할 때까지 데이터베이스에 대한 액세스 권한을 제공합니다. 이 접근법은 SharePoint 탐색기를 사용하여 Microsoft SharePoint 데이터의 개별 복구에 사용할 수도 있습니다.

- 오프라인 바이러스 제거

  머신이 감염된 경우 백업을 마운트하고 바이러스 백신 프로그램으로 바이러스를 삭제하거나 감염되지 않은 최신 백업을 찾은 다음 이 백업에서 머신을 복구합니다.

- 오류 확인

  볼륨 크기 조정 복구에 실패한 경우 백업된 파일 시스템에 오류가 발생했기 때문일 수 있습니다. 읽기/쓰기 모드에서 백업을 마운트하십시오. 그런 다음 `chkdsk /r` 명령을 사용하여 마운트된 볼륨에서 오류가 있는지 확인합니다. 오류가 수정되고 새 증분 백업이 생성된 후 이 백업에서 시스템을 복구합니다.

백업에서 볼륨을 마운트하려면

1. 파일 탐색기를 사용하여 백업 위치를 찾습니다.
2. 백업 파일을 두 번 클릭합니다. 파일 이름은 다음 템플릿에 따라 지정되어 있습니다.

   `<머신 이름> - <보호 계획 GUID>`
3. 백업이 암호화되어 있는 경우 암호화 비밀번호를 입력합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.

   파일 탐색기가 복구 지점을 표시합니다.
4. 복구 지점을 두 번 클릭합니다.

   파일 탐색기가 백업된 볼륨을 표시합니다.

   참고
   내용을 찾으려는 볼륨을 두 번 클릭합니다. 백업에서 파일 및 폴더를 파일 시스템에 있는 폴더에 복사할 수 있습니다.

5. 탑재할 볼륨을 마우스 오른쪽 버튼으로 클릭하고 다음 옵션 중 하나를 선택합니다.
   a. **마운트**

      참고
      아카이브(백업 체인)의 마지막 백업만 읽기/쓰기 모드로 마운트할 수 있습니다.

   b. **읽기 전용 모드로 마운트**.
6. 백업이 네트워크 공유에 저장된 경우 액세스 자격 증명을 제공합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.

   소프트웨어가 선택한 볼륨을 마운트합니다. 사용하지 않은 첫 글자가 볼륨에 할당됩니다.

볼륨을 마운트 해제하려면

1. 파일 탐색기를 사용하여 **컴퓨터**(Windows 8.1 이상에서는 **이 PC**)로 이동합니다.
2. 마운트된 볼륨을 마우스 오른쪽 버튼으로 클릭합니다.
3. **마운트 해제**를 클릭합니다.
4. [선택 사항] 볼륨이 읽기/쓰기 모드에서 마운트되고 내용이 수정된 경우 변경 사항을 포함하는 증분 백업을 생성할지 여부를 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.

© Acronis International GmbH, 2003-2024

소프트웨어가 선택한 볼륨을 마운트 해제합니다.

백업 유효성 검사

백업의 유효성을 검사하면 해당 백업의 데이터 복구 가능 여부를 확인할 수 있습니다. 이 작업에 대한 자세한 내용은 "유효성 검사"(188페이지)을(를) 참조하십시오.

참고
이 기능은 Advanced Backup 팩 내에서 **Advanced Backup – 서버** 또는 **Advanced Backup – NAS** 할당량이 활성화되어 있는 고객 테넌트에서 사용 가능합니다.

백업 유효성을 검사하려면

1. 백업된 워크로드를 선택합니다.
2. **복구**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.
   워크로드가 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 중 하나를 수행하십시오.
   - 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 온라인 상태인 대상 워크로드를 선택한 다음 복구 지점을 선택합니다.
   - 백업 스토리지 탭에서 복구 지점을 선택합니다. 클라우드나 공유 스토리지의 백업에 대한 자세한 내용은 "백업 스토리지 탭"(480페이지)을(를) 참조하십시오.
4. 기어 아이콘을 클릭하고 **유효성 검사**를 클릭합니다.
5. 유효성 검사를 수행할 에이전트를 선택합니다.
6. 유효성 검사 방법을 선택합니다.
7. 백업이 암호화되어 있는 경우 암호화 비밀번호를 제공합니다.
8. **시작**을 클릭합니다.

백업 내보내기

내보내기 작업에서는 사용자가 지정한 위치에 백업의 자급식 사본이 생성됩니다. 원본 백업은 그대로 남아 있습니다. 백업 내보내기를 사용하면 빠른 복구를 위해 증분 및 차등 백업의 체인에서 지정한 백업을 분리하고 이동식 또는 분리 가능한 미디어에 또는 다른 목적으로 쓸 수 있습니다.

참고
이 기능은 Advanced Backup 팩 내에서 **Advanced Backup – 서버** 또는 **Advanced Backup – NAS** 할당량이 활성화되어 있는 고객 테넌트에서 사용 가능합니다.

내보내기 작업의 결과는 항상 전체 백업입니다. 전체 백업 체인을 다른 위치로 복제하고 여러 복구 지점을 유지하려면 백업 복제 계획을 사용하십시오. 이 계획에 대한 자세한 내용은 "백업 복제"(185페이지)을(를) 참조하십시오.

내보낸 백업의 백업 파일 이름은 시퀀스 번호만 제외하고 원래 백업의 파일 이름과 동일합니다. 같은 백업 체인의 여러 백업을 같은 위치로 내보낸 경우에는 첫 번째 백업을 제외하고, 모든 백업의 파일 이름에 네 자리 순차 번호가 붙습니다.

© Acronis International GmbH, 2003-2024

내보낸 백업은 원래 백업에서 암호화 설정 및 비밀번호를 상속합니다. 암호화된 백업을 내보낼 때에는 비밀번호를 지정해야 합니다.

백업을 내보내려면

1. 백업된 워크로드를 선택합니다.
2. **복구**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.
   워크로드가 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 중 하나를 수행하십시오.
   - 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 온라인 상태인 대상 워크로드를 선택한 다음 복구 지점을 선택합니다.
   - 백업 스토리지 탭에서 복구 지점을 선택합니다. 클라우드나 공유 스토리지의 백업에 대한 자세한 내용은 "백업 스토리지 탭"(480페이지)을(를) 참조하십시오.
4. 기어 아이콘을 클릭하고 **내보내기**를 클릭합니다.
5. 내보내기를 수행할 에이전트를 선택합니다.
6. 백업이 암호화되어 있는 경우 암호화 비밀번호를 제공합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
7. 내보내기 대상을 지정합니다.
8. **시작**을 클릭합니다.

백업 삭제

백업 아카이브는 하나 이상의 백업을 포함합니다. 아카이브에서 특정 백업(복구 지점)을 삭제하거나 전체 아카이브를 삭제할 수 있습니다.

백업 아카이브를 삭제하면 그 안의 모든 백업이 삭제됩니다. 워크로드의 모든 백업을 삭제하면 이러한 백업을 포함하는 백업 아카이브가 삭제됩니다.

장치 탭과 **백업 스토리지** 탭에서 Cyber Protect 콘솔을 사용하여 백업을 삭제할 수 있습니다. 또한 웹 복원 콘솔을 사용하여 클라우드 스토리지에서 백업을 삭제할 수 있습니다.

경고!
변경 불가능 스토리지가 비활성화된 경우 백업된 데이터는 영구적으로 삭제되고 복구할 수 없습니다.

백업 또는 백업 아카이브를 삭제하는 방법

장치 탭의 경우

이 절차는 온라인 워크로드에만 적용됩니다.

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 삭제하려는 워크로드 백업을 선택합니다.
3. **복구**를 클릭합니다.
4. [사용 가능한 백업 위치가 두 개 이상인 경우] 백업 위치를 선택합니다.

© Acronis International GmbH, 2003-2024

5. [워크로드의 모든 백업을 삭제하는 방법] **모두 삭제**를 클릭합니다.
   모든 백업을 삭제하면 이러한 백업을 포함하는 백업 아카이브도 삭제됩니다.
6. [특정 백업을 삭제하는 방법] 삭제하려는 백업(복구 지점)을 선택한 다음 **작업** > **삭제**를 클릭합니다.
7. [모든 백업을 삭제하는 경우] 확인란을 선택한 다음 **삭제**를 클릭하여 결정을 확인합니다.
8. [특정 백업을 삭제할 때] **삭제**를 클릭하여 결정을 확인합니다.

백업 스토리지 탭의 경우

이 절차는 온라인 및 오프라인 워크로드에 적용됩니다.

1. Cyber Protect 콘솔에서 **백업 스토리지**로 이동합니다.
2. 백업을 삭제하려는 위치를 선택합니다.
3. 백업을 삭제하려는 백업 아카이브를 선택합니다.
   아카이브 이름은 다음 템플릿을 사용합니다.
   - 클라우드 간 백업 아카이브가 아닌 경우: <워크로드 이름> - <보호 계획 이름>
   - 클라우드 간 백업 아카이브인 경우: <사용자 이름> 또는 <드라이브 이름> 또는 <팀 이름> - <클라우드 서비스> - <보호 계획 이름>
4. [전체 백업 아카이브를 삭제하는 방법] **삭제**를 클릭합니다.
   백업 아카이브를 삭제하면 해당 아카이브의 모든 백업이 삭제됩니다.
5. [백업 아카이브에서 특정 백업을 삭제하는 방법] **백업 보기**를 클릭합니다.
   a. 삭제하려는 백업(복구 지점)을 선택합니다.
   b. **작업** > **삭제**를 클릭합니다.
6. [백업 아카이브를 삭제할 때] 확인란을 선택한 다음 **삭제**를 클릭하여 결정을 확인합니다.
7. [특정 백업을 삭제할 때] **삭제**를 클릭하여 결정을 확인합니다.

웹 복원 콘솔에서

이 절차는 클라우드 스토리지의 백업 아카이브에만 적용됩니다.

1. Cyber Protection 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 삭제하려는 워크로드 백업을 선택한 다음 **복구**를 클릭합니다.
3. [여러 백업 위치가 사용 가능한 경우] 백업 위치를 선택한 다음 **더 많은 복구 방법**을 클릭합니다.
4. **파일 다운로드**를 클릭합니다.
   웹 복원 콘솔로 리디렉션됩니다.
5. 웹 복원 콘솔의 **머신**에서 워크로드 이름을 클릭합니다.
6. **마지막 버전**에서 날짜를 클릭한 다음에 **삭제**를 클릭합니다.
   이 작업은 백업 아카이브 수준에서만 가능합니다. 아카이브를 드릴다운할 수 없고 특정 백업을 삭제할 수는 없습니다.
7. **삭제**를 클릭하여 결정을 확인합니다.

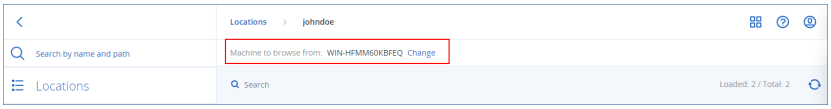
© Acronis International GmbH, 2003-2024

Cyber Protect 콘솔 외부에서 백업 삭제

Cyber Protect 콘솔을 사용하여 백업을 삭제하는 것을 권장합니다. 웹 복원 콘솔을 사용하여 클라우드 스토리지에서 백업을 삭제하거나 파일 관리자를 사용하여 로컬 백업을 삭제하는 경우 변경 사항을 Cyber Protect 콘솔에 동기화하기 위해 백업 위치를 새로 고침해야 합니다.

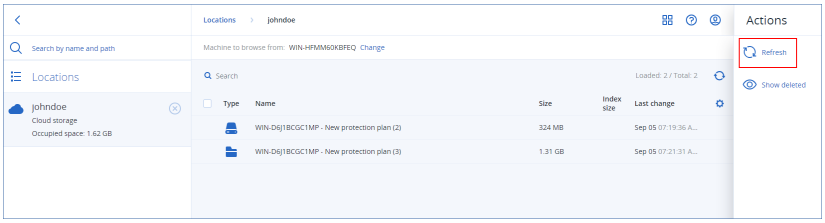
사전 요구 사항

- 백업 위치에 액세스할 수 있는 온라인 에이전트는 **다음 위치에서 탐색할 머신**으로 Cyber Protect 콘솔에서 선택되어야 합니다.



백업 위치를 새로 고침하는 방법

1. Cyber Protect 콘솔에서 **백업 스토리지**로 이동합니다.
2. 삭제된 백업이 저장된 백업 위치를 선택합니다.
3. **작업** 창에서 **새로 고침**을 클릭합니다.



병목 현상 감지 방식 파악

병목 현상 감지 기능을 사용하면 성능을 개선할 수 있는 위치를 파악할 수 있습니다. 백업 또는 복구 프로세스 중에 시스템 속도가 가장 느렸던 컴포넌트가 강조 표시되기 때문입니다.

병목 현상은 *항상* 전송 이벤트에서 발생하므로 반드시 해결해야 하는 상황은 아닙니다. 즉, 백업 속도가 이미 충분히 빨라 백업 할당 시간 내에 백업이 완료되며 SLA도 충족하는 경우도 있습니다. 이러한 경우에는 대개 실제로 해결해야 하는 문제가 없습니다.

작업 상세 정보 탭에서 병목 현상을 쉽게 확인 및 추적할 수 있습니다. 이렇게 하려면 Cyber Protect 콘솔에서 **모니터링 > 작업**으로 이동한 후 관련 작업을 클릭합니다. 병목 현상을 확인하는 방법에 대한 자세한 내용은 "병목 현상 상세 정보 확인"(489페이지) 및 "병목 현상이 표시되는 워크로드, 에이전트 및 백업 위치"(490페이지) 항목을 참조하십시오.

병목 현상이란?

병목 현상은 대개 처리 체인에서 속도가 느린 컴포넌트(실행되기를 다른 컴포넌트가 기다려야 하는 컴포넌트)로 인해 발생합니다.

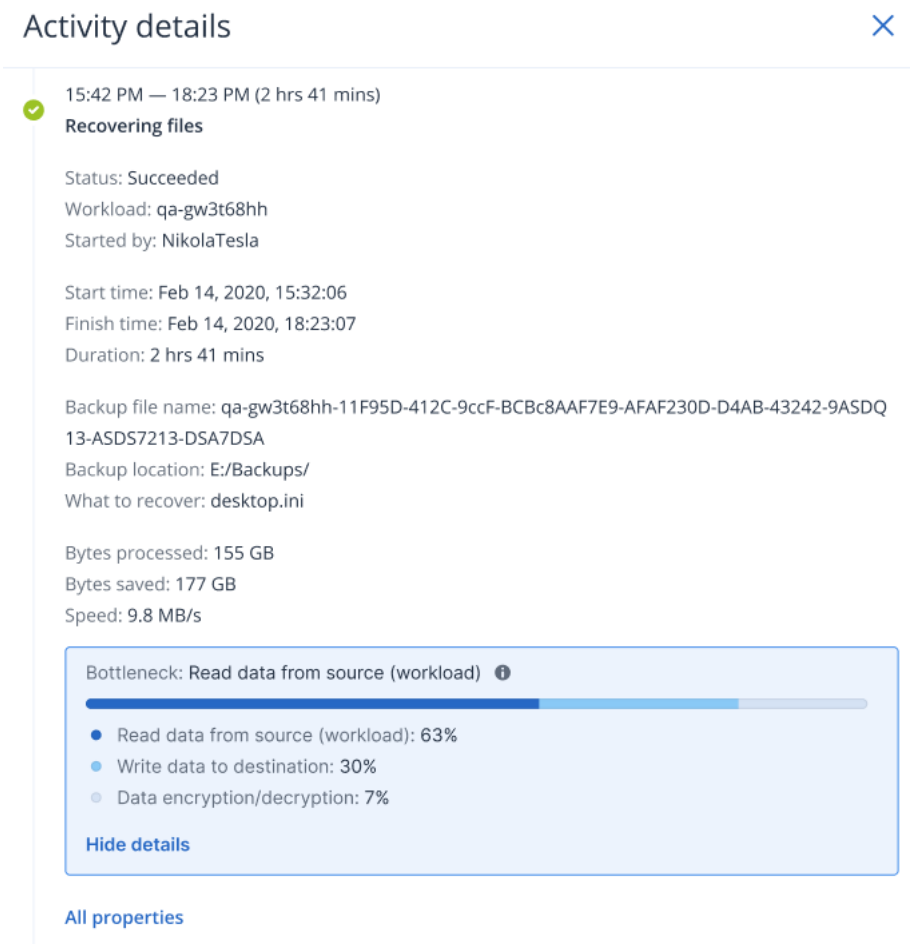
병목 현상 감지 기능을 사용하면 백업 및 복구 프로세스 중에 이처럼 속도가 느린 컴포넌트를 추적하여 다음 중 속도가 가장 느린 컴포넌트 유형을 파악할 수 있습니다.

© Acronis International GmbH, 2003-2024

- **소스**: 백업/복구 소스의 읽기 속도가 느려서 병목 현상이 발생하는지 여부를 한 눈에 확인할 수 있습니다.
- **대상**: 백업/복구 대상으로의 쓰기 속도가 느려서 성능이 저하되는지 여부를 파악할 수 있습니다.
- **에이전트**: 에이전트의 데이터 처리 속도가 충분히 빠른지를 파악할 수 있습니다.

병목 현상 유형(소스, 대상, 에이전트)은 백업/복구 작업 중에 시간별로 변경될 수 있습니다. 아래의 **작업 상세 정보** 탭 **병목 현상** 섹션에 나와 있는 비율은 해당 병목 현상 유형이 발생한 시간의 비율을 나타냅니다. 가령 **소스(워크로드)에서 데이터 읽기: 63%**의 경우 총 데이터 읽기 시간 중 63%에 해당하는 시간에 병목 현상이 발생했다는 의미입니다. 이 경우 전체 복구 작업 시간 중 63%에 해당하는 시간의 병목 현상 유형은 데이터 읽기입니다. 즉, 에이전트가 백업 아카이브에서 데이터를 읽는 속도가 느린 것입니다.

마찬가지로 전체 복구 작업 시간 중 30%에 해당하는 시간의 병목 현상은 복구 대상으로 데이터를 쓰는 속도가 느려서 발생한 것입니다(**대상에 데이터 쓰기: 30%**).



참고
작업 상세 정보 탭에 병목 현상 통계가 표시되는 것은 정상적인 현상입니다. 이러한 통계는 실행 시간이 1분을 초과하는 작업에서만 제공됩니다.

© Acronis International GmbH, 2003-2024

병목 현상을 줄이는 방법

위에서 설명한 것처럼 병목 현상 감지 기능은 백업 컴포넌트 간의 *읽기* 및 *쓰기*데이터 플로우를 강조 표시합니다. *읽기* 통계는 데이터 소스에서 백업/복구 작업을 수행하는 에이전트로의 데이터 플로우를, 그리고 *쓰기* 통계는 에이전트와 백업 아카이브(대상) 간의 데이터 플로우를 지칭합니다.

병목 현상을 줄이고 읽기/쓰기 데이터 플로우 성능을 개선하려면 에이전트와 데이터 소스/백업 아카이브 간의 채널을 분석해야 합니다. 예를 들어 에이전트가 로컬 파일을 백업하는 경우 하드 디스크 벤치마킹을 진행해 볼 수 있습니다.

병목 현상 상세 정보 확인

가상 머신 백업, 머신 백업, 파일/폴더 백업을 비롯한 모든 유형의 백업, 백업 복제 또는 복구 프로세스(모든 유형의 대상 폴더 또는 위치로의)에서 감지된 병목 현상을 확인할 수 있습니다. 가상 머신 복제 및 장애 복구 작업의 병목 현상도 확인할 수 있습니다.

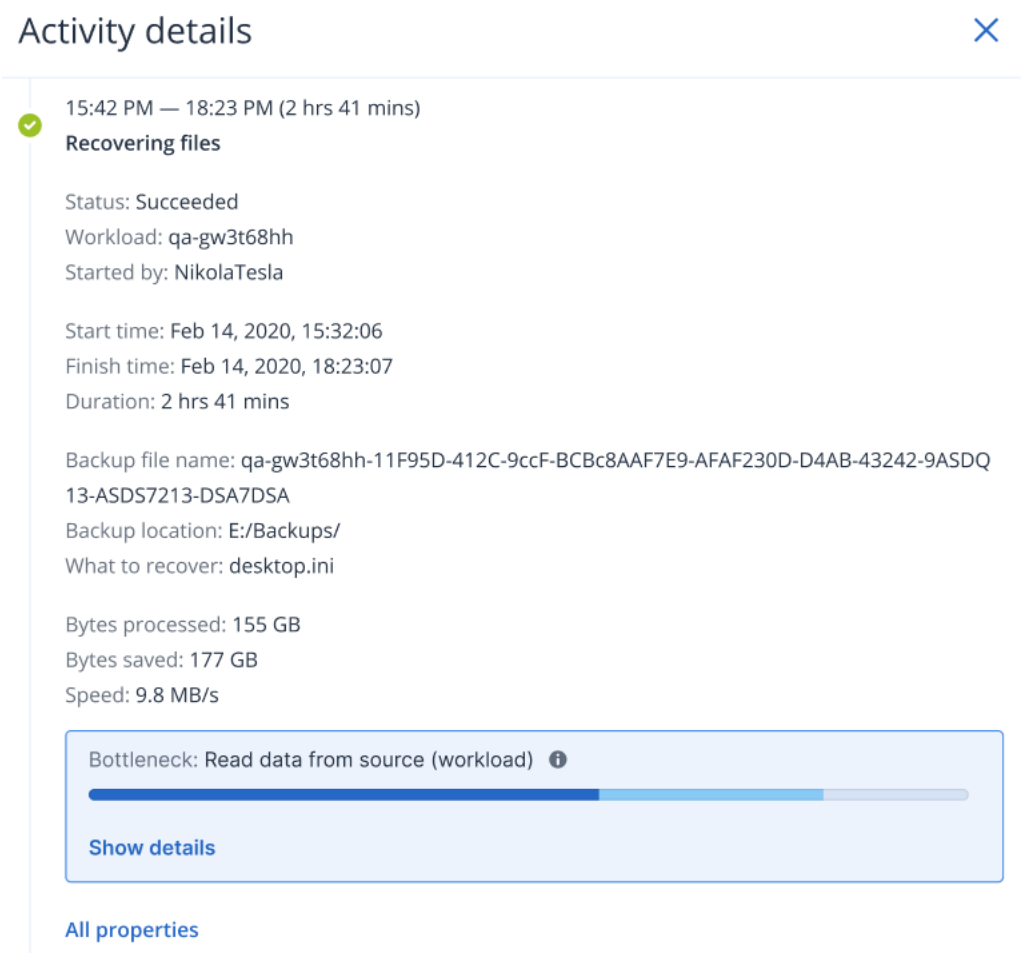
병목 현상 유형의 정의와 병목 현상 관련 핵심 개념에 대한 자세한 내용은 "병목 현상 감지 방식 파악"(487페이지) 항목을 참조하십시오.

병목 현상 상세 정보를 확인하려면

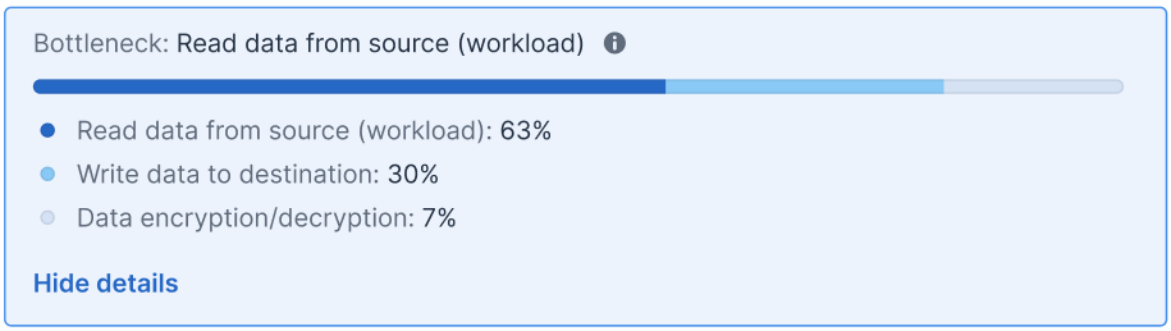
1. Cyber Protect 콘솔에서 **모니터링 > 작업**으로 이동합니다.
2. 관련 작업을 클릭합니다.

   작업 상세 정보 탭에서 **병목 현상** 섹션이 파란색으로 표시됩니다.

© Acronis International GmbH, 2003-2024



3. **상세 정보 표시**를 클릭하여 백업/복구 작업 중에 가장 자주 발생한 병목 현상을 확인합니다. **병목 현상** 섹션이 확장되어 관련 병목 현상 유형의 요약이 표시됩니다.



위의 예에서 전체 작업 시간 중 63%를 차지하는 병목 현상은 에이전트가 수행한 *읽기* 작업으로 인해 발생한 것입니다.

참고
해당 작업을 실행하는 동안 병목 현상 값이 1분마다 동적으로 업데이트됩니다.

병목 현상이 표시되는 워크로드, 에이전트 및 백업 위치

병목 현상을 감지할 수 있는 워크로드, 에이전트 및 백업 위치의 유형은 다음과 같습니다.

© Acronis International GmbH, 2003-2024

- 다음 항목에서 수행하는 디스크/이미지 수준 백업:
  - Agent for Azure
  - Agent for Windows
  - Agent for Linux
  - Agent for Mac
  - Agent for VMware(가상 어플라이언스 및 Windows 둘 다 - VM 복제 및 복제본에서 수행하는 장애 복구(복제본에서 복원) 작업 포함)
  - Agent for Hyper-V
  - Agent for Scale Computing
  - Agent for oVirt(KVM)
  - Virtuozzo Infrastructure Platform을 위한 에이전트
  - Agent for Virtuozzo
  - Agent for VMware Cloud Director(vCD-BA)
- 파일 수준 백업
  - Agent for Windows
  - Agent for Linux
  - Agent for Mac
- 애플리케이션 수준 백업
  - Agent for SQL
  - Agent for Exchange
  - Agent for MySQL/MariaDB
  - Agent for Oracle
  - Agent for SAP HANA
- 백업 위치
  - Acronis Cloud Storage(파트너가 호스팅하는 스토리지 포함)
  - 퍼블릭 클라우드 스토리지
  - 네트워크 공유(SMB + NFS)
  - 로컬 폴더
  - 스크립트에서 정의한 위치
  - Acronis Secure Zone

퍼블릭 클라우드에 워크로드 백업

참고

이 기능은 Advanced Backup 팩에 포함되어 있으며, 이 팩은 Cyber Protection 서비스를 통해 제공됩니다. 보호 계획에 이 기능을 추가하면 추가 요금이 부과될 수 있습니다.

Cyber Protect 콘솔에서 Microsoft Azure, Amazon S3(Simple Storage Service) 등의 퍼블릭 클라우드 서비스를 백업 목적지로 선택할 수 있습니다.

© Acronis International GmbH, 2003-2024

퍼블릭 클라우드에서 백업 위치를 구성하려면 회사 관리자 또는 단위 관리자이거나 Cyber Protection 서비스에서 Cyber 관리자, 관리자 또는 사용자 역할 중 하나를 정의해야 합니다.

Microsoft Azure에서 백업 위치 정의

참고
Microsoft Azure에서 백업 위치를 구성하려면 Cyber Protection 서비스에서 회사 관리자, 사용자, Cyber 관리자 역할 중 하나를 정의해야 합니다.

Microsoft Azure에 워크로드를 백업하려면 Cyber Protect 콘솔에서 Microsoft Azure 백업 위치를 정의한 후 관련 Microsoft Azure 구독에 연결해야 합니다. 이 작업은 다음 방법을 통해 수행할 수 있습니다.

- 보호 계획 생성 또는 편집 시.
- 백업 스토리지 위치 정의 및 관리 시.

중요
관리자와 관리자 이외의 사용자가 모두 Microsoft Azure에 워크로드를 백업할 수 있습니다.

관리자 이외의 사용자는 Microsoft Azure 구독 액세스 권한을 추가할 수는 있지만("Microsoft Azure 구독 액세스 관리"(502페이지) 항목 참조) 본인의 이름으로 Cyber Protect 콘솔에 등록되어 있는 워크로드에 한해 백업 위치가 연결되어 있는 보호 계획만 본인이 추가한 Microsoft Azure 구독에 적용할 수 있습니다.

관리자는 등록을 한 사용자 이름에 관계없이 Cyber Protect 콘솔에 등록되어 있는 워크로드를 대상으로 백업 위치가 연결되어 있는 보호 계획을 본인이나 다른 관리자가 추가한 Microsoft Azure 구독에 적용할 수 있습니다.

Microsoft Azure에서 백업 위치를 정의하려면

1. Cyber Protect 콘솔에서 다음 중 하나를 수행합니다.
   - 보호 계획을 생성하거나 편집하는 경우 **장치**로 이동한 후 Microsoft Azure에 백업하려는 관련 워크로드를 선택합니다. 선택한 워크로드의 보호 계획 **백업** 섹션에서 **백업할 위치** 행의 링크를 클릭합니다.
     보호 계획 사용에 대한 자세한 내용은 "보호 계획 및 모듈"(199페이지) 항목을 참조하십시오.
   - 백업 스토리지 위치 관리 중에 Microsoft Azure를 새 위치로 추가하려는 경우에는 **백업 스토리지**로 이동합니다.
     백업 스토리지 위치 관리에 대한 자세한 내용은 "백업 스토리지 탭"(480페이지) 항목을 참조하십시오.
2. **위치 추가**를 클릭합니다.
3. **퍼블릭 클라우드** 드롭다운 목록에서 **Microsoft Azure**를 선택합니다.
4. 관련 Microsoft Azure 구독이 Cyber Protect 콘솔에 이미 등록되어 있다면 구독 목록에서 해당 구독을 선택합니다.

© Acronis International GmbH, 2003-2024

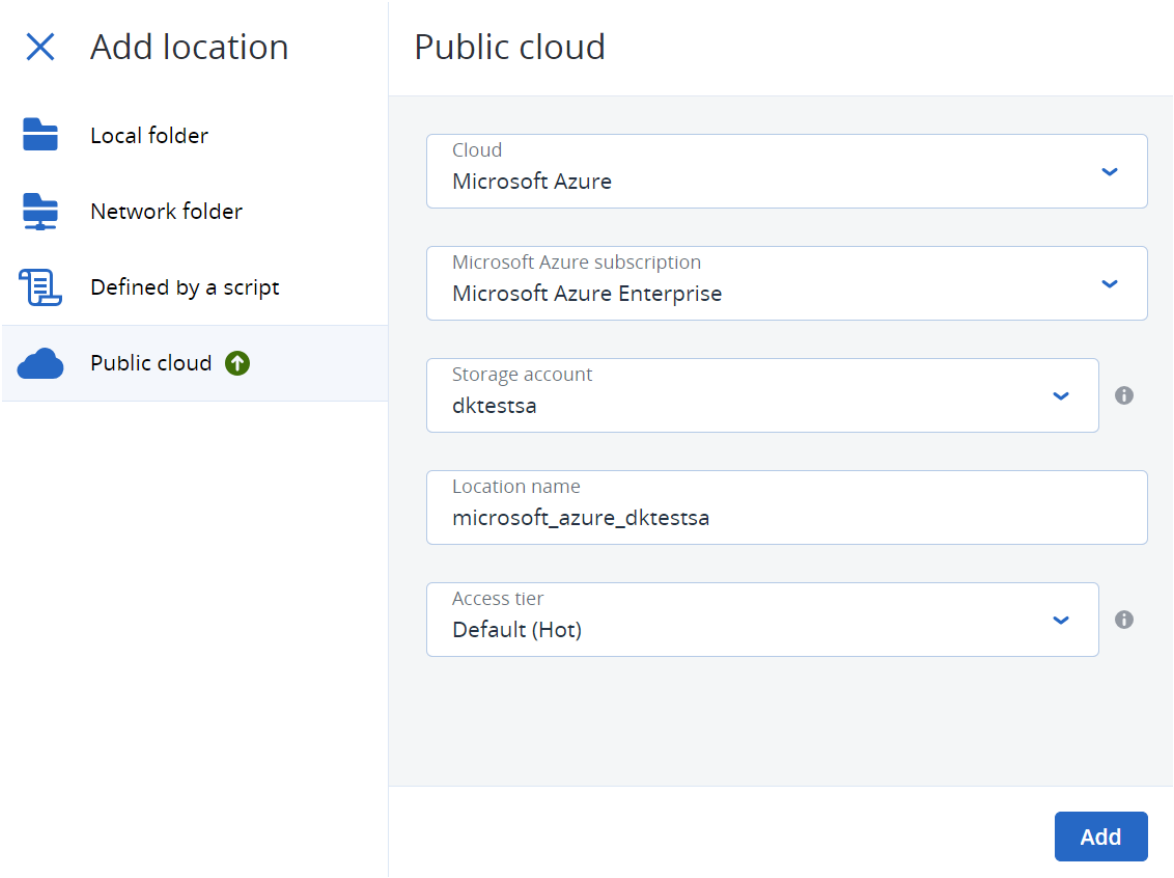
관련 구독이 Cyber Protect 콘솔에 등록되어 있지 않다면 **추가**를 클릭하고 표시되는 대화 상자에서 **로그인**을 클릭합니다. 그러면 Microsoft 로그인 페이지로 리디렉션됩니다. Microsoft Azure 구독 액세스 권한을 추가 및 정의하는 방법에 대한 자세한 내용은 "Microsoft Azure 구독 액세스 권한 추가"(502페이지) 항목을 참조하십시오.

5. **스토리지 계정** 필드에서 관련 계정을 선택합니다.

참고
현재는 `core.windows.net`을 포함하는 일반 엔드포인트 접미부가 있는 Microsoft Azure 스토리지 계정만 지원됩니다. 그리고 선택한 스토리지 계정은 StorageV2 계정 유형이어야 합니다.

선택한 스토리지 계정에 따라 **위치 이름** 및 **액세스 계층** 필드에는 값이 기본적으로 자동 입력됩니다. 표시되는 위치 이름은 `microsoft_azure_[스토리지 계정]`, 선택되는 액세스 계층은 **기본(핫)**입니다. 필요한 경우 두 필드의 내용을 모두 수정할 수 있습니다.

참고
위치 이름을 변경할 때는 고유한 위치 이름을 입력합니다. 즉, 고객 테넌트에서 고유한 이름을 입력해야 합니다. 추가하는 이름이 스토리지 계정에 이미 있으면 Acronis에서 이름에 접미부로 숫자를 추가합니다. 예를 들어 **Microsoft Azure Storage**라는 이름이 이미 있으면 **Microsoft Azure Storage_01**로 이름이 자동 업데이트됩니다.



6. **추가**를 클릭합니다.

© Acronis International GmbH, 2003-2024

보호 계획을 생성하거나 편집하는 경우 **백업할 위치** 행에서 Microsoft Azure 백업 위치가 위치로 설정됩니다. 백업이 수동으로 실행되거나 스케줄에 따라 실행되면 정의된 위치에 백업이 저장됩니다.

백업 스토리지 위치를 관리하는 경우에는 필요에 따라 위치 상세 정보를 확인하고 업데이트할 수 있습니다. 워크로드용 백업 위치를 정의할 때도 Microsoft Azure 위치를 사용할 수 있습니다. 자세한 내용은 "퍼블릭 클라우드 백업 위치 확인 및 업데이트"(497페이지) 항목을 참조하십시오.

Amazon S3에서 백업 위치 정의

참고
Amazon S3에서 백업 위치를 구성하려면 Cyber Protection 서비스에서 회사 관리자, 사용자, Cyber 관리자 역할 중 하나를 정의해야 합니다.

Amazon S3에 워크로드를 백업하려면 Cyber Protect 콘솔에서 Amazon S3 백업 위치를 정의한 후 관련 Amazon S3 연결에 연결해야 합니다. 이 작업은 다음과 같이 수행할 수 있습니다.

- 보호 계획 생성 또는 편집 시.
- 백업 스토리지 위치 정의 및 관리 시.

중요
관리자와 관리자가 아닌 사용자가 모두 Amazon S3에 워크로드를 백업할 수 있습니다.

관리자가 아닌 사용자도 Amazon S3 연결 액세스 권한을 추가할 수 있지만("다른 퍼블릭 클라우드 스토리지 서비스 액세스 관리"(505페이지) 항목 참조) Cyber Protect 콘솔에 본인 이름으로 등록된 워크로드에 한해 본인이 추가한 Amazon S3 연결에 백업 위치가 연결되어 있는 보호 계획만 적용할 수 있습니다.

관리자는 Cyber Protect 콘솔에 등록되어 있는 워크로드(워크로드가 등록된 사용자는 관계없음)를 대상으로 다른 관리자가 추가한 구독이나 본인이 추가한 Amazon S3 연결에 백업 위치가 연결되어 있는 보호 계획을 적용할 수 있습니다.

Amazon S3에서 백업 위치를 정의하려면

1. Cyber Protect 콘솔에서 다음 중 하나를 수행합니다.
   - 보호 계획을 생성하거나 편집하는 경우 **장치**로 이동하여 Amazon S3에 백업하려는 워크로드를 선택합니다. 그런 다음 선택한 워크로드의 보호 계획 내 **백업** 섹션에서 **백업할 위치** 행의 링크를 클릭합니다.

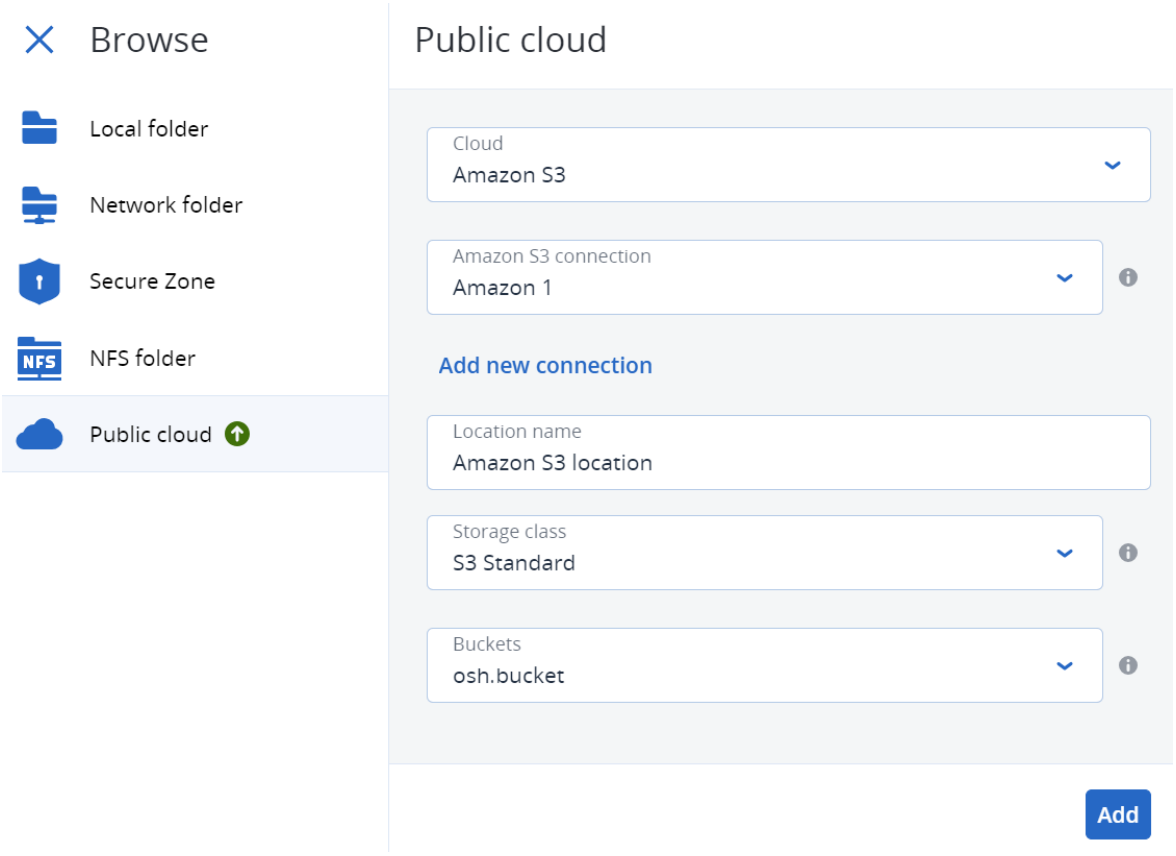
     보호 계획 사용에 대한 자세한 내용은 "보호 계획 및 모듈"(199페이지) 항목을 참조하십시오.
   - 백업 스토리지 위치 관리 시 새 위치로 Amazon S3를 추가하는 경우에는 **백업 스토리지**로 이동합니다.

     백업 스토리지 위치 관리에 대한 자세한 내용은 "백업 스토리지 탭"(480페이지) 항목을 참조하십시오.
2. **위치 추가**를 클릭합니다.

© Acronis International GmbH, 2003-2024

3. **퍼블릭 클라우드** 드롭다운 목록에서 **Amazon S3**를 선택합니다.
4. 관련 Amazon S3 연결이 Cyber Protect 콘솔에 이미 등록되어 있다면 목록에서 해당 연결을 선택합니다.

   관련 연결이 Cyber Protect 콘솔에 등록되어 있지 않으면 **새 연결 추가**를 클릭합니다. Amazon S3 연결 액세스 권한을 추가하고 정의하는 방법에 대한 자세한 내용은 "퍼블릭 클라우드 연결 액세스 권한 추가"(505페이지) 항목을 참조하십시오. 연결이 추가되면 다음 단계를 계속 진행합니다.



5. 다음 항목을 정의합니다.
   - **위치 이름** 필드에 백업 위치의 이름을 입력합니다.

     참고
     해당 고객 테넌트에서 고유한 위치 이름을 입력해야 합니다. 연결에서 이미 사용 중인 이름을 입력하면 Acronis에서 이름에 접미사 번호를 추가합니다. 예를 들어 **Amazon S3 스토리지**라는 이름이 이미 있으면 입력한 이름이 **Amazon S3 스토리지 1**로 자동 업데이트됩니다.

   - **스토리지 클래스** 필드에서 다음의 지원되는 스토리지 클래스 중 하나를 선택합니다.
     - S3 Standard
     - Standard - Infrequent Access(S3 Standard-IA)
     - One Zone - Infrequent Access(S3 One Zone-IA)
     - S3 Intelligent Tiering
   - **버킷** 필드에서 관련 Amazon S3 버킷을 선택합니다.
6. **추가**를 클릭합니다.

© Acronis International GmbH, 2003-2024

보호 계획을 생성하거나 편집하는 경우 Amazon S3 백업 위치가 **백업할 위치** 행의 위치로 설정됩니다. 그러면 백업을 수동으로 실행하거나 스케줄에 따라 실행할 때 정의된 위치에 백업이 저장됩니다.

백업 스토리지 위치를 관리하는 경우에는 필요에 따라 위치 상세 정보를 확인하고 업데이트할 수 있습니다. 워크로드용 백업 위치를 정의할 때도 Amazon S3 위치를 사용할 수 있습니다. 자세한 내용은 "퍼블릭 클라우드 백업 위치 확인 및 업데이트"(497페이지) 항목을 참조하십시오.

Wasabi에서 백업 위치 정의

참고
Wasabi에서 백업 위치를 구성하려면 Cyber Protection 서비스에서 회사 관리자, 사용자, Cyber 관리자 역할 중 하나를 정의해야 합니다.

Wasabi에 워크로드를 백업하려면 Cyber Protect 콘솔에서 Wasabi 백업 위치를 정의한 후 관련 Wasabi 연결에 연결해야 합니다. 이 작업은 다음과 같이 수행할 수 있습니다.

- 보호 계획 생성 또는 편집 시.
- 백업 스토리지 위치 정의 및 관리 시.

중요
관리자와 관리자가 아닌 사용자가 모두 Wasabi에 워크로드를 백업할 수 있습니다.

관리자가 아닌 사용자도 Wasabi 연결 액세스 권한을 추가할 수 있지만("다른 퍼블릭 클라우드 스토리지 서비스 액세스 관리"(505페이지) 항목 참조) Cyber Protect 콘솔에 본인 이름으로 등록된 워크로드에 한해 본인이 추가한 Wasabi 연결에 백업 위치가 연결되어 있는 보호 계획만 적용할 수 있습니다.

관리자는 Cyber Protect 콘솔에 등록되어 있는 워크로드(워크로드가 등록된 사용자는 관계없음)를 대상으로 다른 관리자가 추가한 구독이나 본인이 추가한 Wasabi 연결에 백업 위치가 연결되어 있는 보호 계획을 적용할 수 있습니다.

Wasabi에서 백업 위치를 정의하려면

1. Cyber Protect 콘솔에서 다음 중 하나를 수행합니다.
   - 보호 계획을 생성하거나 편집하는 경우 **장치**로 이동하여 Wasabi에 백업하려는 워크로드를 선택합니다. 그런 다음 선택한 워크로드의 보호 계획 내 **백업** 섹션에서 **백업할 위치** 행의 링크를 클릭합니다.

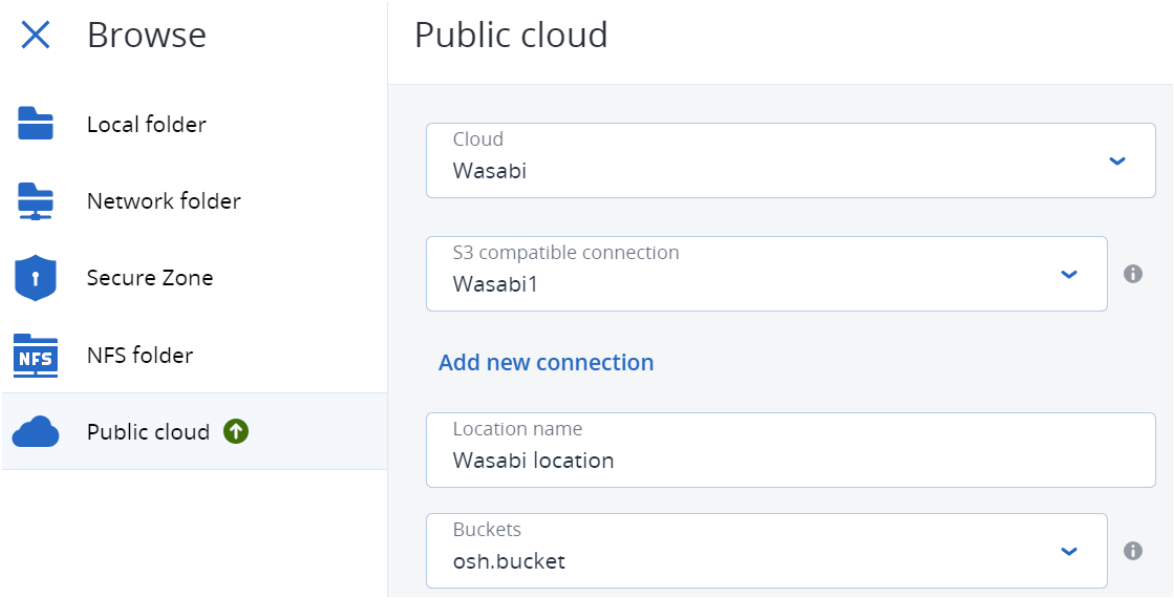
     보호 계획 사용에 대한 자세한 내용은 "보호 계획 및 모듈"(199페이지) 항목을 참조하십시오.
   - 백업 스토리지 위치 관리 시 새 위치로 Wasabi를 추가하는 경우에는 **백업 스토리지**로 이동합니다.

     백업 스토리지 위치 관리에 대한 자세한 내용은 "백업 스토리지 탭"(480페이지) 항목을 참조하십시오.
2. **위치 추가**를 클릭합니다.
3. **퍼블릭 클라우드** 드롭다운 목록에서 **Wasabi**를 선택합니다.

© Acronis International GmbH, 2003-2024

4. 관련 Wasabi 연결이 Cyber Protect 콘솔에 이미 등록되어 있다면 연결 목록에서 해당 연결을 선택합니다.

   관련 연결이 Cyber Protect 콘솔에 등록되어 있지 않으면 **새 연결 추가**를 클릭합니다. Wasabi 연결 액세스 권한을 추가하고 정의하는 방법에 대한 자세한 내용은 "퍼블릭 클라우드 연결 액세스 권한 추가"(505페이지) 항목을 참조하십시오. 연결이 추가되면 다음 단계를 계속 진행합니다.



5. 다음 항목을 정의합니다.
   - **위치 이름** 필드에 백업 위치의 이름을 입력합니다.

     참고
     해당 고객 테넌트에서 고유한 위치 이름을 입력해야 합니다. 연결에서 이미 사용 중인 이름을 입력하면 Acronis에서 이름에 접미사 번호를 추가합니다. 예를 들어 **Wasabi 스토리지**라는 이름이 이미 있으면 입력한 이름이 **Wasabi 스토리지 1**로 자동 업데이트됩니다.

   - **버킷** 필드에서 관련 Wasabi 버킷을 선택합니다.
6. **추가**를 클릭합니다.

   보호 계획을 생성하거나 편집하는 경우 Wasabi 백업 위치가 **백업할 위치** 행의 위치로 설정됩니다. 그러면 백업을 수동으로 실행하거나 스케줄에 따라 실행할 때 정의된 위치에 백업이 저장됩니다.

   백업 스토리지 위치를 관리하는 경우에는 필요에 따라 위치 상세 정보를 확인하고 업데이트할 수 있습니다. 워크로드용 백업 위치를 정의할 때도 Wasabi 위치를 사용할 수 있습니다. 자세한 내용은 "퍼블릭 클라우드 백업 위치 확인 및 업데이트"(497페이지) 항목을 참조하십시오.

퍼블릭 클라우드 백업 위치 확인 및 업데이트

정의한 Microsoft Azure, Amazon S3 및 Wasabi 백업 위치는 **백업 스토리지** 모듈에서 확인 및 업데이트할 수도 있고 보호 계획을 생성하거나 편집할 때 확인 및 업데이트할 수도 있습니다.

© Acronis International GmbH, 2003-2024

Cyber Protect 콘솔에서 Microsoft Azure 구독 액세스 권한을 제거하는 방법에 대한 내용은 "Microsoft Azure 구독 액세스 권한 제거"(504페이지) 항목을 참조하십시오. 다른 퍼블릭 클라우드 연결 액세스 권한을 제거하는 방법에 대한 내용은 "다른 퍼블릭 클라우드 스토리지 서비스 액세스 관리"(505페이지) 항목을 참조하십시오.

참고
백업 스토리지 모듈에서 퍼블릭 클라우드 백업 위치를 수동으로 새로 고치거나 삭제할 수는 없습니다. 백업 위치의 내용은 각 백업 또는 복구 작업 후 자동 업데이트됩니다.

퍼블릭 클라우드 백업 위치를 확인하려면

1. Cyber Protect 콘솔에서 **백업 스토리지**로 이동합니다.
   백업 위치 목록, 그리고 각 위치에 할당된 백업 수와 스토리지 용량 관련 상세 정보가 표시됩니다.
   목록에 포함된 백업 위치 사용 방법에 대한 자세한 내용은 "백업 스토리지 탭"(480페이지) 항목을 참조하십시오.
2. 관련 위치를 선택합니다.
   선택한 위치의 현재 백업이 모두 나열됩니다.
3. (선택 사항) 원하는 백업을 클릭하여 추가 상세 정보를 확인합니다.

보호 계획에서 퍼블릭 클라우드 백업 위치를 업데이트하려면

1. 관련 보호 계획으로 이동한 후 **편집**을 선택합니다.
2. **백업할 위치** 행에서 링크를 클릭합니다.
3. 기존 백업 위치 목록에서 원하는 위치를 선택하거나 **위치 추가**를 클릭하여 새 위치를 추가합니다.
   관련 Microsoft Azure 구독 또는 퍼블릭 클라우드 연결이 Cyber Protect 콘솔에 이미 등록되어 있으면 표시되는 목록에서 해당 연결을 선택합니다.
   새 Microsoft Azure 구독을 추가하는 경우에는 Microsoft 계정 상세 정보를 인증하라는 메시지가 표시됩니다("Microsoft Azure 구독 액세스 권한 추가"(502페이지) 항목 참조). Microsoft Azure에 연결할 때 필요한 권한에 대한 자세한 내용은 Microsoft Azure 연결 보안 및 감사(72684) 문서를 참조하십시오.

퍼블릭 클라우드 계정 액세스 관리

퍼블릭 클라우드 플랫폼에서 Acronis Cyber Protection 서비스를 활성화하려면 관련 퍼블릭 클라우드 계정에 대한 액세스를 구성해야 합니다.

예를 들어 Microsoft Azure 사용 시에는 Microsoft Azure 구독 액세스 권한이 필요합니다. Cyber Protect 콘솔에 추가한 구독은 Microsoft Azure로의 직접 백업을 설정할 때 선택 가능합니다. 마찬가지로 Amazon S3 및 Wasabi 사용 시에는 특정 백업 관련 정책과 연결된 관련 액세스 키가 필요합니다.

콘솔의 **인프라** 메뉴를 통해 퍼블릭 클라우드 액세스를 관리할 수 있습니다.

© Acronis International GmbH, 2003-2024

중요
과도한 송신 트래픽 비용 방지를 위해 퍼블릭 클라우드 스토리지의 백업에서는 백업 유효성 검사가 비활성화됩니다. 그리고 현재는 퍼블릭 클라우드에서 이전에 제거했던 백업 위치를 동일 고객 테넌트나 다른 고객 테넌트에 "다시 연결"할 수 없습니다. 자세한 내용은 지원 팀에 문의하십시오.

퍼블릭 클라우드 스토리지에 백업하려면 충족해야 하는 액세스 요구 사항

퍼블릭 클라우드 스토리지 서비스에 직접 백업할 때는 각 플랫폼별로 여러 가지 액세스 요구 사항을 고려해야 합니다.

- Microsoft Azure
- Amazon S3
- Wasabi

Microsoft Azure에 백업

Microsoft Azure 구독에 연결하려면 여러 가지 권한이 필요합니다. 이러한 권한에 대한 자세한 내용은 Microsoft Azure 연결 보안 및 감사(72684) 문서를 참조하십시오.

Amazon S3에 백업

Amazon S3에 백업하는 경우에는 Amazon S3 백업 위치를 정의할 때 여러 가지 요구 사항을 고려해야 합니다.

- 지원되는 스토리지 클래스
- 정책 권한
- 액세스 키
- 버킷 설정

지원되는 스토리지 클래스

현재 지원되는 Amazon S3 스토리지 클래스는 다음과 같습니다.

- S3 Standard
- Standard - Infrequent Access(S3 Standard-IA)
- One Zone - Infrequent Access(S3 One Zone-IA)
- S3 Intelligent Tiering

정책 권한

Amazon S3에 백업할 때는 Amazon 계정에 최소 권한이 적용되어 있어야 아크로니스가 Amazon S3에 관련 워크로드를 백업할 수 있습니다. 즉, 관련 사용자에게 AWS 관리 콘솔 액세스 권한이 있어야 하며 사용자가 할당된 그룹에 관련 정책이 적용되어 있어야 합니다.

예

© Acronis International GmbH, 2003-2024

다음 예제 정책에는 광범위한 리소스에 적용되는 최소 권한 집합이 나와 있습니다. *는 모든 리소스를 나타냅니다.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:GetBucketObjectLockConfiguration" ], "Resource": "*" },
{ "Effect": "Allow", "Action": "sts:GetFederationToken", "Resource": "*" }, {
"Effect": "Allow", "Action": [ "s3:GetBucketLocation", "s3:PutObject",
"s3:GetObject", "s3:DeleteObject" ], "Resource": "*" }, { "Effect": "Allow",
"Action": [ "s3:ListBucket" ], "Resource": "*" } ] }
```

다음 예제 정책에는 특정 버킷에만 적용되는 최소 권한이 나와 있습니다. [BUCKETNAME]은 버킷 이름으로 바꿔야 합니다.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:GetBucketObjectLockConfiguration" ], "Resource":
"arn:aws:s3:::[BUCKETNAME]" }, { "Effect": "Allow", "Action":
"sts:GetFederationToken", "Resource": "*" }, { "Effect": "Allow", "Action": [
"s3:GetBucketLocation", "s3:PutObject", "s3:GetObject", "s3:DeleteObject" ],
"Resource": "arn:aws:s3:::[BUCKETNAME]/*" }, { "Effect": "Allow", "Action": [
"s3:ListBucket" ], "Resource": "arn:aws:s3:::[BUCKETNAME]" } ] }
```

액세스 키

아크로니스가 각 Amazon S3 연결에 액세스하려면 액세스 키가 필요합니다. 해당 키는 Amazon S3 연결 정의 시에 사용됩니다. 액세스 키와 액세스 키 ID를 생성하는 방법에 대한 자세한 내용은 Amazon S3 설명서를 참조하십시오.

버킷 설정

Amazon S3 버킷을 백업 위치로 사용할 때는 기본 설정으로 버킷을 구성해야 하며 모든 퍼블릭 액세스를 차단해야 합니다(퍼블릭 액세스 차단은 **켜기**로 기본 설정됨). 버킷 사용 방법에 대한 자세한 내용은 Amazon S3 설명서를 참조하십시오.

참고

아크로니스는 현재 Amazon S3에서 버킷 버전 관리와 오브젝트 잠금을 지원하지 않습니다. 버킷에서 이러한 옵션을 활성화하는 경우에도 마찬가지입니다.

Wasabi에 백업

Wasabi에 백업하는 경우 백업 위치를 정의할 때 여러 가지 요구 사항을 고려해야 합니다.

- 정책 권한
- 액세스 키
- 버킷 설정

© Acronis International GmbH, 2003-2024

정책 권한

Wasabi에서 백업 위치를 정의할 때는 Wasabi의 관련 관련 그룹과 사용자에게 관련 정책을 적용해야 합니다.

예

다음 예제 정책에는 광범위한 리소스에 적용되는 최소 권한 집합이 나와 있습니다.*는 모든 리소스를 나타냅니다.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action":
"s3:GetBucketLocation", "Resource": "*" }, { "Effect": "Allow", "Action": [
"iam:CreateRole", "iam:AttachRolePolicy", "sts:GetCallerIdentity", "sts:AssumeRole"
], "Resource": "*" }, { "Effect": "Allow", "Action": [ "s3:PutObject",
"s3:GetObject", "s3:DeleteObject" ], "Resource": "*" }, { "Effect": "Allow",
"Action": "s3:ListBucket", "Resource": "*" } ] }
```

다음 예제 정책에는 제한된 리소스 범위에 적용되는 제한적인 권한이 나와 있습니다.[BUCKETNAME]은 버킷 이름으로,[ACCOUNTID]는 Wasabi 계정의 ID로 바꿔야 합니다.

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action":
"s3:ListAllMyBuckets", "Resource": "*" }, { "Effect": "Allow", "Action":
"s3:GetBucketLocation", "Resource": "arn:aws:s3:::[BUCKETNAME]" }, { "Effect":
"Allow", "Action": [ "iam:CreateRole", "iam:AttachRolePolicy",
"sts:GetCallerIdentity", "sts:AssumeRole" ], "Resource": "arn:aws:iam::
[ACCOUNTID]:*" }, { "Effect": "Allow", "Action": [ "s3:PutObject", "s3:GetObject",
"s3:DeleteObject" ], "Resource": "arn:aws:s3:::[BUCKETNAME]/*" }, { "Effect":
"Allow", "Action": "s3:ListBucket", "Resource": "arn:aws:s3:::[BUCKETNAME]" } ] }
```

액세스 키

아크로니스가 각 Wasabi 연결에 액세스하려면 액세스 키가 필요합니다. 해당 키는 Wasabi 연결 정의 시에 사용됩니다. 액세스 키와 액세스 키 ID를 생성하는 방법에 대한 자세한 내용은 Wasabi 설명서를 참조하십시오.

버킷 설정

Wasabi 버킷을 백업 위치로 사용하는 경우에는 기본 설정으로 버킷을 구성해야 합니다. 버킷 사용 방법에 대한 자세한 내용은 Wasabi 설명서를 참조하십시오.

참고

아크로니스는 현재 Wasabi에서 버킷 버전 관리와 오브젝트 잠금을 지원하지 않습니다. 버킷에서 이러한 옵션을 활성화하는 경우에도 마찬가지입니다.

© Acronis International GmbH, 2003-2024

Microsoft Azure 구독 액세스 관리

Cyber Protect 콘솔에서 관련 Microsoft Azure 구독에 연결하면 Microsoft Azure에 관련 워크로드를 직접 백업할 수 있습니다.

항목의 설명에 따라 **장치** 또는 **백업 스토리지** 메뉴를 통해 백업 위치를 생성할 때 구독 연결을 구성할 수 있습니다.

인프라 > 퍼블릭 클라우드로 이동하면 표시되는 **퍼블릭 클라우드** 화면에서 이러한 Microsoft Azure 구독을 구성할 수도 있습니다. 이 화면에서는 구독 액세스 권한 갱신, 구독의 속성과 구독 관련 작업 확인, 구독 제거 등의 구독 관리 작업도 수행할 수 있습니다.

할당된 사용자 역할에 따라서는 조직 내 다른 사용자가 추가한 Microsoft Azure 구독 관리가 가능할 수 있습니다. 예를 들어 회사 관리자 또는 단위 관리자이거나 Cyber Protection 서비스에서 Cyber 관리자 또는 관리자 역할이 할당되었다면 다른 관리자가 추가한 Microsoft Azure 구독, 그리고 관리자가 아닌 사용자가 추가한 구독을 확인 및 관리할 수 있습니다. 관리자가 아닌 사용자의 경우 본인이 Cyber Protect 콘솔에 추가한 Microsoft Azure 구독 확인 및 액세스만 가능합니다.

참고
파트너는 조직 계층 내에서 본인보다 수준이 낮은 고객의 Microsoft Azure 구독을 관리할 수 있습니다. 그러나 파트너가 **모든 고객**을 선택하면 콘솔에서 **인프라** 메뉴가 제공되지 않습니다.

중요
Microsoft Azure 구독에 연결할 때 Acronis에는 구독 연결을 위한 최소 권한이 필요하다는 메시지가 표시됩니다. 필요한 권한에 대한 자세한 내용은 Microsoft Azure 연결 보안 및 감사(72684) 문서를 참조하십시오.

Microsoft Azure 구독 액세스 권한 추가

Cyber Protect 콘솔에서 Microsoft Azure 구독을 추가하면 Acronis에서 구독에 안전하게 액세스하여 Microsoft Azure에 관련 워크로드를 직접 백업할 수 있습니다.

Microsoft Azure 구독 액세스 권한을 추가하려면

1. Cyber Protect 콘솔에서 **인프라 > 퍼블릭 클라우드**로 이동합니다.
2. **추가**를 클릭한 후 표시되는 옵션 목록에서 **Microsoft Azure**를 선택합니다.
3. 표시되는 대화 상자에서 **로그인**을 클릭합니다. 그러면 Microsoft 로그인 페이지로 리디렉션됩니다.

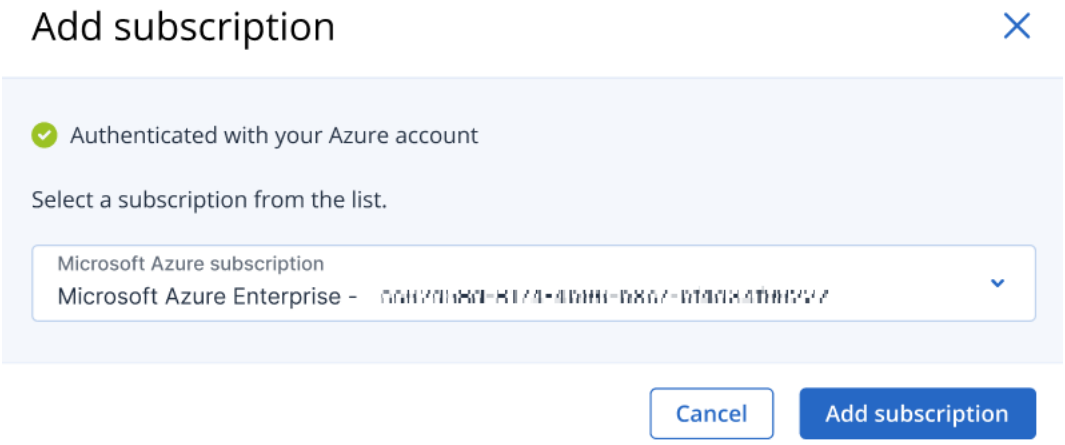
   참고
   구독 연결을 완료하려면 Microsoft Azure AD에서 다음 역할 중 하나가 할당되어 있어야 합니다. 클라우드 애플리케이션 관리자, 애플리케이션 관리자 또는 전역 관리자 역할 중 하나가 할당되어 있어야 합니다. 그리고 선택한 각 구독의 소유자 역할도 할당되어 있어야 합니다.

4. Microsoft 로그인 화면에서 로그인 자격 증명을 입력하고 권한 요청을 승인합니다. 연결 프로세스가 시작됩니다. 이 프로세스는 몇 분 정도 걸릴 수 있습니다.

© Acronis International GmbH, 2003-2024

Microsoft Azure 및 구독에 안전하게 액세스하는 방법에 대한 자세한 내용은 Microsoft Azure 연결 보안 및 감사(72684) 문서를 참조하십시오.

5. 연결이 완료되면 표시되는 대화 상자의 드롭다운 목록에서 관련 구독을 선택하고 **구독 추가**를 클릭합니다.



구독이 퍼블릭 클라우드 목록에 추가됩니다.

구독의 연간 액세스 인증서를 갱신하려면 "Microsoft Azure 구독 액세스 권한 갱신"(503페이지) 항목을 참조하십시오.

구독 액세스 권한을 제거하려면 "Microsoft Azure 구독 액세스 권한 제거"(504페이지) 항목을 참조하십시오.

참고
로그인되어 있는 Microsoft Azure 계정에서 여러 Microsoft Azure AD(게스트 사용자로 초대를 받은 AD 포함)에 액세스할 수 있는 경우에는 기본 사용자 디렉터리만 선택됩니다. 본인이 게스트 사용자인 디렉토리를 사용하려는 경우에는 해당 Microsoft Azure AD에서 새 사용자를 생성해야 합니다. 그러고 나면 해당 계정에 로그인하여 관련 구독에 연결할 수 있습니다.

Microsoft Azure 구독 액세스 권한 갱신

Cyber Protect 콘솔에서 Microsoft Azure 구독 액세스 권한을 등록하면 Acronis에서 고유한 무료 액세스 인증서를 사용하여 1년 동안 구독에 액세스 가능하도록 자동으로 설정합니다. 인증서의 만료 날짜가 임박하면 빠르고 쉽게 인증서를 갱신할 수 있습니다.

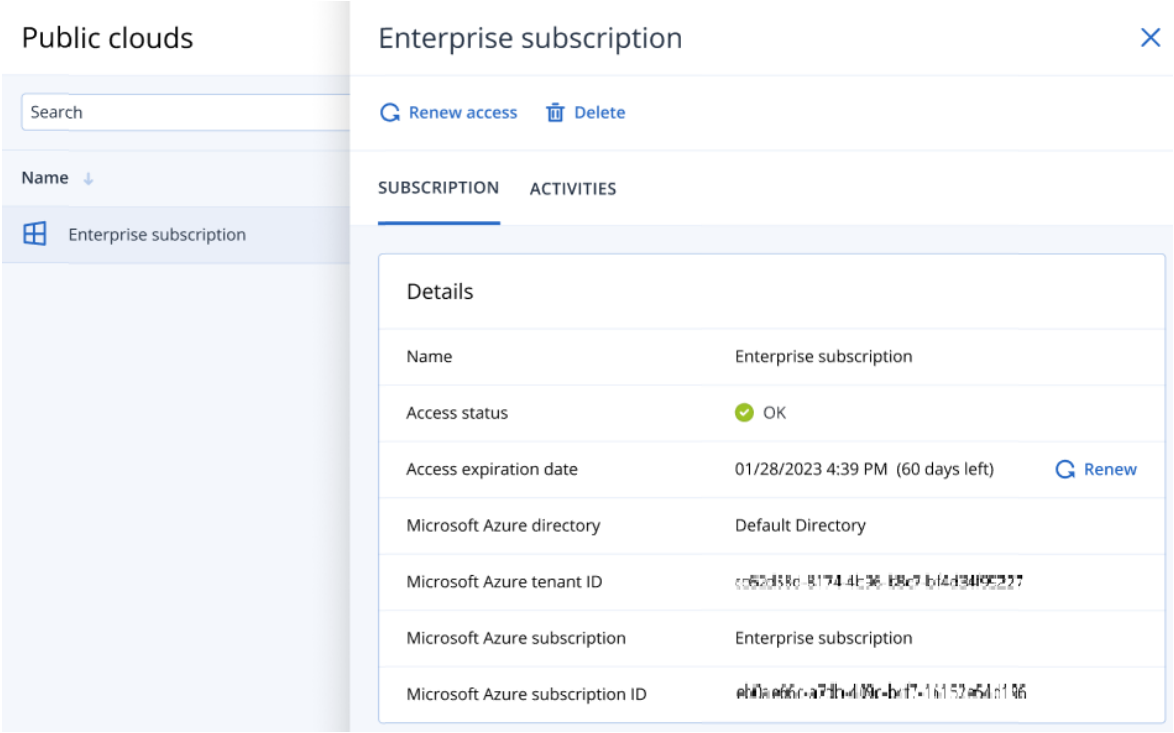
Microsoft Azure 구독의 액세스 인증서를 갱신하려면

1. Cyber Protect 콘솔에서 **인프라 > 퍼블릭 클라우드**로 이동합니다.
2. 표시되는 목록에서 관련 구독을 선택합니다.

참고
액세스 상태 열에 각 구독용 액세스 인증서의 현재 상태가. **정상** 또는 **만료됨** 중 하나로 표시됩니다.

3. 오른쪽 창에서 **액세스 갱신**을 클릭합니다.
구독 탭을 클릭한 다음 **액세스 만료 날짜** 필드에서 **갱신**을 클릭해도 됩니다.

© Acronis International GmbH, 2003-2024



4. Microsoft 로그인 화면에서 로그인 자격 증명을 입력하고 권한 요청을 승인합니다. 연결 프로세스가 시작됩니다. 이 프로세스는 몇 분 정도 걸릴 수 있습니다.
   인증이 정상적으로 완료되면 액세스 권한이 1년 자동 갱신됩니다.
   필요한 권한에 대한 자세한 내용은 Microsoft Azure 연결 보안 및 감사(72684) 문서를 참조하십시오.

Microsoft Azure 구독 액세스 권한 제거

Microsoft Azure에 워크로드를 백업하지 않는다면 Microsoft Azure 구독 액세스 권한을 제거해야 합니다.

Microsoft Azure 구독 액세스 권한을 제거하려면

중요
현재 Microsoft Azure용 백업으로 사용 중인 구독은 제거할 수 없습니다.

1. Cyber Protect 콘솔에서 **인프라 > 퍼블릭 클라우드**로 이동합니다.
2. 표시되는 목록에서 관련 구독을 선택합니다.
3. 오른쪽 창에서 **삭제**를 클릭합니다.

   참고
   본인이 추가한 구독만 제거할 수 있습니다. 회사 관리자이거나 부서 관리자인 경우 또는 Cyber Protection 서비스에서 Cyber 관리자 또는 관리자 역할을 할당받은 경우에도 구독을 제거할 수 있습니다.

4. 표시되는 확인 메시지에서 **제거**를 클릭합니다.

© Acronis International GmbH, 2003-2024

다른 퍼블릭 클라우드 스토리지 서비스 액세스 관리

참고
이 섹션에서는 Microsoft Azure를 제외한 모든 퍼블릭 클라우드 스토리지 서비스 액세스를 관리할 수 있습니다. Microsoft Azure 액세스 관리 방법은 "Microsoft Azure 구독 액세스 관리"(502페이지) 항목에 설명되어 있습니다.

Cyber Protect 콘솔에서 관련 퍼블릭 클라우드 계정에 연결하면 관련 퍼블릭 클라우드 스토리지에 워크로드를 직접 백업할 수 있습니다.

장치 또는 **백업 스토리지** 메뉴를 통해 백업 위치를 생성할 때 퍼블릭 클라우드 스토리지 계정으로의 연결을 구성할 수 있습니다. **퍼블릭 클라우드** 화면에서 **인프라 > 퍼블릭 클라우드**로 이동하여 퍼블릭 클라우드 연결을 구성할 수도 있습니다. 연결 액세스 권한 갱신, 연결 속성 및 연결 관련 활동 확인, 연결 제거 등의 연결 관리 작업도 이 화면에서 수행할 수 있습니다.

할당된 사용자 역할에 따라서는 조직 내 다른 사용자가 추가한 퍼블릭 클라우드 연결 관리가 가능할 수 있습니다. 예를 들어 회사 관리자 또는 단위 관리자이거나 Cyber Protection 서비스에서 Cyber 관리자 또는 관리자 역할이 할당되었다면 다른 관리자가 추가한 퍼블릭 클라우드 연결, 그리고 관리자가 아닌 사용자가 추가한 연결을 확인 및 관리할 수 있습니다. 관리자가 아닌 사용자의 경우 본인이 Cyber Protect 콘솔에 추가한 퍼블릭 클라우드 연결 확인 및 액세스만 가능합니다.

참고
파트너는 계층 구조 내 하위 수준 고객의 퍼블릭 클라우드 연결을 관리할 수 있습니다. 그러나 파트너가 **모든 고객**을 선택하면 콘솔에서 **인프라** 메뉴가 제공되지 않습니다.

중요
Acronis에서 퍼블릭 클라우드 연결에 연결할 때는 여러 가지 권한이 필요합니다. 자세한 내용은 "퍼블릭 클라우드 스토리지에 백업하려면 충족해야 하는 액세스 요구 사항"(499페이지) 항목을 참조하십시오.

퍼블릭 클라우드 연결 액세스 권한 추가

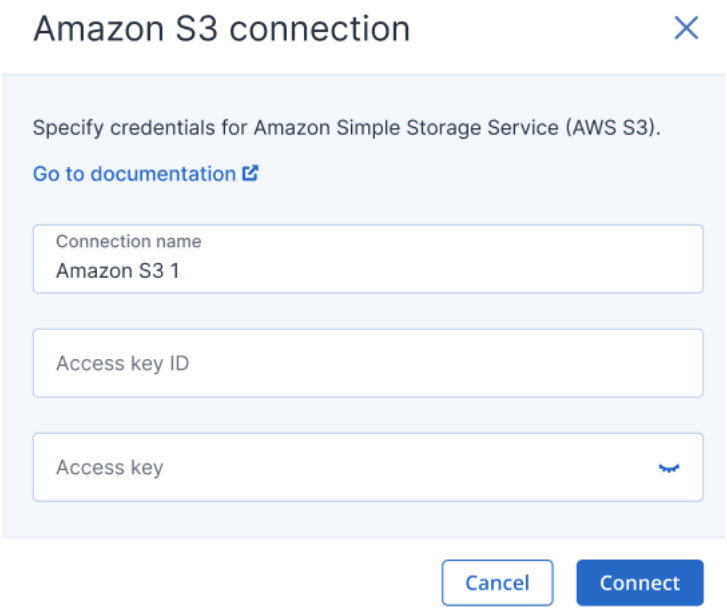
Amazon S3 또는 Wasabi 등의 퍼블릭 클라우드 연결을 Cyber Protect 콘솔에 추가하고 나면 Acronis에서 클라우드 리소스에 안전하게 액세스하여 관련 퍼블릭 클라우드 스토리지에 워크로드를 직접 백업할 수 있습니다.

퍼블릭 클라우드 연결 액세스 권한을 추가하려면

1. Cyber Protect 콘솔에서 **인프라 > 퍼블릭 클라우드**로 이동합니다.
2. **추가**를 클릭하고 다음 옵션 중 하나를 선택합니다.
   - **Amazon S3**
     표시되는 대화 상자에서 다음 항목을 정의합니다.
     - **연결 이름**: Amazon S3 연결의 이름입니다.
     - **액세스 키 ID**: Amazon S3 서비스용 사용자 액세스 키 ID입니다.
     - **액세스 키**: Amazon S3 서비스용 사용자 액세스 키입니다.

© Acronis International GmbH, 2003-2024

액세스 키와 액세스 키 ID를 정의하면 아크로니스가 관련 연결의 스토리지 클래스와 버킷에 액세스할 수 있게 됩니다. 아크로니스가 사용해야 하는 액세스 키와 권한에 대한 자세한 내용은 "퍼블릭 클라우드 스토리지에 백업하려면 충족해야 하는 액세스 요구 사항" (499페이지) 항목을 참조하십시오.



- **Wasabi**

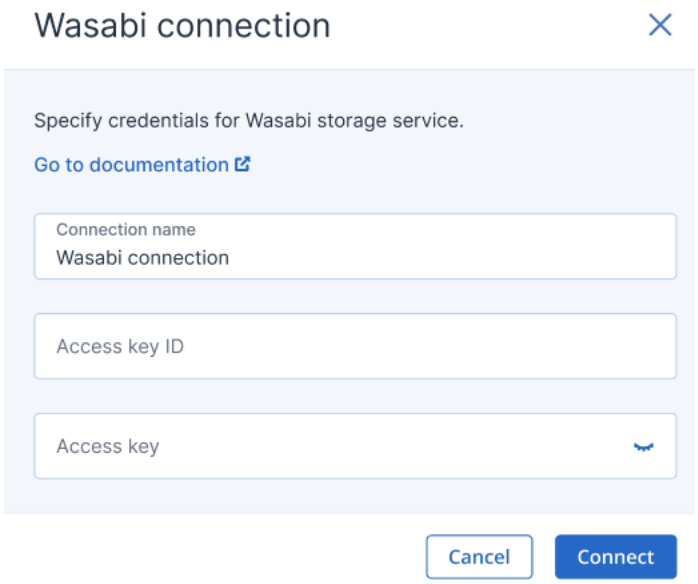
  표시되는 대화 상자에서 다음 항목을 정의합니다.

  - **연결 이름**: Wasabi 연결의 이름입니다.
  - **액세스 키 ID**: Wasabi 서비스용 사용자 액세스 키 ID입니다.
  - **액세스 키**: Wasabi 서비스용 사용자 액세스 키입니다.

    액세스 키와 액세스 키 ID를 정의하면 아크로니스가 관련 연결의 스토리지 클래스와 버킷에 액세스할 수 있게 됩니다. 아크로니스가 사용해야 하는 액세스 키와 권한에 대한 자세한 내용은 "퍼블릭 클라우드 스토리지에 백업하려면 충족해야 하는 액세스 요구 사항"

© Acronis International GmbH, 2003-2024

(499페이지) 항목을 참조하십시오.



3. **연결**을 클릭합니다.
   연결 프로세스가 시작됩니다. 이 프로세스는 몇 분 정도 걸릴 수 있습니다. 프로세스가 완료되면 퍼블릭 클라우드 목록에 연결이 추가됩니다.
   연결의 연간 액세스 인증서를 갱신하려면 "퍼블릭 클라우드 연결 액세스 권한 갱신"(507페이지) 항목을 참조하십시오.
   연결 액세스 권한을 제거하려면 "퍼블릭 클라우드 연결 액세스 권한 제거"(508페이지) 항목을 참조하십시오.

퍼블릭 클라우드 연결 액세스 권한 갱신

Cyber Protect 콘솔에 퍼블릭 클라우드 연결을 등록하고 나면 Acronis에서 고유한 무료 액세스 인증서를 자동 할당하므로 퍼블릭 클라우드 연결에 액세스할 수 있게 됩니다. 해당 인증서는 1년 동안 유효합니다. 만료일이 임박한 인증서는 갱신할 수 있습니다.

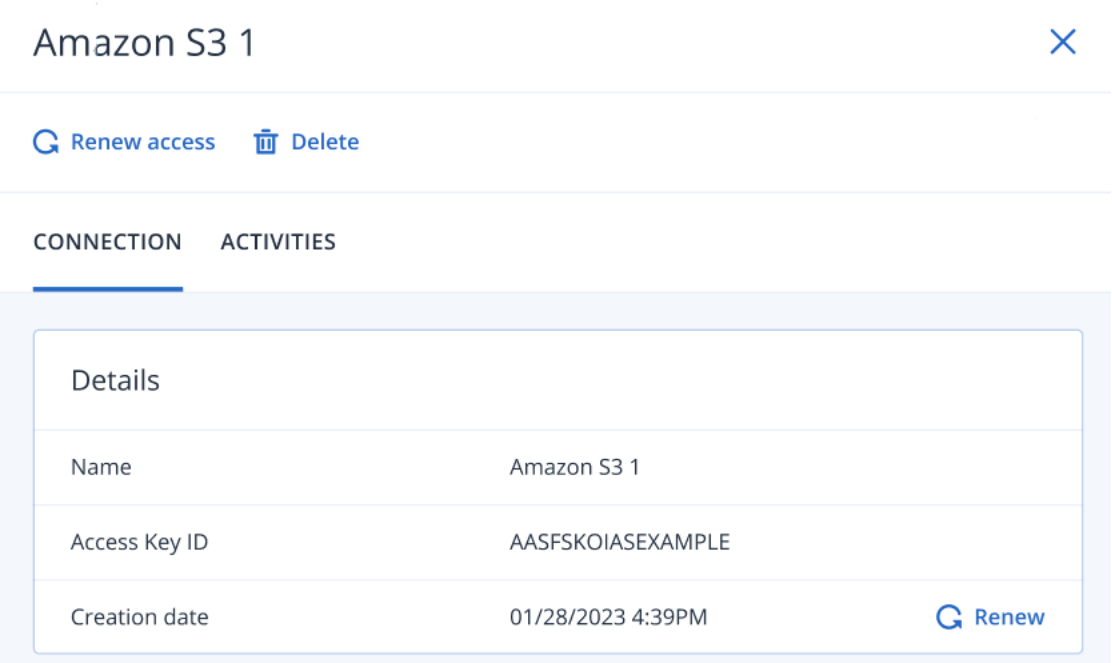
퍼블릭 클라우드 연결의 액세스 인증서를 갱신하려면

1. Cyber Protect 콘솔에서 **인프라 > 퍼블릭 클라우드**로 이동합니다.
2. 목록에서 관련 연결을 선택합니다.

> **참고**
> **액세스 상태** 열에 각 연결용 액세스 인증서의 현재 상태가 **정상** 또는 **만료됨** 중 하나로 표시됩니다.

3. 오른쪽 창에서 **액세스 갱신**을 클릭합니다.
   연결 탭을 클릭한 다음 **생성 날짜** 행에서 **갱신**을 클릭해도 됩니다.

© Acronis International GmbH, 2003-2024



인증이 정상적으로 완료되면 액세스 권한이 1년 자동 갱신됩니다.

퍼블릭 클라우드 연결 액세스 권한 제거

퍼블릭 클라우드에 워크로드를 백업하지 않는 경우에는 퍼블릭 클라우드 연결 액세스 권한을 제거해야 합니다.

퍼블릭 클라우드 연결 액세스 권한을 제거하려면

중요
현재 퍼블릭 클라우드로의 백업에 사용되고 있는 연결은 제거할 수 없습니다.

1. Cyber Protect 콘솔에서 **인프라 > 퍼블릭 클라우드**로 이동합니다.
2. 목록에서 연결을 선택합니다.
3. 오른쪽 창에서 **삭제**를 클릭합니다.

   참고
   본인이 추가한 연결만 제거할 수 있습니다. 회사 관리자이거나 단위 관리자인 경우 또는 Cyber Protection 서비스에서 Cyber 관리자 또는 관리자 역할을 할당받은 경우에도 연결을 제거할 수 있습니다.

4. 표시되는 확인 메시지에서 **삭제**를 클릭합니다.

© Acronis International GmbH, 2003-2024

Microsoft 애플리케이션 보호

Microsoft SQL Server 및 Microsoft Exchange Server 보호

참고
Microsoft SQL 백업은 NTFS, REFS, FAT32 파일 시스템에서 실행되는 데이터베이스에서만 지원됩니다. ExFat는 지원되지 않습니다.

Microsoft 애플리케이션을 보호하는 방법은 두 가지입니다:

- **데이터베이스 백업**
  이는 데이터베이스와 여기에 관련된 메타데이터의 파일 수준 백업을 말합니다. 데이터베이스는 라이브 애플리케이션으로 복구하거나 파일로 복구할 수 있습니다.
- **애플리케이션 인식 백업**
  이는 애플리케이션의 메타데이터도 수집하는 디스크 수준 백업을 말합니다. 이 메타데이터를 통해 전체 디스크 또는 볼륨을 복구하지 않고도 애플리케이션 데이터를 찾아 복구할 수 있습니다. 디스크나 볼륨을 전체적으로 복구할 수도 있습니다. 이는 단일 솔루션과 단일 보호 계획으로 재해 복구와 데이터 보호라는 두 가지 목적을 모두 충족할 수 있다는 의미입니다.

Microsoft Exchange Server의 경우 **사서함 백업**을 선택할 수 있습니다. 이는 Exchange 웹 서비스 프로토콜을 통해 수행된 개별 사서함의 백업입니다. 사서함 또는 사서함 항목은 라이브 Exchange Server 또는 Microsoft 365로 복구할 수 있습니다. 사서함 백업은 Microsoft Exchange Server 2010 SP1(서비스 팩 1) 이상에서 지원됩니다.

Microsoft SharePoint 보호

Microsoft SharePoint 팜은 SharePoint 서비스를 실행하는 프런트 엔드 서버, Microsoft SQL Server를 실행하는 데이터베이스 서버, 그리고 (선택적으로) 프런트 엔드 서버로부터 일부 SharePoint 서비스를 오프로드하는 애플리케이션 서버로 구성됩니다. 일부 프런트 엔드 서버 및 애플리케이션 서버는 서로 동일할 수도 있습니다.

전체 SharePoint 팜을 보호하려면

- 애플리케이션 인식 백업을 통해 모든 데이터베이스 서버를 백업합니다.
- 일반 디스크 수준 백업을 통해 고유한 프런트 엔드 서버 및 애플리케이션 서버를-모두 백업합니다.

모든 서버의 백업이 같은 스케줄에 완료되어야 합니다.

그 내용만 보호하려면 콘텐츠 데이터베이스를 따로 백업하면 됩니다.

도메인 컨트롤러 보호

Active Directory 도메인 서비스를 실행 중인 머신은 애플리케이션 인식 백업을 통해 보호할 수 있습니다. 도메인에 도메인 컨트롤러가 두 개 이상 포함되어 있고 이러한 도메인 컨트롤러 중 하나를

© Acronis International GmbH, 2003-2024

복구하는 경우 신뢰할 수 없는 복원이 수행되고 복구 후 USN 롤백이 발생하지 않습니다.

애플리케이션 복구

다음 표는 사용 가능한 애플리케이션 복구 방법을 요약해서 보여줍니다.

	데이터베이스 백업에서 복구	애플리케이션 인식 백업에서 복구	디스크 백업에서 복구
Microsoft SQL Server	데이터베이스를 라이브 SQL Server 인스턴스로 데이터베이스를 파일로	전체 머신 데이터베이스를 라이브 SQL Server 인스턴스로 데이터베이스를 파일로	전체 머신
Microsoft Exchange 서버	데이터베이스를 라이브 Exchange로 데이터베이스를 파일로 라이브 Exchange 또는 Microsoft 365로 개별 복구*	전체 머신 데이터베이스를 라이브 Exchange로 데이터베이스를 파일로 라이브 Exchange 또는 Microsoft 365로 개별 복구*	전체 머신
Microsoft SharePoint 데이터베이스 서버	데이터베이스를 라이브 SQL Server 인스턴스로 데이터베이스를 파일로 SharePoint 탐색기를 사용하여 개별 복구	전체 머신 데이터베이스를 라이브 SQL Server 인스턴스로 데이터베이스를 파일로 SharePoint 탐색기를 사용하여 개별 복구	전체 머신
Microsoft SharePoint 프런트 엔드 웹 서버	-	-	전체 머신
Active Directory 도메인 서비스	-	전체 머신	-

* 개별 복구는 사서함 백업에서도 사용할 수 있습니다. Exchange 데이터 항목을 Microsoft 365로, 또는 그 반대로 복구하는 작업은 Agent for Microsoft 365가 로컬로 설치되어 있다는 조건 하에서 지원됩니다.

사전 요구 사항

애플리케이션 백업을 구성하기 전에 아래 나열된 요구 사항이 충족되었는지 확인하십시오.

VSS 작성자 상태를 확인하려면 `vssadmin list writers` 명령을 사용합니다.

공통 요구 사항

Microsoft SQL Server의 경우 다음을 확인합니다.

© Acronis International GmbH, 2003-2024

- 최소 하나의 Microsoft SQL Server 인스턴스를 시작했습니다.
- SQL VSS 작성자가 켜져 있습니다.

Microsoft Exchange Server의 경우 다음을 확인합니다.

- Microsoft Exchange 정보 저장소 서비스를 시작했습니다.
- Windows PowerShell이 설치되어 있습니다. Exchange 2010 이상에서는 Windows PowerShell 버전이 2.0 이상이어야 합니다.
- Microsoft .NET Framework가 설치되어 있습니다.
  Exchange 2007에서는 Microsoft .NET Framework 버전이 2.0 이상이어야 합니다.
  Exchange 2010 이상에서는 Microsoft .NET Framework 버전이 3.5 이상이어야 합니다.
- VSS용 Exchange 작성기가 켜집니다.

참고
Agent for Exchange를 작동하려면 임시 스토리지가 필요합니다. 임시 파일은 기본적으로 `%ProgramData%\Acronis\Temp`에 저장됩니다. `%ProgramData%` 폴더가 있는 볼륨에 적어도 Exchange 데이터베이스 크기의 15% 여유 공간이 있는지 확인하십시오. 임시 파일 및 폴더 위치 변경(40040)에 설명된 대로 Exchange 백업을 생성하기 전에 임시 파일 위치를 변경할 수도 있습니다.

도메인 컨트롤러에서 다음을 확인합니다.

- Active Directory VSS 작성자가 켜져 있습니다.

보호 계획을 생성할 때에는 다음을 확인합니다.

- 실제 머신과 내부에 에이전트가 설치된 머신에서 VSS(Volume Shadow Copy Service) 백업 옵션이 활성화되어 있습니다.
- 가상 머신에서 가상 머신용 VSS(Volume Shadow Copy Service) 백업 옵션이 활성화되어 있습니다.

애플리케이션 인식 백업을 위한 추가 요구 사항

보호 계획을 생성할 때 **전체 머신**을 백업하도록 선택되어 있는지 확인합니다. 보호 계획에서 **섹터 단위** 백업 옵션이 비활성화되어 있어야 합니다. 비활성화되지 않은 경우 해당 백업으로부터 애플리케이션 데이터를 복구하는 것이 불가능합니다. **섹터 단위** 모드로 자동 전환되어 백업 계획이 실행된 경우에도 애플리케이션 데이터는 복구할 수 없습니다.

ESXi 가상 머신의 시스템 요구사항

Agent for VMware를 통해 백업되는 가상 머신에서 애플리케이션을 실행 중인 경우 다음을 확인합니다.

- 백업 중인 가상 머신이 VMware 지식 베이스의 "Windows 백업 구현" 문서에 나열된 애플리케이션의 일관성을 보장하는 백업 및 복구를 위한 요구 사항을 충족합니다.
  https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.html
- VMware Tools가 머신에 설치되어 있고 최신 상태입니다.

© Acronis International GmbH, 2003-2024

- 머신에서 사용자 계정 컨트롤(UAC)이 사용하지 않도록 설정되어 있습니다. UAC를 비활성화하지 않으려는 경우 애플리케이션 백업을 활성화할 때 기본 제공 도메인 관리자(DOMAIN\Administrator)의 자격 증명을 제공해야 합니다.
  UAC를 비활성화하지 않으려는 경우 애플리케이션 백업을 활성화할 때 기본 제공 도메인 관리자(DOMAIN\Administrator)의 자격 증명을 제공해야 합니다.

  참고
  도메인을 생성할 때 구성한 기본 제공 도메인 관리자 계정을 사용하십시오. 나중에 생성한 계정은 지원되지 않습니다.

Hyper-V 가상 머신의 시스템 요구사항

Agent for Hyper-V를 통해 백업되는 가상 머신에서 애플리케이션을 실행 중인 경우 다음을 확인합니다.

- 게스트 운영 체제는 Windows Server 2008 이상입니다.
- Hyper-V 2008 R2: 게스트 운영 체제는 Windows Server 2008/2008 R2/2012입니다.
- 가상 머신에 동적 디스크가 없습니다.
- Hyper-V 호스트와 게스트 운영 체제 사이에 네트워크 연결이 있습니다. 이는 가상 머신 내에서 원격 WMI 쿼리를 실행하는 데 필요합니다.
- 머신에서 사용자 계정 컨트롤(UAC)이 사용하지 않도록 설정되어 있습니다. UAC를 비활성화하지 않으려는 경우 애플리케이션 백업을 활성화할 때 기본 제공 도메인 관리자(DOMAIN\Administrator)의 자격 증명을 제공해야 합니다.
  UAC를 비활성화하지 않으려는 경우 애플리케이션 백업을 활성화할 때 기본 제공 도메인 관리자(DOMAIN\Administrator)의 자격 증명을 제공해야 합니다.

  참고
  도메인을 생성할 때 구성한 기본 제공 도메인 관리자 계정을 사용하십시오. 나중에 생성한 계정은 지원되지 않습니다.

- 가상 머신 구성이 다음 조건과 일치합니다.
  - Hyper-V 통합 서비스가 설치되어 있고 최신 상태입니다. 중대한 업데이트는 https://support.microsoft.com/en-us/help/3063109/hyper-v-integration-components-update-for-windows-virtual-machines입니다.
  - 가상 머신 설정에서 **관리 > 통합 서비스 > 백업(볼륨 체크포인트)** 옵션이 활성화되어 있습니다.
  - Hyper-V 2012 이상: 가상 머신에 체크포인트가 없습니다.
  - Hyper-V 2012 R2 이상: 가상 머신에 SCSI 컨트롤러가 있습니다(**설정 > 하드웨어** 확인).

데이터베이스 백업

데이터베이스를 백업하기 전에 "사전 요구 사항"에 나열되어 있는 요구 사항이 충족되었는지 확인하십시오.

아래 설명에 따라 데이터베이스를 선택한 다음, 보호 계획의 기타 설정을 적절하게 지정합니다.

© Acronis International GmbH, 2003-2024

SQL 데이터베이스 선택

SQL 데이터베이스 백업에는 데이터베이스 파일(.mdf, .ndf), 로그 파일(.ldf) 및 기타 관련 파일이 들어 있습니다. 이러한 파일은 SQL 기록기 서비스를 통해 백업합니다. 이 서비스는 VSS(Volume Shadow Copy Service)가 백업 또는 복구를 요청할 당시 실행 중이어야 합니다.

성공적인 각각의 백업 후 SQL 트랜잭션 로그 파일이 잘립니다. SQL 로그 자르기는 보호 계획 옵션에서 비활성화할 수 있습니다.

SQL 데이터베이스를 선택하려면

1. **장치** > **Microsoft SQL**을 클릭합니다.

   SQL Server AAG(Always On 가용성 그룹), Microsoft SQL Server를 실행하는 머신, SQL Server 인스턴스 및 데이터베이스의 트리가 표시됩니다.
2. 백업하려는 데이터로 이동합니다.

   트리 노드를 확장하거나 트리 오른쪽에 있는 목록에서 항목을 두 번 클릭합니다.
3. 백업하려는 데이터를 선택합니다. AAG, SQL Server를 실행하는 머신, SQL Server 인스턴스 또는 개별 데이터베이스를 선택할 수 있습니다.
   - AAG를 선택하면 선택한 AAG에 포함된 모든 데이터베이스가 백업됩니다. AAG 또는 개별 AAG 데이터베이스 백업에 대한 자세한 내용은 "AAG(Always On 가용성 그룹) 보호"를 참조하십시오.
   - SQL Server를 실행하는 머신을 선택하면 선택한 머신에서 실행되는 모든 SQL Server 인스턴스에 연결된 모든 데이터베이스가 백업됩니다.
   - SQL Server 인스턴스를 선택하면 선택한 인스턴스에 연결된 모든 데이터베이스가 백업됩니다.
   - 데이터베이스를 직접 선택하면 선택한 데이터베이스만 백업됩니다.
4. **보호**를 클릭합니다. 메시지가 표시되면 SQL Server 데이터에 액세스하기 위한 자격 증명을 입력합니다.

   Windows 인증을 사용하는 경우 해당 계정은 머신의 **백업 작업자** 또는 **관리자** 그룹 구성원이자 백업하려는 각 인스턴스의 **sysadmin**역할 구성원이어야 합니다.

   SQL Server 인증을 사용하는 경우 해당 계정은 백업하려는 각 인스턴스의 **sysadmin**역할 구성원이어야 합니다.

Exchange Server 데이터 선택

다음 표는 백업하려고 선택할 수 있는 Microsoft Exchange Server 데이터와 이러한 데이터를 백업하는 데 필요한 최소 사용자 권한을 요약해서 보여줍니다.

Exchange 버전	데이터 항목	사용자 권한
2007	스토리지 그룹	**Exchange 조직 관리자** 역할 그룹의 구성원 자격
2010/2013/2016/2019	데이터베이스, DAG(데이터베이스 가용성 그룹)	**서버 관리** 역할 그룹의 구성원 자격.

© Acronis International GmbH, 2003-2024

전체 백업에는 선택한 Exchange Server 데이터가 모두 포함되어 있습니다.

증분 백업에는 해당하는 데이터베이스 체크포인트보다 최신인 데이터베이스 파일의 변경된 블록, 체크포인트 파일 및 소수의 로그 파일이 포함되어 있습니다. 백업에 데이터베이스 파일에 대한 변경 사항이 포함되므로 이전 백업 이후 모든 트랜잭션 로그 레코드를 백업할 필요가 없습니다. 복구 후 해당 체크포인트보다 최신인 로그만 재생해야 합니다. 따라서 복구 속도가 더 빠르고 순환 로깅이 활성화되어 있는 경우에도 성공적인 데이터베이스 백업을 보장합니다.

성공적인 각각의 백업 후 트랜잭션 로그 파일이 잘립니다.

Exchange Server 데이터를 선택하려면

1. **장치** > **Microsoft Exchange**를 클릭합니다.
   소프트웨어에 Exchange Server DAG(데이터베이스 가용성 그룹), Microsoft Exchange Server를 실행하는 머신, Exchange Server 데이터베이스의 트리가 표시됩니다. "사서함 백업"(520페이지)에서 설명된 대로 Agent for Exchange를 구성하면 사서함 역시 이 트리에 표시됩니다.
2. 백업하려는 데이터로 이동합니다.
   트리 노드를 확장하거나 트리 오른쪽에 있는 목록에서 항목을 두 번 클릭합니다.
3. 백업하려는 데이터를 선택합니다.
   - DAG를 선택하면 각 클러스터 데이터베이스마다 사본이 하나씩 백업됩니다. DAG 백업에 대한 자세한 내용은 "DAG(데이터베이스 가용성 그룹) 보호"(516페이지) 항목을 참조하십시오.
   - Microsoft Exchange Server를 실행하는 머신을 선택하면 선택한 머신에서 실행되는 Exchange Server에 마운트된 모든 데이터베이스가 백업됩니다.
   - 데이터베이스를 직접 선택하면 선택한 데이터베이스만 백업됩니다.
   - "사서함 백업"(520페이지)에서 설명한 대로 Agent for Exchange를 구성한 경우 백업용 사서함을 선택할 수 있습니다.

   여러 데이터베이스를 선택한 경우 한 번에 두 개씩 진행됩니다. 첫 그룹의 백업이 완료되면 다음 그룹의 백업이 시작됩니다.
4. 메시지가 표시되면 데이터에 액세스하기 위한 자격 증명을 입력합니다.
5. **보호**를 클릭합니다.

AAG(Always On 가용성 그룹) 보호

참고
이 기능은 Advanced Backup 팩에서 사용할 수 있습니다.

SQL Server 고가용성 솔루션 개요

WSFC(Windows Server 장애 조치 클러스터링) 기능을 사용하면 인스턴스 수준(장애 조치 클러스터 인스턴스, FCI) 또는 데이터베이스 수준(AlwaysOn 가용성 그룹, AAG)에서 이중화를 통해 고가용성 SQL Server를 구성할 수 있습니다. 두 방법 모두 결합시킬 수도 있습니다.

장애 조치 클러스터 인스턴스에서 SQL 데이터베이스는 공유 스토리지에 위치합니다. 이 스토리지는 활성 클러스터 노드에서만 액세스할 수 있습니다. 활성 노드에 장애가 생기면 장애 조치가 발생하고 다른 노드가 활성 노드가 됩니다.

© Acronis International GmbH, 2003-2024

가용성 그룹에서 각 데이터베이스 복제본은 다른 노드에 상주합니다. 주 복제본을 사용할 수 없게 되면 다른 노드에 있는 보조 복제본에 주 역할이 할당됩니다.

따라서 이미 클러스터 자체로 재해 복구 솔루션의 서비스를 제공하고 있습니다. 그러나 예를 들어 데이터베이스 논리 손상이 발생하거나 전체 클러스터가 가동 중단된 경우에는 클러스터가 데이터를 보호하지 못할 수 있습니다. 클러스터 솔루션이 유해한 내용 변경도 차단하지 못하는데, 그 이유는 변경 사항이 즉시 모든 클러스터 노드에 복제되기 때문입니다.

지원되는 클러스터 구성

이 백업 소프트웨어서는 SQL Server 2012 이상의 경우 AAG(Always On 가용성 그룹)*만* 지원합니다. 장애 조치 클러스터 인스턴스, 데이터베이스 미러링 및 로그 전달과 같은 기타 클러스터 구성은 지원되지 *않습니다*.

클러스터 데이터 백업 및 복구에 필요한 에이전트 수는?

클러스터 데이터의 성공적인 백업 및 복구를 위해서는 WSFC 클러스터의 각 노드에 Agent for SQL을 설치해야 합니다.

AAG에 포함된 데이터베이스 백업

1. WSFC 클러스터의 각 노드에 Agent for SQL을 설치합니다.
2. "SQL 데이터베이스 선택"의 설명대로 백업할 AAG를 선택합니다.
   모든 AAG 데이터베이스를 백업할 AAG를 선택해야 합니다. 데이터베이스 세트를 백업하려면 이 데이터베이스 세트를 AAG의 모든 노드에 정의하십시오.

   경고!
   데이터베이스는 모든 노드에서 동일해야 합니다. 하나의 세트라도 다르거나 모든 노드에서 정의되지 않은 경우 클러스터 백업이 올바르게 작동하지 않습니다.

3. "클러스터 백업 모드" 백업 옵션을 구성합니다.

AAG에 포함된 데이터베이스 복구

1. 복구할 데이터베이스를 선택하고 데이터베이스를 복구할 복구 지점을 선택합니다.
   장치 > **Microsoft SQL** > **데이터베이스**에서 클러스터 데이터베이스를 선택하고 **복구**를 클릭하면 데이터베이스의 선택한 복사본이 백업된 시간에 해당하는 복구 지점만 표시됩니다.
   클러스터 데이터베이스의 모든 복구 지점을 보는 가장 쉬운 방법은 백업 스토리지 탭에서 전체 AAG의 백업을 선택하는 것입니다. AAG 백업의 이름은 <AAG 이름> - <보호 계획 이름> 템플릿에 따라 결정되고 특수 아이콘을 포함합니다.
2. 복구를 구성하려면 "SQL 데이터베이스 복구"에 설명된 단계를 5단계부터 따릅니다.
   데이터가 복구될 클러스터 노드가 자동으로 정의됩니다. 노드 이름은 **복구 대상** 필드에 표시됩니다. 대상 노드를 수동으로 변경할 수 있습니다.

© Acronis International GmbH, 2003-2024

중요
Always On 가용성 그룹에 포함된 데이터베이스는 복구 과정에서 덮어쓸 수 없습니다. Microsoft SQL Server가 이를 금지하기 때문입니다. 복구 전에 AAG에서 대상 데이터베이스를 제외해야 합니다. 또는 간단히 AAG가 아닌 새 데이터베이스로 데이터베이스를 복구하면 됩니다. 복구가 완료되면 원래 AAG 구성을 재구성할 수 있습니다.

DAG(데이터베이스 가용성 그룹) 보호

참고
이 기능은 Advanced Backup 팩에서 사용할 수 있습니다.

Exchange Server 클러스터 개요

Exchange 클러스터의 기본 개념은 신속한 장애 조치 및 데이터 손실 방지와 함께 높은 데이터베이스 가용성을 제공하는 것입니다. 보통 데이터베이스 또는 스토리지 그룹의 복사본을 한 개 이상 클러스터 구성 요소(클러스터 노드)에 보유하면 됩니다. 활성 데이터베이스 복사본을 호스팅하는 클러스터 노드 또는 활성 데이터베이스 복사본 자체가 실패하는 경우, 수동 복사본을 호스팅하는 나머지 노드가 실패한 노드의 작업을 자동으로 인계 받아서 최소한의 가동 중단으로 Exchange 서비스에 액세스를 지원합니다. 따라서 이미 클러스터 자체로 재해 복구 솔루션의 서비스를 제공하고 있습니다.

그러나 장애 조치 클러스터 솔루션이 데이터 보호 기능을 제공할 수 없는 경우가 있는데, 예를 들면 데이터베이스 논리 손상 또는 클러스터의 특정 데이터베이스에 복사본(복제본)이 없는 경우 또는 전체 클러스터가 가동 중단된 경우입니다. 클러스터 솔루션이 유해한 내용 변경도 차단하지 못하는데, 그 이유는 변경 사항이 즉시 모든 클러스터 노드에 복제되기 때문입니다.

클러스터 인식 백업

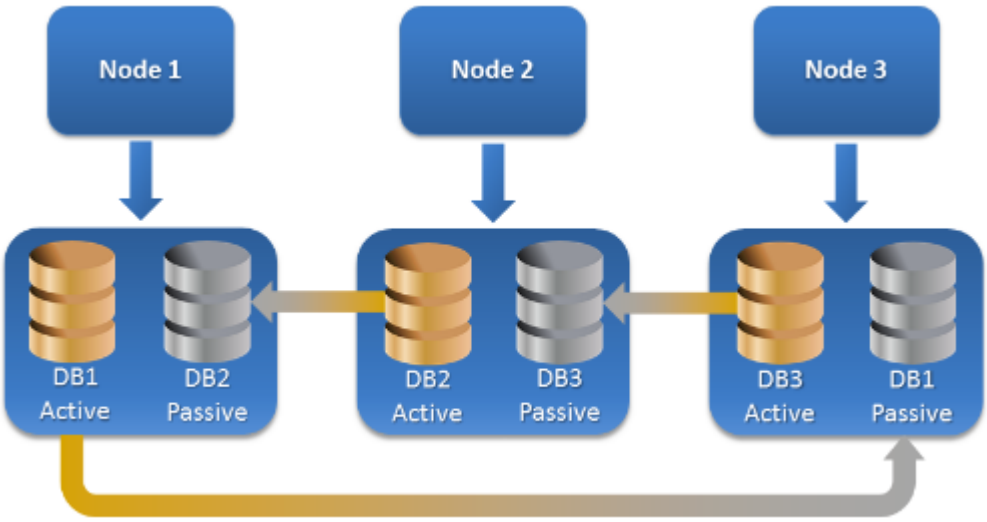
클러스터 인식 백업을 사용하면 클러스터 데이터의 복사본 하나만 백업됩니다. 데이터 위치가 클러스터 내에서 변경되는 경우(예: 전환 또는 장애 조치로 인해) 소프트웨어는 이 데이터의 모든 변경 위치를 추적하여 안전하게 백업합니다.

지원되는 클러스터 구성

클러스터 인식 백업은 Exchange Server 2010 이상에서 DAG(Database Availability Group)에 *대해서만* 지원됩니다. SCC(단일 복사본 클러스터) 및 Exchange 2007용 CCR(클러스터 연속 복제)과 같은 기타 클러스터 구성은 지원되지 *않습니다*.

DAG는 최대 16대의 Exchange 사서함 서버로 구성되는 그룹입니다. 모든 노드가 다른 노드로부터 사서함 데이터베이스 복사본을 호스팅할 수 있습니다. 각 노드가 수동 및 활성 데이터베이스 복사본을 호스팅할 수 있습니다. 각 데이터베이스의 복사본을 16개까지 생성할 수 있습니다.

© Acronis International GmbH, 2003-2024



클러스터 인식 백업 및 복구에 필요한 에이전트 수는?

클러스터 데이터베이스의 성공적인 백업 및 복구를 위해서는 Exchange 클러스터의 각 노드에 Agent for Exchange를 설치해야 합니다

참고
노드 중 하나에 에이전트를 설치하고 나면 Cyber Protect 콘솔의 **장치** > **Microsoft Exchange** > **데이터베이스** 아래에 DAG 및 해당 노드가 표시됩니다. 나머지 노드에 Agent for Exchange를 설치하려면 DAG를 선택하고, **상세정보**를 클릭하고 나서, 각 노드 옆에 있는 **에이전트 설치**를 클릭합니다.

Exchange 클러스터 데이터 백업

1. 보호 계획을 생성할 때는 "Exchange Server 데이터 선택"(513페이지)의 설명대로 DAG를 선택합니다.
2. "클러스터 백업 모드"(416페이지) 백업 옵션을 구성합니다.
3. 보호 계획의 기타 설정을 적합하게 지정합니다.

중요
클러스터 인식 백업의 경우 DAG 자체를 선택하십시오. DAG 내부의 개별 노드 또는 데이터베이스를 선택하면 선택한 항목만 백업되고 **클러스터 백업 모드** 옵션이 무시됩니다.

Exchange 클러스터 데이터 복구

1. 복구할 데이터베이스의 복구 지점을 선택합니다. 전체 클러스터 복구는 선택할 수 없습니다.
   장치 > **Microsoft Exchange** > **데이터베이스** > <클러스터 이름> > <노드 이름>에서 클러스터 데이터베이스 사본을 선택하고 **복구**를 클릭하면 이 사본이 백업된 시간에 해당하는 복구 지점만 표시됩니다.
   클러스터 데이터베이스의 모든 복구 지점을 보는 가장 쉬운 방법은 백업 스토리지 탭에서 백업을 선택하는 것입니다.
2. "Exchange 데이터베이스 복구"(529페이지)에 설명된 단계를 5단계부터 진행합니다.

© Acronis International GmbH, 2003-2024

데이터가 복구될 클러스터 노드가 자동으로 정의됩니다. 노드 이름은 **복구 대상** 필드에 표시됩니다. 대상 노드를 수동으로 변경할 수 있습니다.

Aware 인식→인지

애플리케이션 인식 디스크 수준 백업은 실제 머신, ESXi 가상 머신 및 Hyper-V 가상 머신에 대해 사용할 수 있습니다.

Microsoft SQL Server, Microsoft Exchange Server 또는 Active Directory 도메인 서비스를 실행 중인 머신을 백업하는 경우 이러한 애플리케이션 데이터를 추가로 보호하려면 **애플리케이션 백업**을 사용하도록 설정합니다.

애플리케이션 인식 백업을 사용해야 하는 이유는 무엇입니까?

애플리케이션 인식 백업을 사용하면 다음과 같은 이점을 얻을 수 있습니다.

- 애플리케이션이 일관된 상태에서 백업되므로 머신 복구 후 즉시 사용할 수 있습니다.
- 전체 머신을 복구하지 않고 SQL 및 Exchange 데이터베이스, 사서함 및 사서함 항목을 복구할 수 있습니다.
- 성공적인 각각의 백업 후 SQL 트랜잭션 로그 파일이 잘립니다. SQL 로그 자르기는 보호 계획 옵션에서 비활성화할 수 있습니다. Exchange 트랜잭션 로그는 가상 머신에서만 잘립니다. 실제 머신에서 Exchange 트랜잭션 로그를 자르려면 VSS 전체 백업 옵션을 사용하도록 설정하면 됩니다.
- 도메인에 도메인 컨트롤러가 두 개 이상 포함되어 있고 이러한 도메인 컨트롤러 중 하나를 복구하는 경우 신뢰할 수 없는 복원이 수행되고 복구 후 USN 롤백이 발생하지 않습니다.

애플리케이션 인식 백업을 사용하려면 무엇이 필요합니까?

실제 머신에 Agent for SQL 및/또는 Agent for Exchange, 그리고 Agent for Windows가 설치되어 있어야 합니다.

가상 머신에서는 에이전트 설치가 필요 없습니다. 이 경우에는 머신이 Agent for VMware(Windows) 또는 Agent for Hyper-V에 의해 백업되는 것으로 간주됩니다.

참고
Windows Server 2022를 실행하는 Hyper-V 및 VMware ESXi 가상 머신의 경우 비에이전트 모드에서(Agent for Hyper-V 또는 Agent for VMware가 백업을 수행할 때) 애플리케이션 인식 백업이 지원되지 않습니다. 이러한 머신에서 Microsoft 애플리케이션을 보호하려면 게스트 운영 체제 내에 Agent for Windows를 설치하십시오.

Agent for VMware(가상 어플라이언스)는 응용 프로그램 인식 백업을 생성할 수 있지만 여기에서 응용 프로그램 데이터를 복구할 수는 없습니다. 해당 에이전트를 통해 생성된 백업에서 응용 프로

© Acronis International GmbH, 2003-2024

그램 데이터를 복구하려면 백업이 저장되어 있는 위치에 액세스할 수 있는 머신에 Agent for VMware(Windows), Agent for SQL 또는 Agent for Exchange가 있어야 합니다. 응용 프로그램 데이터 복구를 구성할 때에는 **백업 스토리지** 탭에서 복구 지점을 선택하고 **다음 위치에서 탐색할 머신**에서 이 머신을 선택합니다.

다른 요구 사항은 "사전 요구 사항" 및 "필수 사용자 권한" 섹션에 나열되어 있습니다.

참고
로드가 높은 호스트에서 백업을 수행하는 경우 Windows Management Instrumentation가 응답을 하지 않거나 응답이 지연되어 Hyper-V 가상 머신의 애플리케이션 인식 백업이 실패하고 "WMI 'ExecQuery'가 쿼리를 실행하지 못했습니다." 또는 "WMI를 통해 새 프로세스를 생성하지 못했습니다." 오류가 발생할 수 있습니다. 호스트의 로드가 더 낮은 시간 슬롯에 이러한 백업을 다시 시도합니다.

애플리케이션 인식 백업에 필요한 사용자 권한

애플리케이션 인식 백업에는 디스크에 있는 VSS 인식 애플리케이션의 메타데이터가 포함되어 있습니다. 이 메타데이터에 액세스하려면 아래 나열된 해당 권한이 있는 계정이 에이전트에 필요합니다. 애플리케이션 백업을 사용하도록 설정하는 경우 이러한 계정을 지정하라는 메시지가 표시됩니다.

- SQL Server의 경우:
  계정은 머신에서 **백업 작업자** 또는 **관리자** 그룹의 구성원이어야 하며, 백업할 각 인스턴스에서 **시스템 관리자** 역할의 구성원이어야 합니다.

  참고
  Windows 인증만 지원됩니다.

- Exchange Server의 경우:
  Exchange 2007: 계정이 머신의 **관리자** 그룹 및 **Exchange 조직 관리자** 역할 그룹의 구성원이어야 합니다.
  Exchange 2010 이상: 계정이 머신의 **관리자** 그룹 및 **조직 관리** 역할 그룹의 구성원이어야 합니다.
- Active Directory의 경우:
  계정이 도메인 관리자여야 합니다.

가상 머신의 추가 시스템 요구사항

애플리케이션이 Agent for VMware 또는 Agent for Hyper-V에 의해 백업되는 가상 머신에서 실행되는 경우 머신에서 사용자 계정 컨트롤(UAC)이 비활성화되어 있는지 확인하십시오.

UAC를 비활성화하지 않으려는 경우 애플리케이션 백업을 활성화할 때 기본 제공 도메인 관리자(DOMAIN\Administrator)의 자격 증명을 제공해야 합니다.

© Acronis International GmbH, 2003-2024

참고
도메인을 생성할 때 구성한 기본 제공 도메인 관리자 계정을 사용하십시오. 나중에 생성한 계정은 지원되지 않습니다.

Windows를 실행하는 머신에 대한 추가 요구 사항

모든 Windows 버전의 경우 애플리케이션 인식 백업을 허용하려면 사용자 계정 컨트롤(UAC) 정책을 비활성화해야 합니다.

UAC를 비활성화하지 않으려는 경우 애플리케이션 백업을 활성화할 때 기본 제공 도메인 관리자(DOMAIN\Administrator)의 자격 증명을 제공해야 합니다.

참고
도메인을 생성할 때 구성한 기본 제공 도메인 관리자 계정을 사용하십시오. 나중에 생성한 계정은 지원되지 않습니다.

Windows에서 UAC 정책을 비활성화하려면

1. 레지스트리 편집기에서 다음 레지스트리 키를 찾습니다.
   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`
2. **EnableLUA** 값을 **0**으로 변경합니다.
3. 머신을 다시 시작합니다.

사서함 백업

사서함 백업은 Microsoft Exchange Server 2010 SP1(서비스 팩 1) 이상에서 지원됩니다.

하나 이상의 Agent for Exchange가 관리 서버에 등록된 경우 사서함 백업을 사용할 수 있습니다. 에이전트는 Microsoft Exchange Server와 동일한 Active Directory 포리스트에 속한 머신에 설치되어야 합니다.

사서함을 백업하기 전에 Agent for Exchange를 Microsoft Exchange Server의 **클라이언트 액세스** 서버 역할(CAS)을 실행 중인 머신에 연결해야 합니다. Exchange 2016 이상에서 CAS 역할은 별도 설치 옵션으로 사용할 수 없습니다. 이는 사서함 서버 역할의 일부로 자동 설치됩니다. 따라서 에이전트를 **사서함 역할**을 실행하는 어느 서버로든 연결할 수 있습니다.

참고
데이터베이스 백업 및 애플리케이션 인식 백업에서 사서함과 사서함 항목을 복구할 수 있습니다. 자세한 내용은 "Exchange 사서함 및 사서함 항목 복구"(532페이지)을(를) 참조하십시오. 데이터베이스 백업과 애플리케이션 인식 백업을 사용하여 개별 사서함용 보호 계획을 생성할 수는 없습니다.

Agent for Exchange를 CAS에 연결하려면

1. **장치** > **추가**를 클릭합니다.
2. **Microsoft Exchange Server**를 클릭합니다.
3. **Exchange 사서함**을 클릭합니다.

© Acronis International GmbH, 2003-2024

관리 서버에 등록된 Agent for Exchange가 없는 경우 에이전트를 설치할지 묻는 메시지가 표시됩니다. 설치 후에 이 절차를 1단계부터 반복합니다.

4. [선택 사항] 관리 서버에 여러 Agent for Exchange가 등록되어 있는 경우에는 **에이전트**를 클릭한 다음 백업을 수행할 에이전트를 변경합니다.
5. **클라이언트 액세스 서버**에서 Microsoft Exchange Server의 **클라이언트 액세스** 역할이 활성화된 머신의 FQDN(정규화된 도메인 이름)을 지정합니다.

   Exchange 2016 이상에서는 클라이언트 액세스 서비스가 사서함 서버 역할의 일부로 자동 설치됩니다. 따라서 **사서함 역할**을 실행하는 어느 서버든 지정할 수 있습니다. 이 섹션 뒷부분에서는 이 서버를 CAS로 언급합니다.
6. **인증 유형**에서 CAS에 사용되는 인증 유형을 선택합니다. **Kerberos**(기본값) 또는 **기본**을 선택할 수 있습니다.
7. [기본 인증만 해당] 사용할 프로토콜을 선택합니다. **HTTPS**(기본값) 또는 **HTTP**를 선택할 수 있습니다.
8. [HTTPS 프로토콜을 사용한 기본 인증만 해당] CAS가 인증 기관에서 얻은 SSL 인증서를 사용할 때 소프트웨어를 통해 CAS에 연결할 때 인증서를 확인하려는 경우 **SSL 인증서 확인** 확인란을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
9. 계정의 자격 증명이 제공되며 CAS에 액세스할 때 이 자격 증명을 사용합니다. 이 계정에 대한 요구사항이 "필수 사용자 권한"에 나열됩니다.
10. **추가**를 클릭합니다.

그러면 사서함이 **장치** > **Microsoft Exchange** > **사서함** 아래에 표시됩니다.

Exchange 서버 사서함 선택

아래 설명에 따라 사서함을 선택한 다음, 보호 계획의 기타 설정을 적절하게 지정합니다.

MS Exchange 사서함을 선택하려면

1. **장치** > **Microsoft Exchange**를 클릭합니다.

   Exchange 데이터베이스 및 사서함의 트리가 표시됩니다.
2. **사서함**을 클릭하고 백업할 사서함을 선택합니다.
3. **보호**를 클릭합니다.

필수 사용자 권한

사서함에 액세스하려면 Agent for Exchange에 적절한 권한이 있는 계정이 있어야 합니다. 사서함을 사용하여 다양한 작업을 구성할 때 이 계정을 지정하라는 메시지가 나타납니다.

조직 관리 역할 그룹의 계정 구성원은 미래에 생성될 사서함을 포함하여 모든 사서함에 대한 액세스를 허용합니다.

필요한 최소 사용자 권한은 다음과 같습니다.

- 계정이 **서버 관리** 및 **수신자 관리** 역할 그룹의 구성원이어야 합니다.
- 에이전트가 액세스하는 사서함의 모든 사용자 또는 사용자 그룹에 대해 계정의 **ApplicationImpersonation** 관리 역할이 활성화되어 있어야 합니다.

© Acronis International GmbH, 2003-2024

ApplicationImpersonation 관리 역할의 구성에 대한 자세한 내용은 다음 Microsoft 지식 기반 기사를 참조하십시오. https://msdn.microsoft.com/en-us/library/office/dn722376.aspx.

SQL 데이터베이스 복구

데이터베이스 백업 및 애플리케이션 인식 백업에서 SQL 데이터베이스를 복구할 수 있습니다. 두 백업 유형 간의 차이점에 대한 자세한 내용은 "Microsoft SQL Server 및 Microsoft Exchange Server 보호"(509페이지) 항목을 참고하십시오.

원래 인스턴스, 원래 머신의 다른 인스턴스 또는 원래 머신 외의 머신에 있는 인스턴스에 SQL 데이터베이스를 복구할 수 있습니다. 원래 머신 외의 머신으로 복구를 수행할 때는 대상 머신에 Agent for SQL을 설치해야 합니다.

데이터베이스를 파일로 복구할 수도 있습니다.

SQL 인스턴스에 Windows 인증을 사용하는 경우 머신의 **백업 작업자** 또는 **관리자** 그룹 멤버이자 대상 인스턴스의 **sysadmin** 역할 멤버인 계정의 자격 증명을 입력해야 합니다. SQL Server 인증을 사용하는 경우에는 대상 인스턴스의 **sysadmin** 역할 멤버인 계정의 자격 증명을 입력해야 합니다.

시스템 데이터베이스는 다른 데이터베이스와는 다소 다른 사용자 데이터베이스로 복구됩니다. 이러한 차이점에 대해 자세히 알아보려면 "시스템 데이터베이스 복구"(528페이지) 항목을 참조하십시오.

복구 중에 Cyber Protect 콘솔의 **모니터링** > **작업** 탭에서 작업 진행률을 확인할 수 있습니다.

원래 머신에 SQL 데이터베이스 복구

원래 인스턴스, 원래 머신의 다른 인스턴스 또는 원래 대상 머신 외의 머신에 있는 인스턴스에 SQL 데이터베이스를 복구할 수 있습니다.

원래 머신에 SQL 데이터베이스를 복구하려면

데이터베이스 백업에서 복구

1. Cyber Protect 콘솔에서 **장치** > **Microsoft SQL**로 이동합니다.
2. SQL Server 인스턴스를 선택하거나 인스턴스 이름을 클릭하여 복구할 특정 데이터베이스를 선택한 다음 **복구**를 클릭합니다.

   머신이 오프라인 상태이면 복구 지점이 표시되지 않습니다. 원래 머신 외의 머신에 데이터를 복구하려면 "원래 머신 외의 머신에 SQL 데이터베이스 복구"(524페이지) 항목을 참조하십시오.
3. 복구 지점을 선택합니다.

   복구 지점은 위치별로 필터링됩니다.
4. **복구** > **데이터베이스를 인스턴스로**를 클릭합니다.

   기본적으로 인스턴스와 데이터베이스는 원래 인스턴스와 데이터베이스로 복구됩니다. 원래 데이터베이스를 새 데이터베이스로 복구할 수도 있습니다.
5. [같은 머신의 원래 인스턴스가 아닌 인스턴스에 복구하는 경우] **대상 SQL Server 인스턴스**를 클릭하고 대상 인스턴스를 선택한 후에 **완료**를 클릭합니다.
6. [데이터베이스를 새 데이터베이스로 복구하는 경우] 데이터베이스 이름을 클릭하고 **복구 대상**에서 **새 데이터베이스**를 선택합니다.

© Acronis International GmbH, 2003-2024

- 새 데이터베이스 이름을 지정합니다.
- 새 데이터베이스 경로를 지정합니다.
- 로그 경로를 지정합니다.

7. [선택 사항] [데이터베이스를 새 데이터베이스로 복구할 때는 사용 불가] 복구 후 데이터베이스 상태를 변경하려면 데이터베이스 이름을 클릭한 후 다음 상태 중 하나를 선택하고 **완료**를 클릭합니다.
   - **사용 준비(복구를 통해 복원)**(기본값)
     복구가 완료되면 데이터베이스를 사용할 준비가 끝납니다. 사용자는 이 데이터베이스에 대한 전체 액세스 권한을 갖습니다. 소프트웨어는 트랜잭션 로그에 저장되어 있는 복구된 데이터베이스에서 커밋하지 않은 모든 트랜잭션을 롤백합니다. 네이티브 Microsoft SQL 백업에서 추가 트랜잭션 로그를 복구할 수 없습니다.
   - **비실행(복구가 없는 복원)**
     복구가 완료되면 데이터베이스가 비실행 상태가 됩니다. 사용자는 여기에 액세스할 수 없습니다. 소프트웨어는 복구된 데이터베이스의 커밋하지 않은 모든 트랜잭션을 유지합니다. 네이티브 Microsoft SQL 백업에서 추가 트랜잭션 로그를 복구할 수 있으며, 따라서 필요한 복구 지점에 도달할 수 있습니다.
   - **읽기 전용(대기로 복원)**
     복구가 완료된 후 사용자는 데이터베이스에 읽기 전용으로 액세스할 수 있습니다. 소프트웨어는 커밋하지 않은 모든 트랜잭션을 실행 취소합니다. 그러나 임시 대기 파일에 실행 취소 동작을 저장하므로 복구 효과를 되돌릴 수 있습니다.
     이 값은 주로 SQL Server 오류가 발생한 시점을 찾기 위해 사용됩니다.
8. **복구 시작**을 클릭합니다.

애플리케이션 인식 백업에서 복구

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 복구하려는 데이터가 원래 포함되어 있던 머신을 선택하고 **복구**를 클릭합니다.
   머신이 오프라인 상태이면 복구 지점이 표시되지 않습니다. 원래 머신 외의 머신에 데이터를 복구하려면 "원래 머신 외의 머신에 SQL 데이터베이스 복구"(524페이지) 항목을 참조하십시오.
3. 복구 지점을 선택합니다.
   복구 지점은 위치별로 필터링됩니다.
4. **복구** > **SQL 데이터베이스**를 클릭합니다.
5. SQL Server 인스턴스를 선택하거나 인스턴스 이름을 클릭하여 복구할 특정 데이터베이스를 선택한 다음 **복구**를 클릭합니다.
   기본적으로 인스턴스와 데이터베이스는 원래 인스턴스와 데이터베이스로 복구됩니다. 원래 데이터베이스를 새 데이터베이스로 복구할 수도 있습니다.
6. [같은 머신의 원래 인스턴스가 아닌 인스턴스에 복구하는 경우] **대상 SQL Server 인스턴스**를 클릭하고 대상 인스턴스를 선택한 후에 **완료**를 클릭합니다.
7. [데이터베이스를 새 데이터베이스로 복구하는 경우] 데이터베이스 이름을 클릭하고 **복구 대상**에서 **새 데이터베이스**를 선택합니다.
   - 새 데이터베이스 이름을 지정합니다.
   - 새 데이터베이스 경로를 지정합니다.

© Acronis International GmbH, 2003-2024

- 로그 경로를 지정합니다.

8. [선택 사항] [데이터베이스를 새 데이터베이스로 복구할 때는 사용 불가] 복구 후 데이터베이스 상태를 변경하려면 데이터베이스 이름을 클릭한 후 다음 상태 중 하나를 선택하고 **완료**를 클릭합니다.
   - **사용 준비(복구를 통해 복원)**(기본값)
     복구가 완료되면 데이터베이스를 사용할 준비가 끝납니다. 사용자는 이 데이터베이스에 대한 전체 액세스 권한을 갖습니다. 소프트웨어는 트랜잭션 로그에 저장되어 있는 복구된 데이터베이스에서 커밋하지 않은 모든 트랜잭션을 롤백합니다. 네이티브 Microsoft SQL 백업에서 추가 트랜잭션 로그를 복구할 수 없습니다.
   - **비실행(복구가 없는 복원)**
     복구가 완료되면 데이터베이스가 비실행 상태가 됩니다. 사용자는 여기에 액세스할 수 없습니다. 소프트웨어는 복구된 데이터베이스의 커밋하지 않은 모든 트랜잭션을 유지합니다. 네이티브 Microsoft SQL 백업에서 추가 트랜잭션 로그를 복구할 수 있으며, 따라서 필요한 복구 지점에 도달할 수 있습니다.
   - **읽기 전용(대기로 복원)**
     복구가 완료된 후 사용자는 데이터베이스에 읽기 전용으로 액세스할 수 있습니다. 소프트웨어는 커밋하지 않은 모든 트랜잭션을 실행 취소합니다. 그러나 임시 대기 파일에 실행 취소 동작을 저장하므로 복구 효과를 되돌릴 수 있습니다.
     이 값은 주로 SQL Server 오류가 발생한 시점을 찾기 위해 사용됩니다.
9. **복구 시작**을 클릭합니다.

원래 머신 외의 머신에 SQL 데이터베이스 복구

Agent for SQL이 설치되어 있는 원래 머신 외의 대상 머신에 있는 SQL Server 인스턴스에 애플리케이션 인식 백업과 데이터베이스 백업을 복구할 수 있습니다. 대상 머신이 액세스할 수 있는 클라우드 스토리지나 공유 스토리지에 백업이 있어야 합니다.

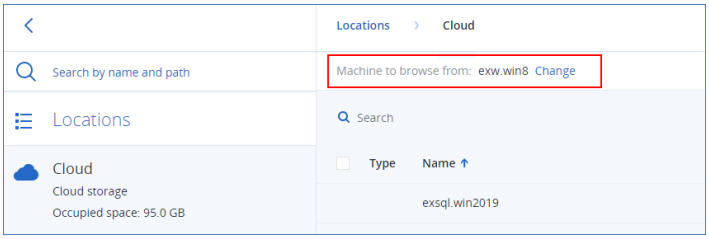
대상 머신의 SQL Server 버전은 원본 머신의 버전 이상이어야 합니다.

원래 머신 외의 머신에 SQL 데이터베이스를 복구하려면

백업 스토리지에서 복구

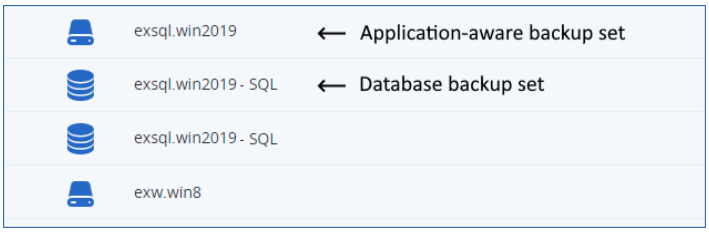
이 절차는 애플리케이션 인식 백업과 데이터베이스 백업에 적용됩니다.

1. Cyber Protect 콘솔에서 **백업 스토리지**로 이동합니다.
2. 데이터를 복구하려는 백업 집합의 위치를 선택합니다.
3. **다음 위치에서 탐색할 머신**에서 대상 머신을 선택합니다.
   이 머신에 데이터가 복구됩니다. 대상 머신은 온라인 상태여야 합니다.



© Acronis International GmbH, 2003-2024

4. 백업 세트를 선택하고 **작업** 창에서 **백업 표시**를 클릭합니다.
   애플리케이션 인식 백업 세트와 데이터베이스 백업 세트는 각기 다른 아이콘으로 표시됩니다.



5. 복구하려는 데이터가 있는 복구 지점을 선택합니다.
6. [데이터베이스 백업의 경우] **SQL 데이터베이스 복구**를 클릭합니다.
7. [애플리케이션 인식 백업의 경우] **복구** > **SQL 데이터베이스**를 클릭합니다.
8. SQL Server 인스턴스를 선택하거나 인스턴스 이름을 클릭하여 복구할 특정 데이터베이스를 선택한 다음 **복구**를 클릭합니다.
9. [대상 머신에 SQL 인스턴스가 여러 개 있는 경우] **대상 SQL Server 인스턴스**를 클릭하고 대상 인스턴스를 선택한 후에 **완료**를 클릭합니다.
10. 데이터베이스 이름을 클릭하고 새 데이터베이스 경로 및 로그 경로를 지정한 후에 **완료**를 클릭합니다.
    다음과 같이 두 필드에서 같은 경로를 지정할 수 있습니다.

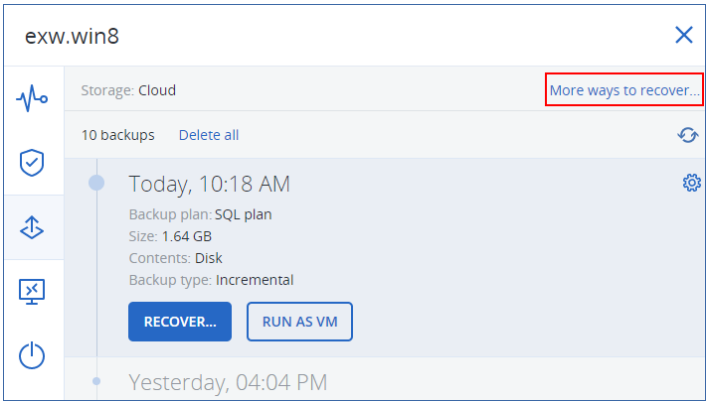
```
C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
```

11. **복구 시작**을 클릭합니다.

장치에서 복구

이 절차는 애플리케이션 인식 백업에만 적용됩니다.

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 복구하려는 데이터가 원래 포함되어 있던 머신을 선택하고 **복구**를 클릭합니다.
3. [원본 머신이 온라인 상태인 경우] **추가 복구 방법**을 클릭합니다.



4. **머신 선택**을 클릭하여 대상 머신을 선택한 다음 **확인**을 클릭합니다.
   이 머신에 데이터가 복구됩니다. 대상 머신은 온라인 상태여야 합니다.
5. 복구 지점을 선택합니다.
   복구 지점은 위치별로 필터링됩니다.

© Acronis International GmbH, 2003-2024

6. **복구** > **SQL 데이터베이스**를 클릭합니다.
7. SQL Server 인스턴스를 선택하거나 인스턴스 이름을 클릭하여 복구할 특정 데이터베이스를 선택한 다음 **복구**를 클릭합니다.
8. [대상 머신에 SQL 인스턴스가 여러 개 있는 경우] **대상 SQL Server 인스턴스**를 클릭하고 대상 인스턴스를 선택한 후에 **완료**를 클릭합니다.
9. 데이터베이스 이름을 클릭하고 새 데이터베이스 경로 및 로그 경로를 지정한 후에 **완료**를 클릭합니다.

   다음과 같이 두 필드에서 같은 경로를 지정할 수 있습니다.

   ```
   C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA\
   ```

10. **복구 시작**을 클릭합니다.

SQL 데이터베이스를 파일로 복구

데이터베이스를 파일로 복구할 수 있습니다. 이 기능은 서드 파티 도구를 사용한 데이터 마이닝, 감사 또는 추가 처리를 위해 데이터를 추출해야 하는 경우 유용할 수 있습니다. SQL 데이터베이스 파일을 SQL Server 인스턴스에 연결하는 방법을 알아보려면 "SQL Server 데이터베이스 연결"(529 페이지) 항목을 참조하십시오.

데이터베이스는 원래 머신에 파일로 복구할 수도 있고 Agent for SQL이 설치되어 있는 원래 머신 이외의 대상 머신에 복구할 수도 있습니다. 원래 머신 이외의 머신에 데이터를 복구할 때는 대상 머신이 액세스할 수 있는 클라우드 스토리지나 공유 스토리지에 백업이 있어야 합니다.

참고

Agent for VMware(Windows)를 사용하는 경우 사용 가능한 복구 방법은 데이터베이스를 파일로 복구하는 것뿐입니다. Agent for VMware(가상 어플라이언스)를 이용한 데이터 복구는 불가능합니다.

SQL 데이터베이스를 파일로 복구하려면

데이터베이스 백업에서 복구

이 절차는 온라인 원본 머신에 적용됩니다.

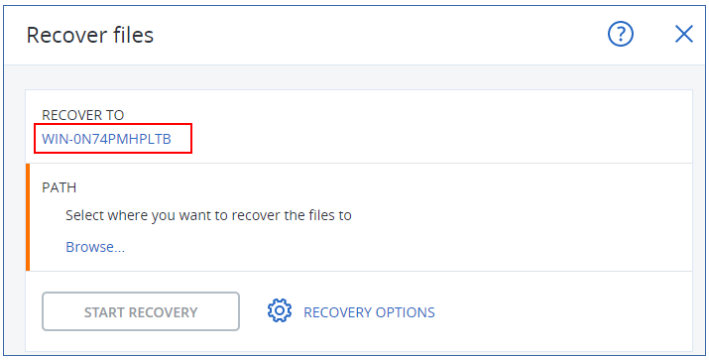
1. Cyber Protect 콘솔에서 **장치** > **Microsoft SQL**로 이동합니다.
2. 복구할 데이터베이스를 선택한 다음 **복구**를 클릭합니다.
3. 복구 지점을 선택합니다.

   복구 지점은 위치별로 필터링됩니다.
4. **복구** > **데이터베이스를 파일로**를 클릭합니다.
5. [원래 머신 외의 머신에 복구하는 경우] **복구 대상**에서 대상 머신을 선택합니다.

   이 머신에 데이터가 복구됩니다. 대상 머신은 온라인 상태여야 합니다.

   선택한 머신을 변경하려면 머신 이름을 클릭하고 다른 머신을 선택한 후에 **확인**을 클릭합니다.

© Acronis International GmbH, 2003-2024

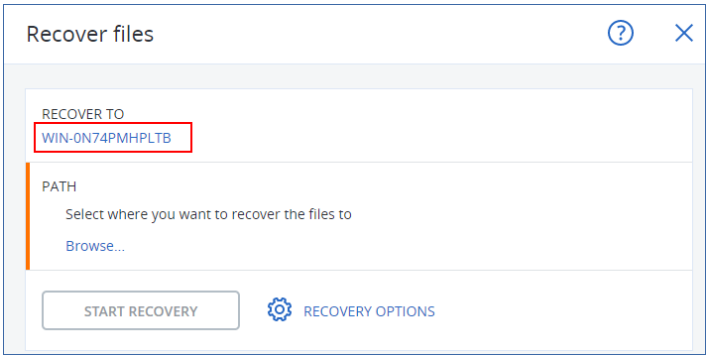


6. **경로**에서 **찾아보기**를 클릭하고 파일을 저장할 로컬 또는 네트워크 폴더를 선택한 후에 **완료**를 클릭합니다.
7. **복구 시작**을 클릭합니다.

애플리케이션 인식 백업에서 복구

이 절차는 온라인 원본 머신에 적용됩니다.

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 복구하려는 데이터가 원래 포함되어 있던 머신을 선택하고 **복구**를 클릭합니다.
3. 복구 지점을 선택합니다.
   복구 지점은 위치별로 필터링됩니다.
4. **복구** > **SQL 데이터베이스**를 클릭하고 복구할 데이터베이스를 선택한 후에 **파일로 복구**를 클릭합니다.
5. [원래 머신 외의 머신에 복구하는 경우] **복구 대상**에서 대상 머신을 선택합니다.
   이 머신에 데이터가 복구됩니다. 대상 머신은 온라인 상태여야 합니다.
   선택한 머신을 변경하려면 머신 이름을 클릭하고 다른 머신을 선택한 후에 **확인**을 클릭합니다.



6. **경로**에서 **찾아보기**를 클릭하고 파일을 저장할 로컬 또는 네트워크 폴더를 선택한 후에 **완료**를 클릭합니다.
7. **복구 시작**을 클릭합니다.

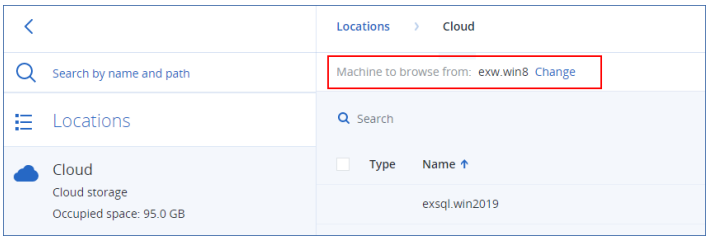
오프라인 머신의 백업에서 복구

이 절차는 오프라인 상태인 원본 머신의 애플리케이션 인식 백업과 데이터베이스 백업에 적용됩니다.

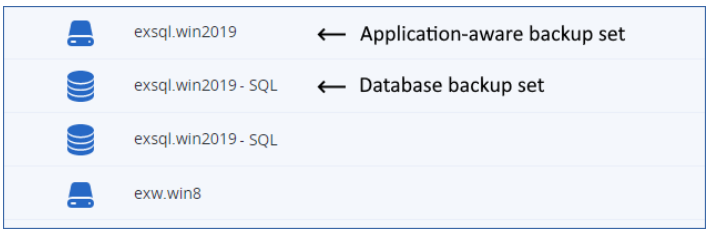
1. Cyber Protect 콘솔에서 **백업 스토리지**로 이동합니다.
2. 데이터를 복구하려는 백업 집합의 위치를 선택합니다.

© Acronis International GmbH, 2003-2024

3. **다음 위치에서 탐색할 머신**에서 대상 머신을 선택합니다.
   이 머신에 데이터가 복구됩니다. 대상 머신은 온라인 상태여야 합니다.



4. 백업 세트를 선택하고 **작업** 창에서 **백업 표시**를 클릭합니다.
   애플리케이션 인식 백업 세트와 데이터베이스 백업 세트는 각기 다른 아이콘으로 표시됩니다.



5. 복구하려는 데이터가 있는 복구 지점을 선택합니다.
6. [데이터베이스 백업의 경우] **SQL 데이터베이스 복구**를 클릭합니다.
7. [애플리케이션 인식 백업의 경우] **복구** > **SQL 데이터베이스**를 클릭합니다.
8. SQL Server 인스턴스를 선택하거나 인스턴스 이름을 클릭하여 복구할 특정 데이터베이스를 선택한 다음 **파일로 복구**를 클릭합니다.
9. **경로**에서 **찾아보기**를 클릭하고 파일을 저장할 로컬 또는 네트워크 폴더를 선택한 후에 **완료**를 클릭합니다.
10. **복구 시작**을 클릭합니다.

시스템 데이터베이스 복구

인스턴스의 모든 시스템 데이터베이스는 한 번에 복구됩니다. 시스템 데이터베이스를 복구하는 경우 단일 사용자 모드에서 목적지 인스턴스가 자동으로 다시 시작됩니다. 복구가 완료된 후, 소프트웨어가 인스턴스를 다시 시작하고 다른 데이터베이스(있는 경우)를 복구합니다.

시스템 데이터베이스를 복구하는 경우 고려할 기타 사항:

- 시스템 데이터베이스는 원본 인스턴스와 동일한 버전의 인스턴스로만 복구할 수 있습니다.
- 시스템 데이터베이스는 항상 "사용 준비" 상태에서 복구됩니다.

마스터 데이터베이스 복구

시스템 데이터베이스에는 **마스터** 데이터베이스가 포함되어 있습니다. **마스터** 데이터베이스는 인스턴스의 모든 데이터베이스에 대한 정보를 기록합니다. 따라서 백업의 **마스터** 데이터베이스에는 백업 당시 인스턴스에 있었던 데이터베이스에 대한 정보가 포함되어 있습니다. **마스터** 데이터베이스를 복구한 후 다음 작업을 수행해야 할 수 있습니다.

- 백업이 완료된 후 인스턴스에 나타난 데이터베이스는 인스턴스별로 표시되지 않습니다. 이러한 데이터베이스를 프로덕션 모드로 전환하려면 SQL Server Management Studio를 사용하여 인

© Acronis International GmbH, 2003-2024

스턴스에 수동으로 연결합니다.

- 백업 완료 후 삭제된 데이터베이스는 인스턴스에 오프라인으로 표시됩니다. SQL Server Management Studio를 사용하여 이러한 데이터베이스를 삭제합니다.

SQL Server 데이터베이스 연결

이 섹션에서는 SQL Server Management Studio를 사용하여 SQL Server에서 데이터베이스를 연결하는 방법에 대해 설명합니다. 한 번에 하나의 데이터베이스만 연결할 수 있습니다.

데이터베이스를 연결하려면 다음 권한이 필요합니다. **데이터베이스 생성**, **모든 데이터베이스 생성** 또는 **모든 데이터베이스 변경**. 일반적으로 이러한 권한은 인스턴스의 **sysadmin** 역할에 부여됩니다.

데이터베이스를 연결하려면

1. Microsoft SQL Server Management Studio를 실행합니다.
2. 필수 SQL Server 인스턴스에 연결한 다음 인스턴스를 확장합니다.
3. **데이터베이스**를 마우스 오른쪽 버튼으로 클릭하고 **연결**을 클릭합니다.
4. **추가**를 클릭합니다.
5. **데이터베이스 파일 찾기** 대화 상자에서 데이터베이스의 .mdf 파일을 찾아서 선택합니다.
6. **데이터베이스 세부정보** 섹션에서 나머지 데이터베이스 파일(.ndf 및 .ldf 파일)을 찾았는지 확인합니다.

   상세정보. 다음과 같은 경우 SQL Server 데이터베이스 파일을 자동으로 찾지 못할 수 있습니다.
   - 데이터베이스 파일이 기본 위치에 있지 않거나 기본 데이터베이스 파일(.mdf)과 동일한 폴더에 있지 않은 경우 해결 방법: **현재 파일 경로** 열에서 경로를 필수 파일로 수동으로 지정합니다.
   - 데이터베이스를 구성하는 불완전한 파일 세트를 복구한 경우 해결 방법: 백업에서 누락된 SQL Server 데이터베이스를 복구합니다.
7. 모든 파일을 찾으면 **확인**을 클릭합니다.

Exchange 데이터베이스 복구

이 섹션에서는 데이터베이스 백업과 애플리케이션 인식 백업 모두에서 복구하는 방법에 대해 설명합니다.

Exchange Server 데이터를 라이브 Exchange Server로 복구할 수 있습니다. 라이브 Exchange Server는 원래 Exchange Server일 수도 있고, FQDN(정규화된 도메인 이름)이 동일한 머신에서 실행 중인 동일한 버전의 Exchange Server일 수도 있습니다. Agent for Exchange가 대상 머신에 설치되어 있어야 합니다.

다음 표는 복구하려고 선택할 수 있는 Exchange Server 데이터와 이러한 데이터를 복구하는 데 필요한 최소 사용자 권한을 요약해서 보여줍니다.

Exchange 버전	데이터 항목	사용자 권한
2007	스토리지 그룹	**Exchange 조직 관리자** 역할 그룹의 구성원 자격.

© Acronis International GmbH, 2003-2024

2010/2013/2016/2019	데이터베이스	**서버 관리** 역할 그룹의 구성원 자격.

또는 데이터베이스(스토리지 그룹)를 파일로 복구할 수 있습니다. 트랜잭션 로그 파일과 함께 데이터베이스 파일은 백업에서 지정한 폴더로 추출됩니다. 감사 또는 서드 파티 도구로 추가 처리를 위해 데이터를 추출해야 하는 경우 또는 어떤 이유로든 복구에 실패하여 데이터베이스를 수동으로 마운트하는 방법을 찾고 있는 경우 이러한 기능이 유용할 수 있습니다.

Agent for VMware(Windows)만 사용하는 경우에는 데이터베이스를 파일로 복구하는 것이 유일하게 사용 가능한 복구 방법입니다. Agent for VMware(가상 어플라이언스)를 이용한 데이터 복구는 불가능합니다.

아래 절차 전체에서는 데이터베이스와 스토리지 그룹 둘 다를 "데이터베이스"라고 지칭할 것입니다.

Exchange 데이터베이스를 라이브 Exchange Server로 복구하려면

1. 다음 중 하나를 수행하십시오.
   - 애플리케이션 인식 백업에서 복구할 경우 **장치** 아래에서 복구할 데이터가 원래 포함된 머신을 선택합니다.
   - 데이터베이스 백업에서 복구할 경우 **장치** > **Microsoft Exchange** > **데이터베이스**를 클릭하고 복구할 데이터베이스를 선택합니다.
2. **복구**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.
   머신이 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 중 하나를 수행하십시오.
   - [애플리케이션 인식 백업에서 복구할 경우만 해당] 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 Agent for Exchange가 있는 온라인 머신을 선택한 다음 복구 지점을 선택합니다.
   - 백업 스토리지 탭에서 복구 지점을 선택합니다.

   위 작업 중 하나에서 찾기 위해 선택한 머신이 Exchange 데이터 복구의 대상 머신이 됩니다.
4. 다음 중 하나를 수행하십시오.
   - 애플리케이션 인식 백업에서 복구할 경우 **복구** > **Exchange 데이터베이스**를 클릭하고, 복구할 데이터베이스를 선택하고 나서, **복구**를 클릭합니다.
   - 데이터베이스 백업에서 복구할 경우 **복구** > **데이터베이스를 Exchange Server로**를 클릭합니다.
5. 기본적으로 데이터베이스는 원본 데이터베이스로 복구됩니다. 원본 데이터베이스가 없으면 재생성됩니다.
   데이터베이스를 다른 데이터베이스로 복구하려면:
   a. 데이터베이스 이름을 클릭합니다.
   b. **복구 대상**에서 **새 데이터베이스**를 선택합니다.
   c. 새 데이터베이스 이름을 지정합니다.
   d. 새 데이터베이스 경로 및 로그인 경로를 지정합니다. 지정한 폴더에는 원본 데이터베이스 및 로그 파일이 들어 있으면 안 됩니다.
6. **복구 시작**을 클릭합니다.

복구 진행률이 작업 탭에 표시됩니다.

© Acronis International GmbH, 2003-2024

Exchange 데이터베이스를 파일로 복구하려면

1. 다음 중 하나를 수행하십시오.
   - 애플리케이션 인식 백업에서 복구할 경우 **장치** 아래에서 복구할 데이터가 원래 포함된 머신을 선택합니다.
   - 데이터베이스 백업에서 복구할 경우 **장치** > **Microsoft Exchange** > **데이터베이스**를 클릭하고 복구할 데이터베이스를 선택합니다.
2. **복구**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.

   머신이 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 중 하나를 수행하십시오.
   - [애플리케이션 인식 백업에서 복구할 경우만 해당] 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 Agent for Exchange 또는 Agent for VMware가 있는 온라인 머신을 선택한 다음 복구 지점을 선택합니다.
   - 백업 스토리지 탭에서 복구 지점을 선택합니다.

   위 작업 중 하나에서 찾기 위해 선택한 머신이 Exchange 데이터 복구의 대상 머신이 됩니다.
4. 다음 중 하나를 수행하십시오.
   - 애플리케이션 인식 백업에서 복구할 경우 **복구** > **Exchange 데이터베이스**를 클릭하고, 복구할 데이터베이스를 선택하고 나서, **파일로 복구**를 클릭합니다.
   - 데이터베이스 백업에서 복구할 경우 **복구** > **데이터베이스를 파일로**를 클릭합니다.
5. **찾아보기**를 클릭하고 파일을 저장할 로컬 또는 네트워크 폴더를 선택합니다.
6. **복구 시작**을 클릭합니다.

복구 진행률이 작업 탭에 표시됩니다.

Exchange Server 데이터베이스 마운트

데이터베이스 파일을 복구한 다음 마운팅하여 온라인으로 데이터베이스를 가져올 수 있습니다. 마운팅은 Exchange Management Console, Exchange System Manager 또는 Exchange Management Shell을 사용하여 수행됩니다.

복구된 데이터베이스는 부적절한 종료 상태가 됩니다. 부적절한 종료 상태에 있는 데이터베이스는 원래 위치로 복구되는 경우(즉, 원본 데이터베이스 정보가 Active Directory에 있는 경우) 시스템에서 마운팅할 수 있습니다. 다른 위치(예: 새 데이터베이스 또는 복구 데이터베이스)에 데이터베이스를 복구하는 경우에는 `Eseutil /r <Enn>` 명령을 사용하여 정상 종료 상태로 전환할 때까지 데이터베이스를 마운트할 수 없습니다. `<Enn>`은 트랜잭션 로그 파일을 적용해야 하는 데이터베이스(또는 데이터베이스를 포함하는 스토리지 그룹)에 대한 로그 파일 접두사를 지정합니다.

데이터베이스를 첨부하는 데 사용하는 계정은 대상 서버에 Exchange Server 관리자 역할 및 로컬 관리자 그룹으로 위임해야 합니다.

데이터베이스를 마운트하는 방법에 대한 자세한 사항은 다음 문서를 참고하십시오.

- Exchange 2010 이상: http://technet.microsoft.com/en-us/library/aa998871.aspx
- Exchange 2007: http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.80).aspx

© Acronis International GmbH, 2003-2024

Exchange 사서함 및 사서함 항목 복구

다음 백업에서 Exchange 사서함 및 사서함 항목을 복구할 수 있습니다.

- 데이터베이스 백업
- 애플리케이션 인식 백업
- 사서함 백업

다음 항목을 복구할 수 있습니다.

- 사서함(아카이브 사서함 제외)
- 공용 폴더

> **참고**
> 데이터베이스 백업에서만 사용 가능합니다. "Exchange Server 데이터 선택"(513페이지)을(를) 참조하십시오.

- 공용 폴더 항목
- 이메일 폴더
- 이메일 메시지
- 달력 이벤트
- 작업
- 연락처
- 업무 일지
- 메모

검색 기능을 사용해 항목을 찾을 수 있습니다.

사서함 또는 사서함 항목은 라이브 Exchange Server 또는 Microsoft 365로 복구할 수 있습니다.

Exchange Server로 복구

개별 복구는 Microsoft Exchange Server 2010 서비스 팩 1(SP1)이상에서 수행할 수 있습니다. 소스 백업은 지원되는 모든 Exchange 버전의 데이터베이스 또는 사서함을 포함할 수 있습니다.

개별 복구는 Agent for Exchange 또는 Agent for VMware(Windows)를 통해 수행할 수 있습니다. 대상 Exchange Server 및 에이전트를 실행하는 머신은 동일한 Active Directory 포리스트에 속해 있어야 합니다.

기존 사서함으로 사서함을 복구하면 일치하는 ID의 기존 항목이 덮어써집니다.

사서함 항목 복구 시에는 무엇도 덮어쓰지 않습니다. 대신, 사서함 항목의 전체 경로가 대상 폴더에 재생성됩니다.

사용자 계정에 대한 요구 사항

백업에서 복구하는 사서함은 Active Directory에 연결된 사용자 계정이 있어야 합니다.

© Acronis International GmbH, 2003-2024

사용자 사서함 및 그 내용은 연결된 사용자 계정이 *활성화됨* 상태인 경우에만 복구할 수 있습니다. 공유, 대화방 및 장비 사서함은 연결된 사용자 계정이 *비활성화됨* 상태인 경우에만 복구할 수 있습니다.

위의 조건을 충족하지 않는 사서함은 복구 중 건너뜁니다.

일부 사서함을 건너뛴 경우에는 경고가 표시되지만 복구는 성공합니다. 모든 사서함을 건너뛰면 복구가 실패합니다.

Microsoft 365로 복구

Exchange 데이터 항목을 Microsoft 365로, 또는 그 반대로 복구하는 작업은 Agent for Microsoft 365가 로컬로 설치되어 있다는 조건 하에서 지원됩니다.

복구는 Microsoft Exchange Server 2010 이상의 백업에서 수행할 수 있습니다.

기존 Microsoft 365 사서함으로 사서함을 복구하면 기존 항목은 그대로 유지되고, 복구된 항목이 기존 항목 옆에 위치합니다.

단일 사서함을 복구할 때에는 대상 Microsoft 365 사서함을 선택해야 합니다. 하나의 복구 작업으로 여러 사서함을 복구할 때에는 사용자 이름이 같은 사용자의 사서함으로 각 사서함을 복구합니다. 사용자 이름이 같은 사용자가 없는 사서함은 건너뜁니다. 일부 사서함을 건너뛴 경우에는 경고가 표시되지만 복구는 성공합니다. 모든 사서함을 건너뛰면 복구가 실패합니다.

Microsoft 365로 복구에 대한 자세한 내용은 "Microsoft 365 데이터 보호"(545페이지) 항목을 참조하십시오.

사서함 복구

애플리케이션 인식 백업 또는 데이터베이스 백업에서 사서함을 복구하려면

1. [데이터베이스 백업을 Microsoft 365로 복구하는 경우에만 해당] Agent for Microsoft 365가 백업한 Exchange Server를 실행하는 머신에 설치되어 있지 않다면 다음 중 하나를 수행합니다.
   - 조직에 Agent for Microsoft 365가 없는 경우 백업한 머신에 Agent for Microsoft 365를 설치합니다(또는 같은 Microsoft Exchange Server 버전을 가진 다른 머신에 설치).
   - 조직에 Agent for Microsoft 365가 이미 있는 경우에는 "Microsoft Exchange 라이브러리 복사"에 설명되어 있는 대로 백업한 머신에서(또는 같은 Microsoft Exchange Server 버전이 있는 다른 머신에서) Agent for Microsoft 365가 있는 머신으로 라이브러리를 복사합니다.
2. 다음 중 하나를 수행하십시오.
   - 애플리케이션 인식 백업에서 복구할 경우 **장치** 아래에서 복구할 데이터가 원래 포함된 머신을 선택합니다.
   - 데이터베이스 백업에서 복구할 경우 **장치** > **Microsoft Exchange** > **데이터베이스**를 클릭하고 복구할 데이터가 원래 포함된 데이터베이스를 선택합니다.
3. **복구**를 클릭합니다.
4. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.

   머신이 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 두 가지 방법으로 복구합니다.

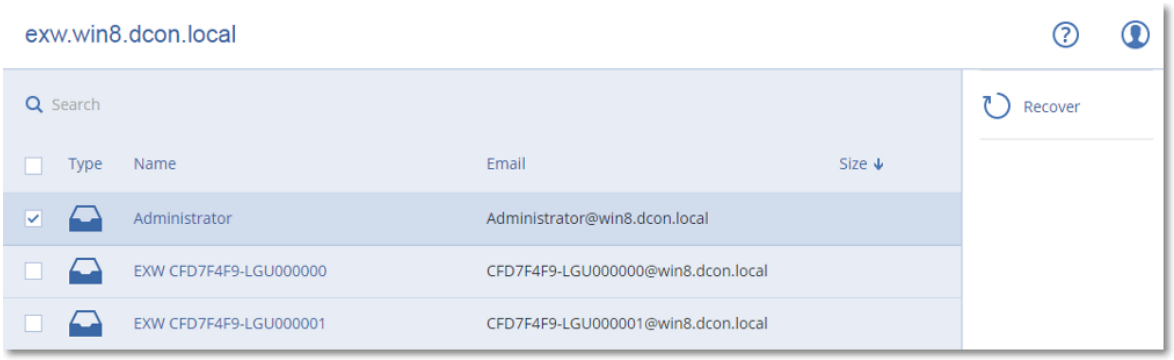
© Acronis International GmbH, 2003-2024

- [애플리케이션 인식 백업에서 복구할 경우만 해당] 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 Agent for Exchange 또는 Agent for VMware가 있는 온라인 머신을 선택한 다음 복구 지점을 선택합니다.
- 백업 스토리지 탭에서 복구 지점을 선택합니다.

위 작업 중 하나에서 찾기 위해 선택한 머신이 오프라인인 원래 머신 대신 복구를 수행합니다.

5. **복구** > **Exchange 사서함**을 클릭합니다.
6. 복구할 사서함을 선택합니다.

   사서함을 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.



7. **복구**를 클릭합니다.
8. [Microsoft 365로 복구하는 경우만 해당]:
   a. **복구 대상**에서 **Microsoft 365**를 선택합니다.
   b. [6단계에서 사서함 하나만 선택한 경우] **대상 사서함**에서 대상 사서함을 지정합니다.
   c. **복구 시작**을 클릭합니다.

   이 절차의 추가 단계는 필수 단계가 아닙니다.

   대상 머신을 선택하거나 변경하려면 **Microsoft Exchange Server가 포함된 대상 머신**을 클릭합니다. 이 단계를 통해 Agent for Exchange를 실행 중이지 않은 머신으로 복구할 수 있습니다.

   클라이언트 액세스 역할(Microsoft Exchange Server 2010/2013) 또는 **사서함 역할**(Microsoft Exchange Server 2016 이상)이 활성화되어 있는 머신의 FQDN(정규화된 도메인 이름)을 지정합니다. 이 머신은 복구를 수행하는 머신과 같은 Active Directory 포리스트에 속해 있어야 합니다.
9. 메시지가 표시되면 시스템에 액세스하는 데 사용될 계정의 자격 증명을 제공합니다. 이 계정에 대한 요구사항이 "필수 사용자 권한"에 나열됩니다.
10. [선택 사항] 자동으로 선택된 데이터베이스를 변경하려면 **누락된 사서함을 재생성할 데이터베이스**를 클릭합니다.
11. **복구 시작**을 클릭합니다.

복구 진행률이 **작업** 탭에 표시됩니다.

사서함 백업에서 사서함을 복구하려면

1. **장치** > **Microsoft Exchange** > **사서함**을 클릭합니다.
2. 복구할 사서함을 선택한 다음 **복구**를 클릭합니다.

   사서함을 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.

   사서함이 삭제된 경우 백업 스토리지 탭에서 이를 선택한 다음 **백업 표시**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.

© Acronis International GmbH, 2003-2024

4. **복구** > **사서함**을 클릭합니다.
5. 위 절차의 8-11단계를 수행합니다.

사서함 항목 복구

애플리케이션 인식 백업 또는 데이터베이스 백업에서 사서함 항목을 복구하려면

1. [데이터베이스 백업을 Microsoft 365로 복구하는 경우에만 해당] Agent for Microsoft 365가 백업한 Exchange Server를 실행하는 머신에 설치되어 있지 않다면 다음 중 하나를 수행합니다.
   - 조직에 Agent for Microsoft 365가 없는 경우 백업한 머신에 Agent for Microsoft 365를 설치합니다(또는 같은 Microsoft Exchange Server 버전을 가진 다른 머신에 설치).
   - 조직에 Agent for Microsoft 365가 이미 있는 경우에는 "Microsoft Exchange 라이브러리 복사"에 설명되어 있는 대로 백업한 머신에서(또는 같은 Microsoft Exchange Server 버전이 있는 다른 머신에서) Agent for Microsoft 365가 있는 머신으로 라이브러리를 복사합니다.
2. 다음 중 하나를 수행하십시오.
   - 애플리케이션 인식 백업에서 복구할 경우 **장치** 아래에서 복구할 데이터가 원래 포함된 머신을 선택합니다.
   - 데이터베이스 백업에서 복구할 경우 **장치** > **Microsoft Exchange** > **데이터베이스**를 클릭하고 복구할 데이터가 원래 포함된 데이터베이스를 선택합니다.
3. **복구**를 클릭합니다.
4. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.

   머신이 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 두 가지 방법으로 복구합니다.
   - [애플리케이션 인식 백업에서 복구할 경우만 해당] 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 Agent for Exchange 또는 Agent for VMware가 있는 온라인 머신을 선택한 다음 복구 지점을 선택합니다.
   - 백업 스토리지 탭에서 복구 지점을 선택합니다.

   위 작업 중 하나에서 찾기 위해 선택한 머신이 오프라인인 원래 머신 대신 복구를 수행합니다.
5. **복구** > **Exchange 사서함**을 클릭합니다.
6. 복구하려는 항목이 원래 포함되어 있는 사서함을 클릭합니다.
7. 복구할 항목을 선택합니다.

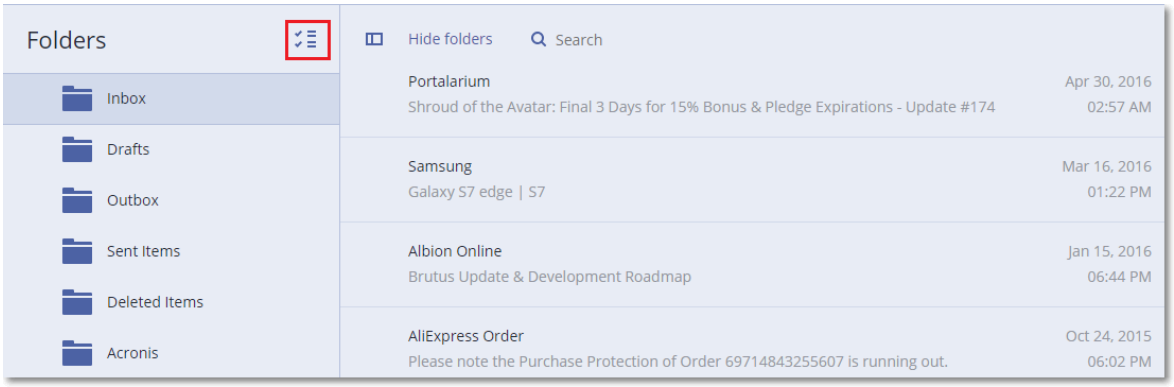
   다음 검색 옵션을 사용할 수 있습니다. 와일드카드는 지원되지 않습니다.
   - 이메일 메시지: 제목, 보낸 사람, 받는 사람, 날짜로 검색합니다.
   - 이벤트: 제목 및 날짜로 검색합니다.
   - 작업: 제목 및 날짜로 검색합니다.
   - 연락처: 이름, 이메일 주소, 전화번호로 검색합니다.

   이메일 메시지를 선택한 경우 **내용 표시**를 클릭해 첨부 파일을 포함한 내용을 볼 수 있습니다.

   참고
   첨부 파일을 다운로드하려면 그 이름을 클릭하십시오.

© Acronis International GmbH, 2003-2024

폴더를 선택하려면 폴더 복구 아이콘을 클릭하십시오.



8. **복구**를 클릭합니다.
9. Microsoft 365로 복구하려면 **복구 대상**에서 **Microsoft 365**를 선택합니다.

   Exchange Server를 복구하려면 **복구 대상**에서 기본값인 **Microsoft Exchange** 값을 유지합니다.

   [Exchange Server로 복구하는 경우에만 해당] 대상 머신을 선택하거나 변경하려면 **Microsoft Exchange Server가 포함된 대상 머신**을 클릭합니다. 이 단계를 통해 Agent for Exchange를 실행 중이지 않은 머신으로 복구할 수 있습니다.

   클라이언트 액세스 역할(Microsoft Exchange Server 2010/2013) 또는 **사서함 역할**(Microsoft Exchange Server 2016 이상)이 활성화되어 있는 머신의 FQDN(정규화된 도메인 이름)을 지정합니다. 이 머신은 복구를 수행하는 머신과 같은 Active Directory 포리스트에 속해 있어야 합니다.
10. 메시지가 표시되면 시스템에 액세스하는 데 사용될 계정의 자격 증명을 제공합니다. 이 계정에 대한 요구사항이 "필수 사용자 권한"에 나열됩니다.
11. **대상 사서함**에서 대상 사서함을 보고, 변경하거나 지정합니다.

    기본적으로 원래 사서함이 선택됩니다. 이 사서함이 존재하지 않거나 원래 대상 머신이 아닌 머신을 선택한 경우에는 대상 사서함을 지정해야 합니다.
12. [이메일 메시지를 복구할 경우만 해당] **대상 폴더**에서 대상 사서함의 대상 폴더를 보거나 변경합니다. 기본적으로 **복구 항목** 폴더가 선택되어 있습니다. Microsoft Exchange 제한으로 인해 이벤트, 작업, 메모 및 연락처는 다른 **대상 폴더** 지정하지 않은 원래 위치에 복원됩니다.
13. **복구 시작**을 클릭합니다.

복구 진행률이 **작업** 탭에 표시됩니다.

사서함 백업에서 사서함 항목을 복구하려면

1. **장치** > **Microsoft Exchange** > **사서함**을 클릭합니다.
2. 복구하려는 항목이 원래 포함되어 있는 사서함을 선택한 다음 **복구**를 클릭합니다.

   사서함을 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.

   사서함이 삭제된 경우 백업 스토리지 탭에서 이를 선택한 다음 **백업 표시**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.
4. **복구** > **이메일 메시지**를 클릭합니다.
5. 복구할 항목을 선택합니다.

   다음 검색 옵션을 사용할 수 있습니다. 와일드카드는 지원되지 않습니다.

   - 이메일 메시지: 제목, 보낸 사람, 받는 사람, 날짜로 검색합니다.
   - 이벤트: 제목 및 날짜로 검색합니다.

© Acronis International GmbH, 2003-2024

- 작업: 제목 및 날짜로 검색합니다.
- 연락처: 이름, 이메일 주소, 전화번호로 검색합니다.

이메일 메시지를 선택한 경우 **내용 표시**를 클릭해 첨부 파일을 포함한 내용을 볼 수 있습니다.

참고
첨부 파일을 다운로드하려면 그 이름을 클릭하십시오.

이메일 메시지를 선택한 경우 **이메일로 보내기**를 클릭해 해당 메시지를 지정한 이메일 주소로 보낼 수 있습니다. 관리자 계정의 이메일 주소에서 메시지가 전송됩니다.

폴더를 선택하려면 폴더 복구 아이콘 을 클릭하십시오.

6. **복구**를 클릭합니다.
7. 위 절차의 9-13단계를 수행합니다.

Microsoft Exchange Server 라이브러리 복사

Exchange 사서함 또는 사서함 항목을 Microsoft 365로 복구할 때에는 백업된 머신에서(또는 같은 Microsoft Exchange Server 버전이 있는 다른 머신에서) Agent for Microsoft 365가 있는 머신으로 다음 라이브러리를 복사해야 할 수 있습니다.

백업된 Microsoft Exchange Server 버전에 따라 다음 파일을 복사합니다.

Microsoft Exchange Server 버전	라이브러리	기본 위치
Microsoft Exchange Server 2010	ese.dll esebcli2.dll store.exe	%ProgramFiles%\Microsoft\Exchange Server\V14\bin
Microsoft Exchange Server 2013	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll	%WINDIR%\system32
Microsoft Exchange Server 2016, 2019	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll msvcp110.dll	%WINDIR%\system32

라이브러리는 %ProgramData%\Acronis\ese 폴더에 위치해야 합니다. 이 폴더가 존재하지 않는 경우 수동으로 생성하십시오.

SQL Server 또는 Exchange Server 액세스 자격 증명 변경

에이전트를 다시 설치하지 않고 SQL Server 또는 Exchange Server에 대한 액세스 자격 증명을 변경할 수 있습니다.

SQL Server 또는 Exchange Server 액세스 자격 증명을 변경하려면

© Acronis International GmbH, 2003-2024

1. **장치**를 클릭하고 **Microsoft SQL** 또는 **Microsoft Exchange**를 클릭합니다.
2. 액세스 자격 증명을 변경할 Always On 가용성 그룹, 데이터베이스 가용성 그룹, SQL Server 인스턴스 또는 Exchange Server를 선택합니다.
3. **자격 증명 지정**을 클릭합니다.
4. 새 액세스 자격 증명을 지정한 다음 **확인**을 클릭합니다.

사서함 백업을 위해 Exchange Server 액세스 자격 증명을 변경하려면

1. **장치** > **Microsoft Exchange**를 클릭한 다음, **사서함**을 확장합니다.
2. 액세스 자격 증명을 변경할 Exchange Server를 선택합니다.
3. **설정**을 클릭합니다.
4. **Exchange 관리자 계정**에서 새 액세스 자격 증명을 지정한 다음 **저장**을 클릭합니다.

모바일 장치 보호

Cyber Protect 앱을 사용하면 모바일 데이터를 클라우드 스토리지에 백업해 두었다가, 데이터 손실 또는 손상이 발생했을 때 복구하는 것이 가능합니다. 클라우드 스토리지로 백업하려면 계정 및 클라우드 가입이 필요합니다.

지원되는 모바일 장치

Cyber Protect 앱은 다음과 같은 운영 체제 중 하나를 실행하는 모바일 장치에 설치할 수 있습니다.

- iOS 14~iOS 16(iPhone, iPod, iPad)
- Android 9~Android 13

백업할 수 있는 항목

- 연락처(이름, 전화번호, 이메일)
- 사진(사진의 원래 크기와 형식은 보존됨)
- 비디오
- 일정표
- 미리 알림(iOS 장치만 해당)

알아야 할 사항

- 클라우드 스토리지에만 데이터를 백업할 수 있습니다.
- 앱을 열 때마다 데이터 변경 사항의 요약을 확인할 수 있으며 백업을 수동으로 시작할 수 있습니다.
- **지속 백업** 기능은 기본적으로 활성화됩니다. 이 설정을 켜면 Cyber Protect 앱이 새 데이터를 즉시 자동으로 감지하여 클라우드에 업로드합니다.
- 앱 설정에서 기본적으로 **Wi-Fi만 사용** 옵션이 활성화되어 있습니다. 이 설정이 켜지면, Wi-Fi 연결을 사용할 수 있는 경우에만 Cyber Protect 앱이 데이터를 백업합니다. Wi-Fi 연결이 끊어지면 백업 프로세스가 시작되지 않습니다. 앱에서 셀룰러 연결도 사용할 수 있도록 하려면 이 옵션을 끕니다.

© Acronis International GmbH, 2003-2024

- 장치의 배터리 최적화 기능으로 인해 Cyber Protect 앱이 올바르게 작동하지 못할 수도 있습니다. 백업을 정시에 실행하려면 앱의 배터리 최적화를 중지해야 합니다.
- 에너지를 절약하는 두 가지 방법이 있습니다.
  - **충전하는 동안 백업** 기능은 기본적으로 비활성화되어 있습니다. 이 설정이 켜지면, 장치가 전원에 연결된 경우에만 Cyber Protect 앱이 데이터를 백업합니다. 지속적인 백업 프로세스 동안 장치가 전원에서 분리되면 백업이 일시 중지됩니다.
  - **절전 모드**는 기본적으로 활성화되어 있습니다. 이 설정이 켜지면, 장치의 배터리 잔량이 낮지 않은 경우에만 Cyber Protect 앱이 데이터를 백업합니다. 장치의 배터리 잔량이 낮아지면 지속적인 백업이 일시 중지됩니다.
- 해당 계정으로 등록한 모바일 장치에서 백업된 데이터에 액세스할 수 있습니다. 이를 통해 이전 모바일 장치에서 새로운 장치로 데이터를 전송할 수 있습니다. Android 장치의 연락처 및 사진을 iOS 장치로 복구하거나 이와 반대로 복구할 수 있습니다. 또한 Cyber Protect 콘솔을 사용하여 사진, 비디오 또는 연락처를 모든 장치에 다운로드할 수도 있습니다.
- 본인 계정으로 등록한 모바일 장치에서 백업한 데이터는 이 계정으로만 사용할 수 있습니다. 다른 누구도 해당 데이터를 보거나 복구할 수 없습니다.
- Cyber Protect 앱에서 최신 데이터 버전만 복구할 수 있습니다. 특정 백업 버전에서 복구해야 하는 경우 태블릿 또는 컴퓨터에서 Cyber Protect 콘솔을 사용합니다.
- 보관 규칙은 모바일 장치의 백업에 적용되지 않습니다.
- [Android 장치만 해당] 백업하는 동안 SD 카드가 있는 경우 이 카드에 저장된 데이터도 백업됩니다. 복구하는 동안 SD 카드가 있는 경우 데이터가 이 SD 카드의 **백업에서 복구됨** 폴더에 복구되거나, 앱에서 데이터를 복구할 다른 위치를 묻습니다.

Cyber Protect 앱 다운로드 방법

모바일 장치에 따라 App Store 또는 Google Play에서 앱을 설치합니다.

데이터 백업 시작 방법

1. 앱을 엽니다.
2. 사용자 계정으로 로그인합니다.
3. **설정**을 탭해서 백업을 생성합니다. 모바일 장치에 백업이 없는 경우에만 이 버튼이 나타납니다.
4. 백업하려는 데이터 카테고리를 선택합니다. 기본적으로 모든 범주가 선택되어 있습니다.
5. [선택 단계] 백업을 암호화로 보호하려면 **백업 암호화**를 활성화합니다. 이 경우 다음 작업도 필요합니다.
   a. 암호화 비밀번호를 두 번 입력합니다.

      참고
      비밀번호를 잊어버리면 복구하거나 변경할 수 없으므로 비밀번호를 잘 기억해 두십시오.

   b. **암호화**를 탭합니다.
6. **백업**을 누릅니다.

© Acronis International GmbH, 2003-2024

7. 앱에서 개인용 데이터에 액세스하도록 허용합니다. 일부 데이터 카테고리에 대한 액세스를 거부하면 해당 데이터는 백업되지 않습니다.

백업이 시작됩니다.

데이터를 모바일 장치로 복구하는 방법

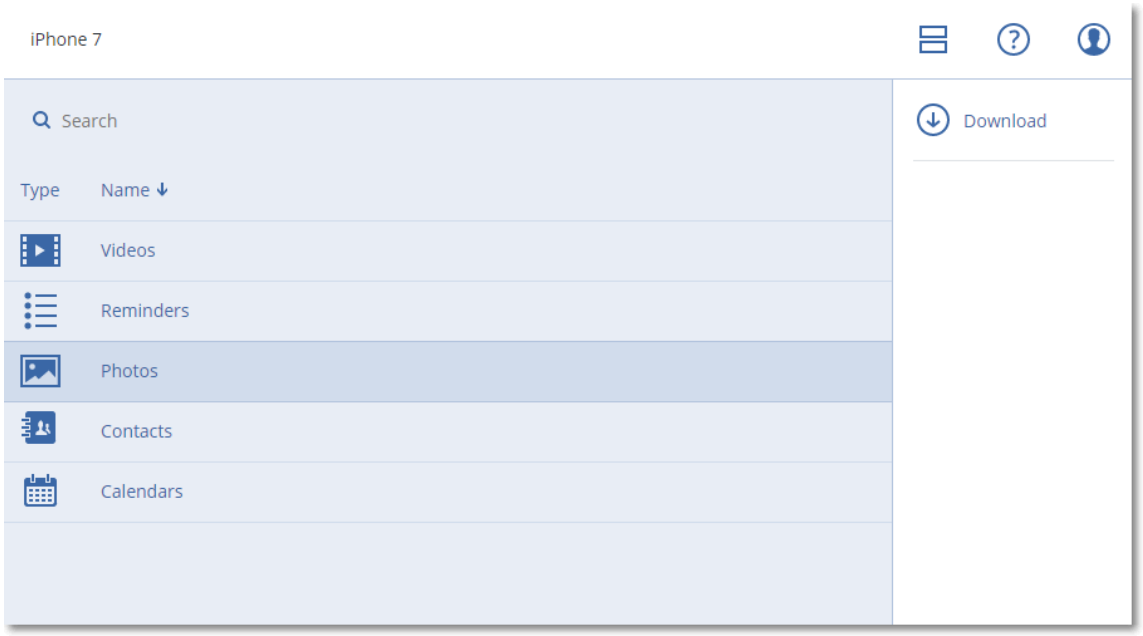
경고!
모바일 데이터를 복구하려면 최종 사용자 계정을 사용해야 합니다.

1. Cyber Protect 앱을 엽니다.
2. **찾아보기**를 탭합니다.
3. 장치 이름을 누릅니다.
4. 다음 중 하나를 수행하십시오.
   - 백업한 데이터를 모두 복구하려면 **모두 복구**를 누릅니다. 추가 작업은 필요하지 않습니다.
   - 하나 이상의 데이터 카테고리를 복구하려면 **선택**을 누른 다음 필요한 데이터 카테고리의 확인란을 누릅니다. **복구**를 누릅니다. 추가 작업은 필요하지 않습니다.
   - 동일한 데이터 카테고리에 속한 하나 이상의 데이터 항목을 복구하려면 데이터 카테고리를 누릅니다. 추가 단계를 진행합니다.
5. 다음 중 하나를 수행하십시오.
   - 단일 데이터 항목을 복구하려면 해당 항목을 누릅니다.
   - 여러 데이터 항목을 복구하려면 **선택**을 누른 다음 필요한 데이터 항목의 확인란을 누릅니다.
6. **복구**를 누릅니다.

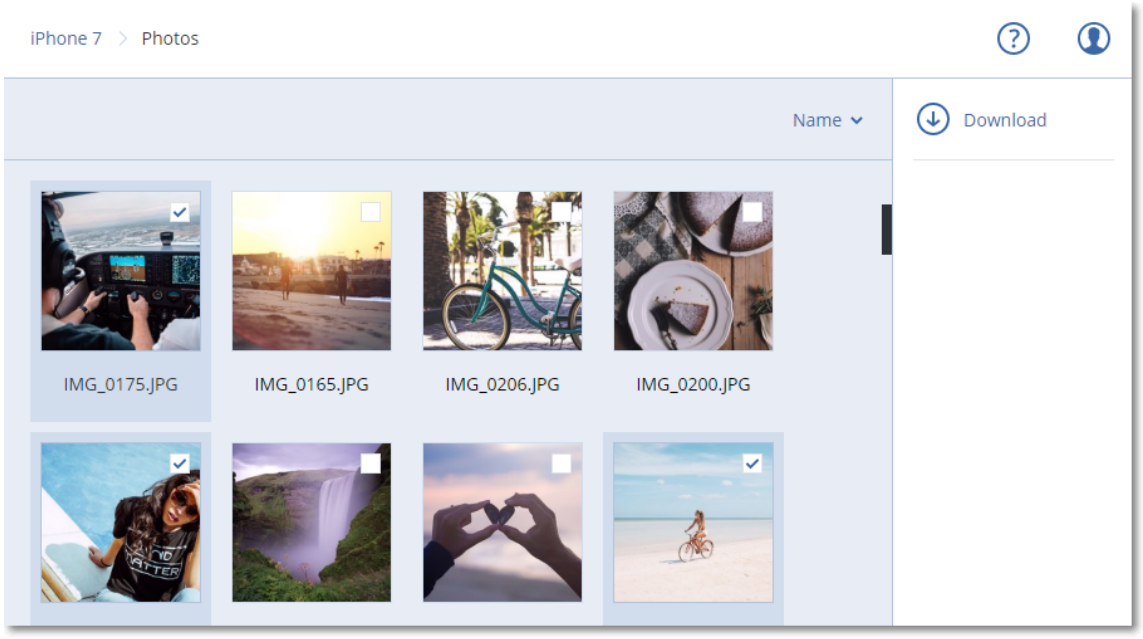
Cyber Protect 콘솔을 통해 데이터를 검토하는 방법

1. 컴퓨터에서 브라우저를 열고 Cyber Protect 콘솔 URL을 입력합니다.
2. 사용자 계정으로 로그인합니다.
3. **모든 장치**에서 모바일 장치 이름 아래의 **복구**를 클릭합니다.
4. 다음 중 하나를 수행하십시오.
   - 모든 사진, 비디오, 연락처, 달력 또는 미리 알림을 다운로드하려면 해당 데이터 카테고리를 선택합니다. **다운로드**를 클릭합니다.

© Acronis International GmbH, 2003-2024



- 개별 사진, 비디오, 연락처, 달력 또는 미리 알림을 다운로드하려면 해당 데이터 카테고리 이름을 클릭한 다음 필요한 데이터 항목의 확인란을 선택합니다. **다운로드**를 클릭합니다.



- 사진 또는 연락처를 미리 보려면 해당 데이터 카테고리 이름을 클릭한 다음 필요한 데이터 항목을 클릭합니다.

Hosted Exchange 데이터 보호

어떤 항목을 백업할 수 있습니까?

사용자 사서함, 공유 사서함, 그룹 사서함을 백업할 수 있습니다. 옵션으로 선택한 사서함의 아카이브 사서함 백업을 선택할 수 있습니다(**내부 아카이브**).

© Acronis International GmbH, 2003-2024

복구할 수 있는 항목은 무엇입니까?

다음과 같은 항목을 사서함 백업에서 복구할 수 있습니다.

- 사서함
- 이메일 폴더
- 이메일 메시지
- 달력 이벤트
- 작업
- 연락처
- 업무 일지
- 메모

검색 기능을 사용해 항목을 찾을 수 있습니다.

사서함, 사서함 항목, 공용 폴더 및 공용 폴더 항목을 복구할 때 대상 위치의 항목을 복구할 것인지 선택할 수 있습니다.

