

Cyber Disaster Recovery Cloud

24.03



Spis treści

Cyber Disaster Recovery Cloud — informacje	5
Najważniejsze funkcje	5
Wymagania dotyczące oprogramowania	6
Obsługiwane systemy operacyjne	6
Obsługiwane platformy wirtualizacji	6
Ograniczenia	7
Wersja próbna rozwiązania Cyber Disaster Recovery Cloud	9
Ograniczenia w przypadku korzystania z magazynu Geo-redundant Cloud Storage	10
Kompatybilność modułu Odzyskiwanie po awarii z programami szyfrującymi	11
Punkty obliczeniowe	12
Tworzenie planu ochrony na potrzeby odzyskiwania po awarii	14
Co dalej	15
Edytowanie domyślnych parametrów serwera odzyskiwania	15
Infrastruktura sieci w chmurze	16
Konfigurowanie łączności	18
Pojęcia dotyczące sieci	18
Tryb Tylko chmura	19
Połączenie Open VPN site-to-site	20
Połączenie IPsec VPN multi-site	26
Zdalny dostęp VPN point-to-site	27
Automatyczne usuwanie nieużywanych środowisk klientów w lokalizacji w chmurze	28
Początkowa konfiguracja łączności	29
Konfigurowanie trybu Tylko chmura	29
Konfigurowanie połączenia Open VPN site-to-site	29
Konfigurowanie połączenia IPsec VPN multi-site	31
Zalecenia dotyczące dostępności usług Active Directory Domain Services	37
Konfigurowanie zdalnego dostępu VPN point-to-site	37
Zarządzanie sieciami	38
Zarządzanie sieciami	39
Zarządzanie ustawieniami urządzenia VPN	42
Ponowne instalowanie bramy VPN	43
Włączanie i wyłączanie połączenia site-to-site	43
Zmienianie typu łączności na site-to-site	44
Zmienianie przypisania adresów IP	45
Konfigurowanie niestandardowych serwerów DNS	46

Usuwanie niestandardowych serwerów DNS	47
Pobieranie adresów MAC	47
Konfigurowanie routingu lokalnego	48
Zezwalanie na ruch DHCP przez połączenie L2 VPN	48
Zarządzanie ustawieniami połączenia point-to-site	49
Aktywne połączenia point-to-site	50
Praca z dziennikami	50
Rozwiązywanie problemów z konfiguracją IPsec VPN	52
Konfigurowanie serwerów odzyskiwania	57
Tworzenie serwera odzyskiwania	57
Przebieg przełączania awaryjnego	60
Produkcyjne przełączanie awaryjne	60
Testuj przełączenie awaryjne	61
Automatyczne testowe przełączanie awaryjne	61
Wykonywanie testowego przełączenia awaryjnego	61
Automatyczne testowe przełączanie awaryjne	64
Wykonywanie przełączenia awaryjnego	66
Przebieg powrotu po awarii	69
Powrót po awarii na docelową maszynę wirtualną	69
Powrót po awarii na docelowy komputer fizyczny	74
Ręczny powrót po awarii	78
Praca z zaszyfrowanymi kopiami zapasowymi	80
Operacje dotyczące maszyn wirtualnych Microsoft Azure	80
Konfigurowanie serwerów podstawowych	82
Tworzenie serwera podstawowego	82
Działania na serwerze podstawowym	84
Zarządzanie serwerami chmurowymi	85
Reguły zapory dotyczące serwerów chmurowych	87
Ustawianie reguł zapory dla serwerów chmurowych	87
Sprawdzanie działań dotyczących zapory chmury	90
Tworzenie kopii zapasowych serwerów chmurowych	91
Orkiestracja (runbooki)	92
Dlaczego warto korzystać z runbooków?	92
Tworzenie runbooka	92
Parametry runbooka	95
Operacje przy użyciu runbooków	96
Wykonywanie runbooka	97

Zatrzymywanie wykonywania runbooka	97
Wyświetlanie historii wykonania	97
Połączenie Open VPN site-to-site — dodatkowe informacje	99
Słownik	107
Indeks	109

Cyber Disaster Recovery Cloud — informacje

Cyber Disaster Recovery Cloud (DR) — wchodzące w skład platformy Cyber Protection rozwiązanie DRaaS (odzyskiwanie po awarii jako usługa). Cyber Disaster Recovery Cloud to szybkie i stabilne rozwiązanie, które pozwala uruchamiać dokładne kopie swoich komputerów w lokalizacji w chmurze i przenosić obciążenia z uszkodzonych oryginalnych komputerów na serwery odzyskiwania w chmurze w razie szkód spowodowanych przez człowieka lub katastrofę naturalną.

Środowisko odzyskiwania po awarii możesz utworzyć i skonfigurować następująco:

- Utwórz plan ochrony zawierający moduł odzyskiwania po awarii i zastosuj go do swoich urządzeń. W ten sposób zostanie automatycznie utworzona domyślna infrastruktura odzyskiwania po awarii. Zobacz [Tworzenie planu ochrony na potrzeby odzyskiwania po awarii](#).
- Ręcznie skonfiguruj chmurową infrastrukturę odzyskiwania po awarii, kontrolując każdy etap. Zobacz "Konfigurowanie serwerów odzyskiwania" (s. 57).

Najważniejsze funkcje

Uwaga

Niektóre funkcje mogą wymagać dodatkowego licencjonowania — w zależności od stosowanego modelu licencjonowania.

- Zarządzanie usługą Cyber Disaster Recovery Cloud z jednej konsoli
- Możliwość rozszerzenia nawet 23 sieci lokalnych do chmury przy użyciu bezpiecznego tunelu VPN
- Nawiązanie połączenia z lokalizacją w chmurze bez wdrażania urządzenia VPN¹ (tryb Tylko chmura)
- Nawiązanie połączenia point-to-site z lokalizacją lokalną i lokalizacją w chmurze
- Ochrona komputerów za pomocą serwerów odzyskiwania w chmurze
- Ochrona aplikacji i urządzeń za pomocą serwerów podstawowych w chmurze
- Automatyczne operacje odzyskiwania po awarii w przypadku szyfrowanych kopii zapasowych
- Testowanie przełączania awaryjnego w odizolowanej sieci
- Skorzystaj z runbooków, aby szybko przygotować środowisko produkcyjne w chmurze

¹Specjalna maszyna wirtualna umożliwiająca połączenie między siecią lokalną a lokalizacją w chmurze przez bezpieczny tunel VPN. Urządzenie VPN jest wdrażane w lokalizacji lokalnej.

Wymagania dotyczące oprogramowania

Obsługiwane systemy operacyjne

Ochrona za pomocą serwera odzyskiwania została przetestowana dla następujących systemów operacyjnych:

- 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 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2019 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2022 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server

Oprogramowanie może działać na innych systemach operacyjnych Windows oraz dystrybucjach systemu Linux, jednak nie jest to gwarantowane.

Uwaga

Ochrona z zastosowaniem serwera odzyskiwania została przetestowana w przypadku maszyn wirtualnych Microsoft Azure z następującymi systemami operacyjnymi:

- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2019 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2022 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Ubuntu Server 20.04 LTS — Gen2 (firmy Canonical) Dodatkowe informacje na temat uzyskiwania dostępu do konsoli serwera odzyskiwania można znaleźć w artykule <https://kb.acronis.com/content/71616>.

Obsługiwane platformy wirtualizacji

Ochrona maszyn wirtualnych za pomocą serwera odzyskiwania została przetestowana dla następujących platform wirtualizacji:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7, 7.0
- Windows Server 2008 R2 z rolą Hyper-V
- Windows Server 2012/2012 R2 z rolą Hyper-V
- Windows Server 2016 z rolą Hyper-V — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2019 z rolą Hyper-V — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2022 z rolą Hyper-V — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- Maszyny wirtualne oparte na jądrze (KVM) — tylko w pełni zwirtualizowane maszyny-goście (HVM). Parawirtualne maszyny-goście (PV) nie są obsługiwane.
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2

Urządzenie VPN zostało przetestowane dla następujących platform wirtualizacji:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- Windows Server 2008 R2 z rolą Hyper-V
- Windows Server 2012/2012 R2 z rolą Hyper-V
- Windows Server 2016 z rolą Hyper-V — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2019 z rolą Hyper-V — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2022 z rolą Hyper-V — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016

Oprogramowanie może działać na innych platformach wirtualizacji lub innych wersjach tych platform, jednak nie jest to gwarantowane.

Ograniczenia

W ramach usługi Cyber Disaster Recovery Cloud nie są obsługiwane następujące platformy i konfiguracje:

1. Nieobsługiwane platformy:

- Agenty dla Virtuozzo
- macOS
- Systemy operacyjne Windows dla komputerów stacjonarnych nie są obsługiwane w związku z warunkami korzystania z produktów firmy Microsoft.

• Wersja Windows Server Azure

Wersja Azure to wersja systemu Windows Server opracowana specjalnie pod kątem działania jako maszyna wirtualna (VM) Azure IaaS na platformie Azure lub jako maszyna wirtualna w klastrze Azure Stack HCI. Wersja Azure — w odróżnieniu od wersji Standard i Datacenter — nie jest licencjonowana do działania na sprzęcie bez systemu operacyjnego, kliencie Windows Hyper-V, Windows Server Hyper-V, hiperwizorach innych firm ani w chmurach innych firm.

2. Nieobsługiwane konfiguracje:

Microsoft Windows

- Dyski dynamiczne nie są obsługiwane
- Systemy operacyjne Windows dla komputerów stacjonarnych nie są obsługiwane (w związku z warunkami korzystania z produktów firmy Microsoft)
- Usługa Active Directory z replikacją FRS nie jest obsługiwana
- Nośniki wymienne bez formatowania GPT lub MBR (tzw. superdyskiety) nie są obsługiwane

Linux

- Systemy plików bez tabeli partycji
- Obciążenia systemu Linux, których kopie zapasowe są tworzone za pomocą agenta z systemu operacyjnego gościa i które mają woluminy z następującymi zaawansowanymi konfiguracjami narzędzia Logical Volume Manager (LVM): Woluminy rozłożone, woluminy dublowane, RAID 0, RAID 4, RAID 5, RAID 6 lub RAID 10.

Uwaga

Obciążenia, na których zainstalowano więcej niż jeden system operacyjny, nie są obsługiwane.

3. Nieobsługiwane typy kopii zapasowych:

- Punkty odzyskiwania tworzone w ramach ciągłej ochrony danych są niekompatybilne.

Ważne

Jeśli utworzysz serwer odzyskiwania na podstawie kopii zapasowej mającej punkt odzyskiwania utworzony w ramach ciągłej ochrony danych, to podczas powrotu po awarii lub tworzenia kopii zapasowej serwera odzyskiwania utracisz dane zawarte w tym punkcie.

- Kopii zapasowych z danymi do analizy śledczej nie można używać do tworzenia serwerów odzyskiwania.

Serwer odzyskiwania ma jeden interfejs sieciowy. Jeśli pierwotna maszyna ma kilka interfejsów sieciowych, emulowany jest tylko jeden interfejs.

Serwery chmurowe nie są szyfrowane.

Wersja próbna rozwiązania Cyber Disaster Recovery Cloud

Z wersji próbnej rozwiązania Acronis Cyber Disaster Recovery Cloud można korzystać przez 30 dni. W okresie tym w rozwiązaniu Disaster Recovery występują następujące ograniczenia dla dzierżawców-partnerów:

- Serwery odzyskiwania i podstawowych nie mają dostępu do publicznego Internetu. Nie można przypisać tym serwerom publicznych adresów IP.
- Połączenie IPsec VPN multi-site jest niedostępne.

Ograniczenia w przypadku korzystania z magazynu Geo-redundant Cloud Storage

Geo-redundant Cloud Storage stanowi lokalizację dodatkową na potrzeby danych kopii zapasowych. Lokalizacja dodatkowa znajduje się w regionie, który jest geograficznie oddalony od lokalizacji głównego magazynu. Geograficzna separacja regionów gwarantuje, że jeśli w jednym z regionów dojdzie do katastrofalnych wydarzeń uniemożliwiających odzyskanie danych z kopii zapasowej, drugiego regionu nie będą one dotyczyć i będzie można kontynuować wszelkie operacje.

Ważne

Usługa Odzyskiwanie po awarii nie jest obsługiwana, jeśli lokalizacja magazynu kopii zapasowych zostanie zmieniona z lokalizacji podstawowej na lokalizację dodatkową cechującą się geograficzną nadmiarowością.

Kompatybilność modułu Odzyskiwanie po awarii z programami szyfrującymi

Moduł Odzyskiwanie po awarii jest kompatybilny z następującymi programami szyfrującymi na poziomie dysku:

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

Uwaga

- W przypadku obciążeń z zastosowanym szyfrowaniem na poziomie dysku zalecamy zainstalowanie agenta ochrony w systemie operacyjnym gościa obciążenia i wykonywanie kopii zapasowych przy użyciu agenta.
- Przełączanie awaryjne i powrót po awarii nie będą obsługiwane w przypadku bezagentowych kopii zapasowych zaszyfrowanych obciążeń.

Aby uzyskać więcej informacji na temat kompatybilności z oprogramowaniem szyfrującym, zapoznaj się z Podręcznikiem użytkownika usługi ochrony cybernetycznej.

Punkty obliczeniowe

W usłudze Disaster Recovery punkty obliczeniowe są używane w przypadku serwerów podstawowych oraz serwerów odzyskiwania podczas testowego i produkcyjnego przełączania awaryjnego. Punkty obliczeniowe odzwierciedlają zasoby obliczeniowe używane do uruchamiania serwerów (maszyn wirtualnych) w chmurze.

Wykorzystanie punktów obliczeniowych podczas odzyskiwania po awarii zależy od parametrów serwera oraz czasu znajdowania się serwera w stanie przełączania awaryjnego. Im wydajniejszy jest serwer i im dłuższy jest ten czas, tym więcej punktów obliczeniowych zostanie wykorzystanych. A im więcej punktów obliczeniowych zostanie wykorzystanych, tym wyższe zostaną naliczone koszty.

W przypadku wszystkich serwerów działających w środowisku Acronis Cloud będą pobierane opłaty za punkty obliczeniowe — w zależności od ich skonfigurowanego wariantu, a niezależnie od ich stanu (włączone czy wyłączone).

Serwery odzyskiwania w stanie gotowości nie wykorzystują punktów obliczeniowych i nie będą za nie pobierane opłaty.

W poniższej tabeli znajduje się przykład ośmiu serwerów w chmurze w różnych wariantach oraz odpowiednie punkty obliczeniowe, które te serwery będą wykorzystywać w ciągu godziny. Warianty serwerów można zmieniać na karcie **Szczegóły**.

Typ	Procesor	Pamięć RAM	Punkty obliczeniowe
W1	1 procesor wirtualny	2 GB	1
F2	1 procesor wirtualny	4 GB	2
W3	2 procesory wirtualne	8 GB	4
W4	4 procesory wirtualne	16 GB	8
W5	8 procesorów wirtualnych	32 GB	16
W6	16 procesorów wirtualnych	64 GB	32
W7	16 procesorów wirtualnych	128 GB	64
W8	16 procesorów wirtualnych	256 GB	128

Dzięki informacjom z tabeli można łatwo oszacować, ile punktów obliczeniowych wykorzysta serwer (maszyna wirtualna).

Jeśli na przykład za pomocą usługi Odzyskiwanie po awarii ma być chroniona jedna maszyna wirtualna z 4 procesorami wirtualnymi* i 16 GB pamięci RAM oraz jedna maszyna wirtualna z 2 procesorami wirtualnymi i 8 GB pamięci RAM, pierwsza maszyna wirtualna wykorzysta 8 punktów obliczeniowych na godzinę, a druga — 4 punkty obliczeniowe na godzinę. Jeśli obie maszyny wirtualne znajdują się w stanie przełączania awaryjnego, łączne wykorzystanie osiągnie poziom 12

punktów obliczeniowych na godzinę lub 288 punktów obliczeniowych na cały dzień (12 punktów obliczeniowych na godzinę x 24 godziny = 288 punktów obliczeniowych).

* Pojęcie „procesor wirtualny” (vCPU) oznacza procesor fizyczny przypisany do maszyny wirtualnej i jest jednostką zależną od czasu.

Uwaga

W przypadku wykorzystania nadwyżki limitu **punktów obliczeniowych** wszystkie serwery podstawowe i serwery odzyskiwania zostaną wyłączone. Korzystanie z tych serwerów będzie możliwe dopiero po rozpoczęciu następnego okresu rozliczeniowego lub zwiększeniu limitu. Domyślnym okresem rozliczeniowym jest cały miesiąc kalendarzowy.

Tworzenie planu ochrony na potrzeby odzyskiwania po awarii

Utwórz plan ochrony obejmujący moduł Odzyskiwanie po awarii i zastosuj go do swoich urządzeń.

