

Cyber Disaster Recovery Cloud

24.03



목차

Cyber Disaster Recovery Cloud 정보	5
주요 기능	5
소프트웨어 요구 사항	6
지원되는 운영 체제	6
지원되는 가상화 플랫폼	6
제한 사항	7
Cyber Disaster Recovery Cloud 평가판 버전	9
Geo-redundant Cloud Storage 사용 시의 제한 사항	10
암호화 소프트웨어와의 재해 복구 호환성	11
컴퓨팅 포인트	12
재해 복구 보호 계획 생성	14
다음에 수행할 작업	14
복구 서버 기본 매개변수 편집	15
클라우드 네트워크 인프라	16
연결 설정	17
네트워킹 개념	17
클라우드 전용 모드	18
사이트 간 OpenVPN 연결	19
다중 사이트 IPsec VPN 연결	25
지점 및 사이트 간 원격 VPN 액세스	26
클라우드 사이트에서 사용되지 않은 고객 환경의 자동 삭제	27
최초 연결 구성	28
클라우드 전용 모드 구성	28
사이트 간 OpenVPN 구성	28
다중 사이트 IPsec VPN 구성	29
Active Directory 도메인 서비스 사용 가능성 관련 권장 사항	34
지점 및 사이트 간 원격 VPN 액세스 구성	35
네트워크 관리	36
네트워크 관리	36
VPN 어플라이언스 설정 관리	40
VPN 게이트웨이 다시 설치	40
사이트 간 연결 활성화 및 비활성화	41
사이트 간 연결 유형 전환	41
IP 주소 다시 할당	42
사용자 정의 DNS 서버 구성	43

사용자 정의 DNS 서버 삭제	44
MAC 주소 다운로드	44
로컬 라우팅 구성	45
L2 VPN을 통한 DHCP 트래픽 허용	45
지점 및 사이트 간 연결 설정 관리	45
활성 상태의 지점 및 사이트 간 연결	46
로그 작업	47
IPsec VPN 구성 문제 해결	49
복구 서버 설정	53
복구 서버 생성	53
장애 조치 작동 방식	55
프로덕션 장애 조치	55
장애 조치 테스트	56
자동 테스트 장애 조치	56
테스트 장애 조치 수행	57
자동 테스트 장애 조치	59
장애 조치 수행	60
장애 복구 작동 방식	62
대상 가상 머신으로 장애 복구	63
대상 실제 머신으로 장애 복구	68
수동 장애 복구	72
암호화된 백업 관련 작업	73
Microsoft Azure 가상 머신 관련 작업	74
기본 서버 설정	75
기본 서버 생성	75
기본 서버 관련 작업	77
클라우드 서버 관리	78
클라우드 서버용 방화벽 규칙	79
클라우드 서버용 방화벽 규칙 설정	79
클라우드 방화벽 활동 확인	82
클라우드 서버 백업	83
조정(작동 실행서)	84
실행서를 사용하는 이유는 무엇인가요?	84
작동 실행서 생성	84
런북 매개변수	86
작동 실행서 관련 작업	87
작동 실행서의 실행	87

작동 실행서 실행 중지	88
실행 기록 보기	88
사이트 간 OpenVPN - 추가 정보	89
용어 설명	96
색인	98

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 생성](#)을 참조하십시오.
- 재해 복구 클라우드 인프라를 수동으로 설정하고 각 단계를 제어합니다. "복구 서버 설정"(53페이지)을(를) 참조하십시오.

주요 기능

참고

일부 기능을 사용하려면 적용되는 라이선스 모델에 따라 추가 라이선스가 필요할 수 있습니다.

- Cyber Disaster Recovery Cloud 서비스를 단일 콘솔에서 관리
- 보안 VPN 터널을 통해 최대 23개의 로컬 네트워크를 클라우드로 확장
- VPN 어플라이언스¹ 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

¹로컬 네트워크와 클라우드 사이트 네트워크를 보안 VPN 터널로 연결하는 특수 가상 머신입니다. VPN 어플라이언스는 로컬 사이트에 디플로이됩니다.

소프트웨어 요구 사항

지원되는 운영 체제

복구 서버를 통한 보호는 다음 운영 체제에서 테스트되었습니다.

- 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/71616>을 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.

- 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:

- 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.
-

암호화 소프트웨어와의 호환성에 대한 자세한 정보는 사이버 보호 사용자 안내서를 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 중속 엔티티인 물리적 CPU(중앙 처리 장치)를 나타냅니다.

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 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 서버를 비롯한 클라우드 네트워크 인프라가 생성됩니다. 복구 서버는 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

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"(42페이지)을(를) 참조하십시오.
-

재해 복구 보호 계획을 생성하려면

- Cyber Protect 콘솔에서 **장치 > 모든 장치**로 이동합니다.
- 보호하려는 머신을 선택합니다.
- 보호**를 클릭하고 **계획 생성**을 클릭합니다.
보호 계획 기본 설정이 열립니다.
- 백업 옵션을 구성합니다.
재해 복구 기능을 사용하려면 계획은 전체 머신을 백업하거나 부팅과 필요한 서비스 제공에 필수적인 디스크만 클라우드 스토리지에 백업해야 합니다.
- 모듈 이름 옆의 스위치를 클릭하여 재해 복구 모듈을 활성화합니다.
- 생성**을 클릭합니다.
계획이 생성된 후 선택된 머신에 적용됩니다.

다음에 수행할 작업

- 복구 서버의 기본 구성을 편집할 수 있습니다. 자세한 내용은 "복구 서버 설정"(53페이지)을(를) 참조하십시오.

- 기본 네트워킹 구성을 편집할 수 있습니다. 자세한 내용은 "연결 설정"(17페이지)을(를) 참조하십시오.
- 복구 서버 기본 매개변수 및 클라우드 네트워크 인프라에 대해 자세히 알아볼 수 있습니다. 자세한 내용은 "복구 서버 기본 매개변수 편집"(15페이지) 및 "클라우드 네트워크 인프라"(16페이지)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.

참고

존재하지 않으면 복구 서버가 생성됩니다. 기존 복구 서버는 변경되거나 다시 생성되지 않습니다.

복구 서버 기본 매개변수를 편집하려면

1. 장치 > 모든 장치로 이동합니다.
2. 장치를 선택하고 재해 복구를 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 인프라 를 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 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" (36페이지)을(를) 참조하십시오.
- 사이트 간 OpenVPN 연결을 설정해야 하는 경우 VPN 어플라이언스를 다운로드한 후 설치하십시오. "사이트 간 OpenVPN 구성" (28페이지)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 라이선스 모델에 따라 추가 라이선스가 필요할 수 있습니다.

Cyber Disaster Recovery Cloud에서 클라우드 사이트에 대한 다음 연결 유형을 정의할 수 있습니다.

- **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 지정 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, 지정 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.

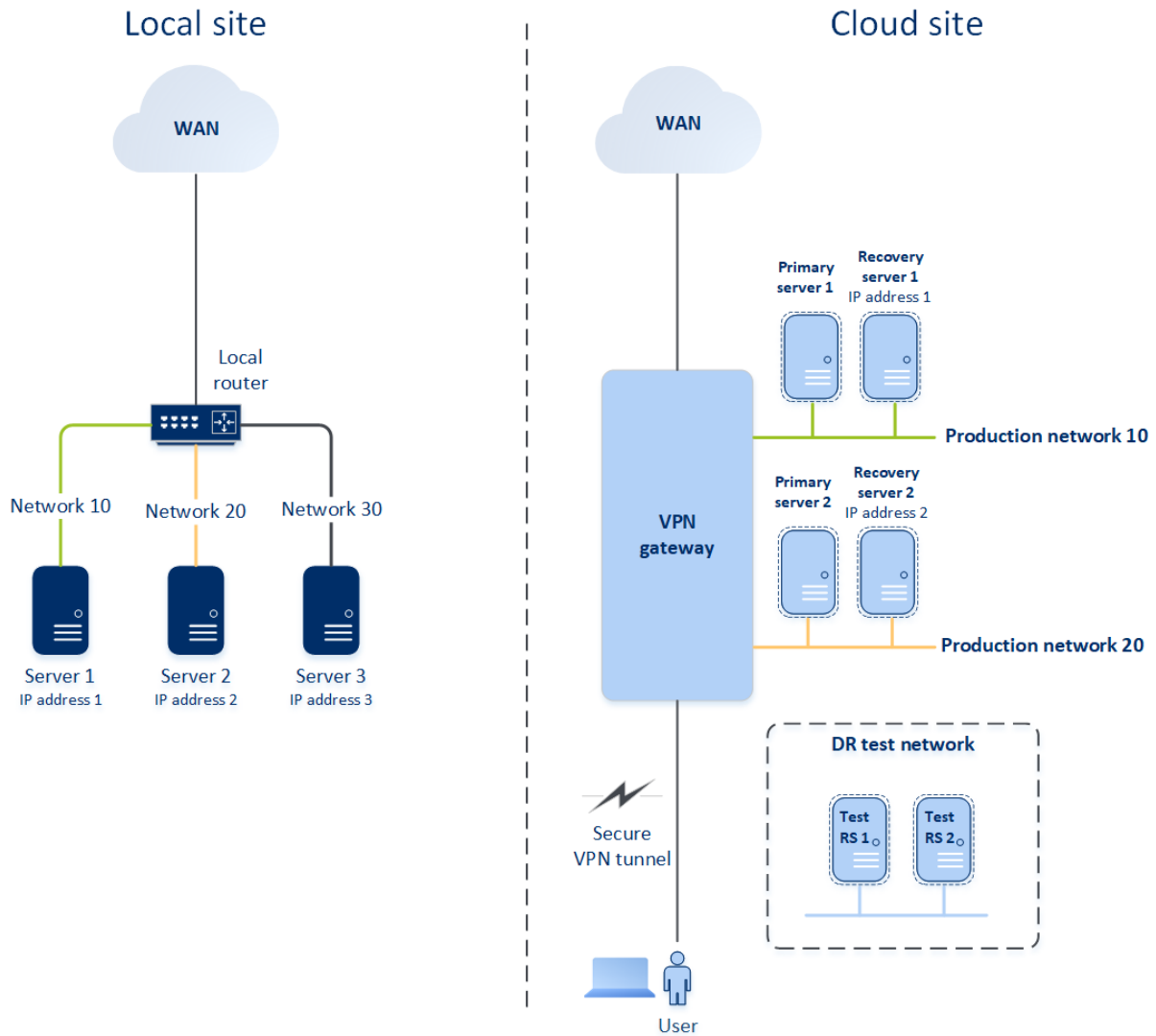
로컬 사이트 액세스의 경우, 이 유형의 연결에는 로컬 사이트에 VPN 어플라이언스 디플로이가 필요합니다.