기존 사서함으로 사서함을 복구하면 일치하는 ID의 기존 항목이 덮어써집니다.

사서함 항목 복구 시에는 무엇도 덮어쓰지 않습니다. 대신, 사서함 항목의 전체 경로가 대상 폴더에 재생성됩니다.

Exchange Online 사서함 선택

아래 설명에 따라 사서함을 선택한 다음, 보호 계획의 기타 설정을 적절하게 지정합니다.

Exchange 온라인 사서함을 선택하려면

1. **장치 > Hosted Exchange**를 클릭합니다.
2. 여러 Hosted Exchange 조직을 Cyber Protection 서비스에 추가한 경우, 사용자 데이터의 백업을 원하는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. 다음 중 하나를 수행하십시오.
   - 전체 사용자의 사서함과 공유 사서함(앞으로 생성될 사서함 포함)을 백업하려면, **사용자** 노드를 확장하고 **전체 사용자**를 선택한 후 **그룹 백업**을 클릭합니다.
   - 개별적인 사용자 또는 공유 사서함을 백업하려면, **사용자** 노드를 확장하고 **전체 사용자**를 선택한 다음 백업하려는 사서함의 사용자를 선택한 후 **백업**을 클릭합니다.
   - 전체 그룹 사서함(앞으로 생성될 그룹의 사서함 포함)을 백업하려면, **그룹** 노드를 확장하고 **전체 그룹**을 선택한 후 **그룹 백업**을 클릭합니다.
   - 개별 그룹 사서함을 복구하려면, **그룹** 노드를 확장하고 **전체 그룹**을 선택하고 백업하려는 사서함의 그룹을 선택한 후 **백업**을 클릭합니다.

© Acronis International GmbH, 2003-2024

사서함 및 사서함 항목 복구

사서함 복구

1. **장치 > Hosted Exchange**를 클릭합니다.
2. 여러 Hosted Exchange 조직을 Cyber Protection 서비스에 추가한 경우 백업 데이터의 복구를 원하는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. 다음 중 하나를 수행하십시오.
   - 사용자 사서함을 복구하려면, **사용자** 노드를 확장하고 **전체 사용자**를 선택하고 복구하려는 사서함의 사용자를 선택한 후 **복구**를 클릭합니다.
   - 공유 사서함을 복구하려면, **사용자** 노드를 확장하고 **전체 사용자**를 선택한 다음 복구하려는 공유 사서함을 선택한 후 **복구**를 클릭합니다.
   - 그룹 사서함의 항목을 복구하려면, **그룹** 노드를 확장하고 **전체 그룹**을 선택하고 복구하려는 사서함의 그룹을 선택한 후 **복구**를 클릭합니다.
   - 사용자 그룹 또는 공유 사서함이 삭제되었다면 백업 스토리지 탭의 **클라우드 애플리케이션 백업** 섹션에서 해당 항목을 선택한 후 **백업 표시**를 클릭합니다.

   사용자와 그룹은 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.
4. 복구 지점을 선택합니다.
5. **복구 > 전체 사서함**을 클릭합니다.
6. 여러 Hosted Exchange 조직을 Cyber Protection 서비스에 추가한 경우, **Hosted Exchange 조직**을 클릭하여 대상 조직을 보기, 변경 또는 지정합니다.

   기본적으로 원래 조직이 선택됩니다. 이 조직이 Cyber Protection 서비스에 등록되지 않았다면 대상 조직을 지정해야 합니다.
7. **사서함으로 복구**에서 대상 사서함을 보고, 변경하거나 지정합니다.

   기본적으로 원래 사서함이 선택됩니다. 이 사서함이 존재하지 않거나 원래 이외 조직을 선택한 경우에는 대상 사서함을 지정해야 합니다.
8. **복구 시작**을 클릭합니다.
9. 다음 덮어쓰기 옵션 중 하나를 선택합니다.
   - **기존 항목 덮어쓰기**
   - **기존 항목 덮어쓰기 안 함**
10. **진행**을 클릭하여 결정을 확인합니다.

사서함 항목 복구

1. **장치 > Hosted Exchange**를 클릭합니다.
2. 여러 Hosted Exchange 조직을 Cyber Protection 서비스에 추가한 경우 백업 데이터의 복구를 원하는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. 다음 중 하나를 수행하십시오.
   - 사용자 사서함의 항목을 복구하려면, **사용자** 노드를 확장하고 **전체 사용자**를 선택하고 복구하려는 항목이 원래 포함된 사서함의 사용자를 선택한 후 **복구**를 클릭합니다.

© Acronis International GmbH, 2003-2024

- 공유 사서함의 항목을 복구하려면, **사용자** 노드를 확장하고 **전체 사용자**를 선택한 다음 처음에 복구하려는 항목을 포함하고 있던 공유 사서함을 선택한 후 **복구**를 클릭합니다.
- 그룹 사서함의 항목을 복구하려면, **그룹** 노드를 확장하고 **전체 그룹**을 선택하고 복구하려는 항목이 원래 포함된 사서함의 그룹을 선택한 후 **복구**를 클릭합니다.
- 사용자 그룹 또는 공유 사서함이 삭제되었다면 백업 스토리지 탭의 **클라우드 애플리케이션 백업** 섹션에서 해당 항목을 선택한 후 **백업 표시**를 클릭합니다.

사용자와 그룹은 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.

4. 복구 지점을 선택합니다.
5. **복구** > **이메일 메시지**를 클릭합니다.
6. 필요한 폴더를 찾거나 검색 기능을 사용하여 필요한 항목 목록을 얻습니다.

   다음 검색 옵션을 사용할 수 있습니다. 와일드카드는 지원되지 않습니다.
   - 이메일 메시지: 제목, 보낸 사람, 받는 사람, 첨부 파일 이름, 날짜로 검색합니다.
   - 이벤트: 제목 및 날짜로 검색합니다.
   - 작업: 제목 및 날짜로 검색합니다.
   - 연락처: 이름, 이메일 주소, 전화번호로 검색합니다.
7. 복구할 항목을 선택합니다. 폴더를 선택하려면 "폴더 복구" 아이콘 을 클릭하십시오.

   뿐만 아니라 다음을 수행할 수 있습니다.
   - 항목을 선택한 경우 첨부 파일을 포함한 내용을 보려면 **내용 표시**를 클릭하십시오. 첨부 파일을 다운로드하려면 그 이름을 클릭하십시오.
   - 이메일 메시지나 달력 항목을 선택한 경우 **이메일로 보내기**를 클릭해 해당 항목을 지정한 이메일 주소로 전송합니다. 발신자를 선택하고 전송 항목에 추가할 텍스트를 작성할 수 있습니다.
   - 백업이 암호화되지 않고 검색을 사용하고 검색 결과에서 단일 항목만 선택한 경우에만: **버전 표시**를 클릭하여 복구할 항목 버전을 선택합니다. 선택한 복구 지점 이전이나 이후 백업된 버전을 선택할 수 있습니다.
8. **복구**를 클릭합니다.
9. 여러 Hosted Exchange 조직을 Cyber Protection 서비스에 추가하였다면, **Hosted Exchange 조직** 을 클릭하여 대상 조직을 보기, 변경 또는 지정합니다.

   기본적으로 원래 조직이 선택됩니다. 이 조직이 Cyber Protection 서비스에 등록되지 않았다면 대상 조직을 지정해야 합니다.
10. **사서함으로 복구**에서 대상 사서함을 보고, 변경하거나 지정합니다.

    기본적으로 원래 사서함이 선택됩니다. 이 사서함이 존재하지 않거나 원래 이외 조직을 선택한 경우에는 대상 사서함을 지정해야 합니다.
11. [사용자 또는 공유 사서함을 복구할 경우에만 해당] **경로**에서 대상 사서함의 대상 폴더를 보거나 변경합니다. 기본적으로 **복구 항목** 폴더가 선택되어 있습니다.

    그룹 사서함 항목은 항상 **받은 편지함** 폴더로 복구됩니다.
12. **복구 시작**을 클릭합니다.
13. 다음 덮어쓰기 옵션 중 하나를 선택합니다.
    - **기존 항목 덮어쓰기**
    - **기존 항목 덮어쓰기 안 함**

© Acronis International GmbH, 2003-2024

14. **진행**을 클릭하여 결정을 확인합니다.

Microsoft 365 데이터 보호

Microsoft 365 데이터를 백업하는 이유?

Microsoft 365는 클라우드 서비스이지만 정기적으로 백업을 하면 사용자 오류 및 의도적인 악성 동작으로부터 한층 더 보호할 수 있습니다. Microsoft 365 보관 기간이 만료된 후에도 백업으로부터 삭제된 항목을 복구할 수 있습니다. 또한, 규정 준수를 위해 필요한 경우 Exchange Online 사서함의 로컬 사본을 유지할 수 있습니다.

백업된 데이터는 자동으로 압축되며 원래 위치보다 백업 위치에서 공간을 덜 차지합니다. 클라우드 간 백업의 압축 수준은 고정되어 있으며 비 클라우드 간 백업의 **보통** 수준에 해당합니다. 이러한 수준에 대한 자세한 내용은 "압축 수준"(417페이지) 항목을 참조하십시오.

클라우드 에이전트 및 로컬 에이전트

Microsoft 365 워크로드에서는 두 가지 에이전트를 사용할 수 있습니다.

- 클라우드 에이전트
  클라우드 에이전트는 확장된 백업 기능을 제공합니다. Cyber Protect 콘솔에서 해당 기능에 직접 액세스할 수 있습니다. 이 에이전트는 설치할 필요가 없습니다. 자세한 내용은 "클라우드 Agent for Microsoft 365 사용"(553페이지)을(를) 참조하십시오.
- 로컬 에이전트
  로컬 에이전트에서는 Exchange Online 사서함 백업 기능만 제공됩니다. 이 에이전트는 인터넷에 연결된 Windows 머신에 설치해야 합니다. 자세한 내용은 "로컬로 설치한 Agent for Office 365 사용"(549페이지)을(를) 참조하십시오.

두 에이전트는 모두 Azure Information Protection(AIP)을 지원합니다.

참고
규제 준수 모드의 테넌트에는 로컬 에이전트만 사용 가능합니다. 이러한 테넌트는 Microsoft 365 사서함만 백업할 수 있으며 클라우드 에이전트가 제공하는 확장 기능을 사용할 수 없습니다.

다음 표에 에이전트 기능이 요약되어 있습니다.

	로컬 에이전트	클라우드 에이전트
백업할 수 있는 데이터 항목	**Exchange Online:** 사용자 사서함 및 공유 사서함(키오스크 계획의 사용자 사서함과 소송 보존이 적용된 사서함 포함)	• **Exchange Online**: ◦ 사용자 사서함 및 공유 사서함(키오스크 계획의 사용자 사서함과 소송 보존이 적용된 사서함 포함) ◦ 그룹 사서함 ◦ 공용 폴더 • **OneDrive**: 사용자 파일 및 폴

© Acronis International GmbH, 2003-2024

	로컬 에이전트	클라우드 에이전트
		더 • **SharePoint Online**: ◦ 클래식 사이트 컬렉션 ◦ 그룹(팀) 사이트 ◦ 통신 사이트 ◦ 개별 데이터 항목 • **Microsoft 365 Teams**: ◦ 전체 팀 ◦ 팀 채널 ◦ 채널 파일 ◦ 팀 사서함 ◦ 팀 사서함의 파일 및 이메일 메시지 ◦ 회의 ◦ 팀 사이트 • **OneNote 노트북**: OneDrive, SharePoint Online 및 Microsoft 365 Teams 백업의 일부분으로 백업 가능
아카이브 사서함 백업(**내부 아카이브**)	아니요	예
백업 스케줄	사용자 정의	매일 최대 6회*
백업 위치	클라우드 스토리지, 로컬 또는 네트워크 폴더	클라우드 스토리지 전용 (파트너 호스팅 스토리지 포함)
신규 Microsoft 365 사용자, 그룹, 사이트 및 팀의 자동 보호	아니요	예, **전체 사용자**, **전체 그룹**, **전체 사이트**, **전체 팀** 그룹에 보호 계획을 적용합니다.
Microsoft 365 조직을 한 곳 이상 보호	아니요	예
개별 복구	예	예
한 조직에 속하는 다른 사용자로 복구	예	예
다른 조직으로 복구	아니요	예
온프레미스 Microsoft Exchange 서버로 복구	아니요	아니요
성능 저하 없이 백업할 수 있는 최대 항목 수	클라우드 스토리지 백업 시 회사당 사서함 5000개	회사당 10000개의 보호 항목(사서함, OneDrive, 사이트)**

© Acronis International GmbH, 2003-2024

	로컬 에이전트	클라우드 에이전트
	다른 위치에 백업하는 경우 보호 계획당 2000개(회사당 사서함 수 제한 없음)	
최대 수동 백업 실행 수	아니요	시간당 10개의 수동 실행
최대 동시 복구 작업 수	아니요	10개 작업(Google Workspace 복구 작업 포함)

* 기본 옵션은 **하루에 한 번**입니다. Advanced Backup 팩을 사용하면 백업을 하루에 6번까지 예약할 수 있습니다. 백업은 클라우드 에이전트(데이터 센터 내 여러 고객의 백업을 처리함)의 현재 로드에 따라 달라지는 대략적인 간격으로 시작됩니다. 그러므로 로드가 하루 종일 일정하게 유지되며 모든 고객에게 동일한 서비스 품질이 제공됩니다.

참고
보호 스케줄은 Microsoft 365 서버의 접근성, Microsoft 서버의 제한 설정 등 타사 서비스 작업의 영향을 받을 수 있습니다. 자세한 내용은 https://docs.microsoft.com/en-us/graph/throttling을 참조하십시오.

** 보호되는 항목은 다음 순서에 따라 점진적으로 백업하는 것이 좋습니다.

1. 사서함
2. 모든 사서함을 백업한 후 OneDrive 백업을 진행합니다.
3. OneDrive 백업을 완료한 후에는 SharePoint Online 사이트를 진행합니다.

보호되는 항목의 수와 크기에 따라 최초 전체 백업에 며칠이 소요될 수도 있습니다.

필수 사용자 권한

Cyber Protection

로컬 에이전트는 회사 관리자 계정에 등록해야 하며 고객 테넌트 수준에서 사용해야 합니다. 부서에 영향을 주는 회사 관리자, 부서 관리자, 사용자는 Microsoft 365 데이터를 백업하거나 복구할 수 없습니다.

클라우드 에이전트는 고객 테넌트 수준과 부서 수준에서 모두 사용할 수 있습니다. 이러한 수준 및 각 수준의 관리자에 대한 자세한 내용은 "다른 수준에 추가된 Microsoft 365 조직 관리"(554페이지) 항목을 참조하십시오.

Microsoft 365의 요구 사항

사용자의 계정이 Microsoft 365에 전역 관리자로 지정되어 있어야 합니다.

Microsoft 365 공용 폴더를 검색, 백업 또는 복구하기 위해서는 최소 하나의 Microsoft 365 관리자 계정에 사서함이 있고 백업하려는 공용 폴더에 대한 읽기/쓰기 권한이 있어야 합니다.

© Acronis International GmbH, 2003-2024

- 로컬 에이전트가 이 계정을 사용하여 Microsoft 365에 로그인합니다. 에이전트가 모든 사서함의 콘텐츠에 액세스할 수 있도록 설정하려면 이 계정에 **ApplicationImpersonation** 관리 역할이 할당됩니다. 계정 암호를 변경하는 경우에는 "Microsoft 365 액세스 자격 증명 변경"(551페이지)의 설명에 따라 Cyber Protect 콘솔에서 암호를 업데이트하십시오.
- 클라우드 에이전트는 Microsoft 365에 로그인하지 않습니다. 이 작업에 필요한 권한을 클라우드 에이전트에 부여하려면 전역 관리자로 Microsoft 365에 한 번 로그인해야 합니다.

  Microsoft 365에서 필요한 권한은 다음과 같습니다.
  - 로그인 및 사용자 프로파일 읽기
  - 모든 사이트 컬렉션에서 파일 읽기 및 쓰기
  - 모든 사용자의 전체 프로파일 읽기 및 쓰기
  - 모든 그룹 읽기 및 쓰기
  - 디렉토리 데이터 읽기
  - 모든 채널메시지 읽기
  - 관리 대상 메타데이터 읽기 및 쓰기
  - 모든 사이트 컬렉션에서 항목과 목록 읽기 및 쓰기
  - 모든 사이트 컬렉션의 완전한 제어 권한 확보
  - 모든 사이트 컬렉션에서 항목 읽기 및 쓰기
  - 모든 사서함에 대한 전체 권한을 확보하여 Exchange Web Services 사용
- 클라우드 에이전트는 사용자 계정 자격 증명을 저장하지 않으며 백업과 복구를 수행하는 데 해당 자격 증명을 사용하지 않습니다. 자격 증명을 변경하거나 계정을 비활성화 또는 삭제하더라도 클라우드 에이전트의 작업에는 아무런 영향이 없습니다.

제한 사항

- 로컬 에이전트를 사용하면 워크로드를 5천 개까지 보호할 수 있습니다. 반면 클라우드 에이전트 사용 시에는 워크로드를 5만 개까지 보호할 수 있습니다.
- Microsoft 365 라이선스가 없는 사용자와 Microsoft 365 서비스 로그인이 차단된 사용자를 포함하여 사서함 또는 OneDrive가 있는 모든 사용자가 Cyber Protect 콘솔에 표시됩니다.
- 사서함 백업에는 사용자에게 보이는 폴더만 포함됩니다. **복구 가능 항목** 폴더 및 해당 하위 폴더(**삭제**, **버전**, **제거**, **감사**, **DiscoveryHold**, **일정 로깅**)는 사서함 백업에 포함되지 않습니다.
- 복구가 진행되는 동안 사용자, 공용 폴더, 그룹, 사이트의 자동 생성은 불가능합니다. 예를 들어, 삭제된 SharePoint Online 사이트의 복구를 원한다면 먼저 새 사이트를 수동으로 생성한 후 복구를 진행하는 동안 대상 사이트로 지정합니다.
- 여러 복구 지점의 항목을 동시에 복구할 수는 없지만 검색 결과에서 여러 구 지점의 항목을 선택할 수는 있습니다.
- 백업 중에 콘텐츠에 적용된 민감도 라벨은 모두 유지됩니다. 따라서 원본 이외의 위치로 복구되고 사용자가 다른 액세스 권한을 가진 경우 민감한 콘텐츠가 표시되지 않을 수도 있습니다.
- 같은 워크로드에 개별 백업 계획을 여러 개 적용할 수는 없습니다.
- 같은 워크로드에 개별 백업 계획과 그룹 백업 계획을 적용하면 개별 계획의 설정이 우선적으로 적용됩니다.

© Acronis International GmbH, 2003-2024

Microsoft 365 시트 라이센스 보고서

회사 관리자는 보호된 Microsoft 365 시트 및 해당 라이센스 관련 보고서를 다운로드할 수 있습니다. 보고서(CSV 형식)에는 시트의 라이센스 상태 및 라이센스 사용 이유 관련 정보가 포함되어 있습니다. 그리고 보호된 시트 이름, 관련 이메일, 그룹, Microsoft 365 조직, 보호된 워크로드의 이름과 유형도 포함되어 있습니다.

이 보고서는 Microsoft 365 조직이 등록된 테넌트에서만 사용 가능합니다.

Microsoft 365 시트 라이센스 보고서를 다운로드하려면

1. Cyber Protect 콘솔에 회사 관리자로 로그인합니다.
2. 오른쪽 위에 있는 계정 아이콘을 클릭합니다.
3. **Microsoft 365 시트 라이센스 보고서**를 클릭합니다.

로깅

백업된 이메일의 내용 보기, 첨부 파일 또는 파일 다운로드, 이메일을 원본이 아닌 사서함으로 복구 또는 이메일로 보내는 등의 클라우드 간 리소스 관련 작업은 사용자 개인 정보를 침해할 수 있습니다. 이러한 작업은 관리 포털의 **모니터링** > **감사 로그**에 로깅됩니다.

로컬로 설치한 Agent for Office 365 사용

Microsoft 365 조직 추가

Microsoft 365 조직을 추가하려면

1. Cyber Protect 콘솔에 회사 관리자로 로그인합니다.
2. 오른쪽 위의 계정 아이콘을 클릭한 후 **다운로드** > **Agent for Office 365**를 클릭합니다.
3. 에이전트를 다운로드하고 인터넷에 연결된 Windows 머신에 설치합니다.
4. Cyber Protect 콘솔에서 **장치** > **Microsoft Office 365(로컬 에이전트)**로 이동합니다.
5. 창이 열리면 애플리케이션 ID, 애플리케이션 암호, Microsoft 365 테넌트 ID를 입력합니다. 이들을 찾는 자세한 방법은 "애플리케이션 ID 및 암호를 가져오는 방법"(549페이지) 항목을 참조하십시오.
6. **확인**을 클릭합니다.

결과적으로 **Microsoft Office 365(로컬 에이전트)** 탭에 있는 Cyber Protect 콘솔에 조직의 데이터 항목이 표시됩니다.

중요
한 조직(회사 그룹)에는 로컬에서 설치된 Agent for Office 365가 하나만 있어야 합니다.

애플리케이션 ID 및 암호를 가져오는 방법

Office 365에 최신 인증을 사용하려면 Entra 관리 센터에서 사용자 정의 애플리케이션을 생성한 후 해당 애플리케이션에 특정 API 권한을 부여해야 합니다. 이렇게 하면 콘솔에 입력해야 하는 **애플**

© Acronis International GmbH, 2003-2024

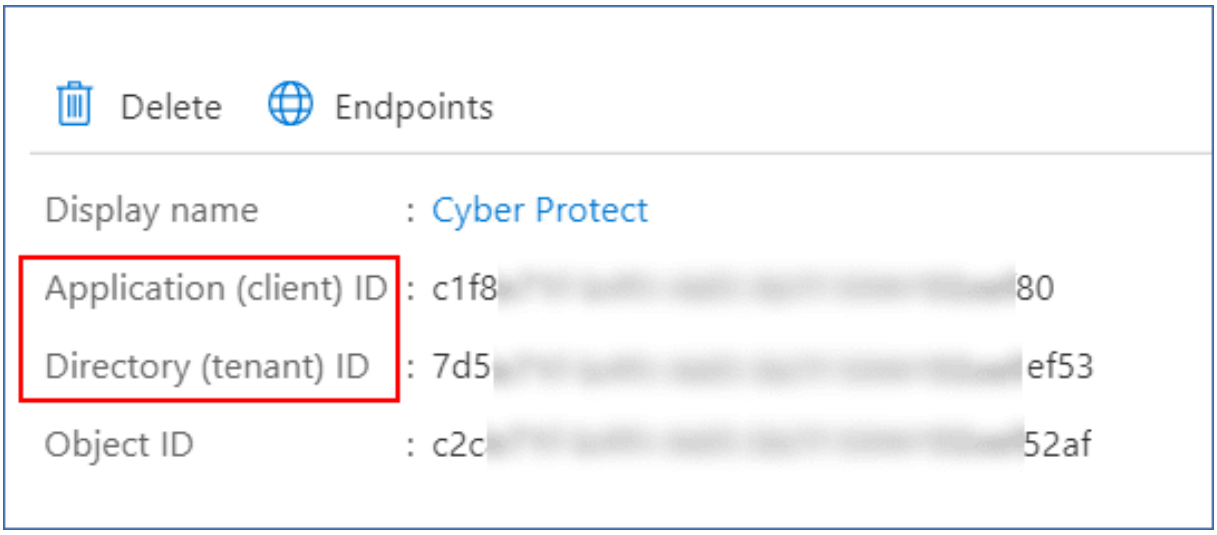
리케이션 ID, **애플리케이션 암호** 및 **디렉토리(테넌트) ID**를 받을 수 있습니다.

참고
Agent for Office 365가 설치되어 있는 머신에서 포트 443을 통한 graph.microsoft.com 액세스를 허용합니다.

Entra 관리 센터에서 애플리케이션을 생성하려면

1. Entra 관리 센터에 관리자로 로그인합니다.
2. **Azure Active Directory** > **App 등록**으로 이동한 뒤, **새로운 등록**을 클릭합니다.
3. 사용자 지정 애플리케이션의 이름을 지정합니다(예: Cyber Protection).
4. **지원 계정 유형**에서 **이 조직 디렉토리 내 계정**을 선택합니다.
5. **등록**을 클릭합니다.

애플리케이션이 생성되었습니다. Entra 관리 센터에서 애플리케이션의 **개요** 페이지로 이동하여 애플리케이션(클라이언트) ID 및 디렉토리(테넌트) ID를 확인합니다.



Entra 관리 센터에서 애플리케이션을 생성하는 방법에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

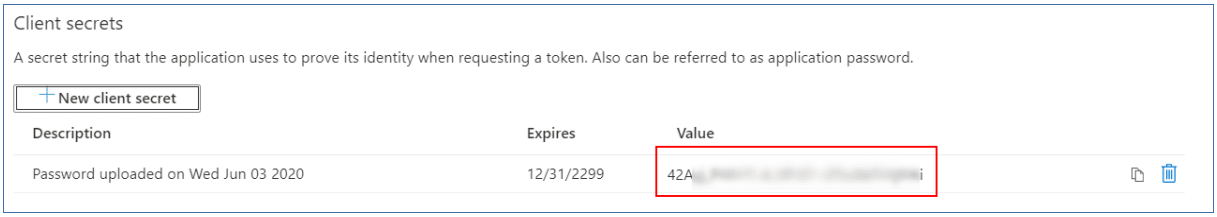
애플리케이션에 필요한 API 권한을 부여하는 방법

1. Entra 관리 센터에서 애플리케이션의 **API 권한**으로 이동하여 **권한 추가**를 클릭합니다.
2. **조직에서 사용하는 API** 탭을 선택한 다음, **Office 365 Exchange Online**을 검색합니다.
3. **Office 365 Exchange Online**, **애플리케이션 권한**을 차례로 클릭합니다.
4. **App으로_전체_액세스** 확인란을 선택하고, **권한 추가**를 클릭하십시오.
5. **API 권한**에서 **권한 추가**를 클릭합니다.
6. **Microsoft Graph**를 선택합니다.
7. **애플리케이션 권한**을 선택합니다.
8. **디렉토리** 탭을 확장한 후 **디렉토리.모두.읽기** 확인란을 선택합니다. **권한 추가**를 클릭합니다.
9. 모든 권한을 확인한 뒤, **<사용자 애플리케이션 이름>에 대한 관리자 동의**를 클릭합니다.
10. **예**를 클릭하여 선택을 확인합니다.

© Acronis International GmbH, 2003-2024

애플리케이션 암호 생성 방법

1. Entra 관리 센터에서 애플리케이션의 **인증서 및 암호** > **새 클라이언트 암호**로 이동합니다.
2. 대화 상자가 열리면 만료 기한을 선택합니다. **해당 없음**을 선택한 뒤, **추가**를 클릭합니다.
3. **값** 필드에서 애플리케이션 암호를 확인하고 기억하십시오.



애플리케이션 암호에 대한 자세한 내용은 Microsoft 문서를 참고하십시오.

Microsoft 365 액세스 자격 증명 변경

에이전트를 다시 설치하지 않고 Microsoft 365에 대한 액세스 자격 증명을 변경할 수 있습니다.

Microsoft 365 액세스 자격 증명을 변경하려면

1. **장치** > **Microsoft Office 365(로컬 에이전트)**를 클릭합니다.
2. Microsoft 365 조직을 선택합니다.
3. **자격 증명 지정**을 클릭합니다.
4. 애플리케이션 ID, 애플리케이션 암호, Microsoft 365 테넌트 ID를 입력합니다. 이들을 찾는 자세한 방법은 "애플리케이션 ID 및 암호를 가져오는 방법"(549페이지) 항목을 참조하십시오.
5. **확인**을 클릭합니다.

Exchange 온라인 사서함 보호

어떤 항목을 백업할 수 있습니까?

사용자 사서함과 공유 사서함을 백업할 수 있습니다. 그룹 사서함과 아카이브 사서함(**내부 아카이브**)은 백업할 수 없습니다.

복구할 수 있는 항목은 무엇입니까?

다음과 같은 항목을 사서함 백업에서 복구할 수 있습니다.

- 사서함
- 이메일 폴더
- 이메일 메시지
- 달력 이벤트
- 작업
- 연락처
- 업무 일지
- 메모

검색 기능을 사용해 항목을 찾을 수 있습니다.

© Acronis International GmbH, 2003-2024

기존 사서함으로 사서함을 복구하면 일치하는 ID의 기존 항목이 덮어써집니다.

사서함 항목 복구 시에는 무엇도 덮어쓰지 않습니다. 대신, 사서함 항목의 전체 경로가 대상 폴더에 재생성됩니다.

Microsoft 365 사서함 선택

아래 설명에 따라 사서함을 선택한 다음, 보호 계획의 기타 설정을 적절하게 지정합니다.

사서함을 선택하려면

1. **Microsoft Office 365(로컬 에이전트)**를 클릭합니다.
2. 백업할 사서함을 선택합니다.
3. **백업**을 클릭합니다.

사서함 및 사서함 항목 복구

사서함 복구

1. **Microsoft Office 365(로컬 에이전트)**를 클릭합니다.
2. 복구할 사서함을 선택한 다음 **복구**를 클릭합니다.
   사서함을 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.
   사서함이 삭제된 경우 백업 스토리지 탭에서 이를 선택한 다음 **백업 표시**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.
4. **복구 > 사서함**을 클릭합니다.
5. **대상 사서함**에서 대상 사서함을 보고, 변경하거나 지정합니다.
   기본적으로 원래 사서함이 선택됩니다. 이 사서함이 존재하지 않는 경우 대상 사서함을 지정해야 합니다.
6. **복구 시작**을 클릭합니다.

사서함 항목 복구

1. **Microsoft Office 365(로컬 에이전트)**를 클릭합니다.
2. 복구하려는 항목이 원래 포함되어 있는 사서함을 선택한 다음 **복구**를 클릭합니다.
   사서함을 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.
   사서함이 삭제된 경우 백업 스토리지 탭에서 이를 선택한 다음 **백업 표시**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.
4. **복구 > 이메일 메시지**를 클릭합니다.
5. 복구할 항목을 선택합니다.
   다음 검색 옵션을 사용할 수 있습니다. 와일드카드는 지원되지 않습니다.
   - 이메일 메시지: 제목, 보낸 사람, 받는 사람, 첨부 파일 이름, 날짜로 검색합니다.
   - 이벤트: 제목 및 날짜로 검색합니다.
   - 작업: 제목 및 날짜로 검색합니다.
   - 연락처: 이름, 이메일 주소, 전화번호로 검색합니다.

   이메일 메시지를 선택한 경우 **내용 표시**를 클릭해 첨부 파일을 포함한 내용을 볼 수 있습니다.

© Acronis International GmbH, 2003-2024

참고
첨부 파일을 다운로드하려면 그 이름을 클릭하십시오.

이메일 메시지를 선택한 경우 **이메일로 보내기**를 클릭해 해당 메시지를 지정한 이메일 주소로 보낼 수 있습니다. 관리자 계정의 이메일 주소에서 메시지가 전송됩니다.

폴더를 선택하려면 "폴더 복구" 아이콘 을 클릭하십시오.

6. **복구**를 클릭합니다.
7. **대상 사서함**에서 대상 사서함을 보고, 변경하거나 지정합니다.
   기본적으로 원래 사서함이 선택됩니다. 이 사서함이 존재하지 않는 경우 대상 사서함을 지정해야 합니다.
8. **복구 시작**을 클릭합니다.
9. 결정을 확인합니다.

사서함 항목은 항상 대상 사서함의 **복구된 항목** 폴더로 복구됩니다.

클라우드 Agent for Microsoft 365 사용

Microsoft 365 조직 추가

관리자는 한 개 이상의 Microsoft 365 조직을 고객 테넌트 혹은 유닛에 추가할 수 있습니다.

회사 관리자가 고객 테넌트에 조직을 추가합니다. 부서 수준에서 업무를 처리하는 부서 관리자와 고객 관리자가 부서에 조직을 추가합니다.

Microsoft 365 조직을 추가하려면

1. 조직을 추가해야 하는 위치에 따라 회사 관리자나 부서 관리자로 Cyber Protect 콘솔에 로그인합니다.
2. [부서 수준에서 업무를 처리하는 회사 관리자의 경우] 관리 포털에서 원하는 부서로 이동합니다.
3. **장치** > **추가** > **Microsoft 365 Business**를 클릭합니다.
   Microsoft 365 로그인 페이지로 리디렉션됩니다.
4. Microsoft 365 전역 관리자 자격 증명으로 로그인합니다.
   조직 데이터를 백업 및 복구하는 데 필요한 권한 목록이 표시됩니다.
5. Cyber Protection 서비스에 이러한 권한을 부여한 사실을 확인합니다.

그러면 콘솔의 **장치** 탭 아래에 Microsoft 365 조직이 표시됩니다.

유용한 팁

- 클라우드 에이전트는 조직이 Cyber Protection 서비스에 추가될 때부터 24시간 간격으로 Microsoft 365에 동기화됩니다. 사용자나 그룹, 사이트를 추가하거나 제거하면 Cyber Protect 콘솔에서 이러한 변경 사항을 즉시 확인할 수 없습니다. 변경 사항을 즉시 동기화하려면 **Microsoft 365** 페이지에서 조직을 선택하고 **새로 고침**을 클릭합니다.

© Acronis International GmbH, 2003-2024

Cyber Protect 콘솔과 Microsoft 365 조직의 리소스 동기화에 대한 자세한 내용은 "Microsoft 365 리소스 검색"(555페이지) 항목을 참조하십시오.

- **전체 사용자**, **전체 그룹** 또는 **전체 사이트** 그룹에 보호 계획을 적용했다면, 새로 추가되는 항목은 동기화 후에만 백업에 포함됩니다.
- Microsoft 정책에 따라, Microsoft 365 그래픽 사용자 인터페이스에서 사용자, 그룹 또는 사이트가 제거되더라도 며칠 동안은 API를 통해 이용할 수 있습니다. 이 기간에는 제거된 항목이 Cyber Protect 콘솔에서 비활성화(회색으로 표시)되며 백업되지 않습니다. 제거한 항목은 API를 통해 사용할 수 없는 상태가 되면 Cyber Protect 콘솔에서 사라집니다. 해당 항목의 백업이 있을 경우 **백업 스토리지** > **클라우드 애플리케이션 백업**에서 확인할 수 있습니다.

다른 수준에 추가된 Microsoft 365 조직 관리

회사 관리자에게는 고객 테넌트 수준에 추가된 Microsoft 365 조직에 대한 전체 액세스 권한이 있습니다.

하지만 부서에 추가된 조직의 경우에는 회사 관리자의 액세스 권한이 제한됩니다. 이러한 조직(부서 이름이 괄호 안에 표시됨)의 경우 회사 관리자는 다음 작업을 수행할 수 있습니다.

- 백업에서 데이터 복구.
  회사 관리자는 조직이 추가된 수준에 관계없이 테넌트의 모든 조직에 데이터를 복구할 수 있습니다.
- 백업에서 백업 및 복구 지점 찾기.
- 백업에서 백업 및 복구 지점 삭제.
- 경보 및 활동 보기.

고객 테넌트 수준에서 업무를 처리하는 회사 관리자가 수행할 수 없는 작업은 다음과 같습니다.

- 부서에 Microsoft 365 조직 추가.
- 부서에서 Microsoft 365 조직 삭제.
- 부서에 추가된 Microsoft 365 조직 동기화.
- 부서에 추가된 Microsoft 365 조직의 데이터 항목용 보호 계획 확인, 생성, 편집, 삭제, 적용, 실행 또는 철회.

부서 수준에서 업무를 처리하는 회사 관리자 및 부서 관리자에게는 부서에 추가된 조직에 대한 전체 액세스 권한이 있습니다. 그러나 상위 고객 테넌트의 리소스(해당 테넌트에 생성된 보호 계획 포함)에는 액세스할 수 없습니다.

Microsoft 365 조직 삭제

Microsoft 365 조직을 삭제해도 해당 조직 데이터의 기존 백업에는 아무런 영향이 없습니다. 이러한 백업이 더 이상 필요하지 않다면 먼저 삭제한 후에 Microsoft 365 조직을 삭제하십시오. 이렇게 하지 않으면 백업이 클라우드 스토리지 공간을 계속 사용하므로 요금이 청구될 수 있습니다.

백업 삭제 방법에 대한 자세한 내용은 "백업 또는 백업 아카이브를 삭제하는 방법"(485페이지)을(를) 참조하십시오.

Microsoft 365 조직을 삭제하려면

© Acronis International GmbH, 2003-2024

1. 조직을 추가할 위치에 따라 회사 관리자나 부서 관리자로 Cyber Protect 콘솔에 로그인합니다.
2. [부서 수준에서 업무를 처리하는 회사 관리자의 경우] 관리 포털에서 원하는 부서로 이동합니다.
3. **장치** > **Microsoft 365**로 이동합니다.
4. 조직을 선택하고 **그룹 삭제**를 클릭합니다.

그러면 이 그룹에 적용된 백업 계획은 철회됩니다.

그러나 Microsoft 365의 조직 데이터에 대한 Backup Service 애플리케이션의 액세스 권한을 수동으로도 철회해야 합니다.

액세스 권한을 철회하려면

1. 전역 관리자로 Microsoft 365에 로그인합니다.
2. **관리자 센터** > **Azure Active Directory** > **기업 애플리케이션** > **모든 애플리케이션**으로 이동합니다.
3. **Backup Service** 애플리케이션을 선택하여 자세히 살펴봅니다.
4. **속성** 탭으로 이동하여 작업 패널에서 **삭제**를 클릭합니다.
5. 작업 삭제를 확인합니다.

그러면 Backup Service 애플리케이션의 Microsoft 365 조직 데이터 액세스 권한이 철회됩니다.

Microsoft 365 리소스 검색

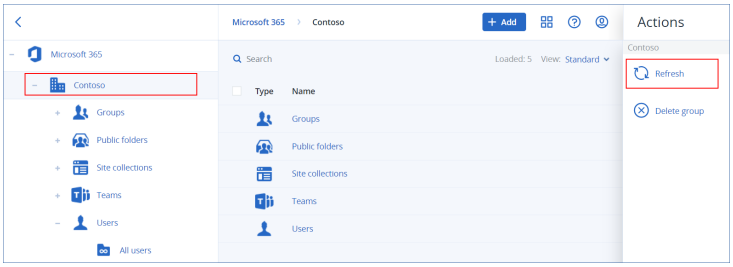
Cyber Protection 서비스에 Microsoft 365 조직을 추가하면 사서함, OneDrive 스토리지, Microsoft Teams, SharePoint 사이트 등 해당 조직의 리소스가 Cyber Protect 콘솔에 동기화됩니다. 이 작업(검색)은 **모니터링** > **활동**에 로깅됩니다.

검색 작업이 완료되면 콘솔의 **장치** > **Microsoft 365** 탭에서 Microsoft 365 조직의 리소스를 확인할 수 있으며 해당 리소스에 백업 계획을 적용할 수 있습니다.

Cyber Protect 콘솔의 리소스 목록을 최신 상태로 유지하기 위해 매일 한 번씩 자동 검색 작업이 실행됩니다. 검색 작업을 수동으로 다시 실행하여 이 목록을 필요에 따라 동기화할 수도 있습니다.

검색 작업을 수동으로 다시 실행하려면

1. Cyber Protect 콘솔에서 **장치** > **Microsoft 365**로 이동합니다.
2. Microsoft 365 조직을 선택한 다음 **작업** 창에서 **새로 고침**을 클릭합니다.



© Acronis International GmbH, 2003-2024

참고
시간당 10회까지 검색 작업을 수동으로 실행할 수 있습니다. 이 횟수를 초과하면 허용되는 실행 수가 시간당 1회로 재설정되며, 그러면 시간당 작업 실행 횟수가 총 10회가 될 때까지 1시간마다 1회씩 작업을 추가로 실행할 수 있습니다.

Microsoft 365 백업의 빈도 설정

기본적으로 Microsoft 365 백업은 하루에 한 번 실행되며 추가 예약 옵션은 제공되지 않습니다.

테넌트에서 Advanced Backup 팩이 활성화되어 있으면 백업 빈도를 더 높게 구성할 수 있습니다. 일별 백업 수를 선택할 수는 있지만 백업 시작 시간은 구성할 수 없습니다. 백업은 클라우드 에이전트(데이터 센터 내 여러 고객의 백업을 처리함)의 현재 로드에 따라 달라지는 대략적인 간격으로 자동 시작됩니다. 그러므로 로드가 하루 종일 일정하게 유지되며 모든 고객에게 동일한 서비스 품질이 제공됩니다.

다음 옵션을 사용할 수 있습니다.

예약 옵션	각 백업 간의 대략적인 간격
하루에 한 번	24시간
하루에 두 번(기본값)	12시간
하루에 세 번	8시간
하루에 6번	4시간

참고
클라우드 에이전트의 로드 및 Microsoft 365 측에서 실행될 수 있는 조절에 따라 백업이 예약한 일정보다 더 늦게 시작될 수도 있고 백업을 완료하는 데 시간이 더 오래 걸릴 수도 있습니다. 백업 시간이 두 백업 간의 평균 간격보다 더 오래 걸리면 다음 백업이 다시 예약되므로 하루에 실행되는 백업 수가 원래 선택한 수보다 더 적어질 수도 있습니다. 예를 들어 하루에 백업 6회를 완료하도록 선택했더라도 2회밖에 완료하지 못할 수도 있습니다.

그룹 사서함의 백업은 하루에 한 번만 실행할 수 있습니다.

Exchange Online 데이터 보호

어떤 항목을 백업할 수 있습니까?

사용자 사서함, 공유 사서함, 그룹 사서함을 백업할 수 있습니다. 원하는 경우 선택한 사서함의 아카이브 사서함 백업을 선택할 수 있습니다(**내부 아카이브**).

Cyber Protection 서비스의 버전 8.0부터 공용 폴더를 백업할 수 있습니다. 조직이 Cyber Protection 서비스에 추가된 것이 버전 8.0 출시 이전일 경우, 이 기능을 사용하려면 조직을 다시 추가해야 합니다. 조직을 삭제할 필요 없이 "Microsoft 365 조직 추가"(553페이지)에 설명된 단계를 반복하면 됩니다.그러면 Cyber Protection 서비스가 해당 API 사용에 대한 권한을 획득하게 됩니다.

© Acronis International GmbH, 2003-2024

복구할 수 있는 항목은 무엇입니까?

다음과 같은 항목을 사서함 백업에서 복구할 수 있습니다.

- 사서함
- 이메일 폴더
- 이메일 메시지
- 달력 이벤트
- 작업
- 연락처
- 업무 일지
- 메모

다음과 같은 항목을 공용 폴더 백업에서 복구할 수 있습니다.

- 하위 폴더
- 게시
- 이메일 메시지

검색 기능을 사용해 항목을 찾을 수 있습니다.

사서함, 사서함 항목, 공용 폴더 및 공용 폴더 항목을 복구할 때 대상 위치의 항목을 복구할 것인지 선택할 수 있습니다.

사서함 선택

아래 설명에 따라 사서함을 선택한 다음, 보호 계획의 기타 설정을 적절하게 지정합니다.

Exchange 온라인 사서함을 선택하려면

1. **Microsoft 365**를 클릭합니다.
2. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우 사용자 데이터의 백업을 원하는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. 다음 중 하나를 수행하십시오.
   - 전체 사용자의 사서함과 공유 사서함(앞으로 생성될 사서함 포함)을 백업하려면, **사용자** 노드를 확장하고 **전체 사용자**를 선택한 후 **그룹 백업**을 클릭합니다.
   - 개별적인 사용자 또는 공유 사서함을 백업하려면, **사용자** 노드를 확장하고 **전체 사용자**를 선택한 다음 백업하려는 사서함의 사용자를 선택한 후 **백업**을 클릭합니다.
   - 전체 그룹 사서함(앞으로 생성될 그룹의 사서함 포함)을 백업하려면, **그룹** 노드를 확장하고 **전체 그룹**을 선택한 후 **그룹 백업**을 클릭합니다.
   - 개별 그룹 사서함을 복구하려면, **그룹** 노드를 확장하고 **전체 그룹**을 선택하고 백업하려는 사서함의 그룹을 선택한 후 **백업**을 클릭합니다.

© Acronis International GmbH, 2003-2024

참고
그룹 사서함에 액세스하려면 클라우드 Agent for Microsoft 365에서 적절한 권한을 가진 계정을 사용해야 합니다. 따라서 그룹 사서함을 백업하려면 최소 한 명의 그룹 소유자가 사서함이 있는 Microsoft 365 라이센스 사용자여야 합니다. 그룹이 비공개 또는 숨긴 구성원 자격으로 설정되어 있는 경우 해당 소유자가 반드시 그룹의 구성원에 포함되어 있어야 합니다.

4. 보호 계획 패널에서:
   - **백업 대상**에서 **Microsoft 365 사서함** 항목이 선택되어 있는지 확인합니다.
     개별적으로 선택한 일부 사용자의 Microsoft 365 계획에 Exchange 서비스가 포함되어 있지 않으면 이 옵션을 선택할 수 없습니다.
     그룹 백업을 위해 선택한 일부 사용자의 Microsoft 365 계획에 Exchange 서비스가 포함되어 있지 않은 경우 이 옵션을 선택할 수 있지만 이러한 사용자에게는 보호 계획이 적용되지 않습니다.
   - 아카이브 사서함의 백업을 원하지 않으면 **아카이브 사서함** 스위치를 비활성화합니다.

공용 폴더 선택

아래 설명에 따라 공용 폴더를 선택한 다음, 보호 계획의 기타 설정을 적절하게 지정합니다.

참고
공용 폴더는 Microsoft 365 시트의 백업 할당량의 라이센스를 소비합니다.

Exchange 온라인 공용 폴더를 선택하려면

1. **Microsoft 365**를 클릭합니다.
2. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, 데이터의 백업을 원하는 조직을 확장합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. **공용 폴더** 노드를 확대한 다음, **모든 공용 폴더**를 선택합니다.
4. 다음 중 하나를 수행하십시오.
   - 모든 공용 폴더(이후 생성할 공용 폴더 포함)를 백업하려면 **그룹 백업**을 클릭합니다.
   - 개별 공용 폴더를 백업하려면 백업하려는 공용 폴더를 선택한 다음, **백업**을 클릭합니다.
5. 보호 계획 패널의 **백업 대상**에서 **Microsoft 365 사서함** 항목이 선택되어 있는지 확인합니다.

사서함 및 사서함 항목 복구

사서함 복구

1. **Microsoft 365**를 클릭합니다.
2. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, 복구를 원하는 백업된 데이터가 있는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. 다음 중 하나를 수행하십시오.
   - 사용자 사서함을 복구하려면, **사용자** 노드를 확장하고 **전체 사용자**를 선택하고 복구하려는 사서함의 사용자를 선택한 후 **복구**를 클릭합니다.

© Acronis International GmbH, 2003-2024

- 공유 사서함을 복구하려면, **사용자** 노드를 확장하고 **전체 사용자**를 선택한 다음 복구하려는 공유 사서함을 선택한 후 **복구**를 클릭합니다.
- 그룹 사서함의 항목을 복구하려면, **그룹** 노드를 확장하고 **전체 그룹**을 선택하고 복구하려는 사서함의 그룹을 선택한 후 **복구**를 클릭합니다.
- 사용자 그룹 또는 공유 사서함이 삭제되었다면 백업 스토리지 탭의 **클라우드 애플리케이션 백업** 섹션에서 해당 항목을 선택한 후 **백업 표시**를 클릭합니다.

사용자와 그룹은 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.

4. 복구 지점을 선택합니다.

참고
사서함이 포함된 복구 지점만 보려면 **내용별 필터에서 사서함**을 선택합니다.

5. **복구** > **전체 사서함**을 클릭합니다.
6. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, **Microsoft 365 조직**을 클릭하여 대상 조직을 보기, 변경 또는 지정합니다.
   기본적으로 원래 조직이 선택됩니다. 이 조직이 Cyber Protection 서비스에 등록되지 않았다면 대상 조직을 지정해야 합니다.
7. **사서함으로 복구**에서 대상 사서함을 보고, 변경하거나 지정합니다.
   기본적으로 원래 사서함이 선택됩니다. 이 사서함이 존재하지 않거나 원래 이외 조직을 선택한 경우에는 대상 사서함을 지정해야 합니다.
   복구 중에는 새로운 대상 사서함을 만들 수 없습니다. 사서함을 새로운 대상으로 복구하려면 먼저 원하는 Microsoft 365 조직에 대상 사서함을 만든 다음 클라우드 에이전트가 변경 사항을 동기화하도록 해야 합니다. 클라우드 에이전트는 매 24시간마다 자동으로 Microsoft 365와 동기화합니다. 변경 사항을 즉시 동기화하려면 Cyber Protect 콘솔에서 **Microsoft 365** 페이지의 조직을 선택한 다음 **새로 고침**을 클릭합니다.
8. **복구 시작**을 클릭합니다.
9. 다음 덮어쓰기 옵션 중 하나를 선택합니다.
   - **기존 항목 덮어쓰기**
   - **기존 항목 덮어쓰기 안 함**
10. **진행**을 클릭하여 결정을 확인합니다.

사서함 항목 복구

1. **Microsoft 365**를 클릭합니다.
2. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, 복구를 원하는 백업된 데이터가 있는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. 다음 중 하나를 수행하십시오.
   - 사용자 사서함의 항목을 복구하려면, **사용자** 노드를 확장하고 **전체 사용자**를 선택하고 복구하려는 항목이 원래 포함된 사서함의 사용자를 선택한 후 **복구**를 클릭합니다.
   - 공유 사서함의 항목을 복구하려면, **사용자** 노드를 확장하고 **전체 사용자**를 선택한 다음 처음에 복구하려는 항목을 포함하고 있던 공유 사서함을 선택한 후 **복구**를 클릭합니다.

© Acronis International GmbH, 2003-2024

- 그룹 사서함의 항목을 복구하려면, **그룹** 노드를 확장하고 **전체 그룹**을 선택하고 복구하려는 항목이 원래 포함된 사서함의 그룹을 선택한 후 **복구**를 클릭합니다.
- 사용자 그룹 또는 공유 사서함이 삭제되었다면 백업 스토리지 탭의 **클라우드 애플리케이션 백업** 섹션에서 해당 항목을 선택한 후 **백업 표시**를 클릭합니다.

사용자와 그룹은 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.

4. 복구 지점을 선택합니다.

참고
사서함이 포함된 복구 지점만 보려면 **내용별 필터에서 사서함**을 선택합니다.

5. **복구** > **이메일 메시지**를 클릭합니다.
6. 필요한 폴더를 찾거나 검색 기능을 사용하여 필요한 항목 목록을 얻습니다.
   다음 검색 옵션을 사용할 수 있습니다. 와일드카드는 지원되지 않습니다.
   - 이메일 메시지: 제목, 보낸 사람, 받는 사람, 첨부 파일 이름, 날짜로 검색합니다. 시작 날짜나 종료 날짜 중 하나를 선택(검색이 해당 날짜에 시작되거나 종료됨)할 수도 있고 두 날짜를 모두 선택하여 특정 시간 범위 내에서 검색을 할 수도 있습니다.
   - 이벤트: 제목 및 날짜로 검색합니다.
   - 작업: 제목 및 날짜로 검색합니다.
   - 연락처: 이름, 이메일 주소, 전화번호로 검색합니다.
7. 복구할 항목을 선택합니다. 폴더를 선택하려면 "폴더 복구" 아이콘 을 클릭하십시오.
   복구 중에는 새로운 대상 사서함을 만들 수 없습니다. 새로운 사서함 항목을 새로운 사서함으로 복구하려면 먼저 Microsoft 365 조직에서 대상 새 사서함 항목을 만든 다음 클라우드 에이전트가 변경 사항을 동기화하도록 해야 합니다. 클라우드 에이전트는 매 24시간마다 자동으로 Microsoft 365와 동기화합니다. 변경 사항을 즉시 동기화하려면 Cyber Protect 콘솔에서 **Microsoft 365** 페이지의 조직을 선택한 다음 **새로 고침**을 클릭합니다.
   뿐만 아니라 다음을 수행할 수 있습니다.
   - 항목이 선택되면 **내용 표시**를 클릭하여 첨부 파일을 포함한 내용을 확인합니다. 첨부된 파일의 이름을 클릭하여 이를 다운로드하십시오.
   - 이메일 메시지나 달력 항목을 선택한 경우 **이메일로 보내기**를 클릭해 해당 항목을 지정한 이메일 주소로 전송합니다. 발신자를 선택하고 전송 항목에 추가할 텍스트를 작성할 수 있습니다.
   - 백업이 암호화되지 않고 검색을 사용하고 검색 결과에서 단일 항목만 선택한 경우에만: **버전 표시**를 클릭하여 복구할 항목 버전을 선택합니다. 선택한 복구 지점 이전이나 이후 백업된 버전을 선택할 수 있습니다.
8. **복구**를 클릭합니다.
9. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, **Microsoft 365 조직**을 클릭하여 대상 조직을 보기, 변경 또는 지정합니다.
   기본적으로 원래 조직이 선택됩니다. 이 조직이 Cyber Protection 서비스에 등록되지 않았다면 대상 조직을 지정해야 합니다.
10. **사서함으로 복구**에서 대상 사서함을 보고, 변경하거나 지정합니다.

© Acronis International GmbH, 2003-2024

기본적으로 원래 사서함이 선택됩니다. 이 사서함이 존재하지 않거나 원래 이외 조직을 선택한 경우에는 대상 사서함을 지정해야 합니다.

11. [사용자 또는 공유 사서함을 복구할 경우에만 해당] **경로**에서 대상 사서함의 대상 폴더를 보거나 변경합니다. 기본적으로 **복구 항목** 폴더가 선택되어 있습니다.

    그룹 사서함 항목은 항상 **받은 편지함** 폴더로 복구됩니다.
12. **복구 시작**을 클릭합니다.
13. 다음 덮어쓰기 옵션 중 하나를 선택합니다.
    - **기존 항목 덮어쓰기**
    - **기존 항목 덮어쓰기 안 함**
14. **진행**을 클릭하여 결정을 확인합니다.

전체 사서함을 PST 데이터 파일로 복구

참고
PST 파일로의 복구 과정에서는 현재 아카이브를 복원할 수 없습니다. 현재 위치 아카이브를 사서함과 함께 복원하려는 경우에는 "사서함 복구"(558페이지) 항목을 참조하십시오.

사서함을 복구하려면

1. **Microsoft 365**를 클릭합니다.
2. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, 복구를 원하는 백업된 데이터가 있는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. 다음 중 하나를 수행하십시오.
   - 사용자 사서함을 PST 데이터 파일로 복구하려면, **사용자** 노드를 확장하고 **전체 사용자**를 선택하고 복구하려는 사서함을 선택한 다음 **복구**를 클릭합니다.
   - 공유 사서함을 PST 데이터 파일로 복구하려면, **사용자** 노드를 확장하고 **전체 사용자**를 선택하고 복구하려는 사서함을 선택한 다음 **복구**를 클릭합니다.
   - 그룹 사서함을 PST 데이터 파일로 복구하려면, **그룹** 노드를 확장하고 **전체 그룹**을 선택하고 복구하려는 사서함의 그룹을 선택한 다음 **복구**를 클릭합니다.

   사용자와 그룹은 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.

   사용자 그룹 또는 공유 Outlook 데이터 파일이 삭제되었다면 백업 스토리지 탭의 **클라우드 애플리케이션 백업** 섹션에서 해당 항목을 선택한 다음 **백업 표시**를 클릭합니다.
4. **복구** > **PST 파일로**를 클릭합니다.
5. PST 파일과 함께 아카이브를 암호화하기 위한 비밀번호를 설정합니다.

   비밀번호에는 하나 이상의 기호가 포함되어야 합니다.
6. 암호를 확인하고 **완료**를 클릭합니다.
7. 선택한 사서함 항목이 PST 데이터 파일로 복구되고 ZIP 포맷으로 아카이브됩니다. PST 파일의 최대 크기는 2GB로 제한되므로 복구하려는 데이터가 2GB를 초과하면 여러 개의 PST 파일로 분할됩니다. ZIP 아카이브는 설정한 비밀번호로 보호됩니다.
8. 생성된 PST 파일이 포함된 ZIP 아카이브에 대한 링크가 포함된 이메일을 수신하게 됩니다.
9. 관리자는 사용자가 복구 절차를 수행했음을 알리는 이메일 알림을 수신하게 됩니다.

© Acronis International GmbH, 2003-2024

참고
사서함을 PST 파일로 복구하는 경우 복잡한 알고리즘을 사용해 데이터를 전송하고 변형하므로 시간이 오래 걸릴 수 있습니다.

PST 파일이 포함된 아카이브를 다운로드하고 복구를 완료하려면

1. 다음 중 하나를 수행하십시오.
   - 이메일에서 아카이브를 다운로드하려면 **파일 다운로드** 링크를 따라갑니다.
     아카이브는 24시간 내에 다운로드할 수 있습니다. 링크가 만료된 경우 복구 절차를 반복합니다.
   - Cyber Protect 콘솔에서 아카이브를 다운로드하려면
     a. **백업 스토리지** > **PST 파일**로 이동합니다.
     b. 강조 표시된 최신 아카이브를 선택합니다.
     c. 오른쪽 창에서 **다운로드**를 클릭합니다.

   컴퓨터의 기본 다운로드 디렉토리에 아카이브가 다운로드됩니다.
2. 아카이브를 암호화할 때 설정한 비밀번호를 사용하여 아카이브에서 PST 파일을 추출합니다.
3. Microsoft Outlook에서 PST 파일을 엽니다.
   결과 PST 파일은 크기가 원래 사서함보다 훨씬 작을 수 있는데 이는 정상적인 현상입니다.

   중요
   이 파일을 **가져오기 및 내보내기 마법사**를 사용해 Microsoft Outlook으로 가져오지 마십시오. 파일을 두 번 클릭하거나 마우스 오른쪽 버튼으로 클릭하고 컨텍스트 메뉴에서 **다음으로 열기...** > **Microsoft Outlook** 을 선택합니다.

사서함 항목을 PST 파일에 복구

참고
PST 파일로의 복구 과정에서는 현재 아카이브를 복원할 수 없습니다. 현재 위치 아카이브를 사서함과 함께 복원하려는 경우에는 "사서함 복구"(558페이지) 항목을 참조하십시오.

사서함 항목을 복구하려면

1. **Microsoft 365**를 클릭합니다.
2. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, 복구를 원하는 백업된 데이터가 있는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. 다음 중 하나를 수행하십시오.
   - 사용자 사서함의 항목을 복구하려면, **사용자** 노드를 확장하고 **전체 사용자**를 선택하고 복구하려는 항목이 원래 포함된 사서함의 사용자를 선택한 후 **복구**를 클릭합니다.
   - 공유 사서함의 항목을 복구하려면, **사용자** 노드를 확장하고 **전체 사용자**를 선택한 다음 처음에 복구하려는 항목을 포함하고 있던 공유 사서함을 선택한 후 **복구**를 클릭합니다.
   - 그룹 사서함의 항목을 복구하려면, **그룹** 노드를 확장하고 **전체 그룹**을 선택하고 복구하려는 항목이 원래 포함된 사서함의 그룹을 선택한 후 **복구**를 클릭합니다.

© Acronis International GmbH, 2003-2024

- 사용자 그룹 또는 공유 사서함이 삭제되었다면 백업 스토리지 탭의 **클라우드 애플리케이션 백업** 섹션에서 해당 항목을 선택한 후 **백업 표시**를 클릭합니다.

사용자와 그룹은 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.

4. **복구** > **이메일 메시지**를 클릭합니다.
5. 필요한 폴더를 찾거나 검색 기능을 사용하여 필요한 항목 목록을 얻습니다.

   다음 검색 옵션을 사용할 수 있습니다. 와일드카드는 지원되지 않습니다.
   - 이메일 메시지: 제목, 보낸 사람, 받는 사람, 첨부 파일 이름, 날짜로 검색합니다.
   - 이벤트: 제목 및 날짜로 검색합니다.
   - 작업: 제목 및 날짜로 검색합니다.
   - 연락처: 이름, 이메일 주소, 전화번호로 검색합니다.
6. 복구할 항목을 선택합니다. 폴더를 선택하려면 "폴더 복구" 아이콘 을 클릭하십시오.

   뿐만 아니라 다음을 수행할 수 있습니다.
   - 항목을 선택한 경우 첨부 파일을 포함한 내용을 보려면 **내용 표시**를 클릭하십시오. 첨부 파일을 다운로드하려면 그 이름을 클릭하십시오.
   - 이메일 메시지나 달력 항목을 선택한 경우 **이메일로 보내기**를 클릭해 해당 항목을 지정한 이메일 주소로 전송합니다. 발신자를 선택하고 전송 항목에 추가할 텍스트를 작성할 수 있습니다.
   - 백업이 암호화되지 않고 검색을 사용하고 검색 결과에서 단일 항목만 선택한 경우에만: **버전 표시**를 클릭하여 복구할 항목 버전을 선택합니다. 선택한 복구 지점 이전이나 이후 백업된 버전을 선택할 수 있습니다.
7. **PST 파일로 복구**를 클릭합니다.
8. PST 파일과 함께 아카이브를 암호화하기 위한 비밀번호를 설정합니다.

   비밀번호에는 하나 이상의 기호가 포함되어야 합니다.
9. 비밀번호를 확인하고 **완료**를 클릭합니다.

선택한 사서함 항목이 PST 데이터 파일로 복구되고 ZIP 포맷으로 아카이브됩니다. PST 파일의 최대 크기는 2GB로 제한되므로 복구하려는 데이터가 2GB를 초과하면 여러 개의 PST 파일로 분할됩니다. ZIP 아카이브는 설정한 비밀번호로 보호됩니다.

생성된 PST 파일이 포함된 ZIP 아카이브에 대한 링크가 포함된 이메일을 수신하게 됩니다.

관리자는 사용자가 복구 절차를 수행했음을 알리는 이메일 알림을 수신하게 됩니다.

PST 파일이 포함된 아카이브를 다운로드하고 복구를 완료하려면

1. 다음 중 하나를 수행하십시오.
   - 이메일에서 아카이브를 다운로드하려면 **파일 다운로드** 링크를 따라갑니다.

     아카이브는 24시간 내에 다운로드할 수 있습니다. 링크가 만료된 경우 복구 절차를 반복합니다.
   - Cyber Protect 콘솔에서 아카이브를 다운로드하려면
     a. **백업 스토리지** > **PST 파일**로 이동합니다.
     b. 강조 표시된 최신 아카이브를 선택합니다.
     c. 오른쪽 창에서 **다운로드**를 클릭합니다.

© Acronis International GmbH, 2003-2024

컴퓨터의 기본 다운로드 디렉토리에 아카이브가 다운로드됩니다.

2. 아카이브를 암호화할 때 설정한 비밀번호를 사용하여 아카이브에서 PST 파일을 추출합니다.
3. Microsoft Outlook에서 PST 파일을 엽니다.

   결과 PST 파일은 크기가 원래 사서함보다 훨씬 작을 수 있는데 이는 정상적인 현상입니다.

중요

이 파일을 **가져오기 및 내보내기 마법사**를 사용해 Microsoft Outlook으로 가져오지 마십시오. 파일을 열려면 해당 파일을 두 번 클릭하거나 마우스 오른쪽 버튼으로 클릭하고 컨텍스트 메뉴에서 **연결 프로그램...** > **Microsoft Outlook** 을 선택합니다.

공용 폴더 및 폴더 항목 복구

공용 폴더 또는 공용 폴더 항목을 복구하려면 대상 Microsoft 365 조직의 관리자 최소 한 명이 대상 공용 폴더에 대한 **소유자** 권한을 갖고 있어야 합니다. 액세스 거부 오류와 함께 복구가 실패하면 대상 폴더 속성에서 이 권한을 할당하고, Cyber Protect 콘솔에서 대상 조직을 선택한 다음, **새로 고침**을 클릭하고 복구를 다시 실행합니다.

공용 폴더 또는 폴더 항목을 복구하려면

1. **Microsoft 365**를 클릭합니다.
2. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, 백업 데이터의 복구를 원하는 조직을 확대합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. 다음 중 하나를 수행하십시오.
   - **공용 폴더** 노드를 확대하고 **모든 공용 폴더**를 선택하고, 복구하려는 공용 폴더 또는 복구하려는 항목을 원래 포함하고 있던 공용 폴더를 선택한 다음, **복구**를 클릭합니다.
   - 공용 폴더가 삭제되었다면 백업 스토리지 탭의 **클라우드 애플리케이션 백업** 섹션에서 선택한 후 **백업 표시**를 클릭합니다.

   공용 폴더를 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.
4. 복구 지점을 선택합니다.
5. **데이터 복구**를 클릭합니다.
6. 필요한 폴더를 찾거나 검색 기능을 사용하여 필요한 항목 목록을 얻습니다.

   이메일 메시지와 게시물을 제목, 보낸 사람, 받는 사람, 날짜로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.
7. 복구할 항목을 선택합니다. 폴더를 선택하려면 "폴더 복구" 아이콘 을 클릭하십시오.

   뿐만 아니라 다음을 수행할 수 있습니다.
   - 이메일 메시지나 게시물을 선택한 경우 첨부 파일을 포함하여 내용을 보려면 **내용 표시**를 클릭하십시오. 첨부 파일을 다운로드하려면 그 이름을 클릭하십시오.
   - 이메일 메시지나 게시물을 선택한 경우 **이메일로 보내기**를 클릭해 해당 항목을 지정한 이메일 주소로 전송합니다. 발신자를 선택하고 전송 항목에 추가할 텍스트를 작성할 수 있습니다.
   - 백업이 암호화되지 않고 검색을 사용하고 검색 결과에서 단일 항목만 선택한 경우에만: **버전 표시**를 클릭하여 복구할 항목 버전을 선택합니다. 선택한 복구 지점 이전이나 이후 백업된 버전을 선택할 수 있습니다.

© Acronis International GmbH, 2003-2024

8. **복구**를 클릭합니다.
9. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, **Microsoft 365 조직**을 클릭하여 대상 조직을 보기, 변경 또는 지정합니다.

   기본적으로 원래 조직이 선택됩니다. 이 조직이 Cyber Protection 서비스에 등록되지 않았다면 대상 조직을 지정해야 합니다.
10. **공용 폴더로 복구**에서 대상 공용 폴더를 보고, 변경하거나 지정합니다.

    기본적으로 원래 폴더가 선택됩니다. 이 폴더가 존재하지 않거나 원래 이외 조직을 선택한 경우 대상 폴더를 지정해야 합니다.

    복구 중에는 새로운 공용 폴더를 만들 수 없습니다. 공용 폴더를 새로운 폴더로 복구하려면 먼저 원하는 Microsoft 365 조직에 대상 공용 폴더를 만든 다음 클라우드 에이전트가 변경 사항을 동기화하도록 해야 합니다. 클라우드 에이전트는 매 24시간마다 자동으로 Microsoft 365와 동기화합니다. 변경 사항을 즉시 동기화하려면 Cyber Protect 콘솔에서 **Microsoft 365** 페이지의 조직을 선택한 다음 **새로 고침**을 클릭합니다.
11. **경로**에서 대상 공용 폴더에 포함된 대상 하위 폴더를 보거나 변경합니다. 기본적으로 원본 경로가 재생성됩니다.
12. **복구 시작**을 클릭합니다.
13. 다음 덮어쓰기 옵션 중 하나를 선택합니다.

옵션	설명
기존 항목 덮어쓰기	대상 위치의 기존 파일을 모두 덮어씁니다.
기존 항목 덮어쓰기 안 함	대상 위치에 이름이 같은 파일이 있으면 해당 파일을 덮어쓰지 않으며 대상 위치에 소스 파일이 저장되지 않습니다.

14. **진행**을 클릭하여 결정을 확인합니다.

OneDrive 파일 보호

어떤 항목을 백업할 수 있습니까?

OneDrive, 또는 개별 파일 및 폴더를 백업할 수 있습니다.

백업 계획에 있는 별도 옵션을 사용하면 OneNote 전자 필기장을 백업할 수 있습니다.

파일은 공유 권한과 함께 백업됩니다. 고급 권한 레벨(**설계**, **전체**, **기여**)은 백업되지 않습니다.

일부 파일에는 민감한 정보가 포함될 수 있으며 Microsoft 365의 DLP(데이터 손실 방지) 규칙에 따라 파일에 대한 액세스가 차단될 수 있습니다. 이러한 파일은 백업되지 않으며 백업 작업이 완료된 후에도 경고가 표시되지 않습니다.

제한 사항

공유 사서함에서는 OneDrive의 내용을 백업할 수 없습니다. 이 내용을 백업하려면 공유 사서함을 일반 사용자 계정으로 변환한 후 해당 계정에 대해 OneDrive가 활성화되어 있는지 확인합니다.

© Acronis International GmbH, 2003-2024

복구할 수 있는 항목은 무엇입니까?

전체 OneDrive 또는 백업되었던 파일이나 폴더를 복구할 수 있습니다.

검색 기능을 사용해 항목을 찾을 수 있습니다.

그 공유 권한을 복구할지 아니면 파일이 복구될 대상 폴더로부터 권한을 상속하게 할지 선택할 수 있습니다.

파일 및 폴더에 대한 공유 링크는 복구되지 않습니다.

OneDrive 파일 선택

아래 설명에 따라 파일을 선택한 다음, 보호 계획의 기타 설정을 적절하게 지정합니다.

OneDrive 파일을 선택하려면

1. **Microsoft 365**를 클릭합니다.
2. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우 사용자 데이터의 백업을 원하는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. 다음 중 하나를 수행하십시오.
   - 전체 사용자의 파일(앞으로 생성될 사용자 포함)을 백업하려면, **사용자** 노드를 확장하고 **전체 사용자**를 선택한 후 **그룹 백업**을 클릭합니다.
   - 개별 사용자의 파일을 백업하려면, **사용자** 노드를 확장하고 **전체 사용자**를 선택하고 백업하려는 파일의 사용자를 선택한 후 **백업**을 클릭합니다.
4. 보호 계획 패널에서:
   - **백업 대상**에서 **OneDrive** 항목이 선택되는지 확인합니다.

     개별적으로 선택한 일부 사용자의 Microsoft 365 계획에 OneDrive 서비스가 포함되어 있지 않으면 이 옵션을 선택할 수 없습니다.

     그룹 백업을 위해 선택한 일부 사용자의 Microsoft 365 계획에 OneDrive 서비스가 포함되어 있지 않은 경우 이 옵션을 선택할 수 있지만 이러한 사용자에게는 보호 계획이 적용되지 않습니다.
   - **백업할 항목**에서 다음 중 하나를 수행하십시오.
     - 기본 설정 **[전체]**(전체 파일)을 유지합니다.
     - 이름이나 경로를 추가하여 백업할 파일과 폴더를 지정합니다.

       와일드카드 문자(*, ** 및 ?)를 사용할 수 있습니다. 경로 지정과 와일드카드 사용에 관한 자세한 내용은 "파일 필터"를 참조하십시오.
     - 찾아보기를 통해 백업할 파일과 폴더를 선택합니다.

       찾아보기 링크는 단일 사용자를 위한 보호 계획을 생성할 때만 사용할 수 있습니다.
   - [선택 사항] **백업할 항목**에서 **예외 표시**를 클릭하여 백업에서 생략할 파일과 폴더를 지정합니다.

     파일 제외는 파일 선택에 우선합니다. 즉, 두 필드에 동일 파일을 지정하면 백업 중 이 파일은 건너뜁니다.
   - [선택 사항] OneNote 전자 필기장을 백업하려면 **OneNote 포함** 스위치를 활성화합니다.

© Acronis International GmbH, 2003-2024

OneDrive 및 OneDrive 파일 복구

전체 OneDrive 복구

1. **Microsoft 365**를 클릭합니다.
2. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, 복구를 원하는 백업된 데이터가 있는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. **사용자** 노드를 확장하고 **전체 사용자**를 선택하고 복구하려는 OneDrive의 사용자를 선택한 후 **복구**를 클릭합니다.

   사용자가 삭제되었다면 백업 스토리지 탭의 **클라우드 애플리케이션 백업** 섹션에서 해당 사용자를 선택한 후 **백업 표시**를 클릭합니다.

   사용자를 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.
4. 복구 지점을 선택합니다.

   참고
   OneDrive 파일이 포함된 복구 지점만 보려면 **내용별 필터링**에서 **OneDrive**를 선택합니다.

5. **복구** > **전체 OneDrive**를 클릭합니다.
6. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, **Microsoft 365 조직**을 클릭하여 대상 조직을 보기, 변경 또는 지정합니다.

   기본적으로 원래 조직이 선택됩니다. 이 조직이 Cyber Protection 서비스에 등록되지 않았다면 대상 조직을 지정해야 합니다.

   복구 중에는 새로운 OneDrive 대상을 만들 수 없습니다. OneDrive를 새로운 대상으로 복구하려면 먼저 Microsoft 365 조직에서 대상 OneDrive를 만든 다음 클라우드 에이전트가 변경 사항을 동기화하도록 해야 합니다. 클라우드 에이전트는 매 24시간마다 자동으로 Microsoft 365와 동기화합니다. 변경 사항을 즉시 동기화하려면 Cyber Protect 콘솔에서 **Microsoft 365** 페이지의 조직을 선택한 다음 **새로 고침**을 클릭합니다.
7. **드라이브로 복구**에서 대상 사용자를 보고, 변경하거나 지정합니다.

   기본적으로 원래 사용자가 선택됩니다. 이 사용자가 존재하지 않거나 원래 조직을 선택한 경우에는 대상 사용자를 지정해야 합니다.
8. 파일에 대해 공유 권한을 복구할 것인지 선택합니다.
9. **복구 시작**을 클릭합니다.
10. 다음 덮어쓰기 옵션 중 하나를 선택합니다.

옵션	설명
오래된 경우 기존 파일 덮어쓰기	대상 위치에 이름이 같으며 소스 파일보다 오래된 파일이 있으면 대상 위치에 소스 파일을 저장하여 이전 버전을 대체합니다.
기존 파일 덮어쓰기	마지막으로 수정한 날짜에 관계없이 대상 위치의 기존 파일을 모두 덮어씁니다.
기존 파일 덮어쓰기 안 함	대상 위치에 이름이 같은 파일이 있으면 해당 파일을 변경하지 않으며 대상 위치에 소스 파일이 저장되지 않습니다.

© Acronis International GmbH, 2003-2024

참고
OneNote 전자 필기장을 복구할 때 **기존 파일이 더 오래된 경우 덮어쓰기** 및 **기존 파일 덮어쓰기** 때문에 기존 OneNote 전자 필기장을 덮어씁니다.

11. **진행**을 클릭하여 결정을 확인합니다.

OneDrive 파일 복구

1. **Microsoft 365**를 클릭합니다.
2. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, 복구를 원하는 백업된 데이터가 있는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. **사용자** 노드를 확장하고 **전체 사용자**를 선택하고 복구하려는 OneDrive 파일의 사용자를 선택한 후 **복구**를 클릭합니다.

   사용자가 삭제되었다면 백업 스토리지 탭의 **클라우드 애플리케이션 백업** 섹션에서 해당 사용자를 선택한 후 **백업 표시**를 클릭합니다.

   사용자를 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.
4. 복구 지점을 선택합니다.

참고
OneDrive 파일이 포함된 복구 지점만 보려면 **내용별 필터링**에서 **OneDrive**를 선택합니다.

5. **복구** > **파일/폴더**를 클릭합니다.
6. 필요한 폴더를 찾거나 검색 기능을 사용하여 필요한 파일 및 폴더 목록을 얻습니다.
7. 복구할 파일을 선택합니다.

   백업이 암호화되지 않고 단일 파일을 선택한 경우 **버전 표시**를 클릭하여 복구할 파일 버전을 선택합니다. 선택한 복구 지점 이전이나 이후 백업된 버전을 선택할 수 있습니다.
8. 파일을 다운로드하려면 **다운로드**를 클릭하고 파일을 저장할 위치를 선택한 다음 **저장**을 클릭합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
9. **복구**를 클릭합니다.
10. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, **Microsoft 365 조직**을 클릭하여 대상 조직을 보기, 변경 또는 지정합니다.

    기본적으로 원래 조직이 선택됩니다. 이 조직이 Cyber Protection 서비스에 등록되지 않았다면 대상 조직을 지정해야 합니다.

    복구 중에는 새로운 OneDrive를 생성할 수 없습니다. 파일을 새로운 OneDrive로 복구하려면 먼저 원하는 Microsoft 365 조직에서 대상 OneDrive를 생성한 다음 클라우드 에이전트가 변경 사항을 동기화하도록 해야 합니다. 클라우드 에이전트는 매 24시간마다 자동으로 Microsoft 365와 동기화합니다. 변경 사항을 즉시 동기화하려면 Cyber Protect 콘솔에서 **Microsoft 365** 페이지의 조직을 선택한 다음 **새로 고침**을 클릭합니다.
11. **드라이브로 복구**에서 대상 사용자를 보고, 변경하거나 지정합니다.

    기본적으로 원래 사용자가 선택됩니다. 이 사용자가 존재하지 않거나 원래 이외 조직을 선택한 경우 대상 사용자를 지정해야 합니다.

© Acronis International GmbH, 2003-2024

12. 경로에서 **대상 사용자**의 OneDrive에 포함된 대상 폴더를 보거나 변경합니다. 기본적으로 원래 위치가 선택됩니다.
13. 파일에 대해 공유 권한을 복구할 것인지 선택합니다.
14. **복구 시작**을 클릭합니다.
15. 다음 파일 덮어쓰기 옵션 중 하나를 선택합니다.

옵션	설명
오래된 경우 기존 파일 덮어쓰기	대상 위치에 이름이 같으며 소스 파일보다 오래된 파일이 있으면 대상 위치에 소스 파일을 저장하여 이전 버전을 대체합니다.
기존 파일 덮어쓰기	마지막으로 수정한 날짜에 관계없이 대상 위치의 기존 파일을 모두 덮어씁니다.
기존 파일 덮어쓰기 안 함	대상 위치에 이름이 같은 파일이 있으면 해당 파일을 변경하지 않으며 대상 위치에 소스 파일이 저장되지 않습니다.

참고
OneNote 전자 필기장을 복구할 때 **기존 파일이 더 오래된 경우 덮어쓰기** 및 **기존 파일 덮어쓰기** 때문에 기존 OneNote 전자 필기장을 덮어씁니다.

16. **진행**을 클릭하여 결정을 확인합니다.

SharePoint 온라인 사이트 보호

어떤 항목을 백업할 수 있습니까?

SharePoint 클래식 사이트 컬렉션과 그룹(모던 팀) 사이트, 통신 사이트를 백업할 수 있습니다. 뿐만 아니라 개별 하위 사이트, 목록, 라이브러리를 백업에 선택할 수도 있습니다.

백업 계획에 있는 별도 옵션을 사용하면 OneNote 전자 필기장을 백업할 수 있습니다.

백업 시 다음 항목은 *생략*됩니다.

- **디자인과 감각** 사이트 설정(**제목, 설명, 로고** 제외).
- 사이트 페이지 주석과 페이지 주석 설정(주석 **설정/해제**).
- **사이트 설정**을 포함한 사이트.
- 위키 페이지에 내장된 웹 파트 페이지와 웹 파트(SharePoint 온라인 API 제한으로 인함).
- 체크아웃된 파일 — 편집을 위해 수동으로 체크아웃된 파일과 **체크아웃 필요** 옵션이 활성화된 라이브러리에서 생성 또는 업로드된 모든 파일. 이러한 파일을 백업하려면 먼저 체크인하십시오.
- 열의 외부 데이터 및 관리 대상 메타데이터 유형
- 기본 사이트 컬렉션 "domain-my.sharepoint.com". 이는 조직 사용자의 OneDrive 파일이 모두 상주하는 컬렉션입니다.
- 휴지통 내 파일.

© Acronis International GmbH, 2003-2024

제한 사항

- 사이트/하위 사이트/목록/열의 제목 및 설명이 10000바이트를 초과할 경우, 백업 중 제목/설명이 잘립니다.
- SharePoint Online에서 생성한 이전 파일 버전은 백업할 수 없습니다. 파일의 최신 버전만 보호됩니다.
- 자료 보존 라이브러리는 백업할 수 없습니다.
- Microsoft 365의 이전 버전인 Business Productivity Online Suite(BPOS)에서 생성된 사이트를 백업할 수 없습니다.
- 관리 대상 경로를 사용하는 사이트의 설정을 백업할 수 없습니다(예: `https://<tenant>.sharepoint.com/portals/...`).
- 대상 Microsoft 365 조직에서 IRM(정보 권한 관리)이 활성화되어 있어야 목록이나 라이브러리의 IRM 설정을 복구할 수 있습니다.

복구할 수 있는 항목은 무엇입니까?

다음과 같은 항목을 사이트 백업에서 복구할 수 있습니다.

- 전체 사이트
- 하위 사이트
- 목록
- 목록 항목
- 문서 라이브러리
- 문서
- 목록 항목 첨부파일
- 사이트 페이지와 위키 페이지

검색 기능을 사용해 항목을 찾을 수 있습니다.

항목은 원래 또는 원래 이외 사이트로 복구할 수 있습니다. 복구 항목에 대한 경로는 원래 항목과 동일합니다. 경로가 존재하지 않는다면 생성됩니다.

공유 권한을 복구할지 아니면 항목이 복구 후 부모 개체로부터 권한을 상속하게 할지 선택할 수 있습니다.

복구할 수 없는 항목은 무엇입니까?

- **Visio Process Repository** 템플릿 기반의 하위 사이트.
- 다음 유형 목록: **설문조사 목록**, **작업 목록**, **사진 목록**, **링크**, **일정표**, **토론 게시판**, **외부**, **중요 스프레드시트**.
- 여러 콘텐츠 유형이 활성화되는 목록.

SharePoint 온라인 데이터 선택

아래 설명에 따라 데이터를 선택한 다음, 보호 계획의 기타 설정을 적절하게 지정합니다.

SharePoint 온라인 데이터를 선택하려면

© Acronis International GmbH, 2003-2024

1. **Microsoft 365**를 클릭합니다.
2. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우 사용자 데이터의 백업을 원하는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. 다음 중 하나를 수행하십시오.
   - 앞으로 생성될 사이트를 포함해 조직의 전체 일반 SharePoint 사이트를 백업하려면, **사이트 컬렉션**을 확장하고 **전체 사이트 컬렉션**을 선택한 후 **그룹 백업**을 클릭합니다.
   - 개별 일반 사이트를 복구하려면, **사이트 컬렉션** 노드를 확장하고 **전체 사이트 컬렉션**을 선택하고 백업하려는 사이트를 선택한 후 **백업**을 클릭합니다.
   - 앞으로 생성될 사이트를 포함해 전체 그룹(모던 팀) 사이트를 백업하려면, **그룹** 노드를 확장하고 **전체 그룹**을 선택한 후 **그룹 백업**을 클릭합니다.
   - 개별 그룹(모던 팀) 사이트를 복구하려면, **그룹** 노드를 확장하고 **전체 그룹**을 선택하고 백업하려는 사이트의 그룹을 선택한 후 **백업**을 클릭합니다.
4. 보호 계획 패널에서:
   - **백업 대상**에서 **SharePoint 사이트** 항목이 선택되는지 확인합니다.
   - **백업할 항목**에서 다음 중 하나를 수행하십시오.
     - 기본 설정 **[전체]** (선택한 사이트의 전체 항목)을 유지합니다.
     - 이름이나 경로를 추가하여 백업할 하위 사이트와 목록, 라이브러리를 지정합니다.

       하위 사이트나 상위 사이트 목록/라이브러리를 백업하려면 아래 포맷으로 표시 이름을 지정합니다: `/display name/**`

       하위 사이트 목록/라이브러리를 백업하려면 아래 포맷으로 표시 이름을 지정합니다: `/subsite display name/list display name/**`

       하위 사이트, 목록 및 라이브러리의 표시 이름은 SharePoint 사이트나 하위 사이트의 **사이트 목차** 페이지에 표시됩니다.
     - 찾아보기를 통해 백업할 하위 사이트를 지정합니다.

       찾아보기 링크는 단일 사이트를 위한 보호 계획을 생성할 때만 사용할 수 있습니다.
   - [선택 사항] **백업할 항목**에서 **예외 표시**를 클릭하여 백업에서 생략할 하위 사이트와 목록, 라이브러리를 지정합니다.

     항목 제외는 항목 선택에 우선합니다. 즉, 두 필드에 동일 하위 사이트를 지정하면 백업 중 이 하위 사이트는 건너뜁니다.
   - [선택 사항] OneNote 전자 필기장을 백업하려면 **OneNote 포함** 스위치를 활성화합니다.

SharePoint 온라인 데이터 복구

1. **Microsoft 365**를 클릭합니다.
2. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, 복구를 원하는 백업된 데이터가 있는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. 다음 중 하나를 수행하십시오.
   - 그룹(모던 팀) 사이트의 데이터를 복구하려면, **그룹** 노드를 확장하고 **전체 그룹**을 선택하고 복구하려는 항목이 원래 포함된 사이트의 그룹을 선택한 후 **복구**를 클릭합니다.
   - 일반 사이트의 데이터를 복구하려면, **사이트 컬렉션** 노드를 확장하고 **전체 사이트 컬렉션**을 선택하고 복구하려는 항목이 원래 포함된 사이트를 선택한 후 **복구**를 클릭합니다.

© Acronis International GmbH, 2003-2024

- 사이트가 삭제되었다면 백업 스토리지 탭의 **클라우드 애플리케이션 백업** 섹션에서 선택한 후 **백업 표시**를 클릭합니다.

그룹과 사이트는 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.

4. 복구 지점을 선택합니다.

참고
SharePoint 사이트가 포함된 복구 지점만 보려면 **내용별 필터링**에서 **SharePoint 사이트**를 선택합니다.

5. **SharePoint 파일 복구**를 클릭합니다.
6. 필요한 폴더를 찾거나 검색 기능을 사용하여 필요한 데이터 항목 목록을 얻습니다.
7. 복구할 항목을 선택합니다.

   백업이 암호화되지 않고 검색을 사용하고 검색 결과에서 단일 항목만 선택한 경우: **버전 표시**를 클릭하여 복구할 항목 버전을 선택할 수 있습니다. 선택한 복구 지점 이전이나 이후 백업된 버전을 선택할 수 있습니다.
8. [선택 사항] 항목을 다운로드하려면 **다운로드**를 클릭하고 항목을 저장할 위치를 선택한 다음 **저장**을 클릭합니다.
9. **복구**를 클릭합니다.
10. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, **Microsoft 365 조직**을 클릭하여 대상 조직을 보기, 변경 또는 지정합니다.

    기본적으로 원래 조직이 선택됩니다. 이 조직이 Cyber Protection 서비스에 등록되지 않았다면 대상 조직을 지정해야 합니다.
11. **사이트로 복구**에서 대상 사이트를 보고, 변경하거나 지정합니다.

    복구 중에는 새 SharePoint 사이트를 만들 수 없습니다. SharePoint 사이트를 새로운 사이트로 복구하려면 먼저 원하는 Microsoft 365 조직에서 대상 사이트를 만든 다음 클라우드 에이전트가 변경 사항을 동기화하도록 해야 합니다. 클라우드 에이전트는 매 24시간마다 자동으로 Microsoft 365와 동기화합니다. 변경 사항을 즉시 동기화하려면 Cyber Protect 콘솔에서 **Microsoft 365** 페이지의 조직을 선택한 다음 **새로 고침**을 클릭합니다.
12. 복구한 항목에 대해 공유 권한을 복구할 것인지 선택합니다.
13. **복구 시작**을 클릭합니다.
14. 다음 덮어쓰기 옵션 중 하나를 선택합니다.

옵션	설명
오래된 경우 기존 파일 덮어쓰기	대상 위치에 이름이 같으며 소스 파일보다 오래된 파일이 있으면 대상 위치에 소스 파일을 저장하여 이전 버전을 대체합니다.
기존 파일 덮어쓰기	마지막으로 수정한 날짜에 관계없이 대상 위치의 기존 파일을 모두 덮어씁니다.
기존 파일 덮어쓰기 안 함	대상 위치에 이름이 같은 파일이 있으면 해당 파일을 변경하지 않으며 대상 위치에 소스 파일이 저장되지 않습니다.

© Acronis International GmbH, 2003-2024

참고
OneNote 전자 필기장을 복구할 때 **기존 파일이 더 오래된 경우 덮어쓰기** 및 **기존 파일 덮어쓰기** 때문에 기존 OneNote 전자 필기장을 덮어씁니다.

15. **진행**을 클릭하여 결정을 확인합니다.

Microsoft 365 Teams 보호

어떤 항목을 백업할 수 있습니까?

팀 전체를 백업할 수 있습니다. 여기에는 팀 이름, 팀 구성원 목록, 팀 채널 및 콘텐츠, 팀 사서함 및 회의, 팀 사이트가 포함됩니다.

백업 계획에 있는 별도 옵션을 사용하면 OneNote 전자 필기장을 백업할 수 있습니다.

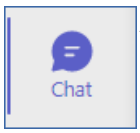
복구할 수 있는 항목은 무엇입니까?

- 전체 팀
- 팀 채널
- 채널 파일
- 팀 사서함
- 팀 사서함의 이메일 폴더
- 팀 사서함의 이메일 메시지
- 회의
- 팀 사이트

팀 채널의 대화는 복구할 수 없지만, 하나의 html 파일로 다운로드할 수 있습니다.

제한 사항

다음 항목은 백업되지 않습니다.

- Microsoft Teams beta API 제한에 따른 일반 채널 설정(중재 설정).
- Microsoft Teams beta API 제한에 따른 사용자 지정 채널 설정(중재 설정).
- 회의 메모.
- 채팅 섹션 

의 메시지. 이 섹션에는 비공개 일대일 채팅과 그룹 채팅이 표시됩니다.
- 스티커 및 칭찬.

백업 및 복구는 다음 채널 탭을 지원합니다.

- Word
- Excel
- PowerPoint

© Acronis International GmbH, 2003-2024

- PDF
- 문서 라이브러리

팀 선택

아래 설명에 따라 팀을 선택한 다음, 보호 계획의 기타 설정을 적절하게로 지정합니다.

팀을 선택하려면

1. **Microsoft 365**를 클릭합니다.
2. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가하였다면, 팀의 백업을 원하는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. 다음 중 하나를 수행하십시오.
   - 조직 내 모든 팀(앞으로 생성될 팀 포함)을 백업하려면 **Teams** 노드를 확장해 **모든 팀**을 선택한 후 **그룹 백업**을 클릭합니다.
   - 개별 팀을 백업하려면 **Teams** 노드를 확장하고 **모든 팀**을 선택하고 백업하려는 팀을 선택한 후 **백업**을 클릭합니다.

   이름으로 팀을 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.
4. 보호 계획 패널에서:
   - **백업 대상**에서 **Microsoft Teams** 항목을 선택했는지 확인합니다.
   - [선택 사항] **보관 기간**에서 정리 옵션을 설정합니다.
   - [선택 사항] 백업을 암호화하려면 **암호화** 스위치를 켠 다음 패스워드를 설정하고 암호화 알고리즘을 선택합니다.
   - [선택 사항] OneNote 전자 필기장을 백업하려면 **OneNote 포함** 스위치를 활성화합니다.

전체 팀 복구

1. **Microsoft 365**를 클릭합니다.
2. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, 복구를 원하는 백업된 팀이 있는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. **Teams** 노드를 확장하고 **모든 팀**을 선택하고 복구하려는 팀을 선택한 후 **복구**를 클릭합니다.

   이름으로 팀을 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.
4. 복구 지점을 선택합니다.
5. **복구** > **모든 팀**을 클릭합니다.

   여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, **Microsoft 365 조직**을 클릭하여 대상 조직을 보기, 변경 또는 지정합니다.

   기본적으로 원래 조직이 선택됩니다. 이 조직이 Cyber Protection 서비스에 등록되지 않았다면 대상 조직을 지정해야 합니다.
6. **팀으로 복구**에서 대상 팀을 확인하거나 다른 팀을 선택합니다.

   기본적으로 원래 팀이 선택됩니다. 이 팀이 삭제되어서 없거나 원래 팀이 포함되어 있지 않은 조직을 선택한 경우에는 드롭다운 목록에서 대상 팀을 선택해야 합니다.

   팀은 기존 팀으로만 복구할 수 있습니다. 복구 작업 중에는 팀을 생성할 수 없습니다.
7. **복구 시작**을 클릭합니다.

© Acronis International GmbH, 2003-2024

8. 다음 덮어쓰기 옵션 중 하나를 선택합니다.
   - **오래된 경우 기존 콘텐츠 덮어쓰기**
   - **기존 콘텐츠 덮어쓰기**
   - **기존 콘텐츠 덮어쓰지 않음**

   참고
   OneNote 전자 필기장을 복구할 때 **기존 콘텐츠가 더 오래된 경우 덮어쓰기** 및 **기존 콘텐츠 덮어쓰기** 옵션 때문에 기존 OneNote 전자 필기장을 덮어씁니다.

9. **진행**을 클릭하여 결정을 확인합니다.

Microsoft Teams의 그래픽 인터페이스에서 채널을 삭제한 경우, 시스템에서 바로 제거되지 않습니다. 따라서 모든 팀을 복구할 때 이 채널의 이름을 사용할 수 없으며 이름 끝에 표기가 추가됩니다.

대화는 채널의 **파일** 탭에 하나의 html 파일로 복구됩니다. 이 파일은 다음 패턴을 따른 이름의 폴더에서 확인할 수 있습니다. <팀 이름>_<채널 이름>_conversations_backup_<복구 날짜>T<복구 시간>Z.

참고
팀 또는 팀 채널을 복구한 후 Microsoft Teams로 이동하여 복구한 채널을 선택하고 **파일** 탭을 선택하십시오. 그러지 않으면 Microsoft Teams beta API 제한으로 해당 채널의 이후 백업에서 이 탭의 콘텐츠가 포함되지 않습니다.

팀 채널 또는 팀 채널의 파일 복구

팀 채널을 복구하려면

1. **Microsoft 365**를 클릭합니다.
2. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, 복구를 원하는 백업된 팀이 있는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. **Teams** 노드를 확장하고 **모든 팀**을 선택하고 채널을 복구하려는 팀을 선택한 후 **복구**를 클릭합니다.
4. 복구 지점을 선택합니다.
5. **복구** > **채널**을 클릭합니다.
6. 복구할 채널을 선택한 다음 **복구**를 클릭합니다. 메인 창에서 채널을 선택하려면 채널 이름 앞에 있는 확인란을 선택하십시오.

   다음 검색 옵션을 사용할 수 있습니다.
   - **대화**: 보낸 사람, 제목, 내용, 언어, 첨부 파일 이름, 날짜 또는 날짜 범위.
   - **파일**: 파일 또는 폴더 이름, 파일 유형, 크기, 마지막 변경 날짜 또는 날짜 범위.

   참고
   파일을 복구하는 대신 로컬로 다운로드할 수도 있습니다.

7. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, **Microsoft 365 조직**을 클릭하여 대상 조직을 보기, 변경 또는 지정합니다.

© Acronis International GmbH, 2003-2024

기본적으로 원래 조직이 선택됩니다. 이 조직이 Cyber Protection 서비스에 등록되지 않았다면 대상 조직을 지정해야 합니다.

8. **팀으로 복구**에서는 대상 팀을 보고, 변경하거나 지정합니다.
   기본적으로 원래 팀이 선택됩니다. 이 팀이 존재하지 않거나 원래 이외 조직을 선택한 경우 대상 팀을 지정해야 합니다.
9. **채널로 복구**에서는 대상 채널을 보고, 변경하거나 지정합니다.
10. **복구 시작**을 클릭합니다.
11. 다음 덮어쓰기 옵션 중 하나를 선택합니다.
    - **오래된 경우 기존 콘텐츠 덮어쓰기**
    - **기존 콘텐츠 덮어쓰기**
    - **기존 콘텐츠 덮어쓰지 않음**

    참고
    OneNote 전자 필기장을 복구할 때 **기존 콘텐츠가 더 오래된 경우 덮어쓰기** 및 **기존 콘텐츠 덮어쓰기** 옵션 때문에 기존 OneNote 전자 필기장을 덮어씁니다.

12. **진행**을 클릭하여 결정을 확인합니다.

대화는 채널의 **파일** 탭에 하나의 html 파일로 복구됩니다. 이 파일은 다음 패턴을 따른 이름의 폴더에서 확인할 수 있습니다. <팀 이름>_<채널 이름>_conversations_backup_<복구 날짜>T<복구 시간>Z.

참고
팀 또는 팀 채널을 복구한 후 Microsoft Teams로 이동하여 복구한 채널을 선택하고 **파일** 탭을 선택하십시오. 그러지 않으면 Microsoft Teams beta API 제한으로 해당 채널의 이후 백업에서 이 탭의 콘텐츠가 포함되지 않습니다.

팀 채널의 파일을 복구하려면

1. **Microsoft 365**를 클릭합니다.
2. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, 복구를 원하는 백업된 팀이 있는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. **Teams** 노드를 확장하고 **모든 팀**을 선택하고 채널을 복구하려는 팀을 선택한 후 **복구**를 클릭합니다.
4. 복구 지점을 선택합니다.
5. **복구** > **채널**을 클릭합니다.
6. 원하는 채널을 선택하고 **파일** 폴더를 엽니다.
   필요한 항목을 찾거나 검색 기능을 사용하여 필요한 항목 목록을 얻습니다. 파일 이름 또는 폴더 이름, 파일 유형, 크기, 마지막 변경 날짜 또는 날짜 범위 등의 검색 옵션을 사용할 수 있습니다.
7. [선택 사항] 항목을 다운로드하려면 **다운로드**를 클릭하고 항목을 저장할 위치를 선택한 다음 **저장**을 클릭합니다.
8. 복구할 항목을 선택한 다음 **복구**를 클릭합니다.

© Acronis International GmbH, 2003-2024

9. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, Microsoft 365 조직을 클릭하여 대상 조직을 보기, 변경 또는 지정합니다.
   기본적으로 원래 조직이 선택됩니다. 이 조직이 Cyber Protection 서비스에 등록되지 않았다면 대상 조직을 지정해야 합니다.
10. **팀으로 복구**에서는 대상 팀을 보고, 변경하거나 지정합니다.
    기본적으로 원래 팀이 선택됩니다. 이 팀이 존재하지 않거나 원래 이외 조직을 선택한 경우 대상 팀을 지정해야 합니다.
11. **채널로 복구**에서는 대상 채널을 보고, 변경하거나 지정합니다.
12. 복구한 항목에 대해 공유 권한을 복구할 것인지 선택합니다.
13. **복구 시작**을 클릭합니다.
14. 다음 덮어쓰기 옵션 중 하나를 선택합니다.
    - **오래된 경우 기존 콘텐츠 덮어쓰기**
    - **기존 콘텐츠 덮어쓰기**
    - **기존 콘텐츠 덮어쓰지 않음**

    참고
    OneNote 전자 필기장을 복구할 때 **기존 콘텐츠가 더 오래된 경우 덮어쓰기** 및 **기존 콘텐츠 덮어쓰기** 옵션 때문에 기존 OneNote 전자 필기장을 덮어씁니다.
15. **진행**을 클릭하여 결정을 확인합니다.

개별 대화는 복구할 수 없습니다. 메인 창에서는 **대화** 폴더를 찾아보거나 폴더 안의 콘텐츠를 하나의 html 파일로 다운로드할 수 있습니다. 이렇게 하려면 "폴더 복구" 아이콘 을 클릭하고 원하는 **대화** 폴더를 선택한 후 **다운로드**를 클릭합니다.

다음에 따라 **대화** 폴더의 메시지를 검색할 수 있습니다.

- 보내는 사람
- 내용
- 첨부 파일 이름
- 날짜

팀 사서함 복구

1. **Microsoft 365**를 클릭합니다.
2. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, 복구를 원하는 백업된 팀이 있는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. **Teams** 노드를 확장하고 **모든 팀**을 선택하고 사서함을 복구하려는 팀을 선택한 후 **복구**를 클릭합니다.
   이름으로 팀을 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.
4. 복구 지점을 선택합니다.
5. **복구 > 이메일 메시지**를 클릭합니다.
6. "폴더 복구" 아이콘 을 클릭하고 루트 사서함 폴더를 선택한 후 **복구**를 클릭합니다.

© Acronis International GmbH, 2003-2024

참고
선택한 사서함의 개별 폴더를 복구할 수 있습니다.

7. **복구**를 클릭합니다.
8. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, **Microsoft 365 조직**을 클릭하여 대상 조직을 보기, 변경 또는 지정합니다.
   기본적으로 원래 조직이 선택됩니다. 이 조직이 Cyber Protection 서비스에 등록되지 않았다면 대상 조직을 지정해야 합니다.
9. **사서함으로 복구**에서 대상 사서함을 보고, 변경하거나 지정합니다.
   기본적으로 원래 사서함이 선택됩니다. 이 사서함이 존재하지 않거나 원래 이외 조직을 선택한 경우에는 대상 사서함을 지정해야 합니다.
10. **복구 시작**을 클릭합니다.
11. 다음 덮어쓰기 옵션 중 하나를 선택합니다.
    - **기존 항목 덮어쓰기**
    - **기존 항목 덮어쓰기 안 함**
12. **진행**을 클릭하여 결정을 확인합니다.

팀 사서함 항목을 PST 파일에 복구

팀 사서함 항목을 복구하려면

1. **Microsoft 365**를 클릭합니다.
2. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, 복구를 원하는 백업된 데이터가 있는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. 사용자와 그룹은 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.
4. **Teams** 노드를 확장하고, **모든 팀**을 선택하고, 복구하려는 항목이 원래 포함되어 있는 사서함의 팀을 선택한 다음 **복구**를 클릭합니다.
5. **복구** > **이메일 메시지**를 클릭합니다.
6. 필요한 폴더를 찾거나 검색 기능을 사용하여 필요한 항목 목록을 얻습니다.
   다음 검색 옵션을 사용할 수 있습니다. 와일드카드는 지원되지 않습니다.
   - 이메일 메시지: 제목, 보낸 사람, 받는 사람, 첨부 파일 이름, 날짜로 검색합니다.
   - 이벤트: 제목 및 날짜로 검색합니다.
   - 작업: 제목 및 날짜로 검색합니다.
   - 연락처: 이름, 이메일 주소, 전화번호로 검색합니다.
7. 복구할 항목을 선택합니다. 폴더를 선택하려면 "폴더 복구" 아이콘 을 클릭하십시오.
   뿐만 아니라 다음을 수행할 수 있습니다.
   - 항목을 선택한 경우 첨부 파일을 포함한 내용을 보려면 **내용 표시**를 클릭하십시오. 첨부 파일을 다운로드하려면 그 이름을 클릭하십시오.
   - 이메일 메시지나 달력 항목을 선택한 경우 **이메일로 보내기**를 클릭해 해당 항목을 지정한 이메일 주소로 전송합니다. 발신자를 선택하고 전송 항목에 추가할 텍스트를 작성할 수 있습니다.

© Acronis International GmbH, 2003-2024

- 백업이 암호화되어 있지 않고 검색을 사용했으며 검색 결과에서 단일 항목만 선택한 경우, **버전 표시**를 클릭하여 복구할 항목 버전을 선택합니다. 선택한 복구 지점 이전이나 이후 관계없이 백업된 버전을 선택할 수 있습니다.

8. **PST 파일로 복구**를 클릭합니다.
9. PST 파일과 함께 아카이브를 암호화하기 위한 비밀번호를 설정합니다.
   비밀번호에는 하나 이상의 기호가 포함되어야 합니다.
10. 비밀번호를 확인하고 **완료**를 클릭합니다.

선택한 사서함 항목이 PST 데이터 파일로 복구되고 ZIP 포맷으로 아카이브됩니다. PST 파일의 최대 크기는 2GB로 제한되므로 복구하려는 데이터가 2GB를 초과하면 여러 개의 PST 파일로 분할됩니다. ZIP 아카이브는 설정한 비밀번호로 보호됩니다.

생성된 PST 파일이 포함된 ZIP 아카이브에 대한 링크가 포함된 이메일을 수신하게 됩니다.

관리자는 사용자가 복구 절차를 수행했음을 알리는 이메일 알림을 수신하게 됩니다.

PST 파일이 포함된 아카이브를 다운로드하고 복구를 완료하려면

1. 다음 중 하나를 수행하십시오.
   - 이메일에서 아카이브를 다운로드하려면 **파일 다운로드** 링크를 따라갑니다.
     아카이브는 24시간 내에 다운로드할 수 있습니다. 링크가 만료된 경우 복구 절차를 반복합니다.
   - Cyber Protect 콘솔에서 아카이브를 다운로드하려면
     a. **백업 스토리지** > **PST 파일**로 이동합니다.
     b. 강조 표시된 최신 아카이브를 선택합니다.
     c. 오른쪽 창에서 **다운로드**를 클릭합니다.

   컴퓨터의 기본 다운로드 디렉토리에 아카이브가 다운로드됩니다.
2. 아카이브를 암호화할 때 설정한 비밀번호를 사용하여 아카이브에서 PST 파일을 추출합니다.
3. Microsoft Outlook에서 PST 파일을 열거나 가져옵니다. 이 작업을 수행하는 방법을 알아보려면 Microsoft 설명서를 참조하십시오.

이메일 메시지 및 회의 복구

1. **Microsoft 365**를 클릭합니다.
2. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, 복구를 원하는 백업된 팀이 있는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. **Teams** 노드를 확장하고 **모든 팀**을 선택하고 이메일 메시지 또는 회의를 복구하려는 팀을 선택한 후 **복구**를 클릭합니다.
   이름으로 팀을 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.
4. 복구 지점을 선택합니다.
5. **복구** > **이메일 메시지**를 클릭합니다.
6. 필요한 항목을 찾거나 검색 기능을 사용하여 필요한 항목 목록을 얻습니다.
   다음 검색 옵션을 사용할 수 있습니다.

© Acronis International GmbH, 2003-2024

- 이메일 메시지: 제목, 보낸 사람, 받는 사람, 날짜로 검색합니다.
- 회의의 경우 이벤트 이름 및 날짜로 검색합니다.

7. 복구할 항목을 선택한 다음 **복구**를 클릭합니다.

참고
회의는 **일정** 폴더에서 확인할 수 있습니다.

뿐만 아니라 다음을 수행할 수 있습니다.

- 항목을 선택한 경우 첨부 파일을 포함한 내용을 보려면 **내용 표시**를 클릭하십시오. 첨부 파일을 다운로드하려면 그 이름을 클릭하십시오.
- 이메일 메시지나 회의를 선택한 경우 **이메일로 보내기**를 클릭해 해당 항목을 지정한 이메일 주소로 전송합니다. 발신자를 선택하고 전송 항목에 추가할 텍스트를 작성할 수 있습니다.

8. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, **Microsoft 365 조직**을 클릭하여 대상 조직을 보기, 변경 또는 지정합니다.
   기본적으로 원래 조직이 선택됩니다. 이 조직이 Cyber Protection 서비스에 등록되지 않았다면 대상 조직을 지정해야 합니다.
9. **사서함으로 복구**에서 대상 사서함을 보고, 변경하거나 지정합니다.
   기본적으로 원래 사서함이 선택됩니다. 이 사서함이 존재하지 않거나 원래 이외 조직을 선택한 경우에는 대상 사서함을 지정해야 합니다.
10. **복구 시작**을 클릭합니다.
11. 다음 덮어쓰기 옵션 중 하나를 선택합니다.
    - **기존 항목 덮어쓰기**
    - **기존 항목 덮어쓰기 안 함**
12. **진행**을 클릭하여 결정을 확인합니다.

팀 사이트 또는 사이트의 특정 항목 복구

1. **Microsoft 365**를 클릭합니다.
2. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, 복구를 원하는 백업된 팀이 있는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. **Teams** 노드를 확장하고 **모든 팀**을 선택하고 사이트를 복구하려는 팀을 선택한 후 **복구**를 클릭합니다.
   이름으로 팀을 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.
4. 복구 지점을 선택합니다.
5. **복구** > **팀 사이트**를 클릭합니다.
6. 필요한 항목을 찾거나 검색 기능을 사용하여 필요한 항목 목록을 얻습니다.
7. [선택 사항] 항목을 다운로드하려면 **다운로드**를 클릭하고 항목을 저장할 위치를 선택한 다음 **저장**을 클릭합니다.
8. 복구할 항목을 선택한 다음 **복구**를 클릭합니다.
9. 여러 Microsoft 365 조직을 Cyber Protection 서비스에 추가한 경우, **Microsoft 365 조직**을 클릭하여 대상 조직을 보기, 변경 또는 지정합니다.

© Acronis International GmbH, 2003-2024

기본적으로 원래 조직 및 팀이 선택됩니다. 이 조직이 Cyber Protection 서비스에 등록되지 않았다면 대상 조직을 지정해야 합니다.

10. **팀으로 복구**에서는 대상 팀을 보고, 변경하거나 지정합니다.
    기본적으로 원래 팀이 선택됩니다. 이 팀이 존재하지 않거나 원래 이외 조직을 선택한 경우 대상 사이트를 지정해야 합니다.
11. 복구한 항목에 대해 공유 권한을 복구할 것인지 선택합니다.
12. **복구 시작**을 클릭합니다.
13. 다음 덮어쓰기 옵션 중 하나를 선택합니다.
    - **오래된 경우 기존 콘텐츠 덮어쓰기**
    - **기존 콘텐츠 덮어쓰기**
    - **기존 콘텐츠 덮어쓰지 않음**

    참고
    OneNote 전자 필기장을 복구할 때 **기존 콘텐츠가 더 오래된 경우 덮어쓰기** 및 **기존 콘텐츠 덮어쓰기** 옵션 때문에 기존 OneNote 전자 필기장을 덮어씁니다.

14. **진행**을 클릭하여 결정을 확인합니다.

OneNote 전자 필기장 보호

OneDrive 파일, Microsoft Teams 및 SharePoint 사이트의 백업에는 OneNote 전자 필기장이 기본적으로 포함됩니다.

이러한 백업에서 OneNote 전자 필기장을 제외하려면 해당 백업 계획에서 **OneNote 포함** 스위치를 비활성화합니다.

백업한 OneNote 전자 필기장 복구

백업한 OneNote 전자 필기장을 복구하는 방법을 알아보려면 관련 주제를 참조하십시오.

- OneDrive 백업의 경우 "전체 OneDrive 복구"(567페이지) 또는 "OneDrive 파일 복구"(568페이지) 항목을 참조하십시오.
- Teams 백업의 경우 "전체 팀 복구"(574페이지), "팀 채널 또는 팀 채널의 파일 복구"(575페이지) 또는 "팀 사이트 또는 사이트의 특정 항목 복구"(580페이지) 항목을 참조하십시오.
- SharePoint 사이트 백업의 경우 "SharePoint 온라인 데이터 복구"(571페이지) 항목을 참조하십시오.

지원되는 버전

- OneNote(OneNote 2016 이상)
- Windows 10용 OneNote

제한 사항 및 알려진 문제

- OneDrive 또는 SharePoint에 저장하는 OneNote 전자 필기장의 크기는 2GB로 제한됩니다. 2GB보다 큰 OneNote 전자 필기장은 OneDrive 또는 SharePoint 대상으로 복구할 수 없습니다.

© Acronis International GmbH, 2003-2024

- 섹션 그룹이 포함된 OneNote 전자 필기장은 지원되지 않습니다.
- 기본 이름이 아닌 이름의 섹션이 포함된 백업된 OneNote 전자 필기장에서 첫 번째 섹션은 기본 이름(예: 새 섹션 제목 없음)으로 표시됩니다. 이는 섹션이 여러 개 있는 전자 필기장에서 섹션 순서에 영향을 줄 수 있습니다.
- OneNote 전자 필기장을 복구할 때 **기존 콘텐츠가 더 오래된 경우 덮어쓰기** 및 **기존 콘텐츠 덮어쓰기** 옵션 때문에 기존 OneNote 전자 필기장을 덮어씁니다.
- 팀 사이트의 전체 팀, 팀 사이트 또는 사이트 자산 폴더를 복구할 때 **기존 콘텐츠가 더 오래된 경우 덮어쓰기** 옵션 또는 **기존 콘텐츠 덮어쓰기** 옵션을 선택한 경우 해당 팀의 기본 OneNote 전자 필기장을 덮어쓰지 않습니다. *'/sites/<Team name>/SiteAssets/<OneNote notebook name>' 파일 속성 업데이트 실패* 경고와 함께 복구에 성공합니다.

Microsoft 365 협업 앱 시트 보호

Microsoft 365, Google Workspace 또는 Open-Xchange 사서함에 대한 실시간 보호 기능을 제공하는 Advanced Email Security 팩을 사용할 수 있습니다.

- 안티맬웨어 및 안티스팸
- 이메일에서 URL 검색
- DMARC 분석
- 피싱 방지
- 가장 보호
- 첨부 파일 검사
- 컨텐츠 무해화 및 재구성
- 신뢰 그래프

Microsoft 365 협업 앱 시트도 활성화할 수 있습니다. 그러면 콘텐츠 기반 보안 위협으로부터 Microsoft 365 클라우드 협업 애플리케이션을 보호할 수 있습니다. 이러한 애플리케이션으로는 OneDrive, SharePoint, Teams 등이 있습니다.

Advanced Email Security는 워크로드나 용량(기가바이트) 단위로 활성화할 수 있으며, 활성화 단위에 따라 라이선스 모델이 달라집니다.

Cyber Protect Cloud 콘솔에서 Advanced Email Security 온보딩을 진행하려면

1. **장치** > **Microsoft 365**를 클릭합니다.
2. **사용자** 노드를 클릭한 다음 오른쪽 상단에 있는 **Email Security로 이동** 링크를 클릭합니다.

Advanced Email Security 데이터 시트에서 Advanced Email Security에 대해 자세히 알 수 있습니다.

구성 지침은 Perception Point가 포함된 Advanced Email Security를 참조하십시오.

Google Workspace 데이터 보호

참고
규제 준수 모드의 테넌트에는 이 기능을 사용할 수 없습니다. 자세한 내용은 "규제 준수 모드"(982 페이지) 항목을 참조하십시오.

© Acronis International GmbH, 2003-2024

Google Workspace 데이터 보호의 의미

- Google Workspace 사용자 데이터(Gmail 사서함, 캘린더, 연락처, Google Drive) 및 Google Workspace Shared Drive의 C2C 백업 및 복구.
- 이메일, 파일, 연락처 및 기타 항목의 개별 복구.
- 다수의 Google Workspace의 조직과 교차 조직 복구에 대한 지원.
- Ethereum 블록체인 데이터베이스를 사용한 백업 파일 공증(선택 사항). 사용 시 파일이 신뢰할 수 있고 백업된 후 변경되지 않았음을 증명할 수 있습니다.
- 전체 텍스트 검색(선택 사항). 사용 시 이메일을 내용으로 검색할 수 있습니다.
- 회사당 최대 5000개의 항목(사서함, Google Drive, Shared Drive)을 성능 저하 없이 보호할 수 있습니다.
- 백업된 데이터는 자동으로 압축되며 원래 위치보다 백업 위치에서 공간을 덜 차지합니다. 클라우드 간 백업의 압축 수준은 고정되어 있으며 비 클라우드 간 백업의 **보통** 수준에 해당합니다. 이러한 수준에 대한 자세한 내용은 "압축 수준"(417페이지) 항목을 참조하십시오.

필수 사용자 권한

Cyber Protection

Cyber Protection에는 고객 테넌트 수준을 담당하는 회사 관리자로 접속해야 합니다. 부서 수준을 담당하는 회사 관리자, 부서 관리자, 사용자는 Google Workspace 데이터를 백업하거나 복구할 수 없습니다.

Google Workspace에서

Google Workspace 조직을 Cyber Protection 서비스에 추가하려면 API 액세스가 활성화되어 있는 슈퍼 관리자로 로그인해야 합니다(Google Admin 콘솔에서 **보안** > **API 참조** > **API 액세스 활성화**).

슈퍼 관리자 비밀번호는 어디에도 저장되지 않으며 백업 및 복구를 수행하는 데 사용되지 않습니다. Google Workspace에서 이 비밀번호를 변경해도 Cyber Protection 서비스 작업에는 영향을 주지 않습니다.

Google Workspace 조직을 추가한 슈퍼 관리자가 Google Workspace에서 삭제되거나 더 낮은 권한을 가진 역할로 변경될 시 백업은 "액세스가 거부됨"과 같은 오류와 함께 실패하게 됩니다. 이 경우 "Google Workspace 조직 추가하기"(584페이지)에 설명되어 있는 절차를 반복하여 유효한 슈퍼 관리자 자격 증명을 지정하십시오. 이런 상황을 방지하려면 백업 및 복구 전용 슈퍼 관리자를 생성하는 것이 좋습니다.

백업 스케줄 정보

클라우드 에이전트는 여러 고객을 대상으로 서비스를 제공하므로, 부하량을 고르게 분산시켜 모든 고객에게 동일한 품질의 서비스를 제공할 수 있도록 자체적으로 각 보호 계획의 시작 시간을 결정합니다.

각 보호 계획은 매일 같은 시간에 실행됩니다.

© Acronis International GmbH, 2003-2024

기본 옵션은 **하루에 한 번**입니다. Advanced Backup 팩을 사용하면 백업을 하루에 6번까지 예약할 수 있습니다. 백업은 클라우드 에이전트(데이터 센터 내 여러 고객의 백업을 처리함)의 현재 로드에 따라 달라지는 대략적인 간격으로 시작됩니다. 그러므로 로드가 하루 종일 일정하게 유지되며 모든 고객에게 동일한 서비스 품질이 제공됩니다.

제한 사항

- 콘솔에는 할당된 Google Workspace 라이센스와 사서함 또는 Google Drive가 있는 사용자만 표시됩니다.
- 기본 Google 형식의 문서는 일반 사무용 문서로 백업되며 Cyber Protect 콘솔에서 다른 확장자(예: .docx 또는 .pptx)로 표시됩니다. 문서는 복구 중에 원래 형식으로 다시 변환됩니다.
- 시간당 10개의 수동 백업 실행을 초과할 수 없습니다.
- 동시 복구 작업은 10개를 초과할 수 없습니다(Microsoft 365 및 Google Workspace 모두 포함한 수).
- 여러 복구 지점의 항목을 동시에 복구할 수는 없지만 검색 결과에서 여러 구 지점의 항목을 선택할 수는 있습니다.
- 삭제된 Google Workspace 사용자 계정의 백업은 클라우드 스토리지에서 자동으로 삭제되지 않습니다. 사용자는 이들 백업이 차지하는 스토리지 공간에 대한 비용을 지불해야 합니다.
- 같은 워크로드에 개별 백업 계획을 여러 개 적용할 수는 없습니다.
- 같은 워크로드에 개별 백업 계획과 그룹 백업 계획을 적용하면 개별 계획의 설정이 우선적으로 적용됩니다.

로깅

백업된 이메일의 내용 보기, 첨부 파일 또는 파일 다운로드, 이메일을 원본이 아닌 사서함으로 복구 또는 이메일로 보내는 등의 클라우드 간 리소스 관련 작업은 사용자 개인 정보를 침해할 수 있습니다. 이러한 작업은 관리 포털의 **모니터링** > **감사 로그**에 로깅됩니다.

Google Workspace 조직 추가하기

Cyber Protection 서비스에 Google Workspace 조직을 추가하려면 개인 전용 Google Cloud 프로젝트가 필요합니다. 이러한 프로젝트를 생성 및 구성하는 방법에 대한 자세한 내용은 "개인용 Google 클라우드 프로젝트 생성"(585페이지)을(를) 참조하십시오.

개인 전용 Google 클라우드 프로젝트를 사용하여 Google Workspace 조직을 추가하려면

1. Cyber Protect 콘솔에 회사 관리자로 로그인합니다.
2. **장치** > **추가** > **Google Workspace**를 클릭합니다.
3. Google Workspace 계정의 슈퍼 관리자 이메일 주소를 입력합니다.
   슈퍼 관리자 이메일 계정에 대해 2단계 확인이 활성화되어 있는지 여부는 이 절차에서 중요하지 않습니다.
4. Google 클라우드 프로젝트에서 생성한 서비스 계정의 개인 키가 포함된 JSON 파일을 찾습니다. 파일 내용을 텍스트로 붙여넣을 수도 있습니다.
5. **확인**을 클릭합니다.

© Acronis International GmbH, 2003-2024

그러면 콘솔의 **장치** 탭 아래에 Google Workspace 조직이 표시됩니다.

유용한 팁

- Google Workspace 조직을 추가하고 나면 기본 도메인과 보조 도메인에 있는 사용자 데이터와 Shared Drive가 백업됩니다. 백업된 리소스는 목록 하나로 표시되며, 도메인별로 그룹화되지 않습니다.
- 클라우드 에이전트는 조직이 Cyber Protection 서비스에 추가될 때부터 24시간 간격으로 Google Workspace에 동기화됩니다. 사용자 또는 Shared Drive를 추가하거나 제거하면 Cyber Protect 콘솔에서 이러한 변경 사항을 즉시 확인할 수 없습니다. 변경 사항을 즉시 동기화하려면 **Google Workspace** 페이지에 표시된 조직을 선택하고 **새로 고침**을 클릭합니다.

  Cyber Protect 콘솔과 Google Workspace 조직의 리소스 동기화에 대한 자세한 내용은 "Google Workspace 리소스 검색"(588페이지) 항목을 참조하십시오.
- **전체 사용자** 또는 **전체 Shared Drive** 그룹에 보호 계획을 적용하였다면, 새로 추가되는 항목은 동기화 후에만 백업에 포함됩니다.
- Google 정책에 따라, Google Workspace 그래픽 사용자 인터페이스에서 사용자나 공유 드라이브가 제거되더라도 며칠 동안은 API를 통해 제거한 사용자나 드라이브를 이용할 수 있습니다. 이 기간에는 제거된 항목이 Cyber Protect 콘솔에서 비활성화(회색으로 표시)되며 백업되지 않습니다. 제거한 항목은 API를 통해 사용할 수 없는 상태가 되면 Cyber Protect 콘솔에서 사라집니다. 해당 항목의 백업이 있을 경우 **백업 스토리지** > **클라우드 애플리케이션 백업**에서 확인할 수 있습니다.

개인용 Google 클라우드 프로젝트 생성

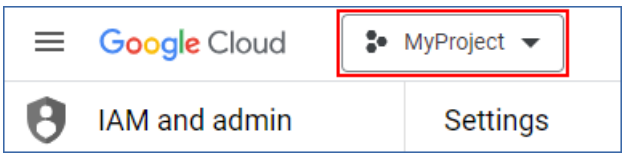
전용 Google 클라우드 프로젝트를 사용하여 Cyber Protection 서비스에 Google Workspace 조직을 추가하려면 다음 작업을 수행해야 합니다.

1. 새 Google 클라우드 프로젝트를 생성합니다.
2. 이 프로젝트에 필요한 API를 활성화합니다.
3. 이 프로젝트용 자격 증명을 구성합니다.
   a. OAuth 동의 화면을 구성합니다.
   b. Cyber Protection 서비스용 서비스 계정을 생성 및 구성합니다.
4. 새 프로젝트에 Google Workspace 계정 액세스 권한을 부여합니다.

참고
이 항목에서는 사전 고지 없이 변경될 수 있는 타사 사용자 인터페이스에 대해 설명합니다.

새 Google 클라우드 프로젝트를 생성하려면

1. 슈퍼 관리자로 Google Cloud Platform(console.cloud.google.com)에 로그인합니다.
2. Google Cloud Platform 콘솔의 왼쪽 위에서 프로젝트 선택을 클릭합니다.



© Acronis International GmbH, 2003-2024

3. 화면이 열리면 조직을 선택하고 **새 프로젝트**를 클릭합니다.

4. 새 프로젝트의 이름을 지정합니다.
5. **생성**을 클릭합니다.

그러면 새 Google 클라우드 프로젝트가 생성됩니다.

이 프로젝트에 필요한 API를 활성화하려면

1. Google Cloud Platform 콘솔에서 새 프로젝트를 선택합니다.
2. 탐색 메뉴에서 **API 및 서비스** > **활성화된 API 및 서비스**를 선택합니다.
3. 이 프로젝트에서 기본적으로 활성화되어 있는 모든 API를 하나씩 비활성화합니다.
   a. **활성화된 API 및 서비스** 페이지 아래쪽으로 스크롤한 다음 활성화된 API의 이름을 클릭합니다.
      그러면 선택한 API의 **API/서비스 상세정보** 페이지가 열립니다.
   b. **API 비활성화**를 클릭한 다음 **비활성화**를 클릭하여 선택을 확인합니다.
   c. [메시지가 표시되는 경우] **확인**을 클릭하여 선택을 확인합니다.
   d. **API 및 서비스** > **대시보드**로 돌아와서 다음 API를 비활성화합니다.
4. 탐색 메뉴에서 **API 및 서비스** > **라이브러리**를 선택합니다.
5. API 라이브러리에서 다음 API를 하나씩 활성화합니다.
   - Admin SDK API
   - Gmail API
   - Google Calendar API
   - Google Drive API
   - Google People API

   검색 창에서 필요한 API를 찾습니다. API를 활성화하려면 API 이름을 클릭한 다음 **활성화**를 클릭합니다. 다음 API를 검색하려면 탐색 메뉴에서 **API 및 서비스** > **라이브러리**를 선택하여 API 라이브러리로 돌아옵니다.

OAuth 동의 화면을 구성하려면

1. Google Cloud Platform의 탐색 메뉴에서 **API 및 서비스** > **OAuth 동의 화면**을 선택합니다.
2. 창이 열리면 사용자 유형으로 **내부**를 선택하고 **생성**을 클릭합니다.
3. **앱 이름** 필드에 애플리케이션의 이름을 지정합니다.
4. **사용자 지원 이메일** 필드에 슈퍼 관리자 이메일을 입력합니다.
5. **개발자 연락처 정보** 필드에 슈퍼 관리자 이메일을 입력합니다.
6. 다른 필드는 모두 비워 두고 **저장 및 계속**을 클릭합니다.
7. **범위** 페이지에서 아무 항목도 변경하지 않고 **저장 및 계속**을 클릭합니다.
8. **요약** 페이지에서 설정을 확인하고 **대시보드로 돌아가기**를 클릭합니다.

Cyber Protection 서비스용 서비스 계정을 생성 및 구성하려면

© Acronis International GmbH, 2003-2024

1. Google Cloud Platform의 탐색 메뉴에서 **API 및 서비스** > **서비스 계정**을 선택합니다.
2. **서비스 계정 생성**을 클릭합니다.
3. 서비스 계정의 이름을 지정합니다.
4. [선택 사항] 서비스 계정의 설명을 지정합니다.
5. **생성하고 계속하기**를 클릭합니다.
6. **이 서비스 계정에 프로젝트 액세스 권한 부여** 및 **사용자에게 이 서비스 계정 액세스 권한 부여** 단계에서는 아무 항목도 변경하지 않습니다.
7. **완료**를 클릭합니다.
   서비스 계정 페이지가 열립니다.
8. **서비스 계정** 페이지에서 새 서비스 계정을 선택하고 **작업** 아래에서 **키 관리**를 클릭합니다.
9. **키** 아래에서 **키 추가** > **새 키 생성**을 클릭하고 **JSON** 키 유형을 선택합니다.
10. **생성**을 클릭합니다.
    그러면 서비스 계정의 개인 키가 포함된 JSON 파일이 머신에 자동으로 다운로드됩니다. Cyber Protection 서비스에 Google Workspace 조직을 추가하려면 이 키가 필요하므로, 이 파일을 안전하게 저장해 두십시오.

새 프로젝트에 Google Workspace 계정 액세스 권한을 부여하려면

1. Google Cloud Platform의 탐색 메뉴에서 **IAM 및 관리자** > **서비스 계정**을 선택합니다.
2. 생성한 서비스 계정을 목록에서 찾은 후 **OAuth 2.0 클라이언트 ID** 열에 표시되는 클라이언트 ID를 복사합니다.
3. 슈퍼 관리자로 Google Admin 콘솔(admin.google.com)에 로그인합니다.
4. 탐색 메뉴에서 **보안** > **액세스 및 데이터 컨트롤** > **API 컨트롤**을 선택합니다.
5. **API 컨트롤** 페이지 아래쪽으로 스크롤한 다음 **도메인 전체 위임** 아래에서 **도메인 전체 위임 관리**를 클릭합니다.
   그러면 **도메인 전체 위임** 페이지가 열립니다.
6. **도메인 전체 위임** 페이지에서 **새로 추가**를 클릭합니다.
   그러면 **새 클라이언트 ID 추가** 창이 열립니다.
7. **클라이언트 ID** 필드에 서비스 계정 클라이언트의 클라이언트 ID를 입력합니다.
8. 다음의 쉼표로 구분된 범위 목록을 복사하여 **OAuth 범위** 필드에 붙여넣습니다.

```
https://mail.google.com,https://www.googleapis.com/auth/contacts,https://www.googleapis.com/auth/calendar,https://www.googleapis.com/auth/admin.directory.user.readonly,https://www.googleapis.com/auth/admin.directory.domain.readonly,https://www.googleapis.com/auth/drive,https://www.googleapis.com/auth/gmail.modify
```

   범위를 한 줄에 하나씩 추가할 수도 있습니다.

   - https://mail.google.com
   - https://www.googleapis.com/auth/contacts
   - https://www.googleapis.com/auth/calendar
   - https://www.googleapis.com/auth/admin.directory.user.readonly
   - https://www.googleapis.com/auth/admin.directory.domain.readonly

© Acronis International GmbH, 2003-2024

- https://www.googleapis.com/auth/drive
- https://www.googleapis.com/auth/gmail.modify

9. **권한 부여**를 클릭합니다.

그러면 새 Google 클라우드 프로젝트가 Google Workspace 계정의 데이터에 액세스할 수 있게 됩니다. 데이터를 백업하려면 Cyber Protection 서비스에 이 프로젝트를 연결해야 합니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 "개인 전용 Google 클라우드 프로젝트를 사용하여 Google Workspace 조직을 추가하려면"(584페이지)을(를) 참조하십시오.

Google 클라우드 프로젝트의 Google Workspace 계정 액세스 권한 및 개별 Cyber Protection 서비스 액세스 권한을 철회하려면 프로젝트에서 사용하는 API 클라이언트를 삭제합니다.

Google Workspace 계정 액세스 권한을 철회하려면

1. Google Admin 콘솔(admin.google.com)에서 슈퍼 관리자로 로그인합니다.
2. 탐색 메뉴에서 **보안** > **액세스 및 데이터 컨트롤** > **API 컨트롤**을 선택합니다.
3. **API 컨트롤** 페이지 아래쪽으로 스크롤한 다음 **도메인 전체 위임** 아래에서 **도메인 전체 위임 관리**를 클릭합니다.
   그러면 **도메인 전체 위임** 페이지가 열립니다.
4. **도메인 전체 위임** 페이지에서 프로젝트가 사용하는 API 클라이언트를 선택하고 **삭제**를 클릭합니다.
   그러면 Google 클라우드 프로젝트와 Cyber Protection 서비스가 Google Workspace 계정에 액세스하지 못하게 되며, 해당 계정에 데이터를 백업할 수 없습니다.

Google Workspace 리소스 검색

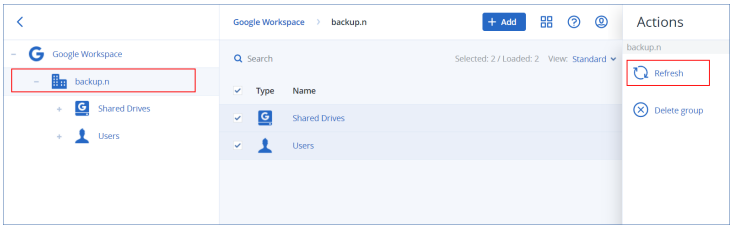
Cyber Protection 서비스에 Google Workspace 조직을 추가하면 사서함, Google Drive 등 해당 조직의 리소스가 Cyber Protect 콘솔에 동기화됩니다. 이 작업(검색)은 **모니터링** > **활동**에 로깅됩니다.

검색 작업이 완료되면 콘솔의 **장치** > **Google Workspace** 탭에서 Google Workspace 조직의 리소스를 확인할 수 있으며 해당 리소스에 백업 계획을 적용할 수 있습니다.

Cyber Protect 콘솔의 리소스 목록을 최신 상태로 유지하기 위해 매일 한 번씩 자동 검색 작업이 실행됩니다. 검색 작업을 수동으로 다시 실행하여 이 목록을 필요에 따라 동기화할 수도 있습니다.

검색 작업을 수동으로 다시 실행하려면

1. Cyber Protect 콘솔에서 **장치** > **Google Workspace**로 이동합니다.
2. Google Workspace 조직을 선택한 다음 **작업** 창에서 **새로 고침**을 클릭합니다.



© Acronis International GmbH, 2003-2024

참고
시간당 10회까지 검색 작업을 수동으로 실행할 수 있습니다. 이 횟수를 초과하면 허용되는 실행 수가 시간당 1회로 재설정되며, 그러면 시간당 작업 실행 횟수가 총 10회가 될 때까지 1시간마다 1회씩 작업을 추가로 실행할 수 있습니다.

Google Workspace 백업의 빈도 설정

기본적으로 Google Workspace 백업은 하루에 한 번 실행되며 추가 예약 옵션은 제공되지 않습니다.

테넌트에서 Advanced Backup 팩이 활성화되어 있으면 백업 빈도를 더 높게 구성할 수 있습니다. 일별 백업 수를 선택할 수는 있지만 백업 시작 시간은 구성할 수 없습니다. 백업은 클라우드 에이전트(데이터 센터 내 여러 고객의 백업을 처리함)의 현재 로드에 따라 달라지는 대략적인 간격으로 자동 시작됩니다. 그러므로 로드가 하루 종일 일정하게 유지되며 모든 고객에게 동일한 서비스 품질이 제공됩니다.

다음 옵션을 사용할 수 있습니다.

예약 옵션	각 백업 간의 대략적인 간격
하루에 한 번	24시간
하루에 두 번(기본값)	12시간
하루에 세 번	8시간
하루에 6번	4시간

참고
클라우드 에이전트의 로드 및 Google Workspace 측에서 실행될 수 있는 조절에 따라 백업이 예약한 일정보다 더 늦게 시작될 수도 있고 백업을 완료하는 데 시간이 더 오래 걸릴 수도 있습니다. 백업 시간이 두 백업 간의 평균 간격보다 더 오래 걸리면 다음 백업이 다시 예약되므로 하루에 실행되는 백업 수가 원래 선택한 수보다 더 적어질 수도 있습니다. 예를 들어 하루에 백업 6회를 완료하도록 선택했더라도 2회밖에 완료하지 못할 수도 있습니다.

Gmail 데이터 보호

어떤 항목을 백업할 수 있습니까?

Gmail 사용자 사서함을 백업할 수 있습니다. 사서함 백업에는 캘린더 및 연락처 데이터가 포함됩니다. 선택적으로 공유된 캘린더 백업을 선택할 수 있습니다.

백업 시 다음 항목은 *생략*됩니다.

- **생일**, **미리 알림**, **작업** 캘린더
- 일정 이벤트에 첨부된 폴더
- 연락처의 **디렉토리** 폴더

© Acronis International GmbH, 2003-2024

Google 캘린더 API 제한으로 인해 다음 캘린더 항목은 *제외됩니다*.

- 일정 슬롯
- 일정의 회의 필드
- **종일 일정 알림** 캘린더 설정
- **초대 자동 승인** 캘린더 설정(회의실 또는 공유 공간용 캘린더)

Google People API 제한으로 인해 다음 연락처 항목은 *제외됩니다*.

- **기타 연락처** 폴더
- 연락처의 외부 프로필(**디렉토리 프로필**, **Google 프로필**)
- **다음 이름으로 저장** 연락처 필드

복구할 수 있는 항목은 무엇입니까?

다음과 같은 항목을 사서함 백업에서 복구할 수 있습니다.

- 사서함
- 이메일 폴더(Google 용어의 "라벨"에 해당. **라벨**은 다른 데이터와의 일관성을 위해 백업 소프트웨어에 폴더로 표시됩니다.)
- 이메일 메시지
- 달력 이벤트
- 연락처

백업에서 항목을 찾기 위해 검색을 사용할 수 있습니다.

사서함과 사서함 항목을 복구할 때 대상 위치의 항목을 복구할 것인지 선택할 수 있습니다.

제한 사항

- 연락처 사진은 복구할 수 없습니다
- Google 캘린더 API 제한으로 인해 **부재중** 캘린더 항목은 일반 캘린더 일정으로 복구됩니다

Gmail 사서함 선택

아래 설명에 따라 사서함을 선택한 다음, 보호 계획의 기타 설정을 적절하게 지정합니다.

Gmail 사서함을 선택하려면

1. **Google Workspace**를 클릭합니다.
2. 여러 Google Workspace 조직을 Cyber Protection 서비스에 추가한 경우 사용자 데이터의 백업을 원하는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. 다음 중 하나를 수행하십시오.
   - 전체 사용자의 사서함(앞으로 생성될 사서함 포함)을 백업하려면 **사용자** 노드를 확장하고 **전체 사용자**를 선택한 후 **그룹 백업**을 클릭합니다.
   - 개별 사용자 사서함을 백업하려면, **사용자** 노드를 확장하고 **전체 사용자**를 선택하고 백업하려는 사서함의 사용자를 선택한 후 **백업**을 클릭합니다.
4. 보호 계획 패널에서:

© Acronis International GmbH, 2003-2024

- **백업 대상**에서 **Gmail** 항목을 선택했는지 확인합니다.
- 선택한 사용자와 공유한 캘린더를 백업하려면 **공유된 캘린더 포함** 스위치를 활성화합니다.
- 백업된 이메일 메시지에 전체 텍스트 검색의 필요 여부를 결정합니다. 이 옵션에 액세스하려면 기어 아이콘 > **백업 옵션** > **전체 텍스트 검색**를 클릭합니다.

사서함 및 사서함 항목 복구

사서함 복구

1. **Google Workspace**를 클릭합니다.
2. 여러 Google Workspace 조직을 Cyber Protection 서비스에 추가한 경우, 백업 데이터의 복구를 원하는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. **사용자** 노드를 확장하고 **전체 사용자**를 선택하고 복구하려는 사서함의 사용자를 선택한 후 **복구**를 클릭합니다.

   사용자가 삭제되었다면 백업 스토리지 탭의 **클라우드 애플리케이션 백업** 섹션에서 해당 사용자를 선택한 후 **백업 표시**를 클릭합니다.

   사용자와 그룹은 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.
4. 복구 지점을 선택합니다.

   참고
   사서함이 포함된 복구 지점만 보려면 **내용별 필터**에서 **Gmail**을 선택합니다.

5. **복구** > **전체 사서함**을 클릭합니다.
6. 여러 Google Workspace 조직을 Cyber Protection 서비스에 추가한 경우 **Google Workspace 조직**을 클릭하여 대상 조직을 보기, 변경 또는 지정합니다.

   기본적으로 원래 조직이 선택됩니다. 이 조직이 Cyber Protection 서비스에 등록되지 않았다면 사용 가능한 등록된 조직들 중에서 새로운 대상 조직을 지정해야 합니다.
7. **사서함으로 복구**에서 대상 사서함을 보고, 변경하거나 지정합니다.

   기본적으로 원래 사서함이 선택됩니다. 이 사서함이 존재하지 않거나 원래 이외 조직을 선택한 경우에는 대상 사서함을 지정해야 합니다.

   복구 중에는 새 대상 사서함을 생성할 수 없습니다. 사서함을 새 사서함으로 복구하려면 먼저 원하는 Google Workspace 조직에 대상 사서함을 생성한 다음 클라우드 에이전트가 변경 사항을 동기화하도록 해야 합니다. 클라우드 에이전트는 24시간 간격으로 Google Workspace에 자동 동기화됩니다. 변경 사항을 즉시 동기화하려면 Cyber Protect 콘솔에서 **Google Workspace** 페이지에 표시된 조직을 선택하고 **새로 고침**을 클릭합니다.
8. **복구 시작**을 클릭합니다.
9. 다음 덮어쓰기 옵션 중 하나를 선택합니다.
   - **기존 항목 덮어쓰기**
   - **기존 항목 덮어쓰기 안 함**
10. **진행**을 클릭하여 결정을 확인합니다.

© Acronis International GmbH, 2003-2024

사서함 항목 복구

1. **Google Workspace**를 클릭합니다.
2. 여러 Google Workspace 조직을 Cyber Protection 서비스에 추가한 경우, 백업 데이터의 복구를 원하는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. **사용자** 노드를 확장하고 **전체 사용자**를 선택하고 복구하려는 항목이 원래 포함된 사서함의 사용자를 선택한 후 **복구**를 클릭합니다.

   사용자가 삭제되었다면 백업 스토리지 탭의 **클라우드 애플리케이션 백업** 섹션에서 해당 사용자를 선택한 후 **백업 표시**를 클릭합니다.

   사용자와 그룹은 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.
4. 복구 지점을 선택합니다.

   참고
   사서함이 포함된 복구 지점만 보려면 **내용별 필터**에서 **Gmail**을 선택합니다.

5. **복구 > 이메일 메시지**를 클릭합니다.
6. 필요한 폴더를 찾습니다. 아직 백업이 암호화되지 않았다면 검색을 사용하여 필요 항목 목록을 얻을 수 있습니다.

   다음 검색 옵션을 사용할 수 있습니다. 와일드카드는 지원되지 않습니다.
   - 이메일 메시지: 제목, 보낸 사람, 받는 사람, 날짜, 첨부 파일 이름, 메시지 내용으로 검색합니다.

     시작 날짜나 종료 날짜 중 하나를 선택(검색이 해당 날짜에 시작되거나 종료됨)할 수도 있고 두 날짜를 모두 선택하여 특정 시간 범위 내에서 검색을 할 수도 있습니다.

     첨부 파일 이름이나 메시지 내용으로 검색을 하면 백업 중 **전문 검색** 옵션을 활성화한 경우에만 결과가 제공됩니다. 검색할 메시지 조각의 언어를 추가 매개변수로 지정할 수 있습니다.
   - 이벤트: 제목 및 날짜로 검색합니다.
   - 연락처: 이름, 이메일 주소, 전화번호로 검색합니다.
7. 복구할 항목을 선택합니다. 폴더를 선택하려면 "폴더 복구" 아이콘 을 클릭하십시오.

   뿐만 아니라 다음을 수행할 수 있습니다.
   - 항목을 선택한 경우 첨부 파일을 포함한 내용을 보려면 **내용 표시**를 클릭하십시오. 첨부 파일을 다운로드하려면 그 이름을 클릭하십시오.
   - 백업이 암호화되지 않고 검색을 사용하고 검색 결과에서 단일 항목만 선택한 경우에만: **버전 표시**를 클릭하여 복구할 항목 버전을 선택합니다. 선택한 복구 지점 이전이나 이후 백업된 버전을 선택할 수 있습니다.
8. **복구**를 클릭합니다.
9. 여러 Google Workspace 조직을 Cyber Protection 서비스에 추가한 경우 **Google Workspace 조직**을 클릭하여 대상 조직을 보기, 변경 또는 지정합니다.

   기본적으로 원래 조직이 선택됩니다. 이 조직이 Cyber Protection 서비스에 등록되지 않았다면 사용 가능한 등록된 조직들 중에서 새로운 대상 조직을 지정해야 합니다.
10. **사서함으로 복구**에서 대상 사서함을 보고, 변경하거나 지정합니다.

© Acronis International GmbH, 2003-2024

기본적으로 원래 사서함이 선택됩니다. 이 사서함이 존재하지 않거나 원래 이외 조직을 선택한 경우에는 대상 사서함을 지정해야 합니다.

11. **경로**에서 대상 사서함에 포함된 대상 폴더를 보거나 변경합니다. 기본적으로 원래 폴더가 선택됩니다.
12. **복구 시작**을 클릭합니다.
13. 다음 덮어쓰기 옵션 중 하나를 선택합니다.
    - **기존 항목 덮어쓰기**
    - **기존 항목 덮어쓰기 안 함**
14. **진행**을 클릭하여 결정을 확인합니다.

Google Drive 파일 보호

어떤 항목을 백업할 수 있습니까?

Google Drive 전체 또는 개별 파일 및 폴더를 백업할 수 있습니다. 파일은 공유 권한과 함께 백업됩니다.

중요
다음 항목은 백업되지 않습니다.

- **공유한 항목** 폴더
- **컴퓨터** 폴더(백업 및 동기화 클라이언트로부터 생성)

제한 사항

Google 전용 파일 형식 중 Google Docs, Google Sheets, Google Slides는 백업 및 복구가 완전히 지원됩니다. 기타 Google 전용 파일 형식은 일부 또는 전혀 지원되지 않을 수 있습니다. 예를 들어 Google Drawings 파일은 `.svg` 파일, Google Sites 파일은 `.txt` 파일, Google Jamboard 파일은 `.pdf` 파일로 복구되며, Google My Maps 파일은 백업 시 건너뜁니다.

참고
Google 전용이 아닌 파일 형식(예: `.txt`, `.docx`, `.pptx`, `.pdf`, `.jpg`, `.png`, `.zip`)은 백업 및 복구가 완전히 지원됩니다.

복구할 수 있는 항목은 무엇입니까?

전체 Google Drive 또는 백업되었던 파일이나 폴더를 복구할 수 있습니다.

그 공유 권한을 복구할지 아니면 파일이 복구될 대상 폴더로부터 권한을 상속하게 할지 선택할 수 있습니다.

제한 사항

- 파일의 댓글은 복구되지 않습니다.
- 파일 및 폴더에 대한 공유 링크는 복구되지 않습니다.

© Acronis International GmbH, 2003-2024

- 공유된 파일에 대한 읽기 전용 **공유자 설정(편집자의 권한 변경 및 신규 사용자 추가 방지** 및 **댓글 또는 보기 권한이 있는 사용자의 다운로드, 인쇄 및 복사 기능 제한**)은 복구 중에 변경될 수 없습니다.
- 공유된 폴더에 대해 **편집자의 권한 변경 및 신규 사용자 추가 방지** 옵션이 활성화되었을 경우 해당 폴더의 소유권을 복구 중에 변경할 수 없습니다. 이 설정으로 Google Drive API가 폴더 권한을 나열하는 것을 방지합니다. 폴더 내 파일의 소유권은 올바르게 복구됩니다.

Google Drive 파일 선택

아래 설명에 따라 파일을 선택한 다음, 보호 계획의 기타 설정을 적절하게 지정합니다.

Google Drive 파일을 선택하려면

1. **Google Workspace**를 클릭합니다.
2. 여러 Google Workspace 조직을 Cyber Protection 서비스에 추가한 경우 사용자 데이터의 백업을 원하는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. 다음 중 하나를 수행하십시오.
   - 전체 사용자의 파일(앞으로 생성될 사용자 포함)을 백업하려면, **사용자** 노드를 확장하고 **전체 사용자**를 선택한 후 **그룹 백업**을 클릭합니다.
   - 개별 사용자의 파일을 백업하려면, **사용자** 노드를 확장하고 **전체 사용자**를 선택하고 백업하려는 파일의 사용자를 선택한 후 **백업**을 클릭합니다.
4. 보호 계획 패널에서:
   - **백업 대상**에서 **Google Drive** 항목을 선택했는지 확인합니다.
   - **백업할 항목**에서 다음 중 하나를 수행하십시오.
     - 기본 설정 **[전체]**(전체 파일)을 유지합니다.
     - 이름이나 경로를 추가하여 백업할 파일과 폴더를 지정합니다.
       와일드카드 문자(*, ** 및 ?)를 사용할 수 있습니다. 경로 지정과 와일드카드 사용에 관한 자세한 내용은 "파일 필터"를 참조하십시오.
     - 찾아보기를 통해 백업할 파일과 폴더를 선택합니다.
       찾아보기 링크는 단일 사용자를 위한 보호 계획을 생성할 때만 사용할 수 있습니다.
   - [선택 사항] **백업할 항목**에서 **예외 표시**를 클릭하여 백업에서 생략할 파일과 폴더를 지정합니다.
     파일 제외는 파일 선택에 우선합니다. 즉, 두 필드에 동일 파일을 지정하면 백업 중 이 파일은 건너뜁니다.
   - 백업용으로 선택된 모든 파일의 공증을 활성화하려면 **공증** 스위치를 활성화합니다. 공증에 대한 자세한 내용은 "공증"을 참조하십시오.

Google Drive 및 Google Drive 파일 복구

전체 Google Drive 복구

1. **Google Workspace**를 클릭합니다.
2. 여러 Google Workspace 조직을 Cyber Protection 서비스에 추가한 경우, 백업 데이터의 복구를 원하는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.

© Acronis International GmbH, 2003-2024

3. **사용자** 노드를 확장하고 **전체 사용자**를 선택하고 복구하려는 Google Drive의 사용자를 선택한 후 **복구**를 클릭합니다.
   사용자가 삭제되었다면 백업 스토리지 탭의 **클라우드 애플리케이션 백업** 섹션에서 해당 사용자를 선택한 후 **백업 표시**를 클릭합니다.
   사용자를 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.
4. 복구 지점을 선택합니다.

   참고
   Google Drive 파일이 포함된 복구 지점만 보려면 **내용별 필터링**에서 **Google Drive**를 선택합니다.

5. **복구** > **전체 드라이브**를 클릭합니다.
6. 여러 Google Workspace 조직을 Cyber Protection 서비스에 추가한 경우 **Google Workspace 조직**을 클릭하여 대상 조직을 보기, 변경 또는 지정합니다.
   기본적으로 원래 조직이 선택됩니다. 이 조직이 Cyber Protection 서비스에 등록되지 않았다면 사용 가능한 등록된 조직들 중에서 새로운 대상 조직을 지정해야 합니다.
7. **드라이브로 복구**에서 대상 사용자 또는 Shared Drive를 보고, 변경하거나 지정합니다.
   기본적으로 원래 사용자가 선택됩니다. 이 사용자가 존재하지 않거나 원래 이외 조직을 선택한 경우 대상 사용자 또는 대상 Shared Drive를 지정해야 합니다.
   백업이 공유된 파일을 포함한다면 그 파일은 대상 드라이브의 루트 폴더로 복구됩니다.
8. 파일에 대해 공유 권한을 복구할 것인지 선택합니다.
9. **복구 시작**을 클릭합니다.
10. 다음 덮어쓰기 옵션 중 하나를 선택합니다.

옵션	설명
오래된 경우 기존 파일 덮어쓰기	대상 위치에 이름이 같으며 소스 파일보다 오래된 파일이 있으면 대상 위치에 소스 파일을 저장하여 이전 버전을 대체합니다.
기존 파일 덮어쓰기	마지막으로 수정한 날짜에 관계없이 대상 위치의 기존 파일을 모두 덮어씁니다.
기존 파일 덮어쓰기 안 함	대상 위치에 이름이 같은 파일이 있으면 해당 파일을 변경하지 않으며 대상 위치에 소스 파일이 저장되지 않습니다.

11. **진행**을 클릭하여 결정을 확인합니다.

Google Drive 파일 복구

1. **Google Workspace**를 클릭합니다.
2. 여러 Google Workspace 조직을 Cyber Protection 서비스에 추가한 경우, 백업 데이터의 복구를 원하는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. **사용자** 노드를 확장하고 **전체 사용자**를 선택하고 복구하려는 Google Drive 파일의 사용자를 선택한 후 **복구**를 클릭합니다.

© Acronis International GmbH, 2003-2024

사용자가 삭제되었다면 백업 스토리지 탭의 **클라우드 애플리케이션 백업** 섹션에서 해당 사용자를 선택한 후 **백업 표시**를 클릭합니다.

사용자를 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.

4. 복구 지점을 선택합니다.

참고

Google Drive 파일이 포함된 복구 지점만 보려면 **내용별 필터링**에서 **Google Drive**를 선택합니다.

5. **복구** > **파일/폴더**를 클릭합니다.
6. 필요한 폴더를 찾거나 검색 기능을 사용하여 필요한 파일 및 폴더 목록을 얻습니다.
7. 복구할 파일을 선택합니다.

   백업이 암호화되지 않고 단일 파일을 선택한 경우 **버전 표시**를 클릭하여 복구할 파일 버전을 선택합니다. 선택한 복구 지점 이전이나 이후 백업된 버전을 선택할 수 있습니다.
8. 파일을 다운로드하려면 **다운로드**를 클릭하고 파일을 저장할 위치를 선택한 다음 **저장**을 클릭합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
9. **복구**를 클릭합니다.
10. 여러 Google Workspace 조직을 Cyber Protection 서비스에 추가한 경우 **Google Workspace 조직**을 클릭하여 대상 조직을 보기, 변경 또는 지정합니다.

    기본적으로 원래 조직이 선택됩니다. 이 조직이 Cyber Protection 서비스에 등록되지 않았다면 사용 가능한 등록된 조직들 중에서 새로운 대상 조직을 지정해야 합니다.
11. **드라이브로 복구**에서 대상 사용자 또는 Shared Drive를 보고, 변경하거나 지정합니다.

    기본적으로 원래 사용자가 선택됩니다. 이 사용자가 존재하지 않거나 원래 이외 조직을 선택한 경우 대상 사용자 또는 대상 Shared Drive를 지정해야 합니다.
12. **경로**에서 대상 사용자의 Google Drive 또는 대상 Shared Drive에 포함된 대상 폴더를 보거나 변경합니다. 기본적으로 원래 위치가 선택됩니다.
13. 파일에 대해 공유 권한을 복구할 것인지 선택합니다.
14. **복구 시작**을 클릭합니다.
15. 다음 파일 덮어쓰기 옵션 중 하나를 선택합니다.

옵션	설명
오래된 경우 기존 파일 덮어쓰기	대상 위치에 이름이 같으며 소스 파일보다 오래된 파일이 있으면 대상 위치에 소스 파일을 저장하여 이전 버전을 대체합니다.
기존 파일 덮어쓰기	마지막으로 수정한 날짜에 관계없이 대상 위치의 기존 파일을 모두 덮어씁니다.
기존 파일 덮어쓰기 안 함	대상 위치에 이름이 같은 파일이 있으면 해당 파일을 변경하지 않으며 대상 위치에 소스 파일이 저장되지 않습니다.

16. **진행**을 클릭하여 결정을 확인합니다.

© Acronis International GmbH, 2003-2024

Shared Drive 파일 보호

어떤 항목을 백업할 수 있습니까?

Shared Drive 전체 또는 개별 파일 및 폴더를 백업할 수 있습니다. 파일은 공유 권한과 함께 백업됩니다.

중요
공유한 항목 폴더는 백업되지 않습니다.

제한 사항

- Google Drive API 제한으로 인해 구성원이 없는 Shared Drive는 백업할 수 없습니다.
- Google 전용 파일 형식 중 Google Docs, Google Sheets, Google Slides는 백업 및 복구가 완전히 지원됩니다. 기타 Google 전용 파일 형식은 일부 또는 전혀 지원되지 않을 수 있습니다. 예를 들어 Google Drawings 파일은 `.svg` 파일, Google Sites 파일은 `.txt` 파일, Google Jamboard 파일은 `.pdf` 파일로 복구되며, Google My Maps 파일은 백업 시 건너뜁니다.

  참고
  Google 전용이 아닌 파일 형식(예: `.txt`, `.docx`, `.pptx`, `.pdf`, `.jpg`, `.png`, `.zip`)은 백업 및 복구가 완전히 지원됩니다.

복구할 수 있는 항목은 무엇입니까?

전체 Shared Drive 또는 백업되었던 파일이나 폴더를 복구할 수 있습니다.

그 공유 권한을 복구할지 아니면 파일이 복구될 대상 폴더로부터 권한을 상속하게 할지 선택할 수 있습니다.

다음 항목은 복구되지 않습니다.

- 대상 Shared Drive 내 조직 외 공유 기능이 비활성화된 경우 조직 외의 사용자와 공유한 파일의 공유 권한은 복구되지 않습니다.
- 대상 Shared Drive의 **비구성원과 공유** 기능이 비활성화된 경우 대상 Shared Drive의 구성원이 아닌 사용자와 공유된 파일에 대한 공유 권한은 복구되지 않습니다.

제한 사항

- 파일의 댓글은 복구되지 않습니다.
- 파일 및 폴더에 대한 공유 링크는 복구되지 않습니다.

Shared Drive 파일 선택

아래 설명에 따라 파일을 선택한 다음, 보호 계획의 기타 설정을 적절하게 지정합니다.

Shared Drive 파일을 선택하려면

© Acronis International GmbH, 2003-2024

1. **Google Workspace**를 클릭합니다.
2. 여러 Google Workspace 조직을 Cyber Protection 서비스에 추가한 경우 사용자 데이터의 백업을 원하는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. 다음 중 하나를 수행하십시오.
   - 전체 Shared Drive의 파일(앞으로 생성될 Shared Drive 포함)을 백업하려면 **Shared Drive** 노드를 확장하고 **전체 Shared Drive**를 선택한 후 **그룹 백업**을 클릭합니다.
   - 개별 Shared Drive의 파일을 백업하려면 **Shared Drive** 노드를 확장하고 **전체 Shared Drive**를 선택하고 백업하려는 Shared Drive를 선택한 후 **백업**을 클릭합니다.
4. 보호 계획 패널에서:
   - **백업할 항목**에서 다음 중 하나를 수행하십시오.
     - 기본 설정 **[전체]**(전체 파일)을 유지합니다.
     - 이름이나 경로를 추가하여 백업할 파일과 폴더를 지정합니다.

       와일드카드 문자(*, ** 및 ?)를 사용할 수 있습니다. 경로 지정과 와일드카드 사용에 관한 자세한 내용은 "파일 필터"를 참조하십시오.
     - 찾아보기를 통해 백업할 파일과 폴더를 선택합니다.

       찾아보기 링크는 단일 Shared Drive를 위한 보호 계획을 생성할 때만 사용할 수 있습니다.
   - [선택 사항] **백업할 항목**에서 **예외 표시**를 클릭하여 백업에서 생략할 파일과 폴더를 지정합니다.

     파일 제외는 파일 선택에 우선합니다. 즉, 두 필드에 동일 파일을 지정하면 백업 중 이 파일은 건너뜁니다.
   - 백업용으로 선택된 모든 파일의 공증을 활성화하려면 **공증** 스위치를 활성화합니다. 공증에 대한 자세한 내용은 "공증"을 참조하십시오.

Shared Drive 및 Shared Drive 파일 복구

전체 Shared Drive 복구

1. **Google Workspace**를 클릭합니다.
2. 여러 Google Workspace 조직을 Cyber Protection 서비스에 추가한 경우, 백업 데이터의 복구를 원하는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. **Shared Drive** 노드를 확장하고 **전체 Shared Drive**를 선택하고 복구하려는 Shared Drive를 선택한 후 **복구**를 클릭합니다.

   Shared Drive가 삭제되었다면 백업 스토리지 탭의 **클라우드 애플리케이션 백업** 섹션에서 선택한 후 **백업 표시**를 클릭합니다.

   Shared Drive를 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.
4. 복구 지점을 선택합니다.
5. **복구** > **전체 드라이브**를 클릭합니다.
6. 여러 Google Workspace 조직을 Cyber Protection 서비스에 추가한 경우 **Google Workspace 조직**을 클릭하여 대상 조직을 보기, 변경 또는 지정합니다.

   기본적으로 원래 조직이 선택됩니다. 이 조직이 Cyber Protection 서비스에 등록되지 않았다면 사용 가능한 등록된 조직들 중에서 새로운 대상 조직을 지정해야 합니다.

© Acronis International GmbH, 2003-2024

7. **드라이브로 복구**에서 대상 Shared Drive 또는 대상 사용자를 보고, 변경하거나 지정합니다. 사용자를 지정하면 데이터가 그 사용자의 Google Drive로 복구됩니다.
   기본적으로 원래 Shared Drive가 선택됩니다. 이 Shared Drive가 존재하지 않거나 원래 이외 조직을 선택한 경우 대상 Shared Drive 또는 대상 사용자를 지정해야 합니다.
8. 파일에 대해 공유 권한을 복구할 것인지 선택합니다.
9. **복구 시작**을 클릭합니다.
10. 다음 덮어쓰기 옵션 중 하나를 선택합니다.

옵션	설명
오래된 경우 기존 파일 덮어쓰기	대상 위치에 이름이 같으며 소스 파일보다 오래된 파일이 있으면 대상 위치에 소스 파일을 저장하여 이전 버전을 대체합니다.
기존 파일 덮어쓰기	마지막으로 수정한 날짜에 관계없이 대상 위치의 기존 파일을 모두 덮어씁니다.
기존 파일 덮어쓰기 안 함	대상 위치에 이름이 같은 파일이 있으면 해당 파일을 변경하지 않으며 대상 위치에 소스 파일이 저장되지 않습니다.

11. **진행**을 클릭하여 결정을 확인합니다.

Shared Drive 파일 복구

1. **Google Workspace**를 클릭합니다.
2. 여러 Google Workspace 조직을 Cyber Protection 서비스에 추가한 경우, 백업 데이터의 복구를 원하는 조직을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. **Shared Drive** 노드를 확장하고 **전체 Shared Drive**를 선택한 다음 복구하려는 파일이 있던 Shared Drive를 선택한 후 **복구**를 클릭합니다.
   Shared Drive가 삭제되었다면 백업 스토리지 탭의 **클라우드 애플리케이션 백업** 섹션에서 선택한 후 **백업 표시**를 클릭합니다.
   Shared Drive를 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.
4. 복구 지점을 선택합니다.
5. **복구** > **파일/폴더**를 클릭합니다.
6. 필요한 폴더를 찾거나 검색 기능을 사용하여 필요한 파일 및 폴더 목록을 얻습니다.
7. 복구할 파일을 선택합니다.
   백업이 암호화되지 않고 단일 파일을 선택한 경우 **버전 표시**를 클릭하여 복구할 파일 버전을 선택합니다. 선택한 복구 지점 이전이나 이후 백업된 버전을 선택할 수 있습니다.
8. 파일을 다운로드하려면 **다운로드**를 클릭하고 파일을 저장할 위치를 선택한 다음 **저장**을 클릭합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
9. **복구**를 클릭합니다.
10. 여러 Google Workspace 조직을 Cyber Protection 서비스에 추가한 경우 **Google Workspace 조직**을 클릭하여 대상 조직을 보기, 변경 또는 지정합니다.
    기본적으로 원래 조직이 선택됩니다. 이 조직이 Cyber Protection 서비스에 등록되지 않았다면 사용 가능한 등록된 조직들 중에서 새로운 대상 조직을 지정해야 합니다.

© Acronis International GmbH, 2003-2024

11. **드라이브로 복구**에서 대상 Shared Drive 또는 대상 사용자를 보고, 변경하거나 지정합니다. 사용자를 지정하면 데이터가 그 사용자의 Google Drive로 복구됩니다.
    기본적으로 원래 Shared Drive가 선택됩니다. 이 Shared Drive가 존재하지 않거나 원래 이외 조직을 선택한 경우 대상 Shared Drive 또는 대상 사용자를 지정해야 합니다.
12. **경로**에서 대상 Shared Drive 또는 대상 사용자의 Google Drive에 포함된 대상 폴더를 보거나 변경합니다. 기본적으로 원래 위치가 선택됩니다.
13. 파일에 대해 공유 권한을 복구할 것인지 선택합니다.
14. **복구 시작**을 클릭합니다.
15. 다음 파일 덮어쓰기 옵션 중 하나를 선택합니다.

옵션	설명
오래된 경우 기존 파일 덮어쓰기	대상 위치에 이름이 같으며 소스 파일보다 오래된 파일이 있으면 대상 위치에 소스 파일을 저장하여 이전 버전을 대체합니다.
기존 파일 덮어쓰기	마지막으로 수정한 날짜에 관계없이 대상 위치의 기존 파일을 모두 덮어씁니다.
기존 파일 덮어쓰기 안 함	대상 위치에 이름이 같은 파일이 있으면 해당 파일을 변경하지 않으며 대상 위치에 소스 파일이 저장되지 않습니다.

16. **진행**을 클릭하여 결정을 확인합니다.

공증

공증을 사용하면 파일이 신뢰할 수 있고 백업된 후 변경되지 않았음을 증명할 수 있습니다. 법적 문서 파일이나 입증된 신뢰성이 필요한 기타 파일을 보호할 때에는 공증을 활성화하는 것이 좋습니다.

공증은 Google Drive 파일 및 Google Workspace Shared Drive 파일 백업 용도로만 사용할 수 있습니다.

공증 사용 방법

백업용으로 선택된 모든 파일의 공증을 활성화하려면 보호 계획을 생성할 때 **공증** 스위치를 활성화합니다.

복구를 구성할 때 공증된 파일에 특별한 아이콘이 표시되고, 이를 통해 파일 신뢰성을 확인할 수 있습니다.

작동법

백업 중에 에이전트가 백업된 파일의 해시 코드를 계산하고, 해시 트리(폴더 구조 기반)를 생성하고, 트리를 백업에 저장한 다음 해시 트리 루트를 공증 서비스로 전송합니다. 공증 서비스는 Ethereum 블록체인 데이터베이스에 해시 트리 루트를 저장하여 이 값이 변경되지 않도록 합니다.

파일 신뢰성을 확인할 때 에이전트가 파일의 해시를 계산한 다음 이를 백업 내부의 해시 트리에 저장되어 있는 해시와 비교합니다. 두 해시가 일치하지 않으면 파일이 신뢰할 수 없는 것으로 간주됩니다. 그렇지 않으면 해시 트리에 의해 파일 신뢰성이 보증됩니다.

© Acronis International GmbH, 2003-2024

해시 트리 자체가 손상되지 않았는지 확인하기 위해 에이전트는 해시 트리 루트를 공증 서비스로 전송합니다. 공증 서비스는 이를 블록체인 데이터베이스에 저장되어 있는 해시 트리 루트와 비교합니다. 해시가 일치하면 선택한 파일은 신뢰할 수 있는 것으로 보증됩니다. 그렇지 않으면 소프트웨어에 파일을 신뢰할 수 없다는 메시지가 표시됩니다.

Notary Service를 통해 파일 신뢰성 확인

백업 중에 공증이 활성화된 경우 백업된 파일의 신뢰성을 확인할 수 있습니다.

파일 신뢰성을 확인하려면

1. 다음 중 하나를 수행하십시오.
   - Google Drive 파일의 신뢰성을 검증하려면 "Google Drive 파일 복구" 섹션의 1~7단계에 설명된 대로 파일을 선택합니다.
   - Google Workspace Shared Drive 파일의 신뢰성을 검증하려면 "Shared Drive 파일 복구" 섹션의 1~7단계에 설명된 대로 파일을 선택합니다.
2. 선택한 파일에 다음 아이콘이 표시되는지 확인합니다. 이는 파일이 공증되었음을 의미합니다.
3. 다음 중 하나를 수행하십시오.
   - **확인**을 클릭합니다.
     소프트웨어에서 파일 신뢰성을 확인하고 결과를 표시합니다.
   - **인증서 가져오기**를 클릭합니다.
     파일 공증을 확인하는 인증서가 웹 브라우저 창에서 열립니다. 이 창에는 파일 신뢰성을 수동으로 확인하는 방법도 포함되어 있습니다.

클라우드 간 백업에서 검색

데이터를 복구할 때, 백업 아카이브를 탐색하는 대신 특정 백업 항목을 검색할 수 있습니다.

암호화되지 않은 백업에서는 항상 검색이 가능합니다. 향상된(인덱스 기반) 검색만 지원됩니다.

인덱스 기반 검색은 더 빠르며 백업된 항목의 버전 표시, 첨부 파일 이름에서 검색 및 Gmail 백업에서의 전체 텍스트 검색과 같은 추가 옵션을 제공합니다.

암호화된 백업에서는 향상된(인덱스 기반) 검색도 활성화할 수 있습니다. 향상된 검색을 활성화하지 않은 경우 Microsoft 365 사서함의 백업에 대해 기본 검색이 가능합니다. 그 외의 모든 워크로드에 대해서는 검색을 사용할 수 없습니다.

아래 표는 암호화된 백업에 대한 사용 가능한 옵션을 요약한 것입니다.

워크로드 유형	복구 대상	향상된 검색이 비활성화되어 있습니다.	향상된 검색이 활성화되어 있습니다.
Microsoft 365 워크로드			
사서함	이메일 메시지	기본(인덱스 기반이 아닌) 검색을 사용할 수 있습니다.	향상된(인덱스 기반) 검색을 사용할 수 있습니다.

© Acronis International GmbH, 2003-2024

워크로드 유형	복구 대상	향상된 검색이 비활성화되어 있습니다.	향상된 검색이 활성화되어 있습니다.
OneDrive	파일/폴더	검색을 사용할 수 없습니다.	향상된(인덱스 기반) 검색을 사용할 수 있습니다.
SharePoint 사이트	SharePoint 파일	검색을 사용할 수 없습니다.	향상된(인덱스 기반) 검색을 사용할 수 있습니다.
Teams	채널	검색을 사용할 수 없습니다.	향상된(인덱스 기반) 검색을 사용할 수 있습니다.
	이메일 메시지	기본(인덱스 기반이 아닌) 검색을 사용할 수 있습니다.	향상된(인덱스 기반) 검색을 사용할 수 있습니다.
	팀 사이트	검색을 사용할 수 없습니다.	향상된(인덱스 기반) 검색을 사용할 수 있습니다.
Google Workspace 워크로드			
사서함	이메일 메시지	검색을 사용할 수 없습니다.	향상된(인덱스 기반) 검색을 사용할 수 있습니다.
Google Drive	파일/폴더	검색을 사용할 수 없습니다.	향상된(인덱스 기반) 검색을 사용할 수 있습니다.
Shared Drive	파일/폴더	검색을 사용할 수 없습니다.	향상된(인덱스 기반) 검색을 사용할 수 있습니다.

전체 텍스트 검색

전체 텍스트 검색은 Gmail 백업에만 사용할 수 있으며, 기본적으로 활성화되어 있습니다. 이를 통해 백업된 이메일의 본문 텍스트에서 검색할 수 있습니다. 이 옵션이 비활성화되어 있는 경우 주제, 발신자, 수신자 및 날짜로만 검색할 수 있습니다.

전체 텍스트 검색 인덱스는 Gmail 백업이 차지하는 스토리지 공간의 10%에서 30%를 차지합니다. 전체 텍스트 검색 데이터가 없는 색인은 훨씬 작습니다. 스토리지 공간을 절약하려면 전체 텍스트 검색을 비활성화하고 전체 텍스트 검색 데이터를 포함하는 인덱스의 부분을 지우면 됩니다.

검색 인덱스

검색 인덱스는 클라우드 간 백업 아카이브에서 향상된 검색 기능을 제공합니다.

아카이브는 각 백업 작업 후 자동으로 인덱싱됩니다. 인덱싱과 백업은 다른 소프트웨어 구성 요소에 의해 수행되므로 인덱싱 과정은 백업 성능에 영향을 주지 않습니다.

인덱싱 작업이 완료된 후에 검색 결과를 표시할 수 있게 되며, 이 작업은 최대 24시간이 소요될 수 있습니다. 전체인 처음 백업을 인덱싱하는 것은 보통 연속 증분 백업을 인덱싱하는 것보다 더 오래 걸립니다.

© Acronis International GmbH, 2003-2024

모든 인덱스는 주제, 발신자, 수신자 또는 날짜별 검색과 같은 주요 검색 기능을 지원하는 메타데이터를 포함하고 있습니다. Gmail 백업을 위한 인덱스는 전체 텍스트 검색이 활성화된 경우 추가 데이터를 포함하고 있습니다.

검색 인덱스의 크기 확인

검색 인덱스는 시간이 지남에 따라 커집니다. 전체 텍스트 검색이 활성화된 백업 아카이브의 인덱스는 아카이브 크기의 최대 30%를 차지할 수 있습니다.

검색 인덱스의 크기를 확인하는 방법

1. Cyber Protect 콘솔에 관리자로 로그인합니다.
2. **백업 스토리지** 탭에서 **클라우드 애플리케이션 백업**을 클릭합니다.
3. **인덱스 크기** 열에서 값을 확인합니다.

인덱스 업데이트, 다시 구축 또는 삭제

클라우드 간 백업에서 검색 관련 문제를 해결하려면 검색 인덱스를 업데이트하거나 다시 구축하거나 삭제할 수 있습니다.

참고
인덱스를 업데이트, 다시 구축 또는 삭제하기 전에 지원 팀에 연락하는 것을 권장합니다.

인덱스를 업데이트, 다시 구축 또는 삭제하는 방법

1. Cyber Protect 콘솔에 관리자로 로그인합니다.
2. **백업 스토리지** 탭에서 **클라우드 애플리케이션 백업**을 클릭합니다.
   업데이트, 다시 구축 또는 삭제하려는 인덱스의 아카이브를 선택합니다.
   이러한 작업의 가용성은 다음과 같은 관리자 수준 및 역할에 따라 달라집니다.

계정 레벨	역할	색인 업데이트 가능	색인 다시 빌드 가능	색인 삭제 가능
파트너 테넌트	회사 관리자	+	+	+
	보호 사이버 관리자	+	-	-
	보호 관리자	+	-	-
	보호 읽기 전용 관리자	-	-	-
고객 테넌트	회사 관리자	+	-	-
	보호 관리자	+	-	-
	보호 읽기 전용 관리자	-	-	-

© Acronis International GmbH, 2003-2024

계정 레벨	역할	색인 업데이트 가능	색인 다시 빌드 가능	색인 삭제 가능
단위	부서 관리자	+	-	-
	보호 관리자	+	-	-
	보호 읽기 전용 관리자	-	-	-

3. **작업** 창에서 수행하려는 작업을 선택합니다.
   - **인덱스 업데이트** - 아카이브에서 복구 지점을 확인하고 누락된 인덱스를 추가합니다.
   - **인덱스 다시 구축**—아카이브의 모든 복구 지점에 대한 인덱스가 삭제된 다음 인덱스가 다시 생성됩니다.
   - **인덱스 삭제**—아카이브의 모든 복구 지점에 대한 인덱스가 삭제됩니다.
4. [암호화된 아카이브의 경우] 암호화 암호를 지정한 다음 **확인**을 클릭합니다.
5. 작업의 범위를 선택한 다음 **확인**을 클릭합니다.
   아카이브와 선택된 작업에 따라 다음 중 하나 이상의 옵션을 사용할 수 있습니다.
   - **메타데이터만**
   - **내용만**
   - **메타데이터 및 내용 검색**

암호화된 백업에서 향상된 검색 활성화

암호화된 클라우드 간 백업을 위한 백업 계획을 생성하는 경우 향상된(인덱스 기반) 검색을 활성화할 수 있습니다.

향상된 검색을 활성화하지 않은 경우 Microsoft 365 사서함의 백업에 대해 기본 검색을 사용할 수 있습니다. 그 외의 모든 워크로드에 대해서는 검색을 사용할 수 없습니다. 사용할 수 있는 옵션에 대한 자세한 정보는 "클라우드 간 백업에서 검색"(601페이지)을(를) 참조하십시오.

참고
이 기능은 선택된 데이터 센터에서만 사용할 수 있으며, 모든 고객이 액세스할 수 있는 것은 아닙니다.

암호화된 백업에서 검색을 활성화하는 방법

1. 백업 계획을 생성하는 경우 **암호화** 스위치를 활성화합니다.
2. 암호화 비밀번호를 지정한 후 확인합니다.
3. **암호화된 백업에서 향상된 검색 허용** 확인란을 선택합니다.
4. **완료**를 클릭합니다.

참고
나중에 암호화를 비활성화하거나 암호화 암호를 변경할 수 없습니다. 암호화되지 않은 백업을 만들거나 암호화 암호를 변경하려면 새 백업 계획을 생성합니다.

© Acronis International GmbH, 2003-2024

기존 계획에서 향상된 검색을 활성화하거나 비활성화하기

암호화된 백업을 위한 기존 계획을 편집하여 향상된(인덱스 기반) 검색을 활성화하거나 비활성화할 수 있습니다.

향상된 검색을 활성화하지 않은 경우 Microsoft 365 사서함의 백업에 대해 기본 검색을 사용할 수 있습니다. 그 외의 모든 워크로드에 대해서는 검색을 사용할 수 없습니다. 사용할 수 있는 옵션에 대한 자세한 정보는 "클라우드 간 백업에서 검색"(601페이지)을(를) 참조하십시오.

암호화되지 않은 백업에서는 항상 향상된 검색이 가능합니다. 이 옵션은 비활성화할 수 없습니다.

암호화된 백업에서 향상된 검색을 활성화하거나 비활성화하는 방법

1. 암호화가 활성화된 백업 계획을 편집하는 경우 오른쪽 상단의 기어 아이콘을 클릭합니다.
2. **검색 옵션** 탭에서 필요에 따라 스위치를 토글합니다.
3. **완료**를 클릭합니다.
4. **설정 저장**을 클릭합니다.

참고
향상된 검색을 다시 활성화하는 경우 이 백업 계획으로 생성된 모든 아카이브가 다시 인덱싱되며, 이는 시간이 많이 소요됩니다.

Gmail 백업에 대한 전체 텍스트 검색 비활성화

전체 텍스트 검색은 Gmail 백업에만 사용할 수 있으며, 기본적으로 활성화되어 있습니다. 이를 통해 백업된 이메일의 본문 텍스트에서 검색할 수 있습니다. 이 옵션이 비활성화되어 있는 경우 주제, 발신자, 수신자 및 날짜로만 검색할 수 있습니다.

검색 인덱스의 크기를 최소한으로 유지해야 하는 경우 전체 텍스트 검색을 비활성화하길 원할 수 있습니다.

전체 텍스트 검색을 비활성화하는 방법

1. 백업 계획을 생성하거나 편집하는 경우 오른쪽 상단의 기어 아이콘을 클릭합니다.
2. **전체 텍스트 검색** 탭에서 스위치를 비활성화합니다.
3. **완료**를 클릭합니다.
4. [계획을 생성하는 경우] **적용**을 클릭합니다.
5. [계획을 편집하는 경우] **설정 저장**을 클릭합니다.

참고
전체 텍스트 검색을 다시 활성화하는 경우 이 백업 계획으로 생성된 모든 아카이브가 다시 인덱싱되며, 이는 시간이 많이 소요됩니다.

© Acronis International GmbH, 2003-2024

Oracle 데이터베이스 보호

참고
이 기능은 Advanced Backup 팩에서 사용할 수 있습니다.

Oracle 데이터베이스 보호는 별도의 문서(https://dl.managed-protection.com/u/pdf/OracleBackup_whitepaper_en-US.pdf)에 설명되어 있습니다.

SAP HANA 보호

참고
이 기능은 Advanced Backup 팩에서 사용할 수 있습니다.

SAP HANA의 보호는 별도 문서(https://dl.managed-protection.com/u/pdf/SAP_HANA_backup_whitepaper_en-US.pdf)에 설명되어 있습니다

MySQL 및 MariaDB 데이터 보호

애플리케이션 인식 백업을 통해 MySQL 또는 MariaDB 데이터를 보호할 수 있습니다. 이를 통해 애플리케이션 메타데이터를 수집하고 인스턴스, 데이터베이스 또는 테이블 수준에서 개별 복구가 가능합니다.

참고
MySQL 또는 MariaDB 데이터의 애플리케이션 인식 백업은 Advanced Backup 팩과 함께 사용할 수 있습니다.

애플리케이션 인식 백업으로 MySQL 또는 MariaDB 인스턴스를 실행하는 물리적 또는 가상 머신을 보호하려면 이 머신에 Agent for MySQL/MariaDB를 설치해야 합니다. Agent for MySQL/MariaDB는 Agent for Linux(64비트)와 함께 제공되므로 64비트 Linux 기반 운영 체제에만 설치할 수 있습니다. "지원되는 운영 체제 및 환경"(23페이지)을(를) 참조하십시오.

Agent for Linux(64비트) 설치 파일을 다운로드하려면

1. Cyber Protect 콘솔에 로그인합니다.
2. 오른쪽 위에 있는 계정 아이콘을 클릭한 다음 **다운로드**를 선택합니다.
3. **Agent for Linux(64비트)**를 클릭합니다.

   머신에 설치 파일이 다운로드됩니다. 에이전트를 설치하려면 "Linux에서 Protection 에이전트 설치"(74페이지) 또는 "Linux에서 무인 설치 또는 제거"(97페이지)의 설명대로 진행합니다. 선택적 컴퍼넌트인 Agent for MySQL/MariaDB를 반드시 선택해야 합니다.

   데이터베이스와 테이블을 라이브 인스턴스로 복구하려면 Agent for MySQL/MariaDB를 작동하기 위한 임시 스토리지가 필요합니다. 기본적으로 `/tmp` 디렉토리가 사용됩니다. 이 디렉토리는 `ACRONIS_MYSQL_RESTORE_DIR` 환경 변수를 설정하여 변경할 수 있습니다.

© Acronis International GmbH, 2003-2024

제한 사항

- MySQL 또는 MariaDB 클러스터는 지원되지 않습니다.
- Docker 컨테이너에서 실행되는 MySQL 또는 MariaDB 인스턴스는 지원되지 않습니다.
- BTRFS 파일 시스템을 사용하는 운영 체제에서 실행되는 MySQL 또는 MariaDB 인스턴스는 지원되지 않습니다.
- 시스템 데이터베이스(`sys`, `mysql`, `information-schema`, `performance_schema`)와 테이블을 포함하지 않는 데이터베이스는 라이브 인스턴스로 복구할 수 없습니다. 하지만 이와 같은 데이터베이스는 전체 인스턴스를 복구할 때 파일로 복구가 가능합니다.
- 복구는 백업된 인스턴스와 버전이 동일한 대상 인스턴스에만 지원되지만 다음과 같은 제한이 있습니다.
  - MySQL 5.x 인스턴스에서 MySQL 8.x 인스턴스로의 복구는 지원되지 않습니다.
  - MySQL 5.x 버전(부 버전 포함) 이상으로의 복구는 전체 인스턴스를 파일로 복구하는 경우에만 지원됩니다. 복구를 시도하기 전에 대상 버전에 대한 공식 MySQL 업그레이드 안내서(예: MySQL 5.7 업그레이드 안내서)를 참조하십시오.
- Secure Zone에 저장된 백업으로부터의 복구는 지원되지 않습니다.
- 데이터베이스 및 테이블은 AppArmor가 설치된 머신에서 실행되는 Agent for MySQL/MariaDB로 복구할 수 없습니다. 인스턴스를 파일 또는 전체 머신으로 복구할 수 있습니다.
- 심볼 링크로 구성된 대상 데이터베이스로의 복구는 지원되지 않습니다. 데이터베이스의 이름을 변경하면 백업된 데이터베이스를 새 데이터베이스로 복구할 수 있습니다.

알려진 문제

암호로 보호된 Samba 공유에서 데이터를 복구하는 동안 문제가 발생하면 Cyber Protect 콘솔에서 로그아웃한 다음 다시 로그인하십시오. 원하는 복구 지점을 선택한 다음 **MySQL/MariaDB 데이터베이스**를 클릭합니다. **전체 머신** 또는 **파일/폴더**는 클릭하지 마십시오.

애플리케이션 인식 백업 구성

사전 요구 사항

- 선택한 머신에서 하나 이상의 MySQL 또는 MariaDB 인스턴스가 실행 중이어야 합니다.
- MySQL 또는 MariaDB 인스턴스가 실행 중인 머신에서 루트 사용자로 보호 에이전트를 시작해야 합니다.
- 애플리케이션 인식 백업은 보호 계획에서 **전체 머신**을 백업 원본으로 선택한 경우에만 사용할 수 있습니다.
- **섹터 단위** 백업 옵션은 보호 계획에서 비활성화할 수 있습니다. 그렇지 않으면, 애플리케이션 데이터를 복구하는 것이 불가능합니다.

애플리케이션 인식 백업을 구성하려면

1. Cyber Protect 콘솔에서 MySQL 또는 MariaDB 인스턴스가 실행 중인 머신을 하나 이상 선택합니다.

© Acronis International GmbH, 2003-2024

각 머신에는 하나 이상의 인스턴스가 있을 수 있습니다.

2. 백업 모듈이 활성화된 상태에서 보호 계획을 생성합니다.
3. **백업 대상**에서 **전체 머신**을 선택합니다.
4. **애플리케이션 백업**을 클릭한 다음, **MySQL/MariaDB Server** 옆에 있는 스위치를 활성화합니다.
5. MySQL 또는 MariaDB 인스턴스 지정 방법 선택:
   - **모든 워크로드용**

     동일한 구성의 인스턴스를 여러 서버에서 실행하는 경우 이 옵션을 사용합니다. 모든 인스턴스에 동일한 연결 매개 변수와 액세스 자격 증명이 사용됩니다.
   - **특정 워크로드용**

     각 인스턴스에 대한 연결 매개 변수와 액세스 자격 증명을 지정하려면 이 옵션을 사용합니다.
6. 연결 매개 변수와 액세스 자격 증명을 구성하려면 **인스턴스 추가**를 클릭합니다.
   a. 연결 유형을 선택한 후 다음을 지정하십시오.
      - [TCP 소켓의 경우] IP 주소 및 포트.
      - [Unix 소켓의 경우] 소켓 경로.
   b. 인스턴스에 대해 다음 권한을 가진 사용자 계정의 자격 증명을 지정하십시오.
      - 모든 데이터베이스 및 테이블의 경우 `FLUSH_TABLES` 또는 `RELOAD(*.*)`
      - `information_schema.tables`의 경우 `SELECT`
   c. **확인**을 클릭합니다.
7. **완료**를 클릭합니다.