W przypadku tworzenia nowego planu ochrony moduł Odzyskiwanie po awarii jest domyślnie wyłączony. Po włączeniu funkcji odzyskiwania po awarii i zastosowaniu planu do urządzeń tworzona jest infrastruktura sieci w chmurze, w tym *serwer odzyskiwania* dla każdego chronionego urządzenia. *Serwer odzyskiwania* to komputer wirtualny w chmurze będący kopią wybranego urządzenia. W przypadku każdego z wybranych urządzeń tworzony jest serwer odzyskiwania w stanie gotowości (bez uruchomienia maszyny wirtualnej) z ustawieniami domyślnymi. Rozmiar serwera odzyskiwania jest dobierany automatycznie — z uwzględnieniem procesora i pamięci RAM chronionego urządzenia. Domyślnie jest też automatycznie tworzona infrastruktura sieci w chmurze: Brama VPN i sieci w lokalizacji w chmurze, z którymi będą połączone serwery odzyskiwania.

Po odwołaniu, usunięciu lub wyłączeniu modułu Odzyskiwanie po awarii z planu ochrony serwery odzyskiwania i sieci w chmurze nie zostaną automatycznie usunięte. W razie potrzeby infrastrukturę odzyskiwania po awarii można usunąć ręcznie.

Uwaga

- Po skonfigurowaniu funkcji odzyskiwania po awarii będziesz mieć możliwość wykonania testowego lub produkcyjnego przełączenia awaryjnego z dowolnego z punktów odzyskiwania wygenerowanych po utworzeniu serwera odzyskiwania dla urządzenia. Punktów odzyskiwania wygenerowanych przed aktywowaniem ochrony urządzenia za pomocą funkcji odzyskiwania po awarii (tj. przed utworzeniem serwera odzyskiwania), nie można użyć do wykonania przełączenia awaryjnego.
- Jeśli nie uda się wykryć adresu IP urządzenia, to nie będzie można włączyć planu ochrony na potrzeby odzyskiwania po awarii. Może tak się zdarzyć na przykład w przypadku, gdy kopie zapasowe maszyn wirtualnych są tworzone bez agentów i maszyny nie mają przypisanych adresów IP.
- Po zastosowaniu planu ochrony w lokalizacji w chmurze są przypisywane te same sieci i adresy IP. Łączność IPsec VPN wymaga, aby segmenty sieci w lokalizacjach w chmurze i lokalnych się nie pokrywały. Jeśli skonfigurowano łączność IPsec VPN multi-site, a następnie zastosowano plan ochrony do jednego lub kilku urządzeń, należy dodatkowo zaktualizować sieci w chmurze i ponownie przypisać adresy IP serwerów chmurowych. Aby uzyskać więcej informacji, zobacz "Zmianianie przypisania adresów IP" (s. 45).

Aby utworzyć plan ochrony na potrzeby odzyskiwania po awarii

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Wybierz komputery, które chcesz chronić.
3. Kliknij **Chroń**, a następnie kliknij **Utwórz plan**.
Zostanie otwarta sekcja domyślnych ustawień planu ochrony.

4. Skonfiguruj opcje kopii zapasowej.
Aby korzystać z funkcji odzyskiwania po awarii ramach planu w chmurze musi zostać utworzona kopia zapasowa całego komputera lub tylko dysków niezbędnych do uruchomienia komputera i udostępnienia potrzebnych usług.
5. Włącz moduł Odzyskiwanie po awarii, klikając przełącznik obok jego nazwy.
6. Kliknij **Utwórz**.
Plan zostanie utworzony i zastosowany do wybranych komputerów.

Co dalej

- Domyślną konfigurację serwera odzyskiwania można edytować. Aby uzyskać więcej informacji, zobacz "Konfigurowanie serwerów odzyskiwania" (s. 57).
- Domyślną konfigurację sieci można edytować. Aby uzyskać więcej informacji, zobacz "Konfigurowanie łączności" (s. 18).
- Można znaleźć więcej informacji na temat domyślnych parametrów serwerów odzyskiwania i infrastruktury sieci w chmurze. Dodatkowe informacje można znaleźć w sekcjach "Edytowanie domyślnych parametrów serwera odzyskiwania" (s. 15) i "Infrastruktura sieci w chmurze" (s. 16).

Edytowanie domyślnych parametrów serwera odzyskiwania

Podczas tworzenia i stosowania planu ochrony na potrzeby odzyskiwania po awarii jest tworzony serwer odzyskiwania z parametrami domyślnymi. Te domyślne parametry można później edytować.

Uwaga

Serwer odzyskiwania jest tworzony tylko wtedy, jeśli jeszcze go nie ma. Istniejące już serwery odzyskiwania nie są zmieniane ani tworzone ponownie.

Aby edytować domyślne parametry serwera odzyskiwania

1. Przejdź do sekcji **Urządzenia > Wszystkie urządzenia**.
2. Wybierz urządzenie i kliknij **Odzyskiwanie po awarii**.
3. Edytuj domyślne parametry serwera odzyskiwania.
Parametry serwera odzyskiwania zostały opisane w poniższej tabeli.

Serwer odzyskiwania parametr	Domyślne wartość	Opis
Procesor i pamięć RAM	automatycznie	Wybierz liczbę procesorów wirtualnych i rozmiar pamięci RAM serwera odzyskiwania. Ustawienia domyślne zostaną określone automatycznie na podstawie oryginalnej konfiguracji procesora i

		pamięci RAM urządzenia.
Sieć w chmurze	automatycznie	Sieć w chmurze, do której ma zostać podłączony serwer. Szczegółowe informacje na temat konfigurowania sieci w chmurze można znaleźć w sekcji Infrastruktura sieci w chmurze .
Adres IP w sieci produkcyjnej	automatycznie	Adres IP, który serwer będzie mieć przypisany w sieci produkcyjnej. Domyślnie używany jest adres IP pierwotnego komputera.
Testowy adres IP	wyłączone	Testowy adres IP umożliwia przetestowanie przełączania awaryjnego w odizolowanej sieci testowej i połączenie serwera odzyskiwania przy użyciu protokołu RDP lub SSH podczas testu przełączania awaryjnego. W trybie testowego przełączania awaryjnego brama VPN zastępuje testowy adres IP produkcyjnym adresem IP za pomocą protokołu NAT. Jeśli testowy adres IP nie zostanie określony, dostęp do serwera będzie możliwy wyłącznie z poziomu konsoli.
Dostęp do Internetu	włączone	Włącz dostęp serwera odzyskiwania do Internetu podczas prawdziwego lub testowego przełączania awaryjnego. Domyślnie w przypadku portu TCP 25 jest skonfigurowana odmowa połączeń wychodzących.
Użyj adresu publicznego	wyłączone	Publiczny adres IP serwera czyni go dostępnym w Internecie podczas prawdziwego lub testowego przełączania awaryjnego. Jeśli nie użyjesz publicznego adresu IP, serwer będzie dostępny wyłącznie w Twojej sieci produkcyjnej. Aby użyć publicznego adresu IP, należy włączyć dostęp do Internetu. Publiczny adres IP zostanie wyświetlony po zakończeniu konfiguracji. Domyślnie port TCP 443 jest otwarty dla połączeń przychodzących.
Ustaw próg RPO	wyłączone	Próg RPO określa maksymalny dozwolony odstęp czasu między ostatnim punktem odzyskiwania a czasem bieżącym. Można ustawić wartość z przedziałów: 15– 60 minut, 1–24 godz., 1–14 dni.

Infrastruktura sieci w chmurze

Infrastruktura sieci w chmurze składa się z bramy VPN w lokalizacji w chmurze oraz sieci w chmurze, z którymi będą połączone serwery odzyskiwania.

Uwaga

Zastosowanie planu ochrony na potrzeby odzyskiwania po awarii powoduje utworzenie infrastruktury sieci w chmurze do odzyskiwania tylko wtedy, gdy takiej infrastruktury jeszcze nie ma. Istniejące już sieci w chmurze nie są zmieniane ani tworzone ponownie.

System sprawdza adresy IP urządzeń i jeśli nie ma jeszcze sieci w chmurze, do której pasuje dany adres IP, zostanie ona automatycznie utworzona. Jeśli zaś istnieje już sieć w chmurze, do której pasuje adres IP serwera odzyskiwania, sieć ta nie jest zmieniana ani tworzona ponownie.

- Jeśli jeszcze nie ma sieci w chmurze lub ustawienia odzyskiwania po awarii są konfigurowane po raz pierwszy, sieci w chmurze zostaną utworzone z maksymalnymi zakresami zalecanymi przez IANA do użytku prywatnego (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) na podstawie zakresu adresów IP urządzeń. Sieć można zawęzić, edytując jej maskę.
- Jeśli masz urządzenia w wielu sieciach lokalnych, sieć w chmurze może stać się obszarem nadrzędnym w stosunku do sieci lokalnych. Konfiguracje sieci można zmieniać w sekcji **Łączność**. Zobacz "Zarządzanie sieciami" (s. 39).
- W razie konieczności skonfigurowania połączenia Open VPN site-to-site pobierz urządzenie VPN i je skonfiguruj. Zobacz "Konfigurowanie połączenia Open VPN site-to-site" (s. 29). Upewnij się, że zakresy sieci w chmurze odpowiadają zakresom sieci lokalnych podłączonych do urządzenia VPN.
- Aby zmienić domyślną konfigurację sieci, kliknij łącze **Przejdź do sekcji łączności** w module Disaster Recovery planu ochrony lub kliknij **Odzyskiwanie po awarii > Łączność**.

Konfigurowanie łączności

W tej sekcji omówiono zagadnienia sieciowe niezbędne do zrozumienia działania wszystkich elementów w ramach usługi Cyber Disaster Recovery Cloud. Dowiesz się, jak skonfigurować różne rodzaje łączności z lokalizacją w chmurze — stosownie do potrzeb. Dowiesz się też, jak należy zarządzać sieciami w chmurze oraz konfigurować ustawienia urządzenia VPN i bramy VPN.

Pojęcia dotyczące sieci

Uwaga

Niektóre funkcje mogą wymagać dodatkowego licencjonowania — w zależności od stosowanego modelu licencjonowania.

Za pomocą usługi Cyber Disaster Recovery Cloud można zdefiniować następujące typy łączności z lokalizacją w chmurze:

- **Tryb Tylko chmura**

Połączenie tego typu nie wymaga wdrożenia urządzenia VPN w lokalizacji lokalnej.

Sieć lokalna i sieć w chmurze działają niezależnie. Ten typ połączenia oznacza albo przełączenie awaryjne wszystkich chronionych serwerów z lokalizacji lokalnej, albo częściowe przełączenie awaryjne niezależnych serwerów, które nie muszą się komunikować z lokalizacją lokalną.

Serwery chmurowe w lokalizacji w chmurze są dostępne przez sieć lokalną, połączenie VPN point-to-site i publiczne adresy IP (jeśli zostały przypisane).

- **Połączenie Open VPN site-to-site**

Połączenie tego typu wymaga wdrożenia urządzenia VPN w lokalizacji lokalnej.

Połączenie Open VPN site-to-site pozwala na rozszerzenie sieci na chmurę z zachowaniem adresów IP.

Lokalizacja lokalna zostaje połączona z lokalizacją w chmurze za pomocą bezpiecznego tunelu VPN. Ten typ połączenia jest odpowiedni w sytuacji, gdy w lokalizacji lokalnej występują mocno zależne serwery, takie jak serwer internetowy czy serwer bazy danych. W przypadku częściowego przełączenia awaryjnego — gdy jeden z serwerów jest odtwarzany w lokalizacji w chmurze, a drugi pozostaje w lokalizacji lokalnej — będą one mogły nadal się ze sobą komunikować przez tunel VPN.

Serwery chmurowe w lokalizacji w chmurze są dostępne przez sieć lokalną, połączenie VPN point-to-site i publiczne adresy IP (jeśli zostały przypisane).

- **Połączenie IPsec VPN multi-site**

Połączenie tego typu wymaga lokalnego urządzenia VPN, które obsługuje protokół IPsec IKE v2.

Gdy zaczniesz konfigurować połączenie IPsec VPN multi-site, usługa Cyber Disaster Recovery Cloud automatycznie utworzy chmurową bramę VPN z publicznym adresem IP.

Dzięki połączeniu IPsec VPN multi-site lokalizacje lokalne zostają połączone z lokalizacją w chmurze za pomocą bezpiecznego tunelu VPN.

Połączenie tego typu jest odpowiednie w scenariuszach usługi Disaster Recovery z jedną lub kilkoma lokalizacjami lokalnymi hostującymi obciążenia krytyczne lub ściśle zależne usługi.

W przypadku częściowego przełączenia awaryjnego jednego z serwerów serwer ten jest odtwarzany w lokalizacji w chmurze, a pozostałe serwery pozostają w lokalizacji lokalnej — będą one mogły nadal się ze sobą komunikować przez tunel IPsec VPN.

W przypadku częściowego przełączenia awaryjnego jednej z lokalizacji lokalnych pozostałe lokalizacje lokalne działają i będą mogły nadal się ze sobą komunikować przez tunel IPsec VPN.

- **Zdalny dostęp VPN point-to-site**

Bezpieczny zdalny dostęp VPN point-to-site do własnych obciążeń w lokalizacji w chmurze i lokalizacji lokalnej z zewnątrz za pomocą własnego urządzenia końcowego.

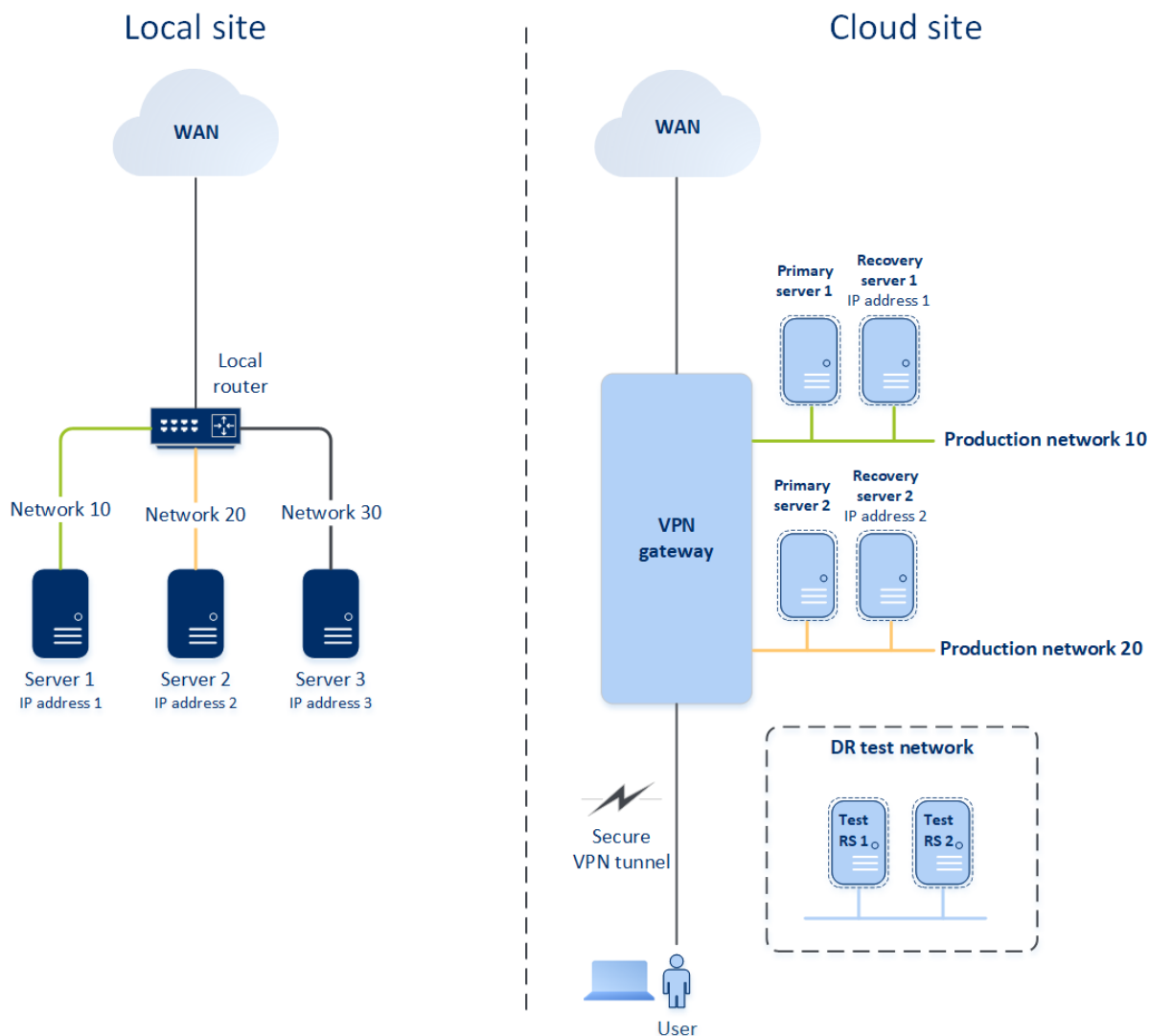
Aby uzyskać dostęp do lokalizacji lokalnej przy użyciu połączenia tego typu, trzeba wdrożyć w niej urządzenie VPN.