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.

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

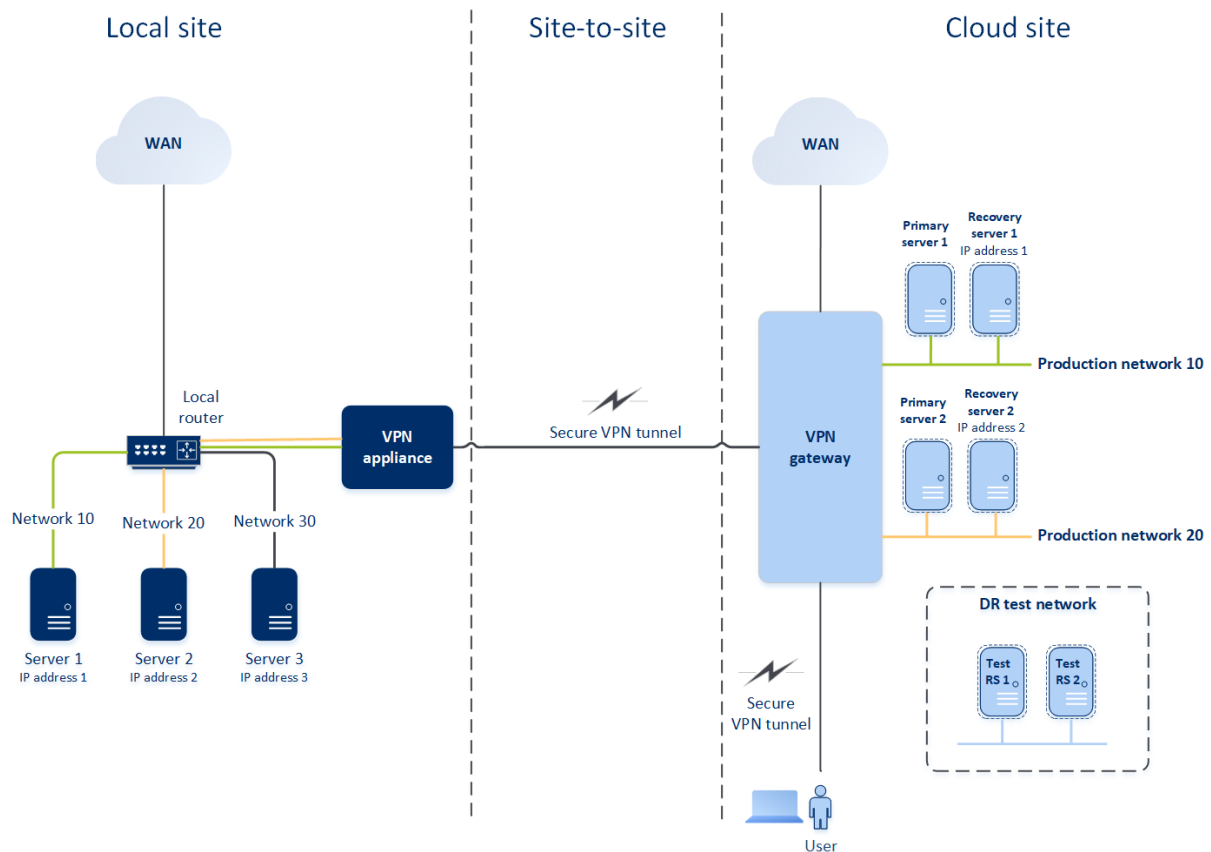
참고

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.

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 방지하기 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 함

니다. 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 지정 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 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.

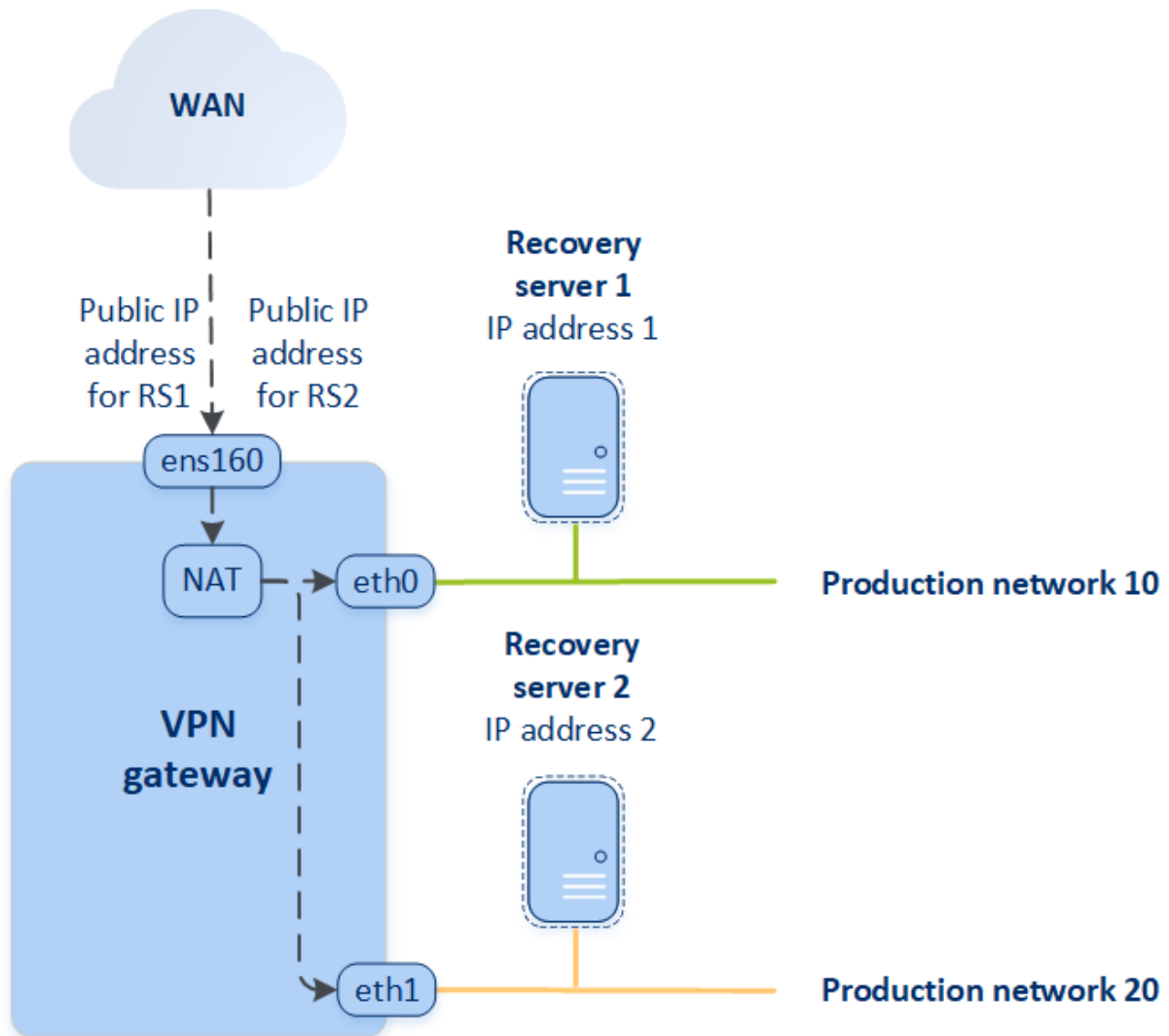
복구 서버를 만들 때 다음과 같은 네트워크 매개변수를 지정해야 합니다.

- **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

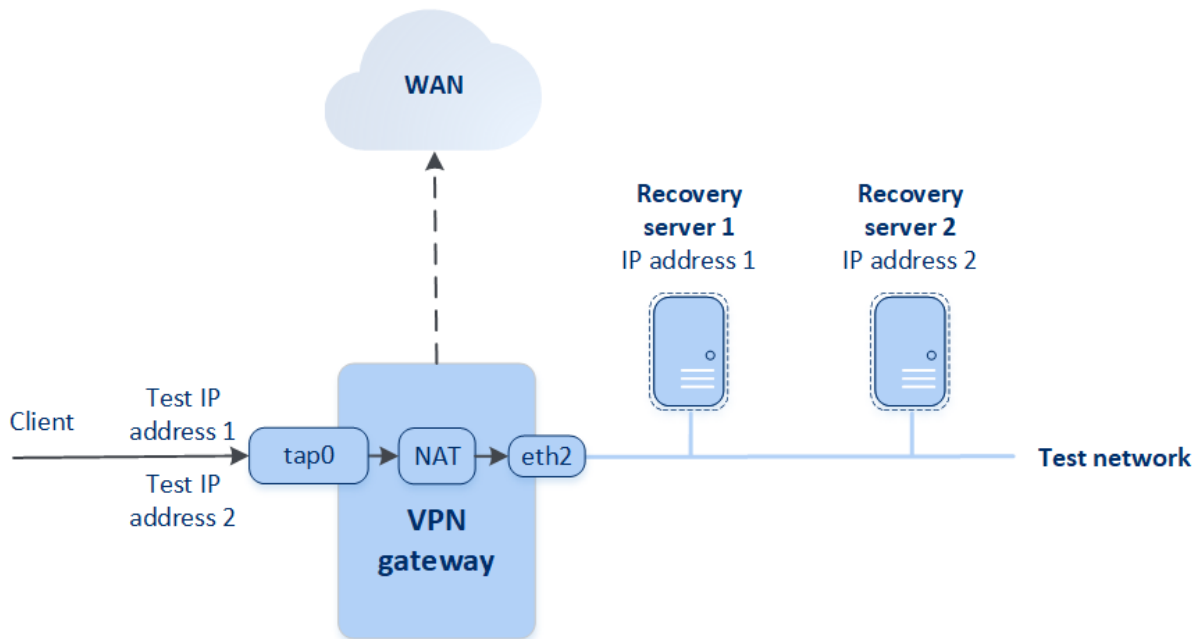
복구 서버 생성 시 공용 IP 주소를 할당하는 경우 이 IP 주소를 통해 인터넷에서 복구 서버를 사용할 수 있게 됩니다. 대상 공용 IP 주소로 인터넷에서 패킷이 수신되면 VPN 게이트웨이는 NAT를 사용하여 해당 운영 IP 주소로 이를 다시 매핑한 다음, 복구 서버로 전송합니다.