애플리케이션 인식 백업에서 데이터 복구

애플리케이션 인식 백업에서 MySQL 또는 MariaDB 인스턴스, 데이터베이스 및 테이블을 복구할 수 있습니다. 인스턴스가 실행 중인 전체 서버 또는 이 서버에서 파일 및 폴더를 복구할 수도 있습니다.

아래 표에 모든 복구 옵션이 요약되어 있습니다.

복구 대상	다음으로 복구	복구 대상
MySQL 서버 MariaDB 서버	전체 머신	Agent for Linux가 설치된 머신*
MySQL 서버 MariaDB 서버	파일 또는 폴더	Agent for Linux가 설치된 머신*
인스턴스	파일	Agent for MySQL/MariaDB가 설치된 머신*
데이터베이스	동일한 데이터	Agent for MySQL/MariaDB가 설치된 머신*

© Acronis International GmbH, 2003-2024

복구 대상	다음으로 복구	복구 대상
	베이스 새 데이터베이스	• 원래 인스턴스 • 다른 인스턴스 • 원래 데이터베이스 • 새 데이터베이스
Table	동일한 테이블 새 테이블	Agent for MySQL/MariaDB가 설치된 머신* • 원래 인스턴스 • 다른 인스턴스 • 원래 데이터베이스 • 원래 테이블 • 새 테이블

* 에이전트를 포함하고 있으며 백업 관점에서 실제 머신으로 처리되는 가상 머신.

전체 서버 복구

MySQL 또는 MariaDB 인스턴스가 실행 중인 전체 서버를 복구하는 방법은 "머신 복구"(454페이지)을(를) 참조하십시오.

인스턴스 복구

애플리케이션 인식 백업에서 MySQL 또는 MariaDB 인스턴스를 파일로 복구할 수 있습니다.

인스턴스를 복구하려면

1. Cyber Protect 콘솔에서 복구하려는 데이터가 원래 포함되어 있던 머신을 선택합니다.
2. **복구**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.
   머신이 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 중 하나를 수행하십시오.
   - 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 Agent for MySQL/MariaDB가 있는 온라인 머신을 선택한 다음 복구 지점을 선택합니다.
   - **백업 스토리지** 탭에서 복구 지점을 선택합니다.

   위 작업 중 하나에서 찾기 위해 선택한 머신이 복구의 대상 머신이 됩니다.
4. **복구** > **MySQL/MariaDB 데이터베이스**를 클릭합니다.
5. 복구할 인스턴스를 선택한 다음 **파일로 복구**를 클릭합니다.
6. **경로**에서 파일을 복구할 디렉토리를 선택합니다.
7. **복구 시작**을 클릭합니다.

© Acronis International GmbH, 2003-2024

데이터베이스 복구

애플리케이션 인식 백업에서 데이터베이스를 라이브 MySQL 또는 MariaDB 인스턴스로 복구할 수 있습니다.

1. Cyber Protect 콘솔에서 복구하려는 데이터가 원래 포함되어 있던 머신을 선택합니다.
2. **복구**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.

   머신이 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 중 하나를 수행하십시오.
   - 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 Agent for MySQL/MariaDB가 있는 온라인 머신을 선택한 다음 복구 지점을 선택합니다.
   - **백업 스토리지** 탭에서 복구 지점을 선택합니다.

   위 작업 중 하나에서 찾기 위해 선택한 머신이 복구의 대상 머신이 됩니다.
4. **복구** > **MySQL/MariaDB 데이터베이스**를 클릭합니다.
5. 원하는 인스턴스의 이름을 클릭하여 해당 데이터베이스를 자세히 살펴봅니다.
6. 복구할 데이터베이스를 하나 이상 선택합니다.
7. **복구**를 클릭합니다.
8. 대상 인스턴스에 대한 연결 매개 변수와 액세스 자격 증명을 지정하려면 **대상 MySQL/MariaDB 인스턴스**를 클릭합니다.
   - 데이터를 복구할 인스턴스를 확인합니다. 기본적으로 원래 인스턴스가 선택됩니다.
   - 대상 인스턴스에 액세스할 수 있는 사용자 계정의 자격 증명을 지정하십시오. 이 사용자 계정에는 모든 데이터베이스 및 테이블에 대해 다음의 권한이 할당되어 있어야 합니다(*.*).
     - `INSERT`
     - `CREATE`
     - `DROP`
     - `LOCK_TABLES`
     - `ALTER`
     - `SELECT`
   - **확인**을 클릭합니다.
9. 대상 데이터베이스를 확인합니다.

   기본적으로 원래 데이터베이스가 선택됩니다.

   데이터베이스를 새 데이터베이스로 복구하려면 대상 데이터베이스의 이름을 클릭하여 변경합니다. 이 작업은 단일 데이터베이스를 복구하는 경우에만 사용할 수 있습니다.
10. **기존 데이터베이스 덮어쓰기**에서 덮어쓰기 모드를 선택합니다.

    기본적으로 덮어쓰기가 활성화되며 백업된 데이터베이스가 동일한 이름의 대상 데이터베이스를 대체합니다.

    덮어쓰기를 비활성화하면 복구 작업 중에 백업된 데이터베이스를 건너뛰고 동일한 이름의 대상 데이터베이스가 대체되지 않습니다.
11. **복구 시작**을 클릭합니다.

© Acronis International GmbH, 2003-2024

테이블 복구

애플리케이션 인식 백업에서 테이블을 라이브 MySQL 또는 MariaDB 인스턴스로 복구할 수 있습니다.

1. Cyber Protect 콘솔에서 복구하려는 데이터가 원래 포함되어 있던 머신을 선택합니다.
2. **복구**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.

   머신이 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 중 하나를 수행하십시오.
   - 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 Agent for MySQL/MariaDB가 있는 온라인 머신을 선택한 다음 복구 지점을 선택합니다.
   - **백업 스토리지** 탭에서 복구 지점을 선택합니다.

   위 작업 중 하나에서 찾기 위해 선택한 머신이 복구의 대상 머신이 됩니다.
4. **복구** > **MySQL/MariaDB 데이터베이스**를 클릭합니다.
5. 원하는 인스턴스의 이름을 클릭하여 해당 데이터베이스를 자세히 살펴봅니다.
6. 원하는 데이터베이스의 이름을 클릭하여 해당 테이블을 자세히 살펴봅니다.
7. 복구할 테이블을 하나 이상 선택합니다.
8. **복구**를 클릭합니다.
9. 대상 인스턴스에 대한 연결 매개 변수와 액세스 자격 증명을 지정하려면 **대상 MySQL/MariaDB 인스턴스**를 클릭합니다.
   - 데이터를 복구할 인스턴스를 확인합니다. 기본적으로 원래 인스턴스가 선택됩니다.
   - 대상 인스턴스에 액세스할 수 있는 사용자 계정의 자격 증명을 지정하십시오. 이 사용자 계정에는 모든 데이터베이스 및 테이블에 대해 다음의 권한이 할당되어 있어야 합니다(*.*).
     - INSERT
     - CREATE
     - DROP
     - LOCK_TABLES
     - ALTER
     - SELECT
   - **확인**을 클릭합니다.
10. 대상 테이블을 확인합니다.

    기본적으로 원래 테이블이 선택됩니다.

    테이블을 새 테이블로 복구하려면 대상 테이블의 이름을 클릭하여 변경합니다. 이 작업은 단일 테이블을 복구하는 경우에만 사용할 수 있습니다.
11. **기존 테이블 덮어쓰기**에서 덮어쓰기 모드를 선택합니다.

    기본적으로 덮어쓰기가 활성화되며 백업된 테이블이 동일한 이름의 대상 테이블을 대체합니다.

    덮어쓰기를 비활성화하면 복구 작업 중에 백업된 테이블을 건너뛰고 동일한 이름의 대상 테이블이 대체되지 않습니다.
12. **복구 시작**을 클릭합니다.

© Acronis International GmbH, 2003-2024

저장된 루틴 복구

전체 MySQL 인스턴스를 복구하면 저장된 루틴이 자동 복구됩니다.

개별 데이터베이스를 원래 인스턴스가 아닌 인스턴스에 복구하거나 새 데이터베이스로 복구하면 저장된 루틴이 자동 복구되지 않습니다. 저장된 루틴을 SQL 파일로 내보낸 후 복구된 데이터베이스에 추가하여 수동으로 복구할 수 있습니다.

저장된 루틴을 내보낸 후 복구된 데이터베이스에 추가하려면

1. 원래 MySQL 인스턴스가 있는 머신에서 터미널을 엽니다.
2. 다음 명령을 실행하여 저장된 루틴을 내보냅니다.
3. ```
   mysqldump -p [source_database_name] --routines --no-create-info --no-data >
   [exported_db_routines.sql]
   ```
4. 데이터베이스를 복구한 머신에서 MySQL 명령줄 클라이언트를 엽니다.
5. 다음 명령을 실행하여 복구된 데이터베이스에 루틴을 추가합니다.

   ```
   mysql>  use [recovered_database_name];
   ```

   ```
   mysql>  source [path_to_exported_db_routines.sql];
   ```

웹사이트 및 호스팅 서버 보호

웹사이트 보호

웹사이트는 무단 액세스나 맬웨어 공격으로 인해 손상될 수 있습니다. 손상 발생 시 웹사이트를 양호한 상태로 손쉽게 되돌리려면 웹사이트를 백업하십시오.

웹사이트를 백업하려면 무엇이 필요합니까?

웹사이트는 SFTP 또는 SSH 프로토콜을 통해 액세스할 수 있어야 합니다. 에이전트를 설치하지 않고 이 섹션 뒷 부분에 설명된 대로 웹사이트를 추가하기만 하면 됩니다.

어떤 항목을 백업할 수 있습니까?

다음과 같은 항목을 백업할 수 있습니다.

- **웹 사이트 콘텐츠 파일**
  SFTP 또는 SSH 연결을 위해 지정한 계정에 액세스할 수 있는 모든 파일.
- **MySQL 서버에서 호스팅하는 연결된 데이터베이스(있는 경우).**
  지정한 MySQL 계정에 액세스할 수 있는 모든 데이터베이스.

웹사이트에서 데이터베이스를 사용하면 경우 파일과 데이터베이스 모두 백업하여 이들을 일관된 상태로 복구할 수 있도록 하는 것이 좋습니다.

© Acronis International GmbH, 2003-2024
   ```

제한 사항

- 웹사이트 백업에 대해 사용할 수 있는 유일한 백업 위치는 클라우드 스토리지입니다.
- 웹사이트에 여러 보호 계획을 적용할 수 있지만 각 스케줄마다 단 하나의 계획만 실행할 수 있습니다. 다른 계획은 수동으로 시작해야 합니다.
- 사용할 수 있는 유일한 백업 옵션은 "백업 파일 이름"입니다.
- 웹사이트 보호 계획은 **관리** > **보호 계획** 탭에 표시되지 않습니다.

웹사이트 백업

웹사이트을 추가하려면

1. **장치** > **추가**를 클릭합니다.
2. **웹사이트**를 클릭합니다.
3. 웹사이트에 다음과 같은 액세스 설정을 구성하십시오.
   - **웹사이트 이름**에 웹사이트에 대한 이름을 생성하고 입력합니다. 이 이름은 Cyber Protect 콘솔에 표시됩니다.
   - **호스트**에 SFTP 또는 SSH를 통해 웹사이트에 액세스하는 데 사용할 호스트 이름 또는 IP 주소를 지정합니다. 예를 들어 `my.server.com` 또는 `10.250.100.100`와 같습니다.
   - **포트**에 포트 번호를 지정합니다.
   - **사용자 이름** 및 **비밀번호**에 SFTP 또는 SSH를 통해 웹사이트에 액세스하는 데 사용할 수 있는 계정의 자격 증명을 지정합니다.

     중요
     지정한 계정에 액세스할 수 있는 파일만 백업됩니다.

     비밀번호 대신 개인 SSH 키를 지정할 수 있습니다. 이렇게 하려면 **비밀번호 대신 SSH 개인 키 사용** 확인란을 선택한 다음 키를 지정합니다.
4. **다음**을 클릭합니다.
5. 웹사이트에서 MySQL 데이터베이스를 사용하는 경우 데이터베이스에 대한 액세스 설정을 구성합니다. 그렇지 않은 경우, **건너뛰기**를 클릭합니다.
   a. **연결 유형**에서 클라우드에서 데이터베이스에 액세스하는 방법을 선택합니다.
      - **호스트에서 SSH를 통해 연결**—3단계에서 지정한 호스트를 통해 데이터베이스에 액세스합니다.
      - **직접 연결**—데이터베이스에 직접 액세스합니다. 인터넷을 통해 데이터베이스에 액세스할 수 있는 경우에만 이 설정을 선택합니다.
   b. **호스트**에 MySQL 서버가 실행되고 있는 호스트의 이름 또는 IP 주소를 지정합니다.
   c. **포트**에 서버로의 TCP/IP 연결을 위한 포트 번호를 지정합니다. 기본 포트 번호는 3306입니다.
   d. **사용자 이름** 및 **비밀번호**에 MySQL 계정 자격 증명을 지정합니다.

      중요

© Acronis International GmbH, 2003-2024

지정한 계정에 액세스할 수 있는 데이터베이스만 백업됩니다.

e. **생성**을 클릭합니다.

웹 사이트가 Cyber Protect 콘솔의 **장치** > **웹 사이트**에 표시됩니다.

연결 설정을 변경하려면

1. **장치** > **웹사이트**에서 웹사이트를 선택합니다.
2. **상세정보**를 클릭합니다.
3. 웹사이트 또는 데이터베이스 연결 설정 옆의 연필 아이콘을 클릭합니다.
4. 필요한 변경 작업을 수행한 다음 **저장**을 클릭합니다.

웹사이트의 보호 계획을 만들려면

1. **장치** > **웹사이트**에서 하나 또는 여러 개의 웹사이트를 선택합니다.
2. **보호**를 클릭합니다.
3. [선택 사항] 데이터베이스 백업을 활성화합니다.

여러 웹사이트를 선택한 경우 데이터베이스의 백업은 기본적으로 비활성화됩니다.
4. [선택 사항] 보관 규칙을 변경합니다.
5. [선택 사항] 백업의 암호화를 비활성화합니다.
6. [선택 사항] **백업 파일 이름**을 편집하려면 기어 아이콘을 클릭합니다. 이는 다음의 두 경우에 유용합니다.
   - 먼저 이 웹사이트를 백업했고 기존 백업 순서로 계속하려는 경우
   - **백업 스토리지** 탭에서 사용자 정의 이름을 보려는 경우
7. **적용**을 클릭합니다.

머신에서와 동일한 방법으로 웹사이트의 보호 계획을 편집, 취소, 삭제할 수 있습니다. 이 작업은 "보호 계획 관련 작업"에 설명되어 있습니다.

웹사이트 복구

웹사이트를 복구하려면

1. 다음 중 하나를 수행하십시오.
   - **장치** > **웹사이트**에서 복구할 웹사이트를 선택한 다음 **복구**를 클릭합니다.

     웹사이트를 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.
   - 웹사이트가 삭제되었다면 백업 스토리지 탭의 **클라우드 애플리케이션 백업** 섹션에서 선택한 후 **백업 표시**를 클릭합니다.

     삭제한 웹사이트를 복구하려면 대상 사이트를 장치로 추가해야 합니다.
2. 복구 지점을 선택합니다.
3. **복구**를 클릭한 다음 **전체 웹사이트**, **데이터베이스**(있는 경우) 또는 **파일/폴더**.

웹 사이트를 일관된 상태로 유지하려면 순서에 상관없이 파일과 데이터베이스를 모두 복구하는 것이 좋습니다.
4. 선택에 따라 아래에 설명된 절차 중 하나를 따릅니다.

© Acronis International GmbH, 2003-2024

전체 웹사이트를 복구하려면

1. **웹사이트로 복구**에서 대상 웹사이트를 보거나 변경합니다.
   기본적으로 원래 웹사이트가 선택됩니다. 원래 웹사이트가 없는 경우 대상 웹사이트를 선택해야 합니다.
2. 복구한 항목에 대해 공유 권한을 복구할 것인지 선택합니다.
3. **복구 시작**을 클릭한 다음 작업을 확인합니다.

데이터베이스를 복구하려면

1. 복구할 데이터베이스를 선택합니다.
2. 파일로 데이터베이스를 다운로드하려면 **다운로드**를 클릭하고 파일을 저장할 위치를 선택한 다음 **저장**을 클릭합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. **복구**를 클릭합니다.
4. **웹사이트로 복구**에서 대상 웹사이트를 보거나 변경합니다.
   기본적으로 원래 웹사이트가 선택됩니다. 원래 웹사이트가 없는 경우 대상 웹사이트를 선택해야 합니다.
5. **복구 시작**을 클릭한 다음 작업을 확인합니다.

웹사이트 파일/폴더를 복구하려면

1. 복구할 파일/폴더를 선택합니다.
2. 파일을 저장하려면 **다운로드**를 클릭하고 파일을 저장할 위치를 선택한 다음 **저장**을 클릭합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. **복구**를 클릭합니다.
4. **웹사이트로 복구**에서 대상 웹사이트를 보거나 변경합니다.
   기본적으로 원래 웹사이트가 선택됩니다. 원래 웹사이트가 없는 경우 대상 웹사이트를 선택해야 합니다.
5. 복구한 항목에 대해 공유 권한을 복구할 것인지 선택합니다.
6. **복구 시작**을 클릭한 다음 작업을 확인합니다.

웹 호스팅 서버 보호

Plesk, cPanel, DirectAdmin, VirtualMin, ISPManager 제어 패널을 실행하는 Linux 기반 웹 호스팅 서버를 보호할 수 있습니다. 다른 벤더의 웹 호스팅 제어 패널을 실행하는 서버의 경우에는 일반 워크로드로 보호됩니다.

할당량

Plesk, cPanel, DirectAdmin, VirtualMin, ISPManager 제어 패널을 실행하는 서버는 웹 호스팅 서버로 간주됩니다. 각 백업된 웹 호스팅 서버는 **웹 호스팅 서버** 할당량을 사용합니다. 이러한 할당량이 비활성화되어 있거나 이 할당량에 대한 초과분을 초과한 경우, 다음과 같이 할당량이 배정되거나 백업이 실패하게 됩니다.

- 실제 서버인 경우, **서버** 할당량이 사용됩니다. 이러한 할당량이 비활성화되어 있거나 이 할당량에 대한 초과분을 초과한 경우, 백업에 실패합니다.

© Acronis International GmbH, 2003-2024

- 가상 서버인 경우, **가상 머신** 할당량이 사용됩니다. 이러한 할당량이 비활성화되어 있거나 이 할당량에 대한 초과분을 초과한 경우, 백업에 실패합니다.

DirectAdmin, cPanel 및 Plesk 통합

DirectAdmin, Plesk 또는 cPanel 플랫폼을 사용하는 웹 호스팅 관리자는 Cyber Protection 서비스에 이러한 제어판을 통합하면 다음을 비롯한 여러 가지 유용한 기능을 활용할 수 있습니다.

- 전체 웹 호스팅 서버를 클라우드 스토리지에 디스크 수준 백업으로 백업
- 모든 웹 사이트와 계정을 포함한 전체 서버 복구
- 계정, 웹 사이트, 개별 파일, 사서함 또는 데이터베이스의 세부 복구 수행 및 이러한 항목 다운로드
- 리셀러와 고객이 데이터의 셀프 서비스 복구를 수행할 수 있도록 지원

통합을 수행하려면 Cyber Protection 서비스 확장을 사용해야 합니다. 자세한 내용은 해당 통합 가이드를 참조하십시오.

- DirectAdmin 통합 가이드
- WHM 및 cPanel 통합 가이드
- Plesk 통합 가이드

가상 머신을 사용한 특수 작업

백업에서 가상 머신 실행(즉시 복원)

운영 체제가 포함된 디스크 수준 백업에서 가상 머신을 실행할 수 있습니다. 즉시 복구라고도 하는 이 작업을 통해 가상 서버를 스핀업할 수 있습니다. 가상 디스크가 백업에서 직접 열거되므로 데이터 저장소(스토리지)의 공간을 사용하지 않습니다. 스토리지 공간은 변경 사항을 가상 디스크에 보관하는 데에만 필요합니다.

이 임시 가상 머신은 최대 3일 동안 작동 상태로 유지하는 것이 좋습니다. 그런 다음 완전히 제거하거나 가동 중지 없이 일반 가상 머신으로 변환(완료)할 수 있습니다.

임시 가상 머신이 존재하는 한 해당 머신에서 사용 중인 백업에는 보관 규칙을 적용할 수 없습니다. 원래 머신의 백업은 계속해서 실행할 수 있습니다.

사용 예제

- **재해 복구**

  실패한 머신의 사본을 온라인으로 즉시 가져옵니다.
- **백업 테스트**

  백업에서 머신을 실행하고 게스트 OS 및 애플리케이션이 제대로 작동하는지 확인합니다.
- **애플리케이션 데이터에 액세스**

  머신 실행 중 애플리케이션의 기본 관리 도구를 사용하여 필수 데이터에 액세스하고 필수 데이터를 추출합니다.

© Acronis International GmbH, 2003-2024

사전 요구 사항

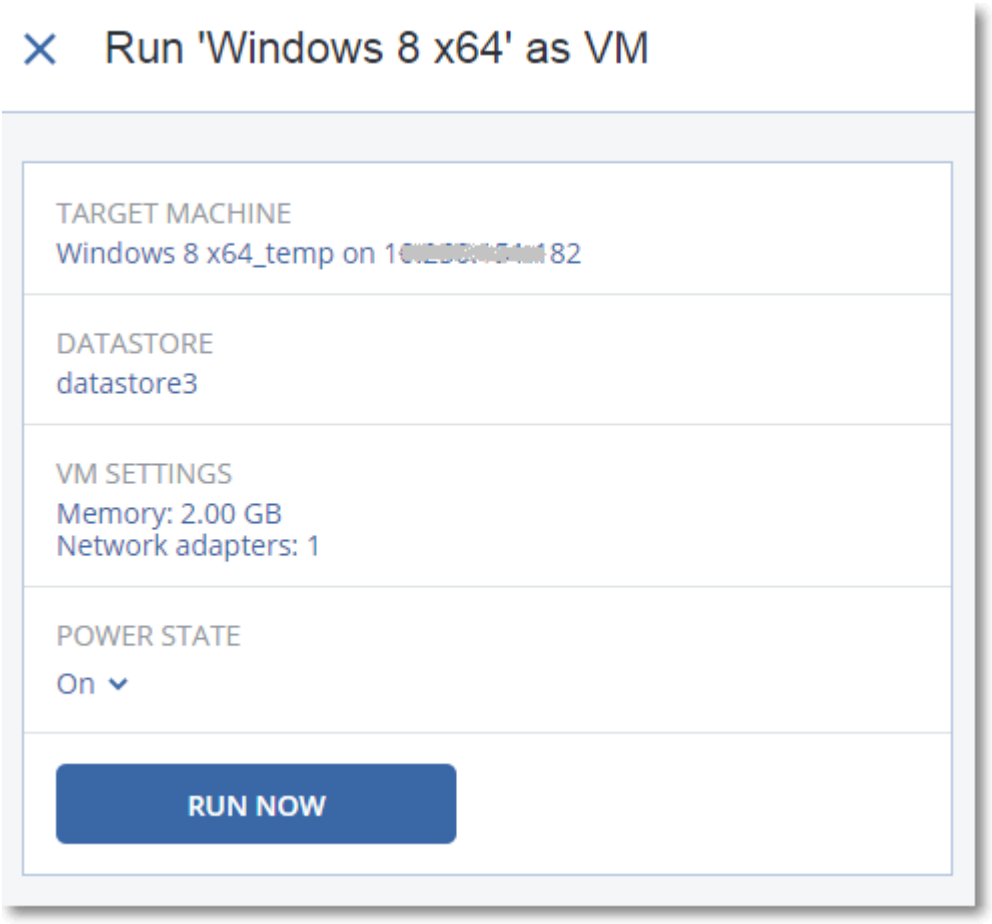
- Cyber Protection 서비스에 Agent for VMware 또는 Agent for Hyper-V가 하나 이상 등록되어 있어야 합니다.
- Agent for VMware 또는 Agent for Hyper-V가 설치된 머신의 네트워크 폴더 또는 로컬 폴더에 백업이 저장될 수 있습니다. 네트워크 폴더를 선택하면 머신에서 액세스할 수 있습니다. 가상 머신을 클라우드 스토리지에 저장되어 있는 백업에서 실행할 수 있지만 이 작업에는 백업으로부터 집중적인 임의 액세스 읽기가 필요하기 때문에 속도가 느려집니다.
- 백업에는 전체 머신이 포함되어 있거나 운영 체제를 시작하는 데 필요한 모든 볼륨이 포함되어 있어야 합니다.
- 실제 머신 및 가상 머신 둘 다의 백업을 사용할 수 있습니다. Virtuozzo *컨테이너*의 백업은 사용할 수 없습니다.
- Linux 논리 볼륨(LVM)을 포함하고 있는 백업은 Agent for VMware 또는 Agent for Hyper-V에서 생성된 것이어야 합니다. 가상 머신은 원래 머신과 동일한 유형이어야 합니다(ESXi 또는 Hyper-V).

머신 실행

1. 다음 중 하나를 수행하십시오.
   - 백업된 머신을 선택하고 **복구**를 클릭한 다음 복구 지점을 선택합니다.
   - 백업 스토리지 탭에서 복구 지점을 선택합니다.
2. **VM으로 실행**을 클릭합니다.

   호스트 및 기타 필수 매개변수가 자동으로 선택됩니다.

© Acronis International GmbH, 2003-2024



3. [선택 사항] **대상 머신**을 클릭한 다음 가상 머신 유형(ESXi 또는 Hyper-V), 호스트 또는 가상 머신 이름을 변경합니다.
4. [선택 사항] ESXi의 경우 **데이터 저장소**를, Hyper-V의 경우 **경로**를 클릭한 다음 가상 머신의 데이터 저장소(스토리지)를 선택합니다.

   머신 실행 중에는 가상 디스크에 대한 변경 사항이 누적됩니다. 선택한 데이터 저장소에 여유 공간이 충분한지 확인합니다. 가상 머신을 영구적으로 설정하여 이 변경 사항을 유지할 계획인 경우, 운영 중인 머신을 실행하는 데 적합한 데이터 저장소를 선택합니다.
5. [선택 사항] **VM 설정**을 클릭하여 가상 머신의 메모리 크기 및 네트워크 연결을 변경합니다.
6. [선택 사항] VM 전원 상태(**켜짐**/**꺼짐**)를 선택합니다.
7. **지금 실행**을 클릭합니다.

따라서 머신이 웹 인터페이스에 아이콘 또는 중 하나와 함께 나타납니다. 이러한 가상 머신은 백업 대상으로 선택할 수 없습니다.

© Acronis International GmbH, 2003-2024

참고
Microsoft Azure의 백업을 사용하여 가상 머신으로 실행(Instant Restore) 작업을 수행할 수 있습니다. 그러나 이 작업에서는 송신 트래픽이 대량으로 발생하므로 Microsoft Azure 구독 요금에 해당 트래픽 요금이 추가됩니다. Microsoft Azure 백업에서 실행되는 Windows 머신에서 일반적으로 발생하는 송신 트래픽(가상 머신 전원을 켜는 시점부터 로그인하는 시점까지 발생하는 트래픽)은 약 5GB입니다.

머신 삭제

vSphere/Hyper-V에서 임시 가상 머신을 직접 삭제하지 않는 것이 좋습니다. 이렇게 하면 웹 인터페이스에서 불필요한 부분이 생길 수 있습니다. 또한 머신이 실행 중이었던 백업은 한 동안 잠금 상태로 남아 있을 수 있습니다. 이러한 백업은 보관 규칙에 따라 삭제할 수 없습니다.

백업에서 실행 중인 가상 머신을 삭제하려면

1. **모든 장치** 탭에서 백업에서 실행 중인 머신을 선택합니다.
2. **삭제**를 클릭합니다.

웹 인터페이스에서 해당 머신이 제거됩니다. vSphere 또는 Hyper-V 인벤토리 및 데이터 저장소(스토리지)에서도 제거됩니다. 머신 실행 중 데이터에 대해 변경된 모든 사항이 손실됩니다.

머신 완료

가상 머신이 백업에서 실행 중인 경우 가상 디스크의 내용은 해당 백업에서 직접 가져옵니다. 따라서 백업 위치 또는 보호 에이전트에 대한 연결이 끊기면 해당 머신에 액세스할 수 없게 되거나 해당 머신이 손상됩니다.

이 머신을 영구적으로 만들 수 있습니다. 즉, 머신 실행 중 변경된 사항과 함께 모든 가상 디스크를 이러한 변경 사항이 저장된 데이터 저장소로 복구합니다. 이러한 프로세스를 완료라고 합니다.

완료는 가동 중지 없이 수행됩니다. 가상 머신은 완료 중 전원이 꺼지지 *않습니다*.

최종 가상 디스크의 위치는 **VM으로 실행** 작업의 매개변수(ESXi용 **데이터 저장소** 또는 Hyper-V용 **경로**)에 정의되어 있습니다. 완료를 시작하기 전에 여유 공간, 공유 기능, 이 데이터 저장소의 성능이 운영 중 머신 실행에 적합한지 여부 등을 확인하십시오.

참고
Windows Server 2008/2008 R2 및 Microsoft Hyper-V Server 2008/2008 R2에서 실행 중인 Hyper-V의 경우 해당 Hyper-V 버전에는 필요한 API가 누락되어 있기 때문에 완료가 지원되지 않습니다.

백업에서 실행 중인 머신을 완료하려면

1. **모든 장치** 탭에서 백업에서 실행 중인 머신을 선택합니다.
2. **완료**를 클릭합니다.
3. [선택 사항] 머신의 새 이름을 지정합니다.
4. [선택 사항] 디스크 프로비저닝 모드를 변경합니다. 기본 설정은 **씬**입니다.
5. **완료**를 클릭합니다.

© Acronis International GmbH, 2003-2024

머신 이름이 즉시 변경됩니다. 복구 진행률이 **작업** 탭에 표시됩니다. 복구가 완료되면 머신 아이콘이 일반적인 가상 머신 아이콘을 바꿉니다.

완료에 대해서 알아야 할 사항

완료와 일반 복구 비교

다음과 같은 이유로 완료 프로세스는 일반 복구보다 속도가 느립니다.

- 완료를 진행하는 동안 에이전트는 백업의 다른 부분에 임의 액세스를 수행합니다. 전체 머신이 복구되는 동안 에이전트가 백업에서 가져온 데이터를 순차적으로 읽습니다.
- 완료 작업 동안 가상 머신이 실행되는 경우 에이전트는 두 프로세스를 동시에 유지 관리하기 위해 백업에서 가져온 데이터를 더 자주 읽습니다. 일반 복구 시에는 가상 머신이 정지됩니다.

클라우드 백업에서 실행 중인 머신의 완료

백업 데이터에 대한 집중적인 액세스로 인해 완료 속도는 백업 위치와 에이전트 사이의 연결 대역폭에에 따라 크게 달라집니다. 로컬 백업과 비교할 때 클라우드에 있는 백업의 완료 속도가 더 느립니다. 인터넷 연결이 매우 느리거나 불안정한 경우 클라우드 백업에서 실행 중인 머신의 완료 작업이 실패할 수 있습니다. 최종 확정을 수행할 계획인 경우 가능하면 로컬 백업의 가상 머신을 실행하는 것이 좋습니다.

참고

"가상 어플라이언스 구성"(126페이지)의 3단계에 설명되어 있듯이 최종 확정 속도는 에이전트가 연결되어 있는 대상(VMware ESXi 호스트 또는 vCenter)에 따라 달라집니다. VMware vCenter 연결 시에는 VMware API 관련 작업으로 인해 최종 확정 작업 속도가 느려질 수 있습니다. 최종 확정 작업 속도를 높이려는 경우 별도의 Agent for VMware를 사용하여 **VM으로 실행** 작업을 수행한 후 최종 확정을 진행합니다. 그러면 이 에이전트가 vCenter 대신 ESXi 호스트에 연결됩니다.

VMware vSphere에서 작업

이 섹션에서는 VMware vSphere 환경에만 관련된 작업을 설명합니다.

가상 머신 복제

복제는 VMware ESXi 가상 머신에 대해서만 가능합니다.

복제는 가상 머신과 똑같은 복사본(복제본)을 생성하고, 이 복제본을 원래 머신과 동기화된 상태로 유지하는 프로세스입니다. 필수 가상 머신을 복제해두면 이 머신의 복사본을 언제든 시작할 준비가 되어 있는 상태로 항상 보유하고 있는 셈입니다.

복제본은 수동으로 또는 지정한 일정에 따라 시작할 수 있습니다. 첫 번째 복제는 전체 복제(전체 머신 복사)입니다. 이후의 모든 복제는 증분 복제로, 이 옵션을 비활성화하지 않는 한, Changed Block Tracking 옵션에 따라 수행됩니다.

© Acronis International GmbH, 2003-2024

복제 대 백업 비교

스케줄대로 이루어지는 백업과 달리 복제본은 가상 머신의 마지막 상태만 유지합니다. 복제본은 데이터 저장소 공간을 사용하는 데 반해, 백업은 더 저렴한 스토리지에 유지할 수 있습니다.

하지만 복제본의 전원을 켜는 것이 복구보다는 훨씬 빠르고, 백업에서 가상 머신을 실행하는 것보다도 빠릅니다. 전원이 켜지면 복제본이 백업에서 실행되는 VM보다 빠르게 작동하고, Agent for VMware를 로드하지 않습니다.

사용 예제

- **가상 머신을 원격 사이트로 복제합니다.**
  복제를 통해 주 사이트에서 보조 사이트로 가상 머신을 복제해두면 부분 또는 전체 데이터 센터 장애 시 대처할 수 있습니다. 대개 보조 사이트는 원격 주 사이트 장애를 유발할 수 있는 환경, 인프라 또는 기타 요인의 영향을 받을 가능성이 거의 없는 원격 설비에 위치합니다.
- **단일 사이트 내에서 가상 머신을 복제합니다(한 호스트/데이터 저장소에서 다른 호스트/데이터 저장소로 복제).**
  온사이트 복제는 고가용성과 재해 복구 시나리오 용도로 사용할 수 있습니다.

복제본으로 할 수 있는 작업

- **복제본 테스트**
  테스트를 위해 복제본의 전원이 꺼집니다. vSphere Client 또는 기타 도구를 사용해 복제본이 올바로 작동하는지 확인합니다. 테스트를 진행하는 동안 복제본은 일시 중지됩니다.
- **복제본으로 장애 조치**
  장애 조치는 원래 가상 머신의 워크로드를 복제본으로 이전하는 작업입니다. 장애 조치를 진행하는 동안 복제본은 일시 중지됩니다.
- **복제본 백업**
  백업과 복제 모두 가상 디스크 액세스가 필요하므로 가상 머신을 실행 중인 호스트의 성능에 영향을 미치게 됩니다. 가상 머신의 복제본과 백업을 모두 확보하고 싶지만 프로덕션 호스트에 추가 로드를 주고 싶지 않다면 머신을 다른 호스트로 복제한 다음, 해당 복제본의 백업을 설정하십시오.

제한 사항

- 다음 유형의 가상 머신은 복제할 수 없습니다.
  - ESXi 5.5 이하에서 실행 중인 내결함성 머신.
  - 백업에서 실행하는 머신.
  - 가상 머신의 복제본.
- ESXi 호스트에 네트워크 인터페이스 카드(NIC)를 추가하거나 호스트에서 NIC를 제거하는 등 하드웨어에서 특정 변경을 수행하면 호스트의 내부 ID가 변경됩니다. 이 변경 작업은 VM 복제 계획에도 영향을 줍니다. 이러한 변경을 수행한 후에는 ESXi 호스트가 소스나 대상으로 선택되어 있는 VM 복제 계획을 다시 생성해야 합니다. 이렇게 하지 않으면 VM 복제 계획이 정상 작동하지 않습니다.

© Acronis International GmbH, 2003-2024

복제 계획 생성

복제 계획은 각 머신마다 개별적으로 생성해야 합니다. 기존 계획을 다른 머신에 적용할 수는 없습니다.

복제 계획을 생성하려면

1. 복제할 가상 머신을 선택합니다.
2. **복제**를 클릭합니다.
   소프트웨어에 새 복제 계획 템플릿이 표시됩니다.
3. [선택 사항] 복제 계획 이름을 수정하려면 기본 이름을 클릭합니다.
4. **대상 머신**을 클릭한 후 다음 작업을 수행합니다.
   a. 새 복제본을 생성할지, 아니면 원래 머신의 기존 복제본을 사용할지 선택합니다.
   b. ESXi 호스트를 선택하고, 새 복제본 이름을 지정하거나 기존 복제본을 선택합니다.
      새 복제본의 기본 이름은 **[원래 머신 이름]_replica**입니다.
   c. **확인**을 클릭합니다.
5. [새 머신으로 복제하는 경우에만 해당] **데이터 저장소**를 클릭한 다음 가상 머신의 데이터 저장소를 선택합니다.
6. [선택 사항] 복제 스케줄을 변경하려면 **스케줄**을 클릭합니다.
   기본적으로 복제는 월요일부터 금요일까지 매일 수행됩니다. 복제를 실행할 시간을 선택할 수 있습니다.
   복제 빈도를 변경하려고 하는 경우 슬라이더를 이동한 다음 스케줄을 지정합니다.
   다음 작업도 수행할 수 있습니다.
   - 스케줄이 적용되는 날짜 범위를 설정합니다. **날짜 범위 내에서 계획 실행** 확인란을 선택한 다음 날짜 범위를 지정합니다.
   - 스케줄을 비활성화합니다. 이 경우에는 복제를 수동으로 시작할 수 있습니다.
7. [선택 사항] 복제 옵션을 수정하려면 기어 아이콘을 클릭합니다.
8. **적용**을 클릭합니다.
9. [선택 사항] 계획을 수동으로 실행하려면 계획 패널에서 **지금 실행**을 클릭합니다.

복제 계획을 실행하고 나면 가상 머신 복제본이 **모든 장치** 목록에 다음 아이콘과 함께 나타납니다.

복제본 테스트

복제본 테스트를 준비하려면

1. 테스트할 복제본을 선택합니다.
2. **복제본 테스트**를 클릭합니다.
3. **테스트 시작**을 클릭합니다.
4. 전원이 켜진 복제본을 네트워크에 연결할지 선택합니다. 기본적으로 복제본은 네트워크에 연결되지 않습니다.

© Acronis International GmbH, 2003-2024

5. [선택 사항] 복제본을 네트워크에 연결하기로 선택한 경우 복제본의 전원을 켜기 전에 먼저 **원래 가상 머신 중지** 확인란을 선택하여 원래 머신을 중지합니다.
6. **시작**을 클릭합니다.

복제본 테스트를 중지하려면

1. 테스트가 진행 중인 복제본을 선택합니다.
2. **복제본 테스트**를 클릭합니다.
3. **테스트 중지**를 클릭합니다.
4. 결정을 확인합니다.

복제본으로 장애 조치

머신을 복제본으로 장애 조치하려면

1. 장애 조치할 복제본을 선택합니다.
2. **복제본 작업**을 클릭합니다.
3. **장애 조치**를 클릭합니다.
4. 전원이 켜진 복제본을 네트워크에 연결할지 선택합니다. 기본적으로 복제본은 원래 머신과 같은 네트워크에 연결됩니다.
5. [선택 사항] 복제본을 네트워크에 연결하기로 선택한 경우 **원래 가상 머신 중지** 확인란을 선택 취소하여 원래 머신을 온라인 상태로 유지합니다.
6. **시작**을 클릭합니다.

복제본이 장애 조치 상태에 있는 동안 다음 작업 중 하나를 선택할 수 있습니다.

- **장애 조치 중지**
  원래 머신이 고쳐진 경우 장애 조치를 중지합니다. 복제본의 전원이 꺼집니다. 복제가 다시 시작됩니다.
- **복제본으로 영구 장애 조치 수행**
  이 즉각적인 작업은 가상 머신에서 '복제본' 플래그를 제거하여 이에 대한 복제가 더 이상 가능하지 않도록 합니다. 복제를 다시 시작하려면 복제 계획을 편집하여 이 머신을 소스로 선택하십시오.
- **장애 복구**
  연속 작업을 위해 마련되지 않은 사이트로 장애 조치한 경우에는 장애 복구를 수행합니다. 복제본이 원래 머신 또는 새 가상 머신으로 복구됩니다. 원래 머신으로의 복구가 완료되고 나면 복제본의 전원이 켜지고, 복제가 다시 시작됩니다. 새 머신으로 복구하기로 선택한 경우 복제 계획을 편집하여 이 머신을 소스로 선택하십시오.

장애 조치 중지

장애 조치를 중지하려면

1. 장애 조치 상태에 있는 복제본을 선택합니다.
2. **복제본 작업**을 클릭합니다.

© Acronis International GmbH, 2003-2024

3. **장애 조치 중지**를 클릭합니다.
4. 결정을 확인합니다.

영구 장애 조치 수행

영구 장애 조치를 수행하려면

1. 장애 조치 상태에 있는 복제본을 선택합니다.
2. **복제본 작업**을 클릭합니다.
3. **영구 장애 조치**를 클릭합니다.
4. [선택 사항] 가상 머신의 이름을 변경합니다.
5. [선택 사항] **원래 가상 머신 중지** 확인란을 선택합니다.
6. **시작**을 클릭합니다.

장애 복구

복제본에서 장애를 복구하려면

1. 장애 조치 상태에 있는 복제본을 선택합니다.
2. **복제본 작업**을 클릭합니다.
3. **복제본에서 장애 복구**를 클릭합니다.
   원래 머신이 대상 머신으로 자동으로 선택됩니다.
4. [선택 사항] **대상 머신**을 클릭한 후 다음 작업을 수행합니다.
   a. 새 머신 또는 기존 머신으로 장애 복구할지 선택합니다.
   b. ESXi 호스트를 선택하고, 새 머신 이름을 지정하거나 기존 머신을 선택합니다.
   c. **확인**을 클릭합니다.
5. [선택 사항] 새 머신으로 장애 복구하는 경우 다음 작업을 수행할 수도 있습니다.
   - **데이터 저장소**를 클릭하여 가상 머신의 데이터 저장소를 선택합니다.
   - **VM 설정**을 클릭해 메모리 크기, 프로세서 수 및 가상 머신의 네트워크 연결을 변경합니다.
6. [선택 사항] **장애 복구 옵션**을 수정하려면 복구 옵션을 클릭합니다.
7. **복구 시작**을 클릭합니다.
8. 결정을 확인합니다.

복제 옵션

복제 옵션을 수정하려면 복제 계획 이름 옆에 있는 기어 아이콘을 클릭한 다음 **복제 옵션**을 클릭합니다.

CBT(Changed Block Tracking)

이 옵션은 백업 옵션 "CBT(Changed Block Tracking)"와 유사합니다.

디스크 프로비저닝

이 옵션은 복제본에 대한 디스크 프로비저닝 설정을 정의합니다.

사전 설정값이 **씬 프로비저닝**입니다.

© Acronis International GmbH, 2003-2024

다음 값을 선택할 수 있습니다. **씬 프로비저닝**, **씩 프로비저닝**, **원래 설정 유지**.

오류 처리

이 옵션은 백업 옵션 "오류 처리"와 유사합니다.

사전/사후 명령어

이 옵션은 백업 옵션 "사전/사후 명령어"와 유사합니다.

가상 머신용 VSS(Volume Shadow Copy Service)

이 옵션은 백업 옵션 "가상 머신용 VSS(Volume Shadow Copy Service)"와 유사합니다.

장애 복구 옵션

장애 복구 옵션을 수정하려면 장애 복구를 구성할 때 **복구 옵션**을 클릭합니다.

오류 처리

이 옵션은 복구 옵션 "오류 처리"와 유사합니다.

성능

이 옵션은 복구 옵션 "성능"과 유사합니다.

사전/사후 명령어

이 옵션은 복구 옵션 "사전/사후 명령어"와 유사합니다.

VM 전원 관리

이 옵션은 복구 옵션 "VM 전원 관리"와 유사합니다.

초기 복제본 시딩

원격 위치로의 복제 속도를 높이고 네트워크 대역폭을 저장하기 위해 복제본 시딩을 수행할 수 있습니다.

중요

복제본 시딩을 수행하려면 Agent for VMware(가상 어플라이언스)가 대상 ESXi에서 실행되어야 합니다.

초기 복제본을 시딩하려면

1. 다음 중 하나를 수행하십시오.
   - 원본 가상 머신의 전원을 끌 수 있다면, 전원을 끈 다음 4단계로 건너뛰십시오.
   - 원본 가상 머신의 전원을 끌 수 없다면 다음 단계를 계속 수행하십시오.
2. 복제 계획을 생성합니다.
   계획을 생성할 때 **대상 머신**에서 **새 복제본** 및 원본 머신을 호스팅하는 ESXi를 선택합니다.
3. 계획을 한 번 실행합니다.

© Acronis International GmbH, 2003-2024

복제본이 원본 ESXi에 생성됩니다.

4. 가상 머신(또는 복제본) 파일을 외장 하드 드라이브로 내보냅니다.
   a. 외장 하드 드라이브를 vSphere Client가 실행 중인 머신과 연결합니다.
   b. vSphere Client를 원본 vCenter\ESXi로 연결합니다.
   c. 새롭게 생성된 복제본을 인벤토리에서 선택합니다.
   d. **파일** > **내보내기** > **OVF 템플릿 내보내기**를 클릭합니다.
   e. **디렉토리**에서 외장 하드 드라이브의 폴더를 지정합니다.
   f. **확인**을 클릭합니다.
5. 하드 드라이브를 원격 위치로 전송합니다.
6. 복제본을 대상 ESXi로 가져옵니다.
   a. 외장 하드 드라이브를 vSphere Client가 실행 중인 머신과 연결합니다.
   b. vSphere Client를 대상 vCenter\ESXi로 연결합니다.
   c. **파일** > **OVF 템플릿 디플로이**를 클릭합니다.
   d. **파일 또는 URL의 디플로이**에서 앞서 4단계에서 내보낸 템플릿을 지정합니다.
   e. 가져오기 절차를 완료합니다.
7. 2단계에서 생성한 복제 계획을 편집합니다. **대상 머신**에서 **기존 복제본**을 선택한 다음, 가져온 복제본을 선택합니다.

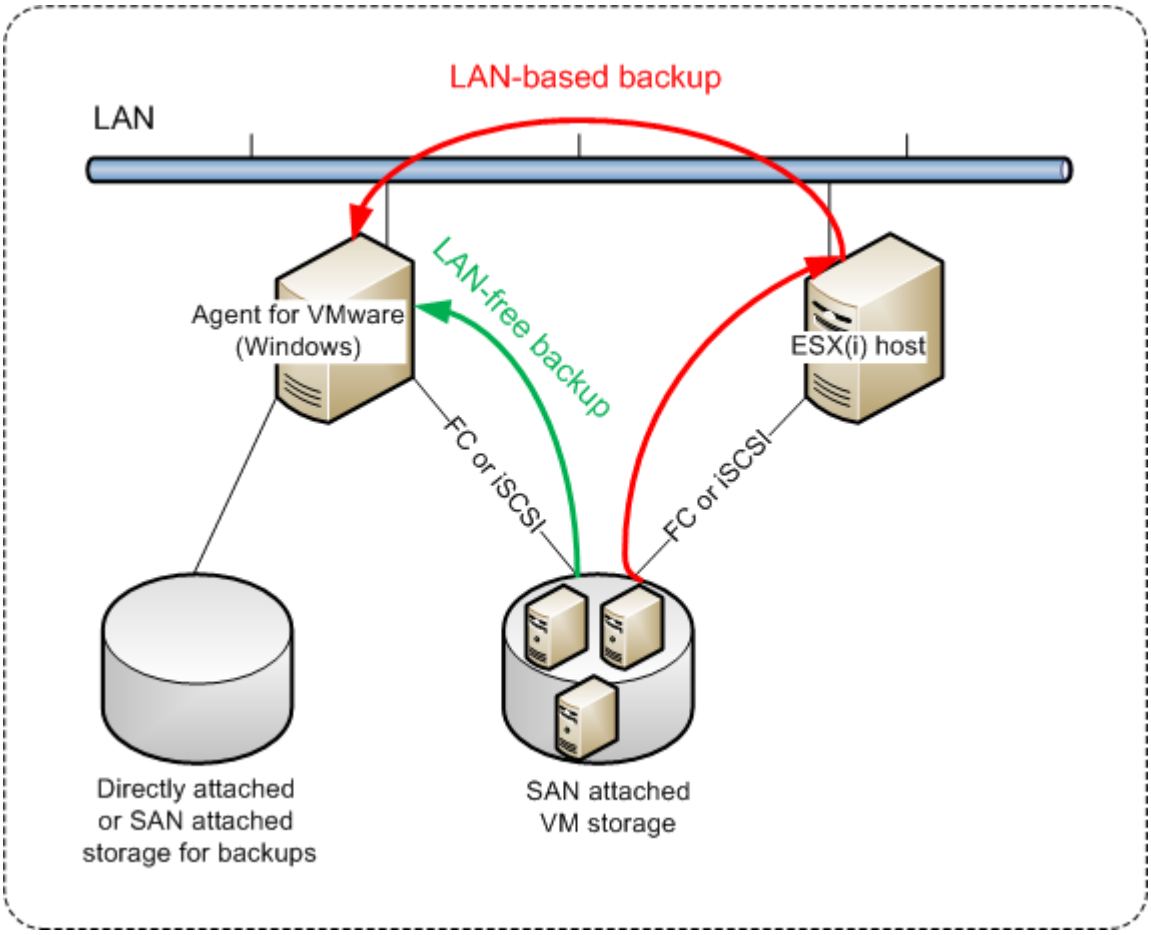
결과적으로 소프트웨어에서 복제본 업데이트를 지속합니다. 모든 복제는 증분식입니다.

Agent for VMware - LAN 프리 백업

ESXi에서 SAN 연결 스토리지를 사용하는 경우 동일한 SAN에 연결된 머신에 에이전트를 설치합니다. 에이전트는 ESXi 호스트 및 LAN을 통해서가 아니라 스토리지에서 가상 머신을 직접 백업합니다. 이 기능을 LAN 프리 백업이라고 부릅니다.

아래 다이어그램은 LAN 기반 및 LAN 프리 백업을 보여줍니다. FC(광채널) 또는 iSCSI Storage Area Network가 있는 경우 가상 머신에 대한 LAN 프리 액세스가 가능합니다. LAN을 통한 백업된 데이터 전송을 완전히 제거하기 위해서는 에이전트 머신의 로컬 디스크 또는 SAN 연결 스토리지에 백업을 저장합니다.

© Acronis International GmbH, 2003-2024



에이전트가 데이터 저장소에 직접 액세스할 수 있도록 하려면

1. vCenter Server에 네트워크를 통해 액세스할 수 있는 Windows 머신에 Agent for VMware를 설치합니다.
2. 머신에 데이터 저장소를 호스팅하는 LUN(Logical Unit Number)을 연결합니다. 다음을 고려하십시오.
   - ESXi로의 데이터 저장소 연결에 사용된 동일한 프로토콜(즉, iSCSI 또는 FC)을 사용합니다.
   - LUN은 초기화되지 *말아야* 하며 **디스크 관리**에 "오프라인" 디스크로 표시되어야 합니다. Windows가 LUN을 초기화하면 손상되고 VMware vSphere에서 읽지 못하게 될 수 있습니다.

따라서 에이전트는 SAN 전송 모드를 사용하여 가상 디스크에 액세스합니다. 즉, Windows에서 인식하지 않는 VMFS 파일 시스템을 식별하지 않고 iSCSI/FC에서 LUN 섹터를 읽습니다.

제한 사항

- VSphere 6.0 이상에서, VM 디스크 중 일부는 VVol(VMware Virtual Volume)에 위치하고 일부는 여기에 위치하지 않는 경우 에이전트가 SAN 전송 모드를 사용할 수 없습니다.이러한 가상 머신으로의 백업이 실패합니다.
- 에이전트에 대해 SAN 전송 모드를 구성하더라도 VMware vSphere 6.5에서 소개된 암호화된 가상 머신은 LAN을 통해 백업됩니다.VMware가 암호화된 가상 디스크 백업에 SAN 전송을 지원하지 않기 때문에 에이전트가 NBD 전송으로 폴백합니다.

© Acronis International GmbH, 2003-2024

예

ISCSI SAN을 사용하고 있는 경우 Agent for VMware가 설치된 Windows를 실행 중인 머신에 iSCSI 초기자를 구성합니다.

SAN 정책을 구성하려면

1. 관리자로 로그온하고 명령 프롬프트를 열고 `diskpart`를 입력한 다음, **Enter**를 누릅니다.
2. `san`을 입력한 다음, **Enter**를 누릅니다. **SAN 정책 : 모두 오프라인**이 표시됩니다.
3. SAN 정책의 다른 값이 설정된 경우:
   a. `san policy=offlineall`을 입력합니다.
   b. **Enter** 키를 누릅니다.
   c. 설정이 올바르게 적용되었는지 확인하려면 2단계를 수행합니다.
   d. 머신을 다시 시작합니다.

iSCSI 초기자를 구성하려면

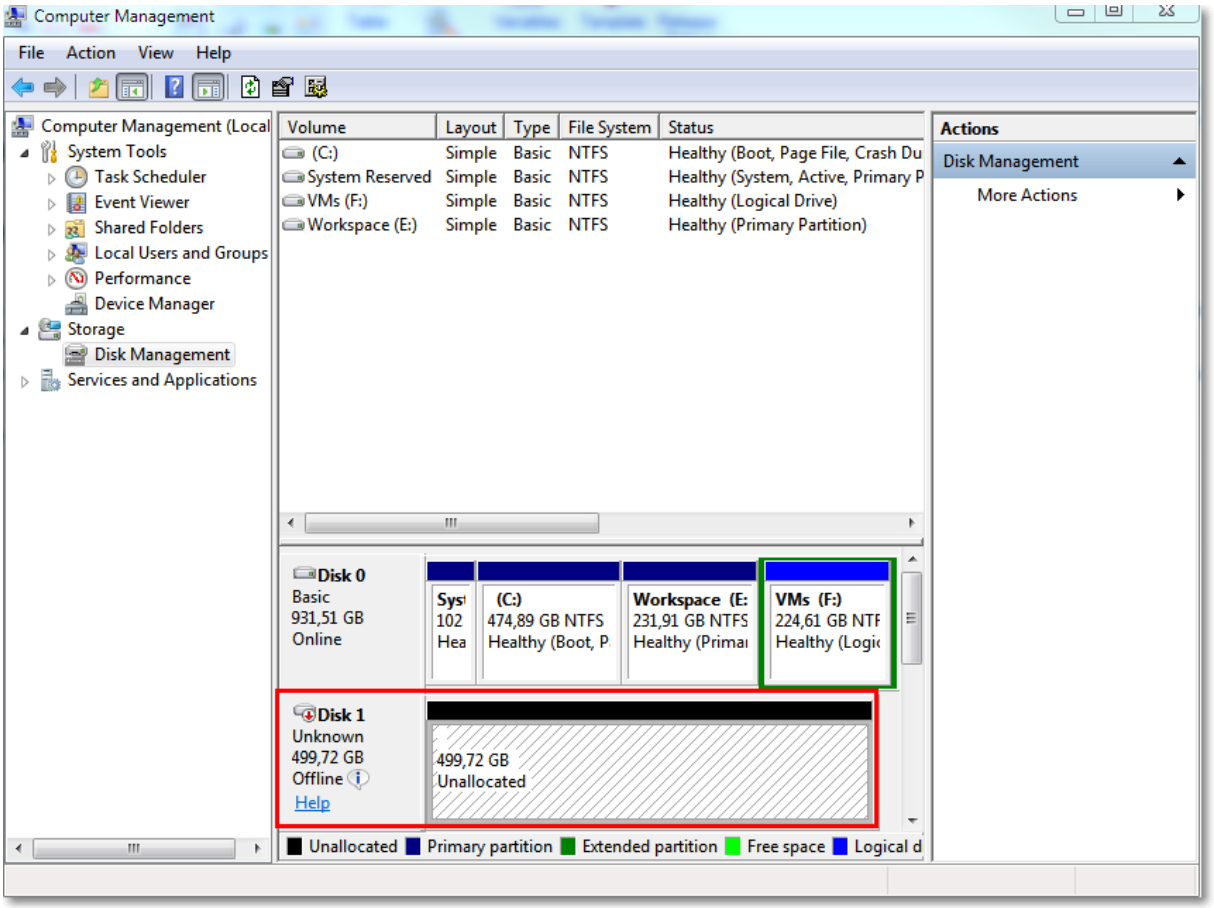
1. **제어판** > **관리 도구** > **iSCSI 초기자**로 이동합니다.

   참고
   관리 도구 애플릿을 찾으려면 **제어판** 보기를 **홈** 또는 **카테고리**가 아닌 다른 것으로 변경하거나 검색을 사용해야 할 수 있습니다.

2. Microsoft iSCSI 초기자를 처음 실행하는 경우라면 Microsoft iSCSI 초기자 서비스를 시작하길 원한다고 확인하십시오.
3. **대상** 탭에서 대상 SAN 장치의 FQDN(정규화된 도메인 이름) 또는 IP 주소를 입력한 다음 **빠른 연결**을 클릭합니다.
4. 데이터 저장소를 호스팅하는 LUN을 선택한 다음 **연결**을 클릭합니다.
   LUN이 표시되지 않는 경우 iSCSI 대상의 조닝(zoning)이 에이전트를 실행 중인 머신에서 LUN에 액세스할 수 있도록 활성화되어 있는지 확인하십시오. 해당 머신이 이 대상에 대해 허용된 iSCSI 초기자 목록에 추가되어야 합니다.
5. **확인**을 클릭합니다.

아래 스크린샷에 표시된 바와 같이 준비된 SAN LUN이 **디스크 관리**에 나타납니다.

© Acronis International GmbH, 2003-2024



로컬로 연결된 스토리지 사용

Agent for VMware(가상 어플라이언스)에 추가 디스크를 연결하여 로컬로 연결된 이 스토리지에 에이전트를 백업할 수 있습니다. 이 접근법은 에이전트와 백업 위치 간 네트워크 트래픽을 없애줍니다.

백업된 가상 머신과 같은 호스트 또는 클러스터에서 실행 중인 가상 어플라이언스는 해당 머신이 존재하는 데이터 저장소에 대한 직접 액세스 권한을 가집니다. 즉, 이 어플라이언스는 HotAdd 전송을 사용하여 백업된 디스크에 연결할 수 있고, 따라서 백업 트래픽이 하나의 로컬 디스크에서 다른 디스크로 향하게 됩니다. 데이터 저장소가 **NFS**가 아닌 **Disk/LUN**으로 연결되어 있는 경우 백업은 완전한 LAN 프리 백업이 됩니다. NFS 데이터 저장소의 경우에는 데이터 저장소와 호스트 간에 네트워크 트래픽이 발생합니다.

로컬로 연결된 스토리지를 사용하는 경우에는 에이전트가 항상 동일한 머신을 백업하는 것으로 가정합니다. vSphere에서 여러 에이전트가 작동하고 그중 하나 이상이 로컬로 연결된 스토리지를 사용하는 경우에는 각 에이전트를 백업해야 하는 모든 머신을 수동으로 결합해야 합니다. 그렇지 않고 관리 서버가 에이전트에 머신을 다시 배포하면 머신 백업이 여러 스토리지에 분산될 수 있습니다.

스토리지는 이미 작동 중인 에이전트에 추가할 수도 있고, OVF 템플릿에서 가져온 에이전트를 디플로이할 때 추가할 수도 있습니다.

스토리지를 이미 작동 중인 에이전트에 연결하려면

© Acronis International GmbH, 2003-2024

1. VMware vSphere 인벤토리에서 Agent for VMware(가상 어플라이언스)를 마우스 오른쪽 버튼으로 클릭합니다.
2. 가상 머신의 설정을 편집하여 디스크를 추가합니다. 디스크 크기는 10GB 이상이어야 합니다.

   경고!
   기존 디스크는 조심스럽게 추가합니다. 스토리지가 생성되면 이전에 이 디스크에 포함된 모든 데이터를 잃게 됩니다.

3. 가상 어플라이언스 콘솔로 이동합니다. 화면 하단에 **스토리지 생성** 링크가 나타납니다. 링크가 나타나지 않으면 **새로 고침**을 클릭합니다.
4. **스토리지 생성** 링크를 클릭하고 디스크를 선택한 다음 디스크 레이블을 지정합니다. 레이블 길이는 파일 시스템 제한에 따라 16자로 제한됩니다.

로컬로 연결된 스토리지를 백업 대상으로 선택하려면

- 보호 계획을 생성할 경우 **백업할 위치**에서 **로컬 폴더**를 선택하고 로컬로 연결된 스토리지에 해당하는 문자(예: **D:**)를 입력합니다.

참고
LAS(로컬 연결 스토리지)는 에이전트(가상 어플라이언스)가 하나인 비교적 규모가 작은 환경용입니다. 로컬 연결 스토리지 단위 테스트는 5TB 크기까지 완료되었습니다. 위험을 감수하고 이보다 더 큰 디스크를 연결할 수도 있지만 해당 구성은 지원되지 않습니다. 백업 데이터가 5TB보다 크다면 다른 유형의 스토리지를 사용하는 것이 좋습니다. 예를 들어 VMware 가상 디스크를 생성하여 임의의 가상 머신에 연결한 후 해당 디스크에 네트워크 공유를 생성할 수 있습니다. 그러면 LAS 대신 해당 디스크가 백업 대상으로 사용됩니다.

가상 머신 결합

이 섹션은 Cyber Protection 서비스가 VMware vCenter에서 여러 에이전트의 작업을 구성하는 방법에 대한 개요를 제공합니다.

아래 배포 알고리즘은 Windows에 설치된 가상 어플라이언스와 에이전트에 모두 적용됩니다.

배포 알고리즘

가상 머신이 Agent for VMware 간에 균일하게 배포됩니다. 균일이란 각 에이전트가 동일한 수의 머신을 관리함을 의미합니다. 가상 머신이 점유하는 저장 공간의 크기는 계산하지 않습니다.

그러나 머신의 에이전트를 선택하는 경우 소프트웨어는 전체 시스템 성능을 최적화하려고 시도합니다. 특히 소프트웨어는 에이전트와 가상 머신 위치를 고려합니다. 동일한 호스트에서 호스팅되는 에이전트를 선호합니다. 동일한 호스트에 에이전트가 없는 경우에는 동일한 클러스터의 에이전트를 선호합니다.

가상 머신이 에이전트에 할당되면 이 머신의 모든 백업이 해당 에이전트에 위임됩니다.

© Acronis International GmbH, 2003-2024

재배포

재배포는 설정된 균형이 깨질 때마다 또는 보다 정확하게는 에이전트 간 로드 불균형이 20%에 도달할 때마다 수행됩니다. 이는 머신 또는 에이전트가 추가 또는 제거되거나 머신이 다른 호스트 또는 클러스터로 마이그레이션되거나 머신을 에이전트에 수동으로 결합하는 경우 해당됩니다. 이러한 경우에는 Cyber Protection 서비스가 동일한 알고리즘을 사용하여 머신을 재배포합니다.

예를 들어, 처리량 문제로 에이전트가 더 필요하다고 판단하여 클러스터에 추가 가상 어플라이언스를 디플로이할 수 있습니다. Cyber Protection 서비스는 새 에이전트에 가장 적합한 머신을 할당합니다. 이전 에이전트의 로드는 감소합니다.

Cyber Protection 서비스에서 에이전트를 제거하는 경우 에이전트에 할당된 머신은 나머지 에이전트에 배포됩니다. 그러나 에이전트가 손상되거나 vSphere에서 수동으로 삭제된 경우에는 머신이 분산되지 않습니다. 재배포는 웹 인터페이스에서 해당 에이전트를 제거한 후에만 시작됩니다.

배포 결과 보기

다음 위치에서 자동 배포의 결과를 볼 수 있습니다.

- **모든 장치** 섹션의 각 가상 머신에 대한 **에이전트** 열
- 에이전트가 **설정** > **에이전트** 섹션에서 선택된 경우 **상세정보** 패널의 **할당된 가상 머신** 섹션

수동 결합

Agent for VMware 결합을 사용하면 이 머신을 항상 백업해야 하는 에이전트를 지정하여 이 배포 프로세스에서 가상 머신을 제외할 수 있습니다. 전체적인 균형은 유지되지만 이 특정 머신은 원래 에이전트가 제거된 경우에만 다른 에이전트로 전달될 수 있습니다.

머신과 에이전트를 결합하려면

1. 머신을 선택합니다.
2. **상세정보**를 클릭합니다.
   할당된 에이전트 섹션에는 선택한 머신을 현재 관리하는 에이전트가 표시됩니다.
3. **변경**을 클릭합니다.
4. **수동**을 선택합니다.
5. 머신을 결합할 에이전트를 선택합니다.
6. **저장**을 클릭합니다.

머신과 에이전트의 결합을 해제하려면

1. 머신을 선택합니다.
2. **상세정보**를 클릭합니다.
   할당된 에이전트 섹션에는 선택한 머신을 현재 관리하는 에이전트가 표시됩니다.
3. **변경**을 클릭합니다.
4. **자동**을 선택합니다.
5. **저장**을 클릭합니다.

© Acronis International GmbH, 2003-2024

에이전트에 대한 자동 할당 비활성화

Agent for VMware가 백업해야 하는 머신 목록을 지정하는 방식으로 이 에이전트에 대한 자동 할당을 비활성화하여 배포 프로세스에서 제외할 수 있습니다. 다른 에이전트 간에 전체적인 균형이 유지됩니다.

다른 등록된 에이전트가 없거나 다른 모든 에이전트에 대한 자동 할당이 비활성화된 경우에는 에이전트에 대한 자동 할당을 비활성화할 수 없습니다.

에이전트에 대한 자동 할당을 비활성화하려면

1. **설정** > **에이전트**를 클릭합니다.
2. 자동 할당을 비활성화할 Agent for VMware를 선택합니다.
3. **상세정보**를 클릭합니다.
4. **자동 할당** 스위치를 비활성화합니다.

사용 예제

- 특정(대규모) 머신을 Agent for VMware(Windows)에서 파이버 채널을 통해 백업하고 다른 머신은 가상 어플라이언스에서 백업하는 경우 수동 결합이 유용합니다.
- 에이전트에 로컬로 연결된 스토리지가 있는 경우 VM을 에이전트에 결합해야 합니다.
- 자동 할당을 비활성화하면 특정 머신을 지정한 스케줄에 따라 예상대로 백업할 수 있습니다. VM을 하나만 백업하는 에이전트는 스케줄된 시간이 되면 다른 VM을 백업하는 데 사용할 수 없습니다.
- 지리적으로 떨어진 여러 ESXi 호스트가 있는 경우 자동 할당을 비활성화하는 것이 좋습니다. 자동 할당을 비활성화하고 각 호스트의 VM을 같은 호스트에서 실행 중인 에이전트에 결합하면, 에이전트가 원격 ESXi 호스트에서 실행 중인 머신을 백업하지 않으므로 네트워크 트래픽을 절약할 수 있습니다.

정지 전 및 해제 후 스크립트 자동 실행

VMware Tools를 사용하면 에이전트 없는 모드에서 백업하는 가상 머신에서 사용자 정의 정지 전 스크립트 및 해제 후 스크립트를 자동으로 실행할 수 있습니다. 예를 들어 사용자 정의 정지 스크립트를 실행하여 VSS 미인식 애플리케이션을 실행하는 가상 머신용으로 애플리케이션 일치 백업을 생성할 수 있습니다.

사전 요구 사항

가상 머신의 특정 폴더에 정지 전 및 해제 후 스크립트가 있어야 합니다.

- Windows 가상 머신의 경우 이 폴더의 위치는 호스트의 ESXi 버전에 따라 달라집니다.
  예를 들어 ESXi 6.5 호스트를 실행하는 가상 머신의 경우 이 폴더는 `C:\Program Files\VMware\VMware Tools\backupScripts.d\`입니다. `backupScritps.d` 폴더는 수동으로 생성해야 합니다.이 폴더에는 다른 유형의 파일을 저장하지 마십시오. 다른 유형의 파일을 저장하면 VMware Tools가 불안정해질 수 있습니다.

© Acronis International GmbH, 2003-2024

다른 ESXi 버전용 정지 전 및 해제 후 스크립트의 위치와 관련된 자세한 내용은 VMware 설명서를 참조하십시오.

- Linux 가상 머신의 경우에는 `/usr/sbin/pre-freeze-script` 및 `/usr/sbin/post-thaw-script` 디렉터리에 정지 전 스크립트와 해제 후 스크립트를 각각 복사합니다. `/usr/sbin/pre-freeze-script`의 스크립트는 스냅샷 생성 시에 실행되며 `/usr/sbin/post-thaw-script`의 스크립트는 스냅샷 완성 시에 실행됩니다. VMware Tools 사용자가 스크립트를 실행할 수 있어야 합니다.

정지 전 및 해제 후 스크립트를 자동 실행하려면

1. 가상 머신에 VMware Tools가 설치되어 있는지 확인합니다.
2. 가상 머신의 필요한 폴더에 사용자 정의 스크립트를 저장합니다.
3. 해당 머신의 보호 계획에서 **가상 머신용 VSS(Volume Shadow Copy Service)** 옵션을 활성화합니다.

   그러면 **게스트 파일 시스템 정지** 옵션이 활성화된 VMware 스냅샷이 생성됩니다. 이 스냅샷이 생성되면 가상 머신 내에서 정지 전 및 해제 후 스크립트가 트리거됩니다.

Microsoft SQL Server, Microsoft Exchange 등 VSS를 인식하는 애플리케이션을 실행 중인 가상 머신에서는 사용자 정의 정지 스크립트를 실행할 필요가 없습니다. 이러한 머신용으로 애플리케이션 일치 백업을 생성하려면 보호 계획에서 **가상 머신용 VSS(Volume Shadow Copy Service)** 옵션을 활성화합니다.

가상 머신 마이그레이션 지원

이 섹션에는 vSphere 클러스터의 일부인 ESXi 호스트 간의 마이그레이션을 포함하여 vSphere 환경 내의 가상 머신 마이그레이션에 대한 정보가 포함되어 있습니다.

vMotion을 사용하면 가상 머신의 상태와 구성을 다른 호스트로 이동할 수 있으며 머신의 디스크는 공유 스토리지의 동일한 위치에 유지됩니다. Storage vMotion을 사용하면 가상 머신의 디스크를 한 데이터 저장소에서 다른 데이터 저장소로 이동할 수 있습니다.

- Storage vMotion을 포함한 vMotion을 사용한 마이그레이션은 Agent for VMware(가상 어플라이언스)를 실행하는 가상 머신에 대해 지원되지 않으며 자동으로 비활성화됩니다. 이 가상 머신은 vSphere 클러스터 구성의 **VM 재정의** 목록에 추가됩니다.
- 가상 머신의 백업이 시작되면 Storage vMotion을 포함한 vMotion을 사용한 마이그레이션이 자동으로 비활성화됩니다. 이 가상 머신은 vSphere 클러스터 구성의 **VM 재정의** 목록에 임시로 추가됩니다. 백업이 완료되면 **VM 재정의** 설정이 자동으로 이전 상태로 되돌아갑니다.
- Storage vMotion을 포함하여 vMotion을 사용한 마이그레이션이 진행 중인 동안에는 가상 머신에 대한 백업을 시작할 수 없습니다. 마이그레이션이 완료되면 이 머신에 대한 백업이 시작됩니다.

가상화 환경 관리

vSphere, Hyper-V 및 Virtuozzo 환경을 각각의 네이티브 표시로 볼 수 있습니다. 해당 에이전트가 설치 및 등록되어 있으면 **VMware**, **Hyper-V** 또는 **Virtuozzo** 탭이 **장치** 아래에 표시됩니다.

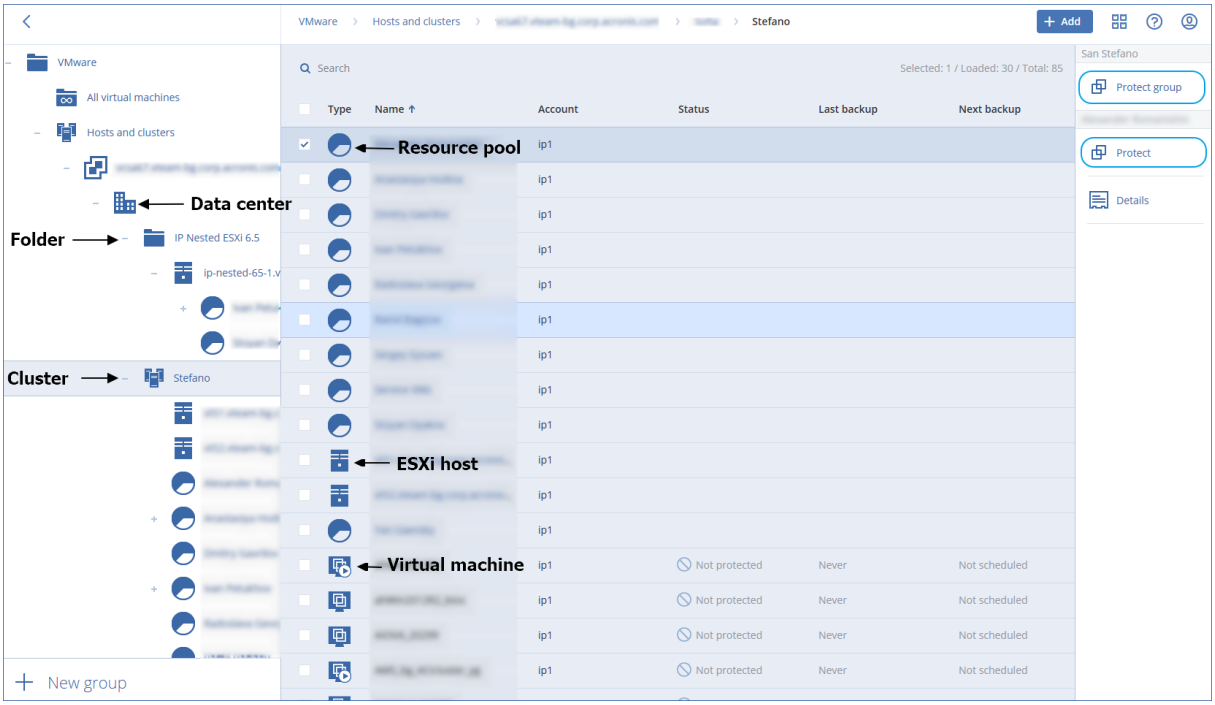
VMware 탭에서 다음과 같은 vSphere 인프라 개체를 백업할 수 있습니다.

© Acronis International GmbH, 2003-2024

- 데이터 센터
- 폴더
- 클러스터
- ESXi 호스트
- 리소스 풀

이러한 인프라 객체 각각은 가상 머신에 대한 그룹 객체로 작동합니다. 이러한 그룹 객체에 보호 계획을 적용할 때 그 안에 포함된 모든 가상 머신이 백업됩니다. **보호**를 클릭하여 선택된 그룹 머신을 백업하거나 **그룹 보호**를 클릭하여 선택된 그룹이 포함된 부모 그룹 머신을 백업할 수 있습니다.

예를 들어 Stefano 클러스터를 선택한 후 그 안의 리소스 풀을 선택했다고 가정해 보겠습니다. **보호**를 클릭하면 선택된 리소스 풀에 포함된 모든 가상 머신이 백업됩니다. **그룹 보호**를 클릭하면 Stefano 클러스터에 포함된 모든 가상 머신이 백업됩니다.



VMware 탭에서는 에이전트를 다시 설치하지 않고 vCenter Server 또는 독립형 ESXi 호스트에 대한 액세스 자격 증명을 변경할 수 있습니다.

vCenter Server 또는 ESXi 호스트 액세스 자격 증명을 변경하려면

1. **장치**에서 **VMware**를 클릭합니다.
2. **호스트 및 클러스터**를 클릭합니다.
3. **호스트 및 클러스터** 트리의 오른쪽에 있는 **호스트 및 클러스터** 목록에서 Agent for VMware 설치 중 지정한 vCenter Server 또는 독립형 ESXi 호스트를 선택합니다.
4. **상세정보**를 클릭합니다.
5. **자격 증명**에서 사용자 이름을 클릭합니다.
6. 새 액세스 자격 증명을 지정한 다음 **확인**을 클릭합니다.

© Acronis International GmbH, 2003-2024

vSphere Client에서 백업 상태 보기

vSphere Client에서 가상 머신의 마지막 백업 시간과 백업 상태를 볼 수 있습니다.

이 정보는 가상 머신 요약(**요약** > **사용자 정의 속성/주석/메모**, 클라이언트 유형 및 vSphere 버전에 따라 달라짐)에 나타납니다. 모든 호스트, 데이터센터, 폴더, 리소스 풀 또는 전체 vCenter Server의 **가상 머신** 탭에서 **마지막 백업** 및 **백업 상태** 열을 활성화할 수도 있습니다.

이러한 속성을 제공하려면 Agent for VMware에는 "Agent for VMware - 필수 권한"에 설명된 권한 외에 다음과 같은 권한이 있어야 합니다.

- **글로벌** > **사용자 정의 속성 관리**
- **글로벌** > **사용자 정의 속성 설정**

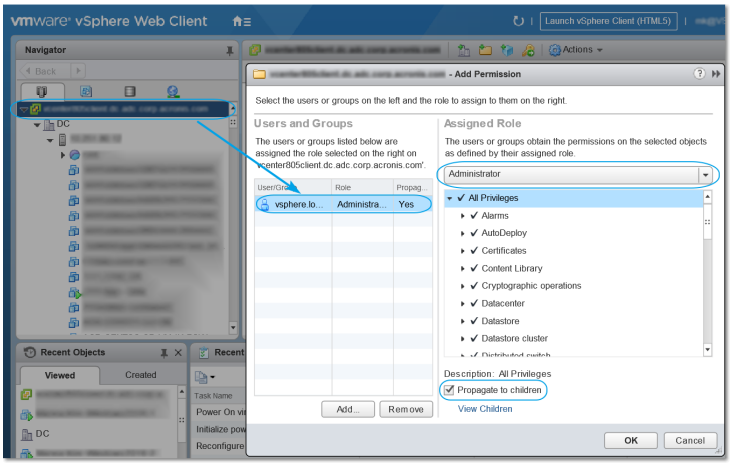
Agent for VMware - 필수 권한

가상 머신, ESXi 호스트, 클러스터, vCenter 같은 vCenter 객체를 사용하여 작업을 수행하기 위해, VMware용 에이전트는 사용자가 제공한 vSphere 자격 증명을 사용하여 vCenter 또는 ESXi 호스트에서 인증합니다. VMware용 에이전트에 의한 vSphere로의 연결에 사용된 vSphere 계정에는 vCenter 수준부터 모든 vSphere 인프라 수준에 대해 필요한 권한이 있어야 합니다.

Agent for VMware를 설치하거나 구성하는 동안 vSphere 계정에 필수 권한을 지정합니다. 나중에 계정을 변경해야 하는 경우 "가상화 환경 관리"(633페이지)을(를) 참조하십시오.

vCenter 수준에서 vSphere 사용자에게 권한을 할당하려면

1. vSphere 웹 클라이언트에 로그인합니다.
2. vCenter를 마우스 오른쪽 버튼으로 클릭한 다음, **권한 추가**를 클릭합니다.
3. 필요한 역할을 가진 새 사용자를 선택하거나 추가합니다(역할은 아래 표의 모든 필수 권한을 포함해야 합니다).
4. **자식에 전파** 옵션을 선택합니다.



© Acronis International GmbH, 2003-2024

객체	권한	작업			
		VM 백업	머신 추가	기존의 VM으로 복구	백업에서 VM 실행
암호화 동작 (vSphere 6.5부터 시작)	디스크 추가	+*			
	직접 액세스	+*			
데이터 저장소	공간 할당		+	+	+
	데이터 저장소 찾기				+
	데이터 저장소 구성	+	+	+	+
	낮은 수준의 파일 작업				+
글로벌	라이센스	+	+	+	+
	방법 비활성화	+	+	+	
	방법 활성화	+	+	+	
	사용자 정의 속성 관리	+	+	+	
	사용자 정의 속성 설정	+	+	+	
호스트 > 구성	저장소 파티션 구성				+
호스트 > 로컬 작업	VM 생성				+
	VM 삭제				+
	VM 재구성				+
네트워크	네트워크 할당		+	+	+
리소스	VM을 리소스 풀로 할당		+	+	+
가상 머신 > 구성	기존의 디스크 추가	+	+		+
	새 디스크 추가		+	+	+
	장치 추가 또는 제거		+		+
	고급	+	+	+	
	CPU 개수 변경		+		
	디스크 변경 추적	+		+	
	디스크 임대	+		+	
	메모리		+		

© Acronis International GmbH, 2003-2024

	디스크 제거	+	+	+	+
	이름 변경		+		
	주석 설정				+
	설정		+	+	+
가상 머신 > 게스트 작업	게스트 작업 프로그램 실행	+**			
	게스트 작업 쿼리	+**			
	게스트 작업 수정	+**			
가상 머신 > 상호 작용	게스트 제어 티켓 획득 (vSphere 4.1 및 5.0)				+
	CD 미디어 구성		+	+	
	VIX API의 게스트 운영 체제 관리(vSphere 5.1 이상)				+
	전원 끄기			+	+
	전원 켜기		+	+	+
가상 머신 > 인벤토리	기존 항목에서 생성		+	+	+
	새로 만들기		+	+	+
	등록				+
	제거		+	+	+
	등록 해제				+
가상 머신 > 프로비저닝	디스크 액세스 허용		+	+	+
	읽기 전용 디스크 액세스 허용	+		+	
	가상 머신 다운로드 허용	+	+	+	+
가상 머신 > 상태 가상 머신 > 스냅샷 관리 (vSphere 6.5 이상)	스냅샷 생성	+		+	+
	스냅샷 제거	+		+	+
vApp	가상 머신 추가				+

* 암호화된 머신 백업에만 이 권한이 필요합니다.

** 애플리케이션 인식 백업에만 이 권한이 필요합니다.

© Acronis International GmbH, 2003-2024

클러스터 Hyper-V 머신 백업

Hyper-V 클러스터에서는 가상 머신이 클러스터 노드 간에 마이그레이션될 수 있습니다. 클러스터 Hyper-V 머신의 올바른 백업을 설정하려면 이 권장 사항을 따릅니다.

1. 어떤 노드로 마이그레이션되었는지에 상관없이 머신을 백업에 사용할 수 있어야 합니다. Agent for Hyper-V가 모든 노드에 있는 머신에 액세스할 수 있도록 보장하려면 에이전트 서비스가 각각의 클러스터 노드에서 관리자 권한을 가진 도메인 사용자 계정에서 실행되어야 합니다. Agent for Hyper-V 설치 중 에이전트 서비스에 대해 그러한 계정을 지정하는 것이 권장됩니다.
2. 클러스터의 각 노드에 Agent for Hyper-V를 설치합니다.
3. Cyber Protection 서비스에 모든 에이전트를 등록합니다.

복구된 머신의 고가용성

백업된 디스크를 *기존* Hyper-V 가상 머신에 복구하는 경우 머신의 고가용성 특성은 그대로 유지됩니다.

백업된 디스크를 *새* Hyper-V 가상 머신으로 복구하는 경우에는 결과 머신이 고가용성 상태가 되지 않습니다. 해당 머신은 예비 머신으로 간주되며 일반적으로 전원이 꺼져 있습니다. 머신을 운영 환경에서 사용해야 하는 경우에는 **장애 조치 클러스터 관리** 스냅인에서 고가용성에 맞게 구성할 수 있습니다.

동시 백업되는 가상 머신의 총 수를 제한합니다.

일정 예약 백업 옵션에서 보호 계획당 동시 백업되는 가상 머신 수를 제한할 수 있습니다.

에이전트가 여러 계획을 동시에 실행하면 동시 백업되는 머신 수가 늘어납니다. 이 경우 백업 성능 영향을 줄 수 있으며 호스트와 가상 머신 스토리지에 과부하가 발생할 수 있습니다. 에이전트 수준에서 제한을 구성하면 이러한 문제를 방지할 수 있습니다.

에이전트 수준에서 동시 백업 수를 제한하려면

Agent for VMware(Windows)

1. 에이전트가 설치된 머신에서 새 텍스트 문서를 생성해 텍스트 편집기에서 엽니다.
2. 다음 라인을 복사하여 파일에 붙여넣습니다.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. `00000001`을 설정하려는 제한의 16진수 값으로 대체합니다.
   예를 들어, `00000001`은 1이고 `0000000A`는 10입니다.
4. 문서를 **limit.reg**로 저장합니다.
5. 이 파일을 관리자로 실행합니다.

© Acronis International GmbH, 2003-2024

6. Windows 레지스트리를 편집할 것인지 확인합니다.
7. 에이전트를 다시 시작합니다.
   a. **시작** 메뉴에서 **실행**을 클릭합니다.
   b. **cmd**를 입력하고 **확인**을 클릭합니다.
   c. 명령줄에서 다음 명령을 실행합니다.

```
net stop mms
net start mms
```

Agent for Hyper-V

1. 에이전트가 설치된 머신에서 새 텍스트 문서를 생성해 텍스트 편집기에서 엽니다.
2. 다음 라인을 복사하여 파일에 붙여넣습니다.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. `00000001`을 설정하려는 제한의 16진수 값으로 대체합니다.
   예를 들어, `00000001`은 1이고 `0000000A`는 10입니다.
4. 문서를 **limit.reg**로 저장합니다.
5. 이 파일을 관리자로 실행합니다.
6. Windows 레지스트리를 편집할 것인지 확인합니다.
7. 에이전트를 다시 시작합니다.
   a. **시작** 메뉴에서 **실행**을 클릭합니다.
   b. **cmd**를 입력하고 **확인**을 클릭합니다.
   c. 명령줄에서 다음 명령을 실행합니다.

```
net stop mms
net start mms
```

가상 어플라이언스

이 절차는 Agent for VMware(가상 어플라이언스), Agent for Scale Computing, Agent for Virtuozzo Hybrid Infrastructure 및 Agent for oVirt에 적용됩니다.

1. 가상 어플라이언스의 콘솔에서 Ctrl+Shift+F2를 눌러 명령줄 인터페이스를 엽니다.
2. 텍스트 편집기에서 `/etc/Acronis/MMS.config` 파일을 엽니다.
3. 다음 섹션을 찾습니다.

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. `10`을 설정하려는 동시 백업의 최대 수로 바꿉니다.

© Acronis International GmbH, 2003-2024

5. 파일을 저장합니다.
6. reboot 명령을 실행하여 에이전트를 다시 시작합니다.

머신 이주

머신의 백업을 원래 머신이 아닌 머신으로 복구하여 머신 이주를 수행할 수 있습니다.

다음 표가 이용 가능한 마이그레이션 방법을 요약하고 있습니다.

백업된 머신 유형	이용 가능한 복구 목적지							
	실제 머신	ESXi 가상 머신	Hyper-V 가상 머신	Virtuozzo		Virtuozzo 하이브리드 인프라 가상 머신	Scale Computing HC3 가상 머신	RHV/oVirt 가상 머신
				가상 머신	컨테이너			
실제 머신	+	+	+	-	-	+	+*	+
VMware ESXi 가상 머신	+	+	+	-	-	+	+*	+
Hyper-V 가상 머신	+	+	+	-	-	+	+*	+
Virtuozzo 가상 머신	+	+	+	+	-	+	+*	+
Virtuozzo 컨테이너	-	-	-	-	+	-	-	-
Virtuozzo Hybrid Infrastructure 가상 머신	+	+	+	-	-	+	+*	+
Scale Computing HC3 가상 머신	+	+	+	-	-	+	+	+
Red Hat Virtualization/oVirt 가상 머신	+	+	+	-	-	+	+*	+

*원본 머신에서 보안 부팅이 활성화되어 있는 경우 복구 후에 VM 콘솔에서 보안 부팅을 비활성화하지 않으면 복구된 VM이 시작되지 않습니다.

© Acronis International GmbH, 2003-2024

참고
Hyper-V는 macOS를 지원하지 않으므로 macOS 가상 머신을 Hyper-V 호스트에 복구할 수 없습니다. macOS 가상 머신은 Mac 하드웨어에 설치된 VMware 호스트에 복구할 수 있습니다.

마이그레이션 작업을 수행하는 방법에 대한 자세한 내용은 다음 항목을 참조하십시오.

- P2V(실제에서 가상으로) 마이그레이션의 경우 "실제 머신에서 가상 머신으로"(457페이지) 항목을 참조하십시오.
- V2V(가상에서 가상으로) 마이그레이션의 경우 "가상 머신 복구가상 머신을 백업에서 복구할 수 있습니다.규제 준수 모드 상태인 테넌트의 경우에는 Cyber Protect 콘솔에서 백업을 복구할 수 없습니다. 이러한 백업을 복구하는 방법에 대한 자세한 내용은 "규제 준수 모드로 설정된 테넌트의 백업 복구"(1페이지) 항목을 참조하십시오.사전 요구 사항이 머신으로 복구 중에는 가상 머신을 중지해야 합니다. 기본적으로 소프트웨어는 메시지를 표시하지 않고 머신을 중지합니다. 복구가 완료되면 머신을 수동으로 시작해야 합니다. VM 전원 관리 복구 옵션(복구 옵션 > VM 전원 관리 클릭)을 사용하여 기본 동작을 변경할 수 있습니다.절차다음 중 하나를 수행하십시오. 백업된 머신을 선택하고 복구를 클릭한 다음 복구 지점을 선택합니다.백업 스토리지 탭에서 복구 지점을 선택합니다.복구 > 전체 머신을 클릭합니다.실제 머신으로 복구하려면 복구 대상에서 실제 머신을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.대상 머신의 디스크 구성이 백업의 디스크 구성과 정확하게 일치하는 경우에만 실제 머신으로 복구가 가능합니다.이 경우 "실제 머신"의 4단계로 계속 진행합니다. 그렇지 않은 경우에는 부트 가능한 미디어 사용으로 V2P 마이그레이션을 수행하는 것이 좋습니다.[선택 사항] 기본적으로 원래 머신이 대상 머신으로 자동으로 선택됩니다. 다른 가상 머신으로 복구하려면 대상 머신을 클릭한 후 다음을 수행합니다.하이퍼바이저(VMware ESXi, Hyper-V, Virtuozzo, Virtuozzo Hybrid Infrastructure, Scale Computing HC3 또는 oVirt)를 선택합니다.Virtuozzo 가상 머신만 Virtuozzo로 복구할 수 있습니다. V2V 이주에 대한 자세한 내용은 "머신 이주"를 참조하십시오.새 머신 또는 기존 머신으로 복구할지 선택합니다.호스트를 선택하고 새 머신 이름을 지정하거나 기존 대상 머신을 선택합니다.확인을 클릭합니다.필요한 추가 복구 옵션을 설정합니다.[Virtuozzo Hybrid Infrastructure 및 Scale Computing HC3에서는 사용 불가] 가상 머신의 데이터 저장소를 선택하려면, ESXi의 경우 데이터 저장소를, Hyper-V 및 Virtuozzo의 경우 경로를, Red Hat Virtualization(oVirt)의 경우에는 스토리지 도메인을 클릭한 다음 가상 머신의 데이터 저장소(스토리지)를 선택합니다.각 가상 디스크에 대한 데이터 저장소(스토리지), 인터페이스, 프로비저닝 모드를 보려면 디스크 매핑을 클릭합니다. Virtuozzo 컨테이너 또는 Virtuozzo Hybrid Infrastructure 가상 머신을 복구하는 것이 아닌 한 이 설정을 변경할 수 있습니다.Virtuozzo Hybrid Infrastructure의 경우, 대상 디스크의 스토리지 정책만 선택할 수 있습니다. 이 작업을 수행하려면 대상 디스크를 선택하고 변경을 클릭합니다. 날개가 열리면 기어 아이콘을 클릭하고 완료를 클릭합니다.매핑 섹션을 사용하여 복구용 개별 디스크를 선택할 수도 있습니다.[VMware ESXi, Hyper-V, Virtuozzo에 사용 가능] 가상 머신의 메모리 크기, 프로세서 수 및 네트워크 연결을 변경하려면 VM 설정을 클릭합니다. [Virtuozzo Hybrid Infrastructure의 경우] 가상 머신의 메모리 크기 및 프로세서 수를 변경하려면 선호 방식을 선택합니다.[보호 에이전트가 설치된 Windows 머신에서만 사용 가능] 맬웨어가 없는 데이터만 복구되도록 하려면 안전 복구 스위치를 활성화하십시오. 안전 복구의 작동 방식에 대한 자세한 내용은 "안전 복구"(1페이지) 항목을 참조하십시오.복구 시작을 클릭합니다.기존 가상 머신으로 복구하는 경우 디스크를 덮어쓸지 확인합니다.복구 진행률이 작업 탭에 표시됩니다."(1페이지) 항목을 참조하십시오.

© Acronis International GmbH, 2003-2024

- V2P(가상에서 실제로) 마이그레이션의 경우 "가상 머신 복구가상 머신을 백업에서 복구할 수 있습니다.규제 준수 모드 상태인 테넌트의 경우에는 Cyber Protect 콘솔에서 백업을 복구할 수 없습니다. 이러한 백업을 복구하는 방법에 대한 자세한 내용은 "규제 준수 모드로 설정된 테넌트의 백업 복구"(1페이지) 항목을 참조하십시오.사전 요구 사항이 머신으로 복구 중에는 가상 머신을 중지해야 합니다. 기본적으로 소프트웨어는 메시지를 표시하지 않고 머신을 중지합니다. 복구가 완료되면 머신을 수동으로 시작해야 합니다. VM 전원 관리 복구 옵션(복구 옵션 > VM 전원 관리 클릭)을 사용하여 기본 동작을 변경할 수 있습니다.절차다음 중 하나를 수행하십시오.백업된 머신을 선택하고 복구를 클릭한 다음 복구 지점을 선택합니다.백업 스토리지 탭에서 복구 지점을 선택합니다.복구 > 전체 머신을 클릭합니다.실제 머신으로 복구하려면 복구 대상에서 실제 머신을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.대상 머신의 디스크 구성이 백업의 디스크 구성과 정확하게 일치하는 경우에만 실제 머신으로 복구가 가능합니다.이 경우 "실제 머신"의 4단계로 계속 진행합니다. 그렇지 않은 경우에는 부트 가능한 미디어 사용으로 V2P 마이그레이션을 수행하는 것이 좋습니다.[선택 사항] 기본적으로 원래 머신이 대상 머신으로 자동으로 선택됩니다. 다른 가상 머신으로 복구하려면 대상 머신을 클릭한 후 다음을 수행합니다. 하이퍼바이저(VMware ESXi, Hyper-V, Virtuozzo, Virtuozzo Hybrid Infrastructure, Scale Computing HC3 또는 oVirt)를 선택합니다.Virtuozzo 가상 머신만 Virtuozzo로 복구할 수 있습니다. V2V 이주에 대한 자세한 내용은 "머신 이주"를 참조하십시오.새 머신 또는 기존 머신으로 복구할지 선택합니다.호스트를 선택하고 새 머신 이름을 지정하거나 기존 대상 머신을 선택합니다.확인을 클릭합니다.필요한 추가 복구 옵션을 설정합니다.[Virtuozzo Hybrid Infrastructure 및 Scale Computing HC3에서는 사용 불가] 가상 머신의 데이터 저장소를 선택하려면, ESXi의 경우 데이터 저장소를, Hyper-V 및 Virtuozzo의 경우 경로를, Red Hat Virtualization(oVirt)의 경우에는 스토리지 도메인을 클릭한 다음 가상 머신의 데이터 저장소(스토리지)를 선택합니다.각 가상 디스크에 대한 데이터 저장소(스토리지), 인터페이스, 프로비저닝 모드를 보려면 디스크 매핑을 클릭합니다. Virtuozzo 컨테이너 또는 Virtuozzo Hybrid Infrastructure 가상 머신을 복구하는 것이 아닌 한 이 설정을 변경할 수 있습니다.Virtuozzo Hybrid Infrastructure의 경우, 대상 디스크의 스토리지 정책만 선택할 수 있습니다. 이 작업을 수행하려면 대상 디스크를 선택하고 변경을 클릭합니다. 날개가 열리면 기어 아이콘을 클릭하고 완료를 클릭합니다.매핑 섹션을 사용하여 복구용 개별 디스크를 선택할 수도 있습니다.[VMware ESXi, Hyper-V, Virtuozzo에 사용 가능] 가상 머신의 메모리 크기, 프로세서 수 및 네트워크 연결을 변경하려면 VM 설정을 클릭합니다.[Virtuozzo Hybrid Infrastructure의 경우] 가상 머신의 메모리 크기 및 프로세서 수를 변경하려면 선호 방식을 선택합니다.[보호 에이전트가 설치된 Windows 머신에서만 사용 가능] 맬웨어가 없는 데이터만 복구되도록 하려면 안전 복구 스위치를 활성화하십시오. 안전 복구의 작동 방식에 대한 자세한 내용은 "안전 복구"(1페이지) 항목을 참조하십시오.복구 시작을 클릭합니다.기존 가상 머신으로 복구하는 경우 디스크를 덮어쓸지 확인합니다.복구 진행률이 작업 탭에 표시됩니다."(1페이지) 및 "부트 가능한 미디어를 사용하여 디스크 복구"(461페이지) 항목을 참조하십시오.

부트 가능한 미디어를 통한 마이그레이션

Cyber Protect 콘솔에서 머신 마이그레이션을 수행하는 대신 부트 가능한 미디어를 사용하여 머신을 복구할 수 있습니다.

다음과 같은 경우에는 부트 가능한 미디어를 사용하는 것이 좋습니다.

© Acronis International GmbH, 2003-2024

- 기본적으로 지원되지 않는 마이그레이션을 수행하는 경우.

  예를 들어 실제 머신이나 Virtuozzo 이외의 가상 머신을 Virtuozzo 호스트의 Virtuozzo 가상 머신으로 복구하려는 경우 부트 가능한 미디어를 사용합니다.
- 논리 볼륨이 포함된 Linux 머신(LVM)의 마이그레이션을 수행하는 경우.

  Agent for Linux 또는 부트 가능한 미디어를 사용하여 백업을 생성한 다음 부트 가능한 미디어를 사용하여 백업을 복구합니다.
- 시스템 부팅 기능에 꼭 필요한 특정 하드웨어용 드라이버를 제공하려는 경우.

  필요한 드라이버를 사용할 수 있는 부트 가능한 미디어를 빌드합니다. 자세한 내용은 "Bootable Media Builder"(645페이지)을(를) 참조하십시오.

Microsoft Azure 및 Amazon EC2 가상 머신

Microsoft Azure 또는 Amazon EC2 가상 머신을 백업하려면 머신에 보호 에이전트를 설치합니다. 백업 및 복구 작업은 실제 머신과 동일합니다. 그럼에도 불구하고 머신 수 할당량을 설정할 때에는 가상 머신으로 계산됩니다.

실제 머신과의 차이점은 Microsoft Azure와 Amazon EC2 가상 머신을 부트 가능한 미디어에서 부팅할 수 없다는 것입니다. 새 Microsoft Azure 또는 Amazon EC2 가상 머신으로 복구해야 하는 경우 아래의 절차를 따르십시오.

참고

다음 복구 절차는 Microsoft Azure에서 실행하는 데 필요한 모든 드라이버가 기본적으로 포함되어 있는 머신의 백업(Azure VM, 로컬 Hyper-V 머신 또는 Windows Server 2016 이상의 원본 머신에서 생성된 백업)에만 적용됩니다. 플랫폼 간 복구의 경우에는 이 기술 자료 문서를 참조하십시오.

머신을 Microsoft Azure 또는 Amazon EC2 가상 머신으로 복구하려면

1. Microsoft Azure 또는 Amazon EC2의 이미지/템플릿에서 새 가상 머신을 생성합니다. 새 머신에는 복구하려는 머신과 동일한 디스크 구성이 있어야 합니다.
2. 새 머신에 Agent for Windows 또는 Agent for Linux를 설치합니다.
3. "실제 머신"에 설명된 대로 백업된 머신을 복구합니다. 복구를 구성할 때 새 머신을 대상 머신으로 선택합니다.

운영 체제 복구용으로 부트 가능한 미디어 생성

부트 가능한 미디어는 Linux 기반 환경 또는 WinPE/WinRE(Windows 사전 설치 환경/Windows 복구 환경)에서 Protection 에이전트를 운영 체제의 도움 없이 실행할 수 있는 CD, DVD, USB 플래시 드라이브 또는 기타 이동식 미디어입니다. 부트 가능한 미디어의 주요 용도는 시작할 수 없는 운영 체제를 복구하는 것입니다.

참고

부트 가능한 미디어는 하이브리드 드라이브를 지원하지 않습니다.

© Acronis International GmbH, 2003-2024

사용자 정의 부트 가능한 미디어 대 이미 생성된 부트 가능한 미디어

Bootable Media Builder를 사용하면 Windows, Linux 또는 macOS 컴퓨터용으로 사용자 정의 부트 가능한 미디어(Linux 기반 또는 WinPE 기반)를 생성할 수 있습니다. Linux 기반 및 WinPE/WinRE 기반 사용자 정의 부트 가능한 미디어에서는 자동 등록, 네트워크 설정, 프록시 서버 설정 등의 추가 설정을 구성할 수 있습니다. WinPE/WinRE 기반 사용자 정의 부트 가능한 미디어에서는 드라이버도 더 추가할 수 있습니다.

또한 이미 생성된 부트 가능한 미디어(Linux 기반만 해당)를 다운로드할 수 있습니다. 이미 생성된 부트 가능한 미디어는 복구 작업과 Universal Restore 기능 액세스용으로 사용할 수 있습니다.

Linux 기반 부트 가능한 미디어 대 WinPE/WinRE 기반 부트 가능한 미디어

Linux 기반

Linux 기반 부트 가능한 미디어에는 Linux 커널 기반의 Protection 에이전트가 포함됩니다. 에이전트는 베어 메탈 및 손상되거나 지원되지 않는 파일 머신이 있는 머신을 포함하여 PC와 호환되는 모든 하드웨어에서 부팅 및 작업을 수행할 수 있습니다.

WinPE/WinRE 기반

WinPE 기반 부트 가능한 미디어에는 WinPE(Windows 사전 설치 환경) 및 Cyber Protection Plug-in for WinPE라고 하는 최소 Windows 시스템, 즉 사전 설치 환경에서 실행할 수 있는 Protection 에이전트의 변형이 포함되어 있습니다. WinRE 기반 부트 가능한 미디어는 Windows 복구 환경을 사용하며, 추가 Windows 패키지를 설치할 필요가 없습니다.

WinPE는 이종 하드웨어가 있는 대규모 환경에서 가장 편리한 부트 가능한 솔루션으로 증명되었습니다.

장점:

- Windows 사전 설치 환경에서 Cyber Protection을(를) 사용하는 경우 Linux 기반 부트 가능한 미디어를 사용하는 것보다 더 많은 기능이 제공됩니다. PC 호환 가능 하드웨어를 WinPE로 부팅하면 Protection 에이전트뿐만 아니라 PE 명령과 스크립트 및 PE에 추가한 기타 플러그 인을 사용할 수도 있습니다.
- PE 기반 부트 가능한 미디어는 특정 RAID 컨트롤러 지원 또는 RAID 어레이의 특정 수준 등과 같은 몇몇 Linux와 관련된 부트 가능한 미디어 문제를 극복하는 데 도움이 됩니다. WinPE 2.x 이상에 기반을 둔 미디어는 필요한 장치 드라이버의 동적 로드를 지원합니다.

제한:

- WinPE 버전 4.0 이전에 기반을 둔 부트 가능한 미디어는 UEFI(Unified Extensible Firmware Interface)를 사용하는 머신에서 부팅되지 않습니다.

© Acronis International GmbH, 2003-2024

실제 부트 가능한 미디어 생성

디스크 수준 백업을 사용하기 시작하는 즉시 부트 가능한 미디어를 생성하여 테스트하는 것이 매우 좋습니다. 또한 보호 에이전트의 주요 업데이트 후에는 항상 부트 가능한 미디어를 다시 생성하는 것이 좋습니다.

동일한 미디어를 사용하여 Windows 또는 Linux를 복구할 수 있습니다. macOS를 복구하려면 macOS를 실행 중인 머신에서 별도의 미디어를 생성합니다.

Windows 또는 Linux에서 실제 부트 가능한 미디어를 생성하려면

1. 사용자 정의 부트 가능한 미디어 ISO 파일 또는 이미 생성된 ISO 파일을 생성합니다.
   사용자 정의 ISO 파일을 생성하려면 "Bootable Media Builder"(645페이지)을(를) 사용합니다.
   이미 생성된 ISO 파일을 다운로드하려면 Cyber Protect 콘솔에서 머신을 선택한 다음 **복구** > **추가 복구 방법...** > **ISO 이미지 다운로드**를 클릭합니다.
2. [선택 사항] Cyber Protect 콘솔에서 등록 토큰을 생성합니다. 이미 생성된 ISO 파일을 다운로드하면 등록 토큰이 자동으로 표시됩니다.
   이 토큰이 있으면 로그인과 비밀번호를 입력하지 않아도 부트 가능한 미디어가 클라우드 스토리지에 액세스할 수 있습니다.
3. 다음 방법 중 하나로 실제 부트 가능한 미디어를 생성합니다.
   - ISO 파일을 CD/DVD에 굽습니다.
   - ISO 파일 및 온라인에서 사용 가능한 무료 도구 중 하나를 사용하여 부트 가능한 USB 플래시 드라이브를 생성합니다.
     UEFI 머신을 부트하려는 경우에는 `ISO-USB` 또는 `RUFUS`를 사용하고 BIOS 머신의 경우에는 `Win32DiskImager`를 사용합니다. Linux에서는 `dd` 유틸리티를 사용합니다.

   가상 머신의 경우 복구하려는 머신에 ISO 파일을 CD/DVD 드라이브로 연결할 수 있습니다.

macOS에서 실제 부트 가능한 미디어를 생성하려면

1. Agent for Mac이 설치되어 있는 머신에서 **애플리케이션** > **복구 미디어 제작기**를 클릭합니다.
2. 연결된 이동식 미디어가 표시됩니다. 부트 가능하도록 만들 미디어를 하나 선택합니다.

   경고!
   디스크에 있는 모든 데이터가 지워집니다.

3. **생성**을 클릭합니다.
4. 부트 가능한 미디어가 생성되는 동안 기다립니다.

Bootable Media Builder

Bootable Media Builder는 부트 가능한 미디어를 생성하기 위한 전용 도구입니다. 이 하드웨어는 Protection 에이전트가 설치된 머신의 선택적 컴포넌트로 설치됩니다.

© Acronis International GmbH, 2003-2024

Bootable Media Builder를 사용하는 이유

Cyber Protect 콘솔에서 다운로드할 수 있는 이미 생성된 부트 가능한 미디어는 Linux 커널을 기반으로 합니다. Windows PE와는 달리 여기에는 사용자 정의 드라이버를 쉽게 삽입할 수 없습니다.

Bootable Media Builder를 사용하면 사용자 정의된 Linux 기반 및 WinPE 기반 부트 가능한 미디어 이미지를 생성할 수 있습니다.

32비트와 64비트 버전 중 선택

Bootable Media Builder는 32비트 및 64비트 구성 요소로 부트 가능한 미디어를 생성합니다. 대부분의 경우 UEFI(통합 확장형 펌웨어 인터페이스)를 사용하는 머신을 부팅하려면 64비트 미디어가 필요합니다.

Linux 기반 부트 가능한 미디어

Linux 기반 부트 가능한 미디어를 생성하려면

1. **Bootable Media Builder**를 시작합니다.
2. **부트 가능한 미디어 유형**에서 **기본값(Linux 기반 미디어)**을 선택합니다.
3. 볼륨 및 네트워크 리소스가 표시되는 방법을 선택합니다.
   - Linux와 같은 볼륨 표현 방식의 부트 가능한 미디어는 볼륨을 hda1, sdb2와 같이 표시합니다. 이 미디어는 복구를 시작하기 전에 MD 장치 및 논리 볼륨(LVM) 재구성을 시도합니다.
   - Windows와 같은 볼륨 표현 방식의 부트 가능한 미디어는 볼륨을 C:, D:와 같이 표시합니다. 그리고 동적 볼륨(LDM) 액세스 권한을 제공합니다.
4. [선택 사항] Linux 커널의 매개변수를 지정합니다. 여러 개의 매개변수를 공백으로 구분합니다. 예를 들어 부트 가능한 에이전트에 대한 표시 모드를 선택하려면 미디어가 시작될 때마다 다음을 입력합니다. **vga=ask** 사용 가능한 매개변수에 대한 자세한 내용은 "커널 매개변수"(647페이지)을(를) 참조하십시오.
5. [선택 사항] 부트 가능한 미디어의 언어를 선택합니다.
6. [선택 사항] 복구 후 Windows가 사용할 부트 모드(BIOS 또는 UEFI)를 선택합니다.
7. 미디어에 배치할 구성 요소(Cyber Protection 부트 가능한 에이전트)를 선택합니다.
8. [선택 사항] 부팅 메뉴의 시간 초과 간격을 지정합니다. 이 설정이 구성되지 않은 경우에는 운영 체제(있는 경우)를 부팅할지 또는 컴퍼넌트를 부팅할지 선택할 때까지 로더가 대기합니다.
9. [선택 사항] 부트 가능한 에이전트 작업을 자동화하려면 **다음 스크립트 사용** 확인란을 선택합니다. 그다음에 스크립트 중 하나를 선택하고 스크립트 매개변수를 지정합니다. 스크립트에 대한 자세한 내용은 "부트 가능한 미디어의 스크립트"(649페이지)을(를) 참조하십시오.
10. [선택 사항] 부트 시 Cyber Protection 서비스에 부트 가능한 미디어를 등록할 방법을 선택합니다. 등록 설정에 대한 자세한 내용은 "부트 가능한 미디어 등록"(657페이지)을(를) 참조하십시오.
11. 부팅한 머신의 네트워크 어댑터용 네트워크 설정을 지정하거나 자동 DHCP 구성을 그대로 유지합니다.
12. [선택 사항] 프록시 서버가 사용자 네트워크에서 활성화된 경우 해당 호스트 이름/IP 주소 및 포트를 지정합니다.

© Acronis International GmbH, 2003-2024

13. 생성된 부트 가능한 미디어의 파일 유형을 선택합니다.
    - ISO 이미지
    - ZIP 파일
14. 부트 가능한 미디어 파일의 파일 이름을 선택합니다.
15. 요약 화면에서 설정을 확인하고 **진행**을 클릭합니다.

커널 매개변수

Linux 커널의 매개변수를 하나 이상 지정할 수 있습니다. 이러한 매개변수는 부트 가능한 미디어를 시작할 때 자동으로 적용됩니다. 일반적으로 부트 가능한 미디어로 작업하는 동안 문제가 발생할 때 이러한 매개변수가 사용됩니다. 보통은 이 필드를 비워둘 수 있습니다.

부트 메뉴에서 F11 키를 눌러 이러한 매개변수를 지정할 수도 있습니다.

매개변수

여러 매개변수를 지정할 때는 공백으로 구분합니다.

- **acpi=off**

  ACPI(Advanced Configuration and Power Interface)를 비활성화합니다. 특정 하드웨어 구성에 문제가 발생할 때 이 매개변수를 사용할 수 있습니다.
- **noapic**

  APIC(Advanced Programmable Interrupt Controller)를 비활성화합니다. 특정 하드웨어 구성에 문제가 발생할 때 이 매개변수를 사용할 수 있습니다.
- **vga=ask**

  부트 가능한 미디어의 그래픽 사용자 인터페이스에서 사용할 비디오 모드를 묻습니다. **vga** 매개변수가 없으면 비디오 모드가 자동으로 감지됩니다.
- **vga=** *mode_number*

  부트 가능한 미디어의 그래픽 사용자 인터페이스에서 사용할 비디오 모드를 지정합니다. 모드 번호는 16진수 형식으로 *mode_number*에서 제공합니다(예: **vga=0x318**).

  모드 번호에 해당하는 화면 해상도와 색상 수는 머신에 따라 다를 수 있습니다. 먼저 **vga=ask** 매개변수를 사용하여 *mode_number*의 값을 선택하는 것이 좋습니다.
- **quiet**

  Linux 커널을 로딩할 때 시작 메시지 표시를 비활성화하고 커널이 로드된 후에 관리 콘솔을 시작합니다.

  이 매개변수는 부트 가능한 이미지를 생성할 때 무조건적으로 지정되지만 부트 메뉴에서 이 매개변수를 제거할 수 있습니다.

  이 매개변수를 제거하면 모든 시작 메시지가 표시된 이후에 명령 프롬프트가 나옵니다. 명령 프롬프트에서 관리 콘솔을 시작하려면 **/bin/product** 명령을 실행합니다.
- **nousb**

  USB(Universal Serial Bus) 하위 시스템의 로딩을 비활성화합니다.
- **nousb2**

© Acronis International GmbH, 2003-2024

USB 2.0 지원을 비활성화합니다. USB 1.1 장치는 이 매개변수에서 여전히 작동합니다. 이 매개변수를 사용하면 USB 2.0 모드에서 작동하지 않는 일부 USB 드라이브를 USB 1.1 모드에서 사용할 수 있습니다.

- **nodma**

  모든 IDE 하드 디스크 드라이브에 대해 직접 메모리 액세스(DMA)를 비활성화합니다. 커널이 일부 하드웨어에서 고정되는 것을 방지합니다.

- **nofw**

  FireWire(IEEE1394) 인터페이스 지원을 비활성화합니다.

- **nopcmcia**

  PCMCIA 하드웨어 감지를 비활성화합니다.

- **nomouse**

  마우스 지원을 비활성화합니다.

- *module_name* **=off**

  *module_name*이 지정한 이름의 모듈을 비활성화합니다. 예를 들어 SATA 모듈 사용을 비활성화하려면 **sata_sis=off**를 지정합니다.

- **pci=bios**

  하드웨어 장치를 직접 액세스하는 대신 PCI BIOS를 강제로 사용합니다. 시스템에 표준 이외의 PCI 호스트 브리지가 있는 경우 이 매개변수를 사용할 수 있습니다.

- **pci=nobios**

  PCI BIOS의 사용을 비활성화합니다. 직접 하드웨어 액세스 방법만 허용됩니다. BIOS로 인해 부트 가능한 미디어를 시작하지 못할 때 이 매개변수를 사용할 수 있습니다.

- **pci=biosirq**

  PCI BIOS 호출을 사용하여 인터럽트 라우팅 테이블을 얻을 수 있습니다. 커널이 인터럽트 요청(IRQ)을 할당할 수 없거나 마더보드에서 보조 PCI 버스를 찾을 수 없는 경우 이 매개변수를 사용할 수 있습니다.

  이러한 호출은 일부 시스템에서는 올바로 작동하지 않을 수 있습니다. 그러나 이 방법으로만 인터럽트 라우팅 테이블을 얻을 수 있습니다.

- **LAYOUTS=en-US, de-DE, fr-FR, ...**

  부트 가능한 미디어의 그래픽 사용자 인터페이스에서 사용할 키보드 레이아웃을 지정합니다.

  이 매개변수가 없으면 두 개의 레이아웃만 사용할 수 있습니다. 영어(미국) 및 미디어의 부트 메뉴에서 선택한 언어에 해당하는 레이아웃.

  다음의 레이아웃 중에서 지정 가능:

  벨기에어: **be-BE**

  체코어: **cz-CZ**

  영어: **en-GB**

  영어(미국): **en-US**

  프랑스어: **fr-FR**

  프랑스어(스위스): **fr-CH**

  독일어: **de-DE**

  독일어(스위스): **de-CH**

© Acronis International GmbH, 2003-2024

이탈리아어: **it-IT**
폴란드어: **pl-PL**
포르투갈어: **pt-PT**
포르투갈어(브라질): **pt-BR**
러시아어: **ru-RU**
세르비아어(키릴): **sr-CR**
세르비아어(라틴): **sr-LT**
스페인어: **es-ES**
부트 가능한 미디어에서 작업할 때에는 Ctrl+Shift를 사용하여 사용 가능한 레이아웃을 차례로 표시할 수 있습니다.

부트 가능한 미디어의 스크립트

부트 가능한 미디어에서 사전 정의된 일련의 작업을 수행하게 하려면 Bootable Media Builder에서 미디어를 생성하는 동안 스크립트를 지정하면 됩니다. 그러면 머신이 미디어에서 부팅될 때마다 지정한 스크립트가 실행되며 사용자 인터페이스는 표시되지 않습니다.

미리 정의된 스크립트 중 하나를 선택하거나 스크립팅 규칙에 따라 사용자 정의 스크립트를 생성할 수 있습니다.

사전 정의된 스크립트

Bootable Media Builder에서는 다음 사전 정의된 스크립트를 제공합니다.

- 클라우드 스토리지에서 복구(**entire_pc_cloud**)
- 네트워크 공유에서 복구(**entire_pc_share**)

스크립트는 Bootable Media Builder가 설치된 머신의 다음 폴더에 있습니다.

- Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

클라우드 스토리지에서 복구

Bootable Media Builder에서 다음 스크립트 매개변수를 지정합니다.

1. 백업 파일 이름.
2. [선택 사항] 스크립트가 암호화된 백업에 액세스하는 데 사용할 비밀번호.

네트워크 공유에서 복구

Bootable Media Builder에서 다음 스크립트 매개변수를 지정합니다.

- 네트워크 공유의 경로.
- 네트워크 공유의 사용자 이름 및 비밀번호.
- 백업 파일 이름. 백업 파일 이름을 찾으려면

© Acronis International GmbH, 2003-2024

a. Cyber Protect 콘솔에서 **백업 스토리지** > **위치**로 이동합니다.
b. 네트워크 공유를 선택합니다(공유가 나열되지 않는 경우 **위치 추가** 클릭).
c. 백업을 선택합니다.
d. **상세정보**를 클릭합니다. 파일 이름이 **백업 파일 이름** 아래에 표시됩니다.

- [선택 사항] 스크립트가 암호화된 백업에 액세스하는 데 사용할 비밀번호.

사용자 정의 스크립트

중요
사용자 지정 스크립트를 생성하려면 Bash 명령 언어 및 JavaScript 객체 표기법(JSON)에 대한 지식이 필요합니다. Bash에 친숙하지 않은 경우 http://www.tldp.org/LDP/abs/html에서 자세히 알아볼 수 있습니다. JSON 사양은 http://www.json.org에서 사용할 수 있습니다.

스크립트 파일

스크립트는 Bootable Media Builder가 설치된 머신의 다음 디렉터리에 있어야 합니다.

- Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

스크립트는 3개 이상의 다음 파일로 구성되어야 합니다.

- **<script_file>.sh** - Bash 스크립트가 포함된 파일. 스크립트를 생성할 때 https://busybox.net/downloads/BusyBox.html에서 찾을 수 있는 제한된 셸 명령 집합만 사용하십시오. 다음 명령도 사용할 수 있습니다.
  - `acrocmd` - 백업 및 복구용 명령줄 유틸리티
  - `product` - 부트 가능한 미디어 사용자 인터페이스를 시작하는 명령

  이 파일과 스크립트에 포함된 추가 파일(예: 점 명령 사용)은 **bin** 하위 폴더에 있어야 합니다. 스크립트에서 추가 파일 경로를 **/ConfigurationFiles/bin/<some_file>**로 지정합니다.
- **autostart** - **<script_file>.sh**를 시작하기 위한 파일. 파일 내용은 다음과 같아야 합니다.

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<script_file>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json** - 다음이 포함된 JSON 파일.
  - Bootable Media Builder에 표시되는 스크립트 이름 및 설명.
  - Bootable Media Builder를 통해 구성할 스크립트 변수의 이름.
  - 각 변수에 대해 Bootable Media Builder에 표시되는 컨트롤의 매개변수.

© Acronis International GmbH, 2003-2024

autostart.json의 구조

최상위 객체

쌍		필요 사항	설명
이름	값 유형		
displayName	string	예	Bootable Media Builder에 표시되는 스크립트 이름.
description	string	아니요	Bootable Media Builder에 표시되는 스크립트 설명.
timeout	number	아니요	스크립트를 시작하기 전 부트 메뉴에 대한 시간 제한(초). 쌍이 지정되지 않으면 시간 제한은 10초가 됩니다.
variables	객체	아니요	Bootable Media Builder를 통해 구성할 **<script_file>.sh**에 대한 변수. 변수는 변수 문자열 식별자 및 변수 객체의 쌍 집합이어야 합니다(아래 표 참조).

변수 객체

쌍		필요 사항	설명
이름	값 유형		
displayName	string	예	**<script_file>.sh**에 사용되는 변수 이름.
type	string	예	Bootable Media Builder에 표시되는 컨트롤의 유형. 이 컨트롤은 변수 값을 구성하는 데 사용됩니다. 모든 지원되는 유형에 대해서는 아래 표를 참조하십시오.
description	string	예	Bootable Media Builder의 컨트롤 위에 표시되는 컨트롤 레이블.
default	type이 string, multiString, password, 또는 enum인 경우 문자열 type이 number, spinner 또는 checkbox인 경	아니요	컨트롤의 기본값. 쌍이 지정되지 않으면 기본값은 컨트롤 유형에 따라 빈 문자열 또는 0이 됩니다. 확인란의 기본값은 0(선택 취소 상태) 또는 1(선택 상태)가 될 수 있습니다.

© Acronis International GmbH, 2003-2024

	우 숫자		
order	number (음수가 아님)	예	Bootable Media Builder의 컨트롤 순서. 값이 높을수록 컨트롤은 **autostart.json**에 정의된 기타 컨트롤을 기준으로 아래쪽에 배치됩니다. 초기 값은 0이어야 합니다.
min (spinner만 해당)	number	아니요	스핀 박스에 있는 스핀 컨트롤의 최소값. 쌍이 지정되지 않으면 값은 0이 됩니다.
max (spinner만 해당)	number	아니요	스핀 박스에 있는 스핀 컨트롤의 최대값. 쌍이 지정되지 않으면 값은 100이 됩니다.
step (spinner만 해당)	number	아니요	스핀 박스에 있는 스핀 컨트롤의 단계 값. 쌍이 지정되지 않으면 값은 1이 됩니다.
items (enum만 해당)	문자열 배열	예	드롭다운 목록의 값.
required (string, multiString, password, enum만 해당)	number	아니요	컨트롤 값이 비어 있을 수 있거나(0) 없는지(1) 여부를 지정합니다. 쌍이 지정되지 않으면 컨트롤 값은 비어 있을 수 있습니다.

컨트롤 유형

이름	설명
string	짧은 문자열을 입력하거나 편집하는 데 사용되는 한 줄의 비제한 텍스트 박스.
multiString	긴 문자열을 입력하거나 편집하는 데 사용되는 여러 줄의 비제한 텍스트 박스.
password	비밀번호를 안전하게 입력하는 데 사용되는 한 줄의 비제한 텍스트 박스.
number	숫자를 입력하거나 편집하는 데 사용되는 한 줄의 숫자 전용 텍스트 박스.
spinner	스킨 컨트롤을 통해 숫자를 입력하거나 편집하는 데 사용되는 한 줄의 숫자 전용 텍스트 박스. 스핀 박스라고도 합니다.
enum	미리 결정된 값의 고정된 집합이 있는 표준 드롭다운 목록.
checkbox	선택 취소 상태 또는 선택 상태의 두 가지 상태를 가지는 확인란.

아래 샘플 **autostart.json**에는 **<script_file>.sh**에 대한 변수를 구성하는 데 사용될 수 있는 컨트롤의 모든 가능한 유형이 포함됩니다.

```
{
```


© Acronis International GmbH, 2003-2024

```
        "displayName": "Autostart script name",
        "description": "This is an autostart script description.",
        "variables": {
                "var_string": {
                        "displayName": "VAR_STRING",
                        "type": "string", "order": 1,
                        "description": "This is a 'string' control:", "default": "Hello,
world!"
                },
                "var_multistring": {
                        "displayName": "VAR_MULTISTRING",
                        "type": "multiString", "order": 2,
                        "description": "This is a 'multiString' control:",
                        "default": "Lorem ipsum dolor sit amet,\nconsectetur adipiscing elit."
                },
                "var_number": {
                        "displayName": "VAR_NUMBER",
                        "type": "number", "order": 3,
                        "description": "This is a 'number' control:", "default": 10
                },
                "var_spinner": {
                        "displayName": "VAR_SPINNER",
                        "type": "spinner", "order": 4,
                        "description": "This is a 'spinner' control:",
                        "min": 1, "max": 10, "step": 1, "default": 5
                },
                "var_enum": {
                        "displayName": "VAR_ENUM",
                        "type": "enum", "order": 5,
                        "description": "This is an 'enum' control:",
                        "items": ["first", "second", "third"], "default": "second"
```


© Acronis International GmbH, 2003-2024

```
            },
            "var_password": {
                    "displayName": "VAR_PASSWORD",
                    "type": "password", "order": 6,
                    "description": "This is a 'password' control:", "default": "qwe"
            },
            "var_checkbox": {
                    "displayName": "VAR_CHECKBOX",
                    "type": "checkbox", "order": 7,
                    "description": "This is a 'checkbox' control", "default": 1
            }
        }
}
```

WinPE 기반 및 WinRE 기반 부트 가능한 미디어

추가적인 준비 없이 WinRE 이미지를 생성할 수도 있고, Windows 자동 설치 키트(AIK) 또는 Windows 평가 및 배포 키트(ADK)를 설치한 후 WinPE 이미지를 생성할 수도 있습니다.

WinRE 이미지

WinRE 이미지 생성은 다음 운영 체제에서 지원됩니다.

- Windows 7(64비트)
- Windows 8(32비트 및 64비트)
- Windows 8.1(32비트 및 64비트)
- Windows 10(32비트 및 64비트)
- Windows 11(64비트)
- Windows Server 2012(64비트)
- Windows Server 2016(64비트)
- Windows Server 2019(64비트)
- Windows Server 2022(64비트)

WinPE 이미지

Windows 자동 설치 키트(AIK) 또는 Windows 평가 및 배포 키트(ADK)를 설치하면 Bootable Media Builder는 다음 커널을 기반으로 하는 WinPE 배포판을 지원합니다.

- Windows Vista (PE 2.0)
- Windows Vista SP1 및 Windows Server 2008(PE 2.1)

© Acronis International GmbH, 2003-2024

- Windows 7(PE 3.0)(Windows 7 SP1(PE 3.1)에 대한 보조 기능 포함 또는 제외)
- Windows 8 (PE 4.0)
- Windows 8.1 (PE 5.0)
- Windows 10 (PE 10.0.1xxx)
- Windows 11 (PE 10.0.2xxx)

부트 가능한 미디어 제작기는 32비트 및 64비트 WinPE 배포판을 모두 지원합니다. 32비트 WinPE 배포판은 64비트 하드웨어에서도 실행할 수 있습니다. 그러나 UEFI(Unified Extensible Firmware Interface)를 사용하는 머신을 부팅하려면 64비트 배포판이 필요합니다.

참고
WinPE 4 이상 기반 PE 이미지를 실행하려면 약 1GB의 RAM이 필요합니다.

WinPE 또는 WinRE 부트 가능한 미디어 생성

Bootable Media Builder는 Cyber Protection을(를) WinPE 및 WinRE와 통합하기 위한 2가지 방법을 제공합니다.

- Cyber Protection 플러그 인을 사용하여 ISO 파일 새로 생성.
- 나중에 사용하기 위해 WMI 파일에 Cyber Protection 플러그 인 추가(수동 ISO 생성, 기타 도구를 이미지에 추가 등)

WinPE 또는 WinRE 부트 가능한 미디어를 생성하려면

1. Protectioon 에이전트가 설치되어 있는 머신에서 Bootable Media Builder를 실행합니다.
2. **부트 가능한 미디어 유형**에서 **Windows PE** 또는 **Windows PE(64비트)**를 선택합니다. UEFI (Unified Extensible Firmware Interface)를 사용하는 머신을 부팅하려면 64비트 미디어가 필요합니다.
3. 부트 가능한 미디어의 하위 유형을 **WinRE** 또는 **WinPE** 중에서 선택합니다.
   WinRE 부트 가능한 미디어를 생성할 때는 추가 패키지를 설치할 필요가 없습니다.
   64비트 WinPE 미디어를 생성하려면 Windows 자동 설치 키트(AIK) 또는 Windows 평가 및 배포 키트(ADK)를 다운로드해야 합니다. 32비트 WinPE 미디어를 생성하려면 AIK 또는 ADK를 다운로드해야 하며 다음 작업도 수행해야 합니다.
   a. **Plug-in for WinPE(32비트) 다운로드**를 클릭합니다.
   b. **%PROGRAM_FILES%\BackupClient\BootableComponents\WinPE32**에 플러그 인을 저장합니다.
4. [선택 사항] 부트 가능한 미디어의 언어를 선택합니다.
5. [선택 사항] 복구 후 Windows가 사용할 부트 모드(BIOS 또는 UEFI)를 선택합니다.
6. 부팅한 머신의 네트워크 어댑터용 네트워크 설정을 지정하거나 자동 DHCP 구성을 그대로 유지합니다.
7. [선택 사항] 부트 시 Cyber Protection 서비스에 부트 가능한 미디어를 등록할 방법을 선택합니다. 등록 설정에 대한 자세한 내용은 "부트 가능한 미디어 등록"(657페이지)을(를) 참조하십시오.
8. [선택 사항] 부트 가능한 미디어에 추가할 Windows 드라이버를 지정합니다.

© Acronis International GmbH, 2003-2024

머신이 Windows PE 또는 Windows RE로 부팅되고 나면 드라이버를 통해 백업이 위치한 장치에 액세스할 수 있습니다. 32비트 WinPE 또는 WinRE 배포판을 사용하는 경우에는 32비트 드라이버를 추가하고 64비트 WinPE 또는 WinRE 배포판을 사용하는 경우에는 64비트 드라이버를 추가합니다.

드라이버를 추가하려면

- **추가**를 클릭하고 해당 SCSI, RAID, SATA 컨트롤러, 네트워크 어댑터, 테이프 드라이브 또는 다른 장치에 필요한 .inf 파일의 경로를 지정합니다.
- 결과로 나오는 WinPE 또는 WinRE 미디어에 포함할 각 드라이버에 대해 이 절차를 반복합니다.

9. 생성된 부트 가능한 미디어의 파일 유형을 선택합니다.
   - ISO 이미지
   - WIM 이미지
10. 결과 이미지 파일의 전체 경로(파일 이름 포함)를 지정합니다.
11. 요약 화면에서 설정을 확인하고 **진행**을 클릭합니다.

결과로 나오는 WIM 파일에서 PE 이미지(ISO 파일)를 생성하려면

- Windows PE 폴더에서 기본 boot.wim 파일을 새로 만든 WIM 파일로 바꿉니다. 위의 예의 경우 다음을 입력합니다.

```
copy c:\RecoveryWIMMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```

- **Oscdimg** 도구를 사용합니다. 위의 예의 경우 다음을 입력합니다.

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso
```

경고!
이 예를 복사하여 붙여 넣지 마십시오. 명령을 직접 입력하지 않으면 작업이 실패합니다.

준비: WinPE 2.x 및 3.x

PE 2.x 또는 3.x 이미지를 생성하거나 수정하려면 Bootable Media Builder와 Windows AIK(자동 설치 키트)를 같은 머신에 설치합니다.

머신을 준비하려면

1. 다음 Microsoft 웹 사이트에서 AIK 이미지 파일을 다운로드합니다.
   - Windows Vista(PE 2.0): https://www.microsoft.com/en-us/download/details.aspx?id=10333
   - Windows Vista SP1 및 Windows Server 2008(PE 2.1): https://www.microsoft.com/en-us/download/details.aspx?id=9085
   - Windows 7(PE 3.0): https://www.microsoft.com/en-gb/download/details.aspx?id=5753
     Windows 7 SP1(PE 3.1)의 경우에는 https://www.microsoft.com/en-us/download/details.aspx?id=5188에서 AIK 추가 기능도 다운로드해야 합니다.
2. 이미지 파일을 DVD 디스크에 굽거나 USB 플래시 드라이브에 저장합니다.
3. 이미지 파일에서 다음 항목을 설치합니다.

© Acronis International GmbH, 2003-2024

- Microsoft .NET Framework(사용 중인 하드웨어에 따라 NETFXx86 또는 NETFXx64 설치)
- MSXML(Microsoft XML 파서)
- Windows AIK

4. 같은 머신에 부트 가능한 미디어 제작기를 설치합니다.

준비: WinPE 4.0 이상

PE 4 이상 버전 이미지를 생성하거나 수정하려면 Bootable Media Builder와 Windows ADK(평가 및 배포 키트)를 같은 머신에 설치합니다.

머신을 준비하려면

1. Microsoft 웹 사이트에서 ADK 설치 프로그램을 다운로드합니다.
   지원되는 Windows 버전은 다음과 같습니다.
   - Windows 11(PE 10.0.2xxx)
   - Windows 10(PE 10.0.1xxx)
   - Windows 8.1(PE 5.0)
   - Windows 8(PE 4.0)
2. 평가 및 배포 키트를 설치합니다.
3. Bootable Media Builder를 설치합니다.

부트 가능한 미디어 등록

Cyber Protection 서비스에서 부트 가능한 미디어를 등록하면 백업용 클라우드 스토리지에 액세스할 수 있습니다. 부트 가능한 미디어를 생성할 때 등록을 사전 구성할 수 있습니다. 등록을 사전 구성하지 않는 경우에는 미디어로 머신을 부팅한 후에 미디어를 등록할 수 있습니다.

Cyber Protection 서비스에서 등록을 사전 구성하려면

1. Bootable Media Builder에서 **부트 가능한 미디어 등록**으로 이동합니다.
2. **서비스 URL**에서 Cyber Protection 서비스 주소를 지정합니다.
3. [선택 사항] **표시 이름**에서 부팅한 머신의 이름을 지정합니다.
4. Cyber Protection 서비스에서 자동 등록을 설정하려면 **부트 가능한 미디어 자동 등록** 확인란을 선택하고 자동 등록 수준을 선택합니다.
   - **부팅 시 등록 토큰 입력 요청**
     머신이 미디어에서 부팅될 때마다 토큰을 제공해야 합니다.
   - **다음 토큰 사용**
     머신은 이 부트 가능한 미디어에서 부팅될 때 자동으로 등록됩니다.

부트 가능한 미디어에서 머신을 부팅한 후 해당 미디어를 등록하려면

1. 부트 가능한 미디어에서 머신을 부트합니다.
2. 시작 창에서 **미디어 등록**을 클릭합니다.
3. **서버**에서 Cyber Protection 서비스 주소를 지정합니다.
4. **등록 토큰**에 등록 토큰을 입력합니다.
5. **등록**을 클릭합니다.

© Acronis International GmbH, 2003-2024

네트워크 설정

부트 가능한 미디어를 생성할 때는 부트 가능한 에이전트에서 사용될 네트워크 연결을 미리 구성할 수 있습니다. 다음 매개변수를 미리 구성할 수 있습니다.

- IP 주소
- 서브넷 마스크
- 게이트웨이
- DNS 서버
- WINS 서버

부트 가능한 에이전트가 머신에서 시작된 후 머신의 네트워크 인터페이스 카드(NIC)에 구성이 적용됩니다. 설정이 미리 구성되지 않은 경우에는 에이전트는 DHCP 자동 구성을 사용합니다.

부트 가능한 에이전트가 머신에서 실행 중인 경우에는 네트워크 설정을 수동으로 구성할 수도 있습니다.

여러 네트워크 연결을 미리 구성

최대 10개의 네트워크 인터페이스 카드(NIC)에 대해 TCP/IP 설정을 미리 구성할 수 있습니다. 각 NIC에 적합한 설정이 할당될 수 있도록 미디어가 사용자 정의된 서버에서 미디어를 생성하십시오. 마법사 창에서 기존 NIC를 선택하면 NIC의 설정이 선택되어 미디어에 저장됩니다. 각 기존 NIC의 MAC 주소 또한 미디어에 저장됩니다.

MAC 주소를 제외하고는 설정을 변경하거나 존재하지 않는 NIC의 설정을 구성할 수 있습니다.

부트 가능한 에이전트는 서버에서 시작된 후, 사용 가능한 NIC 목록을 검색합니다. 이 목록은 NIC가 사용하고 있는 상단에서 프로세서에 가장 가까운 슬롯으로 정렬되어 있습니다.

부트 가능한 에이전트는 각 알려진 NIC에 적합한 설정을 할당하며 NIC를 MAC 주소로 식별합니다. 알려진 MAC 주소가 있는 NIC를 구성한 후에 나머지 NIC에는, 존재하지 않는 NIC에 대해 작성한 설정이 맨 위의 할당되지 않은 NIC부터 시작하여 할당됩니다.

미디어가 생성된 머신뿐만 아니라 모든 머신에서 부트 가능한 미디어를 사용자 정의할 수 있습니다. 이를 수행하려면 해당 머신에서 슬롯 순서에 따라서 NIC를 구성하십시오. NIC1은 프로세서와 가장 가까운 슬롯을 사용하고, NIC2는 그 다음 슬롯을 사용합니다. 부트 가능한 에이전트는 해당 머신에서 시작할 때 알려진 MAC 주소가 있는 NIC를 찾지 않으며, 사용자가 했던 것과 같은 순서로 NIC를 구성합니다.

예

부트 가능한 에이전트는 운영 네트워크를 통한 관리 콘솔과의 통신을 위해 네트워크 어댑터 중 하나를 사용할 수 있습니다. 이 연결을 위해 자동 구성을 수행할 수 있습니다. 복구할 상당량의 데이터를 정적 TCP/IP 설정을 사용하여 전용 백업 네트워크에 포함된 보조 NIC를 통해 전송할 수 있습니다.

© Acronis International GmbH, 2003-2024

부트 가능한 미디어에서 부팅한 머신에 연결

로컬 연결

부트 가능한 미디어에서 부팅된 머신에서 바로 작업하려면 시작 창에서 **이 머신을 로컬로 관리**를 클릭합니다.

머신이 부트 가능한 미디어에서 부팅되고 나면 머신 터미널은 DHCP로부터 얻거나 사전 구성된 값에 따라 설정된 IP 주소와 함께 시작 창을 표시합니다.

네트워크 설정 구성

현재 세션에 대한 네트워크 설정을 변경하려면, 시작 창에서 **네트워크 구성**을 클릭합니다. 표시되는 **네트워크 설정** 창에서 머신의 각 네트워크 인터페이스 카드(NIC)에 대한 네트워크 설정을 구성할 수 있습니다.

세션 중 적용된 변경 사항은 머신 재부팅 후 소실됩니다.

VLAN 추가

네트워크 설정 창에서 VLAN(가상 로컬 영역 네트워크)을 추가할 수 있습니다. 이 기능은 특정 VLAN에 포함된 백업 위치에 액세스해야 하는 경우에만 사용하십시오.

VLAN은 주로 로컬 영역 네트워크를 세그먼트로 분할하는 데 사용됩니다. 스위치의 *액세스* 포트에 연결된 NIC는 항상 포트 구성에 지정된 VLAN으로 액세스됩니다. 네트워크 설정에 VLAN을 지정한 경우에만 스위치의 *트렁크* 포트에 연결된 NIC가 포트 구성에서 허용된 VLAN으로 액세스할 수 있습니다.

트렁크 포트를 통해 VLAN에 액세스하려면

1. **VLAN 추가**를 클릭합니다.
2. 필요한 VLAN이 포함된 로컬 영역 네트워크에 대한 액세스를 제공하는 NIC를 선택합니다.
3. VLAN 식별자를 지정합니다.

확인을 클릭하면 네트워크 어댑터 목록에 새 입력 항목이 표시됩니다.

VLAN을 삭제하려면, 필수 VLAN 입력 항목을 클릭한 다음 **VLAN 제거**를 클릭합니다.

부트 가능한 미디어를 사용한 로컬 작업

부트 가능한 미디어를 사용한 작업은 실행 중인 운영 체제에서 수행되는 복구 작업과 비슷합니다. 차이점은 다음과 같습니다.

1. Windows와 같은 볼륨 표현을 지닌 부트 가능한 미디어의 경우 볼륨 드라이브 문자는 Windows의 드라이브 문자와 같습니다. Windows의 드라이브 문자가 없는 볼륨(예: System Reserved 볼륨)에는 사용 가능 문자가 디스크에서의 순서대로 할당됩니다.
   부트 가능한 미디어가 머신에서 Windows를 감지하지 못하거나 여러 개를 감지하는 경우에는 드라이브 문자가 없는 볼륨을 포함한 모든 볼륨에 디스크와 같은 순서대로 문자가 할당됩니다.

© Acronis International GmbH, 2003-2024

따라서 볼륨 문자가 Windows에서와 다르게 표시됩니다. 예를 들어, 부트 가능한 미디어의 D: 드라이브는 Windows의 E: 드라이브와 일치할 수 있습니다.

참고
볼륨에 고유한 이름을 할당하는 것이 좋습니다.

2. Linux와 같은 볼륨 표현을 지닌 부트 가능한 미디어는 로컬 디스크와 볼륨을 마운트 해제된 것으로 표시합니다(sda1, sda2...).
3. 작업을 예약할 수 없습니다. 작업을 반복해야 하는 경우에는 처음부터 새로 구성하십시오.
4. 로그 수명은 현재 세션으로 제한되어 있습니다. 전체 로그나 필터링된 로그 항목을 파일에 저장할 수 있습니다.

디스플레이 모드 설정

Linux 기반 부트 가능한 미디어를 통해 머신을 부팅할 때, 디스플레이 비디오 모드는 하드웨어 구성(모니터 및 그래픽 카드 사양)에 따라 자동으로 감지됩니다. 비디오 모드가 잘못 감지되는 경우에는 다음을 수행하십시오.

1. 부트 메뉴에서 F11을 누릅니다.
2. 명령줄에 **vga=ask**을 입력한 뒤, 부팅을 계속 진행합니다.
3. 지원되는 비디오 모드 목록에서 번호(예: **318**)를 입력하여 적합한 모드를 선택한 다음 **Enter** 키를 누릅니다.

이 절차를 해당 하드웨어 구성에서 부팅할 때마다 반복하지 않으려면 **커널 매개변수** 필드에서 지정 해당 모드 번호(이 예제에서는 **vga=0x318**)로 부트 가능한 미디어를 재생성합니다.

온프레미스의 부트 가능한 미디어를 사용한 복구

1. 부트 가능한 미디어에서 머신 부팅
2. **이 머신을 로컬로 관리**를 클릭합니다.
3. **복구**를 클릭합니다.
4. **복구 대상**에서 **데이터 선택**을 클릭합니다.
5. 복구할 백업 파일을 선택합니다.
6. 왼쪽 하단 창에서 복구하려는 드라이브/볼륨이나 파일/폴더를 선택한 뒤 **확인**을 클릭합니다.
7. 덮어쓰기 규칙을 구성합니다.
8. 복구 예외를 구성합니다.
9. 복구 옵션을 구성합니다.
10. 설정이 올바른지 살펴본 뒤 **확인**을 클릭합니다.

부트 가능한 미디어를 사용한 원격 작업

참고
이 기능은 Advanced Backup 팩에서 사용할 수 있습니다.

© Acronis International GmbH, 2003-2024

Cyber Protect 콘솔에서 부트 가능한 미디어를 확인하려면 먼저 "부트 가능한 미디어 등록"(657페이지)의 설명에 따라 해당 미디어를 등록해야 합니다.

Cyber Protect 콘솔에서 등록한 미디어는 **장치** > **부트 가능한 미디어** 탭에 표시됩니다. 30일 넘게 오프라인 상태였던 부트 가능한 미디어는 이 탭에서 사라집니다.

Cyber Protect 콘솔에서 원격으로 부트 가능한 미디어를 관리할 수 있습니다. 예를 들어 데이터 복구, 미디어로 부팅한 머신 다시 시작/종료, 미디어 관련 정보/활동/경보 확인 등의 작업을 수행할 수 있습니다.

중요

콘솔의 **설정** > **에이전트** 탭에서 부트 가능한 미디어를 원격으로 업데이트할 수는 없습니다.

부트 가능한 미디어를 업데이트하려면 "Bootable Media Builder"(645페이지) 섹션의 설명에 따라 새 미디어를 생성합니다. 콘솔에서 계정 아이콘 > **다운로드** > **부트 가능한 미디어**를 차례로 클릭하여 이미 생성된 미디어를 다운로드할 수도 있습니다.

부트 가능한 미디어를 사용하여 원격으로 파일이나 폴더를 복구하려면

1. Cyber Protect 콘솔에서 **장치** > **부트 가능한 미디어**로 이동합니다.
1. 데이터 복구에 사용할 미디어를 선택합니다.
2. **복구**를 클릭합니다.
3. 위치를 선택하고 필요한 백업을 선택합니다. 백업은 위치별로 필터링됩니다.
4. 복구 지점을 선택한 다음 **파일/폴더 복구**를 클릭합니다.
5. 필요한 폴더를 찾거나 검색 창을 사용하여 필요한 파일 및 폴더 목록을 얻습니다.
   검색 결과는 언어와 관계없이 동일합니다.
   하나 이상의 와일드 카드 문자(* 및 ?)를 사용할 수 있습니다.와일드카드 사용에 관한 자세한 내용은 "파일 필터(포함/제외)"(419페이지) 항목을 참조하십시오.
6. 복구할 파일을 클릭하여 선택한 다음 **복구**를 클릭합니다.
7. **경로**에서 복구 목적지를 선택합니다.
8. [선택 사항] 고급 복구 구성을 설정하려면 **복구 옵션**을 클릭합니다. 자세한 내용은 "복구 옵션"(473페이지) 항목을 참조하십시오.
9. **복구 시작**을 클릭합니다.
10. 다음 파일 덮어쓰기 옵션 중 하나를 선택합니다.
    - **기존 파일 덮어쓰기**
    - **오래된 경우 기존 파일 덮어쓰기**
    - **기존 파일 덮어쓰기 안 함**

    머신을 자동으로 다시 시작할지 여부를 선택합니다.
11. 복구를 시작하려면 **진행**을 클릭합니다. 복구 진행률이 **작업** 탭에 표시됩니다.

부트 가능한 미디어를 사용하여 원격으로 디스크, 볼륨 또는 전체 머신을 복구하려면

1. **장치** 탭에서 **부트 가능한 미디어** 그룹으로 이동한 다음 데이터 복구에 사용할 미디어를 선택합니다.
2. **복구**를 클릭합니다.

© Acronis International GmbH, 2003-2024

3. 위치를 선택하고 필요한 백업을 선택합니다. 백업은 위치별로 필터링됩니다.
4. 복구 지점을 선택한 다음 **복구** > **전체 머신**을 클릭합니다.

   필요한 경우 "실제 머신 복구이 섹션에서는 웹 인터페이스를 사용한 실제 머신 복구에 대해 설명합니다.다음을 복구하려는 경우에는 웹 인터페이스 대신 부트 가능한 미디어를 사용합니다.macOS를 실행 중인 머신규제 준수 모드가 설정된 테넌트의 머신베어 메탈 또는 오프라인 머신으로 임의의 운영 체제 복구논리 볼륨의 구조(Linux에서는 논리 볼륨 관리자가 생성한 볼륨). 미디어를 사용하여 논리 볼륨 구조를 자동으로 재생성할 수 있습니다.Intel 기반 Mac의 디스크 수준 백업을 Apple 실리콘 프로세서를 사용하는 Mac에 복구할 수는 없으며, 그 반대 방향의 복구도 불가능합니다. 파일과 폴더를 복구할 수 있습니다.복구 및 다시 시작운영 체제 복구 및 BitLocker로 암호화된 볼륨 복구 시에는 머신을 다시 시작해야 합니다. 자동으로 머신을 다시 시작할지 머신을 상호 작용 필요 상태로 할당할지 선택할 수 있습니다. 복구된 운영 체제는 자동으로 온라인이 됩니다.백업된 암호화 볼륨은 암호화되지 않은 볼륨으로 복구됩니다.BitLocker로 암호화된 볼륨을 복구하려면 같은 머신에 암호화되지 않은 볼륨이 있어야 하며, 해당 볼륨의 여유 공간이 1GB 이상이어야 합니다. 두 조건 중 하나라도 충족되지 않으면 복구는 실패합니다.암호화된 시스템 볼륨을 복구할 때는 추가 작업을 수행할 필요가 없습니다. 암호화된 비시스템 볼륨을 복구하려면 먼저 해당 볼륨에 있는 파일을 여는 등의 방식으로 볼륨을 잠가야 합니다. 이렇게 하지 않으면 머신을 다시 시작하지 않고 복구가 계속 진행되므로 Windows에서 복구된 볼륨을 인식하지 못할 수도 있습니다.복구가 실패하고 머신이 다시 시작된 후 파티션에서 파일을 가져올 수 없음 오류가 발생하면 보안 부팅을 비활성화해 보십시오. 이 작업을 수행하는 방법을 자세히 알아보려면 Microsoft 설명서에서 보안 부팅 비활성화를 참조하십시오.실제 머신을 복구하려면백업된 머신을 선택합니다.복구를 클릭합니다.복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.머신이 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 중 하나를 수행하십시오.백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) 머신 선택을 클릭하고 온라인 상태인 대상 머신을 선택한 다음 복구 지점을 선택합니다.백업 스토리지 탭에서 복구 지점을 선택합니다."부트 가능한 미디어를 사용하여 디스크 복구"에서 설명하는 대로 머신을 복구합니다.복구 > 전체 머신을 클릭합니다.소프트웨어가 디스크를 백업에서 대상 머신의 디스크로 자동으로 매핑합니다.다른 실제 머신으로 복구하려면 대상 머신을 클릭한 다음 온라인 상태인 대상 머신을 선택합니다.매핑 결과가 만족스럽지 않거나 디스크 매핑이 실패할 경우 볼륨 매핑을 클릭하여 디스크를 수동으로 다시 매핑합니다.매핑 섹션을 사용하여 복구용 개별 디스크 또는 볼륨을 선택할 수도 있습니다. 오른쪽 위에 있는 전환... 링크를 사용하여 디스크 복구와 볼륨 복구 간에 전환할 수 있습니다.[보호 에이전트가 설치된 Windows 머신에서만 사용 가능] 맬웨어가 없는 데이터만 복구되도록 하려면 안전 복구 스위치를 활성화하십시오. 안전 복구의 작동 방식에 대한 자세한 내용은 "안전 복구"(1페이지) 항목을 참조하십시오.복구 시작을 클릭합니다.백업된 버전으로 디스크를 덮어 쓰려는지 확인합니다. 머신을 자동으로 다시 시작할지 여부를 선택합니다.복구 진행률이 작업 탭에 표시됩니다."(1페이지)의 설명에 따라 대상 머신 및 볼륨 매핑을 구성합니다.
5. 고급 복구 구성을 설정하려면 **복구 옵션**을 클릭합니다. 자세한 내용은 "복구 옵션"(473페이지) 항목을 참조하십시오.
6. **복구 시작**을 클릭합니다.
7. 백업된 버전으로 디스크를 덮어 쓰려는지 확인합니다. 머신을 자동으로 다시 시작할지 여부를 선택합니다.

© Acronis International GmbH, 2003-2024

8. 복구 진행률이 **작업** 탭에 표시됩니다.

부팅한 머신을 원격으로 다시 시작하려면

1. **장치** 탭에서 **부트 가능한 미디어** 그룹으로 이동한 다음 데이터 복구에 사용할 미디어를 선택합니다.
2. **재부팅**을 클릭합니다.
3. 미디어로 부팅한 머신을 다시 시작할 것임을 확인합니다.

부팅한 머신을 원격으로 종료하려면

1. **장치** 탭에서 **부트 가능한 미디어** 그룹으로 이동한 다음 데이터 복구에 사용할 미디어를 선택합니다.
2. **종료**를 클릭합니다.
3. 미디어로 부팅한 머신을 종료할 것임을 확인합니다.

부트 가능한 미디어 관련 정보를 확인하려면

1. **장치** 탭에서 **부트 가능한 미디어** 그룹으로 이동한 다음 데이터 복구에 사용할 미디어를 선택합니다.
2. **상세 정보, 활동** 또는 **경보**를 클릭하여 해당 정보를 확인합니다.

부트 가능한 미디어를 원격으로 삭제하려면

1. **장치** 탭에서 **부트 가능한 미디어** 그룹으로 이동한 다음 데이터 복구에 사용할 미디어를 선택합니다.
2. **삭제**를 클릭하여 Cyber Protect 콘솔에서 부트 가능한 미디어를 삭제합니다.
3. 부트 가능한 미디어를 삭제할 것임을 확인합니다.

Startup Recovery Manager

Startup Recovery Manager은(는) 하드 드라이브에 위치한 부트 가능한 구성 요소입니다. Startup Recovery Manager을(를) 통해 별도의 부트 가능한 미디어를 사용하지 않고도 부트 가능한 복구 유틸리티를 시작할 수 있습니다.

오류가 발생하는 경우 머신을 다시 시작하고 프롬프트인 **Acronis Startup Recovery Manager에 대해 F11 키를 누르십시오**가 나타날 때까지 기다린 다음 F11 키를 누르거나 부팅 메뉴에서 Startup Recovery Manager을(를) 선택합니다(GRUB 부트 로더를 사용하는 경우). Startup Recovery Manager이(가) 시작되고 복구를 수행할 수 있습니다.

제한 사항

- [마스터 부트 레코드에 설치된 GRUB에는 적용되지 않음] Startup Recovery Manager을(를) 활성화하면 자체 부트 코드로 마스터 부트 레코드(MBR)를 덮어씁니다. 따라서 활성화하면 제3자 부트 로더를 다시 활성화해야 할 수도 있습니다.
- [GRUB에는 적용되지 않음] Linux에서 Startup Recovery Manager을(를) 활성화하기 전에 마스터 부트 레코드에 설치하는 대신 루트 파티션의 부트 레코드 또는 /boot 파티션의 부트 레코드에

© Acronis International GmbH, 2003-2024

부트 로더를 설치하는 것이 좋습니다. 그렇지 않으면 활성화 후에 부트 로더를 수동으로 재구성해야 합니다.

Startup Recovery Manager 활성화

부팅 시 표시되는 프롬프트인 **Acronis Startup Recovery Manager에 대해 F11 키를 누르십시오**를 활성화하려면(또는 GRUB 메뉴에 **Startup Recovery Manager** 항목 추가) Startup Recovery Manager을(를) 활성화해야 합니다.

참고

비암호화 시스템 볼륨이 있는 머신에서 Startup Recovery Manager을(를) 활성화하려면 해당 머신에 최소 100MB의 여유 공간이 필요합니다. 다시 시작을 통한 복구의 경우 추가로 100MB가 필요합니다.

BitLocker로 암호화된 볼륨이 있는 머신에서 Startup Recovery Manager을(를) 활성화하려면 이 머신에 최소 500MB의 여유 공간이 있는 비암호화 볼륨이 하나 이상 있어야 합니다. 다시 시작을 통한 복구의 경우 추가로 500MB의 여유 공간이 필요합니다.

Startup Recovery Manager이(가) 활성화되지 않은 경우 원클릭 복구 백업을 생성하는 백업 작업에 실패합니다.

Startup Recovery Manager을(를) 활성화하는 방법

Windows 또는 Linux 머신에 에이전트가 있는 경우

1. Cyber Protect 콘솔에서 Startup Recovery Manager을(를) 활성화하려는 머신을 선택합니다.
2. **상세정보**를 클릭합니다.
3. **Startup Recovery Manager** 스위치를 활성화합니다.

머신에 에이전트가 없는 경우

1. 부트 가능한 미디어를 사용하여 머신을 부팅합니다.
2. 부트 가능한 미디어 그래픽 인터페이스에서 **도구** > **활성화 Startup Recovery Manager**를 클릭합니다.
3. **활성화**를 선택합니다.
4. **확인**을 클릭합니다.
5. **세부 정보** 탭에서, **결과** 행을 확인하여 활성화가 성공적으로 되었는지 확인한 다음 **닫기**를 클릭합니다.

Startup Recovery Manager 비활성화

비활성화하면 부팅 시 표시되는 프롬프트인 **Acronis Startup Recovery Manager에 대해 F11 키를 누르십시오**가 비활성화됩니다(또는 GRUB 메뉴에 **Startup Recovery Manager** 항목을 제거).

Startup Recovery Manager이(가) 활성화되지 않은 경우에도 별도의 부트 가능한 미디어를 사용하여 부팅에 실패한 머신을 복구할 수 있습니다.

© Acronis International GmbH, 2003-2024

참고
Startup Recovery Manager이(가) 활성화되지 않은 경우 원클릭 복구 백업을 생성하는 백업 작업에 실패합니다.

Startup Recovery Manager을(를) 비활성화하는 방법

Windows 또는 Linux 머신에 에이전트가 있는 경우

1. Cyber Protect 콘솔에서 Startup Recovery Manager을(를) 비활성화하려는 머신을 선택합니다.
2. **상세정보**를 클릭합니다.
3. **Startup Recovery Manager** 스위치를 비활성화합니다.

머신에 에이전트가 없는 경우

1. 부트 가능한 미디어를 사용하여 머신을 부팅합니다.
2. 부트 가능한 미디어 그래픽 인터페이스에서 **도구** > **비활성화 Startup Recovery Manager**를 클릭합니다.
3. **비활성화**를 선택합니다.
4. **확인**을 클릭합니다.
5. **세부 정보** 탭에서 **결과** 행을 확인하여 비활성화가 성공적으로 이루어졌는지 확인한 다음 **닫기**를 클릭합니다.

© Acronis International GmbH, 2003-2024

재해 복구 구현

참고
- 이 기능은 Microsoft Azure 백업 위치를 지원하지 않습니다.

Cyber Disaster Recovery Cloud 정보

Cyber Disaster Recovery Cloud(DR)은 재해 복구 서비스(DRaaS)를 제공하는 Cyber Protection의 일부입니다. Cyber Disaster Recovery Cloud은 자연재해 또는 인재 발생 시 머신의 정확한 복제본을 클라우드 사이트에 전송하고 손상된 원본 머신에서 클라우드의 복구 서버로 워크로드를 전환하는 빠르고 안정적인 솔루션을 제공합니다.

다음과 같은 방식으로 재해 복구를 설정하고 구성할 수 있습니다.

- 재해 복구 모듈을 포함하고 장치에 적용하는 보호 계획을 생성합니다. 이렇게 하면 기본 재해 복구 인프라가 자동으로 설정됩니다. 재해 복구 보호 계획 생성을 참조하십시오.
- 재해 복구 클라우드 인프라를 수동으로 설정하고 각 단계를 제어합니다. "복구 서버 설정"(708 페이지)을(를) 참조하십시오.

주요 기능

참고
일부 기능을 사용하려면 적용되는 라이센스 모델에 따라 추가 라이센스가 필요할 수 있습니다.

- Cyber Disaster Recovery Cloud 서비스를 단일 콘솔에서 관리
- 보안 VPN 터널을 통해 최대 23개의 로컬 네트워크를 클라우드로 확장
- VPN 어플라이언스[1] 디플로이 없이 클라우드 사이트와의 연결 구축(클라우드 전용 모드)
- 로컬 사이트 및 클라우드 사이트에 지점 및 사이트간 연결 설정
- 클라우드의 복구 서버를 사용하여 머신 보호
- 클라우드의 기본 서버를 사용하여 애플리케이션 및 어플라이언스 보호
- 암호화된 백업에 대해 자동 재해 복구 작업 수행
- 격리된 네트워크에서 테스트 장애 조치 수행
- 클라우드에서 운영 환경을 향상시키는 방법을 설명하는 작동 실행서 사용

소프트웨어 요구 사항

지원되는 운영 체제

복구 서버를 통한 보호는 다음 운영 체제에서 테스트되었습니다.

[1][Disaster Recovery] 로컬 네트워크와 클라우드 사이트 네트워크를 보안 VPN 터널로 연결하는 특수 가상 머신입니다. VPN 어플라이언스는 로컬 사이트에 디플로이됩니다.

© Acronis International GmbH, 2003-2024

- CentOS 6.6, 7.x, 8.x
- Debian 9.x, 10.x, 11.x
- Red Hat Enterprise Linux 6.6, 7.x, 8.x
- Ubuntu 16.04, 18.04, 20.x, 21.x
- Oracle Linux 7.3 and 7.9 with Unbreakable Enterprise Kernel
- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – Nano Server를 제외한 모든 설치 옵션
- Windows Server 2019 – Nano Server를 제외한 모든 설치 옵션
- Windows Server 2022 – Nano Server를 제외한 모든 설치 옵션

이 소프트웨어는 다른 Windows 운영 체제 및 Linux 배포판에서 작동하지만 이는 보장되지 않습니다.

참고
복구 서버를 통한 보호는 다음 운영 체제가 설치된 Microsoft Azure VM에서 테스트되었습니다.

- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – Nano Server를 제외한 모든 설치 옵션
- Windows Server 2019 – Nano Server를 제외한 모든 설치 옵션
- Windows Server 2022 – Nano Server를 제외한 모든 설치 옵션
- Ubuntu Server 20.04 LTS - Gen2(Canonical) 복구 서버 콘솔 액세스 방법에 대한 자세한 내용은 https://kb.acronis.com/content/71616을 참조하십시오.

지원되는 가상화 플랫폼

복구 서버로 가상 머신을 보호하는 것은 다음 가상화 플랫폼에서 테스트되었습니다.

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7, 7.0
- Windows Server 2008 R2(Hyper-V 사용)
- Windows Server 2012/2012 R2(Hyper-V 사용)
- Windows Server 2016(Hyper-V 사용) – Nano Server를 제외한 모든 설치 옵션
- Windows Server 2019(Hyper-V 사용) – Nano Server를 제외한 모든 설치 옵션
- Windows Server 2022(Hyper-V 사용) – Nano Server를 제외한 모든 설치 옵션
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- 커널 기반 가상 머신(KVM) - 완전 가상화된 게스트(HVM)만 포함됩니다. 반가상화된 게스트(PV)는 지원되지 않습니다.
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2

VPN 어플라이언스는 다음 가상화 플랫폼에서 테스트되었습니다.

© Acronis International GmbH, 2003-2024

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- Windows Server 2008 R2(Hyper-V 사용)
- Windows Server 2012/2012 R2(Hyper-V 사용)
- Windows Server 2016(Hyper-V 사용) – Nano Server를 제외한 모든 설치 옵션
- Windows Server 2019(Hyper-V 사용) – Nano Server를 제외한 모든 설치 옵션
- Windows Server 2022(Hyper-V 사용) – Nano Server를 제외한 모든 설치 옵션
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016

이 소프트웨어는 다른 가상화 플랫폼 및 버전에서도 작동할 수 있지만 이는 보장되지 않습니다.

제한 사항

다음 플랫폼과 구성은 Cyber Disaster Recovery Cloud에서 지원되지 않습니다.

1. 지원되지 않는 플랫폼:
   - Agents for Virtuozzo
   - macOS
   - 윈도우 데스크톱 운영 체제는 마이크로소프트 제품 약관으로 인해 지원하지 않습니다.
   - Windows Server Azure Edition

     Azure Edition은 Azure에서 Azure IaaS 가상 머신(VM)으로 실행하거나 Azure Stack HCI 클러스터에서 VM으로 실행하도록 특수 제작된 특별 Windows Server 버전입니다. Standard 및 Datacenter Edition과 달리 Azure Edition은 베어 메탈 하드웨어, Windows 클라이언트 Hyper-V, Windows Server Hyper-V, 서드 파티 하이퍼바이저 또는 서드 파티 클라우드에서 실행 가능하도록 허가되지 않았습니다.
2. 지원되지 않는 구성:

   Microsoft Windows
   - 동적 디스크는 지원되지 않습니다
   - Windows 데스크톱 운영 체제는 마이크로소프트 제품 약관으로 인해 지원하지 않습니다
   - FRS 복제가 되는 Active Directory 서비스는 지원되지 않습니다
   - GPT 또는 MBR 형식(일명 "슈퍼플로피")이 없는 이동식 미디어는 지원되지 않습니다

   Linux
   - 파티션 테이블이 없는 파일 시스템
   - 게스트 OS의 에이전트를 사용하여 백업되고 다음 고급 LVM(논리 볼륨 관리자) 구성으로 된 볼륨이 있는 Linux 워크로드: 스트라이프 볼륨, 미러 볼륨, RAID 0, RAID 4, RAID 5, RAID 6 또는 RAID 10 볼륨

   참고
   여러 운영 체제가 설치된 워크로드는 지원되지 않습니다.
3. 지원되지 않는 백업 유형:

© Acronis International GmbH, 2003-2024

- CDP(지속적인 데이터 보호) 복구 지점은 호환되지 않습니다.

  중요
  CDP 복구 지점이 있는 백업에서 복구 서버를 생성한 다음 장애 복구를 수행하거나 복구 서버의 백업을 생성하면, CDP 복구 지점에 포함된 데이터는 유실됩니다.

- 포렌직 백업은 복구 서버를 생성하는 데 사용할 수 없습니다.

복구 서버에는 하나의 네트워크 인터페이스가 있습니다. 원래 머신에 여러 네트워크 인터페이스가 있는 경우 하나만 에뮬레이션됩니다.

클라우드 서버는 암호화되지 않습니다.

Cyber Disaster Recovery Cloud 평가판 버전

Acronis Cyber Disaster Recovery Cloud 평가판 버전은 30일 동안 사용할 수 있습니다. 이 경우 파트너 테넌트에서 수행하는 재해 복구에 적용되는 제한 사항은 다음과 같습니다.

- 복구 및 기본 서버에서 공용 인터넷에 액세스할 수 없습니다. 서버에 공용 IP 주소를 할당할 수 없습니다.
- IPsec 다중 사이트 VPN을 사용할 수 없습니다.

Geo-redundant Cloud Storage 사용 시의 제한 사항

Geo-redundant Cloud Storage는 백업 데이터용 보조 위치를 제공합니다. 보조 위치는 기본 스토리지 위치와는 다른 지역에 있습니다. 이처럼 기본 위치와 보조 위치의 지역이 서로 다르므로 지역 중 하나에서 재해가 발생하여 백업 데이터 복구가 불가능해지더라도 나머지 지역은 영향은 받지 않으므로 작업을 계속 진행할 수 있습니다.

중요
백업 스토리지 위치를 주 위치에서 지역 중복 보조 위치로 전환하는 경우에는 Disaster Recovery 서비스가 지원되지 않습니다.

암호화 소프트웨어와의 재해 복구 호환성

재해 복구는 다음 디스크 수준 암호화 소프트웨어와 호환됩니다.

- Microsoft BitLocker Drive Encryption
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption

참고
- 디스크 수준 암호화를 있는 워크로드의 경우 워크로드의 게스트 운영 체제에서 보호 에이전트를 설치하고 에이전트 기반 백업을 수행하도록 권장합니다.
- 장애 조치와 장애 복구는 암호화된 워크로드의 비에이전트 백업에 대해 지원되지 않습니다.

© Acronis International GmbH, 2003-2024

암호화 소프트웨어와의 Cyber Protection 호환성에 대한 자세한 정보는 "암호화 소프트웨어와의 호환성"(39페이지)을(를) 참조하십시오.

컴퓨팅 포인트

Disaster Recovery에서는 테스트 장애 조치 및 프로덕션 장애 조치를 진행할 때 기본 서버와 복구 서버에 컴퓨팅 포인트가 사용됩니다. 클라우드에서 서버(가상 머신)를 실행하는 데 사용되는 컴퓨팅 리소스가 컴퓨팅 포인트에 반영됩니다.

재해 복구 중 컴퓨팅 포인트 소비량은 서버의 매개 변수 및 서버가 장애 조치 상태에 있는 기간에 따라 달라집니다. 서버의 성능이 향상되고 시간이 길어질수록 컴퓨팅 포인트가 더 많이 소비됩니다. 그리고 컴퓨팅 포인트가 더 많이 소비될수록 더 높은 비용이 청구됩니다.

Acronis Cloud에서 실행 중인 모든 서버에서는 사용되는 컴퓨팅 포인트에 해당하는 요금이 청구됩니다. 즉, 서버 상태(전원이 켜져 있는지 여부)에 관계없이 서버가 구성된 상태에 따라 요금이 청구됩니다.

대기 상태의 복구 서버는 컴퓨팅 포인트를 사용하지 않으므로 컴퓨팅 포인트에 해당하는 요금이 청구되지 않습니다.

아래 표에는 구성 방식이 각기 다른 클라우드 내 8개 서버, 그리고 이러한 서버가 시간별로 사용하는 컴퓨팅 포인트가 나와 있습니다. **세부 정보** 탭에서 서버의 구성 방식을 변경할 수 있습니다.

유형	CPU	RAM	컴퓨팅 포인트
F1	1 vCPU	2GB	1
F2	1 vCPU	4GB	2
F3	2 vCPU	8GB	4
F4	4 vCPU	16GB	8
F5	8 vCPU	32GB	16
F6	16 vCPU	64GB	32
F7	16 vCPU	128GB	64
F8	16 vCPU	256GB	128

이 표의 정보를 참조하면 서버(가상 머신)가 사용하는 컴퓨팅 포인트를 쉽게 예측할 수 있습니다.

예를 들어 재해 복구를 사용하여 4 vCPU*인 16GB RAM과 2 vCPU인 8GB RAM을 가진 1개의 가상 머신을 보호하려는 경우, 첫 번째 가상 머신은 시간당 8의 컴퓨팅 포인트를 사용하고 두 번째 가상 머신은 시간당 4의 컴퓨팅 포인트를 사용합니다. 두 가상 머신이 모두 장애 조치 상태인 경우 총 소비량은 시간당 12의 컴퓨팅 포인트 또는 하루 동안 288의 컴퓨팅 포인트(12의 컴퓨팅 포인트 x 24시간 = 288의 컴퓨팅 포인트)가 됩니다.

* vCPU는 가상 머신에 할당되는 시간 종속 엔티티인 물리적 CPU(중앙 처리 장치)를 나타냅니다.

© Acronis International GmbH, 2003-2024

참고
할당량을 초과하여 **컴퓨팅 포인트**를 사용하는 경우에는 기본 서버와 복구 서버가 모두 종료되며 다음 청구 기간이 시작되거나 할당량을 늘릴 때까지는 이러한 서버를 사용할 수 없습니다. 기본 청구 기간은 1개월입니다.

재해 복구 기능 설정

참고
일부 기능을 사용하려면 적용되는 라이센스 모델에 따라 추가 라이센스가 필요할 수 있습니다.

재해 복구 기능을 설정하려면

1. 다음과 같이 클라우드 사이트에 대한 연결 유형을 구성해야 합니다.
   - 지점 및 사이트 간 연결
   - 사이트 간 OpenVPN 연결
   - 다중 사이트 IPsec VPN 연결
   - 클라우드 전용 모드
2. 백업 모듈이 활성화된 상태에서 보호 계획을 생성하고 전체 머신 또는 시스템, 백업을 위한 부트 볼륨을 선택합니다. 복구 서버를 생성하려면 보호 계획이 하나 이상 필요합니다.
3. 원하는 로컬 서버에 보호 계획을 적용합니다.
4. 보호하려는 각 로컬 서버에 대해 복구 서버를 생성합니다.
5. 테스트 장애 조치 수행으로 작동을 확인합니다.
6. [선택 사항] 애플리케이션을 복제하려면 기본 서버를 생성합니다.

그러면 재해로부터 로컬 서버를 보호하기 위한 재해 복구 기능이 설정됩니다.

재해가 발생하면 클라우드의 복구 서버로 워크로드 장애 조치를 할 수 있습니다. 복구 서버 장애 조치를 하기 전에 최소 하나의 복구 지점을 생성해야 합니다. 로컬 사이트를 재해로부터 복구할 때는 장애 복구를 수행하여 워크로드를 다시 로컬 사이트로 전환하면 됩니다. 장애 복구 프로세스에 대한 자세한 내용은 "사전 요구 사항"(721페이지) 및 "사전 요구 사항"(725페이지)을(를) 참조하십시오.

재해 복구 보호 계획 생성

재해 복구 모듈을 포함하고 장치에 적용하는 보호 계획을 생성합니다.

기본적으로 새 보호 계획을 생성할 때 재해 복구 모듈이 비활성화됩니다. 재해 복구 기능을 활성화하고 장치에 계획을 적용하면 각 보호된 장치용 *복구 서버*를 비롯한 클라우드 네트워크 인프라가 생성됩니다. *복구 서버*는 선택한 장치의 사본인 가상 머신입니다. 선택한 각 장치의 경우 기본 설정이 있는 복구 서버가 대기 상태(가상 머신이 실행되지 않음)에서 생성됩니다. 복구 서버 크기는 보호된 장치의 CPU 및 RAM에 따라 자동으로 조정됩니다. 다음과 같은 기본 클라우드 네트워크 인프라도 자동으로 생성됩니다. 복구 서버가 연결되는 클라우드 사이트의 VPN 게이트웨이 및 네트워크

© Acronis International GmbH, 2003-2024

보호 계획의 재해 복구 모듈을 취소, 삭제 또는 해제할 경우 복구 서버 및 클라우드 네트워크가 자동으로 삭제됩니다. 필요한 경우 재해 복구 인프라를 수동으로 제거할 수 있습니다.

참고

- 재해 복구를 구성한 후 장치를 위해 복구 서버가 생성된 이후 생성된 모든 복구 지점에서 테스트 또는 프로덕션 장애 조치를 수행할 수 있게 됩니다. 장치가 재해 복구로 보호되기 전(예: 복구 서버가 생성되기 전)에 생성된 복구 지점은 장애 조치에 사용할 수 없습니다.
- 재해 복구 보호 계획은 장치의 IP 주소를 감지할 수 없는 경우 활성화할 수 없습니다. 가상 머신이 에이전트 없이 백업되어 IP 주소가 할당되지 않은 경우를 예로 들 수 있습니다.
- 보호 계획을 적용하면 클라우드 사이트에서 같은 네트워크 및 IP 주소가 할당됩니다. IPsec VPN 연결을 설정하려면 클라우드 및 로컬 사이트의 네트워크 세그먼트가 겹치지 않아야 합니다. 다중 사이트 IPsec VPN 연결을 구성하고 나중에 장치 하나 또는 여러 개에 보호 계획을 적용하는 경우에는 클라우드 네트워크를 추가로 업데이트하고 클라우드 서버의 IP 주소를 다시 할당해야 합니다. 자세한 내용은 "IP 주소 다시 할당"(699페이지)을(를) 참조하십시오.

재해 복구 보호 계획을 생성하려면

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 보호하려는 머신을 선택합니다.
3. **보호**를 클릭하고 **계획 생성**을 클릭합니다.
   보호 계획 기본 설정이 열립니다.
4. 백업 옵션을 구성합니다.
   재해 복구 기능을 사용하려면 계획은 전체 머신을 백업하거나 부팅과 필요한 서비스 제공에 필수적인 디스크만 클라우드 스토리지에 백업해야 합니다.
5. 모듈 이름 옆의 스위치를 클릭하여 재해 복구 모듈을 활성화합니다.
6. **생성**을 클릭합니다.
   계획이 생성된 후 선택된 머신에 적용됩니다.

다음에 수행할 작업

- 복구 서버의 기본 구성을 편집할 수 있습니다. 자세한 내용은 "복구 서버 설정"(708페이지)을(를) 참조하십시오.
- 기본 네트워킹 구성을 편집할 수 있습니다. 자세한 내용은 "연결 설정"(674페이지)을(를) 참조하십시오.
- 복구 서버 기본 매개변수 및 클라우드 네트워크 인프라에 대해 자세히 알아볼 수 있습니다. 자세한 내용은 "복구 서버 기본 매개변수 편집"(672페이지) 및 "클라우드 네트워크 인프라"(674페이지)을(를) 참조하십시오.

복구 서버 기본 매개변수 편집

재해 복구 보호 계획을 생성 및 적용하면 기본 매개변수를 사용하여 복구 서버가 생성됩니다. 이러한 기본 매개변수는 나중에 편집할 수 있습니다.

© Acronis International GmbH, 2003-2024

참고
존재하지 않으면 복구 서버가 생성됩니다. 기존 복구 서버는 변경되거나 다시 생성되지 않습니다.

복구 서버 기본 매개변수를 편집하려면

1. **장치** > **모든 장치**로 이동합니다.
2. 장치를 선택하고 **재해 복구**를 클릭합니다.
3. 복구 서버 기본 매개변수를 편집합니다.
   다음 표에 복구 서버 매개변수의 설명이 나와 있습니다.

복구 서버 매개변수	**기본 가치**	**설명**
CPU 및 RAM	자동	복구 서버의 가상 CPU의 수 및 RAM의 크기입니다. 원래 장치 CPU 및 RAM 구성에 따라 기본 설정이 자동으로 결정됩니다.
클라우드 네트워크	자동	서버를 연결할 클라우드 네트워크입니다. 클라우드 네트워크가 구성되는 방식에 대한 자세한 내용은 클라우드 네트워크 인프라를 참조하십시오.
운영 네트워크 내 IP 주소	자동	서버가 운영 네트워크에서 가지는 IP 주소입니다. 기본적으로 원래 머신의 ID 주소가 설정됩니다.
테스트 IP 주소	비활성화됨	테스트 IP 주소를 사용하면 격리된 테스트 네트워크에서 장애 조치를 테스트하고, 테스트 장애 조치 중에 RDP 또는 SSH를 통해 복구 서버에 연결할 수 있습니다. 테스트 장애 조치 모드에서 VPN 게이트웨이는 NAT 프로토콜을 사용하여 테스트 IP 주소를 운영 IP 주소로 바꿉니다. 테스트 IP 주소를 지정하지 않으면 콘솔이 테스트 장애 조치 중 서버에 액세스하는 유일한 방법입니다.
인터넷 액세스	활성화됨	실제 또는 테스트 장애 조치 중에 복구 서버가 인터넷에 액세스할 수 있습니다. 기본적으로 아웃바운드 연결에서는 TCP 포트 25가 거부됩니다.
공용 주소 사용	비활성화됨	공용 IP 주소를 사용하면 장애 조치 또는 테스트 장애 조치 중에 복구 서버를 인터넷에서 사용할 수 있습니다. 공용 IP 주소를 사용하지 않는 경우 서버를 운영 네트워크에서만 사용할 수 있습니다. 공용 IP 주소를 사용하려면 인터넷 액세스를 활성화해야 합니다. 구성을 완료하면 공용 IP 주소가 표시됩니다. 기본적으로 인바운드 연결용으로는 TCP 포트 443이 열립니다.
RPO 임계값 설정	비활성화됨	RPO 임계값은 마지막 복구 지점과 현재 시간 사이에 허용되는 최대 시간 간격을 정의합니다. 이

© Acronis International GmbH, 2003-2024

		값은 15 – 60분, 1 – 24시간, 1 – 14일 내에서 설정할 수 있습니다.

클라우드 네트워크 인프라

클라우드 네트워크 인프라는 복구 서버를 연결할 클라우드 사이트 및 클라우드 네트워크의 VPN 게이트웨이로 구성됩니다.

참고
재해 복구 보호 계획을 적용할 경우 복구 클라우드 네트워크 인프라가 존재하지 않는 경우에만 생성됩니다. 기존 클라우드 네트워크는 변경되거나 다시 생성되지 않습니다.

시스템은 장치 IP 주소를 검사한 후, IP 주소와 맞는 기존 클라우드 네트워크가 없으면 적절한 클라우드 네트워크를 자동으로 생성합니다. 복구 서버 IP 주소가 맞는 기존 클라우드 네트워크가 있으면 기존 클라우드 네트워크는 변경되거나 다시 생성되지 않습니다.

- 기존 클라우드 네트워크가 없거나 재해 복구 구성을 처음으로 설정하는 경우에는 장치 IP 주소 범위에 따라 개인 용도로 IANA에서 권장하는 최대 범위(10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)를 사용하여 클라우드 네트워크가 생성됩니다. 네트워크 마스크를 편집하여 네트워크 범위를 좁힐 수 있습니다.
- 장치가 여러 로컬 네트워크에 있는 경우 클라우드 사이트의 네트워크가 로컬 네트워크의 상위 세트가 될 수 있습니다. **연결** 섹션에서 네트워크를 다시 구성할 수 있습니다. "네트워크 관리"(693페이지)을(를) 참조하십시오.
- 사이트 간 OpenVPN 연결을 설정해야 하는 경우 VPN 어플라이언스를 다운로드한 후 설치하십시오. "사이트 간 OpenVPN 구성"(685페이지)을(를) 참조하십시오. 클라우드 네트워크 범위가 VPN 어플라이언스에 연결된 로컬 네트워크 범위와 일치하는지 확인하십시오.
- 기본 네트워크 구성을 변경하려면 보호 계획의 재해 복구 모듈에서 **연결로 이동** 링크를 클릭하거나 **재해 복구** > **연결**로 이동하십시오.

연결 설정

이 섹션에서는 네트워크가 Cyber Disaster Recovery Cloud에서 작동하는 방식을 이해하는 데 필요한 네트워크 개념에 대해 설명합니다. 필요에 따라 클라우드 사이트에 대한 다양한 유형의 연결을 구성하는 방식을 배우게 됩니다. 끝으로 클라우드에서 네트워크를 관리하고, VPN 어플라이언스 및 VPN 게이트웨이의 설정을 관리하는 방법을 배웁니다.

네트워킹 개념

참고
일부 기능을 사용하려면 적용되는 라이센스 모델에 따라 추가 라이센스가 필요할 수 있습니다.

Cyber Disaster Recovery Cloud에서 클라우드 사이트에 대한 다음 연결 유형을 정의할 수 있습니다.

© Acronis International GmbH, 2003-2024

- **클라우드 전용 모드**

  이 유형의 연결에서는 로컬 사이트에 VPN 어플라이언스 배포가 필요하지 않습니다.

  로컬 네트워크와 클라우드 네트워크가 독립 네트워크입니다. 이 유형의 연결에서는 로컬 사이트의 모든 보호되는 서버에 대한 장애 조치 또는 로컬 사이트와 통신할 필요가 없는 독립 서버들의 부분 장애 조치를 염두에 둔 것입니다.

  클라우드 사이트에 있는 클라우드 서버는 지점 및 사이트 간 VPN, 공용 IP 주소(할당되어 있는 경우)를 통해 액세스할 수 있습니다.
- **사이트 간 OpenVPN 연결**

  이 유형의 연결에서는 로컬 사이트에 VPN 어플라이언스 배포가 필요합니다.

  사이트 간 OpenVPN 연결을 사용하면 IP 주소를 그대로 유지하면서 네트워크를 클라우드 사이트로 확장할 수 있습니다.

  로컬 사이트는 보안 VPN 터널을 통해 클라우드 사이트에 연결됩니다. 이 유형의 연결은 웹 서버와 데이터베이스 서버처럼 서버가 로컬 사이트에 밀접하게 종속되어 있는 경우에 적합합니다. 서버 중 하나는 클라우드 사이트에 재생성하고, 다른 하나는 로컬 사이트에 그대로 유지하는 부분 장애 조치의 경우에는 VPN 터널을 통해 두 서버가 계속해서 서로 통신할 수 있습니다.

  클라우드 사이트에 있는 클라우드 서버는 로컬 네트워크, 지점 및 사이트 간 VPN, 공용 IP 주소(할당되어 있는 경우)를 통해 액세스할 수 있습니다.
- **다중 사이트 IPsec VPN 연결**

  이 연결 유형을 사용하려면 IPsec IKE v2를 지원하는 로컬 VPN 장치가 필요합니다.

  다중 사이트 IPsec VPN 연결 구성을 시작하면 Cyber Disaster Recovery Cloud에서 공용 IP 주소를 사용하는 클라우드 VPN 게이트웨이를 자동으로 생성합니다.

  다중 사이트 IPsec VPN 사용 시에는 로컬 사이트가 보안 IPsec VPN 터널을 통해 클라우드 사이트에 연결됩니다.

  로컬 사이트 하나 또는 여러 개에서 중요한 워크로드 또는 이러한 워크로드를 반드시 사용해야 하는 서비스를 호스팅하는 재해 복구 시나리오에서는 이러한 연결 유형이 적합합니다.

  서버 중 하나를 부분 장애 조치하는 경우에는 해당 서버가 클라우드 사이트에 재생성됩니다. 나머지 서버는 로컬 사이트에 유지되며 IPsec VPN 터널을 통해 서로 계속 통신할 수 있습니다.

  로컬 사이트 중 하나를 부분 장애 조치하는 경우에도 나머지 로컬 사이트는 계속 작동하며 IPsec VPN 터널을 통해 서로 계속 통신할 수 있습니다.
- **지점 및 사이트 간 원격 VPN 액세스**

  엔드포인트 장치를 사용하여 외부에서 클라우드 및 로컬 사이트 워크로드에 접근하는 안전한 지점 및 사이트 간 원격 VPN 액세스입니다.