Tryb Tylko chmura

Tryb Tylko chmura nie wymaga wdrożenia urządzenia VPN w lokalizacji lokalnej. Oznacza to dwie niezależne sieci: jedną w lokalizacji lokalnej, drugą w lokalizacji w chmurze. Routing jest obsługiwany przez router w lokalizacji w chmurze.

Jak działa routing

W przypadku ustanowienia trybu Tylko chmura routing jest obsługiwany przez router w lokalizacji w chmurze, dzięki czemu mogą się ze sobą komunikować serwery z różnych sieci w chmurze.



Połączenie Open VPN site-to-site

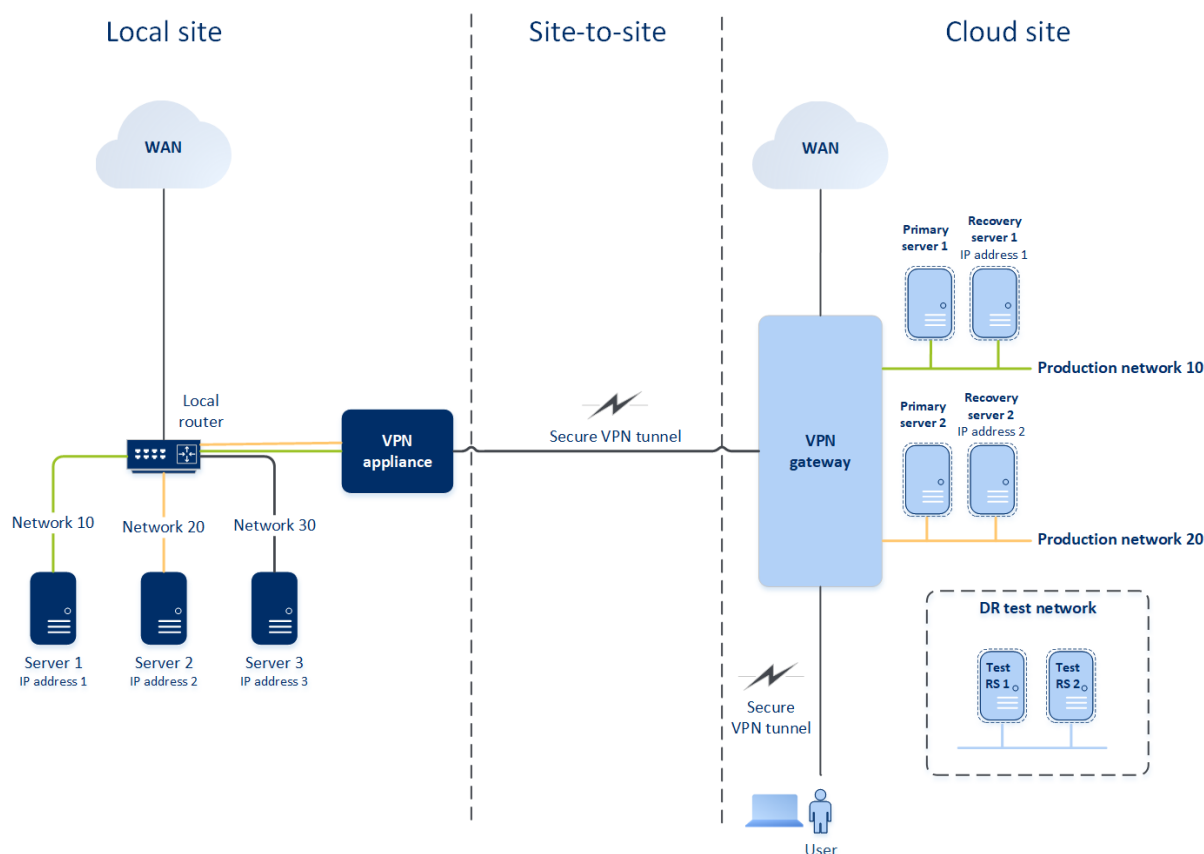
Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Aby przedstawić, jak działają sieci w ramach usługi Cyber Disaster Recovery Cloud, posłużymy się przykładem lokalizacji lokalnej, w której znajdują się trzy sieci z jednym komputerem w każdej z nich. Skonfigurujesz ochronę przed awarią w przypadku dwóch z tych sieci — Network 10 i Network 20.

Na poniższym diagramie widać lokalizację lokalną, w której są hostowane komputery, i lokalizację w chmurze, w której w razie awarii są uruchamiane serwery chmurowe.

Usługa Cyber Disaster Recovery Cloud pozwala na przełączenie awaryjne wszystkich obciążeń z uszkodzonych komputerów w lokalizacji lokalnej na serwery chmurowe w chmurze. Za pomocą usługi Cyber Disaster Recovery Cloud można chronić do 23 sieci.



Do komunikacji Open VPN site-to-site między lokalizacją lokalną i lokalizacją w chmurze służy **urządzenie VPN** i **brama VPN**. Gdy zaczniesz konfigurować połączenie Open VPN site-to-site w konsoli Cyber Protect, w lokalizacji w chmurze automatycznie zostanie wdrożona brama VPN. Następnie trzeba wdrożyć urządzenie VPN w lokalizacji lokalnej, dodać sieci, które mają być chronione, i zarejestrować urządzenie w chmurze. Usługa Cyber Disaster Recovery Cloud utworzy w chmurze replikę sieci lokalnej. Między urządzeniem VPN a bramą VPN jest tworzony bezpieczny tunel VPN. Oznacza on rozszerzenie sieci lokalnej o chmurę. Sieci produkcyjne w chmurze są połączone z sieciami lokalnymi. Serwery lokalne i chmurowe mogą się komunikować przez ten tunel VPN tak, jakby znajdowały się w tym samym segmencie sieci Ethernet. Routing jest obsługiwany przez lokalny router.

Dla każdego komputera źródłowego, który ma być chroniony, trzeba utworzyć serwer odzyskiwania w lokalizacji w chmurze. Dopóki nie nastąpi przełączenie awaryjne, działa on w **trybie gotowości**. Jeśli dojdzie do awarii i uruchomisz proces przełączania awaryjnego (w **trybie produkcyjnym**), w chmurze zostanie uruchomiony serwer odzyskiwania stanowiący dokładną kopię chronionego komputera. Może on mieć przypisany ten sam adres IP, który ma komputer źródłowy, i zostać uruchomiony w tym samym segmencie sieci Ethernet. Klienci nadal mogą korzystać z serwera, nie zauważając żadnych zmian zachodzących w tle.

Proces przełączania awaryjnego można też uruchomić w **trybie testowym**. Oznacza on, że komputer źródłowy nadal działa, a jednocześnie w chmurze zostaje uruchomiony odpowiedni serwer odzyskiwania o tym samym adresie IP. Aby zapobiec konfliktom adresów IP, w chmurze jest tworzona specjalna sieć wirtualna — **sieć testowa**. Sieć testowa jest odizolowana w celu

zapobieżenia zdublowaniu adresu IP komputera źródłowego w tym samym segmencie sieci Ethernet. Aby uzyskać dostęp do serwera odzyskiwania w trybie testowego przełączenia awaryjnego, podczas tworzenia tego serwera trzeba mu przypisać **Testowy adres IP**. Istnieją też inne parametry serwera odzyskiwania, które można zdefiniować — zostały one omówione w dalszej części dokumentu.

Jak działa routing

W przypadku nawiązania połączenia site-to-site routing między sieciami w chmurze jest obsługiwany przez router lokalny. Serwer VPN nie obsługuje routingu między serwerami chmurowymi znajdującymi się w różnych sieciach w chmurze. Jeśli serwer chmurowy z jednej sieci spróbuje się skomunikować z serwerem z innej sieci w chmurze, ruch przechodzi przez tunel VPN do routera lokalnego w lokalizacji lokalnej. Następnie router lokalny kieruje ruch do innej sieci, po czym ruch wraca przez tunel do serwera docelowego w lokalizacji w chmurze.

Brama VPN

Ważnym komponentem, który umożliwia komunikację między lokalizacją lokalną i lokalizacją w chmurze, jest **brama VPN**. Jest to maszyna wirtualna w chmurze z zainstalowanym specjalnym oprogramowaniem i szczególną konfiguracją sieci. Brama VPN pełni następujące funkcje:

- Łączy segmenty Ethernet sieci lokalnej i sieci produkcyjnej w chmurze w trybie L2.
- Udostępnia reguły iptables i ebtables.
- Stanowi domyślny router oraz NAT dla komputerów w sieciach testowych i produkcyjnych.
- Działa jako serwer DHCP. Wszystkie komputery w sieciach produkcyjnych i testowych muszą uzyskać konfigurację sieci (adresy IP, ustawienia DNS) przez DHCP. Serwer chmurowy za każdym razem otrzymuje od serwera DHCP ten sam adres IP. Jeśli zechcesz mieć własną konfigurację DNS, skontaktuj się z zespołem pomocy technicznej.
- Działa jako pamięć podręczna DNS.

Konfiguracja sieci bramy VPN

Brama VPN ma kilka interfejsów sieciowych:

- Interfejs zewnętrzny, połączony z Internetem
- Interfejsy produkcyjne, połączone z sieciami produkcyjnymi
- Interfejs testowy, połączony z siecią testową

Ponadto dodano dwa interfejsy wirtualne na potrzeby połączeń point-to-site i site-to-site.

Po wdrożeniu i zainicjowaniu bramy VPN tworzone są mostki: jeden dla interfejsu zewnętrznego, drugi dla interfejsu klienta i interfejsów produkcyjnych. Mimo że mostek interfejsów klienta i produkcyjnych oraz interfejs testowy używają tych samych adresów IP, brama VPN i tak jest w stanie prawidłowo kierować pakiety przy użyciu pewnej specjalnej techniki.

Urządzenie VPN

Urządzenie VPN to maszyna wirtualna w lokalizacji lokalnej z zainstalowanym systemem Linux i specjalnym oprogramowaniem oraz specjalną konfiguracją sieci. Umożliwia ono komunikację między lokalizacją lokalną i lokalizacją w chmurze.

Serwery odzyskiwania

Serwer odzyskiwania — replika oryginalnego komputera utworzona na podstawie przechowywanych w chmurze kopii zapasowych chronionego serwera. Serwery odzyskiwania służą do przełączania obciążeń z oryginalnych serwerów w razie wystąpienia awarii.

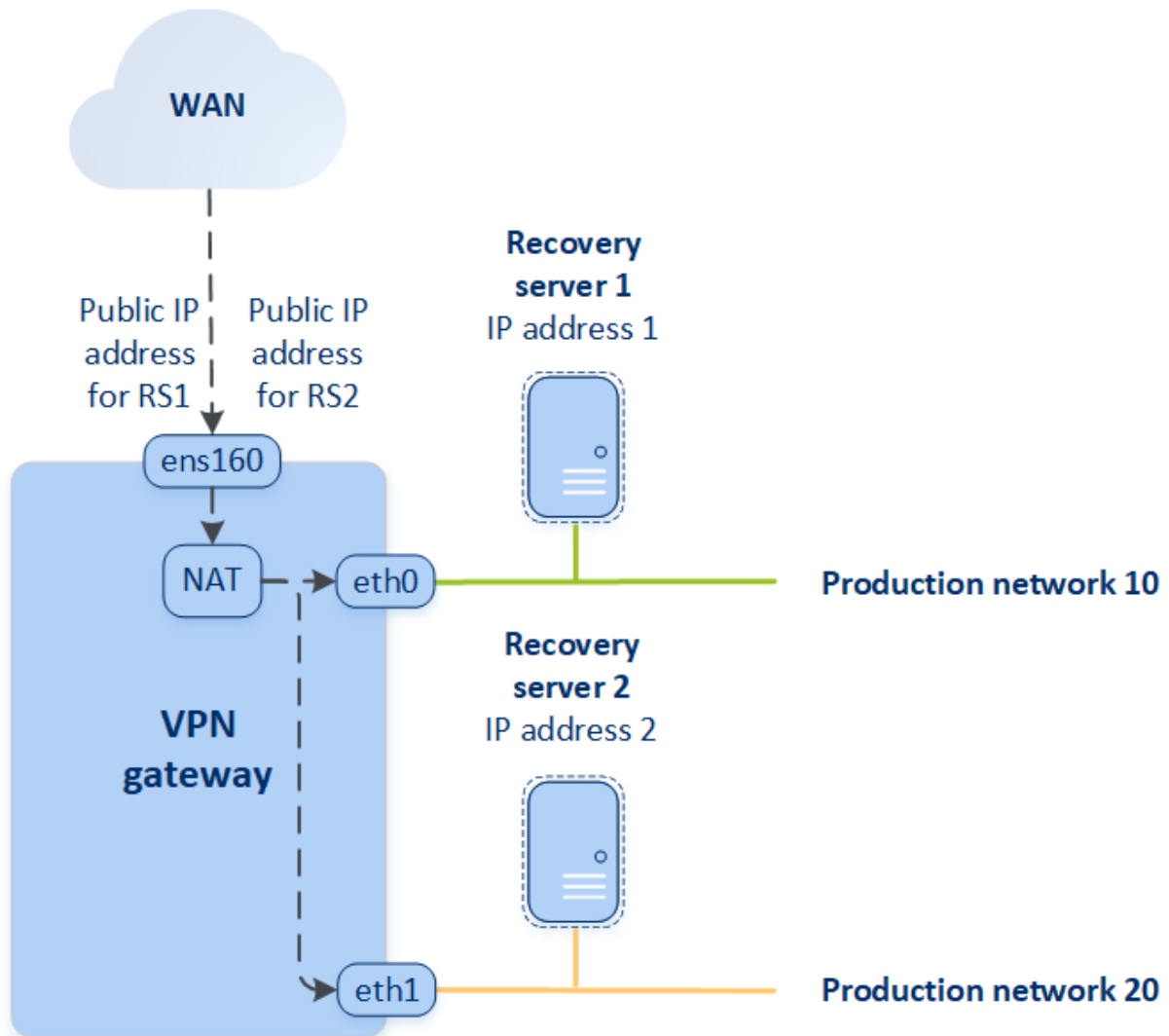
Podczas tworzenia serwera odzyskiwania trzeba określić następujące parametry sieciowe:

- **Sieć w chmurze** (wartość wymagana) — sieć w chmurze, do której zostanie podłączony serwer odzyskiwania.
- **Adres IP w sieci produkcyjnej** (wartość wymagana) — adres IP, z jakim zostanie uruchomiona maszyna wirtualna dla serwera odzyskiwania. Adres ten jest używany zarówno w sieciach produkcyjnych, jak i testowych. Przed uruchomieniem maszyna wirtualna zostaje skonfigurowana tak, aby uzyskała adres IP przez DHCP.
- **Testowy adres IP** (wartość opcjonalna) — adres IP potrzebny do uzyskania dostępu do serwera odzyskiwania z sieci produkcyjnej klienta podczas testowego przełączania awaryjnego, nadawany w celu zapobieżenia zdublowaniu produkcyjnego adresu IP w tej samej sieci. Ten adres IP różni się od adresu IP używanego w sieci produkcyjnej. Serwery w lokalizacji lokalnej mają dostęp do serwera odzyskiwania podczas testowego przełączania awaryjnego przy użyciu testowego adresu IP, podczas gdy dostęp w drugim kierunku nie jest możliwy. Jeśli podczas tworzenia serwera odzyskiwania została zaznaczona opcja **Dostęp do Internetu**, to można uzyskać dostęp do Internetu z serwera odzyskiwania znajdującego się w sieci testowej.
- **Publiczny adres IP** (wartość opcjonalna) — adres IP umożliwiający dostęp do serwera odzyskiwania z Internetu. Jeśli serwer nie ma publicznego adresu IP, można uzyskać do niego dostęp tylko z sieci lokalnej.
- **Dostęp do Internetu** (wartość opcjonalna) — aktywacja dostępu serwera odzyskiwania do Internetu (zarówno przy produkcyjnym, jak i testowym przełączaniu awaryjnym).