Cloud site



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.

Cloud site



사이트 간 OpenVPN에 대한 자세한 내용은 "사이트 간 OpenVPN - 추가 정보"(89페이지)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.

- **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 통해서만 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, 구성된 세그먼트가 로컬 네트워크 세그먼트와 겹치지 않는지 확인해야 합니다. 로컬 사이트와 클라우드 사이트 간에 보안 VPN 터널이 설정됩니다. 로컬 서버와 클라우드 서버가 동일한 인터넷 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 인터넷 세그먼트를 연결합니다.

- 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"(43페이지)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

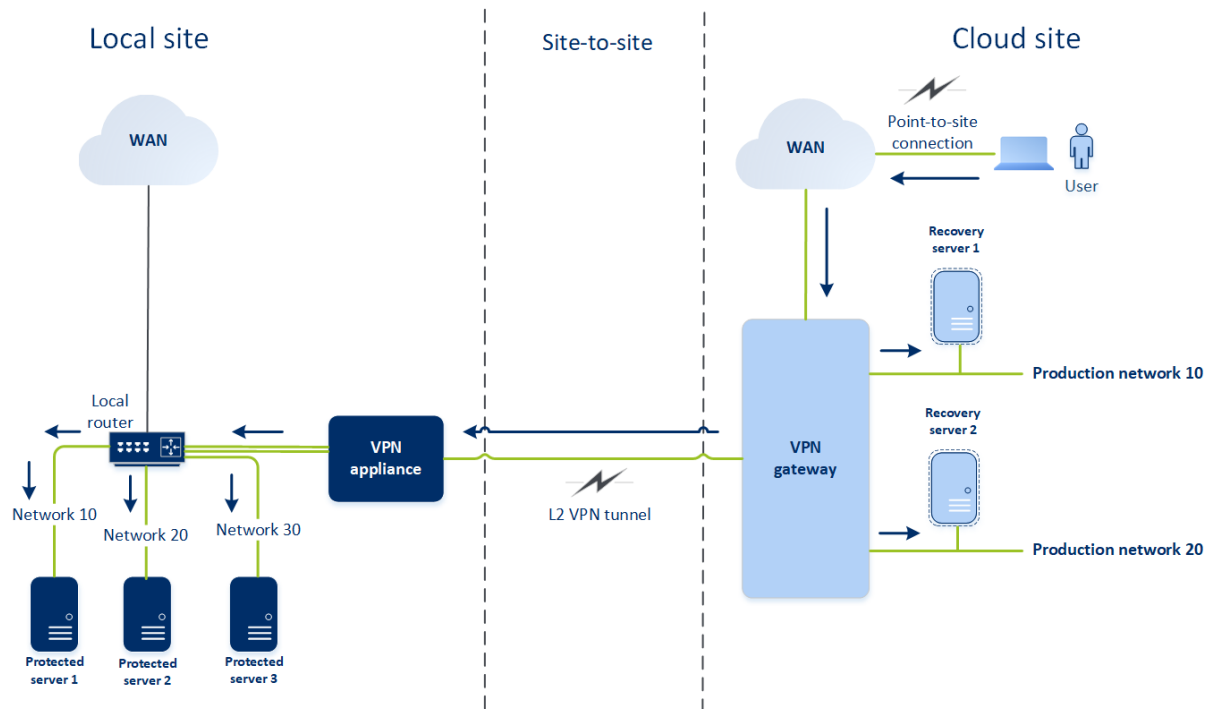
이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

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.



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 생성**한 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.

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 자습서](#)를 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.

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 컵니다.
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.

- **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 할당**합니다.

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"(29페이지) 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

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"(32페이지)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"(32페이지)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.

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

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 시간을 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 퍼지도 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

매개변수	설명
	하는 최대 비율입니다(연결이 많은 호스트에서 중요함). 키 다시 생성 퍼지 값은 100%를 초과할 수 없습니다. 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 작업을 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

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"(43페이지)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"(43페이지)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 자습서](#)를 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 생성](#)합니다.
 - "회사 관리자" 또는 "사이버 보호" 사용자 역할.
5. OpenVPN 클라이언트를 구성합니다.

- 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 코드**를 제공해야 합니다.

중요

계정의 2단계 인증을 활성화한 후 구성 파일을 다시 생성하고 기존 OpenVPN 클라이언트에 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

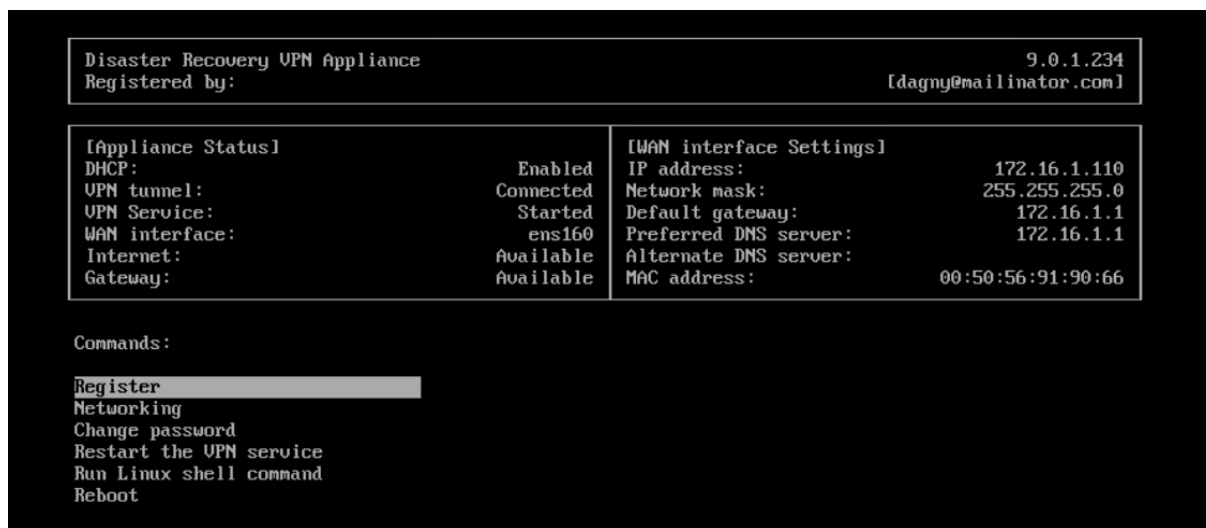
참고

일부 기능을 사용하려면 적용되는 라이선스 모델에 따라 추가 라이선스가 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.



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.

```
Disaster Recovery VPN Appliance
Registered by:
9.0.1.234
[dagny@mailinator.com]

Command: Networking \ configure ens160

Usage:
<Up>, <Down> - to select parameter
<Esc> - to cancel the command

IP address:
VPN gateway IP address:
Network mask:
Default gateway:
Preferred DNS server:
Alternate DNS server:
```

- 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 > 연결로 이동합니다.
2. 클라우드 사이트에서 클라우드 네트워크 추가를 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 네트워크를 삭제하려면

참고

클라우드 서버가 하나라도 포함되어 있는 클라우드 네트워크는 삭제할 수 없습니다. 먼저, 클라우드 서버를 삭제한 다음, 네트워크를 삭제하십시오.

1. 재해 복구 > 연결로 이동합니다.
2. 클라우드 사이트에서 삭제할 네트워크 주소를 클릭합니다.
3. 삭제를 클릭하고 작업을 확인합니다.

클라우드 네트워크 매개변수를 변경하려면

1. 재해 복구 > 연결로 이동합니다.
2. 클라우드 사이트에서 편집할 네트워크 주소를 클릭합니다.
3. 편집을 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.

IP 주소 비밀관성에 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 할당](#)을 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.

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 **WAN**으로 사용할 인터페이스를 정의합니다.
- 등록을 반복하여 등록 계정을 등록/변경합니다.
- VPN 서비스를 다시 시작합니다.
- VPN 어플라이언스를 재부팅합니다.
- Linux 셸 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.

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
VPN 게이트웨이 모드	L2 Open VPN	L3 IPsec VPN
네트워크 세그먼트	로컬 네트워크를 클라우드 네트워킹으로 확장	로컬 네트워크 및 클라우드 네트워크 세그먼트가 겹치면 안 됨
로컬 사이트로의 지정 및 사이트 간 액세스 지원	예	아니요
클라우드 사이트로의 지정 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 VPN**으로 **전환**을 클릭합니다.
4. **재구성**을 클릭합니다.
5. 클라우드 네트워크 및 클라우드 서버의 **IP 주소**를 다시 할당합니다.
6. **다중 사이트 IPsec 연결 설정**을 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 OpenVPN**으로 **전환**을 클릭합니다.
4. **재구성**을 클릭합니다.
5. 클라우드 네트워크 및 클라우드 서버의 **IP 주소**를 다시 할당합니다.
6. **사이트 간 연결 설정**을 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

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.

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.