  로컬 사이트 액세스의 경우, 이 유형의 연결에는 로컬 사이트에 VPN 어플라이언스 디플로이가 필요합니다.

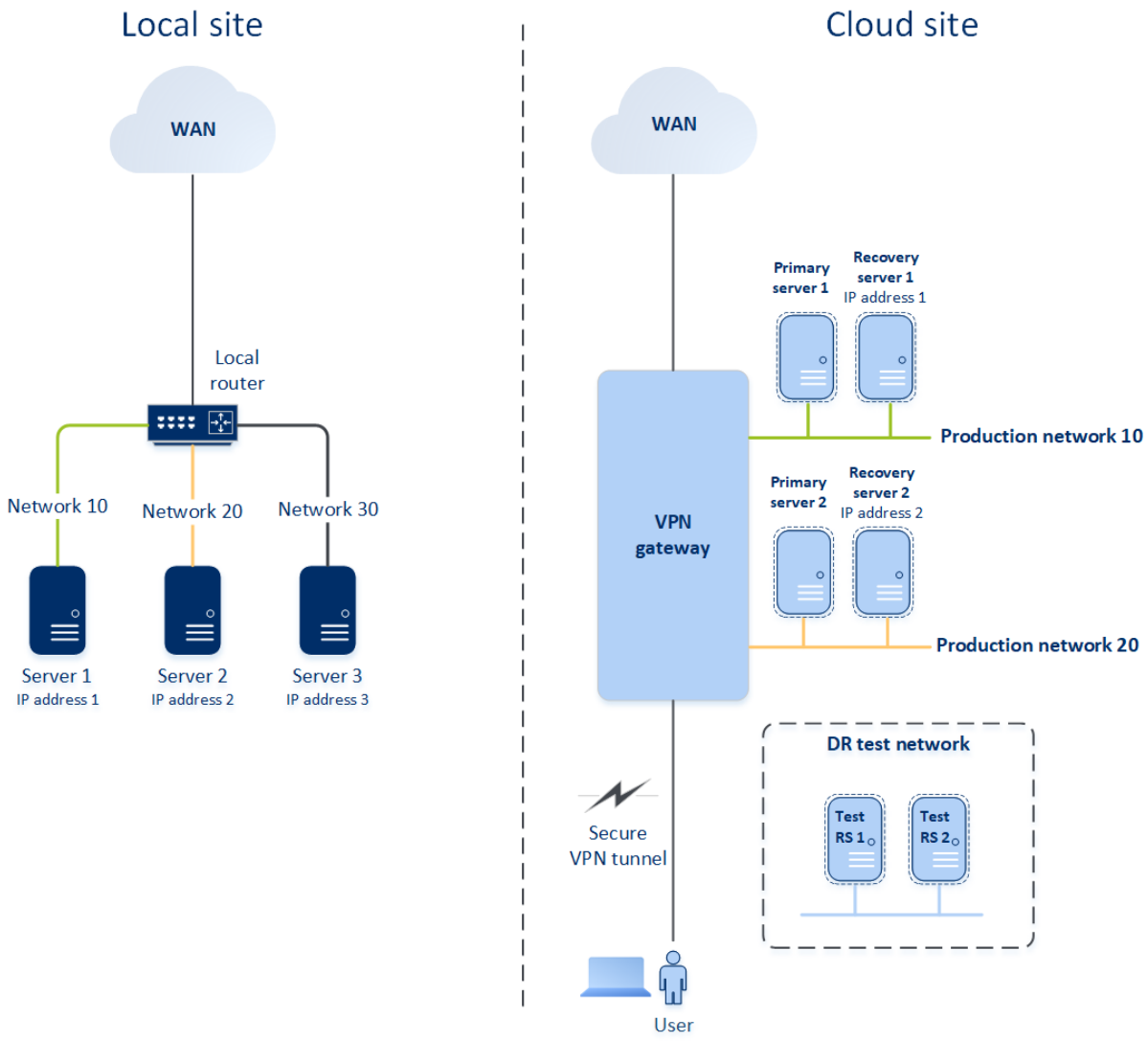
클라우드 전용 모드

클라우드 전용 모드에서는 로컬 사이트에 VPN 어플라이언스 디플로이가 필요하지 않습니다. 즉, 로컬 사이트에 하나, 클라우드 사이트에 하나, 총 두 개의 독립 네트워크를 갖게 됩니다. 클라우드 사이트에서 라우터를 통해 라우팅이 이루어집니다.

© Acronis International GmbH, 2003-2024

라우팅 작동법

클라우드 전용 모드가 설정된 경우에는 서로 다른 클라우드 네트워크에 있는 서버 간에 통신이 이루어질 수 있도록 클라우드 사이트의 라우터를 통해 라우팅이 수행됩니다.



사이트 간 OpenVPN 연결

참고

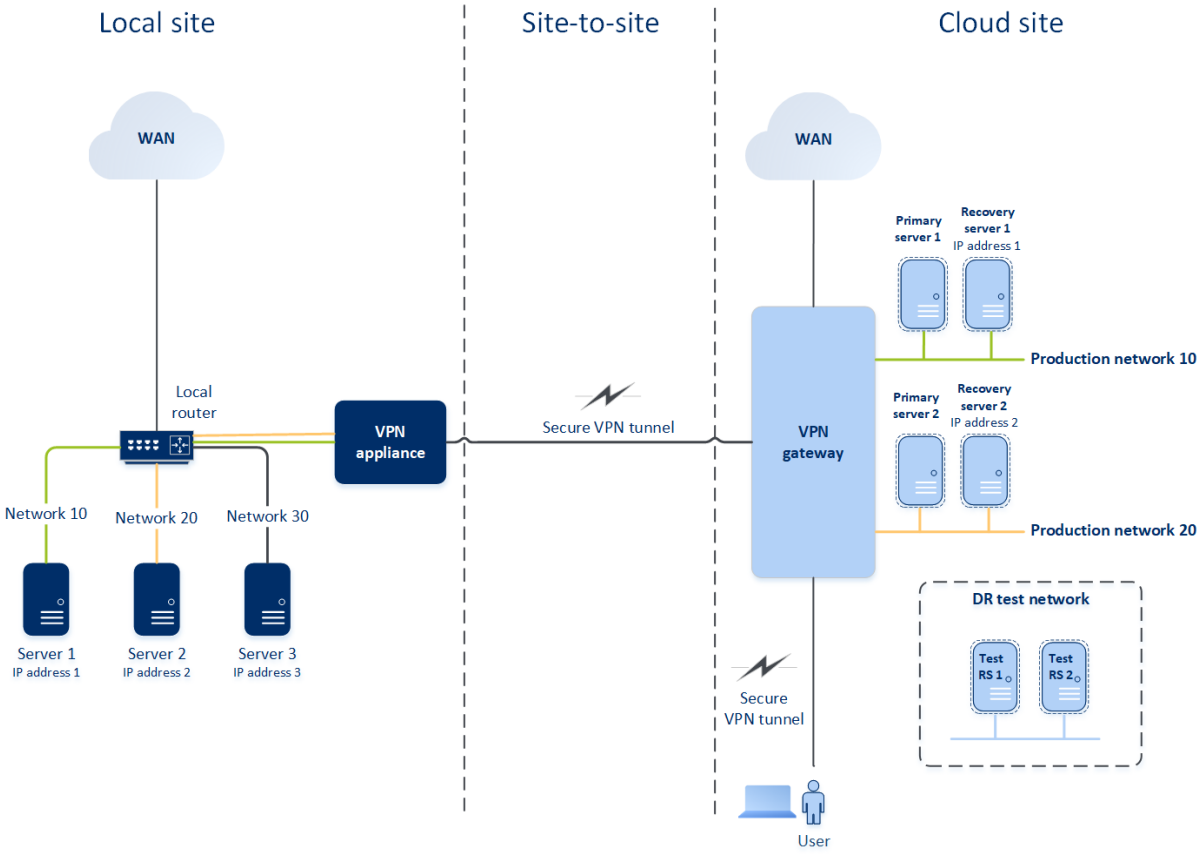
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

네트워킹이 Cyber Disaster Recovery Cloud에서 어떻게 작동하는지 이해하기 위해 로컬 사이트마다 머신이 하나씩 있는 세 개의 네트워크를 가지고 있다고 가정해 보겠습니다. 여기에서 두 개 네트워크(네트워크 10과 네트워크 20)를 위해 재해 보호 기능을 구성하려고 합니다.

아래 다이어그램에서 머신이 호스팅되고 있는 로컬 사이트와 재해 발생 시 클라우드 서버가 실행되는 클라우드 사이트를 볼 수 있습니다.

© Acronis International GmbH, 2003-2024

Cyber Disaster Recovery Cloud 솔루션을 통해 로컬 사이트에 있는 손상된 머신의 모든 워크로드를 클라우드에 있는 클라우드 서버로 장애 조치할 수 있습니다. Cyber Disaster Recovery Cloud에서는 네트워크를 23개까지 보호할 수 있습니다.



로컬 사이트와 클라우드 사이트 간에 사이트 간 OpenVPN 통신을 설정하려면 **VPN 어플라이언스**와 **VPN 게이트웨이**를 사용합니다. Cyber Protect 콘솔에서 사이트 간 OpenVPN 연결 구성을 시작하면 VPN 게이트웨이가 자동으로 클라우드 사이트에 디플로이됩니다. 그다음 로컬 사이트에 VPN 어플라이언스를 디플로이하고, 보호할 네트워크를 추가하고, 해당 어플라이언스를 클라우드에 등록해야 합니다. Cyber Disaster Recovery Cloud에서는 클라우드에서 로컬 네트워크의 복제본을 생성합니다. 보안 VPN 터널이 VPN 어플라이언스와 VPN 게이트웨이 사이에 구축됩니다. 이를 통해 로컬 네트워크가 클라우드로 확장됩니다. 클라우드의 운영 네트워크는 로컬 네트워크와 연결되어 있습니다. 로컬 서버와 클라우드 서버가 동일한 이더넷 세그먼트에 있으면 이 VPN 터널을 통해 서로 통신할 수 있습니다. 로컬 라우터로 라우팅을 수행합니다.

각 원본 머신을 보호할 수 있도록 클라우드 사이트에 복구 서버를 만들어야 합니다. 복구 서버는 장애 조치 이벤트가 발생하기 전까지 **대기** 상태로 유지됩니다. 재해가 발생하고 (**운영 모드**에서) 장애 조치 프로세스를 시작하면 보호되는 머신의 동일한 사본을 보유한 복구 서버가 클라우드에서 실행됩니다. 이 서버에는 소스 머신과 같은 IP 주소를 할당할 수 있으며, 소스 머신과 같은 이더넷 세그먼트에서 이 서버를 실행할 수 있습니다. 서버에서 백그라운드 변경의 아무런 영향 없이 클라이언트가 작업을 계속할 수 있습니다.

테스트 모드에서 장애 조치 프로세스를 시작할 수도 있습니다. 즉, 원본 머신이 계속 작동하는 동안 이와 동일한 IP 주소를 가진 복구 서버가 클라우드에서 실행될 수 있습니다. IP 주소 충돌을 방지

© Acronis International GmbH, 2003-2024

하기 위해 **테스트 네트워크**라는 특별한 가상 네트워크가 클라우드에 생성됩니다. 테스트 네트워크는 하나의 이더넷 세그먼트에서 원본 머신 IP 주소의 중복을 방지하기 위해 격리됩니다. 테스트 장애 조치 모드의 복구 서버에 액세스하려면 복구 서버를 생성할 때 **테스트 IP 주소**를 할당해야 합니다. 복구 서버에 지정할 수 있는 매개변수가 더 많이 있으며, 아래의 해당 섹션에서 이에 대해 다룹니다.

라우팅 작동법

사이트 간 연결이 설정되는 경우에는 로컬 라우터로 클라우드 네트워크 간의 라우팅을 수행합니다. VPN 서버는 서로 다른 클라우드 네트워크에 위치한 클라우드 서버 간의 라우팅을 수행하지 않습니다. 특정 네트워크의 클라우드 서버가 다른 클라우드 네트워크의 서버와 통신하길 원하는 경우, 트래픽이 VPN 터널을 통해 로컬 사이트의 로컬 라우터로 전달되고, 이 트래픽을 로컬 라우터에서 다른 네트워크로 라우팅하면 터널을 통해 클라우드 사이트의 대상 서버로 다시 전달됩니다.

VPN 게이트웨이

로컬 사이트와 클라우드 사이트 간의 통신을 가능하게 해주는 주된 컴퍼넌트는 **VPN 게이트웨이**입니다. 특수 소프트웨어가 설치된 클라우드의 가상 머신인 VPN 게이트웨이에서는 네트워크가 구체적으로 구성됩니다. VPN 게이트웨이는 다음과 같은 기능을 수행합니다.

- L2 모드에서 클라우드의 프로덕션 네트워크와 로컬 네트워크의 이더넷 세그먼트를 연결합니다.
- Iptables 및 ebtables 규칙을 제공합니다.
- 테스트 및 프로덕션 네트워크에서 머신의 기본 라우터 및 NAT 역할을 수행합니다.
- DHCP 서버 역할을 수행합니다. 운영 및 테스트 네트워크에 있는 모든 머신은 DHCP를 통해 네트워크 구성(IP 주소, DNS 설정)을 받아야 합니다. 한 클라우드 서버는 항상 DHCP 서버로부터 동일한 IP 주소를 받습니다. 사용자 정의 DNS 구성을 설정해야 하는 경우 지원 팀에 문의하십시오.
- 캐싱 DHCP 역할을 수행합니다.

VPN 게이트웨이 네트워크 구성

VPN 게이트웨이에는 여러 네트워크 인터페이스가 있습니다.

- 인터넷에 연결된 외부 인터페이스
- 운영 네트워크에 연결된 운영 인터페이스
- 테스트 네트워크에 연결된 테스트 인터페이스

또한 지점 및 사이트 간 연결과 사이트 간 연결용으로 가상 인터페이스 2개가 추가됩니다.

VPN 게이트웨이가 디플로이되고 시작되면 브리지가 하나는 외부 인터페이스용으로 그리고 다른 하나는 클라이언트 및 운영 인터페이스용으로 생성됩니다. 클라이언트-운영 브리지 및 테스트 인터페이스는 동일한 IP 주소를 사용하지만 VPN 게이트웨이는 특정 기술을 사용해 패키지를 올바르게 라우팅할 수 있습니다.

VPN 어플라이언스

VPN 어플라이언스는 특수 소프트웨어가 설치되어 있으며 특수 네트워크 구성이 적용된 Linux를 실행하는 로컬 사이트의 가상 머신입니다. 로컬 사이트와 클라우드 사이트 간의 통신을 가능하게

© Acronis International GmbH, 2003-2024

해줍니다.

복구 서버

복구 서버 – 클라우드에 저장되어 있는 보호되는 서버 백업을 기반으로 하는 원본 머신의 복제본입니다. 복구 서버는 재해 시 원본 서버의 워크로드를 전환하는 데 사용됩니다.

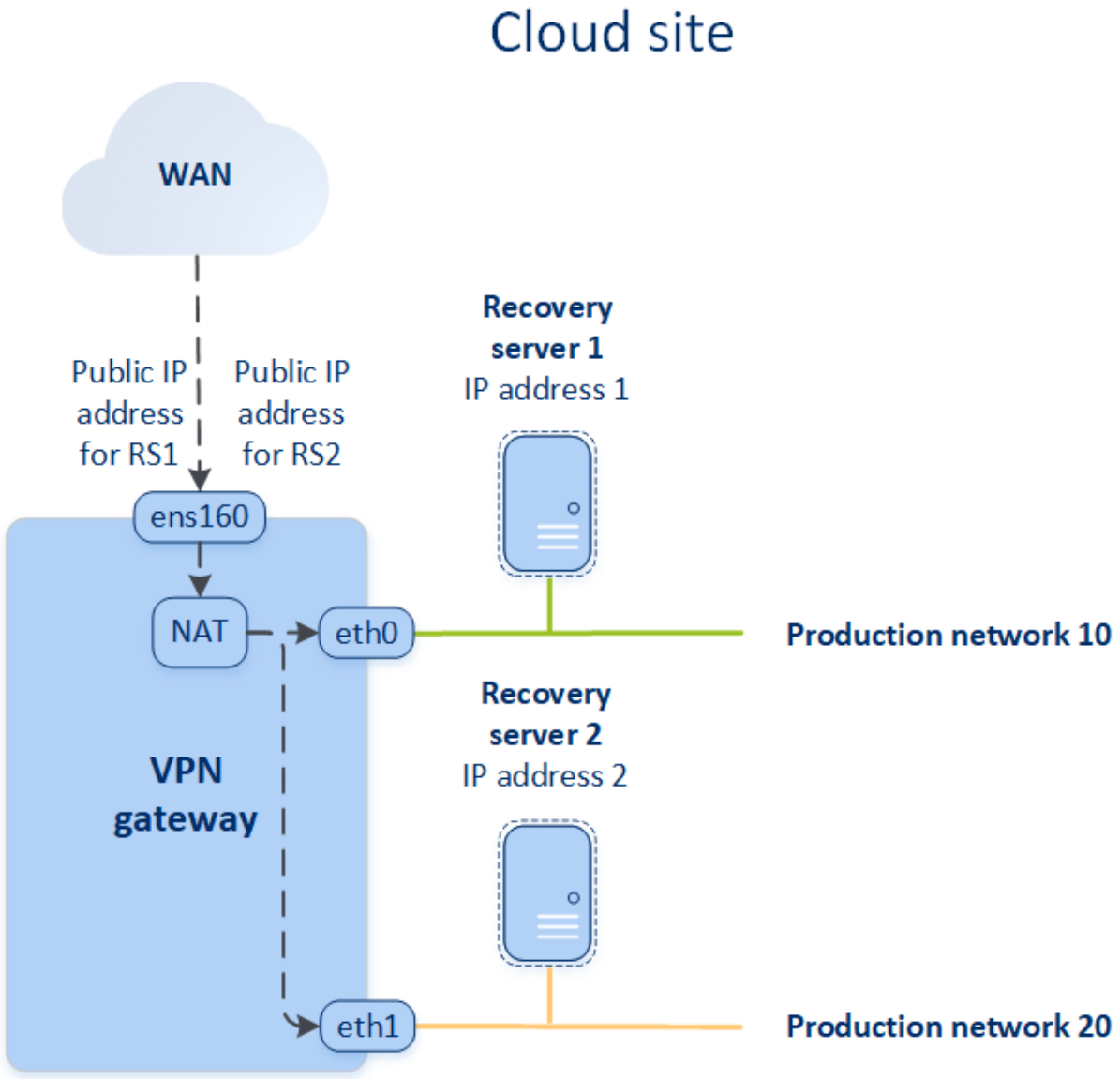
복구 서버를 만들 때 다음과 같은 네트워크 매개변수를 지정해야 합니다.

- **클라우드 네트워크**(필수): 복구 서버를 연결할 클라우드 네트워크입니다.
- **프로덕션 네트워크의 IP 주소**(필수): 복구 서버의 가상 머신을 실행하는 데 필요한 IP 주소입니다. 이 주소는 운영 네트워크와 테스트 네트워크 모두에서 사용됩니다. 실행하기 전에 가상 머신이 DHCP를 통해 IP 주소를 받도록 구성됩니다.
- **테스트 IP 주소**(선택 사항): 테스트 장애 조치 동안 클라이언트-프로덕션 네트워크에서 복구 서버에 액세스하고, 동일한 네트워크에서 프로덕션 IP 주소가 중복되는 것을 방지하는 데 필요한 IP 주소입니다. 이 IP 주소는 운영 네트워크의 IP 주소와 다릅니다. 로컬 사이트의 서버는 테스트 장애 조치 동안 테스트 IP 주소를 통해 복구 서버에 도달할 수 있지만, 그 반대 방향으로의 액세스는 불가능합니다. 복구 서버를 생성할 때 **인터넷 액세스** 옵션을 선택하면 테스트 네트워크의 복구 서버에서 인터넷 액세스가 가능합니다.
- **공용 IP 주소**(선택 사항): 인터넷에서 복구 서버에 액세스하는 데 사용되는 IP 주소입니다. 서버에 공용 IP 주소가 없는 경우 로컬 네트워크를 통해서만 접속할 수 있습니다.
- **인터넷 액세스**(선택 사항): 이를 통해 복구 서버가 인터넷에 액세스할 수 있습니다(운영 및 테스트 장애 조치 모두).

공용 및 테스트 IP 주소

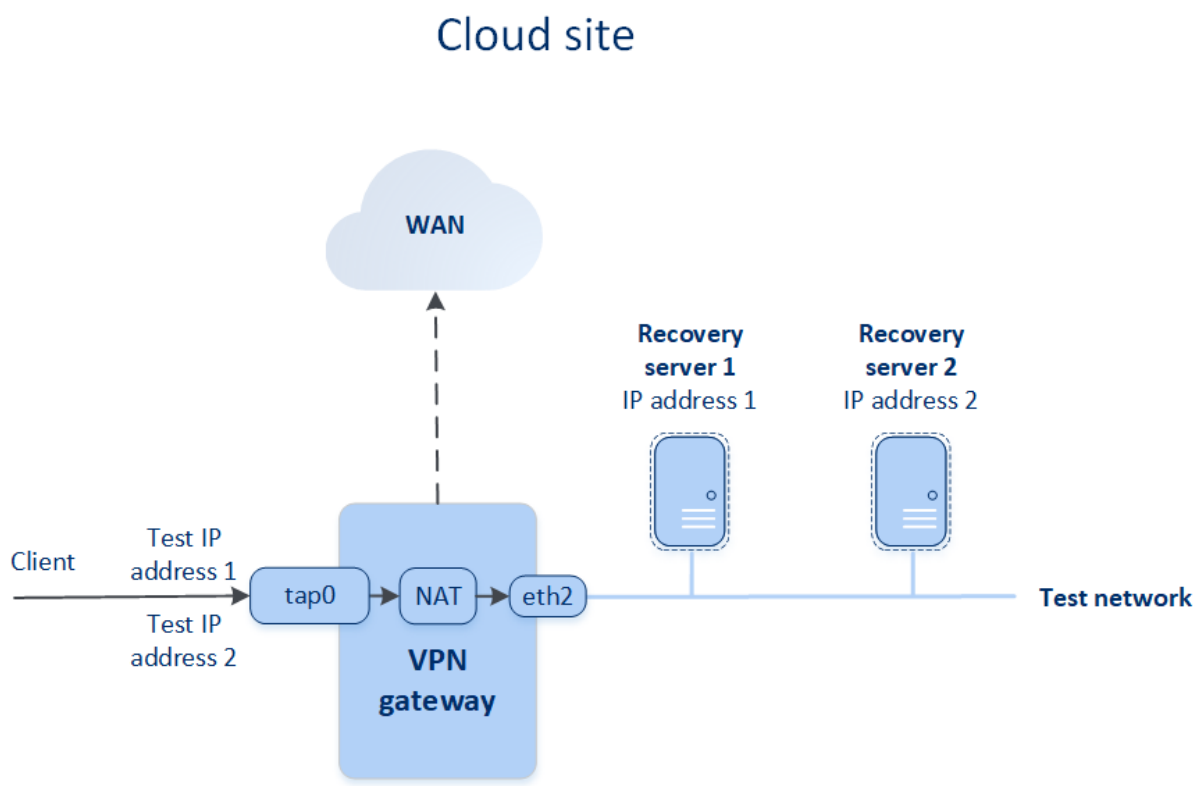
복구 서버 생성 시 공용 IP 주소를 할당하는 경우 이 IP 주소를 통해 인터넷에서 복구 서버를 사용할 수 있게 됩니다. 대상 공용 IP 주소로 인터넷에서 패킷이 수신되면 VPN 게이트웨이는 NAT를 사용하여 해당 운영 IP 주소로 이를 다시 매핑한 다음, 복구 서버로 전송합니다.

© Acronis International GmbH, 2003-2024



복구 서버 생성 시 테스트 IP 주소를 할당하는 경우 이 IP 주소를 통해 테스트 네트워크에서 복구 서버를 사용할 수 있게 됩니다. 테스트 장애 조치를 수행할 때 원본 머신이 계속 실행 중이면 같은 IP 주소를 가지는 복구 서버가 클라우드의 테스트 네트워크에서 실행됩니다. 테스트 네트워크는 격리 상태이기 때문에 IP 주소 충돌은 없습니다. 테스트 네트워크의 복구 서버는 NAT를 통해 프로덕션 IP 주소로 다시 매핑된 테스트 IP 주소를 통해 접속할 수 있습니다.

© Acronis International GmbH, 2003-2024



사이트 간 OpenVPN에 대한 자세한 내용은 "사이트 간 OpenVPN - 추가 정보"(173페이지)을(를) 참조하십시오.

기본 서버

기본 서버 – 복구 서버와 달리 로컬 사이트에 연결된 머신이 없는 가상 머신입니다. 기본 서버를 사용하여 복제를 통해 애플리케이션을 보호하거나 다양한 보조 서비스(웹 서버 등)를 실행합니다.

일반적으로 기본 서버는 중요한 애플리케이션을 실행하는 서버에서 실시간 데이터 복제에 사용됩니다 애플리케이션의 고유 도구를 사용하여 직접 복제를 설정합니다. 예를 들어, 로컬 서버와 기본 서버 간에 Active Directory 복제 또는 SQL 복제를 구성할 수 있습니다.

또는 기본 서버를 AlwaysOn 가용성 그룹(AAG) 또는 데이터베이스 가용성 그룹(DAG)에 포함시킬 수 있습니다.

두 가지 방법 모두 애플리케이션 관련 심층 지식 및 관리자 권한이 필요합니다. 기본 서버는 빠른 재해 복구 스토리지의 컴퓨팅 리소스와 공간을 지속적으로 사용합니다. 기본 서버는 직접 유지보수해야 합니다. 예를 들어 복제 모니터링, 소프트웨어 업데이트 설치, 백업 등을 직접 수행해야 합니다. 전체 서버를 클라우드에 백업하는 것과 비교하여 이점은 운영 환경에 대한 부하가 최소화된 최소 RPO 및 RTO입니다

기본 서버는 항상 운영 네트워크에서만 실행되고, 다음과 같은 네트워크 매개변수를 가집니다.

- **클라우드 네트워크**(필수): 기본 서버를 연결할 클라우드 네트워크입니다.
- **프로덕션 네트워크의 IP 주소**(필수): 기본 서버가 운영 네트워크에서 가지게 될 IP 주소입니다. 기본적으로 운영 네트워크의 첫 번째 사용 가능한 IP 주소가 설정됩니다.

© Acronis International GmbH, 2003-2024

- **공용 IP 주소**(선택 사항): 인터넷에서 기본 서버에 액세스하는 데 사용되는 IP 주소입니다. 서버에 공용 IP 주소가 없는 경우 로컬 네트워크를 통해서만 해당 서버에 접속할 수 있으며 인터넷을 통해서는 서버에 접속할 수 없습니다.
- **인터넷 액세스**(선택 사항): 기본 서버가 인터넷에 액세스할 수 있도록 해줍니다.

다중 사이트 IPsec VPN 연결

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

다중 사이트 IPsec VPN 연결을 사용하면 로컬 사이트 하나를 Cyber Disaster Recovery Cloud에 연결할 수도 있고 보안 L3 IPsec VPN 연결을 통해 여러 로컬 사이트를 연결할 수도 있습니다.

다음 사용 사례 중 하나에 해당하는 경우 재해 복구 시나리오에서 이 연결 유형을 사용하면 유용합니다.

- 로컬 사이트 하나에서 중요 워크로드를 호스팅하는 경우.
- 여러 로컬 사이트(예: 여러 위치의 사무실)에서 중요 워크로드를 호스팅하는 경우.
- 타사 소프트웨어 사이트 또는 관리되는 서비스 제공업체 사이트를 사용하며 IPsec VPN 터널을 통해 이러한 사이트에 연결하는 경우.

로컬 사이트와 클라우드 사이트 간에 다중 사이트 IPsec VPN 통신을 설정하려면 **VPN 게이트웨이**를 사용합니다. Cyber Protect 콘솔에서 다중 사이트 IPsec VPN 연결 구성을 시작하면 VPN 게이트웨이가 자동으로 클라우드 사이트에 디플로이됩니다. 그리고 나면 클라우드 네트워크 세그먼트를 구성해야 하며, 구성한 세그먼트가 로컬 네트워크 세그먼트와 겹치지 않는지 확인해야 합니다. 로컬 사이트와 클라우드 사이트 간에 보안 VPN 터널이 설정됩니다. 로컬 서버와 클라우드 서버가 동일한 이더넷 세그먼트에 있으면 이 VPN 터널을 통해 서로 통신할 수 있습니다.

각 원본 머신을 보호할 수 있도록 클라우드 사이트에 복구 서버를 만들어야 합니다. 복구 서버는 장애 조치 이벤트가 발생하기 전까지 **대기** 상태로 유지됩니다. 재해가 발생하고 (**운영 모드**에서) 장애 조치 프로세스를 시작하면 보호되는 머신의 동일한 사본을 보유한 복구 서버가 클라우드에서 실행됩니다. 서버에서 백그라운드 변경의 아무런 영향 없이 클라이언트가 작업을 계속할 수 있습니다.

테스트 모드에서 장애 조치 프로세스를 실행할 수도 있습니다. 즉, 소스 머신은 계속 작동하며 클라우드에 생성된 특수 가상 네트워크(**테스트 네트워크**)에서 개별 복구 서버가 실행됩니다. 테스트 네트워크는 IP 주소가 다른 클라우드 네트워크 세그먼트의 IP 주소와 중복되지 않도록 격리됩니다.

VPN 게이트웨이

로컬 사이트와 클라우드 사이트 간의 통신을 가능하게 해주는 주된 구성 요소는 **VPN 게이트웨이**입니다. 이는 특별한 소프트웨어가 설치된 클라우드 내의 가상 머신으로, 네트워크가 특별하게 구성됩니다. VPN 게이트웨이는 다음과 같은 기능을 수행합니다.

- L2 IPsec 모드에서 클라우드의 프로덕션 네트워크와 로컬 네트워크의 이더넷 세그먼트를 연결합니다.

© Acronis International GmbH, 2003-2024

- 테스트 및 프로덕션 네트워크에서 머신의 기본 라우터 및 NAT 역할을 수행합니다.
- DHCP 서버 역할을 수행합니다. 운영 및 테스트 네트워크에 있는 모든 머신은 DHCP를 통해 네트워크 구성(IP 주소, DNS 설정)을 받아야 합니다. 한 클라우드 서버는 항상 DHCP 서버로부터 동일한 IP 주소를 받습니다.

  원하는 경우 사용자 정의 DNS 구성을 설정할 수 있습니다. 자세한 내용은 "사용자 정의 DNS 서버 구성"(700페이지)을(를) 참조하십시오.
- 캐싱 DHCP 역할을 수행합니다.

라우팅 작동법

서로 다른 클라우드 네트워크에 있는 서버 간에 통신이 이루어질 수 있도록 클라우드 사이트의 라우터를 통해 라우팅이 수행됩니다.

지점 및 사이트 간 원격 VPN 액세스

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

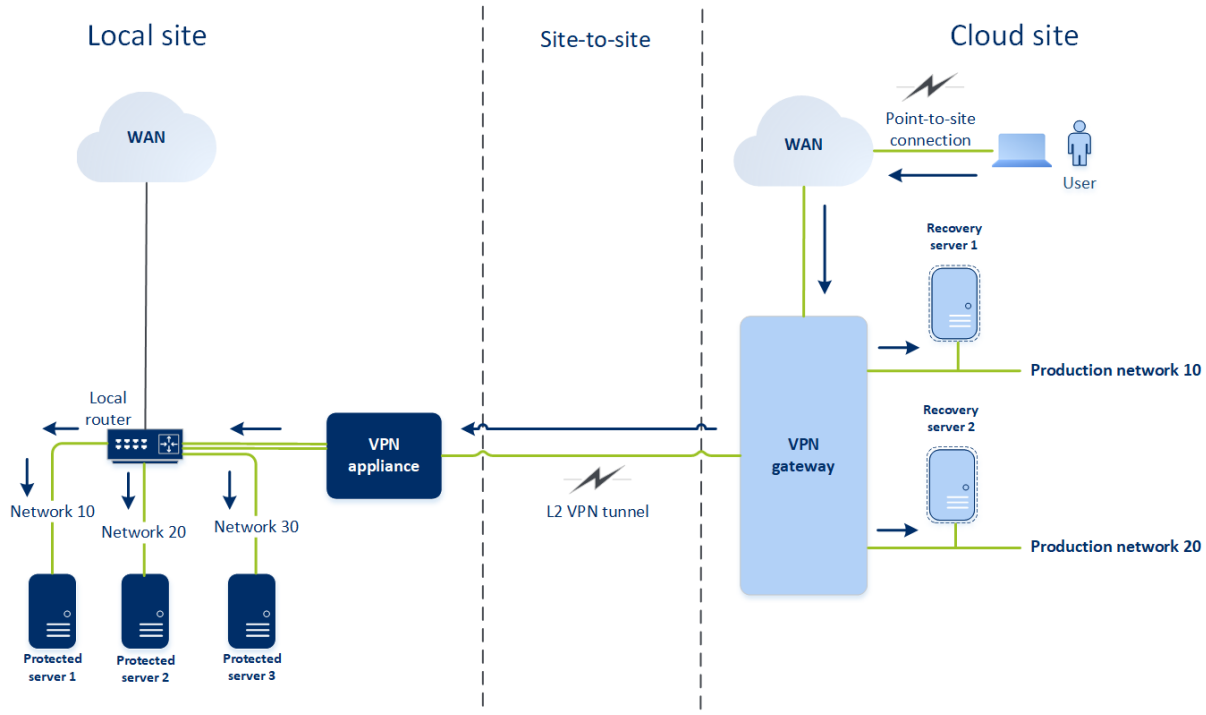
지점 및 사이트 간 연결은 VPN을 통해 외부에서 엔드포인트 장치(컴퓨터나 랩톱)를 사용하여 클라우드 사이트 및 로컬 사이트에 접속할 수 있는 안전한 연결입니다. Cyber Disaster Recovery Cloud 사이트에 대한 사이트 간 OpenVPN 연결을 설정하고 나면 이 연결을 사용할 수 있습니다. 이러한 유형의 연결은 다음과 같은 경우 유용합니다.

- 많은 회사의 경우 기업 네트워크에서만 기업 서비스와 웹 리소스를 이용할 수 있습니다. 지점 및 사이트 간 연결을 사용하면 로컬 사이트로 안전하게 연결할 수 있습니다.
- 재해 발생 시 워크로드가 클라우드 사이트로 전환되고 로컬 네트워크가 다운되면 클라우드 서버에 대한 직접 액세스가 필요할 수 있습니다. 이는 클라우드 사이트에 대한 지점 및 사이트 간 연결을 통해 가능합니다.

로컬 사이트에 대한 지점 및 사이트 간 연결을 사용하려면 로컬 사이트에 VPN 어플라이언스를 설치하고 사이트 간 연결을 구성한 다음 로컬 사이트에 대해 지점 및 사이트 간 연결을 설정해야 합니다. 이렇게 하면 원격 직원은 L2 VPN을 통해 기업 네트워크에 대한 액세스 권한을 갖게 됩니다.

아래 구성표에는 로컬 사이트, 클라우드 사이트 및 서버 간 통신이 초록색으로 강조 표시되어 있습니다. L2 VPN 터널은 로컬 사이트와 클라우드 사이트를 연결합니다. 사용자가 지점 및 사이트 간 연결을 설정하면 로컬 사이트로의 통신은 클라우드 사이트를 통해 수행됩니다.

© Acronis International GmbH, 2003-2024



지점 및 사이트 간 구성에서는 인증서를 사용하여 VPN 클라이언트를 인증합니다. 또한, 사용자 자격 증명도 인증에 사용됩니다. 로컬 사이트로의 지점 및 사이트 간 연결에 대한 다음 정보를 참고하십시오.

- VPN 클라이언트에서 인증하려는 사용자는 Cyber Protect Cloud 자격 증명을 사용해야 합니다. 이때 "회사 관리자" 또는 "사이버 보호" 사용자 역할이 필요합니다.
- OpenVPN 구성을 다시 생성한 경우에는 클라우드 사이트에 대한 지점 및 사이트 간 연결을 사용하는 모든 사용자의 업데이트된 구성을 제공해야 합니다.

클라우드 사이트에서 사용되지 않은 고객 환경의 자동 삭제

재해 복구 서비스는 재해 복구 목적으로 생성된 고객 환경의 사용을 추적하며 해당 환경이 사용되지 않는 경우 자동으로 삭제합니다.

고객 테넌트의 활성 여부를 정의하는 데 다음 기준이 사용됩니다.

- 현재 하나 이상의 클라우드 서버가 있거나 지난 7일 내에 클라우드 서버가 있었습니다.
  또는
- **로컬 사이트로의 VPN 액세스** 옵션이 활성화되었으며 사이트 간 OpenVPN 터널이 설정되었거나 지난 7일 동안 VPN 어플라이언스에서 보고한 데이터가 있습니다.

그 외의 테넌트는 모두 비활성 테넌트로 간주됩니다. 이러한 테넌트에 대해 시스템은 다음 작업을 수행합니다.

- VPN 게이트웨이 및 테넌트와 관련된 모든 클라우드 리소스를 삭제합니다.
- VPN 어플라이언스를 등록 해제합니다.

비활성 클라이언트는 연결이 구성되기 전의 상태로 롤백됩니다.

© Acronis International GmbH, 2003-2024

최초 연결 구성

이 섹션에서는 연결 구성 시나리오에 대해 설명합니다.

클라우드 전용 모드 구성

클라우드 전용 모드에서 연결을 구성하려면

1. Cyber Protect 콘솔에서 **재해 복구** > **연결**로 이동합니다.
2. **클라우드 전용**을 선택하고 **구성**을 클릭합니다.
   그러면 정의된 주소 및 마스크를 가진 VPN 게이트웨이와 클라우드 네트워크가 클라우드 사이트에 디플로이됩니다.

클라우드에서 네트워크를 관리하고 VPN 게이트웨이 설정을 설정하는 자세한 방법은 "관리 클라우드 네트워크"를 참조하십시오.

사이트 간 OpenVPN 구성

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

VPN 어플라이언스에 대한 요구사항

시스템 요구 사항

- 1 CPU
- 1 GB RAM
- 8 GB 디스크 공간

포트

- TCP 443 (아웃바운드) - VPN 연결용
- TCP 80 (아웃바운드) - 어플라이언스의 자동 업데이트용

방화벽 및 네트워크 보안 시스템의 다른 컴포넌트가 이러한 포트를 통해 IP 주소에 연결하도록 허용하는지 확인합니다.

사이트 간 OpenVPN 연결 구성

VPN 어플라이언스는 안전한 VPN 터널을 통해 로컬 네트워크를 클라우드로 확장합니다. 이러한 유형의 연결을 대개 "사이트 간"(S2S) 연결이라고 합니다. 아래 절차를 따르거나 비디오 자습서를 시청할 수 있습니다.

VPN 어플라이언스를 통한 연결을 구성하려면

1. Cyber Protect 콘솔에서 **재해 복구** > **연결**로 이동합니다.
2. **사이트 간 OpenVPN 연결**을 선택하고 **구성**을 클릭합니다.

© Acronis International GmbH, 2003-2024

시스템은 클라우드에 VPN 게이트웨이를 디플로이하기 시작합니다. 이 절차는 약간의 시간이 소요됩니다. 한편 다음 단계로 진행할 수 있습니다.

참고
VPN 게이트웨이는 추가 비용 없이 제공됩니다. 재해 복구 기능을 사용하지 않을 경우 삭제됩니다. 즉, 기본 또는 복구 서버가 7일 동안 클라우드에 없는 경우입니다.

3. **VPN 어플라이언스** 블록에서 **다운로드 및 디플로이**를 클릭합니다. 사용 중인 가상화 플랫폼에 따라 VMware vSphere 또는 Microsoft Hyper-V용 VPN 어플라이언스를 다운로드하십시오.
4. 어플라이언스를 디플로이하고 운영 네트워크에 연결합니다.

   vSphere에서 VPN 어플라이언스를 운영 네트워크에 연결하는 모든 가상 스위치에 대해 **무차별 모드** 및 **위조 전송**이 활성화되어 있고 **수락**으로 설정되어 있는지 확인하십시오. 이러한 설정에 액세스하려면 vSphere Client에서 호스트 > **요약** > **네트워크**를 선택한 다음, 스위치 > **설정 편집...** > **보안**을 선택합니다.

   Hyper-V에서 1024MB 메모리가 있는 **1세대** 가상 머신을 만듭니다. 또한, 머신에서 **동적 메모리**를 활성화하는 것이 좋습니다. 머신이 생성되면 **설정** > **하드웨어** > **네트워크 어댑터** > **고급 기능**으로 이동하여 **MAC 주소 스푸핑 활성화** 확인란을 선택합니다.
5. 어플라이언스를 켭니다.
6. 어플라이언스 콘솔을 열고 "admin"/"admin" 사용자 이름과 패스워드로 로그인합니다.
7. [선택 사항]패스워드를 변경합니다.
8. [선택 사항] 필요 시 네트워크 설정을 변경하십시오. 인터넷 연결을 위한 WAN으로 사용할 인터페이스를 정의합니다.
9. 회사 관리자의 자격 증명을 사용하여 어플라이언스를 Cyber Protection 서비스에 등록합니다. 이 자격 증명은 인증서를 검색할 때 한 번만 사용됩니다. 데이터 센터 URL은 사전 정의됩니다.

참고
2단계 인증이 계정에 구성되어 있는 경우 TOTP 코드를 입력하라는 메시지가 뜰 수도 있습니다. 2단계 인증이 활성화되어 있지만 계정에 구성되어 있지 않다면 VPN 어플라이언스를 등록할 수 없습니다. 우선 Cyber Protect 콘솔 로그인 페이지로 이동하여 계정에 대한 2단계 인증 구성을 완료해야 합니다. 2단계 인증에 대한 자세한 내용은 관리 포털 관리자 안내서를 참조하십시오.

구성을 완료하고 나면 어플라이언스가 **온라인** 상태로 표시됩니다. 어플라이언스가 VPN 게이트웨이에 연결되고, 모든 활성 인터페이스에서 Cyber Disaster Recovery Cloud 서비스로 네트워크에 관한 정보를 보고하기 시작합니다. Cyber Protect 콘솔이 VPN 어플라이언스의 정보를 기반으로 인터페이스를 표시합니다.

다중 사이트 IPsec VPN 구성

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

다음의 두 가지 방법으로 다중 사이트 IPsec VPN 연결을 구성할 수 있습니다.

© Acronis International GmbH, 2003-2024

- **재해 복구** > **연결** 탭에서 구성.
- 장치 하나 또는 여러 개에 보호 계획을 적용한 다음 자동으로 생성된 사이트 간 OpenVPN 연결에서 다중 사이트 IPsec VPN 연결로 수동 전환합니다. 그런 다음 다중 사이트 IPsec VPN 설정을 구성하고 IP 주소를 다시 할당합니다.

연결 탭에서 다중 사이트 IPsec VPN 연결을 구성하려면

1. Cyber Protect 콘솔에서 **재해 복구** > **연결**로 이동합니다.
2. **다중 사이트 VPN 연결** 섹션에서 **구성**을 클릭합니다.
   VPN 게이트웨이는 클라우드 사이트에 디플로이됩니다.
3. 다중 사이트 IPsec VPN 설정을 구성합니다.

보호 계획에서 다중 사이트 IPsec VPN 연결을 구성하려면

1. Cyber Protect 콘솔에서 **장치**로 이동합니다.
2. 목록의 장치 하나 또는 여러 개에 보호 계획을 적용합니다.
   사이트 간 OpenVPN 연결용으로 복구 서버 및 클라우드 인프라 설정이 자동 구성됩니다.
3. **재해 복구** > **연결**로 이동합니다.
4. **속성 표시**를 클릭합니다.
5. **다중 사이트 IPsec VPN으로 전환**을 클릭합니다.
6. 다중 사이트 IPsec VPN 설정을 구성합니다.
7. 클라우드 네트워크 및 클라우드 서버의 IP 주소를 다시 할당합니다.

다중 사이트 IPsec VPN 설정 구성

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

다중 사이트 IPsec VPN을 구성한 후에는 **재해 복구** > **연결** 탭에서 클라우드 사이트 및 로컬 사이트 설정을 구성해야 합니다.

사전 요구 사항

- 다중 사이트 IPsec VPN 연결이 구성됩니다. 다중 사이트 IPsec VPN 연결 구성에 대한 자세한 내용은 "다중 사이트 IPsec VPN 구성"(686페이지) 항목을 참조하십시오.
- 각 로컬 IPsec VPN 게이트웨이에는 공용 IP 주소가 있습니다.
- 클라우드 네트워크에는 운영 네트워크 내 보호되는 머신의 사본인 클라우드 서버 및 복구 서버(필요에 따라 각 서버에 IP 주소 1~2개 사용)에 사용할 수 있는 충분한 IP 주소가 있습니다.
- [로컬 사이트와 클라우드 사이트 간에 방화벽을 사용하는 경우] 로컬 사이트에서 다음 IP 프로토콜 및 UDP 포트가 허용됩니다. IP 프로토콜 ID 50(ESP), UDP 포트 500(IKE), UDP 포트 4500.
- 로컬 사이트의 NAT-T 구성은 비활성화됩니다.

다중 사이트 IPsec VPN 연결을 구성하려면

© Acronis International GmbH, 2003-2024

1. 클라우드 사이트에 네트워크를 하나 이상 추가합니다.
   a. **네트워크 추가**를 클릭합니다.

      참고
      클라우드 네트워크를 추가하면 테스트 장애 조치 수행을 위해 네트워크 주소와 마스크가 동일한 해당 테스트 네트워크가 자동으로 추가됩니다. 테스트 네트워크의 클라우드 서버 IP 주소는 클라우드 프로덕션 네트워크의 주소와 같습니다. 테스트 장애 조치 중에 프로덕션 네트워크에서 클라우드 서버에 액세스해야 하는 경우 복구 서버를 생성할 때 두 번째 테스트 IP 주소를 할당하십시오.

   b. **네트워크 주소** 필드에 네트워크의 IP 주소를 입력합니다.
   c. **네트워크 마스크** 필드에 네트워크의 마스크를 입력합니다.
   d. **추가**를 클릭합니다.
2. 로컬 사이트용 권장 사항에 따라 클라우드 사이트에 연결하려는 각 로컬 사이트의 설정을 구성합니다. 이러한 권장 사항에 대한 자세한 내용은 "로컬 사이트 관련 일반 권장 사항"(689페이지)을(를) 참조하십시오.
   a. **연결 추가**를 클릭합니다.
   b. 로컬 VPN 게이트웨이의 이름을 입력합니다.
   c. 로컬 VPN 게이트웨이의 공용 IP 주소를 입력합니다.
   d. [선택 사항] 로컬 VPN 게이트웨이의 설명을 입력합니다.
   e. **다음**을 클릭합니다.
   f. **사전에 공유된 키** 필드에 사전에 공유된 키를 입력합니다. 자동으로 생성된 값을 사용하려면 **사전에 공유된 키 새로 생성**을 클릭합니다.

      참고
      로컬 및 클라우드 VPN 게이트웨이에 같은 사전에 공유된 키를 사용해야 합니다.

   g. **IPsec/IKE 보안 설정**을 클릭하여 설정을 구성합니다. 구성할 수 있는 설정에 대한 자세한 내용은 "IPsec/IKE 보안 설정"(689페이지)을(를) 참조하십시오.

      참고
      자동으로 입력되는 기본 설정을 사용할 수도 있고 사용자 정의 값을 사용할 수도 있습니다. IKEv2 프로토콜 연결만 지원됩니다. VPN 설정 시의 기본 **시작 작업**은 **추가**(로컬 VPN 게이트웨이가 연결을 시작함)입니다. 그러나 기본값을 **시작**(클라우드 VPN 게이트웨이가 연결을 시작함) 또는 **경로**(경로 옵션을 지원하는 방화벽에 적합함)로 변경할 수 있습니다.

   h. **네트워크 정책**을 구성합니다.
      네트워크 정책에 따라 IPsec VPN이 연결하는 네트워크가 지정됩니다. CIDR 형식을 사용하여 네트워크의 IP 주소와 마스크를 입력합니다. 로컬 및 클라우드 네트워크 세그먼트가 겹치면 안 됩니다.
   i. **저장**을 클릭합니다.

© Acronis International GmbH, 2003-2024

로컬 사이트 관련 일반 권장 사항

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

다중 사이트 IPsec VPN 연결용으로 로컬 사이트를 구성할 때는 다음 권장 사항을 고려하십시오.

- 각 IKE 단계에서 다음 매개변수용으로 클라우드 사이트에 구성되어 있는 값 중 하나 이상을 설정합니다. 암호화 알고리즘, 해시 알고리즘, Diffie-Hellman 그룹 번호.
- IKE 단계 2용으로 클라우드 사이트에 구성되어 있는 Diffie-Hellman 그룹 번호의 값 중 하나 이상을 사용하여 Perfect Forward Secrecy를 활성화합니다.
- IKE 단계 1 및 IKE 단계 2에 클라우드 사이트와 같은 **수명** 값을 구성합니다.
- NAT 트래버설(NAT-T)을 사용하는 구성은 지원되지 않습니다. 로컬 사이트에서 NAT-T 구성을 비활성화하십시오. 이렇게 하지 않으면 추가 UDP 캡슐화를 협상할 수 없습니다.
- **시작 작업** 구성에 따라 연결이 시작되는 쪽이 정의됩니다. 기본값인 **추가**를 사용하는 경우 로컬 사이트에서 연결이 시작되며 클라우드 사이트는 연결 시작을 대기합니다. 클라우드 사이트에서 연결이 시작되도록 하려면 값을 **시작**으로 변경합니다. 양쪽이 모두 연결을 시작할 수 있도록 하려면 값을 **경로**로 변경합니다. 경로 옵션을 지원하는 방화벽의 경우에는 이 값이 적합합니다.

다양한 솔루션에 대한 자세한 내용과 구성 예제는 다음 페이지를 참조하십시오.

- 이 기술 자료 문서 시리즈
- 이 비디오 예제:

IPsec/IKE 보안 설정

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

다음 표에는 IPsec/IKE 보안 매개변수에 대한 자세한 내용이 나와 있습니다.

매개변수	설명
암호화 알고리즘	전송 중인 데이터를 확인할 수 없도록 하는 데 사용할 암호화 알고리즘입니다. 기본적으로는 모든 알고리즘이 선택되어 있습니다. 각 IKE 단계용으로 로컬 게이트웨이 장치에서 선택한 알고리즘 중 하나 이상을 구성해야 합니다.
해시 알고리즘	데이터의 무결성과 신뢰성(Authenticity)을 확인하는 데 사용할 해시 알고리즘입니다. 기본적으로는 모든 알고리즘이 선택되어 있습니다. 각 IKE 단계용으로 로컬 게이트웨이 장치에서 선택한 알고리즘 중 하나 이상을 구성해야 합니다.
Diffie-Hellman 그룹 번호	Diffie-Hellman 그룹 번호에 따라 IKE(Internet Key

© Acronis International GmbH, 2003-2024

매개변수	설명
	Exchange) 프로세스에서 사용되는 키의 안전성이 정의됩니다. 그룹 번호가 높을수록 안전성도 높아지지만 키 계산 시간은 더 길어집니다. 기본적으로는 모든 그룹이 선택되어 있습니다. 각 IKE 단계용으로 로컬 게이트웨이 장치에서 선택한 그룹 중 하나 이상을 구성해야 합니다.
수명(초)	수명 값에 따라 사용자 패킷용 암호화/인증 키 세트를 사용하는 연결 인스턴스에서 협상 완료부터 만료까지의 기간이 결정됩니다. 1단계의 범위: 900-28800초(기본값: 28800초)입니다. 2단계의 범위는 900-3600초(기본값: 3600초)입니다. 2단계의 수명은 1단계의 수명보다 짧아야 합니다. 연결이 만료되기 전에 키 생성 채널을 통해 다시 협상됩니다. **키 다시 생성 예비 시간**을 참조하십시오. 로컬 측과 원격 측이 수명에 동의하지 않으면 수명이 더 긴 측에서 일련의 대체 연결이 설정됩니다. **키 다시 생성 예비 시간** 및 **키 다시 생성 퍼지**도 참조하십시오.
키 다시 생성 예비 시간(초)	연결이나 키 생성 채널이 만료될 때까지의 예비 시간입니다. 이 시간 동안 VPN 연결의 로컬 측에서 키 대체 협상을 시도합니다. 정확한 키 다시 생성 시간은 **키 다시 생성 퍼지** 값에 따라 임의로 선택됩니다. 로컬에서만 사용되며 원격 측에서는 이 비율을 사용하지 않아도 됩니다. 범위는 900-3600초입니다. 기본값은 3600입니다.
재생 창 크기(패킷)	이 연결의 IPsec 재생 창 크기입니다. 기본값인 -1을 적용하면 strongswan.conf 파일의 charon.replay_window를 사용하여 값을 구성합니다. 32보다 큰 값은 Netlink 백엔드 사용 시에만 지원됩니다. 값을 0으로 설정하면 Psec 재생 보호가 비활성화됩니다.
키 다시 생성 퍼지(%)	키 다시 생성 간격을 임의로 설정하기 위해 예비 바이트, 예비 패킷 및 예비 시간이 무작위로 증가

© Acronis International GmbH, 2003-2024

매개변수	설명
	하는 최대 비율입니다(연결이 많은 호스트에서 중요함). 키 다시 생성 퍼지 값은 100%를 초과할 수 있습니다. 무작위로 증가한 marginTYPE 값은 lifeTYPE을 초과할 수 없습니다. 여기서 TYPE은 바이트, 패킷, 시간 중 하나입니다. 값을 0%로 지정하면 무작위 증가가 비활성화됩니다. 로컬에서만 사용되며 원격 측에서는 이 비율을 사용하지 않아도 됩니다.
DPD 시간 초과(초)	DPD(Dead Peer Detection) 시간이 초과될 때까지의 시간입니다. 30 이상의 값을 지정할 수 있습니다. 기본값은 30입니다.
DPD(Dead Peer Detection) 시간 초과 작업	DPD(Dead Peer Detection) 시간이 초과된 후에 수행할 작업입니다. **다시 시작** - DPD 시간이 초과되면 세션을 다시 시작합니다. **지우기** - DPD 시간이 초과되면 세션을 종료합니다. **없음** - DPD 시간이 초과되어도 아무런 작업을 수행하지 않습니다.
시작 작업	연결을 시작하고 VPN 연결용 터널을 설정하는 측을 결정합니다. **추가** - 로컬 VPN 게이트웨이가 연결을 시작합니다. **시작** - 클라우드 VPN 게이트웨이가 연결을 시작합니다. **경로** - 경로 옵션을 지원하는 VPN 게이트웨이에 적합한 옵션입니다. 로컬 VPN 게이트웨이나 클라우드 VPN 게이트웨이에서 시작되는 트래픽이 있을 때만 터널이 작동합니다.

Active Directory 도메인 서비스 사용 가능성 관련 권장 사항

도메인 컨트롤러에서 보호된 워크로드를 인증해야 하는 경우에는 재해 복구 사이트에 AD DC(Active Directory 도메인 컨트롤러) 인스턴스를 생성하는 것이 좋습니다.

L2 OpenVPN 연결용 Active Directory 도메인 컨트롤러

L2 OpenVPN 연결을 설정하면 테스트 장애 조치 또는 프로덕션 장애 조치 중에 보호된 워크로드의 IP 주소가 클라우드 사이트에 보존됩니다. 따라서 테스트 장애 조치 또는 프로덕션 장애 조치 중에

© Acronis International GmbH, 2003-2024

AD DC의 IP 주소가 로컬 사이트와 동일하게 설정됩니다.

사용자 정의 DNS를 사용하면 모든 클라우드 서버용으로 고유한 사용자 정의 DNS 서버를 설정할 수 있습니다. 자세한 내용은 "사용자 정의 DNS 서버 구성"(700페이지)을(를) 참조하십시오.

L2 IPsec VPN 연결용 Active Directory 도메인 컨트롤러

L3 IPsec 연결을 설정하면 보호된 워크로드의 IP 주소가 클라우드 사이트에 보존되지 않습니다. 따라서 프로덕션 장애 조치를 수행하기 전에 클라우드 사이트에서 전용 AD DC 인스턴스를 기본 서버로 추가 생성하는 것이 좋습니다.

클라우드 사이트에서 기본 서버로 구성하는 전용 AD DC 인스턴스 관련 권장 사항은 다음과 같습니다.

- Windows 방화벽을 끕니다.
- Active Directory 서비스에 기본 서버를 연결합니다.
- 기본 서버가 인터넷에 액세스할 수 있는지 확인합니다.
- Active Directory 기능을 추가합니다.

사용자 정의 DNS를 사용하면 모든 클라우드 서버용으로 고유한 사용자 정의 DNS 서버를 설정할 수 있습니다. 자세한 내용은 "사용자 정의 DNS 서버 구성"(700페이지)을(를) 참조하십시오.

지점 및 사이트 간 원격 VPN 액세스 구성

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

원격으로 로컬 사이트에 연결해야 하는 경우, 로컬 사이트에 대한 지점 및 사이트 간 연결을 구성할 수 있습니다. 아래 절차를 따르거나 비디오 자습서를 시청할 수 있습니다.

사전 요구 사항

- 사이트 간 OpenVPN 연결이 구성됩니다.
- VPN 어플라이언스는 로컬 사이트에 설치됩니다.

로컬 사이트로의 지점 및 사이트 간 연결을 구성하려면

1. Cyber Protect 콘솔에서 **재해 복구** > **연결**로 이동합니다.
2. **속성 표시**를 클릭합니다.
3. **로컬 사이트로의 VPN 액세스** 옵션을 활성화합니다.
4. 로컬 사이트로의 지점 및 사이트 간 연결을 설정해야 하는 사용자가 다음 항목을 소유하고 있는지 확인합니다.
   - Cyber Protect Cloud의 사용자 계정. 이러한 자격 증명은 VPN 클라이언트에서의 인증에 사용됩니다. 사용자 계정이 없다면 Cyber Protect Cloud에서 사용자 계정을 생성합니다.
   - "회사 관리자" 또는 "사이버 보호" 사용자 역할.
5. OpenVPN 클라이언트를 구성합니다.

© Acronis International GmbH, 2003-2024

a. https://openvpn.net/community-downloads/에서 OpenVPN 클라이언트 버전 2.4.0 이상을 다운로드합니다.
b. 로컬 사이트에 연결하려는 머신에 OpenVPN 클라이언트를 설치합니다.
c. **OpenVPN 구성 다운로드**를 클릭합니다. 구성 파일은 "회사 관리자" 또는 "사이버 보호" 사용자 역할을 가진 조직 내 사용자에게 유효합니다.
d. 다운로드한 구성을 OpenVPN으로 가져옵니다.
e. Cyber Protect Cloud 사용자 자격 증명을 사용하여 OpenVPN 클라이언트에 로그인합니다(위의 4단계 참조).
f. [선택 사항] 조직에 대한 2단계 인증이 활성화되면 일회성으로 생성되는 TOTP 코드를 제공해야 합니다.

중요
계정의 2단계 인증을 활성화한 후 구성 파일을 다시 생성하고 기존 OpenVPN 클라언트에 대해 갱신해야 합니다. 계정에 대한 2단계 인증을 설정하려는 사용자는 Cyber Protect Cloud에 다시 로그인해야 합니다.

결과적으로, 사용자는 로컬 사이트에서 머신에 연결할 수 있습니다.

네트워크 관리

이 섹션에서는 네트워크 관리 시나리오에 대해 설명합니다.

네트워크 관리

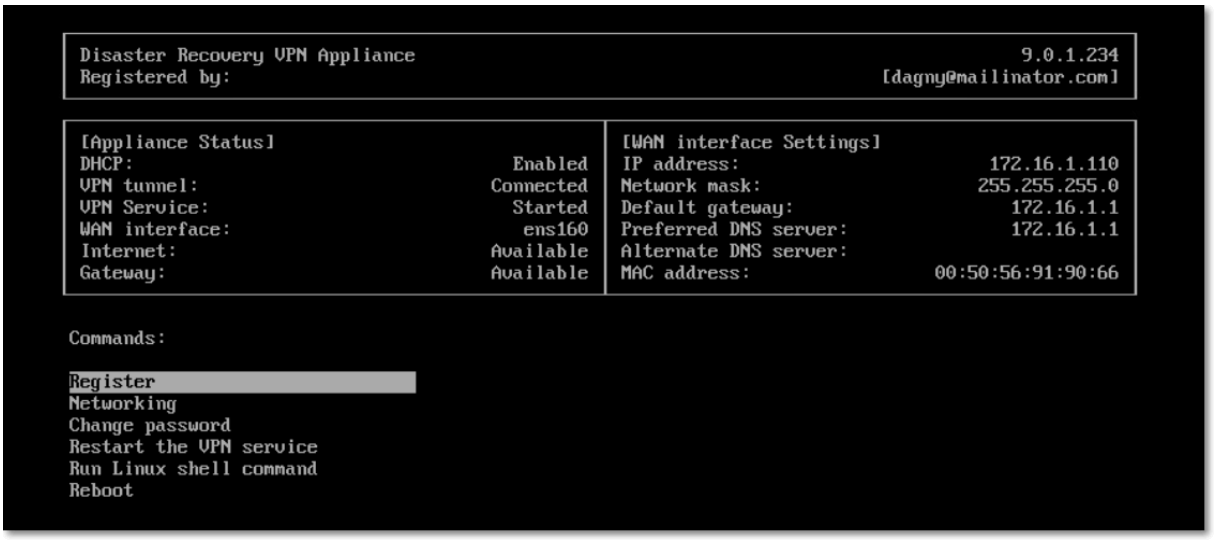
참고
일부 기능을 사용하려면 적용되는 라이센스 모델에 따라 추가 라이센스가 필요할 수 있습니다.

사이트 간 OpenVPN 연결

네트워크를 로컬 사이트에 추가하고 클라우드로 확장하려면

1. VPN 어플라이언스에서 클라우드로 확장하려는 로컬 네트워크에 새로운 네트워크 인터페이스를 설정합니다.
2. VPN 어플라이언스 콘솔에 로그인합니다.
3. **네트워킹** 섹션에서 새 인터페이스의 네트워크 설정을 설정합니다.

© Acronis International GmbH, 2003-2024



VPN 어플라이언스가 모든 활성 인터페이스에서 Cyber Disaster Recovery Cloud에 네트워크에 관한 정보를 보고하기 시작합니다. Cyber Protect 콘솔이 VPN 어플라이언스의 정보를 기반으로 인터페이스를 표시합니다.

클라우드로 확장한 네트워크를 삭제하려면

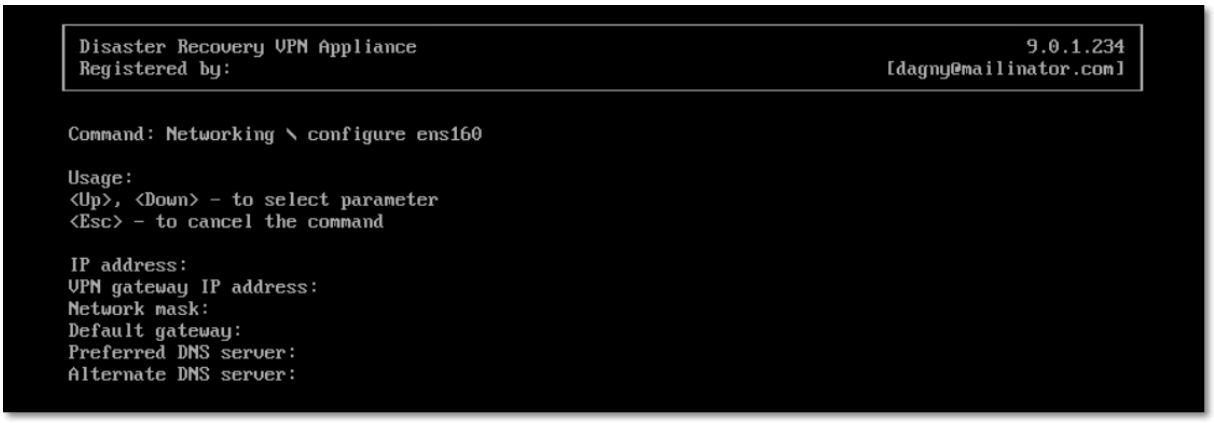
1. VPN 어플라이언스 콘솔에 로그인합니다.
2. **네트워킹** 섹션에서 삭제할 인터페이스를 선택하고, **네트워크 설정 지우기**를 클릭합니다.
3. 작업을 확인합니다.

그러면 보안 VPN 터널을 통한 클라우드로의 로컬 네트워크 확장이 중지됩니다. 이 네트워크는 독립 클라우드 세그먼트로 작동합니다. 이 인터페이스가 클라우드 사이트 간 트래픽 전송에 사용되는 경우 해당 클라우드 사이트 간 모든 네트워크 연결이 끊깁니다.

네트워크 매개변수를 변경하려면

1. VPN 어플라이언스 콘솔에 로그인합니다.
2. **네트워킹** 섹션에서 편집할 인터페이스를 선택합니다.
3. **네트워크 설정 편집**을 클릭합니다.
4. 가능한 두 가지 옵션 중 하나를 선택하십시오.
   - DHCP를 통한 자동 네트워크 구성의 경우 **DHCP 사용**을 클릭합니다. 작업을 확인합니다.
   - 수동 네트워크 구성의 경우 **고정 IP 주소 설정**을 클릭합니다. 다음 설정을 편집할 수 있습니다.
     - **IP 주소**: 로컬 네트워크 내 인터페이스의 IP 주소입니다.
     - **VPN 게이트웨이 IP 주소**: 올바른 Cyber Disaster Recovery Cloud 서비스 작업용 네트워크의 클라우드 세그먼트를 위해 예약된 특별한 IP 주소입니다.
     - **네트워크 마스크**: 로컬 네트워크의 네트워크 마스크입니다.
     - **기본 게이트웨이**: 로컬 사이트의 기본 게이트웨이입니다.
     - **기본 DNS 서버**: 로컬 사이트의 주 DNS 서버입니다.
     - **대체 DNS 서버**: 로컬 사이트의 보조 DNS 서버입니다.

© Acronis International GmbH, 2003-2024



- 필요한 변경 작업을 수행하고 Enter 키를 눌러 확인합니다.

클라우드 전용 모드

클라우드에 최대 23개의 네트워크를 설정할 수 있습니다.

새로운 클라우드 네트워크를 추가하려면

1. **재해 복구** > **연결**로 이동합니다.
2. **클라우드 사이트**에서 **클라우드 네트워크 추가**를 클릭합니다.
3. 클라우드 네트워크 매개변수(네트워크 주소와 마스크)를 정의합니다. 준비가 되면 **완료**를 클릭합니다.

그러면 정의된 주소 및 마스크를 가진 추가 클라우드 네트워크가 클라우드 사이트에 생성됩니다.

클라우드 네트워크을 삭제하려면

참고
클라우드 서버가 하나라도 포함되어 있는 클라우드 네트워크는 삭제할 수 없습니다. 먼저, 클라우드 서버를 삭제한 다음, 네트워크를 삭제하십시오.

1. **재해 복구** > **연결**로 이동합니다.
2. **클라우드 사이트**에서 삭제할 네트워크 주소를 클릭합니다.
3. **삭제**를 클릭하고 작업을 확인합니다.

클라우드 네트워크 매개변수를 변경하려면

1. **재해 복구** > **연결**로 이동합니다.
2. **클라우드 사이트**에서 편집할 네트워크 주소를 클릭합니다.
3. **편집**을 클릭합니다.
4. 네트워크 주소 및 마스크를 정의하고 **완료**를 클릭합니다.

IP 주소 재구성

적합한 재해 복구 성능을 얻기 위해서는 로컬 및 클라우드 서버에 할당된 IP 주소가 일관되어야 합니다. IP 주소에 비일관성이나 불일치 문제가 있으면 **재해 복구** > **연결**의 해당 네트워크 옆에 느낌표가 표시됩니다.

© Acronis International GmbH, 2003-2024

IP 주소 비일관성에 대한 일반적으로 알려진 이유 중 몇 가지가 아래에 나와 있습니다.

1. 복구 서버가 한 네트워크에서 다른 네트워크로 마이그레이션되었거나 클라우드 네트워크의 네트워크 마스크가 변경된 경우. 이 경우 클라우드 서버가 실제 연결되어 있지 않은 네트워크의 IP 주소를 가지게 됩니다.
2. 연결 유형이 사이트 간 연결 없음에서 사이트 간 연결로 전환되었습니다. 이 경우 로컬 서버가 클라우드 사이트에 복구 서버용으로 생성된 네트워크와 다른 네트워크에 위치합니다.
3. 연결 유형이 사이트 간 OpenVPN에서 다중 사이트 IPsec VPN으로 전환되었거나 그 반대로 전환되었습니다. 이 시나리오에 대한 자세한 내용은 연결 전환 및 IP 주소 다시 할당을 참조하십시오.
4. VPN 어플라이언스 사이트에서 다음 네트워크 매개변수 편집:
   - 네트워크 설정을 통해 인터페이스 추가
   - 인터페이스 설정을 통해 네트워크 마스크를 수동으로 편집
   - DHCP를 통해 네트워크 마스크 편집
   - 인터페이스 설정을 통해 네트워크 주소 및 마스크를 수동으로 편집
   - DHCP를 통해 네트워크 마스크 및 주소 편집

   위에 나열한 작업을 진행하고 나면 클라우드 사이트의 네트워크가 로컬 네트워크의 하위 세트나 상위 세트가 될 수 있고, 또는 VPN 어플라이언스 인터페이스가 서로 다른 인터페이스에 대해 같은 네트워크 설정을 보고할 수도 있습니다.

네트워크 설정 관련 문제를 해결하려면

1. IP 주소 재구성이 필요한 네트워크를 클릭합니다.
   선택한 네트워크에 속한 서버 목록, 해당 서버의 상태와 IP 주소가 표시됩니다. 네트워크 설정이 일관되지 않은 서버에는 느낌표가 표시됩니다.
2. 서버의 네트워크 설정을 변경하려면 **서버로 이동**을 클릭합니다. 모든 서버의 네트워크 설정을 한 번에 변경하려면 알림 블록에서 **변경**을 클릭합니다.
3. IP 주소를 변경해야 하는 경우에는 **새 IP** 및 **새 테스트 IP** 필드에 IP 주소를 정의하여 변경합니다.
4. 준비가 되면 **확인**을 클릭합니다.

적합한 네트워크로 서버 이동

재해 복구 보호 계획을 생성한 후 선택한 장치에 적용하면, 시스템은 장치 IP 주소를 검사한 후, IP 주소와 맞는 기존 클라우드 네트워크가 없으면 클라우드 네트워크를 자동으로 생성합니다. 기본적으로 개인 용도로 IANA에서 권장하는 최대 범위(10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)를 사용하여 클라우드 네트워크가 구성됩니다. 네트워크 마스크를 편집하여 네트워크 범위를 좁힐 수 있습니다.

선택한 장치가 여러 로컬 네트워크에 있는 경우 클라우드 사이트의 네트워크가 로컬 네트워크의 상위 세트가 될 수 있습니다. 이 경우 클라우드 네트워크를 구성하려면:

1. 네트워크 크기 구성이 필요한 클라우드 네트워크를 클릭하고 **편집**을 클릭합니다.
2. 올바른 설정으로 네트워크 크기를 재구성합니다.
3. 다른 필수 네트워크를 생성합니다.
4. 네트워크에 연결된 장치 수 옆에 있는 알림 아이콘을 클릭합니다.

© Acronis International GmbH, 2003-2024

5. **적합한 네트워크로 이동**을 클릭합니다.
6. 적절한 네트워크로 이동할 서버를 선택하고 **이동**을 클릭합니다.

VPN 어플라이언스 설정 관리

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

Cyber Protect 콘솔에서 **재해 복구** > **연결**로 이동하여 다음을 수행할 수 있습니다.

- 로그 파일을 다운로드합니다.
- 어플라이언스를 등록 해제합니다(VPN 어플라이언스 설정을 재설정하거나 클라우드 전용 모드로 전환해야 하는 경우).

해당 설정에 액세스하려면 **VPN 어플라이언스** 블록의 **i** 아이콘을 클릭하십시오.

VPN 어플라이언스 콘솔에서 다음을 수행할 수 있습니다.

- 어플라이언스 비밀번호를 변경합니다.
- 네트워크 설정을 확인/변경하고, 인터넷 연결을 위한 WAN으로 사용할 인터페이스를 정의합니다.
- 등록을 반복하여 등록 계정을 등록/변경합니다.
- VPN 서비스를 다시 시작합니다.
- VPN 어플라이언스를 재부팅합니다.
- Linux 쉘 명령을 실행합니다(고급 문제 해결 케이스에만 사용).

VPN 게이트웨이 다시 설치

VPN 게이트웨이에 해결할 수 없는 문제가 있는 경우 VPN 게이트웨이를 다시 설치해야 할 수 있습니다. 다음과 같은 문제가 발생할 수 있습니다.

- VPN 게이트웨이가 **오류** 상태입니다.
- VPN 게이트웨이가 오랫동안 **보류 중** 상태입니다.
- VPN 게이트웨이 상태가 오랫동안 확인되지 않습니다.

VPN 게이트웨이 프로세스 재설치에는 기존 VPN 게이트웨이 가상 머신을 완전히 삭제하고, 템플릿에서 새 가상 머신을 설치하고, 새 가상 머신에 이전 VPN 게이트웨이의 설정을 적용하는 자동 작업이 포함됩니다.

전제조건:

클라우드 사이트에 대한 연결 유형 하나를 설정해야 합니다.

VPN 게이트웨이를 다시 설치하려면

1. Cyber Protect 콘솔에서 **재해 복구** > **연결**로 이동합니다.
2. VPN 게이트웨이의 기어 아이콘을 클릭하고 **VPN 게이트웨이 다시 설치**를 선택합니다.

© Acronis International GmbH, 2003-2024

3. **VPN 게이트웨이 다시 설치** 대화창에서 로그인을 입력합니다.
4. **다시 설치**를 클릭합니다.

사이트 간 연결 활성화 및 비활성화

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

다음의 경우 사이트 간 연결을 활성화할 수 있습니다.

- 로컬 사이트의 서버와 통신하는 데 클라우드 사이트의 클라우드 서버가 필요한 경우.
- 클라우드로의 장애 조치 이후 로컬 인프라가 복구되고, 서버를 로컬 사이트로 다시 장애 복구하려는 경우.

사이트 간 연결을 활성화하려면

1. **재해 복구** > **연결**로 이동합니다.
2. **속성 표시**를 클릭한 다음 **사이트 간 연결** 옵션을 활성화합니다.

그러면 로컬 사이트와 클라우드 사이트 사이에 사이트 간 VPN 연결이 활성화됩니다. Cyber Disaster Recovery Cloud 서비스가 VPN 어플라이언스에서 네트워크 설정을 가져오고, 로컬 네트워크를 클라우드 사이트로 확장합니다.

로컬 사이트의 서버와 통신하는 데 클라우드 사이트의 클라우드 서버가 필요하지 않다면 사이트 간 연결을 비활성화할 수 있습니다.

사이트 간 연결을 비활성화하려면

1. **재해 복구** > **연결**로 이동합니다.
2. **속성 표시**를 클릭한 다음 **사이트 간 연결** 옵션을 비활성화합니다.

그러면 로컬 사이트가 클라우드 사이트에서 연결 해제됩니다.

사이트 간 연결 유형 전환

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

사이트 간 OpenVPN 연결과 다중 사이트 IPsec VPN 연결 간을 쉽게 전환할 수 있습니다.

연결 유형을 전환하면 활성 VPN 연결은 삭제되지만 클라우드 서버 및 네트워크 구성은 유지됩니다. 하지만 클라우드 네트워크 및 서버의 IP 주소는 다시 할당해야 합니다.

다음 표에는 사이트 간 OpenVPN 연결과 다중 사이트 IPsec VPN 연결의 기본적인 특성을 비교한 내용이 나와 있습니다.

	사이트 간 OpenVPN	**다중 사이트 IPsec VPN**
로컬 사이트 지원	1개	1개, 여러 개

© Acronis International GmbH, 2003-2024

	사이트 간 OpenVPN	다중 사이트 IPsec VPN
VPN 게이트웨이 모드	L2 Open VPN	L3 IPsec VPN
네트워크 세그먼트	로컬 네트워크를 클라우드 네트워크로 확장	로컬 네트워크 및 클라우드 네트워크 세그먼트가 겹치면 안 됨
로컬 사이트로의 지점 및 사이트 간 액세스 지원	예	아니요
클라우드 사이트로의 지점 및 사이트 간 액세스 지원	예	예
공용 IP 제공 항목 필요	아니요	예

사이트 간 OpenVPN 연결에서 다중 사이트 IPsec VPN 연결로 전환하려면

1. Cyber Protect 콘솔에서 **재해 복구** -> **연결**로 이동합니다.
2. **속성 표시**를 클릭합니다.
3. **다중 사이트 IPsec VPN으로 전환**을 클릭합니다.
4. **재구성**을 클릭합니다.
5. 클라우드 네트워크 및 클라우드 서버의 IP 주소를 다시 할당합니다.
6. 다중 사이트 IPsec 연결 설정을 구성합니다.

다중 사이트 IPsec VPN 연결에서 사이트 간 OpenVPN 연결로 전환하려면

1. Cyber Protect 콘솔에서 **재해 복구** -> **연결**로 이동합니다.
2. **속성 표시**를 클릭합니다.
3. **사이트 간 OpenVPN으로 전환**을 클릭합니다.
4. **재구성**을 클릭합니다.
5. 클라우드 네트워크 및 클라우드 서버의 IP 주소를 다시 할당합니다.
6. 사이트 간 연결 설정을 구성합니다.

IP 주소 다시 할당

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

다음과 같은 경우 구성을 완료하려면 클라우드 네트워크 및 클라우드 서버의 IP 주소를 다시 할당해야 합니다.

- 사이트 간 OpenVPN에서 다중 사이트 IPsec VPN으로 전환하거나 그 반대로 전환한 후.
- 보호 계획을 적용한 후(다중 사이트 IPsec VPN 연결이 구성되어 있는 경우)

클라우드 네트워크의 IP 주소를 다시 할당하려면

© Acronis International GmbH, 2003-2024

1. **연결** 탭에서 클라우드 네트워크의 IP 주소를 클릭합니다.
2. **네트워크** 팝업에서 **편집**을 클릭합니다.
3. 새 네트워크 주소 및 네트워크 마스크를 입력합니다.
4. **완료**를 클릭합니다.

클라우드 네트워크의 IP 주소를 다시 할당한 후에는 다시 할당된 클라우드 네트워크에 속하는 클라우드 서버를 다시 할당해야 합니다.

서버의 IP 주소를 다시 할당하려면

1. **연결** 탭에서 클라우드 네트워크 내 서버의 IP 주소를 클릭합니다.
2. **서버** 팝업에서 **IP 주소 변경**을 클릭합니다.
3. **IP 주소 변경** 팝업에서 서버의 새 IP 주소를 입력하거나, 다시 할당된 클라우드 네트워크의 일부분인 자동 생성 IP 주소를 사용합니다.

   참고
   Cyber Disaster Recovery Cloud에서는 네트워크 IP 주소를 다시 할당하기 전에 클라우드 네트워크에 포함되어 있었던 모든 클라우드 서버에 클라우드 네트워크의 IP 주소를 자동 할당합니다. 제안된 IP 주소를 사용하여 모든 클라우드 서버의 IP 주소를 한 번에 다시 할당할 수 있습니다.

4. **확인**을 클릭합니다.

사용자 정의 DNS 서버 구성

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

연결을 구성할 때 Cyber Disaster Recovery Cloud에서는 클라우드 네트워크 인프라를 생성합니다. Cloud DHCP 서버는 복구 서버와 기본 서버에 기본 DNS 서버를 자동 할당합니다. 그러나 기본 설정을 변경하여 사용자 정의 DNS 서버를 구성할 수 있습니다. 새 DNS 설정은 다음번에 DHCP 서버에 요청할 때 적용됩니다.

전제조건:

클라우드 사이트에 대한 연결 유형 하나를 설정해야 합니다.

사용자 정의 DNS 서버를 구성하려면

1. Cyber Protect 콘솔에서 **재해 복구** > **연결**로 이동합니다.
2. **속성 표시**를 클릭합니다.
3. **기본값(클라우드 사이트 제공)**을 클릭합니다.
4. **사용자 정의 서버**를 선택합니다.
5. DNS 서버의 IP 주소를 입력합니다.
6. [선택 사항] 다른 DNS 서버를 추가하려면 **추가**를 클릭하고 DNS 서버 IP 주소를 입력합니다.

© Acronis International GmbH, 2003-2024

참고
사용자 정의 DNS 서버를 추가한 후에는 기본 DNS 서버도 추가할 수 있습니다. 이렇게 하면 사용자 정의 DNS 서버를 사용할 수 없을 때 Cyber Disaster Recovery Cloud에서 기본 DNS 서버를 사용합니다.

7. **완료**를 클릭합니다.

사용자 정의 DNS 서버 삭제

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

사용자 정의 DNS 목록에서 DNS 서버를 삭제할 수 있습니다.

전제조건:

사용자 정의 DNS 서버가 구성됩니다.

사용자 정의 DNS 서버를 삭제하려면

1. Cyber Protect 콘솔에서 **재해 복구** > **연결**로 이동합니다.
2. **속성 표시**를 클릭합니다.
3. **사용자 정의 서버**를 클릭합니다.
4. DNS 서버 옆의 삭제 아이콘을 클릭합니다.

참고
사용 가능한 사용자 정의 DNS 서버가 하나뿐이면 삭제 작업은 비활성화됩니다. 사용자 정의 DNS 서버를 모두 삭제하려면 **기본값(클라우드 사이트 제공)**을 선택합니다.

5. **완료**를 클릭합니다.

로컬 라우팅 구성

VPN 어플라이언스를 통해 클라우드로 확장된 로컬 네트워크 외에 VPN 어플라이언스에 등록되어 있지 않지만 속해 있는 서버가 클라우드 서버와 통신해야 하는 다른 로컬 네트워크가 있는 경우가 있습니다. 이러한 로컬 서버와 클라우드 서버 간에 연결을 구축하려면 로컬 라우팅 설정을 구성해야 합니다.

로컬 라우팅을 구성하려면

1. **재해 복구** > **연결**로 이동합니다.
2. **속성 표시**를 클릭한 다음 **로컬 라우팅**을 클릭합니다.

© Acronis International GmbH, 2003-2024

3. CIDR 표기법에 해당 로컬 네트워크를 지정합니다.
4. **저장**을 클릭합니다.

그러면 지정된 로컬 네트워크의 서버가 클라우드 서버와 통신할 수 있습니다.

L2 VPN을 통한 DHCP 트래픽 허용

로컬 사이트의 장치가 DHCP 서버에서 IP 주소를 가져오는 경우, 재해 복구를 통해 DHCP 서버를 보호하고 클라우드로 장애 조치하여 L2 VPN을 통해 DHCP 트래픽이 실행되도록 허용할 수 있습니다. 이 경우 DHCP 서버가 클라우드에서 실행되게 되지만 계속 로컬 장치에 IP 주소를 할당합니다.

전제조건:

클라우드 사이트에 대한 사이트 간 L2 VPN 연결 유형 하나를 설정해야 합니다.

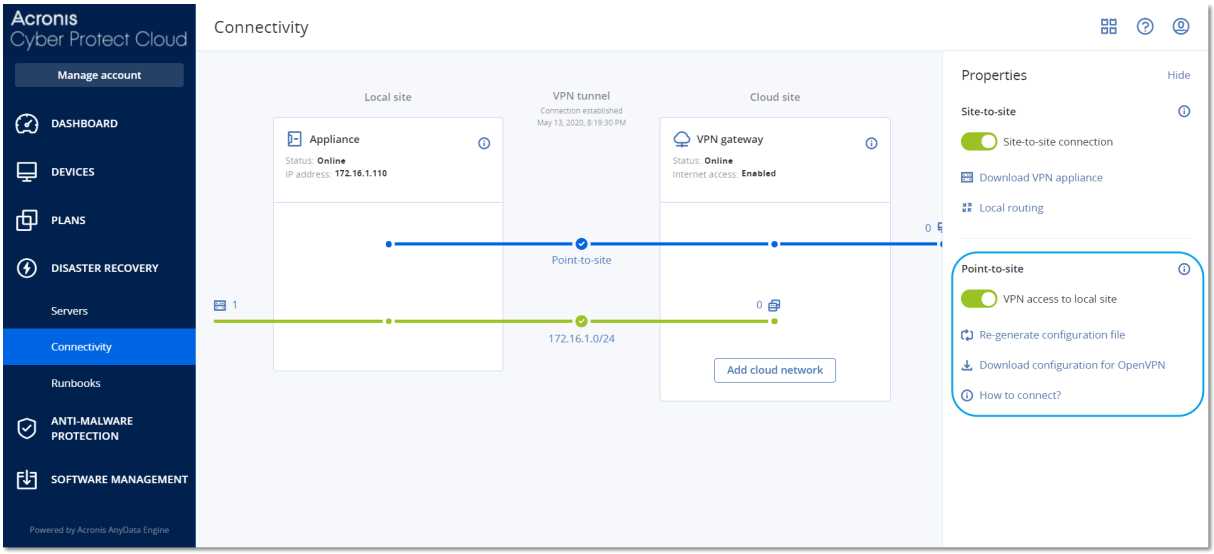
L2 VPN 연결을 통한 DHCP 트래픽을 허용하려면

1. **재해 복구** > **연결** 탭으로 이동합니다.
2. **속성 표시**를 클릭합니다.
3. **L2 VPN을 통한 DHCP 트래픽 허용** 스위치를 활성화합니다.

지점 및 사이트 간 연결 설정 관리

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

Cyber Protect 콘솔에서 **재해 복구** > **연결**로 이동한 다음, 오른쪽 위에 있는 **속성 표시**를 클릭합니다.



로컬 사이트로의 VPN 액세스

이 옵션은 로컬 사이트에 대한 VPN 액세스를 관리하는 데 사용되며 기본적으로 활성화되어 있습니다. 이 옵션을 비활성화하면 로컬 사이트에 대한 지점 및 사이트 간 액세스가 허용되지 않습니

© Acronis International GmbH, 2003-2024

다.

OpenVPN 구성 다운로드

그러면 OpenVPN 클라이언트의 구성 파일이 다운로드됩니다. 이 파일은 클라우드 사이트에 대한 지점 및 사이트간 연결을 설정하는 데 필요합니다.

구성 재생성

OpenVPN 클라이언트의 구성 파일을 재생성할 수 있습니다.

이는 다음과 같은 경우에 필요합니다.

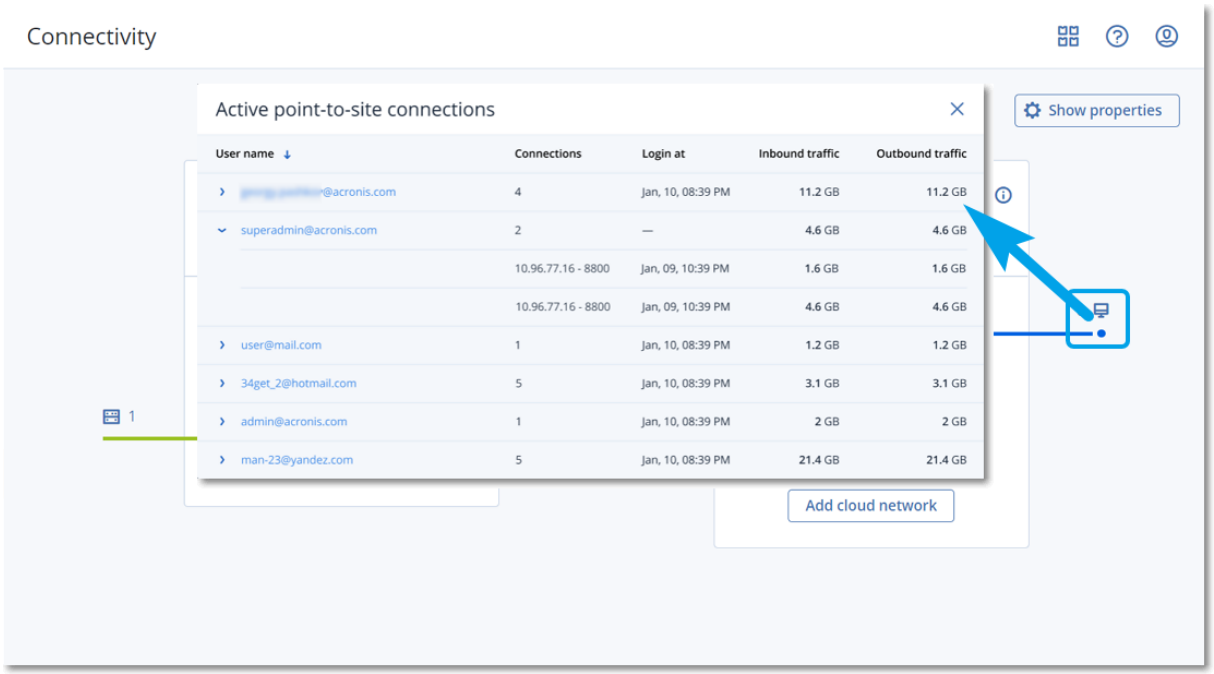
- 구성 파일이 손상된 것으로 의심되는 경우.
- 계정에 대해 2단계 인증이 활성화된 경우.

구성 파일이 업데이트되는 즉시 이전 구성 파일을 통한 연결이 불가능 해집니다. 지점 및 사이트 간 연결을 사용할 수 있는 사용자간에 새 파일을 배포해야 합니다.

활성 상태의 지점 및 사이트 간 연결

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

재해 복구 > **연결**에서 활성화된 모든 지점 및 사이트 간 연결을 볼 수 있습니다. 파란색 **지점 및 사이트 간** 행에서 머신 아이콘을 클릭하면 사용자 이름별로 그룹화된 활성 상태의 지점 및 사이트 간 연결에 대한 상세 정보를 확인할 수 있습니다.



© Acronis International GmbH, 2003-2024

로그 작업

재해 복구는 VPN 어플라이언스와 VPN 게이트웨이의 로그를 수집합니다. 로그는 .txt 파일로 저장되고 .zip 아카이브로 압축됩니다. 아카이브를 다운로드하고 추출하여 해당 정보를 문제 해결이나 모니터링에 사용할 수 있습니다.

아래에서는 zip 아카이브에 포함된 로그 파일 및 파일에 포함된 정보에 대해 설명합니다.

`dnsmasq.config.txt` - DNS 및 DHCP 주소를 제공하는 서비스의 구성에 대한 정보가 포함되어 있습니다.

`dnsmsq.leases.txt` - 현재 DHCP 주소 임대에 대한 정보가 포함되어 있습니다.

`dnsmasq_log.txt` - dnsmasq 서비스의 로그가 포함되어 있습니다.

`ebtables.txt` - 방화벽 테이블에 대한 정보가 포함되어 있습니다.

`free.txt` - 사용 가능한 메모리에 대한 정보가 포함되어 있습니다.

`ip.txt` - **네트워크 패킷 캡처** 설정 구성에 사용할 수 있는 이름을 포함하여 네트워크 인터페이스 구성의 로그가 포함되어 있습니다.

`NetworkManager_log.txt` - NetworkManager 서비스의 로그가 포함되어 있습니다.

`NetworkManager_status.txt` - NetworkManager 서비스의 상태에 대한 정보가 포함되어 있습니다.

`openvpn@p2s_log.txt` - OpenVPN 서비스의 로그가 포함되어 있습니다.

`openvpn@p2s_status.txt` - VPN 터널의 상태에 대한 정보가 포함되어 있습니다.

`ps.txt` - VPN 게이트웨이 또는 VPN 어플라이언스에서 현재 실행 중인 프로세스에 대한 정보가 포함되어 있습니다.

`resolf.conf.txt` - DNS 서버의 구성에 대한 정보가 포함되어 있습니다.

`routes.txt` - 네트워킹 경로에 대한 정보가 포함되어 있습니다.

`uname.txt` - 운영 체제 커널의 현재 버전에 대한 정보가 포함되어 있습니다.

`uptime.txt` - 운영 체제가 다시 시작되지 않은 기간에 대한 정보가 포함되어 있습니다.

`vpnserver_log.txt` - VPN 서비스의 로그가 포함되어 있습니다.

`vpnserver_status.txt` - VPN 서버의 상태에 대한 정보가 포함되어 있습니다.

IPsec VPN 연결과 관련된 로그 파일에 대한 자세한 내용은 "다중 사이트 IPsec VPN 로그 파일"(708 페이지) 항목을 참조하십시오.

VPN 어플라이언스의 로그 다운로드

VPN 어플라이언스의 로그가 포함된 아카이브를 다운로드하고 추출하여 해당 정보를 문제 해결이나 모니터링에 사용할 수 있습니다.

VPN 어플라이언스의 로그를 다운로드하려면

© Acronis International GmbH, 2003-2024

1. **연결** 페이지에서 해당 VPN 어플라이언스 옆에 있는 기어 아이콘을 클릭합니다.
2. **로그 다운로드**를 클릭합니다.
3. [선택 사항] **네트워크 패킷 캡처**를 선택하고 설정을 구성합니다. 자세한 내용은 "네트워크 패킷 캡처"(705페이지)을(를) 참조하십시오.
4. **완료**를 클릭합니다.
5. .zip 아카이브를 다운로드할 준비가 되었으면 **로그 다운로드**를 클릭하고 로컬에 저장합니다.

VPN 게이트웨이의 로그 다운로드

VPN 게이트웨이의 로그가 포함된 아카이브를 다운로드하고 추출하여 해당 정보를 문제 해결이나 모니터링에 사용할 수 있습니다.

VPN 게이트웨이의 로그를 다운로드하려면

1. **연결** 페이지에서 해당 VPN 게이트웨이 옆에 있는 기어 아이콘을 클릭합니다.
2. **로그 다운로드**를 클릭합니다.
3. [선택 사항] **네트워크 패킷 캡처**를 선택하고 설정을 구성합니다. 자세한 내용은 "네트워크 패킷 캡처"(705페이지)을(를) 참조하십시오.
4. **완료**를 클릭합니다.
5. .zip 아카이브를 다운로드할 준비가 되었으면 **로그 다운로드**를 클릭하고 로컬에 저장합니다.

네트워크 패킷 캡처

로컬 프로덕션 사이트와 기본 또는 복구 서버 간의 통신 문제를 분석하고 해결하려면 VPN 게이트웨이 또는 VPN 어플라이언스의 네트워크 패킷을 수집하십시오.

수집된 네트워크 패킷의 수가 32,000개를 넘거나 시간 제한에 도달하면 네트워크 패킷 캡처가 중지되고 결과가 .libpcap 파일에 기록됩니다. .libpcap 파일은 로그 .zip 아카이브에 추가됩니다.

다음 표에는 사용자가 구성할 수 있는 **네트워크 패킷 캡처** 설정에 대한 자세한 내용이 나와 있습니다.

설정	설명
네트워크 인터페이스 이름	네트워크 패킷을 캡처할 네트워크 인터페이스입니다. 모든 네트워크 인터페이스의 네트워크 패킷을 캡처하려면 **모두**를 선택합니다.
시간 제한(초)	네트워크 패킷 캡처에 대한 시간 제한입니다. 설정할 수 있는 최대값은 1,800입니다.
필터링	캡처된 네트워크 패킷에 적용할 추가 필터입니다. 다음과 같이 프로토콜, 포트, 방향 및 그 조합을 공백으로 구분하여 포함하는 문자열을 입력할 수 있습니다. "and", "or", "not", " (", ") ", "src", "dst", "net", "host", "port", "ip", "tcp", "udp", "icmp", "arp", "esp". 대괄호를 사용하려면 대괄호 앞뒤에 공백을 넣으십시오. IP 주소 및 네트워크 주소를 입력해도 됩니다. 예: "icmp 또는 arp" 및 "port 67 또는 68". 입력할 수 있는 값에 대한 자세한 내용은 Linux tpcdump 도움말을 참조하십시오.

© Acronis International GmbH, 2003-2024

IPsec VPN 구성 문제 해결

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

IPsec VPN 연결을 구성할 때 문제가 발생할 수 있습니다.

IPsec 로그에서 발생한 문제에 대해 자세히 알아볼 수 있으며, IPsec VPN 구성 문제 해결 항목에서 흔히 발생할 수 있는 몇 가지 문제에 사용할 수 있는 해결 방법을 확인할 수 있습니다.

IPsec VPN 구성 문제 해결

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

다음 표에는 가장 많이 발생하는 IPsec VPN 구성 문제 및 이러한 문제를 해결하는 방법이 설명되어 있습니다.

문제	가능한 해결 방법
다음 오류 메시지가 표시됩니다. **IKE 1단계 협상 오류가 발생했습니다. 클라우드 및 로컬 사이트의 IPsec IKE 설정을 확인하십시오.**	**다시 시도**를 클릭하고 더 구체적인 오류 메시지가 표시되는지 확인합니다. 더 구체적인 오류 메시지란 알고리즘 불일치, 잘못된 사전에 공유된 키 등과 관련된 오류 메시지일 수 있습니다. **참고** 보안상 IPsec VPN 연결에는 다음 제한이 적용됩니다. • IKEv1은 RFC8247에 따라 사용이 중단되었으며 보안 위험으로 인해 지원되지 않습니다. IKEv2 프로토콜 연결만 지원됩니다. • 다음 암호화 알고리즘은 안전하지 않은 것으로 간주되어 지원되지 않습니다. DES 및 3DES. • 다음 해시 알고리즘은 안전하지 않은 것으로 간주되어 지원되지 않습니다. SHA1 및 MD5. • Diffie-Hellman 그룹 번호 2는 안전하지 않은 것으로 간주되어 지원되지 않습니다.
내 로컬 사이트와 클라우드 사이트 간의 연결 상태가 계속 **연결 중**으로 표시됩니다.	다음 사항을 확인합니다. • 방화벽을 사용하는 경우 UDP 포트 500이 열려 있는지 확인합니다. • 로컬 사이트와 클라우드 사이트 간의 연결을 확인합니다. • 로컬 사이트의 IP 주소가 정확한지 확인합니다.

© Acronis International GmbH, 2003-2024

문제	가능한 해결 방법
내 로컬 사이트와 클라우드 사이트 간의 연결 상태가 계속 **연결 대기 중**으로 표시됩니다.	클라우드 사이트의 **시작 작업**이 **추가**로 설정되어 있으면 이 상태가 표시됩니다. 클라우드 사이트가 로컬 사이트에서 연결을 시작하기를 대기하기 때문입니다. 로컬 사이트에서 연결을 시작합니다.
내 로컬 사이트와 클라우드 사이트 간의 연결 상태가 계속 **트래픽 대기 중**으로 표시됩니다.	클라우드 사이트의 **시작 작업**이 **경로**로 설정되어 있으면 이 상태가 표시됩니다. 로컬 사이트에서 연결해야 하는 경우 다음 작업을 수행합니다. • 로컬 사이트에서 클라우드 사이트의 가상 머신으로 Ping을 시도해 봅니다. Cisco ASA 등의 일부 장치에서 터널을 설정하려면 수행해야 하는 표준 동작입니다. (경로 모드) • 로컬 사이트의 **시작 작업**을 **시작**으로 설정하여 로컬 사이트가 터널을 설정했는지 확인합니다.
내 로컬 사이트와 클라우드 사이트 간에 연결은 설정되었는데 네트워크 정책 중 하나 이상이 다운된 것으로 표시됩니다.	이 문제는 다음과 같은 이유로 인해 발생할 수 있습니다. • 클라우드 IPsec 사이트의 네트워크 매핑이 로컬 사이트의 네트워크 매핑과 다릅니다. 로컬 사이트와 클라우드 사이트에서 네트워크 정책의 순서 및 네트워크 매핑이 정확하게 일치하는지 확인합니다. • Cisco ASA 등의 장치에서 로컬 사이트 및/또는 클라우드 사이트의 **시작 작업**이 **경로**로 설정되어 있으면 이 상태는 올바른 상태이며 현재 트래픽이 없는 것입니다. Ping을 시도하여 터널이 설정되어 있는지를 확인할 수 있습니다. Ping이 정상적으로 진행되지 않으면 로컬 및 클라우드 사이트의 네트워크 매핑을 확인합니다.
특정 IPsec 연결을 다시 시작하고 싶습니다.	특정 IPsec 연결을 다시 시작하려면 1. **재해 복구** > **연결** 화면에서 IPsec 연결을 클릭합니다. 2. **연결 비활성화**를 클릭합니다. 3. IPsec 연결을 다시 클릭합니다. 4. **연결 활성화**를 클릭합니다.

IPsec VPN 로그 파일 다운로드

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

© Acronis International GmbH, 2003-2024

VPN 서버의 로그 파일에서 IPsec 연결 관련 추가 정보를 확인할 수 있습니다. 로그 파일은 .zip 아카이브로 압축되어 있습니다. 이 아카이브를 다운로드하여 압축을 풀면 됩니다.

사전 요구 사항

다중 사이트 IPsec VPN 연결이 구성됩니다.

로그 파일이 포함된 .zip 아카이브를 다운로드하려면

1. Cyber Protect 콘솔에서 **재해 복구** > **연결**로 이동합니다.
2. 클라우드 사이트의 VPN 게이트웨이 옆에 있는 기어 아이콘을 클릭합니다.
3. **로그 다운로드**를 클릭합니다.
4. **완료**를 클릭합니다.
5. .zip 아카이브를 다운로드할 준비가 되었으면 **로그 다운로드**를 클릭하고 로컬에 저장합니다.

다중 사이트 IPsec VPN 로그 파일

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

아래에서는 zip 아카이브에 포함된 IPsec VPN 로그 파일 및 파일에 포함된 정보에 대해 설명합니다.

- `ip.txt` - 네트워크 인터페이스 구성의 로그가 포함된 파일입니다. 이 파일에는 IP 주소 2개(공용 IP 주소와 로컬 IP 주소)가 포함되어 있어야 합니다. 로그에 이러한 IP 주소가 없으면 문제가 있는 것입니다. 지원 팀에 문의하십시오.

  참고
  공용 IP 주소의 마스크는 32여야 합니다.

- `swanctl-list-loaded-config.txt` - 모든 IPsec 사이트 관련 정보가 포함된 파일입니다.
  파일에 사이트가 포함되어 있지 않으면 IPsec 구성이 적용되지 않은 것입니다. 구성을 업데이트한 후 저장해 보거나 지원 팀에 문의하십시오.
- `swanctl-list-active-sas.txt` - 활성 또는 연결 중 상태인 연결 및 정책이 포함된 파일입니다.

복구 서버 설정

이 섹션에서는 장애 조치 및 장애 복구의 개념, 복구 서버 생성 및 재해 복구 작업에 대해 설명합니다.

복구 서버 생성

워크로드의 복사본이 될 복구 서버를 생성하려면 아래 절차를 따르십시오. 이 프로세스를 보여 주는 비디오 자습서를 시청할 수도 있습니다.

© Acronis International GmbH, 2003-2024

중요
장애 조치를 수행할 때 복구 서버가 생성된 이후에 생성된 복구 지점만 선택할 수 있습니다.

사전 요구 사항

- 보호하려는 원본 머신에 보호 계획이 적용되어야 합니다. 이 계획은 전체 머신을 백업하거나 부팅과 필요한 서비스 제공에 필수적인 디스크만 클라우드 스토리지에 백업해야 합니다.
- 클라우드 사이트에 대한 연결 유형 하나를 설정해야 합니다.

복구 서버를 생성하려면:

1. **모든 장치** 탭에서 보호할 머신을 선택합니다.
2. **재해 복구**를 클릭한 다음, **복구 서버 생성**을 클릭합니다.
3. 가상 코어 수와 RAM 크기를 선택합니다.

   참고
   모든 옵션의 컴퓨팅 포인트를 볼 수 있습니다. 컴퓨팅 포인트의 수는 복구 서버를 시간당 실행하는 비용을 반영합니다. 자세한 내용은 "컴퓨팅 포인트"(670페이지)을(를) 참조하십시오.

4. 서버를 연결할 클라우드 네트워크를 지정합니다.
5. **DHCP** 옵션을 선택합니다.

DHCP 옵션	설명
클라우드 사이트 제공	기본 설정. 서버의 IP 주소는 클라우드에 자동으로 구성된 DHCP 서버에서 제공합니다.
사용자 정의	서버의 IP 주소는 클라우드에 있는 자신의 DHCP 서버에서 제공합니다.

6. [선택 사항] **MAC 주소**를 지정합니다.
   MAC 주소는 서버의 네트워크 어댑터에 할당된 고유 식별자입니다. 사용자 DHCP를 사용하는 경우 특정 IP 주소를 항상 특정 MAC 주소에 할당하도록 DHCP를 구성할 수 있습니다. 이를 통해 복구 서버는 항상 동일한 IP 주소를 얻게 됩니다. MAC 주소로 등록된 라이센스가 있는 애플리케이션을 실행할 수 있습니다.
7. 서버가 운영 네트워크에서 가지는 IP 주소를 지정합니다. 기본적으로 원래 머신의 ID 주소가 설정됩니다.

   참고
   DHCP 서버를 사용하는 경우 IP 주소 충돌을 피할 수 있도록 이 IP 주소를 서버 제외 목록에 추가하십시오.
   사용자 지정 DHCP 서버를 사용하는 경우 **운영 네트워크의 IP 주소**에 DHCP 서버에 구성된 것과 동일한 IP 주소를 지정해야 합니다. 그렇지 않으면 테스트 장애 조치가 제대로 작동하지 않고 공용 IP 주소를 통해 서버에 연결할 수 없습니다.

8. [선택 사항] **테스트 IP 주소** 확인란을 선택한 다음, IP 주소를 지정합니다.

© Acronis International GmbH, 2003-2024

이렇게 하면 격리된 테스트 네트워크에서 장애 조치를 테스트하고, 테스트 장애 조치 중에 RDP 또는 SSH를 통해 복구 서버에 연결할 수 있습니다. 테스트 장애 조치 모드에서 VPN 게이트웨이는 NAT 프로토콜을 사용하여 테스트 IP 주소를 운영 IP 주소로 바꿉니다.

확인란을 선택하지 않은 상태로 두면 콘솔이 테스트 장애 조치 중 서버에 액세스하는 유일한 방법입니다.

참고

DHCP 서버를 사용하는 경우 IP 주소 충돌을 피할 수 있도록 이 IP 주소를 서버 제외 목록에 추가하십시오.

제안된 IP 주소 중 하나를 선택하거나 다른 IP 주소를 입력할 수 있습니다.

9. [선택 사항] **인터넷 액세스** 확인란을 선택합니다.

   이렇게 하면 실제 또는 테스트 장애 조치 중에 복구 서버가 인터넷에 액세스할 수 있습니다. 기본적으로 공용 IP 주소에 대한 아웃바운드 연결용으로는 TCP 포트 25가 열립니다.

10. [선택 사항] **RPO 임계값**을 설정합니다.

    RPO 임계값은 현재 시각과 장애 조치에 적합한 마지막 복구 지점 사이의 최대 시간을 정의합니다. 이 값은 15 – 60분, 1 – 24시간, 1 – 14일 내에서 설정할 수 있습니다.

11. [선택 사항] **공용 IP 주소 사용** 확인란을 선택합니다.

    공용 IP 주소를 사용하면 장애 조치 또는 테스트 장애 조치 중에 복구 서버를 인터넷에서 사용할 수 있습니다. 확인란을 선택하지 않은 상태로 두면 서버를 운영 네트워크에서만 사용할 수 있습니다.

    공용 IP 주소 사용 옵션을 사용하려면 **인터넷 액세스** 옵션을 활성화해야 합니다.

    구성을 완료하면 공용 IP 주소가 표시됩니다. 기본적으로 공용 IP 주소에 대한 인바운드 연결용으로는 TCP 포트 443이 열립니다.

    참고

    공용 IP 주소 사용 확인란의 선택을 취소하거나 복구 서버를 삭제하면 해당 공용 IP 주소가 예약되지 않습니다.

12. [선택 사항] [선택한 머신의 백업이 머신 속성으로서의 암호화를 사용하여 암호화된 경우], 암호화된 백업에서 복구 서버를 위한 가상 머신을 생성할 때 자동으로 사용될 암호를 지정합니다.

    a. **지정**을 클릭하고 암호화된 백업의 비밀번호를 입력한 후 자격 증명용 이름을 정의합니다.

       기본적으로 목록에서 가장 최근의 백업이 보입니다.

    b. [선택 사항] 모든 백업을 보려면 **모든 백업 표시**를 선택합니다.

    c. **완료**를 클릭합니다.

    참고

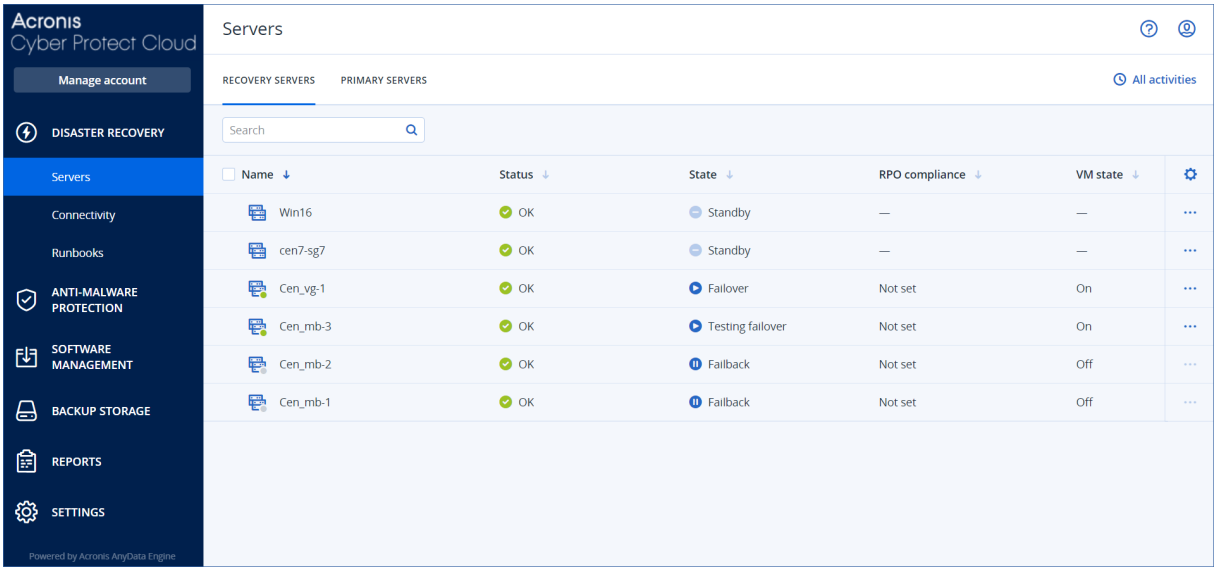
    여기서 지정하는 암호는 보안 자격 증명 저장소에 저장되지만 암호를 저장하면 규제 준수 관련 의무를 위반하게 될 수도 있습니다.

13. [선택 사항]복구 서버 이름을 변경합니다.
14. [선택 사항] 복구 서버에 대한 설명을 입력합니다.

© Acronis International GmbH, 2003-2024

15. [선택 사항] **클라우드 방화벽 규칙** 탭을 클릭하여 기본 방화벽 규칙을 편집합니다. 자세한 내용은 "클라우드 서버용 방화벽 규칙 설정"(734페이지)을(를) 참조하십시오.
16. **생성**을 클릭합니다.

복구 서버는 Cyber Protect 콘솔의 **재해 복구** > **서버** > **복구 서버** 탭에 표시됩니다. 원래 머신을 선택하고 **재해 복구**를 클릭하여 해당 설정을 볼 수 있습니다.



장애 조치 작동 방식

프로덕션 장애 조치

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

복구 서버를 생성하면 **대기** 상태로 유지됩니다. 해당 가상 머신은 장애 조치를 시작할 때까지 존재하지 않습니다. 장애 조치 프로세스를 시작하기 전에 원본 머신의 디스크 이미지 백업(부팅 가능 볼륨 포함)을 최소 하나 생성해야 합니다.

장애 조치 프로세스를 시작할 때는 매개변수가 사전 정의되어 있는 가상 머신을 생성할 원본 머신의 복구 지점(백업)을 선택합니다. 장애 조치 작업은 "백업에서 VM 실행" 기능을 사용합니다. 복구 서버가 전환 상태 **완료**를 가집니다. 이 프로세스에서는 서버의 가상 디스크가 백업 스토리지('콜드' 스토리지)에서 재해 복구 스토리지('핫' 스토리지)로 전송됩니다.

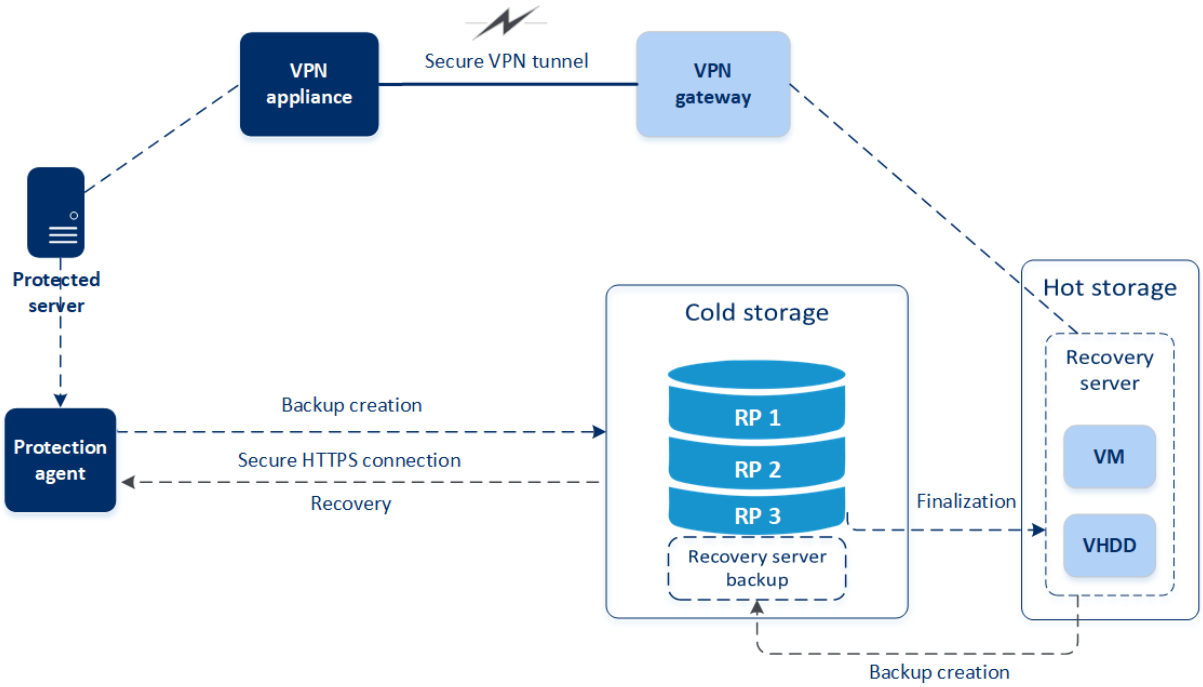
참고
완료 과정에서 서버에 액세스하고 작동할 수 있지만, 성능은 일반적인 경우보다 낮습니다. **콘솔이 준비됨** 링크를 클릭하여 서버 콘솔을 열 수 있습니다. 이 링크는 **재해 복구** > **서버** 화면의 **VM 상태** 열과 서버의 **상세 정보** 보기에서 사용할 수 있습니다.

완료가 완료되면 서버 성능은 정상값에 도달합니다. 서버 상태는 **장애 조치**로 변경됩니다. 이제 워크로드가 원본 머신에서 클라우드 사이트의 복구 서버로 전환됩니다.

© Acronis International GmbH, 2003-2024

복구 서버에 보호 에이전트가 있는 경우 에이전트 서비스가 중지되어 백업을 시작하거나 오래된 상태를 백업 컴퍼넌트에 보고하는 등의 간섭을 방지합니다.

아래 다이어그램에 장애 조치와 장애 복구 프로세스가 모두 나와 있습니다.



장애 조치 테스트

장애 조치 테스트 조치 중에는 가상 머신이 종료되지 않습니다. 즉, 에이전트가 가상 디스크의 내용을 백업에서 직접 읽으며 여러 백업 부분에 임의로 액세스하므로 성능이 일반 장애 조치 성능보다 약간 떨어질 수 있습니다. 테스트 장애 조치 프로세스에 대한 자세한 내용은 "테스트 장애 조치 수행"(712페이지)에서 참조하십시오.

자동 테스트 장애 조치

자동 테스트 장애 조치는 구성되어 있는 경우 수동 상호 작용을 수행하지 않아도 매월 한 번씩 수행됩니다. 자세한 내용은 "자동 테스트 장애 조치"(714페이지) 및 "자동 테스트 장애 조치 구성"(715페이지)을(를) 참조하십시오.

테스트 장애 조치 수행

테스트 장애 조치를 수행한다는 것은 운영 네트워크에서 격리된 테스트 VLAN에서 복구 서버를 시작한다는 것을 의미합니다. 한 번에 여러 복구 서버를 테스트하여 서버 간 상호 작용을 확인할 수 있습니다. 테스트 네트워크에서 서버는 운영 IP 주소를 사용하여 통신하지만 로컬 네트워크의 워크로드에 대한 TCP 또는 UDP 연결을 시작할 수 없습니다.

테스트 장애 조치 중에는 가상 머신(복구 서버)이 최종 확정되지 않습니다. 에이전트는 가상 디스크의 내용을 백업에서 직접 읽고 백업의 다른 부분에 임의로 액세스합니다. 이로 인해 테스트 장애 조치 상태에서 복구 서버의 성능이 정상 성능보다 느려질 수 있습니다.

© Acronis International GmbH, 2003-2024

테스트 장애 조치 수행은 선택 사항이지만 비용 및 안전면에서 적절한 빈도의 정기적인 프로세스로 설정하는 것이 좋습니다. 클라우드에서 운영 환경을 향상시키는 방법을 설명하는 지침인 실행서를 작성하는 것이 좋습니다.

중요
장치를 재해로부터 보호하려면 사전에 복구 서버를 생성해야 합니다.

장치의 복구 서버가 생성된 이후에 생성된 복구 지점에서만 장애 조치를 수행할 수 있습니다.

복구 서버 장애 조치를 하기 전에 최소 하나의 복구 지점을 생성해야 합니다. 지원되는 최대 복구 지점 수는 100개입니다.

테스트 장애 조치 수행

1. 원래 머신을 선택하거나 테스트할 복구 서버를 선택합니다.
2. **재해 복구**를 클릭합니다.
   복구 서버에 대한 설명이 열립니다.
3. **장애 조치**를 클릭합니다.
4. **테스트 장애 조치** 유형을 선택합니다.
5. 복구 지점(백업)을 선택한 다음 **시작**을 클릭합니다.
6. 선택한 백업이 머신 속성으로 암호화를 사용하여 암호화된 경우입니다.
   a. 백업 세트의 암호화 비밀번호를 입력합니다.

      참고
      암호는 임시로만 저장되며 현재 테스트 장애 조치 작업에만 사용됩니다. 암호는 테스트 장애 조치를 중지하는 경우 또는 테스트 장애 조치가 완료된 후에 자격 증명 저장소에서 자동으로 삭제됩니다.

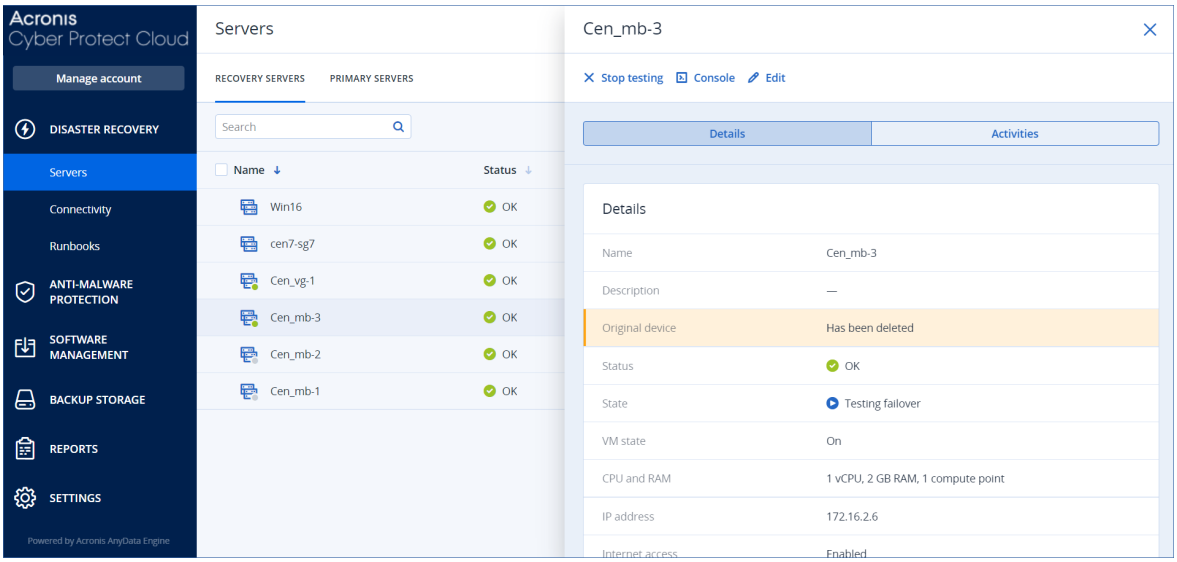
   b. [선택 사항] 백업 세트의 암호를 저장해 두었다가 후속 장애 조치 작업에 사용하려면 **보안 자격 증명 저장소에 암호 저장...** 확인란을 선택하고 **자격 증명 이름** 필드에 자격 증명용 이름을 입력합니다.

      중요
      암호가 보안 자격 증명 저장소에 저장되며 후속 장애 조치 작업에서 자동으로 적용됩니다. 그러나 암호 저장 시에는 규제 준수 관련 의무를 위반하게 될 수도 있습니다.

   c. **완료**를 클릭합니다.

   복구 서버가 시작되면 상태가 **장애 조치 테스트**로 변경됩니다.

© Acronis International GmbH, 2003-2024



7. 다음 방법을 사용하여 복구 서버를 테스트합니다.
   - **재해 복구** > **서버**에서 복구 서버를 선택한 다음, **콘솔**을 클릭합니다.
   - RDP 또는 SSH 및 복구 서버를 만들 때 지정한 테스트 IP 주소를 사용하여 복구 서버에 연결합니다. "지점 및 사이트 간 연결"에서 설명한 대로 운영 네트워크의 내부 및 외부 모두에서 연결을 시도합니다.
   - 복구 서버 내에서 스크립트를 실행합니다.

     스크립트에서 로그인 화면, 애플리케이션 시작 여부, 인터넷 연결 및 다른 머신이 복구 서버에 연결할 수 있는지 여부를 확인할 수 있습니다.
   - 복구 서버가 인터넷 및 공용 IP 주소에 액세스 할 수 있는 경우 TeamViewer를 사용할 수 있습니다.
8. 테스트가 완료되면 **테스트 중지**를 클릭합니다.

   복구 서버가 중지됩니다. 테스트 장애 조치 중 복구 서버에 대한 모든 변경 사항이 유지되지 않습니다.

참고

실행서에서, 그리고 테스트 장애 조치를 수동으로 시작할 때는 테스트 장애 조치 작업에서 **서버 시작** 및 **서버 중지** 작업을 실행할 수 없습니다. 이러한 작업을 실행하려고 하면 작업이 실패하며 다음 오류 메시지가 표시됩니다.

실패: 해당 작업은 현재 서버 상태에 적용될 수 없습니다.

자동 테스트 장애 조치

자동 테스트 장애 조치 사용 시에는 수동 상호 작용을 수행하지 않아도 매월 한 번씩 복구 서버 테스트가 자동으로 진행됩니다.

자동 테스트 장애 조치 프로세스에서는 다음 작업이 수행됩니다.

1. 마지막 복구 지점에서 가상 머신 생성
2. 가상 머신의 스크린샷 생성

© Acronis International GmbH, 2003-2024

3. 가상 머신의 운영 체제가 정상적으로 시작되는지 분석
4. 테스트 장애 조치 상태 관련 알림 표시

참고
자동 테스트 장애 조치에서는 컴퓨팅 포인트가 사용됩니다.

복구 서버의 설정에서 자동 테스트 장애 조치를 구성할 수 있습니다. 자세한 내용은 "자동 테스트 장애 조치 구성"(715페이지)을(를) 참조하십시오.

드물지만 자동 테스트 장애 조치가 건너뛰기되어 예약된 시간에 수행되지 않는 경우도 있습니다. 프로덕션 장애 조치의 우선 순위가 자동 테스트 장애 조치보다 높으므로, 동시에 실행되는 프로덕션 장애 조치에서 충분한 리소스를 사용할 수 있도록 자동 테스트 장애 조치에 할당되는 하드웨어 리소스(CPU 및 RAM)가 일시적으로 제한될 수도 있기 때문입니다.

자동 테스트 장애 조치를 건너뛰는 경우에는 경보가 표시됩니다.

참고
원래 머신의 백업이 머신 속성으로서의 암호화를 사용하여 암호화되고 복구 서버를 생성할 때 암호화 암호가 지정되지 않으면 자동화된 테스트 장애 조치가 실패합니다. 암호화 암호를 지정하는 방법에 대한 자세한 정보는 "복구 서버 생성"(708페이지)을(를) 참조하십시오.

자동 테스트 장애 조치 구성

자동 테스트 장애 조치를 구성하면 수동 작업을 수행하지 않고도 매월 복구 서버를 테스트할 수 있습니다.

자동 테스트 장애 조치를 구성하려면

1. 콘솔에서 **재해 복구** > **서버** > **복구 서버**로 이동해 복구 서버를 선택합니다.
2. **편집**을 클릭합니다.
3. **자동 테스트 장애 조치** 섹션의 **예약** 필드에서 **월간**을 선택합니다.
4. [선택 사항] **스크린샷 시간 초과**에서 시스템이 자동 테스트 장애 조치 수행을 시도하도록 할 최대 기간(분)의 기본값을 변경합니다.
5. [선택 사항] **스크린샷 시간 초과** 값을 기본값으로 저장하여 다른 복구 서버에서 자동 테스트 장애 조치를 활성화할 때 자동으로 입력하려면 **기본 시간 초과로 설정**을 선택합니다.
6. **저장**을 클릭합니다.

자동 테스트 장애 조치 상태 확인

완료된 자동 테스트 장애 조치의 상세 정보(예: 장애 조치 상태, 시작 시간, 종료 시간, 소요 시간, 가상 머신의 스크린샷)를 확인할 수 있습니다.

복구 서버의 자동 테스트 장애 조치 상태를 확인하려면

1. 콘솔에서 **재해 복구** > **서버** > **복구 서버**로 이동해 복구 서버를 선택합니다.
2. **자동 테스트 장애 조치** 섹션에서 마지막 자동 테스트 장애 조치의 상세 정보를 확인합니다.
3. [선택 사항] **스크린샷 표시**를 클릭하여 가상 머신의 스크린샷을 확인합니다.

© Acronis International GmbH, 2003-2024

자동 테스트 장애 조치 비활성화

리소스를 절약하려는 경우나 특정 복구 서버에서는 자동 테스트 장애 조치를 수행할 필요가 없는 경우에는 자동 테스트 장애 조치를 비활성화할 수 있습니다.

자동 테스트 장애 조치를 비활성화하려면

1. 콘솔에서 **재해 복구** > **서버** > **복구 서버**로 이동해 복구 서버를 선택합니다.
2. **편집**을 클릭합니다.
3. **자동 테스트 장애 조치** 섹션의 **예약** 필드에서 **안 함**을 선택합니다.
4. **저장**을 클릭합니다.

장애 조치 수행

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

장애 조치는 작업 부하를 프레미스에서 클라우드로 이동하는 프로세스이며 작업 부하가 클라우드에 남아있는 상태입니다.

장애 조치를 시작하면 복구 서버가 운영 네트워크에서 시작됩니다. 간섭 및 원치 않는 문제를 방지하려면 원래 워크로드가 온라인 상태가 아니며 VPN을 통해 액세스할 수 없는지 확인하십시오.

같은 클라우드 아카이브에 대해 수행하는 백업이 중단되는 상황을 방지하려면 현재 **장애 조치** 상태인 워크로드에서 보호 계획을 수동으로 해지합니다. 계획 철회에 대한 자세한 내용은 보호 계획 철회를 참조하십시오.

중요
장치를 재해로부터 보호하려면 사전에 복구 서버를 생성해야 합니다.

장치의 복구 서버가 생성된 이후에 생성된 복구 지점에서만 장애 조치를 수행할 수 있습니다.

복구 서버 장애 조치를 하기 전에 최소 하나의 복구 지점을 생성해야 합니다. 지원되는 최대 복구 지점 수는 100개입니다.

아래 지침을 따르거나 비디오 자습서를 시청할 수 있습니다.

장애 조치를 수행하려면:

1. 원래 머신을 네트워크에서 사용할 수 없는지 확인하십시오.
2. Cyber Protect 콘솔에서 **재해 복구** > **서버** > **복구 서버**로 이동해 복구 서버를 선택합니다.
3. **장애 조치**를 클릭합니다.
4. **프로덕션 장애 조치** 유형을 선택합니다.
5. 복구 지점(백업)을 선택한 다음 **시작**을 클릭합니다.
6. [선택한 백업이 머신 속성으로 암호화를 사용하여 암호화된 경우]

© Acronis International GmbH, 2003-2024

a. 백업 세트의 암호화 비밀번호를 입력합니다.

참고
암호는 임시로만 저장되며 현재 장애 조치 작업에만 사용됩니다. 장애 조치 작업이 완료되고 나면 암호가 자격 증명 저장소에서 자동으로 삭제되며 서버는 **대기** 상태로 돌아갑니다.

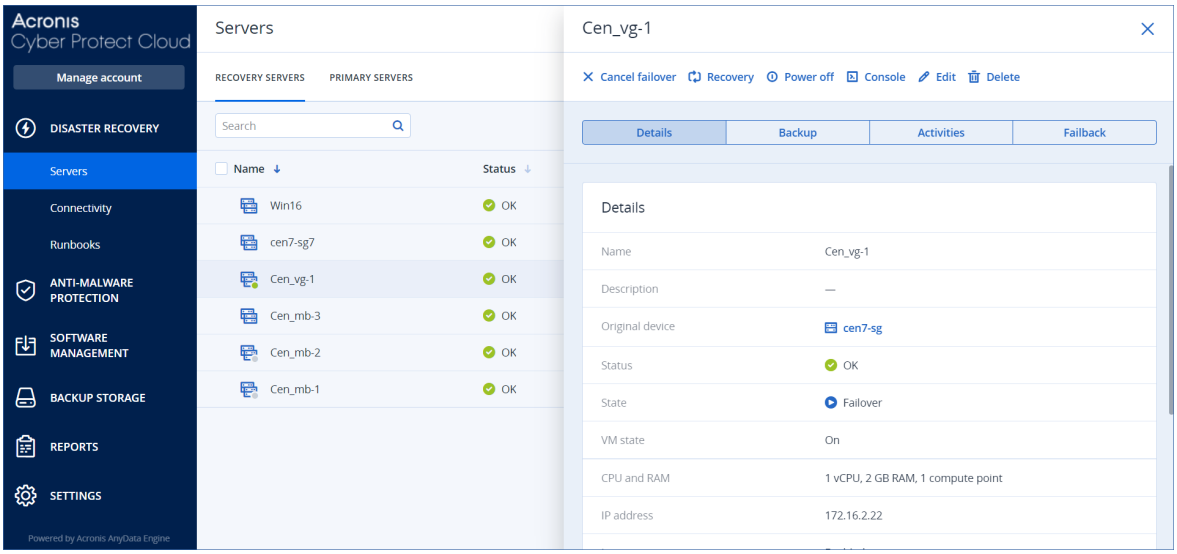
b. [선택 사항] 백업 세트의 암호를 저장해 두었다가 후속 장애 조치 작업에 사용하려면 **보안 자격 증명 저장소에 암호 저장...** 확인란을 선택하고 **자격 증명 이름** 필드에 자격 증명용 이름을 입력합니다.

중요
암호가 보안 자격 증명 저장소에 저장되며 후속 장애 조치 작업에서 자동으로 적용됩니다. 그러나 암호 저장 시에는 규제 준수 관련 의무를 위반하게 될 수도 있습니다.

c. **완료**를 클릭합니다.

복구 서버가 시작되면 상태가 **완료**로 변경된 후 일정 시간이 지난 후 **장애 조치**로 변경됩니다.

중요
완료 및 **장애 조치** 상태에서도 서버를 사용할 수 있다는 점을 이해해야 합니다. **완료** 과정에서 **콘솔이 준비됨** 링크를 클릭하여 서버 콘솔에 액세스할 수 있습니다. 이 링크는 **재해 복구** > **서버** 화면의 **VM 상태** 열과 서버의 **상세 정보** 보기에서 사용할 수 있습니다. 자세한 내용은 "장애 조치 작동 방식"(711페이지) 항목을 참조하십시오.



7. 콘솔을 보고 복구 서버가 시작되었는지 확인하십시오. **재해 복구** > **서버**에서 복구 서버를 선택한 다음, **콘솔**을 클릭합니다.
8. 복구 서버를 만들 때 지정한 운영 IP 주소를 사용하여 복구 서버에 액세스할 수 있는지 확인하십시오.

복구 서버가 완료되면 새 보호 계획이 자동으로 생성되어 복구 서버에 적용됩니다. 이 보호 계획은 특정 제한 사항이 있는 복구 서버를 만드는 데 사용된 보호 계획을 기반으로 합니다. 이 계획에서는 일정 및 보관 규칙만 변경할 수 있습니다. 자세한 내용은 "클라우드 서버 백업"을 참조하십시오.

© Acronis International GmbH, 2003-2024

장애 조치를 취소하고 싶으면 해당 복구 서버를 선택한 다음 **장애 조치 취소**를 클릭합니다. 장애 조치 시점부터 적용된 모든 변경 사항(복구 서버 백업은 제외)이 손실됩니다. 복구 서버가 **대기** 상태로 돌아갑니다.

장애 복구를 수행하려는 경우 복구 서버를 선택하고 **장애 복구**를 클릭합니다.

로컬 DNS를 사용하는 서버의 장애 조치 수행 방법

머신 이름을 해석하는 데 로컬 사이트의 DNS 서버를 사용 중인 경우, 장애 조치를 수행하고 나면 이 DNS에 의존하는 머신들에 해당하는 복구 서버가 통신에 실패하는데, 이는 클라우드에서 사용되는 DNS 서버가 로컬 사이트의 서버와 다르기 때문입니다. 기본적으로 클라우드 사이트의 DNS 서버는 새로 생성된 클라우드 서버용으로 사용됩니다. 사용자 정의 DNS 설정을 적용해야 하는 경우 지원 팀에 문의하십시오.

DHCP 서버의 장애 조치 수행 방법

로컬 인프라에 Windows 또는 Linux 호스트에 배치된 DHCP 서버가 있을 수 있습니다. 이러한 호스트가 클라우드 사이트로 장애 조치된 경우 클라우드의 VPN 게이트웨이 역시 DHCP 역할을 하므로 DHCP 서버 중복 문제가 발생합니다. 이 문제를 해결하려면 다음 중 하나를 수행합니다.

- DHCP 호스트만 클라우드로 장애 조치하고, 나머지 로컬 서버는 그대로 로컬 사이트에 유지하는 경우에는 클라우드에서 DHCP 호스트에 로그인하고 해당 DHCP 서버를 꺼야 합니다. 그러면 충돌이 발생하지 않고, VPN 게이트웨이만 DHCP 서버의 역할을 하게 됩니다.
- 클라우드 서버가 DHCP 호스트로부터 IP 주소를 이미 가져온 경우에는 클라우드의 DHCP 호스트에 로그인하고 해당 DHCP 서버를 꺼야 합니다. 또한, 클라우드 서버에 로그인하고 DHCP 임대를 갱신하여 올바른 DHCP 서버(VPN 게이트웨이에서 호스팅되는 서버)에서 할당되는 새 IP 주소를 할당해야 합니다.

참고
클라우드 DHCP 서버가 **사용자 지정 DHCP** 옵션으로 구성되어 있고 일부 복구 서버 또는 기본 서버가 이 DHCP 서버에서 IP 주소를 가져오는 경우에는 지침이 유효하지 않습니다.

장애 복구 작동 방식

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

장애 복구는 클라우드에서 로컬 사이트의 실제 머신이나 가상 머신으로 워크로드를 다시 이동하는 프로세스입니다. **장애 조치** 상태의 복구 서버에서 장애 복구를 수행하고 로컬 사이트의 서버를 계속 사용할 수 있습니다.

로컬 사이트의 실제 대상 머신으로 자동 장애 조치를 수행할 수 있습니다. 장애 복구 중에는 클라우드의 가상 머신을 계속 실행하면서 로컬 사이트로 백업 데이터를 전송할 수 있습니다. 이 기술을 활용하면 다운타임을 대폭 줄일 수 있습니다. 예상 다운타임은 Cyber Protect 콘솔에 표시됩니다. 이 정보를 확인한 후 활동을 계획할 때 사용할 수 있습니다. 필요한 경우에는 예정된 정지 시간 관련 경고를 고객에게 제공할 수도 있습니다.

© Acronis International GmbH, 2003-2024

대상 가상 머신 및 대상 실제 머신으로의 장애 복구 프로세스는 약간 다릅니다. 장애 복구 프로세스의 단계에 대한 자세한 내용은 "대상 가상 머신으로 장애 복구"(719페이지) 및 "대상 실제 머신으로 장애 복구"(724페이지)을(를) 참조하십시오.

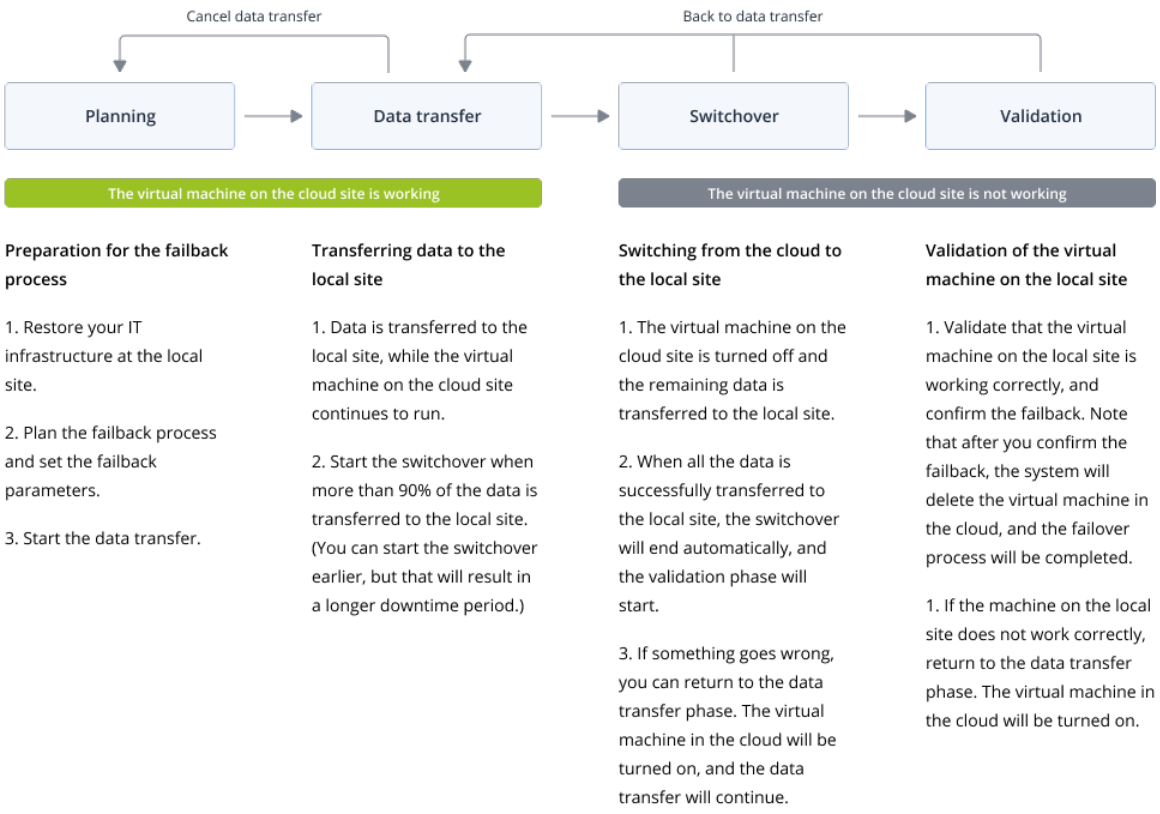
자동 장애 복구 절차를 사용할 수 없는 경우에는 수동 장애 복구를 수행할 수 있습니다. 자세한 내용은 "수동 장애 복구"(727페이지)을(를) 참조하십시오.

참고
런북 작업에서는 수동 모드의 장애 복구만 지원됩니다. 즉, **서버 장애 복구** 단계가 포함된 런북을 실행하여 장애 복구 프로세스를 시작하는 경우 장애 복구 절차에서 수동 상호 작용을 수행해야 합니다. 구체적으로는 머신을 수동으로 복구한 다음 **재해 복구** > **서버** 탭에서 장애 복구 프로세스를 확인하거나 취소해야 합니다.

대상 가상 머신으로 장애 복구

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

대상 가상 머신으로의 장애 복구 프로세스에서는 다음의 4단계를 수행합니다.



1. **계획**. 이 단계에서는 호스트, 네트워크 구성과 같은 로컬 사이트의 IT 인프라를 복원하고 장애 복구 매개변수를 구성한 다음 데이터 전송을 시작할 시기를 계획합니다.

© Acronis International GmbH, 2003-2024

참고
장애 복구 프로세스에 소요되는 총 시간을 최소화하려면 로컬 서버를 설정한 직후 데이터 전송 단계를 시작하고, 그런 다음 데이터 전송 단계 중에 네트워크 및 로컬 인프라의 나머지 부분을 계속 구성하는 것이 좋습니다.

2. **데이터 전송**. 이 단계에서는 클라우드 사이트에서 로컬 사이트로 데이터를 전송합니다. 데이터를 전송하는 동안 클라우드의 가상 머신은 계속 실행됩니다. 데이터 전송 단계 도중 언제든지 다음 단계인 전환을 시작할 수 있습니다. 단, 이 경우에는 다음과 같은 관계를 고려해야 합니다.
   데이터 전송 단계의 소요 시간이 길어질수록
   - 클라우드의 가상 머신이 계속 실행되는 시간도 길어집니다.
   - 로컬 사이트로 전송되는 데이터의 양도 많아집니다.
   - 컴퓨팅 포인트를 더 많이 사용하므로 지불해야 비용도 늘어납니다.
   - 전환 단계에서 발생하는 다운타임 기간이 짧아집니다.

   다운타임을 최소화하려면 90% 이상의 데이터가 로컬 사이트로 전송된 후에 전환 단계를 시작하십시오.

   다운타임 기간이 길어지면 안 되며 클라우드에서 가상 머신을 실행하는 데 컴퓨팅 포인트를 추가로 사용하지 않으려는 경우에는 전환 단계를 더 일찍 시작하면 됩니다.

   데이터 전송 단계 중에 장애 복구 프로세스를 취소하더라도 전송된 데이터는 로컬 사이트에서 삭제되지 않습니다. 문제 발생 가능성을 방지하려면 새 장애 복구 프로세스를 시작하기 전에 전송된 데이터를 수동으로 삭제하십시오. 후속 데이터 전송 프로세스는 처음부터 시작됩니다.
3. **전환**. 이 단계에서는 클라우드의 가상 머신이 꺼지며 마지막 백업 증분을 포함한 나머지 데이터가 로컬 사이트로 전송됩니다. 복구 서버에 백업 계획이 적용되어 있지 않으면 전환 단계에서 백업이 자동으로 수행되므로 프로세스 속도가 느려집니다.

   Cyber Protect 콘솔에서 이 단계의 예상 완료 시간(다운타임 기간)을 확인할 수 있습니다. 모든 데이터가 로컬 사이트로 전송되면(손실된 데이터가 없으며 로컬 사이트의 가상 머신이 클라우드 가상 머신의 정확한 복사본임) 전환 단계가 완료됩니다. 그리고 나면 로컬 사이트의 가상 머신이 복구되며 유효성 검사 단계가 자동으로 시작됩니다.
4. **유효성 검사**. 이 단계에서는 로컬 사이트의 가상 머신이 준비되고 자동으로 시작됩니다. 가상 머신이 정상 작동 중인지를 확인하여 다음 작업 중 하나를 수행할 수 있습니다.
   - 모든 기능이 정상 작동하면 장애 복구를 확인할 수 있습니다. 장애 복구 확인 후에는 클라우드의 가상 머신이 삭제되며 복구 서버가 **대기** 상태로 돌아갑니다. 그러면 장애 복구 프로세스가 종료됩니다.
   - 문제가 발생하면 전환을 취소하고 데이터 전송 단계로 돌아갈 수 있습니다.

가상 머신으로의 장애 복구 수행

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

로컬 사이트의 대상 가상 머신으로 장애 복구를 수행할 수 있습니다.

© Acronis International GmbH, 2003-2024

사전 요구 사항

- 장애 복구를 수행하는 데 사용할 에이전트가 온라인 상태여야 하며 현재 다른 장애 복구 작업에 사용되고 있지 않아야 합니다.
- 인터넷에 안정적으로 연결할 수 있어야 합니다.
- 클라우드에 가상 머신의 전체 백업이 하나 이상 있습니다.

가상 머신으로의 장애 복구를 수행하려면

1. Cyber Protect 콘솔에서 **재해 복구** > **서버**로 이동합니다.
2. **장애 조치** 상태에 있는 복구 서버를 선택합니다.
3. **장애 복구** 탭을 클릭합니다.
4. **장애 복구 매개변수** 섹션에서 **가상 머신**을 **대상**으로 선택하고 다른 매개변수를 구성합니다.
   기본적으로 일부 **장애 복구 매개변수**에는 제안 값이 자동 입력됩니다. 하지만 이러한 값을 변경할 수 있습니다.
   다음 표에는 **장애 복구 매개변수**에 대한 자세한 내용이 나와 있습니다.

매개변수	설명
백업 크기	장애 복구 프로세스 중에 로컬 사이트로 전송되는 데이터의 양입니다. 대상 가상 머신으로 장애 복구 프로세스를 시작한 후에는 클라우드의 가상 머신이 계속 실행되고 새 데이터가 생성되기 때문에 데이터 전송 단계에서 **백업 크기**가 증가합니다. 대상 가상 머신에 대한 장애 복구 프로세스 중에 예상 다운타임 기간을 계산하려면 **백업 크기** 값의 10%를 인터넷 속도의 값으로 나눕니다. 백업 크기 값의 10%를 사용하는 이유는, 데이터 중 90%가 로컬 사이트로 전송된 후에 전환 단계를 시작하는 것이 좋기 때문입니다. **참고** 여러 장애 복구 프로세스를 동시에 수행하면 인터넷 속도 값이 줄어듭니다.
대상	클라우드 서버를 복구할 로컬 사이트의 워크로드 유형입니다. **실제 머신** 또는 **가상 머신** 중 하나를 선택합니다.
대상 머신 위치	장애 복구 위치: VMware ESXi 호스트 또는 Microsoft Hyper-V 호스트 중 하나를 선택합니다. Cyber Protection 서비스에 등록된 에이전트가 설치되어 있는 모든 호스트 중에서 선택할 수 있습니다.
에이	장애 복구 작업을 수행할 에이전트입니다. 에이전트 하나를 사용해 장애 복구 작업 하나를 동시에 수행할 수 있습니다.

© Acronis International GmbH, 2003-2024

매개변수	설명
전트	온라인 상태이고, 백업 액세스 권한이 있으며, 현재 다른 장애 복구 프로세스에 사용되고 있지 않고, 장애 복구 기능을 지원하는 버전의 에이전트를 선택할 수 있습니다. VMware ESXi 호스트에 여러 에이전트를 설치한 다음 각 에이전트를 사용하여 각기 별도의 장애 복구 프로세스를 시작할 수 있습니다. 이러한 장애 복구 프로세스는 동시에 수행 가능합니다.
대상 머신 설정	가상 머신 설정: • **가상 프로세서**. 가상 프로세서의 수를 선택합니다. • **메모리**. 가상 머신에 할당할 메모리를 선택합니다. • **단위**. 메모리의 단위를 선택합니다. • [선택 사항] **네트워크 어댑터**. 네트워크 어댑터를 추가하려면 **추가**를 클릭하고 **네트워크** 필드에서 네트워크를 선택합니다. 변경할 매개변수를 모두 설정한 후 **완료**를 클릭합니다.
경로	(Microsoft Hyper-V 호스트에 해당됨) 머신을 저장할 호스트의 폴더입니다. 호스트에 머신용으로 사용 가능한 메모리 공간이 충분한지 확인하십시오.
데이터 저장소	(VMware ESXi 호스트에 해당됨) 머신을 저장할 호스트의 데이터 저장소입니다. 호스트에 머신용으로 사용 가능한 메모리 공간이 충분한지 확인하십시오.
프로비저닝 모드	가상 디스크의 할당 방법입니다. Microsoft Hyper-V 호스트: • **동적 확장**(기본값). • **고정 크기**. Microsoft Hyper-V 호스트: • **씬**(기본값). • **씩**.
대상 머신 이름	대상 머신의 이름입니다. 기본적으로 대상 머신 이름은 복구 서버 이름과 같습니다. 대상 머신 이름은 선택한 **대상 머신 위치**에서 고유해야 합니다.

5. **데이터 전송 시작**을 클릭하고 확인 창에서 **시작**을 클릭합니다.

© Acronis International GmbH, 2003-2024

참고
클라우드에 가상 머신 백업이 없으면 시스템이 데이터 전송 단계 전에 자동으로 백업을 수행합니다.

데이터 전송 단계가 시작됩니다. 콘솔에는 다음 정보가 표시됩니다.

필드	설명
진행률	로컬 사이트로 이미 전송된 데이터의 양과 전송해야 하는 총 데이터 양을 보여 주는 매개변수입니다. 데이터 전송 단계에서도 가상 머신은 계속 실행되므로 총 데이터 양에는 데이터 전송 단계가 시작되기 전에 마지막으로 수행한 백업의 데이터, 그리고 새로 생성된 데이터의 백업(백업 증분)이 포함됩니다. 그러므로 **진행률** 매개변수의 두 값은 시간이 지남에 따라 커집니다.
예상 다운타임	지금 전환 단계를 시작하는 경우 클라우드의 가상 머신을 사용할 수 없는 시간을 보여 주는 매개변수입니다. 이 값은 **진행률** 매개변수의 값을 기준으로 계산되며 시간이 지남에 따라 작아집니다.

6. **전환**을 클릭하고 확인 창에서 **전환**을 다시 클릭합니다.
   전환 단계가 시작됩니다. 콘솔에는 다음 정보가 표시됩니다.

필드	설명
진행률	로컬 사이트에서 머신을 복원하는 작업의 진행률을 보여 주는 매개변수입니다.
완료까지의 예상 시간	전환 단계가 완료되어 로컬 사이트에서 머신을 시작할 수 있는 대략적인 시간을 보여 주는 매개변수입니다.

참고
클라우드의 가상 머신에 백업 계획이 적용되어 있지 않으면 전환 단계에서 백업이 자동으로 수행되므로 다운타임이 길어집니다.

7. **전환** 단계가 완료되어 로컬 사이트에서 가상 머신이 자동으로 시작되고 나면 해당 머신이 정상 작동 중인지 유효성을 검사합니다.
8. **장애 복구 확인**을 클릭하고 확인 창에서 **확인**을 클릭하여 프로세스를 완료합니다.
   클라우드의 가상 머신이 삭제되며 복구 서버가 **대기** 상태로 돌아갑니다.

© Acronis International GmbH, 2003-2024

참고

복구된 서버에서 보호 계획을 적용하는 것은 장애 복구 프로세스에 포함되지 않습니다. 장애 복구 프로세스가 완료된 후 복구된 서버에서 보호 계획을 적용하여 서버가 다시 보호되도록 하십시오. 원래 서버에 적용했던 것과 같은 보호 계획을 적용할 수도 있고 **Disaster Recovery** 모듈이 활성화된 새 보호 계획을 적용할 수도 있습니다.

대상 실제 머신으로 장애 복구

참고

이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

대상 실제 머신으로의 자동 장애 복구 프로세스에서는 다음 단계를 수행합니다.

1. **계획**. 이 단계에서는 호스트, 네트워크 구성과 같은 로컬 사이트의 IT 인프라를 복원하고 장애 복구 매개변수를 구성한 다음 데이터 전송을 시작할 시기를 계획합니다.
2. **데이터 전송**. 이 단계에서는 클라우드 사이트에서 로컬 사이트로 데이터를 전송합니다. 데이터를 전송하는 동안 클라우드의 가상 머신은 계속 실행됩니다. 데이터 전송 단계 도중 언제든지 다음 단계인 전환을 시작할 수 있습니다. 단, 이 경우에는 다음과 같은 관계를 고려해야 합니다.

   데이터 전송 단계의 소요 시간이 길어질수록
   - 클라우드의 가상 머신이 계속 실행되는 시간도 길어집니다.
   - 로컬 사이트로 전송되는 데이터의 양도 많아집니다.
   - 컴퓨팅 포인트를 더 많이 사용하므로 지불해야 비용도 늘어납니다.
   - 전환 단계에서 발생하는 다운타임 기간이 짧아집니다.

   다운타임을 최소화하려면 90% 이상의 데이터가 로컬 사이트로 전송된 후에 전환 단계를 시작하십시오.

   다운타임 기간이 길어지면 안 되며 클라우드에서 가상 머신을 실행하는 데 컴퓨팅 포인트를 추가로 사용하지 않으려는 경우에는 전환 단계를 더 일찍 시작하면 됩니다.

   참고

   데이터 전송 프로세스에서는 플래시백 기술을 사용합니다. 이 기술은 대상 머신에서 사용 가능한 데이터를 클라우드의 가상 머신 데이터와 비교합니다. 데이터 중 대상 머신에서 이미 사용 가능한 데이터는 다시 전송되지 않습니다. 이 기술로 인해 데이터 전송 단계가 더욱 빠르게 진행됩니다.

   그러므로 로컬 사이트의 원래 머신으로 서버를 복원하는 것이 좋습니다.
3. **전환**. 이 단계에서는 클라우드의 가상 머신이 꺼지며 마지막 백업 증분을 포함한 나머지 데이터가 로컬 사이트로 전송됩니다. 복구 서버에 백업 계획이 적용되어 있지 않으면 전환 단계에서 백업이 자동으로 수행되므로 프로세스 속도가 느려집니다.
4. **유효성 검사**. 이 단계에서는 로컬 사이트의 실제 머신이 준비되며 Linux 기반 부트 가능한 미디어를 사용하여 해당 머신을 재부팅할 수 있습니다. 가상 머신이 정상 작동 중인지 확인하고
   - 모든 기능이 정상 작동하면 장애 복구를 확인할 수 있습니다. 장애 복구 확인 후에는 클라우드의 가상 머신이 삭제되며 복구 서버가 **대기** 상태로 돌아갑니다. 그러면 장애 복구 프로세

© Acronis International GmbH, 2003-2024

스가 종료됩니다.

- 문제가 발생하면 장애 조치를 취소하고 계획 단계로 돌아갈 수 있습니다.

참고
부트 가능한 미디어는 재부팅 후에는 다시 사용할 수 없습니다. 유효성 검사 단계에서 문제가 확인되면 새 부트 가능한 미디어를 등록하고 장애 복구 프로세스를 다시 시작해야 합니다.
그러나 데이터 전송 프로세스에서는 플래시백 기술이 사용되므로 로컬 사이트에 이미 있는 데이터는 다시 전송되지 않기 때문에 장애 복구 프로세스의 속도가 훨씬 빨라집니다.

실제 머신으로의 장애 복구 수행

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

로컬 사이트의 대상 실제 머신으로 자동 장애 복구를 수행할 수 있습니다.

참고
데이터 전송 프로세스에서는 플래시백 기술을 사용합니다. 이 기술은 대상 머신에서 사용 가능한 데이터를 클라우드의 가상 머신 데이터와 비교합니다. 데이터 중 대상 머신에서 이미 사용 가능한 데이터는 다시 전송되지 않습니다. 이 기술로 인해 데이터 전송 단계가 더욱 빠르게 진행됩니다.

그러므로 로컬 사이트의 원래 머신으로 서버를 복원하는 것이 좋습니다.

사전 요구 사항

- 장애 복구를 수행하는 데 사용할 에이전트가 온라인 상태여야 하며 현재 다른 장애 복구 작업에 사용되고 있지 않아야 합니다.
- 인터넷에 안정적으로 연결할 수 있어야 합니다.
- 등록되어 있는 부트 가능한 미디어를 사용할 수 있습니다. 자세한 내용은 Cyber Protection 사용자 안내서에서 "운영 체제 복구용으로 부트 가능한 미디어 생성"을 참조하십시오.
- 대상 실제 머신은 로컬 사이트의 원래 머신이거나 원래 머신과 펌웨어가 동일한 머신입니다.
- 클라우드에 가상 머신의 전체 백업이 하나 이상 있습니다.

실제 머신으로의 장애 복구를 수행하려면

1. Cyber Protect 콘솔에서 **재해 복구** > **서버**로 이동합니다.
2. **장애 조치** 상태에 있는 복구 서버를 선택합니다.
3. **장애 복구** 탭을 클릭합니다.
4. **대상** 필드에서 **실제 머신**을 선택합니다.
5. **대상 부트 가능한 미디어 필드에서 지정**을 클릭하고 부트 가능한 미디어를 선택한 후 **완료**를 클릭합니다.

© Acronis International GmbH, 2003-2024

참고
이미 생성되어 구성이 완료된 부트 가능한 미디어를 사용하는 것이 좋습니다. 자세한 내용은 Cyber Protection 사용자 안내서에서 "운영 체제 복구용으로 부트 가능한 미디어 생성"을 참조하십시오.

6. [선택 사항] 기본 디스크 매핑을 변경하려면 **디스크 매핑** 필드에서 **지정**을 클릭하고 백업의 디스크를 대상 머신의 디스크로 매핑한 후 **완료**를 클릭합니다.
7. **데이터 전송 시작**을 클릭하고 확인 창에서 **시작**을 클릭합니다.

참고
클라우드에 가상 머신 백업이 없으면 시스템이 데이터 전송 단계 전에 자동으로 백업을 수행합니다.

데이터 전송 단계가 시작됩니다. 콘솔에는 다음 정보가 표시됩니다.

필드	설명
진행률	로컬 사이트로 이미 전송된 데이터의 양과 전송해야 하는 총 데이터 양을 보여 주는 매개변수입니다. 데이터 전송 단계에서도 가상 머신은 계속 실행되므로 총 데이터 양에는 데이터 전송 단계가 시작되기 전에 마지막으로 수행한 백업의 데이터, 그리고 새로 생성된 데이터의 백업(백업 증분)이 포함됩니다. 그러므로 **진행률** 값은 시간이 지남에 따라 커집니다. 시스템은 데이터 전송 중에 플래시백 기술을 사용하며 대상 머신에서 이미 사용 가능한 데이터는 전송하지 않으므로 콘솔에서 처음 계산되어 표시되었던 것보다 전송이 더 빠르게 진행될 수도 있습니다.
예상 다운타임	지금 전환 단계를 시작하는 경우 클라우드의 가상 머신을 사용할 수 없는 시간을 보여 주는 매개변수입니다. 이 값은 **진행률** 매개변수의 값을 기준으로 계산되며 시간이 지남에 따라 작아집니다. 시스템은 데이터 전송 중에 플래시백 기술을 사용하며 대상 머신에서 이미 사용 가능한 데이터는 전송하지 않으므로 다운타임이 콘솔에 처음 표시되었던 값보다 훨씬 짧아질 수도 있습니다.

8. **전환**을 클릭하고 확인 창에서 **전환**을 다시 클릭합니다.
전환 단계가 시작됩니다. 콘솔에는 다음 정보가 표시됩니다.

필드	설명
진행률	로컬 사이트에서 머신을 복원하는 작업의 진행률을 보여 주는 매개변수입니다.
완료까지의 예상 시간	전환 단계가 완료되어 로컬 사이트에서 머신을 시작할 수 있는 대략적인 시간을 보여 주는 매개변수입니다.

© Acronis International GmbH, 2003-2024

참고
클라우드의 가상 머신에 백업 계획이 적용되어 있지 않으면 전환 단계에서 백업이 자동으로 수행되므로 다운타임이 길어집니다.

9. **전환** 단계가 완료되면 부트 가능한 미디어를 재부팅하고 로컬 사이트의 실제 머신이 정상적으로 작동하는지를 확인합니다.
   자세한 내용은 Cyber Protection 사용자 안내서에서 "부트 가능한 미디어를 사용하여 디스크 복구"를 참조하십시오.
10. **장애 복구 확인**을 클릭하고 확인 창에서 **확인**을 클릭하여 프로세스를 완료합니다.
    클라우드의 가상 머신이 삭제되며 복구 서버가 **대기** 상태로 돌아갑니다.

참고
복구된 서버에서 보호 계획을 적용하는 것은 장애 복구 프로세스에 포함되지 않습니다. 장애 복구 프로세스가 완료된 후 복구된 서버에서 보호 계획을 적용하여 서버가 다시 보호되도록 하십시오. 원래 서버에 적용했던 것과 같은 보호 계획을 적용할 수도 있고 **Disaster Recovery** 모듈이 활성화된 새 보호 계획을 적용할 수도 있습니다.

수동 장애 복구

참고
지원 팀의 지시가 있을 때만 수동 모드의 장애 복구 프로세스를 사용하는 것이 좋습니다.

수동 모드에서 장애 복구 프로세스를 시작할 수도 있습니다. 이 경우에는 클라우드의 백업에서 로컬 사이트로 데이터가 자동 전송되지 않습니다. 즉, 클라우드의 가상 머신 전원이 꺼진 후 데이터를 수동으로 전송해야 합니다. 그러므로 수동 모드 장애 복구 프로세스는 속도가 훨씬 느리며 다운타임 시간도 더 길어집니다.

수동 모드 장애 복구 프로세스에서는 다음 단계를 수행합니다.

1. **계획**. 이 단계에서는 호스트, 네트워크 구성과 같은 로컬 사이트의 IT 인프라를 복원하고 장애 복구 매개변수를 구성한 다음 데이터 전송을 시작할 시기를 계획합니다.
2. **전환**. 이 단계에서는 클라우드의 가상 머신이 꺼지며 새로 생성된 데이터가 백업됩니다. 복구 서버에 백업 계획이 적용되어 있지 않으면 전환 단계에서 백업이 자동으로 수행되므로 프로세스 속도가 느려집니다. 백업이 완료되면 로컬 사이트에 머신을 수동으로 복구합니다. 부팅 가능한 미디어를 사용하여 디스크를 복구할 수도 있고 클라우드 백업 스토리지에서 전체 머신을 복구할 수도 있습니다.
3. **유효성 검사**. 이 단계에서는 로컬 사이트의 가상 머신이나 실제 머신이 정상 작동 중인지 확인하고 장애 복구를 확인합니다. 확인 후에는 클라우드 사이트의 가상 머신이 삭제되며 복구 서버가 **대기** 상태로 돌아갑니다.

수동 장애 복구 수행

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

© Acronis International GmbH, 2003-2024

로컬 사이트의 대상 실제 머신이나 가상 머신으로 수동 장애 복구를 수행할 수 있습니다.

수동 장애 복구를 수행하려면

1. Cyber Protect 콘솔에서 **재해 복구** > **서버**로 이동합니다.
2. **장애 조치** 상태에 있는 복구 서버를 선택합니다.
3. **장애 복구** 탭을 클릭합니다.
4. **대상** 필드에서 **실제 머신**을 선택합니다.
5. 기어 아이콘을 클릭하고 **수동 모드 사용** 스위치를 활성화합니다.
6. [선택 사항] **백업 크기** 값을 인터넷 속도 값으로 나누어 장애 복구 프로세스 중 예상 중단 시간을 계산합니다.

   참고
   여러 장애 복구 프로세스를 동시에 수행하면 인터넷 속도 값이 줄어듭니다.

7. **전환**을 클릭하고 확인 창에서 **전환**을 다시 클릭합니다.
   클라우드 사이트의 가상 머신이 꺼집니다.

   참고
   클라우드의 가상 머신에 백업 계획이 적용되어 있지 않으면 전환 단계에서 백업이 자동으로 수행되므로 다운타임이 길어집니다.

8. 클라우드 백업에서 로컬 사이트의 실제 머신이나 가상 머신으로 서버를 복구합니다. 자세한 내용은 Cyber Protection 사용자 안내서에서 "머신 복구"를 참조하십시오.
9. 복구가 완료되고 복구된 머신이 올바르게 작동하는지 확인한 후에 **머신이 복원되었습니다.**를 클릭합니다.
10. 모든 기능이 정상 작동하면 **장애 복구 확인**을 클릭하고 확인 창에서 **확인**을 다시 클릭합니다.
    복구 서버 및 복구 지점은 다음 장애 조치를 위해 준비됩니다. 새 복구 지점을 만들려면 새 로컬 서버에 보호 계획을 적용합니다.

    참고
    복구된 서버에서 보호 계획을 적용하는 것은 장애 복구 프로세스에 포함되지 않습니다. 장애 복구 프로세스가 완료된 후 복구된 서버에서 보호 계획을 적용하여 서버가 다시 보호되도록 하십시오. 원래 서버에 적용했던 것과 같은 보호 계획을 적용할 수도 있고 **Disaster Recovery** 모듈이 활성화된 새 보호 계획을 적용할 수도 있습니다.

암호화된 백업 관련 작업

암호화된 백업으로부터 복구 서버를 생성할 수 있습니다. 편의를 위해 복구 서버로의 장애 조치 중에 자동 비밀번호 애플리케이션을 암호화된 백업으로 설정하면 됩니다.

복구 서버를 생성할 때 자동 재해 복구 작업에 사용할 비밀번호를 지정할 수 있습니다. 이 비밀번호는 **설정** > **자격 증명** 섹션에서 찾을 수 있는 안전한 자격 증명 스토리지인 자격 증명 저장소에 저장됩니다.

자격 증명 하나를 여러 백업에 연결할 수 있습니다.

© Acronis International GmbH, 2003-2024

자격 증명 저장소에 저장된 비밀번호를 관리하려면

1. **설정** > **자격 증명**으로 이동합니다.
2. 특정 자격 증명을 관리하려면 마지막 열의 아이콘을 클릭합니다. 이 자격 증명에 연결된 항목을 볼 수 있습니다.
   - 선택한 자격 증명에서 백업을 링크 해제하려면 해당 백업 근처의 휴지통 아이콘을 클릭하십시오. 그러면 복구 서버로의 장애 조치 중에 비밀번호를 수동으로 지정해야 합니다.
   - 자격 증명을 편집하려면 **편집**을 클릭한 다음, 이름 또는 비밀번호를 지정합니다.
   - 자격 증명을 삭제하려면 **삭제**를 클릭합니다. 이 경우, 복구 서버로의 장애 조치 중에 비밀번호를 수동으로 지정해야 합니다.

Microsoft Azure 가상 머신 관련 작업

참고
일부 기능을 사용하려면 적용되는 라이센스 모델에 따라 추가 라이센스가 필요할 수 있습니다.

Acronis Cyber Protect Cloud로의 Microsoft Azure 가상 머신 장애 조치를 수행할 수 있습니다. 자세한 내용은 "장애 조치 수행"(716페이지)을(를) 참조하십시오.

그 후에는 Acronis Cyber Protect Cloud에서 Azure 가상 머신으로의 장애 복구를 수행할 수 있습니다. 장애 복구 프로세스는 실제 머신으로의 장애 복구 프로세스와 동일합니다. 자세한 내용은 "사전 요구 사항"(725페이지)을(를) 참조하십시오.

참고
장애 복구용으로 새 Azure 가상 머신을 등록하려는 경우 Azure에서 제공되는 Acronis 백업 VM 확장을 사용할 수 있습니다.

Acronis Cyber Protect Cloud와 Azure VPN 게이트웨이 간의 다중 사이트 IPsec VPN 연결을 구성할 수 있습니다. 자세한 내용은 "다중 사이트 IPsec VPN 구성"(686페이지)을(를) 참조하십시오.

기본 서버 설정

이 섹션에서는 기본 서버를 생성하고 관리하는 방법에 대해 설명합니다.

기본 서버 생성

사전 요구 사항

- 클라우드 사이트에 대한 연결 유형 하나를 설정해야 합니다.

기본 서버를 생성하려면:

1. **재해 복구** > **서버** > **기본 서버** 탭으로 이동합니다.
2. **생성**을 클릭합니다.
3. 새 가상 머신의 템플릿을 선택합니다.

© Acronis International GmbH, 2003-2024

4. 구성의 선호 방식(가상 코어 수와 RAM 크기)을 선택합니다. 각 선호 방식의 총 디스크 공간(GB) 최대값이 아래 표에 나와 있습니다.

유형	vCPU	RAM(GB)	총 디스크 공간(GB)의 최대값
F1	1	2	500
F2	1	4	1000
F3	2	8	2000
F4	4	16	4000
F5	8	32	8000
F6	16	64	16000
F7	16	128	32000
F8	16	256	64000

참고
모든 옵션의 컴퓨팅 포인트를 볼 수 있습니다. 컴퓨팅 포인트의 수는 기본 서버를 시간당 실행하는 비용을 반영합니다. 자세한 내용은 "컴퓨팅 포인트"(670페이지)을(를) 참조하십시오.

5. [선택 사항]가상 디스크 크기를 변경합니다. 두 개 이상의 하드 디스크가 필요한 경우 **디스크 추가**를 클릭한 다음 새 디스크 크기를 지정합니다. 현재는 기본 서버에 디스크를 10개보다 많이 추가할 수 없습니다.
6. 기본 서버를 포함할 클라우드 네트워크를 지정합니다.
7. **DHCP** 옵션을 선택합니다.

DHCP 옵션	설명
클라우드 사이트 제공	기본 설정. 서버의 IP 주소는 클라우드에 자동으로 구성된 DHCP 서버에서 제공합니다.
사용자 정의	서버의 IP 주소는 클라우드에 있는 자신의 DHCP 서버에서 제공합니다.

8. [선택 사항] **MAC 주소**를 지정합니다.
   MAC 주소는 서버의 네트워크 어댑터에 할당된 고유 식별자입니다. 사용자 DHCP를 사용하는 경우 특정 IP 주소를 항상 특정 MAC 주소에 할당하도록 DHCP를 구성할 수 있습니다. 이를 통해 기본 서버는 항상 동일한 IP 주소를 얻게 됩니다. MAC 주소로 등록된 라이센스가 있는 애플리케이션을 실행할 수 있습니다.
9. 서버가 운영 네트워크에서 가지는 IP 주소를 지정합니다. 기본적으로 운영 네트워크의 첫 번째 사용 가능한 IP 주소가 설정됩니다.

© Acronis International GmbH, 2003-2024

참고

DHCP 서버를 사용하는 경우 IP 주소 충돌을 피할 수 있도록 이 IP 주소를 서버 제외 목록에 추가하십시오.

사용자 지정 DHCP 서버를 사용하는 경우 **운영 네트워크의 IP 주소**에 DHCP 서버에 구성된 것과 동일한 IP 주소를 지정해야 합니다. 그렇지 않으면 테스트 장애 조치가 제대로 작동하지 않고 공용 IP 주소를 통해 서버에 연결할 수 없습니다.

10. [선택 사항] **인터넷 액세스** 확인란을 선택합니다.

    이렇게 하면 기본 서버가 인터넷에 액세스할 수 있습니다. 기본적으로 공용 IP 주소에 대한 아웃바운드 연결용으로는 TCP 포트 25가 열립니다.
11. [선택 사항] **공용 IP 주소 사용** 확인란을 선택합니다.

    공용 IP 주소를 사용하면 기본 서버를 인터넷에서 사용할 수 있습니다. 확인란을 선택하지 않은 상태로 두면 서버를 운영 네트워크에서만 사용할 수 있습니다.

    구성을 완료하면 공용 IP 주소가 표시됩니다. 기본적으로 공용 IP 주소에 대한 인바운드 연결용으로는 TCP 포트 443이 열립니다.

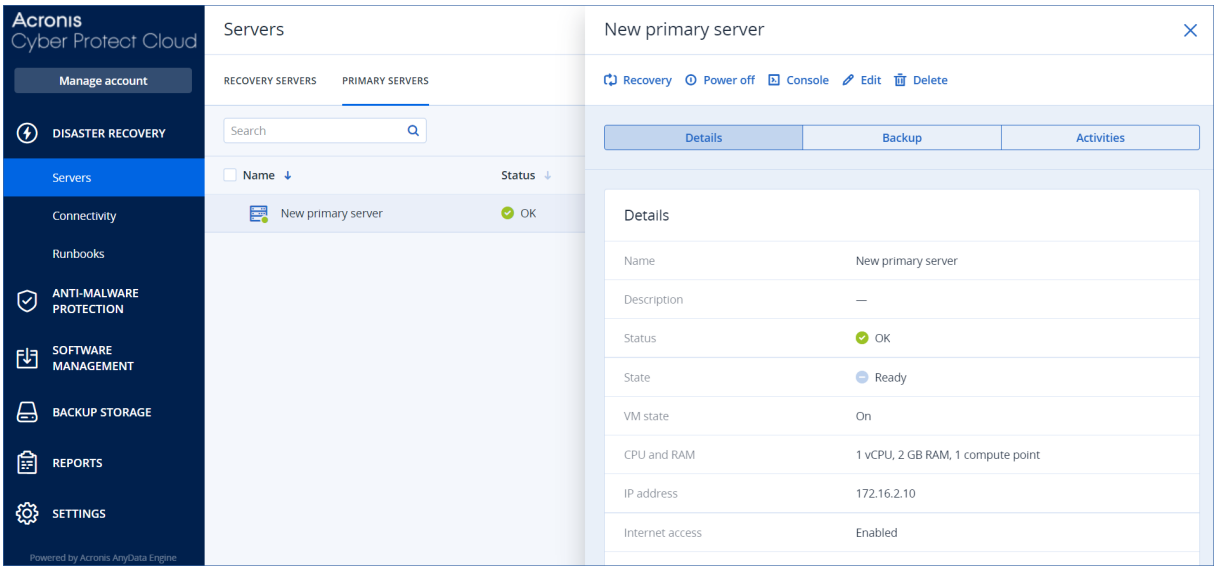
    참고

    공용 IP 주소 사용 확인란의 선택을 취소하거나 복구 서버를 삭제하면 해당 공용 IP 주소가 예약되지 않습니다.
12. [선택 사항] **RPO 임계값 설정**을 선택합니다.

    RPO 임계값은 마지막 복구 지점과 현재 시간 사이에 허용되는 최대 시간 간격을 정의합니다. 이 값은 15 – 60분, 1 – 24시간, 1 – 14일 내에서 설정할 수 있습니다.
13. 기본 서버 이름을 정의합니다.
14. [선택 사항] 기본 서버에 대한 설명을 지정합니다.
15. [선택 사항] **클라우드 방화벽 규칙** 탭을 클릭하여 기본 방화벽 규칙을 편집합니다. 자세한 내용은 "클라우드 서버용 방화벽 규칙 설정"(734페이지)을(를) 참조하십시오.
16. **생성**을 클릭합니다.

기본 서버를 운영 네트워크에서 사용할 수 있게 됩니다. 콘솔, RDP, SSH 또는 TeamViewer를 사용하여 서버를 관리할 수 있습니다.

© Acronis International GmbH, 2003-2024



기본 서버 관련 작업

기본 서버는 콘솔의 **재해 복구** > **서버** > **기본 서버** 탭에 표시됩니다.

서버를 시작 또는 중지하려면 기본 서버 패널에서 **켜기** 또는 **끄기**를 클릭합니다.

기본 서버 설정을 편집하려면 서버를 중지하고 **편집**을 클릭합니다.

보호 계획을 기본 서버에 적용하려면 선택한 다음 **계획** 탭에서 **생성**을 클릭합니다. 스케줄 및 보관 규칙만 변경할 수 있는 미리 정의된 보호 계획이 표시됩니다. 자세한 내용은 "클라우드 서버 백업"을 참조하십시오.

클라우드 서버 관리

클라우드 서버를 관리하려면 **재해 복구** > **서버**로 이동합니다. 다음과 같이 **복구 서버**와 **기본 서버**라는 2개 탭이 있습니다. 모든 선택 사항 열도 표로 표시하려면 기어 아이콘을 클릭하십시오.

선택하면 각 클라우드 서버에 대해 다음과 같은 정보를 확인할 수 있습니다.

열 이름	설명
이름	사용자가 정의한 클라우드 서버 이름
상태	클라우드 서버와 관련된 가장 심각한 문제를 반영하는 상태(활성 경보 기반)
상태	클라우드 서버 상태
VM 상태	클라우드 서버와 연결되어 있는 가상 머신의 전원 상태
활성화 위치	클라우드 서버가 호스팅되는 위치입니다. 예: **클라우드**
RPO 임계값	현재 시각과 장애 조치에 적합한 마지막 복구 지점 사이의 최대 시간. 그 값은 15-60분, 1-24시간, 1-14일 내로 설정할 수 있습니다.

© Acronis International GmbH, 2003-2024

RPO 규제 준수	RPO 규제 준수는 실제 RPO와 RPO 임계값 간 비율입니다. RPO 규제 준수는 RPO 임계값을 정의한 경우에 표시됩니다. 이는 다음과 같이 계산됩니다. **RPO 규제 준수 = 실제 RPO / RPO 임계값** 여기서, **실제 RPO = 현재 시간 – 마지막 복구 지점 시간** **RPO 규제 준수 상태** 실제 RPO와 RPO 임계값 간 비율의 값에 따라 다음 상태가 사용됩니다. • **규제 준수**. RPO 규제 준수 < 1배. 서버가 RPO 임계값을 준수합니다. • **초과**. RPO 규제 준수 <= 2배. 서버가 RPO 임계값을 위반합니다. • **심각한 초과**. RPO 규제 준수 <= 4배. 서버가 RPO 임계값을 2배 이상 위반합니다. • **치명적인 초과**. RPO 규제 준수 > 4배. 서버가 RPO 임계값을 4배 이상 위반합니다. • **보류 중(백업 없음)**. 보호 계획에 의해 서버가 보호되지만 백업이 생성되는 중이며 아직 완료되지 않았습니다.
실제 RPO	마지막 복구 지점 생성 이후 경과한 시간
마지막 복구 지점	마지막 복구 지점 생성 시 날짜 및 시간

클라우드 서버용 방화벽 규칙

클라우드 사이트에 있는 기본 서버와 복구 서버의 인바운드 트래픽 및 아웃바운드 트래픽을 제어하도록 방화벽 규칙을 구성할 수 있습니다.

클라우드 서버용 공용 IP 주소를 프로비저닝한 후에 인바운드 규칙을 구성할 수 있습니다. 기본적으로는 TCP 포트 443이 허용되며 기타 모든 인바운드 연결은 거부됩니다. 기본 방화벽 규칙을 변경할 수 있으며 인바운드 예외를 추가하거나 제거할 수 있습니다. 공용 IP를 프로비저닝하지 않으면 인바운드 규칙을 확인만 할 수 있으며 구성할 수는 없습니다.

클라우드 서버용 인터넷 액세스를 프로비저닝한 후 아웃바운드 규칙을 구성할 수 있습니다. 기본적으로 TCP 포트 25는 거부되며 기타 모든 아웃바운드 연결은 허용됩니다. 기본 방화벽 규칙을 변경할 수 있으며 아웃바운드 예외를 추가하거나 제거할 수 있습니다. 인터넷 액세스를 프로비저닝하지 않으면 아웃바운드 규칙을 확인만 할 수 있으며 구성할 수는 없습니다.

© Acronis International GmbH, 2003-2024

참고
보안상의 이유로, 변경할 수 없는 사전 정의된 방화벽 규칙이 있습니다.

인바운드 및 아웃바운드 연결용 옵션은 다음과 같습니다.

- Permit ping: ICMP echo-request(type 8, code 0) 및 ICMP echo-reply(type 0, code 0)
- Permit ICMP need-to-frag(type 3, code 4)
- Permit TTL exceeded(type 11, code 0)

인바운드 연결에만 적용되는 옵션은 다음과 같습니다.

- 구성 불가 부분: 모두 거부

아웃바운드 연결에만 적용되는 옵션은 다음과 같습니다.

- 구성 불가 부분: 모두 거부

클라우드 서버용 방화벽 규칙 설정

클라우드의 기본 서버 및 복구 서버용 기본 방화벽 규칙을 편집할 수 있습니다.

클라우드 사이트의 서버 방화벽 규칙을 편집하려면

1. Cyber Protect 콘솔에서 **재해 복구** > **서버**로 이동합니다.
2. 복구 서버의 방화벽 규칙을 편집하려면 **복구 서버** 탭을 클릭합니다. 기본 서버의 방화벽 규칙을 편집하려면 **기본 서버** 탭을 클릭합니다.
3. 서버를 클릭한 다음 **편집**을 클릭합니다.
4. **클라우드 방화벽 규칙** 탭을 클릭합니다.
5. 인바운드 연결의 기본 작업을 변경하려면:
   a. **인바운드** 드롭다운 필드에서 기본 작업을 선택합니다.

작업	설명
모두 거부	모든 인바운드 트래픽을 거부합니다. 예외를 추가하여 특정 IP 주소, 프로토콜 및 포트에서 전송되는 트래픽을 허용할 수 있습니다.
모두 허용	모든 인바운드 TCP 및 UDP 트래픽을 허용합니다. 예외를 추가하여 특정 IP 주소, 프로토콜 및 포트에서 전송되는 트래픽을 거부할 수 있습니다.

   참고
   기본 작업을 변경하면 기존 인바운드 규칙이 무효화되며 해당 구성이 제거됩니다.

   b. [선택 사항] 기존 예외를 저장하려면 확인 창에서 **작성된 예외 저장**을 선택합니다.
   c. **확인**을 클릭합니다.
6. 예외를 추가하려면:

© Acronis International GmbH, 2003-2024

a. **예외 추가**를 클릭합니다.

b. 방화벽 매개변수를 지정합니다.

방화벽 매개변수	설명
프로토콜	연결용 프로토콜을 선택합니다. 지원되는 옵션은 다음과 같습니다. • **TCP** • **UDP** • **TCP+UDP**
서버 포트	규칙이 적용되는 포트를 선택합니다. 다음 항목을 지정할 수 있습니다. • 특정 포트 번호(예: 2298) • 포트 번호 범위(예: 6000-6700) • 임의의 포트 번호 임의의 포트 번호에 규칙을 적용하려면 *를 사용합니다.
클라이언트 IP 주소	규칙이 적용되는 IP 주소를 선택합니다. 다음 항목을 지정할 수 있습니다. • 특정 IP 주소(예: 192.168.0.0) • CIDR 표기법을 사용하는 IP 주소 범위(예: 192.168.0.0/24) • 임의의 IP 주소 임의의 IP 주소에 규칙을 적용하려면 *를 사용합니다.

7. 기존 인바운드 예외를 제거하려면 해당 예외 옆의 휴지통 아이콘을 클릭합니다.

8. 아웃바운드 연결의 기본 작업을 변경하려면:

a. **아웃바운드** 드롭다운 필드에서 기본 작업을 선택합니다.

작업	설명
모두 거부	모든 아웃바운드 트래픽을 거부합니다. 예외를 추가하여 특정 IP 주소, 프로토콜 및 포트로 전송되는 트래픽을 허용할 수 있습니다.
모두 허용	모든 아웃바운드 트래픽을 허용합니다. 예외를 추가하여 특정 IP 주소, 프로토콜 및 포트에서 전송되는 트래픽을 거부할 수 있습니다.

참고
기본 작업을 변경하면 기존 아웃바운드 규칙이 무효화되며 해당 구성이 제거됩니다.

b. [선택 사항] 기존 예외를 저장하려면 확인 창에서 **작성된 예외 저장**을 선택합니다.

c. **확인**을 클릭합니다.

9. 예외를 추가하려면:

a. **예외 추가**를 클릭합니다.

b. 방화벽 매개변수를 지정합니다.

© Acronis International GmbH, 2003-2024

방화벽 매개변수	설명
프로토콜	연결용 프로토콜을 선택합니다. 지원되는 옵션은 다음과 같습니다. • **TCP** • **UDP** • **TCP+UDP**
서버 포트	규칙이 적용되는 포트를 선택합니다. 다음 항목을 지정할 수 있습니다. • 특정 포트 번호(예: 2298) • 포트 번호 범위(예: 6000-6700) • 임의의 포트 번호 임의의 포트 번호에 규칙을 적용하려면 *를 사용합니다.
클라이언트 IP 주소	규칙이 적용되는 IP 주소를 선택합니다. 다음 항목을 지정할 수 있습니다. • 특정 IP 주소(예: 192.168.0.0) • CIDR 표기법을 사용하는 IP 주소 범위(예: 192.168.0.0/24) • 임의의 IP 주소 임의의 IP 주소에 규칙을 적용하려면 *를 사용합니다.