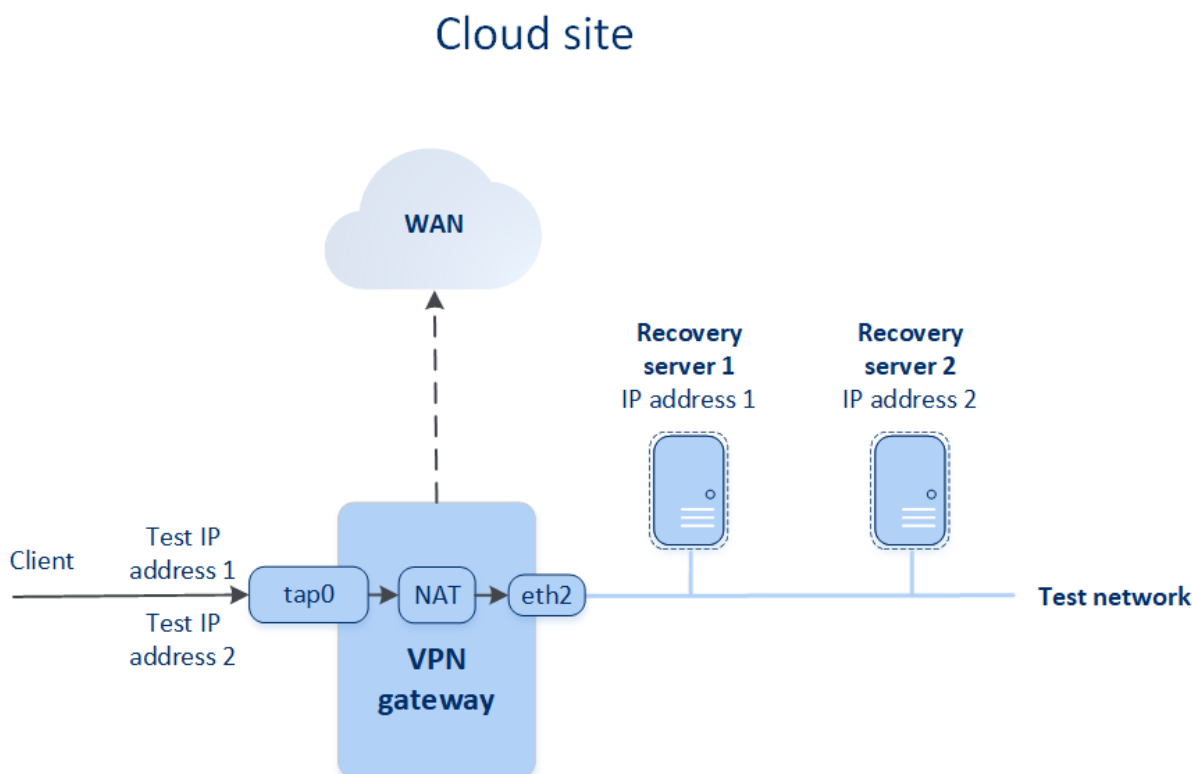
Publiczny i testowy adres IP

Jeśli podczas tworzenia serwera odzyskiwania zostanie mu przypisany publiczny adres IP, serwer ten będzie dostępny z Internetu przy użyciu tego adresu. Gdy z Internetu nadejdzie pakiet z publicznym adresem IP obiektu docelowego, brama VPN mapuje go na odpowiedni produkcyjny adres IP za pomocą usługi NAT i wysyła pakiet do odpowiadającego mu serwera odzyskiwania.

Cloud site



Jeśli podczas tworzenia serwera odzyskiwania zostanie mu przypisany testowy adres IP, serwer ten będzie dostępny w sieci testowej przy użyciu tego adresu. W przypadku wykonania testowego przełączenia awaryjnego oryginalny komputer nadal działa, a w sieci testowej w chmurze zostaje uruchomiony serwer odzyskiwania o tym samym adresie IP. Ponieważ sieć testowa jest odizolowana, nie występuje konflikt adresów IP. Serwery odzyskiwania w sieci testowej są dostępne przy użyciu ich testowych adresów IP, które są mapowane na produkcyjne adresy IP przez usługę NAT.



Dodatkowe informacje na temat połączeń VPN site-to-site: "Połączenie Open VPN site-to-site — dodatkowe informacje" (s. 99).

Serwery podstawowe

Serwer podstawowy — maszyna wirtualna, z którą nie jest powiązana żadna maszyna w lokalizacji lokalnej, w odróżnieniu od serwera odzyskiwania. Serwery podstawowe służą do ochrony aplikacji przy użyciu replikacji lub obsługi różnych usług pomocniczych (np. serwera internetowego).

Serwer główny jest najczęściej wykorzystywany w celu replikacji danych (w czasie rzeczywistym) ze wszystkich serwerów, na których uruchomione są kluczowe aplikacje. Replikację można ustawić samodzielnie za pomocą macierzystych narzędzi aplikacji. Na przykład replikacja Active Directory lub SQL może zostać skonfigurowana na potrzeby serwerów lokalnych oraz serwera podstawowego.

Serwer główny można też dołączyć do grupy AlwaysOn Availability Group (AAG) lub Database Availability Group (DAG).

Obie metody wymagają posiadania obszernej wiedzy na temat aplikacji oraz uprawnień administratora. Serwer główny nieustannie wykorzystuje zasoby obliczeniowe oraz miejsce w magazynie szybkiego odzyskiwania po awarii. Wymaga konserwacji ze strony użytkownika – monitorowania replikacji, instalowania aktualizacji oprogramowania, tworzenia kopii zapasowych. Korzyści serwera głównego to minimalne docelowe punkty i czasy odzyskiwania (RPO i RTO), obciążające środowisko produkcyjne w minimalnym stopniu (w porównaniu z metodą tworzenia w chmurze kopii zapasowych całych serwerów).

Serwery podstawowe zawsze są uruchamiane wyłącznie w sieci produkcyjnej i mają następujące parametry sieciowe:

- **Sieć w chmurze** (wartość wymagana) — sieć w chmurze, do której zostanie podłączony serwer podstawowy.
- **Adres IP w sieci produkcyjnej** (wartość wymagana) — adres IP serwera podstawowego w sieci produkcyjnej. Domyślnie wybierany jest pierwszy niezajęty adres IP w Twojej sieci produkcyjnej.
- **Publiczny adres IP** (wartość opcjonalna) — adres IP używany w celu uzyskania dostępu do serwera podstawowego z Internetu. Jeśli serwer nie ma publicznego adresu IP, można uzyskać do niego dostęp tylko z sieci lokalnej, a nie z Internetu.
- **Dostęp do Internetu** (wartość opcjonalna) — aktywacja dostępu serwera podstawowego do Internetu.

Połączenie IPsec VPN multi-site

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Połączenia IPsec VPN multi-site można użyć w celu połączenia jednej lub wielu lokalizacji lokalnych z usługą Cyber Disaster Recovery Cloud przez bezpieczne połączenie L3 IPsec VPN.

Łączność tego typu jest przydatna w scenariuszach usługi Disaster Recovery, jeśli występuje jedna z poniższych sytuacji:

- Masz jedną lokalizację lokalną hostującą krytyczne obciążenia.
- Masz wiele lokalizacji lokalnych hostujących krytyczne obciążenia, na przykład biura w różnych miejscach.
- korzystasz z lokalizacji oprogramowania innych firm lub lokalizacji dostawców usług zarządzanych i łączysz się z nimi za pośrednictwem tunelu IPsec VPN.

Do komunikacji IPsec VPN multi-site między lokalizacjami lokalnymi a lokalizacją w chmurze służy **brama VPN**. Gdy zaczniesz konfigurować połączenie IPsec VPN multi-site w konsoli Cyber Protect, w lokalizacji w chmurze automatycznie zostanie wdrożona brama VPN. Należy skonfigurować segmenty sieci w chmurze i dopilnować, aby nie pokrywały się z segmentami sieci lokalnej. Między lokalnymi lokalizacjami a lokalizacją w chmurze jest tworzony bezpieczny tunel VPN. Serwery lokalne i chmurowe mogą się komunikować przez ten tunel VPN tak, jakby znajdowały się w tym samym segmencie sieci Ethernet.

Dla każdego komputera źródłowego, który ma być chroniony, trzeba utworzyć serwer odzyskiwania w lokalizacji w chmurze. Dopóki nie nastąpi przełączenie awaryjne, działa on w **trybie gotowości**. Jeśli dojdzie do awarii i uruchomisz proces przełączania awaryjnego (w **trybie produkcyjnym**), w chmurze zostanie uruchomiony serwer odzyskiwania stanowiący dokładną kopię chronionego komputera. Klienci nadal mogą korzystać z serwera, nie zauważając żadnych zmian zachodzących w tle.

Proces przełączania awaryjnego można też uruchomić w **trybie testowym**. Oznacza on, że komputer źródłowy nadal działa, a jednocześnie w specjalnej sieci wirtualnej utworzonej w chmurze — **sieci testowej** — zostaje uruchomiony odpowiedni serwer odzyskiwania. Sieć testowa jest odizolowana w celu zapobieżenia duplikatom adresów IP w innych segmentach sieci w chmurze.

Brama VPN

Ważnym komponentem, który umożliwia komunikację między lokalizacjami lokalnymi a lokalizacją w chmurze, jest **brama VPN**. Jest to maszyna wirtualna w chmurze z zainstalowanym specjalnym oprogramowaniem i szczególną konfiguracją sieci. Brama VPN pełni następujące funkcje:

- Łączy segmenty Ethernet sieci lokalnej i sieci produkcyjnej w chmurze w trybie L3 IPsec.
- Stanowi domyślny router oraz NAT dla komputerów w sieciach testowych i produkcyjnych.
- Działa jako serwer DHCP. Wszystkie komputery w sieciach produkcyjnych i testowych muszą uzyskać konfigurację sieci (adresy IP, ustawienia DNS) przez DHCP. Serwer chmurowy za każdym razem otrzymuje od serwera DHCP ten sam adres IP.

Jeśli wolisz, możesz zdefiniować niestandardową konfigurację DNS. Aby uzyskać więcej informacji, zobacz "Konfigurowanie niestandardowych serwerów DNS" (s. 46).

- Działa jako pamięć podręczna DNS.

Jak działa routing

Routing między sieciami w chmurze jest obsługiwany przez router w lokalizacji w chmurze, dzięki czemu mogą się ze sobą komunikować serwery z różnych sieci w chmurze.

Zdalny dostęp VPN point-to-site

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

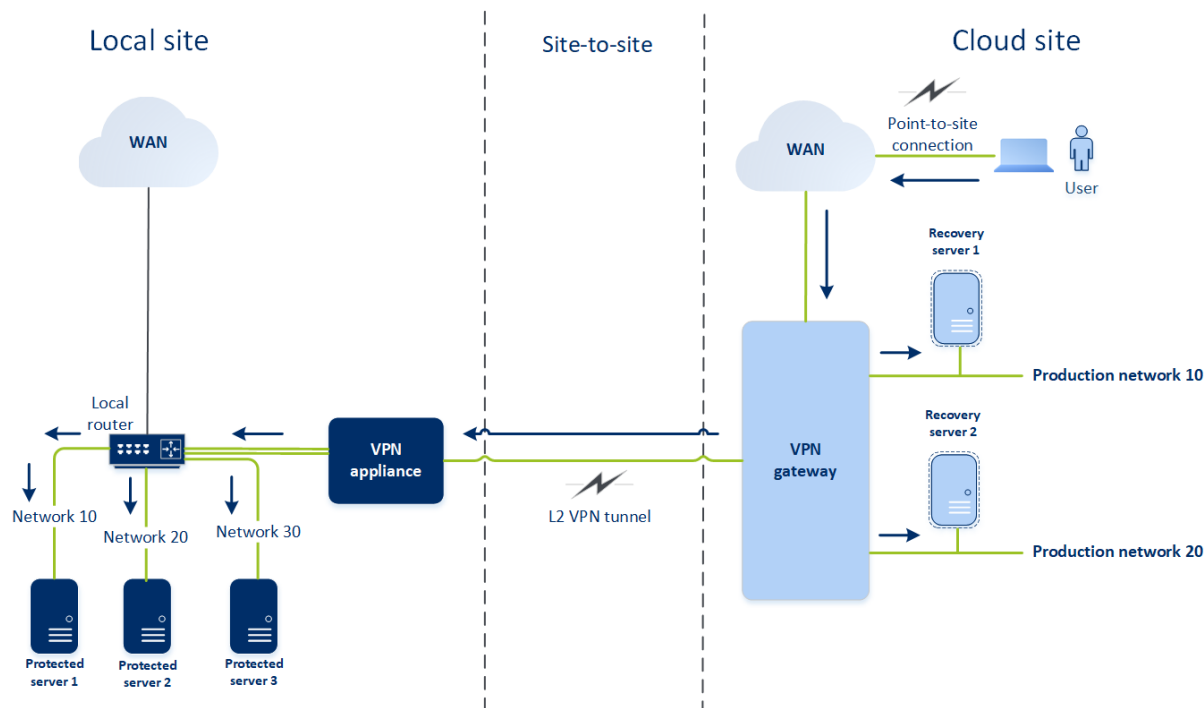
Połączenie point-to-site to bezpieczne połączenie z zewnątrz nawiązywane z urządzeń końcowych (np. komputera stacjonarnego lub laptopa) z lokalizacją lokalną lub lokalizacją w chmurze za pośrednictwem sieci VPN. Jest dostępne po nawiązaniu połączenia Open VPN site-to-site z lokalizacją Cyber Disaster Recovery Cloud. Połączenie tego typu jest przydatne w następujących przypadkach:

- W wielu firmach ich usługi i zasoby internetowe są dostępne tylko z firmowych sieci. Połączenie point-to-site umożliwia bezpieczne łączenie się z lokalizacją lokalną.
- W razie wystąpienia awarii, gdy obciążenie jest przenoszone do lokalizacji w chmurze, a sieć lokalna nie działa, może być konieczny bezpośredni dostęp do serwerów chmurowych. Jest to możliwe za pośrednictwem połączenia point-to-site z lokalizacją w chmurze.

W celu ustanowienia połączenia point-to-site z lokalizacją lokalną należy zainstalować w niej urządzenie VPN i skonfigurować połączenie site-to-site, a następnie połączenie point-to-site z

lokalizacją lokalną. Dzięki temu pracownicy zdalni będą mieli dostęp do firmowej sieci przez VPN warstwy 2 (L2 VPN).

Poniższy schemat przedstawia lokalizację lokalną, lokalizację w chmurze oraz komunikację między serwerami wyróżnioną kolorem zielonym. Tunel VPN warstwy 2 łączy lokalizację lokalną z lokalizacją w chmurze. Gdy użytkownik nawiąże połączenie point-to-site, komunikacja z lokalizacją lokalną odbywa się za pośrednictwem lokalizacji w chmurze.



W konfiguracji połączenia point-to-site do uwierzytelniania klienta VPN są używane certyfikaty. Dodatkowo do uwierzytelniania służą też poświadczenia użytkownika. Warto pamiętać o następujących kwestiach dotyczących połączenia point-to-site z lokalizacją lokalną:

- W celu uwierzytelnienia się w kliencie VPN użytkownicy powinni używać swoich poświadczeń z platformy Cyber Protect Cloud. Muszą też mieć przypisaną rolę użytkownika „Administrator firmy” lub „Cyber Protection”.
- W razie [ponownego utworzenia konfiguracji OpenVPN](#) trzeba przekazać zaktualizowaną konfigurację wszystkim użytkownikom korzystającym z połączenia point-to-site z lokalizacją w chmurze.

Automatyczne usuwanie nieużywanych środowisk klientów w lokalizacji w chmurze

Disaster Recovery monitoruje wykorzystanie środowisk klientów utworzonych na potrzeby odzyskiwania po awarii i automatycznie je usuwa, jeśli nie są używane.

W celu ustalenia, czy dzierżawca-klient jest aktywny, są używane następujące kryteria:

- Co najmniej jeden serwer chmurowy istnieje obecnie lub istniał w ciągu ostatnich 7 dni.

LUB

- Opcja **Dostęp VPN do lokalizacji lokalnej** jest włączona i albo został utworzony tunel Open VPN site-to-site, albo istnieją dane zgłoszone z urządzenia VPN dotyczące ostatnich 7 dni.

Pozostali dzierżawcy są uznawani za nieaktywnych. W przypadku takich dzierżawców system wykonuje następujące czynności:

- Usuwa bramę VPN i wszystkie zasoby chmury powiązane z danym dzierżawcą.
- Wyrejestrowuje urządzenie VPN.

W przypadku nieaktywnych dzierżawców przywracany jest ich stan sprzed skonfigurowania łączności.

Początkowa konfiguracja łączności

W tej sekcji opisano scenariusze konfiguracji łączności.

Konfigurowanie trybu Tylko chmura

Aby skonfigurować połączenie w trybie Tylko chmura

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii > Łączność**.
2. Wybierz **Tylko chmura** i kliknij **Konfiguruj**.
W wyniku tego w lokalizacji w chmurze zostanie wdrożona brama VPN i sieć w chmurze o zdefiniowanym adresie i masce.

Informacje na temat zarządzania sieciami w chmurze i konfigurowania ustawień bramy VPN można znaleźć w sekcji „[Zarządzanie sieciami w chmurze](#)”.

Konfigurowanie połączenia Open VPN site-to-site

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Wymagania urządzenia VPN

Wymagania systemowe

- 1 PROCESOR
- 1 GB PAMIĘCI RAM
- 8 GB miejsca na dysku

Porty

- TCP 443 (połączenia wychodzące) — do połączenia VPN
- TCP 80 (połączenia wychodzące) — do automatycznych [aktualizacji urządzenia](#)

Upewnij się, że zapory i inne składniki systemu zabezpieczeń sieci umożliwiają połączenia przez te porty z dowolnym adresem IP.