MAC 주소 다운로드

MAC 주소 목록을 다운로드한 다음 추출하고 사용자 지정 DHCP 서버의 구성으로 가져올 수 있습니다.

전제조건:

- 클라우드 사이트에 대한 연결 유형 하나를 설정해야 합니다.
- MAC 주소를 가진 기본 서버 또는 복구 서버를 하나 이상 구성해야 합니다.

MAC 주소 목록을 다운로드하려면

1. Cyber Protect 콘솔에서 **재해 복구 > 연결**로 이동합니다.
2. **속성 표시**를 클릭합니다.
3. **MAC 주소 목록 다운로드**를 클릭한 다음 CSV 파일을 저장합니다.

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.
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

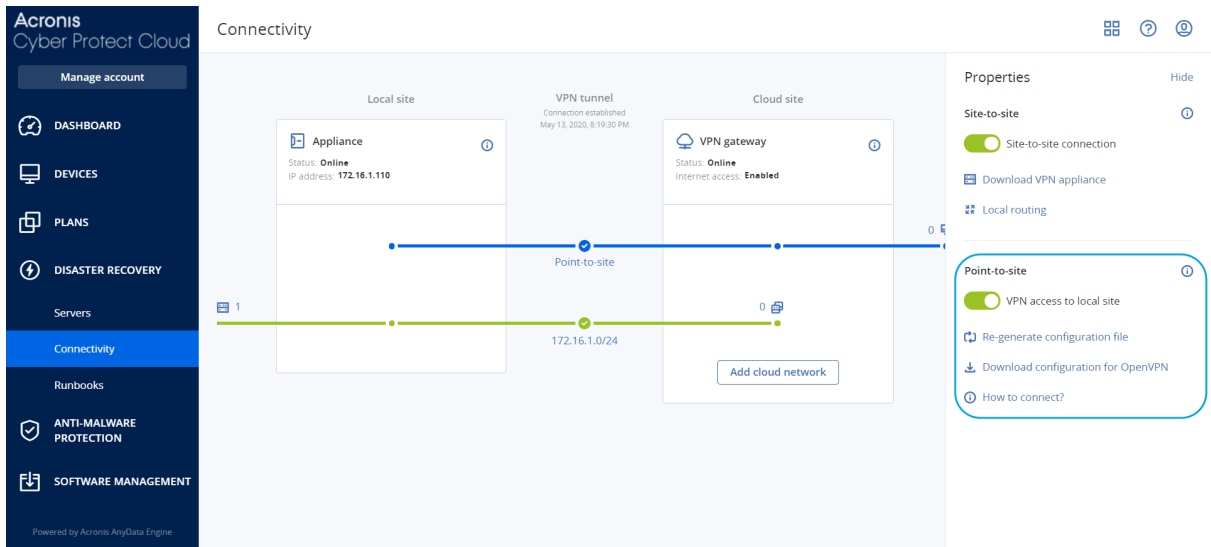
1. **재해 복구 > 연결** 탭으로 이동합니다.
2. **속성 표시**를 클릭합니다.
3. **L2 VPN을 통한 DHCP 트래픽 허용** 스위치를 활성화합니다.

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 않습니다.

OpenVPN 구성 다운로드

그러면 OpenVPN 클라이언트의 구성 파일이 다운로드됩니다. 이 파일은 클라우드 사이트에 대한 지점 및 사이트 간 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.

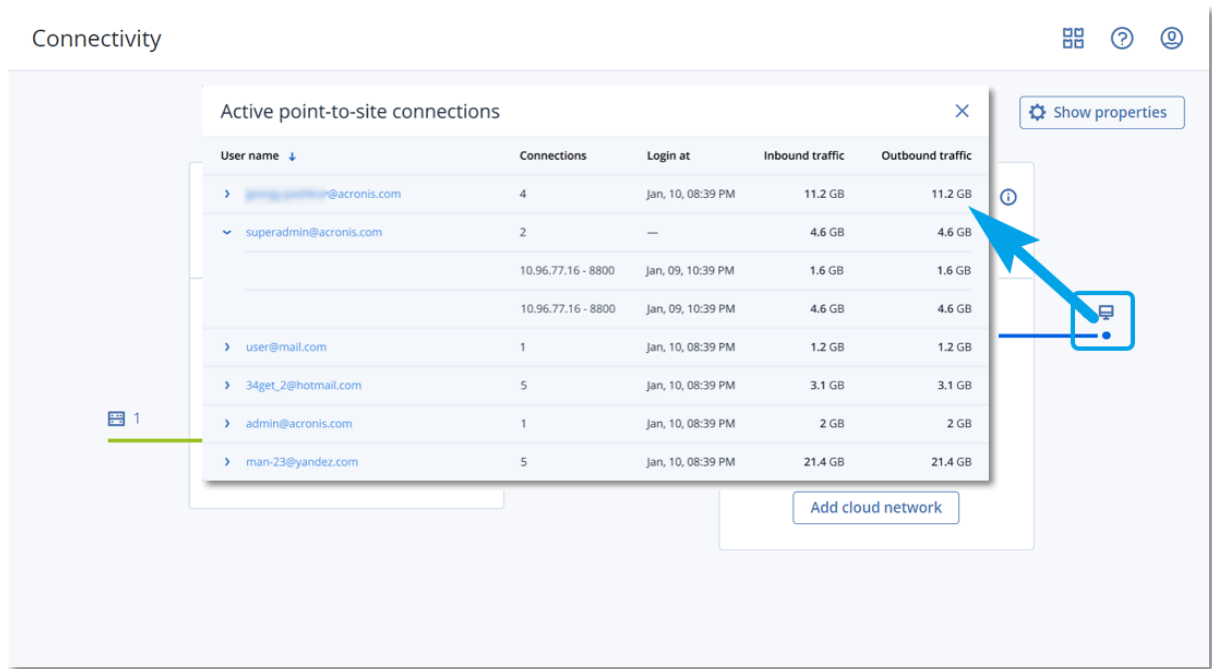
구성 파일이 업데이트되는 즉시 이전 구성 파일을 통한 연결이 불가능 해집니다. 지점 및 사이트 간 연결을 사용할 수 있는 사용자간에 새 파일을 배포해야 합니다.

활성 상태의 지점 및 사이트 간 연결

참고

이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

재해 복구 > 연결에서 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.



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.

dnsmasq.leases.txt - 현재 DHCP 주소 임대에 대한 정보가 포함되어 있습니다.

dnsmasq_log.txt - dnsmasq 서비스의 로그가 포함되어 있습니다.

ehtables.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.

resolv.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.

vpnservice_log.txt - VPN 서비스의 로그가 포함되어 있습니다.

vpnservice_status.txt - VPN 서버의 상태에 대한 정보가 포함되어 있습니다.

IPsec VPN 연결과 관련된 로그 파일에 대한 자세한 내용은 "다중 사이트 IPsec VPN 로그 파일"(51페이지) 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

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"(48페이지)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"(48페이지)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 tcpdump 도움말을 참조하십시오.

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 시도를 클릭하고 더 구체적인 오류 메시지가 표시되는지 확인합니다. 더 구체적인 오류 메시지란 알고리즘 불일치, 잘못된 사전에 공유된 키 등과 관련된 오류 메시지일 수 있습니다.

문 제	가 능 한 해 결 방 법
	참 고 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.
내 로컬 사이트와 클라우드 사이트 간의 연결 상태가 계속 연결 대기 중 으로 표시됩니다.	클라우드 사이트의 시작 작업이 추가로 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 작업이 경로로 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 작업을 시작으로 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 일치

문제	가능한 해결 방법
	하는지 확인합니다. Cisco ASA 등의 장치에서 로컬 사이트 및/또는 클라우드 사이트의 시작 작업이 경로로 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 비활성화를 클릭합니다. 3. IPsec 연결을 다시 클릭합니다. 4. 연결 활성화를 클릭합니다.

IPsec VPN 로그 파일 다운로드

참고

이 기능의 사용 가능 여부는 계정에서 활성화할 수 있는 서비스 할당량에 따라 다릅니다.

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 자습서](#)를 시청할 수도 있습니다.

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 복구를 클릭한 다음, 복구 서버 생성을 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"(12페이지)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** 주소를 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 라이선스가 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.

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.
15. [선택 사항] **클라우드 방화벽 규칙** 탭을 클릭하여 기본 방화벽 규칙을 편집합니다. 자세한 내용은 "클라우드 서버용 방화벽 규칙 설정"(79페이지)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.

Acronis
Cyber Protect Cloud

Manage account

DISASTER RECOVERY

Servers

Connectivity

Runbooks

ANTI-MALWARE PROTECTION

SOFTWARE MANAGEMENT

BACKUP STORAGE

REPORTS

SETTINGS

Servers

RECOVERY SERVERSPRIMARY SERVERS

All activities

Search

☐ Name	Status	State	RPO compliance	VM state	
Win16	OK	Standby	—	—	...
cen7-sg7	OK	Standby	—	—	...
Cen_vg-1	OK	Failover	Not set	On	...
Cen_mb-3	OK	Testing failover	Not set	On	...
Cen_mb-2	OK	Failback	Not set	Off	...
Cen_mb-1	OK	Failback	Not set	Off	...

Powered by Acronis AnyData Engine

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.