10. 기존 아웃바운드 예외를 제거하려면 해당 예외 옆의 휴지통 아이콘을 클릭합니다.
11. **저장**을 클릭합니다.

클라우드 방화벽 활동 확인

클라우드 서버의 방화벽 규칙 구성을 업데이트하고 나면 Cyber Protect 콘솔에서 업데이트 활동 로그가 제공됩니다. 로그에서 확인할 수 있는 정보는 다음과 같습니다.

- 구성을 업데이트한 사용자의 사용자 이름
- 업데이트 날짜 및 시간
- 인바운드 및 아웃바운드 연결용 방화벽 설정
- 인바운드 및 아웃바운드 연결의 기본 작업
- 인바운드 및 아웃바운드 연결에 대한 예외의 프로토콜, 포트 및 IP 주소

클라우드 방화벽 규칙 구성 변경 관련 세부 정보를 확인하려면

1. Cyber Protect 콘솔에서 **모니터링** > **활동**을 클릭합니다.
2. 해당 활동을 클릭하고 **모든 속성**을 클릭합니다.
   활동 설명이 **클라우드 서버 구성 업데이트 중**이어야 합니다.
3. **컨텍스트** 필드에서 원하는 정보를 확인합니다.

© Acronis International GmbH, 2003-2024

클라우드 서버 백업

기본 및 복구 서버는 클라우드 사이트에서 에이전트를 사용하지 않고 백업됩니다. 이러한 백업에는 다음 제한이 적용됩니다.

- 유일하게 가능한 백업 위치는 클라우드 스토리지입니다. 기본 서버는 **기본 서버 백업** 스토리지에 백업됩니다.

  참고
  Microsoft Azure 백업 위치는 지원되지 않습니다.

- 백업 계획은 여러 서버에 적용될 수 없습니다. 모든 백업 계획의 설정이 동일하더라도 각 서버에서 자체 백업 계획을 갖고 있어야 합니다.
- 한 서버에 하나의 백업 계획만 적용할 수 있습니다.
- 애플리케이션 인식 백업은 지원되지 않습니다.
- 암호화를 사용할 수 없습니다.
- 백업 옵션은 사용할 수 없습니다.

기본 서버를 삭제할 경우 해당 백업도 삭제됩니다.

복구 서버는 장애 조치 상태에서만 백업됩니다. 백업은 원래 서버의 백업 순서를 계속합니다. 장애 복구가 수행되면 원래 서버는 이 백업 순서를 계속할 수 있습니다. 따라서 복구 서버의 백업은 수동으로 또는 보존 규칙을 적용한 결과로만 삭제할 수 있습니다. 복구 서버가 삭제되면 백업이 항상 유지됩니다.

참고
클라우드 서버용 백업 계획은 UTC 시간에 따라 수행됩니다.

조정(작동 실행서)

참고
일부 기능을 사용하려면 적용되는 라이센스 모델에 따라 추가 라이센스가 필요할 수 있습니다.

런북은 클라우드에서 프로덕션 환경을 어떻게 시작할지 설명하는 지침 세트입니다. Cyber Protect 콘솔에서 런북을 만들 수 있습니다. **런북** 화면에 액세스하려면 **재해 복구** > **런북**을 선택합니다.

실행서를 사용하는 이유는 무엇인가요?

런북을 사용하면 다음을 수행할 수 있습니다.

- 1대 이상의 서버에 대한 장애 조치를 자동화합니다.
- 서버 IP 주소를 핑하고 지정된 포트 연결을 점검하여 장애 조치 결과를 자동으로 점검합니다.
- 분산 애플리케이션을 실행하는 서버의 동작 순서를 설정합니다.

© Acronis International GmbH, 2003-2024

- 워크플로우에 수동 동작을 포함시킵니다.
- 테스트 모드에서 실행서를 실행하여 재해 복구 솔루션의 무결성을 확인합니다.

작동 실행서 생성

런북은 연속적으로 실행되는 단계로 구성됩니다. 단계는 동시에 시작하는 작업으로 구성됩니다.

아래 지침을 따르거나 비디오 자습서를 시청할 수 있습니다.

런북을 생성하는 방법

1. Cyber Protection 콘솔에서 **재해 복구** > **런북**으로 이동합니다.
2. **런북 생성**을 클릭합니다.
3. **단계 추가**를 클릭합니다.
4. **작업 추가**를 클릭한 다음 단계에 추가하려는 작업을 선택합니다.

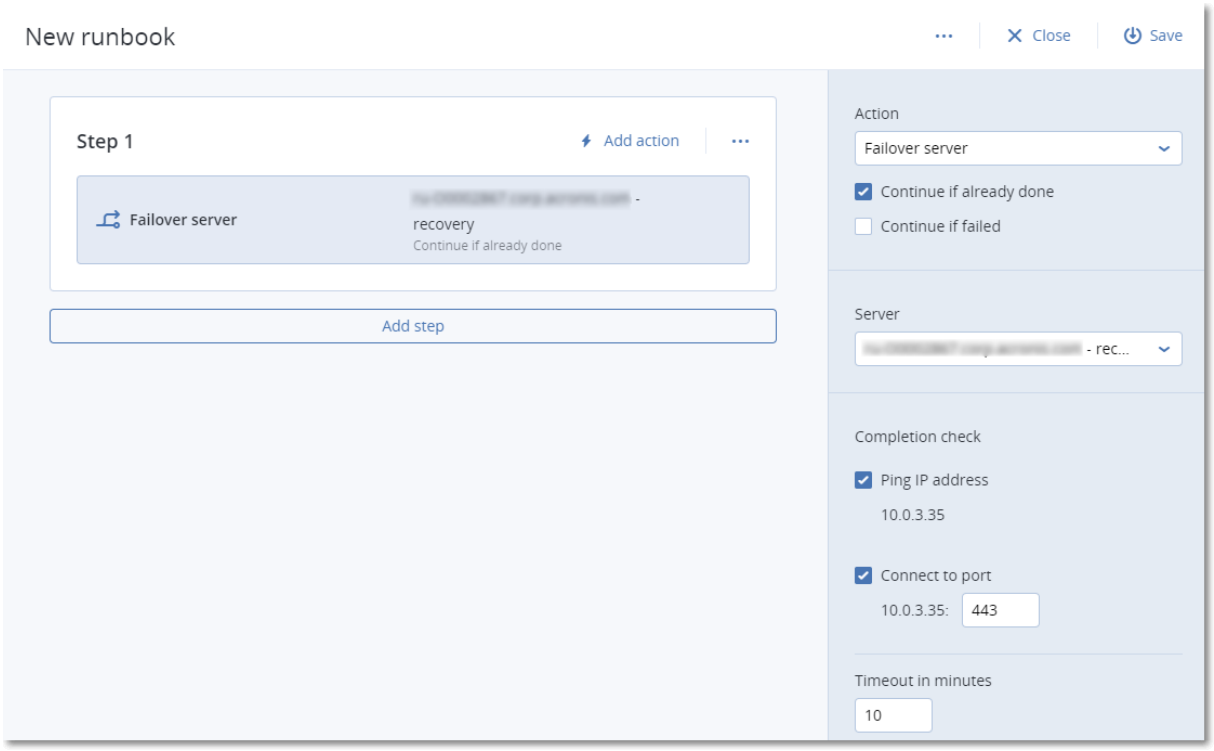
작업	설명
장애 조치 서버	클라우드 서버의 장애 조치를 수행합니다. 이 작업을 정의하려면 클라우드 서버를 선택하고 이 작업에 사용할 수 있는 런북 매개변수를 구성해야 합니다. 이 매개변수에 대한 자세한 정보는 "런북 매개변수"(740페이지)을(를) 참조하십시오. **참고** 선택한 서버의 백업이 머신 속성으로 암호화를 사용하여 암호화된 경우, **장애 조치 서버** 작업은 일시 정지되고 자동으로 **상호 작용 필요**로 변경됩니다. 런북의 실행을 계속하려면 암호화된 백업의 암호를 제공해야 합니다.
서버 장애 복구	클라우드 서버의 장애 복구를 수행합니다. 이 작업을 정의하려면 클라우드 서버를 선택하고 이 작업에 사용할 수 있는 런북 매개변수를 구성해야 합니다. 이러한 설정에 대한 자세한 정보는 "런북 매개변수"(740페이지)을(를) 참조하십시오. **참고** 런북 작업에서는 수동 모드의 장애 복구만 지원됩니다. 즉, **서버 장애 복구** 단계가 포함된 런북을 실행하여 장애 복구 프로세스를 시작하는 경우 장애 복구 절차에서 수동 상호 작용을 수행해야 합니다. 구체적으로는 머신을 수동으로 복구한 다음 **재해 복구** > **서버** 탭에서 장애 복구 프로세스를 확인하거나 취소해야 합니다.
서버 시작	클라우드 서버를 시작합니다. 이 작업을 정의하려면 클라우드 서버를 선택하고 이 작업에 사용할 수 있는 런북 매개변수를 구성해야 합니다. 이러한 설정에 대한 자세한 정보는 "런북 매개변수"(740페이지)을(를) 참조하십시오. **참고** **서버 시작** 작업은 런북에서의 테스트 장애 조치 작업에 적용할 수 없습니다. 이러한 작업을 실행하려고 하면 다음 오류 메시지와 함께 실패합니다. 실패: 이 작업은 현재 서버 상태에 적용할 수 없습니다.
서버 중지	클라우드 서버를 중지합니다. 이 작업을 정의하려면 클라우드 서버를 선택하고 이 작업에 사용할 수 있는 런북 매개변수를 구성해야 합니다. 이러한 설정에 대

© Acronis International GmbH, 2003-2024

작업	설명
	한 자세한 정보는 "런북 매개변수"(740페이지)을(를) 참조하십시오. **참고** **서버 중지** 작업은 런북에서의 테스트 장애 조치 작업에 적용할 수 없습니다. 이러한 작업을 실행하려고 하면 다음 오류 메시지와 함께 실패합니다. 실패: 이 작업은 현재 서버 상태에 적용할 수 없습니다.
수동 작업	수동 작업은 사용자의 상호 작용을 필요로 합니다. 이 작업을 정의하려면 설명을 입력해야 합니다. 런북 시퀀스가 수동 작업에 도달하면 런북은 일시 정지되며 사용자가 확인 버튼을 클릭하는 등의 필수 수동 작업을 수행하기 전까지 진행되지 않습니다.
런북 실행	다른 런북을 실행합니다. 이 작업을 정의하려면 런북을 선택해야 합니다. 작동 실행서에는 특정 실행성의 1회성 실행만 포함될 수 있습니다. 예를 들어, "작동 실행서 A 실행" 작업을 추가하였다면 "작동 실행서 B 실행" 작업을 추가할 수 있지만 다른 작업 "작동 실행서 A 실행"은 추가할 수 없습니다.

5. 작업에 대한 런북 매개변수를 정의하십시오. 이러한 매개변수에 대한 자세한 정보는 "런북 매개변수"(740페이지)을(를) 참조하십시오.
6. [선택 사항] 단계에 대한 설명 추가 방법
   a. 말줄임표 아이콘을 클릭한 다음 **설명**을 클릭합니다.
   b. 단계에 대한 설명을 입력합니다.
   c. **완료**를 클릭합니다.
7. 원하는 단계와 작업의 시퀀스를 만들 때까지 3-6단계를 반복합니다.
8. [선택 사항] 런북의 기본 이름을 변경하는 방법
   a. 말줄임표 아이콘을 클릭합니다.
   b. 런북의 이름을 입력합니다.
   c. 런북에 대한 설명을 입력합니다.
   d. **완료**를 클릭합니다.
9. **저장**을 클릭합니다.
10. **닫기**를 클릭합니다.

© Acronis International GmbH, 2003-2024



런북 매개변수

런북 매개변수는 런북 작업을 정의하기 위해 구성해야 하는 특정 설정입니다. 런북 매개변수에는 두 가지 카테고리가 있으며, 이는 작업 매개변수 및 무결성 검사 매개변수입니다.

작업 매개변수는 작업의 초기 상태 또는 결과에 따라 런북의 행동을 정의합니다.

무결성 검사 매개변수는 서버가 사용 가능하고 필요한 서비스를 제공하는지 확인합니다. 무결성 검사가 실패하면 해당 작업은 실패로 간주됩니다.

다음 표는 각 작업에 대한 구성 가능한 런북 매개변수를 설명합니다.

런북 매개변수	카테고리	작업 사용 가능	설명
이미 완료된 경우 계속 진행	작업 매개변수	• **장애 조치 서버** • **서버 시작** • **서버 중지** • **서버 장애 복구**	이 매개변수는 필요한 작업이 이미 완료된 경우(예: 장애 조치가 이미 수행되었거나 서버가 이미 실행 중인 경우) 런북의 행동을 정의합니다. 활성화되면 런북은 경고를 발행하고 계속 진행합니다. 비활성화되면 작업이 실패하고, 그런 다음 런북도 실패합니다. 기본적으로 이 매개변수는 활성화되어 있습니다.
실패한 경우 계속 진행	작업 매개변수	• **장애 조치 서버** • **서버 시작** • **서버 중지**	이 매개변수는 필요한 작업이 실패한 경우 런북의 행동을 정의합니다. 활성화되면 런북은 경고를 발행하고 계속 진행합니다. 비활성화되면 작업이 실패하고, 그런 다음 런북도 실패합니다.

© Acronis International GmbH, 2003-2024

런북 매개변수	카테고리	작업 사용 가능	설명
		• **서버 장애 복구**	기본적으로 이 매개변수는 비활성화되어 있습니다.
IP 주소 핑	무결성 검사	• **서버 시작**	소프트웨어는 서버가 응답하거나 타임아웃이 만료되는 것 중에서 먼저 해당하는 시간이 될 때까지 클라우드 서버의 생산 IP 주소를 핑합니다.
포트에 연결(기본값 443)	무결성 검사	• **서버 장애 조치** • **서버 시작**	소프트웨어는 연결이 확정되거나 타임아웃이 만료되는 것 중에서 먼저 해당하는 시간이 될 때까지 귀하가 지정하는 생산 IP 주소와 포트를 이용하여 클라우드 서버에 연결하기 위해 노력합니다. 이렇게 하면 지정 포트에서 수신하는 애플리케이션이 실행되는지 확인할 수 있습니다.
시간 초과(분)	무결성 검사	• **서버 장애 조치** • **서버 시작**	기본 타임아웃은 10분입니다.

작동 실행서 관련 작업

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

작업 목록에 액세스하려면 작동 실행서를 마우스로 가리키고 말줄임표 아이콘을 클릭합니다. 작동 실행서가 실행되지 않으면 다음 작업을 이용할 수 있습니다.

- **실행**
- **편집**
- **복제**
- **삭제**

작동 실행서의 실행

실행을 클릭할 때마다 실행 매개변수가 표시됩니다. 이 매개변수는 작동 실행서에 포함되는 장애 조치와 장애 복구 작업에 모두 적용됩니다. **작동 실행서 실행** 작업에 지정되는 작동 실행서는 주요 작동 실행서에서 이러한 매개변수를 상속합니다.

- **장애 조치 및 복구 모드**
  장애 조치 테스트(기본값)나 실제(생산) 장애 조치의 실행을 선택합니다. 장애 복구 모드는 선택한 장애 조치 모드에 해당합니다.
- **복구 지점 오류 해결**
  가장 최근의 복구 지점(기본값)을 선택하거나 과거 특정 시점을 선택합니다. 후자에 해당하는 경우, 지정 일시 이전에 가장 근접한 복구 지점은 각 서버별로 선택합니다.

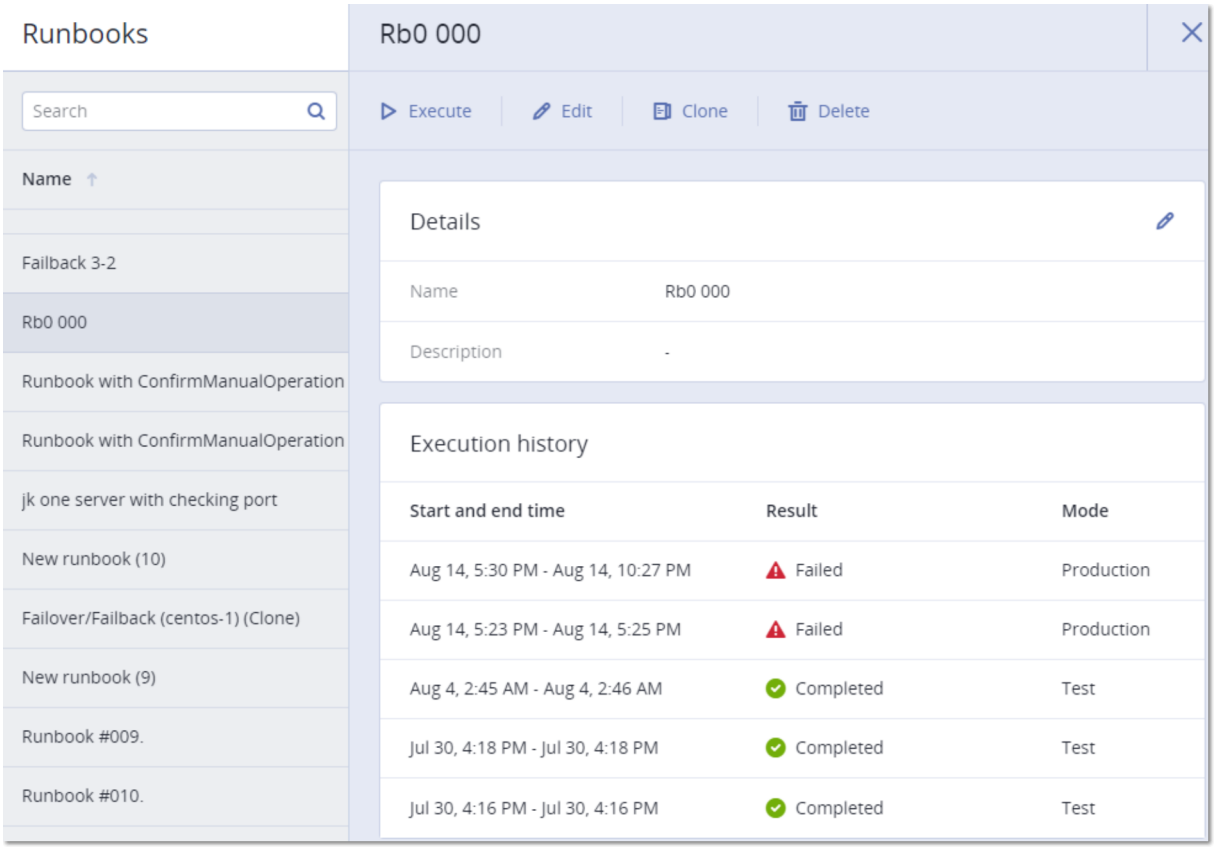
© Acronis International GmbH, 2003-2024

작동 실행서 실행 중지

작동 실행서를 실행하는 동안 작업 목록에서 **중지**를 선택할 수 있습니다. 소프트웨어는 사용자 상호 작용을 요구하는 작업을 제외하고 이미 시작된 작업을 모두 완료합니다.

실행 기록 보기

작동 실행서 탭에서 작동 실행서를 선택하면, 소프트웨어는 실행서 내용과 실행 기록을 표시합니다. 실행 로그를 보려면 특정 실행에 해당하는 라인을 클릭합니다.



© Acronis International GmbH, 2003-2024

안티바이러스 및 안티맬웨어 보호 구성

참고
Windows 머신에서는 맬웨어 방지 보호 기능을 사용하려면 맬웨어 방지 보호 에이전트를 설치해야 하며, URL 필터링 기능을 사용하려면 URL 필터링 에이전트를 설치해야 합니다. 보호 계획에서 **안티바이러스 및 맬웨어 방지 보호** 및/또는 **URL 필터링** 모듈이 활성화되어 있으면 이러한 에이전트가 보호 대상 워크로드에 자동 설치됩니다.

Cyber Protection의 맬웨어 방지 기능에는 다음과 같은 이점이 있습니다.

- 모든 스테이지에서 사전 예방적이고, 능동적이며, 대응적인 최고의 보호 성능을 발휘합니다.
- 내장된 4가지 맬웨어 방지 기술이 최고 수준의 다중 계층 보호를 제공합니다.
- Microsoft Security Essentials와 Microsoft Defender 바이러스 백신을 관리합니다.

  참고
  이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

중요
고급 안티맬웨어 옵션이 보호 계획 옵션에서 활성화되어 있는 경우에만 EICAR 테스트 파일이 감지됩니다. 그러나 EICAR 파일을 감지하지 않아도 Cyber Protection의 안티맬웨어 기능에는 영향을 미치지 않습니다.

지원되는 플랫폼

Active Protection, 안티바이러스 및 맬웨어 방지 기능은 다음 플랫폼에서 지원됩니다.

운영 체제	버전/배포판
Windows	Windows 7 서비스 팩 1 이상 버전 Windows Server 2008 R2 서비스 팩 1 이상 **참고** Windows 7에서는 보호 에이전트를 설치하기 전에 Microsoft의 다음 업데이트를 설치해야 합니다. • Windows 7 ESU(확장 보안 업데이트) • KB4474419 • KB4490628 필요한 업데이트에 대한 자세한 내용은 이 지식 베이스 문서를 참조하십시오.
Linux	Red Hat Linux 7.x, 8.x, 9.x CloudLinux 6.10, 7.x, 8.x CentOS 6.5 이상 6.x 버전, 7.x, 8.x

© Acronis International GmbH, 2003-2024

운영 체제	버전/배포판
	Ubuntu 16.04, 18.04, 20.04, 22.04, 22.10 Debian 8.x, 9.x, 10,x, 11.x Oracle Linux 7.x, 8.x, 9.x SUSE Enterprise Linux 15.x openSUSE Leap 15.x
macOS	macOS 10.13.x 이상

플랫폼별로 지원되는 기능

참고
Linux 및 macOS용 맬웨어 방지 보호 기능은 고급 안티맬웨어 팩에서 사용 가능합니다.

기능 세트	Windows	Linux	macOS
바이러스 백신 및 맬웨어 방지 기능			
완전 통합 Active Protection 기능	예	아니요	아니요
실시간 안티맬웨어 보호	예	예(고급 맬웨어 방지 팩 사용)	예(고급 맬웨어 방지 팩 사용)
로컬 서명 기반 감지 기능이 포함된 고급 실시간 안티맬웨어 보호	예	예	예
이식 가능 파일에 대한 고정 분석	예	아니요	예*
온디맨드 맬웨어 방지 스캔	예	예**	예
네트워크 폴더 보호	예	예	아니요
서버측 보호	예	아니요	아니요
아카이브 파일 스캔	예	아니요	예
이동식 드라이브 스캔	예	아니요	예
새로운 파일 및 변경된 파일만 스캔	예	아니요	예
파일/폴더 제외	예	예	예***
프로세스 제외	예	아니요	예
동작 분석 엔진	예	아니요	예

© Acronis International GmbH, 2003-2024

기능 세트	Windows	Linux	macOS
바이러스 백신 및 맬웨어 방지 기능			
악용 방지	예	아니요	아니요
격리	예	예	예
격리 자동 정리	예	예	예
URL 필터링(http/https)	예	아니요	아니요
기업 전반 허용 목록	예	아니요	예
방화벽 관리****	예	아니요	아니요
Microsoft Defender 안티바이러스 관리*****	예	아니요	아니요
Microsoft Security Essentials 관리	예	아니요	아니요
Windows 보안 센터를 통한 바이러스 백신 및 맬웨어 방지 기능 등록 및 관리	예	아니요	아니요
지원되는 운영 체제 및 해당 버전에 대한 자세한 내용은 "지원되는 플랫폼"(743페이지) 항목을 참조하십시오.			

* 이식 가능 파일에 대한 고정 분석은 macOS의 예약된 스캔에 대해서만 지원됩니다.

** Linux의 온디맨드 스캔에서는 시작 조건이 지원되지 않습니다.

*** 파일/폴더 제외는 macOS의 실시간 보호 또는 예약된 스캔에 의해 스캔되지 않을 파일 및 폴더를 지정할 때에만 지원됩니다.

**** 방화벽 관리는 Windows 8 이상에서 지원됩니다. Windows Server는 지원되지 않습니다.

***** Microsoft Defender 안티바이러스 관리는 Windows 8.1 이상에서 지원됩니다.

기능 세트	Windows	Linux	macOS
Active Protection			
프로세스 주입 감지	예	아니요	아니요
로컬 캐시에서 영향을 받는 파일 자동 복구	예	예	예
Acronis 백업 파일의 자체 보호	예	아니요	아니요
Acronis 소프트웨어 자체 보호	예	아니요	예 (Active Protection 및 안티맬웨어

© Acronis International GmbH, 2003-2024

기능 세트	Windows	Linux	macOS
Active Protection			
			컴퓨넌트만 해당)
신뢰할 수 있는/차단된 프로세스 관리	예	아니요	예
프로세스/폴더 제외	예	예	예
프로세스 동작 기반(AI 기반) 랜섬웨어 감지	예	예	예
프로세스 동작 기반 크립토마이닝 프로세스 감지됨	예	아니요	아니요
외장 드라이브 보호(HDD, 플래시 드라이브, SD 카드)	예	아니요	예
네트워크 폴더 보호	예	예	예
서버측 보호	예	아니요	아니요
Zoom, Cisco Webex, Citrix Workspace 및 Microsoft Teams 보호	예	아니요	아니요
지원되는 운영 체제 및 해당 버전에 대한 자세한 내용은 "지원되는 플랫폼"(743페이지) 항목을 참조하십시오.			

안티바이러스 및 안티맬웨어 보호 기능

참고
일부 기능을 사용하려면 적용되는 라이센스 모델에 따라 추가 라이센스가 필요할 수 있습니다.

안티바이러스 및 맬웨어 방지 모듈은 모든 최신 맬웨어 위협으로부터 Windows, Linux 및 macOS 머신을 보호합니다. 지원되는 안티맬웨어 기능의 전체 목록은 "지원되는 플랫폼"(743페이지) 항목을 참조하십시오.

안티바이러스 및 안티맬웨어 보호 기능은 Windows 보안 센터에서 지원 및 등록됩니다.

안티맬웨어 기능

- 실시간 보호 및 온디맨드 모드에서 파일의 맬웨어 감지
- 프로세스에서 악성 동작 감지(Windows)
- 악성 URL에 대한 액세스 차단(Windows)
- 위험 파일 격리
- 신뢰하는 기업 애플리케이션을 허용 목록에 추가

© Acronis International GmbH, 2003-2024

스캐닝 유형

안티바이러스 및 안티맬웨어 보호를 백그라운드에서 지속적으로 실행되거나 요청 시 실행되도록 구성할 수 있습니다.

실시간 보호

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

실시간 보호는 머신에서 실행되거나 열리는 모든 파일을 확인해 맬웨어 위협을 방지합니다.

잠재적인 호환성 및 성능 문제 방지를 위해, 실시간 보호 기능은 역시 실시간 보호 기능을 사용하는 다른 바이러스 백신 솔루션과 함께 사용할 수 없습니다. 설치되어 있는 다른 바이러스 백신 솔루션의 상태는 Windows 보안 센터를 통해 확인할 수 있습니다. Windows 머신을 이미 다른 바이러스 백신 솔루션으로 보호하고 있는 경우 실시간 보호 기능이 자동으로 꺼집니다.

실시간 보호 기능을 활성화하려면 다른 바이러스 백신 솔루션을 비활성화하거나 제거하십시오. 실시간 보호 기능은 Microsoft Defender 실시간 보호 기능을 자동으로 대체할 수 있습니다.

참고
Windows Server 운영 체제를 실행하는 머신의 경우 실시간 보호를 활성화해도 Microsoft Defender는 자동으로 꺼지지 않습니다. 그러므로 관리자가 잠재적인 호환성 문제를 방지하기 위해 Microsoft Defender를 수동으로 꺼야 합니다.

다음 스캔 모드 중 하나를 선택할 수 있습니다.

- **스마트 온액세스** 감지 기능은 안티맬웨어 프로그램이 백그라운드에서 실행되어 시스템이 켜져 있는 동안 내내 시스템을 능동적이고 지속적으로 스캔하여 바이러스 및 기타 악성 위협을 찾아냅니다. 맬웨어는 파일이 실행될 때는 물론, 파일을 읽거나 편집하기 위해 여는 것과 같은 다양한 작업 중에서도 감지됩니다.
- **온엑시큐션** 감지 기능은 실행 파일만을 대상으로 하는데, 그러한 파일이 실행되는 시점에 자동으로 스캔을 수행하여 문제가 없는지 머신 또는 데이터에 어떤 손상도 야기하지 않는지 확인합니다. 감염된 파일의 사본은 감지되지 않은 채 유지됩니다.

예약된 스캔

맬웨어 방지 스캔은 스케줄에 따라 수행됩니다.

다음 스캔 모드 중 하나를 선택할 수 있습니다.

- **빠른 스캔** - 워크로드 시스템 파일만 확인합니다.
- **전체 스캔** - 워크로드의 모든 파일을 확인합니다.
- **사용자 정의 스캔** - 관리자가 보호 계획에 추가한 파일/폴더를 확인합니다.

안티맬웨어 스캔이 완료된 후 **모니터링** > **개요** > 최근 영향 받은 항목 위젯에서 위협의 영향을 받는 워크로드에 대한 상세정보를 확인할 수 있습니다.

© Acronis International GmbH, 2003-2024

안티바이러스 및 맬웨어 방지 기능 설정

이 섹션에서는 보호 계획의 **안티바이러스 및 맬웨어 방지 보호** 모듈에서 구성할 수 있는 기능에 대해 설명합니다. 보호 계획 생성 방법을 알아보려면 "보호 계획 생성"(200페이지) 항목을 참조하십시오.

안티바이러스 및 맬웨어 방지 보호 모듈에서 보호 계획용으로 다음 기능을 구성할 수 있습니다.

- "Active Protection"(748페이지)
- "고급 안티맬웨어"(749페이지)
- "네트워크 폴더 보호"(749페이지)
- "서버측 보호"(750페이지)
- "자체 보호"(751페이지)
- "크립토마이닝 프로세스 감지됨"(752페이지)
- "격리"(752페이지)
- "동작 엔진"(752페이지)
- "악용 방지"(753페이지)
- "실시간 보호"(755페이지)
- "스캔 예약"(756페이지)
- "보호 제외"(759페이지)

참고
안티바이러스 및 맬웨어 방지 보호 기능을 지원하지 않는 운영 체제도 있습니다. 지원되는 운영 체제와 기능에 대한 자세한 내용은 "지원되는 플랫폼"(743페이지) 항목을 참조하십시오. 라이선스가 있어야 보호 계획에서 사용 가능한 기능도 있습니다.

Active Protection

Active Protection은 파일을 암호화한 후 암호화 키 제공의 대가로 금전을 요구하는 랜섬웨어라는 악성 소프트웨어로부터 시스템을 보호합니다.

기본 설정: **활성화됨**.

참고
보호 에이전트가 보호되는 머신에 설치되어 있어야 합니다. 지원되는 운영 체제 및 기능에 대한 자세한 내용은 "지원되는 플랫폼"(743페이지) 항목을 참조하십시오.

Active Protection을 구성하려면

1. **보호 계획 생성** 창에서 **안티바이러스 및 맬웨어 방지 보호** 모듈을 확장합니다.
2. **Active Protection**을 클릭합니다.
3. **감지에 대한 작업** 섹션에서 사용 가능한 옵션 중 하나를 선택합니다.
   기본 설정: **캐시를 사용해 되돌림**

© Acronis International GmbH, 2003-2024

- **알리기만 함** - 소프트웨어에서 랜섬웨어 활동이 의심되는 프로세스에 대해 경보를 생성합니다.
- **프로세스 중지** - 소프트웨어에서 경보를 생성하고 랜섬웨어 활동이 의심되는 프로세스를 중지합니다.
- **캐시를 사용해 되돌림** - 소프트웨어에서 경보를 생성하고 프로세스를 중지한 후 서비스 캐시를 사용하여 파일 변경 사항을 되돌립니다.

4. **완료**를 클릭하여 선택한 옵션을 보호 계획에 적용합니다.

고급 안티맬웨어

이 엔진은 향상된 바이러스 서명 데이터베이스를 사용하여 빠른 스캔과 전체 스캔에서 모두 맬웨어 방지 감지 효율성을 높입니다.

중요
Advanced Security 보호 팩을 활성화해야 이 기능을 사용할 수 있습니다. 자세한 내용은 https://www.acronis.com/en-us/products/cloud/cyber-protect/security/를 참조하십시오

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

고급 맬웨어 방지를 구성하려면

1. **보호 계획 생성** 창에서 **안티바이러스 및 맬웨어 방지 보호** 모듈을 확장합니다.
2. **고급 안티맬웨어** 섹션에서 토글을 사용하여 서명 기반 로컬 엔진을 활성화합니다.

참고
macOS 및 Linux용 안티바이러스 및 안티맬웨어 보호에서도 로컬 서명 기반 엔진이 필요합니다. Windows의 경우에는 이 엔진의 유무에 관계없이 안티바이러스 및 안티맬웨어 보호를 사용할 수 있습니다.

네트워크 폴더 보호

네트워크 폴더 보호 기능은 안티바이러스 및 맬웨어 방지 보호 기능이 로컬 드라이브로 매핑된 네트워크 폴더를 보호하는지 여부를 정의합니다. 이 방지 기능은 SMB나 NFS 프로토콜을 통해 공유된 폴더에 적용됩니다.

네트워크 폴더 보호를 구성하려면

1. **보호 계획 생성** 창에서 **안티바이러스 및 맬웨어 방지 보호** 모듈을 확장합니다.
2. **네트워크 폴더 보호**를 클릭합니다.
3. 네트워크 폴더를 백업할 파일을 추가합니다.
   - 예를 들어 Windows 워크로드의 경우 네트워크 폴더를 백업할 Windows 파일의 경로를 **Windows** 필드에 입력합니다. 기본값: C:\ProgramData\Acronis\Restored Network Files.
   - 예를 들어 macOS 워크로드의 경우 네트워크 폴더를 백업할 macOS 파일의 경로를 **macOS** 필드에 입력합니다. 기본값: /Library/Application Support/Acronis/Restored Network Files/.

© Acronis International GmbH, 2003-2024

참고
로컬 폴더의 경로를 입력합니다. 매핑된 드라이브의 폴더를 비롯한 네트워크 폴더는 네트워크 폴더용 백업 목적지로 지원되지 않습니다.

4. **완료**를 클릭하여 선택한 옵션을 보호 계획에 적용합니다.

서버측 보호

이 기능을 사용하면 위협을 야기할 가능성이 있는 네트워크의 다른 서버에서 들어오는 외부 연결을 통해 공유한 네트워크 폴더를 Active Protection이 보호하는지 여부를 정의할 수 있습니다.

기본 설정: **끄기**.

참고
Linux에서는 서버 측 보호가 지원되지 않습니다.

신뢰할 수 있는 연결을 설정하려면

1. **보호 계획 생성** 창에서 **안티바이러스 및 맬웨어 방지 보호** 모듈을 확장합니다.
2. **서버 측 보호**를 클릭합니다.
3. **서버측 보호** 토글을 사용하여 서버측 보호를 활성화합니다.
4. **신뢰함** 탭을 선택합니다.
5. **신뢰할 수 있는 연결** 필드에서 **추가**를 클릭하여 데이터를 수정할 수 있는 연결을 정의합니다.
6. **컴퓨터 이름/계정** 필드에 보호 에이전트가 설치된 머신의 컴퓨터 이름과 계정을 입력합니다. 예를 들어 `MyComputer\TestUser`와 같이 입력합니다.
7. **호스트 이름** 필드에 보호 에이전트를 사용하여 머신에 연결할 수 있는 머신의 호스트 이름을 입력합니다.
8. 연결 정의를 저장하려면 우측의 확인 표시를 클릭합니다.
9. **완료**를 클릭합니다.

차단된 연결을 설정하려면

1. **보호 계획 생성** 창에서 **안티바이러스 및 맬웨어 방지 보호** 모듈을 확장합니다.
2. **서버 측 보호**를 클릭합니다.
3. **서버측 보호** 토글을 사용하여 서버측 보호를 활성화합니다.
4. **차단됨** 탭을 선택합니다.
5. **차단된 연결** 필드에서 **추가**를 클릭하여 데이터를 수정할 수 없는 연결을 정의합니다.
6. **컴퓨터 이름/계정** 필드에 보호 에이전트가 설치된 머신의 컴퓨터 이름과 계정을 입력합니다. 예를 들어 `MyComputer\TestUser`와 같이 입력합니다.
7. **호스트 이름** 필드에 보호 에이전트를 사용하여 머신에 연결할 수 있는 머신의 호스트 이름을 입력합니다.
8. 오른쪽 확인란을 선택하여 연결 정의를 저장합니다.
9. **완료**를 클릭합니다.

© Acronis International GmbH, 2003-2024

자체 보호

자체 보호는 로컬 폴더에 있는 소프트웨어 고유 프로세스, 레지스트리 기록, 실행 파일과 구성 파일 및 백업의 무단 변경을 방지합니다.

관리자는 **Active Protection**을 활성화하지 않고도 **자체 보호**를 활성화할 수 있습니다.

기본 설정: **켜기**입니다.

참고
Linux에서는 자체 보호가 지원되지 않습니다.

자체 보호를 활성화하려면

1. **보호 계획 생성** 창에서 **안티바이러스 및 맬웨어 방지 보호** 모듈을 확장합니다.
2. **자체 보호**를 클릭합니다.
3. **자체 보호** 토글을 사용하여 자체 보호를 활성화합니다.

패스워드 보호를 활성화하려면

1. **자체 보호** 기능을 활성화한 후에는 토글을 사용하여 **암호 보호** 기능을 활성화할 수 있습니다.
2. **새 암호 생성**을 클릭하여 로컬 에이전트 수정 또는 삭제용 암호를 생성합니다.
3. **복사**를 클릭한 후 암호를 안전한 위치에 붙여넣습니다. 컴포넌트 목록을 로컬에서 수정할 때 암호를 입력하라는 메시지가 표시되기 때문입니다.

   중요
   창을 닫은 후에는 암호를 사용할 수 없습니다. 이 패스워드를 장치에 적용하려면 보호 계획 설정을 저장해야 합니다.

4. **닫기**를 클릭합니다.

암호 보호는 권한이 없는 사용자나 소프트웨어가 Agent for Windows를 설치 제거하거나 해당 컴포넌트를 변경하는 것을 방지합니다. 이 작업은 관리자가 제공하는 패스워드로만 가능합니다.

다음 작업에는 비밀번호가 필요하지 않습니다:

- 설정 프로그램을 로컬에서 실행하여 설치를 업데이트
- Cyber Protect 콘솔을 사용하여 설치 업데이트
- 설치를 복구

기본 설정: **비활성화됨**

암호 보호를 활성화하는 방법에 대한 자세한 내용은 에이전트 무단 설치 제거 또는 수정 방지를 참조하십시오.

© Acronis International GmbH, 2003-2024

크립토마이닝 프로세스 감지됨

크립토마이닝 맬웨어에 감염되면 유용한 애플리케이션의 성능이 저하되고 전기세가 증가하며, 시스템이 남용되어 작동이 중단되거나 하드웨어가 손상될 수도 있습니다. **크립토마이닝 프로세스 감지됨** 기능은 컴퓨터 리소스의 승인되지 않은 사용을 방지하기 위해 크립토마이닝 맬웨어로부터 장치를 보호합니다.

관리자는 **Active Protection**을 활성화하지 않고도 **크립토마이닝 프로세스 감지됨**를 활성화할 수 있습니다. 기본 설정: **활성화됨**.

참고
Linux에서는 크립토마이닝 프로세스 감지가 지원되지 않습니다.

네트워크 폴더 보호를 구성하려면

1. **보호 계획 생성** 창에서 **안티바이러스 및 맬웨어 방지 보호** 모듈을 확장합니다.
2. **크립토마이닝 프로세스 감지됨**를 클릭합니다.
3. **크립토마이닝 프로세스 감지됨** 토글을 사용하여 기능을 활성화하거나 비활성화합니다.
4. 크립토마이닝 활동이 의심되는 프로세스 감지 시에 수행할 작업을 선택합니다.
   기본 설정: **프로세스 중지**
   - **알리기만 함** - 소프트웨어에서 경보를 생성합니다.
   - **프로세스 중지** - 소프트웨어에서 경보를 생성하고 프로세스를 중지합니다.
5. **완료**를 클릭하여 선택한 옵션을 보호 계획에 적용합니다.

격리

격리는 감염 가능성이 있는 의심스러운 파일 또는 위험할 수도 있는 파일을 격리하는 데 사용되는 폴더입니다.

격리를 구성하려면

1. **보호 계획 생성** 창에서 **안티바이러스 및 맬웨어 방지 보호** 모듈을 확장합니다.
2. **격리**를 클릭합니다.
3. **다음 후에 격리된 파일을 제거** 필드에서 격리된 파일을 제거하기 전까지 보관할 기간(일)을 정의할 수 있습니다.
   기본 설정: **30일**
4. **완료**를 클릭합니다.

이 보호에 대한 자세한 내용은 격리를 참조하십시오.

동작 엔진

동작 엔진 기능은 동작 추정을 사용해 악성 프로세스를 파악하여 맬웨어로부터 시스템을 보호합니다.

© Acronis International GmbH, 2003-2024

기본 설정: **활성화됨**.

참고
동작 엔진은 Linux에서 지원되지 않습니다.

네트워크 폴더 보호를 구성하려면

1. **보호 계획 생성** 창에서 **안티바이러스 및 맬웨어 방지 보호** 모듈을 확장합니다.
2. **동작 엔진**을 클릭합니다.
3. **동작 엔진** 토글을 사용하여 기능을 활성화하거나 비활성화합니다.
4. **감지에 대한 작업** 섹션에서 맬웨어 활동이 감지되었을 때 소프트웨어에서 수행할 작업을 선택합니다.
   기본 설정: **격리**
   - **알리기만 함** - 소프트웨어에서 맬웨어 활동이 의심되는 프로세스에 대해 경보를 생성합니다.
   - **프로세스 중지** - 소프트웨어에서 경보를 생성하고 맬웨어 활동이 의심되는 프로세스를 중지합니다.
   - **격리** - 소프트웨어에서 경보를 생성하고 프로세스를 중지한 후 실행 파일을 격리 폴더로 이동합니다.
5. **완료**를 클릭하여 선택한 옵션을 보호 계획에 적용합니다.

악용 방지

중요
Advanced Security 보호 팩을 활성화해야 이 기능을 사용할 수 있습니다. 자세한 내용은 https://www.acronis.com/en-us/products/cloud/cyber-protect/security/를 참조하십시오

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

익스플로잇 방지 기능은 시스템의 소프트웨어 취약성을 퍼뜨리고 악용하는 감염된 악성 프로세스를 감지하고 방지합니다. 악용이 감지되면 소프트웨어가 악용 활동이 의심되는 프로세스에 대해 경보를 생성하고 프로세스를 중지합니다.

악용 방지 기능은 에이전트 버전 12.5.23130(21.08, 2020년 8월에 릴리스됨) 이상에서만 사용할 수 있습니다.

기본 설정: 새로 생성된 보호 계획에 대해서는 **활성화됨**이고, 이전 에이전트 버전에서 생성된 기존 보호 계획에 대해서는 **비활성화됨**입니다.

참고
Linux에서는 악용 방지가 지원되지 않습니다.

악용이 감지되었을 때 프로그램의 대응 방식과 프로그램에서 적용할 악용 방지 방법을 선택할 수 있습니다.

© Acronis International GmbH, 2003-2024

익스플로잇 방지를 구성하려면

1. **보호 계획 생성** 창에서 **안티바이러스 및 맬웨어 방지 보호** 모듈을 확장합니다.
2. **익스플로잇 방지**를 클릭합니다.
3. **감지에 대한 작업** 섹션에서 사용 가능한 옵션 중 하나를 선택합니다.
   기본 설정: **프로세스 중지**

   - **알리기만 함**
     소프트웨어에서 익스플로잇 활동이 의심되는 프로세스에 대해 경보를 생성합니다.
   - **프로세스 중지**
     소프트웨어에서 익스플로잇 활동이 의심되는 프로세스에 대해 경보를 생성하고 프로세스를 중지합니다.
4. **활성화된 익스플로잇 방지 기술** 섹션에서 제공되는 옵션 중 적용하려는 옵션을 선택합니다.
   기본 설정: **모든 방식이 활성화됨**

   - **메모리 보호**
     메모리 페이지에 대한 의심스러운 실행 권한 수정을 감지하고 방지합니다. 악의적인 프로세스는 스택, 힙과 같이 실행할 수 없는 메모리 영역에서 셸 코드 실행을 활성화하기 위해 페이지 속성에 이러한 수정을 적용합니다.
   - **반환 지향 프로그래밍(ROP) 보호**
     ROP 악용 기술 사용 시도를 감지 및 방지합니다.
   - **권한 확장 보호**
     무단 코드 또는 애플리케이션에 의한 권한 확장 시도를 감지하고 방지합니다. 권한 확장은 악성 코드가 공격당한 머신에 대한 전체 액세스 권한을 얻은 후 중요하고 민감한 작업을 수행하려고 할 때 사용됩니다. 무단 코드는 중요한 시스템 리소스에 액세스하거나 시스템 설정을 수정할 수 없습니다.
   - **코드 주입 보호**
     원격 프로세스로의 악성 코드 주입을 감지하고 방지합니다. 코드 주입은 안티맬웨어 제품에 의한 감지를 피하기 위해 애플리케이션의 악의적인 의도를 깨끗한 프로세스 또는 양성 프로세스 뒤로 숨기는 데 사용됩니다.
5. **완료**를 클릭하여 선택한 옵션을 보호 계획에 적용합니다.

참고
제외 목록에서 신뢰할 수 있는 프로세스로 나열된 프로세스는 악용 감지를 위한 스캔 대상에서 제외됩니다.

프로세스가 백업을 수정할 수 있도록 허용

특정 프로세스가 백업을 수정할 수 있도록 허용 설정은 **자체 보호**가 활성화되어 있을 때만 사용 가능합니다.

확장자가 .tibx, .tib, .tia이고 로컬 폴더에 위치한 파일에 적용됩니다.

이 설정을 이용하면 백업 파일이 자체 보호로 보호되더라도 백업 파일을 수정할 수 있습니다. 예를 들면 이 옵션은 스크립트를 사용하여 백업 파일을 제거하거나 다른 위치로 이동할 때 유용합니다.

© Acronis International GmbH, 2003-2024

이 설정을 비활성화할 경우, 백업 파일은 백업 소프트웨어 벤더가 서명하는 프로세스로만 수정할 수 있습니다. 이 상태에서 소프트웨어는 사용자가 웹 인터페이스에서 이를 요청할 때 보관 규칙을 적용하고 백업을 삭제할 수 있습니다. 다른 프로세스는 아무리 의심스러워도 백업을 수정할 수 없습니다.

이 설정을 활성화할 경우, 다른 프로세스에 백업을 수정하도록 허용할 수 있습니다. 드라이브 문자로 시작하는 프로세스 실행 파일의 전체 경로를 지정합니다.

기본 설정: **비활성화됨**.

실시간 보호

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

실시간 보호는 컴퓨터 사용자가 일시적으로 정지하지 않는 한 시스템이 켜져 있는 동안에 지속적으로 컴퓨터 시스템의 바이러스 및 기타 악성 위협을 검사합니다.

기본 설정: **활성화됨**.

중요
Advanced Security 보호 팩을 활성화해야 이 기능을 사용할 수 있습니다. 자세한 내용은 https://www.acronis.com/en-us/products/cloud/cyber-protect/security/를 참조하십시오

실시간 보호를 구성하려면

1. **보호 계획 생성** 창에서 **안티바이러스 및 맬웨어 방지 보호** 모듈을 확장합니다.
2. **실시간 보호**를 클릭합니다.
3. **감지에 대한 작업** 드롭다운에서 사용 가능한 옵션 중 하나를 선택합니다.
   기본 설정: **격리**
   - **알리기만 함**
     소프트웨어는 랜섬웨어 활동을 의심하는 프로세스에 대한 경보를 생성합니다.
   - **차단 및 알림**
     소프트웨어가 맬웨어 활동이 의심되는 프로세스를 차단하고 경보를 생성합니다.
   - **격리**
4. 소프트웨어가 경보를 생성하고, 프로세스를 중지하고, 실행 파일을 격리 폴더로 이동합니다.
5. **스캔 모드** 섹션에서 바이러스나 기타 악성 위협이 감지되었을 때 소프트웨어에서 수행할 작업을 선택합니다.
   기본 설정: **스마트 온액세스**
   - **스마트 온액세스** – 모든 시스템 활동을 모니터링하면서 읽기 또는 쓰기를 위한 액세스가 발생할 경우 또는 프로그램이 실행될 경우 자동으로 파일을 스캔합니다.
   - **온엑시큐션** – 실행 파일만 시작 시 자동으로 스캔하여 파일에 문제가 없으며 컴퓨터 또는 데

© Acronis International GmbH, 2003-2024

이터에 손상을 야기하지 않는지 확인합니다.

6. **완료**를 클릭합니다.

스캔 예약

온디맨드 스캔은 지정된 스케줄에 따라 컴퓨터 시스템의 바이러스를 검사합니다. 전체 스캔은 머신의 모든 파일을 확인하고 빠른 스캔은 머신 시스템 파일만 확인합니다.

스캔 예약을 구성하려면

기본 설정:

- **사용자 정의 스캔**은 비활성화됩니다.
- **빠른 스캔 전체** 스캔이 예약됩니다.

1. **보호 계획 생성** 창에서 **안티바이러스 및 맬웨어 방지 보호** 모듈을 확장합니다.
2. **스캔 예약**을 클릭합니다.
3. 토글을 사용하여 머신에 적용할 스캔 유형을 활성화합니다.

사용 가능한 스캔 유형:

- **전체 스캔** - 모든 파일을 확인하므로 빠른 스캔에 비해 완료되기까지 훨씬 많은 시간이 걸립니다.
- **빠른 스캔** - 일반적으로 머신에 맬웨어가 위치하는 영역만 스캔합니다.
- **사용자 정의 스캔** - 보호 계획 관리자가 선택한 파일/폴더를 확인합니다.

> **참고**
> 보호 계획 하나에서 **빠른 스캔**, **전체 스캔**, **사용자 정의 스캔**의 세 가지 스캔을 모두 예약할 수 있습니다.

사용자 정의 스캔을 구성하려면

- **사용자 정의 스캔 토글**을 사용하여 이 스캔 유형을 활성화하거나 비활성화합니다.
- **감지에 대한 작업** 드롭다운 목록에서 사용 가능한 옵션 중 하나를 선택합니다.

기본 설정: **격리**

격리

소프트웨어가 경보를 생성하고 실행 파일을 격리 폴더로 이동합니다.

알리기만 함

소프트웨어가 맬웨어가 의심되는 프로세스에 대해 경보를 생성합니다.

필드	설명
다음 이벤트를 사용해 작업 실행 예약	작업을 실행할 시간을 정의하는 설정입니다. 다음 값을 선택할 수 있습니다. • **시간 기준 예약** - 기본 설정입니다. 지정한 시간에 따라 작업을 실행합니다.

© Acronis International GmbH, 2003-2024

필드	설명
	• **사용자가 시스템에 로그인할 때** – 기본적으로 사용자가 로그인하면 작업이 트리거됩니다. 특정 사용자 계정만 작업을 트리거할 수 있도록 이 설정을 수정할 수 있습니다. • **사용자가 시스템에서 로그오프할 때** – 기본적으로 사용자가 로그오프하면 작업이 트리거됩니다. 특정 사용자 계정만 작업을 트리거할 수 있도록 이 설정을 수정할 수 있습니다. **참고** 작업은 시스템 종료 시 실행되지 않습니다. 일정 예약 구성에서 시스템 종료와 로그오프는 다른 작업입니다. • **시스템 시작 시** – 운영 체제가 시작될 때 작업을 실행합니다. • **시스템 종료 시** – 운영 체제가 종료될 때 작업을 실행합니다.
예약 유형	**다음 이벤트를 사용해 작업 실행 예약**에서 **시간 기준 예약**을 선택한 경우 이 필드가 표시됩니다. 다음 값을 선택할 수 있습니다. • **월간** – 작업을 실행할 월과 주 또는 일을 선택합니다. • **일일** - 기본 설정입니다. 작업을 실행할 요일을 선택합니다. • **매시간** – 작업을 실행할 요일, 반복 횟수, 시간 간격을 선택합니다.
시작 시간	**다음 이벤트를 사용해 작업 실행 예약**에서 **시간 기준 예약**을 선택한 경우 이 필드가 표시됩니다 작업을 실행할 정확한 시간을 선택합니다.
날짜 범위 내에서 실행	**다음 이벤트를 사용해 작업 실행 예약**에서 **시간 기준 예약**을 선택한 경우 이 필드가 표시됩니다. 구성된 스케줄이 실행될 기간의 범위를 설정합니다.
운영 체제에 로그인할 때 작업을 시작하게 할 사용자 계정 지정	**다음 이벤트를 사용해 작업 실행 예약**에서 **사용자가 시스템에 로그인할 때**를 선택한 경우 이 필드가 표시됩니다. 다음 값을 선택할 수 있습니다. • **모든 사용자** - 어떤 사용자가 로그인하든 작업이 트리거되도록 하려는 경우 이 옵션을 사용합니다. • **다음 사용자** - 특정 사용자 계정의 로그인 시에만 작업이 트리거되도록 하려는 경우 이 옵션을 사용합니다.
운영 체제에서 로그아웃할 때 작업을 시작하게 할 사용자 계정 지정	**다음 이벤트를 사용해 작업 실행 예약**에서 **사용자가 시스템에서 로그오프할 때**를 선택한 경우 이 필드가 표시됩니다. 다음 값을 선택할 수 있습니다. • **모든 사용자** - 어떤 사용자가 로그아웃하든 작업이 트리거되도록 하려는 경우 이 옵션을 사용합니다. • **다음 사용자** - 특정 사용자 계정의 로그아웃 시에만 작업이 트리거되도록

© Acronis International GmbH, 2003-2024

필드	설명
	하려는 경우 이 옵션을 사용합니다.
시작 조건	작업을 시작하기 위해 동시에 충족되어야 하는 모든 조건을 정의합니다. 맬웨어 방지 스캔용 시작 조건은 "시작 조건"에 설명되어 있는 **백업 모듈**용 시작 조건과 유사합니다. 다음과 같이 추가적인 시작 조건을 정의할 수 있습니다. • **기간 내에서 작업 시작 시간 분배** – 이 옵션을 사용하면 작업을 수행해야 하는 기간을 정의할 수 있습니다. 이 옵션을 사용해 작업 시간대를 설정하여 네트워크 병목현상을 피할 수 있습니다. 지연 시간은 시간 또는 분 단위로 지정할 수 있습니다. 예를 들어 기본 시작 시간이 오전 10시이고 지연 시간이 60분인 경우 작업은 오전 10시~오전 11시 사이에 시작됩니다. • **머신이 꺼진 경우 머신 시작 시 누락된 작업 실행** • **작업 실행 중 절전 또는 최대 절전 모드가 되는 것을 방지** – 이 옵션은 Windows를 구동 중인 머신에서만 유효합니다. • **시작 조건이 충족되지 않아도 다음 후에 작업 실행** - 다른 시작 조건에 관계없이 지정한 기간이 지나면 작업이 시작됩니다. **참고** Linux에서는 시작 조건이 지원되지 않습니다.

- 새로 생성된 파일과 수정된 파일만 스캔하려면 **새 파일 및 변경된 파일만 스캔** 확인란을 선택합니다.

기본 설정: **활성화됨**

- **사용자 정의 스캔**에서 **전체 스캔** 전용으로 표시되는 두 가지 추가 옵션:

1. **아카이브 파일 스캔**

   기본 설정: **활성화됨**.

   최대 재귀 깊이

   기본 설정: **16**

   스캔할 임베디드된 아카이브의 수준입니다. 예: MIME 문서 > ZIP 아카이브 > Office 아카이브 > 문서 콘텐츠

   최대 크기

   기본 설정: **100**

   스캔할 아카이브 파일의 최대 크기입니다.

2. **이동식 드라이브 스캔**

기본 설정: **비활성화됨**

© Acronis International GmbH, 2003-2024

- **매핑된 (원격) 네트워크 드라이브**
- **USB 스토리지 장치**(펜 드라이브 및 외장 하드 드라이브)
- **CD/DVD**

참고
Linux에서는 이동식 드라이브 스캔이 지원되지 않습니다.

보호 제외

보호 제외 기능을 사용하면 신뢰하는 프로그램이 랜섬웨어나 맬웨어로 간주될 때 위양성을 제거할 수 있습니다. 신뢰하는 항목과 차단되는 항목을 정의하려는 경우 해당 항목을 보호 제외 목록에 추가하면 됩니다.

신뢰하는 항목 목록에 추가하는 파일, 프로세스, 폴더는 시스템에서 안전한 항목으로 간주되므로 더 이상 위험한 항목으로 감지되지 않습니다.

차단되는 항목 목록에는 프로세스와 해시를 추가할 수 있습니다. 이 옵션을 사용하면 해당 프로세스가 차단되므로 워크로드를 안전하게 유지할 수 있습니다.

보호 제외 항목	차단됨	신뢰함
해시	차단되는 항목 목록에 해시를 추가하면 제공된 해시에 따라 시스템이 프로세스를 중지합니다. 예를 들어 MD5 해시 938c2cc0dcc05f2b68c4287040cfcf71을 추가하면 이 해시와 연관된 프로세스가 차단됩니다.	신뢰하는 항목 목록에 해시를 추가하면 제공된 해시에 따라 시스템이 모니터링에서 무시할 프로세스를 확인하게 됩니다. 예를 들어 MD5 해시 938c2cc0dcc05f2b68c4287040cfcf71을 추가하면 이 해시와 연관된 프로세스가 신뢰되어 모니터링에서 제외됩니다.
프로세스	차단되는 항목 목록에 프로세스를 추가하면 시스템이 해당 프로세스를 모니터링해야 함을 확인하게 되며 프로세스가 항상 차단됩니다. 예를 들어 차단되는 항목 목록에 C:\Users\user1\application\nppInstaller.exe 경로를 추가하면 이 특정 프로세스가 차단되며 해당 파일을 열려고 하면 파일 시작이 허용되지 않습니다.	신뢰하는 항목 목록에 프로세스를 추가하면 시스템이 해당 프로세스를 모니터링에서 제외해야 함을 확인하게 됩니다. **참고** Microsoft에서 서명한 프로세스는 항상 신뢰됩니다. 예를 들어 C:\Users\user1\application\nppInstaller.exe 경로를 추가하면 이 특정 프로세스가 모니터링에서 제외되며 이 프로세스가 안티바이러스 프로그램에 의해 중단되지 않습니다.
파일/		신뢰하는 항목 목록에 파일이나 폴더를 추가하면 시스템이 해당 파일이나 폴더를

© Acronis International GmbH, 2003-2024

보호 제외 항목	차단됨	신뢰함
폴더		항상 스캔/모니터링할 필요가 없는 안전한 항목으로 간주해야 함을 확인하게 됩니다.

항상 신뢰할 항목을 지정하려면

1. 보호 계획을 엽니다.
2. **안티바이러스 및 안티맬웨어 보호 기능** 모듈을 확장합니다.
3. **제외** 옵션을 선택합니다.
   보호 제외 창이 열립니다.
4. **신뢰하는 항목** 섹션에서 **추가**를 클릭하여 사용 가능한 옵션 중에서 원하는 옵션을 선택합니다.
   - 파일, 폴더 또는 프로세스를 신뢰하는 항목으로 지정하려면 **파일/폴더/프로세스** 옵션을 선택합니다. **파일/폴더/프로세스 추가** 창이 열립니다.
     - **파일/프로세스/폴더** 필드에 각 프로세스, 폴더 또는 파일의 경로를 한 라인에 하나씩 입력합니다. 신뢰하는 항목 목록에서 변경 사항을 확인할 수 있도록 **설명** 섹션에 간략한 설명을 입력합니다.
     - 파일/폴더를 신뢰하는 항목으로 지정하려면 **파일/폴더로 추가** 확인란을 선택합니다.
       폴더 설명의 예: D:\folder\, /home/Folder/folder2, F:\
     - 프로세스를 신뢰하는 항목으로 지정하려면 **프로세스로 추가** 확인란을 선택합니다. 선택한 프로세스가 모니터링에서 제외됩니다.

       참고
       드라이브 문자로 시작하는 프로세스 실행 파일의 전체 경로를 지정합니다. 예를 들어 `C:\Windows\Temp\er76s7sdkh.exe` 등을 지정할 수 있습니다.

       참고
       \\localhost\folderpath\file.exe 등의 로컬 네트워크 경로도 삽입할 수 있습니다.

   - 신뢰하는 항목 목록에 MD5 해시를 추가하려면 **해시** 옵션을 선택합니다. **해시 추가** 창이 열립니다.
     - 여기에서 보호 제외 목록에 신뢰하는 항목으로 포함할 각 MD5 해시를 한 행에 하나씩 삽입할 수 있습니다. Cyber Protection에서는 이러한 해시에 따라 MD5 해시가 설명하는 프로세스를 모니터링에서 제외합니다.

기본 설정: 기본적으로 제외가 정의되어 있지 않습니다.

항상 차단할 항목을 지정하려면

1. 보호 계획을 엽니다.
2. **안티바이러스 및 안티맬웨어 보호 기능** 모듈을 확장합니다.
3. **보호 제외** 옵션을 선택합니다. **보호 제외** 창이 열립니다.

© Acronis International GmbH, 2003-2024

차단되는 항목 섹션에서 **추가**를 클릭하여 사용 가능한 옵션 중에서 원하는 옵션을 선택합니다.

- 프로세스를 차단하려면 **프로세스** 옵션을 선택합니다. **프로세스 추가** 창이 열립니다.
  - **프로세스** 필드에 각 프로세스의 경로를 한 라인에 하나씩 입력합니다. 차단되는 항목 목록에서 변경 사항을 확인할 수 있도록 **설명** 필드에 간략한 설명을 입력합니다.

참고
Active Protection이 머신에서 활성화되어 있는 한 이 프로세스는 시작될 수 없습니다.

- 해시를 차단하려면 **해시** 옵션을 선택합니다. **해시 추가** 창이 표시됩니다.
  - **해시** 필드에 각 프로세스의 해시를 한 라인에 하나씩 입력합니다. 차단되는 항목 목록에서 변경 사항을 확인할 수 있도록 **설명** 필드에 간략한 설명을 입력합니다.

기본 설정: 기본적으로 제외가 정의되어 있지 않습니다.

와일드카드

폴더를 지정하는 데는 와일드카드 문자 * 및 ?를 사용할 수 있습니다. 0개 이상의 문자는 별표(*)로 대체할 수 있습니다. 정확히 하나의 문자는 물음표(?)로 대체할 수 있습니다. %AppData%와 같은 환경 변수는 사용할 수 없습니다.

와일드카드(*)를 사용하여 제외 목록에 항목을 추가할 수 있습니다.

- 와일드카드는 설명의 중간이나 끝에 사용할 수 있습니다.

설명에 사용할 수 있는 와일드카드의 예:

C:*.pdf

D:\folders\file.*

C:\Users*\AppData\Roaming

- 와일드카드는 설명의 시작 부분에는 사용할 수 없습니다.

설명에 사용할 수 없는 와일드카드의 예:

*.docx

*:\folder\

변수

변수를 사용하여 보호 제외 목록에 항목을 추가할 수도 있으며 이 경우 다음과 같은 제한이 따릅니다.

- Windows의 경우 SYSTEM 변수만을 지원합니다. 예를 들면, %USERNAME%, %APPDATA%와 같은 사용자 지정 변수는 지원되지 않습니다. {username}을 포함하는 변수는 지원되지 않습니다. 자세한 내용은 https://ss64.com/nt/syntax-variables.html 을 참조하십시오.
- macOS의 경우 환경 변수는 지원되지 않습니다.
- Linux의 경우 환경 변수는 지원되지 않습니다.

지원되는 양식은 다음과 같습니다:

© Acronis International GmbH, 2003-2024

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

설명

보호 제외 목록에 추가한 제외에 대한 설명을 입력하려면 **설명** 필드를 사용할 수 있습니다. 다음은 입력할 수 있는 설명의 예입니다.

- 제외 이유 및 목적
- 해시 제외의 실제 파일 이름
- 타임 스탬프

단일 엔트리에 여러 개의 항목이 추가된 경우 여러 항목에 대해 하나의 주석만 캡처할 수 있습니다.

Cyber Backup Standard Edition의 Active Protection

Cyber Backup 표준 버전에서 Active Protection은 보호 계획 내 별도의 모듈입니다. 따라서 장치와 장치 그룹마다 다르게 구성하고 적용할 수 있습니다.

기타 모든 Cyber Protection 서비스 버전에서는 Active Protection이 보호 계획의 **안티바이러스 및 맬웨어 방지** 모듈에 포함되어 제공됩니다.

기본 설정: **활성화됨**.

참고
보호 에이전트가 보호되는 머신에 설치되어 있어야 합니다. 지원되는 운영 체제 및 기능에 대한 자세한 내용은 "지원되는 플랫폼"(743페이지) 항목을 참조하십시오.

작동법

Active Protection은 보호된 머신에서 실행 중인 프로세스를 모니터링합니다. 서드 파티 프로세스에서 파일 암호화 또는 암호화폐 채굴을 시도하면 Active Protection은 경보를 생성하고 보호 계획 지정된 추가 작업을 수행합니다.

또한, 로컬 폴더에 위치하는 소프트웨어 고유 프로세스, 레지스트리 기록, 실행 가능한 구성 파일, 백업의 무단 변경을 방지합니다.

악성 프로세스를 식별하기 위해 Active Protection에는 동작 추론이 사용됩니다. Active Protection은 프로세스에서 수행한 작업 체인을 악의적인 동작 패턴의 데이터베이스에 기록된 이벤트 체인과 비교합니다. 이 방법을 사용하면 Active Protection이 일반적인 동작에 따라 새로운 맬웨어를 탐지할 수 있습니다.

Cyber Backup Standard의 Active Protection 설정

Cyber Backup Standard Edition에서는 다음 Active Protection 기능을 구성할 수 있습니다.

© Acronis International GmbH, 2003-2024

- 감지에 대한 작업
- 자체 보호
- 네트워크 폴더 보호
- 서버 측 보호
- 크립토마이닝 프로세스 감지됨
- 제외

참고
Linux용 Active Protection은 다음 설정을 지원합니다. 감지에 대한 작업, 네트워크 폴더 보호 및 제외. 네트워크 폴더 보호는 항상 켜져 있으며 구성할 수 없습니다.

감지에 대한 작업

감지에 대한 작업 섹션에서 사용 가능한 옵션 중 하나를 선택합니다.

- **알리기만 함**
  소프트웨어에서 랜섬웨어 활동이 의심되는 프로세스에 대해 경보를 생성합니다.
- **프로세스 중지**
  소프트웨어에서 랜섬웨어 활동이 의심되는 프로세스에 대해 경보를 생성하고 프로세스를 중지합니다.
- **캐시를 사용해 되돌림**
  소프트웨어에서 경보를 생성하고 프로세스를 중지하고 서비스 캐시를 사용해 파일 변경 사항을 되돌립니다.

기본 설정: **캐시를 사용해 되돌림**.

자체 보호는 로컬 폴더에 있는 소프트웨어 고유 프로세스, 레지스트리 기록, 실행 파일과 구성 파일 및 백업의 무단 변경을 방지합니다.

관리자는 **Active Protection**을 활성화하지 않고도 **자체 보호**를 활성화할 수 있습니다.

기본 설정: **켜기**입니다.

참고
Linux에서는 자체 보호가 지원되지 않습니다.

자체 보호를 활성화하려면

1. **보호 계획 생성** 창에서 **안티바이러스 및 맬웨어 방지 보호** 모듈을 확장합니다.
2. **자체 보호**를 클릭합니다.
3. **자체 보호** 토글을 사용하여 자체 보호를 활성화합니다.

패스워드 보호를 활성화하려면

1. **자체 보호** 기능을 활성화한 후에는 토글을 사용하여 **암호 보호** 기능을 활성화할 수 있습니다.
2. **새 암호 생성**을 클릭하여 로컬 에이전트 수정 또는 삭제용 암호를 생성합니다.

© Acronis International GmbH, 2003-2024

3. **복사**를 클릭한 후 암호를 안전한 위치에 붙여넣습니다. 컴포넌트 목록을 로컬에서 수정할 때 암호를 입력하라는 메시지가 표시되기 때문입니다.

   중요
   창을 닫은 후에는 암호를 사용할 수 없습니다. 이 패스워드를 장치에 적용하려면 보호 계획 설정을 저장해야 합니다.

4. **닫기**를 클릭합니다.

암호 보호는 권한이 없는 사용자나 소프트웨어가 Agent for Windows를 설치 제거하거나 해당 컴포넌트를 변경하는 것을 방지합니다. 이 작업은 관리자가 제공하는 패스워드로만 가능합니다.

다음 작업에는 비밀번호가 필요하지 않습니다:

- 설정 프로그램을 로컬에서 실행하여 설치를 업데이트
- Cyber Protect 콘솔을 사용하여 설치 업데이트
- 설치를 복구

기본 설정: **비활성화됨**

암호 보호를 활성화하는 방법에 대한 자세한 내용은 에이전트 무단 설치 제거 또는 수정 방지를 참조하십시오.

네트워크 폴더 보호

로컬 드라이브로 매핑된 네트워크 폴더 보호 설정은 로컬 악성 프로세스에서 Active Protection이 로컬 드라이브로 매핑된 네트워크 폴더를 보호하는지 정의합니다.

이 설정은 SMB나 NFS 프로토콜을 통해 공유된 폴더에 적용됩니다.

파일이 원래 매핑된 드라이브에 위치할 경우에는 **캐시를 사용해 되돌림** 작업을 통해 캐시에서 추출할 때 원래 위치에 저장할 수 없습니다. 그 대신 파일은 이 설정에 지정되는 폴더에 저장됩니다. 기본 폴더는 Windows의 경우 `C:\ProgramData\Acronis\Restored Network Files`이고 macOS의 경우 `Library/Application Support/Acronis/Restored Network Files/`입니다. 이 폴더가 없는 경우에는 새로 생성됩니다. 이 경로의 변경을 원할 경우에는 로컬 폴더를 지정해야 합니다. 매핑된 드라이브의 폴더를 포함하여 네트워크 폴더는 지원되지 않습니다.

기본 설정: **켜기**입니다.

이 기능을 사용하면 위협을 야기할 가능성이 있는 네트워크의 다른 서버에서 들어오는 외부 연결을 통해 공유한 네트워크 폴더를 Active Protection이 보호하는지 여부를 정의할 수 있습니다.

기본 설정: **끄기**.

참고
Linux에서는 서버 측 보호가 지원되지 않습니다.

신뢰할 수 있는 연결을 설정하려면

© Acronis International GmbH, 2003-2024

1. **보호 계획 생성** 창에서 **안티바이러스 및 맬웨어 방지 보호** 모듈을 확장합니다.
2. **서버 측 보호**를 클릭합니다.
3. **서버측 보호** 토글을 사용하여 서버측 보호를 활성화합니다.
4. **신뢰함** 탭을 선택합니다.
5. **신뢰할 수 있는 연결** 필드에서 **추가**를 클릭하여 데이터를 수정할 수 있는 연결을 정의합니다.
6. **컴퓨터 이름/계정** 필드에 보호 에이전트가 설치된 머신의 컴퓨터 이름과 계정을 입력합니다. 예를 들어 `MyComputer\TestUser`와 같이 입력합니다.
7. **호스트 이름** 필드에 보호 에이전트를 사용하여 머신에 연결할 수 있는 머신의 호스트 이름을 입력합니다.
8. 연결 정의를 저장하려면 우측의 확인 표시를 클릭합니다.
9. **완료**를 클릭합니다.

차단된 연결을 설정하려면

1. **보호 계획 생성** 창에서 **안티바이러스 및 맬웨어 방지 보호** 모듈을 확장합니다.
2. **서버 측 보호**를 클릭합니다.
3. **서버측 보호** 토글을 사용하여 서버측 보호를 활성화합니다.
4. **차단됨** 탭을 선택합니다.
5. **차단된 연결** 필드에서 **추가**를 클릭하여 데이터를 수정할 수 없는 연결을 정의합니다.
6. **컴퓨터 이름/계정** 필드에 보호 에이전트가 설치된 머신의 컴퓨터 이름과 계정을 입력합니다. 예를 들어 `MyComputer\TestUser`와 같이 입력합니다.
7. **호스트 이름** 필드에 보호 에이전트를 사용하여 머신에 연결할 수 있는 머신의 호스트 이름을 입력합니다.
8. 오른쪽 확인란을 선택하여 연결 정의를 저장합니다.
9. **완료**를 클릭합니다.

크립토마이닝 맬웨어에 감염되면 유용한 애플리케이션의 성능이 저하되고 전기세가 증가하며, 시스템이 남용되어 작동이 중단되거나 하드웨어가 손상될 수도 있습니다. **크립토마이닝 프로세스 감지됨** 기능은 컴퓨터 리소스의 승인되지 않은 사용을 방지하기 위해 크립토마이닝 맬웨어로부터 장치를 보호합니다.

관리자는 **Active Protection**을 활성화하지 않고도 **크립토마이닝 프로세스 감지됨**를 활성화할 수 있습니다. 기본 설정: **활성화됨**.

참고
Linux에서는 크립토마이닝 프로세스 감지가 지원되지 않습니다.

네트워크 폴더 보호를 구성하려면

1. **보호 계획 생성** 창에서 **안티바이러스 및 맬웨어 방지 보호** 모듈을 확장합니다.
2. **크립토마이닝 프로세스 감지됨**를 클릭합니다.
3. **크립토마이닝 프로세스 감지됨** 토글을 사용하여 기능을 활성화하거나 비활성화합니다.

© Acronis International GmbH, 2003-2024

4. 크립토마이닝 활동이 의심되는 프로세스 감지 시에 수행할 작업을 선택합니다.
   기본 설정: **프로세스 중지**
   - **알리기만 함** - 소프트웨어에서 경보를 생성합니다.
   - **프로세스 중지** - 소프트웨어에서 경보를 생성하고 프로세스를 중지합니다.
5. **완료**를 클릭하여 선택한 옵션을 보호 계획에 적용합니다.

보호 제외 기능을 사용하면 신뢰하는 프로그램이 랜섬웨어나 맬웨어로 간주될 때 위양성을 제거할 수 있습니다. 신뢰하는 항목과 차단되는 항목을 정의하려는 경우 해당 항목을 보호 제외 목록에 추가하면 됩니다.

신뢰하는 항목 목록에 추가하는 파일, 프로세스, 폴더는 시스템에서 안전한 항목으로 간주되므로 더 이상 위험한 항목으로 감지되지 않습니다.

차단되는 항목 목록에는 프로세스와 해시를 추가할 수 있습니다. 이 옵션을 사용하면 해당 프로세스가 차단되므로 워크로드를 안전하게 유지할 수 있습니다.

보호 제외 항목	차단됨	신뢰함
해시	차단되는 항목 목록에 해시를 추가하면 제공된 해시에 따라 시스템이 프로세스를 중지합니다. 예를 들어 MD5 해시 938c2cc0dcc05f2b68c4287040cfcf71을 추가하면 이 해시와 연관된 프로세스가 차단됩니다.	신뢰하는 항목 목록에 해시를 추가하면 제공된 해시에 따라 시스템이 모니터링에서 무시할 프로세스를 확인하게 됩니다. 예를 들어 MD5 해시 938c2cc0dcc05f2b68c4287040cfcf71을 추가하면 이 해시와 연관된 프로세스가 신뢰되어 모니터링에서 제외됩니다.
프로세스	차단되는 항목 목록에 프로세스를 추가하면 시스템이 해당 프로세스를 모니터링해야 함을 확인하게 되며 프로세스가 항상 차단됩니다. 예를 들어 차단되는 항목 목록에 C:\Users\user1\application\nppInstaller.exe 경로를 추가하면 이 특정 프로세스가 차단되며 해당 파일을 열려고 하면 파일 시작이 허용되지 않습니다.	신뢰하는 항목 목록에 프로세스를 추가하면 시스템이 해당 프로세스를 모니터링에서 제외해야 함을 확인하게 됩니다. **참고** Microsoft에서 서명한 프로세스는 항상 신뢰됩니다. 예를 들어 C:\Users\user1\application\nppInstaller.exe 경로를 추가하면 이 특정 프로세스가 모니터링에서 제외되며 이 프로세스가 안티바이러스 프로그램에 의해 중단되지 않습니다.
파일/폴더		신뢰하는 항목 목록에 파일이나 폴더를 추가하면 시스템이 해당 파일이나 폴더를 항상 스캔/모니터링할 필요가 없는 안전한 항목으로 간주해야 함을 확인하게 됩니다.

© Acronis International GmbH, 2003-2024

항상 신뢰할 항목을 지정하려면

1. 보호 계획을 엽니다.
2. **안티바이러스 및 안티맬웨어 보호 기능** 모듈을 확장합니다.
3. **제외** 옵션을 선택합니다.
   보호 제외 창이 열립니다.
4. **신뢰하는 항목** 섹션에서 **추가**를 클릭하여 사용 가능한 옵션 중에서 원하는 옵션을 선택합니다.
   - 파일, 폴더 또는 프로세스를 신뢰하는 항목으로 지정하려면 **파일/폴더/프로세스** 옵션을 선택합니다. **파일/폴더/프로세스 추가** 창이 열립니다.
     - **파일/프로세스/폴더** 필드에 각 프로세스, 폴더 또는 파일의 경로를 한 라인에 하나씩 입력합니다. 신뢰하는 항목 목록에서 변경 사항을 확인할 수 있도록 **설명** 섹션에 간략한 설명을 입력합니다.
     - 파일/폴더를 신뢰하는 항목으로 지정하려면 **파일/폴더로 추가** 확인란을 선택합니다.
       폴더 설명의 예: D:\folder\, /home/Folder/folder2, F:\
     - 프로세스를 신뢰하는 항목으로 지정하려면 **프로세스로 추가** 확인란을 선택합니다. 선택한 프로세스가 모니터링에서 제외됩니다.

     참고
     드라이브 문자로 시작하는 프로세스 실행 파일의 전체 경로를 지정합니다. 예를 들어 `C:\Windows\Temp\er76s7sdkh.exe` 등을 지정할 수 있습니다.

     참고
     \\localhost\folderpath\file.exe 등의 로컬 네트워크 경로도 삽입할 수 있습니다.

   - 신뢰하는 항목 목록에 MD5 해시를 추가하려면 **해시** 옵션을 선택합니다. **해시 추가** 창이 열립니다.
     - 여기에서 보호 제외 목록에 신뢰하는 항목으로 포함할 각 MD5 해시를 한 행에 하나씩 삽입할 수 있습니다. Cyber Protection에서는 이러한 해시에 따라 MD5 해시가 설명하는 프로세스를 모니터링에서 제외합니다.

기본 설정: 기본적으로 제외가 정의되어 있지 않습니다.

항상 차단할 항목을 지정하려면

1. 보호 계획을 엽니다.
2. **안티바이러스 및 안티맬웨어 보호 기능** 모듈을 확장합니다.
3. **보호 제외** 옵션을 선택합니다. **보호 제외** 창이 열립니다.
   차단되는 항목 섹션에서 **추가**를 클릭하여 사용 가능한 옵션 중에서 원하는 옵션을 선택합니다.
   - 프로세스를 차단하려면 **프로세스** 옵션을 선택합니다. **프로세스 추가** 창이 열립니다.
     - **프로세스** 필드에 각 프로세스의 경로를 한 라인에 하나씩 입력합니다. 차단되는 항목 목록에서 변경 사항을 확인할 수 있도록 **설명** 필드에 간략한 설명을 입력합니다.

     참고
     Active Protection이 머신에서 활성화되어 있는 한 이 프로세스는 시작될 수 없습니다.

© Acronis International GmbH, 2003-2024

- 해시를 차단하려면 **해시** 옵션을 선택합니다. **해시 추가** 창이 표시됩니다.
  - **해시** 필드에 각 프로세스의 해시를 한 라인에 하나씩 입력합니다. 차단되는 항목 목록에서 변경 사항을 확인할 수 있도록 **설명** 필드에 간략한 설명을 입력합니다.

기본 설정: 기본적으로 제외가 정의되어 있지 않습니다.

와일드카드

폴더를 지정하는 데는 와일드카드 문자 * 및 ?를 사용할 수 있습니다. 0개 이상의 문자는 별표(*)로 대체할 수 있습니다. 정확히 하나의 문자는 물음표(?)로 대체할 수 있습니다. %AppData%와 같은 환경 변수는 사용할 수 없습니다.

와일드카드(*)를 사용하여 제외 목록에 항목을 추가할 수 있습니다.

- 와일드카드는 설명의 중간이나 끝에 사용할 수 있습니다.

설명에 사용할 수 있는 와일드카드의 예:

C:*.pdf

D:\folders\file.*

C:\Users*\AppData\Roaming

- 와일드카드는 설명의 시작 부분에는 사용할 수 없습니다.

설명에 사용할 수 없는 와일드카드의 예:

*.docx

*:\folder\

변수

변수를 사용하여 보호 제외 목록에 항목을 추가할 수도 있으며 이 경우 다음과 같은 제한이 따릅니다.

- Windows의 경우 SYSTEM 변수만을 지원합니다. 예를 들면, %USERNAME%, %APPDATA%와 같은 사용자 지정 변수는 지원되지 않습니다. {username}을 포함하는 변수는 지원되지 않습니다. 자세한 내용은 https://ss64.com/nt/syntax-variables.html 을 참조하십시오.
- macOS의 경우 환경 변수는 지원되지 않습니다.
- Linux의 경우 환경 변수는 지원되지 않습니다.

지원되는 양식은 다음과 같습니다:

- %WINDIR%\Media
- %public%
- %CommonProgramFiles%\Acronis\

© Acronis International GmbH, 2003-2024

설명

보호 제외 목록에 추가한 제외에 대한 설명을 입력하려면 **설명** 필드를 사용할 수 있습니다. 다음은 입력할 수 있는 설명의 예입니다.

- 제외 이유 및 목적
- 해시 제외의 실제 파일 이름
- 타임 스탬프

단일 엔트리에 여러 개의 항목이 추가된 경우 여러 항목에 대해 하나의 주석만 캡처할 수 있습니다.

URL 필터링

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

맬웨어는 악성 또는 감염된 사이트에서 배포되는 경우가 많으며 드라이브 바이 다운로드라는 감염 방법을 사용합니다.

URL 필터링 기능은 인터넷의 맬웨어와 피싱 같은 위협에서 머신을 보호합니다. 사용자가 악성 콘텐츠를 포함할 가능성이 있는 웹사이트에 액세스하지 못하도록 차단하여 조직을 보호할 수 있습니다.

또 이 URL 필터링으로 외부 규정 및 회사 내부 정책을 준수하며 웹을 사용하도록 제어할 수 있습니다. 웹사이트와 관련된 카테고리에 따라 웹사이트에 대한 액세스를 구성할 수 있습니다. URL 필터링은 현재 44개의 웹사이트 카테고리를 지원하며 이에 대한 액세스를 관리할 수 있습니다.

현재 보호 에이전트는 Windows 머신의 HTTP/HTTPS 연결을 검사합니다.

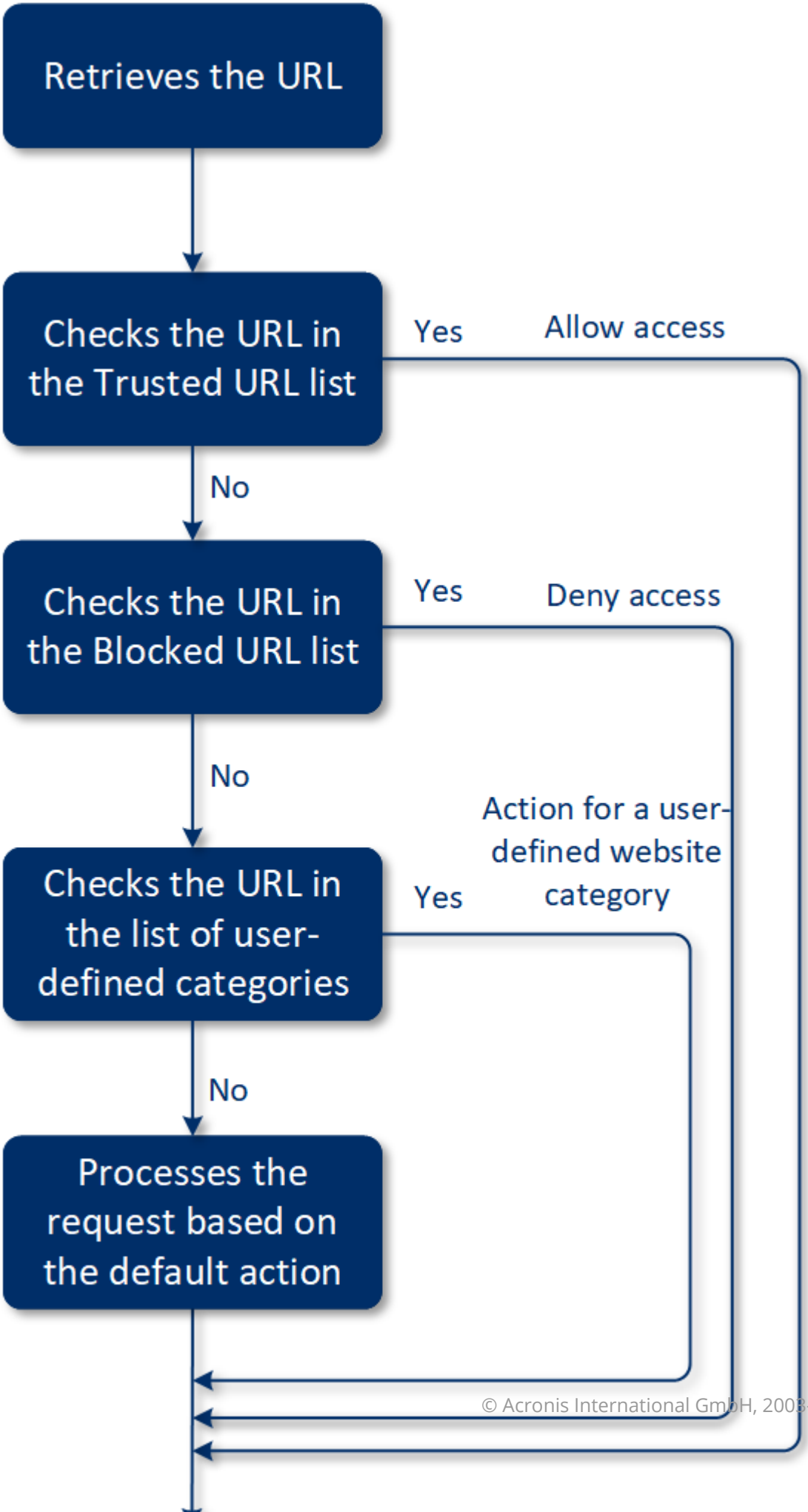
URL 필터링 기능을 사용하려면 기능이 인터넷에 연결할 수 있어야 합니다.

참고
Protection 에이전트 빌드 15.0.26692(릴리스 C21.03 HF1) 이하에서 발생할 가능성이 있는 호환성 문제를 방지하기 위해 다른 안티바이러스 솔루션이 감지되거나 시스템에 Windows 보안 센터 서비스가 없으면 URL 필터링 기능이 자동으로 비활성화됩니다.
최신 Protection 에이전트에서는 호환성 문제가 해결되었으므로 정책에 따라 URL 필터링이 항상 활성화됩니다.

작동법

사용자가 브라우저에서 URL 링크를 입력합니다. 인터셉터가 링크를 입수해 보호 에이전트로 전송합니다. 에이전트가 URL를 입수해 구문 분석하고 검사합니다. 인터셉터는 사용자를 사용 가능한 작업 메시지가 있는 페이지로 리디렉션하여 요청한 페이지에 대한 작업을 수동으로 진행하도록 합니다.

© Acronis International GmbH, 2003-2024



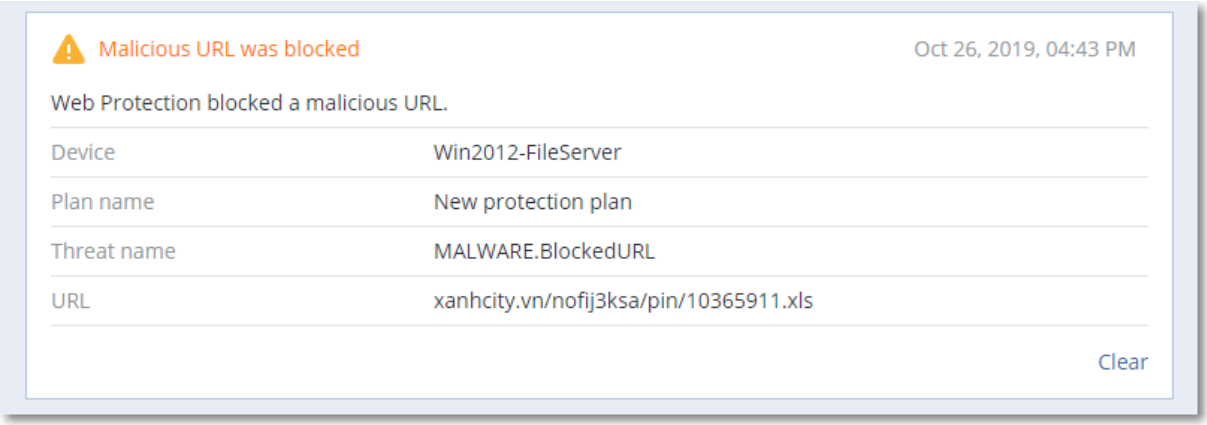
© Acronis International GmbH, 2003-2024

URL 필터링 구성 작업 흐름

일반적으로 URL 필터링 구성은 다음과 같은 단계로 이루어집니다.

1. **URL 필터링** 모듈이 활성화된 보호 계획을 생성합니다.
2. URL 필터링 설정을 지정합니다(아래 참고).
3. 머신에 보호 계획을 할당합니다.

차단된 URL을 확인하려면 **모니터링** > **경보**로 이동합니다.



URL 필터링 설정

URL 필터링 모듈에 대해 다음 설정을 지정할 수 있습니다.

악성 웹사이트 액세스

사용자가 악성 웹사이트를 열 경우 수행할 작업을 지정합니다.

- **알리기만 함**—소프트웨어는 랜섬웨어 활동을 의심하는 프로세스에 대한 경보를 생성합니다.
- **차단** — 악성 웹 사이트에 대한 액세스를 차단합니다. 사용자는 웹 사이트에 액세스할 수 없으며 경고 경보가 생성됩니다.
- **항상 사용자에게 확인**—사용자에게 웹 사이트로 계속 진행할지 아니면 다시 돌아갈지를 묻습니다.

필터링할 카테고리

다음과 같이 액세스를 구성할 수 있는 44개의 웹사이트 카테고리가 있습니다.

- **허용** – 선택한 카테고리와 관련된 웹사이트의 액세스를 허용합니다.
- **거부** – 선택한 카테고리와 관련된 웹사이트의 액세스를 거부합니다.

기본적으로 모든 카테고리가 허용됩니다.

차단된 URL에 대한 모든 알림을 카테고리별로 표시 - 이 기능을 사용하면 차단된 URL에 대한 모든 알림이 카테고리별로 트레이에 표시됩니다. 웹사이트에 하위 도메인이 여러 개 있으면 시스템에서 그에 대한 알림 역시 생성하기 때문에 알림 수가 많을 수 있습니다.

© Acronis International GmbH, 2003-2024

아래 표에서 카테고리 설명을 확인할 수 있습니다.

	웹사이트 카테고리	설명
1	**광고**	이 카테고리에는 주 목적이 광고인 도메인이 포함됩니다.
2	**메시지 게시판**	이 카테고리에는 포럼, 토론 게시판, 질의 응답형 웹사이트가 포함됩니다. 이 카테고리에 고객이 질문을 게시하는 기업 웹 사이트의 특정 섹션은 포함되지 않습니다.
3	**개인용 웹사이트**	이 카테고리에는 개인 웹사이트와 모든 유형의 블로그(개인, 그룹, 회사 블로그 등)가 포함됩니다. '블로그'란 WWW(World Wide Web)에 게시된 저널입니다. 게시글('포스팅')로 이루어져 있으며, 일반적으로 가장 최근 포스팅이 가장 먼저 보이도록 역순으로 배열됩니다.
4	**기업/비즈니스 웹사이트**	이 카테고리는 보통 다른 어떤 카테고리에도 속하지 않는 기업 웹사이트가 포함되는 광범위한 카테고리입니다.
5	**컴퓨터 소프트웨어**	이 카테고리에는 보통 오픈 소스, 프리웨어 또는 쉐어웨어 같은 컴퓨터 소프트웨어를 제공하는 웹사이트가 포함됩니다. 일부 온라인 소프트웨어 스토어도 포함될 수 있습니다.
6	**의약품**	이 카테고리에는 의약품/주류/담배와 관련되어 (합법) 의약용품, 주류, 담배 제품의 사용이나 판매에 관해 토론하는 웹사이트가 포함됩니다. 불법 약물은 마약 카테고리에 포함됩니다.
7	**교육**	이 카테고리에는 .edu 도메인 이외의 웹사이트까지 포함하여 공식 교육 기관이 소유한 웹사이트가 포함됩니다. 백과사전과 같은 교육적인 웹사이트도 포함됩니다.
8	**엔터테인먼트**	이 카테고리에는 예술 활동 및 박물관에 관한 정보를 제공하는 웹사이트와 영화, 음악, 미술 등의 콘텐츠를 리뷰하거나 평가하는 웹사이트가 포함됩니다.
9	**파일 공유**	이 카테고리에는 사용자가 파일을 업로드하고 다른 사람과 공유할 수 있는 파일 공유 웹사이트가 포함됩니다. 토렌트 공유 웹사이트 및 토렌트 트래커도 포함됩니다.
10	**금융**	이 카테고리에는 온라인 액세스를 제공하는 전 세계 모든 은행의 웹사이트가 포함됩니다. 일부 신용 조합과 기타 금융 기관도 포함됩니다. 그러나 일부 지방 은행은 포함되지 않을 수 있습니다.
11	**도박**	이 카테고리에는 도박 웹사이트가 포함됩니다. 이는 일반적으로 사용자가 온라인 룰렛, 포커, 블랙잭 등의 게임에 돈을 걸기 전에 결제를 해야 하는 '온라인 카지노' 또는 '온라인 복권' 유형의 웹사이트를 의미합니다. 이런 웹사이트 중 일부는 합법적이고 이길 확률도

© Acronis International GmbH, 2003-2024

		있지만, 일부는 사기 행위이며, 이길 확률이 없음을 의미합니다. 이 외에 도박 및 온라인 복권 웹사이트에서 이익을 얻는 방법을 알려주는 '이기는 팁과 치트' 웹사이트까지 감지합니다.
12	**게임**	이 카테고리에는 보통 Adobe Flash 또는 JAVA 애플릿 기반의 온라인 게임 웹사이트가 포함됩니다. 게임이 무료인지, 구독을 필요로 하는지의 여부는 웹사이트 감지에 영향을 주지 않지만, 카지노 식 웹 사이트는 도박 카테고리로 감지됩니다. 이 카테고리에는 다음이 포함되지 않습니다. • 비디오 게임을 개발하는 기업의 공식 웹사이트(온라인 게임을 제작하는 경우 제외) • 게임을 논의하는 토론 웹사이트 • 비온라인 게임을 다운로드할 수 있는 웹 사이트(일부는 불법 카테고리에 포함) • World of Warcraft와 같이 사용자가 실행 파일을 다운로드하고 실행해야 하는 게임(이런 유형은 방화벽 등의 다른 수단에 의해 차단될 수 있음)
13	**정부**	이 카테고리에는 정부 기관, 대사관, 사무소 웹사이트 등의 정부 웹사이트가 포함됩니다.
14	**해킹**	이 카테고리에는 해커들을 위한 해킹 도구, 문서, 토론 플랫폼을 제공하는 웹사이트가 포함됩니다. 일반적인 플랫폼에 대한 악용 수단을 제공해 Facebook 또는 Gmail 계정 해킹을 용이하게 하는 웹사이트도 포함됩니다.
15	**불법 활동**	이 카테고리는 혐오, 폭력, 인종차별과 관련된 광범위한 카테고리이며, 다음 카테고리의 웹사이트를 차단하려는 목적을 가지고 있습니다. • 테러리스트 조직이 소유한 웹사이트 • 인종차별 또는 외국인 혐오적인 콘텐츠가 포함된 웹사이트 • 격렬한 스포츠를 논의하고/논의하거나 폭력을 조장하는 웹사이트
16	**건강 및 피트니스**	이 카테고리에는 의료기관 웹사이트, 질병 예방 및 치료 관련 웹사이트, 체중 감량, 다이어트, 스테로이드, 아나볼릭 또는 HGH 제품 관련 정보나 제품을 제공하는 웹사이트 및 성형 수술 관련 정보를 제공하는 웹사이트가 포함됩니다.
17	**취미**	이 카테고리에는 수집, 예술 및 공예, 자전거 타기 등 보통 개인의 여가 시간에 이루어지는 활동과 관련한 자료를 제공하는 웹사이트가 포함됩니다.
18	**웹 호스팅**	이 카테고리에는 개인 사용자와 조직이 웹페이지를 만들어 공개할 수 있도록 지원하는 무료 및 상용 웹사이트 호스팅 서비스가 포함됩니다.
19	**불법 다운로드**	이 카테고리에는 소프트웨어 프라이버시와 관련된 다음 웹사이트가 포함됩니다. • 저작권자의 동의 없이 저작권이 있는 콘텐츠를 배포하는 데 일조하는 것으로 알려진 P2P(BitTorrent, emule, DC++) 트래커 웹사이트 • Warez(해적판 상업용 소프트웨어) 웹사이트 및 토론 게시판 • 사용자에게 크랙, 키 생성기, 시리얼 번호를 제공해 불법적인 소프트웨어 사용을 조장하는 웹 사이트 이중 일부 웹 사이트는 포르노 또는 주류 광고를 사용해 이익을 창출하기 때문에 포르노 또는 주류/담배로도 감지될 수 있습니다.
20	**인스**	이 카테고리에는 실시간 채팅 서비스를 제공하는 인스턴트 메시징 및 채팅 웹사이트가 포

© Acronis International GmbH, 2003-2024

	턴트 메시징	함됩니다. 이 외에도 임베디드 인스턴트 메신저 서비스가 있는 yahoo.com 및 gmail.com도 감지할 것입니다.
21	**구직/구인**	이 카테고리에는 구직 게시판, 구직 관련 광고, 커리어 기회를 제공하는 웹사이트와 이러한 서비스를 종합하여 제공하는 웹사이트가 포함됩니다. 채용 기관 웹사이트 또는 일반 기업의 '채용' 페이지는 포함되지 않습니다.
22	**성인 콘텐츠**	이 카테고리에는 웹사이트 제작자가 성인용이라고 명시한 콘텐츠가 포함됩니다. 카마 수트라 책 및 성교육 웹사이트부터 노골적인 포르노까지 넓은 범위의 웹사이트를 감지합니다.
23	**마약**	이 카테고리에는 오락용 불법 약물에 관한 정보를 공유하는 웹사이트가 포함됩니다. 이 카테고리에는 마약 재배 및 개발과 관련된 웹사이트도 포함됩니다.
24	**뉴스**	이 카테고리에는 텍스트 및 동영상 뉴스를 제공하는 뉴스 웹사이트가 포함됩니다. 세계 및 지역 뉴스 웹사이트를 모두 포함하기 위해 노력합니다. 그러나 일부 소규모 지역 뉴스 웹사이트는 포함되지 않을 수 있습니다.
25	**온라인 데이트**	이 카테고리에는 사용자가 몇 가지 조건을 기준으로 다른 사람을 검색해 볼 수 있는 유료 및 무료 온라인 데이트 웹사이트가 포함됩니다. 사용자는 프로필을 게시해 다른 사람이 검색하도록 할 수 있습니다. 이 카테고리에는 유무료 온라인 데이트 웹사이트가 모두 포함됩니다. 대부분의 유명 소셜 네트워크가 온라인 데이트 웹사이트로 사용될 수 있기 때문에, Facebook과 같은 일부 인기 웹사이트도 이 카테고리에 감지됩니다. 이 카테고리는 소셜 네트워크 카테고리와 함께 사용하는 것이 좋습니다.
26	**온라인 결제**	이 카테고리에는 온라인 결제 또는 자금 이체 서비스를 제공하는 웹사이트가 포함됩니다. PayPal 또는 Moneybookers와 같은 인기 결제 웹사이트를 감지합니다. 또, 이 카테고리는 일반 웹사이트 중 신용 카드 정보를 요청하는 페이지를 스스로 감지해 숨겨지거나 알려지지 않거나 불법적인 온라인 스토어를 감지합니다.
27	**사진 공유**	이 카테고리에는 주 목적이 사진 업로드 및 공유인 사진 공유 웹사이트가 포함됩니다.
28	**온라인 스토어**	이 카테고리에는 알려진 온라인 스토어가 포함됩니다. 상품이나 서비스를 온라인으로 판매하는 웹사이트는 온라인 스토어로 간주됩니다.
29	**포르노**	이 카테고리에는 성적 콘텐츠와 포르노를 다루는 웹사이트가 포함됩니다. 유료 및 무료 웹사이트가 모두 포함됩니다. 사진, 이야기, 동영상을 제공하는 웹사이트가 포함되고, 여러 종류의 콘텐츠를 담고 있는 웹사이트에 포함된 포르노 콘텐츠도 감지합니다.
30	**포털**	이 카테고리에는 여러 출처 및 다양한 도메인에서 정보를 수집하고, 보통 검색 엔진, 이메일, 뉴스, 엔터테인먼트 정보 등의 기능을 제공하는 웹사이트가 포함됩니다.
31	**라디오**	이 카테고리에는 온라인 라디오 방송국부터 주문형(무료 또는 유료) 오디오 콘텐츠를 제공하는 웹사이트까지, 인터넷 음악 스트리밍 서비스를 제공하는 다양한 웹사이트가 포함됩니다.
32	**종교**	이 카테고리에는 종교 또는 종파를 홍보하는 웹사이트가 포함됩니다. 한 종교 또는 여러

© Acronis International GmbH, 2003-2024

		종교에 관한 토론 포럼도 다룹니다.
33	**검색 엔진**	이 카테고리에는 Google, Yahoo, Bing 같은 검색 엔진 웹사이트가 포함됩니다.
34	**소셜 네트워크**	이 카테고리에는 MySpace.com, Facebook.com, Bebo.com 등의 소셜 네트워크 웹사이트가 포함됩니다. YouTube.com과 같은 특별한 유형의 소셜 네트워크는 비디오/사진 카테고리에 나열됩니다.
35	**스포츠**	이 카테고리에는 스포츠 정보, 뉴스, 튜토리얼을 제공하는 웹사이트가 포함됩니다.
36	**자살**	이 카테고리에는 자살을 홍보, 조장, 옹호하는 웹사이트가 포함됩니다. 자살 방지 클리닉은 포함되지 않습니다.
37	**타블로이드**	이 카테고리에는 보통 소프트 포르노 및 셀럽 가십 웹사이트가 포함됩니다. 상당수의 타블로이드 뉴스가 여기에 해당하는 하위 카테고리를 갖고 있을 수 있습니다. 또한,이 카테고리의 감지는 휴리스틱을 기반으로 합니다.
38	**시간 낭비**	이 카테고리에는 사람들이 많은 시간을 소비하게 되는 웹사이트가 포함됩니다. 여기에는 소셜 네트워크나 엔터테인먼트와 같은 다른 카테고리의 웹사이트도 포함될 수 있습니다.
39	**여행**	이 카테고리에는 여행 상품과 여행 장비, 여행지 소개와 평가 등의 정보를 제공하는 웹사이트가 포함됩니다.
40	**비디오**	이 카테고리에는 사용자가 업로드하거나 다양한 콘텐츠 제공업체가 제공하는 동영상과 사진을 호스팅하는 웹사이트가 포함됩니다. 여기에는 YouTube, Metacafe, Google Video와 같은 웹사이트 및 Picasa나 Flickr와 같은 사진 웹사이트가 포함됩니다. 또한, 다른 웹사이트나 블로그에 포함된 비디오도 감지합니다.
41	**폭력적인 만화**	이 카테고리에는 폭력성, 외설적 언어, 성적 콘텐츠가 담겨 있어 미성년자에게 부적절한 폭력적인 만화나 애니메이션을 이야기하고, 공유하고, 제공하는 웹사이트가 포함됩니다. "톰과 제리"와 같은 대중적인 만화를 제공하는 웹사이트는 이 카테고리에 포함되지 않습니다.
42	**무기**	이 카테고리에는 판매 또는 교환, 제조, 사용을 목적으로 무기를 제공하는 웹사이트가 포함됩니다. 여기에는 사냥 도구, 공기총 및 BB총의 사용은 물론 근거리 무기도 포함됩니다.
43	**이메일**	이 카테고리에는 웹 응용 프로그램처럼 이메일 기능을 제공하는 웹사이트가 포함됩니다.
44	**웹 프록시**	이 카테고리에는 웹 프록시 서비스를 제공하는 웹사이트가 포함됩니다. 사용자가 웹 페이지를 열고 양식에 요청된 URL을 입력한 다음 "제출"을 클릭할 때 연결되는 "브라우저 내 브라우저" 유형의 웹사이트입니다. 웹 프록시 사이트는 실제 페이지를 다운로드한 다음 사용자 브라우저 내에 표시합니다. 이러한 유형을 감지하는 이유는 다음과 같습니다(또한 이런 이유로 차단이 필요할 수 있습니다). • 익명 브라우징. 대상 웹 서버가 프록시 웹 서버로부터 요청을 받으면 IP 주소만 표시되고, 서버 관리자가 사용자를 추적할 때 웹 프록시에서 추적이 끝나게 됩니다. 원래 사용자의 위치를 확인하는 데 필요한 로그가 남을 수도, 남지 않을 수도 있습니다.

© Acronis International GmbH, 2003-2024

		• 위치 스푸핑. 소스 위치에서 서비스 정보를 수집할 때 종종 사용자 IP 주소가 사용되며 (일부 국내 정부 웹사이트는 로컬 IP 주소로만 이용할 수 있음), 사용자가 실제 위치를 기만하는 데 이러한 서비스가 이용될 수도 있습니다. • 금지되는 콘텐츠에 액세스. 간단한 URL 필터를 사용하는 경우에는 웹 프록시 URL만 확인할 수 있고 사용자가 방문하는 실제 서버는 확인하지 못합니다. • 회사의 모니터링 회피. 기업 정책상 직원의 인터넷 사용을 모니터링 해야 하는 경우가 있습니다. 웹 프록시를 통해 액세스하게 되면 사용자가 올바른 정보를 제공하지 않으며 모니터링에서 벗어날 수 있습니다. SDK는 URL만이 아니라 HTML 페이지(제공된 경우)도 분석하므로, 일부 카테고리의 경우 여전히 SDK가 콘텐츠를 감지할 수 있습니다. 하지만 SDK를 사용하는 것만으로 그 외의 경우에 해당하는 문제를 방지할 수는 없습니다.

URL 제외

안전하다고 알려진 URL은 신뢰할 수 있는 도메인 목록에 추가할 수 있습니다. 위협에 해당하는 URL은 차단된 도메인 목록에 추가할 수 있습니다.

항상 신뢰하거나 차단하려는 URL을 지정하려면

1. 보호 계획의 URL 필터링 모듈에서 **URL 제외**를 클릭합니다.
   URL 제외 창이 열립니다.
   다음 옵션이 표시됩니다.

신뢰하는 항목 - **추가**를 클릭하여 사용 가능한 옵션 중에서 원하는 옵션을 선택합니다.

- **도메인** - 이 옵션을 선택하면 **도메인 추가** 창이 열립니다.
  - **도메인** 필드에 각 도메인을 한 라인에 하나씩 입력합니다. 신뢰하는 항목 목록에서 변경 사항을 확인할 수 있도록 **설명** 필드에 간략한 설명을 입력합니다.
- **프로세스** - 이 옵션을 선택하면 **프로세스 추가** 창이 표시됩니다.
  - **프로세스** 필드에 각 프로세스의 경로를 한 라인에 하나씩 입력합니다. 신뢰하는 항목 목록에서 변경 사항을 확인할 수 있도록 **설명** 섹션에 간략한 설명을 입력합니다.

차단되는 항목 - **추가**를 클릭합니다. **도메인 추가** 창이 표시됩니다.

도메인 필드에 각 도메인을 한 라인에 하나씩 입력합니다. 차단되는 항목 목록에서 변경 사항을 확인할 수 있도록 **설명** 필드에 간략한 설명을 입력합니다.

참고
로컬 네트워크 경로도 입력할 수 있습니다. 예를 들어 \\localhost\folderpath\file.exe 등의 경로를 입력할 수 있습니다.

설명

설명 필드를 사용하여 URL 제외 목록에 추가한 제외 항목 관련 참고 사항을 입력할 수 있습니다. 참고 사항에 입력할 수 있는 몇 가지 제안 항목은 다음과 같습니다.

© Acronis International GmbH, 2003-2024

- 제외 이유 및 목적
- 타임 스탬프

단일 엔트리에 여러 개의 항목이 추가된 경우 여러 항목에 대해 하나의 주석만 캡처할 수 있습니다.

Microsoft Defender 안티바이러스 및 Microsoft Security Essentials

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

Windows Defender 안티바이러스

Microsoft Defender 안티바이러스는 Windows 8부터 제공된 Microsoft Windows의 기본 맬웨어 방지 구성 요소입니다.

Microsoft Defender 안티바이러스(WDA) 모듈에서는 Microsoft Defender 안티바이러스 보안 정책을 구성하고 Cyber Protect 콘솔을 통해 해당 정책의 상태를 추적할 수 있습니다.

이 모듈은 Microsoft Defender 안티바이러스가 설치된 워크로드에 대해 적용 가능합니다.

Microsoft Security Essentials

Microsoft Security Essentials는 Windows 8 이전 버전에서 제공된 Microsoft Windows의 기본 맬웨어 방지 구성 요소입니다.

Microsoft Security Essentials 모듈에서는 Microsoft Security Essentials 보안 정책을 구성하고 Cyber Protect 콘솔을 통해 해당 정책의 상태를 추적할 수 있습니다.

이 모듈은 Microsoft Security Essentials가 설치된 워크로드에 대해 적용 가능합니다.

Microsoft Security Essentials의 설정도 Microsoft Defender 안티바이러스와 비슷합니다. 단, Cyber Protect 콘솔을 통해 제외 항목을 정의할 수는 없으며 실시간 보호도 구성할 수 없습니다.

스캔 예약

예약된 스캔의 스케줄을 지정합니다.

스캔 모드:

- **전체** – 빠른 스캔에서 스캔되는 항목을 비롯한 모든 파일과 폴더를 전체 검사합니다. 빠른 스캔에 비해 실행에 더 많은 머신 리소스가 필요합니다.
- **빠른 스캔** – 일반적으로 맬웨어가 발견되는 메모리 내 프로세스와 폴더를 빠르게 검사합니다. 실행 시 머신 리소스를 적게 사용합니다.

스캔이 실행될 시간과 요일을 정의합니다.

일일 빠른 스캔 – 매일 빠른 스캔을 수행할 시간을 정의합니다.

© Acronis International GmbH, 2003-2024

필요에 따라 다음 옵션을 설정할 수 있습니다.

머신이 켜져 있지만 사용 중이 아닐 때 예약된 스캔을 시작

예약된 스캔을 실행하기 전에 최신 바이러스 및 스파이웨어 정의를 확인합니다

스캔 중 CPU 사용을 다음으로 제한

Microsoft Defender 안티바이러스의 설정에 대한 자세한 내용은 https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#scheduled-scans-settings를 참고하십시오.

기본 작업

다양한 보안 수준의 감지된 위협에 대해 수행할 기본 작업을 정의합니다.

- **정리** – 워크로드에서 감지된 맬웨어를 정리합니다.
- **격리** – 감지된 맬웨어를 격리 폴더로 이동하지만 제거하지는 않습니다.
- **제거** – 워크로드에서 감지된 맬웨어를 제거합니다.
- **허용** – 감지된 맬웨어를 제거하거나 격리하지 않습니다.
- **사용자 정의** – 감지된 맬웨어에 대해 수행할 작업을 지정해 달라는 메시지가 표시됩니다.
- **작업 없음** – 아무런 작업도 수행하지 않습니다.
- **차단** – 감지된 맬에어를 차단합니다.

Microsoft Defender 안티바이러스의 기본 작업 설정에 대한 자세한 내용은 https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#default-actions-settings를 참고하십시오.

실시간 보호

실시간 보호를 활성화해 맬웨어를 감지하고 워크로드에서 설치 또는 실행되지 않도록 방지합니다.

모든 다운로드 스캔 – 이 옵션을 선택한 경우 다운로드된 모든 파일과 첨부 파일을 스캔합니다.

행동 모니터링 활성화 – 이 옵션을 선택한 경우 행동 모니터링이 활성화됩니다.

네트워크 파일 스캔 – 이 옵션을 선택한 경우 네트워크 파일이 스캔됩니다.

매핑된 네트워크 드라이브에서 전체 스캔 허용 – 이 옵션을 선택한 경우 매핑된 네트워크 드라이브 전체가 스캔됩니다.

이메일 스캔 허용 – 활성화된 경우 메일 본문과 첨부 파일을 분석하기 위해 엔진이 사서함과 메일 파일을 특정 형식에 따라 구문 분석합니다.

Microsoft Defender 안티바이러스의 실시간 보호 설정에 대한 자세한 내용은 https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#real-time-protection-settings를 참고하십시오.

© Acronis International GmbH, 2003-2024

Advanced

고급 스캔 설정 지정:

- **아카이브 파일 스캔** – .zip 또는 .rar 파일과 같은 아카이브 파일을 스캔에 포함합니다.
- **이동식 드라이브 스캔** – 전체 스캔 중 이동식 드라이브를 스캔합니다.
- **시스템 복원 지점 생성** – 중요 파일 또는 레지스트리 항목을 "감지 오류"로 제거할 수 없는 경우 복원 지점에서 복구할 수 있습니다.
- **다음 후에 격리된 파일을 제거** – 격리된 파일을 제거하기까지 보관할 기간을 정의합니다.
- **추가 분석이 필요할 경우 자동으로 파일 샘플 전송:**
  - **항상 메시지 표시** – 파일을 전송하기 전 확인 메시지가 표시됩니다.
  - **자동으로 안전한 샘플 전송** – 개인 정보를 포함할 가능성이 있는 파일을 제외하고 대부분의 경우 자동으로 샘플이 전송됩니다. 개인 정보를 포함할 가능성이 있는 파일의 경우 추가 확인이 필요합니다.
  - **자동으로 모든 샘플 전송** – 모든 샘플이 자동으로 전송됩니다.
- **Windows Defender 바이러스 백신 GUI 비활성화** – 이 옵션을 선택한 경우 사용자는 WDA 사용자 인터페이스를 사용할 수 없습니다. Cyber Protect 콘솔을 통해 WDA 정책을 관리할 수 있습니다.
- **MAPS(Microsoft Active Protection Service)** – 잠재적 위협에 대해 어떤 대응을 선택할지 지원하는 온라인 커뮤니티입니다.
  - **MAPS에 참여하지 않겠습니다** – 감지된 소프트웨어에 대한 그 어떤 정보도 Microsoft에 전송하지 않습니다.
  - **기본 구성원 자격** – 감지된 소프트웨어에 대한 기본 정보만 Microsoft에 전송합니다.
  - **고급 구성원 자격** – 감지된 소프트웨어에 대한 보다 상세한 정보를 Microsoft에 전송합니다.

  자세한 내용은 https://www.microsoft.com/security/blog/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise/를 참고하십시오.

Microsoft Defender 안티바이러스의 고급 설정에 대한 자세한 내용은 https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settings를 참고하십시오.

제외

다음과 같이 스캔에서 제외될 파일과 폴더를 정의할 수 있습니다.

- **프로세스** – 여기에서 정의한 프로세스가 읽거나 쓰는 모든 파일이 스캔에서 제외됩니다. 프로세스의 실행 파일에 대한 전체 경로를 정의해야 합니다.
- **파일 및 폴더** – 지정한 파일과 폴더가 스캔에서 제외됩니다. 폴더 또는 파일에 대한 전체 경로나 파일 확장자를 정의해야 합니다.

Microsoft Defender 안티바이러스의 제외 설정에 대한 자세한 내용은 https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings를 참고하십시오.

© Acronis International GmbH, 2003-2024

방화벽 관리

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

방화벽 관리 기능을 사용하면 보호된 워크로드에서 방화벽 설정을 쉽게 구성할 수 있습니다.

Cyber Protect에 포함되어 있는 이 기능은 Microsoft Windows의 기본 제공 Microsoft Defender 방화벽 컴포넌트를 통해 제공됩니다. Microsoft Defender 방화벽은 워크로드에서 들어오고 나가는 승인되지 않은 네트워크 트래픽을 차단합니다.

방화벽 관리는 Microsoft Defender 방화벽이 설치된 워크로드에 대해 적용 가능합니다.

지원되는 Windows 운영 체제

방화벽 관리를 지원하는 Windows 운영 체제는 다음과 같습니다.

Windows

- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Windows Server는 지원되지 않습니다.

방화벽 관리 활성화 및 비활성화

보호 계획을 생성할 때 방화벽 관리를 활성화할 수 있습니다. 기존 보호 계획을 변경하여 방화벽 관리를 활성화하거나 비활성화할 수 있습니다.

방화벽 관리를 활성화하거나 비활성화하려면

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 다음 중 하나를 수행하여 보호 계획 패널을 엽니다.
   - 새 보호 계획을 생성하려면 보호할 머신을 선택하고 **보호**를 클릭한 다음 **계획 생성**을 클릭합니다.
   - 기존 보호 계획을 변경하려면 보호된 머신을 선택하고 **보호**를 클릭한 다음 보호 계획 이름 옆의 말줄임표(...)를 클릭하고 **편집**을 클릭합니다.
3. 보호 계획 패널에서 **방화벽 관리** 영역으로 이동한 다음 **방화벽 관리**를 활성화하거나 비활성화합니다.
4. 다음 중 하나를 수행하여 변경 사항을 적용합니다.
   - 보호 계획을 생성하는 경우 **생성**을 클릭합니다.
   - 보호 계획을 편집하는 경우 **저장**을 클릭합니다.

방화벽 관리 활성화 여부에 따라 보호 계획 패널 **방화벽 관리** 영역의 **Microsoft Defender 방화벽 상태**가 **켜짐** 또는 **꺼짐**으로 표시됩니다.

© Acronis International GmbH, 2003-2024

관리 탭에서 보호 계획 패널에 액세스할 수도 있습니다. 그러나 Cyber Protection 서비스의 모든 에디션에서 이 기능이 제공되는 것은 아닙니다.

격리

격리는 머신의 하드 디스크에 특별히 격리된 폴더로, 위협이 확산되지 않도록 바이러스 백신 및 맬웨어 방지 보호 기능이 의심스럽다고 감지한 파일이 위치하는 곳입니다.

격리를 통해 모든 머신에서 의심스럽거나 잠재적으로 위험한 파일을 검토하고 이러한 파일을 제거 또는 복원할지 선택할 수 있습니다. 격리된 파일은 머신이 시스템에서 제거되는 경우 자동으로 제거됩니다.

파일은 어떻게 격리 폴더로 이동합니까?

1. 보호 계획을 구성해 감염된 파일을 격리 폴더로 이동하기 위한 기본 작업을 정의합니다.
2. 시스템은 예약 또는 온액세스 스캔 도중 악성 파일을 감지하여 격리라는 보안 폴더로 이동합니다.
3. 시스템은 머신의 격리 목록을 업데이트합니다.
4. 파일은 보호 계획의 **다음 후의 격리된 파일을 제거** 설정에서 정의한 기간 후 격리 폴더에서 자동으로 정리됩니다.

격리된 파일 관리

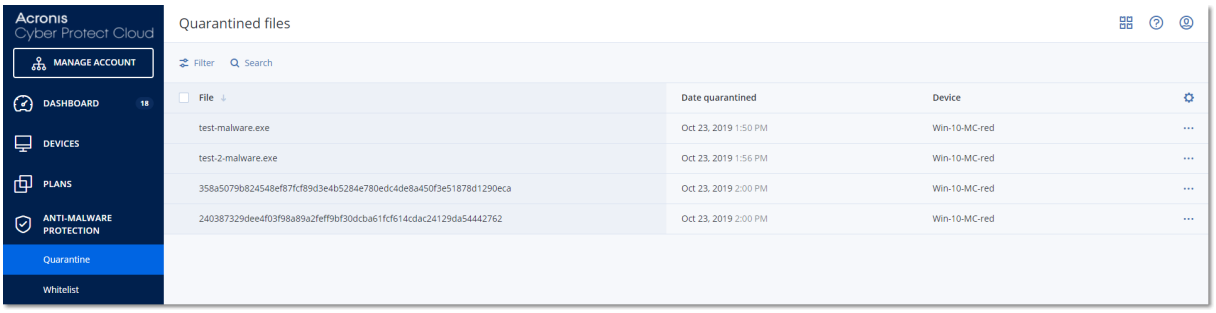
격리된 파일을 관리하려면 **맬웨어 방지 기능** > **격리**로 이동합니다. 모든 머신에서 격리된 파일 목록을 확인할 수 있습니다.

이름	설명
파일	파일 이름입니다.
격리된 날짜	파일이 격리 폴더로 이동된 날짜와 시간입니다.
장치	감염된 파일이 발견된 장치입니다.
위협 이름	위협 이름.
보호 계획	의심스러운 파일을 격리 폴더에 보관한 보호 계획입니다.

격리된 파일에 가능한 작업은 2가지입니다.

- **삭제** – 모든 머신에서 격리된 파일을 영구적으로 제거합니다. 동일한 파일 해시를 가진 모든 파일을 제거할 수 있습니다. 동일한 파일 해시를 가진 모든 파일을 복구할 수 있습니다. 해시 단위로 파일을 분류하고, 필요한 파일을 선택한 뒤 제거합니다.
- **복원** – 아무 수정 없이 원래 위치로 격리된 파일을 복원합니다. 원래 위치에 동일한 이름의 파일이 존재하면 복원된 파일이 해당 파일을 덮어씁니다. 복원된 파일은 허용 목록에 포함되며 추가 맬웨어 방지 스캔에서 제외됩니다.

© Acronis International GmbH, 2003-2024



머신의 격리 위치

격리된 파일의 기본 위치는 다음과 같습니다.

- Windows 머신용: `%programdata%\Acronis\NGMP\quarantine`
- Mac 머신용: `/Library/Application Support/Acronis/NGMP/quarantine`
- Linux 머신용: `/var/lib/Acronis/NGMP/quarantine`

격리 스토리지에는 서비스 제공업체의 자체 보호가 적용됩니다.

셀프 서비스 사용자 정의 폴더 온디맨드

워크로드에서 사용자 정의 폴더를 선택하고 컨텍스트 메뉴에서 직접 스캔할 수 있습니다.

컨텍스트 메뉴의 Cyber Protect 옵션을 사용하여 스캔에 액세스하려면

보호 계획에 안티바이러스 및 안티맬웨어가 활성화되어 있는 워크로드의 경우 스캔하려는 파일/폴더를 마우스 오른쪽 버튼으로 클릭합니다.

참고
이 옵션은 워크로드 관리자만 사용할 수 있습니다.

기업 허용 목록

안티바이러스 솔루션에서 합법적인 회사 관련 애플리케이션을 의심스러운 항목으로 식별할 수도 있습니다. 이러한 감지 오류를 방지하기 위해 신뢰할 수 있는 애플리케이션을 허용 목록에 수동으로 추가하는데, 이렇게 하려면 많은 시간이 소요됩니다.

참고
기업 허용 목록은 백업의 맬웨어 방지 스캔에 영향을 주지 않습니다.

Cyber Protection에서는 이 프로세스를 자동화할 수 있습니다. 즉, 안티바이러스 및 맬웨어 방지 보호 모듈이 백업을 스캔한 후 스캔한 데이터가 분석되며, 이를 통해 신뢰할 수 있는 애플리케이션이 허용 목록으로 이동하고 감지 오류가 방지됩니다. 또한 전사적 허용 목록을 통해 맬웨어 방지 스캔 성능이 추가로 개선됩니다.

허용 목록은 고객별로 생성되며 개별 고객의 데이터만을 기준으로 합니다.

© Acronis International GmbH, 2003-2024

허용 목록은 활성화 및 비활성화할 수 있습니다. 비활성화되어 있을 때는 허용 목록에 추가된 파일이 일시적으로 숨겨집니다.

참고
관리자 역할(예: Cyber Protection 관리자, 회사 관리자, 회사 관리자의 업무를 대행하는 파트너 관리자, 단위 관리자)이 있는 계정만이 허용 목록을 구성하고 관리할 수 있습니다. 읽기 전용 관리자 계정이나 사용자 계정은 이 기능을 사용할 수 없습니다.

허용 목록에 자동 추가

1. 최소 2개의 머신에서 백업의 클라우드 스캔을 실행합니다. 이렇게 하려면 백업 스캔 계획을 사용합니다.
2. 허용 목록 설정에서 **허용 목록 자동 생성** 스위치를 활성화합니다.

허용 목록에 수동 추가

허용 목록 자동 생성 스위치가 비활성화되어 있더라도 허용 목록에 파일을 수동으로 추가할 수 있습니다.

1. Cyber Protect 콘솔에서 **맬웨어 방지 보호** > **허용 목록**으로 이동합니다.
2. **파일 추가**를 클릭합니다.
3. 파일 경로를 지정한 다음 **추가**를 클릭합니다.

허용 목록에 격리된 파일 추가

격리된 파일을 허용 목록에 추가할 수 있습니다.

1. Cyber Protect 콘솔에서 **맬웨어 방지 보호** > **격리**로 이동합니다.
2. 격리된 파일을 선택한 다음 **허용 목록에 추가**를 클릭합니다.

허용 목록 설정

허용 목록 자동 생성 스위치를 활성화하는 경우 다음 휴리스틱 보호 수준 중 하나를 지정해야 합니다.

- **낮음**
  상당한 시간이 지나고 확인이 완료된 후에만 기업 애플리케이션을 허용 목록에 추가합니다. 이러한 애플리케이션은 신뢰도가 높습니다. 하지만 이 방식을 사용하면 감지 오류의 가능성이 커집니다. 안전하며 신뢰할 수 있는 파일이라고 판단하기까지의 기준이 높습니다.
- **기본**
  잠재적인 감지 오류를 줄이기 위해 권장 보호 수준에 따라 기업 애플리케이션을 허용 목록에 추가합니다. 안전하며 신뢰할 수 있는 파일이라고 판단하기까지의 기준이 중간 수준입니다.
- **높음**
  잠재적인 감지 오류를 줄이기 위해 기업 애플리케이션을 허용 목록에 더욱 빠르게 추가합니다. 하지만 이 방식은 소프트웨어가 안전하다는 것을 보장하지 않으며 추후 소프트웨어가 의심스

© Acronis International GmbH, 2003-2024

러운 소프트웨어나 맬웨어로 인식될 수도 있습니다. 안전하며 신뢰할 수 있는 파일이라고 판단하기까지의 기준이 낮습니다.

허용 목록의 항목 관련 상세 정보 확인

허용 목록의 항목을 클릭하면 해당 항목과 관련된 추가 정보를 확인하고 온라인에서 항목을 분석할 수 있습니다.

추가한 항목을 모르는 경우 VirtusTotal 분석기에서 항목을 확인할 수 있습니다. **VirusTotal에서 확인**을 클릭하면 해당 사이트에서는 사용자가 추가한 항목의 파일 해시를 사용하여 의심스러운 파일과 URL을 분석해 맬웨어 유형을 감지합니다. **파일 해시(MD5)** 문자열에서 해시를 확인할 수 있습니다.

머신 값은 백업 스캔 중에 해당 해시가 확인된 머신의 수를 나타냅니다. 백업 스캔 또는 격리에 포함되어 있었던 항목의 경우에만 이 값이 입력됩니다. 허용 목록에 파일을 수동으로 추가한 경우 이 필드는 비어 있는 상태로 유지됩니다.

백업 맬웨어 방지 스캔

백업의 안티맬웨어 스캔을 수행하면 백업에 맬웨어가 없는지를 확인하여 감염된 파일의 복구를 방지할 수 있습니다. Cyber Protection 데이터 센터에 있는 클라우드 에이전트가 안티맬웨어 스캔을 수행하며 로컬 컴퓨팅 리소스는 사용되지 않습니다.

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

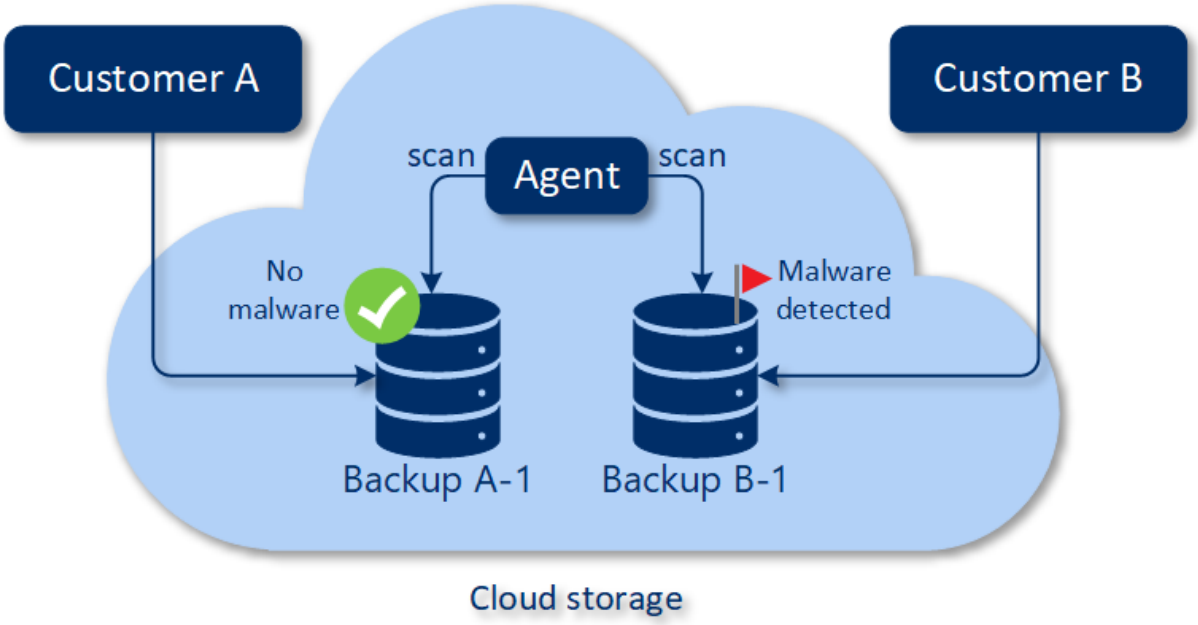
안티맬웨어 스캔을 수행하려면 백업 스캔 계획을 구성해야 합니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 "백업 스캔 계획"(184페이지) 항목을 참조하십시오.

모든 백업 스캔 계획에서는 클라우드 에이전트용 스캔 작업이 생성되어 대기열(데이터 센터당 하나씩 있음)에 추가됩니다. 스캔 작업은 대기열의 순서에 따라 처리됩니다. 그리고 스캔 시간은 백업 크기에 따라 달라집니다. 따라서 백업 스캔 계획이 생성되는 시점과 스캔이 완료되는 시점 사이에는 지연 시간이 있습니다.

스캔을 위해 선택한 백업은 다음 상태 중 하나일 수 있습니다.

- 스캔되지 않음
- 맬웨어 없음
- 맬웨어 감지됨

© Acronis International GmbH, 2003-2024



백업 스캔의 결과는 **백업 스캔 세부정보(위협)** 위젯에서 확인할 수 있습니다. 해당 위젯은 Cyber Protect 콘솔의 **모니터링** > **개요** 탭에 있습니다.

제한 사항

- 맬웨어 방지 스캔은 다음 워크로드의 **전체 머신** 또는 **디스크/볼륨** 백업에서 지원됩니다.
  - 보호 에이전트가 설치된 Windows 머신
  - Agent for Hyper-V 및 Agent for VMware(Windows)를 통해 하이퍼바이저 수준에서 백업된 Windows 가상 머신(비에이전트 백업)

  Agent for VMware(가상 어플라이언스), Agent for Virtuozzo, Agent for Scale Computing HC3 등의 가상 어플라이언스를 통해 생성된 백업에서는 맬웨어 방지 스캔이 지원되지 않습니다.
- NTFS 파일 시스템과 GPT 또는 MBR 파티셔닝을 사용하는 볼륨만 스캔됩니다.
- 기본 클라우드 스토리지만 백업 위치로 지원됩니다. 로컬 스토리지와 파트너 소유 클라우드 스토리지는 지원되지 않습니다.
- 스캔할 백업을 선택할 때는 CDP(지속적인 데이터 보호) 백업이 포함된 백업 집합을 선택할 수 있습니다. 그러나 해당 백업 집합에서 CDP가 아닌 백업만 스캔됩니다. CDP 백업에 대한 자세한 내용은 "지속적인 데이터 보호(CDP)"(372페이지) 항목을 참조하십시오.
- 전체 머신의 안전 복구를 수행할 때는 CDP 백업이 포함된 백업 집합을 선택할 수 있습니다. 그러나 CDP 백업의 데이터는 이 복구 작업에 사용되지 않습니다. CDP 데이터를 복구하려면 **파일/폴더** 복구 작업을 추가로 실행하십시오.

© Acronis International GmbH, 2003-2024

고급 보호 기능 사용

Cyber Protect에는 기본적으로 대다수 사이버 보안 위협을 방지하는 기능이 포함되어 있습니다. 이러한 기능은 추가 비용 없이 사용할 수 있습니다. 또한 고급 기능을 활성화하여 워크로드 보호 수준을 높일 수 있습니다.

- 사용 가능한 Advanced Protection 기능의 경우 보호 계획에서 고급 기능 아이콘 이 표시됩니다.
- Advanced 보호 기능을 사용할 수 없는 경우 관리자에게 문의하여 필요한 Advanced 보호 팩을 활성화하십시오.
- 관리자가 추가 보안 팩 구매 기능을 활성화한 경우에는 고급 기능을 선택하여 활성화할 수 있습니다. 이 경우 추가 요금이 청구된다는 메시지가 화면에 표시됩니다.

참고
기능을 하나 이상 활성화하는 경우 해당하는 Advanced Protection 팩을 구매해야 합니다.

참고
보호 계획에서 모든 고급 기능을 비활성화하면 해당 Advanced Protection 팩도 비활성화됩니다.

Advanced Protection 팩	Advanced Protection 기능
Advanced Backup	워크로드를 지속적으로 보호하고 작업의 마지막 순간 변경 사항이 손실되지 않도록 보장합니다. 기능에는 다음이 포함됩니다. • 원클릭 복구 • 지속적인 데이터 보호 • Microsoft SQL Server 클러스터 및 Microsoft Exchange 클러스터의 백업 지원 - Always On 가용성 그룹(AAG) 및 데이터베이스 가용성 그룹(DAG) • MariaDB, MySQL, Oracle DB 및 SAP HANA의 백업 지원 • 데이터 보호 맵 및 규제 준수 보고 • 오프호스트 데이터 처리 • Microsoft 365 및 Google Workspace 워크로드의 백업 빈도 • 부트 가능한 미디어를 사용한 원격 작업 • Microsoft Azure 퍼블릭 클라우드 스토리지에 직접 백업
Advanced Security + EDR	모든 맬웨어 위협으로부터 워크로드를 지속적으로 보호합니다. 기능에는 다음이 포함됩니다. • 중앙 집중식 인시던트 페이지에서 인시던트 관리 • 인시던트의 범위와 영향 시각화 • 권장 사항 및 수정 단계 • 위협 피드를 사용하여 워크로드와 관련해 공개된 공격 확인 • 180일 동안 보안 이벤트 저장 • 로컬 서명 기반 감지 기능이 포함된 안티바이러스 및 안티맬웨어 보호(실시간 보호

© Acronis International GmbH, 2003-2024

	기능 제공) • 악용 방지 • URL 필터링 • 엔드포인트 방화벽 관리 • 포렌식 백업, 맬웨어 대비 백업 스캔, 안전 복구, 기업 허용 목록 • 스마트 보호 계획(CPOC 경보와의 통합) • 중앙 집중식 맬웨어 스캔 • 원격 지우기 • Windows Defender 안티바이러스 • Microsoft Security Essentials
Advanced Management	보호된 워크로드에서 취약점을 패치할 수 있도록 합니다. 기능에는 다음이 포함됩니다. • 패치 관리 • 디스크 상태 • 소프트웨어 인벤토리 • 유사시 대기 패칭 • Cyber Scripting • 원격 지원 • 파일 전송 및 공유 • 연결할 세션 선택 • 다중 보기에서 워크로드 관찰 • 연결 모드: 제어, 보기 전용 및 커튼 • 빠른 지원 애플리케이션을 통한 연결 • 원격 연결 프로토콜: NEAR 및 Apple 화면 공유 • NEAR 연결을 위한 세션 녹화 • 스크린샷 전송 • 세션 내역 보고서 • 모니터 24개 • 임계값 기반 모니터링 • 이상 현상 기반 모니터링
Advanced Data Loss Prevention	보호된 워크로드에서 민감한 정보의 유출을 방지합니다. 기능에는 다음이 포함됩니다. • 주변 장치 및 네트워크 통신을 통한 워크로드의 데이터 손실 콘텐츠 인식 방지 • PII(개인 식별 정보), PHI(개인 건강 정보), PCI DSS(결제 카드 산업 데이터 보안 표준) 데이터 및 "기밀로 표시됨" 카테고리의 문서에 대한 사전 구축된 자동 탐지 • 선택적 최종 사용자 지원을 통한 자동 데이터 손실 방지 정책 생성 • 자동 학습 기반 정책 조정을 통한 적응형 데이터 손실 방지 적용 • 클라우드 기반 중앙 집중식 감사 로깅, 경보 및 최종 사용자 알림

Advanced Data Loss Prevention

© Acronis International GmbH, 2003-2024

Advanced Data Loss Prevention 모듈은 보호된 워크로드에서 데이터 전송 내용과 상황을 분석하며, 데이터 플로우 정책에 따라 회사 네트워크 내외에서 주변 장치 또는 네트워크 전송을 통한 민감한 데이터 유출을 방지합니다.

이 고객에 대해 보호 서비스 및 Advanced Data Loss Prevention 팩을 사용하도록 설정한 경우 고객 테넌트에 대한 보호 계획에 Advanced Data Loss Prevention 기능을 포함할 수 있습니다.

Advanced Data Loss Prevention 모듈을 사용하기 전에 기본 가이드에 설명된 고급 DLP 관리의 기본 개념과 논리를 읽고 이해했는지 확인해야 합니다.

기술 사양 문서를 검토할 수도 있습니다.

데이터 플로우 정책 및 정책 규칙 생성

데이터 손실 방지의 핵심 원칙은 기업 IT 시스템 사용자가 업무 수행에 필요한 범위 내에서만 민감한 데이터를 처리할 수 있도록 허용해야 한다는 것입니다. 비즈니스 프로세스와 무관한 다른 민감한 데이터 전송은 차단되어야 합니다. 따라서 비즈니스 관련 데이터 전송과 악성 데이터 전송 또는 플로우를 구분하는 것이 중요합니다.

데이터 플로우 정책에는 허용되는 데이터 플로우와 금지된 데이터 플로우를 지정하는 규칙이 포함되어 있으므로 데이터 손실 방지 모듈이 보호 계획에서 활성화되고 적용 모드로 실행될 때 민감한 정보의 무단 전송을 방지합니다.

정책의 각 민감도 카테고리에는 별표(*)로 표시된 하나의 기본 규칙과 특정 사용자 또는 그룹에 대한 데이터 플로우를 정의하는 하나 이상의 명시적(기본값이 아닌) 규칙이 포함됩니다. 정책 규칙 유형에 관한 자세한 내용은 기본 가이드를 참조하시기 바랍니다.

데이터 플로우 정책은 일반적으로 Advanced Data Loss Prevention이 관찰 모드로 실행되는 동안 자동으로 생성됩니다. 대표적인 데이터 플로우 정책을 구축하는 데 걸리는 시간은 약 1개월이지만 조직의 비즈니스 프로세스에 따라 다를 수 있습니다. 데이터 플로우 정책은 회사 또는 부서 관리자가 수동으로 생성, 구성 또는 편집할 수도 있습니다.

데이터 플로우 정책 자동 생성을 시작하려면

1. Cyber Protect 콘솔에 관리자로 로그인합니다.
2. **관리** > **보호 계획**으로 이동합니다.
3. **계획 생성**을 클릭합니다.
4. **데이터 손실 방지** 섹션을 확장하고 **모드** 행을 클릭합니다.

© Acronis International GmbH, 2003-2024

5. 모드 대화창에서 **관찰 모드**를 선택하고 데이터 전송을 처리하는 방법을 선택합니다.

옵션	설명
모두 허용	사용자 워크로드에서 모든 민감한 데이터의 전송은 비즈니스 프로세스에 필요한 것으로 간주되고 안전하게 처리됩니다. 정책에 이미 정의된 규칙과 일치하지 않는 탐지된 모든 데이터 플로우에 대해 새 규칙이 생성됩니다.
모두 정당화	사용자 워크로드에서 민감한 데이터의 모든 전송은 비즈니스 프로세스에 필요한 것으로 간주되지만, 위험합니다. 따라서 이전에 생성된 데이터 플로우 규칙과 일치하지 않는 조직 내외부의 수신자 또는 대상으로 가로챈 민감한 데이터 전송의 경우, 사용자는 일회성 비즈니스 정당화를 제공해야 합니다. 정당화가 제출되면 데이터 플로우 정책에 새 데이터 플로우 규칙이 생성됩니다.
혼합	모든 내부 민감한 데이터 플로우에 대해 모든 허용 로직이 적용되고 모든 외부 데이터 플로우에 대해 모든 정당화 로직이 적용됩니다. **참고** 내부 및 외부 데이터에 대한 자세한 내용은 대상 자동 감지를 참조하십시오.

6. 보호 계획을 저장하고 정책을 빌드하기 위해 데이터를 수집할 워크로드에 적용합니다.

참고
관찰 모드 중에는 데이터 유출이 방지되지 않습니다.

데이터 플로우 정책을 수동으로 구성하려면

1. Cyber Protect 콘솔에서 **보호 > 데이터 플로우 정책**으로 이동합니다.
2. **새 데이터 플로우 규칙**을 클릭합니다.
   오른쪽에 새 데이터 플로우 규칙 창이 확장됩니다.
3. 민감도 카테고리를 선택하고 발신자 및 수신자를 추가한 다음 선택한 범주, 발신자 및 수신자에 대한 데이터 전송 권한을 정의합니다.

옵션	설명
허용	이 발신자가 이 민감도 카테고리의 데이터를 이 수신자에게 전송할 수 있도록 허용합니다.
예외	이 발신자가 이 민감도 카테고리의 데이터를 이 수신자에게 전송하도록 허용하지 않지만, 발신자가 특정 전송에 대한 규칙에 예외를 제출하도록 허용합니다. 이 발신자가 이 민감도 카테고리의 데이터를 이 수신자에게 전송하려고 할 때 전송을 차단하고 이 전송을 허용하는 예외를 제출하도록 발신자에게 요청합니다. 예외가 제출되면 데이터 전송을 계속할 수 있습니다.

© Acronis International GmbH, 2003-2024

옵션	설명
	중요 이 민감도 카테고리에 관한 이 발신자와 수신자 간의 이후 모든 데이터 전송은 예외가 제출된 후 5분 동안 허용됩니다.
거부	이 발신자가 이 민감도 카테고리의 데이터를 이 수신자에게 전송하도록 허용하지 않으며, 발신자가 규칙에 대한 예외를 요청하도록 허용하지 않습니다.

4. (선택사항) 규칙이 트리거될 때 실행할 작업을 선택합니다.

작업	설명
로그에 쓰기	규칙이 트리거될 때 감사 로그에 이벤트 기록을 저장합니다. **예외** 권한이 있는 규칙에 대해 이 작업을 선택하는 것이 좋습니다.
경보 생성	규칙이 트리거될 때 Cyber Protect **경보** 탭에서 경보를 생성합니다. 관리자 알림이 활성화된 경우 이메일 알림도 전송됩니다.
데이터 전송이 거부되면 최종 사용자에게 알림	규칙을 트리거할 때 화면상의 경고를 통해 사용자에게 실시간으로 알립니다.

5. **저장**을 클릭합니다.
6. 2~5단계를 반복하여 서로 다른 민감도 카테고리 및 옵션의 규칙을 여러 개 생성하고 결과 규칙이 선택한 옵션에 해당하는지 확인합니다.

데이터 플로우 정책 구조

데이터 플로우 정책 보기에서 정책 규칙은 정책 규칙이 제어하는 민감한 데이터 카테고리에 따라 그룹화됩니다. 민감도 카테고리 식별자는 정책 규칙 그룹 바로 위에 표시됩니다.

- 민감함
  - PHI(개인 건강 정보)
  - PII(개인 식별 정보)
  - PCI DSS(결제 카드 산업 데이터 보안 표준)
  - 기밀로 표시됨
- 민감하지 않음

데이터 플로우 정책의 개념 및 기능에 대한 자세한 내용은 기본 가이드를 참조하시기 바랍니다.

규칙 구조

각 정책 규칙은 다음 요소로 구성됩니다.

- **민감도 카테고리**
  - **PHI(개인 건강 정보)**
  - **PII(개인 식별 정보)**
  - **PCI DSS(결제 카드 산업 데이터 보안 표준)**

© Acronis International GmbH, 2003-2024

  - **기밀로 표시됨**

    "민감한 데이터 정의"(800페이지)을(를) 참조하십시오.
- **발신자** - 이 규칙에 의해 제어되는 데이터 전송의 시작자를 지정합니다. 이는 단일 사용자, 사용자 목록 또는 사용자 그룹일 수 있습니다.
  - **모든 내부** - 조직의 모든 내부 사용자가 포함된 사용자 그룹입니다.
  - **연락처 / 발신 조직** - 조직에서 Advanced Data Loss Prevention으로 인식되는 Windows 계정과 지정된 Windows 계정이 이전에 사용했던 기타 모든 계정(서드 파티 통신 애플리케이션이 사용했던 계정 포함)입니다.
  - **연락처 / 사용자 지정 ID** - 이메일, Skype ID, ICQ 식별자, IRC 식별자, Jabber 이메일, Mail.ru 에이전트 이메일, Viber 휴대폰번호, Zoom 이메일 형식 중 하나로 지정된 내부 사용자의 식별자입니다.

    연락처 그룹을 지정하는 데 사용할 수 있는 와일드 카드는 다음과 같습니다.
    - ***** - 모든 수의 기호
    - **?** - 모든 단일 기호
- **수신자** - 이 규칙에 의해 제어되는 데이터 전송의 대상을 지정합니다. 이는 단일 사용자, 사용자 목록 또는 사용자 그룹 및 아래에 지정된 다른 유형의 대상일 수 있습니다.
  - **모두** - 고급 DLP에서 지원하는 수신자 유형입니다.
  - **연락처 / 모든 연락처** - 내부 또는 외부 연락처입니다.
  - **연락처/모든 내부 연락처** - 내부 사용자의 모든 연락처입니다("대상 자동 감지"(799페이지) 참조).
  - **연락처 / 모든 외부 연락처** - 외부 개인 또는 엔티티의 모든 연락처입니다.
  - **연락처 / 발신 조직** - 발신자 필드에 설명된 것과 동일한 원리입니다.
  - **연락처 / 사용자 지정 ID** - 발신자 필드에 설명된 것과 동일한 원리입니다.
  - **파일 공유 서비스** - 제어된 파일 공유 서비스의 식별자입니다.
  - **소셜 네트워크** - 제어된 소셜 네트워크의 식별자입니다.
  - **호스트 / 모든 호스트** - 고급 DLP에서 내부 또는 외부로 인식되는 모든 컴퓨터입니다.
  - **호스트 / 모든 내부 호스트** - 고급 DLP에서 내부로 인식되는 모든 컴퓨터입니다.
  - **호스트 / 모든 외부 호스트** - 고급 DLP에서 외부로 인식되는 모든 컴퓨터입니다.
  - **호스트 / 특정 호스트** - 호스트 이름(예: FQDN) 또는 IP 주소(IPv4 또는 IPv6)로 지정된 컴퓨터 식별자입니다.
  - **장치 / 모든 장치** - 워크로드에 연결된 모든 주변 디바이스입니다.
  - **장치/외부 스토리지** - 워크로드에 연결된 이동식 스토리지 또는 리디렉션된 매핑된 드라이브입니다.
  - **장치/암호화된 이동식** - BitLocker To Go로 암호화된 이동식 스토리지 장치
  - **장치 / 리디렉션된 클립보드** - 워크로드에 연결된 리디렉션된 클립보드입니다.
  - **프린터** - 워크로드에 연결된 모든 로컬 또는 네트워크 프린터입니다.
- **권한** - 이 규칙에 의해 제어되는 데이터 전송에 대한 예방적 제어가 적용됩니다. 데이터 플로우 정책 규칙의 권한 항목에 자세히 설명되어 있습니다.
- **작업** - 이 규칙이 트리거될 때 수행되는 비예방적 작업입니다. 기본적으로 이 필드는 "작업 없음"으로 설정됩니다. 옵션은 다음과 같습니다.

© Acronis International GmbH, 2003-2024

- **로그에 쓰기** - 규칙이 트리거될 때 감사 로그에 이벤트 기록을 저장합니다.
- **데이터 전송이 거부될 때 최종 사용자에게 알림** - 규칙을 트리거할 때 실시간 화면 경고를 사용자에게 알립니다.
- **경보 생성** - 규칙이 트리거될 때 관리자에게 경고합니다.

경고!
작업 없음을 선택하면 규칙이 트리거됩니다.
- 감사 로그에 이벤트 레코드가 추가되지 않습니다.
- 관리자에게 경보가 전송됩니다.
- 최종 사용자에게 화면 알림이 표시됩니다.

정책 규칙을 트리거하는 요소는?

다음 조건이 모두 해당되는 경우 데이터 전송은 데이터 플로우 정책 규칙과 일치합니다.

- 이 데이터 전송의 모든 발신자가 나열되거나 규칙의 **발신자** 필드에 지정된 사용자 그룹에 속해 있습니다.
- 이 데이터 전송의 모든 수신자가 나열되거나 규칙의 **수신자** 필드에 지정된 사용자 그룹에 속해 있습니다.
- 전송되는 데이터가 규칙의 **민감도 카테고리**와 일치합니다.

데이터 플로우 정책 규칙의 권한 조정

Advanced Data Loss Prevention은 데이터 플로우 정책 규칙에서 세 가지 유형의 권한을 지원합니다. 권한은 정책의 각 규칙에서 개별적으로 구성됩니다.

허용 (허용)
규칙에 정의된 민감도 카테고리, 발신자 및 수신자의 조합과 일치하는 데이터 전송이 허용됩니다.

예외 (금지)
규칙에 정의된 민감도 카테고리, 발신자 및 수신자의 조합과 일치하는 데이터 전송은 허용되지 않지만 발신자는 규칙에 예외를 제출하여 특정 전송을 허용할 수 있습니다.

중요
이 민감도 카테고리에 관한 이 발신자와 수신자 간의 이후 모든 데이터 전송은 예외가 제출된 후 5분 동안 허용됩니다.

거부 (금지)
규칙에 정의된 민감도 카테고리, 발신자 및 수신자의 조합과 일치하는 데이터 전송은 허용되지 않으며 발신자는 예외를 제출할 수 있는 옵션이 없습니다.

또한 정책 관리의 유연성을 높이기 위해 **허용** 및 **예외** 권한에 우선 순위 플래그를 할당할 수 있습니다. 이 설정을 사용하면 정책의 다른 데이터 플로우 규칙에 있는 특정 그룹에 대해 설정된 권한을 재정의할 수 있습니다. 사용자는 그룹 데이터 플로우 규칙을 일부 멤버에만 적용할 수 있습니다. 이를 수행하려면 그룹 규칙에서 제외할 특정 사용자에 대한 데이터 플로우 규칙을 생성한 다음 해당 사용자가 속한 그룹의 규칙에 구성된 데이터 플로우 제한보다 해당 사용자의 권한에 우선 순

© Acronis International GmbH, 2003-2024

위를 지정해야 합니다. 규칙 결합 시 권한 우선 순위에 대한 내용은 "데이터 플로우 정책 규칙 결합"(793페이지)을(를) 참조하시기 바랍니다.

중요
회사 또는 부서 정책을 관찰 모드에서 적용 모드로 전환하기 전에 각 민감한 데이터 카테고리에 대한 기본 규칙을 허용에서 금지 상태로 조정하는 것이 중요합니다. 기본 규칙은 **데이터 플로우 정책** 보기에서 별표(*)로 표시됩니다. 정책 규칙 유형에 관한 자세한 내용은 기본 가이드를 참조하시기 바랍니다.

정책 규칙에서 권한을 편집하려면

1. Cyber Protect 콘솔에 관리자로 로그인합니다.
2. **보호** > **데이터 플로우 정책**으로 이동합니다.
3. 편집할 정책 규칙을 선택하고 규칙 목록 위에 있는 **편집**을 클릭합니다.
   데이터 플로우 규칙 편집 창이 열립니다.
4. **권한** 섹션에서 **허용**, **예외** 또는 **거부**를 선택합니다.
5. (선택사항) 이 규칙의 **허용** 또는 **예외** 권한에 다른 규칙의 권한보다 우선 순위를 지정하려면 **우선 순위 지정** 확인란을 선택합니다.
   데이터 플로우 규칙은 기본적으로 정책에서 가장 낮은 우선 순위를 가지므로 기본 모두 > 기타 규칙보다 우선 순위를 지정하기 위해 이 확인란을 사용할 필요는 없습니다.
   규칙 결합 시 권한 우선 순위에 대한 내용은 "데이터 플로우 정책 규칙 결합"(793페이지)을(를) 참고하시기 바랍니다.
6. (선택사항) 규칙이 트리거될 때 실행할 작업을 선택합니다.
7. 정책 규칙의 변경 내용을 저장합니다.

데이터 플로우 정책 규칙 결합

데이터 전송이 둘 이상의 규칙과 일치하면 모든 규칙에 대해 구성된 사용 권한과 작업이 다음과 같이 결합되고 적용됩니다.

권한

데이터 전송이 둘 이상의 규칙과 일치하고 이러한 규칙이 동일한 데이터 카테고리에 대해 서로 다른 권한을 갖는 경우, 다음 권한 우선 순위 목록(내림차순)에 따라 우선 순위가 높은 규칙이 적용됩니다.

1. **우선 순위가 지정된** 플래그에 대한 예외
2. **우선 순위가 지정된** 플래그를 사용하여 허용
3. 거부
4. 예외
5. 허용

데이터 전송이 둘 이상의 규칙과 일치하고 이러한 규칙에 서로 다른 데이터 카테고리에 대한 권한이 있는 경우 재정의에 다음 로직이 적용됩니다.

© Acronis International GmbH, 2003-2024

1. 가장 제한적인 규칙 권한은 데이터 전송과 일치하는 각 민감도 범주에 대해 정의됩니다.
2. 지점 1에 정의된 규칙 권한 중 가장 제한적인 권한이 적용됩니다.

예

파일 전송은 다음과 같이 서로 다른 민감도 카테고리의 세 가지 규칙과 일치합니다.

민감도 카테고리	권한
PII	허용 - 우선 순위가 지정됨
PHI	예외 - 우선 순위가 지정됨
PCI	거부

거부 권한이 적용됩니다.

작업

데이터 전송이 둘 이상의 규칙과 일치하고 이러한 규칙에 **작업** 필드에 구성된 옵션이 서로 다른 경우 트리거된 모든 규칙에서 구성된 모든 작업이 수행됩니다.

정책 검토 및 관리

자동으로 생성된 기본 데이터 플로우 정책을 시행하기 전에 클라이언트에 의해 검토, 검증 및 승인이 이루어져야 합니다. 이는 클라이언트가 비즈니스 프로세스의 모든 세부 사항을 본질적으로 알고 있으며 기본 정책에서 일관되게 해석되는지 여부를 평가할 수 있기 때문입니다. 또한, 클라이언트는 부정확한 부분을 식별하여 파트너 관리자가 해당 부분을 수정할 수 있습니다.

정책 검토 중에 파트너 관리자는 기본 데이터 플로우 정책을 고객에게 제시합니다. 클라이언트는 정책의 각 데이터 플로우를 검토하고 비즈니스 프로세스와의 일관성을 확인합니다. Cyber Protect 콘솔의 정책 규칙 표현은 직관적으로 명확하므로 유효성 검사에는 기술이 필요하지 않습니다. 각 규칙은 민감한 데이터 플로우의 발신자 및 수신자를 설명합니다.

파트너 관리자는 클라이언트의 지침에 따라 데이터 플로우 정책 규칙을 편집, 삭제 및 생성하여 기준 정책을 수동으로 조정합니다. 클라이언트의 승인을 받은 후, 검토된 정책은 이러한 워크로드에 적용되는 보호 계획을 적용 모드로 전환하여 보호된 워크로드에 적용됩니다.

검토된 정책을 적용하기 전에 민감한 데이터 카테고리에 대해 자동으로 생성된 모든 기본 정책 규칙에서 **허용** 권한을 **거부** 또는 **예외**로 변경하는 것이 중요합니다. **거부** 권한은 사용자가 재정의할 수 없지만 **예외** 권한은 규칙과 일치하는 전송을 차단하지만 비상 상황에서는 비즈니스 관련 예외를 제출하여 차단을 재정의할 수 있습니다.

데이터 플로우 정책 갱신

회사 또는 부서의 비즈니스 프로세스가 크게 변경될 경우 업데이트된 비즈니스 프로세스의 민감한 데이터 플로우의 변화와 일관되도록 DLP 정책을 갱신해야 합니다. 직원의 직무 역할이 변경된 경우에도 정책 갱신이 필요합니다. 이 경우, 직원의 워크로드를 보호하는 데 사용되는 부서 정책의 일부도 갱신해야 합니다.

© Acronis International GmbH, 2003-2024

관리자는 고급 DLP 정책 관리 워크플로를 사용하여 전체 회사, 부서, 사용자 또는 부서의 일부 사용자에 대한 정책 갱신을 자동화할 수 있습니다.

회사 또는 부서에 대한 정책 갱신

관찰 모드의 모든 옵션을 사용하여 회사 정책 또는 부서 전체 정책을 갱신하고 부서에 있는 한 명 이상의 사용자에 대한 부서 정책의 일부를 갱신할 수 있습니다.

회사 또는 부서에 대한 정책을 갱신하려면

갱신 프로세스는 회사 관리자 또는 회사 워크로드를 관리하는 파트너가 수행해야 하는 다음 단계로 구성됩니다.

1. 적용된 정책에서 기본이 아닌 모든 규칙을 삭제합니다.
2. 갱신을 시작하려면 회사 또는 부서에 적용된 고급 DLP로 보호 계획을 특정 회사 또는 장치에 가장 적합한 옵션에 따라 관찰 모드 옵션 중 하나로 전환한 다음, 회사 또는 부서의 모든 워크로드에 계획을 적용합니다.
3. 갱신 기간이 끝나면 클라이언트와 함께 새 회사 또는 부서 정책을 검토하고 필요한 경우 조정하여 고객의 승인을 받습니다.
4. 회사 또는 부서 워크로드에 적용되는 보호 계획을 적절한 적용 모드 옵션으로 전환합니다. 이 옵션은 클라이언트가 부서 워크로드에서 데이터가 누출되는 것을 방지하는 데 최적이라고 간주하는 것이어야 합니다.

회사 또는 부서에 있는 한 명 이상의 사용자에 대한 정책 갱신

사용자 수준 정책은 관찰 모드 옵션과 적응적 적용 모드를 사용하여 갱신할 수 있습니다.

관찰 모드를 사용하여 사용자 정책 갱신

회사(또는 부서)의 사용자 또는 일부 사용자에 대한 정책 갱신을 위해 관찰 모드를 사용하는 경우, 전체 회사(또는 부서)에 대해 시행되는 데이터 플로우 정책은 갱신 기간 동안 사용자의 데이터 전송에 적용되지 않습니다. 따라서 갱신 중에 회사(또는 부서)에 대해 시행되는 정책의 기존 그룹 규칙과 모순되거나 일치할 수 있는 사용자에 대한 새 개별 규칙을 만들 수 있습니다. 갱신이 완료되고 정책이 사용자의 데이터 전송에 대해 다시 적용된 후, 사용자를 위해 만들어진 이러한 새로운 개별 규칙이 사용자의 데이터 전송에 실제로 적용되는지 여부는 이러한 데이터 전송이 일치하는 정책의 다른 규칙과 비교하여 우선 순위에 따라 달라집니다.

관찰 모드를 통해 사용자에 대한 정책을 갱신하려면

갱신 프로세스는 회사 관리자 또는 회사 워크로드를 관리하는 파트너가 수행해야 하는 다음 단계로 구성됩니다.

1. 사용자가 단일 발신자인 회사(또는 부서)에 대해 시행되는 정책에서 기본이 아닌 모든 규칙을 삭제합니다.
2. 적용된 정책의 기본이 아닌 모든 데이터 플로우 규칙의 발신자 목록에서 사용자를 제거합니다.
3. 관찰 모드에서 고급 DLP를 사용하여 새 보호 계획을 만들고 사용자의 워크로드에 적용하여 갱신(관찰) 기간을 시작합니다.

© Acronis International GmbH, 2003-2024

갱신 기간은 사용자가 워크로드에서 민감한 데이터를 전송하는 일반 비즈니스 활동의 전부 또는 90~95%를 수행하는 데 걸리는 시간에 따라 달라집니다.

4. 갱신 기간이 끝나면 적용 정책에 추가된 이 사용자와 관련된 새 규칙을 검토하고 필요한 경우 규칙을 조정한 후 클라이언트의 승인을 받습니다.
5. 사용자의 워크로드에 적용된 보호 계획을 클라이언트가 사용자 워크로드에서 데이터 유출을 방지하기 위해 최적으로 고려하는 옵션에 따라 **엄격한 적용** 모드 또는 **적응적 적용** 모드로 전환합니다.
   또는 회사(혹은 부서)에 적용된 보호 계획을 사용자의 워크로드에 다시 적용할 수 있습니다.

적응적 적용 모드를 사용하여 사용자 정책 갱신

단일 사용자 또는 회사(또는 부서)의 모든 사용자의 일부에 대한 정책 갱신은 사용자의 워크로드에 고급 DLP가 적용된 보호 계획의 적응적 적용 모드를 사용하여 수행할 수 있습니다.

참고
이 정책 갱신 방법에는 다음과 같은 세부사항이 있습니다. 사용자의 구성원 자격(예: 모든 내부 구성원 자격)을 가진 발신자 그룹에 대해 시행되는 회사(부서) 정책 규칙도 갱신 중에 이 사용자의 데이터 전송에 적용됩니다. 따라서 갱신은 발신자 그룹에 대해 이미 존재하는 정책 규칙과 모순되거나 일치하는 사용자에 대한 새 개별 규칙을 만들지 않습니다. 다음 두 가지 방법 중 특정 IT 보안 요구사항에 따라 특정 클라이언트의 사용자 정책 갱신에 더 효과적인 방법

적응적 적용 모드를 통해 사용자에 대한 정책을 갱신하려면

갱신 프로세스는 회사 관리자 또는 회사 워크로드를 관리하는 파트너가 수행해야 하는 다음 단계로 구성됩니다.

1. 사용자가 단일 발신자인 회사(부서)에 대해 시행되는 정책에서 기본이 아닌 모든 규칙을 삭제합니다.
2. 적용된 정책의 기본이 아닌 모든 데이터 플로우 규칙의 발신자 목록에서 사용자를 제거합니다.
3. 회사(또는 부서)에 대해 적용되는 정책의 모든 기본 규칙에 대해 해당 권한을 **예외**로 설정하고 **작업** 필드에서 **로그에 쓰기** 작업을 선택합니다.
4. 현재 사용자 워크로드에 적용된 보호 계획이 **엄격한 적용** 모드로 설정된 경우, 고급 DLP를 사용하여 새 보호 계획을 생성하고 **적응적 적용** 모드의 사용자 워크로드에 적용하여 갱신 기간을 시작합니다.
   갱신 기간은 사용자가 워크로드에서 민감한 데이터를 전송하는 일반 비즈니스 활동의 전부 또는 90~95%를 수행하는 데 걸리는 시간에 따라 달라집니다.
5. 갱신 기간이 끝나면 적용 정책에 추가된 이 사용자와 관련된 새 규칙을 검토하고 필요한 경우 규칙을 조정한 후 클라이언트의 승인을 받습니다.
6. 사용자의 워크로드에 적용된 보호 계획을 **엄격한 적용** 모드로 전환하거나, 클라이언트가 사용자 워크로드에서 데이터 유출을 방지하기 위해 최적으로 고려하는 옵션에 따라 **적응적 적용** 모드로 유지합니다.
   또는 회사(혹은 부서)에 적용된 보호 계획을 사용자의 워크로드에 다시 적용할 수 있습니다.

보호 계획에서 Advanced Data Loss Prevention 활성화

© Acronis International GmbH, 2003-2024

이 고객에 대해 보호 서비스 및 Advanced Data Loss Prevention 팩을 사용하도록 설정한 경우 고객 테넌트에 대한 보호 계획에 Advanced Data Loss Prevention 기능을 포함할 수 있습니다.

고급 DLP는 데이터 손실 방지 기능 그룹의 고급 모듈입니다. 고급 DLP 기능과 장치 제어는 독립적으로 사용하거나 함께 사용할 수 있습니다(단일 보호 계획에서 또는 동일한 워크로드를 보호하는 두 개의 계획에서). 함께 사용할 경우 해당 기능은 다음과 같이 조정됩니다.

- 장치 제어는 고급 DLP가 전송된 데이터의 내용을 검사하는 로컬 채널에 대한 사용자 액세스를 제어하는 것을 중단합니다. 그러나 장치 제어는 다음과 같이 읽기 전용 또는 액세스 거부로 설정된 장치 유형에 대한 제어는 유지합니다.
  - 이동식
  - 암호화된 이동식
  - 매핑된 드라이브

  예를 들어 단일 보호 계획 또는 동일한 워크로드를 보호하는 두 개의 계획에서 장치 제어와 고급 DLP를 모두 활성화한 경우 및 장치 제어에서 USB 장치에 대해 읽기 전용 액세스를 설정한 경우, 고급 DLP 모듈의 액세스 설정에 관계없이 읽기 전용 액세스는 허용 목록에 있는 것들을 제외한 모든 USB 장치에 적용됩니다 만약 기본값인 액세스 활성화가 장치 제어에서 설정된 경우, 고급 DLP의 액세스 설정이 적용됩니다.
- 허용 목록의 다음 로컬 채널 및 주변에 대한 사용자 액세스는 장치 제어에 의해 시행됩니다.
  - 광학 드라이브
  - 플로피 드라이브
  - MTP 연결 모바일 장치
  - Bluetooth 어댑터
  - Windows 클립보드
  - 스크린샷 캡처
  - USB 장치 및 장치 유형(이동식 스토리지 및 암호화된 장치 제외)

고급 DLP로 보호 계획을 생성하려면

1. **관리** > **보호 계획**으로 이동합니다.
2. **계획 생성**을 클릭합니다.
3. **데이터 손실 방지** 섹션을 확장하고 **모드** 행을 클릭합니다.
   모드 대화창을 엽니다.
   - 데이터 플로우 정책의 생성 또는 갱신을 시작하려면 **관찰 모드**를 선택하고 데이터 전송을 처리하는 방법을 선택합니다.

옵션	설명
모두 허용	사용자 워크로드에서 모든 민감한 데이터의 전송은 비즈니스 프로세스에 필요한 것으로 간주되고 안전하게 처리됩니다. 정책에 이미 정의된 규칙과 일치하지 않는 탐지된 모든 데이터 플로우에 대해 새 규칙이 생성됩니다.
모	사용자 워크로드에서 민감한 데이터의 모든 전송은 비즈니스 프로세스에 필요한 것으로

© Acronis International GmbH, 2003-2024

옵션	설명
두 정당화	간주되지만, 위험합니다. 따라서 이전에 생성된 데이터 플로우 규칙과 일치하지 않는 조직 내외부의 수신자 또는 대상으로 가로챈 민감한 데이터 전송의 경우, 사용자는 일회성 비즈니스 정당화를 제공해야 합니다. 정당화가 제출되면 데이터 플로우 정책에 새 데이터 플로우 규칙이 생성됩니다.
혼합	민감한 데이터의 모든 내부 전송에 모든 허용 로직이 적용되고 민감한 데이터의 모든 외부 전송에 모든 정당화 로직이 적용됩니다. 내부 대상에 대한 정의는 "대상 자동 감지"(799페이지)을(를) 참조하시기 바랍니다.

경고!

- **관찰 모드**는 데이터 플로우 정책이 생성되지 않았거나 정책을 갱신하는 경우에만 선택해야 합니다. 정책 갱신을 시작하기 전에 "데이터 플로우 정책 갱신"(794페이지)을(를) 참조하십시오.
- 관찰 모드에서는 데이터 유출이 방지되지 않습니다. 기본 가이드의 관찰 모드를 참조하십시오.

- 기존 데이터 플로우 정책을 적용하려면 **적용 모드**를 선택한 다음 데이터 플로우 정책 규칙을 적용하는 정도를 선택합니다.

옵션	설명
엄격한 적용	데이터 플로우 정책이 그대로 적용되며 이전에 관찰되지 않은 민감한 데이터 플로우가 탐지될 경우 새 허용 정책 규칙으로 확장되지 않습니다. 기본 가이드의 엄격한 적용을 참조하십시오.
적응적 적용(학습을 통해 적용)	시행되는 정책은 관찰 기간 동안 수행되지 않은 비즈니스 작업 또는 비즈니스 프로세스 변경에 대해 자동으로 계속 적응합니다. 이 모드를 사용하면 적용된 데이터 플로우 정책을 워크로드에서 발견된 새로 학습된 데이터 플로우를 기반으로 확장할 수 있습니다. 기본 가이드의 적응적 적용을 참조하십시오.

중요

회사 또는 부서 정책을 관찰 모드에서 적용 모드로 전환하기 전에 각 민감한 데이터 카테고리에 대한 기본 규칙을 허용에서 금지 상태로 조정하는 것이 중요합니다. 기본 규칙은 **데이터 플로우 정책** 보기에서 별표(*)로 표시됩니다. 정책 규칙 유형에 관한 자세한 내용은 기본 가이드를 참조하시기 바랍니다.

4. **완료**를 클릭하여 모드 대화창을 닫습니다.
5. (선택사항) 광학식 문자 인식, 허용 목록 및 기타 보호 옵션을 구성하려면 **고급 설정**을 클릭합니다.
   사용 가능한 옵션에 대한 자세한 내용은 "고급 설정"(799페이지)을(를) 참조하십시오.
6. 보호 계획을 저장하고 보호하려는 워크로드에 적용합니다.

© Acronis International GmbH, 2003-2024

고급 설정

Advanced Data Loss Prevention과 함께 보호 계획에서 고급 설정을 사용하여 Advanced Data Loss Prevention가 제어하는 채널의 데이터 콘텐츠 검사 품질을 높일 수 있으며, 모든 예방 제어에서 허용 목록에 있는 애플리케이션에 의해 시작된 데이터 전송뿐만 아니라 허용 목록의 주변 장치 유형, 네트워크 통신 범주, 대상 호스트를 제외할 수 있습니다. 사용자는 다음 고급 설정을 구성할 수 있습니다.

- **광학 문자 인식**
  이 설정은 문서, 메시지, 스캔, 스크린샷 및 기타 개체의 그래픽 파일 및 이미지에서 추가 내용 검사를 위해 31개 언어로 된 텍스트 조각을 추출하기 위해 광학 문자 인식(OCR)을 설정하거나 해제합니다.
- **비밀번호로 보호된 데이터 전송**
  비밀번호로 보호된 아카이브 및 문서의 내용은 검사할 수 없습니다. 이 설정을 사용하여 관리자는 고급 DLP를 사용하여 암호로 보호된 데이터의 나가는 전송을 허용할지 차단할지 선택할 수 있습니다.
- **오류 발생 시 데이터 전송 차단**
  간혹 전송 중인 내용을 분석하는 데 실패하거나 DLP 에이전트 작업에서 다른 제어 오류가 발생할 수 있습니다. 이 옵션이 활성화되어 있으면 전송이 차단됩니다. 이 옵션이 활성화되어 있으면 오류가 발생하더라도 전송이 허용됩니다.
- **장치 유형 및 네트워크 통신에 대한 허용 목록**
  이 목록에서 확인된 주변 장치 유형 및 네트워크 통신 유형으로의 데이터 전송은 데이터 민감도 및 적용된 데이터 플로우 정책에 관계없이 허용됩니다.

  경고!
  이 옵션은 특정 장치 유형 또는 프로토콜과 관련된 문제가 발생할 경우 사용됩니다. 지원 담당자의 지시가 없으면 이를 활성화하지 마십시오.

- **원격 호스트에 대한 허용 목록**
  이 목록에 지정된 대상 호스트로의 데이터 전송은 데이터 민감도 및 적용된 데이터 플로우 정책에 관계없이 허용됩니다.
- **애플리케이션에 대한 허용 목록**
  이 목록에 지정된 애플리케이션에서 수행한 데이터 전송은 데이터 민감도 및 적용된 데이터 플로우 정책에 관계없이 허용됩니다.

보호 계획 생성 보기 및 보호 계획의 "세부 정보" 보기에 표시되는 고급 설정의 **보안 수준** 표시기에는 다음과 같은 수준 표시 로직이 있습니다.

- **기본**은 켜진 고급 설정이 없음을 나타냅니다.
- **보통**은 둘 이상의 설정이 켜져 있지만 **OCR**, **비밀번호로 보호된 데이터 전송** 및 **오류 발생 시 데이터 전송 차단**의 조합이 활성화되지 않았음을 나타냅니다.
- **엄격**은 **OCR**, **비밀번호로 보호된 데이터 전송** 및 **오류 시 데이터 전송 방지 설정** 이상의 조합이 활성화되었음을 나타냅니다.

대상 자동 감지

© Acronis International GmbH, 2003-2024

혼합 관찰 모드에서 Advanced Data Loss Prevention은 감지된 데이터 전송의 대상(내부 또는 내부)에 따라 다른 규칙을 적용합니다. 대상을 내부로 결정하는 로직은 아래에 설명되어 있습니다. 다른 모든 대상은 외부로 간주됩니다.

가로챈 각 데이터 전송에 대해 Advanced Data Loss Prevention은 DNS 요청을 수행하고 데이터 손실 방지 에이전트가 실행되는 머신과 원격 서버의 FQDN 이름을 비교하여 대상 HTTP, FTP 또는 SMB 서버가 내부인지 여부를 자동으로 탐지합니다. DNS 요청이 실패하면 보호된 워크로드와 원격 서버가 동일한 네트워크에 있는지 여부도 확인합니다. 데이터 손실 방지 에이전트가 실행되는 머신과 도메인 이름이 같거나 하위 네트워크에 있는 서버는 내부 서버로 간주됩니다.

이메일 통신의 경우 Advanced Data Loss Prevention은 수신자 전자 메일이 발신자 이메일과 동일한 도메인에 있고 수신자 이메일 서버 이름이 동일한 경우 회사 메일 서버를 사용하여 회사 이메일 서버에서 보낸 모든 이메일을 내부 전송으로 처리합니다.

수신자 계정을 알 수 없는 한 회사 이메일이 아닌 이메일은 외부 통신으로 간주됩니다. 데이터 손실 방지가 네트워크의 사용자 활동을 모니터링하고 백엔드의 데이터베이스를 사용자와 연결된 이메일 주소의 데이터로 업데이트하면 알려진 이메일 주소가 업데이트됩니다.

수신자 계정을 알 수 없는 한 메신저를 통한 통신은 외부 통신으로 간주됩니다. 데이터 손실 방지가 네트워크의 사용자 활동을 모니터링하고 백엔드의 데이터베이스를 사용자와 연결된 계정의 데이터로 업데이트하면 알려진 계정이 업데이트됩니다.

민감한 데이터 정의

이 항목에서는 내용 분석 중에 민감한 데이터를 식별하는 로직에 대해 설명합니다.

가양성의 수를 줄이기 위해 동일한 일치 항목이 설명된 논리식의 모든 그룹에 대해 하나의 일치 항목으로 계산됩니다.

중요
내용 식별에 사용되는 논리식은 정보 제공용으로만 제공되며 솔루션에 대해 자세히 설명하지는 않습니다.

PHI(개인 건강 정보)

지원되는 언어

- 미국, 영국, 국제 영어
- 핀란드어
- 이탈리아어
- 프랑스어
- 폴란드어
- 러시아어
- 헝가리어
- 노르웨이어
- 스페인어

© Acronis International GmbH, 2003-2024

개인 건강 정보로 간주되는 데이터

다음 데이터는 개인 건강 정보로 간주됩니다.

- 이름 및 성
- 주소(거리, 시, 군, 구, 우편번호 및 이에 상응하는 지오코드)
- 휴대폰 번호
- 이메일 주소
- 사회 보장 번호
- 의료 보험 수혜자 번호
- 은행 계좌번호
- URL
- IP 주소 번호
- ICD-10-CM 코드
- ICD-10-PCS-and-GEMs
- HIPAA
- 기타 의료 관련
- 신용 카드 번호

내용 탐지에 사용되는 논리식

논리식은 논리 연산자 OR에 의해 결합되는 다음 문자열로 구성됩니다. AND 논리 연산자가 명시적으로 지정되지 않은 경우 OR 연산자는 위의 목록에서 다른 데이터 그룹을 결합하는 데 사용됩니다. 괄호 안의 숫자는 양의 탐지 결과를 반환하는 탐지된 인스턴스 수를 나타냅니다.

- **사회 보장 번호** (5)
- (이름 및 성 (3) OR 주소 (3) OR 전화번호 (3) OR 이메일 주소 (3) OR 은행 계좌번호 (3) OR 신용 카드 번호 (3)) AND (사회 보장 번호 (3) OR 의료 보험 수혜자 번호 (3) * OR ICD-10-CM 코드 (3) OR ICD-10-PCS-and-GEMs (3) OR HIPAA (3) OR * 기타 의료 관련 정보 (3))

PII(개인 식별 정보)

지원되는 언어

- 미국, 영국, 국제 영어
- 불가리아어
- 중국어
- 체코어
- 덴마크어
- 네덜란드어
- 핀란드어
- 프랑스어
- 독일어

© Acronis International GmbH, 2003-2024

- 헝가리어
- 인도네시아어
- 이탈리아어
- 한국어
- 말레이시아어
- 노르웨이어
- 폴란드어
- 포르투갈어(브라질)
- 포르투갈어(포르투갈)
- 루마니아어
- 러시아어
- 세르비아어
- 싱가포르
- 스페인어
- 스웨덴어
- 타이완
- 튀르키예어
- 태국어
- 일본어

PII(개인 식별 정보)로 간주되는 데이터

- 이름 및 성
- 주소(거리, 시, 군, 구, 우편번호)
- 은행 계좌번호
- 개인 및 회계 ID 번호
- 여권 번호
- 사회 보장 번호
- 휴대폰 번호
- 자동차 번호
- 운전면허증 번호
- 식별자 및 일련 번호
- IP 주소
- 이메일 주소
- 신용 카드 번호

내용 탐지에 사용되는 논리식

일본어를 제외한 지원되는 모든 언어에 대한 논리식

논리식은 논리 연산자 OR 및 AND에 의해 결합되는 다음 문자열로 구성됩니다. 괄호 안의 숫자는 양의 탐지 결과를 반환하는 탐지된 인스턴스 수를 나타냅니다.

© Acronis International GmbH, 2003-2024

- 개인 및 회계 ID 번호 (5)
- 이름 및 성 (3) AND **(**신용 카드 번호 (3) OR 사회 보장 번호 (3) OR 은행 계좌번호 (3) OR 개인 및 회계 ID 번호 (3) OR 운전면허증 번호 (3) OR 여권 번호 (3) OR 사회 보장 번호 (3) OR IP 주소 (3) OR 자동차 번호 (3) OR 식별자 및 일련 번호**)**
- 휴대폰 번호 (3) AND **(**신용 카드 번호 (3) OR 사회 보장 번호 (3) OR 은행 계좌번호 (3) OR 주소 (3) OR 개인 및 회계 ID 번호 (3) OR 운전면허증 번호 (3) OR 여권 번호 (3) OR 사회 보장 번호 (3) OR 자동차 번호 (3) OR 식별자 및 일련 번호 (3)**)**
- **(**이름 및 성 (30) OR 주소 (30)**)** AND **(**이메일 주소 (30) OR 전화번호 (30) OR IP 주소 (30)**)**
- 이메일 주소 (3) AND **(**신용 카드 번호 (3) OR 사회 보장 번호 (3) OR 은행 계좌번호 (3) OR 개인 및 회계 ID 번호 (3) OR 운전면허증 번호 (3) OR 여권 번호 (3) OR 사회 보장 번호 (3) OR 자동차 번호 (3) OR 식별자 및 일련 번호 (3)**)**
- 이메일 주소 (30) AND **(**주소 (30) OR 휴대폰 번호 (30)**)**
- 이름 및 성 (30) AND 주소 (30)
- 휴대폰 번호 (30) AND 주소 (30)
- 이름 및 성 (3) AND 은행 계좌번호 (3)
- 휴대폰 번호 (3) AND **(**신용 카드 번호 (3) OR 은행 계좌번호 (3) OR 사회 보장 번호 (3) OR 개인 및 회계 ID 번호 (3) OR 운전면허증 번호 (3) OR 여권 번호 (3)**)**

일본어 논리식

참고
고유한 일치 항목만 내용 탐지에 의해 계산됩니다.

논리식은 논리 연산자 OR에 의해 결합되는 다음 문자열로 구성됩니다. 논리 연산자 AND가 명시적으로 지정되지 않은 경우 연산자 OR은 다른 그룹을 결합하는 데 사용됩니다.

- 사회 보장 번호 (5)
- 이름 및 성 (3) AND **(**신용 카드 번호 (3) OR 은행 계좌번호 (3) OR 운전면허증 번호 (3) OR 여권 번호 (3) OR 사회 보장 번호 (3)**)**
- 이름 및 성 (30) AND **(**이메일 주소 (30) OR 휴대폰 번호 (30) OR IP 주소 (30) OR 주소 (30)**)**
- 주소 (3) AND **(**신용 카드 번호 (3) OR 은행 계좌번호 (3) OR 운전면허증 번호 (3) OR 여권 번호 (3) OR 사회 보장 번호 (3)**)**
- 이메일 주소 (3) AND **(**신용 카드 번호 (3) OR 은행 계좌번호 (3) OR 사회 보장 번호 (3) OR 운전면허증 번호 (3)**)**
- 주소 (5) AND **(**이메일 주소 (5) OR 이름 및 성 (5) OR 휴대폰 번호 (5) OR IP 주소 (5)**)**
- 이름 및 성 (3) AND 은행 계좌번호 (3)
- 휴대폰 번호 (3) AND **(**신용 카드 번호 (3) OR 은행 계좌번호 (3) OR 주소 (3) OR 사회 보장 번호 (3) OR 운전면허증 번호 (3)**)**

PCI DSS(결제 카드 산업 데이터 보안 표준)

지원되는 언어

이 민감도 그룹은 언어 독립적입니다. PCI DSS 데이터는 모든 국가에서 영어로 제공됩니다.

© Acronis International GmbH, 2003-2024

PCI DSS로 간주되는 데이터

- 카드 소유자 데이터
  - 기본 계정 번호(PAN)
  - 카드 소유자 성명
  - 만료일
  - 서비스 코드
- 민감한 인증 데이터
  - 전체 트랙 데이터(자기대 데이터 또는 칩의 동등한 데이터)
  - CAV2/CVC2/CVV2/CID
  - PIN/PIN 블록

내용 탐지에 사용되는 논리식

논리식은 논리 연산자 OR에 의해 결합되는 다음 문자열로 구성됩니다. 괄호 안의 숫자는 양의 탐지 결과를 반환하는 탐지된 인스턴스 수를 나타냅니다.