Konfigurowanie połączenia Open VPN site-to-site

Urządzenie VPN rozszerza Twoją sieć lokalną o chmurę przy użyciu bezpiecznego tunelu VPN. Połączenie tego rodzaju jest często nazywane połączeniem „site-to-site” (S2S). Możesz postąpić zgodnie z poniższą procedurą lub obejrzeć [instruktaż wideo](#).

Aby skonfigurować połączenie za pośrednictwem urządzenia VPN

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii > Łączność**.
2. Wybierz **Połączenie Open VPN site-to-site** i kliknij **Konfiguruj**.
System rozpocznie wdrażanie bramy VPN w chmurze. Może to potrwać jakiś czas. W międzyczasie możesz przejść do następnego kroku.

Uwaga

Brama VPN jest udostępniana bez dodatkowych opłat. Zostanie usunięta w razie nieskorzystania z funkcji Disaster Recovery, tj. w razie braku jakiegokolwiek serwera podstawowego lub serwera odzyskiwania w chmurze przez 7 dni.

3. W sekcji **Urządzenie VPN** kliknij **Pobierz i wdróż**. Pobierz urządzenie VPN dla VMware vSphere lub Microsoft Hyper-V – zależnie od używanej platformy wirtualizacji.
4. Wdróż urządzenie i połącz je z sieciami produkcyjnymi.
W środowisku vSphere upewnij się, że włączono **tryb nieograniczony** i że opcja **Fałszywe transmisje** ma ustawienie **Akceptuj** w przypadku wszystkich przełączników wirtualnych łączących urządzenie VPN z sieciami produkcyjnymi. Aby uzyskać dostęp do tych ustawień, wybierz w kliencie vSphere host > **Podsumowanie > Sieć > przełącznik > Edytuj ustawienia > Bezpieczeństwo**.
Jeśli używasz Hyper-V, utwórz maszynę wirtualną typu **Generacja 1** mającą co najmniej 1024 MB pamięci. Warto też włączyć dla tej maszyny opcję **Pamięć dynamiczna**. Po utworzeniu maszyny kliknij **Ustawienia > Sprzęt > Karta sieciowa > Funkcje zaawansowane** i zaznacz pole wyboru obok opcji **Włącz fałszowanie adresów MAC**.
5. Włącz urządzenie
6. Przejdź do konsoli urządzenia i zaloguj się przy użyciu nazwy użytkownika i hasła „admin/admin”.
7. [Opcjonalnie] Zmień hasło.
8. [Opcjonalnie] Zmień ustawienia sieci, jeśli jest to konieczne. Określ, który interfejs będzie używany jako interfejs sieci WAN na potrzeby połączenia z Internetem.

9. Zarejestruj urządzenie w usłudze Cyber Protection przy użyciu poświadczeń administratora firmy.

Poświadczenia są używane tylko raz w celu pobrania certyfikatu. Adres URL centrum danych jest wstępnie zdefiniowany.

Uwaga

Jeśli na koncie jest skonfigurowane uwierzytelnianie dwuskładnikowe, pojawi się również monit o wprowadzenie kodu TOTP. Jeśli uwierzytelnianie dwuskładnikowe jest włączone, ale nie jest skonfigurowane na koncie, nie można zarejestrować urządzenia VPN. Najpierw trzeba przejść do strony logowania się do konsoli Cyber Protect i skonfigurować na koncie uwierzytelnianie dwuskładnikowe. Więcej informacji na temat uwierzytelniania dwuskładnikowego można znaleźć w Podręczniku administratora portalu zarządzania.

Gdy konfiguracja zostanie zakończona, urządzenie będzie miało status **Online**. Urządzenie połączy się z bramą VPN i zacznie zgłaszać usłudze Cyber Disaster Recovery Cloud informacje o sieciach ze wszystkich aktywnych interfejsów. Interfejsy te są wyświetlane w konsoli Cyber Protect na podstawie informacji z urządzenia VPN.

Konfigurowanie połączenia IPsec VPN multi-site

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Połączenie IPsec VPN multi-site można skonfigurować na dwa sposoby:

- Na karcie **Odzyskiwanie po awarii** > **Łączność**.
- Przez zastosowanie planu ochrony na jednym lub kilku urządzeniach, a następnie ręczne przełączenie z automatycznie utworzonego połączenia Open VPN site-to-site na połączenie IPsec VPN multi-site, skonfigurowanie ustawień IPsec VPN multi-site i zmianę przypisania adresów IP.

Aby skonfigurować połączenie IPsec VPN multi-site na karcie Łączność

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii** > **Łączność**.
2. W sekcji **Połączenie VPN multi-site** kliknij **Konfiguruj**.
Brama VPN jest wdrażana w lokalizacji w chmurze.
3. [Skonfiguruj ustawienia połączenia IPsec VPN multi-site](#).

Aby skonfigurować połączenie IPsec VPN multi-site w planie ochrony

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia**.
2. Zastosuj plan ochrony do jednego lub wielu urządzeń z listy.
Serwer odzyskiwania i ustawienia infrastruktury chmury są automatycznie konfigurowane do łączności Open VPN site-to-site.
3. Wybierz **Odzyskiwanie po awarii** > **Łączność**.
4. Kliknij **Pokaż właściwości**.

5. Kliknij **Zmień na połączenie IPsec VPN multi-site**.
6. [Skonfiguruj ustawienia połączenia IPsec VPN multi-site](#).
7. [Zmień przypisanie adresów IP](#) sieci w chmurze i serwerów chmurowych.

Konfigurowanie ustawień połączenia IPsec VPN multi-site

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Po skonfigurowaniu łączności IPsec VPN multi-site trzeba skonfigurować ustawienia lokalizacji w chmurze i lokalizacji lokalnych na karcie **Odzyskiwanie po awarii > Łączność**.

Wymagania wstępne

- Skonfigurowano łączność IPsec VPN multi-site. Dodatkowe informacje na temat konfigurowania łączności IPsec VPN multi-site można znaleźć w sekcji "Konfigurowanie połączenia IPsec VPN multi-site" (s. 31).
- Każda lokalna brama IPsec VPN ma publiczny adres IP.
- Dostępna sieć w chmurze ma wystarczająco dużo adresów IP dla serwerów chmurowych, które są kopiami chronionych komputerów (z sieci produkcyjnej), oraz dla serwerów odzyskiwania (z jednym lub dwoma adresami IP, w zależności od potrzeb).
- W przypadku stosowania zapory między lokalizacjami lokalnymi a lokalizacją w chmurze dozwolone są następujące protokoły IP i porty UDP w lokalizacjach lokalnych: Protokół IP ID 50 (ESP), port UDP 500 (IKE) i port UDP 4500.
- Konfiguracja NAT-T w miejscach lokalnych jest wyłączona.

Aby skonfigurować połączenie IPsec VPN multi-site

1. Dodaj jedną lub więcej sieci do lokalizacji w chmurze.
 - a. Kliknij **Dodaj sieć**.

Uwaga

W przypadku dodawania sieci w chmurze odpowiednia sieć testowa jest dodawana automatycznie z tym samym adresem sieciowym i maską na potrzeby testowego przełączania awaryjnego. Serwery chmurowe w sieci testowej będą miały takie same adresy IP jak w sieci produkcyjnej w chmurze. Jeśli podczas testowego przełączania awaryjnego jest konieczny dostęp do serwera chmurowego z sieci produkcyjnej, to w trakcie tworzenia serwera odzyskiwania należy przypisać drugi testowy adres IP.

- b. W polu **Adres sieciowy** wpisz adres IP sieci.
 - c. W polu **Maska sieci** wpisz adres maskę sieci.
 - d. Kliknij **Dodaj**.

2. Skonfiguruj ustawienia dla każdej lokalizacji lokalnej, która ma być połączona z lokalizacją w chmurze, zgodnie z zaleceniami dotyczącymi lokalizacji lokalnych. Dodatkowe informacje na temat tych zaleceń można znaleźć w sekcji "Ogólne zalecenia dotyczące lokalizacji lokalnych" (s. 33).
 - a. Kliknij **Dodaj połączenie**.
 - b. Wprowadź nazwę lokalnej bramy VPN.
 - c. Wprowadź publiczny adres IP lokalnej bramy VPN.
 - d. [Opcjonalnie] Wprowadź opis lokalnej bramy VPN.
 - e. Kliknij **Dalej**.
 - f. W polu **Klucz współdzielony (PSK)** wpisz klucz PSK lub kliknij **Wygeneruj nowy klucz współdzielony (PSK)**, aby użyć wartości wygenerowanej automatycznie.

Uwaga

W przypadku lokalnej i chmurowej bramy VPN trzeba użyć tego samego klucza PSK.

- g. Kliknij **Ustawienia zabezpieczeń IPsec/IKE**, aby skonfigurować te ustawienia. Dodatkowe informacje na temat ustawień, które można konfigurować, można znaleźć w sekcji "Ustawienia zabezpieczeń IPsec/IKE" (s. 34).

Uwaga

Można użyć ustawień domyślnych, które są wprowadzane automatycznie, lub użyć własnych wartości. Obsługiwane są tylko połączenia przy użyciu protokołu IKEv2. W przypadku ustanawiania łączności VPN domyślną wartością pola **Czynność podczas uruchamiania** jest **Dodaj** (połączenie inicjuje lokalna brama VPN), ale można ją zmienić na **Rozpocznij** (połączenie inicjuje chmurowa brama VPN) lub **Przekieruj** (opcja odpowiednia w przypadku zapór obsługujących opcję routingu).

- h. Skonfiguruj **Zasady dotyczące sieci**.

Zasady dotyczące sieci określają, z którymi sieciami łączy się IPsec VPN. Wprowadź adres IP i maskę sieci w formacie CIDR. Segmenty sieci lokalnej i sieci w chmurze nie powinny się na siebie nakładać.
 - i. Kliknij **Zapisz**.

Ogólne zalecenia dotyczące lokalizacji lokalnych

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Konfigurując lokalizacje lokalne pod kątem łączności IPsec VPN multi-site, warto wziąć pod uwagę następujące zalecenia:

- W przypadku każdej fazy IKE należy ustawić co najmniej jedną z wartości skonfigurowanych w lokalizacji w chmurze w ramach następujących parametrów: algorytm szyfrowania, algorytm

skrótów i liczby z grup Diffiego-Hellmana.

- Włącz doskonale utajnianie z wyprzedzeniem przy użyciu co najmniej jednej z wartości dla liczb z grup Diffiego-Hellmana skonfigurowanych w lokalizacji w chmurze w przypadku fazy 2 IKE.
- W przypadku fazy 1 IKE i fazy 2 IKE skonfiguruj tę samą wartość ustawienia **Czas aktywności** co w lokalizacji w chmurze.
- Konfiguracje z przechodzenie translacji NAT (NAT-T) nie są obsługiwane. Wyłącz konfigurację NAT-T w lokalizacji lokalnej. W przeciwnym razie nie będzie możliwa negocjacja dodatkowej hermetyzacji UDP.
- Konfiguracja **Czynność podczas uruchamiania** określa, która strona inicjuje połączenie. Wartość domyślna **Dodaj** oznacza, że lokalizacja lokalna inicjuje połączenie, a lokalizacja w chmurze oczekuje na zainicjowanie połączenia. Zmień wartość na **Rozpocznij**, jeśli to lokalizacja w chmurze ma inicjować połączenie, lub na **Przekieruj**, jeśli obie strony mają mieć możliwość inicjowania połączenia (ustawienie odpowiednie w przypadku zapór obsługujących opcję routingu).

Dodatkowe informacje i przykłady konfiguracji dotyczące innych rozwiązań można znaleźć na stronie:

- [Seria artykułów z bazy wiedzy Knowledge Base](#)
- [Film z przykładem](#)

Ustawienia zabezpieczeń IPsec/IKE

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Poniższa tabela zawiera dodatkowe informacje na temat parametrów zabezpieczeń IPsec/IKE.

Parametr	Opis
Algorytm szyfrowania	Algorytm szyfrowania, który będzie używany do blokowania wglądu w dane podczas przesyłania. Domyślnie są wybrane wszystkie algorytmy. Na lokalnym urządzeniu bramy trzeba skonfigurować co najmniej jeden z wybranych algorytmów dla każdej fazy IKE.
Algorytm skrótów	Algorytm skrótów, który będzie używany do weryfikowania integralności i autentyczności danych. Domyślnie są wybrane wszystkie algorytmy. Na lokalnym urządzeniu bramy trzeba skonfigurować co najmniej jeden z wybranych algorytmów dla każdej fazy IKE.
Liczby z grup Diffiego-Hellmana	Liczby z grup Diffiego-Hellmana definiują siłę klucza używanego w procesie wymiany kluczy

Parametr	Opis
	<p>Internet Key Exchange (IKE).</p> <p>Liczby z wyższych grup są bezpieczniejsze, ale wymagają dodatkowego czasu na obliczenie klucza.</p> <p>Domyślnie są wybrane wszystkie grupy. Na lokalnym urządzeniu bramy trzeba skonfigurować co najmniej jedną z wybranych grup dla każdej fazy IKE.</p>
Czas aktywności (w sekundach)	<p>Wartość czasu aktywności oznacza czas trwania instancji połączenia z ustawionymi kluczami szyfrowania/uwierzelniania dla pakietów użytkowników: od pomyślnej negocjacji po wygaśnięcie.</p> <p>Zakres dla fazy 1: 900–28800 s, domyślny: 28800.</p> <p>Zakres dla fazy 2: 900–3600 s, domyślny: 3600.</p> <p>Czas aktywności dla fazy 2 musi być krótszy od czasu aktywności dla fazy 1.</p> <p>Połączenie jest ponownie negocjowane przez kanał negocjujący klucz przed jego wygaśnięciem. Zobacz Czas marginesu ponownej negocjacji klucza. Jeśli strona lokalna i zdalna nie zgadzają się co do czasu aktywności, po stronie z dłuższym czasem aktywności wystąpią bezładne zastąpione połączenia. Zobacz także Czas marginesu ponownej negocjacji klucza i Zakres wahań ponownej negocjacji kluczy.</p>
Czas marginesu ponownej negocjacji klucza (w sekundach)	<p>Czas marginesu poprzedzający wygaśnięcie połączenia lub kanału negocjacji klucza, w ramach którego lokalna strona połączenia VPN próbuje wynegocjować zamianę. Dokładny czas ponownej negocjacji klucza jest wybierany losowo z uwzględnieniem wartości Zakres wahań ponownej negocjacji kluczy. Jest to istotne tylko lokalnie — strona zdalna nie musi się na to zgadzać. Zakres: 900–3600 s. Wartość domyślna to 3600.</p>
Rozmiar okna tłumienia ataku powtórki (pakiet)	<p>Rozmiar okna tłumienia ataku powtórki dla połączenia.</p> <p>Domyślna wartość -1 używa wartości skonfigurowanej za pomocą charon.replay_window</p>

Parametr	Opis
	<p>w pliku strongswan.conf.</p> <p>Wartości większe niż 32 są obsługiwane tylko w przypadku korzystania z infrastruktury zaplecza Netlink.</p> <p>Wartość 0 powoduje wyłączenie ochrony IPsec przed atakami powtórki.</p>
Zakres wahań ponownej negocjacji kluczy (%)	<p>Maksymalny procent, o jaki losowo są zwiększane wartości bajtów, pakietów i czasu marginesu w celu randomizacji przedziałów czasu ponownej negocjacji kluczy (istotne w przypadku hostów z wieloma połączeniami).</p> <p>Wartość zakresu wahań ponownej negocjacji kluczy może przekraczać 100%. Wartość ustawienia marginTYPE po losowym zwiększeniu nie może przekraczać progu lifeTYPE, gdzie TYPE jest jednym z bajtów bądź pakietów albo czasem.</p> <p>Wartość 0% powoduje wyłączenie randomizacji. Jest to istotne tylko lokalnie — strona zdalna nie musi się na to zgadzać.</p>
Limit czasu funkcji DPD (w sekundach)	<p>Czas, po którym następuje upływanie limitu czasu funkcji Dead Peer Detection (DPD). Można określić wartość 30 lub wyższą. Wartość domyślna to 30.</p>
Czynność po upływie limitu czasu funkcji Dead Peer Detection (DPD)	<p>Czynność podejmowana po upływie limitu czasu funkcji Dead Peer Detection (DPD).</p> <p>Uruchom ponownie — po upływie limitu czasu funkcji DPD nastąpi ponowne uruchomienie sesji.</p> <p>Wyczyść — po upływie limitu czasu funkcji DPD nastąpi zakończenie sesji.</p> <p>Brak — po upływie limitu czasu funkcji DPD nie zostanie podjęta żadna czynność.</p>
Czynność podczas uruchamiania	<p>Określa, która strona inicjuje połączenie i ustanawia tunel dla połączenia VPN.</p> <p>Dodaj — połączenie inicjuje lokalna brama VPN.</p> <p>Rozpocznij — połączenie inicjuje brama VPN w chmurze.</p> <p>Przekieruj — opcja odpowiednia w przypadku bram VPN obsługujących opcję routingu. tunel jest aktywny tylko wtedy, gdy ruch jest inicjowany z lokalnej bramy VPN lub chmurowej bramy VPN.</p>

Zalecenia dotyczące dostępności usług Active Directory Domain Services

Jeśli chronione obciążenia muszą być uwierzytelniane na kontrolerze domeny, zalecamy zastosowanie instancji kontrolera domeny usługi Active Directory w lokalizacji usługi Disaster Recovery.