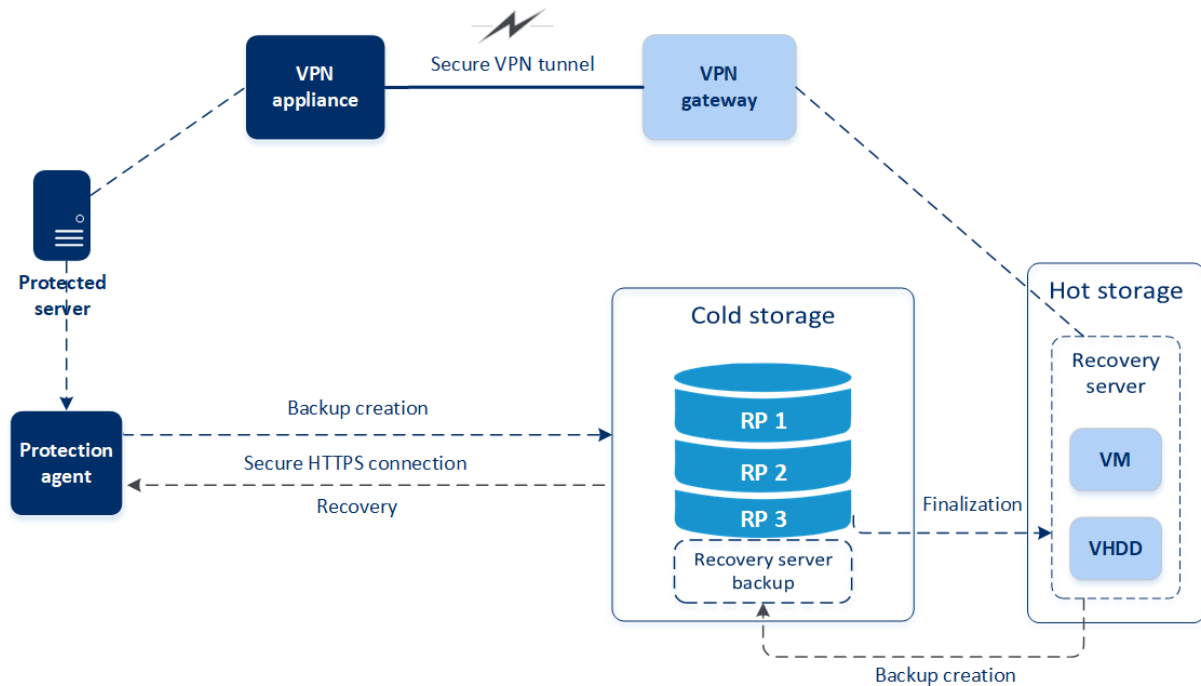
참고

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.

복구 서버에 보호 에이전트가 있는 경우 에이전트 서비스가 중지되어 백업을 시작하거나 오래된 상태를 백업 컴퓨터에 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"(57페이지)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"(59페이지) 및 "자동 테스트 장애 조치 구성"(59페이지)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.

테스트 장애 조치 수행은 선택 사항이지만 비용 및 안전면에서 적절한 빈도의 정기적인 프로세스 로 설정하는 것이 좋습니다. 클라우드에서 운영 환경을 향상시키는 방법을 설명하는 지침인 실행서를 작성하는 것이 좋습니다.

중요

장치를 재해로부터 보호하려면 사전에 **복구 서버를 생성**해야 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.

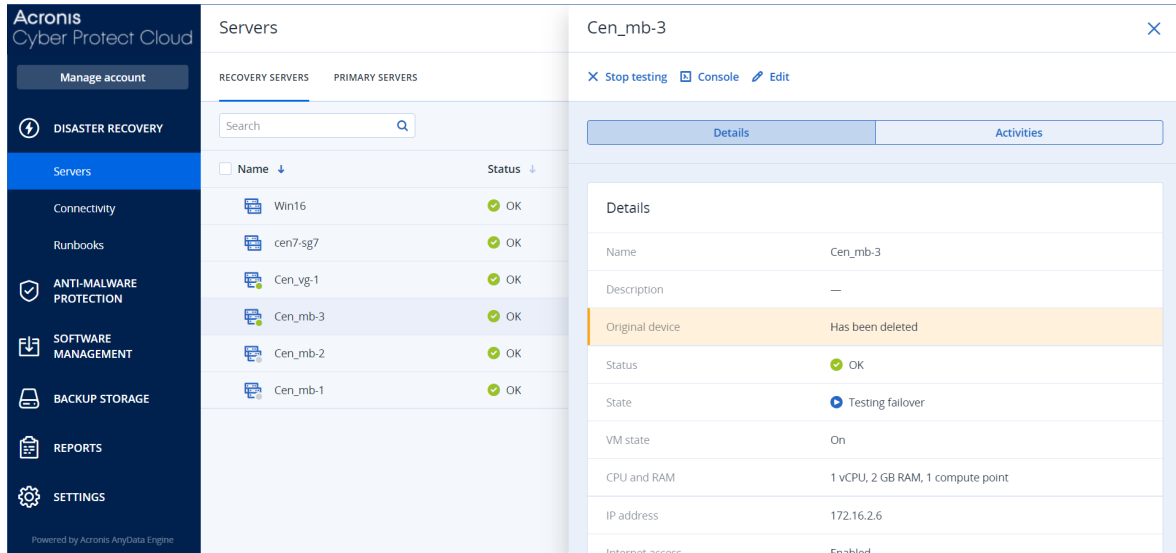
- b. [선택 사항] 백업 세트의 암호를 저장해 두었다가 후속 장애 조치 작업에 사용하려면 **보안 자격 증명 저장소에 암호 저장...** 확인란을 선택하고 **자격 증명 이름** 필드에 자격 증명용 이름을 입력합니다.

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.



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 **TeamViewer**를 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
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"(59페이지)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"(53페이지)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.

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 프리미스에서 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 철회](#)를 참조하십시오.

중요

장치를 재해로부터 보호하려면 사전에 **복구 서버를 생성**해야 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 자습서](#)를 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]
 - 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"(55페이지) 항목을 참조하십시오.

The screenshot displays the Acronis Cyber Protect Cloud web interface. On the left is a dark blue sidebar with navigation options: Manage account, DISASTER RECOVERY, Servers (selected), Connectivity, Runbooks, ANTI-MALWARE PROTECTION, SOFTWARE MANAGEMENT, BACKUP STORAGE, REPORTS, and SETTINGS. The main area is titled 'Servers' and is split into 'RECOVERY SERVERS' and 'PRIMARY SERVERS'. A table lists several servers with their names and status (all 'OK').

Name	Status
Win16	OK
cen7-sg7	OK
Cen_vg-1	OK
Cen_mb-3	OK
Cen_mb-2	OK
Cen_mb-1	OK

A modal window titled 'Cen_vg-1' is open on the right, showing details for the selected server. It includes tabs for Details, Backup, Activities, and Failback. The 'Details' tab is active, showing the following information:

Field	Value
Name	Cen_vg-1
Description	—
Original device	cen7-sg
Status	OK
State	Fallover
VM state	On
CPU and RAM	1 vCPU, 2 GB RAM, 1 compute point
IP address	172.16.2.22

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.

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 임대 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.

대상 가상 머신 및 대상 실제 머신으로의 장애 복구 프로세스는 약간 다릅니다. 장애 복구 프로세스의 단계에 대한 자세한 내용은 "대상 가상 머신으로 장애 복구"(63페이지) 및 "대상 실제 머신으로 장애 복구"(68페이지)을(를) 참조하십시오.

자동 장애 복구 절차를 사용할 수 없는 경우에는 수동 장애 복구를 수행할 수 있습니다. 자세한 내용은 "수동 장애 복구"(72페이지)을(를) 참조하십시오.

참고

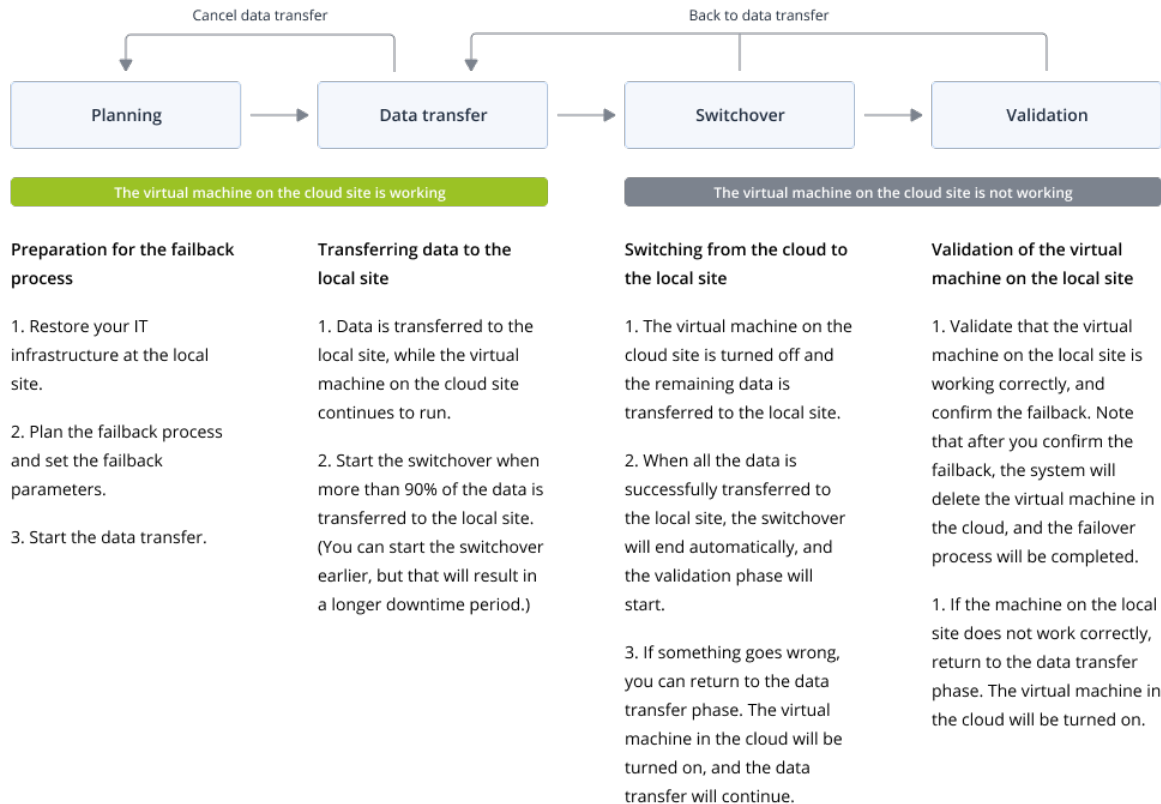
런북 작업에서는 수동 모드의 장애 복구만 지원됩니다. 즉, **서버 장애 복구** 단계가 포함된 런북을 실행하여 장애 복구 프로세스를 시작하는 경우 장애 복구 절차에서 수동 상호 작용을 수행해야 합니다. 구체적으로는 머신을 수동으로 복구한 다음 **재해 복구 > 서버** 탭에서 장애 복구 프로세스를 확인하거나 취소해야 합니다.