- 신용 카드 번호 (5)
- 신용 카드 번호 (3) AND (미국 이름 (Ex) (3) OR 미국 이름 (3) OR PCI DSS 키워드 (3) OR 날짜(월/년) (3))
- 신용 카드 덤프 (5)

기밀로 표시됨

기밀로 표시된 데이터는 키워드 그룹을 통해 탐지됩니다.

일치 조건은 가중치 기반이며 모든 단어는 가중치 == 1입니다. 가중치가 > 3인 경우 내용 탐지는 양으로 간주됩니다.

지원되는 언어

- 영어
- 불가리아어
- 중국어 간체
- 중국어 번체
- 체코어
- 덴마크어
- 네덜란드어
- 핀란드어
- 프랑스어
- 독일어
- 헝가리어
- 인도네시아어
- 이탈리아어

© Acronis International GmbH, 2003-2024

- 일본어
- 한국어
- 말레이시아어
- 노르웨이어
- 폴란드어
- 포르투갈어 - 브라질
- 포르투갈어 - 포르투갈
- 러시아어
- 세르비아어
- 스페인어
- 스웨덴어
- 튀르키예어

키워드 그룹

각 언어의 키워드 그룹에는 영어(대문자와 소문자를 구분하지 않음)에 사용되는 다음 키워드와 같은 국가별 키워드가 포함됩니다.

- 기밀
- 내부 배포
- 배포용이 아님
- 배포 금지
- 공용이 아님
- 외부 배포용이 아님
- 내부 사용 전용
- 매우 제한적인 문서
- 비공개
- 권한이 필요한 정보
- 내부 사용 전용
- 공무 사용 전용

데이터 손실 방지 이벤트

Advanced Data Loss Prevention은 다음과 같이 DLP 이벤트 보기에서 이벤트를 생성합니다.

- 관찰 모드 중에는 모든 정당화된 데이터 전송에 대한 이벤트가 생성됩니다.
- 적용 모드에서는 트리거되는 각 정책 규칙에 대해 구성된 **로그에 쓰기** 작업에 따라 이벤트가 생성됩니다.

데이터 플로우 정책에서 규칙에 대한 이벤트를 보려면

1. Cyber Protect 콘솔에 관리자로 로그인합니다.
2. **보호** > **데이터 플로우 정책**으로 이동합니다.

© Acronis International GmbH, 2003-2024

3. 이벤트를 볼 규칙을 찾고 규칙 줄 끝에 있는 말줄임표를 클릭합니다.
4. **이벤트 보기**를 선택합니다.

DLP 이벤트 보기에서 이벤트에 대한 상세 정보를 보려면

1. Cyber Protect 콘솔에 관리자로 로그인합니다.
2. **보호** > **DLP 이벤트**로 이동합니다.
3. 자세한 내용을 보려면 목록에서 이벤트를 클릭합니다.
   이벤트 상세정보 창이 오른쪽으로 확장됩니다.
4. 이벤트 상세정보 창에서 아래로 스크롤하고 위로 스크롤하여 사용 가능한 정보를 확인합니다.
   창에 표시되는 상세정보는 이벤트를 트리거한 규칙 및 규칙 설정 유형에 따라 달라집니다.

DLP 이벤트 목록에서 이벤트를 필터링하려면

1. Cyber Protect 콘솔에 관리자로 로그인합니다.
2. **보호** > **DLP 이벤트**로 이동합니다.
3. 왼쪽 상단에서 **필터**를 클릭합니다.
4. 드롭다운 메뉴에서 민감도 카테고리, 워크로드, 작업 유형, 사용자 및 채널을 선택합니다.
   드롭다운 메뉴에서 둘 이상의 항목을 선택할 수 있습니다. 필터링은 동일한 메뉴의 항목 간에 논리 연산자 OR을 적용하지만 논리 연산자 AND는 다른 메뉴의 항목 간에 사용됩니다.
   예를 들어 **PHI** 및 **PII** 민감도 카테고리를 선택하는 경우, 결과는 PHI 또는 PII 또는 둘 모두를 포함하는 모든 이벤트를 반환합니다. 민감도 카테고리 **PHI** 및 작업 **쓰기 액세스**를 선택하는 경우, 두 범주와 일치하는 이벤트만 필터링된 결과에 표시됩니다.
5. **적용**을 클릭합니다.
6. 모든 이벤트를 다시 보려면 **필터**를 클릭한 다음 **기본값으로 재설정**하고 마지막으로 **적용**을 클릭합니다.

DLP 이벤트 목록에서 이벤트를 검색하려면

1. 위의 절차에 따라 1~2단계를 반복합니다.
2. 필터 오른쪽에 있는 드롭다운 목록에서 검색할 카테고리를 선택합니다. **발신자**, **대상**, **프로세스**, **메시지 제목** 또는 **이유**.
3. 텍스트 상자에 관심 있는 문구를 입력하고 키보드에서 Enter 키를 눌러 확인합니다.
   입력한 문구와 일치하는 이벤트만 목록에 나타납니다.
4. 이벤트 목록을 재설정하려면 검색 텍스트 상자에서 **X** 기호를 클릭하고 Enter 키를 누릅니다.

데이터 플로우 정책의 특정 규칙과 관련된 이벤트 목록을 보려면

1. Cyber Protect 콘솔에 관리자로 로그인합니다.
2. **보호** > **데이터 플로우 정책**으로 이동합니다.
3. 관심 있는 정책 규칙 이름 앞에 있는 확인란을 선택합니다.
   필요한 경우 여러 정책 규칙을 선택할 수 있습니다.
4. **이벤트 보기**를 클릭합니다.
   보기가 **보호**>**DLP 이벤트**로 전환되고 선택한 정책 규칙과 관련된 이벤트가 목록에 나타납니다.

개요 대시보드의 Advanced Data Loss Prevention 위젯

© Acronis International GmbH, 2003-2024

개요 대시보드에서는 Advanced Data Loss Prevention를 비롯하여 Cyber Protection 서비스와 관련된 작업의 개요를 알려주는 사용자 정의 가능한 다양한 위젯을 제공합니다. 다음과 같은 Advanced Data Loss Prevention 위젯은 **모니터링**의 **개요** 대시보드에서 찾을 수 있습니다.

- **민감한 데이터 전송** - 내부 및 외부 수신자에 대한 총 민감한 데이터 전송 작업 수를 표시합니다. 차트는 권한 유형(허용됨, 정당화됨 또는 차단됨)으로 구분됩니다. 사용자는 원하는 기간(1일, 7일, 30일 또는 이번 달)을 선택하여 위젯을 사용자 정의할 수 있습니다.
- **아웃바운드 민감한 데이터 카테고리** - 외부 수신자에게 전송된 총 민감한 데이터 수를 표시합니다. 차트가 민감한 카테고리인 PHI(개인 건강 정보), PII(개인 식별 정보), PCI DSS 및 기밀로 표시됨(기밀)으로 구분됩니다.
- **아웃바운드 민감한 데이터의 상위 발신자** - 조직에서 외부 수신자에게 전송한 총 민감한 데이터 전송 수와 함께 전송 수가 가장 많은 상위 5명 사용자 목록을 표시합니다. 이 통계에는 허용된 전송과 정당화된 전송이 모두 포함됩니다. 사용자는 원하는 기간(1일, 7일, 30일 또는 이번 달)을 선택하여 위젯을 사용자 정의할 수 있습니다.
- **차단된 중요 데이터 전송의 상위 발신자** - 차단된 총 민감한 데이터 전송 수와 함께 전송 수가 가장 많은 상위 5명의 사용자 목록을 표시합니다. 사용자는 원하는 기간(1일, 7일, 30일 또는 이번 달)을 선택하여 위젯을 사용자 정의할 수 있습니다.
- **최근 DLP 이벤트** - 선택한 시간 범위에서 발생한 최근 데이터 손실 방지 이벤트 상세정보를 표시합니다. 다음 옵션을 사용하여 이 위젯을 사용자 정의할 수 있습니다.
  - **범위(게시 날짜)**(1일, 7일, 30일 또는 이번 달)
  - **워크로드**의 이름
  - **작업 상태**(허용됨, 정당화됨 또는 차단됨)
  - **민감도** (PHI, PII, 기밀, PCI DSS)
  - **대상 유형**(외부, 내부)
  - **그룹화** (워크로드, 사용자, 채널, 대상 유형)

위젯은 5분마다 업데이트됩니다. 위젯에는 조사할 수 있고 문제를 해결할 수 있는 클릭 가능한 요소가 있습니다. 대시보드의 현재 상태를 다운로드하거나 이메일을 통해 .pdf 및/또는 .xlsx 형식으로 보낼 수 있습니다.

사용자 정의 민감도 카테고리

조직에서는 사용자 정의 민감한 데이터 카테고리를 활용하여 해당 조직과 관련된 지적 재산 및 기밀 데이터를 보호할 수 있습니다. 규제 준수 규정 관련 내용 정의가 포함된 Advanced DLP 기본 제공 카탈로그를 확장하면 됩니다.

사용자 정의 민감도 카테고리를 생성하려면

1. Cyber Protect 콘솔에 관리자로 로그인합니다.
2. **보호** > **데이터 손실 방지** > **데이터 분류자**로 이동합니다.
3. **민감도 카테고리**를 선택합니다.
4. 기본 제공 민감도(예: 개인 건강 정보, 개인 식별 정보)와 사용자 정의 민감도가 모두 포함된 민감도 목록이 표시됩니다.
5. 창 오른쪽 위의 **민감도 생성**을 클릭합니다.

© Acronis International GmbH, 2003-2024

6. 다음 창에 민감도의 이름을 입력합니다.
7. 새로 생성하는 사용자 정의 민감도는 기본적으로 항상 비활성화됩니다. 모든 매개변수를 구성한 후 사용자 정의 민감도를 활성화할 수 있습니다.
8. 새 민감도를 생성한 후에는 민감도의 내용 감지기를 설정해야 합니다. 화살표를 클릭하여 새 민감도의 내용을 확장하고 **내용 감지기 추가**를 선택합니다.
9. 다음 창에서 기존 내용 감지기 이름 옆의 확인 표시를 클릭하고 오른쪽 아래의 **추가**를 클릭하여 기존 내용 감지기를 사용할 수도 있고 새 내용 감지기를 정의할 수도 있습니다.
10. 새 민감도를 처음부터 생성하는 대신 기존 민감도(기본 제공 민감도 또는 기존 사용자 정의 민감도)를 복제한 다음 매개변수를 조정하여 재사용할 수도 있습니다.
    - 기존 민감도를 복제하려면 민감도 이름 옆의 확인 표시를 클릭한 다음 왼쪽 위의 말줄임표로 표시된 작업 드롭다운 메뉴에서 **복제**를 선택합니다. 한 번에 여러 항목을 선택해 여러 민감도를 복제할 수 있습니다.
    - 다음 창에서는 기존 민감도의 각 매개변수 옆에 있는 확인 표시를 클릭하여 보존할 매개변수를 선택할 수 있습니다.

참고
특정 테넌트 내에서 기본 제공 민감도를 복사하면 같은 감지기가 포함된 새 민감도가 생성됩니다. 이렇게 복사한 민감도는 사용자 정의 민감도가 됩니다

새 내용 감지기를 생성하려면

1. Cyber Protect 콘솔에 관리자로 로그인합니다.
2. **보호** > **데이터 손실 방지** > **데이터 분류자**로 이동합니다.
3. **내용 감지기**를 선택합니다.
4. 기본 제공 내용 감지기와 사용자 정의 내용 감지기가 모두 포함된 내용 감지기 목록이 표시됩니다.
5. 창 오른쪽 위의 **내용 감지기 생성**을 클릭합니다.
6. 그러면 열리는 드롭다운 메뉴에서 생성할 감지기 유형을 선택할 수 있습니다. 현재는 **파일 형식** 내용 감지기만 사용 가능하며 향후 업데이트에서 내용 감지기가 추가로 제공될 예정입니다.
7. 다음 창에서 내용 감지기를 구성할 수 있습니다.

내용 감지기의 유형	설명
파일 형식	a. 이 창에는 **지원되는 파일 형식** 및 **선택한 파일 형식**의 2개 목록이 있습니다. 지원되는 파일 형식 오른쪽의 "더하기" 아이콘을 클릭하면 해당 파일 형식이 선택한 파일 형식 목록으로 옮겨집니다. 지원되는 파일 형식 여러 개를 선택할 수도 있습니다. 지원되는 파일 형식 이름 옆의 확인 표시를 클릭한 다음 오른쪽 위의 **선택한 항목 추가** 버튼을 사용하면 됩니

© Acronis International GmbH, 2003-2024

내용 감지기의 유형	설명
내용 감지기	다. b. 선택한 파일 형식 목록에서 특정 파일 형식을 제거하려면 해당 파일 형식 이름 오른쪽의 휴지통 아이콘을 클릭합니다. 확인 표시와 **선택한 항목 제거** 버튼을 사용해 여러 파일 형식을 한꺼번에 제거할 수도 있습니다.
키워드 내용 감지기	a. 새 키워드 내용 감지기를 생성할 때는 파일에서 키워드를 가져와야 합니다. 키워드를 정상적으로 가져온 후에는 새 키워드를 기존 키워드 목록과 병합하거나 기존 키워드를 가져온 키워드로 대체할 수 있습니다. b. 내용 감지기가 일치 여부를 확인하도록 할 대상(목록의 모든 키워드, 목록 내 임의의 키워드, 사용자 정의 개수만큼의 키워드)도 결정해야 합니다.

8. 새 내용 감지기를 처음부터 생성하는 대신 기존 내용 감지기(기본 제공 내용 감지기 또는 기존 사용자 정의 내용 감지기)를 복제한 다음 매개변수를 조정하여 재사용할 수도 있습니다.
   - 기존 내용 감지기를 복제하려면 내용 감지기 이름 옆의 확인 표시를 클릭한 다음 왼쪽 위의 말줄임표로 표시된 작업 드롭다운 메뉴에서 **복제**를 선택합니다. 한 번에 여러 항목을 선택해 여러 내용 감지기를 복제할 수 있습니다.

참고
기본 제공 내용 감지기를 복사하면 사용자 정의 감지기가 생성됩니다.

조직 매핑

참고
이 기능은 회사 관리자 사용자만 액세스할 수 있습니다.

조직 맵은 사용자 및 해당하는 모든 계정에 대한 데이터를 포함하는 데이터베이스로, 인스턴트 메시징, 이메일 또는 다른 수단을 통해 데이터 전송이 Advanced DLP에 의해 가로채진 경우에 사용됩니다.

조직 맵은 Advanced DLP에서 사용자 그룹을 생성하고 관리하는 수단 및 Advanced DLP에서 사용자와 사용자에 연결된 사용자 계정을 관리하는 수단을 제공합니다. 그런 다음 사용자 그룹은 그룹 기반 DLP 정책 관리에 사용될 수 있습니다.

조직 맵의 위치를 찾는 방법

© Acronis International GmbH, 2003-2024

- Cyber Protect Cloud 콘솔에서, **보호** > **데이터 손실 방지** > **조직 맵**으로 이동합니다.

작업의 원리는 다음과 같습니다.

참고
조직 맵은 Advanced DLP 모듈이 관찰 모드에서 작동하는 동안 채워집니다.

DLP 에이전트가 가로챈 모든 데이터 전송에 대해 다음의 속성들이 백엔드에서 수집됩니다.

속성	설명	UI에서의 레이블
조직 단위	수동으로 생성된 그룹입니다. 조직 단위는 하나 이상의 중첩된 조직 단위를 가질 수 있습니다.	그룹 이름, 정의에 따름
보안 ID	고유한 보안 식별자입니다.	사용자 세부 정보 페이지 > **SID**의 경우
	사용자 친화적인 표시 이름은 사용자의 계정 이름에서 파생됩니다. 이 이름은 항상 조직 맵에서 사용할 수 있는 것은 아닙니다.	**이름**
PC\사용자 이름	엔드포인트(워크로드)의 사용자 이름입니다. 사용자 이름은 조직 단위 하나에만 할당될 수 있습니다.	**사용자 이름**
장치(워크로드)	엔드포인트(워크로드)의 이름입니다.	**워크로드**
계정	사용자가 인스턴트 메시징 및 이메일을 통한 커뮤니티에 사용되었던 계정을 DLP 에이전트가 가로챘습니다. 예를 들어 에이전트가 사용자 이름 'PC\John'이 john@gmail.com을 사용하여 이메일을 보내는 것을 감지한 경우 이 계정은 PC\John 사용자 이름에 연결됩니다.	**계정**

조직 맵에서는 계정, 사용자 및 그룹을 보고 검색할 수 있으며, 그룹을 생성, 편집 및 삭제할 수 있습니다.

특정 계정을 검색하는 방법

인시던트 조사의 일부로 관리자 사용자는 잠재적 데이터 위반과 관련된 특정 계정의 소유자를 찾아야 할 수도 있습니다.

1. Cyber Protect Cloud 콘솔에서, **보호** > **데이터 손실 방지** > **조직 맵**으로 이동합니다.
2. 사용자 목록 위의 **검색** 텍스트 상자에서 계정을 입력하거나 붙여넣기를 시작합니다.
   입력할 때마다 목록이 필터링됩니다.

특정 사용자 이름을 검색하는 방법

© Acronis International GmbH, 2003-2024

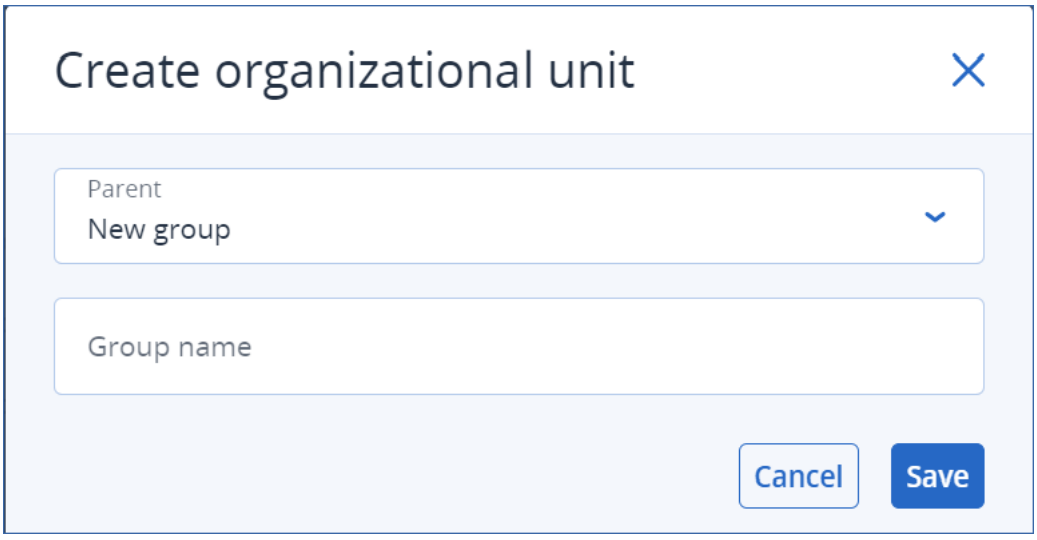
1. Cyber Protect Cloud 콘솔에서, **보호** > **데이터 손실 방지** > **조직 맵**으로 이동합니다.
2. 특정 그룹에서 검색하려면 목록에서 그룹 이름을 클릭합니다.
3. 사용자 목록 위의 **검색** 텍스트 상자에서 사용자 이름을 입력하거나 붙여넣기를 시작합니다.
   입력할 때마다 목록이 필터링됩니다.

특정 사용자 이름으로 사용된 계정을 보는 방법

1. 사용자 목록에서 사용자의 위치를 찾습니다.
2. 사용자 행의 끝에 있는 세 개의 점을 클릭하고 **보기**를 선택합니다.
3. 사용자 세부 정보 대화 상자에서 **연결된 계정** 섹션을 찾습니다.
4. 설명 텍스트 상자에 주석을 추가할 수 있습니다.

사용자 그룹을 생성하는 방법

1. Cyber Protect Cloud 콘솔에서, **보호** > **데이터 손실 방지** > **조직 맵**으로 이동합니다.
2. 그룹 목록의 왼쪽 하단 섹션에서 **그룹 생성**을 클릭합니다.
   조직 단위 생성 대화 상자가 열립니다.



3. 상위 드롭다운 메뉴에서 새 그룹의 컨텍스트를 선택합니다.

   참고
   상위 항목은 나중에 변경할 수 없습니다. 그룹은 이 컨텍스트에서 중첩된 상태로 남게 됩니다.

4. 그룹 이름을 입력하고 **저장**을 클릭합니다.

그룹에 사용자를 추가하는 방법

1. Cyber Protect Cloud 콘솔에서, **보호** > **데이터 손실 방지** > **조직 맵**으로 이동합니다.
2. 사용자 목록에서 추가하려는 사용자를 찾고 사용자 행의 시작 부분에 있는 확인란을 선택합니다.
   선택 항목 이동 버튼과 **선택 항목 삭제** 버튼이 사용자 목록 위에 표시됩니다.

3. **선택 항목 이동**을 클릭합니다.
   이동 사용자 대화 상자가 열립니다.

© Acronis International GmbH, 2003-2024

4. 선택한 사용자에 대해 새로운 상위를 선택하고 **저장**을 클릭합니다.

참고
사용자는 하나의 그룹에만 속할 수 있습니다.

사용자와 연결된 계정을 삭제하는 방법

1. 사용자 목록에서 사용자의 위치를 찾습니다.
2. 사용자 행의 끝에 있는 세 개의 점을 클릭하고 **보기**를 선택합니다.
3. 사용자 세부 정보 대화 상자에서 **연결된 계정** 섹션을 찾습니다.
4. 삭제하려는 계정을 찾고 그 옆에 있는 세 개의 점을 클릭합니다.
5. 드롭다운 목록에서 **삭제**를 선택합니다.

사용자 그룹의 이름을 변경하는 방법

1. Cyber Protect Cloud 콘솔에서, **보호** > **데이터 손실 방지** > **조직 맵**으로 이동합니다.
2. 그룹의 이름 옆에 있는 세 개의 점을 클릭하고 **이름 변경**을 클릭합니다.

사용자 그룹을 삭제하려면

1. Cyber Protect Cloud 콘솔에서, **보호** > **데이터 손실 방지** > **조직 맵**으로 이동합니다.
2. 그룹의 이름 옆에 있는 세 개의 점을 클릭하고 **삭제**를 클릭합니다.
   그룹의 모든 사용자가 상위 엔티티로 이동되었습니다.

알려진 문제 및 제한 사항

- [DEVLOCK-4028] Zoom 데스크탑 에이전트에 그룹 채팅용 제어 기능이 없습니다.
- [DEVLOCK-4016] 초안 생성 시 GMX 웹 메일 및 Web.de 메일에서 이름과 보내는 사람 ID가 캡처되지 않습니다.
- [DEVLOCK-4447] 초안 생성 시 naver.com 웹 메일에 양쪽 맞춤 대화 상자가 표시되지 않습니다.
- [DEVLOCK-1033] DeviceLockDriver: IRP_MN_QUERY_DEVICE_RELATIONS 처리 중의 교착으로 인해 버그 가능성 검사 DRIVER_POWER_STATE_FAILURE가 실행되었습니다.

EDR(Endpoint Detection and Response)

참고
이 기능은 Advanced Security + EDR 보호 팩에 포함되어 있으며, 이 보호 팩은 Cyber Protection 서비스를 통해 제공됩니다. 보호 계획에 EDR 기능을 추가하면 추가 요금이 부과될 수 있습니다.

EDR은 워크로드에서 감지되지 않은 공격을 비롯한 의심스러운 활동을 감지합니다. 그런 다음 인시던트를 생성합니다. 이러한 인시던트에서는 각 공격의 단계별 개요를 제공하므로 공격이 발생한 방식 및 해당 공격의 재발 방지 방법을 파악할 수 있습니다. 공격의 각 단계를 쉽게 이해할 수 있는 해석 정보가 제공되므로 공격 조사에 소요되는 시간을 몇 분으로 단축할 수 있습니다.

© Acronis International GmbH, 2003-2024

EDR(Endpoint Detection and Response)이 필요한 이유

오늘날에는 사이버 위협과 악의적인 공격의 범위가 갈수록 확대되고 있으므로 어떤 방지 조치를 취하더라도 환경을 완벽하게 보호할 수는 없습니다. 수단과 방법을 가리지 않고 방지 레이어를 통과하여 네트워크 침투에 성공하는 공격이 있게 마련이기 때문입니다. 기존 솔루션에서는 이러한 공격을 확인할 수 없으므로 공격자가 장기간 환경 내에서 공격을 자유롭게 진행할 수 있습니다.

기존 EDR 솔루션도 공격자를 빠르게 찾아낸 다음 차단함으로써 이와 같은 "조용한 공격"을 방지할 수는 있습니다. 하지만 기존 솔루션으로 이러한 공격을 방지하려면 대개 높은 수준의 보안 관련 전문 지식을 보유하고 있어야 하거나 많은 비용을 투자하여 Security Operation Center(SOC) 분석가를 채용해야 합니다. 그리고 인시던트를 분석하려면 시간이 매우 많이 걸릴 수 있습니다.

Acronis Advanced Security + EDR 기능을 활용하면 이러한 제한을 해소할 수 있습니다. 감지되지 않은 공격을 감지할 수 있으며, 공격이 발생한 방식 및 해당 공격의 재발 방지 방법을 파악할 수 있기 때문입니다. 그러면 공격 조사에 소요되는 시간도 단축할 수 있습니다.

EDR이 필요한 이유는 다음과 같습니다.

- **모든 공격을 자세하고 정확하게 파악**: 감지되지 않은 공격을 비롯하여 발생한 모든 공격과 공격 방식을 파악할 수 있습니다. 각 공격의 진행 과정도 단계별 그래픽으로 제공됩니다. 즉, 공격자의 초기 진입 지점부터 공격자가 표적으로 정했거나 유출한 데이터까지 전체 공격 과정을 확인할 수 있으므로 인시던트의 범위와 영향을 빠르게 파악할 수 있습니다. 자세한 내용은 "사이버 킬 체인에서 인시던트를 조사하는 방법"(824페이지)을(를) 참조하십시오.
- **조사 시간 최소화**: 인시던트 조사 시간을 몇 시간에서 몇 분으로 단축할 수 있습니다. EDR은 공격의 각 단계 관련 상세 정보를 사람이 쉽게 이해할 수 있는 명확한 언어로 제공합니다. 그러므로 많은 비용을 투자하여 전문가나 추가 인력을 채용할 필요성을 줄일 수 있습니다. 자세한 내용은 "인시던트 조사"(824페이지) 항목을 참조하십시오.
- **워크로드에서 알려진 위협 확인**: 워크로드에서 맬웨어, 취약성, 그리고 데이터 보호에 영향을 줄 수 있는 기타 유형의 글로벌 이벤트로 인해 발생한 위협을 자동으로 검색할 수 있습니다. 이러한 위협, 즉 침해 지표(IOC)는 Cyber Protection Operations Center(CPOC)에서 수신된 위협 데이터를 토대로 생성됩니다. 자세한 내용은 "워크로드에서 공개된 공격의 침해 지표(IOC) 확인"(834페이지)을(를) 참조하십시오.
- **인시던트에 더욱 신속하게 대응**: EDR에서는 위반 발생 후에 수행한 모든 작업을 파악하고 킬 체인의 각 단계를 세부적으로 확인할 수 있으므로 다양한 작업을 수행하여 각 공격 지점을 수정할 수 있습니다. 예를 들어 원격 제어 및 포렌식 백업(Early Access 버전에서는 이 기능을 사용할 수 없음)을 사용하여 조사를 진행해 워크로드 격리, 맬웨어 프로세스 삭제 등을 수행할 수 있습니다. Cyber Disaster Recovery Cloud을(를) 사용하여 업무 운영을 정상 상태로 복구할 수도 있습니다. 자세한 내용은 "인시던트 수정"(837페이지)을(를) 참조하십시오.
- **안정적으로 보고되는 보안 체계 파악**: EDR을 활성화하면 대다수 보안 취약성을 방지하고 사이버 공격이 기업에 줄 수 있는 영향에 대한 우려를 해소할 수 있습니다. 또한 인시던트 관련 정보가 180일 동안 저장되므로 감사용으로 해당 정보를 사용할 수 있습니다.

기능

EDR(Endpoint Detection and Response)에는 다음 기능이 포함되어 있습니다.

© Acronis International GmbH, 2003-2024

- 위반 발생 시 경보 알림 수신
- 인시던트 페이지에서 인시던트 관리
- 쉽게 이해할 수 있도록 시각화된 공격 진행 과정
- 권장 사항 및 수정 단계
- 위협 피드를 사용하여 워크로드와 관련해 공개된 공격 확인
- 대시보드에서 간편하게 개요 정보 파악
- 180일 동안 보안 이벤트 저장

위반 발생 시 경보 알림 수신

EDR은 인시던트가 발생할 때마다 경보 알림을 제공합니다. 이러한 경보는 Cyber Protect 콘솔의 주 메뉴에서 강조 표시됩니다. 경보가 강조 표시되면 **인시던트 조사** 버튼을 클릭하여 경보를 조사할 수 있습니다. 이 버튼을 클릭하면 인시던트 조사 화면(사이버 킬 체인이라고도 함)으로 리디렉션됩니다.

자세한 내용은 "인시던트 검토"(817페이지)을(를) 참조하십시오.

인시던트 페이지에서 인시던트 관리

EDR의 인시던트 페이지에서는 모든 인시던트를 관리할 수 있습니다. Cyber Protect 콘솔의 보호 메뉴에서 인시던트 페이지에 액세스할 수 있습니다. 인시던트 페이지는 요구 사항에 따라 필터링할 수 있으므로 인시던트의 현재 상태(심각도, 영향을 받은 워크로드, 양성 레벨 포함)를 빠르고 쉽게 파악할 수 있습니다. 사이버 킬 체인으로 직접 이동하여 공격 진행 과정을 노드별로 확인할 수도 있습니다.

인시던트 페이지에 대한 자세한 내용은 "인시던트 검토"(817페이지) 항목을 참조하십시오.

쉽게 이해할 수 있도록 시각화된 공격 진행 과정

EDR에서는 쉽게 읽을 수 있는 그림 형식의 공격 정보가 제공됩니다. 그러므로 보안 담당자가 아니더라도 공격의 목표와 심각도를 파악할 수 있습니다. 이처럼 EDR에서는 다음을 비롯하여 정확한 공격 발생 방식에 대한 상세 정보를 제공하므로 Security Operation Center(SOC) 서비스를 이용하거나 보안 전문가를 별도로 채용할 필요가 없습니다.

- 공격자의 침입 방법
- 공격자가 공격 흔적을 숨긴 방법
- 공격으로 인해 발생한 피해
- 공격의 확산 방법

자세한 내용은 "사이버 킬 체인에서 인시던트를 조사하는 방법"(824페이지)을(를) 참조하십시오.

권장 사항 및 수정 단계

EDR은 워크로드에 대한 공격을 해결하기 위해 쉽게 구현할 수 있는 명확한 권장 사항을 제공합니다. 공격을 빠르게 해결하려면 **전체 인시던트 수정** 버튼을 클릭하여 인시던트 완화를 위한 권장 단계를 확인한 후 진행합니다. 이러한 권장 단계를 진행하면 공격의 영향을 받은 작업을 빠르게 다

© Acronis International GmbH, 2003-2024

시 시작할 수 있습니다. 그러나 더 자세한 수정 단계를 진행하려는 경우에는 각 노드로 이동한 후 관련 조치를 취하여 해당 노드를 수정할 수 있습니다.

자세한 내용은 "인시던트 수정"(837페이지)을(를) 참조하십시오.

위협 피드를 사용하여 워크로드와 관련해 공개된 공격 확인

EDR에는 워크로드를 대상으로 진행된 알려진 기존 공격을 위협 피드에서 검토하는 기능이 포함되어 있습니다. 이러한 위협 피드는 사이버 보호 작업 센터(CPOC)에서 수신된 위협 데이터를 토대로 하여 자동으로 생성됩니다. EDR에서는 위협이 워크로드에 영향을 주는지 여부를 확인한 후 해당 위협을 무력화하는 데 필요한 단계를 진행할 수 있습니다.

자세한 내용은 "워크로드에서 공개된 공격의 침해 지표(IOC) 확인"(834페이지)을(를) 참조하십시오.

대시보드에서 간편하게 개요 정보 파악

EDR의 Cyber Protect 콘솔 대시보드에서는 광범위한 통계가 제공됩니다. 이 통계에서는 다음 정보를 확인할 수 있습니다.

- 현재 위협 상태(조사해야 하는 인시던트의 수 포함).
- 심각도별 공격 진행 과정(발생 가능한 공격 캠페인을 나타냄).
- 인시던트 종결의 유효 속도.
- 고객을 공격할 때 가장 많이 사용되는 전술.
- 워크로드의 네트워크 상태(워크로드가 분리되어 있는지 연결되어 있는지를 나타냄).

180일 동안 보안 이벤트 저장

EDR은 워크로드 및 애플리케이션 이벤트를 수집하여 180일 동안 저장합니다. 180일보다 오래 전에 발생한 이벤트는 삭제됩니다. 즉, 이벤트는 스토리지 공간이 아닌 발생 이후의 기간을 기준으로 삭제됩니다. EDR을 꺼도 워크로드와 관련하여 이전에 수집된 이벤트는 모두 보관되므로 인시던트 조사 시에 사용할 수 있습니다.

소프트웨어 요구 사항

EDR(Endpoint Detection and Response)은 다음 운영 체제를 지원합니다.

- Microsoft Windows 7 서비스 팩 1 이상
- Microsoft Windows Server 2008 R2 이상

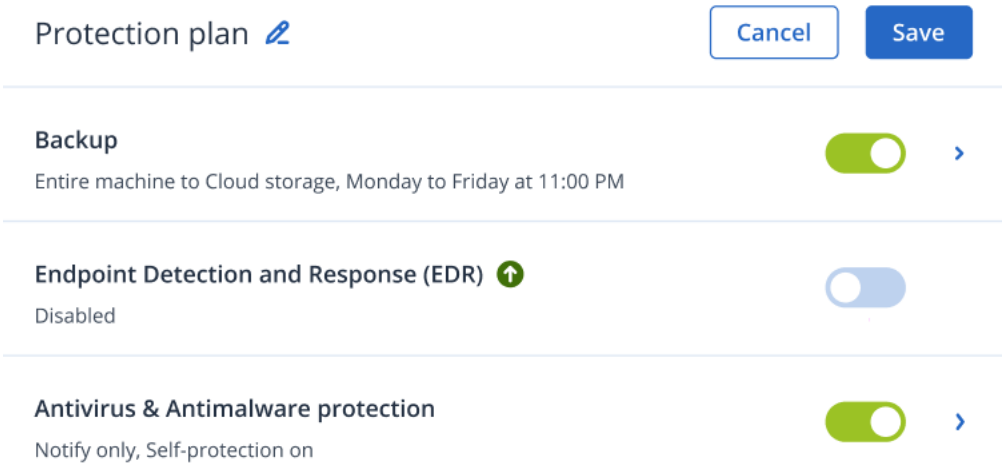
EDR(Endpoint Detection and Response) 기능 활성화

어떤 보호 계획에서나 EDR을 활성화할 수 있습니다.

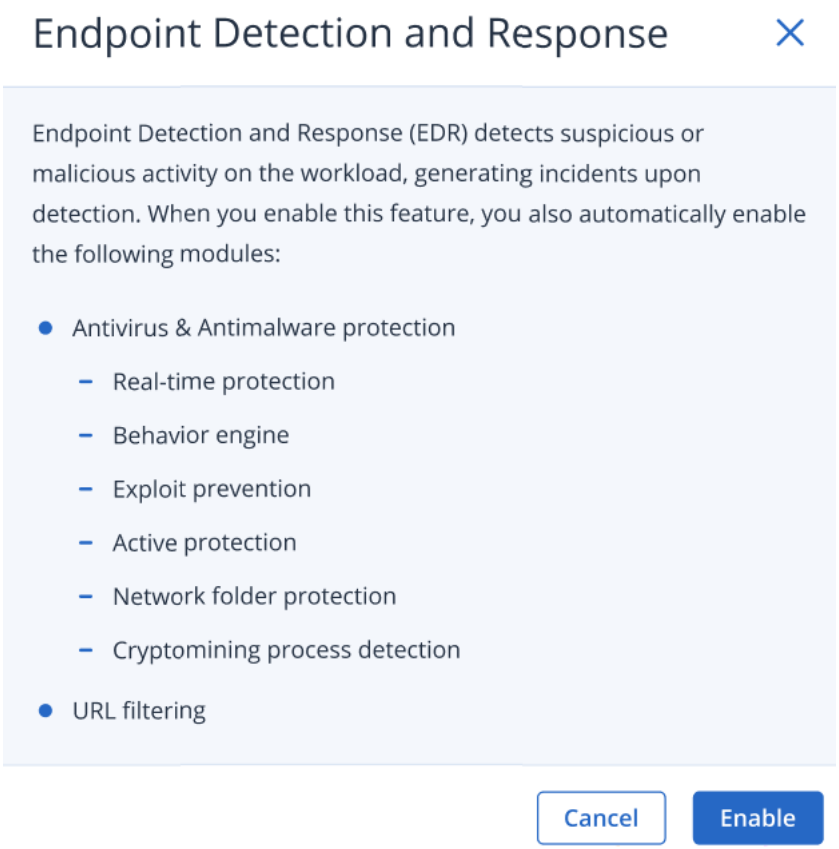
EDR을 활성화하려면

© Acronis International GmbH, 2003-2024

1. Cyber Protect 콘솔에서 **관리 > 보호 계획**으로 이동합니다.
2. 표시되는 목록에서 관련 보호 계획을 선택하고 오른쪽 사이드바에서 **편집**을 클릭합니다.
   새 보호 계획을 생성하고 다음 단계를 계속 진행해도 됩니다. 보호 계획 사용에 대한 자세한 내용은 "보호 계획 및 모듈"(199페이지) 항목을 참조하십시오.
3. 보호 계획 사이드바에서 모듈 이름 옆의 스위치를 클릭하여 **EDR(Endpoint Detection and Response)** 모듈을 활성화합니다.



4. 표시되는 대화 상자에서 **활성화**를 클릭합니다. EDR을 활성화하면 표시된 대화 상자에 나와 있는 기타 보호 모듈도 활성화됩니다.



© Acronis International GmbH, 2003-2024

참고
Active Protection, **동작 엔진**, **악용 방지** 또는 **URL 필터링** 중 하나라도 **꺼짐**으로 설정하면 **EDR(Endpoint Detection and Response)**도 **꺼짐**으로 설정됩니다.

5. 아래에 나와 있는 것처럼 선택한 추가 팩에 따라 **Advanced Security + EDR** 팩 아이콘이 보호 계획 구현에 필요한 보호 팩 목록에 추가됩니다.

EDR(Endpoint Detection and Response) 사용 방법

EDR에서는 감지되지 않은 공격을 감지할 수 있으며, 공격이 발생한 방식 및 해당 공격의 재발 방지 방법을 파악할 수 있습니다. 공격의 각 단계를 쉽게 이해할 수 있는 해석 정보가 제공되므로 공격 조사에 소요되는 시간을 몇 분으로 단축할 수 있습니다.

EDR 사용 시에 일반적으로 진행되는 워크플로우의 설명이 아래 표에 나와 있습니다. 먼저 새 인시던트를 검토하여 수정 우선 순위를 지정합니다. 그리고 사이버 킬 체인에서 인시던트를 추가로 조사한 후에 관련 수정 작업을 진행합니다.

단계	EDR 사용 방법
1단계: 인시던트 검토	EDR 인시던트 목록에서 다음을 수행합니다. • 조직의 보안 상태와 조사해야 하는 인시던트의 수 파악 • 가장 중요한 인시던트를 파악한 후 심각도에 따라 조사 우선 순위 지정. • 새로 발생한 인시던트나 계속 진행되고 있는 인시던트 파악.
2단계: 인시던트 조사	EDR 사이버 킬 체인에서 다음을 수행합니다. • 공격자의 목표를 파악하고 공격자가 사용한 공격 기술 확인. • 인시던트가 실제 악의적인 공격일 가능성 확인. • 위협 피드가 워크로드에 영향을 주는지 여부 확인. • 인시던트에 이미 적용된 대응 조치 확인.
3단계: 인시던트 수정	관련 EDR 수정 섹션에서 다음을 수행합니다. • 글로벌 대응 조치를 적용하여 빠르고 쉽게 전체 인시던트 수정. • 인시던트 내의 개별 공격 지점 수정. • 현재 공격이나 향후 공격이 확산되거나 공격자가 아직 표적으로 선택하지 않은 워크로드에 영향을 주는 상황을 방지하기 위한 조치 적용.

인시던트 검토

EDR(Endpoint Detection and Response)에서 제공하는 인시던트 목록에는 워크로드에서 감지된 방지 항목 또는 맬웨어와 의심스러운 항목이 모두 포함되어 있습니다. 인시던트 목록에서는 아직 완화하지 않은 위협을 비롯하여 워크로드에 영향을 주는 공격이나 위협의 개요 정보를 간편하게 파악할 수 있습니다.

인시던트 목록에서는 다음 정보를 빠르게 확인 수 있습니다.

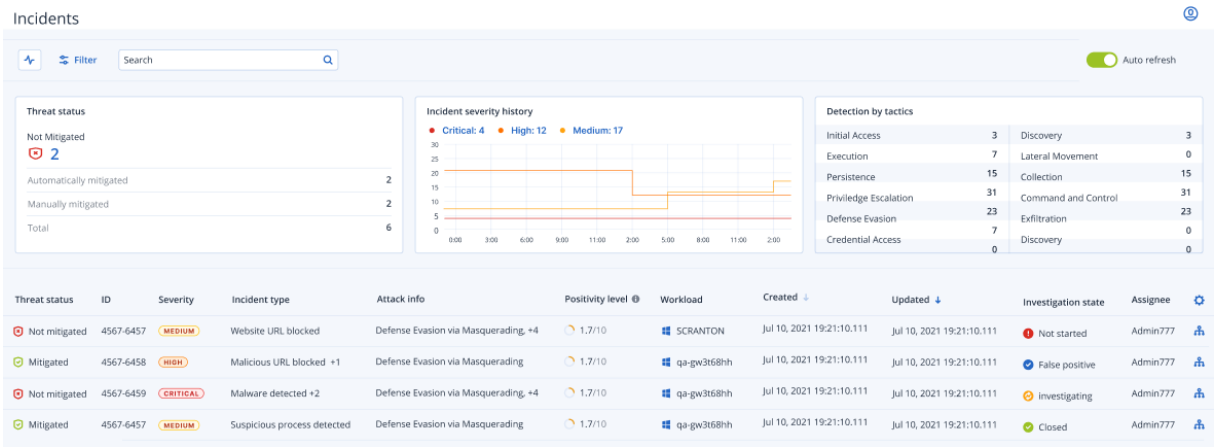
© Acronis International GmbH, 2003-2024

- 조직의 보안 상태와 조사해야 하는 인시던트의 수
- 가장 중요한 인시던트(심각도에 따라 조사 우선 순위 지정)
- 새로 발생한 인시던트나 계속 진행되고 있는 인시던트.

참고
파트너 관리자로 로그인하면 모든 고객의 인시던트가 통합 표시되는 한 화면에서 모든 EDR 인시던트를 확인할 수 있으므로 각 고객의 개별 인시던트 보기에 일일이 액세스하지 않아도 됩니다. 이 화면에 추가로 표시되는 **고객** 열에는 각 인시던트가 발생한 고객의 이름이 포함되어 있습니다. 그리고 **개요** 대시보드에 표시되는 위젯에는 모든 고객을 대상으로 집계된 지표 데이터가 표시됩니다.

아래에 나와 있는 것처럼 Cyber Protect 콘솔의 **보호** 메뉴에서 인시던트 목록에 액세스할 수 있습니다. 인시던트 목록에서 인시던트를 검토하는 방법에 대한 자세한 내용은 "현재 완화되지 않은 인시던트 확인"(820페이지) 항목을 참조하십시오. 인시던트가 생성되는 상황을 자세히 알아보려면 인시던트란?을 참조하십시오.

참고
워크로드에서 관리형 탐지 및 대응(MDR)이 활성화되어 있으면 **MDR 티켓** 열이 추가로 표시됩니다. 해당 열에는 MDR 공급업체가 제공한 티켓 번호가 표시됩니다.



참고
Cyber Protect 콘솔이 열려 있어야 인시던트 알림이 수신됩니다.

인시던트란?

인시던트(보안 인시던트)는 방지 항목이나 의심스러운 항목이 하나 이상 감지된 지점이 포함되어 있는 *컨테이너*로 간주할 수 있습니다. 단일 공격과 관련된 모든 이벤트와 감지 항목이 인시던트에 포함됩니다. 발생한 상황과 관련하여 더 자세한 상황 정보를 제공하는 추가적인 정상 프로세스도 이러한 보안 인시던트에 포함될 수 있습니다.

그러므로 인시던트 하나에서 모든 공격 이벤트를 함께 확인하여 공격자가 수행한 논리적 단계를 파악할 수 있습니다. 그리고 공격 조사도 더 빠르게 진행할 수 있습니다.

EDR이 보호 계획에서 활성화되어 있으면 다음과 같은 상황에서 보안 인시던트가 생성됩니다.

© Acronis International GmbH, 2003-2024

- **방지 레이어로 인해 특정 항목이 중지되는 경우:** 이러한 인시던트는 보호 계획 설정에 따라 시스템에서 자동으로 종결됩니다. 그러나 맬웨어가 중지되기 전에 정확히 어떤 작업을 수행했는지를 조사할 수 있습니다. 예를 들어 파일 암호화를 시작할 때 중지된 랜섬웨어가 암호화를 시작하기 전에 자격 증명을 도용했거나 서비스를 설치했을 수도 있습니다.
- **EDR에서 의심스러운 활동이 감지되는 경우:** 이렇게 감지된 작업은 조사하여 수정해야 합니다. 쉽게 이해할 수 있도록 자세한 그림으로 표시되는 사이버 킬 체인을 검토하면(자세한 내용은 "사이버 킬 체인에서 인시던트를 조사하는 방법"(824페이지) 참조) 관련 수정 작업을 쉽게 적용할 수 있습니다.

즉시 확인해야 하는 인시던트의 우선 순위 지정

Cyber Protect 콘솔의 **보호** 메뉴에서 언제든지 Cyber Protect 콘솔 인시던트 목록에 액세스할 수 있습니다. 인시던트 목록에서는 공격이나 위협의 개요 정보를 간편하게 파악할 수 있으므로 확인해야 하는 인시던트의 우선 순위를 지정할 수 있습니다.

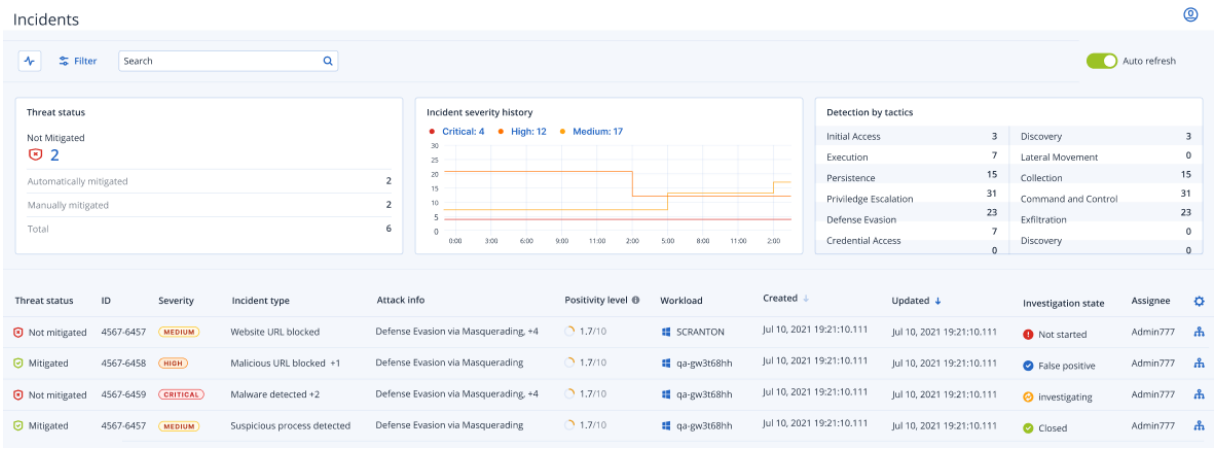
중요
워크로드의 보안을 유지하려면 *항상* 진행 중이거나 완화되지 않은 인시던트를 분석하여 확인 우선 순위를 지정해야 합니다.

즉시 확인해야 하는 보안 인시던트를 분석하는 방법

인시던트 목록에서는 확인해야 하는 목록 내 인시던트를 분석하여 확인 우선 순위를 지정할 수 있습니다. 다음을 수행할 수 있습니다.

- 현재 완화되지 않은 인시던트 확인: 인시던트 목록에서 현재 진행 중인 공격이 있는지를 빠르게 파악할 수 있습니다. 완화되지 않은 인시던트(**위협 상태** 열에 표시됨)는 즉시 확인해야 합니다. 인시던트 목록은 기본적으로 이러한 인시던트가 표시되도록 필터링됩니다.
- 인시던트의 범위와 영향 파악: 새로 시작된 공격이나 계속 진행되고 있는 공격이 표시되도록 목록을 필터링한 후 필터링된 인시던트의 심각도 및 기업에 대한 영향을 파악합니다.

가장 중요한 인시던트만 포함된 세부 목록을 표시한 후 인시던트 상세 정보를 분석하여 특정 인시던트, 그리고 공격자가 목표를 달성하기 위해 사용한 기술을 더 자세히 파악할 수 있습니다. 자세한 내용은 "인시던트 상세 정보 분석"(822페이지)을(를) 참조하십시오.



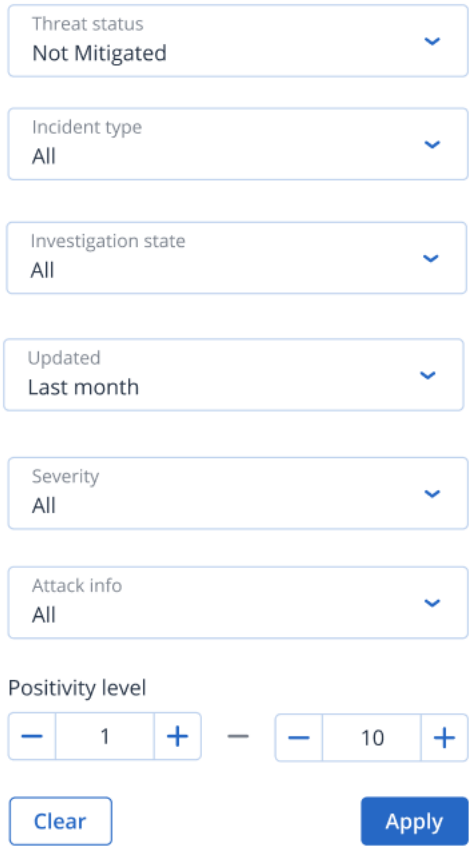
© Acronis International GmbH, 2003-2024

참고

인시던트 목록은 기본적으로 **업데이트한 날짜** 열을 기준으로 정렬됩니다. 업데이트한 날짜 열에는 인시던트 내에서 기록된 새 감지 항목이 추가되어 인시던트가 마지막으로 업데이트된 날짜와 시간이 자세히 표시됩니다. 이전에 종결된 기존 인시던트도 언제든지 업데이트할 수 있습니다. 아래 절차에 설명되어 있는 것처럼 요구 사항에 따라 새로 시작된 공격이나 계속 진행되고 있는 공격이 표시되도록 목록을 필터링할 수도 있습니다.

인시던트 목록을 필터링하려면

1. 인시던트 목록 맨 위에서 **필터**를 클릭하여 표시된 인시던트의 목록을 필터링합니다. 예를 들어 **생성된 날짜** 필드에서 시작 날짜와 종료 날짜를 선택하면 인시던트 목록과 위젯에는 정의된 기간 동안 생성된 관련 인시던트가 표시됩니다.



2. 작업을 완료한 후 **적용**을 클릭합니다.

현재 완화되지 않은 인시던트 확인

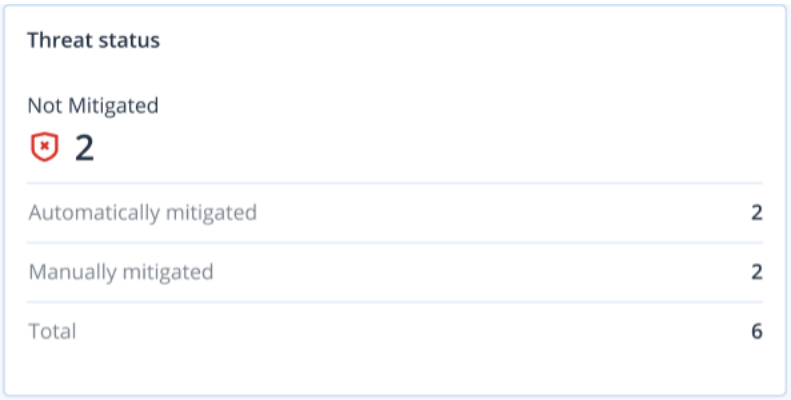
위협 상태 열에서 인시던트의 현재 위협 상태를 확인할 수 있습니다. 이 열에는 인시던트가 **완화됨** 상태인지 아니면 **완화되지 않음** 상태인지가 표시됩니다. 위협 상태는 EDR에서 자동 정의됩니다. 완화되지 않은 인시던트는 최대한 빨리 조사해야 합니다.

그런 후에는 필터를 적용하여 표시된 인시던트 목록을 상세 검색할 수 있습니다. 예를 들어 위협 상태 및 특정 심각도 수준에 따라 목록을 필터링하려는 경우 관련 필터 옵션을 선택합니다. 확인하

© Acronis International GmbH, 2003-2024

려는 인시던트가 표시되도록 필터링한 후 "인시던트 조사"(824페이지)의 설명에 따라 해당 인시던트를 조사할 수 있습니다.

아래에 나와 있는 **위협 상태** 위젯을 사용하여 현재 위협 상태의 개요 정보를 간편하게 확인할 수도 있습니다. 이 위젯에 표시되는 데이터에는 적용한 필터가 반영됩니다. "인시던트 목록을 필터링하려면"(820페이지) 항목을 참조하십시오.



인시던트의 범위와 영향 파악

심각도, **공격 정보** 및 **양성 레벨** 열을 검토하여 인시던트의 범위와 영향을 빠르게 파악할 수 있습니다. 위에서 설명한 것처럼 현재 진행 중인 인시던트를 확인한 후에는 이러한 추가 열을 필터링하여 다음을 수행할 수 있습니다.

- **심각도** 열에서 더 심각한 인시던트 검토. 인시던트의 심각도는 **심각**, **높음** 또는 **중간** 중 하나일 수 있습니다.
  - **심각**: 악의적인 사이버 활동이 진행 중일 위험성이 매우 높으며, 환경의 중요 호스트가 손상될 위험성도 있습니다.
  - **높음**: 악의적인 사이버 활동이 진행 중일 위험성이 높으며, 환경이 심각하게 손상될 위험성도 있습니다.
  - **중간**: 악의적인 사이버 활동 발생 위험성이 어느 정도 높습니다.

  참고
  EDR 알고리즘은 심각도를 결정할 때 워크로드 유형과 공격의 각 단계 범위를 모두 고려합니다. 예를 들어 자격 증명 도난 관련 단계가 포함된 인시던트는 **심각**로 설정됩니다.

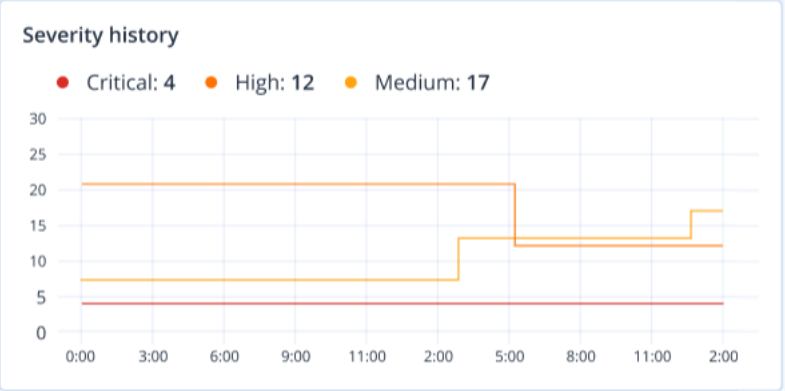
- **인시던트 유형** 열에서 인시던트가 생성된 이유를 이해하십시오. 인시던트 유형은 다음 중 하나 이상을 포함할 수 있습니다.
  - **랜섬웨어가 탐지됨**
  - **맬웨어 감지됨**
  - **의심스러운 프로세스가 탐지됨**
  - **악성 프로세스가 탐지됨**
  - **의심스러운 URL이 차단됨**
  - **악성 URL이 차단됨**

© Acronis International GmbH, 2003-2024

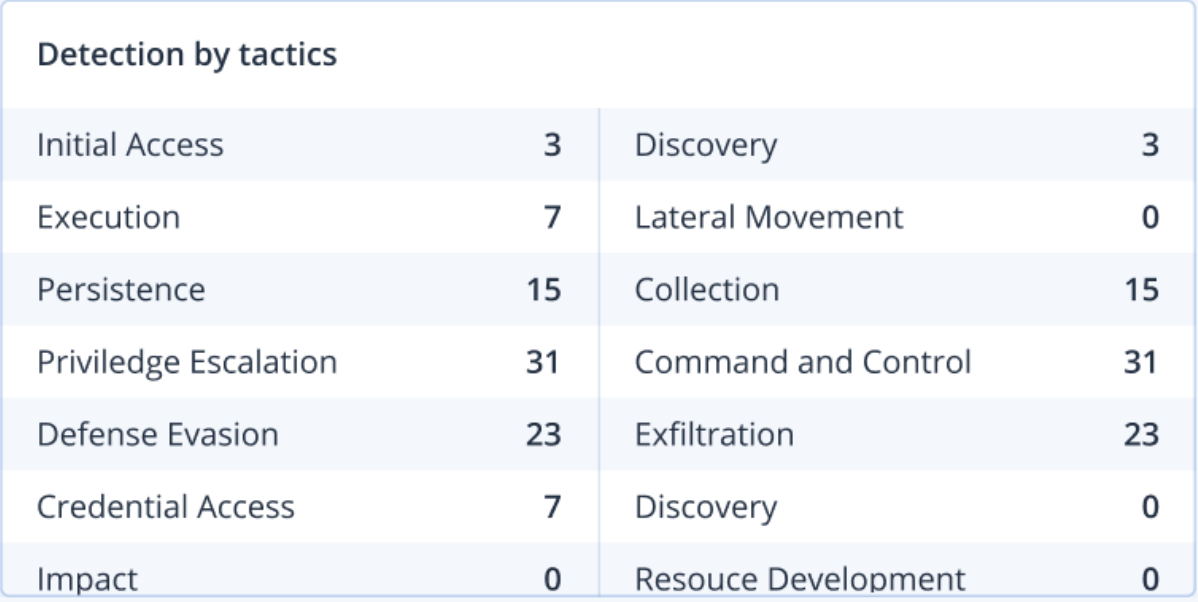
- **공격 정보** 열에서 공격에 사용되는 공격 기술을 확인하고 공격에서 공통적으로 나타나는 테마나 패턴이 있는지를 파악합니다.
- 인시던트가 실제 악의적인 공격일 가능성을 확인합니다. **양성 레벨** 열에는 1~10 사이의 점수가 표시되는데 점수가 높을수록 공격이 실제 악의적인 공격일 가능성도 높은 것입니다.

즉시 확인해야 하는 인시던트를 파악한 후에는 "인시던트 조사"(824페이지)의 설명에 따라 해당 인시던트를 조사할 수 있습니다.

심각도 내역 및 **전술별 감지** 위젯을 사용하여 심각도 및 공격 기술의 개요 정보를 간편하게 확인할 수도 있습니다.



전술별 감지 위젯에는 공격에 사용되는 다양한 공격 기술이 표시됩니다. 그리고 지정된 이전 시간 범위 동안 감지된 공격 수가 늘어났는지 아니면 줄어들었는지를 나타내는 녹색이나 빨간색 값도 표시됩니다. 이 위젯에서는 인시던트를 필터링한 후 공격의 모든 목표를 통합 확인할 수 있으므로 공격이 고객에게 주는 영향 관련 개요 정보를 빠르게 파악할 수 있습니다.



인시던트 상세 정보 분석

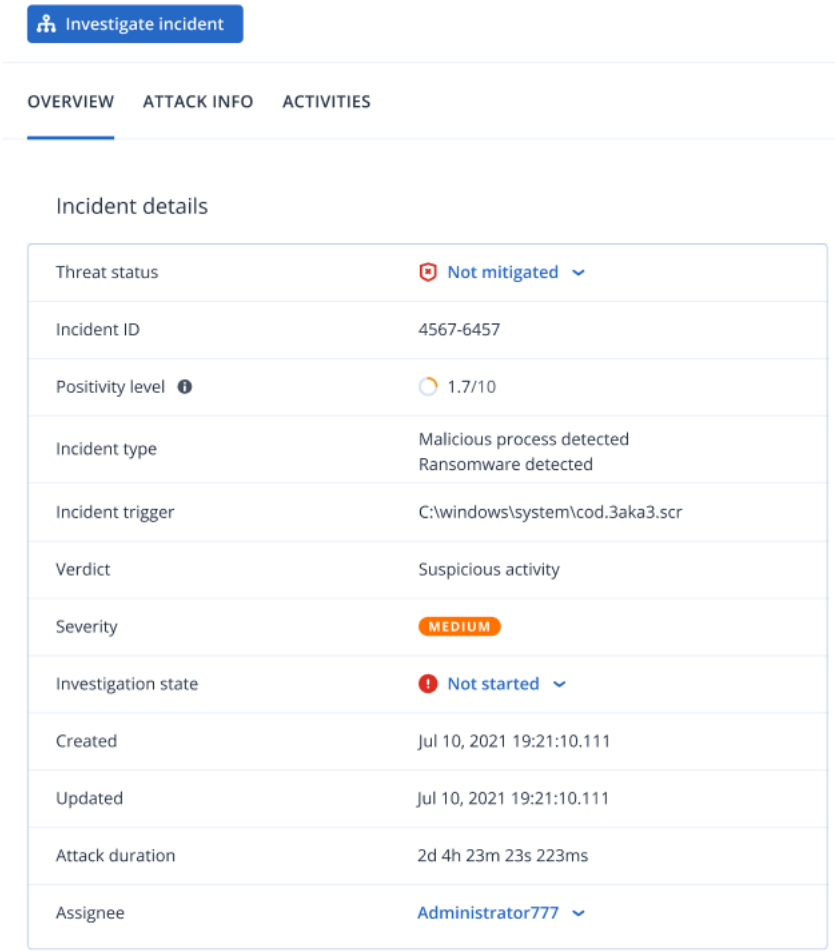
인시던트 검토 단계에서는 EDR(Endpoint Detection and Response) 인시던트 목록에서 각 인시던트의 상세 정보도 분석할 수 있습니다. 이러한 상세 정보를 분석하면 전체 인시던트로 드릴다운하여

© Acronis International GmbH, 2003-2024

인시던트가 발생한 방식과 시간을 파악할 수 있습니다. 또한 특정 사용자에게 조사할 인시던트를 할당하고 조사 상태를 설정할 수도 있습니다.

인시던트 상세 정보를 분석하려면

1. Cyber Protect 콘솔에서 **보호 > 인시던트**로 이동합니다. 인시던트 목록이 표시됩니다.
2. 검토할 인시던트를 클릭합니다. 선택한 인시던트의 상세 정보가 표시됩니다.
3. 표시되는 **개요** 탭에서 현재 위협 상태 및 심각도를 비롯한 인시던트 및 워크로드 상세 정보를 검토할 수 있습니다. **조사 상태**도 정의할 수 있습니다. **조사 중**, **시작되지 않음**(기본 상태), **위양성** 또는 **종결됨** 중 하나를 선택하면 됩니다. 인시던트를 할당할 사용자도 선택할 수 있습니다. **담당자** 드롭다운 목록에서 관련 사용자를 선택하면 됩니다.

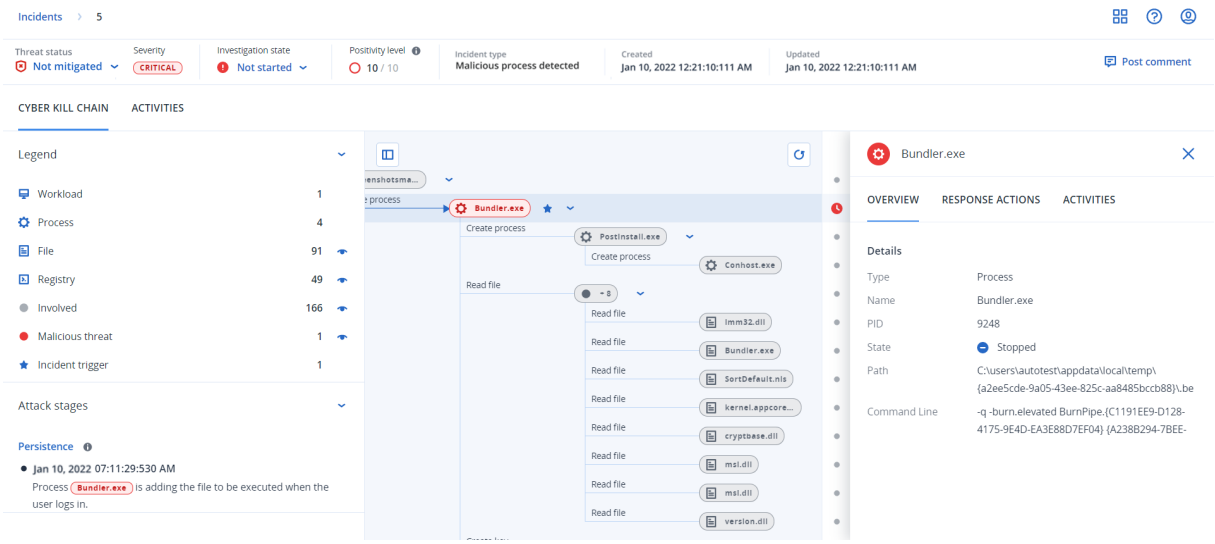


4. 공격 및 공격에 사용된 기술의 상세 정보를 검토하려면 **공격 정보** 탭을 클릭합니다. MITRE.org에서 공격 기술 관련 추가 정보를 검토하려면 나열된 각 공격 기술 옆의 링크를 클릭합니다.
5. 인시던트 완화를 위해 사이버 킬 체인에서 취한 조치를 검토하려면 **작업** 탭을 클릭합니다. 자세한 내용은 "사이버 킬 체인에서 인시던트를 조사하는 방법"(824페이지)을(를) 참조하십시오. 예를 들어 워크로드에서 패치를 실행했다면 패치를 시작한 사람, 패치에 걸린 시간, 그리고 패치 구현 중에 발생한 오류를 확인할 수 있습니다.
6. 인시던트를 노드별로 조사할 수 있는 사이버 킬 체인에 액세스하려면 **인시던트 조사**를 클릭합니다. 자세한 내용은 "사이버 킬 체인에서 인시던트를 조사하는 방법"(824페이지)을(를) 참조하십시오.

© Acronis International GmbH, 2003-2024

인시던트 조사

EDR(Endpoint Detection and Response)에서는 모든 공격 단계와 공격의 영향을 받은 객체(프로세스, 레지스트리, 예약된 작업, 도메인)를 비롯하여 전체 인시던트를 조사할 수 있습니다. 이러한 객체는 아래에 나와 있는 것처럼 쉽게 이해할 수 있는 사이버 킬 체인의 노드로 표시됩니다. 사이버 킬 체인을 사용하면 정확히 발생한 상황 및 발생 시기를 빠르게 파악할 수 있습니다.



사이버 킬 체인에서는 공격의 모든 단계를 각각 확인할 수 있습니다. 각 공격 단계에서는 인시던트가 발생한 방식과 이유 관련 세부 해석이 제공됩니다. 사이버 킬 체인은 쉽게 이해할 수 있는 문장과 그래프를 사용하므로 공격의 각 단계를 쉽게 설명할 수 있습니다. 따라서 조사 시간을 최소화할 수 있습니다.

MITRE 프레임워크에 매핑된 공격 진행 과정을 통해 인시던트의 범위와 영향을 빠르게 파악할 수 있습니다. 그러므로 다음을 비롯해 각 공격 단계에서 발생한 상황을 분석할 수 있습니다.

- 초기 진입점
- 공격 실행 방법
- 권한 에스컬레이션
- 회피 감지 기술
- 다른 워크로드로의 횡적 확산
- 자격 증명 도난
- 유출 시도

참고

공격의 영향을 받은 각 객체(프로세스, 레지스트리, 예약된 작업 또는 도메인)는 사이버 킬 체인의 노드로 표시됩니다.

사이버 킬 체인에서 인시던트를 조사하는 방법

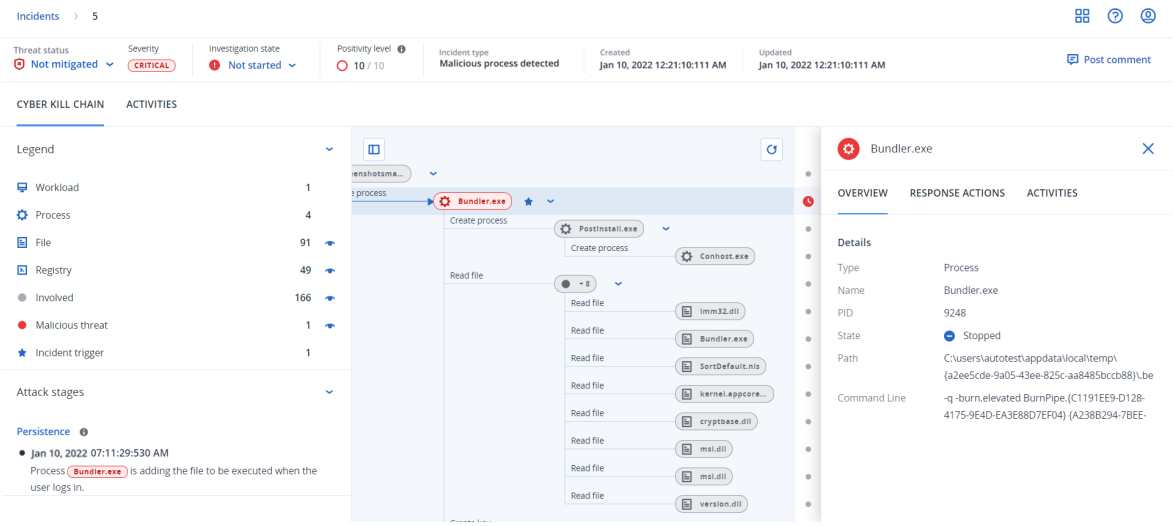
사이버 킬 체인에서는 공격의 모든 단계를 각각 조사할 수 있습니다. 쉽게 이해할 수 있는 사이버 킬 체인의 문장과 그래프를 통해 공격의 각 단계를 파악할 수 있습니다. 따라서 조사 시간을 최소

© Acronis International GmbH, 2003-2024

화할 수 있습니다.

사이버 킬 체인에서 조사를 시작하려면

1. Cyber Protect 콘솔에서 **보호 > 인시던트**로 이동합니다.
2. 표시되는 인시던트 목록에서 조사할 인시던트의 맨 오른쪽 열에 있는 을 클릭합니다. 선택한 인시던트의 사이버 킬 체인이 표시됩니다.



3. 페이지 위쪽의 위협 상태 바에서 인시던트 요약을 확인합니다. 위협 상태 바에는 다음 정보가 포함되어 있습니다.
   - 현재 위협 상태: 위협 상태는 시스템에서 자동 정의됩니다. **완화되지 않음** 상태인 인시던트는 최대한 빨리 조사해야 합니다.

     중요
     백업에서 복원하는 작업이 정상적으로 완료되었거나 감지된 모든 항목이 중지 프로세스, 격리 또는 롤백 작업을 통해 정상적으로 수정된 경우 인시던트는 **완화됨**으로 설정됩니다.

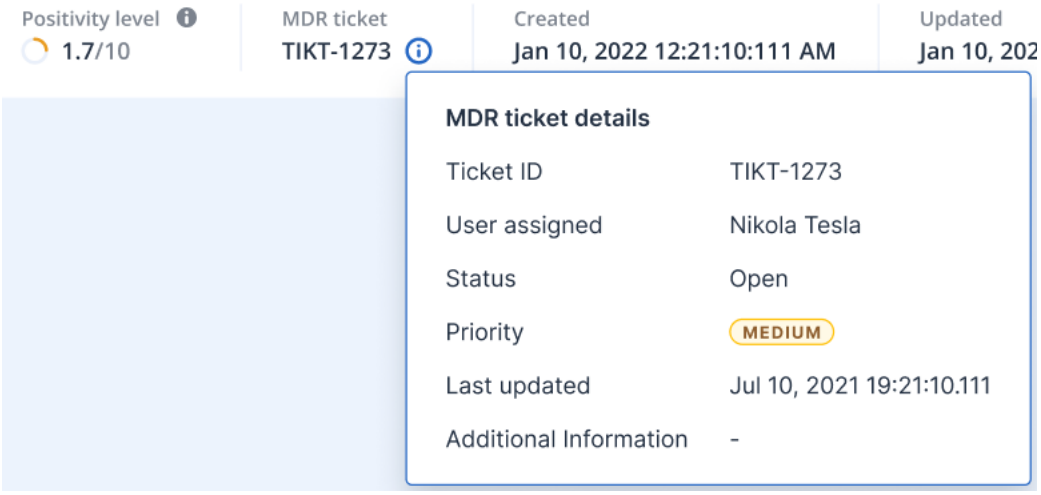
     백업에서 복원하는 작업이 정상적으로 완료되지 않았거나 감지된 항목 중 하나 이상이 중지 프로세스, 격리 또는 롤백 작업을 통해 정상적으로 수정되지 않은 경우 인시던트는 **완화되지 않음**으로 설정됩니다.

     위협 상태를 **완화됨** 또는 **완회되지 않음**으로 수동 설정할 수도 있습니다. 이 두 상태 중 하나를 선택하면 주석을 입력하라는 메시지가 표시됩니다. 해당 주석은 조사 작업의 일부로 저장되며 **작업** 탭에서 확인할 수 있습니다. 새로 감지된 인시던트가 검색되었거나 대응 조치가 실행되어 정상 완료되었다면 EDR이 위협 상태를 **완화됨** 또는 **완화되지 않음**으로 되돌릴 수 있습니다.

   - 인시던트 심각도: **심각**, **높음** 또는 **중간** 중 하나입니다. 자세한 내용은 "인시던트 검토"(817 페이지)을(를) 참조하십시오.
   - 현재 조사 상태: **조사 중**, **시작되지 않음**(기본 상태), **위양성** 또는 **종결됨** 중 하나입니다. 인시던트 조사를 시작할 때 상태를 변경해야 합니다. 그래야 다른 동료들이 인시던트의 변경 사항을 파악할 수 있습니다.

© Acronis International GmbH, 2003-2024

- 양성 레벨: 인시던트가 실제 악의적인 공격일 가능성을 1~10 범위 내에서 선택할 수 있습니다. 자세한 내용은 "인시던트 검토"(817페이지)을(를) 참조하십시오.
- 인시던트 유형: 하나 이상의 **랜섬웨어가 탐지됨**, **맬웨어가 탐지됨**, **의심스러운 프로세스가 탐지됨**, **악성 프로세스가 탐지됨**, **의심스러운 URL이 차단됨** 및 **악성 URL이 차단됨**.
- 워크로드에서 관리형 탐지 및 대응(MDR)이 활성화되어 있으면 **MDR 티켓** 필드가 표시됩니다. 해당 필드에서 인시던트용으로 생성된 MDR 티켓의 상세 정보, 그리고 인시던트에 할당된 MDR 보안 분석가를 확인할 수 있습니다.



- 인시던트가 생성 및 업데이트된 시간: 인시던트가 감지된 날짜와 시간 또는 인시던트 내에서 기록된 새 감지 항목이 추가되어 인시던트가 마지막으로 업데이트된 시간입니다.

4. **범례** 탭을 클릭하여 킬 체인 그래프에 포함된 여러 노드를 표시한 후 확인할 노드를 정의합니다. 자세한 내용은 "사이버 킬 체인 보기 이해 및 사용자 정의"(826페이지) 항목을 참조하십시오.
5. 다음 단계를 수행하여 인시던트를 조사하고 수정합니다. 이 단계는 인시던트를 조사 및 수정할 때 진행하는 표준 워크플로우입니다. 하지만 실제 단계는 각 인시던트와 사용자별 요구 사항에 따라 달라질 수 있습니다.
   a. **공격 단계** 탭에서 공격의 각 단계를 조사합니다. 자세한 내용은 "공격 단계로 이동하는 방법"(829페이지) 항목을 참조하십시오.
   b. **전체 인시던트 수정**을 클릭하여 수정 작업을 적용합니다. 자세한 내용은 "전체 인시던트 수정"(837페이지) 항목을 참조하십시오.

      "개별 사이버 킬 체인 노드에 대한 대응 조치"(841페이지)의 설명에 따라 사이버 킬 체인의 개별 노드를 수정할 수도 있습니다.
   c. **작업** 탭에서 인시던트를 완화하기 위해 수행한 작업을 검토합니다. 자세한 내용은 "인시던트 완화를 위해 수행한 작업 파악"(832페이지) 항목을 참조하십시오.

사이버 킬 체인 보기 이해 및 사용자 정의

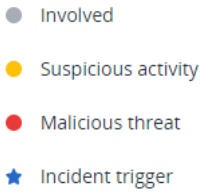
사이버 킬 체인에서 인시던트의 영향을 받은 노드를 파악하려면 범례에 액세스합니다. 범례에는 인시던트와 관련이 있는 모든 노드가 표시됩니다. 따라서 공격자가 여러 노드를 공격한 방식을 파악할 수 있습니다. 사이버 킬 체인에서 숨기거나 표시할 노드를 정의할 수도 있습니다.

© Acronis International GmbH, 2003-2024

범례에 액세스하려면

1. 범례 섹션 오른쪽의 화살표 아이콘을 클릭합니다.
   아래에 나와 있는 것처럼 범례 섹션이 확장됩니다.

2. 범례에서는 기본적으로 네 가지 색상이 사용됩니다. 그러므로 아래에 나와 있는 것처럼 사이버 킬 체인의 각 노드에서 발생한 상황을 빠르게 파악할 수 있습니다. 이처럼 색상 코드가 지정된 노드는 "공격 단계로 이동하는 방법"(829페이지)에 설명되어 있는 것처럼 공격 단계에도 포함되어 있습니다.



사이버 킬 체인에서 노드를 숨기거나 표시하려면

1. 확장된 범례 섹션에서 사이버 킬 체인에 표시할 노드 옆에 이 표시되어 있는지 확인합니다. 아이콘이 표시되어 있다면 해당 아이콘을 클릭하여 으로 변경합니다.
2. 사이버 킬 체인에서 노드를 숨기려면 을 클릭합니다. 아이콘이 으로 바뀌고 노드가 사이버 킬 체인에 표시되지 않습니다.

인시던트의 공격 단계 조사

인시던트의 공격 단계에서는 쉽게 이해할 수 있는 모든 인시던트의 해석 정보가 제공됩니다.

© Acronis International GmbH, 2003-2024

각 공격 단계에는 정확히 발생한 상황 및 공격의 표적이 된 객체(사이버 킬 체인의 노드) 관련 요약 정보가 표시됩니다. 예를 들어 다른 항목으로 가장한 파일을 다운로드한 경우 공격 단계에 해당 파일을 다운로드했다는 정보가 표시됩니다. 그리고 조사 가능한 사이버 킬 체인의 관련 노드 및 관련 MITRE ATT&CK 기술로 이동하는 링크도 포함됩니다.

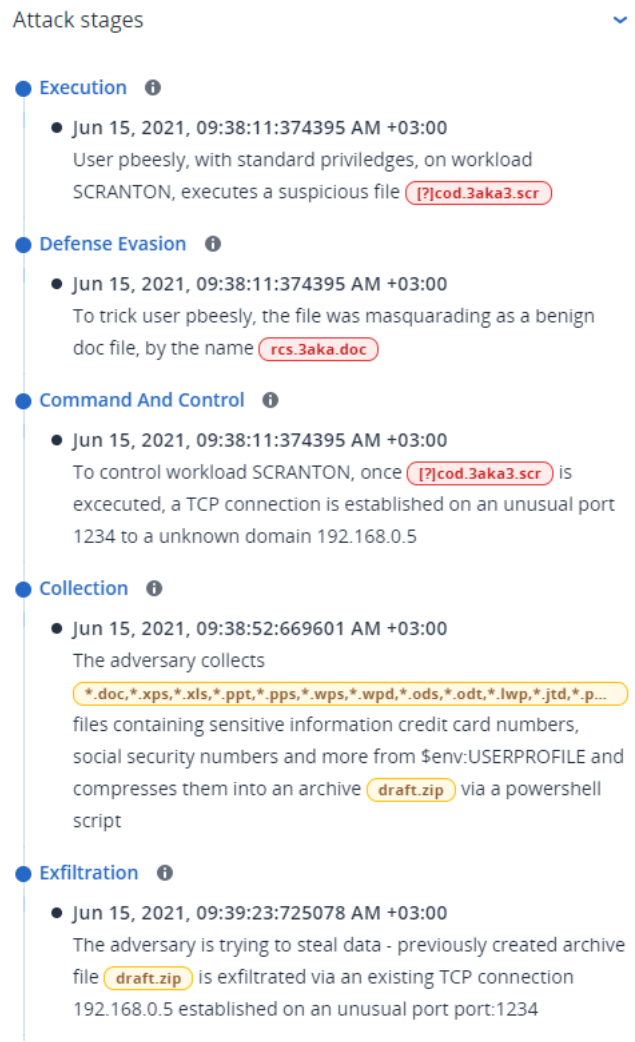
공격의 각 단계에서는 다음의 세 가지 중요 정보를 파악하는 데 필요한 정보가 제공됩니다.

- 공격자의 목표
- 공격자가 해당 목표를 달성한 방법
- 공격의 표적이 된 노드

뿐만 아니라 공격 단계에서 제공되는 해석 정보를 자세히 파악하면 인시던트 조사에 소요되는 시간을 대폭 단축할 수 있습니다. 더 이상 타임라인이나 그래프 노드에서 각 보안 이벤트를 확인한 후 공격 해석 정보를 생성할 필요가 없기 때문입니다.

아래 예제의 **수집** 단계에 나와 있는 것처럼 공격 단계에는 신용 카드 번호, 사회 보장 번호 등의 민감한 정보를 포함하는 손상된 파일 관련 정보도 포함되어 있습니다.

자세한 내용은 "공격 단계에 포함되는 정보"(829페이지)을(를) 참조하십시오.



© Acronis International GmbH, 2003-2024

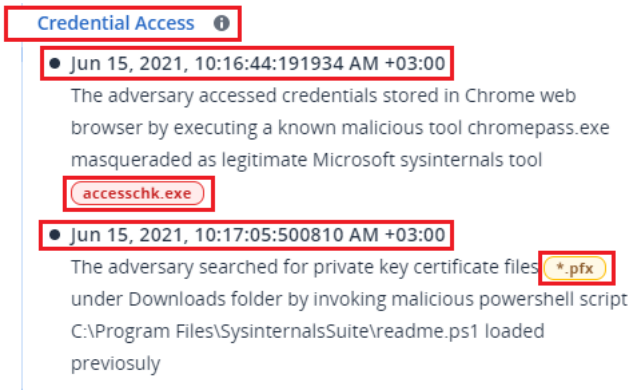
공격 단계로 이동하는 방법

공격 단계는 시간순으로 나열됩니다. 아래쪽으로 스크롤하면 특정 인시던트에 대한 공격 단계의 전체 목록을 확인할 수 있습니다.

특정 공격 단계를 자세히 조사하려는 경우 공격 단계에서 아무 곳이나 클릭하여 사이버 킬 체인 그래프의 관련 노드로 이동합니다. 사이버 킬 체인 그래프와 특정 노드를 살펴보는 방법에 대한 자세한 내용은 "사이버 킬 체인의 개별 노드 조사"(830페이지) 항목을 참조하십시오.

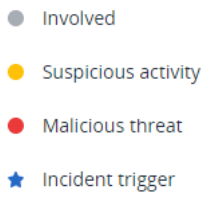
공격 단계에 포함되는 정보

각 공격 단계에서는 사람이 쉽게 읽을 수 있는 언어로 작성되어 바로 이해 가능한 공격 해석 정보가 제공됩니다. 이 해석 정보에는 여러 가지 요소가 포함됩니다. 아래 표에 해당 요소 및 설명이 나와 있습니다.



공격 단계 요소	설명
머리말	공격자가 시도한 작업과 공격자의 목표(위 예제의 경우 **자격 증명 액세스**) 관련 설명, 그리고 알려진 MITRE ATT&CK 기술 정보를 확인할 수 있는 링크가 제공됩니다. 해당 링크를 클릭하면 MITRE ATT&CK 웹 사이트에서 자세한 내용을 확인할 수 있습니다. **참고** 공격 단계가 알려진 MITRE ATT&CK 기술이 아닌 경우에는 헤더 텍스트에 링크가 설정되지 않습니다. 가령 임의의 폴더에서 감지된 파일처럼 일반 기술에 해당하는 공격 단계의 경우에는 링크가 없는 헤더 텍스트가 표시됩니다.
타임스탬프	공격 단계가 발생한 시간입니다.
기술	공격자가 기술을 활용하여 목표를 달성한 방법 및 영향을 받은 객체(레지스트리 항목,

© Acronis International GmbH, 2003-2024

공격 단계 요소	설명
	파일, 예약된 작업 등)입니다. 공격 기술의 텍스트 설명에는 위의 예제와 같이 사이버 킬 체인에서 영향을 받은 각 노드에 해당하는 색상 코드가 지정된 링크가 포함되어 있습니다. 이처럼 색상 코드가 지정된 링크를 클릭하면 영향을 받은 노드로 빠르게 이동하여 발생한 상황을 정확히 조사할 수 있습니다. 공격 단계에서 사용되는 색상의 의미는 다음과 같습니다.  위의 범례에 나와 있듯이 예제 공격 단계(자격 증명 액세스)에는 맬웨어 노드 accesschk.exe 및 의심스러운 파일 노드 *.pfx 의 링크가 포함되어 있습니다. 이러한 링크를 클릭하면 사이버 킬 체인의 해당 노드로 이동할 수 있습니다. 이러한 노드로 이동하는 방법과 수행 가능한 작업에 대한 자세한 내용은 "사이버 킬 체인의 개별 노드 조사" (830페이지) 항목을 참조하십시오. 공격 단계에는 파일 노드로 이동하는 링크도 포함되어 있습니다. 해당 파일 노드로 이동하면 보호 대상 PHI(개인 건강 정보), 신용카드 번호, 사회 보장 번호 등의 민감한 정보를 포함하는 손상된 파일 관련 정보를 확인할 수 있습니다.

참고

각 공격 단계는 단일 감지 이벤트입니다. 각 단계에서 나열되는 내용(헤더, 타임 스탬프, 기술)은 EDR(Endpoint Detection and Response)이 저장하는 공격 단계 템플릿을 기준으로 하여 감지 이벤트의 특정 매개변수에 따라 생성됩니다.

사이버 킬 체인의 개별 노드 조사

공격 단계를 검토할 수 있을 뿐 아니라 사이버 킬 체인의 각 공격 노드도 살펴볼 수 있습니다. 그러면 사이버 킬 체인의 특정 노드로 드릴다운하여 필요에 따라 각 노드를 조사하고 수정할 수 있습니다.

© Acronis International GmbH, 2003-2024

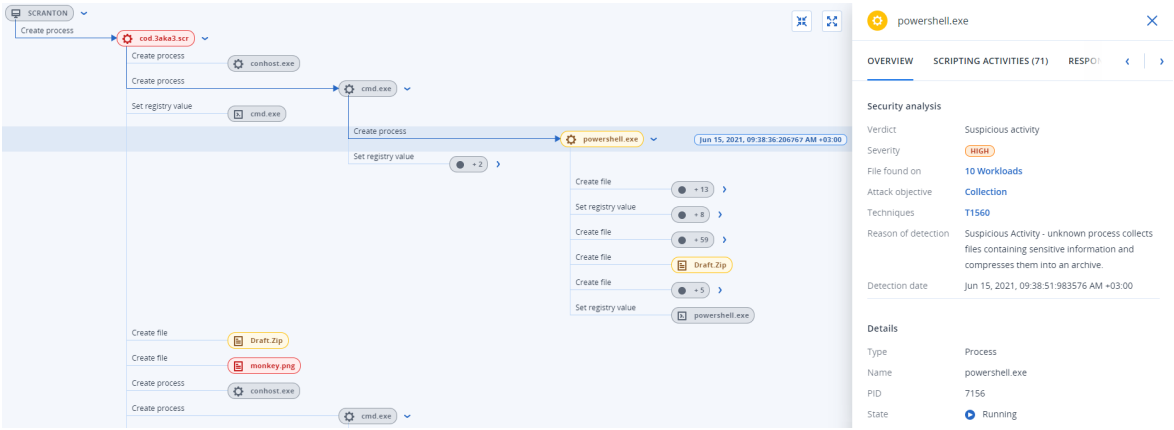
예를 들어 특정 인시던트가 실제 악의적인 공격일 가능성이 어느 정도인지 확인할 수 있습니다. 그리고 조사 결과에 따라 워크로드 분리, 의심스러운 파일 격리 등의 다양한 대응 조치를 노드에 적용할 수도 있습니다.

사이버 킬 체인의 개별 노드를 조사하려면

1. Cyber Protect 콘솔에서 **보호 > 인시던트**로 이동합니다.
2. 표시되는 인시던트 목록에서 조사할 인시던트의 맨 오른쪽 열에 있는 을 클릭합니다. 선택한 인시던트의 사이버 킬 체인이 표시됩니다.
3. 관련 노드로 이동한 후 해당 노드를 클릭하여 노드의 사이드바를 표시합니다.

참고
노드를 클릭하여 확장한 후 관련 노드를 표시합니다.

예를 들어 아래 예제에서 **powershell.exe** 노드를 클릭하면 해당 노드의 사이드바가 열립니다. 노드 옆의 화살표 아이콘을 클릭하여 **powershell.exe** 노드의 영향을 받을 수 있는 관련 노드(파일 및 레지스트리 값 포함)를 확인할 수도 있습니다. 그 후에는 해당 관련 노드를 클릭하여 추가로 조사할 수 있습니다.



4. 사이드바 탭에 포함된 정보를 조사합니다.
   - **개요**: 2개의 주 섹션에서 공격을 받은 노드 관련 보안 요약 정보가 제공됩니다.
     - **보안 분석**: 공격을 받은 노드의 분석 정보를 제공합니다. 이러한 정보에는 위협과 관련한 EDR의 결정 사항(예: 의심스러운 활동), MITRE 공격 기술에 따른 공격의 목표(링크를 클릭하면 MITRE 웹 사이트로 이동 가능), 감지 이유, 공격의 영향을 받을 수 있는 워크로드의 수(**n개 워크로드** 링크를 클릭하면 영향받은 워크로드 확인 가능) 등이 포함됩니다.

참고
n개 워크로드 링크가 표시되는 경우 다른 워크로드에서도 특정 악성 객체 또는 의심스러운 객체가 *발견*되었다는 의미입니다. 즉, 이 링크는 다른 워크로드에서도 공격이 진행되고 있다는 의미가 아니라 해당 워크로드에 침해 지표가 적용된다는 의미입니다. 해당 워크로드에서 공격이 이미 진행되어 다른 인시던트가 생성되었을 수도 있고, 공격자가 공격 "툴킷"을 사용하여 다른 워크로드에 대한 공격을 준비하고 있을 수도 있습니다.

© Acronis International GmbH, 2003-2024

  - **상세 정보**: 노드 관련 상세 정보가 포함됩니다. 이러한 정보에는 노드의 유형/이름/현재 상태, 노드로 이동하는 경로, 그리고 파일 해시와 디지털 서명(예: MD5 및 인증서 일련 번호) 등이 있습니다.
- **스크립트 작업**: 공격에서 호출되거나 로드된 스크립트의 상세 정보가 포함됩니다. 을 클릭하면 스크립트를 클립보드에 복사하여 추가로 조사할 수 있습니다.

참고
스크립트 작업 탭은 명령이나 스크립트(예: cmd 또는 PowerShell 명령)를 실행하는 프로세스 노드에만 표시됩니다.

- **대응 조치**: 노드 유형에 따라 추가 조사, 수정 및 방지 조치를 제공하는 여러 섹션이 포함되어 있습니다.
  예를 들어 워크로드 노드의 경우 포렌식 백업과 백업에서 복원을 비롯한 여러 대응을 정의할 수 있습니다. 악성 노드나 의심스러운 노드의 경우에는 노드를 중지하거나 격리하고, 공격에 의해 적용된 변경 사항을 롤백한 후 보호 계획 허용 목록이나 차단 목록에 해당 노드를 추가할 수 있습니다.
  특정 노드에 대응 조치를 적용하는 방법에 대한 자세한 내용은 "개별 사이버 킬 체인 노드에 대한 대응 조치"(841페이지) 항목을 참조하십시오.
- **작업**: 인시던트에 적용된 작업이 시간순으로 표시됩니다. 자세한 내용은 "인시던트 완화를 위해 수행한 작업 파악"(832페이지)을(를) 참조하십시오.

인시던트 완화를 위해 수행한 작업 파악

인시던트를 검토하고 공격이 발생한 방식을 조사한 후에는 대개 대응 조치를 적용합니다. 적용한 대응 조치는 여러 위치에서 확인할 수 있으므로 인시던트를 완화하기 위해 수행한 단계를 더욱 쉽게 파악할 수 있습니다.

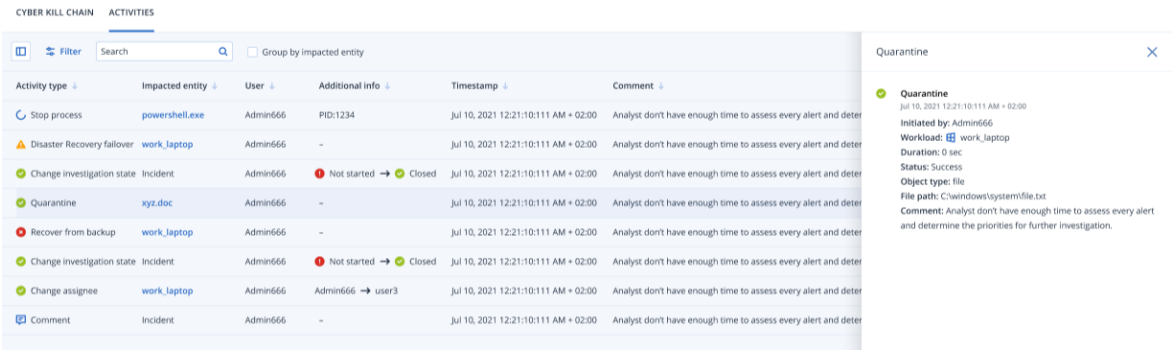
참고
방지 레이어에 의해 인시던트가 생성되면 보호 계획에 구성되어 있는 조치가 자동으로 적용됩니다. 감지 지점이 여러 개이면 각 공격 시나리오를 완화할 수 있는 관련 대응 조치를 정의해야 합니다.

수행한 대응 조치를 파악하려는 경우 전체 인시던트에 적용된 모든 대응 조치를 확인할 수도 있고 인시던트 사이버 킬 체인의 특정 노드에 적용된 조치를 확인할 수도 있습니다.

인시던트에 적용된 모든 대응 조치를 확인하려면

1. Cyber Protect 콘솔에서 **보호 > 인시던트**로 이동합니다.
2. 표시되는 인시던트 목록에서 조사할 인시던트의 맨 오른쪽 열에 있는 을 클릭합니다. 선택한 인시던트의 사이버 킬 체인이 표시됩니다.
3. **작업** 탭을 클릭합니다.
   인시던트에 이미 적용된 대응 조치의 목록이 표시됩니다.

© Acronis International GmbH, 2003-2024

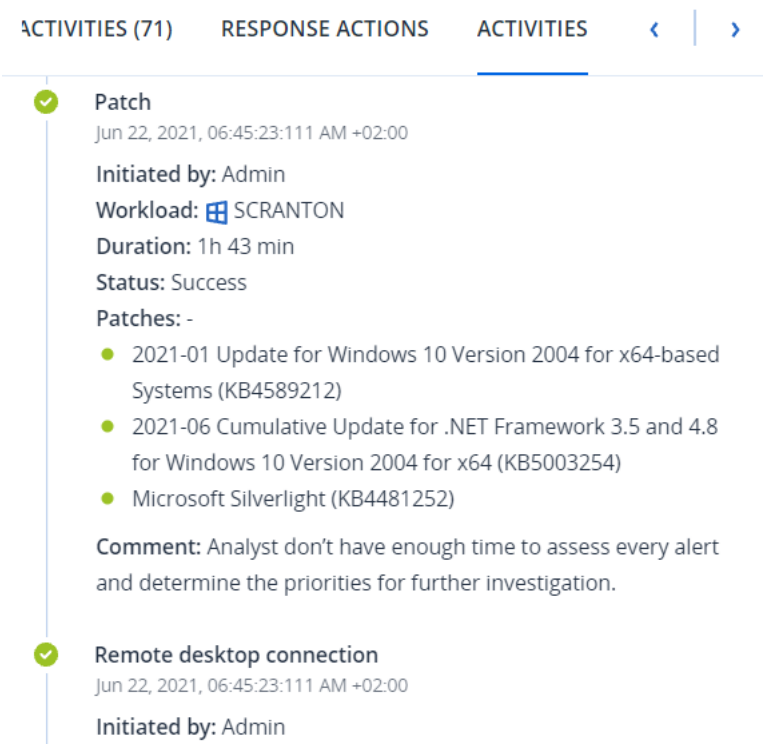


4. 표시된 목록에서 다음과 같은 여러 가지 작업을 수행할 수 있습니다.
   - 활동 유형 열을 클릭하여 선택한 활동에 대한 추가 정보 표시. 정보는 3단계에 나와 있는 것처럼 사이드바에 표시됩니다. 표시되는 정보에는 조치를 시작한 사람, 조치 상태, 파일 경로, 조치를 시작한 사람이 추가한 주석 등의 상세 정보가 포함됩니다.
   - **검색** 박스를 사용하여 특정 조치 검색.
   - **필터**를 클릭하여 목록에 필터 적용.
   - **영향받은 항목별 그룹화** 확인란을 선택하여 항목별로 관련 조치 그룹화.
   - 을 클릭하여 완료한 조치 목록 표시/숨기기.
     표시할 조치 옆에 이 표시되어 있는지 확인합니다. 표시된 목록에서 특정 조치를 숨기려면 해당 아이콘을 다시 클릭하여 으로 변경합니다.

특정 노드에 적용된 대응 조치를 확인하려면

© Acronis International GmbH, 2003-2024

1. 사이버 킬 체인에서 노드를 클릭하여 해당 노드의 사이드바를 표시합니다.
2. **작업** 탭을 클릭합니다.



3. 적용된 조치와 해당 조치가 적용된 이유를 자세히 파악하려는 경우 해당 노드에 적용된 대응 조치를 스크롤해야 할 수 있습니다. 예를 들어 원격 데스크탑 연결 조치의 경우 해당 조치를 시작한 사람과 조치 시작 시간, 조치 소요 시간과 조치의 전체 상태(성공, 실패, 성공했으나 오류 발생)를 확인할 수 있습니다.

워크로드에서 공개된 공격의 침해 지표(IOC) 확인

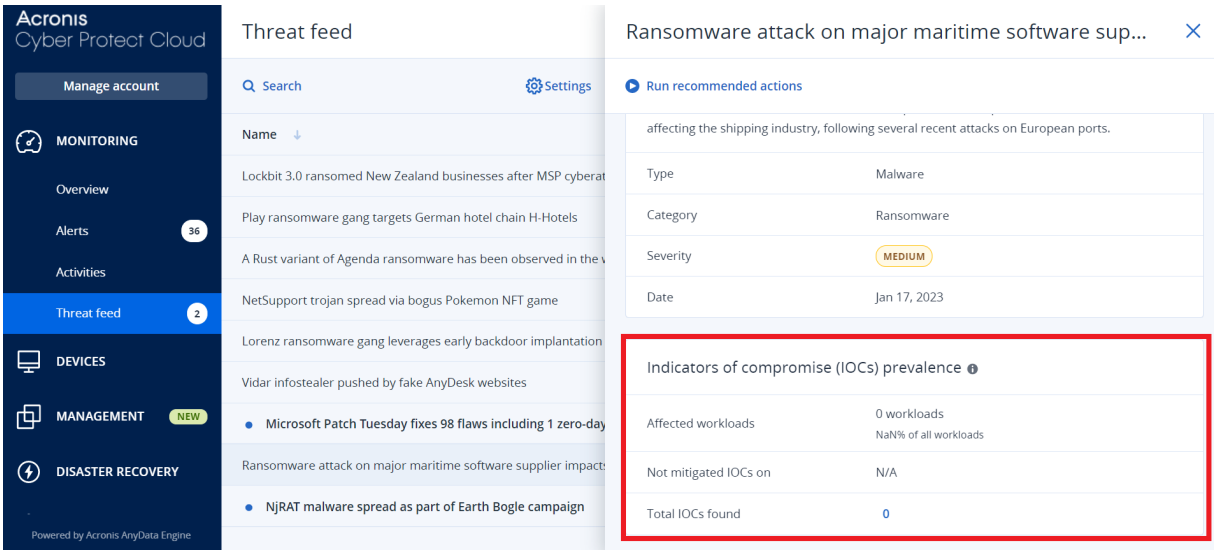
EDR(Endpoint Detection and Response)에는 워크로드를 대상으로 진행된 알려진 기존 공격을 위협 피드에서 검토하는 기능이 포함되어 있습니다. 이러한 위협 피드는 사이버 보호 작업 센터(CPOC)에서 수신된 위협 데이터를 토대로 하여 자동으로 생성됩니다. EDR에서는 위협이 워크로드에 영향을 주는지 여부를 확인한 후 해당 위협을 무력화하는 데 필요한 단계를 진행할 수 있습니다.

Cyber Protect 콘솔의 **모니터링** 메뉴에서 위협 피드에 액세스할 수 있습니다. 자세한 내용은 "위협 피드"(278페이지)을(를) 참조하십시오.

특정 위협 상세 정보를 검토하여 해당 위협이 워크로드에 영향을 주는지 확인하려면 위협 피드를 클릭합니다. 감지된 IOC와 영향을 받는 워크로드 수를 확인할 수 있으며 완화되지 않은 IOC가 포함된 워크로드로 드릴다운할 수 있습니다.

참고
보호 계획에서 EDR이 활성화되어 있지 않으면 아래에 나와 있는 것처럼 이 추가 위협 피드 기능이 표시되지 않습니다.

© Acronis International GmbH, 2003-2024



위협 피드 설정 정의

다양한 위협 피드 설정을 정의하여 알려진 위협을 자동으로 찾아 완화할 수 있습니다.

위협 피드 설정을 정의하려면

1. Cyber Protect 콘솔에서 **모니터링 > 위협 피드**로 이동합니다.
2. 표시되는 위협 피드 페이지에서 **설정**을 클릭합니다.
3. 표시되는 대화 상자에서 다음 옵션 중 하나를 선택합니다.

옵션	설명
침해 지표(IOC) 검색	스위치를 클릭하여 워크로드에서 IOC 자동 검색을 활성화합니다. 이 옵션을 활성화하면 **감지에 대한 작업** 및 **경보 생성** 옵션도 표시됩니다.
감지에 대한 작업	워크로드에서 위협이 검색되면 관련 파일에 수행할 작업을 드롭다운 목록에서 선택합니다. • **작업 없음** • **격리** • **삭제** • **워크로드 분리**
경보 생성	워크로드에서 IOC가 확인되는 경우 경보를 생성하려면 확인란을 선택합니다. 경보는 경보 페이지에 표시됩니다.

4. **적용**을 클릭합니다.

영향받은 워크로드에서 IOC 검토 및 완화

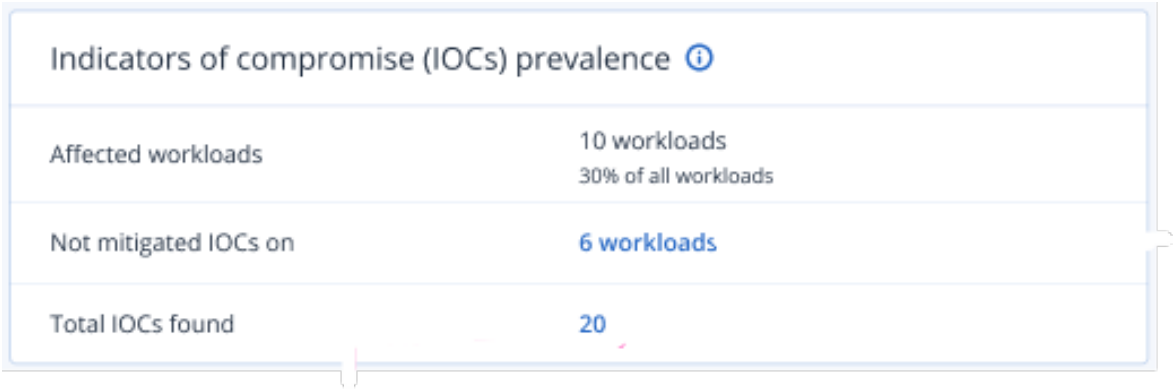
보호 계획에서 EDR(Endpoint Detection and Response)이 활성화되어 있으면 보호 계획에서 워크로드에 영향을 주는 알려진 위협을 확인할 수 있습니다. 자동으로 완화되지 않고 남아 있는 침해 지

© Acronis International GmbH, 2003-2024

표(IOC)도 완화할 수 있습니다. IOC를 자동으로 완화하는 방법에 대한 자세한 내용은 "위협 피드 설정 정의"(835페이지) 항목을 참조하십시오.

영향받은 워크로드를 검토 및 완화하려면

1. Cyber Protect 콘솔에서 **모니터링 > 위협 피드**로 이동합니다.
2. 스레드를 클릭하여 해당 위협의 상세 정보를 표시합니다.
3. **침해 지표(IOC) 배포** 섹션에서 ***n*개 워크로드** 링크를 클릭하여 완화되지 않은 IOC가 포함된 워크로드를 확인합니다.



4. 표시되는 워크로드 페이지에서 관련 워크로드를 클릭하여 해당 상세 정보를 검토합니다. 워크로드에서 특정 기능을 실행할 수 있습니다. 가령 필터링할 추가 URL을 정의하거나("URL 필터링"(769페이지) 참조) 악의적인 프로세스를 차단("안티바이러스 및 맬웨어 방지 기능 설정"(748페이지)의 제외 항목 섹션 참조)할 수 있습니다.
   예를 들어 워크로드가 IOC의 영향을 받았다는 내용이 위협 피드에 표시되면 먼저 "검색된 IOC 검토 및 분석"(836페이지)의 설명에 따라 IOC를 찾아서 분석합니다. 그런 다음 워크로드의 보호 계획으로 이동하여 추가 보호 방법(예: 악의적인 파일 해시나 프로세스 차단)을 정의합니다.

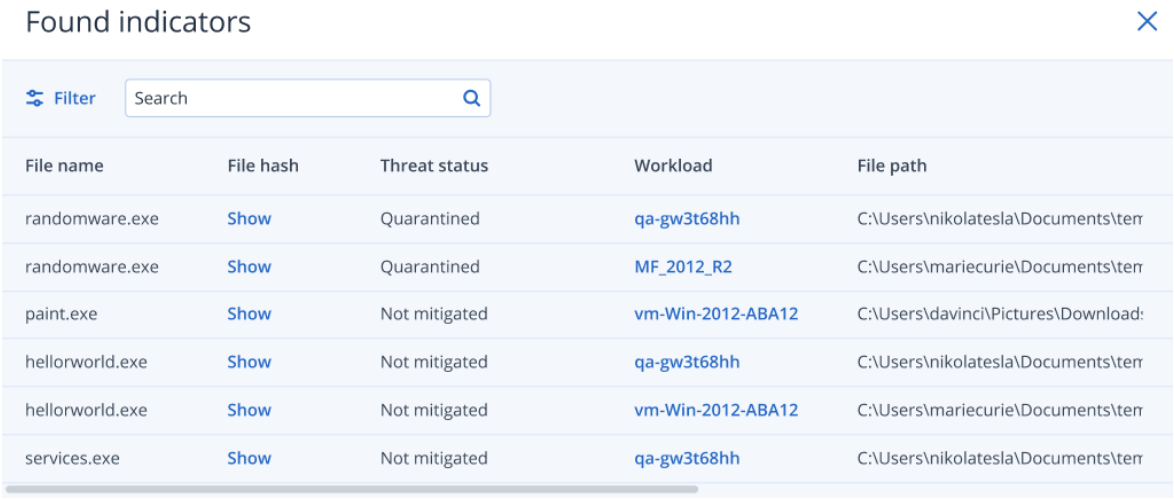
검색된 IOC 검토 및 분석

알려진 위협의 영향을 받은 워크로드를 검토할 수 있을 뿐 아니라 특정 침해 지표(IOC)도 검토 및 분석할 수 있습니다. 그러면 IOC의 영향을 받는 개별 워크로드를 확인하고 IOC를 완화할 수 있습니다.

IOC를 검토 및 분석하려면

1. Cyber Protect 콘솔에서 **모니터링 > 위협 피드**로 이동합니다.
2. 스레드를 클릭하여 해당 위협의 상세 정보를 표시합니다.
3. **침해 지표(IOC) 배포** 섹션에서 **확인된 총 IOC 수** 링크를 클릭합니다.
   확인된 지표 페이지가 표시됩니다.

© Acronis International GmbH, 2003-2024



4. (선택 사항) **필터** 옵션을 사용하여 상태에 따라 IOC 목록을 필터링합니다. **검색** 옵션을 사용하여 특정 IOC를 검색할 수도 있습니다.
5. IOC의 영향을 받는 워크로드를 확인하려면 **워크로드** 열의 링크를 클릭합니다. 그런 다음 패치 관리 실행, 보호 계획 수정 등의 다양한 작업을 워크로드에서 수행할 수 있습니다.
6. (선택 사항) **파일 해시** 열에서 **표시**를 클릭하여 특정 IOC와 관련하여 발견된 파일 해시를 표시합니다. 표시되는 대화 상자에서 을 클릭하여 IOC의 파일 해시를 텍스트 편집기에 복사합니다.

인시던트 수정

EDR(Endpoint Detection and Response)에서는 전체 인시던트나 특정 인시던트의 개별 공격 지점을 수정할 수 있습니다.

전체 인시던트를 수정할 때는 인시던트 전체에서 실행할 수정 작업을 선택할 수 있습니다. 인시던트를 더욱 세부적으로 관리해야 한다면 필요에 따라 개별 공격 지점을 수정할 수 있습니다. 예를 들어 워크로드의 네트워크 분리를 관리하여 횡적 확산과 명령 및 제어(C&C) 활동을 중지할 수 있습니다. 그러면 워크로드가 분리되어 있어도 모든 Acronis Cyber Protect 기술이 계속 작동하므로 조사를 시작할 수 있습니다.

EDR에서는 다음 작업을 통해 인시던트를 효율적으로 수정할 수 있습니다.

- 완화 - 위협을 중지합니다.
- 복구 - 서비스를 즉시 온라인 상태로 다시 설정합니다.
- 방지 - 공격에 사용된 기술이 향후 공격에서 다시 사용되지 않도록 방지합니다.

전체 인시던트 수정

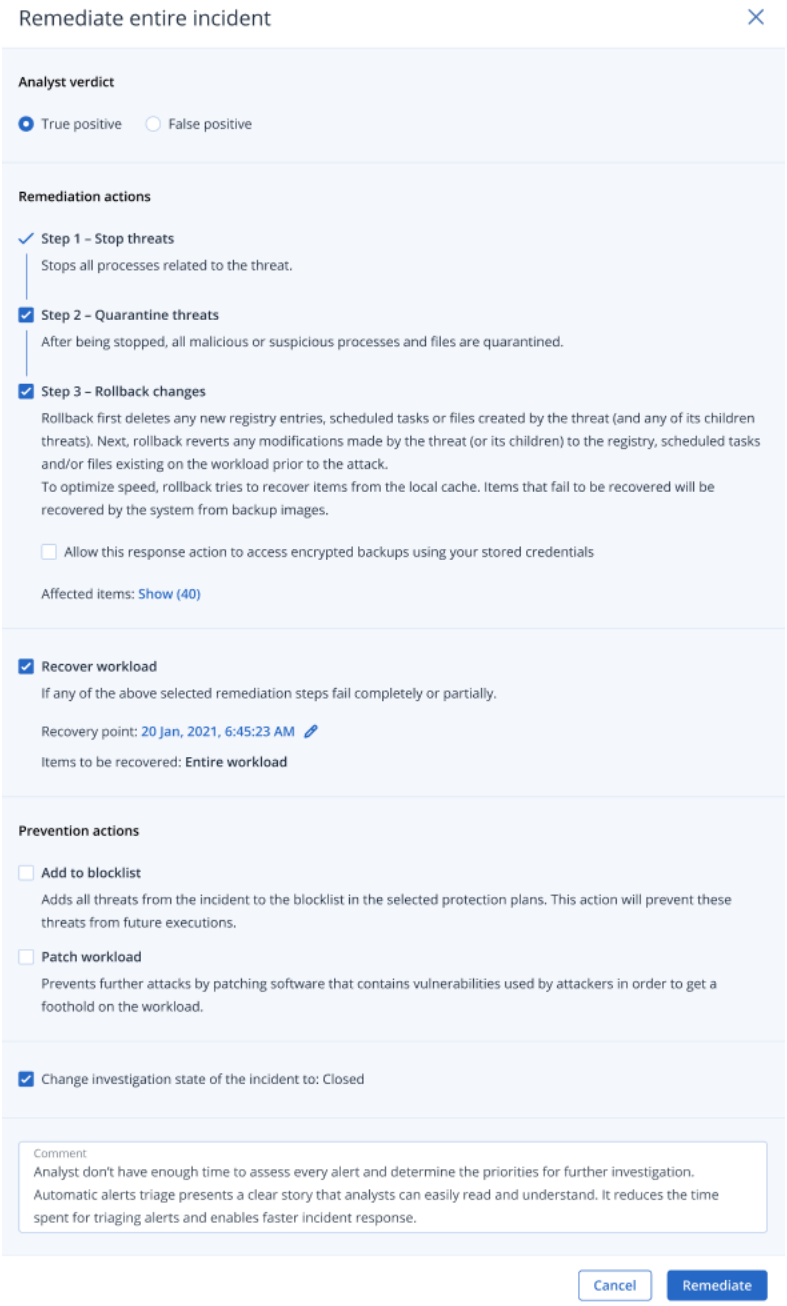
전체 인시던트를 수정할 때는 인시던트 전체에서 실행할 수정 작업을 빠르고 쉽게 선택할 수 있습니다. EDR(Endpoint Detection and Response)에서는 단계별 수정 프로세스를 안내합니다.

네트워크와 인시던트를 더욱 세부적으로 관리해야 한다면 "개별 사이버 킬 체인 노드에 대한 대응 조치"(841페이지) 항목을 참조하십시오.

전체 인시던트를 수정하려면

© Acronis International GmbH, 2003-2024

1. Cyber Protect 콘솔에서 **보호 > 인시던트**로 이동합니다.
2. 표시되는 인시던트 목록에서 조사할 인시던트의 맨 오른쪽 열에 있는 을 클릭합니다. 선택한 인시던트의 사이버 킬 체인이 표시됩니다.
3. **전체 인시던트 수정**을 클릭합니다. 전체 인시던트 수정 대화 상자가 표시됩니다.



4. **분석 결정** 섹션에서 인시던트 조사 결과에 따라 다음 중 하나를 선택합니다.
   - **진양성**: 공격이 실제 공격임이 확실한 경우 선택합니다. 이 옵션을 선택한 후에는 다음 단계의 설명에 따라 수정 및 방지 조치를 수행할 수 있습니다.
   - **위양성**: 공격이 실제 공격이 아님이 확실한 경우 선택합니다. 이 모드에서는 공격 재발 방지 방법을 정의할 수 있습니다. 예를 들어 보호 계획 허용 목록에 인시던트를 추가할 수 있습니다.

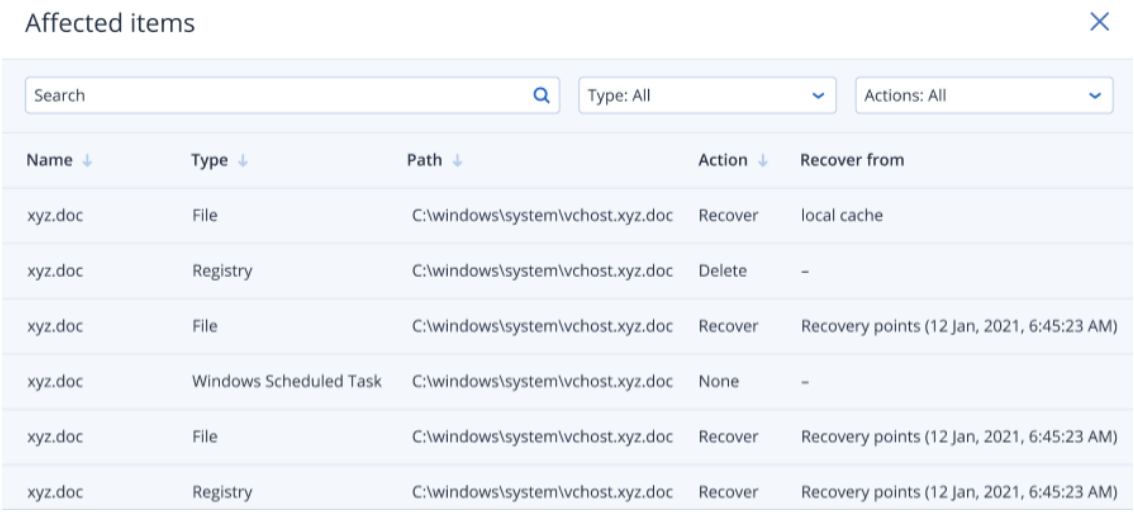
© Acronis International GmbH, 2003-2024

참고
위양성을 선택한 후에는 방지 조치만 정의할 수 있습니다. 자세한 내용은 "위양성 인시던트 수정"(841페이지)을(를) 참조하십시오.

5. **수정 작업** 섹션에서 다음 수정 단계를 수행합니다. 수정 단계는 순서대로 수행해야 합니다. 예를 들어 1단계를 완료하기 전에 2단계를 선택할 수는 없습니다.
   a. **1단계 - 위협 중지**: 위협과 관련된 모든 프로세스를 중지하려면 이 확인란을 선택합니다.
   b. **2단계 - 위협 격리**: 위협이 중지된 후 악의적인/의심스러운 프로세스 및 파일을 모두 격리하려면 이 확인란을 선택합니다.
   c. **3단계 - 변경 사항 롤백**: 위협이 격리된 후 위협 및 해당 자식 위협에 의해 생성된 모든 새 레지스트리 항목, 예약된 작업 또는 파일을 삭제하려면 이 확인란을 선택합니다. 그러면 롤백 프로세스에서 위협과 해당 자식 위협으로 인해 공격 전에 워크로드에 있었던 레지스트리, 예약된 작업 및/또는 파일에 적용된 수정 사항을 원래 상태로 되돌립니다. 롤백 프로세스는 속도를 최적화하기 위해 로컬 캐시에서 항목을 복구하려고 시도합니다. 복구에 실패한 항목은 시스템이 백업 이미지에서 복구합니다.

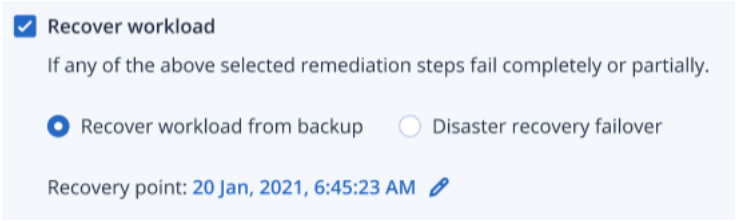
   참고
   롤백 프로세스에서는 로컬 캐시의 항목에서만 복구를 수행합니다. 백업 아카이브로부터의 롤백은 향후 릴리스에서 제공될 예정입니다.

   액세스하려는 관련 백업이 암호화되어 있는 경우 **이 대응 작업에서 저장된 자격 증명을 사용하여 암호화된 백업에 액세스하도록 허용** 확인란을 선택합니다. 그러면 EDR이 저장된 사용자 자격 증명에 액세스하여 암호화된 아카이브를 해독한 후 관련 파일을 검색합니다.
   영향받은 항목을 클릭하여 롤백의 영향을 받는 모든 항목(파일, 레지스트리 또는 예약된 작업), 적용된 작업(**삭제**, **복구** 또는 **없음**), 그리고 해당 항목을 복원 중인 위치(로컬 캐시 또는 백업 이미지)를 확인할 수도 있습니다.



   d. **워크로드 복구**: 위의 수정 단계 중 하나라도 완전히 또는 부분적으로 실패하는 경우 워크로드를 복구하려면 이 확인란을 선택합니다.

© Acronis International GmbH, 2003-2024



다음 복구 옵션 중 하나를 선택합니다.

- **백업에서 워크로드 복구**: 특정 복구 지점에서 워크로드를 복구할 수 있습니다. 복구 지점 편집 아이콘을 클릭하여 복구 백업 목록에서 원하는 백업을 선택합니다.
- **재해 복구 장애 조치**: 보호 계획에서 재해 복구 기능을 활성화한 경우 재해 복구를 실행할 수 있습니다. AD 서버나 데이터베이스 서버 등의 중요한 워크로드에는 이 옵션을 사용하는 것이 좋습니다. 자세한 내용은 "재해 복구 구현"(666페이지)을(를) 참조하십시오.

6. **방지 조치** 섹션에서 관련 수정 단계를 선택합니다.
   - **차단 목록에 추가**: 확인란을 선택하고 표시되는 보호 계획 목록에서 관련 보호 계획을 선택합니다. 이 방지 조치를 수행하면 선택한 보호 계획에서는 해당 인시던트 감지의 실행이 차단됩니다.
   - **워크로드 패치**: 취약한 소프트웨어를 패치하고 공격자의 워크로드 액세스 권한 확보를 방지하려면 이 확인란을 선택합니다. 그런 후에 패치가 완료되면 사용자의 로그인 여부에 따라 수행할 관련 작업(**다시 시작 안 함**, **다시 시작** 또는 **필요한 경우에만 다시 시작**)을 선택할 수 있습니다.
     백업 중에는 워크로드가 다시 시작되지 않도록 **백업이 진행되는 동안 다시 시작 안 함** 확인란을 선택할 수도 있습니다.

7. **인시던트의 조사 상태를 다음으로 변경: 종결됨** 확인란을 선택합니다. 이 확인란을 선택하지 않으면 조사 상태가 이전 상태로 유지됩니다.
8. **수정**을 클릭합니다. 선택한 수정 작업이 단계별로 실행되며 전체 인시던트 수정 대화 상자에 각 수정 단계의 진행률이 표시됩니다.
   그러면 버튼이 **작업으로 이동**으로 바뀝니다. **작업으로 이동**을 클릭하여 인시던트에 적용된 모든 대응 조치를 검토합니다. 자세한 내용은 "인시던트 완화를 위해 수행한 작업 파악"(832페이지)을(를) 참조하십시오.

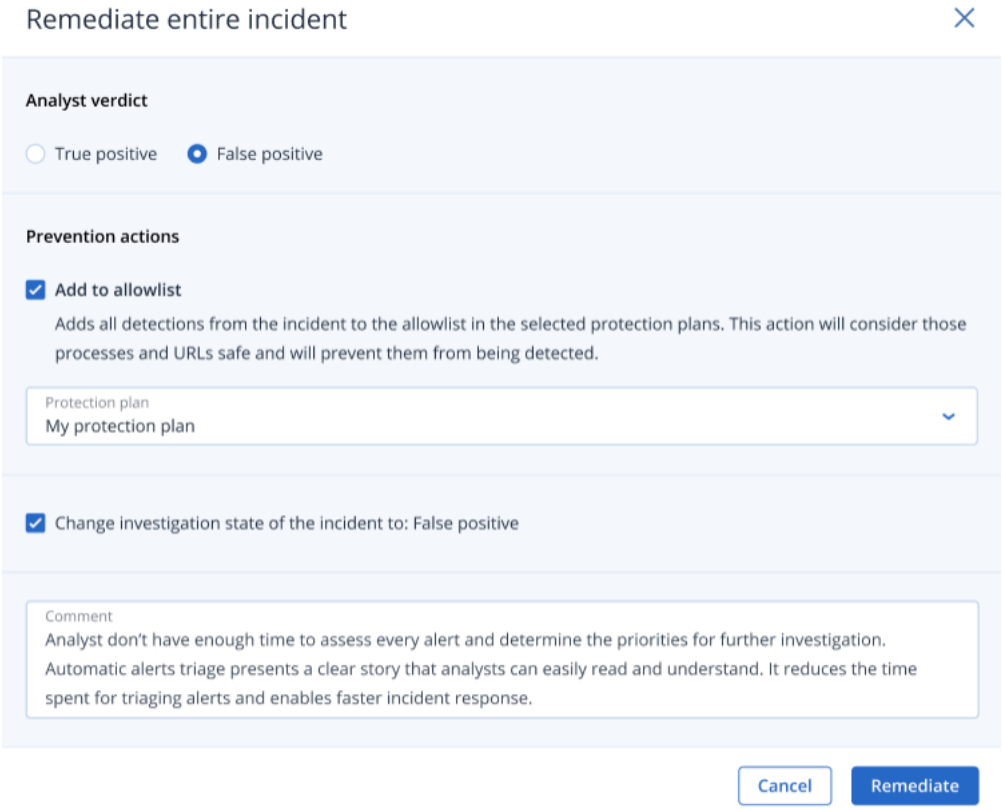
© Acronis International GmbH, 2003-2024

위양성 인시던트 수정

특정 공격이 실제 공격이 아닌 "위양성" 공격이라고 생각된다면 인시던트 재발 방지 방법을 정의할 수 있습니다. 예를 들어 보호 계획 허용 목록에 해당 인시던트를 추가할 수 있습니다.

위양성 인시던트를 수정하려면

1. 선택한 인시던트의 사이버 킬 체인에서 **전체 인시던트 수정**을 클릭합니다. 전체 인시던트 수정 대화 상자가 표시됩니다.
2. **분석 결정** 섹션에서 **위양성**을 선택합니다.



3. **방지 조치** 섹션에서 **허용 목록에 추가** 확인란을 선택합니다. 표시되는 보호 계획 목록에서 관련 보호 계획을 선택합니다.
   이 방지 조치를 수행하면 선택한 보호 계획에서는 해당 인시던트가 전혀 감지되지 않습니다.
4. **인시던트의 조사 상태를 다음으로 변경: 위양성** 확인란을 선택합니다.
5. **수정**을 클릭합니다.
   그러면 버튼이 **작업으로 이동**으로 바뀝니다. **작업으로 이동**을 클릭하여 인시던트에 적용된 대응 조치를 검토합니다. 자세한 내용은 "인시던트 완화를 위해 수행한 작업 파악"(832페이지)을(를) 참조하십시오.

개별 사이버 킬 체인 노드에 대한 대응 조치

인시던트를 더욱 세부적으로 관리해야 한다면 개별 사이버 킬 체인 노드에 다양한 대응 조치를 적용할 수 있습니다. 이러한 대응 조치를 적용하면 어떤 노드든 빠르고 쉽게 수정할 수 있습니다.

© Acronis International GmbH, 2003-2024

참고
전체 인시던트에 글로벌 대응 조치를 적용하려는 경우에는 "전체 인시던트 수정"(837페이지) 항목을 참조하십시오.

대응 조치는 다음 카테고리로 구분되지만 모든 노드에 다음 카테고리가 모두 포함되는 것은 아닙니다.

- **수정**: 이 카테고리의 조치를 수행하면 공격에 대한 대응 조치를 즉시 적용할 수 있습니다. 이러한 조치에는 워크로드의 네트워크 분리 관리, 파일/프로세스/레지스트리 값 삭제와 격리 등이 있습니다.
- **조사**: 이 카테고리의 조치(워크로드에만 해당되는 조치)를 수행하면 포렌식 백업을 실행하거나 심층 조사를 위한 원격 데스크탑 연결을 설정할 수 있습니다.
- **조사**: 이 카테고리의 조치(워크로드에만 해당되는 조치)를 수행하면 심층 조사를 위한 원격 데스크탑 연결을 실행할 수 있습니다.
- **복구**: 이 카테고리의 조치(워크로드에만 해당되는 조치)를 수행하면 백업에서 복구 또는 재해 복구 장애 조치를 실행하여 집중 공격에 대응할 수 있습니다.
- **방지**: 이 카테고리의 조치를 수행하면 특정 위협이나 위양성을 보호 계획 허용 목록 또는 차단 목록에 추가하여 향후 해당 위협이나 위양성과 관련된 인시던트 발생을 방지할 수 있습니다.

참고
인시던트가 종결되면 노드에 대응 조치를 적용할 수 없습니다. 그러나 조사 상태를 **조사 중**으로 변경하면 종결된 인시던트를 다시 열 수 있습니다. 인시던트를 다시 연 후 대응 조치를 적용할 수 있습니다.

아래 표에는 사이버 킬 체인의 각 노드 유형, 각 노드에 해당하는 카테고리 및 수행 가능한 대응 조치가 설명되어 있습니다.

노드	카테고리	대응 조치
워크로드	수정	• 네트워크 분리 관리 • 워크로드 다시 시작
	조사	• 포렌식 백업 • 원격 데스크톱 연결
	조사	• 원격 데스크톱 연결

© Acronis International GmbH, 2003-2024

노드	카테고리	대응 조치
	복구	• 백업에서 복구 • 재해 복구 장애 조치
	방지	• 패치
프로세스	수정	• 프로세스 중지 • 격리
	방지	• 허용 목록에 추가 • 차단 목록에 추가
파일	수정	• 삭제 • 격리
	방지	• 허용 목록에 추가 • 차단 목록에 추가
레지스트리	수정	• 삭제
네트워크	방지	• 허용 목록에 추가 • 차단 목록에 추가

영향을 받은 워크로드에 대한 대응 조치 정의

공격 대응의 일환으로 영향을 받은 워크로드에 다음 조치를 적용할 수 있습니다.

- **네트워크 분리 관리**: 워크로드의 네트워크 분리를 관리하여 횡적 확산과 명령 및 제어(C&C) 활동을 중지할 수 있습니다. 자세한 내용은 "워크로드의 네트워크 분리 관리"(844페이지)을(를) 참조하십시오.

© Acronis International GmbH, 2003-2024

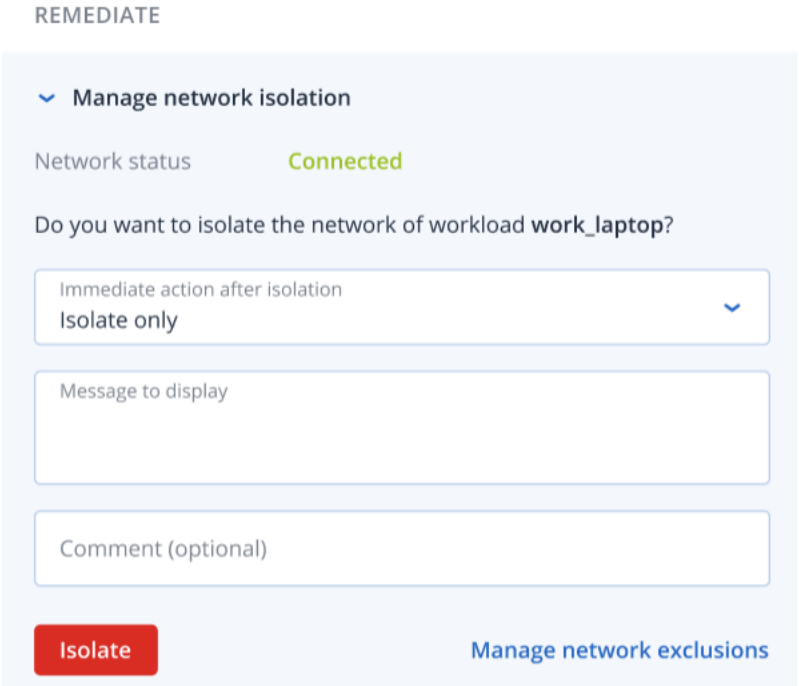
- **패치**: 향후 발생 가능한 공격에서 취약성의 추가 악용을 방지하기 위해 워크로드를 패치할 수 있습니다. 자세한 내용은 "워크로드 패치"(847페이지)을(를) 참조하십시오.
- **워크로드 다시 시작**: 워크로드를 즉시 다시 시작하거나 사전 정의된 시간 초과 기간에 따라 다시 시작할 수 있습니다. 자세한 내용은 "워크로드 다시 시작"(849페이지)을(를) 참조하십시오.
- **포렌식 백업**: 감사 또는 추가 조사를 위해 온디맨드 포렌식 백업을 수행할 수 있습니다. 자세한 내용은 "워크로드에서 온디맨드 포렌식 백업 실행"(850페이지)을(를) 참조하십시오.
- **원격 데스크탑 연결**: 조사 중인 워크로드에 원격으로 액세스할 수 있습니다. 자세한 내용은 "워크로드에 대한 원격 연결"(851페이지)을(를) 참조하십시오.
- **백업에서 복구**: 백업에서 전체 머신이나 특정 파일 또는 폴더를 복구할 수 있습니다. 자세한 내용은 "백업에서 복구"(851페이지)을(를) 참조하십시오.
- **재해 복구 장애 조치**: "재해 복구 구현"(666페이지)을(를) 실행할 수 있습니다. 워크로드에 Advanced Disaster Recovery 구독이 있어야 합니다. 자세한 내용은 "재해 복구 장애 조치"(852페이지)을(를) 참조하십시오.

워크로드의 네트워크 분리 관리

EDR에서는 워크로드의 네트워크 분리를 관리하여 횡적 확산과 명령 및 제어(C&C) 활동을 중지할 수 있습니다. 요구 사항에 따라 다양한 분리 옵션 중에서 선택할 수 있습니다. 모든 Acronis Cyber Protect 기술은 워크로드가 분리되어 있어도 작동하므로 철저한 조사를 진행할 수 있습니다.

네트워크에서 워크로드를 분리하려면

1. 사이버 킬 체인에서 수정할 워크로드 노드를 클릭합니다.
2. 표시되는 사이드바에서 **대응 조치** 탭을 클릭합니다.
3. **수정** 섹션에서 **네트워크 분리 관리**를 클릭합니다.



© Acronis International GmbH, 2003-2024

참고
네트워크 상태 값은 워크로드가 현재 연결되어 있는지 여부를 나타냅니다. 값이 **분리됨**으로 표시되면 아래 절차에 설명되어 있는 것처럼 분리된 워크로드를 네트워크에 다시 연결할 수 있습니다. 오프라인인 워크로드도 분리할 수 있습니다. 이 경우 해당 워크로드는 다시 온라인 상태가 되면 자동으로 **분리됨** 상태가 됩니다.

4. **분리 후 즉각적인 작업** 드롭다운 목록에서 다음 중 하나를 선택합니다.
   - **분리만**
   - **워크로드 분리 및 백업**
   - **포렌식 데이터가 있는 워크로드 분리 및 백업**
   - **워크로드 분리 및 전원 끄기**

   워크로드를 백업할 위치와 암호화 옵션을 정의하는 방법에 대한 자세한 내용은 "워크로드와 파일의 백업 및 복구 관리"(361페이지) 항목을 참조하십시오.
5. [선택 사항] 분리된 워크로드에 액세스하는 최종 사용자에게 표시할 메시지를 **표시할 메시지** 필드에 추가합니다. 예를 들어 워크로드가 현재 분리되어 있으며 네트워크에서 해당 워크로드로의 액세스와 해당 워크로드에서 네트워크로의 액세스는 현재 불가능하다는 정보를 사용자에게 제공할 수 있습니다. 이 메시지는 트레이 모니터 알림으로도 표시되며 사용자가 해제할 때까지 표시된 상태로 유지됩니다.
6. [선택 사항] **주석** 필드에 주석을 추가합니다. 이 주석은 단일 노드나 전체 인시던트의 **활동** 탭에 표시되므로 작성자 본인이나 동료가 인시던트를 다시 확인할 때 해당 조치를 취한 이유를 파악할 수 있습니다.
7. **네트워크 제외 항목 관리**를 클릭하여 분리 상태에서 워크로드에 액세스할 수 있는 포트, URL, 호스트 이름 및 IP 주소를 추가합니다. 자세한 내용은 네트워크 제외 항목을 관리하는 방법을 참조하십시오.
8. **분리**를 클릭합니다.
   워크로드가 분리됩니다. 개별 노드와 전체 인시던트의 **활동** 탭에서도 이 조치를 확인할 수 있습니다. 자세한 내용은 "인시던트 완화를 위해 수행한 작업 파악"(832페이지)을(를) 참조하십시오.

참고
해당 워크로드는 Cyber Protect 콘솔의 **워크로드** 메뉴에서도 **분리됨**으로 표시됩니다. **워크로드 > 에이전트가 있는 워크로드** 메뉴에서도 워크로드를 하나 이상 분리할 수 있습니다. 이렇게 하려면 관련 워크로드를 선택하고 오른쪽 사이드바에서 **네트워크 분리 관리**를 선택합니다. 표시되는 대화 상자에서 네트워크 제외 항목을 관리할 수 있으며, **분리** 또는 **모두 분리**를 클릭하여 선택한 워크로드를 분리할 수 있습니다.

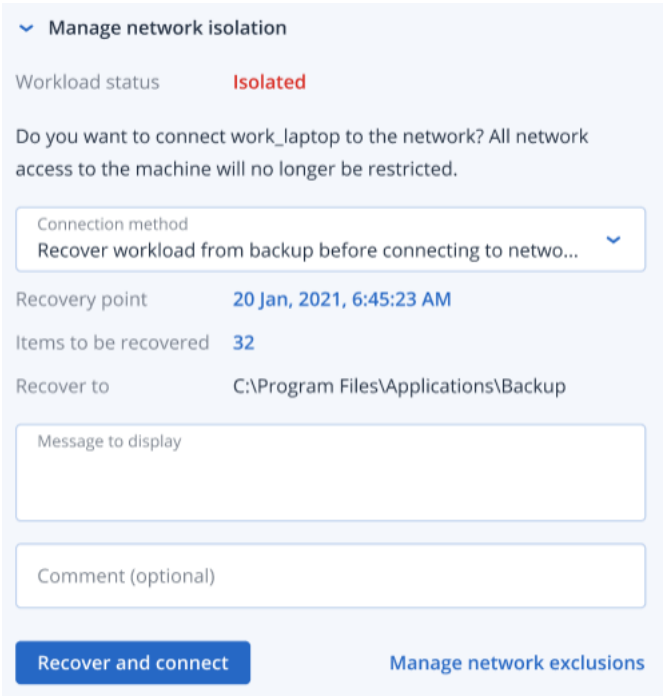
분리된 워크로드를 네트워크에 다시 연결하려면

© Acronis International GmbH, 2003-2024

1. 사이버 킬 체인에서 다시 연결할 워크로드 노드를 클릭합니다.

참고
분리된 워크로드가 현재 오프라인이라도 네트워크에 다시 연결할 수 있습니다. 이 경우 해당 워크로드는 다시 온라인 상태가 되면 자동으로 **연결됨** 상태가 됩니다.

2. 표시되는 사이드바에서 **대응 조치** 탭을 클릭합니다.
3. **수정** 섹션에서 **네트워크 분리 관리**를 클릭합니다.
4. 다음 중 하나를 선택합니다.
   - **네트워크에 즉시 연결**: 워크로드가 네트워크에 다시 연결됩니다.
   - **네트워크에 연결하기 전에 백업에서 워크로드 복구**: 워크로드를 복구할 복구 지점을 선택합니다.
     a. **복구 지점** 필드에서 **선택**을 클릭합니다.
     b. 표시되는 사이드바에서 관련 복구 지점을 선택합니다.
     c. **복구 > 전체 워크로드**를 클릭하여 워크로드의 모든 파일과 폴더를 복구합니다.
     또는
     복구 > 파일/폴더를 클릭하여 워크로드의 특정 파일과 폴더를 복구합니다. 그러면 관련 파일이나 폴더를 선택하라는 메시지가 표시됩니다. 파일이나 폴더를 선택한 후 **복구할 항목** 필드에서 관련 값을 클릭하여 항목 목록을 확인할 수 있습니다.



참고
암호화된 복구 지점을 선택하면 비밀번호를 입력하라는 메시지가 표시됩니다.

5. [선택 사항] **필요할 때 자동으로 워크로드 다시 시작** 확인란을 선택합니다. 이 옵션은 4단계에서 **복구 > 전체 워크로드**를 선택한 경우에만 사용 가능합니다.

© Acronis International GmbH, 2003-2024

6. [선택 사항] 연결된 워크로드에 액세스하는 최종 사용자에게 표시할 메시지를 **표시할 메시지** 필드에 추가합니다. 예를 들어 워크로드에 백업이 복원되었으며 네트워크에서 해당 워크로드로의 액세스와 해당 워크로드에서 네트워크로의 액세스가 다시 가능해졌다는 정보를 사용자에게 제공할 수 있습니다.
7. [선택 사항] **주석** 필드에 주석을 추가합니다. 이 주석은 단일 노드나 전체 인시던트의 **활동** 탭에 표시되므로 작성자 본인이나 동료가 인시던트를 다시 확인할 때 해당 조치를 취한 이유를 파악할 수 있습니다.
8. 4단계에서 **네트워크에 즉시 연결**을 선택한 경우 **연결**을 클릭합니다.
   또는
   4단계에서 **네트워크에 연결하기 전에 백업에서 워크로드 복구**를 선택한 경우 **복구 및 연결**을 클릭합니다.
   워크로드가 네트워크에 다시 연결되며 네트워크에서 워크로드로의 모든 연결이 더 이상 제한되지 않습니다.

참고
Cyber Protect 콘솔의 **워크로드 > 에이전트가 있는 워크로드** 메뉴에서도 분리된 워크로드를 하나 이상 연결할 수 있습니다. 이렇게 하려면 관련 워크로드를 선택하고 오른쪽 사이드바에서 **네트워크 분리 관리**를 선택합니다. 표시되는 대화 상자에서 **연결** 또는 **모두 연결**을 클릭하여 선택한 워크로드를 네트워크에 다시 연결합니다.

네트워크 제외 항목을 관리하려면

참고
워크로드가 분리되어 있어도 모든 Acronis Cyber Protect 기술은 작동하지만, 워크로드에서 공유 디렉토리에 파일을 업로드해야 하는 경우 등 추가 네트워크 연결을 설정해야 하는 상황도 있습니다. 이러한 상황에서는 네트워크 제외 항목을 추가할 수 있습니다. 단, 제외 항목을 추가하기 전에 위협을 제거해야 합니다.

1. **대응 조치** 탭의 **수정** 섹션에서 **네트워크 제외 항목 관리**를 클릭합니다.
2. 네트워크 제외 항목 사이드바에서 관련 제외 항목을 추가합니다. 사용 가능한 각 옵션(포트, URL 주소 및 호스트 이름/IP 주소)에 대해 다음을 수행합니다.
   a. **추가**를 클릭한 후 관련 포트, URL 주소 또는 호스트 이름/IP 주소를 입력합니다.
   b. **트래픽 방향** 드롭다운 목록에서 **들어오는 연결 및 나가는 연결**, **들어오는 연결만** 또는 **나가는 연결만** 중 하나를 선택합니다.
   c. **추가**를 클릭합니다.
3. **저장**을 클릭합니다.

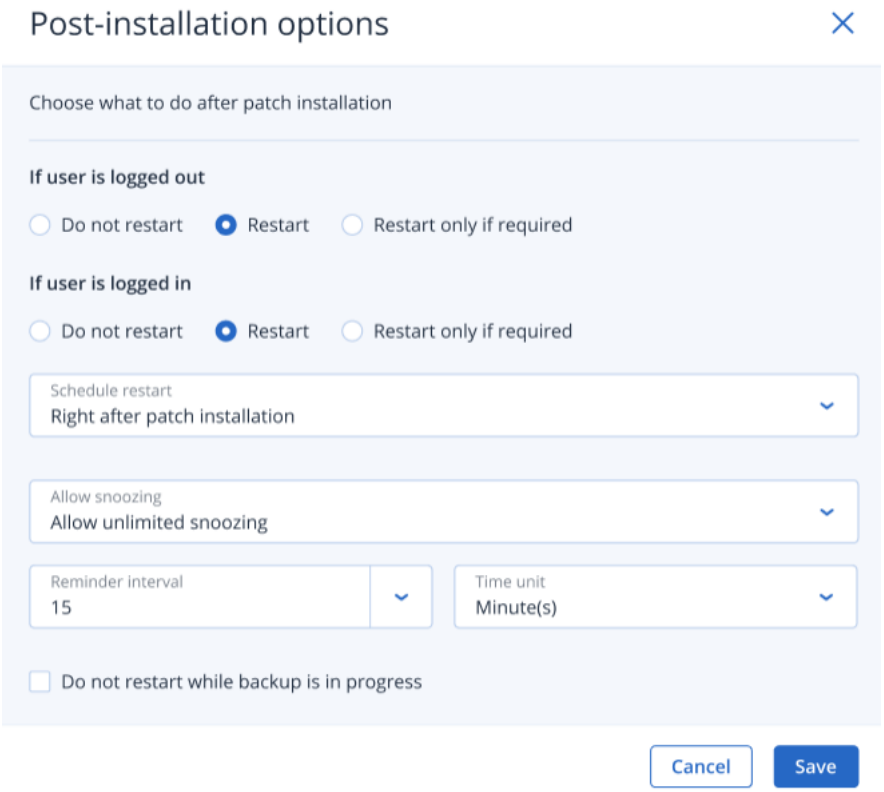
워크로드 패치

EDR은 워크로드를 패치해야 하는지를 자동으로 감지합니다. 그러므로 향후 발생 가능한 공격에서 취약성 익스플로잇을 방지하기 위해 워크로드를 패치할 수 있습니다. 파트너 워크로드에 Advanced Management 구독이 있어야 이 기능을 사용할 수 있습니다.

워크로드를 패치하려면

© Acronis International GmbH, 2003-2024

1. 사이버 킬 체인에서 패치할 워크로드 노드를 클릭합니다.
2. 표시되는 사이드바에서 **대응 조치** 탭을 클릭합니다.
3. **수정** 섹션에서 **패치**를 클릭합니다.
4. **설치할 패치** 필드에서 **선택**을 클릭합니다. 표시되는 대화 상자에서 관련 패치를 선택하고 **선택**을 클릭합니다.
5. **설치 후 옵션** 필드에서 표시되는 링크를 클릭합니다. 설치 후 옵션 대화 상자가 표시됩니다.



6. 패치를 설치한 후에 수행할 작업을 선택합니다.
   - **사용자가 로그아웃한 경우: 다시 시작 안 함, 다시 시작** 또는 **필요한 경우에만 다시 시작** 중 하나를 선택합니다.
   - **사용자가 로그인되어 있는 경우: 다시 시작 안 함, 다시 시작** 또는 **필요한 경우에만 다시 시작** 중 하나를 선택합니다.
     다시 시작을 선택하면 다음 항목도 정의할 수 있습니다.
     - 다시 시작 예약.
     - 다시 알림 허용(다시 알림 사이의 정의된 간격 포함).
7. [선택 사항] 현재 백업이 진행 중인 경우 워크로드가 다시 시작되지 않도록 하려면 **백업이 진행되는 동안 다시 시작 안 함** 확인란을 선택합니다.
8. **저장**을 클릭합니다.
9. **대응 조치** 탭에서 **패치**를 클릭합니다.
   선택한 패치가 실행됩니다. 개별 노드와 전체 인시던트의 **활동** 탭에서도 이 조치를 확인할 수 있습니다. 자세한 내용은 "인시던트 완화를 위해 수행한 작업 파악"(832페이지)을(를) 참조하십시오.

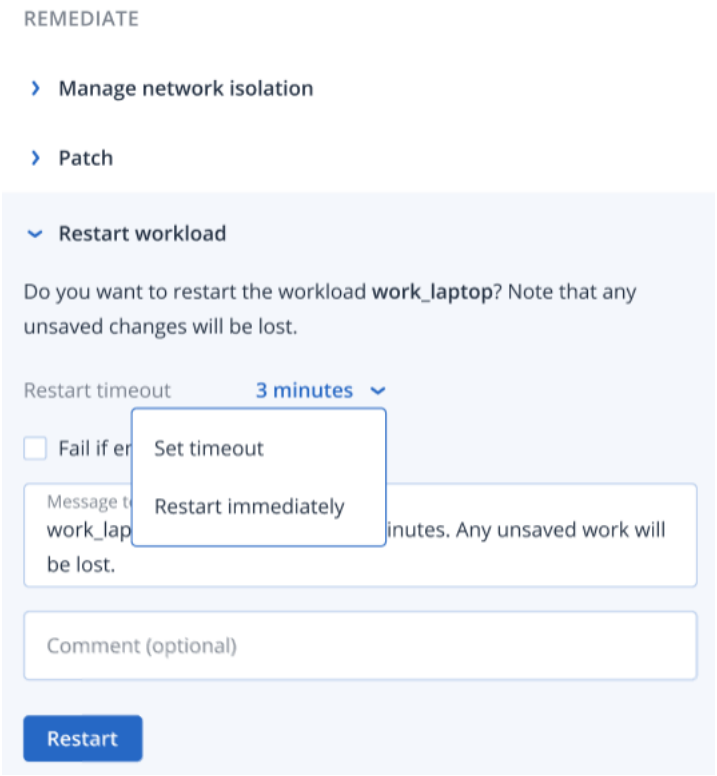
© Acronis International GmbH, 2003-2024

워크로드 다시 시작

공격 조사 대응의 일환으로 EDR에서는 워크로드를 즉시 다시 시작하거나 사전 정의된 시간 초과 기간에 따라 다시 시작할 수 있습니다.

워크로드를 다시 시작하려면

1. 사이버 킬 체인에서 다시 시작 스케줄을 설정할 워크로드 노드를 클릭합니다.
2. 표시되는 사이드바에서 **대응 조치** 탭을 클릭합니다.
3. **수정** 섹션에서 **워크로드 다시 시작**을 클릭합니다.



4. **다시 시작 제한 시간** 필드에서 표시된 링크를 클릭한 후 다음 중 하나를 선택합니다.
   - **제한 시간 설정**: 다시 시작 제한 시간 대화 상자에서 워크로드 다시 시작 기간을 설정한 후 **저장**을 클릭합니다.
   - **즉시 다시 시작**: 워크로드를 즉시 다시 시작하려면 선택합니다.
5. [선택 사항] 사용자가 로그인되어 있는 경우 워크로드가 다시 시작되지 않도록 하려면 **최종 사용자가 로그인한 경우 실패** 확인란을 선택합니다.
6. 분리된 워크로드에 액세스하는 사용자에게 표시할 메시지를 **표시할 메시지** 필드에 추가합니다.
7. [선택 사항] **주석** 필드에 주석을 추가합니다. 이 주석은 단일 노드나 전체 인시던트의 **활동** 탭에 표시되므로 작성자 본인이나 동료가 인시던트를 다시 확인할 때 해당 조치를 취한 이유를 파악할 수 있습니다.
8. **다시 시작**을 클릭합니다.

© Acronis International GmbH, 2003-2024

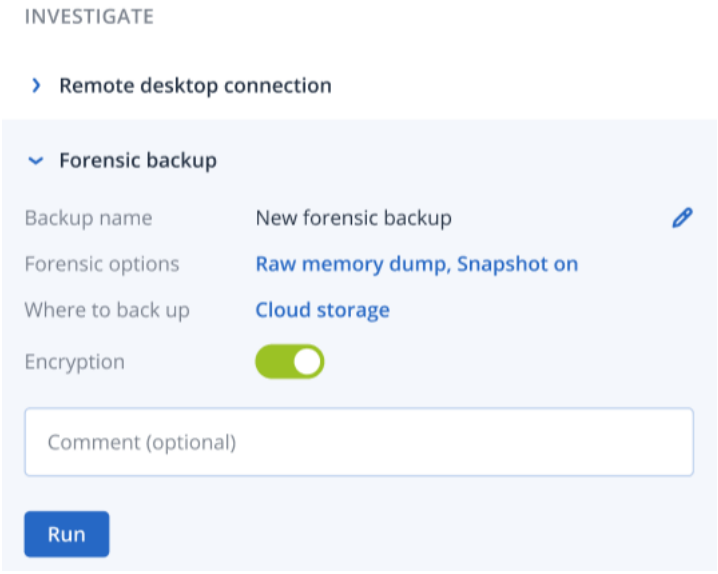
워크로드가 정의된 스케줄에 따라 다시 시작되도록 설정됩니다. 개별 노드와 전체 인시던트의 **활동** 탭에서도 이 조치를 확인할 수 있습니다. 자세한 내용은 "인시던트 완화를 위해 수행한 작업 파악"(832페이지)을(를) 참조하십시오.

워크로드에서 온디맨드 포렌식 백업 실행

EDR에서는 공격 조사의 일환으로 감사 또는 추가 조사를 위해 온디맨드 포렌식 백업을 실행할 수 있습니다. 파트너 워크로드에 Advanced Backup 구독이 있어야 이 기능을 사용할 수 있습니다.

포렌식 백업을 실행하려면

1. 사이버 킬 체인에서 포렌식 백업을 실행할 워크로드 노드를 클릭합니다.
2. 표시되는 사이드바에서 **대응 조치** 탭을 클릭합니다.
3. **조사** 섹션에서 **포렌식 백업**을 클릭합니다.



4. [선택 사항] **백업 이름** 필드에서 편집 아이콘을 클릭하여 백업 이름을 편집합니다.
5. **포렌식 옵션** 필드에서 표시되는 링크를 클릭합니다. 표시되는 포렌식 옵션 대화 상자에서 다음 중 하나를 선택합니다.
   - **원시 메모리 덤프 수집**
   - **커널 메모리 덤프 수집**

   실행 중인 프로세스의 스냅샷 확인란을 선택하여 백업 시작 시에 실행 중인 프로세스 관련 정보를 추가할 수도 있습니다. 이 정보는 백업 이미지에 저장됩니다.

   저장을 클릭하여 포렌식 옵션 대화 상자를 닫습니다.
6. **백업 위치** 필드에서 표시되는 링크를 클릭하여 백업의 위치를 정의합니다.
7. [선택 사항] **암호화** 옵션을 클릭하여 암호화를 활성화합니다. 표시되는 대화 상자에서 암호화된 백업의 비밀번호를 입력하고 관련 암호화 알고리즘을 선택합니다.
8. [선택 사항] **주석** 필드에 주석을 추가합니다. 이 주석은 단일 노드나 전체 인시던트의 **활동** 탭에 표시되므로 작성자 본인이나 동료가 인시던트를 다시 확인할 때 해당 조치를 취한 이유를 파악할 수 있습니다.

© Acronis International GmbH, 2003-2024

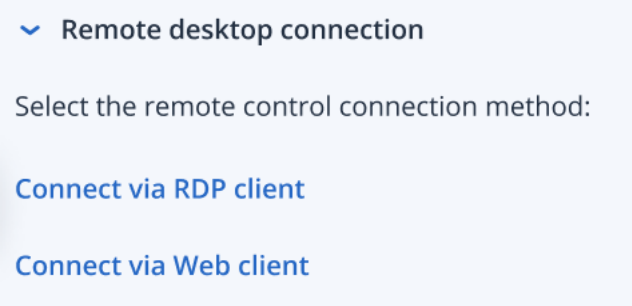
9. **실행**을 클릭합니다.
   포렌식 백업이 시작됩니다. 개별 노드와 전체 인시던트의 **활동** 탭에서도 이 조치를 확인할 수 있습니다. 자세한 내용은 "인시던트 완화를 위해 수행한 작업 파악"(832페이지)을(를) 참조하십시오.

워크로드에 대한 원격 연결

EDR에서는 공격 조사의 일환으로 조사 중인 워크로드에 원격으로 연결할 수 있습니다.

워크로드에 원격으로 연결하려면

1. 사이버 킬 체인에서 원격으로 연결할 워크로드 노드를 클릭합니다.
2. 표시되는 사이드바에서 **대응 조치** 탭을 클릭합니다.
3. **조사** 섹션에서 **원격 데스크탑 연결**을 클릭합니다.



4. 다음 원격 연결 방법 중 하나를 선택합니다.
   - **RDP 클라이언트를 통해 연결**: 이 방법을 선택하면 원격 데스크탑 연결 클라이언트를 다운로드하여 설치하라는 메시지가 표시됩니다. 클라이언트를 다운로드하여 설치한 후 콘솔에서 워크로드에 원격으로 연결할 수 있습니다.
   - **웹 클라이언트를 통해 연결**: 이 방법을 선택하면 워크로드에 RDP 클라이언트를 설치하지 않아도 됩니다. 즉, 로그인 화면으로 바로 리디렉션되며 이 화면에서 원격 머신용 자격 증명을 입력해야 합니다.

   원격 연결이 시작되면 개별 노드와 전체 인시던트의 **활동** 탭에서 이 조치를 확인할 수 있습니다. 자세한 내용은 "인시던트 완화를 위해 수행한 작업 파악"(832페이지)을(를) 참조하십시오.

백업에서 복구

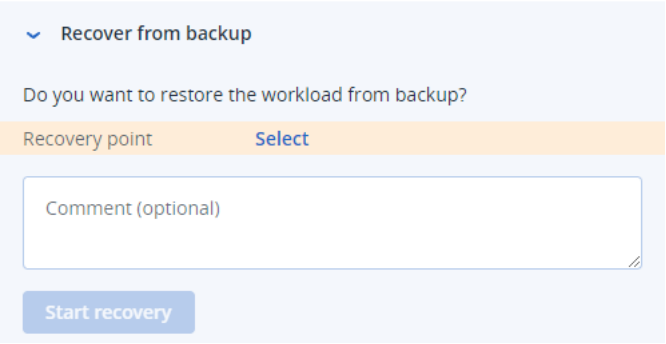
EDR에서는 공격 복구 대응의 일환으로 백업에서 전체 머신이나 특정 파일 또는 폴더를 복구할 수 있습니다.

백업에서 워크로드를 복구하려면

1. 사이버 킬 체인에서 복구할 워크로드 노드를 클릭합니다.
2. 표시되는 사이드바에서 **대응 조치** 탭을 클릭합니다.

© Acronis International GmbH, 2003-2024

3. **복구** 섹션에서 **백업에서 복구**를 클릭합니다.



4. **복구 지점** 필드에서 **선택**을 클릭하고 다음 단계를 수행합니다.
   a. 표시되는 사이드바에서 관련 복구 지점을 선택합니다.
   b. **복구 > 전체 워크로드**를 클릭하여 워크로드의 모든 파일과 폴더를 복구합니다.
   또는
   복구 > 파일/폴더를 클릭하여 워크로드의 특정 파일과 폴더를 복구합니다. 그러면 관련 파일이나 폴더를 선택하라는 메시지가 표시됩니다. 파일이나 폴더를 선택한 후 **복구할 항목** 필드에서 관련 값을 클릭하여 복구를 위해 선택한 항목을 확인할 수 있습니다.

   참고
   암호화된 복구 지점을 선택하면 비밀번호를 입력하라는 메시지가 표시됩니다.

5. [선택 사항] **자동으로 워크로드 다시 시작** 확인란을 선택합니다. 이 옵션은 4단계에서 **복구 > 전체 워크로드**를 선택한 경우에만 사용 가능합니다.
6. [선택 사항] **주석** 필드에 주석을 추가합니다. 이 주석은 단일 노드나 전체 인시던트의 **활동** 탭에 표시되므로 작성자 본인이나 동료가 인시던트를 다시 확인할 때 해당 조치를 취한 이유를 파악할 수 있습니다.
7. **복구 시작**을 클릭합니다.
   워크로드 복구 프로세스가 시작됩니다. 개별 노드와 전체 인시던트의 **활동** 탭에서 이 작업의 진행률을 확인할 수 있습니다. 자세한 내용은 "인시던트 완화를 위해 수행한 작업 파악"(832페이지)을(를) 참조하십시오.

재해 복구 장애 조치

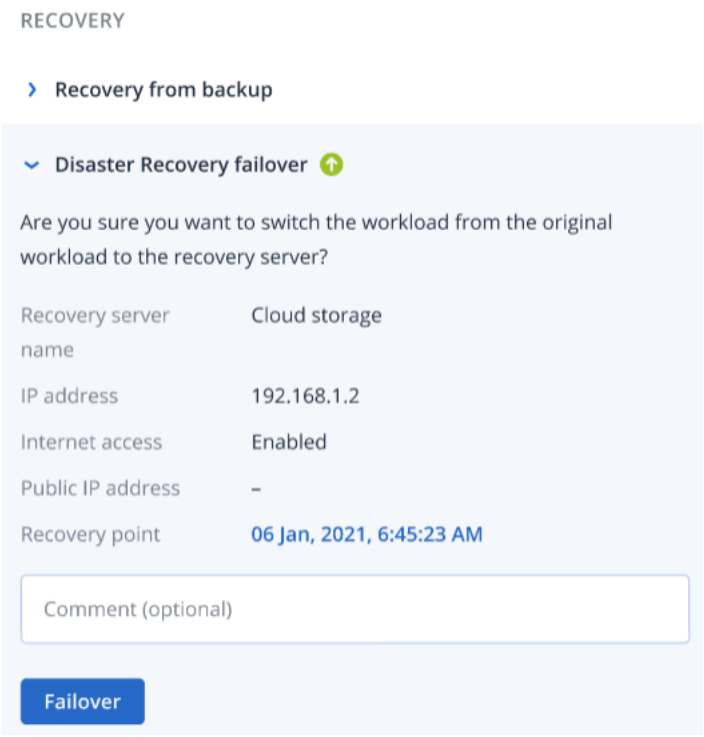
EDR에서는 공격 복구 대응의 일환으로 "재해 복구 구현"(666페이지)을(를) 실행할 수 있습니다. 그러면 워크로드를 복구 서버로 전환할 수 있습니다. 워크로드에 Advanced Disaster Recovery 구독이 있어야 합니다.

재해 복구 장애 조치를 실행하려면

1. 사이버 킬 체인에서 복구할 워크로드 노드를 클릭합니다.
2. 표시되는 사이드바에서 **대응 조치** 탭을 클릭합니다.

© Acronis International GmbH, 2003-2024

3. **복구** 섹션에서 **재해 복구 장애 조치**를 클릭합니다.



4. **복구 지점** 필드에서 다음 단계를 수행합니다.
   a. 현재 복구 지점 날짜를 클릭하여 복구 지점을 선택합니다.
   b. 표시되는 사이드바에서 관련 복구 지점을 선택합니다.

   참고
   Advanced Disaster Recovery 구독이 있다면 재해 복구에서 생성한 관련 복구 서버(오프라인 VM)를 선택할 수 있습니다. Advanced Disaster Recovery 구독이 없다면 재해 복구를 구성하라는 메시지가 표시됩니다.

5. [선택 사항] **주석** 필드에 주석을 추가합니다. 이 주석은 단일 노드나 전체 인시던트의 **활동** 탭에 표시되므로 작성자 본인이나 동료가 인시던트를 다시 확인할 때 해당 조치를 취한 이유를 파악할 수 있습니다.
6. **장애 조치**를 클릭합니다.
   워크로드가 복구 서버로 전환됩니다. 개별 노드와 전체 인시던트의 **활동** 탭에서 이 조치를 확인할 수 있습니다. 자세한 내용은 "인시던트 완화를 위해 수행한 작업 파악"(832페이지)을(를) 참조하십시오.

의심스러운 프로세스에 대한 대응 조치 정의

공격 수정 대응의 일환으로 의심스러운 프로세스에 다음 조치를 적용할 수 있습니다.

- 프로세스 중지(아래 설명 참조)
- 프로세스 격리(아래 설명 참조)
- 프로세스에서 적용한 변경 사항 롤백(아래 설명 참조)
- 보호 계획 허용 목록이나 차단 목록에 프로세스 추가("보호 계획의 차단 목록 또는 허용 목록에서 프로세스, 파일 또는 네트워크를 추가하거나 제거합니다."(859페이지) 참조)

© Acronis International GmbH, 2003-2024

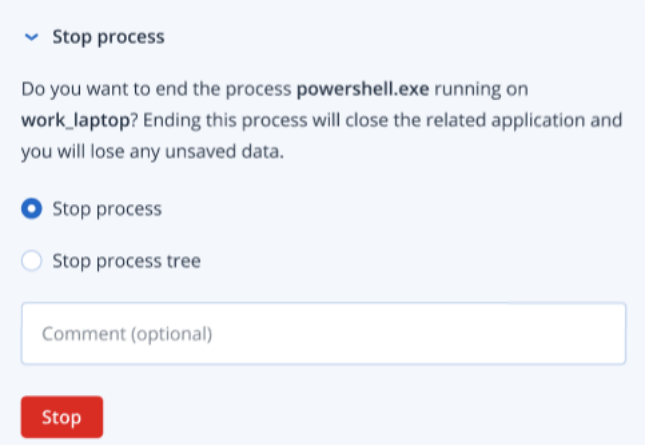
의심스러운 프로세스를 중지하려면

1. 사이버 킬 체인에서 수정할 프로세스 노드를 클릭합니다.

   참고
   Windows의 중요 프로세스나 실행 중이 아닌 프로세스는 중지할 수 없으며 사이버 킬 체인에서 비활성화됩니다.

2. 표시되는 사이드바에서 **대응 조치** 탭을 클릭합니다.
3. **수정** 섹션에서 **프로세스 중지**를 클릭합니다.

   REMEDIATE

4. 다음 중 하나를 선택합니다.
   - **프로세스 중지**(특정 프로세스가 중지됨)
   - **프로세스 트리 중지**(특정 프로세스와 모든 자식 프로세스가 중지됨)
5. [선택 사항] 주석을 추가합니다. 이 주석은 단일 노드나 전체 인시던트의 **활동** 탭에 표시되므로 작성자 본인이나 동료가 인시던트를 다시 확인할 때 해당 조치를 취한 이유를 파악할 수 있습니다.
6. **중지**를 클릭합니다. 프로세스가 중지됩니다.

   참고
   관련 애플리케이션이 닫히고 저장되지 않은 데이터는 손실됩니다.

   개별 노드와 전체 인시던트의 **활동** 탭에서도 이 조치를 확인할 수 있습니다. 자세한 내용은 "인시던트 완화를 위해 수행한 작업 파악"(832페이지)을(를) 참조하십시오.

의심스러운 프로세스를 격리하려면

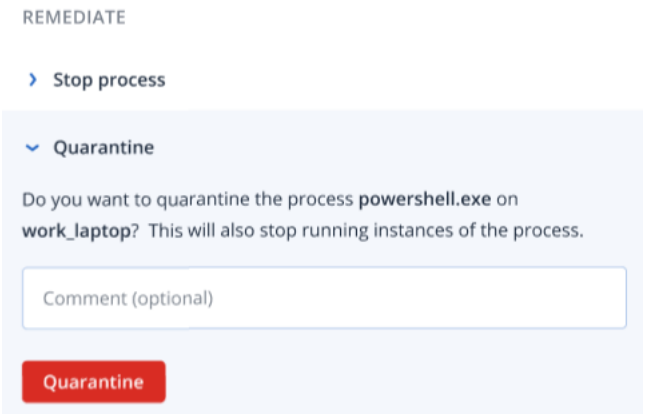
1. 사이버 킬 체인에서 격리할 프로세스 노드를 클릭합니다.

   참고
   Windows의 중요 프로세스는 격지할 수 없으며 사이버 킬 체인에서 비활성화됩니다.

2. 표시되는 사이드바에서 **대응 조치** 탭을 클릭합니다.

© Acronis International GmbH, 2003-2024

3. **수정** 섹션에서 **격리**를 클릭합니다.



4. [선택 사항] 주석을 추가합니다. 이 주석은 단일 노드나 전체 인시던트의 **활동** 탭에 표시되므로 작성자 본인이나 동료가 인시던트를 다시 확인할 때 해당 조치를 취한 이유를 파악할 수 있습니다.
5. **격리**를 클릭합니다. 프로세스가 중지된 후에 격리됩니다.

참고
안티맬웨어 보호 아래에서 제공되는 격리 섹션에서 프로세스를 추가하고 관리할 수 있습니다.

개별 노드와 전체 인시던트의 **활동** 탭에서도 이 조치를 확인할 수 있습니다. 자세한 내용은 "인시던트 완화를 위해 수행한 작업 파악"(832페이지)을(를) 참조하십시오.

변경 사항을 롤백하려면

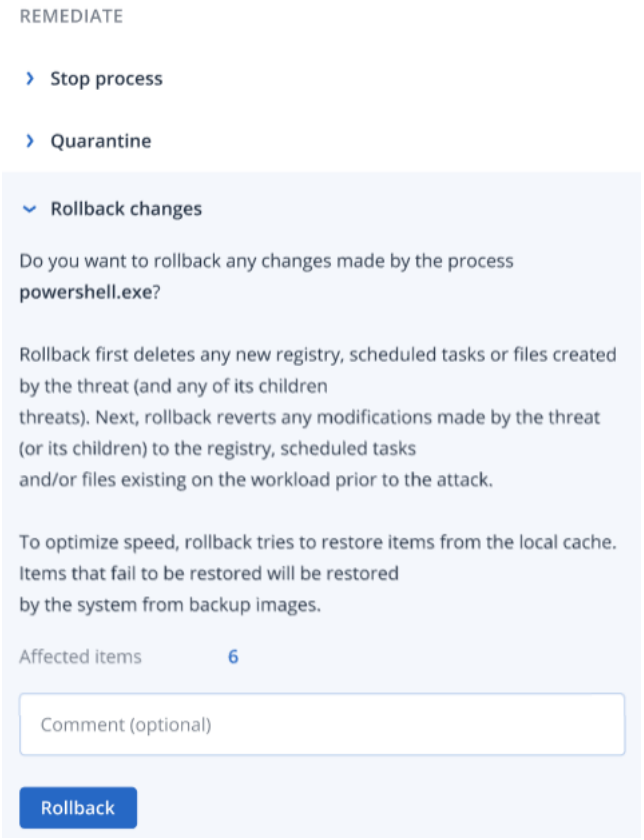
1. 사이버 킬 체인에서 변경 사항을 롤백할 프로세스 노드를 클릭합니다.

참고
이 작업은 빨간색이나 노란색 노드로 표시되는 감지 노드에서만 사용 가능합니다.

2. 표시되는 사이드바에서 **대응 조치** 탭을 클릭합니다.

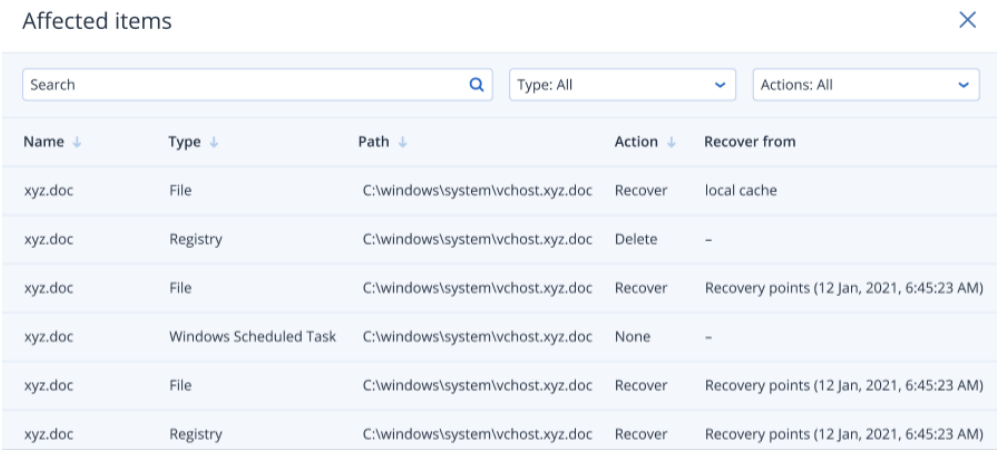
© Acronis International GmbH, 2003-2024

3. **수정** 섹션에서 **변경 사항 롤백**을 클릭합니다.



참고
롤백 프로세스에서는 로컬 캐시의 항목에서만 복구를 수행합니다. 백업 아카이브로부터의 롤백은 향후 릴리스에서 제공될 예정입니다.

4. 변경 사항 롤백의 영향을 받은 항목을 확인하려면 **영향받은 항목** 링크를 클릭합니다. 표시되는 대화 상자에서 롤백 시 이전 상태로 돌아가는 모든 항목(파일, 레지스트리, 예약된 작업)과 이러한 항목을 롤백하기 위해 수행되는 작업(**삭제**, **복구** 또는 **없음**)을 확인할 수 있습니다. 또한 복원된 항목이 로컬 캐시에서 복구되는지 아니면 백업 복구 지점에서 복구되는지도 확인할 수 있습니다.



© Acronis International GmbH, 2003-2024

5. [선택 사항] 주석을 추가합니다. 이 주석은 단일 노드나 전체 인시던트의 **활동** 탭에 표시되므로 작성자 본인이나 동료가 인시던트를 다시 확인할 때 해당 조치를 취한 이유를 파악할 수 있습니다.
6. **롤백**을 클릭합니다. 롤백 기능은 다음 단계를 수행하여 프로세스에서 적용된 레지스트리, 파일 또는 예약된 작업의 변경 사항을 되돌립니다.
   a. 위협(해당 자식 위협 포함)에 의해 생성된 모든 새 항목(레지스트리, 예약된 작업, 파일)이 삭제됩니다.
   b. 위협과 해당 자식 위협으로 인해 공격 전에 워크로드에 있었던 레지스트리, 예약된 작업 및/또는 파일에 적용된 수정 사항이 원래 상태로 돌아갑니다.
   c. 롤백은 로컬 캐시에서 항목을 복구하려고 시도합니다. EDR은 복구할 수 없는 항목을 정상 백업 이미지에서 자동 복구합니다.

   개별 노드와 전체 인시던트의 **활동** 탭에서도 롤백 작업을 확인할 수 있습니다. 자세한 내용은 "인시던트 완화를 위해 수행한 작업 파악"(832페이지)을(를) 참조하십시오.

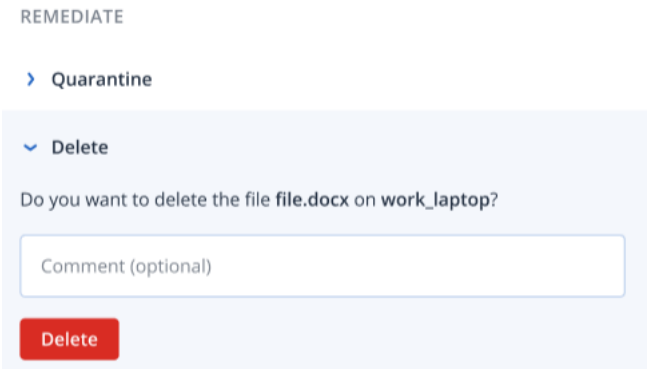
의심스러운 파일에 대한 대응 조치 정의

공격 수정 대응의 일환으로 의심스러운 파일에 다음 조치를 적용할 수 있습니다.

- 파일 삭제(아래 설명 참조)
- 파일 격리(아래 설명 참조)
- 보호 계획 허용 목록이나 차단 목록에 파일 추가("보호 계획의 차단 목록 또는 허용 목록에서 프로세스, 파일 또는 네트워크를 추가하거나 제거합니다."(859페이지) 참조)

의심스러운 파일을 삭제하려면

1. 사이버 킬 체인에서 수정할 파일 노드를 클릭합니다.
2. 표시되는 사이드바에서 **대응 조치** 탭을 클릭합니다.
3. **수정** 섹션에서 **삭제**를 클릭합니다.

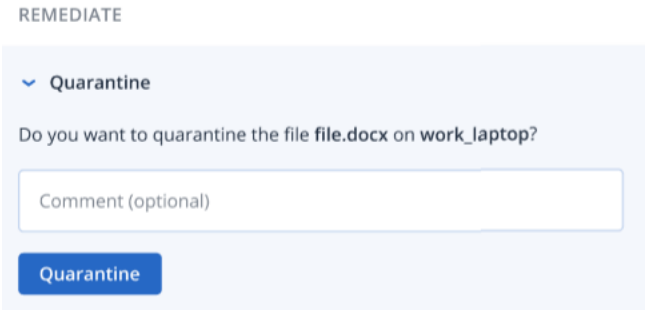


4. [선택 사항] 주석을 추가합니다. 이 주석은 단일 노드나 전체 인시던트의 **활동** 탭에 표시되므로 작성자 본인이나 동료가 인시던트를 다시 확인할 때 해당 조치를 취한 이유를 파악할 수 있습니다.
5. **삭제**를 클릭합니다.
   파일이 삭제됩니다. 개별 노드와 전체 인시던트의 **활동** 탭에서도 이 조치를 확인할 수 있습니다. 자세한 내용은 "인시던트 완화를 위해 수행한 작업 파악"(832페이지)을(를) 참조하십시오.

의심스러운 파일을 격리하려면

© Acronis International GmbH, 2003-2024

1. 사이버 킬 체인에서 수정할 파일 노드를 클릭합니다.
2. 표시되는 사이드바에서 **대응 조치**로 이동합니다.
3. **수정** 섹션에서 **격리**를 클릭합니다.



4. [선택 사항] 주석을 추가합니다. 이 주석은 단일 노드나 전체 인시던트의 **활동** 탭에 표시되므로 작성자 본인이나 동료가 인시던트를 다시 확인할 때 해당 조치를 취한 이유를 파악할 수 있습니다.
5. **격리**를 클릭합니다.
   파일이 격리됩니다. 개별 노드와 전체 인시던트의 **활동** 탭에서도 이 조치를 확인할 수 있습니다. 자세한 내용은 "인시던트 완화를 위해 수행한 작업 파악"(832페이지)을(를) 참조하십시오.

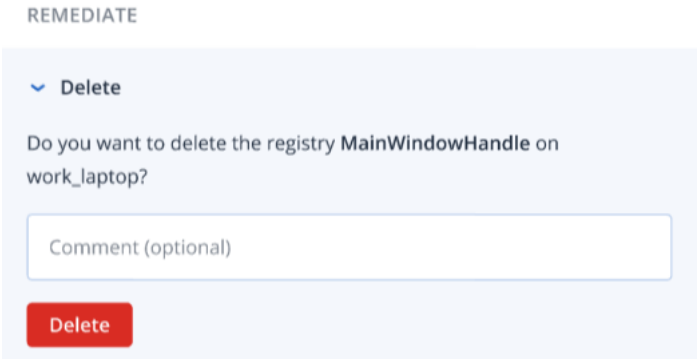
의심스러운 레지스트리 항목에 대한 대응 조치 정의

공격 수정 대응의 일환으로 의심스러운 레지스트리 항목을 삭제할 수 있습니다.

이 옵션은 레지스트리 사이버 킬 체인 노드에 사용 가능합니다.

의심스러운 레지스트리 항목을 삭제하려면

1. 사이버 킬 체인에서 수정할 노드를 클릭합니다.
2. 표시되는 사이드바에서 **대응 조치** 탭을 클릭합니다.
3. **수정** 섹션에서 **삭제**를 클릭합니다.



4. [선택 사항] 주석을 추가합니다. 이 주석은 단일 노드나 전체 인시던트의 **활동** 탭에 표시되므로 작성자 본인이나 동료가 인시던트를 다시 확인할 때 해당 조치를 취한 이유를 파악할 수 있습니다.
5. **삭제**를 클릭합니다.
   레지스트리 항목이 삭제됩니다. 개별 노드와 전체 인시던트의 **활동** 탭에서도 이 조치를 확인할 수 있습니다. 자세한 내용은 "인시던트 완화를 위해 수행한 작업 파악"(832페이지)을(를) 참조하십시오.

© Acronis International GmbH, 2003-2024

보호 계획의 차단 목록 또는 허용 목록에서 프로세스, 파일 또는 네트워크를 추가하거나 제거합니다.

공격 방지 대응의 일환으로 보호 계획 허용 목록이나 차단 목록에 노드를 추가할 수 있습니다.

안전한 것으로 간주되는 노드는 허용 목록에 추가할 수 있습니다. 그러면 앞으로 해당 노드는 공격으로 감지되지 않습니다. 차단 목록에 추가하는 목록은 더 이상 실행되지 않습니다.

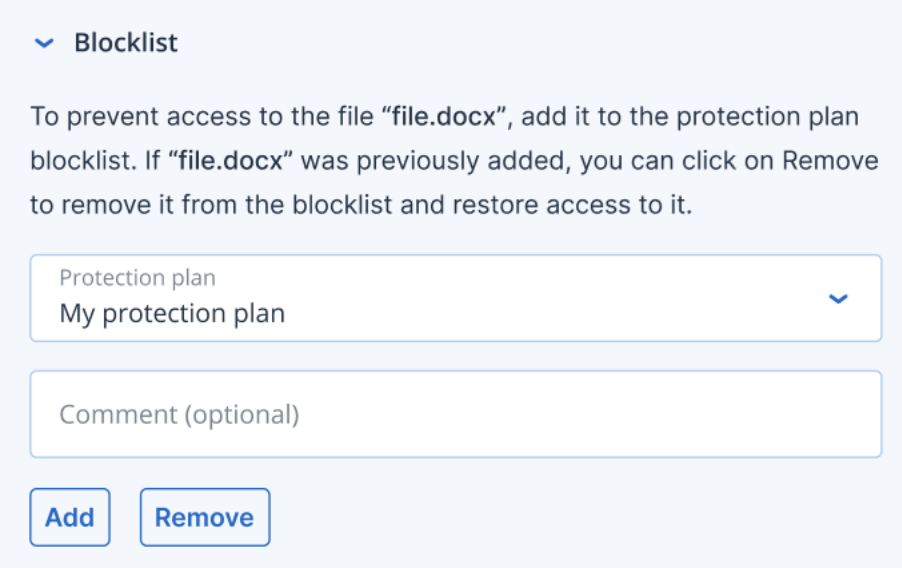
또한 노드를 허용 목록이나 차단 목록에서 제거하여 향후 노드 액세스를 허용하거나 방지할 수 있습니다.

이 옵션을 사용할 수 있는 사이버 킬 체인 노드는 다음과 같습니다.

- 프로세스
- 파일
- 네트워크

보호 계획 차단 목록에서 프로세스, 파일 또는 네트워크를 추가하거나 제거하는 방법

1. 사이버 킬 체인에서 조치를 취하려는 프로세스, 파일 또는 네트워크 노드를 클릭합니다.
2. 표시되는 사이드바에서 **대응 조치** 탭을 클릭합니다.
3. **방지** 섹션에서 **차단 목록** 옆의 화살표 아이콘을 클릭합니다.



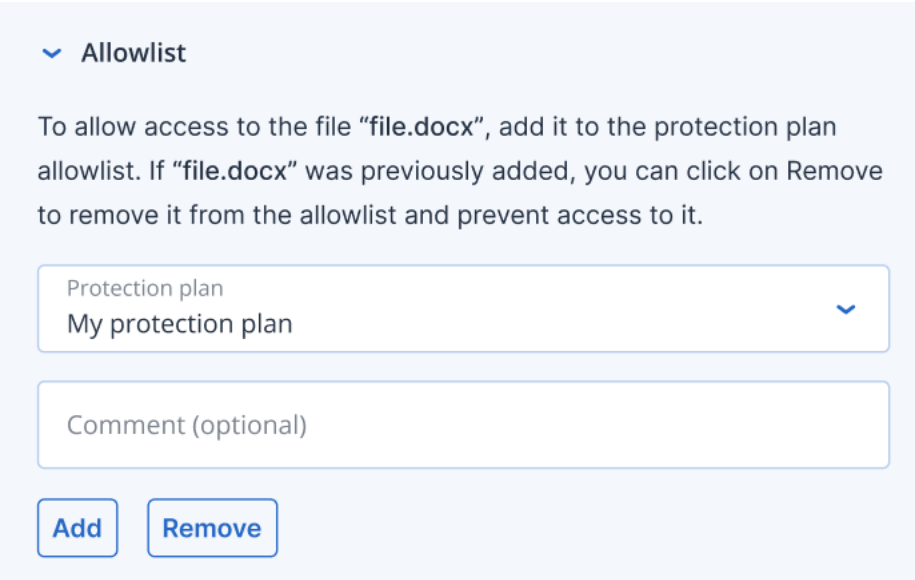
4. 이 조치를 적용할 관련 보호 계획을 선택합니다.
5. [선택 사항] 주석을 추가합니다. 이 주석은 단일 노드나 전체 인시던트의 **활동** 탭에 표시되므로 작성자 본인이나 동료가 인시던트를 다시 확인할 때 해당 조치를 취한 이유를 파악할 수 있습니다.
6. **추가**를 클릭합니다.
   작업이 구현되었으며, 프로세스, 파일 또는 네트워크가 향후 시작되는 것이 방지됩니다.
   또는 프로세스, 파일 또는 네트워크가 이전에 차단 목록에 추가되었고 이제 차단 목록에서 제거하려는 경우 **제거**를 클릭합니다. 이렇게 하면 노드에 대한 향후 액세스를 허용할 수 있습니다.