Kontroler domeny usługi Active Directory na potrzeby łączności L2 Open VPN

Dzięki łączności L2 Open VPN adresy IP chronionych obciążeń są zachowywane w lokalizacji w chmurze podczas testowego lub produkcyjnego przełączania awaryjnego. W związku z tym kontroler domeny usługi Active Directory podczas testowego lub produkcyjnego przełączania awaryjnego ma taki sam adres IP jak w lokalizacji lokalnej.

Dzięki niestandardowym ustawieniom usługi DNS możesz ustawić własny serwer DNS dla wszystkich serwerów chmurowych. Aby uzyskać więcej informacji, zobacz "Konfigurowanie niestandardowych serwerów DNS" (s. 46).

Kontroler domeny usługi Active Directory na potrzeby łączności L3 IPsec VPN

W przypadku łączności L3 IPsec VPN adresy IP chronionych obciążeń nie są zachowywane w lokalizacji w chmurze. Dlatego przed wykonaniem produkcyjnego przełączenia awaryjnego warto wdrożyć dodatkową specjalną instancję kontrolera domeny usługi AD jako serwer podstawowy w lokalizacji w chmurze.

Oto zalecenia dotyczące specjalnej instancji kontrolera domeny usługi AD skonfigurowanej jako serwer podstawowy w lokalizacji w chmurze:

- Wyłącz Zaporę systemu Windows.
- Dołącz serwer podstawowy do usługi Active Directory.
- Dopilnuj, aby serwer podstawowy miał dostęp do Internetu.
- Dodaj funkcję Active Directory.

Dzięki niestandardowym ustawieniom usługi DNS możesz ustawić własny serwer DNS dla wszystkich serwerów chmurowych. Aby uzyskać więcej informacji, zobacz "Konfigurowanie niestandardowych serwerów DNS" (s. 46).

Konfigurowanie zdalnego dostępu VPN point-to-site

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

W przypadku konieczności nawiązania połączenia zdalnego z lokalizacją lokalną można skonfigurować połączenie point-to-site z lokalizacją lokalną. Możesz postąpić zgodnie z poniższą procedurą lub obejrzeć [instruktaż wideo](#).

Wymagania wstępne

- Skonfigurowano łączność Open VPN site-to-site.
- Urządzenie VPN jest zainstalowane w lokalizacji lokalnej.

Aby skonfigurować połączenie point-to-site z lokalizacją lokalną

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii > Łączność**.
2. Kliknij **Pokaż właściwości**.
3. Włącz opcję **Dostęp VPN do lokalizacji lokalnej**.
4. Sprawdź, czy użytkownik nawiązujący połączenie point-to-site z lokalizacją lokalną ma:
 - Konto użytkownika na platformie Cyber Protect Cloud. To tych poświadczeń musi użyć w celu uwierzytelnienia się w kliencie VPN. Jeśli nie ma, [utwórz odpowiednie konto użytkownika na platformie Cyber Protect Cloud](#).
 - Rolę użytkownika „Administrator firmy” lub „Cyber Protection”.
5. Skonfiguruj klienta OpenVPN:
 - a. Pobierz klienta OpenVPN w wersji 2.4.0 lub nowszej ze strony:
<https://openvpn.net/community-downloads/>.
 - b. Zainstaluj klienta OpenVPN na komputerze, z którego chcesz się połączyć z lokalizacją lokalną.
 - c. Kliknij **Pobierz konfigurację dla pakietu OpenVPN**. Plik konfiguracyjny działa w przypadku użytkowników z organizacji mających rolę użytkownika „Administrator firmy” lub „Cyberochrona”.
 - d. Zaimportuj pobraną konfigurację do OpenVPN.
 - e. Zaloguj się do klienta OpenVPN, korzystając ze swoich poświadczeń użytkownika z platformy Cyber Protect Cloud (patrz krok 4 powyżej).
 - f. [Opcjonalnie] Jeśli w organizacji jest włączone uwierzytelnianie dwuskładnikowe, podaj również [wygenerowany jednorazowy kod TOTP](#).

Ważne

W przypadku włączenia dla konta uwierzytelniania dwuskładnikowego trzeba ponownie wygenerować plik konfiguracyjny i odnowić go na potrzeby istniejących klientów OpenVPN. Aby skonfigurować uwierzytelnianie dwuskładnikowe dla swojego konta, użytkownik musi się ponownie zalogować na platformie Cyber Protect Cloud.

Dzięki temu będzie mógł nawiązywać połączenia z komputerami w lokalizacji lokalnej.

Zarządzanie sieciami

W tej sekcji opisano scenariusze zarządzania sieciami.

Zarządzanie sieciami

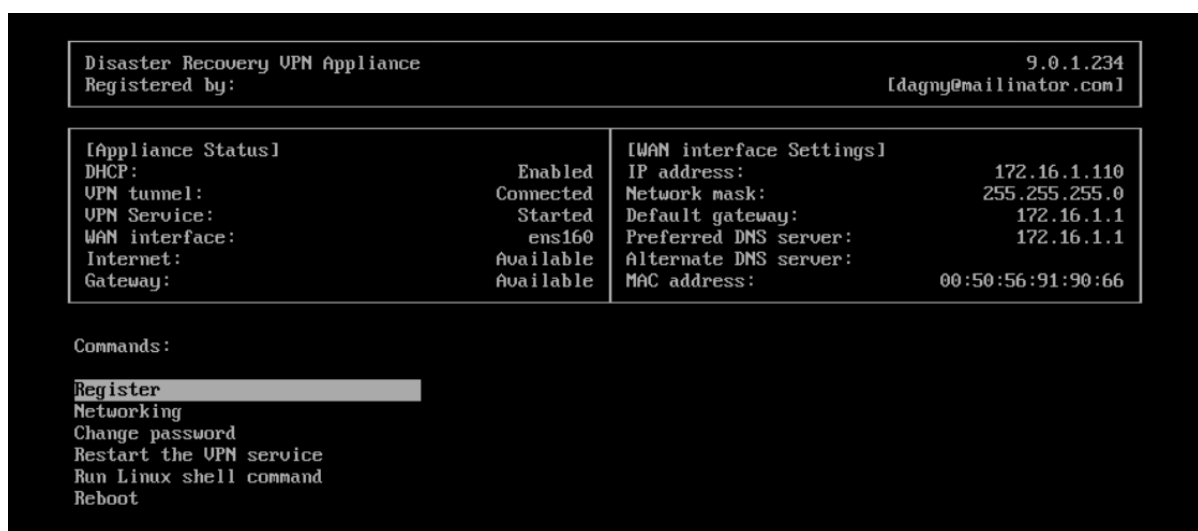
Uwaga

Niektóre funkcje mogą wymagać dodatkowego licencjonowania — w zależności od stosowanego modelu licencjonowania.

Połączenie Open VPN site-to-site

Aby dodać sieć do lokalizacji lokalnej i rozszerzyć ją o chmurę

1. Skonfiguruj w urządzeniu VPN nowy interfejs sieciowy dla sieci lokalnej, którą chcesz rozszerzyć o chmurę.
2. Zaloguj się do konsoli urządzenia VPN.
3. W sekcji **Sieć** skonfiguruj ustawienia sieciowe nowego interfejsu.



Urządzenie VPN zacznie zgłaszać usłudze Cyber Disaster Recovery Cloud informacje o sieciach ze wszystkich aktywnych interfejsów. Interfejsy te są wyświetlane w konsoli Cyber Protect na podstawie informacji z urządzenia VPN.

Aby usunąć sieć rozszerzoną o chmurę

1. Zaloguj się do konsoli urządzenia VPN.
2. W sekcji **Sieć** wybierz interfejs, który chcesz usunąć, a następnie kliknij **Wyczyść ustawienia sieciowe**.
3. Potwierdź operację.

W rezultacie zostanie wyłączone rozszerzenie sieci lokalnej o chmurę przy użyciu bezpiecznego tunelu VPN. Sieć będzie działać jako niezależny segment chmury. Jeśli ten interfejs służył do przekazywania ruchu z (do) lokalizacji w chmurze, wszystkie połączenia sieciowe z (do) lokalizacji w chmurze zostaną zerwane.

Aby zmienić parametry sieciowe

1. Zaloguj się do konsoli urządzenia VPN.
2. W sekcji **Sieć** wybierz interfejs, który chcesz edytować.
3. Kliknij **Edytuj ustawienia sieciowe**.
4. Wybierz jedną z dwóch możliwych opcji:
 - Aby uzyskać automatyczną konfigurację sieci przez DHCP, kliknij **Użyj DHCP**. Potwierdź operację.
 - Aby ręcznie skonfigurować sieć, kliknij **Ustaw statyczny adres IP**. Można edytować następujące ustawienia:
 - **Adres IP** — adres IP interfejsu w sieci lokalnej.
 - **Adres IP bramy VPN** — specjalny adres IP zarezerwowany dla tego chmurowego segmentu sieci w celu zapewnienia odpowiedniego działania usługi Cyber Disaster Recovery Cloud.
 - **Maska sieci** — maska sieci lokalnej.
 - **Brama domyślna** — domyślna brama w lokalizacji lokalnej.
 - **Preferowany serwer DNS** — podstawowy serwer DNS w lokalizacji lokalnej.
 - **Alternatywny serwer DNS** — dodatkowy serwer DNS w lokalizacji lokalnej.

```
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:
```

- Wprowadź niezbędne zmiany i potwierdź je klawiszem Enter.

Tryb Tylko chmura

W chmurze można mieć do 23 sieci.

Aby dodać nową sieć w chmurze

1. Wybierz **Odzyskiwanie po awarii > Łączność**.
2. W sekcji **Lokalizacja w chmurze** kliknij **Dodaj sieć w chmurze**.
3. Zdefiniuj parametry sieci w chmurze: adres i maskę sieci. Gdy skończysz, kliknij **Gotowe**.

W rezultacie do lokalizacji w chmurze zostanie dodana sieć o zdefiniowanym adresie i masce.

Aby usunąć sieć w chmurze

Uwaga

Jeśli w sieci w chmurze znajduje się choć jeden serwer chmurowy, nie można jej usunąć. Najpierw trzeba usunąć serwer chmurowy, a dopiero potem sieć.

1. Wybierz **Odzyskiwanie po awarii > Łączność**.
2. Na karcie **Lokalizacja w chmurze** kliknij adres sieci, którą chcesz usunąć.
3. Kliknij **Usuń** i potwierdź operację.

Aby zmienić parametry sieci w chmurze

1. Wybierz **Odzyskiwanie po awarii > Łączność**.
2. Na karcie **Lokalizacja w chmurze** kliknij adres sieci, którą chcesz edytować.
3. Kliknij **Edytuj**.
4. Zdefiniuj adres oraz maskę sieci i kliknij **Gotowe**.

Zmienianie konfiguracji adresu IP

Aby uzyskać właściwą wydajność odzyskiwania po awarii, trzeba zadbać o spójność adresów IP przypisanych do serwerów lokalnych i chmurowych. W razie jakichkolwiek niespójności lub niedopasowania adresów IP obok odpowiadającej adresowi sieci na stronie **Odzyskiwanie po awarii > Łączność** będzie wyświetlany wykrzyknik.

Poniżej przedstawiono kilka powszechnie znanych przyczyn niespójności adresów IP:

1. Przeniesiono serwer odzyskiwania z jednej sieci do drugiej lub zmieniono maskę sieci w chmurze. W rezultacie serwery chmurowe mają adresy IP z sieci, do których nie są podłączone.
2. Zmieniono typ łączności z „Bez połączenia site-to-site” na „Połączenie site-to-site”. W rezultacie serwer lokalny znajduje się w innej sieci niż ta, która została utworzona dla serwera odzyskiwania w lokalizacji w chmurze.
3. Zmieniono typ łączności z Open VPN site-to-site na IPsec VPN multi-site lub z IPsec VPN multi-site na Open VPN site-to-site. Dodatkowe informacje na temat tego scenariusza można znaleźć w sekcjach [Zmienianie połączeń](#) i [Zmienianie przypisania adresów IP](#).
4. Edytowano następujące parametry sieciowe na stronie urządzenia VPN:
 - Dodano interfejs przez ustawienia sieciowe
 - Ręcznie edytowano maskę sieci przez ustawienia interfejsu
 - Edytowano maskę sieci przez DHCP
 - Ręcznie edytowano adres i maskę sieci przez ustawienia interfejsu
 - Edytowano maskę i adres sieci przez DHCP

W wyniku wymienionych wyżej działań sieć w lokalizacji w chmurze może stać się obszarem podrzędnym lub nadrzędnym sieci lokalnej albo interfejs urządzenia VPN może zgłosić te same ustawienia sieciowe w przypadku różnych interfejsów.

Aby rozwiązać problem z ustawieniami sieciowymi

1. Kliknij sieć wymagającą zmiany konfiguracji adresu IP.
Zostanie wyświetlona lista serwerów znajdujących się w wybranej sieci, ich statusów i adresów IP. Serwery o niespójnych ustawieniach sieciowych są oznaczone wykrzyknikiem.
2. Aby zmienić ustawienia sieciowe serwera, kliknij **Przejdź do serwera**. Aby zmienić ustawienia sieciowe wszystkich serwerów naraz, kliknij **Zmień** w obszarze powiadomień.
3. Zmień adresy IP stosownie do potrzeb, definiując je w polach **Nowy adres IP** i **Nowy testowy adres IP**.
4. Gdy skończysz, kliknij **Potwierdź**.

Przenoszenie serwerów do odpowiedniej sieci

Po utworzeniu planu ochrony na potrzeby odzyskiwania po awarii i zastosowaniu go do wybranych urządzeń system sprawdza adresy IP urządzeń i automatycznie tworzy sieci w chmurze, jeśli nie ma jeszcze sieci w chmurze, do których pasuje adres IP. Domyślnie sieci w chmurze są konfigurowane z maksymalnymi zakresami zalecanymi przez IANA do użytku prywatnego (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Sieć można zawęzić, edytując jej maskę.

Jeśli wybrane urządzenia znajdują się w wielu sieciach lokalnych, sieć w chmurze może stać się obszarem nadrzędnym w stosunku do tych sieci lokalnych. W takim przypadku można zmienić konfigurację sieci w chmurze:

1. Kliknij sieć w chmurze wymagającą zmiany konfiguracji rozmiaru sieci i kliknij **Edytuj**.
2. Skonfiguruj ponownie rozmiar sieci przy użyciu poprawnych ustawień.
3. Utwórz inne wymagane sieci.
4. Kliknij ikonę powiadomienia obok liczby urządzeń podłączonych do sieci.
5. Kliknij **Przenieś do odpowiedniej sieci**.
6. Zaznacz serwery, które chcesz przenieść do odpowiednich sieci, a następnie kliknij **Przenieś**.

Zarządzanie ustawieniami urządzenia VPN

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

W konsoli Cyber Protect (**Odzyskiwanie po awarii** > **Łączność**) można:

- Pobrać pliki dzienników.
- Wyrejestrować urządzenie (jeśli trzeba zresetować ustawienia urządzenia VPN lub zmienić tryb na Tylko chmura).

Aby uzyskać dostęp do tych ustawień, kliknij ikonę **i** w sekcji **Urządzenie VPN**.

W konsoli urządzenia VPN można:

- Zmienić hasło urządzenia.
- Wyświetlić/zmienić ustawienia sieciowe i określić, który interfejs ma być używany jako interfejs sieci WAN na potrzeby połączenia z Internetem.
- Zarejestrować lub zmienić zarejestrowane konto (drogą ponownej rejestracji).
- Uruchomić ponownie usługę VPN.
- Zrestartować urządzenie VPN.
- Uruchomić polecenie powłoki systemu Linux (tylko w przypadku zaawansowanego rozwiązywania problemu).

Ponowne instalowanie bramy VPN

W razie napotkania problemu z bramą VPN, którego nie uda się rozwiązać, może być konieczna ponowna instalacja bramy VPN. Możliwe są między innymi następujące problemy:

- Brama VPN ma status **Błąd**.
- Brama VPN przez długi czas ma status **Oczekujące**.
- Od dłuższego czasu nie ustalono statusu bramy VPN.

Proces ponownej instalacji bramy VPN obejmuje następujące zautomatyzowane czynności: całkowite usunięcie obecnej maszyny wirtualnej z bramą VPN, zainstalowanie nowej maszyny wirtualnej z szablonu oraz zastosowanie ustawień poprzedniej bramy VPN na nowej maszynie wirtualnej.

Wymagania wstępne:

Trzeba ustawić typ łączności z lokalizacją w chmurze.