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.

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.

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 대상으로 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.

매 개 변 수	설 명
백 업 크 기	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 크기가 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.
대 상	클라우드 서버를 복구할 로컬 사이트의 워크로드 유형입니다. 실제 머신 또는 가상 머신 중 하나를 선택합니다.
대 상 머 신 위 치	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.
에 이 전 트	장애 복구 작업을 수행할 에이전트입니다. 에이전트 하나를 사용해 장애 복구 작업 하나를 동시에 수행할 수 있습니다. 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.
대 상 머 신 설 정	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 추가를 클릭하고 네트워크 필드에서 네트워크를 선택합니다. 변경할 매개변수를 모두 설정한 후 완료를 클릭합니다.
경 로	(Microsoft Hyper-V 호스트에 해당됨) 머신을 저장할 호스트의 폴더입니다. 호스트에 머신용으로 사용 가능한 메모리 공간이 충분한지 확인하십시오.

매개변수	설명
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: • 썸(기본값). • 씹.
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 시작을 클릭하고 확인 창에서 시작을 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 매개변수의 두 값은 시간이 지남에 따라 커집니다.
예상다	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.

필드	설명
운 타 임	

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.

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** 모둘이 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 프로세스가 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.

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
진	로컬 사이트로 이미 전송된 데이터의 양과 전송해야 하는 총 데이터 양을 보여 주는

필드	설명
행 률	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.
예 상 다 운 타 임	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.

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.

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 지정**할 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.

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 라이선스 모델에 따라 추가 라이선스가 필요할 수 있습니다.

Acronis Cyber Protect Cloud로 Microsoft Azure 가상 머신 장애 조치를 수행할 수 있습니다. 자세한 내용은 "장애 조치 수행"(60페이지)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 "실제 머신으로의 장애 복구 수행"(69페이지)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"(29페이지)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:

- 재해 복구 > 서버 > 기본 서버 탭으로 이동합니다.
- 생성을 클릭합니다.
- 새 가상 머신의 템플릿을 선택합니다.
- 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"(12페이지)을(를) 참조하십시오.

- [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.
- 기본 서버를 포함할 클라우드 네트워크를 지정합니다.
- DHCP** 옵션을 선택합니다.

DHCP 옵션	설명
클라우드 사이트	기본 설정. 서버의 IP 주소는 클라우드에 자동으로 구성된 DHCP 서버

DHCP 옵션	설명
제공	에서 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 라이선스가 있는 애플리케이션을 실행할 수 있습니다.

9. 서버가 운영 네트워크에서 가지는 IP 주소를 지정합니다. 기본적으로 운영 네트워크의 첫 번째 사용 가능한 IP 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.

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.

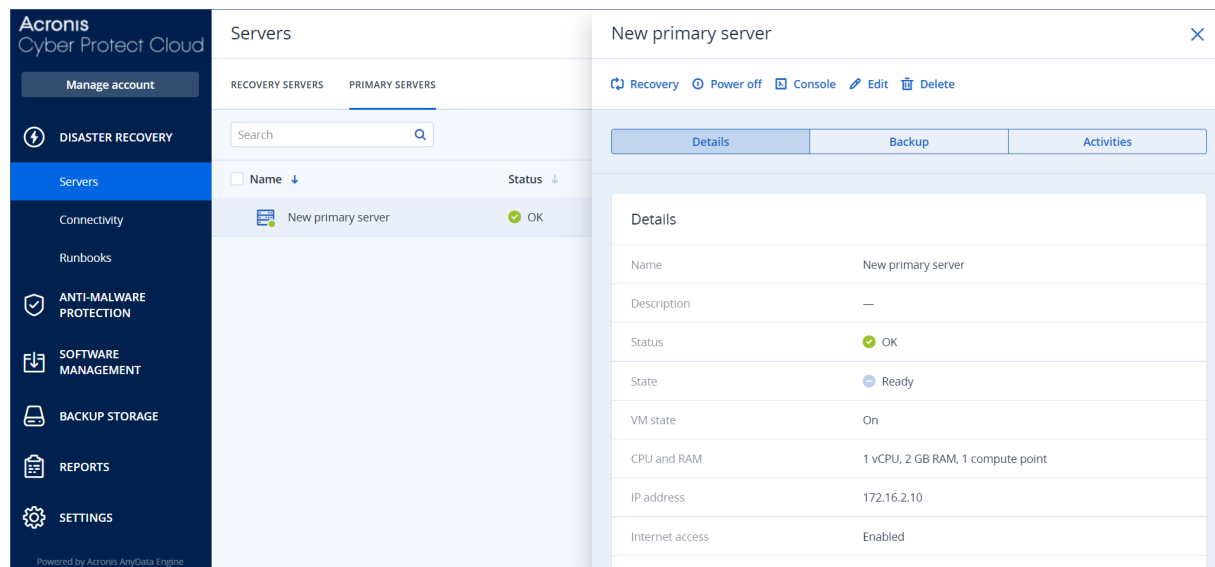
13. 기본 서버 이름을 정의합니다.

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"(79페이지)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.



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 경고 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.
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. 기본적으로 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.

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:
- 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.

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** 중이어야 합니다.
3. **컨텍스트** 필드에서 원하는 정보를 확인합니다.

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 라이선스 모델에 따라 추가 라이선스가 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 ping하고 지정된 포트 연결을 점검하여 장애 조치 결과를 자동으로 점검합니다.
- 분산 애플리케이션을 실행하는 서버의 동작 순서를 설정합니다.
- 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 자습서](#)를 시청할 수 있습니다.

런북을 생성하는 방법

1. Cyber Protection 콘솔에서 **재해 복구 > 런북**으로 이동합니다.
2. 런북 생성을 클릭합니다.
3. 단계 추가를 클릭합니다.
4. 작업 추가를 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"(86페이지)을(를) 참조하십시오. 참고 선택한 서버의 백업이 머신 속성으로 암호화를 사용하여 암호화된 경우, 장애 조치 서버 작업은 일시 중지되고 자동으로 상호 작용 필요로 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"(86페이지)을(를) 참조하십시오.

작업	설명
	참고 러닝 작업에서는 수동 모드의 장애 복구만 지원됩니다. 즉, 서버 장애 복구 단계가 포함된 러닝을 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 러닝 매개변수를 구성해야 합니다. 이러한 설정에 대한 자세한 정보는 "러닝 매개변수"(86페이지)을(를) 참조하십시오. 참고 서버 시작 작업은 러닝에서의 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 러닝 매개변수를 구성해야 합니다. 이러한 설정에 대한 자세한 정보는 "러닝 매개변수"(86페이지)을(를) 참조하십시오. 참고 서버 중지 작업은 러닝에서의 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. 러닝 시퀀스가 수동 작업에 도달하면 러닝은 일시 정지되며 사용자가 확인 버튼을 클릭하는 등의 필수 수동 작업을 수행하기 전까지 진행되지 않습니다.
러닝 실행	다른 러닝을 실행합니다. 이 작업을 정의하려면 러닝을 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.

- 작업에 대한 러닝 매개변수를 정의하십시오. 이러한 매개변수에 대한 자세한 정보는 "러닝 매개변수"(86페이지)을(를) 참조하십시오.
- [선택 사항] 단계에 대한 설명 추가 방법
 - 말줄임표 아이콘을 클릭한 다음 **설명**을 클릭합니다.
 - 단계에 대한 설명을 입력합니다.
 - 완료**를 클릭합니다.
- 원하는 단계와 작업의 시퀀스를 만들 때까지 3-6단계를 반복합니다.
- [선택 사항] 러닝의 기본 이름을 변경하는 방법
 - 말줄임표 아이콘을 클릭합니다.
 - 러닝의 이름을 입력합니다.

- c. 런북에 대한 설명을 입력합니다.
- d. **완료**를 클릭합니다.
9. **저장**을 클릭합니다.
10. **닫기**를 클릭합니다.

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.

런북 매개변수	카테고리	작업 사용 가능	설명
실패한 경우 계속 진행	작업 매개변수	- 장애 조치 서버 - 서버 시작 - 서버 중지 - 서버 장애 복구	이 매개변수는 필요한 작업이 실패한 경우 런북의 행동을 정의합니다. 활성화되면 런북은 경고를 발행하고 계속 진행합니다. 비활성화되면 작업이 실패하고, 그런 다음 런북도 실패합니다. 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 지정 오류 해결

가장 최근의 복구 지정(기본값)을 선택하거나 과거 특정 시점을 선택합니다. 후자에 해당하는 경우, 지정 일시 이전에 가장 근접한 복구 지정은 각 서버별로 선택합니다.

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.

Runbooks

Rb0 000

Execute
Edit
Clone
Delete

Details

NameRb0 000

Description-

Execution history

Start and end time	Result	Mode
Aug 14, 5:30 PM - Aug 14, 10:27 PM	Failed	Production
Aug 14, 5:23 PM - Aug 14, 5:25 PM	Failed	Production
Aug 4, 2:45 AM - Aug 4, 2:46 AM	Completed	Test
Jul 30, 4:18 PM - Jul 30, 4:18 PM	Completed	Test
Jul 30, 4:16 PM - Jul 30, 4:16 PM	Completed	Test

Search

Name ↑

Failback 3-2

Rb0 000

Runbook with ConfirmManualOperation

Runbook with ConfirmManualOperation

jk one server with checking port

New runbook (10)

Failover/Failback (centos-1) (Clone)

New runbook (9)

Runbook #009.

Runbook #010.