© Acronis International GmbH, 2003-2024

추가 또는 제거 작업은 개별 노드 및 전체 인시던트의 **활동** 탭에서도 볼 수 있습니다. 자세한 내용은 "인시던트 완화를 위해 수행한 작업 파악"(832페이지)을(를) 참조하십시오.

보호 계획 허용 목록에서 프로세스, 파일 또는 네트워크를 추가하거나 제거하는 방법

1. 사이버 킬 체인에서 조치를 취하려는 프로세스, 파일 또는 네트워크 노드를 클릭합니다.
2. 표시되는 사이드바에서 **대응 조치** 탭을 클릭합니다.
3. **방지** 섹션에서 **허용 목록** 옆의 화살표 아이콘을 클릭합니다.



4. 이 조치를 적용할 관련 보호 계획을 선택합니다.
5. [선택 사항] 주석을 추가합니다. 이 주석은 단일 노드나 전체 인시던트의 **활동** 탭에 표시되므로 작성자 본인이나 동료가 인시던트를 다시 확인할 때 해당 조치를 취한 이유를 파악할 수 있습니다.
6. **추가**를 클릭합니다.
   작업이 구현되었으며, 프로세스, 파일 또는 네트워크가 향후 탐지되는 것이 방지됩니다.
   또는 프로세스, 파일 또는 네트워크가 이전에 허용 목록에 추가되었고 이제 허용 목록에서 제거하려는 경우 **제거**를 클릭합니다. 이렇게 하면 노드에 대한 모든 향후 액세스를 방지할 수 있습니다.
   추가 또는 제거 작업은 개별 노드 및 전체 인시던트의 **활동** 탭에서도 볼 수 있습니다. 자세한 내용은 "인시던트 완화를 위해 수행한 작업 파악"(832페이지)을(를) 참조하십시오.

EDR(Endpoint Detection and Response)을 위한 모니터링 모드 활성화

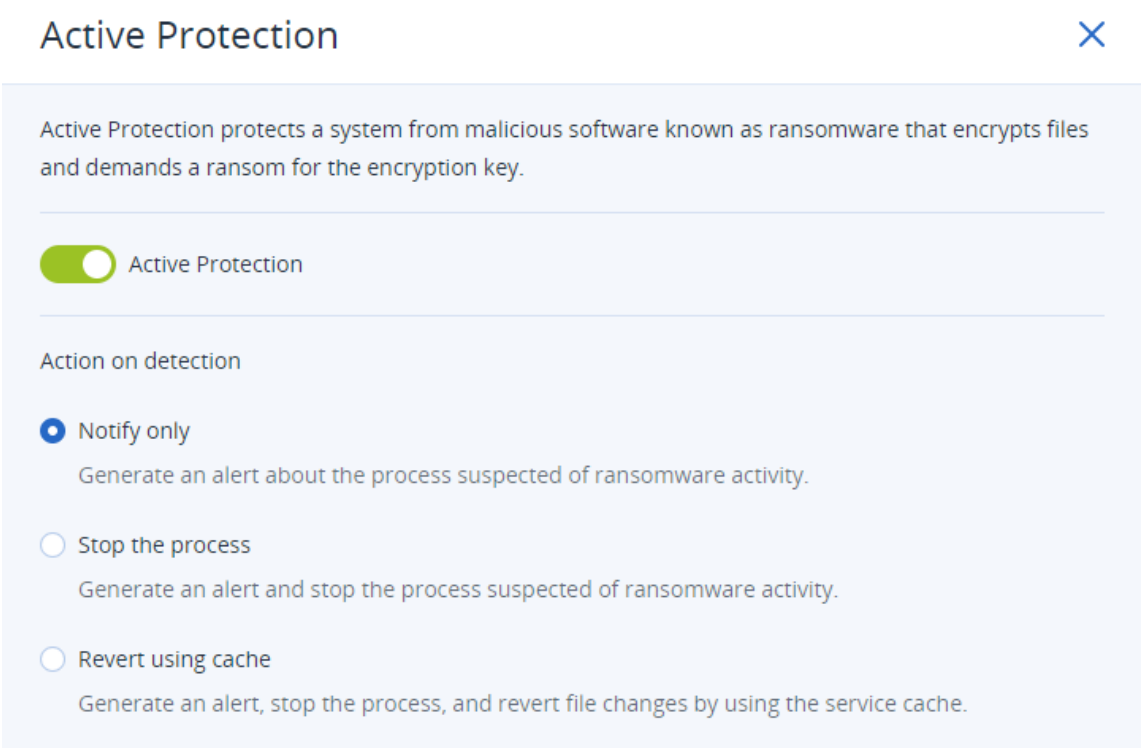
Cyber Protection의 모니터링 모드를 통해 프로덕션 환경에서 EDR을 사용할 수 있습니다. 결과적으로 오탐을 확인하고, EDR을 완전히 배포하기 전에 필요한 제외를 만들 수 있습니다.

모니터링 모드에서는 아무것도 차단되거나 중단되지 않으며, 인시던트가 생성되지만 응답은 초기화되지 않습니다.

EDR의 모니터링 모드를 활성화하는 방법

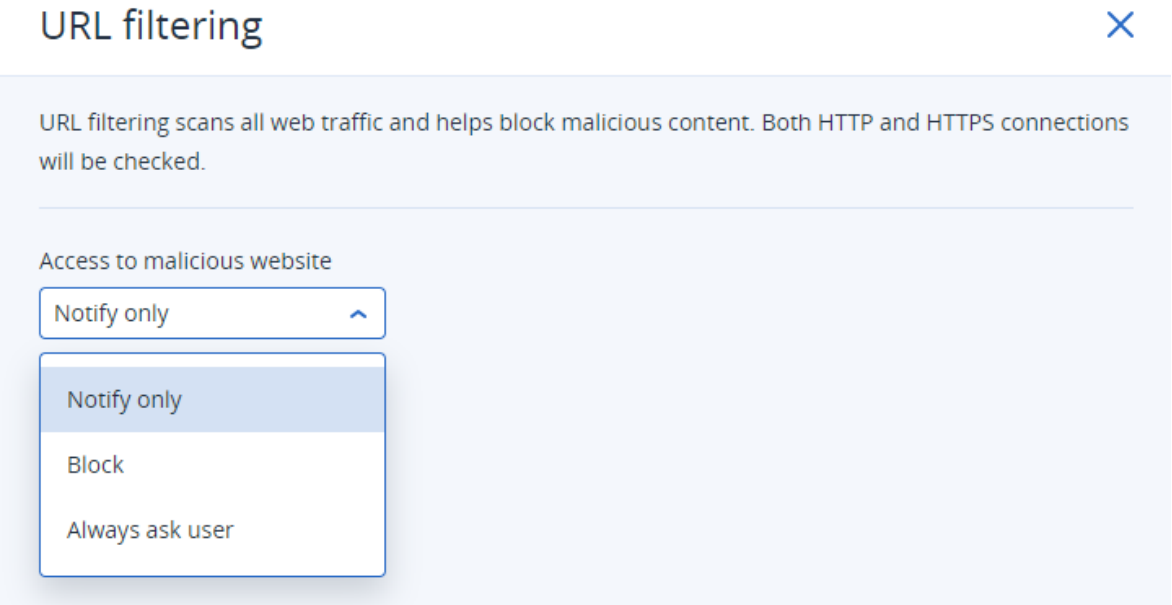
© Acronis International GmbH, 2003-2024

1. 관련 보호 계획에서 EDR이 활성화되어 있는지 확인하십시오. 자세한 정보는 "EDR(Endpoint Detection and Response) 기능 활성화"(815페이지)을(를) 참조하십시오.
2. **안티바이러스 및 안티맬웨어 보호** 모듈을 확장하고 다음을 정의합니다.
   - **Active Protection**을 클릭하고, **감지에 대한 작업** 섹션에서 **알리기만 함**을 선택합니다. 그런 다음 **완료**를 클릭합니다. 자세한 정보는 "Active Protection"(748페이지)을(를) 참조하십시오.



   - **동작 엔진**을 클릭하고, **감지에 대한 작업** 섹션에서 **알리기만 함**을 선택합니다. 그런 다음 **완료**를 클릭합니다. 자세한 정보는 "동작 엔진"(752페이지)을(를) 참조하십시오.
   - **악용 방지**를 클릭하고, **감지에 대한 작업** 섹션에서 **알리기만 함**을 선택합니다. 그런 다음 **완료**를 클릭합니다. 자세한 정보는 "악용 방지"(753페이지)을(를) 참조하십시오.
   - **실시간 보호**를 클릭하고, **감지에 대한 작업** 섹션에서 **알리기만 함**을 선택합니다. 그런 다음 **완료**를 클릭합니다. 자세한 정보는 "실시간 보호"(755페이지)을(를) 참조하십시오.
   - **스캔 예약**을 클릭하고, **감지에 대한 작업** 섹션에서 **알리기만 함**을 선택합니다. 그런 다음 **완료**를 클릭합니다. 자세한 정보는 "스캔 예약"(756페이지)을(를) 참조하십시오.
3. **URL 필터링** 모듈을 확장하고, **악성 웹 사이트에 액세스** 드롭다운 목록에서 **알리기만 함**을 선택합니다. 그런 다음 **완료**를 클릭합니다. 자세한 정보는 "URL 필터링"(769페이지)을(를) 참조하십시오.

© Acronis International GmbH, 2003-2024



EDR(Endpoint Detection and Response)이 정상 작동 중인지 테스트하는 방법

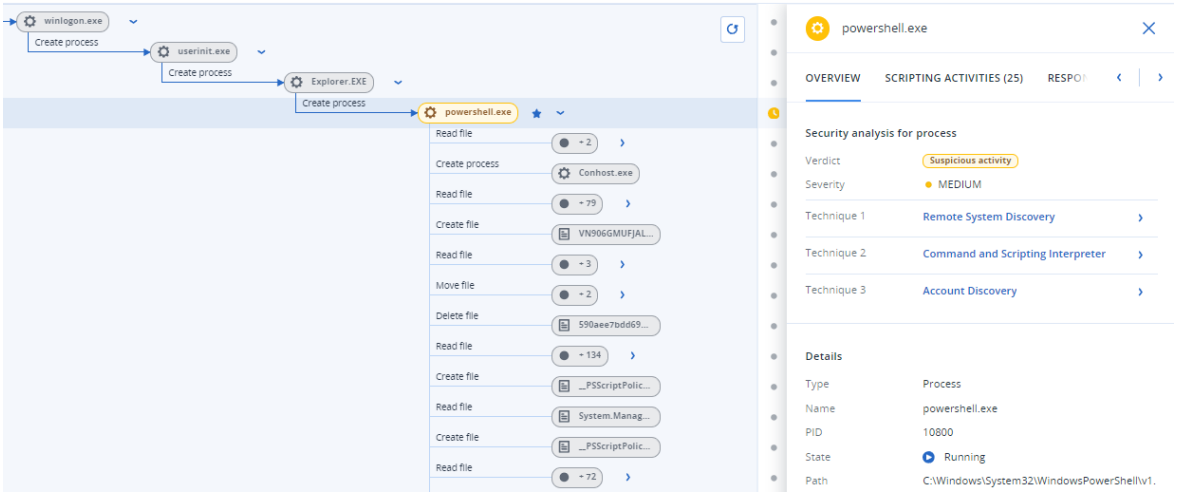
EDR이 디플로이되었으며 작동 중인지를 확인하려는 경우 EDR 감지를 트리거하는 여러 명령을 실행하면 됩니다.

참고
EDR이 디플로이되어 있으면 의심스러운 활동 발생 시 인시던트가 즉시 표시됩니다. 며칠 동안 신규 인시던트가 트리거되지 않은 경우 아래 단계를 진행하면 EDR이 작동 중인지를 확인할 수 있습니다.

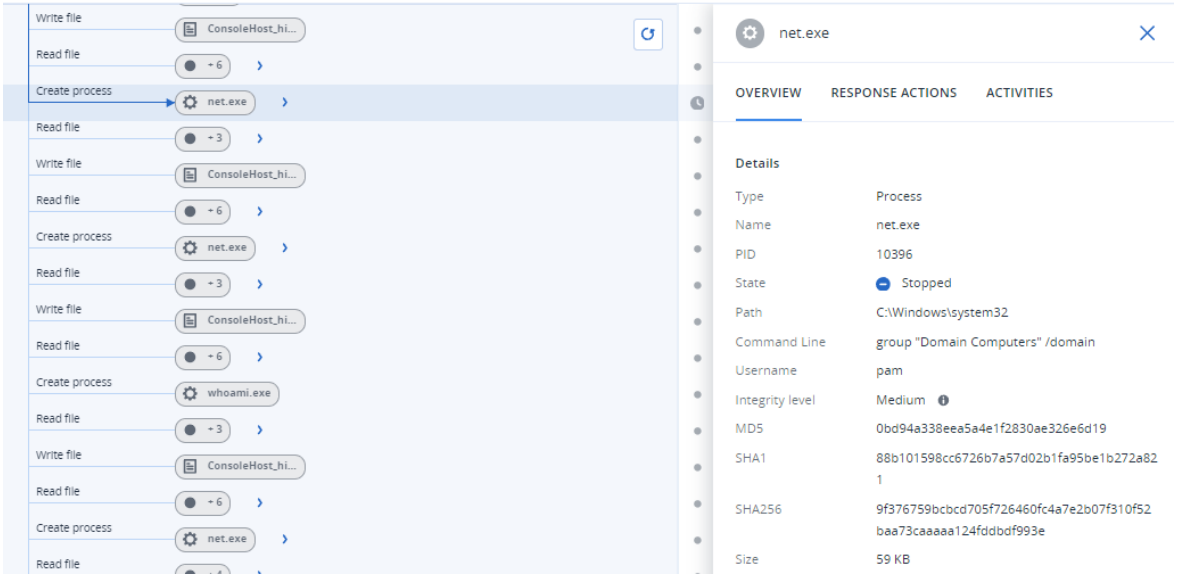
EDR이 디플로이되었으며 작동 중인지를 테스트하려면

1. 관련 도메인에 가입된 Active Directory 사용자 계정에 로그인합니다.
2. Windows PowerShell에서 다음 2개 명령을 실행합니다.
   - `net group "Domain Computers" /domain`
   - `net user administrator /domain`
3. Cyber Protect 콘솔에서 **보호 > 인시던트**로 이동하여 생성된 인시던트를 확인합니다.
   아래 예에 나와 있는 것처럼 트리거된 **보통** 심각도 유형 인시던트를 클릭하여 EDR 사이버 킬 체인에 표시한 후 이전 단계에서 실행한 PowerShell 명령을 확인할 수도 있습니다.

© Acronis International GmbH, 2003-2024



4. Windows PowerShell에서 다음 명령을 실행합니다.
   - `c:\>whoami`
   - `c:\>net localgroup`
   - `c:\>net localgroup administrators`
   - `c:\>powershell -command start-process cmd -verb runas`
   - `c:\WINDOWS\system32>net user administrator /active:yes`
   - `c:\>powershell -command Get-Hotfix`
5. EDR 사이버 킬 체인에서 실행 가능 노드(예: **net.exe** 또는 **whoami.exe**)를 클릭하여 명령줄에서 실행했던 정확한 PowerShell 명령을 표시합니다. 아래 예에는 **개요** 탭의 **상세 정보** 섹션에 이러한 명령이 표시되어 있습니다.



6. EDR 인시던트가 생성되었음을 확인한 후 인시던트의 **위협 상태**를 **완화됨**으로, **조사 상태**를 **종결됨**으로 수동 설정합니다. 자세한 내용은 "사이버 킬 체인에서 인시던트를 조사하는 방법"(824페이지)을(를) 참조하십시오. 인시던트의 주석을 입력하여 테스트 인시던트임을 표시할 수도 있습니다.

© Acronis International GmbH, 2003-2024

취약성 평가 및 패치 관리

취약점 평가(VA)는 시스템에서 발견한 취약점을 식별하고, 수량화하고, 우선순위를 지정하는 프로세스입니다. 취약점 평가 모듈에서는 머신의 취약점을 스캔하고, 운영 체제 및 설치된 애플리케이션이 최신 상태이며 제대로 작동하는지 확인할 수 있습니다.

취약성 평가 스캔은 다음 운영 체제가 설치된 머신에서 지원됩니다.

- Windows 자세한 내용은 "지원되는 Microsoft 및 서드 파티 제품"(864페이지)을(를) 참조하십시오.
- macOS 자세한 내용은 "지원되는 Apple 및 서드 파티 제품"(866페이지)을(를) 참조하십시오.
- Linux(CentOS 7/Virtuozzo/Acronis Cyber Infrastructure) 머신 자세한 내용은 "지원되는 Linux 제품"(867페이지)을(를) 참조하십시오.

패치 관리(PM) 기능을 사용하면 머신에 설치된 애플리케이션 및 운영 체제에 대한 패치(업데이트)를 관리하고, 시스템을 최신 상태로 유지할 수 있습니다. 패치 관리 모듈에서 머신에 대한 업데이트 설치를 자동 또는 수동으로 승인할 수 있습니다.

패치 관리는 Windows 운영 체제가 설치된 머신에서 지원됩니다. 자세한 내용은 "지원되는 Microsoft 및 서드 파티 제품"(864페이지)을(를) 참조하십시오.

취약성 평가

취약성 평가 프로세스에서는 다음 단계를 수행합니다.

1. 취약성 평가 모듈이 활성화된 보호 계획을 생성하고 취약성 평가 설정을 지정하고 머신에 계획을 할당합니다.
2. 시스템은 스케줄에 따르거나 온디맨드로 취약성 평가 스캔 실행 명령을 머신에 설치된 보호 에이전트로 전송합니다.
3. 에이전트에서 명령을 수신해 머신에서 취약성 스캔을 시작하고, 스캔 활동을 생성합니다.
4. 취약성 평가 스캔이 완료되면 에이전트에서 결과를 생성해 모니터링 서비스로 전송합니다.
5. 모니터링 서비스는 에이전트의 데이터를 처리해 취약성 평가 위젯에 결과와 발견된 취약성 목록을 표시합니다.
6. 발견된 취약성 목록을 수신하면, 이를 처리하고 발견된 취약성 중 수정해야 할 항목을 결정할 수 있습니다.

모니터링 > **개요** > **취약성/기존 취약성** 위젯에서 취약성 평가 스캔 결과를 모니터링할 수 있습니다.

지원되는 Microsoft 및 서드 파티 제품

취약점 평가 및 패치 관리에서 지원되는 Microsoft 제품 및 Windows 운영 체제용 서드 파티 제품은 다음과 같습니다.

지원되는 Microsoft 제품

Windows OS

© Acronis International GmbH, 2003-2024

- Windows 7(Enterprise, Professional, Ultimate)
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11

Windows Server OS

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Microsoft Office 및 관련 컴퍼넌트

- Microsoft Office 2019 (x64, x86)
- Microsoft Office 2016 (x64, x86)
- Microsoft Office 2013 (x64, x86)
- Microsoft Office 2010 (x64, x86)

Windows OS 관련 컴퍼넌트

- Internet Explorer
- Microsoft EDGE
- Windows Media Player
- .NET Framework
- Visual Studio 및 애플리케이션
- 운영 체제 컴퍼넌트

서버 애플리케이션

- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019
- Microsoft SharePoint Server 2016
- Microsoft SharePoint Server 2019

© Acronis International GmbH, 2003-2024

지원되는 Windows OS용 서드 파티 제품

재택 근무가 세계적으로 점점 늘고 있는 지금은 협업 및 커뮤니케이션 도구와 VPN 클라이언트를 항상 최신 상태로 유지하고, 가능한 취약성을 확인하는 것이 중요합니다. Cyber Protection 서비스는 그러한 애플리케이션을 위한 취약성 평가 및 패치 관리를 지원합니다.

협업 및 커뮤니케이션 도구, VPN 클라이언트

- Microsoft Teams
- Zoom
- Skype
- Slack
- Webex
- NordVPN
- TeamViewer

지원되는 Windows OS용 서드 파티 제품에 대한 자세한 내용은 패치 관리에서 지원하는 서드 파티 제품 목록(62853)을 참조하십시오.

지원되는 Apple 및 서드 파티 제품

취약성 평가에서 지원되는 Apple 제품 및 macOS용 서드 파티 제품은 다음과 같습니다.

지원되는 Apple 제품

macOS

- macOS 10.13.x 이상

macOS 기본 제공 애플리케이션

- Safari, iTunes 및 기타 애플리케이션

지원되는 macOS용 서드 파티 제품

- Microsoft Office(Word, Excel, PowerPoint, Outlook, OneNote)
- Adobe Acrobat Reader
- Google Chrome
- Firefox
- Opera
- Zoom
- Skype
- Thunderbird
- VLC 미디어 플레이어

© Acronis International GmbH, 2003-2024

지원되는 Linux 제품

VA에서 지원되는 Linux 배포판 및 버전은 다음과 같습니다.

- Virtuozzo 7.x
- CentOS 7.x
- CentOS 8.x

취약성 평가 설정

취약성 평가 모듈이 있는 보호 계획을 생성하는 방법을 알아보려면 "보호 계획 생성"을 참고하십시오. VA 스캔은 스케줄에 따라 또는 온디맨드로 수행할 수 있습니다(보호 계획에서 **지금 실행** 작업 사용).

취약성 평가 모듈에서는 다음 설정을 지정할 수 있습니다.

스캔 대상

취약성을 스캔할 소프트웨어 제품을 정의합니다.

- Windows 머신:
  - **Microsoft 제품**
  - **Windows 서드 파티 제품**(지원되는 Windows OS용 서드 파티 제품에 대한 자세한 내용은 패치 관리에서 지원하는 서드 파티 제품 목록(62853) 참조)
- macOS 머신:
  - **Apple 제품**
  - **macOS 서드 파티 제품**
- Linux 머신:
  - **Linux 패키지 스캔**

예약

선택한 머신에서 취약성 평가 스캔을 수행할 스케줄을 정의합니다.

필드	설명
다음 이벤트를 사용해 작업 실행 예약	작업을 실행할 시간을 정의하는 설정입니다. 다음 값을 선택할 수 있습니다. • **시간 기준 예약** - 기본 설정입니다. 지정한 시간에 따라 작업을 실행합니다. • **사용자가 시스템에 로그인할 때** – 기본적으로 사용자가 로그인하면 작업이 트리거됩니다. 특정 사용자 계정만 작업을 트리거할 수 있도록 이 설정을 수정할 수 있습니다. • **사용자가 시스템에서 로그오프할 때** – 기본적으로 사용자가 로그오프하면 작업이 트리거됩니다. 특정 사용자 계정만 작업을 트리거할 수 있도록 이 설정을 수정할 수 있습니다.

© Acronis International GmbH, 2003-2024

필드	설명
	참고 작업은 시스템 종료 시 실행되지 않습니다. 일정 예약 구성에서 시스템 종료와 로그오프는 다른 작업입니다. • **시스템 시작 시** – 운영 체제가 시작될 때 작업을 실행합니다. • **시스템 종료 시** – 운영 체제가 종료될 때 작업을 실행합니다.
예약 유형	**다음 이벤트를 사용해 작업 실행 예약**에서 **시간 기준 예약**을 선택한 경우 이 필드가 표시됩니다. 다음 값을 선택할 수 있습니다. • **월간** – 작업을 실행할 월과 주 또는 일을 선택합니다. • **일일** - 기본 설정입니다. 작업을 실행할 요일을 선택합니다. • **매시간** – 작업을 실행할 요일, 반복 횟수, 시간 간격을 선택합니다.
시작 시간	**다음 이벤트를 사용해 작업 실행 예약**에서 **시간 기준 예약**을 선택한 경우 이 필드가 표시됩니다 작업을 실행할 정확한 시간을 선택합니다.
날짜 범위 내에서 실행	**다음 이벤트를 사용해 작업 실행 예약**에서 **시간 기준 예약**을 선택한 경우 이 필드가 표시됩니다. 구성된 스케줄이 실행될 기간의 범위를 설정합니다.
운영 체제에 로그인할 때 작업을 시작하게 할 사용자 계정 지정	**다음 이벤트를 사용해 작업 실행 예약**에서 **사용자가 시스템에 로그인할 때**를 선택한 경우 이 필드가 표시됩니다. 다음 값을 선택할 수 있습니다. • **모든 사용자** - 어떤 사용자가 로그인하든 작업이 트리거되도록 하려는 경우 이 옵션을 사용합니다. • **다음 사용자** - 특정 사용자 계정의 로그인 시에만 작업이 트리거되도록 하려는 경우 이 옵션을 사용합니다.
운영 체제에서 로그아웃할 때 작업을 시작하게 할 사용자 계정 지정	**다음 이벤트를 사용해 작업 실행 예약**에서 **사용자가 시스템에서 로그오프할 때**를 선택한 경우 이 필드가 표시됩니다. 다음 값을 선택할 수 있습니다. • **모든 사용자** - 어떤 사용자가 로그아웃하든 작업이 트리거되도록 하려는 경우 이 옵션을 사용합니다. • **다음 사용자** - 특정 사용자 계정의 로그아웃 시에만 작업이 트리거되도록 하려는 경우 이 옵션을 사용합니다.
시작 조건	작업을 시작하기 위해 동시에 충족되어야 하는 모든 조건을 정의합니다. 맬웨어 방지 스캔용 시작 조건은 "시작 조건"에 설명되어 있는 **백업 모듈**용 시작 조건과 유사합니다. 다음과 같이 추가적인 시작 조건을 정의할 수 있습니다.

© Acronis International GmbH, 2003-2024

필드	설명
	• **기간 내에서 작업 시작 시간 분배** – 이 옵션을 사용하면 작업을 수행해야 하는 기간을 정의할 수 있습니다. 이 옵션을 사용해 작업 시간대를 설정하여 네트워크 병목현상을 피할 수 있습니다. 지연 시간은 시간 또는 분 단위로 지정할 수 있습니다. 예를 들어 기본 시작 시간이 오전 10시이고 지연 시간이 60분인 경우 작업은 오전 10시~오전 11시 사이에 시작됩니다. • **머신이 꺼진 경우 머신 시작 시 누락된 작업 실행** • **작업 실행 중 절전 또는 최대 절전 모드가 되는 것을 방지** – 이 옵션은 Windows를 구동 중인 머신에서만 유효합니다. • **시작 조건이 충족되지 않아도 다음 후에 작업 실행** - 다른 시작 조건에 관계없이 지정한 기간이 지나면 작업이 시작됩니다. **참고** Linux에서는 시작 조건이 지원되지 않습니다.

Windows 머신 취약성 평가

Windows 머신 및 Windows용 서드 파티 제품을 스캔하여 취약성을 확인할 수 있습니다.

Windows 머신 취약성 평가를 구성하려면

1. Cyber Protect 콘솔에서 보호 계획을 생성하고 **취약점 평가** 모듈을 활성화합니다.
2. 취약성 평가 설정을 지정합니다.
   - **스캔 대상** - **Microsoft 제품**이나 **Windows 서드 파티 제품** 중 하나를 선택하거나 두 제품을 모두 선택합니다.
   - **스케줄** – 취약성 평가를 수행할 스케줄을 정의합니다.

   예약 옵션 관련 추가 정보는 "취약성 평가 설정"(867페이지)의 내용을 참조하십시오.
3. Windows 머신에 계획을 할당합니다.

취약성 평가 스캔을 완료하면 검색된 취약성 목록을 확인할 수 있습니다. 정보를 처리하고 검색된 취약성 중 수정해야 할 항목을 결정할 수 있습니다.

취약성 평가의 결과를 모니터링하려면 **모니터링** > **개요** > **취약성/기존 취약성** 위젯을 확인합니다.

Linux 머신 취약성 평가

Linux 머신의 애플리케이션 수준 취약성과 커널 수준 취약성을 스캔할 수 있습니다.

Linux 머신에 대한 취약성 평가 구성하기

1. Cyber Protect 콘솔에서 보호 계획을 생성하고 **취약점 평가** 모듈을 활성화합니다.
2. 취약성 평가 설정을 지정합니다.
   - **스캔 대상** – **Linux 패키지 스캔**을 선택합니다.
   - **스케줄** – 취약성 평가를 수행할 스케줄을 정의합니다.

© Acronis International GmbH, 2003-2024

예약 옵션 관련 추가 정보는 "취약성 평가 설정"(867페이지)의 내용을 참조하십시오.

3. Linux 머신에 계획을 할당합니다.

취약성 평가 스캔을 완료하면 검색된 취약성 목록을 확인할 수 있습니다. 정보를 처리하고 검색된 취약성 중 수정해야 할 항목을 결정할 수 있습니다.

취약성 평가의 결과를 모니터링하려면 **모니터링** > **개요** > **취약성/기존 취약성** 위젯을 확인합니다.

macOS 장치의 취약성 평가

macOS 장치를 스캔하여 시스템 수준 및 애플리케이션 수준 취약성을 확인할 수 있습니다.

macOS 장치의 취약성 평가를 구성하려면

1. Cyber Protect 콘솔에서 보호 계획을 생성하고 **취약점 평가** 모듈을 활성화합니다.
2. 취약성 평가 설정을 지정합니다.
   - **스캔 대상** - **Apple 제품**이나 **macOS 서드 파티 제품** 중 하나를 선택하거나 두 제품을 모두 선택합니다.
   - **스케줄** – 취약성 평가를 수행할 스케줄을 정의합니다.

   예약 옵션 관련 추가 정보는 "취약성 평가 설정"(867페이지)의 내용을 참조하십시오.
3. macOS 장치에 계획을 할당합니다.

취약성 평가 스캔을 완료하면 검색된 취약성 목록을 확인할 수 있습니다. 정보를 처리하고 검색된 취약성 중 수정해야 할 항목을 결정할 수 있습니다.

취약성 평가의 결과를 모니터링하려면 **모니터링** > **개요** > **취약성/기존 취약성** 위젯을 확인합니다.

발견된 취약성 관리

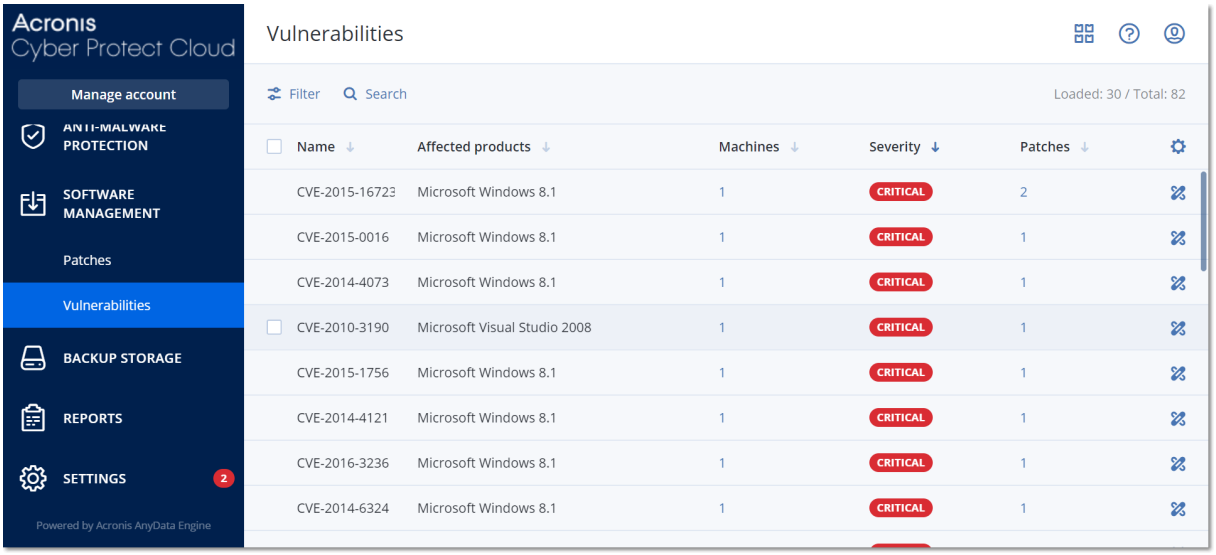
취약성 평가를 한 번 이상 수행했으며 취약성이 검색되었다면 **소프트웨어 관리** > **취약성**에서 취약성을 확인할 수 있습니다. 취약성 목록에는 설치해야 할 패치가 있거나, 제안된 패치가 없는 취약성이 모두 표시됩니다. 필터를 사용해 패치가 있는 취약성만 표시할 수 있습니다.

이름	설명
이름	취약성의 이름입니다.
영향을 받은 제품	취약성이 발견된 소프트웨어 제품입니다.
머신	영향을 받는 머신의 개수입니다.
심각도	발견된 취약성의 심각도입니다. CVSS(일반 취약성 점수 시스템)에 따라 취약성의 심각도 수준은 다음으로 나누어집니다. • **심각**: CVSS 9~10점 • **높음**: CVSS 7~9점 • **중간**: CVSS 3~7점

© Acronis International GmbH, 2003-2024

	• **낮음**: CVSS 0~3점 • **없음**
패치	해당 패치의 개수입니다.
게시됨	취약성이 CVE(일반 취약성 및 노출)에 게시된 날짜와 시간입니다.
감지됨	머신에서 기존 취약성이 최초로 감지된 날짜입니다.

목록에서 이름을 클릭해 발견된 취약성에 대한 설명을 찾을 수 있습니다.



취약성 수정 프로세스를 시작하려면

1. Cyber Protect 콘솔에서 **소프트웨어 관리** > **취약성**으로 이동합니다.
2. 목록에서 취약성을 선택한 후 **패치 설치**를 클릭합니다. 취약성 수정 마법사가 열립니다.
3. 선택한 머신에 설치할 패치를 선택하고 **다음**을 클릭합니다.
4. 패치를 설치하려는 머신을 선택합니다.
5. 재부팅 옵션을 선택합니다.
   a. 패치 설치 후 머신을 재부팅할지 여부를 선택합니다.

옵션	설명
아니요	패치 설치 후 머신을 자동으로 재부팅하지 않습니다.
필요 시	패치 적용에 필요한 경우에만 머신을 재부팅합니다.
예	패치 설치 후 머신을 자동으로 재부팅합니다. 재부팅 지연을 지정할 수도 있습니다.

   b. [선택 사항] 머신 백업이 진행 중인 동안 머신 재부팅을 지연시키려면 **백업이 끝날 때까지 재부팅하지 마십시오**를 선택합니다.
6. **패치 설치**를 클릭합니다.

그러면 선택한 머신에 선택한 패치가 설치됩니다.

© Acronis International GmbH, 2003-2024

패치 관리

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

지원되는 Windows OS용 서드 파티 제품에 대한 자세한 내용은 패치 관리에서 지원하는 서드 파티 제품 목록(62853)을 참조하십시오.

패치 관리 기능을 사용하면 다음 작업을 수행할 수 있습니다.

- OS 수준 및 애플리케이션 수준 업데이트 설치
- 패치 수동 또는 자동 승인
- 패치를 온디맨드로 또는 스케줄에 따라 설치
- 심각도, 카테고리, 승인 상태 등 각기 다른 조건에 따라 어떤 패치를 설치할지 정확하게 정의
- 사전 업데이트 백업을 수행해 업데이트 실패 방지
- 패치 설치 후의 재부팅 작업 정의

참고
Windows 업데이트를 작업하려면 패치 관리 기능이 워크로드에서 Windows 업데이트를 활성화해야 합니다.

Cyber Protection에서는 피어 투 피어 기술을 사용해 네트워크 대역폭 트래픽을 최소화합니다. 인터넷에서 업데이트를 다운로드할 전용 에이전트를 하나 이상 선택하여 네트워크의 다른 에이전트 사이에 분산시킬 수 있습니다. 또한 모든 에이전트는 피어 투 피어 에이전트로 서로 업데이트를 공유합니다.

패치 관리 워크플로우

패치 관리 워크플로우에서는 보호 계획 구성과 적용, 취약점 평가 스캔 실행, 패치 설정 구성, 패치 승인, 그리고 마지막으로 승인된 패치 설치 단계를 수행합니다. 워크플로우의 정확한 단계는 다음과 같습니다.

1. **취약점 평가** 및 **패치 관리** 모듈이 활성화되어 있는 보호 계획을 구성합니다.
2. 취약점 평가 설정을 구성합니다. 이러한 설정에 대한 자세한 내용은 "취약성 평가 설정"(867페이지) 항목을 참조하십시오.
3. 패치 관리 설정을 구성합니다. 이러한 설정에 대한 자세한 내용은 "보호 계획의 패치 관리 설정"(873페이지) 항목을 참조하십시오
4. 머신 하나 이상에 보호 계획을 적용합니다.
5. 취약점 평가 스캔이 완료될 때까지 기다립니다. 스캔은 보호 계획에 구성되어 있는 스케줄에 따라 자동으로 시작됩니다. 보호 계획의 **취약점 평가** 모듈에서 **지금 실행** 아이콘을 클릭하여 요청 시에 스캔을 수동으로 시작할 수도 있습니다.
6. 패치를 승인합니다. 자동 패치 승인용 설정(테스트 머신에 패치 자동 설치 포함)을 정의할 수 있습니다. 자세한 내용은 "자동 패치 승인"(880페이지)을(를) 참조하십시오. 패치의 승인 상태를

© Acronis International GmbH, 2003-2024

승인됨으로 설정하여 패치를 수동으로 승인할 수도 있습니다. 자세한 내용은 "수동으로 패치 승인"(883페이지)을(를) 참조하십시오.

7. 패치를 설치합니다. 승인된 패치는 보호 계획에 구성되어 있는 스케줄에 따라 자동으로 설치할 수 있습니다. 요청 시에 패치를 수동으로 설치할 수도 있습니다. 자세한 내용은 "요청 시 패치 설치"(884페이지)을(를) 참조하십시오.

모니터링 > **개요** > **패치 설치 내역** 위젯에서 패치 설치 결과를 모니터링할 수 있습니다.

보호 계획의 패치 관리 설정

보호 계획의 **패치 관리** 모듈에서 다음 패치 관리 설정을 구성할 수 있습니다.

- Windows OS의 Microsoft 및 서드 파티 제품용으로 설치할 업데이트.
- 자동 패치 설치를 실행할 시간.
- 업데이트 전 실행 여부.

보호 계획을 생성하고 **패치 관리** 모듈을 활성화하는 방법에 대한 자세한 내용은 "보호 계획 생성"(200페이지) 항목을 참조하십시오.

참고
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

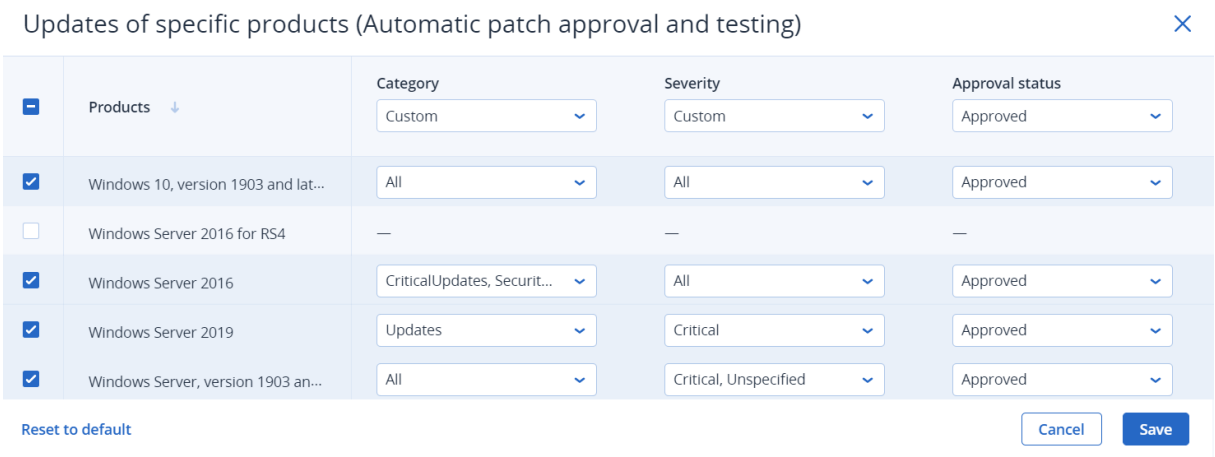
Microsoft 제품

선택한 머신에 Microsoft 업데이트를 설치하려면 **Microsoft 제품 업데이트** 옵션을 활성화합니다.

설치 옵션을 선택합니다.

옵션	설명
모두 업데이트	승인된 모든 업데이트를 설치하려면 이 옵션을 사용합니다.
보안 및 중요 업데이트만	승인된 모든 보안 및 중대한 업데이트를 설치하려면 이 옵션을 사용합니다.
특정 제품의 업데이트(자동 패치 승인 및 테스트)	각 제품별로 사용자 정의 설정을 정의하려면 이 옵션을 사용합니다. 특정 제품을 업데이트하려는 경우 각 제품에 대해 설치할 업데이트를 카테고리, 심각도, 승인 상태별로 정의할 수 있습니다. 자동 테스트 승인 및 패치 테스트를 구성하려면 이 옵션을 선택합니다.

© Acronis International GmbH, 2003-2024



Microsoft 제품의 경우 패치 배포에서는 Windows API 서비스를 사용합니다. 패치와 업데이트는 내부 위치나 배포 에이전트에 다운로드되거나 저장되지 않으며. Microsoft CDN에서 다운로드됩니다. 그러므로 업데이터 역할이 할당되어 있더라도 에이전트는 패치를 다운로드하여 배포할 수 없습니다.

Windows 서드 파티 제품

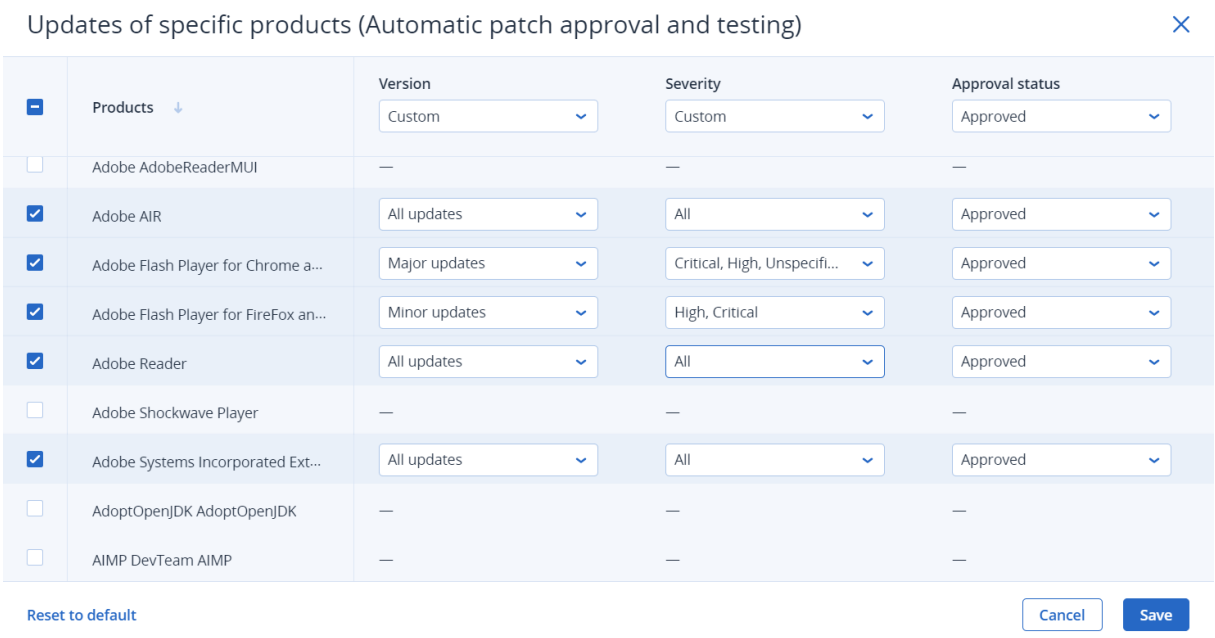
선택한 머신에 Windows OS용 서드 파티 업데이트를 설치하려면 **Windows 서드 파티 제품** 옵션을 활성화합니다.

설치 옵션을 선택합니다.

옵션	설명
모두 업데이트	승인된 모든 업데이트를 설치하려면 이 옵션을 사용합니다.*
대규모 업데이트만	승인된 모든 대규모 업데이트를 설치하려면 이 옵션을 사용합니다.
마이너 업데이트만	승인된 마이너 업데이트를 설치하려면 이 옵션을 사용합니다.
특정 제품의 업데이트(자동 패치 승인 및 테스트)	각 제품별로 사용자 정의 설정을 정의하려면 이 옵션을 사용합니다. 특정 제품을 업데이트하려는 경우 각 제품에 대해 설치할 업데이트를 카테고리, 심각도, 승인 상태별로 정의할 수 있습니다. 자동 테스트 승인 및 패치 테스트를 구성하려면 이 옵션을 선택합니다.
취약성이 감지된 애플리케이션의 최신 버전만 설치	취약성이 감지된 애플리케이션의 최신 업데이트만 설치하려면 이 확인란을 선택합니다.*

* 이 옵션을 사용하려면 Cyber Protect 에이전트 버전 23.11.36772 이상이 필요합니다.

© Acronis International GmbH, 2003-2024



Windows 서드 파티 제품의 경우에는 내부 Acronis 데이터베이스에서 관리 대상 워크로드로 패치가 직접 배포됩니다. 에이전트에 업데이터 역할이 할당되어 있으면 해당 에이전트가 패치 다운로드 및 배포에 사용됩니다.

예약

선택한 머신에 업데이트를 설치할 스케줄과 조건을 정의합니다.

필드	설명
다음 이벤트를 사용해 작업 실행 예약	작업을 실행할 시간을 정의하는 설정입니다. 다음 값을 선택할 수 있습니다. • **시간 기준 예약** - 기본 설정입니다. 지정한 시간에 따라 작업을 실행합니다. • **사용자가 시스템에 로그인할 때** – 기본적으로 사용자가 로그인하면 작업이 시작됩니다. 특정 사용자 계정만 작업을 트리거할 수 있도록 이 설정을 수정할 수 있습니다. • **사용자가 시스템에서 로그오프할 때** – 기본적으로 사용자가 로그오프하면 작업이 시작됩니다. 특정 사용자 계정만 작업을 트리거할 수 있도록 이 설정을 수정할 수 있습니다. **참고** 작업은 시스템 종료 시 실행되지 않습니다. 일정 예약 구성에서 시스템 종료와 로그오프는 다른 작업입니다. • **시스템 시작 시** – 운영 체제가 시작될 때 작업을 실행합니다. • **시스템 종료 시** – 운영 체제가 종료될 때 작업을 실행합니다.
예약 유형	**다음 이벤트를 사용해 작업 실행 예약**에서 **시간 기준 예약**을 선택한 경우 이 필드가 표시됩니다.

© Acronis International GmbH, 2003-2024

필드	설명
	다음 값을 선택할 수 있습니다. • **월간** – 작업을 실행할 월과 주 또는 일을 선택합니다. • **일일** - 기본 설정입니다. 작업을 실행할 요일을 선택합니다. • **매시간** – 작업을 실행할 요일, 반복 횟수, 시간 간격을 선택합니다.
시작 시간	**다음 이벤트를 사용해 작업 실행 예약**에서 **시간 기준 예약**을 선택한 경우 이 필드가 표시됩니다 작업을 실행할 정확한 시간을 선택합니다.
패치용 유지보수 기간 구성	**다음 이벤트를 사용해 작업 실행 예약**에서 **시간 기준 예약**을 선택한 경우 이 필드가 표시됩니다. 지정하는 시간 간격 동안에만 패치 설치가 실행되도록 하려면 이 설정을 선택합니다. 패치용 유지보수 기간에 따라 정의된 종료 시간까지 완료되지 않은 패치 설치 프로세스는 자동으로 중지됩니다.
날짜 범위 내에서 실행	**다음 이벤트를 사용해 작업 실행 예약**에서 **시간 기준 예약**을 선택한 경우 이 필드가 표시됩니다. 구성된 예약이 실행될 기간의 범위를 설정합니다.
운영 체제에 로그인할 때 작업을 시작하게 할 사용자 계정 지정	**다음 이벤트를 사용해 작업 실행 예약**에서 **사용자가 시스템에 로그인할 때**를 선택한 경우 이 필드가 표시됩니다. 다음 값을 선택할 수 있습니다. • **모든 사용자** - 어떤 사용자가 로그인하든 작업이 트리거되도록 하려는 경우 이 옵션을 사용합니다. • **다음 사용자** - 특정 사용자 계정의 로그인 시에만 작업이 트리거되도록 하려는 경우 이 옵션을 사용합니다.
운영 체제에서 로그아웃할 때 작업을 시작하게 할 사용자 계정 지정	**다음 이벤트를 사용해 작업 실행 예약**에서 **사용자가 시스템에서 로그오프할 때**를 선택한 경우 이 필드가 표시됩니다. 다음 값을 선택할 수 있습니다. • **모든 사용자** - 어떤 사용자가 로그아웃하든 작업이 트리거되도록 하려는 경우 이 옵션을 사용합니다. • **다음 사용자** - 특정 사용자 계정의 로그아웃 시에만 작업이 트리거되도록 하려는 경우 이 옵션을 사용합니다.
시작 조건	작업을 시작하기 위해 동시에 충족되어야 하는 모든 조건을 정의합니다. 맬웨어 방지 스캔용 시작 조건은 "시작 조건"에 설명되어 있는 **백업 모듈**용 시작 조건과 유사합니다. 다음과 같이 추가적인 시작 조건을 정의할 수 있습니다. • **기간 내에서 작업 시작 시간 분배** – 이 옵션을 사용하면 작업을 수행해야 하는 기간을 정의할 수 있습니다. 이 옵션을 사용해 작업 시간대를 설정하여 네트워크 병목현상을 피할 수 있습니다. 지연 시간은 시간 또는 분 단위

© Acronis International GmbH, 2003-2024

필드	설명
	로 지정할 수 있습니다. 예를 들어 기본 시작 시간이 오전 10시이고 지연 시간이 60분인 경우 작업은 오전 10시~오전 11시 사이에 시작됩니다. • **머신이 꺼진 경우 머신 시작 시 누락된 작업 실행** • **작업 실행 중 절전 또는 최대 절전 모드가 되는 것을 방지** – 이 옵션은 Windows를 구동 중인 머신에서만 유효합니다. • **시작 조건이 충족되지 않아도 다음 후에 작업 실행** - 다른 시작 조건에 관계없이 지정한 기간이 지나면 작업이 시작됩니다. **참고** Linux에서는 시작 조건이 지원되지 않습니다.
업데이트 후 재부팅	업데이트 설치 완료 후 머신을 자동으로 재부팅할지 여부를 정의합니다. 다음 값을 선택할 수 있습니다. • **해당 없음** – 업데이트 후 재부팅이 시작되지 않습니다. • **필요 시** – 업데이트 적용에 필요한 경우에만 재부팅이 시작됩니다. • **항상** – 업데이트 후 항상 재부팅이 시작됩니다. 재부팅 지연을 지정할 수 있습니다.
백업이 끝날 때까지 재부팅하지 마십시오	이 옵션을 선택하면 백업 프로세스가 실행 중인 경우 백업이 완료될 때까지 머신 재부팅이 지연됩니다.

업데이트 전 백업

소프트웨어 업데이트 설치 전에 백업 실행 – 시스템에서 업데이트를 설치하기 전에 머신의 증분 백업을 생성합니다. 이전에 생성한 백업이 없는 경우에는 머신의 전체 백업이 생성됩니다. 업데이트 설치에 실패하여 이전 상태로 돌아가야 하는 경우를 방지할 수 있게 해줍니다. **업데이트 전 백업** 옵션이 작동하려면 해당 머신에 패치 관리 및 백업 모듈이 활성화된 보호 계획과 백업될 항목(전체 머신 또는 부팅 + 시스템 볼륨)이 있어야 합니다. 백업에 적절하지 않은 항목을 선택한 경우에는 시스템이 **업데이트 전 백업** 옵션의 활성화를 허용하지 않습니다.

사용 가능한 패치 목록 확인

취약점 평가 스캔이 완료되고 나면 **소프트웨어 관리** > **패치**에서 사용 가능한 패치 관련 정보를 확인할 수 있습니다.

특정 패치 관련 상세 정보를 확인하려면 패치 목록에서 해당 패치를 클릭합니다.

화면에서 확인할 수 있는 패치 관련 정보가 아래 표에 설명되어 있습니다.

필드	설명
승인 상태	승인 상태는 주로 자동 승인 시나리오에서 필요합니다. 패치에 대해 다음 상태 중 하나를 정의할 수 있습니다.

© Acronis International GmbH, 2003-2024

	• **승인됨** – 패치가 최소 1개의 머신에 설치되어 있으며 유효성이 검증되었습니다. • **거절됨** – 패치가 안전하지 않으며 머신 시스템을 손상시킬 수 있습니다. • **승인 보류 중** – 패치 상태를 알 수 없으며 유효성을 검사해야 합니다
라이센스 계약	• 동의함 • 동의하지 않음. 라이센스 계약에 동의하지 않은 경우 패치 상태는 **거절됨**으로 설정되며 설치되지 않습니다.
심각도	패치의 심각도: • **심각** • **높음** • **중간** • **낮음** • **없음**
벤더	패치의 벤더
영향을 받은 제품	패치를 적용할 수 있는 제품
설치된 버전	이미 설치된 제품 버전
버전	패치 버전
카테고리	패치가 속한 카테고리: • **중대한 업데이트** – 심각하며 보안과 관련되지 않은 버그를 해결하고자 특정 문제에 대해 광범위하게 릴리스된 수정 항목입니다. • **보안 업데이트** – 보안 문제를 해결하고자 특정 제품에 대해 광범위하게 릴리스된 수정 항목입니다. • **정의 업데이트** – 바이러스 또는 기타 정의 파일을 업데이트합니다. • **업데이트 롤업** – 핫픽스, 보안 업데이트, 중대한 업데이트, 손쉬운 디플로이를 위해 패키징된 업데이트의 누적입니다. 롤업은 일반적으로 보안과 같은 특정 영역이나 인터넷 정보 서비스(IIS)와 같은 특정 컴퍼넌트를 대상으로 합니다. • **서비스 팩** – 모든 핫픽스, 보안 업데이트, 중대한 업데이트, 제품 출시 후 생성된 업데이트의 누적입니다. 서비스 팩에는 고객이 요청한 제한된 수의 설계 변경 또는 기능이 포함될 수도 있습니다. • **도구** – 작업 또는 일련의 작업을 완료할 수 있도록 지원하는 유틸리티 또는 기능입니다. • **기능 팩** – 새로운 기능 릴리스로, 일반적으로 다음 릴리스에서 제품에 적용됩니다. • **업데이트** – 심각하지 않으며 보안과 관련되지 않은 버그를 해결하고자 특정 문제에 대해 광범위하게 릴리스된 수정 항목입니다. • **애플리케이션** – 애플리케이션용 패치.
릴리스 날짜	패치가 릴리스된 날짜입니다.
마지막으로	패치가 마지막으로 보고된 날짜입니다

© Acronis International GmbH, 2003-2024

보고된 날짜	
처음 설치한 날짜	패치가 머신에 처음 정상적으로 설치된 날짜입니다
Microsoft KB	Microsoft 제품용 패치의 경우 KB 문서 ID가 필드에 표시됩니다
머신	영향을 받는 머신의 개수입니다.
취약성	취약성의 개수입니다. 클릭하면 취약성 목록으로 리디렉션됩니다.
크기	패치의 평균 크기
언어	패치가 지원하는 언어
벤더 사이트	벤더의 공식 사이트

패치 목록 수명 구성

패치 화면에서 패치 목록 수명을 구성하면 패치 목록을 최신 상태로 유지할 수 있습니다. 이 설정은 사용 가능한 상태로 감지된 패치가 패치 목록에 표시되는 기간을 정의합니다. 패치는 설치가 누락된 것으로 표시되었던 모든 머신에 정상적으로 설치되거나 목록 수명이 경과되고 나면 목록에서 제거됩니다.

패치 목록 수명을 구성하려면

1. Cyber Protect 콘솔에서 **소프트웨어 관리** > **패치**로 이동합니다.
2. **설정**을 클릭합니다.
3. **목록 수명**에서 적절한 옵션을 선택합니다.

옵션	설명
영구	패치가 항상 목록에 유지됩니다.
7일	첫 설치 후 7일이 경과하면 패치가 목록에서 제거됩니다. 머신 2대에 패치를 설치해야 하는 경우를 예로 들어 보겠습니다. 두 머신 하나는 온라인이고 다른 하나는 오프라인입니다. 첫 번째 머신에 패치가 설치되었습니다. 이 경우 7일이 지나면 패치는 오프라인 상태였던 두 번째 머신에 설치되지 않았더라도 패치 목록에서 제거됩니다.
30일	첫 설치 후 30일이 경과하면 패치가 목록에서 제거됩니다.

© Acronis International GmbH, 2003-2024

자동 패치 승인

자동 패치 승인을 설정하면 머신에 업데이트를 설치하는 프로세스를 더욱 쉽게 진행할 수 있습니다. 자동 패치 승인 사용 시에는 수동 패치 승인 프로세스로 인해 패치 설치가 지연되는 상황이 발생하지 않습니다. 또한 중요 업데이트와 수정이 더 빠르게 설치되므로 시스템의 신뢰성도 높아집니다.

테스트 시나리오에서 자동 패치 승인을 사용하여 패치를 자동으로 설치할 수 있습니다. 테스트 머신에 정상적으로 설치되는 패치는 운영 머신에도 자동 설치됩니다. 이 시나리오에 대한 자세한 내용은 "자동 패치 승인 및 테스트용 사용 사례"(881페이지) 항목을 참조하십시오.

테스트 단계를 건너뛰고 운영 환경에 패치를 자동 설치하려는 시나리오에서도 자동 패치 승인을 사용할 수 있습니다. 이 시나리오에 대한 자세한 내용은 "자동 패치 승인(테스트 없음)용 사용 사례"(883페이지) 항목을 참조하십시오.

자동 패치 승인 구성

자동 패치 승인을 구성하면 수동 패치 승인 프로세스로 인해 패치 설치가 지연되는 상황을 방지할 수 있습니다.

자동 패치 승인을 구성하려면

1. Cyber Protect 콘솔에서 **소프트웨어 관리** > **패치**로 이동합니다.
2. **설정**을 클릭합니다.
3. **자동 패치 승인**을 활성화합니다.
4. 자동 패치 승인의 설정을 구성합니다.
   a. 자동 패치 승인 옵션을 선택합니다.

옵션	설명
자동 패치 승인 및 테스트	패치를 정상적으로 설치한 후 선택한 기간(일)이 지나면 패치의 승인 상태가 **승인됨**으로 변경됩니다. 먼저 테스트 머신에 패치를 설치하여 모든 기능이 정상 작동하는지 테스트한 후에 운영 환경에 패치를 설치하려는 경우 이 설정을 사용하는 것이 좋습니다.
자동 패치 승인(테스트 없음)	패치가 검색된 후 선택한 기간(일)이 지나면 패치의 승인 상태가 **승인됨**으로 변경됩니다.

   b. 자동 패치 승인 옵션의 조건이 충족된 후에 경과되어야 하는 기간(일)을 선택합니다. 이 기간이 지나면 패치 승인 상태가 **승인 보류 중**에서 **승인됨**으로 자동 변경됩니다.
5. **라이선스 계약을 자동으로 수락**을 선택합니다.
6. **적용**을 클릭합니다.

© Acronis International GmbH, 2003-2024

자동 패치 승인 및 테스트용 사용 사례

새 패치를 운영 머신에 설치하기 전에 테스트 머신에서 테스트를 하려는 경우 두 가지 보호 계획(테스트용 패치 설치를 위한 계획과 테스트한 패치를 운영 머신에 설치하기 위한 계획)을 구성할 수 있습니다. 이렇게 하면 운영 환경에 설치하는 패치가 안전하며 패치 설치 후 운영 머신이 정상 작동함을 확인할 수 있습니다.

이 사용 사례에서는 다음 단계를 수행합니다.

1. 자동 패치 승인의 설정을 구성합니다. **자동 패치 승인 및 테스트** 옵션을 선택합니다. 자세한 내용은 "자동 패치 승인 구성"(880페이지)을(를) 참조하십시오.
2. **패치 관리** 모듈이 활성화된 테스트용 보호 계획(예: '테스트 패칭')을 구성한 후 테스트 환경의 머신에 적용합니다. 다음과 같이 패치 설치 조건을 지정합니다. 패치 승인 상태는 **승인 보류 중**이어야 합니다. 이 단계는 패치를 검증하고 머신이 패치 설치 후에도 제대로 작동하는지 확인하는 데 필요합니다. 자세한 내용은 "테스트 패치 보호 계획 구성"(881페이지)을(를) 참조하십시오.
3. **패치 관리** 모듈이 활성화된 운영 환경용 보호 계획(예: '운영 패치')을 구성한 후 운영 환경의 머신에 적용합니다. 다음과 같이 패치 설치 조건을 지정합니다. 패치 상태가 **승인됨**이어야 합니다. 자세한 내용은 "운영 패치 보호 계획 구성"(882페이지)을(를) 참조하십시오.
4. 테스트 패치 계획을 실행하고 결과를 확인합니다. 문제가 없는 머신의 승인 상태는 **승인 보류 중**으로 유지하고 정상 작동하지 않는 머신의 승인 상태는 **거절됨**으로 변경합니다. **자동 패치 승인** 설정에 지정되어 있는 기간(일)에 따라 패치 상태가 **승인 보류 중**에서 **승인됨**으로 자동 변경됩니다. 운영 패치 계획을 실행하면 **승인됨** 상태의 패치만 운영 머신에 설치됩니다. 자세한 내용은 "테스트 패치 보호 계획 실행 및 안전하지 않은 패치 거절"(883페이지)을(를) 참조하십시오.
5. 운영 패치 계획을 실행합니다.

테스트 패치 보호 계획 구성

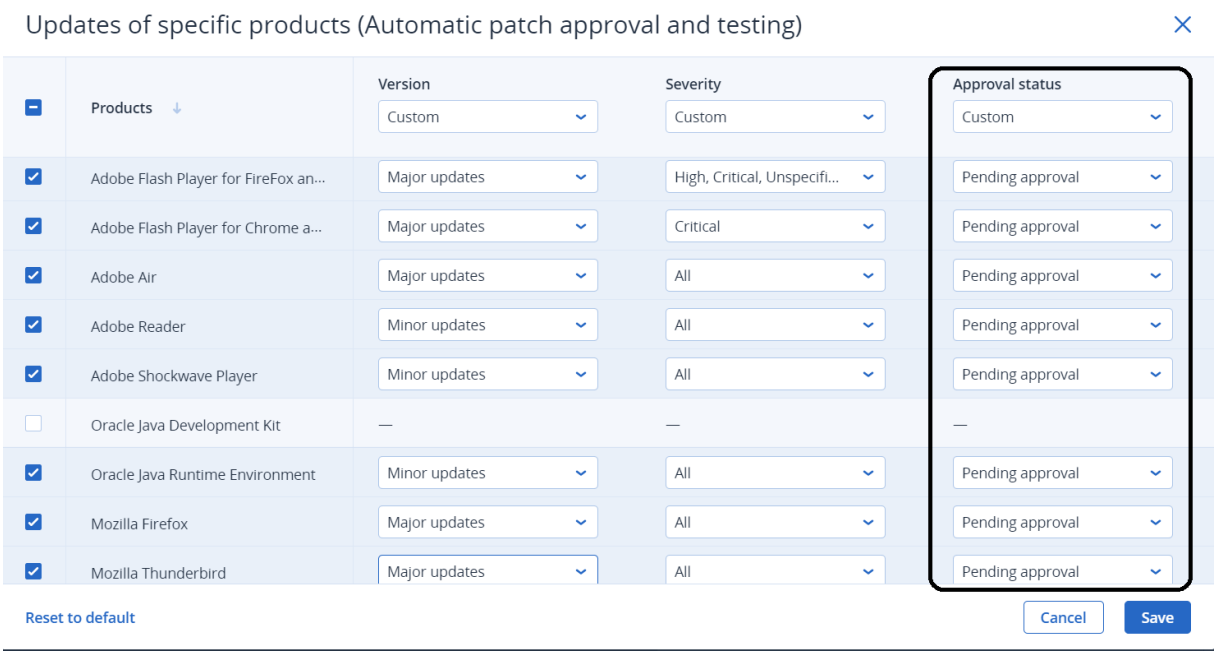
테스트 환경의 머신용 패치 설치 설정을 사용하여 보호 계획을 구성할 수 있습니다.

테스트 패치 보호 계획을 구성하려면

1. Cyber Protect 콘솔에서 **관리** > **보호 계획**으로 이동합니다.
2. **계획 생성**을 클릭합니다.
3. **패치 관리** 모듈을 활성화합니다.
4. Microsoft 및 서드 파티 제품, 스케줄, 사전 업데이트 백업에 대해 설치할 업데이트를 정의합니다. 이러한 설정에 대한 자세한 내용은 "보호 계획의 패치 관리 설정"(873페이지) 항목을 참조하십시오.

중요
업데이트하려는 모든 제품의 승인 상태로 **승인 보류 중**을 선택합니다. 그러면 에이전트가 테스트 환경의 선택한 머신에 **승인 보류 중** 상태의 패치만 설치합니다.

© Acronis International GmbH, 2003-2024



운영 패치 보호 계획 구성

운영 환경의 머신용 패치 설치 설정을 사용하여 보호 계획을 구성할 수 있습니다.

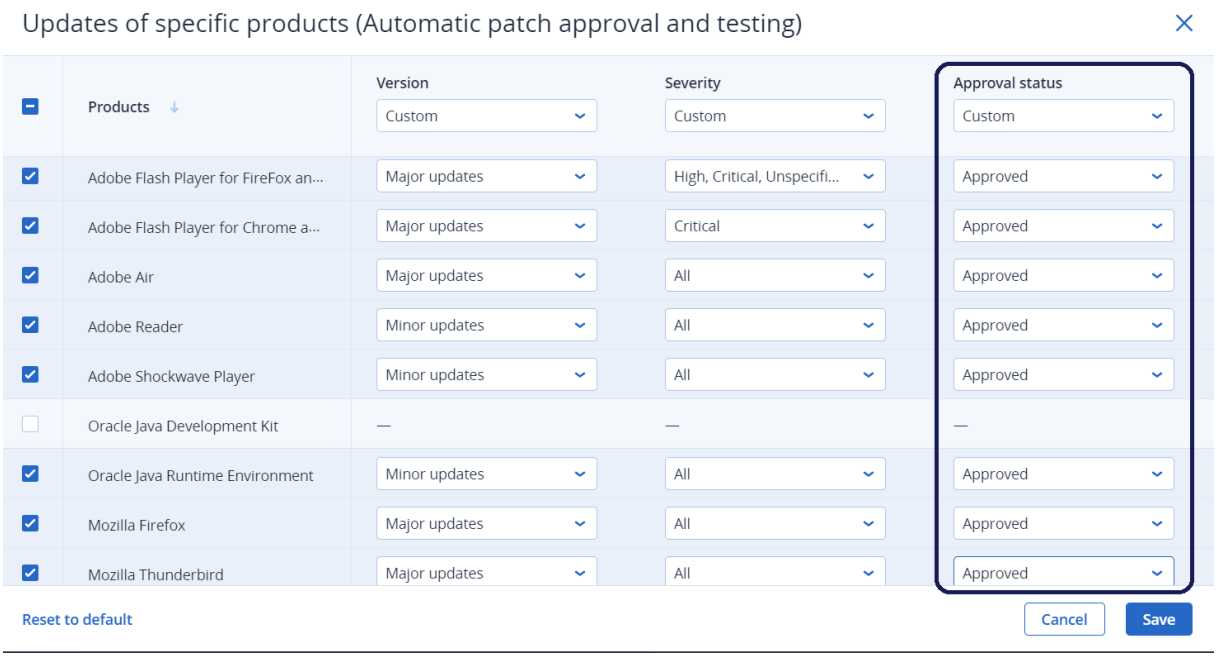
운영 패치 보호 계획을 구성하려면

1. Cyber Protect 콘솔에서 **관리** > **보호 계획**으로 이동합니다.
2. **계획 생성**을 클릭합니다.
3. **패치 관리** 모듈을 활성화합니다.
4. Microsoft 및 서드 파티 제품, 스케줄, 사전 업데이트 백업에 대해 설치할 업데이트를 정의합니다. 이러한 설정에 대한 자세한 내용은 "보호 계획의 패치 관리 설정"(873페이지) 항목을 참조하십시오.

중요

업데이트하려는 모든 제품의 **승인 상태**를 **승인됨**으로 설정합니다. 그러면 에이전트가 운영 환경의 선택한 머신에 **승인됨** 상태의 패치만 설치합니다.

© Acronis International GmbH, 2003-2024



테스트 패치 보호 계획 실행 및 안전하지 않은 패치 거절

테스트 환경의 머신에 패치를 설치한 후에는 모든 기능이 정상 작동하는지를 확인할 수 있습니다. 문제가 없는 머신의 승인 상태는 **승인 보류 중**으로 유지하고 정상 작동하지 않는 머신의 승인 상태는 **거절됨**으로 변경할 수 있습니다.

테스트 패치 보호 계획을 실행하고 안전하지 않은 패치를 거절하려면

1. 테스트 패치 보호 계획을 수동으로 실행하거나 스케줄에 따라 실행합니다.
2. 결과에 따라 설치된 패치 중 안전한 패치를 확인합니다.
3. **소프트웨어 관리** > **패치**로 이동해 안전하지 않은 패치의 **승인 상태**를 **거절됨**으로 설정합니다.

자동 패치 승인(테스트 없음)용 사용 사례

새 패치를 테스트 머신에 먼저 설치하지 않고 운영 머신에 최대한 빨리 자동 설치하려는 경우에는 보호 계획을 하나만 구성하면 됩니다.

이 사용 사례에서는 다음 단계를 수행합니다.

1. 자동 패치 승인의 설정을 구성합니다. **자동 패치 승인(테스트 없음)** 옵션을 선택합니다. 자세한 내용은 "자동 패치 승인 구성"(880페이지)을(를) 참조하십시오.
2. **패치 관리** 모듈이 활성화된 운영 환경용 보호 계획(예: '운영 패치')을 구성한 후 운영 환경의 머신에 적용합니다. 다음과 같이 패치 설치 조건을 지정합니다. 패치 상태가 **승인됨**이어야 합니다. 자세한 내용은 "운영 패치 보호 계획 구성"(882페이지)을(를) 참조하십시오.
3. 운영 패치 계획을 실행합니다.

수동으로 패치 승인

패치를 수동으로 승인한 후 테스트 단계를 건너뛰면 패치를 더 빠르게 설치할 수 있습니다.

© Acronis International GmbH, 2003-2024

사전 요구 사항

- **패치 관리** 모듈이 활성화된 보호 계획이 Windows 머신 하나 이상에 적용되어 있어야 합니다.
- 보호 계획이 적용되어 있는 머신 하나 이상에 아직 설치되지 않은 패치가 있어야 합니다.

수동으로 패치를 승인하려면

1. Cyber Protect 콘솔에서 **소프트웨어 관리** > **패치**로 이동합니다.
2. 설치하려는 패치를 선택한 다음 라이선스 계약을 수락합니다.
3. 패치의 **승인 상태**를 **승인됨**으로 설정합니다.
   패치의 승인 상태가 **승인됨**으로 설정됩니다. 보호 계획에 정의되어 있는 스케줄에 따라 패치가 머신에 자동으로 설치됩니다. 패치를 즉시 설치하려면 "요청 시 패치 설치"(884페이지) 항목에 설명되어 있는 절차를 진행하십시오.

요청 시 패치 설치

예약된 설치 시간까지 기다리기를 원하지 않는다면 요청 시에 패치를 수동 설치할 수 있습니다.

수동 패치 설치를 시작할 수 있는 3개 화면은 **패치**, **취약성** 및 **모든 장치**입니다.

수동으로 패치를 설치하려면

패치 화면에서 설치

1. Cyber Protect 콘솔에서 **소프트웨어 관리** > **패치**로 이동합니다.
2. 설치하려는 패치에 대한 라이센스 계약을 수락합니다.
3. **패치 설치** 마법사에서 설치하려는 패치를 선택한 다음 **설치**를 클릭합니다.
4. 패치를 설치하려는 머신을 선택합니다.
5. 재부팅 옵션을 선택합니다.
   a. 패치 설치 후 머신을 재부팅할지 여부를 선택합니다.

옵션	설명
아니요	패치 설치 후 머신을 자동으로 재부팅하지 않습니다.
필요 시	패치 적용에 필요한 경우에만 머신을 재부팅합니다.
예	패치 설치 후 머신을 자동으로 재부팅합니다. 재부팅 지연을 지정할 수도 있습니다.

   b. [선택 사항] 머신 백업이 진행 중인 동안 머신 재부팅을 지연시키려면 **백업이 끝날 때까지 재부팅하지 마십시오**를 선택합니다.
6. **패치 설치**를 클릭합니다.

취약성 화면에서 설치

1. Cyber Protect 콘솔에서 **소프트웨어 관리** > **취약성**으로 이동합니다.
2. "발견된 취약성 관리"(870페이지) 항목의 설명에 따라 수정 프로세스를 수행합니다.

© Acronis International GmbH, 2003-2024

모든 장치에서

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 패치를 설치하려는 머신을 선택합니다.
3. **패치**를 클릭합니다.
4. 설치하려는 패치를 선택하고 **다음**을 클릭합니다.
5. 재부팅 옵션을 선택합니다.
   a. 패치 설치 후 머신을 재부팅할지 여부를 선택합니다.

옵션	설명
아니요	패치 설치 후 머신을 자동으로 재부팅하지 않습니다.
필요시	패치 적용에 필요한 경우에만 머신을 재부팅합니다.
예	패치 설치 후 머신을 자동으로 재부팅합니다. 재부팅 지연을 지정할 수도 있습니다.

   b. [선택 사항] 머신 백업이 진행 중인 동안 머신 재부팅을 지연시키려면 **백업이 끝날 때까지 재부팅하지 마십시오**를 선택합니다.
6. **패치 설치**를 클릭합니다.

© Acronis International GmbH, 2003-2024

소프트웨어 및 하드웨어 인벤토리 관리

소프트웨어 인벤토리

소프트웨어 인벤토리 기능은 Advanced 팩이 활성화되어 있거나 (레거시) Cyber Protect 라이선스가 있는 장치에 사용할 수 있습니다. 이 기능을 사용하면 모든 Windows 및 macOS 장치에 설치되어 있는 모든 소프트웨어 애플리케이션을 볼 수 있습니다.

소프트웨어 인벤토리 데이터를 가져오려면 장치에서 자동 또는 수동 스캔을 실행하면 됩니다.

소프트웨어 인벤토리 데이터를 사용하여 다음을 수행할 수 있습니다.

- 회사 장치에 설치된 모든 애플리케이션에 대한 정보 찾아보기 및 비교
- 애플리케이션을 업데이트해야 하는지 결정
- 사용하지 않는 애플리케이션을 제거해야 하는지 결정
- 여러 회사 장치의 소프트웨어 버전이 동일한지 확인
- 연속 스캔 사이의 소프트웨어 상태 변경 사항 모니터링

소프트웨어 인벤토리 스캐닝 활성화

장치에서 소프트웨어 인벤토리 스캐닝이 활성화된 경우 시스템에서 자동으로 12시간마다 소프트웨어 데이터를 수집합니다.

소프트웨어 인벤토리 스캐닝 기능은 필요한 라이선스가 있는 모든 장치에 대해 기본적으로 활성화되지만 필요한 경우 설정을 변경할 수 있습니다.

참고
고객 테넌트는 소프트웨어 인벤토리 스캐닝을 활성화하거나 비활성화할 수 있습니다. 단위 테넌트는 소프트웨어 인벤토리 스캐닝 설정을 볼 수만 있고 변경할 수는 없습니다.

소프트웨어 인벤토리 스캐닝을 활성화하려면

1. Cyber Protect 콘솔에서 **설정**으로 이동합니다.
2. **보호**를 클릭합니다.
3. **인벤토리 스캐닝**을 클릭합니다.
4. 모듈 이름 옆의 스위치를 클릭하여 **소프트웨어 인벤토리 스캐닝** 모듈을 활성화합니다.

소프트웨어 인벤토리 스캐닝을 비활성화하려면

1. Cyber Protect 콘솔에서 **설정**으로 이동합니다.
2. **보호**를 클릭합니다.
3. **인벤토리 스캐닝**을 클릭합니다.
4. 모듈 이름 옆의 스위치를 클릭하여 **소프트웨어 인벤토리 스캐닝** 모듈을 비활성화합니다.

© Acronis International GmbH, 2003-2024

수동으로 소프트웨어 인벤토리 스캔 실행

소프트웨어 인벤토리 화면 또는 **인벤토리** 화면의 **소프트웨어** 탭에서 수동으로 소프트웨어 인벤토리 스캔을 실행할 수 있습니다.

사전 요구 사항

- 장치가 Windows 또는 macOS 운영 체제를 사용합니다.
- 장치에 필요한 (레거시) Cyber Protect 라이선스가 있거나 고급 관리 팩이 활성화되어 있습니다.

소프트웨어 인벤토리 화면에서 소프트웨어 인벤토리 스캔을 실행하려면

1. Cyber Protect 콘솔에서 **소프트웨어 관리**로 이동합니다.
2. **소프트웨어 인벤토리**를 클릭합니다.
3. **그룹화 기준:** 드롭다운 필드에서 **장치**를 선택합니다.
4. 스캔할 장치를 찾고 **지금 스캔**을 클릭합니다.

인벤토리 화면의 소프트웨어 탭에서 소프트웨어 인벤토리 스캔을 실행하려면

1. Cyber Protect 콘솔에서 **장치**로 이동합니다.
2. 스캔할 장치를 클릭하고 **인벤토리**를 클릭합니다.
3. **소프트웨어** 탭에서 **지금 스캔**을 클릭합니다.

소프트웨어 인벤토리 찾아보기

모든 회사 장치에서 사용할 수 있는 모든 소프트웨어 애플리케이션의 데이터를 조회하고 찾아볼 수 있습니다.

사전 요구 사항

- 장치가 Windows 또는 macOS 운영 체제를 사용합니다.
- 장치에 필요한 (레거시) Cyber Protect 라이선스가 있거나 고급 관리 팩이 활성화되어 있습니다.
- 장치의 소프트웨어 인벤토리 스캔이 완료되었습니다.

모든 Windows 및 macOS 회사 장치에서 사용할 수 있는 모든 소프트웨어 애플리케이션을 보려면

1. Cyber Protect 콘솔에서 **소프트웨어 관리**로 이동합니다.
2. **소프트웨어 인벤토리**를 클릭합니다.
   기본적으로 데이터는 장치별로 그룹화되어 있습니다. 다음 표에서는 **소프트웨어 인벤토리** 화면에 표시되는 데이터를 설명합니다.

열	설명
이름	애플리케이션의 이름.
버전	애플리케이션의 버전.
상태	애플리케이션의 상태.

© Acronis International GmbH, 2003-2024

열	설명
	• **새로 만들기**. • **업데이트됨**. • **제거됨**. • **변경 사항 없음**.
벤더	애플리케이션의 벤더.
설치 날짜	애플리케이션이 설치된 날짜 및 시간.
마지막 실행 시간	MacOS 장치만 해당. 애플리케이션이 마지막으로 활성화된 날짜 및 시간.
위치	애플리케이션이 설치된 디렉토리.
사용자	애플리케이션을 설치한 사용자.
시스템 유형	Windows 장치만 해당. 애플리케이션의 비트 유형입니다. • 32비트 애플리케이션의 경우 **X86**. • 64비트 애플리케이션의 경우 **X64**.

3. 데이터를 애플리케이션별로 그룹화하려면 **그룹화 기준:** 드롭다운 필드에서 **애플리케이션**을 선택합니다.
4. 화면에 표시되는 정보의 범위를 좁히려면 필터 하나 또는 여러 필터의 조합을 사용하십시오.
   a. **필터**를 클릭합니다.
   b. 필터 하나 또는 여러 필터의 조합을 선택합니다.
      다음 표에서는 **소프트웨어 인벤토리** 화면의 필터를 설명합니다.

필터	설명
장치 이름	장치 이름. 여러 항목을 선택할 수 있습니다. 특정 장치에서 소프트웨어를 비교하려면 이 필터를 사용합니다.
애플리케이션	애플리케이션 이름. 여러 항목을 선택할 수 있습니다. 특정 장치 또는 모든 장치에서 특정 애플리케이션에 대한 데이터를 비교하려면 이 필터를 사용합니다.
벤더	애플리케이션의 벤더. 여러 항목을 선택할 수 있습니다. 특정 장치 또는 모든 장치에서 특정 벤더의 모든 애플리케이션을 보려면 이 필터를 사용합니다.
상태	애플리케이션 상태. 여러 항목을 선택할 수 있습니다. 특정 장치 또는 모든 장치에서 선택된 상태의 모든 애플리케이션을 보려면 이 필터를 사용합니다.
설치 날짜	애플리케이션이 설치된 날짜. 특정 장치 또는 모든 장치에서 특정 날짜에 설치된 모든 애플리케이션을 보려면 이 필터를 사용합니다.

© Acronis International GmbH, 2003-2024

필터	설명
스캔 날짜	소프트웨어 인벤토리 스캔 날짜. 해당 날짜에 스캔된 특정 장치 또는 모든 장치의 소프트웨어에 대한 정보를 보려면 이 필터를 사용합니다.

c. **적용**을 클릭합니다.

5. 전체 소프트웨어 인벤토리 목록을 찾아보려면 화면의 왼쪽 아래의 페이지 매김을 사용하십시오.

- 열려는 페이지의 번호를 클릭합니다.
- 드롭다운 필드에서 열려는 페이지의 페이지 번호를 선택합니다.

단일 장치의 소프트웨어 인벤토리 보기

상태, 버전, 벤더, 설치 날짜, 마지막 실행 날짜 및 위치와 같은 애플리케이션에 대한 자세한 정보뿐 아니라 단일 장치에 설치된 모든 소프트웨어 애플리케이션의 목록도 볼 수 있습니다.

사전 요구 사항

- 장치가 Windows 또는 macOS 운영 체제를 사용합니다.
- 장치에 필요한 (레거시) Cyber Protect 라이선스가 있거나 고급 관리 팩이 활성화되어 있습니다.
- 장치의 소프트웨어 인벤토리 스캔이 완료되었습니다.

소프트웨어 인벤토리 화면에서 단일 장치의 소프트웨어 인벤토리를 보려면

1. Cyber Protect 콘솔에서 **소프트웨어 관리**로 이동합니다.
2. **소프트웨어 인벤토리**를 클릭합니다.
3. **그룹화 기준:** 드롭다운 필드에서 **장치**를 선택합니다.
4. 다음 옵션 중 하나를 사용하여 검사할 장치를 찾습니다.
   - **필터**를 사용하여 장치 찾기:
     a. **필터**를 클릭합니다.
     b. **장치 이름** 필드에서 보려는 장치의 이름을 선택합니다.
     c. **적용**을 클릭합니다.
   - 동적 **검색**을 사용하여 장치 찾기:
     a. **검색**을 클릭합니다.
     b. 전체 장치 이름 또는 장치 이름의 일부를 입력합니다.

장치 화면에서 단일 장치의 소프트웨어 인벤토리를 보려면

1. Cyber Protect 콘솔에서 **장치**로 이동합니다.
2. 보려는 장치를 클릭하고 **인벤토리**를 클릭합니다.
3. **소프트웨어** 탭을 클릭합니다.

© Acronis International GmbH, 2003-2024

하드웨어 인벤토리

하드웨어 인벤토리 기능을 사용하여 다음 위치에서 사용할 수 있는 모든 하드웨어 컴포넌트를 볼 수 있습니다.

- 하드웨어 인벤토리 기능을 지원하는 라이센스가 있는 물리적 Windows 및 macOS 장치.
- 다음 가상화 플랫폼에서 실행되는 가상 Windows 및 macOS 머신: VMware, Hyper-V, Citrix, Parallels, Oracle, Nutanix, Virtuozzo, Virtuozzo Hybrid Infrastructure. 지원되는 가상화 플랫폼 버전 관련 추가 정보는 "지원되는 가상화 플랫폼"(30페이지)의 내용을 참고하십시오.

참고
Cyber Protect 레거시 버전에서는 가상 머신용 하드웨어 인벤토리 기능이 지원되지 않습니다.

하드웨어 인벤토리 기능은 보호 에이전트가 설치된 장치에서만 지원됩니다.

하드웨어 인벤토리 데이터를 가져오려면 장치에서 자동 또는 수동 스캔을 실행하면 됩니다.

하드웨어 인벤토리 데이터를 사용하여 다음을 수행할 수 있습니다.

- 조직의 모든 하드웨어 자산 검색
- 조직 내 모든 장치의 하드웨어 인벤토리 찾아보기
- 여러 회사 장치의 하드웨어 컴포넌트 비교
- 하드웨어 컴포넌트에 대한 자세한 정보 보기

하드웨어 인벤토리 스캐닝 활성화

물리적인 장치와 가상 머신에서 하드웨어 인벤토리 스캐닝이 활성화된 경우 시스템에서 자동으로 12시간마다 하드웨어 데이터를 수집합니다.

하드웨어 인벤토리 스캐닝 기능은 기본적으로 활성화되어 있지만 필요한 경우 이러한 설정을 변경할 수 있습니다.

참고
고객 테넌트는 하드웨어 인벤토리 스캐닝을 활성화하거나 비활성화할 수 있습니다. 단위 테넌트는 하드웨어 인벤토리 스캐닝 설정을 볼 수만 있고 변경할 수는 없습니다.

하드웨어 인벤토리 스캐닝을 활성화하려면

1. Cyber Protect 콘솔에서 **설정**으로 이동합니다.
2. **보호**를 클릭합니다.
3. **인벤토리 스캐닝**을 클릭합니다.
4. 모듈 이름 옆의 스위치를 클릭하여 **하드웨어 인벤토리 스캐닝** 모듈을 활성화합니다.

하드웨어 인벤토리 스캐닝을 비활성화하려면

1. Cyber Protect 콘솔에서 **설정**으로 이동합니다.
2. **보호**를 클릭합니다.

© Acronis International GmbH, 2003-2024

3. **인벤토리 스캐닝**을 클릭합니다.
4. 모듈 이름 옆의 스위치를 클릭하여 **하드웨어 인벤토리 스캐닝** 모듈을 비활성화합니다.

수동으로 하드웨어 인벤토리 스캔 실행

단일 장치에 대해 하드웨어 인벤토리 스캔을 수동으로 실행하고 해당 장치의 하드웨어 컴퍼넌트에 대한 현재 데이터를 볼 수 있습니다.

참고
가상 머신의 현재 날짜와 시간이 UTC 기준 현재 날짜 및 시간에 해당하는 경우에만 가상 머신의 하드웨어 인벤토리 스캔이 지원됩니다. 가상 머신이 정확한 시간 설정을 사용하도록 하려면 가상 머신의 **시간 동기화** 옵션을 비활성화하고 현재 날짜, 시간, 시간대를 설정한 후에 **Acronis Agent Core Service** 및 **Acronis Managed Machine Service**를 다시 시작합니다.

사전 요구 사항

- (모든 장치) 장치가 Windows 또는 macOS 운영 체제를 사용합니다.
- (모든 장치) 장치에 하드웨어 인벤토리 기능을 지원하는 라이선스가 있습니다. (레거시) Cyber Protect 버전에서는 가상 머신용 하드웨어 인벤토리 기능이 지원되지 않습니다.
- (모든 장치) 보호 에이전트가 장치에 설치되어 있습니다.
- (가상 머신) 머신이 지원되는 가상화 플랫폼 중 하나에서 실행됩니다. 자세한 내용은 "하드웨어 인벤토리"(890페이지)을(를) 참조하십시오.

단일 장치에서 하드웨어 인벤토리 스캔을 실행하려면

1. Cyber Protect 콘솔에서 **장치**로 이동합니다.
2. 스캔할 장치를 클릭하고 **인벤토리**를 클릭합니다.
3. **하드웨어** 탭에서 **지금 스캔**을 클릭합니다.

하드웨어 인벤토리 찾아보기

모든 회사 장치에서 사용할 수 있는 모든 하드웨어 컴퍼넌트의 데이터를 조회하고 찾아볼 수 있습니다.

사전 요구 사항

- (모든 장치) 장치가 Windows 또는 macOS 운영 체제를 사용합니다.
- (모든 장치) 장치에 하드웨어 인벤토리 기능을 지원하는 라이센스가 있습니다. Cyber Protect 레거시 버전에서는 가상 머신용 하드웨어 인벤토리 기능이 지원되지 않습니다.
- (모든 장치) 보호 에이전트가 장치에 설치되어 있습니다.
- (모든 장치) 장치의 하드웨어 인벤토리 스캔이 완료되었습니다.
- (가상 머신) 머신이 지원되는 가상화 플랫폼 중 하나에서 실행됩니다. 자세한 내용은 "하드웨어 인벤토리"(890페이지)을(를) 참조하십시오.

Windows 및 macOS 회사 장치에서 사용할 수 있는 모든 하드웨어 컴퍼넌트를 보려면

© Acronis International GmbH, 2003-2024

1. Cyber Protect 콘솔에서 **장치**로 이동합니다.
2. **보기:** 드롭다운 필드에서 **하드웨어**를 선택합니다.

참고
이 보기는 화면에 표시되는 데이터를 결정하는 열 세트입니다. 사전 정의된 보기는 **표준** 및 **하드웨어**입니다. 다양한 열 세트를 포함하고 필요에 따라 더 편리하게 이용하도록 사용자 정의 보기를 만들고 저장할 수 있습니다.

다음 표에서는 **하드웨어** 보기에 표시되는 데이터를 설명합니다.

열	설명
이름	장치 이름.
하드웨어 스캔 상태	하드웨어 스캔의 상태. • **완료됨**. • **시작되지 않음**. • **지원되지 않음**. 이 상태는 하드웨어 인벤토리 기능이 지원되지 않는 워크로드에 표시됩니다(예: 가상 머신, 모바일 장치, Linux 장치). • **에이전트 업데이트**. 오래된 버전의 에이전트가 장치에 설치되어 있는 경우 표시됩니다. 이 작업을 클릭하면 설정 > 에이전트 페이지로 리디렉션되며, 여기에서 관리자는 에이전트 업데이트를 수행할 수 있습니다. • **할당량 업그레이드**. 클릭하면 관리자가 현재 라이센스를 테넌트 라이센스에 사용할 수 있는 다른 라이센스 중 하나로 전환할 수 있는 대화 상자가 열립니다.
프로세서	장치의 모든 프로세서 모델.
프로세서 코어	장치의 모든 프로세서 코어 수.
디스크 스토리지	사용된 스토리지 및 장치의 모든 디스크에 대한 총 스토리지.
메모리	장치의 총 RAM 용량.
스캔 날짜	마지막 하드웨어 인벤토리 스캔의 날짜 및 시간.
마더보드	장치의 마더보드.
마더보드 시리얼 번호	마더보드의 시리얼 번호.
BIOS 버전	시스템의 BIOS 버전.
조직	장치가 속한 조직.
소유자	장치의 소유자.

© Acronis International GmbH, 2003-2024

열	설명
도메인	장치의 도메인.
운영 체제	장치의 운영 체제.
운영 체제 빌드	장치의 운영 체제 빌드.

3. 표에 열을 추가하려면 열 옵션 아이콘을 클릭하고 표에 표시할 열을 선택합니다.
4. 화면에 표시되는 정보의 범위를 좁히려면 하나 이상의 필터를 사용합니다.
   a. **검색**을 클릭합니다.
   b. 화살표를 클릭한 다음 **하드웨어**를 클릭합니다.
   c. 필터 하나 또는 여러 필터의 조합을 선택합니다.
      다음 표에서는 **하드웨어** 필터를 설명합니다.

필터	설명
프로세서 모델	여러 항목을 선택할 수 있습니다. 지정된 프로세서 모델이 있는 장치의 하드웨어 데이터를 보려면 이 필터를 사용합니다.
프로세서 코어	지정된 수의 프로세서 코어가 있는 장치의 하드웨어 데이터를 보려면 이 필터를 사용합니다.
디스크 전체 크기	지정된 총 스토리지 크기를 가진 장치의 하드웨어 데이터를 보려면 이 필터를 사용합니다.
메모리 용량	지정된 RAM 용량이 있는 장치의 하드웨어 데이터를 보려면 이 필터를 사용합니다.

   d. **적용**을 클릭합니다.
5. 데이터를 오름차순으로 정렬하려면 열 이름을 클릭합니다.

단일 장치의 하드웨어 보기

특정 장치의 마더보드, 프로세서, 메모리, 그래픽, 스토리지 드라이브, 네트워크 및 시스템에 대한 자세한 정보를 볼 수 있습니다.

사전 요구 사항

- (모든 장치) 장치가 Windows 또는 macOS 운영 체제를 사용합니다.
- (모든 장치) 장치에 하드웨어 인벤토리 기능을 지원하는 라이센스가 있습니다. Cyber Protect 레거시 버전에서는 가상 머신용 하드웨어 인벤토리 기능이 지원되지 않습니다.
- (모든 장치) 보호 에이전트가 장치에 설치되어 있습니다.
- (모든 장치) 장치의 하드웨어 인벤토리 스캔이 완료되었습니다.
- (가상 머신) 머신이 지원되는 가상화 플랫폼 중 하나에서 실행됩니다. 자세한 내용은 "하드웨어 인벤토리"(890페이지)을(를) 참조하십시오.

특정 장치의 하드웨어에 대한 자세한 정보를 보려면

© Acronis International GmbH, 2003-2024

1. Cyber Protect 콘솔에서 **장치->모든 장치**로 이동합니다.
2. **보기:** 드롭다운 필드에서 **하드웨어**를 선택합니다.
3. 아래 설명된 방법 중 하나를 사용하여 검사할 장치를 찾습니다.
   - **필터**를 사용하여 장치 찾기:
     a. **필터**를 클릭합니다.
     b. 필터 매개변수 하나 또는 여러 필터 매개변수의 조합을 선택하여 장치를 찾습니다.
     c. **적용**을 클릭합니다.
   - **검색**을 사용하여 장치 찾기:
     a. **검색**을 클릭합니다.
     b. 전체 장치 이름 또는 장치 이름의 일부를 입력하고 **입력**을 클릭합니다.
4. 장치가 표시된 행을 선택하고 **인벤토리**를 클릭합니다.
5. **하드웨어** 탭을 클릭합니다.
   다음 하드웨어 데이터를 사용할 수 있습니다.

하드웨어 컴포넌트	표시되는 정보
마더보드	장치 마더보드의 이름, 제조업체, 모델 및 시리얼 번호.
프로세서	장치 각 프로세서의 제조업체, 모델, 최대 클럭 속도 및 코어 수.
메모리	장치 메모리의 용량, 제조업체 및 시리얼 번호.
그래픽	장치 GPU의 제조업체 및 모델.
스토리지 드라이브	장치 스토리지 드라이브의 모델, 미디어 유형, 가용 공간 및 크기.
네트워크	장치의 MAC 주소, IP 주소 및 네트워크 어댑터 유형.
시스템	시스템의 제품 ID, 원래 설치 날짜, 시스템 부팅 시간, 시스템 제조업체, 시스템 모델, BIOS 버전, 부트 장치, 시스템 로캘 및 시간대.

© Acronis International GmbH, 2003-2024

원격 데스크탑 또는 원격 지원을 위해 워크로드에 연결

원격 데스크탑 및 지원 기능을 사용하면 원격 제어 또는 원격 지원을 위해 조직의 워크로드에 편리하게 연결할 수 있습니다. 2022년 12월부터는 해당 기능이 NEAR, RDP 및 Apple 화면 공유 프로토콜을 지원합니다. 자세한 내용은 "원격 연결 프로토콜"(900페이지)을(를) 참조하십시오.

원격 데스크탑 기능을 사용하여 수행할 수 있는 작업은 다음과 같습니다.

- 보기 전용 모드에서 NEAR를 사용하여 원격 Windows, macOS 및 Linux 워크로드에 연결.
- RDP를 사용하여 원격 Windows 워크로드에 연결.
- 보기 전용 또는 커튼 모드에서 Apple 화면 공유를 사용하여 원격 macOS 워크로드에 연결.
- 클라우드 원격 연결을 사용하여 관리 대상 워크로드에 연결한 후 원격으로 해당 워크로드 제어.
- 직접 원격 연결을 사용하여 비관리 대상 워크로드에 연결한 후 원격으로 해당 워크로드 제어.
- Acronis 빠른 지원을 사용하여 비관리 대상 원격 워크로드에 연결.
- 다양한 인증 방법을 사용하여 원격 워크로드에 연결. 원격 워크로드 자격 증명을 사용하거나, 관찰 또는 제어 권한을 요청하거나, 액세스 코드(빠른 지원의 경우)를 사용할 수 있습니다.
- 다중 보기에서 여러 모니터 동시 관찰.
- NEAR를 통해 연결한 경우 원격 세션 녹화.
- 세션 내역 보고서 확인.

Standard 및 Advanced Management 팩에 포함된 기능에 대한 자세한 내용은 "지원되는 원격 데스크탑 및 지원 기능"(896페이지) 항목을 참조하십시오.

원격 지원 기능을 사용하여 수행할 수 있는 작업은 다음과 같습니다.

- 제어 모드에서 NEAR를 사용하여 원격 Windows, macOS 및 Linux 워크로드에 연결.
- 제어 모드에서 Apple 화면 공유를 사용하여 원격 macOS 워크로드에 연결.
- 클라우드 원격 연결을 사용하여 워크로드에 원격 지원 제공.
- 로컬 워크로드와 원격 워크로드 간에 파일 전송.
- 원격 워크로드에서 다시 시작, 종료, 절전 모드 설정, 휴지통 비우기, 원격 사용자 로그아웃 처리 등의 기본적인 관리 작업 수행.
- 정기적으로 원격 워크로드의 데스크탑 스크린샷을 생성하여 해당 워크로드 모니터링.

Standard 보호 및 Advanced Management에 포함된 기능에 대한 자세한 내용은 "지원되는 원격 데스크탑 및 지원 기능"(896페이지) 항목을 참조하십시오.

© Acronis International GmbH, 2003-2024

중요

관리 대상 워크로드에 대해 전체 원격 데스크탑 및 지원 기능을 활성화하려면 원격 관리 계획을 구성하여 워크로드에 적용해야 합니다. 각 워크로드에는 원격 관리 계획을 하나만 적용할 수 있지만 필요에 따라 여러 원격 관리 계획을 구성한 후 각 워크로드에 적용할 수 있습니다.

예를 들어 RDP 프로토콜만 활성화된 원격 관리 계획을 생성하여 일부 워크로드에 적용할 수 있습니다. 그러면 추가 요금을 지불하고 워크로드별로 Advanced Management 라이선스를 활성화하지 않아도 이러한 워크로드에 원격으로 연결할 수 있습니다.

NEAR 및 Apple 화면 공유 프로토콜이 활성화된 다른 원격 관리 계획을 생성할 수도 있습니다. 이 경우에는 워크로드별 Advanced Management 라이선스가 활성화되며 해당 원격 관리 계획이 적용되는 각 워크로드에서 요금이 부과됩니다.

원격 관리 계획, 그리고 원격 관리 계획 사용 방법에 대한 자세한 내용은 "원격 관리 계획"(903페이지) 항목을 참조하십시오.

참고

원격 데스크탑 및 지원 기능을 사용하려면 다음 요건을 충족해야 합니다.

- 관리 중인(호스트) 워크로드에 Connect 클라이언트를 설치(1회)해야 합니다. 대상 워크로드에서 처음으로 원격 작업(원격 제어 또는 원격 지원)을 수행하려고 하면 클라이언트를 다운로드하라는 메시지가 표시됩니다. 보호 콘솔의 **다운로드** 창에서 Connect 클라이언트를 다운로드할 수도 있습니다. 구성할 수 있는 설정에 대한 자세한 내용은 "Connect 클라이언트 설정 구성"(930페이지)을(를) 참조하십시오.
- 관리 대상 워크로드에 Connect 에이전트를 설치해야 합니다. Connect 에이전트는 보호 에이전트 버전 15.0.31266부터 제공되는 모듈입니다.
- macOS 원격 워크로드의 경우에는 Connect 에이전트에 필요한 시스템 권한을 부여해야 합니다. 자세한 내용은 "macOS에서 Protection 에이전트 설치"(76페이지)을(를) 참조하십시오.
- 비관리 대상 워크로드에서 Acronis빠른 지원 애플리케이션을 실행해야 합니다. 웹 사이트에서 Acronis 빠른 지원을 다운로드할 수 있습니다.

각 원격 데스크탑 및 지원 컴포넌트가 지원하는 플랫폼에 대한 자세한 내용은 "지원되는 플랫폼"(899페이지) 항목을 참고하십시오.

지원되는 원격 데스크탑 및 지원 기능

2022년 12월에 도입된 원격 데스크탑 및 지원 기능의 지원되는 기능 변경 사항이 아래 표에 자세히 설명되어 있습니다.

기능	Standard Protection 2022년 12월 이전	Advanced Management 2022년 12월 이전	Standard Protection 2022년 12월 이후	Advanced Management 2022년 12월 이후
Windows용 RDP를 통한	예	아니요	아니요	아니요

© Acronis International GmbH, 2003-2024

기능	Standard Protection 2022년 12월 이전	Advanced Management 2022년 12월 이전	Standard Protection 2022년 12월 이후	Advanced Management 2022년 12월 이후
원격 지원				
사용자와 원격 접속 공유	아니요	예	아니요	아니요
원격 연결				
원격 작업	아니요	아니요	예	예
연결할 Windows/macOS/Linux 세션 선택	아니요	아니요	아니요	예
RDP 및 Apple 화면 공유를 통해 직접 연결	아니요	아니요	아니요	예
여러 창 제어	아니요	아니요	아니요	예
연결 모드: 제어/보기 전용/커튼	아니요	아니요	아니요	예
원격 연결용 일반 자격 증명 지원	아니요	아니요	예	예
기술 담당자당 동시 연결 수				
RDP	예	예	예	예
NEAR	아니요	아니요	아니요	예
파일 전송 및 공유				
Windows - Windows/macOS/Linux 간	아니요	아니요	아니요	예
macOS - Windows/macOS/Linux 간	아니요	아니요	아니요	예
Linux - Windows/macOS/Linux 간	아니요	아니요	아니요	예
빠른 지원 애플리케이션을 통해 연결				
Windows - Windows/macOS/Linux 간	아니요	아니요	아니요	예

© Acronis International GmbH, 2003-2024

기능	Standard Protection 2022년 12월 이전	Advanced Management 2022년 12월 이전	Standard Protection 2022년 12월 이후	Advanced Management 2022년 12월 이후
macOS - Windows/macOS/Linux 간	아니요	아니요	아니요	예
Linux - Windows/macOS/Linux 간	아니요	아니요	아니요	예
프로토콜을 통한 원격 연결				
NEAR를 통한 원격 연결				
Windows - Windows/macOS/Linux 간	아니요	아니요	아니요	예
macOS - Windows/macOS/Linux 간	아니요	아니요	아니요	예
Linux - Windows/macOS/Linux 간	아니요	아니요	아니요	예
RDP를 통한 원격 연결(데스크톱 클라이언트)				
Windows 간	예	예	예	예
macOS - Windows 간	예	예	예	예
Linux - Windows 간	아니요	아니요	예	예
RDP를 통한 원격 연결(웹 클라이언트)				
Windows 간	예	예	예	예
macOS - Windows 간	예	예	예	예
Linux - Windows 간	아니요	아니요	예	예
Apple 화면 공유를 통한 원격 연결				
Windows/macOS/Linux - macOS 간	아니요	아니요	아니요	예
세션 관리				
세션 녹화	아니요	아니요	아니요	예

© Acronis International GmbH, 2003-2024

기능	Standard Protection 2022년 12월 이전	Advanced Management 2022년 12월 이전	Standard Protection 2022년 12월 이후	Advanced Management 2022년 12월 이후
보고 및 모니터링				
세션 내역 및 검색	아니요	아니요	아니요	예
스크린샷 전송	아니요	아니요	아니요	예

지원되는 플랫폼

아래 표에는 원격 데스크탑 및 지원 기능의 각 컴포넌트가 지원하는 운영 체제가 나와 있습니다.

원격 데스크탑 컴포넌트	지원되는 플랫폼
Connect 클라이언트	• Windows 7 이상 • macOS 10.13 이상 • Linux: openSUSE 8 Debian 9, 10 Ubuntu 18.0-20.10 Red Hat Enterprise Linux 8 CentOS 8 Fedora 31-33 SUSE Linux Enterprise Server 15 SP2 Linux Mint 20 Manjaro 20
Connect 에이전트	• Windows 7 이상 • Windows Server 2008 R2 이상 • macOS 10.13 이상 • Linux: Red Hat Enterprise Linux 8, 8.1 Fedora 30 Ubuntu 18.4 LTS(Bionic Beaver) -19.04(Disco Dingo) Debian 9, 10 CentOS 8 openSUSE 15.1
Acronis 빠른 지원	• Windows 7 이상 • Windows Server 2008 R2 이상 • macOS 10.13 이상 • Linux: Red Hat Enterprise Linux 8, 8.1

© Acronis International GmbH, 2003-2024

원격 데스크탑 컴포넌트	지원되는 플랫폼
	Fedora 30 Ubuntu 18.4 LTS(Bionic Beaver) -19.04(Disco Dingo) Debian 9, 10 CentOS 8 openSUSE 15.1

원격 연결 프로토콜

원격 데스크탑 기능이 원격 연결에 사용하는 프로토콜은 다음과 같습니다.

NEAR

Acronis에서 개발했으며 매우 안전한 프로토콜인 NEAR의 특성은 다음과 같습니다.

- ### H.264

  NEAR에서 구현되는 3개 품질 모드는 **부드럽게**, **균형 조정**, **선명**입니다. **부드럽게** 모드에서 NEAR는 macOS 및 Windows의 하드웨어 H.264 인코딩을 사용하여 바탕 화면을 인코딩하며 하드웨어 인코더를 사용할 수 없으면 소프트웨어 인코더를 대신 사용합니다.바탕 화면 크기는 현재 Full HD 해상도(1920x1080)로만 설정할 수 있습니다.

- ### 적응 코덱

  균형 조정 및 **선명** 품질 모드에서 NEAR는 적응 코덱을 사용합니다. 이 코덱은 H.264에 사용되는 '비디오' 모드보다 훨씬 선명한 최고 수준의 화면 품질(32비트)을 제공합니다.

  균형 조정 모드에서는 현재 네트워크 상태에 따라 화면 품질이 자동 조정되며 현재 프레임 속도가 유지됩니다.

  선명 모드에서도 화면이 최고 품질로 표시되지만 네트워크, 프로세서 또는 비디오 카드 과부하 시에는 프레임 속도가 낮아질 수도 있습니다.

  적응 코덱은 그래픽 드라이버에서 사용 가능한 경우 Windows와 macOS에서 OpenCL을 사용합니다.

- ### 사운드 전송

  NEAR에서는 원격 컴퓨터 사운드를 캡처하여 호스트로 전송할 수 있습니다. Windows, macOS 및 Linux에서 원격 사운드 리디렉션을 활성화하는 방법에 대한 자세한 내용은 "원격 사운드 리디렉션"(901페이지) 항목을 참조하십시오.

- ### 다양한 로그인 옵션

  다음 방법을 사용하여 원격 워크로드에 로그인할 수 있습니다.

© Acronis International GmbH, 2003-2024

액세스 코드: 원격 워크로드에 로그인되어 있는 사용자가 빠른 지원을 실행하여 액세스 코드를 알려 주는 방식입니다. 이 방법을 사용할 때는 항상 현재 로그인되어 있는 사용자의 세션에 연결됩니다.

워크로드 자격 증명: 워크로드에 등록되어 있는 관리자 자격 증명을 사용하여 원격 워크로드에 로그인하는 방식입니다.

관찰 또는 제어 권한 요청: 원격 워크로드에 로그인되어 있는 사용자에게 연결을 허용할지 아니면 거부할지를 확인하라는 메시지가 표시됩니다.

- 보안

  NEAR에서는 데이터가 항상 AES 암호화를 통해 양방향으로 암호화됩니다.

RDP

Microsoft가 개발한 독점 프로토콜인 원격 데스크탑 프로토콜(RDP)에서는 네트워크 연결을 통해 원격 Windows 컴퓨터에 연결할 수 있습니다.

Apple 화면 공유

Apple 화면 공유는 macOS 버전 10.5 이상에 포함되어 있는 Apple의 VNC 클라이언트입니다.

원격 사운드 리디렉션

Connect 클라이언트에서는 NEAR 연결 프로토콜을 통한 오디오 스트리밍이 지원됩니다. NEAR에 대한 자세한 내용은 "원격 연결 프로토콜"(900페이지) 항목을 참조하십시오.

원격 Windows 워크로드에서 사운드 리디렉션

Windows 워크로드의 경우에는 원격 사운드가 자동으로 전송됩니다. 원격 워크로드에 사운드 출력 장치(스피커 또는 헤드폰)가 연결되어 있는지 확인합니다.

원격 macOS 워크로드에서 사운드 리디렉션

macOS 워크로드에서 사운드 리디렉션을 활성화하려면 다음 사항을 확인합니다.

- 워크로드에 보호 에이전트가 설치되어 있습니다.
- 워크로드에 사운드 캡처 드라이버가 설치되어 있습니다.
- 워크로드가 원격 연결에 NEAR 프로토콜을 사용합니다.

참고

macOS 10.15 Catalina의 경우 Connect 에이전트에 마이크 권한을 부여해야 합니다.Connect 에이전트에 마이크 권한을 부여하는 방법에 대한 자세한 내용은 "Connect 에이전트에 필요한 시스템 권한 부여"(77페이지) 항목을 참조하십시오.

에이전트가 사용하는 사운드 캡처 드라이버는 Soundflower 또는 Blackhole입니다.

© Acronis International GmbH, 2003-2024

최신 버전 설치 프로세스는 Blackhole 위키 페이지 https://github.com/ExistentialAudio/BlackHole/wiki/Installation에 설명되어 있습니다.

참고
Connect 클라이언트는 현재 Blackhole의 2채널 버전만 지원합니다.

워크로드에 Homebrew가 설치되어 있으면 다음 명령을 실행하여 Blackhole을 설치할 수도 있습니다.

```
brew install --cask blackhole-2ch
```

참고
원격 macOS 워크로드의 사운드가 리디렉션되는 동안에는 원격 워크로드에 로그인되어 있는 사용자가 사운드를 들을 수 없습니다.

원격 Linux 워크로드에서 사운드 리디렉션

대다수 Linux 배포판에서는 원격 사운드 리디렉션이 자동으로 작동합니다. 원격 사운드 리디렉션이 기본적으로 작동하지 않는 경우 다음 명령을 실행하여 PulseAudio 드라이버를 설치합니다.

```
sudo apt-get install pulseaudio
```

원격 데스크탑 또는 원격 지원을 위한 원격 워크로드로의 연결

원격 데스크탑 및 지원 기능을 사용하면 여러 가지 방식으로 워크로드로의 원격 직접 연결이나 클라우드 연결을 설정할 수 있습니다.

직접 연결은 에이전트가 설치되어 있지 않은 원격 워크로드와 Connect 클라이언트 간에 로컬 영역 네트워크(LAN)에서 TCP/IP를 통해 설정됩니다. 직접 연결 시에는 인터넷에 액세스할 필요가 없습니다.

클라우드 연결은 워크로드의 에이전트나 빠른 지원 및 Connect 클라이언트 간에 Acronis Cloud를 통해 설정됩니다.

다음 표에는 클라우드 연결 옵션에 대한 자세한 내용이 나와 있습니다.

클라우드 연결	클라우드 연결 옵션	보기 모드	지원되는 원격 작업	사용 가능한 운영 체제
NEAR	Connect 클라이언트에서 Connect 에이전트로의 연결 Connect 클라이언트에서 빠른 지원로의 연결	제어 보기 전용	원격 데스크톱 원격 지원	관리 대상 워크로드
RDP	Connect 클라이언트에서 Connect 에이전트로의 연결	제어	원격 데스크톱	관리 대상 워크로드

© Acronis International GmbH, 2003-2024

클라우드 연결	클라우드 연결 옵션	보기 모드	지원되는 원격 작업	사용 가능한 운영 체제
	웹 클라이언트에서 Connect 에이전트로의 연결			
Apple 화면 공유 사용	Connect 클라이언트에서 Connect 에이전트로의 연결	제어 보기 전용 커튼	원격 데스크톱 원격 지원	관리 대상 워크로드

다음 표에는 직접 연결 옵션에 대한 자세한 내용이 나와 있습니다.

직접 연결	직접 연결 옵션	지원되는 원격 작업	사용 가능한 운영 체제
RDP	Connect 클라이언트에서 RDP 서버로의 연결	원격 데스크톱	비관리 대상 워크로드
Apple 화면 공유 사용	Connect 클라이언트에서 Apple 화면 공유 서버로의 연결	원격 데스크톱 원격 지원	비관리 대상 워크로드

원격 관리 계획

원격 관리 계획은 관리 대상 워크로드에서 원격 데스크탑 및 지원 기능을 활성화하고 구성하기 위해 보호 에이전트에 적용하는 계획입니다.

원격 관리 계획이 적용되어 있지 않은 워크로드에서는 원격 작업(다시 시작, 종료, 절전 상태 설정, 휴지통 비우기, 원격 사용자 로그아웃)에만 원격 데스크탑 및 지원 기능을 사용할 수 있습니다.

참고
원격 관리 계획에서 구성할 수 있는 설정의 가용성은 테넌트에 적용된 서비스 팩에 따라 달라집니다. 모든 설정에 액세스하려면 Advanced Management 팩을 활성화합니다. Standard 및 Advanced Management 팩에 포함된 기능에 대한 자세한 내용은 "지원되는 원격 데스크탑 및 지원 기능"(896 페이지) 항목을 참조하십시오.

원격 관리 계획 생성

원격 관리 계획을 생성한 다음 워크로드에 할당하여 관리 대상 워크로드에서 원격 데스크탑 및 지원 기능을 구성할 수 있습니다.

참고
원격 관리 계획의 설정 가용성은 테넌트에 할당된 서비스 할당량에 따라 달라집니다. 표준 기능을 사용 중이라면 RDP를 통한 연결만 구성할 수 있습니다.

© Acronis International GmbH, 2003-2024

사전 요구 사항

사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

원격 관리 계획 생성 방법

원격 관리 계획에서

1. Cyber Protect 콘솔에서 **관리** > **원격 관리 계획**으로 이동합니다.
2. 두 옵션 중 하나를 사용하여 원격 관리 계획을 생성합니다.
   - 목록에 원격 관리 계획이 없으면 **생성**을 클릭합니다.
   - 목록에 원격 관리 계획이 있으면 **계획 생성**을 클릭합니다.
3. [선택 사항] 계획의 기본 이름을 변경하려면 연필 아이콘을 클릭하고 계획의 이름을 입력한 후 **진행**을 클릭합니다.
4. **연결 프로토콜**을 클릭하고 이 원격 관리 계획에서 원격 연결용으로 제공할 프로토콜(NEAR, RDP, Apple 화면 공유)을 활성화합니다.
5. [선택 사항] NEAR 프로토콜의 경우 **보안 설정** 섹션에서 확인란을 선택하거나 취소하여 해당 설정을 활성화하거나 비활성화한 후에 **완료**를 클릭합니다.

설정	설명	사용 가능한 운영 체제
사용자가 콘솔 세션에서 연결을 끊을 때 워크로드 잠금	이 설정을 선택하는 경우 콘솔 세션에서 연결을 끊을 때 원격 워크로드가 잠깁니다.	Windows, macOS
한 번에 한 명의 사용자만 NEAR를 사용하여 연결하거나 파일을 전송하도록 허용	이 설정을 선택하는 경우 워크로드에 활성 원격 연결이 설정되어 있는 동안에는 NEAR 및 파일 전송을 사용하는 연결이 불가능합니다.	Windows, macOS, Linux
워크로드 관리자가 모든 비관리자 사용자 세션에 연결하도록 허용	이 설정을 선택하는 경우 관리자가 워크로드에서 원하는 표준 사용자 세션에 연결할 수 있습니다. **워크로드 관리자가 모든 비관리자 사용자 세션에 연결하도록 허용** 및 **시스템 세션 생성 허용**을 모두 선택 취소하면 원격 macOS 워크로드의 활성 관리자 세션에만 연결할 수 있습니다.	Windows, macOS
시스템 세션 생성 허용	이 설정을 선택하는 경우 원격 연결을 설정할 때 관리자가 기존 활성 세션 중 하나가 아닌 새 세션에서 연결하게	macOS

© Acronis International GmbH, 2003-2024

설정	설명	사용 가능한 운영 체제
	됩니다.	
클립보드 동기화 허용	이 설정을 선택하는 경우 원격 워크로드의 클립보드와 사용자 클립보드 간에 데이터를 전송할 수 있습니다. 예를 들어 원격 워크로드의 파일에서 텍스트를 복사한 다음 사용자 워크로드의 파일에 붙여넣을 수도 있고 사용자 워크로드의 파일에서 텍스트를 복사하여 원격 워크로드의 파일에 붙여넣을 수도 있습니다.	Windows, macOS, Linux

6. **보안 설정**을 클릭하고 확인란을 선택하거나 취소하여 해당 설정을 활성화하거나 비활성화한 후에 **완료**를 클릭합니다.

설정	설명
워크로드가 원격으로 제어되는지 여부 표시	이 설정을 선택하는 경우 워크로드에 대한 활성 원격 데스크탑 연결이 설정되어 있으면 원격 워크로드의 데스크탑에 알림이 표시됩니다.
워크로드 스크린샷 생성을 위한 사용자 권한 요청	이 설정을 선택하는 경우 관리자가 워크로드에서 스크린샷 전송을 요청할 때 원격 워크로드 사용자에게 알림이 표시됩니다.

7. **워크로드 관리**를 클릭한 다음 원격 워크로드에서 사용할 기능을 선택하고 **완료**를 클릭합니다.

설정	설명	사용 가능한 운영 체제
파일 전송	로컬 워크로드와 원격 워크로드 간의 파일 전송을 활성화합니다.	Windows, macOS, Linux
스크린샷 전송	원격 워크로드의 데스크탑 스크린샷을 Cyber Protect 콘솔로 전송하는 기능을 활성화합니다.	Windows, macOS, Linux

8. **표시 설정**을 클릭하고 확인란을 선택하거나 선택을 취소하여 해당 설정을 활성화하거나 비활성화한 후에 **완료**를 클릭합니다.

참고
표시 설정은 NEAR을 통한 연결에서만 제공됩니다.

© Acronis International GmbH, 2003-2024

설정	설명	사용 가능한 운영 체제
데스크탑 캡처를 위해 Desktop Duplication 사용	Desktop Duplication은 Windows의 화면 캡처 방법 중 하나입니다. 일부 환경에서는 이 기능이 불안정할 수도 있습니다. Desktop Duplication을 사용하지 않는 경우에는 기본 방법(BitBit)이 대신 사용됩니다. BitBit는 Desktop Duplication에 비해 속도는 훨씬 느리지만 안정성은 높습니다.	Windows
OpenCL 가속 사용	OpenCL 가속을 켜면 **균형 조정** 품질 모드에 사용되는 적응 코덱의 속도를 높일 수 있습니다. 그래픽 처리 장치(GPU)에서 일부 계산이 실행되기 때문입니다. OpenCL 가속을 켜려면 원격 Linux에 OpenCL 드라이버를 설치해야 합니다. 적응 코덱은 그래픽 드라이버에서 사용 가능한 경우 macOS와 Windows에서 OpenCL을 사용합니다.	Linux
하드웨어 H.264 인코딩 사용	NEAR에서 지원되는 3개 품질 모드는 **부드럽게**, **균형 조정**, **선명**입니다. **부드럽게** 모드에서는 하드웨어 H.264 인코딩을 사용하여 바탕 화면을 인코딩합니다. **균형 조정** 모드에서는 적응 코덱을 사용합니다. 이 코덱은 H.264에 사용되는 '비디오' 모드보다 훨씬 선명한 최고 수준의 화면 품질(32비트)을 제공합니다.현재 네트워크 상태에 따라 화면 품질이 자동 조정되며 현재 프레임 속도가 유지됩니다. **선명** 모드에서는 적응 코덱을 사용합니다. 이 코덱은	Windows, macOS

© Acronis International GmbH, 2003-2024

설정	설명	사용 가능한 운영 체제
	H.264에 사용되는 '비디오' 모드보다 훨씬 선명한 최고 수준의 화면 품질(32비트)을 제공합니다.화면은 항상 최고 품질로 표시되지만 네트워크, 프로세서 또는 비디오 카드 과부하 시에는 초당 프레임 수가 낮아질 수도 있습니다.	

9. 워크로드에 마지막으로 로그인한 사용자 관련 정보를 워크로드 상세정보에 표시하려는 경우 **도구 상자**를 클릭하고 **마지막으로 로그인한 사용자 표시**를 선택한 후에 **완료**를 클릭합니다. 마지막으로 로그인한 사용자에 대한 자세한 내용은 "마지막으로 로그인한 사용자 찾기"(359페이지) 항목을 참조하십시오.
10. [선택 사항] 계획에 워크로드를 추가하려면:
    a. **워크로드 추가**를 클릭합니다.
    b. 워크로드를 선택하고 **추가**를 클릭합니다.
    c. 호환성 문제를 해결하려는 경우 "원격 관리 계획과의 호환성 문제 해결"(914페이지) 항목에 설명되어 있는 절차를 진행합니다.
11. **생성**을 클릭합니다.

모든 장치에서

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 원격 관리 계획을 적용할 워크로드를 클릭합니다.
3. **보호**를 클릭하고 **계획 추가**를 클릭합니다.
4. **계획 생성**을 클릭하고 **원격 관리**를 선택합니다.
5. [선택 사항] 계획의 기본 이름을 변경하려면 연필 아이콘을 클릭하고 계획의 이름을 입력한 후 **진행**을 클릭합니다.
6. **연결 프로토콜**을 클릭하고 이 원격 관리 계획에서 원격 연결용으로 제공할 프로토콜(NEAR, RDP, Apple 화면 공유)을 활성화합니다.
7. [선택 사항] NEAR 프로토콜의 경우 **보안 설정** 섹션에서 확인란을 선택하거나 취소하여 해당 설정을 활성화하거나 비활성화한 후에 **완료**를 클릭합니다.

설정	설명	사용 가능한 운영 체제
사용자가 콘솔 세션에서 연결을 끊을 때 워크로드 잠금	이 설정을 선택하는 경우 콘솔 세션에서 연결을 끊을 때 원격 워크로드가 잠깁니다.	Windows, macOS
한 번에 한 명의 사용자만 NEAR를 사용하여 연결하거나 파일을 전송하도록 허용	이 설정을 선택하는 경우 워크로드에 활성 원격 연결이 설정되어 있는 동안에는	Windows, macOS, Linux

© Acronis International GmbH, 2003-2024

설정	설명	사용 가능한 운영 체제
	NEAR 및 파일 전송을 사용하는 연결이 불가능합니다.	
워크로드 관리자가 모든 비관리자 사용자 세션에 연결하도록 허용	이 설정을 선택하는 경우 관리자가 워크로드에서 원하는 표준 사용자 세션에 연결할 수 있습니다. **워크로드 관리자가 모든 비관리자 사용자 세션에 연결하도록 허용** 및 **시스템 세션 생성 허용**을 모두 선택 취소하면 원격 macOS 워크로드의 활성 관리자 세션에만 연결할 수 있습니다.	Windows, macOS
시스템 세션 생성 허용	이 설정을 선택하는 경우 원격 연결을 설정할 때 관리자가 기존 활성 세션 중 하나가 아닌 새 세션에서 연결하게 됩니다.	macOS
클립보드 동기화 허용	이 설정을 선택하는 경우 원격 워크로드의 클립보드와 사용자 클립보드 간에 데이터를 전송할 수 있습니다. 예를 들어 원격 워크로드의 파일에서 텍스트를 복사한 다음 사용자 워크로드의 파일에 붙여넣을 수도 있고 사용자 워크로드의 파일에서 텍스트를 복사하여 원격 워크로드의 파일에 붙여넣을 수도 있습니다.	Windows, macOS, Linux

8. **보안 설정**을 클릭하고 확인란을 선택하거나 취소하여 해당 설정을 활성화하거나 비활성화한 후에 **완료**를 클릭합니다.

설정	설명
워크로드가 원격으로 제어되는지 여부 표시	이 설정을 선택하는 경우 워크로드에 대한 활성 원격 데스크탑 연결이 설정되어 있으면 원격 워크로드의 데스크탑에 알림이 표시됩니다.
워크로드 스크린샷 생성을 위한 사용자 권한 요청	이 설정을 선택하는 경우 관리자가 워크로드에서 스크린샷 전송을 요청할 때 원격 워크로드 사용자에게 알림이 표시됩니다.

© Acronis International GmbH, 2003-2024

9. **워크로드 관리**를 클릭한 다음 원격 워크로드에서 사용할 기능을 선택하고 **완료**를 클릭합니다.

설정	설명	사용 가능한 운영 체제
파일 전송	로컬 워크로드와 원격 워크로드 간의 파일 전송을 활성화합니다.	Windows, macOS, Linux
스크린샷 전송	원격 워크로드의 데스크탑 스크린샷을 Cyber Protect 콘솔로 전송하는 기능을 활성화합니다.	Windows, macOS, Linux

10. **표시 설정**을 클릭하고 확인란을 선택하거나 선택을 취소하여 해당 설정을 활성화하거나 비활성화한 후에 **완료**를 클릭합니다.

참고
표시 설정은 NEAR을 통한 연결에서만 제공됩니다.

설정	설명	사용 가능한 운영 체제
데스크탑 캡처를 위해 Desktop Duplication 사용	Desktop Duplication은 Windows의 화면 캡처 방법 중 하나입니다. 일부 환경에서는 이 기능이 불안정할 수도 있습니다. Desktop Duplication을 사용하지 않는 경우에는 기본 방법(BitBit)이 대신 사용됩니다. BitBit는 Desktop Duplication에 비해 속도는 훨씬 느리지만 안정성은 높습니다.	Windows
OpenCL 가속 사용	OpenCL 가속을 켜면 **균형 조정** 품질 모드에 사용되는 적응 코덱의 속도를 높일 수 있습니다. 그래픽 처리 장치(GPU)에서 일부 계산이 실행되기 때문입니다. OpenCL 가속을 켜려면 원격 Linux에 OpenCL 드라이버를 설치해야 합니다. 적응 코덱은 그래픽 드라이버에서 사용 가능한 경우 macOS와 Windows에서 OpenCL을 사용합니다.	Linux
하드웨어 H.264 인코딩 사	NEAR에서 지원되는 3개 품	Windows, macOS

© Acronis International GmbH, 2003-2024

설정	설명	사용 가능한 운영 체제
용	질 모드는 다음과 같습니다. **부드럽게**, **균형 조정**, **선명**입니다. **부드럽게** 모드에서는 하드웨어 H.264 인코딩을 사용하여 바탕 화면을 인코딩합니다. **균형 조정** 모드에서는 적응 코덱을 사용합니다. 이 코덱은 H.264에 사용되는 '비디오' 모드보다 훨씬 선명한 최고 수준의 화면 품질(32비트)을 제공합니다.현재 네트워크 상태에 따라 화면 품질이 자동 조정되며 현재 프레임 속도가 유지됩니다. **선명** 모드에서는 적응 코덱을 사용합니다. 이 코덱은 H.264에 사용되는 '비디오' 모드보다 훨씬 선명한 최고 수준의 화면 품질(32비트)을 제공합니다.화면은 항상 최고 품질로 표시되지만 네트워크, 프로세서 또는 비디오 카드 과부하 시에는 초당 프레임 수가 낮아질 수도 있습니다.	

11. 워크로드에 마지막으로 로그인한 사용자 관련 정보를 워크로드 상세정보에 표시하려는 경우 **도구 상자**를 클릭하고 **마지막으로 로그인한 사용자 표시**를 선택한 후에 **완료**를 클릭합니다. 마지막으로 로그인한 사용자에 대한 자세한 내용은 "마지막으로 로그인한 사용자 찾기"(359페이지) 항목을 참조하십시오.
12. **생성**을 클릭합니다.

원격 관리 계획에 워크로드 추가

필요에 따라 원격 관리 계획을 생성한 후 해당 계획에 워크로드를 추가할 수 있습니다.

사전 요구 사항

사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

원격 관리 계획에 워크로드를 추가하는 방법

원격 관리 계획에서

© Acronis International GmbH, 2003-2024

1. Cyber Protect 콘솔에서 **관리** > **원격 관리 계획**으로 이동합니다.
2. 원격 관리 계획을 클릭합니다.
3. 워크로드에 계획을 이미 적용했는지 여부에 따라 다음을 수행합니다.
   - 워크로드에 계획을 아직 적용하지 않았다면 **워크로드 추가**를 클릭합니다.
   - 워크로드에 계획을 적용했다면 **워크로드 관리**를 클릭합니다.
4. 목록에서 워크로드를 선택하고 **추가**를 클릭합니다.
5. **저장**을 클릭합니다.
6. **확인**을 클릭하여 워크로드에 필요한 서비스 할당량을 적용합니다.

모든 장치에서

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 원격 관리 계획을 적용할 워크로드를 클릭합니다.
3. **보호**를 클릭하고 **계획 추가**를 클릭합니다.
4. **아래 목록에서 계획 선택**에서 **원격 관리**를 선택하여 원격 관리 계획만 표시합니다.
5. **적용**을 클릭합니다.
6. **확인**을 클릭하여 워크로드에 필요한 서비스 할당량을 적용합니다.

원격 관리 계획에서 워크로드 제거

필요에 따라 원격 관리 계획에서 워크로드를 제거할 수 있습니다.

사전 요구 사항

사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

원격 관리 계획에서 워크로드를 제거하는 방법

1. Cyber Protect 콘솔에서 **관리** > **원격 관리 계획**으로 이동합니다.
2. 원격 관리 계획을 클릭합니다.
3. **워크로드 관리**를 클릭합니다.
4. 원격 관리 계획에서 제거할 워크로드를 하나 이상 선택하고 **제거**를 클릭합니다.
5. **완료**를 클릭합니다.
6. **저장**을 클릭합니다.

기존 원격 관리 계획을 사용하여 추가 작업 수행

원격 관리 계획 화면에서는 원격 관리 계획과 관련하여 세부 정보 보기, 편집, 활동 보기, 경보 보기, 이름 변경, 활성화, 비활성화, 복제, 내보내기 및 삭제와 같은 추가 작업을 수행할 수 있습니다.

상세 정보 보기

사전 요구 사항

사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

원격 관리 계획의 상세 정보 확인 방법

© Acronis International GmbH, 2003-2024

1. **원격 관리 계획** 화면에서 원격 관리 계획의 **추가 작업** 아이콘을 클릭합니다.
2. **상세 정보 보기**를 클릭합니다.

편집

사전 요구 사항

사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

계획을 편집하려면

1. **원격 관리 계획** 화면에서 원격 관리 계획의 **추가 작업** 아이콘을 클릭합니다.
2. **편집**을 클릭합니다.

작업

원격 관리 계획 관련 작업 확인 방법

1. **원격 관리 계획** 화면에서 원격 관리 계획의 **추가 작업** 아이콘을 클릭합니다.
2. **작업**을 클릭합니다.
3. 활동을 클릭하면 해당 활동 관련 추가 상세 정보를 확인할 수 있습니다.

경보

경보를 확인하려면

1. **원격 관리 계획** 화면에서 원격 관리 계획의 **추가 작업** 아이콘을 클릭합니다.
2. **경보**를 클릭합니다.

이름 변경

사전 요구 사항

사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

원격 관리 계획 이름 변경 방법

1. **원격 관리 계획** 화면에서 원격 관리 계획의 **추가 작업** 아이콘을 클릭합니다.
2. **이름 변경**을 클릭합니다.
3. 계획의 새 이름을 입력하고 **진행**을 클릭합니다.

활성화

사전 요구 사항

사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

원격 관리 계획 활성화 방법

1. **원격 관리 계획** 화면에서 원격 관리 계획의 **추가 작업** 아이콘을 클릭합니다.
2. **활성화**를 클릭합니다.

비활성화

© Acronis International GmbH, 2003-2024

사전 요구 사항

사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

원격 관리 계획 비활성화 방법

1. **원격 관리 계획** 화면에서 원격 관리 계획의 **추가 작업** 아이콘을 클릭합니다.
2. **비활성화**를 클릭합니다.

복제

사전 요구 사항

사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

원격 관리 계획을 복제하는 방법

1. **원격 관리 계획** 화면에서 원격 관리 계획의 **추가 작업** 아이콘을 클릭합니다.
2. **복제**를 클릭합니다.
3. **생성**을 클릭합니다.

내보내기

사전 요구 사항

사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

원격 관리 계획을 내보내는 방법

1. **원격 관리 계획** 화면에서 원격 관리 계획의 **추가 작업** 아이콘을 클릭합니다.
2. **내보내기**를 클릭합니다.
   계획 구성은 JSON 형식으로 로컬 머신에 내보내집니다.

삭제

사전 요구 사항

사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

원격 관리 계획 삭제 방법

1. **원격 관리 계획** 화면에서 원격 관리 계획의 **추가 작업** 아이콘을 클릭합니다.
2. **삭제**를 클릭합니다.
3. **확인**을 선택하고 **삭제**를 클릭합니다.

원격 관리 계획과의 호환성 문제

워크로드에 원격 관리 계획 계획을 적용하면 호환성 문제가 발생하는 경우도 있습니다. 다음과 같은 호환성 문제가 발생할 수 있습니다.

© Acronis International GmbH, 2003-2024

- 충돌하는 계획 - 워크로드에 다른 원격 관리 계획이 이미 적용되어 있으면 이 문제가 표시됩니다. 각 워크로드에는 원격 관리 계획을 하나만 적용할 수 있습니다.
- 호환되지 않는 운영 체제 - 워크로드의 운영 체제가 지원되지 않으면 이 문제가 표시됩니다.
- 지원되지 않는 에이전트 - 워크로드의 보호 에이전트 버전이 오래되어 원격 데스크탑 기능을 지원하지 않으면 이 문제가 표시됩니다.
- 부족한 할당량 - 테넌트의 서비스 할당량이 선택한 워크로드에 할당하기에 충분하지 않으면 이 문제가 표시됩니다.

원격 관리 계획을 개별적으로 선택된 워크로드(최대 150개)에 적용하면 계획을 저장하기 전에 기존 충돌을 해결하라는 메시지가 표시됩니다. 충돌을 해결하려면 충돌의 근본 원인을 제거하거나 영향을 받는 워크로드를 계획에서 제거합니다. 자세한 내용은 "원격 관리 계획과의 호환성 문제 해결"(914페이지)을(를) 참조하십시오. 충돌을 해결하지 않고 계획을 저장하면 호환되지 않는 워크로드에 대해 계획이 자동으로 비활성화되고 경보가 표시됩니다.

원격 관리 계획을 150개가 넘는 워크로드 또는 장치 그룹에 적용하면 계획이 저장된 후 호환성이 검사됩니다. 호환되지 않는 워크로드에 대해서는 계획이 자동으로 비활성화되고 경보가 표시됩니다.

원격 관리 계획과의 호환성 문제 해결

호환성 문제의 원인에 따라 각기 다른 작업을 수행하여 새 원격 관리 계획 생성 프로세스의 일부분으로 호환성 문제를 해결할 수 있습니다.

참고
계획에서 워크로드를 제거하여 호환성 문제를 해결할 때 장치 그룹에 포함된 워크로드는 제거할 수 없습니다.

호환성 문제를 해결하려면

1. **문제 검토**를 클릭합니다.
2. [새 계획에서 워크로드를 제거하여 기존 원격 관리 계획의 호환성 문제를 해결하려면]
   a. **충돌하는 계획** 탭에서 제거할 워크로드를 선택합니다.
   b. **계획에서 워크로드 제거**를 클릭합니다.
   c. **제거**를 클릭한 다음 **닫기**를 클릭합니다.
3. [워크로드에 이미 적용되어 있는 원격 관리 계획을 비활성화하여 해당 계획의 호환성 문제를 해결하려면]
   a. **적용된 계획 비활성화**를 클릭합니다.
   b. **비활성화**를 클릭한 다음 **닫기**를 클릭합니다.
4. [호환되지 않는 운영 체제의 호환성 문제를 해결하려면]
   a. **호환되지 않는 운영 체제** 탭에서 제거할 워크로드를 선택합니다.
   b. **계획에서 워크로드 제거**를 클릭합니다.
   c. **제거**를 클릭한 다음 **닫기**를 클릭합니다.
5. [계획에서 워크로드를 제거하여 지원되지 않는 에이전트의 호환성 문제를 해결하려면]

© Acronis International GmbH, 2003-2024

a. **지원되지 않는 에이전트** 탭에서 제거할 워크로드를 선택합니다.
b. **계획에서 워크로드 제거**를 클릭합니다.
c. **제거**를 클릭한 다음 **닫기**를 클릭합니다.

6. [에이전트 버전을 업데이트하여 지원되지 않는 에이전트의 호환성 문제를 해결하려면] **에이전트 목록으로 이동**을 클릭합니다.

참고
이 옵션은 고객 관리자만 사용할 수 있습니다.

7. [계획에서 워크로드를 제거하여 부족한 할당량으로 인한 호환성 문제를 해결하려면]
a. **부족한 할당량** 탭에서 제거할 워크로드를 선택합니다.
b. **계획에서 워크로드 제거**를 클릭합니다.
c. **제거**를 클릭한 다음 **닫기**를 클릭합니다.

8. [테넌트의 할당량을 늘려 부족한 할당량으로 인한 호환성 문제를 해결하려면]

참고
이 옵션은 파트너 관리자만 사용할 수 있습니다.

a. **부족한 할당량** 탭에서 **관리 포털로 이동**을 클릭합니다.
b. 고객의 서비스 할당량을 늘립니다.

워크로드 자격 증명

원격 워크로드의 관리자 또는 관리자가 아닌 사용자 자격 증명(사용자 이름과 암호 또는 VNC 암호)을 추가하고 클라우드 자격 증명 저장소에 저장한 다음 관리 대상 워크로드에 연결할 때 자동 인증용으로 사용할 수 있습니다. 이렇게 하면 연결의 인증 단계에서 매번 자격 증명을 수동으로 입력하는 대신 자격 증명 저장소에 이러한 자격 증명을 한 번 저장한 후 여러 워크로드에 할당할 수 있습니다. 그러면 해당 워크로드에 원격으로 연결할 때마다 Connect 클라이언트에서 이러한 자격 증명을 사용합니다.

참고
자격 증명 저장소에 저장한 자격 증명은 여러 테넌트 수준 간에 공유되지 않습니다. 즉, 같은 고객 테넌트나 파트너 테넌트의 동일 테넌트 수준에서만 공유됩니다.

그러므로 한 고객 테넌트에 관리자가 여러 명인 경우 관리자들이 자격 증명 저장소의 자격 증명을 확인 및 공유할 수 있습니다. 반면 다른 파트너 관리자나 다른 테넌트의 고객 관리자는 이러한 자격 증명을 확인하거나 사용할 수 없습니다.

자격 증명 추가

자격 증명을 추가한 후 여러 워크로드로의 원격 연결에 사용할 수 있습니다.

자격 증명을 워크로드에 추가한 후 자격 증명 저장소에 저장하려면

© Acronis International GmbH, 2003-2024

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 자격 증명을 추가할 워크로드를 클릭합니다.
3. 다음 방법 중 하나로 **설정** 메뉴에 액세스합니다.
   - **원격 데스크톱**을 클릭한 다음 **설정**을 클릭합니다.
   - **관리**를 클릭한 다음 **설정**을 클릭합니다.
4. **자격 증명 추가**를 클릭합니다.
5. **자격 증명 저장소**에서 **자격 증명 추가**를 클릭합니다.
6. 자격 증명을 입력합니다.

필드	설명
자격 증명 이름	자격 증명 저장소에 표시되는 자격 증명의 식별자입니다.
사용자 이름	대상 워크로드로의 원격 연결에 사용할 사용자 이름입니다.
암호	대상 워크로드로의 원격 연결에 사용할 암호입니다.
VNC 암호	이 필드는 Apple 화면 공유에서만 사용 가능합니다.

7. **저장**을 클릭합니다.

워크로드에 자격 증명 할당

자격 증명을 추가한 후에는 관리 대상 워크로드에 연결할 때 해당 자격 증명을 사용하여 자동으로 인증을 할 수 있습니다.

워크로드에 자동으로 인증할 수 있도록 저장된 자격 증명을 할당하려면

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 다음 방법 중 하나로 **설정** 메뉴에 액세스합니다.
   - **원격 데스크톱**을 클릭한 다음 **설정**을 클릭합니다.
   - **관리**를 클릭한 다음 **설정**을 클릭합니다.
3. 지원되는 프로토콜의 탭(NEAR, RDP, Apple 화면 공유)에서 **자격 증명 추가**를 클릭합니다.
4. **자격 증명 저장소**의 목록에서 자격 증명을 선택한 다음 **자격 증명 선택**을 클릭합니다.

자격 증명 삭제

더 이상 필요하지 않은 자격 증명은 삭제할 수 있습니다.

자격 증명 저장소에서 자격 증명을 삭제하려면

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 다음 방법 중 하나로 **설정** 메뉴에 액세스합니다.
   - **원격 데스크톱**을 클릭한 다음 **설정**을 클릭합니다.
   - **관리**를 클릭한 다음 **설정**을 클릭합니다.
3. 지원되는 프로토콜의 탭(NEAR, RDP, Apple 화면 공유)에서 **삭제**를 클릭합니다.
4. 확인 창에서 **삭제**를 클릭합니다.

© Acronis International GmbH, 2003-2024

워크로드에서 자격 증명 할당 해제

워크로드에서 자격 증명 할당을 해제하되 자격 증명 저장소에는 자격 증명을 계속 보관할 수 있습니다.

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 다음 방법 중 하나로 **설정** 메뉴에 액세스합니다.
   - **원격 데스크톱**을 클릭한 다음 **설정**을 클릭합니다.
   - **관리**를 클릭한 다음 **설정**을 클릭합니다.
3. 지원되는 프로토콜의 탭(NEAR, RDP, Apple 화면 공유)에서 **할당 해제**를 클릭합니다.
4. 확인 창에서 **할당 해제**를 클릭합니다.

관리 대상 워크로드 사용

관리 대상 워크로드는 보호 에이전트가 설치된 워크로드입니다.

원격 관리 대상 워크로드에서는 다음 작업을 수행할 수 있습니다.

- 제어 또는 보기 전용 모드로 NEAR를 사용하여 원격 지원 또는 원격 데스크탑용으로 연결
- 제어 모드로 RDP를 사용하여 원격 데스크탑용으로 연결
- 제어, 보기 전용 또는 커튼 모드로 Apple 화면 공유를 사용하여 원격 지원 또는 원격 데스크탑용으로 연결
- 웹 클라이언트를 통해 원격 데스크탑용으로 연결
- 원격 워크로드에서 다시 시작, 종료, 절전 모드 설정, 휴지통 비우기, 원격 사용자 로그아웃 처리
- 사용자 워크로드와 원격 워크로드 간에 파일 전송
- 스크린샷을 생성하여 워크로드 모니터링

참고
관리 대상 워크로드로의 원격 데스크탑 연결을 설정하려면 보호 에이전트를 설치해야 하며 워크로드에 원격 관리 계획을 적용해야 합니다.

RDP 설정 구성

관리 대상 워크로드에 대한 원격 제어 RDP 연결에 자동 적용할 설정을 구성할 수 있습니다.

워크로드의 RDP 설정을 구성하려면

1. Cyber Protect 콘솔에서 **장치** > **에이전트가 있는 머신**으로 이동합니다.
2. 다음 방법 중 하나로 **설정** 메뉴에 액세스합니다.
   - **원격 데스크톱**을 클릭한 다음 **설정**을 클릭합니다.
   - **관리**를 클릭한 다음 **설정**을 클릭합니다.

© Acronis International GmbH, 2003-2024

3. **RDP** 탭에서 설정을 구성합니다.

설정	설명
오디오 재생	이 설정을 선택하거나 선택을 취소하면 로컬 워크로드에서 원격 워크로드 사운드 리디렉션이 활성화되거나 비활성화됩니다.
오디오 녹음	이 설정의 선택 여부에 따라 마이크에 말을 하여 녹음한 오디오가 원격 워크로드로 전송되는지 여부가 결정됩니다.
프린터 리디렉션	이 설정을 선택하는 경우 원격 워크로드에서 워크로드의 프린터를 사용할 수 있습니다.
파일 리디렉션	이 설정의 선택 여부에 따라 로컬 워크로드의 파일이 원격 워크로드와 공유되는지 여부가 정의됩니다.
색 농도	이 설정에 따라 RDP가 전송할 그림의 색상 수가 결정됩니다. 값이 클수록 대역폭이 더 많이 필요합니다. **하이 컬러**: 16비트 **트루 컬러**: • 24비트(웹 클라이언트를 통한 RDP 연결) • 32비트(Connect 클라이언트를 통한 RDP 연결)

4. 닫기 버튼을 클릭합니다.

원격 데스크탑 또는 원격 지원을 위해 관리 대상 워크로드에 연결

참고
원격 연결에 사용할 수 있는 연결 프로토콜의 가용성은 원격 관리 계획 구성과 원격 워크로드의 운영 체제에 따라 다릅니다.

사전 요구 사항

- 해당하는 연결 프로토콜이 활성화된 원격 관리 계획이 관리 대상 워크로드에 적용되어 있어야 합니다.
- 필요한 서비스 할당량이 워크로드에 할당되어 있어야 합니다. (워크로드에 원격 관리 계획을 적용하면 서비스 할당량이 자동으로 적용됩니다.)
- [Apple 화면 공유 연결의 경우] macOS 워크로드에서 Apple 화면 공유가 활성화되어 있어야 합니다.
- Acronis Cyber Protect Cloud에서 사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

원격 데스크탑 또는 원격 지원을 위해 관리 대상 워크로드에 원격으로 연결하려면

1. Cyber Protect 콘솔에서 **장치** > **에이전트가 있는 머신**으로 이동합니다.
2. 연결할 워크로드를 클릭합니다.
3. **원격 데스크톱**을 클릭합니다.
   기본적으로 NEAR는 연결 프로토콜로 선택됩니다.
4. [선택 사항] **연결 프로토콜** 드롭다운 목록에서 사용하려는 연결 프로토콜을 선택합니다.

© Acronis International GmbH, 2003-2024

5. 사용하려는 보기 모드를 클릭합니다.

프로토콜	원격 연결 대상	보기 모드	지원되는 원격 작업
NEAR	Windows Linux macOS	**제어** - 이 모드에서는 원격 워크로드를 관찰하고 해당 워크로드에서 작업을 수행할 수 있습니다. **보기 전용** - 이 모드에서는 원격 워크로드를 관찰만 할 수 있습니다.	원격 데스크톱 원격 지원
RDP	Windows	**제어** - 이 모드에서는 원격 워크로드를 확인하고 해당 워크로드에서 작업을 수행할 수 있습니다. **참고** 워크로드의 OS 설정에서 RDP가 비활성화되어 있으면 팝업 창이 나타납니다. 이 창을 통해 현재 세션 또는 일반 설정에서 워크로드에 대해 RDP를 활성화합니다. • 현재 세션에서만 이 워크로드에 대해 RDP를 활성화하려면 **세션이 끝나면 비활성화합니다**를 선택하고 **허용**을 클릭합니다. • 이 워크로드에 대해 RDP를 활성화하려면 **허용**을 클릭합니다.	원격 데스크톱
Apple 화면 공유	macOS	**제어** - 이 모드에서는 원격 워크로드를 관찰하고 해당 워크로드에서 작업을 수행할 수 있습니다. **보기 전용** - 이 모드에서는 원격 워크로드를 관찰만 할 수 있습니다. **커튼** - macOS 워크로드에만 사용 가능합니다. 커튼 모드에서 원격 워크로드에 연결하는 경우에는 원격 워크로드가 흐리게 표시되며, 워크로드에서 수행하는 작업을 원격 사용자가 확인할 수 없습니다.	원격 데스크톱 원격 지원

6. 워크로드에 Connect 클라이언트가 설치되어 있는지 여부에 따라 다음 중 하나를 수행합니다.
   - Connect 클라이언트가 설치되어 있지 않은 경우 다운로드하여 설치한 후 확인 팝업이 표시되면 **허용**을 선택합니다.
   - Connect 클라이언트가 이미 설치되어 있는 경우 확인 팝업이 표시되면 **Connect 클라이언트 열기**를 클릭합니다.
7. **인증** 창에서 인증 옵션을 선택하고 필요한 자격 증명을 입력합니다.

참고
워크로드에 자격 증명을 할당했다면 인증이 자동 진행되며 이 단계를 건너뛰게 됩니다. 자세한 내용은 "워크로드에 자격 증명 할당"(916페이지)을(를) 참조하십시오.

© Acronis International GmbH, 2003-2024

인증 옵션	설명
원격 워크로드 자격 증명 사용	원격 워크로드 관리 사용자의 사용자 이름과 암호를 입력하면 원격 연결을 설정할 수 있습니다. 이 옵션은 NEAR, RDP 및 Apple 화면 공유에 사용할 수 있습니다. 이 옵션을 사용하여 원격 데스크탑과 원격 지원을 위한 인증을 진행할 수 있습니다.
관찰 권한 요청	원격 워크로드에 로그인되어 있는 사용자가 허용을 하면 원격 연결을 관찰 모드로 설정할 수 있습니다. 이 옵션은 NEAR 및 Apple 화면 공유에 사용할 수 있습니다. 이 옵션을 사용하여 원격 지원을 위한 인증을 진행할 수 있습니다.
제어 권한 요청	원격 워크로드에 로그인되어 있는 사용자가 허용을 하면 원격 연결을 제어 모드로 설정할 수 있습니다. 이 옵션은 NEAR 및 Apple 화면 공유에 사용할 수 있습니다. 이 옵션을 사용하여 원격 지원을 위한 인증을 진행할 수 있습니다.

8. **연결**을 클릭하고 표시할 세션을 클릭합니다(워크로드에서 여러 사용자 세션을 사용할 수 있는 경우).

   Connect 클라이언트에서 새 뷰어 창이 열립니다. 이 창에서 원격 워크로드의 데스크탑을 확인할 수 있습니다. 원격 연결이 설정되고 나면 뷰어의 도구 모음에서 원격 워크로드에 대해 추가 작업을 수행할 수 있습니다. 자세한 내용은 "뷰어 창에서 도구 모음 사용"(927페이지)을(를) 참조하십시오.

웹 클라이언트를 통해 관리 대상 워크로드에 연결

웹 클라이언트를 통해 관리 대상 워크로드로의 원격 데스크탑 연결을 설정할 수 있습니다.

사전 요구 사항

- 표준 서비스 할당량이 워크로드에 할당되어 있어야 합니다.
- RDP가 활성화된 원격 관리 계획이 관리 대상 워크로드에 적용되어 있어야 합니다.
- 관리 대상 워크로드에서 RDP가 활성화되어 있어야 합니다.
- 브라우저가 HTML5를 지원해야 합니다.
- Acronis Cyber Protect Cloud에서 사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

웹 클라이언트를 통해 워크로드에 원격으로 연결하려면

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 원격으로 연결하려는 워크로드를 클릭한 다음 **원격 데스크탑**>**웹 클라이언트를 통해 연결**을 클릭합니다.
3. 워크로드에 액세스하는 데 사용할 로그인 및 암호를 입력하고 **연결**을 클릭합니다.

참고

워크로드에 자격 증명을 할당했다면 인증이 자동 진행되며 이 단계를 건너뛰게 됩니다. 자세한 내용은 "워크로드에 자격 증명 할당"(916페이지)을(를) 참조하십시오.

© Acronis International GmbH, 2003-2024

파일 전송

로컬 워크로드와 관리 대상 워크로드 간에 파일을 쉽게 전송할 수 있습니다.

사전 요구 사항

- NEAR 프로토콜과 파일 전송이 활성화된 원격 관리 계획이 워크로드에 적용되어 있어야 합니다.
- 워크로드에 Advanced Management 할당량이 적용되어 있어야 합니다.
- Acronis Cyber Protect Cloud에서 사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

사용자 워크로드와 관리 대상 워크로드 간에 파일을 원격으로 전송하려면

1. Cyber Protect 콘솔에서 **장치** > **에이전트가 있는 머신**으로 이동합니다.
2. 파일을 전송할 워크로드를 클릭합니다.
3. **관리**를 클릭한 다음 **파일 전송**을 클릭합니다.
4. 워크로드에 Connect 클라이언트가 설치되어 있는지 여부에 따라 다음 중 하나를 수행합니다.
   - Connect 클라이언트가 설치되어 있지 않은 경우 다운로드하여 설치한 후 확인 팝업이 표시되면 **허용**을 클릭합니다.
   - Connect 클라이언트가 이미 설치되어 있는 경우 확인 팝업이 표시되면 **Connect 클라이언트 열기**를 클릭합니다.
5. **인증** 창에서 인증 옵션을 선택하고 필요한 자격 증명을 입력합니다.

인증 옵션	설명
원격 워크로드 자격 증명 사용	원격 워크로드 관리 사용자의 사용자 이름과 암호를 입력하면 원격 연결을 설정할 수 있습니다.
파일 전송 권한 요청	원격 워크로드에 로그인되어 있는 사용자가 허용을 하면 파일을 전송할 수 있습니다.

6. **파일 전송** 창에서 파일을 찾은 다음 끌어서 원하는 대상에 놓습니다.

   참고
   로컬 워크로드의 파일은 왼쪽 창에, 원격 워크로드의 파일은 오른쪽 창에 나열됩니다.
   시작된 파일 전송은 **작업** 창에 표시됩니다.

7. [선택 사항] **작업** 창에서 완료된 작업을 제거하려면 **완료된 작업 지우기**를 클릭합니다.
8. 모든 전송이 완료되면 창을 닫습니다.

관리 대상 워크로드에서 제어 작업 수행

원격 워크로드에서 휴지통 비우기, 절전 모드 설정, 다시 시작, 종료, 원격 사용자 로그아웃 처리 등의 기본적인 제어 작업을 수행하여 해당 워크로드를 관리할 수 있습니다.

© Acronis International GmbH, 2003-2024

사전 요구 사항

- 표준 서비스 할당량이 워크로드에 적용되어 있어야 합니다.
- Acronis Cyber Protect Cloud에서 사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

휴지통 비우기

원격 워크로드에서 휴지통을 비우려면

1. Cyber Protect 콘솔에서 **장치** > **에이전트가 있는 머신**으로 이동합니다.
2. 이 작업을 수행할 워크로드를 클릭합니다.
3. **관리**를 클릭하고 **휴지통 비우기**을 클릭합니다.
4. 이 작업을 수행할 사용자 세션을 선택하고 **휴지통 비우기**를 클릭합니다.

절전 모드

원격 워크로드를 절전 모드로 설정하려면

1. Cyber Protect 콘솔에서 **장치** > **에이전트가 있는 머신**으로 이동합니다.
2. 이 작업을 수행할 워크로드를 클릭합니다.
3. **관리**를 클릭하고 **절전 모드**를 클릭합니다.

다시 시작

원격 워크로드를 다시 시작하려면

1. Cyber Protect 콘솔에서 **장치** > **에이전트가 있는 머신**으로 이동합니다.
2. 이 작업을 수행할 워크로드를 클릭합니다.
3. **관리**를 클릭하고 **다시 시작**을 클릭합니다.
   - Windows 워크로드의 경우 워크로드를 다시 시작하기 전에 현재 워크로드에 로컬로 로그인되어 있는 사용자가 변경 사항을 저장하도록 허용할지 여부를 선택하고 사용자를 선택한 후에 **다시 시작**을 다시 클릭합니다.
   - macOS 워크로드의 경우 워크로드를 다시 시작하기 전에 현재 워크로드에 로컬로 로그인되어 있는 사용자가 변경 사항을 저장하도록 허용할지 여부를 선택하고 **다시 시작**을 다시 클릭합니다.
   - Linux 워크로드의 경우에는 **다시 시작**을 클릭합니다.

종료

원격 워크로드를 종료하려면

1. Cyber Protect 콘솔에서 **장치** > **에이전트가 있는 머신**으로 이동합니다.
2. 이 작업을 수행할 워크로드를 클릭합니다.
3. **관리**를 클릭하고 **종료**를 클릭합니다.
   - Windows 워크로드의 경우 워크로드를 종료하기 전에 현재 워크로드에 로컬로 로그인되어 있는 사용자가 변경 사항을 저장하도록 허용할지 여부를 선택하고 사용자를 선택한 후에 **종료**를 다시 클릭합니다.

© Acronis International GmbH, 2003-2024

- macOS 워크로드의 경우 워크로드를 종료하기 전에 현재 워크로드에 로컬로 로그인되어 있는 사용자가 변경 사항을 저장하도록 허용할지 여부를 선택하고 **종료**를 다시 클릭합니다.
- Linux 워크로드의 경우에는 **종료**를 클릭합니다.

원격 사용자 로그아웃

원격 워크로드의 사용자를 로그아웃 처리하려면

1. Cyber Protect 콘솔에서 **장치** > **에이전트가 있는 머신**으로 이동합니다.
2. 이 작업을 수행할 워크로드를 클릭합니다.
3. **관리**를 클릭하고 **원격 사용자 로그아웃**을 클릭합니다.
4. 로그아웃 처리할 사용자를 선택하고 **로그아웃**을 클릭합니다.

스크린샷 전송을 통해 워크로드 모니터링

스크린샷 전송 기능을 사용하여 워크로드의 상태를 모니터링할 수 있습니다.

사전 요구 사항

- 스크린샷 전송 기능이 활성화된 원격 관리 계획이 워크로드에 적용되어 있어야 합니다.
- 보호 에이전트가 최신 버전이며 스크린샷 전송 기능을 지원해야 합니다.
- 워크로드에 Advanced Management 서비스 할당량이 적용되어 있어야 합니다.
- 워크로드가 온라인이어야 합니다.
- Acronis Cyber Protect Cloud에서 사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

스크린샷 전송을 통해 워크로드 모니터링

스크린샷 전송을 통해 워크로드를 모니터링하려면

1. Cyber Protect 콘솔에서 **장치**>**스크린샷 전송**으로 이동합니다.
2. 모니터링할 워크로드를 클릭합니다.
3. 사용자 세션을 선택합니다.
4. 디스플레이를 선택합니다.
5. 데스크탑의 새 스크린샷을 생성할 새로 고침 속도를 선택합니다.
6. 이미지 품질을 선택합니다.
7. 스크린샷을 다운로드하려면 다운로드 아이콘을 클릭합니다.

워크로드의 스크린샷 생성

관리 대상 워크로드의 스크린샷을 생성하려면

1. Cyber Protect 콘솔에서 **장치** > **에이전트가 있는 머신**으로 이동합니다.
2. 스크린샷을 생성하려는 워크로드를 클릭합니다.
3. **관리**를 클릭하고 **데스크탑 스크린샷 생성**을 클릭합니다.
   워크로드가 사전 선택되어 있는 **스크린샷 전송** 화면이 열립니다. 워크로드에 적용된 원격 관리 계획의 설정에 따라 스크린샷이 바로 표시될 수도 있고, 원격 워크로드의 사용자가 요청을 승인해야 스크린샷이 표시될 수도 있습니다.

© Acronis International GmbH, 2003-2024

동시에 여러 관리 대상 워크로드 관찰

창 하나에서 여러 원격 워크로드의 데스크탑을 동시에 관찰할 수 있습니다.

참고
창에서 동시에 확인할 수 있는 데스크탑의 수는 모니터 크기에 따라 달라집니다.

사전 요구 사항

- 워크로드에 적용된 원격 관리 계획에서 NEAR/Apple 화면 공유가 활성화되어 있어야 합니다.
- 워크로드에 Advanced Management 서비스 할당량이 적용되어 있어야 합니다.
- Acronis Cyber Protect Cloud에서 사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

여러 워크로드를 동시에 관찰하려면

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 관찰하려는 워크로드를 선택합니다.
3. **다중 보기**를 클릭합니다.
4. 워크로드에 Connect 클라이언트가 설치되어 있는지 여부에 따라 다음 중 하나를 수행합니다.
   - Connect 클라이언트가 설치되어 있지 않은 경우 다운로드하여 설치한 후 확인 팝업이 표시되면 **허용**을 선택합니다.
   - Connect 클라이언트가 이미 설치되어 있는 경우 확인 팝업이 표시되면 **Connect 클라이언트 열기**를 클릭합니다.
5. **인증** 창에서 인증 옵션을 선택하고 필요한 자격 증명을 입력합니다.

인증 옵션	설명
원격 워크로드 자격 증명 사용	원격 워크로드의 관리자 사용자 이름과 암호를 입력하고 나면 원격 연결을 설정할 수 있습니다.
관찰 권한 요청	원격 워크로드에 로그인되어 있는 사용자가 허용을 하면 원격 연결을 관찰 모드로 설정할 수 있습니다.

6. 2단계에서 선택한 모든 원격 워크로드에 연결할 때 같은 인증 방법과 자격 증명을 사용하려는 경우 **다른 컴퓨터에서 사용**을 선택합니다.
7. **연결**을 클릭합니다.

   다중 보기 창의 도구 모음에서 워크로드에 연결하려는 보기 모드를 선택할 수 있습니다. 이 작업을 수행하면 해당 워크로드용으로 별도의 뷰어 창이 열립니다.

   참고
   선택한 워크로드 중에서 오프라인 상태이거나 오래된 에이전트 버전이 설치된 워크로드는 다중 보기 창에 표시되지 않습니다.
   원격 워크로드에 대한 모든 다중 보기 연결은 **보기 전용** 모드로 설정됩니다.

© Acronis International GmbH, 2003-2024

비관리 대상 워크로드 사용

비관리 대상 워크로드는 보호 에이전트가 설치되지 않은 워크로드입니다.

비관리 대상 원격 워크로드에서는 다음 작업을 수행할 수 있습니다.

- Acronis 빠른 지원을 사용하여 원격 지원용으로 연결
- IP 주소를 사용하여 원격 데스크탑 또는 원격 지원용으로 연결
- 빠른 지원을 사용하여 사용자 워크로드와 원격 워크로드 간에 파일 전송

참고
빠른 지원을 사용하여 비관리 대상 워크로드에 원격으로 연결. 이 경우 다음 사항을 확인해야 합니다.

- 고객 테넌트에 대해 Advanced Management 팩이 활성화되어 있습니다.
- 연결하려는 원격 워크로드에서 빠른 지원 애플리케이션이 실행되고 있습니다.

Acronis 빠른 지원을 통해 관리 대상 워크로드에 연결

빠른 지원 기능을 사용하면 요청 시 비관리 대상 워크로드에 원격으로 연결하여 일회성 지원을 제공할 수 있습니다.

사전 요구 사항

- 고객 테넌트에 Advanced Management 팩이 할당되어 있어야 합니다.
- Acronis Cyber Protect Cloud에서 사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.
- 원격 사용자가 빠른 지원에서 워크로드 ID와 액세스 코드를 입력한 상태여야 합니다.
- 원격 사용자가 Acronis 빠른 지원을 다운로드하여 실행한 상태여야 합니다.

빠른 지원을 사용하여 원격 지원을 위해 워크로드에 연결하려면

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. **빠른 지원**을 클릭합니다.
3. **빠른 지원** 창에서 최종 사용자가 제공한 워크로드 ID를 입력하고 **연결**을 선택합니다.
4. **연결**을 클릭합니다.
5. 워크로드에 Connect 클라이언트가 설치되어 있는지 여부에 따라 다음 중 하나를 수행합니다.
   - Connect 클라이언트가 설치되어 있지 않은 경우 다운로드하여 설치한 후 확인 팝업이 표시되면 **허용**을 선택합니다.
   - Connect 클라이언트가 이미 설치되어 있는 경우 확인 팝업이 표시되면 **Connect 클라이언트 열기**를 클릭합니다.
6. **인증** 창에서 액세스 코드를 입력합니다.
7. Connect 클라이언트에서 새 뷰어 창이 열립니다. 이 창에서 원격 워크로드의 데스크탑을 확인할 수 있습니다. 원격 연결이 설정되고 나면 뷰어의 도구 모음에서 원격 워크로드에 대해 추가 작업을 수행할 수 있습니다. 자세한 내용은 "뷰어 창에서 도구 모음 사용"(927페이지)을(를) 참조하십시오.

© Acronis International GmbH, 2003-2024

IP 주소를 통해 비관리 대상 워크로드에 연결

비관리 대상 워크로드가 LAN에 있으면 워크로드의 IP 주소를 사용하여 원격 제어나 원격 지원을 위해 워크로드에 연결할 수 있습니다. 이렇게 연결할 때는 인터넷에 액세스할 필요가 없습니다.

사전 요구 사항

- 고객 테넌트에 Advanced Management 팩이 할당되어 있어야 합니다.
- Acronis Cyber Protect Cloud에서 사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

워크로드의 IP 주소를 사용하여 원격 데스크탑 또는 원격 지원을 위해 워크로드에 연결하려면

1. Cyber Protect 콘솔에서 **모든 장치**로 이동합니다.
2. **빠른 지원**을 클릭합니다.
3. **IP 주소를 통해** 탭을 클릭합니다.
4. 워크로드의 IP 주소 및 포트를 입력합니다.
5. 원격 워크로드의 운영 체제에 따라 연결 프로토콜을 RDP(Windows 워크로드) 또는 Apple 화면 공유(macOS 워크로드) 중에서 선택합니다.

   참고
   RDP를 통한 연결에서는 원격 데스크탑 작업이 지원되며 Apple 화면 공유를 통한 연결에서는 원격 데스크톱 및 원격 지원 작업이 모두 지원됩니다.

6. **연결**을 클릭합니다.
7. **인증** 창에서 필요한 자격 증명을 입력합니다.

Apple 화면 공유 연결의 경우 Connect 클라이언트에서 새 뷰어 창이 열립니다. 이 창에서 원격 워크로드의 데스크탑을 확인할 수 있습니다. 원격 연결이 설정되고 나면 뷰어의 도구 모음에서 원격 워크로드에 대해 추가 작업을 수행할 수 있습니다. 자세한 내용은 "뷰어 창에서 도구 모음 사용" (927페이지)을(를) 참조하십시오.

Acronis 빠른 지원을 통한 파일 전송

빠른 지원 기능을 사용하면 사용자 워크로드와 비관리 대상 워크로드 간에 파일을 전송할 수 있습니다.

사전 요구 사항

- 고객 테넌트에 Advanced Management 팩이 할당되어 있어야 합니다.
- Acronis Cyber Protect Cloud에서 사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.
- 원격 사용자가 Acronis 빠른 지원을 다운로드하여 실행한 상태여야 합니다.
- 원격 사용자가 빠른 지원에서 컴퓨터 ID와 액세스 코드를 입력한 상태여야 합니다.

빠른 지원을 사용하여 워크로드에 파일을 전송하려면

© Acronis International GmbH, 2003-2024

1. Cyber Protect 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. **빠른 지원**을 클릭합니다.
3. **빠른 지원** 창에서 최종 사용자가 제공한 워크로드 ID를 입력하고 **파일 전송**을 선택합니다.
4. **연결**을 클릭합니다.
5. 워크로드에 Connect 클라이언트가 설치되어 있는지 여부에 따라 다음 중 하나를 수행합니다.
   - Connect 클라이언트가 설치되어 있지 않은 경우 다운로드하여 설치한 후 확인 팝업이 표시되면 **허용**을 선택합니다.
   - Connect 클라이언트가 이미 설치되어 있는 경우 확인 팝업이 표시되면 **Connect 클라이언트 열기**를 클릭합니다.
6. **인증** 창에서 액세스 코드를 입력합니다.
7. **파일 전송** 창에서 파일을 찾은 다음 끌어서 원하는 대상에 놓습니다.

   참고
   로컬 워크로드의 파일은 왼쪽 창에, 원격 워크로드의 파일은 오른쪽 창에 나열됩니다.
   시작된 파일 전송은 **작업** 창에 표시됩니다.

8. [선택 사항] **작업** 창에서 완료된 작업을 제거하려면 **완료된 작업 지우기**를 클릭합니다.
9. 모든 전송이 완료되면 창을 닫습니다.

뷰어 창에서 도구 모음 사용

원격 워크로드에 연결한 후에는 뷰어 창의 도구 모음을 사용하여 다양한 작업을 빠르게 수행할 수 있습니다.

아이콘	설명
	실제 크기 원격 데스크탑과 뷰어 창의 픽셀 수가 일치하도록 원격 워크로드의 데스크탑 크기를 조정합니다.
	크기에 맞게 뷰어 창의 크기에 맞게 원격 워크로드 데스크탑의 크기를 조정합니다.
	잠금 및 **잠금 해제 화면** 원격 사용자가 작업을 확인할 수 없도록 원격 워크로드의 디스플레이에 자리 표시자를 표시합니다.
	스크린샷 생성 원격 서버의 데스크탑 이미지를 로컬 파일에 저장합니다.
	디스플레이 선택 확인하려는 원격 워크로드 디스플레이와 원하는 해상도를 선택합니다.

© Acronis International GmbH, 2003-2024

아이콘	설명
	macOS로의 Apple 화면 공유 연결과 모든 운영 체제로의 NEAR 연결에 사용 가능합니다.
	이미지 품질 원격 화면 이미지 품질을 흑백에서 Apple 화면 공유 연결에 적용 가능한 최고 품질로 조정합니다.
	NEAR 이미지 품질 NEAR 연결의 품질/성능 비율을 조정합니다. 슬라이더를 왼쪽(부드럽게)으로 이동하면 이미지 품질보다 성능을 우선적으로 높입니다. 슬라이더를 오른쪽(선명)으로 이동하면 최고 품질의 원격 데스크탑 화면이 제공되지만 성능은 저하될 수 있습니다.
	Ctrl+Alt+Del 전송 원격 워크로드에 Ctrl+Alt+Delete 시퀀스를 전송합니다. Windows 및 Linux 워크로드에 사용 가능합니다.
	파일 전송 원격 워크로드와 로컬 워크로드 간에 파일을 교환할 수 있는 파일 관리자 창을 엽니다. NEAR 연결에 사용 가능합니다.
	도구 모음 고정 뷰어 도구 모음 자동 숨기기를 끕니다. Windows 워크로드에 사용 가능합니다.
	전체 화면 전체 화면 모드로 전환하여 로컬 화면의 전체 크기에 맞게 원격 워크로드 크기를 조정합니다. Windows 워크로드에 사용 가능합니다.
	닫기 뷰어 창을 닫고 원격 제어 세션을 종료합니다. Windows 워크로드에 사용 가능합니다.

연결 유형에 따라 **기타** 아이콘을 클릭하면 추가 옵션이 제공될 수도 있습니다.

옵션	설명
녹화 시작/녹화 중지	현재 원격 데스크탑 세션을 녹화합니다. 세션 녹화는 로컬 워크로드에서 .crec 파일로 저장됩니다. Acronis Connect 클라이언트(으)로 .crec 파일을 열 수 있습니다. NEAR 연결에 사용 가능합니다.

© Acronis International GmbH, 2003-2024

옵션	설명
클립보드 자동 동기화	이 옵션을 켜면 클라이언트가 원격 컴퓨터의 클립보드와 로컬 클립보드를 자동으로 동기화합니다. NEAR 및 Apple 화면 공유 연결에 사용 가능합니다
클립보드 전송 **클립보드 가져오기**	**클립보드 전송**을 선택하면 원격 컴퓨터 클립보드의 내용이 로컬 클립보드의 내용으로 바뀝니다. **클립보드 가져오기**를 선택하면 원격 컴퓨터 클립보드의 내용이 로컬 클립보드로 전송됩니다.
스마트 키보드/원시 키/원시 키(모든 바로 가기 포함)	현재 연결의 키보드 입력 모드를 변경합니다. **스마트 키보드** - 클라이언트가 로컬에서 입력한 기호의 유니코드 코드를 원격 컴퓨터로 전송합니다. **원시 키** - 키보드 버튼을 누르면 클라이언트가 해당 버튼의 원시 코드를 사용합니다. **원시 키(모든 바로 가기 포함)** - 클라이언트가 로컬 시스템 바로 가기를 비활성화합니다(바로 가기가 원격 운영 체제로도 전송됨).
마우스로 가리키면 키보드 포커스 설정	이 옵션을 활성화하면 뷰어 창 위에 로컬 마우스 커서를 놓을 때만 클라이언트가 키보드 입력을 캡처합니다. 이 옵션을 비활성화하면 창을 활성화할 때마다 클라이언트가 키보드를 캡처합니다.
연결 정보 표시/연결 정보 숨기기	**연결 정보 표시**를 선택하면 원격 데스크탑 화면 위에 작은 정보 패널이 나타나며 현재 연결의 가장 중요한 정보가 표시됩니다.
원격 사운드	클라이언트가 원격 컴퓨터에서 로컬 컴퓨터로 사운드를 리디렉션하는 기능을 활성화합니다. NEAR 연결에 사용 가능합니다.
기본 설정	Connect 클라이언트의 설정 구성. 자세한 내용은 "Connect 클라이언트 설정 구성"(930페이지)을(를) 참조하십시오.

원격 세션 녹화 및 재생

Acronis Connect 클라이언트에서 NEAR을 통해 원격 세션을 녹화할 수 있습니다.

원격 연결 세션을 녹화하려면

1. Connect 클라이언트의 뷰어 도구 모음에서 **기타**를 클릭하고 **녹화 시작**을 선택합니다.
2. 녹화본의 이름과 위치를 선택합니다.
   기본적으로 파일은 현재 날짜와 시간으로 이름이 지정되며, 현재 사용자 홈 디렉토리의 **문서** 폴더에 위치하게 됩니다. 녹화본이 활성화되어 있는 동안 **보기** 도구 모음에서는 원격 화면의 오른쪽 상단 모서리 및 녹화 타이머 위에서 반짝이는 붉은 원을 볼 수 있습니다.

© Acronis International GmbH, 2003-2024

3. 녹화를 중지하려면 **기타**를 클릭한 다음 **녹화 중지**를 클릭합니다. Mac의 경우 도구 모음에서 **중지**를 클릭할 수도 있습니다.

   Acronis Connect 클라이언트에서 만든 모든 .crec 파일은 기본적으로 Acronis Connect 클라이언트에서 열립니다.

녹화본을 재생하는 방법

1. 녹화 파일을 찾습니다.
2. 파일을 엽니다.

   AcronisConnect 클라이언트의 녹화 플레이어가 열립니다. 녹화본에서 특정 시점으로 이동할 수는 없습니다. 녹화본에서 특정 시점을 찾으려면 플레이어에서 녹화본이 해당 시점까지 재생될 때까지 기다려야 합니다.
3. [선택 사항] 재생 속도를 조정하려면 재생 제어 섹션의 **<<** 및 **>>** 아이콘을 사용하십시오.

   녹화본은 연결 동안 원격 서버로 전송되고 받은 이벤트의 순서로 저장됩니다. 이는 최소한의 파일 크기로 녹화본의 최상의 품질을 보장합니다. 그러나 녹화본을 통해 이동할 수 없음을 의미하기도 합니다. 현재 녹화본을 비디오 형식으로 변환하는 것도 불가능합니다.

Connect 클라이언트 설정 구성

워크로드에서 Connect 클라이언트를 설치하고 나면 기본 설정에 따라 해당 설정을 구성할 수 있습니다.

Connect 클라이언트의 설정을 구성하려면

1. 시작 메뉴에서 **Connect 클라이언트**를 찾아서 시작합니다.
2. **일반** 탭에서 설정을 구성합니다.

옵션	설명
자세한 로그 쓰기	Connect 클라이언트가 자세한 로그를 쓰도록 허용하려면 이 옵션을 선택합니다. 이 옵션을 비활성화하면 클라이언트가 로그 파일에 일반 정보만 씁니다.
프록시 설정	기본 시스템 프록시를 사용할지 아니면 사용자 정의 SOCKSS 프록시를 구성할지를 선택합니다.

3. **뷰어** 탭에서 설정을 구성합니다.

옵션	설명
뷰어를 닫을 때 확인 메시지 표시	뷰어 창을 실수로 닫는 상황을 방지하기 위해 뷰어 창을 닫으려 할 때 Connect 클라이언트에서 확인 메시지가 표시되도록 하려면 이 옵션을 선택합니다.
최소화 시	CPU 로드를 줄이기 위해 뷰어를 최소화할 때 뷰어 활동을 일시 중단할지 여부를 선택합니다.
최대화 시	최대화 시 전체 화면 모드를 활성화할지 여부를 선택합니다.

© Acronis International GmbH, 2003-2024

옵션	설명
클립보드 전송	텍스트와 이미지를 복사하거나 붙여넣을 때마다 뷰어 창에서 클립보드 전송 표시기 표시를 활성화합니다.
키보드 모드	원격 머신으로 마우스와 키보드 이벤트를 전송할 때마다 뷰어 창 제목에서 입력 모드 표시기 표시를 활성화합니다.
클립보드	사용 가능한 경우 자동 클립보드 동기화를 활성화하려면 **자동으로 클립보드 동기화**를 선택합니다.
키보드 이벤트 전송	Connect 클라이언트 창을 활성화할 때마다 로컬 키보드 입력을 가져올지 아니면 로컬 마우스 포인터가 창 위에 있을 때만 입력을 가져올지를 선택합니다.
뷰어 배경 색상	뷰어 창의 배경 색상을 변경합니다.
자동으로 다시 연결	연결이 중단된 경우 가 연결을 자동으로 다시 설정하도록 하려면 **자동으로 다시 연결 활성화**를 선택합니다.
H.264	하드웨어 디코더를 비활성화할 수 있습니다.
유휴 상태일 때 닫기	유휴 상태를 유지할 시간 간격을 선택합니다. 이 시간이 지나면 뷰어 창이 닫힙니다.

4. **키보드** 탭에서 설정을 구성합니다.

옵션	설명
보조키 매핑	팝업 메뉴를 사용하여 보조키의 동작을 변경합니다. 이러한 설정은 NEAR, Apple 화면 공유, RDP 연결용으로 각각 별도로 저장됩니다.
입력 모드	창 헤더에 선택되어 있는 각 입력 유형용으로 기본 키보드 입력 모드를 선택합니다.

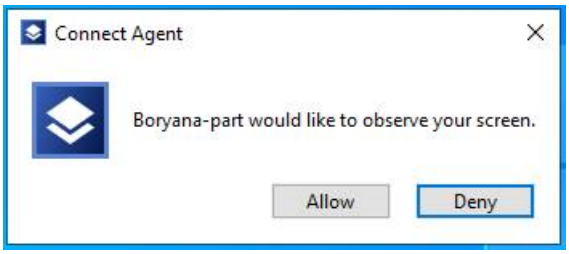
5. **확인**을 클릭합니다.

원격 데스크탑 Notifier

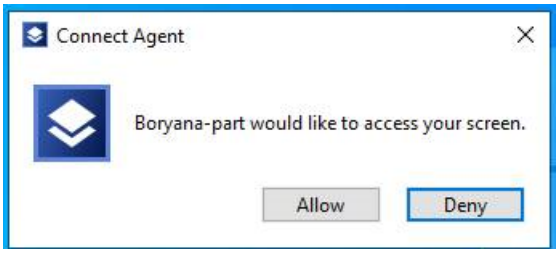
Connect 에이전트는 다음과 같은 경우 원격 워크로드의 데스크탑에 작업 대화 상자(Notifier)를 표시합니다.

- 관찰 권한을 요청하여 워크로드에 원격으로 연결을 시도할 때. 원격 워크로드에 로컬로 로그인되어 있는 사용자가 요청을 허용하거나 거부할 수 있습니다.

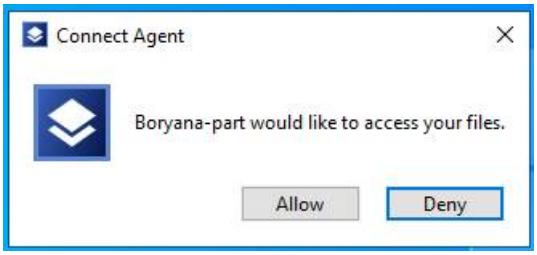
© Acronis International GmbH, 2003-2024



- 제어 권한을 요청하여 워크로드에 원격으로 연결을 시도할 때. 원격 워크로드에 로컬로 로그인되어 있는 사용자가 요청을 허용하거나 거부할 수 있습니다.



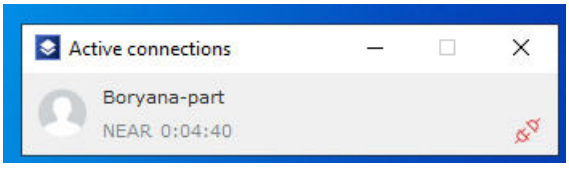
- 파일 전송 권한을 요청하여 사용자 워크로드와 원격 워크로드 간의 파일 교환을 시도할 때. 원격 워크로드에 로컬로 로그인되어 있는 사용자가 요청을 허용하거나 거부할 수 있습니다.



워크로드에 대한 원격 데스크탑 연결을 설정하면 해당 워크로드에 로그인되어 있는 사용자에게는 다음 정보가 포함된 다른 연결 Notifier가 표시됩니다.

- 원격으로 연결한 사용자의 이름
- 원격 연결을 설정하는 데 사용되는 연결 프로토콜
- 원격 연결의 기간

원격 워크로드에 로컬로 로그인되어 있는 사용자는 **연결 끊기** 아이콘이나 **닫기** 아이콘을 클릭하여 언제든지 연결을 종료할 수 있습니다.



© Acronis International GmbH, 2003-2024

워크로드의 상태와 성능 모니터링

조직의 워크로드 상태와 시스템 매개변수를 모니터링할 수 있습니다. 매개변수가 정상 범위를 벗어나면 즉시 알림이 표시되므로 문제를 빠르게 해결할 수 있습니다. 사용자 정의 경보와 자동 대응 조치도 구성할 수 있습니다. 자동 대응 조치는 워크로드 동작의 이상 현상 해결을 위해 자동으로 수행되는 작업입니다.

참고
모니터링 기능을 사용하려면 워크로드에 보호 에이전트 버전 15.0.35324 이상을 설치해야 합니다.

모니터링 계획

관리 대상 워크로드의 성능, 하드웨어, 소프트웨어, 시스템 및 보안 매개변수 모니터링을 시작하려면 워크로드에 모니터링 계획을 적용합니다. 모니터링 계획은 활성화 및 구성 가능한 여러 모니터로 구성됩니다. 이상 현상 기반 모니터링 유형을 지원하는 모니터도 있습니다. 모니터링 계획에 대한 자세한 내용은 "모니터링 계획"(962페이지) 항목을 참조하십시오. 모니터링 계획에서 구성할 수 있는 사용 가능 모니터에 대한 자세한 내용은 "구성 가능한 모니터"(934페이지) 항목을 참조하십시오.

에이전트가 워크로드에서 데이터를 수집할 수 없는 경우 시스템이 경보를 생성합니다.

모니터링 유형

계획에서 활성화하는 각 모니터의 모니터링 유형을 구성해야 합니다. 모니터링 유형에 따라 모니터가 워크로드의 정상 동작과 편차를 예측하는 데 사용할 알고리즘이 결정됩니다. 모니터링 유형에는 임계값 기반 모니터링과 이상 현상 기반 모니터링의 두 가지가 있습니다. 임계값 기반 모니터링 유형만 지원하는 모니터도 있습니다.

임계값 기반 모니터링에서는 매개변수의 값이 구성된 임계값보다 큰지 아니면 작은지를 추적합니다. 이 모니터링 유형 사용 시에는 사용자가 워크로드의 정확한 임계값을 정의해야 합니다. 그러면 시스템은 이러한 정적 임계값을 기준으로 시스템이 정상 동작을 결정하며, 해당 동작을 야기할 수 있는 기타 특정 조건은 고려하지 않습니다. 따라서 임계값 기반 모니터링은 이상 현상 기반 모니터링에 비해 정확도가 낮을 수도 있습니다.

이상 현상 기반 모니터링에서는 머신 러닝을 사용하여 특정 워크로드 관련 정상 동작 패턴을 생성하고 이상 동작을 감지합니다. 자세한 내용은 "이상 현상 기반 모니터링"(933페이지)을(를) 참조하십시오.