Aby ponownie zainstalować bramę VPN

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii > Łączność**.
2. Kliknij ikonę koła zębatego obok bramy VPN i wybierz **Zainstaluj ponownie bramę VPN**.
3. W oknie dialogowym **Zainstaluj ponownie bramę VPN** wprowadź swoją nazwę logowania.
4. Kliknij **Zainstaluj ponownie**.

Włączanie i wyłączanie połączenia site-to-site

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Połączenie site-to-site warto włączyć w następujących przypadkach:

- Jeśli serwery chmurowe z lokalizacji w chmurze muszą się komunikować z serwerami w lokalizacji lokalnej.

- Po przełączeniu awaryjnym na chmurę przywrócono normalne działanie lokalnej infrastruktury i chcesz przywrócić serwery do lokalizacji lokalnej przy użyciu operacji powrotu po awarii.

Aby włączyć połączenie site-to-site

1. Wybierz **Odzyskiwanie po awarii > Łączność**.
2. Kliknij **Pokaż właściwości** i włącz opcję **Połączenie site-to-site**.

W wyniku tego zostanie aktywowane połączenie VPN site-to-site między lokalizacją lokalną i lokalizacją w chmurze. Usługa Cyber Disaster Recovery Cloud uzyskuje ustawienia sieciowe z urządzenia VPN i rozszerza sieci lokalne o lokalizację w chmurze.

Jeśli serwery chmurowe z lokalizacji w chmurze nie muszą się komunikować z serwerami w lokalizacji lokalnej, można wyłączyć połączenie site-to-site.

Aby wyłączyć połączenie site-to-site

1. Wybierz **Odzyskiwanie po awarii > Łączność**.
2. Kliknij **Pokaż właściwości** i wyłącz opcję **Połączenie site-to-site**.

W rezultacie lokalizacja lokalna zostanie odłączona od lokalizacji w chmurze.

Zmienianie typu łączności na site-to-site

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Typ łączności można łatwo zmienić z Open VPN site-to-site na IPsec VPN multi-site oraz z IPsec VPN multi-site na Open VPN site-to-site.

Po zmianie typu łączności aktywne połączenia VPN są usuwane, ale konfiguracje serwerów chmurowych i sieci zostają zachowane. Nadal jednak trzeba będzie zmienić przypisanie adresów IP sieci i serwerów w chmurze.

W poniższej tabeli zamieszczono porównanie podstawowych cech połączenia Open VPN site-to-site i połączenia IPsec VPN multi-site.

	Połączenie Open VPN site-to-site	Połączenia IPsec VPN multi-site
Obsługa lokalizacji lokalnych	Jedna	Jedna, wiele
Tryb bramy VPN	L2 Open VPN	L3 IPsec VPN
Segmenty sieci	Rozszerzenie sieci lokalnej na sieć w chmurze	Segmenty sieci lokalnej i sieci w chmurze nie powinny się na siebie nakładać.
Obsługa dostępu point-to-site	Tak	Nie

	Połączenie Open VPN site-to-site	Połączenia IPsec VPN multi-site
do lokalizacji lokalnej		
Obsługa dostępu point-to-site do lokalizacji w chmurze	Tak	Tak
Wymóg pozycji oferty publicznego adresu IP	Nie	Tak

Aby zmienić połączenie Open VPN site-to-site na połączenie IPsec VPN multi-site

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii > Łączność**.
2. Kliknij **Pokaż właściwości**.
3. Kliknij **Zmień na połączenie IPsec VPN multi-site**.
4. Kliknij **Zmień konfigurację**.
5. [Zmień przypisanie adresów IP](#) sieci w chmurze i serwerów chmurowych.
6. [Skonfiguruj ustawienia połączenia IPsec multi-site](#).

Aby zmienić połączenie IPsec VPN multi-site na połączenie Open VPN site-to-site

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii > Łączność**.
2. Kliknij **Pokaż właściwości**.
3. Kliknij **Zmień na połączenie Open VPN site-to-site**.
4. Kliknij **Zmień konfigurację**.
5. [Zmień przypisanie adresów IP](#) sieci w chmurze i serwerów chmurowych.
6. [Skonfiguruj ustawienia połączenia site-to-site](#).

Zmienianie przypisania adresów IP

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

W następujących przypadkach w celu ukończenia konfiguracji trzeba zmienić przypisanie adresów IP do sieci i serwerów chmurowych:

- Zmieniono typ łączności z Open VPN site-to-site na IPsec VPN multi-site lub na odwrót.
- Zastosowano plan ochrony (jeśli jest skonfigurowana łączność IPsec VPN multi-site).

Aby zmienić przypisanie adresu IP sieci w chmurze

1. Na karcie **Łączność** kliknij adres IP sieci w chmurze.
2. W wyskakującym okienku **Sieć** kliknij **Edytuj**.
3. Wprowadź nowy adres i maskę sieci.
4. Kliknij **Gotowe**.

Po zmianie przypisania adresu IP sieci w chmurze należy zmienić przypisanie serwerów chmurowych znajdujących się w tej sieci.

Aby zmienić przypisanie adresu IP serwera

1. Na karcie **Łączność** kliknij adres IP serwera w danej sieci w chmurze.
2. W wyskakującym okienku **Serwery** kliknij **Zmień adres IP**.
3. W wyskakującym okienku **Zmień adres IP** wpisz nowy adres IP serwera lub użyj automatycznie wygenerowanego adresu IP należącego do sieci w chmurze, której przypisanie zmieniono.

Uwaga

Usługa Cyber Disaster Recovery Cloud automatycznie przypisuje adresy IP z sieci w chmurze do wszystkich serwerów chmurowych należących do tej sieci przed zmianą przypisania jej adresu IP. Sugerowane adresy IP można wykorzystać do zmiany przypisania adresów IP wszystkich serwerów chmurowych naraz.

4. Kliknij **Potwierdź**.

Konfigurowanie niestandardowych serwerów DNS

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Podczas konfigurowania łączności usługa Cyber Disaster Recovery Cloud tworzy infrastrukturę sieci w chmurze. Serwer DHCP w chmurze automatycznie przypisuje domyślne serwery DNS do serwerów odzyskiwania i serwerów podstawowych, ale można zmienić ustawienia domyślne i skonfigurować niestandardowe serwery DNS. Nowe ustawienia serwerów DNS zostaną zastosowane od następnego żądania skierowanego do serwera DHCP.

Wymagania wstępne:

Trzeba ustawić typ łączności z lokalizacją w chmurze.

Aby skonfigurować niestandardowy serwer DNS

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii > Łączność**.
2. Kliknij **Pokaż właściwości**.
3. Kliknij **Domyślne (dostępne w lokalizacji w chmurze)**.
4. Wybierz **Serwery niestandardowe**.

5. Wpisz adres IP serwera DNS.
6. [Opcjonalnie] Jeśli chcesz dodać kolejny serwer DNS, kliknij **Dodaj** i wpisz adres IP tego serwera DNS.

Uwaga

Po dodaniu niestandardowych serwerów DNS możesz też dodać domyślne serwery DNS. Dzięki temu w przypadku niedostępności niestandardowych serwerów DNS usługa Cyber Disaster Recovery Cloud skorzysta z domyślnego serwera DNS.

7. Kliknij **Gotowe**.

Usuwanie niestandardowych serwerów DNS

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Można usuwać serwery DNS z listy niestandardowych serwerów DNS.

Wymagania wstępne:

Skonfigurowano niestandardowe serwery DNS.

Aby usunąć niestandardowy serwer DNS

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii > Łączność**.
2. Kliknij **Pokaż właściwości**.
3. Kliknij **Serwery niestandardowe**.
4. Kliknij ikonę usuwania obok nazwy serwera DNS.

Uwaga

Jeśli jest dostępny tylko jeden niestandardowy serwer DNS, operacja usuwania jest wyłączona. Jeśli chcesz usunąć wszystkie niestandardowe serwery DNS, wybierz **Domyślne (dostępne w lokalizacji w chmurze)**.

5. Kliknij **Gotowe**.

Pobieranie adresów MAC

Można pobrać listę adresów MAC, a następnie je wyodrębnić i zaimportować do konfiguracji niestandardowego serwera DHCP.

Wymagania wstępne:

- Trzeba ustawić typ łączności z lokalizacją w chmurze.
- Musi być skonfigurowany co najmniej jeden serwer podstawowy lub serwer odzyskiwania z adresem MAC.

Aby pobrać listę adresów MAC

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii > Łączność**.
2. Kliknij **Pokaż właściwości**.
3. Kliknij **Pobierz listę adresów MAC**, a następnie zapisz ten plik CSV.

Konfigurowanie routingu lokalnego

Oprócz sieci lokalnych, które są rozszerzane o chmurę za pomocą urządzenia VPN, można mieć inne sieci lokalne, które nie są zarejestrowane w urządzeniu VPN, ale znajdujące się w nich serwery muszą się komunikować z serwerami chmurowymi. Aby zapewnić łączność między takimi serwerami lokalnymi a serwerami chmurowymi, należy skonfigurować ustawienia routingu lokalnego.

Aby skonfigurować routing lokalny

1. Przejdź do karty **Odzyskiwanie po awarii > Łączność**.
2. Kliknij **Pokaż właściwości**, a następnie **Routing lokalny**.
3. Wskaż sieci lokalne w notacji CIDR.
4. Kliknij **Zapisz**.

W wyniku tych działań serwery z określonych sieci lokalnych mogą się komunikować z serwerami chmurowymi.

Zezwalanie na ruch DHCP przez połączenie L2 VPN

Jeśli urządzenia w lokalizacji lokalnej uzyskują adresy IP z serwera DHCP, można chronić ten serwer DHCP za pomocą funkcji Odzyskiwanie po awarii, przełączyć go awaryjnie do chmury, a następnie zezwolić na ruch DHCP przez połączenie L2 VPN. W wyniku tych czynności serwer DHCP będzie działał w chmurze, ale nadal będzie przydzielać adresy IP urządzeniom lokalnym.

Wymagania wstępne:

Trzeba ustawić łączność L2 VPN site-to-site z lokalizacją w chmurze.

Aby zezwolić na ruch DHCP przez połączenie L2 VPN

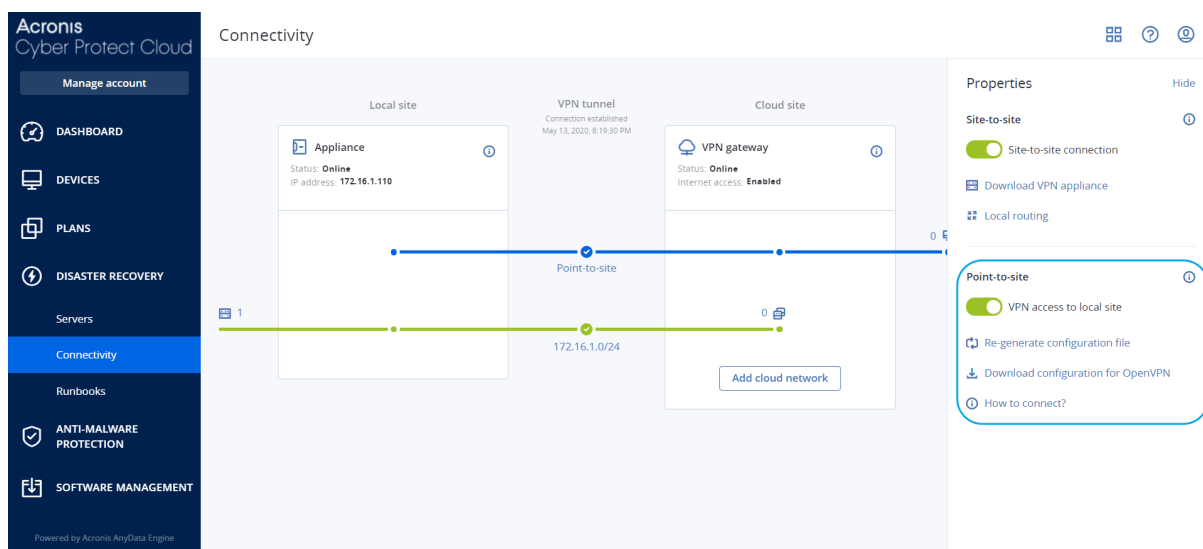
1. Przejdź do karty **Odzyskiwanie po awarii > Łączność**.
2. Kliknij **Pokaż właściwości**.
3. Włącz przełącznik **Zezwól na ruch DHCP przez połączenie L2 VPN**.

Zarządzanie ustawieniami połączenia point-to-site

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii > Łączność** i kliknij **Pokaż właściwości** w prawym górnym rogu okna.



Dostęp VPN do lokalizacji lokalnej

Ta opcja służy do zarządzania dostępem VPN do lokalizacji lokalnej. Domyślnie jest ona włączona. W przypadku jej wyłączenia dostęp point-to-site do lokalizacji lokalnej nie będzie dozwolony.

Pobierz konfigurację dla pakietu OpenVPN

Spowoduje to pobranie pliku konfiguracji klienta OpenVPN. Plik ten jest wymagany do nawiązania połączenia point-to-site z lokalizacją w chmurze.

Ponowne generowanie konfiguracji

Możesz ponownie wygenerować plik konfiguracyjny klienta OpenVPN.

Jest to wymagane w następujących przypadkach:

- Jeśli podejrzewasz, że do pliku konfiguracyjnego mogły mieć dostęp osoby niepowołane.
- Jeśli na Twoim koncie włączono uwierzytelnianie dwuskładnikowe.

Po zaktualizowaniu pliku konfiguracyjnego nie można nawiązać połączenia przy użyciu starego pliku. Udostępnij nowy plik konfiguracyjny wszystkim użytkownikom uprawnionym do korzystania z połączenia point-to-site.

Aktywne połączenia point-to-site

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Wszystkie aktywne połączenia point-to-site można zobaczyć w sekcji **Odzyskiwanie po awarii > Łączność**. Kliknij ikonę komputera na niebieskiej linii **Point-to-site** — zostaną wyświetlone szczegółowe informacje o aktywnych połączeniach point-to-site pogrupowanych według nazwy użytkownika.

Connectivity

Active point-to-site connections

User name	Connections	Login at	Inbound traffic	Outbound traffic
> [redacted]@acronis.com	4	Jan, 10, 08:39 PM	11.2 GB	11.2 GB
▼ superadmin@acronis.com	2	—	4.6 GB	4.6 GB
10.96.77.16 - 8800		Jan, 09, 10:39 PM	1.6 GB	1.6 GB
10.96.77.16 - 8800		Jan, 09, 10:39 PM	4.6 GB	4.6 GB
> user@mail.com	1	Jan, 10, 08:39 PM	1.2 GB	1.2 GB
> 34get_2@hotmail.com	5	Jan, 10, 08:39 PM	3.1 GB	3.1 GB
> admin@acronis.com	1	Jan, 10, 08:39 PM	2 GB	2 GB
> man-23@yandex.com	5	Jan, 10, 08:39 PM	21.4 GB	21.4 GB

Show properties

Add cloud network

Praca z dziennikami

Funkcja Odzyskiwanie po awarii zbiera dzienniki w przypadku urządzenia VPN i bramy VPN. Dzienniki są zapisywane w postaci plików .txt i kompresowane w archiwum .zip. Możesz pobrać i wyodrębnić archiwum, a następnie skorzystać z tych informacji w celu rozwiązania problemów lub monitorowania.

Poniższa lista udostępnia opisy plików dzienników zawartych w archiwum .zip oraz zawartych w nich informacji.

dnsmasq.config.txt — ten plik zawiera informacje o konfiguracji usługi udostępniającej adresy DNS i DHCP.

dnsmasq.leases.txt — ten plik zawiera informacje o bieżących dzierżawach adresów DHCP.

dnsmasq_log.txt — ten plik zawiera dzienniki usługi dnsmasq.

ehtables.txt — ten plik zawiera informacje o tabelach zapory.

free.txt — ten plik zawiera informacje o wolnym miejscu w pamięci.

ip.txt — ten plik zawiera dzienniki z konfiguracji interfejsów sieciowych, w tym ich nazwy, które można wykorzystać w konfiguracji ustawień funkcji **Przechwytywanie pakietów sieciowych**.

NetworkManager_log.txt — ten plik zawiera dzienniki z usługi NetworkManager.

NetworkManager_status.txt — ten plik zawiera informacje o statusie usługi NetworkManager.

openvpn@p2s_log.txt — ten plik zawiera dzienniki z usługi OpenVPN.

openvpn@p2s_status.txt — ten plik zawiera informacje o statusie tuneli VPN.

ps.txt — ten plik zawiera informacje o aktualnie uruchomionych procesach na bramie VPN lub urządzeniu VPN.

resolv.conf.txt — ten plik zawiera informacje o konfiguracji serwerów DNS.

routes.txt — ten plik zawiera informacje o trasach sieciowych.

uname.txt — ten plik zawiera informacje o bieżącej wersji jądra systemu operacyjnego.

uptime.txt — ten plik zawiera informacje o czasie, przez jaki system operacyjny nie był ponownie uruchamiany.

vpnsrv_log.txt — ten plik zawiera dzienniki z usługi VPN.

vpnsrv_status.txt — ten plik zawiera informacje o statusie serwera VPN.