사이트 간 OpenVPN - 추가 정보

복구 서버를 생성할 때는 **운영 네트워크** 내의 서버 **IP** 주소와 서버의 **테스트 IP** 주소를 구성합니다.

장애 조치(클라우드에서 가상 머신 실행)를 수행하고 가상 머신에 로그인하여 서버의 IP 주소를 확인하면 **운영 네트워크 내의 서버 IP** 주소가 표시됩니다.

테스트 장애 조치를 수행할 때는 **테스트 IP** 주소를 통해서만 테스트 서버에 연결할 수 있습니다. 테스트 IP 주소는 복구 서버의 구성에만 표시됩니다.

로컬 사이트에서 테스트 서버에 연결하려면 **테스트 IP** 주소를 사용해야 합니다.

참고

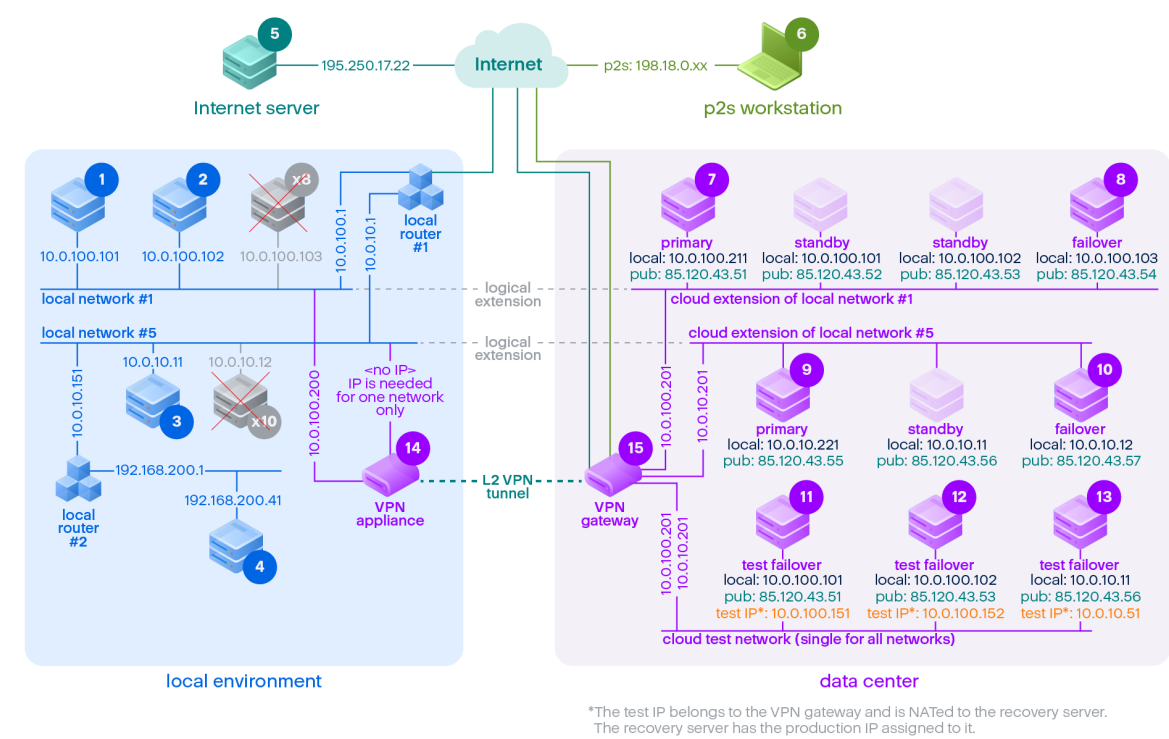
서버의 네트워크 구성에는 항상 **운영 네트워크 내의 서버 IP** 주소가 표시됩니다. 테스트 서버는 운영 서버의 표시 방식을 미러링하기 때문입니다. 테스트 서버가 운영 서버의 표시 방식을 미러링하는 이유는, 테스트 IP 주소는 테스트 서버가 아니라 VPN 게이트웨이에 속하는 주소이며 NAT를 사용하여 운영 IP 주소로 변환되기 때문입니다.

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.



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	장애 조치	기본	장애 조치	테스트 장애 조치	테스트 장애 조치	테스트 장애 조치	VPN 어플라이	VPN 서버

	종료:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
															언스	
1	로컬		직접	로컬 라우터 1을 통한 연결	로컬 라우터 2를 통한 연결	로컬 라우터 1을 통한 연결 및 인터넷	아니오	터널을 통한 연결: 로컬 라우터 1을 통한 연결 및 인터넷: 공용	터널을 통한 연결: 로컬 라우터 1을 통한 연결 및 인터넷: 공용	터널을 통한 연결: 로컬 라우터 1을 통한 연결 및 인터넷: 공용	터널을 통한 연결: 로컬 라우터 1을 통한 연결 및 인터넷: 공용	터널을 통한 연결: NAT (VPN 서버) 로컬 라우터 1을 통한 연결 및 인터넷: 공용	터널을 통한 연결: NAT (VPN 서버) 로컬 라우터 1을 통한 연결 및 인터넷: 공용	로컬 라우터 1을 통한 연결 및 터널: NAT (VPN 서버) 로컬 라우터 1을 통한 연결 및 인터넷: 공용	직접	아니오
2	로컬	직접		로컬 라우터 1을 통한 연결	로컬 라우터 2를 통한 연결	로컬 라우터 1을 통한 연결 및 인터넷	아니오	터널을 통한 연결: 로컬 라우터 1을 통한 연결 및 인터넷: 공용	터널을 통한 연결: 로컬 라우터 1을 통한 연결 및 인터넷: 공용	터널을 통한 연결: 로컬 라우터 1을 통한 연결 및 인터넷: 공용	터널을 통한 연결: 로컬 라우터 1을 통한 연결 및 인터넷: 공용	터널을 통한 연결: NAT (VPN 서버) 로컬 라우터 1을 통한 연결 및 인터넷: 공용	터널을 통한 연결: NAT (VPN 서버) 로컬 라우터 1을 통한 연결 및 인터넷: 공용	로컬 라우터 1을 통한 연결 및 터널: NAT (VPN 서버) 로컬 라우터 1을 통한	직접	아니오

	종료:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
														연결 및 인터넷: 공용		
3	로컬	로컬 라우터 1을 통한 연결	로컬 라우터 1을 통한 연결		로컬 라우터 2를 통한 연결	로컬 라우터 1을 통한 연결 및 인터넷	아니오	터널을 통한 연결: 로컬 라우터 1을 통한 연결 및 인터넷: 공용	터널을 통한 연결: 로컬 라우터 1을 통한 연결 및 인터넷: 공용	터널을 통한 연결: 로컬 라우터 1을 통한 연결 및 인터넷: 공용	터널을 통한 연결: 로컬 라우터 1을 통한 연결 및 인터넷: 공용	터널을 통한 연결: NAT (VPN 서버) 로컬 라우터 1을 통한 연결 및 인터넷: 공용	터널을 통한 연결: NAT (VPN 서버) 로컬 라우터 1을 통한 연결 및 인터넷: 공용	로컬 라우터 1을 통한 연결 및 터널: NAT (VPN 서버) 로컬 라우터 1을 통한 연결 및 인터넷: 공용	로컬 라우터를 통한 연결	아니오
4	로컬	로컬 라우터 2와 라우터 1을 통한 연결	로컬 라우터 2와 라우터 1을 통한 연결	로컬 라우터 2를 통한 연결		로컬 라우터 2와 라우터 1을 통한 연결 및 인터넷	아니오	로컬 라우터 2를 통한 연결 및 터널: 로컬 라우터 2와 로컬 라	로컬 라우터 2를 통한 연결 및 터널: 로컬 라우터 2와 로컬 라	로컬 라우터 2를 통한 연결 및 터널: 로컬 라우터 2와 로컬 라	로컬 라우터 2를 통한 연결 및 터널: 로컬 라우터 2와 로컬 라	터널을 통한 연결: NAT (VPN 서버) 로컬 라우터 2와 라우	터널을 통한 연결: NAT (VPN 서버) 로컬 라우터 2와 라우	터널을 통한 연결: NAT (VPN 서버) 로컬 라우터 2와 라우	로컬 라우터 2를 통한 연결	아니오

	종료:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								우터 1을 통한 연 결 및 인 터넷: 공 용	우터 1을 통한 연 결 및 인 터넷: 공 용	우터 1을 통한 연 결 및 인 터넷: 공 용	우터 1을 통한 연 결 및 인 터넷: 공 용	터 1을 통한 연 결 및 인 터넷: 공 용	터 1을 통한 연 결 및 인 터넷: 공 용	터 1을 통한 연 결 및 인 터넷: 공 용		
5	인터 넷	아니 오	아니 오	아니 오	아니 오		해당 없음	인터넷을 통한 연 결: 공용	인터넷을 통한 연 결: 공용	인터넷을 통한 연 결: 공용	인터넷을 통한 연 결: 공용	인터넷 을 통한 연결: 공 용	인터넷 을 통한 연결: 공 용	인터넷 을 통한 연결: 공 용	아니 오	아니오
6	p2s	아니 오	아니 오	아니 오	아니 오	인터넷 을 통한 연결		p2s VPN (VPN 서 버)를 통 한 연결: 로컬 인터넷을 통한 연 결: 공용	p2s VPN (VPN 서 버)를 통 한 연결: 로컬 인터넷을 통한 연 결: 공용	p2s VPN (VPN 서 버)를 통 한 연결: 로컬 인터넷을 통한 연 결: 공용	p2s VPN (VPN 서 버)를 통 한 연결: 로컬 인터넷을 통한 연 결: 공용	p2s VPN - NAT (VPN 서 버)를 통 한 연결 인터넷 을 통한 연결: 공 용	p2s VPN - NAT (VPN 서 버)를 통 한 연결 인터넷 을 통한 연결: 공 용	p2s VPN - NAT (VPN 서 버)를 통 한 연결 인터넷 을 통한 연결: 공 용	아니 오	아니오
7	기본	터널 을 통 한 연 결	터널 을 통 한 연 결	터널 및 로 컬 라 우터 1을 통한 연결	터널 및 로 컬 라 우터 1/2를 통한 연결	인터넷 을 통한 연결 (VPN 서 버를 통 해 연결)	아니 오		클라우드 에서 직 접: 로컬	터널 및 로컬 라 우터 1을 통한 연 결: 로컬	터널 및 로컬 라 우터 1을 통한 연 결: 로컬	VPN 서 버를 통 한 연결: NAT	VPN 서 버를 통 한 연결: NAT	터널 및 로컬 라 우터 1 을 통한 연결: NAT	아니 오	DHCP 및 DNS 프로토 콜 전용