이상 현상 기반 모니터링

이상 현상 기반 모니터링에서는 머신 러닝 모델을 사용하여 특정 워크로드 관련 정상 동작 패턴을 생성하고 해당 워크로드의 동작에서 이상 현상(시계열 데이터의 비정상적인 급증 현상)을 감지합니다. 이 모니터링 유형을 활성화하면 시스템이 모델을 생성한 후 워크로드에서 수집하는 데이터를 기반으로 자체 교육을 진행해 특정 워크로드용으로 모델을 조정하는 과정을 시작합니다. 그러므로 교육 기간 시작 시에는 데이터가 100% 정확하지 않을 수도 있습니다. 안정적인 모델을 생성하려면 3주 이상 모델 교육을 진행해야 합니다. 시스템은 데이터를 추가로 수집하여 내역 데이터

© Acronis International GmbH, 2003-2024

세트를 분석하는 과정에서 모델을 점진적으로 구체화하고 워크로드의 각 메트릭에 적용되는 동적 상한 임계값과 하한 임계값을 생성합니다. 이 모니터링 유형은 임계값 기반 모니터링에 비해 유동성이 우수합니다. 시스템이 매개변수의 값과 해당 컨텍스트를 모니터링하기 때문입니다. 예를 들어 특정 시간에는 특정 워크로드의 로드가 커지는 상황이 정상적인 현상일 수 있습니다. 임계값 기반 모니터링 유형에서는 이러한 현상을 비정상적인 동작으로 잘못 해석하여 경보를 트리거합니다.

워크로드의 머신 러닝 모델을 재설정할 수 있습니다. 그러면 시스템이 워크로드에 적용되어 있는 모니터의 모든 데이터와 모델을 삭제합니다. 자세한 내용은 "머신 러닝 모델 재설정"(971페이지)을(를) 참조하십시오.

모니터링용으로 지원되는 플랫폼

모니터링 기능이 지원되는 운영 체제는 다음과 같습니다.

지원되는 Windows 버전	지원되는 macOS 버전
• Windows 7 SP1 • Windows 8, 8.1 • Windows 10 • Windows 11 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022	• macOS 10.14 (Mojave) • macOS 10.15 (Catalina) • macOS 11.x(Big Sur) • macOS 12.x(Monterey) • macOS 13.x(Ventura)

구성 가능한 모니터

모니터링 기능이 지원하는 모니터는 하드웨어, 성능, 소프트웨어, 시스템, 보안, 사용자 정의의 6개 카테고리로 구분할 수 있습니다.

모니터	설명	지원되는 운영 체제	데이터 수집 빈도	이상 현상 기반 모니터링 지원	Standard Protection 또는 Advanced Management에서의 사용 가능 여부
하드웨어					
디스크 공간	워크로드의 특정 드라이브 여유 공간을 모니터링합니다.	Windows macOS	1분	예	Standard Protection

© Acronis International GmbH, 2003-2024

모니터	설명	지원되는 운영 체제	데이터 수집 빈도	이상 현상 기반 모니터링 지원	Standard Protection 또는 Advanced Management에서의 사용 가능 여부
CPU 온도	CPU 온도를 모니터링합니다.	Windows macOS	30초	예	Advanced Management
GPU 온도	GPU 온도를 모니터링합니다.	Windows macOS	30초	예	Advanced Management
하드웨어 변경	워크로드에서 하드웨어 추가, 제거, 교체와 같은 하드웨어 변경 사항을 모니터링합니다	Windows macOS	24시간	아니요	Standard Protection
성능					
CPU 사용량	워크로드의 모든 CPU에서 사용되는 전체 메모리 사용량을 모니터링합니다.	Windows macOS	30초	예	Advanced Management
메모리 사용량	워크로드의 모든 메모리 슬롯에서 사용되는 전체 메모리 사용량을 모니터링합니다.	Windows macOS	30초	예	Advanced Management
디스크 전송 속도	워크로드에서 각 실제 디스크의 읽기 및 쓰기 속도를 모니터링합니다.	Windows macOS	30초	예	Advanced Management
네트워크 사용량	워크로드에 있는 각 네트워크 어댑터의 수신 트래픽과 보내는 트래픽을 모니터링합니다.	Windows macOS	30초	예	Advanced Management
프로세스별 CPU 사용량	특정 프로세스의 CPU 사용량을 모니터링합니다.	Windows macOS	30초	아니요	Advanced Management
프로세스별 메모리 사용량	선택한 프로세스의 메모리 사용량을 모니터링합니다.	Windows macOS	30초	아니요	Advanced Management
프로세스별 디스크 전송 속도	선택한 프로세스의 읽기 및 쓰기 속도를 모니터링합니다.	Windows macOS	30초	아니요	Advanced Management

© Acronis International GmbH, 2003-2024

모니터	설명	지원되는 운영 체제	데이터 수집 빈도	이상 현상 기반 모니터링 지원	Standard Protection 또는 Advanced Management에서의 사용 가능 여부
프로세스별 네트워크 사용량	선택한 프로세스의 수신 트래픽과 보내는 트래픽을 모니터링합니다.	Windows macOS	30초	아니요	Advanced Management
소프트웨어					
Windows 서비스 상태	선택한 Windows 서비스의 상태(실행 중 또는 중지됨)를 모니터링합니다.	Windows	30초	아니요	Advanced Management
프로세스 상태	선택한 프로세스의 상태(실행 중 또는 중지됨)를 모니터링합니다.	Windows macOS	30초	아니요	Advanced Management
설치된 소프트웨어	소프트웨어 애플리케이션 설치, 업데이트 또는 삭제를 모니터링합니다.	Windows macOS	24시간	아니요	Advanced Management
시스템					
마지막 시스템 다시 시작	워크로드를 다시 시작한 시간을 모니터링합니다.	Windows macOS	1시간	아니요	Standard Protection
Windows 이벤트 로그	Windows 이벤트 로그에서 특정 중요 이벤트를 모니터링합니다.	Windows	10분	아니요	Advanced Management
파일 및 폴더 크기	선택한 파일이나 폴더의 총 크기를 모니터링합니다.	Windows macOS	10분	아니요	Standard Protection
보안					
Windows 업데이트 상태	워크로드의 Windows 업데이트 상태와 최신 업데이트 설치 여부를 모니터링합니다.	Windows	15분	아니요	Advanced Management
방화벽 상태	워크로드에 설치되어 있는 기본 제공 또는 서드 파티 방화벽의 상태를 모니터링합니다.	Windows macOS	5분	아니요	Advanced Management
안티맬웨어	워크로드에 설치되어 있는	Windows	5분	아니	Advanced

© Acronis International GmbH, 2003-2024

모니터	설명	지원되는 운영 체제	데이터 수집 빈도	이상 현상 기반 모니터링 지원	Standard Protection 또는 Advanced Management에서의 사용 가능 여부
소프트웨어 상태	기본 제공 또는 서드 파티 안티맬웨어 소프트웨어의 상태를 모니터링합니다.	macOS		요	Management
실패한 로그인	워크로드에서 실패한 로그인 시도를 모니터링합니다.	Windows	1시간	아니요	Advanced Management
자동 실행 상태	이동식 스토리지 미디어용 자동 실행 기능이 활성화되어 있는지를 모니터링합니다.	Windows	1시간	아니요	Advanced Management
사용자 정의					
사용자 정의	스크립트를 실행하여 사용자 정의 객체를 모니터링합니다.	Windows macOS	사용자 정의	아니요	Advanced Management

디스크 공간 모니터의 설정

디스크 공간은 워크로드의 특정 드라이브 여유 공간을 모니터링합니다.

참고
모니터는 공간을 계산할 때 Windows 워크로드와 macOS 워크로드 모두에 대해 이진 바이트(KB당 1,024바이트, MB당 1,024KB, GB당 1,024MB)를 사용합니다.

모니터에 대해 다음 설정을 구성할 수 있습니다.

설정	설명
임계값 기반 모니터링	
드라이브	모니터링할 드라이브입니다. 사용 가능한 값은 다음과 같습니다. • **시스템 드라이브** - 기본값입니다. • **모든 드라이브**
연산자	연산자는 메트릭의 성능 측정 방법을 정의하는 조건부 함수입니다.

© Acronis International GmbH, 2003-2024

설정	설명
	사용 가능한 값은 다음과 같습니다. • **보다 작음** - 기본값입니다. • **보다 작음 또는 같음**
디스크의 사용 가능한 공간 임계값	임계값과 **연산자** 값에 따라 모니터링되는 메트릭의 정상 성능이 결정됩니다. 모니터링되는 메트릭의 값이 정상 범위를 벗어나면 시스템에서 경보를 생성합니다. 1~100(%) 사이의 정수 값을 입력합니다. 기본값은 20입니다.
이동식 드라이브 포함	**드라이브** 값이 **모든 드라이브**이면 이 설정을 사용할 수 있습니다. USB 플래시 드라이브 등의 이동식 드라이브를 모니터링 대상으로 추가하려면 이 설정을 선택합니다. 해당 설정은 기본적으로 비활성화됩니다.
기간	메트릭 값이 지정된 기간 동안 정상 범위를 벗어나는 경우에만 시스템에서 감지된 문제 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 30입니다.
이상 현상 기반 모니터링	
드라이브	모니터링할 드라이브입니다. 사용 가능한 값은 다음과 같습니다. • **시스템 드라이브** - 기본값입니다. • **모든 드라이브**
모델 교육 기간	시스템이 에이전트에서 수집한 데이터를 기반으로 머신 러닝 모델을 교육한 후 워크로드의 정상 동작 패턴을 생성하는 기간입니다. 모델 교육 기간이 길수록 시스템이 생성하는 장기 행동 패턴의 정밀도도 높아집니다. 최소 모델 교육 기간은 21일로 설정하는 것이 좋습니다. 정수 값(기간, 일)을 입력합니다. 기본값은 21입니다.
교육 기간 동안 이상 경보 수신	이 설정을 선택하면 모델 교육 기간 동안 이상 동작 관련 경보가 수신됩니다. 교육 중에는 모델의 정확도가 아직 높지 않을 수도 있으므로 거짓 경보가 수신될 수도 있습니다. 해당 설정은 기본적으로 선택됩니다.
민감도 수준	민감도 수준은 값이 특정 범위 내의 숫자인 이상 동작의 예비 필터로 사용됩니다. 이 필터는 이상 동작 감지 알고리즘과는 독립적으로 작동합니다. 이 필터를 사용하면 지정된 범위 내의 이상 동작을 이상 동작 감지 알고리즘이 더 이상 처리하지 않도록 제외할 수 있습니다. 교육 기간 동안 수행되는 작업은 다음과 같습니다. 1. 교육 중에 수집된 데이터를 사용하여 알고리즘 교육이 진행됩니다. 2. 알고리즘이 교육 데이터에서 이상 동작 감지를 수행합니다.

© Acronis International GmbH, 2003-2024

설정	설명
	3. 평균 및 표준 편차 기준 필터링 프로세스가 적용됩니다. 4. 지정된 간격 내에서 확인된 모든 이상 동작이 필터링됩니다. 5. 이상 동작이 확인된 나머지 데이터 요소에서는 이상 동작 수준이 가장 낮은 이상 동작이 선택됩니다. 이 수준(0~1 사이의 부동 소수점 숫자)이 모델에 기록됩니다. 예측 중에 수행되는 작업은 다음과 같습니다. 1. 알고리즘이 유추 데이터에서 이상 동작을 예측합니다. 2. 민감도 수준에 따라 평균 및 표준 편차를 기준으로 예측된 이상 동작을 필터링합니다. 3. 나머지 이상 동작도 추가로 필터링되는데, 이때 임계값 수준을 초과하는 값은 이상 동작으로 간주되며 임계값 수준 미만의 값은 정상 동작으로 간주됩니다. 사용 가능한 값은 다음과 같습니다. • **낮음** - 평균 값 및 표준 편차 값에 해당하는 수준입니다. • **보통** - 기본값입니다. 평균 값 및 표준 편차 값의 2배에 해당하는 수준입니다. • **높음** - 평균 값 및 표준 편차 값의 3배에 해당하는 수준입니다.
이상 발생 기간	비정상적 동작이 지정된 기간 동안 계속 발생하는 경우에만 시스템에서 감지된 이상 동작 관련 경보를 생성합니다. 기본값은 30분입니다.

CPU 온도 모니터의 설정

CPU 온도는 워크로드의 CPU 온도를 모니터링합니다.

모니터에 대해 다음 설정을 구성할 수 있습니다.

설정	설명
임계값 기반 모니터링	
CPU 온도가 초과됨(°C)	모니터링되는 메트릭의 최대값입니다. 해당 값이 초과되면 시스템이 경보를 생성합니다. 정수 값(C°)을 입력합니다. 기본값은 80입니다.
기간	메트릭 값이 지정된 기간 동안 정상 범위를 벗어나는 경우에만 시스템에서 감지된 문제 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 5입니다.
이상 현상 기반 모니터링	
모델 교육 기간	시스템이 에이전트에서 수집한 데이터를 기반으로 머신 러닝 모델을 교육한 후 워크로드의 정상 동작 패턴을 생성하는 기간입니다. 모델 교육 기간이 길수록 시스템이 생성하는 장기 행동 패턴의 정밀도도 높아집니다. 최소 모델 교육 기간은 21일로 설

© Acronis International GmbH, 2003-2024

설정	설명
	정하는 것이 좋습니다. 정수 값(기간, 일)을 입력합니다. 기본값은 21입니다.
민감도 수준	민감도 수준은 값이 특정 범위 내의 숫자인 이상 동작의 예비 필터로 사용됩니다. 이 필터는 이상 동작 감지 알고리즘과는 독립적으로 작동합니다. 이 필터를 사용하면 지정된 범위 내의 이상 동작을 이상 동작 감지 알고리즘이 더 이상 처리하지 않도록 제외할 수 있습니다. 교육 기간 동안 수행되는 작업은 다음과 같습니다. 1. 교육 중에 수집된 데이터를 사용하여 알고리즘 교육이 진행됩니다. 2. 알고리즘이 교육 데이터에서 이상 동작 감지를 수행합니다. 3. 평균 및 표준 편차 기준 필터링 프로세스가 적용됩니다. 4. 지정된 간격 내에서 확인된 모든 이상 동작이 필터링됩니다. 5. 이상 동작이 확인된 나머지 데이터 요소에서는 이상 동작 수준이 가장 낮은 이상 동작이 선택됩니다. 이 수준(0~1 사이의 부동 소수점 숫자)이 모델에 기록됩니다. 예측 중에 수행되는 작업은 다음과 같습니다. 1. 알고리즘이 유추 데이터에서 이상 동작을 예측합니다. 2. 민감도 수준에 따라 평균 및 표준 편차를 기준으로 예측된 이상 동작을 필터링합니다. 3. 나머지 이상 동작도 추가로 필터링되는데, 이때 임계값 수준을 초과하는 값은 이상 동작으로 간주되며 임계값 수준 미만의 값은 정상 동작으로 간주됩니다. 사용 가능한 값은 다음과 같습니다. • **낮음** - 평균 값 및 표준 편차 값에 해당하는 수준입니다. • **보통** - 기본값입니다. 평균 값 및 표준 편차 값의 2배에 해당하는 수준입니다. • **높음** - 평균 값 및 표준 편차 값의 3배에 해당하는 수준입니다.
이상 발생 기간	비정상적 동작이 지정된 기간 동안 계속 발생하는 경우에만 시스템에서 감지된 이상 동작 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 15입니다.

GPU 온도 모니터의 설정

GPU 온도는 워크로드의 GPU 온도를 모니터링합니다.

모니터에 대해 다음 설정을 구성할 수 있습니다.

© Acronis International GmbH, 2003-2024

설정	설명
임계값 기반 모니터링	
GPU 온도가 초과됨	모니터링되는 메트릭의 최대값입니다. 해당 값이 초과되면 시스템이 이상 동작을 감지합니다. 정수 값(C°)을 입력합니다. 기본값은 80입니다.
기간	메트릭 값이 지정된 기간 동안 정상 범위를 벗어나는 경우에만 시스템에서 감지된 문제 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 5입니다.
이상 현상 기반 모니터링	
모델 교육 기간	시스템이 에이전트에서 수집한 데이터를 기반으로 머신 러닝 모델을 교육한 후 워크로드의 정상 동작 패턴을 생성하는 기간입니다. 모델 교육 기간이 길수록 시스템이 생성하는 장기 행동 패턴의 정밀도도 높아집니다. 최소 모델 교육 기간은 21일로 설정하는 것이 좋습니다. 정수 값(기간, 일)을 입력합니다. 기본값은 21입니다.
민감도 수준	민감도 수준은 값이 특정 범위 내의 숫자인 이상 동작의 예비 필터로 사용됩니다. 이 필터는 이상 동작 감지 알고리즘과는 독립적으로 작동합니다. 이 필터를 사용하면 지정된 범위 내의 이상 동작을 이상 동작 감지 알고리즘이 더 이상 처리하지 않도록 제외할 수 있습니다. 교육 기간 동안 수행되는 작업은 다음과 같습니다. 1. 교육 중에 수집된 데이터를 사용하여 알고리즘 교육이 진행됩니다. 2. 알고리즘이 교육 데이터에서 이상 동작 감지를 수행합니다. 3. 평균 및 표준 편차 기준 필터링 프로세스가 적용됩니다. 4. 지정된 간격 내에서 확인된 모든 이상 동작이 필터링됩니다. 5. 이상 동작이 확인된 나머지 데이터 요소에서는 이상 동작 수준이 가장 낮은 이상 동작이 선택됩니다. 이 수준(0~1 사이의 부동 소수점 숫자)이 모델에 기록됩니다. 예측 중에 수행되는 작업은 다음과 같습니다. 1. 알고리즘이 유추 데이터에서 이상 동작을 예측합니다. 2. 민감도 수준에 따라 평균 및 표준 편차를 기준으로 예측된 이상 동작을 필터링합니다. 3. 나머지 이상 동작도 추가로 필터링되는데, 이때 임계값 수준을 초과하는 값은 이상 동작으로 간주되며 임계값 수준 미만의 값은 정상 동작으로 간주됩니다. 사용 가능한 값은 다음과 같습니다. • **낮음** - 평균 값 및 표준 편차 값에 해당하는 수준입니다. • **보통** - 기본값입니다. 평균 값 및 표준 편차 값의 2배에 해당하는 수준입니다. • **높음** - 평균 값 및 표준 편차 값의 3배에 해당하는 수준입니다.
이상 발생	비정상적 동작이 지정된 기간 동안 계속 발생하는 경우에만 시스템에서 감지된 이상 동작 관련 경보를 생성합니다.

© Acronis International GmbH, 2003-2024

설정	설명
기간	1~60(분) 사이의 정수 값을 입력합니다. 기본값은 15입니다.

하드웨어 변경 모니터의 설정

하드웨어 변경은 워크로드에서 하드웨어 추가, 제거, 교체와 같은 하드웨어 변경 사항을 모니터링합니다.

모니터에 대해 다음 설정을 구성할 수 있습니다.

설정	설명
하드웨어 컴포넌트	변경을 모니터링할 하드웨어 컴포넌트를 하나 이상 선택합니다. 사용 가능한 값은 다음과 같습니다. • **모두** - 기본값입니다. • **마더보드** • **CPU** • **RAM** • **디스크** • **GPU** • **네트워크 어댑터**
모니터링 대상	선택한 하드에어 컴포넌트에서 모니터링할 변경 사항을 지정합니다. 목록에서 여러 항목을 선택할 수 있습니다. 사용 가능한 값은 다음과 같습니다. • **모든 변경 사항** - 기본값입니다. • **새로 추가된 컴포넌트** • **교체된 컴포넌트** • **제거된 컴포넌트**

CPU 사용량 모니터의 설정

CPU 사용량은 워크로드의 총 CPU 사용량(프로세서 사용률)을 모니터링합니다. 워크로드의 CPU가 여러 개이면 총 CPU 사용량은 각 CPU의 사용량 합계입니다.

모니터에 대해 다음 설정을 구성할 수 있습니다.

설정	설명
임계값 기반 모니터링	
연산자	연산자는 메트릭의 성능 측정 방법을 정의하는 조건부 함수입니다. 사용 가능한 값은 다음과 같습니다. • **이상** - 기본값입니다.

© Acronis International GmbH, 2003-2024

설정	설명
	• **보다 큼 또는 같음** • **보다 작음** • **보다 작음 또는 같음**
CPU 사용량 임계값	임계값과 **연산자** 값에 따라 모니터링되는 메트릭의 정상 성능이 결정됩니다. 모니터링되는 메트릭의 값이 정상 범위를 벗어나면 시스템에서 경보를 생성합니다. 1~100(%) 사이의 정수 값을 입력합니다. 기본값은 90입니다.
기간	메트릭 값이 지정된 기간 동안 정상 범위를 벗어나는 경우에만 시스템에서 감지된 문제 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 5입니다.
이상 현상 기반 모니터링	
모델 교육 기간	시스템이 에이전트에서 수집한 데이터를 기반으로 머신 러닝 모델을 교육한 후 워크로드의 정상 동작 패턴을 생성하는 기간입니다. 모델 교육 기간이 길수록 시스템이 생성하는 장기 행동 패턴의 정밀도도 높아집니다. 최소 모델 교육 기간은 21일로 설정하는 것이 좋습니다. 정수 값(기간, 일)을 입력합니다. 기본값은 21입니다.
교육 기간 동안 이상 경보 수신	이 설정을 선택하면 모델 교육 기간 동안 이상 동작 관련 경보가 수신됩니다. 교육 중에는 모델의 정확도가 아직 높지 않을 수도 있으므로 거짓 경보가 수신될 수도 있습니다. 해당 설정은 기본적으로 선택됩니다.
민감도 수준	민감도 수준은 값이 특정 범위 내의 숫자인 이상 동작의 예비 필터로 사용됩니다. 이 필터는 이상 동작 감지 알고리즘과는 독립적으로 작동합니다. 이 필터를 사용하면 지정된 범위 내의 이상 동작을 이상 동작 감지 알고리즘이 더 이상 처리하지 않도록 제외할 수 있습니다. 교육 기간 동안 수행되는 작업은 다음과 같습니다. 1. 교육 중에 수집된 데이터를 사용하여 알고리즘 교육이 진행됩니다. 2. 알고리즘이 교육 데이터에서 이상 동작 감지를 수행합니다. 3. 평균 및 표준 편차 기준 필터링 프로세스가 적용됩니다. 4. 지정된 간격 내에서 확인된 모든 이상 동작이 필터링됩니다. 5. 이상 동작이 확인된 나머지 데이터 요소에서는 이상 동작 수준이 가장 낮은 이상 동작이 선택됩니다. 이 수준(0~1 사이의 부동 소수점 숫자)이 모델에 기록됩니다. 예측 중에 수행되는 작업은 다음과 같습니다. 1. 알고리즘이 유추 데이터에서 이상 동작을 예측합니다. 2. 민감도 수준에 따라 평균 및 표준 편차를 기준으로 예측된 이상 동작을 필터링합니다. 3. 나머지 이상 동작도 추가로 필터링되는데, 이때 임계값 수준을 초과하는 값은 이상 동작으로 간주되며 임계값 수준 미만의 값은 정상 동작으로 간주됩니다.

© Acronis International GmbH, 2003-2024

설정	설명
	사용 가능한 값은 다음과 같습니다. • **낮음** - 평균 값 및 표준 편차 값에 해당하는 수준입니다. • **보통** - 기본값입니다. 평균 값 및 표준 편차 값의 2배에 해당하는 수준입니다. • **높음** - 평균 값 및 표준 편차 값의 3배에 해당하는 수준입니다.
이상 발생 기간	비정상적 동작이 지정된 기간 동안 계속 발생하는 경우에만 시스템에서 감지된 이상 동작 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 15입니다.

메모리 사용량 모니터의 설정

메모리 사용량은 워크로드의 모든 메모리 모듈에서 사용되는 총 메모리 사용량을 모니터링합니다.

모니터에 대해 다음 설정을 구성할 수 있습니다.

설정	설명
임계값 기반 모니터링	
연산자	연산자는 메트릭의 성능 측정 방법을 정의하는 조건부 함수입니다. 사용 가능한 값은 다음과 같습니다. • **이상** - 기본값입니다. • **보다 큼 또는 같음** • **보다 작음** • **보다 작음 또는 같음**
메모리 사용량 임계값	임계값과 **연산자** 값에 따라 모니터링되는 메트릭의 정상 성능이 결정됩니다. 모니터링되는 메트릭의 값이 정상 범위를 벗어나면 시스템에서 경보를 생성합니다. 1~100(%) 사이의 정수 값을 입력합니다. 기본값은 90입니다.
기간	메트릭 값이 지정된 기간 동안 정상 범위를 벗어나는 경우에만 시스템에서 감지된 문제 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 5입니다.
이상 현상 기반 모니터링	
모델 교육 기간	시스템이 에이전트에서 수집한 데이터를 기반으로 머신 러닝 모델을 교육한 후 워크로드의 정상 동작 패턴을 생성하는 기간입니다. 모델 교육 기간이 길수록 시스템이 생성하는 장기 행동 패턴의 정밀도도 높아집니다. 최소 모델 교육 기간은 21일로 설정하는 것이 좋습니다. 정수 값(기간, 일)을 입력합니다. 기본값은 21입니다.
교육 기간 동안	이 설정을 선택하면 모델 교육 기간 동안 이상 동작 관련 경보가 수신됩니다. 교육 중에는 모델의 정확도가 아직 높지 않을 수도 있으므로 거짓 경보가 수신될 수도

© Acronis International GmbH, 2003-2024

설정	설명
이상 경보 수신	있습니다. 해당 설정은 기본적으로 선택됩니다.
민감도 수준	민감도 수준은 값이 특정 범위 내의 숫자인 이상 동작의 예비 필터로 사용됩니다. 이 필터는 이상 동작 감지 알고리즘과는 독립적으로 작동합니다. 이 필터를 사용하면 지정된 범위 내의 이상 동작을 이상 동작 감지 알고리즘이 더 이상 처리하지 않도록 제외할 수 있습니다. 교육 기간 동안 수행되는 작업은 다음과 같습니다. 1. 교육 중에 수집된 데이터를 사용하여 알고리즘 교육이 진행됩니다. 2. 알고리즘이 교육 데이터에서 이상 동작 감지를 수행합니다. 3. 평균 및 표준 편차 기준 필터링 프로세스가 적용됩니다. 4. 지정된 간격 내에서 확인된 모든 이상 동작이 필터링됩니다. 5. 이상 동작이 확인된 나머지 데이터 요소에서는 이상 동작 수준이 가장 낮은 이상 동작이 선택됩니다. 이 수준(0~1 사이의 부동 소수점 숫자)이 모델에 기록됩니다. 예측 중에 수행되는 작업은 다음과 같습니다. 1. 알고리즘이 유추 데이터에서 이상 동작을 예측합니다. 2. 민감도 수준에 따라 평균 및 표준 편차를 기준으로 예측된 이상 동작을 필터링합니다. 3. 나머지 이상 동작도 추가로 필터링되는데, 이때 임계값 수준을 초과하는 값은 이상 동작으로 간주되며 임계값 수준 미만의 값은 정상 동작으로 간주됩니다. 사용 가능한 값은 다음과 같습니다. • **낮음** - 평균 값 및 표준 편차 값에 해당하는 수준입니다. • **보통** - 기본값입니다. 평균 값 및 표준 편차 값의 2배에 해당하는 수준입니다. • **높음** - 평균 값 및 표준 편차 값의 3배에 해당하는 수준입니다.
이상 발생 기간	비정상적 동작이 지정된 기간 동안 계속 발생하는 경우에만 시스템에서 감지된 이상 동작 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 30분입니다.

디스크 전송 속도 모니터의 설정

디스크 전송 속도는 워크로드에서 각 실제 디스크의 읽기 및 쓰기 속도를 모니터링합니다.

모니터에 대해 다음 설정을 구성할 수 있습니다.

설정	설명
임계값 기반 모니터링	
모니터링 대상	모니터링할 속도를 선택합니다. 사용 가능한 값은 다음과 같습니다.

© Acronis International GmbH, 2003-2024

설정	설명
	• **읽기 속도 및 쓰기 속도** 기본값입니다. • **읽기 속도** • **쓰기 속도**
읽기 속도 연산자	연산자는 메트릭의 성능 측정 방법을 정의하는 조건부 함수입니다. 사용 가능한 값은 다음과 같습니다. • **이상** - 기본값입니다. • **보다 큼 또는 같음** • **보다 작음** • **보다 작음 또는 같음**
읽기 속도 임계값	임계값과 **연산자** 값에 따라 모니터링되는 메트릭의 정상 성능이 결정됩니다. 모니터링되는 메트릭의 값이 정상 범위를 벗어나면 시스템에서 경보를 생성합니다. 정수 값(KB/초)을 입력합니다. 기본값은 0KB/초입니다.
읽기 속도 기간	메트릭 값이 지정된 기간 동안 정상 범위를 벗어나는 경우에만 시스템에서 감지된 문제 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 5입니다.
쓰기 속도 연산자	연산자는 메트릭의 성능 측정 방법을 정의하는 조건부 함수입니다. 사용 가능한 값은 다음과 같습니다. • **이상** - 기본값입니다. • **보다 큼 또는 같음** • **보다 작음** • **보다 작음 또는 같음**
쓰기 속도 임계값	임계값과 **연산자** 값에 따라 모니터링되는 메트릭의 정상 성능이 결정됩니다. 모니터링되는 메트릭의 값이 정상 범위를 벗어나면 시스템에서 경보를 생성합니다. 정수 값(KB/초)을 입력합니다. 기본값은 0KB/초입니다.
쓰기 속도 기간	메트릭 값이 지정된 기간 동안 정상 범위를 벗어나는 경우에만 시스템에서 감지된 문제 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 5입니다.
이상 현상 기반 모니터링	
모델 교육 기간	시스템이 에이전트에서 수집한 데이터를 기반으로 머신 러닝 모델을 교육한 후 워크로드의 정상 동작 패턴을 생성하는 기간입니다. 모델 교육 기간이 길수록 시스템이 생성하는 장기 행동 패턴의 정밀도도 높아집니다. 최소 모델 교육 기간은 21일로 설정하는 것이 좋습니다. 정수 값(기간, 일)을 입력합니다. 기본값은 21입니다.
교육 기	이 설정을 선택하면 모델 교육 기간 동안 이상 동작 관련 경보가 수신됩니다. 교육

© Acronis International GmbH, 2003-2024

설정	설명
간 동안 이상 경보 수신	중에는 모델의 정확도가 아직 높지 않을 수도 있으므로 거짓 경보가 수신될 수도 있습니다. 해당 설정은 기본적으로 선택됩니다.
모니터링 대상	모니터링할 속도를 선택합니다. 사용 가능한 값은 다음과 같습니다. • **읽기 속도 및 쓰기 속도** 기본값입니다. • **읽기 속도** • **쓰기 속도**
민감도 수준	민감도 수준은 값이 특정 범위 내의 숫자인 이상 동작의 예비 필터로 사용됩니다. 이 필터는 이상 동작 감지 알고리즘과는 독립적으로 작동합니다. 이 필터를 사용하면 지정된 범위 내의 이상 동작을 이상 동작 감지 알고리즘이 더 이상 처리하지 않도록 제외할 수 있습니다. 교육 기간 동안 수행되는 작업은 다음과 같습니다. 1. 교육 중에 수집된 데이터를 사용하여 알고리즘 교육이 진행됩니다. 2. 알고리즘이 교육 데이터에서 이상 동작 감지를 수행합니다. 3. 평균 및 표준 편차 기준 필터링 프로세스가 적용됩니다. 4. 지정된 간격 내에서 확인된 모든 이상 동작이 필터링됩니다. 5. 이상 동작이 확인된 나머지 데이터 요소에서는 이상 동작 수준이 가장 낮은 이상 동작이 선택됩니다. 이 수준(0~1 사이의 부동 소수점 숫자)이 모델에 기록됩니다. 예측 중에 수행되는 작업은 다음과 같습니다. 1. 알고리즘이 유추 데이터에서 이상 동작을 예측합니다. 2. 민감도 수준에 따라 평균 및 표준 편차를 기준으로 예측된 이상 동작을 필터링합니다. 3. 나머지 이상 동작도 추가로 필터링되는데, 이때 임계값 수준을 초과하는 값은 이상 동작으로 간주되며 임계값 수준 미만의 값은 정상 동작으로 간주됩니다. 사용 가능한 값은 다음과 같습니다. • **낮음** - 평균 값 및 표준 편차 값에 해당하는 수준입니다. • **보통** - 기본값입니다. 평균 값 및 표준 편차 값의 2배에 해당하는 수준입니다. • **높음** - 평균 값 및 표준 편차 값의 3배에 해당하는 수준입니다.
이상 발생 기간(읽기 속도)	비정상적 동작이 지정된 기간 동안 계속 발생하는 경우에만 시스템에서 감지된 이상 동작 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 25입니다.
이상 발생 기간	비정상적 동작이 지정된 기간 동안 계속 발생하는 경우에만 시스템에서 감지된 이상 동작 관련 경보를 생성합니다.

© Acronis International GmbH, 2003-2024

설정	설명
(쓰기 속도)	1~60(분) 사이의 정수 값을 입력합니다. 기본값은 25입니다.

네트워크 사용량 모니터의 설정

네트워크 사용량은 워크로드에 있는 각 네트워크 어댑터의 수신 트래픽과 보내는 트래픽을 모니터링합니다.

모니터에 대해 다음 설정을 구성할 수 있습니다.

설정	설명
임계값 기반 모니터링	
트래픽 방향	모니터링할 트래픽 방향입니다. 사용 가능한 값은 다음과 같습니다. • **수신 트래픽 및 보내는 트래픽** 기본값입니다. • **수신 트래픽** • **보내는 트래픽**
수신 트래픽 연산자	연산자는 메트릭의 성능 측정 방법을 정의하는 조건부 함수입니다. 사용 가능한 값은 다음과 같습니다. • **이상** - 기본값입니다. • **보다 큼 또는 같음** • **보다 작음** • **보다 작음 또는 같음**
수신 트래픽 임계값	임계값과 **연산자** 값에 따라 모니터링되는 메트릭의 정상 성능이 결정됩니다. 모니터링되는 메트릭의 값이 정상 범위를 벗어나면 시스템에서 경보를 생성합니다. 정수 값(KB/초)을 입력합니다. 기본값은 0KB/초입니다.
수신 트래픽 기간	메트릭 값이 지정된 기간 동안 정상 범위를 벗어나는 경우에만 시스템에서 감지된 문제 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 5입니다.
보내는 트래픽 연산자	연산자는 메트릭의 성능 측정 방법을 정의하는 조건부 함수입니다. 사용 가능한 값은 다음과 같습니다. • **이상** - 기본값입니다. • **보다 큼 또는 같음** • **보다 작음** • **보다 작음 또는 같음**
보내는	임계값과 **연산자** 값에 따라 모니터링되는 메트릭의 정상 성능이 결정됩니다. 모니

© Acronis International GmbH, 2003-2024

설정	설명
트래픽 임계값	터링되는 메트릭의 값이 정상 범위를 벗어나면 시스템에서 경보를 생성합니다. 정수 값(KB/초)을 입력합니다. 기본값은 0KB/초입니다.
보내는 트래픽 기간	임계값과 **연산자** 값에 따라 모니터링되는 메트릭의 정상 성능이 결정됩니다. 모니터링되는 메트릭의 값이 정상 범위를 벗어나면 시스템에서 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 5입니다.
이상 현상 기반 모니터링	
모델 교육 기간	시스템이 에이전트에서 수집한 데이터를 기반으로 머신 러닝 모델을 교육한 후 워크로드의 정상 동작 패턴을 생성하는 기간입니다. 모델 교육 기간이 길수록 시스템이 생성하는 장기 행동 패턴의 정밀도도 높아집니다. 최소 모델 교육 기간은 21일로 설정하는 것이 좋습니다. 정수 값(기간, 일)을 입력합니다. 기본값은 21입니다.
교육 기간 동안 이상 경보 수신	이 설정을 선택하면 모델 교육 기간 동안 이상 동작 관련 경보가 수신됩니다. 교육 중에는 모델의 정확도가 아직 높지 않을 수도 있으므로 거짓 경보가 수신될 수도 있습니다. 해당 설정은 기본적으로 선택됩니다.
트래픽 방향	• **수신 트래픽 및 보내는 트래픽** 기본값입니다. • **수신 트래픽** • **보내는 트래픽**
민감도 수준	민감도 수준은 값이 특정 범위 내의 숫자인 이상 동작의 예비 필터로 사용됩니다. 이 필터는 이상 동작 감지 알고리즘과는 독립적으로 작동합니다. 이 필터를 사용하면 지정된 범위 내의 이상 동작을 이상 동작 감지 알고리즘이 더 이상 처리하지 않도록 제외할 수 있습니다. 교육 기간 동안 수행되는 작업은 다음과 같습니다. 1. 교육 중에 수집된 데이터를 사용하여 알고리즘 교육이 진행됩니다. 2. 알고리즘이 교육 데이터에서 이상 동작 감지를 수행합니다. 3. 평균 및 표준 편차 기준 필터링 프로세스가 적용됩니다. 4. 지정된 간격 내에서 확인된 모든 이상 동작이 필터링됩니다. 5. 이상 동작이 확인된 나머지 데이터 요소에서는 이상 동작 수준이 가장 낮은 이상 동작이 선택됩니다. 이 수준(0~1 사이의 부동 소수점 숫자)이 모델에 기록됩니다. 예측 중에 수행되는 작업은 다음과 같습니다. 1. 알고리즘이 유추 데이터에서 이상 동작을 예측합니다. 2. 민감도 수준에 따라 평균 및 표준 편차를 기준으로 예측된 이상 동작을 필터링합니다. 3. 나머지 이상 동작도 추가로 필터링되는데, 이때 임계값 수준을 초과하는 값은 이상 동작으로 간주되며 임계값 수준 미만의 값은 정상 동작으로 간주됩니다.

© Acronis International GmbH, 2003-2024

설정	설명
	사용 가능한 값은 다음과 같습니다. • **낮음** - 평균 값 및 표준 편차 값에 해당하는 수준입니다. • **보통** - 기본값입니다. 평균 값 및 표준 편차 값의 2배에 해당하는 수준입니다. • **높음** - 평균 값 및 표준 편차 값의 3배에 해당하는 수준입니다.
이상 발생 기간 (수신)	비정상적 동작이 지정된 기간 동안 계속 발생하는 경우에만 시스템에서 감지된 이상 동작 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 25입니다.
이상 발생 기간 (발신)	비정상적 동작이 지정된 기간 동안 계속 발생하는 경우에만 시스템에서 감지된 이상 동작 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 25입니다.

프로세스별 CPU 사용량 모니터의 설정

프로세스별 CPU 사용량은 선택한 프로세스의 CPU 사용량을 모니터링합니다. 동일 프로세스의 인스턴스가 여러 개이면 시스템은 모든 프로세스 인스턴스의 총 사용량을 모니터링하며 조건이 충족되면 경보를 생성합니다.

모니터에 대해 다음 설정을 구성할 수 있습니다.

설정	설명
프로세스 이름	모니터링할 프로세스의 이름입니다. 확장자는 포함하지 않고 프로세스 이름을 입력합니다.
연산자	연산자는 메트릭의 성능 측정 방법을 정의하는 조건부 함수입니다. 사용 가능한 값은 다음과 같습니다. • **이상** - 기본값입니다. • **보다 큼 또는 같음** • **보다 작음** • **보다 작음 또는 같음**
임계값	임계값과 **연산자** 값에 따라 모니터링되는 메트릭의 정상 성능이 결정됩니다. 모니터링되는 메트릭의 값이 정상 범위를 벗어나면 시스템에서 경보를 생성합니다. 1~100(%) 사이의 정수 값을 입력합니다. 기본값은 90입니다.
기간	메트릭 값이 지정된 기간 동안 정상 범위를 벗어나는 경우에만 시스템에서 감지된 문제 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 5입니다.

© Acronis International GmbH, 2003-2024

프로세스별 메모리 사용량 모니터의 설정

프로세스별 메모리 사용량은 선택한 프로세스의 메모리 사용량을 모니터링합니다. 동일 프로세스의 인스턴스가 여러 개이면 시스템은 모든 프로세스 인스턴스의 총 사용량을 모니터링하며 조건이 충족되면 경보를 생성합니다.

참고
에이전트는 총 프로세스 작업 세트(비공개 및 공유)를 사용하여 프로세스별 메모리 사용량의 크기를 예상합니다. 이 때문에 위젯에 표시되는 크기와 Windows 작업 관리자에 표시되는 메모리 사용량의 크기가 다를 수도 있습니다.

모니터에 대해 다음 설정을 구성할 수 있습니다.

설정	설명
프로세스 이름	모니터링할 프로세스의 이름입니다. 확장자는 포함하지 않고 프로세스 이름을 입력합니다.
연산자	연산자는 메트릭의 성능 측정 방법을 정의하는 조건부 함수입니다. 사용 가능한 값은 다음과 같습니다. • **이상** - 기본값입니다. • **보다 큼 또는 같음** • **보다 작음** • **보다 작음 또는 같음**
임계값	임계값과 **연산자** 값에 따라 모니터링되는 메트릭의 정상 성능이 결정됩니다. 모니터링되는 메트릭의 값이 정상 범위를 벗어나면 시스템에서 경보를 생성합니다. 정수 값(KB)을 입력합니다. 기본값은 1입니다.
기간	메트릭 값이 지정된 기간 동안 정상 범위를 벗어나는 경우에만 시스템에서 감지된 문제 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 5입니다.

프로세스별 디스크 전송 속도 모니터의 설정

프로세스별 디스크 전송 속도는 선택한 프로세스의 읽기 및 쓰기 속도를 모니터링합니다. 동일 프로세스의 인스턴스가 여러 개이면 시스템은 모든 프로세스 인스턴스의 총 사용량을 모니터링하며 조건이 충족되면 경보를 생성합니다.

모니터에 대해 다음 설정을 구성할 수 있습니다.

설정	설명
프로세스 이름	모니터링할 프로세스의 이름입니다. 확장자는 포함하지 않고 프로세스 이름을 입력합니다.

© Acronis International GmbH, 2003-2024

설정	설명
모니터링 대상	모니터링할 속도입니다. 사용 가능한 값은 다음과 같습니다. • **읽기 속도 및 쓰기 속도** 기본값입니다. • **읽기 속도** • **쓰기 속도**
읽기 속도 연산자	연산자는 메트릭의 성능 측정 방법을 정의하는 조건부 함수입니다. 사용 가능한 값은 다음과 같습니다. • **이상** - 기본값입니다. • **보다 큼 또는 같음** • **보다 작음** • **보다 작음 또는 같음**
읽기 속도 임계값	임계값과 **연산자** 값에 따라 모니터링되는 메트릭의 정상 성능이 결정됩니다. 모니터링되는 메트릭의 값이 정상 범위를 벗어나면 시스템에서 경보를 생성합니다. 정수 값(KB/초)을 입력합니다. 기본값은 0KB/초입니다.
읽기 속도 기간	메트릭 값이 지정된 기간 동안 정상 범위를 벗어나는 경우에만 시스템에서 감지된 문제 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 5입니다.
쓰기 속도 연산자	연산자는 메트릭의 성능 측정 방법을 정의하는 조건부 함수입니다. 사용 가능한 값은 다음과 같습니다. • **이상** - 기본값입니다. • **보다 큼 또는 같음** • **보다 작음** • **보다 작음 또는 같음**
쓰기 속도 임계값	임계값과 **연산자** 값에 따라 모니터링되는 메트릭의 정상 성능이 결정됩니다. 모니터링되는 메트릭의 값이 정상 범위를 벗어나면 시스템에서 경보를 생성합니다. 정수 값(KB/초)을 입력합니다. 기본값은 0KB/초입니다.
쓰기 속도 기간	메트릭 값이 지정된 기간 동안 정상 범위를 벗어나는 경우에만 시스템에서 감지된 문제 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 5입니다.

프로세스별 네트워크 사용량 모니터의 설정

프로세스별 네트워크 사용량은 선택한 프로세스의 수신 트래픽과 보내는 트래픽을 모니터링합니다. 동일 프로세스의 인스턴스가 여러 개이면 시스템은 모든 프로세스 인스턴스의 총 사용량을 모니터링하며 모든 인스턴스에서 조건이 충족되면 경보를 생성합니다.

모니터에 대해 다음 설정을 구성할 수 있습니다.

© Acronis International GmbH, 2003-2024

설정	설명
프로세스 이름	모니터링할 프로세스의 이름입니다. 확장자는 포함하지 않고 프로세스 이름을 입력합니다.
트래픽 방향	모니터링할 트래픽 방향입니다. 사용 가능한 값은 다음과 같습니다. • **수신 트래픽 및 보내는 트래픽** 기본값입니다. • **수신 트래픽** • **보내는 트래픽**
수신 트래픽 연산자	연산자는 메트릭의 성능 측정 방법을 정의하는 조건부 함수입니다. 사용 가능한 값은 다음과 같습니다. • **이상** - 기본값입니다. • **보다 큼 또는 같음** • **보다 작음** • **보다 작음 또는 같음**
수신 트래픽 임계값	임계값과 **연산자** 값에 따라 모니터링되는 메트릭의 정상 성능이 결정됩니다. 모니터링되는 메트릭의 값이 정상 범위를 벗어나면 시스템에서 경보를 생성합니다. 정수 값(KB/초)을 입력합니다. 기본값은 0KB/초입니다.
수신 트래픽 기간	메트릭 값이 지정된 기간 동안 정상 범위를 벗어나는 경우에만 시스템에서 감지된 문제 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 5입니다.
보내는 트래픽 연산자	연산자는 메트릭의 성능 측정 방법을 정의하는 조건부 함수입니다. 사용 가능한 값은 다음과 같습니다. • **이상** - 기본값입니다. • **보다 큼 또는 같음** • **보다 작음** • **보다 작음 또는 같음**
보내는 트래픽 임계값	임계값과 **연산자** 값에 따라 모니터링되는 메트릭의 정상 성능이 결정됩니다. 모니터링되는 메트릭의 값이 정상 범위를 벗어나면 시스템에서 경보를 생성합니다. 정수 값(KB/초)을 입력합니다. 기본값은 0KB/초입니다.
보내는 트래픽 기간	메트릭 값이 지정된 기간 동안 정상 범위를 벗어나는 경우에만 시스템에서 감지된 문제 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 5입니다.

© Acronis International GmbH, 2003-2024

Windows 서비스 상태 모니터의 설정

Windows 서비스 상태는 선택한 Windows 서비스가 실행 중인지 아니면 중지되었는지를 모니터링합니다.

모니터에 대해 다음 설정을 구성할 수 있습니다.

설정	설명
서비스 이름	모니터링할 Windows 서비스의 이름입니다. Windows 서비스 목록에서 서비스 이름을 선택할 수 있습니다. 워크로드에서 소프트웨어 인벤토리 검색이 정상적으로 완료되면 이 목록에 테넌트의 모든 에이전트가 입력됩니다. 목록에 없는 서비스 이름을 추가할 수도 있습니다. 워크로드에서 소프트웨어 인벤토리 검색을 수행하지 않은 경우에는 이 옵션만 사용 가능합니다.
서비스 상태	서비스가 선택한 상태로 설정되어 있으면 시스템이 이벤트를 생성합니다. 사용 가능한 값은 다음과 같습니다. • **실행 중** • **중지됨** - 기본값입니다.
기간	메트릭 값이 지정된 기간 동안 정상 범위를 벗어나는 경우에만 시스템에서 감지된 문제 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 1입니다.

프로세스 상태 모니터의 설정

프로세스 상태는 선택한 프로세스가 실행 중인지 아니면 중지되었는지를 모니터링합니다. 동일 프로세스의 인스턴스가 여러 개이면 시스템은 프로세스의 각 인스턴스를 모니터링하며 프로세스의 모든 인스턴스에서 조건이 충족되면 경보를 생성합니다.

모니터에 대해 다음 설정을 구성할 수 있습니다.

설정	설명
프로세스 이름	모니터링할 프로세스의 이름입니다. 확장자를 제외한 실행 파일 이름을 입력합니다.
프로세스 상태	프로세스가 선택한 상태이면 시스템이 이벤트를 생성합니다. 사용 가능한 값은 다음과 같습니다. • **실행 중** • **중지됨** - 기본값입니다.
기간	메트릭 값이 지정된 기간 동안 정상 범위를 벗어나는 경우에만 시스템에서 감지된 문제 관련 경보를 생성합니다. 1~60(분) 사이의 정수 값을 입력합니다. 기본값은 1입니다.

© Acronis International GmbH, 2003-2024

설치된 소프트웨어 모니터의 설정

설치된 소프트웨어는 워크로드에서 소프트웨어 애플리케이션 설치, 업데이트 또는 삭제를 모니터링합니다.

모니터에 대해 다음 설정을 구성할 수 있습니다.

설정	설명
모니터링할 소프트웨어	모니터링할 소프트웨어를 지정합니다. 사용 가능한 값은 다음과 같습니다. • **모든 소프트웨어** - 기본값입니다. • **특정 소프트웨어**
소프트웨어 이름	**모니터링할 소프트웨어**로 **특정 소프트웨어** 값을 선택하면 이 설정을 사용할 수 있습니다. 소프트웨어 애플리케이션의 이름을 하나 이상 입력합니다. Windows 서비스 목록에서 소프트웨어 애플리케이션 이름을 선택할 수 있습니다. 워크로드에서 소프트웨어 인벤토리 검색이 정상적으로 완료되면 이 목록에 테넌트의 모든 에이전트가 입력됩니다. 목록에 없는 소프트웨어 애플리케이션 이름을 추가할 수도 있습니다. 워크로드에서 소프트웨어 인벤토리 검색을 수행하지 않은 경우에는 이 옵션만 사용 가능합니다.
설치 상태	업데이트할 소프트웨어의 상태(설치됨, 설치되지 않음, 업데이트됨)를 지정합니다. 사용 가능한 값은 다음과 같습니다. • **설치됨** - 기본값입니다. 이 값을 선택하는 경우 워크로드에 새 소프트웨어 애플리케이션이 설치되면 모니터에서 경보를 생성합니다. • **업데이트됨** - 이 값을 선택하는 경우 소프트웨어 애플리케이션이 업데이트될 때 모니터가 경보를 생성합니다. • **설치되지 않음** - 이 값을 선택하는 경우 모니터는 소프트웨어 애플리케이션이 워크로드에서 설치 제거되거나 사용할 수 없을 때 경보를 생성합니다.

마지막 시스템 다시 시작 모니터의 설정

마지막 시스템 다시 시작은 워크로드를 마지막으로 다시 시작한 시간을 모니터링합니다.

모니터에 대해 다음 설정을 구성할 수 있습니다.

© Acronis International GmbH, 2003-2024

설정	설명
워크로드가 다시 시작되지 않은 기간	워크로드를 마지막으로 다시 시작한 이후 경과된 기간(일)입니다. 여기서 지정하는 기간보다 오랫동안 워크로드가 다시 시작되지 않은 경우 시스템이 경보를 생성합니다. 1~180(일) 사이의 정수 값을 입력합니다. 기본값은 30입니다.

Windows 이벤트 로그 모니터의 설정

Windows 이벤트 로그는 Windows 이벤트 로그에서 업무상 중요한 특정 이벤트를 모니터링합니다.

모니터에 대해 다음 설정을 구성할 수 있습니다.

설정	설명
이벤트 로그 이름	Windows 이벤트 뷰어에서 사용 가능한 Windows 이벤트 로그 목록에서 특정 이벤트 로그를 선택합니다. 사용 가능한 값은 다음과 같습니다. • **임의** - 기본값입니다. • **애플리케이션** • **보안** • **시스템**
이벤트 소스	이벤트 원본 이름 테넌트의 모든 에이전트에서 수집된 이벤트 원본 목록에서 값을 선택할 수도 있고 새 원본 이름을 수동으로 입력할 수도 있습니다. 테넌트의 소프트웨어 인벤토리가 비활성화되어 있으면 이벤트 원본 목록은 비어 있습니다.
일치 모드	이 필드에서는 임의 또는 모두 연산자를 사용하여 **이벤트 ID**, **이벤트 유형** 및 **이벤트 설명** 설정 연결 여부를 지정할 수 있습니다. 사용 가능한 값은 다음과 같습니다. • **임의** - 기본값입니다.선택한 기준 중 하나라도 일치하면 경보가 생성됩니다. • **모두** - 선택한 기준이 모두 일치해야 경보가 생성됩니다.
이벤트 ID	이벤트 ID를 하나 이상 쉼표로 구분하여 입력합니다. 이 필드에 입력한 이벤트 코드가 이벤트 로그에서 확인되면 시스템이 경보를 생성합니다.
이벤트 유형	모니터링할 이벤트 유형을 하나 이상 선택합니다. 사용 가능한 값은 다음과 같습니다. • **임의** - 기본값입니다. • **오류** • **경고**

© Acronis International GmbH, 2003-2024

설정	설명
	• **정보** • **성공-감사** • **실패-감사**
이벤트 설명	이벤트 설명에서 검색할 특정 키워드나 구를 입력합니다. 각 키워드나 구는 쉼표로 구분하고 따옴표로 묶어 입력해야 합니다. 입력한 키워드나 구가 확인되면 시스템이 경보를 생성합니다.
발생 수	시스템에서 경보가 생성되려면 일정 기간 동안 이벤트가 로그에서 발생해야 하는 최소 횟수입니다. 1~1000 사이의 정수 값을 입력합니다.
기간	메트릭 값이 지정된 기간 동안 정상 범위를 벗어나는 경우에만 시스템에서 감지된 문제 관련 경보를 생성합니다. 정수 값을 입력하고 단위를 분이나 시간 중에서 선택합니다. 기본값은 60분입니다.

파일 및 폴더 크기 모니터의 설정

파일 및 폴더 크기는 선택한 파일이나 폴더의 총 크기를 모니터링합니다.

모니터에 대해 다음 설정을 구성할 수 있습니다.

설정	설명
모니터링할 파일 또는 폴더	모니터링할 파일이나 폴더의 경로입니다. 모니터링에서 제외할 파일이나 폴더를 지정할 수도 있습니다. 다음 와일드카드를 사용할 수 있습니다. • *- 파일이나 폴더 이름에 포함된 문자 0개 이상 • ?- 파일이나 폴더 이름에 포함된 정확히 하나의 문자 Windows 워크로드: • 전체 경로는 드라이브 문자로 시작해야 하며 뒤에 :\ 구분 기호가 있어야 합니다. • 경로 구분 기호 문자로 슬래시나 백슬래시를 사용할 수 있습니다. • 파일이나 폴더 이름은 공백이나 마침표로 끝날 수 없습니다. macOS 워크로드: • 전체 경로는 루트 디렉토리로 시작해야 합니다. • 경로 구분 기호 문자로 슬래시를 사용할 수 있습니다. • 파일이나 폴더 이름은 공백이나 마침표로 끝날 수 없습니다. 제외 필터를 적용할 특정 위치를 반드시 지정해야 하는 것은 아닙니다. 특정 위치를 지정하지 않고 입력하는 파일은 모니터링되는 폴더에서 제외됩니다.
연산자	연산자는 메트릭의 성능 측정 방법을 정의하는 조건부 함수입니다.

© Acronis International GmbH, 2003-2024

설정	설명
	사용 가능한 값은 다음과 같습니다. • **이상** - 기본값입니다. • **보다 작음**
임계값	임계값과 **연산자** 값에 따라 모니터링되는 메트릭의 정상 성능이 결정됩니다. 모니터링되는 메트릭의 값이 정상 범위를 벗어나면 시스템에서 경보를 생성합니다. 정수 값(MB)을 입력합니다.
기간	메트릭 값이 지정된 기간 동안 정상 범위를 벗어나는 경우에만 시스템에서 감지된 문제 관련 경보를 생성합니다. 10~60(분) 사이의 정수 값을 입력합니다. 기본값은 10입니다.

Windows 업데이트 상태 모니터의 설정

Widows 업데이트 상태는 워크로드의 Windows 업데이트 상태와 최신 업데이트 설치 여부를 모니터링합니다.

이 모니터를 활성화하면 시스템이 다음과 같은 경우에 경보를 생성합니다.

- 워크로드에서 Windows 업데이트가 비활성화되어 있는 경우.
- 워크로드에서 Windows 업데이트가 활성화되어 있기는 하지만 최신 업데이트는 설치되지 않은 경우.

방화벽 상태 모니터의 설정

방화벽 상태는 워크로드에 설치되어 있는 기본 제공 또는 서드 파티 방화벽을 모니터링합니다.

이 모니터를 활성화하면 시스템이 다음과 같은 경우에 경보를 생성합니다.

- 기본 제공 OS 방화벽(Windows Defender 방화벽 또는 macOS 방화벽)이 비활성화되어 있으며 실행 중인 타사 방화벽이 없는 경우.
- 공개 네트워크에서 Windows Defender 방화벽이 비활성화되어 있는 경우.
- 비공개 네트워크에서 Windows Defender 방화벽이 비활성화되어 있는 경우.
- 도메인 네트워크에서 Windows Defender 방화벽이 비활성화되어 있는 경우.

실패한 로그인 모니터의 설정

실패한 로그인은 워크로드에서 실패한 로그인 시도를 모니터링합니다.

모니터에 대해 다음 설정을 구성할 수 있습니다.

설정	설명
실패한 로그인 시도 임계값	임계값에 따라 모니터링되는 메트릭의 정상 성능 경계가 결정됩니다. 임계값이 초과되면 메트릭 값이 정상 범위를 벗어난 것입니다.

© Acronis International GmbH, 2003-2024

설정	설명
	정수 값을 입력합니다. 기본값은 60입니다.
기간	메트릭 값이 지정된 기간 동안 정상 범위를 벗어나는 경우에만 시스템에서 감지된 문제 관련 경보를 생성합니다. 1~24 사이의 정수 값을 입력하고 단위를 시간이나 일 중에서 선택합니다. 기본값은 12입니다.

안티맬웨어 소프트웨어 상태 모니터의 설정

안티맬웨어 소프트웨어 상태는 워크로드에 설치되어 있는 기본 제공 또는 서드 파티 안티맬웨어 소프트웨어를 모니터링합니다.

이 모니터를 활성화하면 시스템은 다음 상황 중 하나가 확인되는 경우 경보를 생성합니다.

- 워크로드에 안티맬웨어 소프트웨어가 설치되어 있지 않은 경우.
- 안티맬웨어 소프트웨어가 설치는 되어 있지만 실행 중이지는 않은 경우.
- 안티맬웨어 소프트웨어가 설치되어 있고 실행 중이지만 맬웨어 정의가 최신 상태가 아닌 경우.

참고
Windows 및 Windows Server 운영 체제에서 이 조건을 확인합니다.

운영 체제	지원되는 맬웨어 방지 소프트웨어
Windows	• Acronis Cyber Protect • Windows Defender • Symantec Endpoint Security • Norton 360 • Norton Antivirus • SentinelOne • Trend Micro Endpoint Security(Apex One 포함) • Trend Micro Worry-Free Business • McAfee Endpoint Security • McAfee Endpoint Protection for SMB • FireEye Endpoint Security • F-Secure SAFE • F-Secure Client Security • CrowdStrike Falcon • Kaspersky Endpoint Security Cloud • BitDefender Antivirus • Sophos Intercept X Endpoint • Avast Business Antivirus • AVG Antivirus Business Edition • AVG Internet Security Business Edition

© Acronis International GmbH, 2003-2024

운영 체제	지원되는 맬웨어 방지 소프트웨어
	• Panda Endpoint Protection • Tencent PC Manager • Webroot Business Endpoint Protection • ESET Endpoint Security • Avira Antivirus • Comodo Internet Security • Comodo Business Antivirus • K7 Business Security • K7 Total Security • Vipre Endpoint Protection • Total AV
Windows Server	• Acronis Cyber Protect • Windows Defender • ESET Endpoint Security **참고** 모니터는 다른 맬웨어 방지 애플리케이션과 연동될 수 있지만 연동이 보장되지는 않습니다.
macOS	• Acronis Cyber Protect • F-Secure Safe • BitDefender Anti-virus for Mac • Sophos Home • Sophos Endpoint Protection • Avast Security for Mac • AVG AntiVirus for Mac • Webroot SecureAnywhere • ESET Cybersecurity • Avira Antivirus for Mac • Comodo Antivirus for Mac • K7 Antivirus for Mac • Vipre Advanced Security • Total AV for Mac **참고** 모니터는 다른 맬웨어 방지 애플리케이션과 연동될 수 있지만 연동이 보장되지는 않습니다.

자동 실행 기능 상태 모니터의 설정

자동 실행 기능 상태는 이동식 미디어의 자동 실행 기능이 활성화되어 있는지를 모니터링합니다.

© Acronis International GmbH, 2003-2024

보안상 워크로드의 이동식 미디어에서는 자동 실행 기능을 비활성화하는 것이 좋습니다. 이 기능을 활성화하면 시스템이 경보를 생성합니다.

사용자 정의 모니터의 설정

사용자 정의는 스크립트를 실행하여 사용자 정의 객체를 모니터링합니다.

모니터에 대해 다음 설정을 구성할 수 있습니다.

설정	설명
실행할 스크립트	스크립트 저장소의 사전 정의된 스크립트 목록입니다.
예약	스크립트를 실행할 시간 및 스크립트를 실행하려면 충족되어야 하는 추가 조건(선택 사항)입니다. 사용 가능한 값은 다음과 같습니다. • **시간 기준 예약** - 지정된 정확한 시간, 날짜, 주 또는 월에 스크립트가 실행됩니다. 기본값입니다. **예약 유형** - **매시간**, **매일** 또는 **매월** 중에서 선택할 수 있습니다 **날짜 범위 내에서 실행** - 스크립트를 실행할 시간 범위입니다. • **사용자가 시스템에 로그인할 때** - 사용자가 워크로드에 로그인하면 스크립트가 실행됩니다. • **사용자가 시스템에서 로그오프할 때** - 사용자가 워크로드에서 로그아웃하면 스크립트가 실행됩니다. • **시스템 시작 시** – 워크로드의 운영 체제가 시작될 때 스크립트가 실행됩니다. • **시스템이 중단된 경우** - 워크로드가 중단되면 스크립트가 실행됩니다. • **시스템이 온라인인 경우** - 워크로드를 온라인에서 사용할 수 있게 되면 스크립트가 실행됩니다. **시작 조건** - 조건이 충족된 경우에만 지정된 시간이 되거나 지정된 이벤트가 발생하면 작업이 수행됩니다. 조건을 여러 개 선택한 경우에는 모든 조건이 동시에 충족되어야만 작업이 시작됩니다. 기본적으로는 **예약된 작업을 시작하기 위해 절전 또는 최대 절전 모드 방지** 조건이 선택됩니다. **시작 조건이 충족되지 않아도 다음 후에 작업 실행** - 이 조건은 기본적으로 활성화됩니다. 기본값은 1시간입니다.
스크립트를 실행할 계정	스크립트를 실행할 계정입니다. 사용 가능한 값은 다음과 같습니다. • **시스템 계정** - 기본값입니다. • **현재 로그인한 계정**
최대 기간	워크로드에서 스크립트를 실행할 수 있는 최대 기간입니다.

© Acronis International GmbH, 2003-2024

설정	설명
	이 기간 동안 스크립트가 완료되지 않으면 작업은 실패합니다. 1~1440(분) 사이의 정수 값을 입력합니다. 기본값은 3분입니다.
PowerShell 실행 정책	PowerShell 실행 정책입니다. 사용 가능한 값은 다음과 같습니다. • **Undefined** • **AllSigned** • **Bypass** - 기본값입니다. • **RemoteSigned** • **Restricted** • **Unrestricted** 이러한 값에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

모니터링 계획

모니터링 계획은 모니터링 기능을 활성화하고 구성하기 위해 관리 대상 워크로드에 적용하는 계획입니다.

모니터링 계획이 적용되어 있지 않은 워크로드에서는 모니터링 기능을 사용할 수 없습니다.

참고
모니터링 계획에서 구성할 수 있는 설정의 가용성은 테넌트에 적용된 서비스 팩에 따라 달라집니다. 모든 설정에 액세스하려면 Advanced Management 팩을 활성화합니다.

모니터링 계획 생성

모니터링 계획을 생성한 다음 해당 계획에 워크로드를 추가하여 관리 대상 워크로드에서 모니터링 기능을 구성할 수 있습니다.

사전 요구 사항

워크로드에 설치된 에이전트 버전이 모니터링 기능을 지원해야 합니다.

모니터링 계획을 생성하려면

모니터링 계획에서

1. 보호 콘솔에서 **관리** > **모니터링 계획**으로 이동합니다.
2. 두 옵션 중 하나를 사용하여 모니터링 계획을 생성합니다.
   - 목록에 모니터링 계획이 없으면 **생성**을 클릭합니다.
   - 목록에 모니터링 계획이 있으면 **계획 생성**을 클릭합니다.
3. 테넌트에서 Advanced Management 팩이 활성화되어 있는지 여부에 따라 **모니터링 계획 생성** 창에서 다음 작업을 수행합니다.

© Acronis International GmbH, 2003-2024

- 테넌트가 Standard Protection을 사용 중이라면 모니터링 계획에 디스크 공간, 하드웨어 변경, 마지막 시스템 다시 시작, 파일 및 폴더 크기의 4개 모니터가 자동으로 추가됩니다.
- 테넌트에서 Advanced Management 팩이 활성화되어 있으면 템플릿 옵션 중 하나를 선택하고 **다음**을 클릭합니다.

옵션	설명
권장	기본 모니터링 구성을 사용하여 모니터링 계획을 생성하려면 이 옵션을 선택합니다.
사용자 정의	모니터링 계획을 처음부터 생성하려면 이 옵션을 선택합니다.

4. [선택 사항] 계획의 기본 이름을 변경하려면 연필 아이콘을 클릭하고 계획의 이름을 입력한 후 **확인**을 클릭합니다.
5. [선택 사항] 계획에 모니터를 추가하려면 **모니터 추가**를 클릭하고 목록에서 모니터를 클릭한 후 **추가**를 클릭합니다.

   참고
   모니터 설정(기본값)이 자동으로 입력됩니다.
   모니터링 계획에는 같은 유형의 모니터를 3개까지 추가할 수 있습니다. 모니터링 계획에 추가할 수 있는 총 모니터 수는 30개입니다.

6. [선택 사항] 모니터 매개변수 화면에서 모니터와 경보의 기본 설정을 변경하고 **완료**를 클릭합니다.

   참고
   각 모니터에 대해 서로 다른 설정을 구성할 수 있습니다. 자세한 내용은 "구성 가능한 모니터"(934페이지) 및 "모니터링 경보 구성"(971페이지)을(를) 참조하십시오.

7. [선택 사항] 모니터를 삭제하려면 휴지통 아이콘을 클릭한 후에 **삭제**를 클릭합니다.
8. [선택 사항] 계획에 워크로드를 추가하려면:
   a. **워크로드 추가**를 클릭합니다.
   b. 워크로드를 선택하고 **추가**를 클릭합니다.
   c. 호환성 문제를 해결하려는 경우 "모니터링 계획의 호환성 문제 해결"(970페이지) 항목에 설명되어 있는 절차를 진행합니다.
9. **생성**을 클릭합니다.

모든 장치에서

1. 보호 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 모니터링 계획을 적용할 워크로드를 클릭합니다.
3. **보호**를 클릭합니다.
4. 워크로드에 모니터링 계획이 적용되어 있는지 여부에 따라 다음을 수행합니다.
   - 워크로드에 모니터링 계획이 이미 적용되어 있으면 **계획 생성**을 클릭하고 **모니터링**을 선택합니다.

© Acronis International GmbH, 2003-2024

- 워크로드에 모니터링 계획이 적용되어 있지 않으면 **계획 추가**, **계획 생성**을 차례로 클릭하고 **모니터링**을 선택합니다.

5. **모니터링 계획 생성** 창에서 템플릿 옵션 중 하나를 선택하고 **다음**을 클릭합니다.

옵션	설명
권장	기본 모니터링 구성을 사용하여 모니터링 계획을 생성하려면 이 옵션을 선택합니다.
사용자 정의	모니터링 계획을 처음부터 생성하려면 이 옵션을 선택합니다.

6. [선택 사항] 계획의 기본 이름을 변경하려면 연필 아이콘을 클릭하고 계획의 이름을 입력한 후 **확인**을 클릭합니다.
7. [선택 사항] 모니터와 경보의 기본 설정을 변경하려면 새 값을 구성하고 **완료**를 클릭합니다.

   참고
   모니터링 계획에는 같은 유형의 모니터를 3개까지 추가할 수 있습니다. 모니터링 계획에 추가할 수 있는 총 모니터 수는 30개입니다.

8. [선택 사항] 모니터 매개변수 화면에서 모니터와 경보의 기본 설정을 변경하고 **완료**를 클릭합니다.

   참고
   각 모니터에 대해 서로 다른 설정을 구성할 수 있습니다. 자세한 내용은 "구성 가능한 모니터"(934페이지) 및 "모니터링 경보 구성"(971페이지)을(를) 참조하십시오.

9. [선택 사항] 모니터를 삭제하려면 휴지통 아이콘을 클릭한 후에 **삭제**를 클릭합니다.
10. **생성**을 클릭합니다.

모니터링 계획에 워크로드 추가

필요에 따라 모니터링 계획을 생성한 후 해당 계획에 워크로드를 추가할 수 있습니다.

사전 요구 사항

- 사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.
- 워크로드에 설치된 에이전트 버전이 모니터링 기능을 지원해야 합니다.
- 모니터링 계획을 하나 이상 사용할 수 있어야 합니다.

모니터링 계획에 워크로드를 추가하려면

모니터링 계획에서

1. 보호 콘솔에서 **관리** > **모니터링 계획**으로 이동합니다.
2. 모니터링 계획을 클릭합니다.
3. 워크로드에 계획을 이미 적용했는지 여부에 따라 다음을 수행합니다.

© Acronis International GmbH, 2003-2024

- 워크로드에 계획을 아직 적용하지 않았다면 **워크로드 추가**를 클릭합니다.
- 워크로드에 계획을 적용했다면 **워크로드 관리**를 클릭합니다.

4. 목록에서 워크로드를 선택하고 **추가**를 클릭합니다.
5. **저장**을 클릭합니다.
6. 필요한 경우 **확인**을 클릭하여 워크로드에 필요한 서비스 할당량을 적용합니다.

모든 장치에서

1. 보호 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 모니터링 계획을 적용할 워크로드를 클릭합니다.
3. **보호**를 클릭합니다.
4. 워크로드를 추가할 모니터링 계획을 찾아서 **적용**을 클릭합니다.
5. 필요한 경우 **확인**을 클릭하여 워크로드에 필요한 서비스 할당량을 적용합니다.

모니터링 계획 해지

모니터링 계획이 적용된 워크로드에서 해당 계획을 해지할 수 있습니다.

사전 요구 사항

워크로드에 모니터링 계획이 하나 이상 적용되어 있어야 합니다.

모니터링 계획을 해지하려면

1. 보호 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 워크로드를 클릭하고 **보호**를 클릭합니다.
3. 해지할 모니터링 계획의 **추가 작업** 아이콘을 클릭하고 **해지**를 클릭합니다.

자동 대응 조치 구성

경보가 발생한 이벤트에 대해 수행되는 자동 대응 조치는 감지된 이벤트나 인시던트에 대응하여 자동으로 트리거되는 사전 정의된 작업이나 조치입니다. 이러한 조치를 취하면 잠재적 위협을 완화하고 피해를 최소화할 수 있습니다.

경보가 발생한 이벤트에 대해 자동 대응 조치를 하나 이상 구성할 수 있습니다. 자동 대응 조치는 모니터당 20개까지 구성할 수 있습니다.

자동 대응 조치 구성 방법

1. 보호 콘솔에서 **관리** > **모니터링 계획**으로 이동합니다.
2. 자동 대응 조치를 구성할 모니터링 계획을 선택합니다.
3. 자동 대응 조치를 구성할 모니터를 선택하거나, 모니터를 아직 추가하지 않았다면 **모니터 추가**를 클릭하고 목록에서 모니터를 클릭한 후에 **추가**를 클릭하고 모니터를 선택합니다.
4. **자동 대응 조치** 옆의 링크를 클릭합니다.
5. **자동 대응 조치** 창에서 경보가 트리거되면 자동 수행할 대응 조치를 하나 이상 추가합니다.
6. 각 대응 조치를 구성합니다. 예를 들어 **Windows 서비스 시작** 대응 조치를 추가했다면 다음을 수행합니다.

© Acronis International GmbH, 2003-2024

a. **Windows 서비스** 옆의 **지정**을 클릭합니다.
b. **서비스** 필드에서 대응 조치로 시작할 서비스를 선택합니다.
c. **완료**를 클릭합니다.

7. 추가한 모든 대응 조치가 표시된 목록에서 위쪽 및 아래쪽 화살표나 끌어서 놓기를 사용하여 대응 조치의 순서를 설정합니다.
8. 이전 대응 조치가 실패하는 경우 후속 대응 조치를 처리할 방법을 구성합니다. 다음 중 하나를 선택합니다.
   a. **다음 대응 조치 계속 진행**.
   b. **다음 대응 조치를 계속 진행하지 않음**.
9. **완료**를 클릭합니다.

   모니터링 계획의 **자동 대응 조치** 설정 옆에 구성한 작업 수가 표시됩니다. 나중에 언제든지 이러한 작업을 편집하거나 삭제할 수도 있고 새 작업을 추가할 수도 있습니다.

모니터링 설정에서 사용 가능한 모든 자동 대응 조치와 해당 설명이 아래 표에 나와 있습니다.

자동 대응 조치	설명	지원되는 OS
스크립트 실행	이 조치를 추가하면 다음 작업을 수행할 수 있습니다. 1. 워크로드에서 실행할 특정 스크립트 선택. 2. 스크립트를 실행할 계정 지정. 3. 작업의 최대 기간 지정. 4. PowerShell 실행 정책 지정. 5. 스크립트 실행. 이 작업을 수행하려면 워크로드용 Advanced Management 팩 라이선스(아직 할당되지 않은 경우)가 필요합니다. 조건이 충족되면 시스템은 지정된 매개변수를 사용하여 선택한 원격 스크립트를 실행합니다.	Windows, macOS
워크로드 다시 시작	이 조치를 추가하면 조건 충족 시 시스템이 워크로드를 원격으로 다시 시작합니다.	Windows, macOS
프로세스 중지	이 조치를 추가하면 프로세스 이름을 수동으로 입력하여 프로세스 중지를 지정할 수 있습니다. 조건이 충족되면 시스템은 프로세스를 중지합니다.	Windows, macOS
Windows 서비스 시작	이 조치를 추가하면 에이전트에서 입력된 동적 서비스 목록에서 시작할 Windows 서비스를 선택할 수 있습니다. 조건이 충족되면 시스템은 해당 서비스를 시작합니다.	Windows

© Acronis International GmbH, 2003-2024

자동 대응 조치	설명	지원되는 OS
Windows 서비스 중지	이 조치를 추가하면 에이전트에서 입력된 동적 서비스 목록에서 중지할 Windows 서비스를 선택할 수 있습니다. 조건이 충족되면 시스템은 해당 서비스를 중지합니다.	Windows
Windows 업데이트 활성화	이 조치를 추가하면 조건 충족 시 시스템이 Windows 업데이트를 활성화합니다. 이 조치는 Windows 업데이트 상태 모니터에만 사용 가능합니다.	Windows
이동식 드라이브에서 자동 실행 비활성화	이 조치를 추가하면 조건 충족 시 시스템이 워크로드의 이동식 스토리지 미디어에서 자동 실행 기능을 비활성화합니다. 이 조치는 자동 실행 기능 상태 모니터에만 사용 가능합니다.	Windows

모니터링 계획 관련 추가 작업

모니터링 계획 화면에서는 모니터링 계획과 관련하여 세부 정보 보기, 편집, 활동 보기, 경보 보기, 이름 변경, 활성화, 비활성화, 복제, 내보내기 및 삭제와 같은 추가 작업을 수행할 수 있습니다.

상세 정보 보기

모니터링 계획의 상세정보를 확인하려면

1. **모니터링 계획** 화면에서 모니터링 계획의 **추가 작업** 아이콘을 클릭합니다.
2. **상세 정보 보기**를 클릭합니다.
3. [선택 사항] 계획에서 활성화된 모니터의 상세정보를 확인하려면 모니터 이름을 클릭합니다.

편집

사전 요구 사항

사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

계획을 편집하려면

1. **모니터링 계획** 화면에서 모니터링 계획의 **추가 작업** 아이콘을 클릭합니다.
2. **편집**을 클릭합니다.
3. [선택 사항] 계획에서 모니터를 삭제하려면 모니터 이름 오른쪽에 있는 휴지통 아이콘을 클릭합니다.
4. [선택 사항] 계획에서 모니터를 활성화하거나 비활성화하려면 모니터 이름 옆의 토글을 사용합니다.
5. [선택 사항] 모니터 매개변수를 편집하려면 다음을 수행합니다.

© Acronis International GmbH, 2003-2024

a. 모니터 이름을 클릭합니다.
b. 모니터 매개변수의 개요를 클릭합니다.
c. **모니터 매개변수** 화면에서 매개변수를 구성하고 **완료**를 클릭합니다.

> **참고**
> 각 모니터에 대해 서로 다른 설정을 구성할 수 있습니다. 자세한 내용은 "구성 가능한 모니터"(934페이지) 및 "모니터링 경보 구성"(971페이지)을(를) 참조하십시오.

d. 변경 사항을 확인하고 화면을 닫습니다.

6. [선택 사항] 모니터를 추가하려면 **모니터 추가**를 클릭하고 필요한 경우 이전 단계의 설명대로 매개변수를 편집합니다.
7. **저장**을 클릭합니다.

작업

모니터링 계획 관련 작업을 확인하려면

1. **모니터링 계획** 화면에서 모니터링 계획의 **추가 작업** 아이콘을 클릭합니다.
2. **작업**을 클릭합니다.
3. 활동을 클릭하면 해당 활동 관련 추가 상세 정보를 확인할 수 있습니다.

경보

경보를 확인하려면

1. **모니터링 계획** 화면에서 모니터링 계획의 **추가 작업** 아이콘을 클릭합니다.
2. **경보**를 클릭합니다.

이름 변경

사전 요구 사항

사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

모니터링 계획 이름을 변경하려면

1. **모니터링 계획** 화면에서 모니터링 계획의 **추가 작업** 아이콘을 클릭합니다.
2. **이름 변경**을 클릭합니다.
3. 계획의 새 이름을 입력하고 **확인**을 클릭합니다.

활성화

사전 요구 사항

- 사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.
- 워크로드 하나 이상에 모니터링 계획이 적용되어 있어야 합니다.

모니터링 계획을 활성화하려면

1. **모니터링 계획** 화면에서 모니터링 계획의 **추가 작업** 아이콘을 클릭합니다.
2. **활성화**를 클릭합니다.

© Acronis International GmbH, 2003-2024

비활성화

사전 요구 사항

사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

모니터링 계획을 비활성화하려면

1. **모니터링 계획** 화면에서 모니터링 계획의 **추가 작업** 아이콘을 클릭합니다.
2. **비활성화**를 클릭합니다.

복제

사전 요구 사항

사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

모니터링 계획을 복제하는 방법

1. **모니터링 계획** 화면에서 모니터링 계획의 **추가 작업** 아이콘을 클릭합니다.
2. **복제**를 클릭합니다.
3. **생성**을 클릭합니다.

내보내기

사전 요구 사항

사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

모니터링 계획을 내보내는 방법

1. **모니터링 계획** 화면에서 모니터링 계획의 **추가 작업** 아이콘을 클릭합니다.
2. **내보내기**를 클릭합니다.
   계획 구성은 JSON 형식으로 로컬 머신에 내보내집니다.

삭제

사전 요구 사항

사용자 계정에 대해 2FA가 활성화되어 있어야 합니다.

모니터링 계획을 삭제하려면

1. **모니터링 계획** 화면에서 모니터링 계획의 **추가 작업** 아이콘을 클릭합니다.
2. **삭제**를 클릭합니다.
3. **확인**을 선택하고 **삭제**를 클릭합니다.

모니터링 계획의 호환성 문제

워크로드에 모니터링 계획을 적용하면 호환성 문제가 발생하는 경우도 있습니다. 다음과 같은 호환성 문제가 발생할 수 있습니다.

© Acronis International GmbH, 2003-2024

- 호환되지 않는 운영 체제 - 워크로드의 운영 체제가 지원되지 않으면 이 문제가 표시됩니다.
- 지원되지 않는 에이전트 - 워크로드의 보호 에이전트 버전이 오래되어 모니터링 기능을 지원하지 않으면 이 문제가 표시됩니다.
- 부족한 할당량 - 테넌트의 서비스 할당량이 선택한 워크로드에 할당하기에 충분하지 않으면 이 문제가 표시됩니다.

모니터링 계획을 개별적으로 선택된 워크로드(최대 150개)에 적용하면 계획을 저장하기 전에 기존 충돌을 해결하라는 메시지가 표시됩니다. 충돌을 해결하려면 충돌의 근본 원인을 제거하거나 영향을 받는 워크로드를 계획에서 제거합니다. 자세한 내용은 "모니터링 계획의 호환성 문제 해결"(970페이지)을(를) 참조하십시오. 충돌을 해결하지 않고 계획을 저장하면 호환되지 않는 워크로드에 대해 계획이 자동으로 비활성화되고 경보가 표시됩니다.

모니터링 계획을 150개가 넘는 워크로드 또는 장치 그룹에 적용하면 계획이 저장된 후 호환성이 검사됩니다. 호환되지 않는 워크로드에 대해서는 계획이 자동으로 비활성화되고 경보가 표시됩니다.

모니터링 계획의 호환성 문제 해결

호환성 문제의 원인에 따라 각기 다른 작업을 수행하여 새 모니터링 계획 생성 프로세스의 일부분으로 호환성 문제를 해결할 수 있습니다.

호환성 문제를 해결하려면

1. **문제 검토**를 클릭합니다.
2. [선택 사항] 계획에서 워크로드를 제거하여 비호환 운영 체제로 인한 호환성 문제를 해결하려면:
   a. **호환되지 않는 운영 체제** 탭에서 제거할 워크로드를 선택합니다.
   b. **계획에서 워크로드 제거**를 클릭합니다.
   c. **제거**를 클릭한 다음 **닫기**를 클릭합니다.
3. [선택 사항] 계획에서 모니터를 비활성화하여 비호환 운영 체제로 인한 호환성 문제를 해결하려면:
   a. **호환되지 않는 운영 체제** 탭에서 제거할 모니터를 선택합니다.
   b. **모니터 비활성화**를 클릭합니다.
   c. **비활성화**를 클릭한 다음 **닫기**를 클릭합니다.
4. [선택 사항] 계획에서 워크로드를 제거하여 지원되지 않는 에이전트의 호환성 문제를 해결하려면:
   a. **지원되지 않는 에이전트** 탭에서 제거할 워크로드를 선택합니다.
   b. **계획에서 워크로드 제거**를 클릭합니다.
   c. **제거**를 클릭한 다음 **닫기**를 클릭합니다.
5. [선택 사항] 에이전트 버전을 업데이트하여 지원되지 않는 에이전트의 호환성 문제를 해결하려면 **에이전트 목록으로 이동**을 클릭합니다.

참고
이 옵션은 고객 관리자만 사용할 수 있습니다.

© Acronis International GmbH, 2003-2024

6. [선택 사항] 계획에서 워크로드를 제거하여 부족한 할당량으로 인한 호환성 문제를 해결하려면:
   a. **부족한 할당량** 탭에서 제거할 워크로드를 선택합니다.
   b. **계획에서 워크로드 제거**를 클릭합니다.
   c. **제거**를 클릭한 다음 **닫기**를 클릭합니다.
7. [선택 사항] 테넌트의 할당량을 늘려 부족한 할당량으로 인한 호환성 문제를 해결하려면:
   a. **부족한 할당량** 탭에서 **관리 포털로 이동**을 클릭합니다.
   b. 고객의 서비스 할당량을 늘립니다.

참고
이 옵션은 파트너 관리자만 사용할 수 있습니다.

머신 러닝 모델 재설정

오래되었거나 유효하지 않은 워크로드의 모델을 재설정할 수 있습니다. 이 작업을 수행하면 이상 현상 기반 모니터링 유형의 모니터가 해당 워크로드를 대상으로 수집한 데이터와 생성된 모델이 삭제됩니다. 그런 후에 워크로드용 머신 러닝 모델 교육이 처음부터 시작됩니다.

워크로드용 머신 러닝 모델을 재설정하려면

1. 보호 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 목록에서 워크로드를 클릭하고 **상세정보** 탭을 클릭합니다.
3. **머신 러닝 모델 재설정** 섹션에서 **재설정**을 클릭합니다.
4. 확인 창에서 **재설정**을 다시 클릭합니다.

모니터링 경보

모니터링 경보는 보호 콘솔에 표시되며, 워크로드의 모니터링된 행동이 정상 범위를 벗어날 때 이메일을 통해 전송됩니다. 이 경보는 조직의 IT 환경에 문제가 발생하는 경우 이해관계자가 가능한 한 빨리 알 수 있도록 합니다.

참고
모니터링 경보를 이메일을 통해 활성화하려면 해당하는 경보 유형에 대해 적어도 하나의 이메일 알림 정책을 구성해야 합니다. 자세한 정보는 "이메일 알림 정책 구성"(978페이지)을(를) 참조하십시오.

모니터링 경보 구성

모니터링 계획에 모니터를 추가할 때나 모니터링 계획에서 이미 제공되는 모니터를 편집할 때 모니터의 경보 설정을 구성할 수 있습니다.

모니터링 경보를 구성하려면

1. **모니터 매개변수** 창에서 **경보 생성** 섹션으로 이동합니다.
2. **경보 심각도**에서 경보 우선 순위에 해당하는 심각도를 선택합니다.

© Acronis International GmbH, 2003-2024

옵션	설명
심각	워크로드 작동 시 중요한 문제와 관련된 경보이며 우선 순위가 가장 높습니다. 이러한 문제는 최대한 빨리 해결해야 합니다.
오류	심각 경보보다 심각도가 낮은 오류 경보는 워크로드에 문제가 있거나 워크로드가 정상적으로 동작하지 않음을 나타냅니다. 더욱 심각한 문제가 발생하지 않도록 문제를 제때 해결해야 합니다.
경고	확인은 해야 하지만 아직 문제를 야기하지는 않는 상황이 있음을 나타내는 오류입니다. 이러한 문제는 중요 및 오류 경보 발생의 원인인 문제를 해결한 후에 해결하면 됩니다. 기본값입니다.
정보	우선 순위가 가장 낮은 경보입니다. 정보 심각도는 문제를 나타내지는 않습니다. 이러한 경보는 모니터링되는 객체 관련 작업에 대한 정보를 제공합니다.

3. **경보 빈도**에서 조건 충족 시 시스템이 경보를 생성하도록 할 빈도를 선택합니다.

옵션	설명
한 번(확인 합격 시까지)	확인이 정상적으로 완료될 때까지 시스템이 경보를 한 번에 하나씩 생성합니다. 기본값입니다.
X회 연속 실패한 후	확인이 X번 연속으로 실패하면 시스템이 경보를 생성합니다. 여기서 X는 정수 값입니다.

4. **경보 메시지**에서 연필 아이콘을 클릭하여 시스템이 경보를 생성할 때 사용되는 기본 경보 메시지를 편집합니다. 변수가 포함된 사용자 정의 경보 메시지를 지정할 수 있습니다. 사용할 수 있는 변수에 대한 자세한 내용은 "모니터링 경보 변수"(972페이지) 항목을 참조하십시오.

   참고
   일부 모니터의 경우에는 경보 메시지를 여러 개 구성할 수 있습니다.

5. 모니터링되는 메트릭이 정상 상태로 돌아가 다시 정상적으로 동작하면 시스템이 자동으로 경보를 해결 처리하도록 하려는 경우 **경보 자동 해결**을 활성화합니다. 해당 설정은 기본적으로 활성화됩니다.

모니터링 경보 변수

모니터별로 각기 다른 경보 변수를 구성할 수 있습니다. 변수는 {{}}로 묶어서 사용해야 합니다.

사용 가능한 변수에 대한 자세한 내용이 아래 표에 나와 있습니다.

변수	설명	사용 가능한 모니터
plan_name	정책의 이름	모든 모니터

© Acronis International GmbH, 2003-2024

변수	설명	사용 가능한 모니터
monitor_name	모니터링 계획의 하위 정책 이름	모든 모니터
workload_name	워크로드의 이름	모든 모니터
threshold_value	경보가 생성되는 특정 모니터링 조건이나 임계값	임계값 기반 모니터링을 지원하는 모든 모니터.
threshold_unit	임계값과 연결된 단위. %, MB, MB/초 등을 예로 들 수 있습니다.	임계값 기반 모니터링을 지원하는 모든 모니터.
time_period	메트릭 값이 지정된 기간 동안 정상 범위를 벗어나는 경우에만 시스템에서 감지된 문제 관련 경보를 생성합니다.	임계값 기반 모니터링을 지원하는 모든 모니터.
time_unit	기간과 연결된 단위(초/분/시/일).	임계값 기반 모니터링을 지원하는 모든 모니터.
anomaly_value	이상 동작 값	이상 현상 기반 모니터링을 지원하는 모든 모니터.
anomaly_unit	이상 동작 값과 연결된 단위	이상 현상 기반 모니터링을 지원하는 모든 모니터.
deviation_value	편차 값	이상 현상 기반 모니터링을 지원하는 모든 모니터.
deviation_unit	편차 값과 연결된 단위	이상 현상 기반 모니터링을 지원하는 모든 모니터.
drive_name	드라이브(Windows) 또는 파티션(macOS)	디스크 공간
CPU_model	모니터링되는 CPU의 모델	CPU 온도
GPU_model	모니터링되는 GPU의 모델	GPU 온도
hardware_model	모니터링되는 컴포넌트의 모델	하드웨어 변경
hardware_component	모니터링되는 하드웨어의 유형	하드웨어 변경
hardware_model_old	모니터링 중이다가 교체된 컴포넌트의 모델	하드웨어 변경

© Acronis International GmbH, 2003-2024

변수	설명	사용 가능한 모니터
hardware_model_new	추가되어 모니터링 중인 새 컴포넌트의 모델	하드웨어 변경
disk_model	디스크의 모델	디스크 전송 속도
network_adapter_model	네트워크 어댑터의 모델	네트워크 사용량
process_name	프로세스의 이름	프로세스별 CPU 사용량 프로세스별 메모리 사용량 프로세스별 디스크 전송 속도 프로세스별 네트워크 사용량 프로세스 상태
service_name	서비스의 이름	Windows 서비스 상태
software_name	소프트웨어 애플리케이션의 이름	설치된 소프트웨어
software_version	소프트웨어 애플리케이션의 버전	설치된 소프트웨어
software_version_old	업데이트 전의 소프트웨어 애플리케이션 버전	설치된 소프트웨어
software_version_new	새로 설치했거나 업데이트한 소프트웨어 애플리케이션의 버전	설치된 소프트웨어
number_of_occurrences	로그에서 이벤트가 표시되는 횟수	Windows 이벤트 로그
event_types	이벤트의 유형	Windows 이벤트 로그
event_source	이벤트의 소스	Windows 이벤트 로그
event_log_name	이벤트의 이름	Windows 이벤트 로그
firewall_software_name	방화벽 소프트웨어의 이름	방화벽 상태
antimalware_software_name	안티맬웨어 소프트웨어의 이름	안티맬웨어 소프트웨어 상태

© Acronis International GmbH, 2003-2024

변수	설명	사용 가능한 모니터
user_name	사용자의 이름	자동 실행 기능 상태
script_name	스크립트의 이름	사용자 정의

수동 대응 조치

경보가 표시되면 경보 발생 이벤트와 관련하여 수행하려는 대응 조치를 선택할 수 있습니다.

수동 대응 조치를 수행하려면

1. 보호 콘솔에서 **경보**로 이동합니다.
2. 확인할 경보를 엽니다.
3. **대응 조치**를 클릭하고 드롭다운 목록에서 대응 조치를 선택합니다.

특정 경보와 관련하여 수행 가능한 대응 조치 목록은 경보 유형, 특정 테넌트에서의 기능 사용 가능 여부 및 워크로드 운영 체제에 따라 달라집니다.

아래 표에 모든 수동 대응 조치와 해당 설명이 참조용으로 나와 있습니다.

수동 대응 조치	설명	지원되는 OS
디스크 공간 사용량 추세 찾아보기	**디스크 공간 사용량** 그래프가 있는 창이 열립니다. 이 창에서 다음 작업을 수행할 수 있습니다. • 시간별(지난 1일/7일/1개월) 디스크 공간 사용량 변화 정보 찾아보기. • 선택한 기간의 디스크 공간 사용량 델타에 해당하는 상대 값(%) 찾아보기.	Windows, macOS
파일 크기 증가 추세 찾아보기	**파일 크기 증가** 그래프가 있는 창이 열립니다. 이 창에서 다음 작업을 수행할 수 있습니다. • 시간별(지난 1일/7일/1개월) 모니터링되는 파일과 폴더의 총 크기 변화 정보 찾아보기. • 선택한 기간의 총 파일 크기 델타에 해당하는 상대 값(%) 찾아보기.	Windows, macOS
스크립트 실행	열리는 창에서 다음 작업을 수행할 수 있습니다. 1. 워크로드에서 실행할 특정 스크립트 선택. 2. 스크립트를 실행할 계정 지정. 3. 작업의 최대 기간 지정. 4. PowerShell 실행 정책 지정. 5. 스크립트 실행. 이 작업을 수행하려면 워크로드용 Advanced	Windows, macOS

© Acronis International GmbH, 2003-2024

수동 대응 조치	설명	지원되는 OS
	Management 팩 라이선스(아직 할당되지 않은 경우)가 필요합니다.	
NEAR를 통해 연결	Acronis Connect 클라이언트에서 원격 연결을 설정합니다.	Windows, macOS
RDP를 통해 연결	Acronis Connect 클라이언트에서 원격 연결을 설정합니다.	Windows
하드웨어 인벤토리 열기	현재 워크로드의 **하드웨어 인벤토리** 탭으로 리디렉션됩니다.	Windows, macOS
CPU를 로드한 10대 프로세스 찾아보기	CPU를 로드했으며 CPU 과열을 야기했을 수 있는 10대 프로세스(경보 생성 시의 시스템 스냅샷)가 나와 있는 창이 열립니다.	Windows, macOS
GPU를 로드한 10대 프로세스 찾아보기	GPU를 로드했으며 GPU 과열을 야기했을 수 있는 10대 프로세스(경보 생성 시의 시스템 스냅샷)가 나와 있는 창이 열립니다.	Windows, macOS
메모리를 로드한 10대 프로세스 찾아보기	메모리를 로드한 10대 프로세스(경보 생성 시의 시스템 스냅샷)가 나와 있는 창이 열립니다.	Windows, macOS
디스크를 로드한 10대 프로세스 찾아보기	디스크를 로드한 10대 프로세스(경보 생성 시의 시스템 스냅샷)가 나와 있는 창이 열립니다.	Windows, macOS
네트워크를 로드한 10대 프로세스 찾아보기	네트워크 인터페이스 어댑터를 로드한 10대 프로세스(경보 생성 시의 시스템 스냅샷)가 나와 있는 창이 열립니다.	Windows, macOS
프로세스별 리소스 사용량 찾아보기	관련 프로세스별 하드웨어 리소스 사용량에 대한 상세 정보가 나와 있는 창이 열립니다. 해당 창에는 CPU 사용량, 메모리 사용량, 디스크 I/O, 네트워크 사용량이 표시됩니다.	Windows, macOS
워크로드 다시 시작	확인 창이 열립니다. 다시 시작을 확인하면 워크로드가 다시 시작됩니다.	Windows, macOS
Windows 서비스 시작	확인 창이 열립니다. 시작을 확인하면 Windows 서비스가 시작됩니다.	Windows
Windows 서비스 중지	확인 창이 열립니다. 중지를 확인하면 Windows 서비스가 중지됩니다.	Windows
프로세스 중지	확인 창이 열립니다. 중지를 확인하면 경보에 나와 있는 프로세스가 중지됩니다.	Windows, macOS
Windows 업데이트 활성화	확인 창이 열립니다. 활성화를 확인하면 Windows 업데이트가 활성화됩니다.	Windows

© Acronis International GmbH, 2003-2024

수동 대응 조치	설명	지원되는 OS
이동식 드라이브에서 자동 실행 기능 비활성화	확인 창이 열립니다. 비활성화를 확인하면 워크로드의 시스템 수준에서 자동 실행 기능이 비활성화됩니다.	Windows

중요
다음의 수동 대응 조치를 수행할 때는 보안 유지를 위해 2단계 인증을 사용해야 합니다.

- 스크립트 실행
- NEAR를 통해 연결
- RDP를 통해 연결
- 워크로드 다시 시작
- Windows 서비스 시작
- Windows 서비스 중지
- 프로세스 중지
- Windows 업데이트 활성화
- 이동식 드라이브에서 자동 실행 기능 비활성화

워크로드에 대한 모니터링 경보 보기

경보 탭에서 특정 워크로드의 모니터링 경보를 볼 수 있으며 다양한 경보 작업을 수행할 수 있습니다.

워크로드에 대한 모니터링 경보를 보는 방법

1. 보호 콘솔에서 **모든 장치**로 이동합니다.
2. 워크로드를 클릭한 다음 **경보** 탭을 선택합니다.
3. [선택 사항] 모니터링 경보 창에서 다음 작업 중 하나를 수행합니다.
   - 경보를 지우려면 **지우기**를 클릭합니다.
   - 대응 조치를 취하려면 **대응 조치**를 클릭한 다음 조치를 클릭합니다.
   - 지원팀에 문의하려면 **지원 받기**를 클릭합니다.
4. [선택 사항] 워크로드에 대한 모든 모니터링 경보를 지우려면 **모두 지우기**를 클릭합니다.

모니터링 경보의 경보 로그 확인

자동이나 수동으로 수행한 대응 조치, 전송된 이메일 알림 등 모니터링 경보와 관련된 모든 이벤트를 시간순으로 확인할 수 있습니다.

모니터링 경보의 감사 로그를 확인하려면

1. 보호 콘솔에서 **경보**로 이동합니다.
2. **테이블 보기**를 엽니다.

© Acronis International GmbH, 2003-2024

3. 경보 목록에서 확인할 모니터링 경보를 클릭합니다.
4. **상세정보**, **경보 로그**를 차례로 클릭합니다.

이메일 알림 정책 구성

이메일 알림 정책은 다른 모니터들로부터 이메일 알림을 받을 사용자를 지정합니다.

이메일 알림 화면에서 추가, 편집, 활성화, 비활성화 및 삭제와 같은 이메일 알림 정책에 대한 작업을 수행할 수 있습니다.

추가

새 이메일 알림 정책을 추가하려면

1. 보호 콘솔에서 **설정** > **이메일 알림**으로 이동합니다.
2. **정책 추가**를 클릭합니다.
3. **수신자 선택**을 클릭합니다.
4. **수신자 선택** 화면에서 이메일 경보를 받고자 하는 사용자를 선택한 다음 **선택**을 클릭합니다.
5. **경보 유형**에서 시스템이 이메일 경보를 보내길 원하는 모니터를 선택합니다.
6. **추가**를 클릭합니다.

편집

이메일 알림 정책을 편집하는 방법

1. 보호 콘솔에서 **설정** > **이메일 알림**으로 이동합니다.
2. 알림 정책의 말줄임표 아이콘을 클릭한 다음 다음 **편집**을 클릭합니다.
3. [선택 사항] 수신자를 변경하려면 **수신자 편집**을 클릭하고, 목록에서 사용자를 추가하거나 제거한 다음 **선택**을 클릭합니다.
4. [선택 사항] **경보 유형**에서 선택한 수신자에게 보낼 모니터링 경보의 유형을 선택합니다.
5. **저장**을 클릭합니다.

활성화

이메일 알림 정책을 활성화하는 방법

1. 보호 콘솔에서 **설정** > **이메일 알림**으로 이동합니다.
2. **이메일 알림** 화면의 이메일 알림 정책에서 **...** 아이콘을 클릭합니다.
3. **활성화**를 클릭합니다.

비활성화

이메일 알림 정책을 비활성화하는 방법

1. 보호 콘솔에서 **설정** > **이메일 알림**으로 이동합니다.
2. **이메일 알림** 화면의 이메일 알림 정책에서 **...** 아이콘을 클릭합니다.
3. **비활성화**를 클릭합니다.

삭제

이메일 알림 정책을 삭제하는 방법

© Acronis International GmbH, 2003-2024

1. 보호 콘솔에서 **설정** > **이메일 알림**으로 이동합니다.
2. **이메일 알림** 화면의 이메일 알림 정책에서 **...** 아이콘을 클릭합니다.
3. **삭제**를 클릭한 다음 **확인**을 클릭합니다.

모니터 데이터 보기

각 워크로드에 적용된 모니터 목록을 볼 수 있으며 모니터의 현재 상태 및 성능 내역 상세정보를 그래픽 보기에서 확인할 수 있습니다. 이 정보를 사용하여 워크로드의 상태와 시간에 따른 상태 변화를 분석할 수 있습니다.

사전 요구 사항

- 워크로드에 모니터링 계획이 적용되어 있어야 합니다.
- 워크로드가 온라인이며 해당 모니터용 데이터가 있어야 합니다.
- 워크로드에 설치된 에이전트 버전이 모니터링 계획을 지원해야 합니다.

워크로드에 적용된 모니터와 모니터 데이터를 확인하려면

1. 보호 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 워크로드를 클릭하고 **모니터링** 탭을 클릭합니다.
   워크로드용으로 활성화된 각 모니터의 위젯이 **모니터링** 탭에 표시됩니다. 각 위젯에는 다음 정보가 표시됩니다.

표시되는 정보	설명
모니터 이름	모니터 이름
마지막 결과	모니터링되는 메트릭의 최신 값 또는 이벤트의 최신 상태
마지막 확인	모니터가 마지막 데이터를 수집한 날짜와 시간
경보	모니터에 의해 생성된 아직 해결되지 않은 경보의 수입니다. 이 모니터에서 생성된 해결되지 않은 경보가 하나라도 있는 경우 그 숫자를 클릭하면 **경보** 탭이 열립니다. 경보가 필터링되며, 이 모니터에 대한 경보만 나열됩니다.

참고
워크로드에 모니터링 계획을 적용하면 15분(또는 모니터에 대해 설정한 최소 모니터 빈도) 후에 위젯이 탭에 표시됩니다.

© Acronis International GmbH, 2003-2024

3. [선택 사항] 모니터 관련 추가 상세정보 및 모니터링되는 메트릭과 관련하여 수집된 내역 데이터(해당하는 경우)를 확인하려면 모니터의 위젯에서 말줄임표 아이콘을 클릭하고 **상세정보**를 클릭합니다.

   위젯에서 확인할 수 있는 모니터 상세정보에 대한 자세한 내용은 "모니터 위젯"(980페이지) 항목을 참조하십시오.

모니터 위젯

모니터 위젯에서는 모니터와 관련된 다음 상세정보를 확인할 수 있습니다.

세부정보	설명
모니터링 계획	모니터가 포함된 모니터링 계획의 이름. 모니터링 계획의 이름 링크를 클릭하면 해당 모니터링 계획이 보기 모드에서 열립니다.
모니터 빈도	모니터가 워크로드에서 데이터를 수집하는 시간 간격
마지막 결과	모니터링되는 메트릭의 최신 값 또는 이벤트의 최신 상태
마지막 확인	모니터가 마지막 데이터를 수집한 날짜와 시간
마지막 경보	마지막 경보가 생성된 날짜와 시간. 모니터와 관련하여 경보가 하나 이상 생성된 경우에만 이 필드가 표시됩니다.
과거 내역 그래프	시계열 데이터를 수집하는 모니터의 경우 위젯은 선택된 기간(1시간, 6시간, 12시간, 1일, 1주, 또는 1개월)에 대한 과거 내역 데이터를 그래픽 뷰로 표시합니다. 그래프는 사용자가 선택한 기간 동안의 지표 실제 값들을 표시합니다. 에이전트가 클라우드로 수집된 데이터를 전송하지 않은 경우에는 누락된 값이 점선으로 표시됩니다. 누락된 값 앞뒤의 실제 값과 데이터 요소가 해당 점선으로 연결됩니다. **이상 현상 기반** 모니터링을 사용하는 모니터의 경우에는 기준 영역, 메트릭의 실제 값이 표시되는 선 및 이상 현상이 그래프에 표시됩니다. 이상 현상은 기준 범위를 벗어나는 값이나 급격한 값 증가 현상이며, 그래프에서 빨간색 점으로 표시됩니다. 그래프를 마우스로 가리키면 특정 시간의 실제 값과 임계값을 확인할 수 있습니다.

© Acronis International GmbH, 2003-2024

세부 정보	설명
	 참고 그래프의 데이터는 로컬 시스템의 시간대로 표시됩니다. 즉, 보호 콘솔에 액세스하는 워크로드의 브라우저 시간대가 사용됩니다.

© Acronis International GmbH, 2003-2024

추가 Cyber Protection 도구

규제 준수 모드

일반적인 수준보다 더 높은 보안 관련 요구를 충족해야 하는 고객은 규제 준수 모드를 사용할 수 있습니다. 이 모드에서는 모든 백업을 암호화해야 하며 로컬에서 설정한 암호화 암호만 사용 가능합니다.

규제 준수 모드에서는 고객 테넌트 및 해당 단위에서 생성하는 모든 백업이 AES 알고리즘과 256비트 키를 사용하여 자동 암호화됩니다. 사용자는 암호화 암호를 보호되는 장치에서만 설정할 수 있으며 보호 계획에서는 설정할 수 없습니다.

중요
규제 준수 모드는 비활성화할 수 없습니다.

제한 사항

- 규제 준수 모드는 버전이 15.0.26390 이상의 에이전트 버전과만 호환됩니다.
- Red Hat Enterprise Linux 4.x 또는 5.x 버전과 해당 파생 버전을 실행하는 장치에서는 규제 준수 모드를 사용할 수 없습니다.
- 클라우드 서비스는 암호화 암호에 액세스할 수 없습니다. 이 제한으로 인해 규제 준수 모드가 적용된 테넌트에서는 일부 기능을 사용할 수 없습니다.

지원되지 않는 기능

규제 준수 모드가 설정된 테넌트에 사용할 수 없는 기능은 다음과 같습니다.

- Cyber Protect 콘솔을 통한 복구
- Cyber Protect 콘솔을 통해 파일 수준에서 백업 찾아보기
- 클라우드 간 백업
- 웹 사이트 백업
- 애플리케이션 백업
- 모바일 장치 백업
- 백업 맬웨어 방지 스캔
- 안전 복구
- 회사 허용 목록 자동 생성
- 데이터 보호 맵
- 재해 복구
- 사용 불가능 기능 관련 보고서 및 대시보드

암호화 비밀번호 설정

암호화 비밀번호는 보호된 장치에서 로컬로 설정해야 합니다. 보호 계획에서 암호화 비밀번호를 설정할 수는 없습니다. 암호가 없으면 백업 생성이 실패합니다.

© Acronis International GmbH, 2003-2024

경고!
비밀번호를 잃어버리거나 기억나지 않으면 암호화된 백업을 복구할 방법이 없습니다.

다음과 같은 방법으로 암호화 비밀번호를 설정할 수 있습니다.

1. 보호 에이전트 설치 중에 설정(Windows, macOS, Linux에 해당됨).
2. 명령줄을 사용하여 변경(Windows 및 Linux에 해당됨).
   이것이 가상 어플라이언스에서 암호화 암호를 설정하는 유일한 방법입니다.
   Acropsh 도구를 사용하여 암호화 비밀번호를 설정하는 방법에 대한 자세한 내용은 "암호화"(402페이지)을(를) 참조하십시오.
3. Cyber Protect Monitor에서 변경(Windows 및 macOS에 해당됨).

Cyber Protect Monitor에서 암호화 비밀번호를 설정하려면

1. 보호된 장치에서 관리자로 로그온합니다.
2. 알림 영역(Windows) 또는 메뉴 모음(macOS)에서 Cyber Protect Monitor 아이콘을 클릭합니다.
3. 기어 아이콘을 클릭합니다.
4. **암호화**를 클릭합니다.
5. 암호화 비밀번호를 설정합니다.
6. **확인**을 클릭합니다.

암호화 비밀번호 변경

보호 계획이 백업을 생성하기 전에 암호화 비밀번호를 변경할 수 있습니다.

백업이 생성된 후에는 암호화 암호를 변경하지 않는 것이 좋습니다. 이렇게 하면 후속 백업이 실패합니다. 같은 머신을 계속 보호하려면 해당 머신용으로 새 보호 계획을 생성해야 합니다. 암호화 비밀번호와 보호 계획을 모두 변경하면 변경된 비밀번호로 암호화된 새 백업이 생성됩니다. 이러한 변경 이전에 생성된 백업은 그대로 유지됩니다.

적용된 보호 계획을 그대로 유지하고 해당 계획 내의 백업 파일 이름만 변경할 수도 있습니다. 이 경우에도 변경된 비밀번호로 암호화된 새 백업이 생성됩니다. 백업 파일 이름에 대해 자세히 알아보려면 "백업 파일 이름"(410페이지)을(를) 참조하십시오.

다음과 같은 방법으로 암호화 비밀번호를 변경할 수 있습니다.

1. Cyber Protect Monitor에서 변경(Windows 및 macOS에 해당됨).
2. 명령줄을 사용하여 변경(Windows 및 Linux에 해당됨).
   Acropsh 도구를 사용하여 암호화 비밀번호를 설정하는 방법에 대한 자세한 내용은 "암호화"(402페이지)을(를) 참조하십시오.

규제 준수 모드로 설정된 테넌트의 백업 복구

규제 준수 모드에서는 Cyber Protect 콘솔에서 백업을 복구할 수 없습니다.

다음 옵션을 사용할 수 있습니다.

© Acronis International GmbH, 2003-2024

- 부트 가능한 미디어를 사용하여 전체 머신, 디스크 또는 파일 복구.
- Windows 파일 탐색기를 사용하여 에이전트가 설치된 Windows 머신의 로컬 백업에서 파일 추출.

변경 불가 스토리지

변경 불가능 스토리지 사용 시에는 지정된 보존 기간 동안 삭제된 백업에 액세스할 수 있습니다. 이러한 백업의 내용을 복구할 수는 있지만 백업을 변경, 이동, 삭제할 수는 없습니다. 보존 기간이 끝나면 삭제된 백업은 영구적으로 삭제됩니다.

변경 불가능 스토리지에는 다음 백업이 포함됩니다.

- 수동으로 삭제하는 백업.
- 보호 계획의 **보관 기간** 섹션 또는 정리 계획의 **보존 규칙** 섹션 내 설정에 따라 자동으로 삭제되는 백업.

변경 불가능 스토리지에서 삭제된 백업은 계속 스토리지 공간을 사용하며, 그에 따라 요금이 청구됩니다.

삭제된 테넌트는 변경 불가능 스토리지를 포함한 모든 스토리지에 대해 청구되지 않습니다.

변경 불가능 스토리지 모드

고객 테넌트에서 변경 불가능 스토리지를 사용할 수 있는 모드는 다음과 같습니다.

변경 불가능 스토리지를 사용할 수 있는 모드는 다음과 같습니다.

- **거버넌스 모드**
  변경 불가능 스토리지를 비활성화하고 다시 활성화할 수 있습니다. 보존 기간을 변경하거나 규제 준수 모드로 전환할 수 있습니다.
- **규제 준수 모드**

  경고!
  규제 준수 모드 선택은 되돌릴 수 없습니다.

  변경 불가능 스토리지를 비활성화할 수 없습니다. 보존 기간을 변경하거나 거버넌스 모드로 다시 전환할 수 없습니다.

지원되는 스토리지 및 에이전트

- 변경 불가능한 스토리지는 클라우드 스토리지에서만 지원됩니다.
  변경 불가능한 스토리지는 Acronis Cyber Infrastructure 버전 4.7.1 이상을 사용하는 Acronis 호스팅 및 파트너 호스팅 클라우드 스토리지에 사용할 수 있습니다.
  Acronis Cyber Infrastructure Backup Gateway와 함께 사용할 수 있는 모든 스토리지가 지원됩니다. Acronis Cyber Infrastructure 스토리지, Amazon S3 및 EC2 스토리지, Microsoft Azure 스토리지 등을 예로 들 수 있습니다.

© Acronis International GmbH, 2003-2024

변경 불가능 스토리지는 Acronis Cyber Infrastructure에서 Backup Gateway 서비스에 대해 TCP 포트 40440이 열려 있어야 합니다. 버전 4.7.1 이상에서는 TCP 포트 40440이 **Backup(ABGW) Public** 트래픽 유형으로 자동으로 열립니다. 트래픽 유형에 대한 자세한 정보는 Acronis Cyber Infrastructure 문서를 참조하십시오.

- 변경 불가 스토리지를 사용하려면 보호 에이전트 버전 21.12(빌드 15.0.28532) 이상이 필요합니다.
- TIBX(버전 12) 백업만 지원됩니다.

변경 불가능 스토리지 활성화

Cyber Protect 콘솔 또는 관리 포털에서 변경 불가능 스토리지 설정을 구성할 수 있습니다. 둘 다 동일한 설정에 액세스를 제공합니다. 아래의 절차는 Cyber Protect 콘솔을 사용합니다. 관리 포털에서 변경 불가능 스토리지 설정을 구성하는 방법을 알아보려면 관리자 안내서의 변경 불가능 스토리지 구성을 참조하십시오.

변경 불가능 스토리지 설정을 구성하려면 관리자 계정이 속하는 테넌트에서 2단계 인증을 사용해야 합니다.

변경 불가 스토리지를 활성화하려면

1. Cyber Protect 콘솔에 관리자로 로그인합니다.
2. **설정** > **시스템 설정**으로 이동합니다.
3. 기본 백업 옵션 목록을 스크롤하여 **변경 불가 스토리지**를 클릭합니다.
4. **변경 불가 스토리지** 스위치를 활성화합니다.
5. 14~3650일 사이의 보존 기간을 지정합니다.
   기본 보관 기간은 14일입니다. 보존 기간이 길수록 스토리지 사용량도 많아집니다.
6. 변경 불가능 스토리지 모드를 선택한 다음 필요한 경우 선택 사항을 확인하십시오.
   거버넌스 모드에서는 변경 불가능 스토리지를 활성화하거나 비활성화하고 보존 기간을 변경할 수 있습니다. 거버넌스 모드에서 규제 준수 모드로 전환할 수 있습니다.

   경고!
   규제 준수 모드로 전환하는 것은 되돌릴 수 없습니다. 규제 준수 모드를 선택한 후에는 변경 불가능 스토리지를 비활성화하거나 모드 또는 보존 기간을 변경할 수 없습니다.

7. **저장**을 클릭합니다.
8. 기존 아카이브가 변경 불가능 스토리지를 지원하도록 설정하려면 해당 아카이브에서 새 백업을 생성합니다.
   새 백업을 생성하려면 보호 계획을 수동으로 실행하거나 스케줄에 따라 실행합니다.

   경고!
   아카이브가 변경 불가능 스토리지를 지원하도록 설정하기 전에 삭제하는 백업은 영구적으로 삭제됩니다.

© Acronis International GmbH, 2003-2024

변경 불가능 스토리지 비활성화

참고
거버넌스 모드에서만 변경 불가능 스토리지를 비활성화 할 수 있습니다.

변경 불가 스토리지를 비활성화하려면

1. Cyber Protect 콘솔에 관리자로 로그인합니다.
2. 탐색 메뉴에서 **설정** > **시스템 설정**을 클릭합니다.
3. 기본 백업 옵션 목록을 스크롤하여 **변경 불가 스토리지**를 클릭합니다.
4. **변경 불가 스토리지** 스위치를 비활성화합니다.
5. **비활성화**를 클릭하여 선택을 확인합니다.

경고!
변경 불가능 스토리지 비활성화는 즉시 적용되지 않습니다. 즉, 유예 기간인 14일 동안은 변경 불가능 스토리지가 계속 활성 상태로 유지되므로 원래 보존 기간에 따라 삭제된 백업에 액세스할 수 있습니다. 유예 기간이 끝나면 변경 불가능 스토리지의 모든 백업은 영구적으로 삭제됩니다.

변경 불가 스토리지에서 삭제된 백업 액세스

보존 기간 동안 삭제된 백업에 액세스하여 해당 백업에서 데이터를 복구할 수 있습니다.

참고
삭제된 백업에 대한 액세스 권한을 허용하려면 백업 스토리지의 40440 포트를 수신 연결을 위해 활성화해야 합니다.

삭제된 백업에 액세스하려면

1. **백업 스토리지** 탭에서 삭제된 백업이 포함되어 있는 클라우드 스토리지를 선택합니다.
2. [삭제된 아카이브에만 해당됨] 삭제된 아카이브를 보려면 **삭제된 항목 표시**를 클릭합니다.
3. 복구하려는 백업이 포함된 아카이브를 선택합니다.
4. **백업 표시**를 클릭하고 **삭제된 항목 표시**를 클릭합니다.
5. 복구할 백업을 선택합니다.
6. "복구"(451페이지)의 설명대로 복구 작업을 진행합니다.

지역 중복 스토리지

지역 중복 스토리지 사용 시에는 데이터가 주 위치와 멀리 떨어져 있는 보조 위치에 비동기식으로 복사되므로 데이터 내구성이 높아집니다. 이처럼 데이터가 여러 지역에 중복 저장되므로 주 위치를 사용할 수 없게 되더라도 데이터에 액세스할 수 있습니다.

중요
복제된 데이터는 원래 데이터와 동일한 양의 스토리지 공간을 사용합니다.

© Acronis International GmbH, 2003-2024

지역 중복 스토리지 활성화 및 비활성화

사전 요구 사항

- 지역 중복 스토리지는 파트너 관리자가 관리 포털이나 API를 통해 활성화해야 Cyber Protect 콘솔에서 사용 가능합니다.
- 관리자만 Cyber Protect 콘솔에서 지역 중복 스토리지를 활성화하거나 비활성화할 수 있습니다. 지역 중복 스토리지를 활성화하거나 비활성화하려면 관리자 권한이 있는지 확인하십시오.

지역 중복 스토리지를 활성화하려면

1. [API를 통해 지역 중복 스토리지를 활성화한 경우만 해당됨] 상단 "클라우드의 모든 데이터에 대해 지역 중복 기능 사용 가능"의 경보에서 **Geo-redundant Cloud Storage 활성화**를 클릭합니다.
2. Cyber Protect 콘솔에서 **설정** > **시스템 설정**으로 이동합니다.
3. 기본 백업 옵션 목록을 스크롤하여 **Geo-redundant Cloud Storage**를 클릭합니다.
4. **Geo-redundant Cloud Storage** 스위치를 활성화합니다.
5. **저장**을 클릭합니다.
   이제 데이터가 보조 위치로 복제되므로 주 위치에서 장애가 발생하더라도 데이터를 계속 사용할 수 있습니다.

지역 중복 스토리지를 비활성화하려면

경고!
지역 중복 기능을 비활성화하고 나면 1일 내에 복제된 데이터가 삭제됩니다.

1. Cyber Protect 콘솔에서 **설정** > **시스템 설정**으로 이동합니다.
2. 백업 옵션 목록을 스크롤하여 **Geo-redundant Cloud Storage**를 클릭합니다.
3. **Geo-redundant Cloud Storage** 스위치를 비활성화합니다.
4. **비활성화**를 입력하여 선택을 확인한 다음 **비활성화**를 클릭합니다.

지역 간 복제 상태

지역 중복 기능 사용 시에는 데이터가 보조 위치에 복제됩니다. 지역 간 복제 상태에는 이 프로세스의 단계가 표시됩니다. 표시될 수 있는 상태는 다음과 같습니다.

- **동기화됨** - 데이터가 보조 위치에 복제되었습니다.
- **동기화 중** - 데이터를 보조 위치에 복제하는 중입니다. 이 작업의 소요 시간은 데이터 크기에 따라 달라집니다.
- **보류 중** - 데이터 복제가 일시 중지되었습니다.
- **비활성화됨** - 데이터 복제가 비활성화되었습니다.

Cyber Protect 콘솔에서 복제 상태를 확인하려면

1. Cyber Protect 콘솔에서 **백업 스토리지**로 이동합니다.
2. 위치와 백업 세트를 선택합니다.

© Acronis International GmbH, 2003-2024

3. **상세 정보**를 클릭하고 **지역 간 복제 상태**에서 상태를 확인합니다.

제한 사항

- 현재 복제된 데이터용 보조 위치는 미국과 캐나다에서만 사용 가능합니다.
- 지역 중복 기능 사용 시의 Disaster Recovery 서비스 관련 제한 사항에 대한 자세한 내용은 Disaster Recovery 설명서를 참조하십시오.

© Acronis International GmbH, 2003-2024

용어 설명

U

USB 장치 데이터베이스

[장치 제어] 장치 제어 모듈이 유지보수하는 USB 장치 데이터베이스에서 장치를 선택하여 장치 액세스 제어 제외 목록에 추가할 수 있습니다. 데이터베이스에는 USB 장치가 장치 ID로 등록됩니다. 장치 ID는 수동으로 입력할 수도 있고, Cyber Protect 콘솔에 표시되는 알려진 장치에서 선택할 수도 있습니다.

V

VPN 게이트웨이(이전 VPN 서버 또는 연결 게이트웨이)

[Disaster Recovery] 로컬 사이트와 클라우드 사이트 네트워크를 보안 VPN 터널로 연결하는 특수 가상 머신입니다. VPN 게이트웨이는 클라우드 사이트에 디플로이됩니다.

VPN 어플라이언스

[Disaster Recovery] 로컬 네트워크와 클라우드 사이트 네트워크를 보안 VPN 터널로 연결하는 특수 가상 머신입니다. VPN 어플라이언스는 로컬 사이트에 디플로이됩니다.

가

가상 머신

Agent for VMware 또는 Agent for Hyper-V와 같은 외부 에이전트에 의해 하이퍼바이저 수준에서 백업된 가상 머신입니다. 에이전트를 내부에 포함하고 있으며 백업 관점에서 실제 머신으로 처리되는 가상 머신입니다.

공

공용 IP 주소

[Disaster Recovery] 클라우드를 인터넷에서도 사용할 수 있게 하는 IP 주소입니다.

기

기본 서버

[Disaster Recovery] 로컬 사이트에 연결된 머신(복구 서버 등)이 없는 가상 머신입니다. 기본 서버를 사용하여 애플리케이션을 보호하거나 여러 개의 보조 서비스(웹 서버 등)를 실행합니다.

네

네트워크 테스트

[Disaster Recovery] 장애 조치 과정을 테스트하기 위한 격리된 가상 네트워크입니다.

단

단일 파일 백업 형식

초기 전체 백업 및 이후 증분 백업이 단일 .tibx 파일로 저장되는 백업 형식입니다. 이 형식은 오래된 백업의 삭제가 어렵다는 주요 단점을 피하면서 증분 백업 방식의 빠른 속도를 활용합니다. 이 소프트웨어는 오래된 백업에서 사용하는 블록을 "여유"로 표시하고 이러한 블록에 새 백업을 씁니다. 이를 통해 최소한의 리소스를 사용하여 매우 빠른 정리가 가능합니다. 임의 액세스 읽기 및 쓰기가 지원되지 않는 위치로 백업할 때는 단일 파일 백업 형식을 사용할 수 없습니다.

© Acronis International GmbH, 2003-2024

데

데이터 손실 방지 에이전트

기밀 데이터, 보호된 데이터 또는 중요한 데이터의 무단 사용, 전송, 저장으로부터 호스트 컴퓨터를 보호하는 데이터 손실 방지 시스템의 클라이언트 구성 요소입니다. 이 에이전트는 상황 및 내용 분석 기술을 함께 적용하고 중앙에서 관리되는 데이터 손실 방지 정책을 적용함으로써 컴퓨터를 보호합니다. Cyber Protection에서는 모든 기능을 갖춘 데이터 손실 방지 에이전트를 제공합니다. 그러나 보호된 컴퓨터의 에이전트 기능은 Cyber Protection에서 라이센스를 통해 사용 가능한 데이터 손실 방지 기능 세트로 제한됩니다. 사용 가능한 기능은 해당 컴퓨터에 적용되는 보호 계획에 따라 달라집니다.

데이터 손실 방지(이전 명칭 데이터 유출 방지)

조직 내/외부의 권한이 없는 항목에 의한 실수 또는 의도적인 기밀 데이터, 보호된 데이터 또는 중요한 데이터 공개/액세스나 신뢰할 수 없는 환경으로의 해당 데이터 전송을 감지하고 방지하는 데 사용할 수 있는 통합 기술 및 조직 대책 시스템입니다.

로

로컬 사이트

[Disaster Recovery] 회사 프레미스에 디플로이된 로컬 인프라입니다.

모

모듈

백업, 안티바이러스 및 안티맬웨어 보호 기능 등의 모듈은 특정 데이터 보호 기능을 제공하는 보호 계획의 일부입니다.

백

백업 세트

개별적인 보관 규칙이 적용되는 백업 그룹입니다. 사용자 정의 백업 구성표의 경우 백업 세트는 백업 방식에 해당합니다(전체, 차등, 증분). 이외의 경우 백업 세트는 월간, 일일, 주간, 매시간입니다. 월간 백업은 한 달이 시작된 후 생성된 첫 번째 백업입니다. 주간 백업은 주간 백업 옵션(기어 아이콘을 클릭한 다음 백업 옵션 > 주간 백업 클릭)에서 선택한 주중 특정일에 생성된 첫 번째 백업입니다. 한 달이 시작된 후 생성된 첫 번째 백업이 주간 백업인 경우 해당 백업은 월간인 것으로 간주됩니다. 이 경우 주간 백업은 다음 주 선택한 요일에 생성됩니다. 일일 백업은 해당 백업이 월간 또는 주간 백업의 정의에 포함되지 않는 한 하루가 시작된 후 생성된 첫 번째 백업입니다. 매시간 백업은 해당 백업이 월간, 주간 또는 일일 백업의 정의에 포함되지 않는 1시간이 시작된 후 생성된 첫 번째 백업입니다.

보

보호 계획

보호 계획이란 백업, 안티바이러스 및 맬웨어 방지, URL 필터링, Windows Defender 안티바이러스, Microsoft Security Essentials, 취약성 평가, 패치 관리, 데이터 보호 맵, 장치 제어를 비롯한 여러 가지 데이터 보호 모듈을 조합한 계획입니다.

보호 에이전트

보호 에이전트는 데이터 보호를 위해 머신에 설치되는 에이전트입니다.

복

복구 서버

[Disaster Recovery] 클라우드에 저장되어 있는 보호되는 서버 백업을 기반으로 하는 원본 머

© Acronis International GmbH, 2003-2024

신의 VM 복제본입니다. 복구 서버는 재해 시 원본 서버의 워크로드를 전환하는 데 사용됩니다.

복구 지점 목표(RPO)

[재해 복구] 중단으로 손실된 데이터 양으로, 계획된 중단 또는 재해 이벤트로부터의 시간으로 측정합니다. RPO 임계값은 현재 시각과 장애 조치에 적합한 마지막 복구 지점 사이의 최대 시간을 정의합니다.

분

분리된 백업

분리된 백업은 더 이상 보호 계획과 연결되어 있지 않은 백업입니다.

사

사이트 간(S2S) 연결

[Disaster Recovery] 보안 VPN 터널을 통해 로컬 네트워크를 클라우드로 확장하는 연결입니다.

실

실제 머신

운영 체제에 설치된 에이전트에 의해 백업된 머신.

실행서

[Disaster Recovery] 재해 복구 작업을 자동화하는 구성 가능한 단계로 이루어진 계획된 시나리오입니다.

완

완료

백업에서 운영 중인 임시 가상 머신을 영구적인 가상 머신으로 만드는 작업입니다. 실제로, 이는 머신이 운영되는 동안 발생한 변경 사항을 포함한 모든 가상 머신 디스크를 해당 변경 사항을 저장하는 데이터 저장소로 복구하는 것을 의미합니다.

운

운영 네트워크

[Disaster Recovery] VPN 터널링으로 확장되어 로컬 및 클라우드 사이트를 모두 지원하는 내부 네트워크입니다. 로컬 및 클라우드 서버는 운영 네트워크에서 서로 통신할 수 있습니다.

유

유효성 검사

백업으로부터 데이터 복구 가능성을 확인하는 작업. 파일 백업 유효성 검사는 백업에 있는 모든 파일을 더미 목적지로 복구하는 작업과 유사합니다. 디스크 백업의 유효성 검사는 백업에 저장된 모든 데이터 블록의 체크섬을 계산합니다. 두 절차 모드 리소스 집약적입니다. 성공적인 유효성 검사는 높은 확률의 성공적인 복구를 의미하지만 복구 프로세스에 영향을 미치는 모든 요인을 검사하는 것은 아닙니다.

장

장애 복구

예비 서버(가상 머신 복제본 또는 클라우드에서 운영 중인 복구 서버 등)의 워크로드를 운영 서버로 다시 전환하는 과정입니다.

장애 조치

운영 서버의 워크로드를 예비 서버(가상 머신 복제본 또는 클라우드에서 운영 중인 복구 서버 등)로 전환하는 과정입니다.

장치 제어 모듈

장치 제어 모듈은 보호 계획의 일환으로 보호되는 각 컴퓨터의 데이터 손실 방지 에이전트 기능 중 일부를 활용하여 무단 액세스 및 로컬

© Acronis International GmbH, 2003-2024

컴퓨터 채널을 통한 데이터 전송을 감지 및 방지합니다. 이러한 작업으로는 사용자의 주변 장치 및 포트 액세스, 문서 인쇄, 클립보드 복사/붙여넣기 작업, 미디어 포맷 및 꺼내기 작업, 그리고 로컬에 연결된 모바일 장치와의 동기화 등이 있습니다. 장치 제어 모듈에서는 사용자가 보호된 컴퓨터에서 액세스할 수 있는 포트 및 장치 유형, 그리고 사용자가 해당 장치에서 수행할 수 있는 작업을 상황별로 자세하게 제어할 수 있습니다.

전

전체 백업

업에 선택된 모든 데이터를 포함하는 자급식 백업. 데이터를 전체 백업에서 복구하기 위해서 다른 백업에 액세스할 필요가 없습니다.

증

증분 백업

백업은 가장 최근의 백업 이후 데이터에 대한 변경 내용을 저장합니다. 증분 백업에서 데이터를 복구하려면 다른 백업에 액세스해야 합니다.

지

지점 및 사이트 간(P2S) 연결

[Disaster Recovery] 엔드포인트 장치(컴퓨터나 랩톱)를 사용하여 외부에서 클라우드 사이트 및 로컬 사이트로 접속할 수 있는 안전한 VPN 연결입니다.

차

차등 백업

차등 백업은 최신 전체 백업 이후 데이터 변경 사항을 저장합니다. 차등 백업에서 데이터를 복구하기 위해서는 해당하는 전체 백업에 액세스해야 합니다.

클

클라우드 사이트(또는 DR 사이트)

[Disaster Recovery] 재해 시 복구 인프라를 실행할 때 사용하는 클라우드에 호스팅된 원격 사이트입니다.

클라우드 서버

[Disaster Recovery] 복구 또는 기본 서버에 대한 일반 참조입니다.

테

테스트 IP 주소

[Disaster Recovery] 테스트 장애 조치 시 운영 중인 IP 주소의 중복을 방지하기 위해 필요한 IP 주소입니다.

© Acronis International GmbH, 2003-2024

색인

#

#CyberFit Score 스캔 실행 중 215

#CyberFit Score 책정 메커니즘 212

1

180일 동안 보안 이벤트 저장 815

1단계 55

2

2단계 55

2단계 인증 19

3

32비트와 64비트 버전 중 선택 646

3단계 55

4

4단계 55

5

5단계 56

6

6단계 57

A

AAG(Always On 가용성 그룹) 보호 514

AAG에 포함된 데이터베이스 백업 515

AAG에 포함된 데이터베이스 복구 515

Acronis 빠른 지원을 통한 파일 전송 926

Acronis 빠른 지원을 통해 관리 대상 워크로드에 연결 925

Active Directory 도메인 서비스 사용 가능성 관련 권장 사항 691

Active Protection 748

Advanced 779

Advanced Data Loss Prevention 787

Agent for Advanced Data Loss Prevention 24

Agent for Exchange(사서함 백업용) 25

Agent for File Sync & Share 25

Agent for Hyper-V 28

Agent for Linux 26

Agent for Mac 27

Agent for Microsoft 365 25

Agent for MySQL/MariaDB 26

Agent for Oracle 25

Agent for oVirt 28

Agent for oVirt – 필요한 역할과 포트 147

Agent for oVirt(가상 어플라이언스) 디플로이 중 142

Agent for Scale Computing HC3 28

Agent for Scale Computing HC3 – 필요한 역할 133

Agent for Scale Computing HC3(가상 어플라이언스) 배포 중 129

Agent for SQL, Agent for Active Directory, Agent for Exchange(데이터베이스 백업 및 애플리케이션 인식 백업용) 24

Agent for Synology 28

Agent for Synology 디플로이 147

Agent for Synology 설치 149

© Acronis International GmbH, 2003-2024

Agent for Synology 업데이트 153

Agent for Virtuozzo 28

Agent for Virtuozzo Hybrid Infrastructure 28

Agent for Virtuozzo Hybrid Infrastructure(가상 어플라이언스) 디플로이 134

Agent for VMware - LAN 프리 백업 626

Agent for VMware - 필수 권한 635

Agent for VMware(Windows) 27

Agent for VMware(가상 어플라이언스) 27

Agent for VMware(가상 어플라이언스) 배포 125

Agent for Windows 23

AI(ScriptPilot)를 사용하여 스크립트 생성 223

Amazon 39

Amazon S3에 백업 499

Amazon S3에서 백업 위치 정의 494

Apple 화면 공유 901

ASign으로 파일에 서명 468

autostart.json의 구조 651

Aware 인식→인지 518

B

BitLocker로 보호된 워크로드에서 에이전트 업데이트 166

Bootable Media Builder 645

Bootable Media Builder를 사용하는 이유 646

C

calculate hash 428

CBT(Changed Block Tracking) 416, 624

CDP 백업 구성 375

Citrix 35

Connect 에이전트에 필요한 시스템 권한 부여 77

Connect 클라이언트 설정 구성 930

CPU 사용량 모니터의 설정 942

CPU 온도 모니터의 설정 939

CPU 우선 순위 438

Cyber Backup Standard Edition의 Active Protection 762

Cyber Backup Standard의 Active Protection 설정 762

Cyber Disaster Recovery Cloud 정보 666

Cyber Disaster Recovery Cloud 평가판 버전 669

Cyber Protect Monitor에서 프록시 서버 설정 구성 287

Cyber Protect 모니터 28, 286

Cyber Protect 앱 다운로드 방법 539

Cyber Protect 콘솔 293

Cyber Protect 콘솔 외부에서 백업 삭제 487

Cyber Protect 콘솔에 워크로드 추가 303

Cyber Protect 콘솔에서 워크로드 관리 293

Cyber Protect 콘솔에서 워크로드 제거 307

Cyber Protect 콘솔에서 파일 복구 466

Cyber Protect 콘솔에서 파일을 복구할 때 적용되는 제한 사항 471

Cyber Protect 콘솔을 통해 데이터를 검토하는 방법 540

Cyber Protect 콘솔의 새로운 기능 294

Cyber Protect 콘솔의 파트너 테넌트 수준 295

Cyber Protection 260, 583

Cyber Protection 서비스 액세스 21

Cyber Protection 시작하기 19

© Acronis International GmbH, 2003-2024

Cyber Protection 에이전트 설치 및 디플로이 55

Cyber Scripting 217

CyberApp 워크로드 357

CyberApp 워크로드 사용 357

D

DAG(데이터베이스 가용성 그룹) 보호 516

Data Loss Prevention용 에이전트 24

Dell EMC Data Domain 스토리지와의 호환성 40

DHCP 서버의 장애 조치 수행 방법 718

DirectAdmin, cPanel 및 Plesk 통합 616

E

EDR 경보 257

EDR(Endpoint Detection and Response) 812

EDR(Endpoint Detection and Response) 기능 활성화 815

EDR(Endpoint Detection and Response) 사용 방법 817

EDR(Endpoint Detection and Response)을 위한 모니터링 모드 활성화 860

EDR(Endpoint Detection and Response)이 정상 작동 중인지 테스트하는 방법 862

EDR(Endpoint Detection and Response)이 필요한 이유 813

EDR(엔드포인트 탐지 및 대응) 위젯 261

ESXi 가상 머신의 시스템 요구사항 511

ESXi 구성 복구 472

ESXi 구성 선택 372

Exchange Online 데이터 보호 556

Exchange Online 사서함 선택 542

Exchange Server 데이터 선택 513

Exchange Server 데이터베이스 마운트 531

Exchange Server 클러스터 개요 516

Exchange 데이터베이스 복구 529

Exchange 사서함 및 사서함 항목 복구 532

Exchange 서버 사서함 선택 521

Exchange 온라인 사서함 보호 551

Exchange 클러스터 데이터 백업 517

Exchange 클러스터 데이터 복구 517

EXE 파일을 통한 무인 설치 및 설치 제거 81

G

Geo-redundant Cloud Storage 사용 시의 제한 사항 669

get content 428

Gmail 데이터 보호 589

Gmail 백업에 대한 전체 텍스트 검색 비활성화 605

Gmail 사서함 선택 590

Google Drive 및 Google Drive 파일 복구 594

Google Drive 파일 보호 593

Google Drive 파일 복구 595

Google Drive 파일 선택 594

Google Workspace 데이터 보호 582

Google Workspace 데이터 보호의 의미 583

Google Workspace 백업의 빈도 설정 589

Google Workspace 조직 추가하기 584

Google Workspace에서 583

GPU 온도 모니터의 설정 940

H

H.264 900

© Acronis International GmbH, 2003-2024

Hosted Exchange 데이터 보호 541

Hyper-V 가상 머신의 시스템 요구사항 512

I

IP 주소 다시 할당 699

IP 주소 재구성 695

IP 주소를 통해 비관리 대상 워크로드에 연결 926

IPsec VPN 구성 문제 해결 706

IPsec VPN 로그 파일 다운로드 707

IPsec/IKE 보안 설정 689

L

L2 IPsec VPN 연결용 Active Directory 도메인 컨트롤러 692

L2 OpenVPN 연결용 Active Directory 도메인 컨트롤러 691

L2 VPN을 통한 DHCP 트래픽 허용 702

Linux 368

Linux 기반 644

Linux 기반 부트 가능한 미디어 646

Linux 기반 부트 가능한 미디어 대 WinPE/WinRE 기반 부트 가능한 미디어 644

Linux 머신 취약성 평가 869

Linux 패키지 64

Linux에서 Protection 에이전트 설치 74

Linux에서 무인 설치 또는 제거 97

Linux의 Universal Restore 465

list backups 426

list content 427

LVM 스냅샷 촬영 430

M

Mac 368

Mac 사용자 참고 사항 453

macOS 장치의 취약성 평가 870

macOS에 무인 설치 및 제거 103

macOS에 설치되는 서비스 173

macOS에서 Protection 에이전트 설치 76

macOS에서 장치 제어 모듈 사용 활성화 335

macOS의 무인 설치에 필요한 권한 105

McAfee Endpoint Encryption 및 PGP Whole Disk Encryption 40

Microsoft 33

Microsoft 365 Teams 보호 573

Microsoft 365 데이터 보호 545

Microsoft 365 데이터를 백업하는 이유? 545

Microsoft 365 백업의 빈도 설정 556

Microsoft 365 사서함 선택 552

Microsoft 365 시트 라이센스 보고서 549

Microsoft 365 액세스 자격 증명 변경 551

Microsoft 365 조직 삭제 554

Microsoft 365 조직 추가 549, 553

Microsoft 365 협업 앱 시트 보호 582

Microsoft 365의 요구 사항 547

Microsoft Azure 39

Microsoft Azure 가상 머신 관련 작업 729

Microsoft Azure 구독 액세스 관리 502

Microsoft Azure 구독 액세스 권한 갱신 503

Microsoft Azure 구독 액세스 권한 제거 504

Microsoft Azure 구독 액세스 권한 추가 502

Microsoft Azure 및 Amazon EC2 가상 머신 643

© Acronis International GmbH, 2003-2024

Microsoft Azure에 백업 499

Microsoft Azure에서 백업 위치 정의 492

Microsoft BitLocker Drive Encryption 40

Microsoft Defender 안티바이러스 및 Microsoft Security Essentials 777

Microsoft Exchange Server 라이브러리 복사 537

Microsoft Exchange 서버 417

Microsoft Security Essentials 777

Microsoft SharePoint 보호 509

Microsoft SQL Server 416

Microsoft SQL Server 및 Microsoft Exchange Server 보호 509

Microsoft 애플리케이션 보호 509

Microsoft 제품 873

MSI 파일을 통한 무인 설치 및 설치 제거 89

MSI, MST 및 CAB 파일 추출 89

MySQL 및 MariaDB 데이터 보호 606

N

NEAR 900

Notary Service를 통해 파일 신뢰성 확인 468, 601

Nutanix 37

O

OneDrive 및 OneDrive 파일 복구 567

OneDrive 파일 보호 565

OneDrive 파일 복구 568

OneDrive 파일 선택 566

OneNote 전자 필기장 보호 581

OpenVPN 구성 다운로드 703

Oracle 37

Oracle 데이터베이스 보호 606

OS 알림 및 서비스 경보 345

OS 알림 및 서비스 경보 활성화 또는 비활성화 338

OVA 템플릿 디플로이 143

OVF 템플릿 디플로이 126

oVirt/Red Hat Virtualization 4.2 및 4.3/Oracle Virtualization Manager 4.3 147

oVirt/Red Hat Virtualization 4.4, 4.5 147

P

Parallels 36

PCI DSS(결제 카드 산업 데이터 보안 표준) 803

PCI DSS로 간주되는 데이터 804

PHI(개인 건강 정보) 800

PII(개인 식별 정보) 801

PII(개인 식별 정보)로 간주되는 데이터 802

Protection 에이전트 다운로드 72

Protection 에이전트 설치 72

Protection 에이전트가 사용하는 포트 변경 57

Q

QCOW2 템플릿 디플로이 130, 138

R

RDP 901

RDP 설정 구성 917

Red Hat 및 Linux 35

S

SAP HANA 보호 606

Scale Computing 35

Secure Zone 사용 방법 40

© Acronis International GmbH, 2003-2024

Secure Zone 삭제 방법 380

Secure Zone 생성 방법 379

Secure Zone 생성으로 디스크가 변환되는 방식 378

Secure Zone 정보 378

Secure Zone을 사용하는 이유는 무엇일까요? 378

Shared Drive 및 Shared Drive 파일 복구 598

Shared Drive 파일 보호 597

Shared Drive 파일 복구 599

Shared Drive 파일 선택 597

SharePoint 온라인 데이터 복구 571

SharePoint 온라인 데이터 선택 570

SharePoint 온라인 사이트 보호 569

SID 변경 479

SQL Server 고가용성 솔루션 개요 514

SQL Server 데이터베이스 연결 529

SQL Server 또는 Exchange Server 액세스 자격 증명 변경 537

SQL 데이터베이스 복구 522

SQL 데이터베이스 선택 513

SQL 데이터베이스를 파일로 복구 526

SSH 클라이언트를 통해 가상 어플라이언스 액세스 161

Startup Recovery Manager 663

Startup Recovery Manager 비활성화 664

Startup Recovery Manager 활성화 664

T

TCP 포트는 VMware 가상 머신을 백업하고 복제하는 데 필요합니다. 56

U

UAC(User Account Control)에 대한 요구 사항 121

Universal Restore 사용 463

Universal Restore 설정 464

Universal Restore 프로세스 464

URL 제외 776

URL 필터링 769

URL 필터링 경보 256

URL 필터링 구성 작업 흐름 771

URL 필터링 설정 771

USB 장치 데이터베이스 348

USB 장치 데이터베이스 관리 페이지 349

USB 장치 허용 목록 347

USB 장치를 데이터베이스에 추가하거나 데이터베이스에서 제거 339

V

Virtuozzo 38

Virtuozzo Hybrid Infrastructure 38

Virtuozzo Hybrid Infrastructure(가상 어플라이언스)용 Agent의 네트워크 요구조건 135

Virtuozzo Hybrid Infrastructure의 네트워크 구성 135

Virtuozzo Hybrid Infrastructure의 사용자 계정 구성 135

Virtuozzo 컨테이너 또는 Virtuozzo 가상 머신으로 복구 471

VLAN 추가 659

VM 스냅샷 생성 도중 오류가 발생하는 경우 재시도 419

© Acronis International GmbH, 2003-2024

VM 전원 관리 480, 625

VM 하트비트 192

VM 하트비트 및 스크린샷 유효성 검사의 시간 초과 값 변경 193

VMware 31

VMware vSphere에서 작업 620

VPN 게이트웨이 678, 682

VPN 게이트웨이 네트워크 구성 678

VPN 게이트웨이 다시 설치 697

VPN 게이트웨이의 로그 다운로드 705

VPN 어플라이언스 678

VPN 어플라이언스 설정 관리 697

VPN 어플라이언스에 대한 요구사항 685

VPN 어플라이언스의 로그 다운로드 704

vSphere Client에서 백업 상태 보기 635

VSS 전체 백업 활성화 449

VSS(Volume Shadow Copy Service) 447

W

Wasabi에 백업 500

Wasabi에서 백업 위치 정의 496

Windows 367

Windows Defender 안티바이러스 777

Windows 머신 취약성 평가 869

Windows 머신에서 로그온 계정 변경 79

Windows 서드 파티 제품 874

Windows 서비스 상태 모니터의 설정 954

Windows 업데이트 상태 모니터의 설정 958

Windows 이벤트 로그 451, 480

Windows 이벤트 로그 모니터의 설정 956

Windows 이벤트 로그 이벤트 시 387

Windows를 실행하는 머신에 대한 추가 요구 사항 520

Windows에 설치되는 서비스 172

Windows에서 Protection 에이전트 설치 72

Windows에서 무인 설치 또는 제거 81

Windows의 Universal Restore 463

WinPE 기반 및 WinRE 기반 부트 가능한 미디어 654

WinPE 또는 WinRE 부트 가능한 미디어 생성 655

WinPE 이미지 654

WinPE/WinRE 기반 644

WinRE 이미지 654

가

가상 머신 결합 630

가상 머신 마이그레이션 지원 633

가상 머신 복구 459

가상 머신 복제 620

가상 머신용 VSS(Volume Shadow Copy Service) 449, 625

가상 머신으로 실행 192

가상 머신으로 전환 195

가상 머신으로의 장애 복구 수행 720

가상 머신으로의 정기적인 변환 작동 방식 198

가상 머신으로의 정기적인 변환과 백업에서 가상 머신 실행 비교 198

가상 머신을 가상 서버에 생성하도록 선택하는 경우 199

가상 머신을 사용한 특수 작업 616

가상 머신을 파일 세트로 저장하도록 선택하는 경우 199

© Acronis International GmbH, 2003-2024

가상 머신의 추가 시스템 요구사항 519
가상 어플라이언스 구성 126, 131, 139, 144
가상 어플라이언스에 대한 SSH 연결 160
가상 어플라이언스에서 루트 암호 설정 161
가상화 환경 관리 633

감

감지에 대한 작업 763

개

개별 및 그룹 계획 사이의 충돌 205
개별 사이버 킬 체인 노드에 대한 대응 조치 841
개요 대시보드 240
개요 대시보드의 Advanced Data Loss Prevention 위젯 806
개인 건강 정보로 간주되는 데이터 801
개인 정보 보호 설정 21
개인용 Google 클라우드 프로젝트 생성 585

검

검색 연산자 327
검색 인덱스 602
검색 인덱스의 크기 확인 603
검색된 IOC 검토 및 분석 836
검색된 머신 261
검색된 머신 관리 123

격

격리 752, 781
격리된 파일 관리 781

경

경보 409
경보 대시보드 241
경보 위젯 259
경보 유형 242
경보 탭 296

계

계정 활성화 19
계획 상태 183
계획 충돌 해결 205
계획의 대상 워크로드 관리 234

고

고객 테넌트 수준 295
고급 보호 기능 사용 786
고급 설정 799
고급 스토리지 옵션 377
고급 안티맬웨어 749

공

공격 단계로 이동하는 방법 829
공격 단계에 포함되는 정보 829
공용 및 테스트 IP 주소 679
공용 폴더 및 폴더 항목 복구 564
공용 폴더 선택 558
공증 405, 600
공증 사용 방법 405, 600
공통 백업 규칙 40
공통 설치 규칙 39
공통 요구 사항 510

© Acronis International GmbH, 2003-2024

관

관리 대상 워크로드 사용 917

관리 대상 워크로드에서 데이터 소거 356

관리 대상 워크로드에서 제어 작업 수행 921

관리 탭 183

관찰 모드를 사용하여 사용자 정책 갱신 795

구

구성 가능한 모니터 934

구성 재생성 703

권

권장 사항 475

권장 사항 및 수정 단계 814

권한 793

규

규제 준수 모드 982

규제 준수 모드로 설정된 테넌트의 백업 복구 983

규제 준수 모드의 테넌트 471

규칙 구조 790

그

그룹 삭제 330

그룹 정책 객체 설정 159

그룹 정책을 통해 에이전트 배포 156

그룹에 계획 적용 330

그룹에서 계획 철회 331

기

기능 813

기밀로 표시됨 804

기본 매개변수 99

기본 백업 옵션 405

기본 백업 파일 이름 412

기본 보호 계획 206

기본 보호 계획 비교 206

기본 보호 계획 적용 211

기본 보호 계획 편집 211

기본 서버 681

기본 서버 관련 작업 732

기본 서버 생성 729

기본 서버 설정 729

기본 작업 778

기본 제공 그룹 311

기본 제공 그룹 및 사용자 지정 그룹 311

기업 허용 목록 782

기존 계획과 새 계획 사이의 충돌 205

기존 계획에서 향상된 검색을 활성화하거나 비활성화하기 605

기존 백업 아카이브에서 백업 생성하기 413

기존 원격 관리 계획을 사용하여 추가 작업 수행 911

기존 취약성 272

내

내용 탐지에 사용되는 논리식 801-802, 804

네

네트워크 공유에서 복구 649

네트워크 관리 693

네트워크 사용량 모니터의 설정 948

네트워크 설정 658

© Acronis International GmbH, 2003-2024

네트워크 설정 구성 659

네트워크 패킷 캡처 705

네트워크 폴더 보호 749

네트워킹 개념 674

논

논리 볼륨에서 지원되는 작업 53

다

다른 백업 옵션과 상호 작용 443

다른 수준에 추가된 Microsoft 365 조직 관리 554

다른 퍼블릭 클라우드 스토리지 서비스 액세스 관리 505

다양한 관리 수준의 계획 235

다양한 로그인 옵션 900

다운로더 컴퍼넌트에 필요한 포트 57

다음과 같은 Wi-Fi 네트워크에 연결된 경우 시작하지 않음 393

다음에 수행할 작업 672

다중 볼륨 스냅샷 431

다중 사이트 IPsec VPN 구성 686

다중 사이트 IPsec VPN 로그 파일 708

다중 사이트 IPsec VPN 설정 구성 687

다중 사이트 IPsec VPN 연결 682

다중 테넌시 지원 301

단

단일 장치의 소프트웨어 인벤토리 보기 889

단일 장치의 하드웨어 보기 893

대

대상 가상 머신으로 장애 복구 719

대상 실제 머신으로 장애 복구 724

대상 자동 감지 799

대시보드에서 간편하게 개요 정보 파악 815

데

데이터 백업 시작 방법 539

데이터 보호 맵 270, 282

데이터 보호 맵 설정 283

데이터 손실 방지 이벤트 805

데이터 요금제 사용 시 시작하지 않음 392

데이터 중복 제거 52

데이터 캡처 전 명령 443

데이터 캡처 전/후 명령 443

데이터 캡처 후 명령 444

데이터 플로우 정책 갱신 794

데이터 플로우 정책 구조 790

데이터 플로우 정책 규칙 결합 793

데이터 플로우 정책 규칙의 권한 조정 792

데이터 플로우 정책 및 정책 규칙 생성 788

데이터를 모바일 장치로 복구하는 방법 540

데이터베이스 백업 512

데이터베이스 복구 610

도

도메인 컨트롤러 보호 509

동

동시 백업되는 가상 머신의 총 수를 제한합니다. 638

동시에 여러 관리 대상 워크로드 관찰 924

동작 엔진 752

동적 그룹 312

© Acronis International GmbH, 2003-2024

동적 그룹 생성 315

동적 그룹 편집 329

드

드라이버 준비 463

등

등록 매개변수 100

등록 토큰 생성 156

디

디스크 공간 모니터의 설정 937

디스크 또는 볼륨 백업은 어떤 항목을 저장합니까? 367

디스크 또는 볼륨 선택 366

디스크 및 볼륨용 정책 규칙 368

디스크 상태 경보 270

디스크 상태 모니터링 266

디스크 상태 위젯 267

디스크 전송 속도 모니터의 설정 945

디스크 프로비저닝 624

디스플레이 모드 설정 660

라

라우팅 작동법 676, 678, 683

라이선스 경보 255

라이센스 문제 205

런

런북 매개변수 740

레

레거시 기능에 대한 매개변수 102

로

로그 자르기 430

로그 작업 704

로그온 계정에 필요한 권한 79

로컬 DNS를 사용하는 서버의 장애 조치 수행 방법 718

로컬 라우팅 구성 701

로컬 백업에서 파일 추출 471

로컬 사이트 관련 일반 권장 사항 689

로컬 사이트로의 VPN 액세스 702

로컬 연결 659

로컬로 설치한 Agent for Office 365 사용 549

로컬로 연결된 스토리지 사용 629

리

리포지토리에서 패키지 설치 66

마

마스터 데이터베이스 복구 528

마운트 포인트 431, 477

마지막 시스템 다시 시작 모니터의 설정 955

마지막으로 로그인한 사용자 찾기 359

매

매개변수 647

매시간 구성표를 사용하는 월별 백업이 있는 이유 398

머

머신 러닝 모델 재설정 971

머신 복구 454

머신 삭제 619

© Acronis International GmbH, 2003-2024

머신 속성으로 암호화 설정 403
머신 실행 617
머신 완료 619
머신 이주 640
머신 자동 검색 115
머신별 #CyberFit Score 211, 265
머신의 격리 위치 782
머신의 서비스 할당량 변경 171

메

메모리 사용량 모니터의 설정 944

모

모니터 데이터 보기 979
모니터 위젯 980
모니터링 240
모니터링 경보 971
모니터링 경보 구성 971
모니터링 경보 변수 972
모니터링 경보의 경보 로그 확인 977
모니터링 계획 933, 962
모니터링 계획 관련 추가 작업 967
모니터링 계획 생성 962
모니터링 계획 해지 965
모니터링 계획에 워크로드 추가 964
모니터링 계획의 호환성 문제 969
모니터링 계획의 호환성 문제 해결 970
모니터링 유형 933
모니터링용으로 지원되는 플랫폼 934
모든 경보 삭제 281
모바일 장치 보호 538

목

목적지 선택 376

무

무인 설치 또는 제거 81
무인 설치 또는 제거 매개변수 99
무인 설치(EXE)용 매개변수 83
무인 설치(MSI)용 매개변수 92
무인 설치용 컴포넌트(EXE) 88
무인 설치용 컴포넌트(MSI) 96

문

문제 해결 124

민

민감한 데이터 정의 800

발

발견된 취약성 관리 870

방

방화벽 관리 780
방화벽 관리 활성화 및 비활성화 780
방화벽 상태 모니터의 설정 958

배

배터리 전원 절약 392
배포 결과 보기 631
배포 알고리즘 630

백

백업 53, 361

© Acronis International GmbH, 2003-2024

백업 경보 243
백업 관련 작업 480
백업 구성표 381
백업 구성표에 따른 보존 규칙 397
백업 내보내기 484
백업 데이터를 받기 위한 "tibxread" 도구 425
백업 맬웨어 방지 스캔 784
백업 복제 185
백업 복제 계획 생성 186
백업 삭제 485
백업 스캔 계획 184
백업 스캔 세부 정보 274
백업 스케줄 381
백업 스케줄 정보 583
백업 스토리지 탭 480
백업 옵션 406
백업 옵션의 사용 가능성 406
백업 위치의 호스트를 사용할 수 있음 390
백업 유형 383
백업 유효성 검사 415, 474, 484
백업 전 명령 441
백업 중 출력 속도 439
백업 통합 409
백업 파일 이름 410
백업 파일 이름에 대한 제한 사항 411
백업 파일 이름은 어디에서 볼 수 있습니까? 411
백업 파일이란 무엇입니까? 410
백업 할당 시간 437
백업 형식 414
백업 형식 및 백업 파일 414
백업 형식을 버전 12(TIBX)로 변경 415
백업 후 명령 442
백업에서 가상 머신 실행(즉시 복원) 616
백업에서 복구 851
백업에서 볼륨 마운트 482
백업에서 포렌직 데이터를 가져오는 방법은? 423
백업의 유효성 검사 상태 확인 194
백업한 OneNote 전자 필기장 복구 581
백업할 데이터 선택 365
백업할 수 있는 항목 538

버

버킷 설정 500-501

변

변경 불가 스토리지 984
변경 불가 스토리지에서 삭제된 백업 액세스 986
변경 불가능 스토리지 모드 984
변경 불가능 스토리지 비활성화 986
변경 불가능 스토리지 활성화 985
변수 객체 651
변수 사용 413
변수 없는 이름 413
변환 파일 생성 및 설치 패키지 추출 159
변환에 대해서 알아야 할 사항 197

병

병목 현상 감지 방식 파악 487
병목 현상 상세 정보 확인 489
병목 현상을 줄이는 방법 489

© Acronis International GmbH, 2003-2024

병목 현상이 표시되는 워크로드, 에이전트 및 백업 위치 490

병목 현상이란? 487

보

보고 287

보관 규칙 396

보안 901

보안 셸 데몬 시작 160

보안 인시던트 MTTR 263

보안 인시던트 번다운(Burndown) 264

보존 규칙 구성 399

보호 계획 183

보호 계획 및 모듈 199

보호 계획 삭제 204

보호 계획 생성 200

보호 계획 치트 시트 363

보호 계획 편집 203

보호 계획 해지 203

보호 계획 활성화/비활성화 204

보호 계획에서 Advanced Data Loss Prevention 활성화 796

보호 계획에서 암호화 구성 402

보호 계획의 차단 목록 또는 허용 목록에서 프로세스, 파일 또는 네트워크를 추가하거나 제거합니다. 859

보호 계획의 패치 관리 설정 873

보호 계획이 있는 작업 201

보호 방법과 대상 정의 183

보호 상태 260

보호 설정 169

보호 제외 759

보호되지 않는 것으로 감지된 파일 관리 282

복

복구 53, 451

복구 및 다시 시작 455

복구 서버 679

복구 서버 기본 매개변수 편집 672

복구 서버 생성 708

복구 서버 설정 708

복구 시작 시 대상 가상 머신의 전원 끄기 480

복구 옵션 473

복구 옵션의 사용 가능성 473

복구 완료 시 대상 가상 머신 전원 켜기 480

복구 전 명령 478

복구 치트 시트 451

복구 후 명령 479

복구된 머신의 고가용성 638

복구할 수 없는 항목은 무엇입니까? 570

복구할 수 있는 항목은 무엇입니까? 542, 551, 557, 566, 570, 573, 590, 593, 597

복제 400

복제 계획 생성 622

복제 대 백업 비교 621

복제 대상 187

복제 옵션 624

복제본 테스트 622

복제본으로 장애 조치 623

복제본으로 할 수 있는 작업 621

부

부트 가능한 미디어 등록 657

© Acronis International GmbH, 2003-2024

부트 가능한 미디어를 사용하여 디스크 복구 461

부트 가능한 미디어를 사용하여 파일 복구 470

부트 가능한 미디어를 사용한 로컬 작업 659

부트 가능한 미디어를 사용한 원격 작업 660

부트 가능한 미디어를 통한 마이그레이션 642

부트 가능한 미디어에서 부팅한 머신에 연결 659

부트 가능한 미디어의 스크립트 649

부트 가능한 환경에서 드라이버에 대한 액세스 확인 464

부트 모드 475

분

분할 446

불

불량 섹터 무시 418

뷰

뷰어 창에서 도구 모음 사용 927

비

비관리 대상 워크로드 사용 925

비밀번호 요구 사항 19

빠

빠른 증분/차등 백업 419

사

사건 심각도 이력 263

사서함 및 사서함 항목 복구 543, 552, 558, 591

사서함 백업 520

사서함 복구 533, 543, 552, 558, 591

사서함 선택 557

사서함 항목 복구 535, 543, 552, 559, 592

사서함 항목을 PST 파일에 복구 562

사용 가능한 패치 목록 확인 877

사용 시나리오 482

사용 예제 400, 616, 621, 632

사용자 계정에 대한 요구 사항 532

사용자 권한 할당 방법 80

사용자 역할 및 Cyber Scripting 권한 218

사용자 정의 DNS 서버 구성 700

사용자 정의 DNS 서버 삭제 701

사용자 정의 그룹 311

사용자 정의 모니터의 설정 961

사용자 정의 민감도 카테고리 807

사용자 정의 부트 가능한 미디어 대 이미 생성된 부트 가능한 미디어 644

사용자 정의 스크립트 650

사용자 환경에 설치된 Cyber Protection 서비스 172

사용자가 로그오프함 391

사용자가 유휴 상태임 390

사운드 전송 900

사이버 킬 체인 보기 이해 및 사용자 정의 826

사이버 킬 체인에서 인시던트를 조사하는 방법 824

사이버 킬 체인의 개별 노드 조사 830

사이트 간 OpenVPN - 추가 정보 173

사이트 간 OpenVPN 구성 685

사이트 간 OpenVPN 연결 676, 693

사이트 간 OpenVPN 연결 구성 685

사이트 간 연결 유형 전환 698

© Acronis International GmbH, 2003-2024

사이트 간 연결 활성화 및 비활성화 698

사전 요구 사항 115, 149, 152, 154-156, 161, 163, 217, 227, 295, 298, 358-359, 372, 434, 471, 510, 607, 617, 632, 687, 692, 708-709, 721, 725, 729, 884, 887, 889, 891, 893, 904, 910-913, 918, 920-926, 962, 964-965, 967-969, 979

사전 정의된 스크립트 649

사전/사후 명령어 441, 478, 625

서

서버측 보호 750

설

설명 776

설정 프로그램을 다운로드합니다. 148

설치 74

설치 매개변수 99

설치된 소프트웨어 모니터의 설정 955

설치할 대용량 스토리지 드라이버 464

설치할 컴퍼넌트 선택 122

성

성능 478, 625

성능 및 백업 할당 시간 436

섹

섹터 단위 백업 446

셀

셀프 서비스 사용자 정의 폴더 온디맨드 782

소

소프트웨어 관리 탭 296

소프트웨어 및 하드웨어 인벤토리 관리 886

소프트웨어 요구 사항 22, 666, 815

소프트웨어 인벤토리 886

소프트웨어 인벤토리 스캐닝 활성화 886

소프트웨어 인벤토리 위젯 276

소프트웨어 인벤토리 찾아보기 887

소프트웨어별 복구 절차 40

수

수동 결합 631

수동 대응 조치 975

수동 장애 복구 727

수동 장애 복구 수행 727

수동으로 백업 실행 395

수동으로 소프트웨어 인벤토리 스캔 실행 887

수동으로 워크로드 등록 및 등록 해제 110

수동으로 패치 승인 883

수동으로 패키지 설치 67

수동으로 하드웨어 인벤토리 스캔 실행 891

쉽

쉽게 이해할 수 있도록 시각화된 공격 진행 과정 814

스

스냅샷 공급자 선택 448

스마트 보호 278

스캐닝 유형 747

스캔 대상 867

스캔 예약 756, 777

스케줄 및 시작 조건 232

스케줄별로 Cyber Protection 정의 업데이

© Acronis International GmbH, 2003-2024

트 170
스케줄에 따라 백업 실행 383
스케줄의 조건이 충족될 때까지 대기 447
스크린샷 유효성 검사 192
스크린샷 전송을 통해 워크로드 모니터링 923
스크립트 220
스크립트 버전 226
스크립트 버전 비교 228
스크립트 복제 225
스크립트 빠른 실행 238
스크립트 상태 변경 227
스크립트 생성 221
스크립트 저장소 229
스크립트 파일 650
스크립트 편집 또는 삭제 226
스크립팅 계획 229
스크립팅 계획 생성 230
스크립팅 계획의 호환성 문제 236
스크립팅 계획의 호환성 문제 해결 237
스크립팅 작업의 출력 다운로드 228

시

시간 간격에 맞음 391
시간 기준 예약 384
시스템 경보 259
시스템 데이터베이스 복구 528
시스템 상태 복구 472
시스템 상태 선택 371
시스템 요구 사항 685
시작 조건 232, 388
시작하기 전에 125, 129, 134, 142, 147

실

실시간 보호 747, 755, 778
실제 데이터 전달 440
실제 데이터 전달 서비스 정보 440
실제 데이터 전달 프로세스 개요 440
실제 머신 복구 454
실제 머신에서 가상 머신으로 457
실제 머신으로의 장애 복구 수행 725
실제 부트 가능한 미디어 생성 645
실패한 로그인 모니터의 설정 958
실행 기록 보기 742
실행서를 사용하는 이유는 무엇인가요? 737

아

아카이브 내 중복 제거 415

악

악성 웹사이트 액세스 771
악용 방지 753

안

안전 복구 453
안티맬웨어 기능 746
안티맬웨어 보호 경보 252
안티맬웨어 소프트웨어 상태 모니터의 설정 959
안티바이러스 및 맬웨어 방지 기능 설정 748
안티바이러스 및 안티맬웨어 보호 구성 743
안티바이러스 및 안티맬웨어 보호 기능 746

© Acronis International GmbH, 2003-2024

알

알려진 문제 607

알려진 문제 및 제한 사항 812

알아야 할 사항 538

암

암호화 402

암호화 비밀번호 변경 983

암호화 비밀번호 설정 982

암호화 소프트웨어와의 재해 복구 호환성 669

암호화 소프트웨어와의 호환성 39

암호화된 백업 관련 작업 728

암호화된 백업에서 향상된 검색 활성화 604

압

압축 수준 417

애

애플리케이션 ID 및 암호를 가져오는 방법 549

애플리케이션 복구 510

애플리케이션 인식 백업 구성 607

애플리케이션 인식 백업에 필요한 사용자 권한 519

애플리케이션 인식 백업에서 데이터 복구 608

애플리케이션 인식 백업을 사용하려면 무엇이 필요합니까? 518

애플리케이션 인식 백업을 사용해야 하는 이유는 무엇입니까? 518

애플리케이션 인식 백업을 위한 추가 요구 사항 511

액

액세스 설정 341

액세스 설정 확인 또는 변경 337

액세스 제어에서 개별 USB 장치 제외 338

액세스 제어에서 장치 하위 클래스 제외 338

액세스 제어에서 프로세스 제외 351

액세스 키 500-501

어

어떤 항목을 백업할 수 있습니까? 541, 551, 556, 565, 569, 573, 589, 593, 597, 612

업

업데이트 전 백업 877

에

에이전트 기반 백업 및 비에이전트 백업 61

에이전트 로그 파일 저장 173

에이전트 및 컴포넌트 설치(MSI 및 MST 조합) 90

에이전트 수동 업데이트 162

에이전트 업데이트 162

에이전트 원격 설치의 작동 방식 118

에이전트 자동 DRS 비활성화 126

에이전트 제거 167

에이전트에 대한 시스템 요구사항 125, 129, 134, 142

에이전트에 대한 자동 할당 비활성화 632

에이전트와 컴포넌트 설치 및 설치 제거(EXE) 81

에이전트와 컴포넌트 설치 및 설치 제거(MSI 및 직접 선택) 90

© Acronis International GmbH, 2003-2024

에이전트의 무단 설치 제거 또는 변경의 방지 166

에이전트의 시스템 요구 사항 62

여

여러 네트워크 연결을 미리 구성 658

여러 제품 버전 간의 백업 형식 호환성 415

연

연결 설정 674

영

영구 장애 조치 수행 624

영향받은 워크로드에서 IOC 검토 및 완화 835

영향을 받은 워크로드에 대한 대응 조치 정의 843

예

예 82-83, 91-92, 103-104, 136-137, 390-394, 399

Fedora 14에서 수동으로 패키지 설치 67

하드 디스크에 불량 블록이 있는 경우의 응급 백업 388

예약 232, 283, 867, 875

예약된 스캔 747

오

오류 발생 시 재시도 418, 476

오류 발생 시 재시도 횟수 구성 194

오류 처리 418, 476, 625

오류가 발생한 VSS Writer 무시 448

오프호스트 데이터 처리 185

온

온프레미스 관리 서버용 라이센스 관리 182

온프레미스의 부트 가능한 미디어를 사용한 복구 660

옵

옵션 설명 429

완

완료에 대해서 알아야 할 사항 620

완료와 일반 복구 비교 620

요

요구 사항 471, 482

요청 시 패치 설치 884

운

운영 체제 복구용으로 부트 가능한 미디어 생성 643

운영 체제별 지원되는 보호 기능 41

운영 패치 보호 계획 구성 882

워

워크로드 301

워크로드 네트워크 상태 265

워크로드 다시 시작 849

워크로드 등록 변경 115

워크로드 자격 증명 915

워크로드 패치 847

워크로드별 상위 인시던트 분산 262

워크로드에 대한 모니터링 경보 보기 977

워크로드에 대한 원격 연결 851

© Acronis International GmbH, 2003-2024

워크로드에 보호 계획 적용 202

워크로드에 자격 증명 할당 916

워크로드에서 공개된 공격의 침해 지표(IOC) 확인 834

워크로드에서 온디맨드 포렌식 백업 실행 850

워크로드에서 자격 증명 할당 해제 917

워크로드와 파일의 백업 및 복구 관리 361

워크로드의 네트워크 분리 관리 844

워크로드의 상태와 성능 모니터링 933

원

원격 Linux 워크로드에서 사운드 리디렉션 902

원격 macOS 워크로드에서 사운드 리디렉션 901

원격 Windows 워크로드에서 사운드 리디렉션 901

원격 관리 계획 903

원격 관리 계획 생성 903

원격 관리 계획과의 호환성 문제 913

원격 관리 계획과의 호환성 문제 해결 914

원격 관리 계획에 워크로드 추가 910

원격 관리 계획에서 워크로드 제거 911

원격 데스크탑 Notifier 931

원격 데스크탑 또는 원격 지원을 위한 원격 워크로드로의 연결 902

원격 데스크탑 또는 원격 지원을 위해 관리 대상 워크로드에 연결 918

원격 데스크탑 또는 원격 지원을 위해 워크로드에 연결 895

원격 사운드 리디렉션 901

원격 설치를 위해 머신 준비 121

원격 세션 녹화 및 재생 929

원격 세션 위젯 278

원격 연결 프로토콜 900

원래 머신 외의 머신에 SQL 데이터베이스 복구 524

원래 머신에 SQL 데이터베이스 복구 522

원본 초기 RAM 디스크로 되돌리기 465

원클릭 복구 432

원클릭 복구 비활성화 434

원클릭 복구 활성화 433

원클릭 복구를 사용하여 머신 복구 434

웹

웹 클라이언트를 통해 관리 대상 워크로드에 연결 920

웹 호스팅 서버 보호 615

웹사이트 및 호스팅 서버 보호 612

웹사이트 백업 613

웹사이트 보호 612

웹사이트 복구 614

웹사이트를 백업하려면 무엇이 필요합니까? 612

위

위반 발생 시 경보 알림 수신 814

위양성 인시던트 수정 841

위젯 유형에 따라 보고된 데이터 290

위협 상태 262

위협 피드 278

위협 피드 설정 정의 835

위협 피드를 사용하여 워크로드와 관련해 공개된 공격 확인 815

© Acronis International GmbH, 2003-2024

유

유용한 팁 553, 585

유효성 검사 188

유효성 검사 계획 생성 189

유효성 검사 방법 191

유효성 검사 상태 189

의

의심스러운 레지스트리 항목에 대한 대응 조치 정의 858

의심스러운 파일에 대한 대응 조치 정의 857

의심스러운 프로세스에 대한 대응 조치 정의 853

이

이메일 메시지 및 회의 복구 579

이메일 알림 정책 구성 978

이벤트 매개변수 387

이벤트별 스케줄 386

이상 현상 기반 모니터링 933

인

인덱스 업데이트, 다시 구축 또는 삭제 603

인스턴스 복구 609

인시던트 검토 817

인시던트 상세 정보 분석 822

인시던트 수정 837

인시던트 완화를 위해 수행한 작업 파악 832

인시던트 조사 824

인시던트 페이지에서 인시던트 관리 814

인시던트란? 818

인시던트의 공격 단계 조사 827

인시던트의 범위와 영향 파악 821

일

일본어 논리식 803

일본어를 제외한 지원되는 모든 언어에 대한 논리식 802

일정 예약 445

자

자격 증명 삭제 916

자격 증명 추가 915

자동 검색 및 수동 검색 수행 118

자동 검색의 작동 방식 116

자동 대응 조치 구성 965

자동 드라이버 검색 464

자동 실행 기능 상태 모니터의 설정 960

자동 테스트 장애 조치 712, 714

자동 테스트 장애 조치 구성 715

자동 테스트 장애 조치 비활성화 716

자동 테스트 장애 조치 상태 확인 715

자동 패치 승인 880

자동 패치 승인 구성 880

자동 패치 승인 및 테스트용 사용 사례 881

자동 패치 승인(테스트 없음)용 사용 사례 883

자동으로 에이전트 업데이트 164

자체 보호 751

작

작동 실행서 관련 작업 741

작동 실행서 생성 738

작동 실행서 실행 중지 742

© Acronis International GmbH, 2003-2024

작동 실행서의 실행 741

작동법 212, 266, 279, 282, 373, 405, 424, 600, 762, 769

작업 794

작업 시작 조건 447

작업 실패 처리 446

작업 실행 건너뛰기 447

작업 필드 값 354

작업의 원리는 다음과 같습니다. 810

장

장애 복구 624

장애 복구 옵션 625

장애 복구 작동 방식 718

장애 조치 수행 716

장애 조치 작동 방식 711

장애 조치 중지 623

장애 조치 테스트 712

장치 IP 주소 확인 394

장치 그룹 311

장치 그룹에 지원되는 계획 312

장치 유형 허용 목록 346

장치 제어 경보 258, 353

장치 제어 경보 확인 341

장치 제어 모듈 사용 332

장치 제어 사용 334

장치 제어 활성화 또는 비활성화 335

장치 탭 296

재

재배포 631

재부팅을 이용한 복구가 실패하는 경우 시스템 정보 저장 476

재해 복구 경보 246

재해 복구 구현 666

재해 복구 기능 설정 671

재해 복구 보호 계획 생성 671

재해 복구 장애 조치 852

저

저장된 루틴 복구 612

적

적응 코덱 900

적응적 적용 모드를 사용하여 사용자 정책 갱신 796

전

전술별 감지 264

전제조건 697, 700-701

전체 Google Drive 복구 594

전체 OneDrive 복구 567

전체 Shared Drive 복구 598

전체 경로 복구 477

전체 머신 선택 365

전체 사서함을 PST 데이터 파일로 복구 561

전체 서버 복구 609

전체 인시던트 수정 837

전체 텍스트 검색 602

전체 팀 복구 574

정

정리 195

정보 매개변수 102

© Acronis International GmbH, 2003-2024

정적 그룹 312

정적 그룹 생성 313

정적 그룹과 동적 그룹 312

정적 그룹에 워크로드 추가 314

정지 전 및 해제 후 스크립트 자동 실행 632

정책 검토 및 관리 794

정책 권한 499, 501

정책 규칙을 트리거하는 요소는? 792

제

제거 매개변수 102

제외 779

제한 사항 32, 34-38, 135, 143, 148, 198, 217, 266, 366-367, 370, 372, 378, 454, 467, 475, 548, 565, 570, 573, 584, 590, 593, 597, 607, 613, 621, 627, 663, 668, 785, 982

제한 사항 및 알려진 문제 581

조

조정(작동 실행서) 737

조직 매핑 809

주

주간 백업 451

주요 기능 666

준

준비 55, 74, 463

WinPE 2.x 및 3.x 656

WinPE 4.0 이상 657

중

중간 스냅샷 199

중요 팁 397

즉

즉시 확인해야 하는 보안 인시던트를 분석하는 방법 819

즉시 확인해야 하는 인시던트의 우선 순위 지정 819

지

지속적인 데이터 보호(CDP) 372

지역 간 복제 상태 987

지역 중복 스토리지 986

지역 중복 스토리지 활성화 및 비활성화 987

지원되는 Apple 및 서드 파티 제품 866

지원되는 Apple 제품 866

지원되는 Linux 제품 867

지원되는 macOS용 서드 파티 제품 866

지원되는 MariaDB 버전 30

지원되는 Microsoft Exchange Server 버전 29

지원되는 Microsoft SharePoint 버전 29

지원되는 Microsoft SQL Server 버전 29

지원되는 Microsoft 및 서드 파티 제품 864

지원되는 Microsoft 제품 864

지원되는 MySQL 버전 30

지원되는 Oracle 데이터베이스 버전 30

지원되는 SAP HANA 버전 30

지원되는 Windows OS용 서드 파티 제품 866

지원되는 Windows 운영 체제 780

지원되는 가상 머신 유형 197

지원되는 가상화 플랫폼 30, 667

지원되는 대상 375

지원되는 데이터 소스 374

© Acronis International GmbH, 2003-2024

지원되는 모바일 장치 538

지원되는 버전 581

지원되는 스토리지 클래스 499

지원되는 언어 800-801, 803-804

지원되는 운영 체제 666

지원되는 운영 체제 및 버전 42

지원되는 운영 체제 및 환경 23

지원되는 원격 데스크탑 및 지원 기능 896

지원되는 웹 브라우저 22

지원되는 위치 188, 195, 401

지원되는 클러스터 구성 515-516

지원되는 파일 시스템 50

지원되는 플랫폼 217, 743, 899

지원되지 않는 기능 982

지점 및 사이트 간 연결 설정 관리 702

지점 및 사이트 간 원격 VPN 액세스 683

지점 및 사이트 간 원격 VPN 액세스 구성 692

지정된 기간(일) 동안 성공적인 백업이 진행되지 않음 409

집

집계된 워크로드 357

집계된 워크로드 사용 358

처

처리하는 동안 메시지 및 대화 상자 표시 안 함(자동 모드) 418

처리할 동안 메시지 및 대화 상자 표시 안 함(자동 모드) 476

체

체크섬 확인 191

초

초기 복제본 시딩 625

최

최근 영향 받은 워크로드 관련 데이터 다운로드 275

최근 영향 받은 항목 274

최상위 객체 651

최초 연결 구성 685

추

추가 Cyber Protection 도구 982

추가 매개변수 101

추가 예약 옵션 394

추가 옵션 384

취

취약성 평가 864

취약성 평가 및 패치 관리 864

취약성 평가 설정 867

취약성 평가 위젯 271

취약한 머신 271

카

카테고리별 누락 업데이트 273

캐

캐시 스토리지 171

커

커널 매개변수 647

© Acronis International GmbH, 2003-2024

컨

컨트롤 유형 652

컴

컴퍼넌트에 대한 자동 업데이트 169

컴퍼넌트의 동적 설치 및 설치 제거 80

컴퓨터의 USB 장치 목록 351

컴퓨팅 포인트 670

크

크립토마이닝 프로세스 감지됨 752

클

클라우드 Agent for Microsoft 365 사용 553

클라우드 간 그룹과 클라우드 간 그룹이 아닌 그룹 312

클라우드 간 백업에서 검색 601

클라우드 간 백업을 수동으로 실행 184

클라우드 간 워크로드가 아닌 워크로드의 속성 검색 318

클라우드 간 워크로드의 속성 검색 317

클라우드 네트워크 인프라 674

클라우드 방화벽 활동 확인 736

클라우드 백업에서 실행 중인 머신의 완료 620

클라우드 사이트에서 사용되지 않은 고객 환경의 자동 삭제 684

클라우드 서버 관리 732

클라우드 서버 백업 737

클라우드 서버용 방화벽 규칙 733

클라우드 서버용 방화벽 규칙 설정 734

클라우드 스토리지에서 복구 649

클라우드 스토리지에서 파일 다운로드 467

클라우드 애플리케이션 275

클라우드 애플리케이션의 백업 계획 184

클라우드 에이전트 및 로컬 에이전트 545

클라우드 전용 모드 675, 695

클라우드 전용 모드 구성 685

클러스터 Hyper-V 머신 백업 638

클러스터 데이터 백업 및 복구에 필요한 에이전트 수는? 515

클러스터 백업 모드 416

클러스터 인식 백업 516

클러스터 인식 백업 및 복구에 필요한 에이전트 수는? 517

키

키워드 그룹 805

테

테넌트 수준 선택 295

테스트 장애 조치 수행 712

테스트 패치 보호 계획 구성 881

테스트 패치 보호 계획 실행 및 안전하지 않은 패치 거절 883

테이블 복구 611

특

특수 문자 또는 공백이 포함된 비밀번호 114

특정 고객의 워크로드 확인 297

팀

팀 사서함 복구 577

팀 사서함 항목을 PST 파일에 복구 578

팀 사이트 또는 사이트의 특정 항목 복구 580

© Acronis International GmbH, 2003-2024

팀 선택 574

팀 채널 또는 팀 채널의 파일 복구 575

파

파일 또는 폴더 선택 369

파일 및 폴더 크기 모니터의 설정 957

파일 및 폴더용 정책 규칙 370

파일 복구 466

파일 수준 백업 스냅샷 421

파일 수준 보안 477

파일 전송 921

파일 제외 476

파일 필터(포함/제외) 419

파일은 어떻게 격리 폴더로 이동합니까? 781

파일의 날짜 및 시간 476

파트너 관리자로 Cyber Protect 콘솔 사용 294

파트너 관리자용 정보 307

파트너 수준에서 동적 장치 그룹 생성 297

파트너 수준에서 정적 장치 그룹 생성 297

파트너 테넌트 수준에서 머신 자동 검색 수행 298

파트너 테넌트(모든 고객) 수준 294

패

패치 관리 872

패치 관리 워크플로우 872

패치 목록 수명 구성 879

패치 설치 내역 273

패치 설치 상태 272

패치 설치 요약 273

패치 설치 위젯 272

퍼

퍼블릭 클라우드 계정 액세스 관리 498

퍼블릭 클라우드 백업 위치 확인 및 업데이트 497

퍼블릭 클라우드 스토리지에 백업하려면 충족해야 하는 액세스 요구 사항 499

퍼블릭 클라우드 연결 액세스 권한 갱신 507

퍼블릭 클라우드 연결 액세스 권한 제거 508

퍼블릭 클라우드 연결 액세스 권한 추가 505

퍼블릭 클라우드에 워크로드 백업 491

포

포렌직 데이터 421

포렌직 데이터를 포함하는 백업에 대한 인증서 받기 425

포렌직 데이터를 포함하는 백업의 공증 424

포렌직 백업 프로세스 422

포트 685

포함 및 제외 필터 420

프

프로덕션 장애 조치 711

프로세스 상태 모니터의 설정 954

프로세스별 CPU 사용량 모니터의 설정 950

프로세스별 네트워크 사용량 모니터의 설정 952

프로세스별 디스크 전송 속도 모니터의 설정 951

프로세스별 메모리 사용량 모니터의 설정 951

프록시 서버 설정 구성 68

© Acronis International GmbH, 2003-2024

플

플래시백 477

플랫폼 간 복구 452

플랫폼별로 지원되는 기능 744

필

필수 사용자 권한 521, 547, 583

필요에 따라 Cyber Protection 정의 업데이트 171

필요한 백업 유형 확인 61

필요한 에이전트 57

필요한 에이전트 수는? 126, 130, 134, 142

필요한 역할 147

필요한 패키지가 이미 설치되어 있습니까? 65

필요한 포트 147

필터 기준 420

필터링할 카테고리 771

하

하드웨어 변경 모니터의 설정 942

하드웨어 인벤토리 890

하드웨어 인벤토리 스캐닝 활성화 890

하드웨어 인벤토리 위젯 277

하드웨어 인벤토리 찾아보기 891

할

할당량 615

허

허용 목록 설정 783

허용 목록에 격리된 파일 추가 783

허용 목록에 수동 추가 783

허용 목록에 자동 추가 783

허용 목록의 항목 관련 상세 정보 확인 784

현

현재 보호 수준 이해 240

현재 완화되지 않은 인시던트 확인 820

협

협업 및 커뮤니케이션 애플리케이션 보호 239

호

호스팅 제어판 통합용 개별 보호 계획 211

확

확장자 및 예외 규칙 284

활

활동 대시보드 241

활동 탭 285, 296

활성 상태의 지점 및 사이트 간 연결 703

회

회사 또는 부서에 대한 정책 갱신 795

회사 또는 부서에 있는 한 명 이상의 사용자에 대한 정책 갱신 795

© Acronis International GmbH, 2003-2024