	종료:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
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
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 서버를 통	아니오	아니오	아니오	아니오	아니오		클라우드에서 직접: 로컬	VPN 서버를 통한 연결: 로컬(라우팅)	아니오	DHCP 및 DNS 프로토콜 전용

	종료:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
						해 연결)										
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 어플라이언스	직접	직접	로컬 라우터 1을 통한 연결	로컬 라우터 2를 통한 연결	인터넷 (로컬 라우터 1)을 통한 연결	아니오	아니오	아니오	아니오	아니오	아니오	아니오	아니오		아니오
15	VPN 서버	아니오	아니오	아니오	아니오	아니오	아니오	아니오	아니오	아니오	아니오	아니오	아니오	아니오	아니오	

용어 설명

V

VPN 게이트웨이(이전 **VPN 서버** 또는 **연결 게이트웨이**)

로컬 사이트와 클라우드 사이트 네트워크를 보안 VPN 터널로 연결하는 특수 가상 머신입니다. VPN 게이트웨이는 클라우드 사이트에 배포됩니다.

VPN 어플라이언스

로컬 네트워크와 클라우드 사이트 네트워크를 보안 VPN 터널로 연결하는 특수 가상 머신입니다. VPN 어플라이언스는 로컬 사이트에 배포됩니다.

공

공용 IP 주소

클라우드를 인터넷에서도 사용할 수 있게 하는 IP 주소입니다.

기

기본 서버

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

장애 조치 과정을 테스트하기 위한 격리된 가상 네트워크입니다.

로

로컬 사이트

회사 premises에 배포된 로컬 인프라입니다.

보

보호된 서버

고객이 소유하는 실제 또는 가상 머신으로, 서비스의 보호를 받습니다.

복

복구 서버

클라우드에 저장되어 있는 보호되는 서버 백업을 기반으로 하는 원본 머신의 VM 복제본입니다. 복구 서버는 재해 시 원본 서버의 워크로드를 전환하는 데 사용됩니다.

복구 지정 목표(RPO)

중단으로 손실된 데이터 양으로, 계획된 중단 또는 재해 이벤트로부터의 시간으로 측정합니다. RPO 임계값은 현재 시각과 장애 조치에 적합한 마지막 복구 지정 사이의 최대 시간을 정의합니다.

사

사이트 간(S2S) 연결

보안 VPN 터널을 통해 로컬 네트워크를 클라우드로 확장하는 연결입니다.

실

실행서

재해 복구 작업을 자동화하는 구성 가능한 단계로 이루어진 계획된 시나리오입니다.

완

완료

클라우드 서버의 생산 장애 조치 또는 복구 과정의 중간 상태입니다. 이 과정은 백업 스토리지("콜드" 스토리지)에서 서버의 가상 디스크를 재해 복구 스토리지("핫" 스토리지)로 전송함을 의미합니다. 완료 과정에서 서버를 액세스 및 작동할 수 있지만, 성능은 일반적인 경우보다 낮습니다.

운

운영 네트워크

VPN 터널링으로 확장되어 로컬 및 클라우드 사이트를 모두 지원하는 내부 네트워크입니다. 로컬 및 클라우드 서버는 운영 네트워크에서 서로 통신할 수 있습니다.

장

장애 복구

장애 조치 동안 클라우드 사이트로 옮겨진 서버를 로컬 사이트로 복원하는 과정입니다.

장애 조치

로컬 사이트에서 자연재해 또는 인재가 발생했을 경우 워크로드 또는 애플리케이션을 클라우드 사이트로 전환하는 것을 의미합니다.

지

지점 및 사이트 간(P2S) 연결

엔드포인트 장치(컴퓨터나 랩톱)를 사용하여 외부에서 클라우드 사이트 및 로컬 사이트로 접속할 수 있는 안전한 VPN 연결입니다.

클

클라우드 사이트(또는 DR 사이트)

재해 시 복구 인프라를 실행할 때 사용하는 클라우드에 호스팅된 원격 사이트입니다.

클라우드 서버

복구 또는 기본 서버에 대한 일반 참조입니다.

테

테스트 IP 주소

테스트 장애 조치 시 운영 중인 IP 주소의 중복을 방지하기 위해 필요한 IP 주소입니다.

색인

A

Active Directory 도메인 서비스 사용 가능성 관련 권장 사항 34

C

Cyber Disaster Recovery Cloud 정보 5

Cyber Disaster Recovery Cloud 평가판 버전 9

D

DHCP 서버의 장애 조치 수행 방법 62

G

Geo-redundant Cloud Storage 사용 시의 제한 사항 10

I

IP 주소 다시 할당 42

IP 주소 재구성 38

IPsec VPN 구성 문제 해결 49

IPsec VPN 로그 파일 다운로드 51

IPsec/IKE 보안 설정 32

L

L2 IPsec VPN 연결용 Active Directory 도메인 컨트롤러 35

L2 OpenVPN 연결용 Active Directory 도메인 컨트롤러 34

L2 VPN을 통한 DHCP 트래픽 허용 45

M

MAC 주소 다운로드 44

Microsoft Azure 가상 머신 관련 작업 74

O

OpenVPN 구성 다운로드 46

V

VPN 게이트웨이 21, 25

VPN 게이트웨이 네트워크 구성 21

VPN 게이트웨이 다시 설치 40

VPN 게이트웨이의 로그 다운로드 48

VPN 어플라이언스 21

VPN 어플라이언스 설정 관리 40

VPN 어플라이언스에 대한 요구사항 28

VPN 어플라이언스의 로그 다운로드 48

가

가상 머신으로의 장애 복구 수행 65

공

공용 및 테스트 IP 주소 22

구

구성 재생성 46

기

기본 서버 24

기본 서버 관련 작업 77

기본 서버 생성 75

기본 서버 설정 75

네

네트워크 관리 36

네트워크 패킷 캡처 48

네트워킹 개념 17

다

다음에 수행할 작업 14

다중 사이트 IPsec VPN 구성 29

다중 사이트 IPsec VPN 로그 파일 51

다중 사이트 IPsec VPN 설정 구성 30

다중 사이트 IPsec VPN 연결 25

대

대상 가상 머신으로 장애 복구 63

대상 실제 머신으로 장애 복구 68

라

라우팅 작동법 18, 21, 26

런

런북 매개변수 86

로

로그 작업 47

로컬 DNS를 사용하는 서버의 장애 조치 수행
방법 62

로컬 라우팅 구성 45

로컬 사이트 관련 일반 권장 사항 32

로컬 사이트로의 VPN 액세스 46

복

복구 서버 22

복구 서버 기본 매개변수 편집 15

복구 서버 생성 53

복구 서버 설정 53

사

사용자 정의 DNS 서버 구성 43

사용자 정의 DNS 서버 삭제 44

사이트 간 OpenVPN - 추가 정보 89

사이트 간 OpenVPN 구성 28

사이트 간 OpenVPN 연결 19, 36

사이트 간 OpenVPN 연결 구성 28

사이트 간 연결 유형 전환 41

사이트 간 연결 활성화 및 비활성화 41

사전 요구 사항 30, 35, 51, 53, 65, 70, 75

소

소프트웨어 요구 사항 6

수

수동 장애 복구 72

수동 장애 복구 수행 72

시

시스템 요구 사항 28

실

실제 머신으로의 장애 복구 수행 69

실행 기록 보기 88

실행서를 사용하는 이유는 무엇인가요? 84

암

암호화 소프트웨어와의 재해 복구 호환성 11

암호화된 백업 관련 작업 73

연

연결 설정 17

자

- 자동 테스트 장애 조치 56, 59
- 자동 테스트 장애 조치 구성 59
- 자동 테스트 장애 조치 비활성화 60
- 자동 테스트 장애 조치 상태 확인 60

작

- 작동 실행서 관련 작업 87
- 작동 실행서 생성 84
- 작동 실행서 실행 중지 88
- 작동 실행서의 실행 87

장

- 장애 복구 작동 방식 62
- 장애 조치 수행 60
- 장애 조치 작동 방식 55
- 장애 조치 테스트 56

재

- 재해 복구 보호 계획 생성 14

전

- 전제 조건 40, 43-44

제

- 제한 사항 7

조

- 조정(작동 실행서) 84

주

- 주요 기능 5

지

- 지원되는 가상화 플랫폼 6
- 지원되는 운영 체제 6
- 지점 및 사이트 간 연결 설정 관리 45
- 지점 및 사이트 간 원격 VPN 액세스 26
- 지점 및 사이트 간 원격 VPN 액세스 구성 35

최

- 최초 연결 구성 28

컴

- 컴퓨팅 포인트 12

클

- 클라우드 네트워크 인프라 16
- 클라우드 방화벽 활동 확인 82
- 클라우드 사이트에서 사용되지 않은 고객 환경의 자동 삭제 27
- 클라우드 서버 관리 78
- 클라우드 서버 백업 83
- 클라우드 서버용 방화벽 규칙 79
- 클라우드 서버용 방화벽 규칙 설정 79
- 클라우드 전용 모드 18, 38
- 클라우드 전용 모드 구성 28

테

- 테스트 장애 조치 수행 57

포

- 포트 28

프

프로덕션 장애 조치 55

활

활성 상태의 지점 및 사이트 간 연결 46