Dodatkowe informacje na temat plików dzienników dotyczących łączności IPsec VPN można znaleźć w sekcji "Pliki dziennika IPsec VPN multi-site" (s. 55).

Pobieranie dzienników urządzenia VPN

Możesz pobrać i wyodrębnić archiwum zawierające dzienniki urządzenia VPN, a następnie skorzystać z tych informacji w celu rozwiązania problemów lub monitorowania.

Aby pobrać dzienniki urządzenia VPN

1. Na stronie **Łączność** kliknij ikonę koła zębatego obok urządzenia VPN.
2. Kliknij **Pobierz dziennik**.
3. [Opcjonalnie] Wybierz **Przechwytyj pakiety sieciowe** i skonfiguruj ustawienia. Aby uzyskać więcej informacji, zobacz "Przechwytywanie pakietów sieciowych" (s. 52).
4. Kliknij **Gotowe**.
5. Kiedy archiwum .zip będzie gotowe do pobrania, kliknij **Pobierz dziennik** i zapisz go lokalnie.

Pobieranie dzienników bramy VPN

Możesz pobrać i wyodrębnić archiwum zawierające dzienniki bramy VPN, a następnie skorzystać z tych informacji w celu rozwiązania problemów lub monitorowania.

Aby pobrać dzienniki bramy VPN

1. Na stronie **Łączność** kliknij ikonę koła zębatego obok bramy VPN.
2. Kliknij **Pobierz dziennik**.
3. [Opcjonalnie] Wybierz **Przechwytyj pakiety sieciowe**, a następnie skonfiguruj ustawienia. Aby uzyskać więcej informacji, zobacz "Przechwytywanie pakietów sieciowych" (s. 52).
4. Kliknij **Gotowe**.
5. Kiedy archiwum .zip będzie gotowe do pobrania, kliknij **Pobierz dziennik** i zapisz go lokalnie.

Przechwytywanie pakietów sieciowych

Z myślą o rozwiązywaniu problemów i analizowaniu komunikacji między lokalną lokalizacją produkcyjną a serwerem podstawowym lub serwerem odzyskiwania można wybrać opcję zbierania pakietów sieciowych na bramie VPN lub urządzeniu VPN.

Po zebraniu 32 000 pakietów sieciowych lub wyczerpaniu się limitu czasu przechwytywanie pakietów sieciowych zostanie zatrzymane, a wyniki zostaną zapisane w pliku .libpcap, który zostanie dodany do archiwum .zip dzienników.

Poniższa tabela zawiera dodatkowe informacje na temat ustawień funkcji **Przechwytyj pakiety sieciowe**, które można skonfigurować.

Ustawienie	Opis
Nazwa interfejsu sieciowego	Interfejs sieciowy, na którym mają być przechwytywane pakiety sieciowe. Jeśli pakiety sieciowe mają być przechwytywane na wszystkich interfejsach sieciowych, wybierz opcję Dowolny .
Limit czasu (w sekundach)	Limit czasu przechwytywania pakietów sieciowych. Wartość maksymalna to 1800.
Filtrowanie	<p>Dodatkowy filtr do zastosowania do przechwytywanych pakietów sieciowych.</p> <p>Można wprowadzić ciąg obejmujący protokoły, porty i kierunki oraz ich kombinacje oddzielone spacją, takie jak: „and”, „or”, „not”, „ („ , „) ”, „src”, „dst”, „net”, „host”, „port”, „ip”, „tcp”, „udp”, „icmp”, „arp”, „esp”.</p> <p>Jeśli chcesz użyć nawiasu, dodaj przed nim i po nim spacje. Możesz też wprowadzić adresy IP i adresy sieciowe, na przykład: „icmp or arp” i „port 67 or 68”.</p> <p>Dodatkowe informacje na temat wartości, które można wprowadzić, można znaleźć w pomocy do narzędzia tpcdump w systemie Linux.</p>

Rozwiązywanie problemów z konfiguracją IPsec VPN

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Podczas konfigurowania połączenia IPsec VPN lub korzystania z niego mogą wystąpić pewne problemy.

Więcej informacji na temat napotkanych problemów można znaleźć w plikach dziennika IPsec, a w celu uzyskania możliwych rozwiązań niektórych często występujących problemów zapoznaj się z tematem „Rozwiązywanie napotkanych problemów z konfiguracją IPsec VPN”.

Rozwiązywanie napotkanych problemów z konfiguracją IPsec VPN

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

W poniższej tabeli opisano najczęściej występujące problemy z konfiguracją IPsec VPN oraz wyjaśniono, jak je rozwiązać.

Problem	Możliwe rozwiązanie
Pojawił się następujący komunikat o błędzie: Błąd negocjacji w fazie 1 IKE. Sprawdź ustawienia IPsec IKE w magazynie Cloud i lokalizacji lokalnej.	<p>Kliknij Spróbuj ponownie i sprawdź, czy pojawi się bardziej szczegółowy komunikat o błędzie. Bardziej szczegółowym komunikatem o błędzie może być na przykład komunikat o niezgodności algorytmów lub niepoprawnym kluczu PSK.</p> <hr/> <p>Uwaga Ze względów bezpieczeństwa w przypadku łączności IPsec VPN występują następujące ograniczenia:</p> <ul style="list-style-type: none">• W dokumencie RFC8247 zaleca się wycofywanie protokołu IKEv1 i nie jest on obsługiwany ze względu na zagrożenia bezpieczeństwa. Obsługiwane są tylko połączenia przy użyciu protokołu IKEv2.• Następujące algorytmy szyfrowania nie są uznawane za bezpieczne i nie są obsługiwane: DES i 3DES.• Następujące algorytmy skrótów nie są uznawane za bezpieczne i nie są obsługiwane: SHA1 i MD5.• Liczba 2 z grupy Diffiego-Hellmana 2 nie jest uznawana za bezpieczną i nie jest obsługiwana.
Połączenie między moją lokalizacją lokalną a lokalizacją w chmurze stale ma status Łączenie .	<p>Sprawdź, czy:</p> <ul style="list-style-type: none">• Port UDP 500 jest otwarty (jeśli korzystasz z zapory).• Jest łączność między lokalizacją lokalną a lokalizacją w chmurze.

Problem	Możliwe rozwiązanie
	<ul style="list-style-type: none"> Adres IP lokalizacji lokalnej jest poprawny.
Połączenie między moją lokalizacją lokalną a lokalizacją w chmurze stale ma status Oczekiwanie na połączenie .	<p>Status ten pojawia się, gdy opcja Czynność podczas uruchamiania w przypadku lokalizacji w chmurze ma ustawienie Dodaj, co oznacza, że lokalizacja w chmurze czeka, aż lokalizacja lokalna zainicjuje połączenie.</p> <p>Zainicjuj połączenie z lokalizacji lokalnej.</p>
Połączenie między moją lokalizacją lokalną a lokalizacją w chmurze stale ma status Oczekiwanie na ruch .	<p>Status ten pojawia się, gdy opcja Czynność podczas uruchamiania w przypadku lokalizacji w chmurze ma ustawienie Przekieruj.</p> <p>Jeśli oczekujesz na połączenie z lokalizacji lokalnej, zrób tak:</p> <ul style="list-style-type: none"> Z lokalizacji lokalnej spróbuj wysłać polecenie ping do maszyny wirtualnej w lokalizacji w chmurze. Jest to standardowe zachowanie niezbędne do ustanowienia tunelu w przypadku niektórych urządzeń, na przykład Cisco ASA. (Tryb przekierowania) Zadbaj, aby lokalizacja lokalna utworzyła tunel, ustawiając jej Czynność podczas uruchamiania na Rozpocznij.
Połączenie między moją lokalizacją lokalną a lokalizacją w chmurze zostało nawiązane, ale co najmniej jedna z zasad sieciowych nie działa.	<p>Ten problem może mieć jedną z następujących przyczyn:</p> <ul style="list-style-type: none"> Mapowanie sieci w lokalizacji IPsec w chmurze jest inne niż mapowanie sieci w lokalizacji lokalnej. Zadbaj, aby mapowania sieci i kolejność zasad sieciowych w lokalizacji lokalnej i lokalizacji w chmurze były dokładnie takie same. Ten stan jest poprawny, gdy opcja Czynność podczas uruchamiania w przypadku lokalizacji lokalnej i/lub lokalizacji w chmurze ma ustawienie Przekieruj (na przykład na urządzeniach Cisco ASA), a w danej chwili nie ma ruchu. Spróbuj wysłać polecenie ping, aby sprawdzić, czy tunel został ustanowiony. Jeśli polecenie ping nie działa, sprawdź mapowanie sieci na lokalizacji lokalnej i lokalizacji w chmurze.
Chcę ponownie uruchomić wybrane	Aby ponownie uruchomić wybrane połączenie

Problem	Możliwe rozwiązanie
połączenie IPsec.	<p>IPsec:</p> <ol style="list-style-type: none"> 1. Na ekranie Odzyskiwanie po awarii > Łączność kliknij odpowiednie połączenie IPsec. 2. Kliknij Wyłącz połączenie. 3. Ponownie kliknij połączenie IPsec. 4. Kliknij Włącz połączenie.

Pobieranie plików dziennika IPsec VPN

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

W plikach dziennika na serwerze VPN można znaleźć dodatkowe informacje na temat łączności IPsec. Pliki dziennika są skompresowane w archiwum .zip, które można pobrać i wyodrębnić.

Wymagania wstępne

Skonfigurowano łączność IPsec VPN multi-site.

Aby pobrać archiwum .zip z plikami dziennika

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii** > **Łączność**.
2. Kliknij ikonę koła zębatego obok bramy VPN lokalizacji w chmurze.
3. Kliknij **Pobierz dziennik**.
4. Kliknij **Gotowe**.
5. Kiedy archiwum .zip będzie gotowe do pobrania, kliknij **Pobierz dziennik** i zapisz go lokalnie.

Pliki dziennika IPsec VPN multi-site

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Poniższa lista udostępnia opisy plików dzienników IPsec VPN zawartych w archiwum .zip oraz zawartych w nich informacji.

- ip.txt — ten plik zawiera dziennik konfiguracji kart sieciowych. Powinny być widoczne dwa adresy IP: publiczny adres IP i lokalny adres IP. Jeśli nie ma tych adresów IP w dzienniku, to znaczy, że wystąpił jakiś problem. Skontaktuj się z zespołem pomocy technicznej.

Uwaga

Maską publicznego adresu IP musi być 32.

- swanctl-list-loaded-config.txt — ten plik zawiera informacje o wszystkich lokalizacjach IPsec.

Jeśli w pliku nie ma lokalizacji, to konfiguracja IPsec nie została zastosowana. Spróbuj zaktualizować konfigurację i ją zapisać, lub skontaktuj się z zespołem pomocy technicznej.

- `swanctl-list-active-sas.txt` — ten plik zawiera połączenia i zasady ze statusem aktywności lub łączenia.

Konfigurowanie serwerów odzyskiwania

W tej sekcji omówiono pojęcia przełączania awaryjnego i powrotu po awarii, tworzenie serwera odzyskiwania oraz operacje odzyskiwania po awarii.

Tworzenie serwera odzyskiwania

Aby utworzyć serwer odzyskiwania, który będzie kopią obciążenia, możesz skorzystać z poniższej procedury. Możesz też obejrzeć [instruktaż wideo](#), w którym pokazano cały ten proces.

Ważne

Podczas wykonywania przełączenia awaryjnego można wybrać tylko te punkty odzyskiwania, które zostały utworzone po utworzeniu serwera odzyskiwania.

Wymagania wstępne

- Do oryginalnego komputera, który chcesz chronić, musi być stosowany plan ochrony. W ramach planu w chmurze musi zostać utworzona kopia zapasowa całego komputera lub tylko dysków niezbędnych do uruchomienia komputera i udostępnienia potrzebnych usług.
- Trzeba ustawić typ łączności z lokalizacją w chmurze.

Aby stworzyć serwer odzyskiwania

1. Na karcie **Wszystkie urządzenia** wybierz komputer, który ma być chroniony.
2. Kliknij **Odzyskiwanie po awarii**, a następnie kliknij **Utwórz serwer odzyskiwania**.
3. Wybierz liczbę rdzeni wirtualnych i rozmiar pamięci RAM.

Uwaga

Podano liczbę punktów obliczeniowych wykorzystywanych w przypadku każdej opcji. Liczba punktów obliczeniowych odzwierciedla koszt działania serwera odzyskiwania przez godzinę. Aby uzyskać więcej informacji, zobacz "Punkty obliczeniowe" (s. 12).

4. Wskaż sieć w chmurze, do której ma zostać podłączony serwer.
5. Wybierz **DHCP**.

Opcja DHCP	Opis
Dostępne w lokalizacji w chmurze	Ustawienie domyślne. Adres IP serwera zostanie udostępniony przez automatycznie skonfigurowany serwer DHCP w chmurze.
Niestandardowe	Adres IP serwera zostanie udostępniony przez Twój własny serwer DHCP w chmurze.

6. [Opcjonalnie] Podaj **adres MAC**.

Adres MAC jest unikatowym identyfikatorem przypisanym do karty sieciowej serwera. W przypadku korzystania z niestandardowego serwera DHCP można go skonfigurować tak, aby zawsze przypisywał określone adresy IP do określonych adresów MAC. Dzięki temu serwer odzyskiwania zawsze otrzymuje ten sam adres IP. Można uruchamiać aplikacje, które mają licencje zarejestrowane na adres MAC.

7. Określ adres IP, który będzie znajdował się w sieci produkcyjnej serwera. Domyślnie używany jest adres IP pierwotnego komputera.

Uwaga

Jeśli korzystasz z serwera DHCP, dodaj ten adres IP do listy elementów wykluczonych serwera, aby uniknąć konfliktu adresów IP.

W przypadku korzystania z niestandardowego serwera DHCP trzeba w polu **Adres IP w sieci produkcyjnej** podać ten sam adres, który został skonfigurowany na serwerze DHCP. W przeciwnym razie testowe przełączanie awaryjne nie będzie działać prawidłowo i nie będzie można się komunikować z serwerem przy użyciu publicznego adresu IP.

8. [Opcjonalnie] Zaznacz pole wyboru **Testowy adres IP**, a następnie wprowadź adres IP. Umożliwi to przetestowanie przełączania awaryjnego w odizolowanej sieci testowej i połączenie serwera odzyskiwania przy użyciu protokołu RDP lub SSH podczas testu przełączania awaryjnego. W trybie testowego przełączania awaryjnego brama VPN zastępuje testowy adres IP produkcyjnym adresem IP za pomocą protokołu NAT. Jeśli pole wyboru pozostanie niezaznaczone, dostęp do serwera będzie możliwy wyłącznie z poziomu konsoli.

Uwaga

Jeśli korzystasz z serwera DHCP, dodaj ten adres IP do listy elementów wykluczonych serwera, aby uniknąć konfliktu adresów IP.

Możesz wybrać jeden z sugerowanych adresów IP lub wprowadzić inny.

9. [Opcjonalnie] Zaznacz pole wyboru **Dostęp do Internetu**. Opcja ta pozwala serwerowi odzyskiwania na dostęp do Internetu podczas prawdziwego lub testowego przełączania awaryjnego. Domyślnie port TCP 25 jest otwarty dla połączeń wychodzących do publicznych adresów IP.
10. [Opcjonalnie] Ustaw **Próg RPO**. Próg RPO określa maksymalny dozwolony odstęp czasu między ostatnim punktem odzyskiwania nadającym się do wykorzystania do przełączania awaryjnego a czasem bieżącym. Można ustawić wartość z przedziałów: 15– 60 minut, 1–24 godz., 1–14 dni.
11. [Opcjonalnie] Zaznacz pole wyboru **Użyj publicznego adresu IP**. Publiczny adres IP serwera czyni go dostępnym w Internecie podczas prawdziwego lub testowego przełączania awaryjnego. Jeśli pole wyboru pozostanie niezaznaczone, serwer będzie dostępny wyłącznie w Twojej sieci produkcyjnej. Opcja **Użyj publicznego adresu IP** wymaga włączenia opcji **Dostęp do Internetu**.

Publiczny adres IP zostanie wyświetlony po zakończeniu konfiguracji. Domyślnie port TCP 443 jest otwarty dla połączeń przychodzących do publicznych adresów IP.

Uwaga

Jeśli wyczyścisz pole wyboru **Użyj publicznego adresu IP** lub usuniesz serwer odzyskiwania, jego publiczny adres IP nie zostanie zastrzeżony.

12. [Opcjonalnie] [Jeśli kopie zapasowe wybranego komputera są szyfrowane za pomocą szyfrowania jako właściwości komputera], określ hasło, które zostanie automatycznie użyte podczas tworzenia maszyny wirtualnej na potrzeby serwera odzyskiwania z zaszyfrowanej kopii zapasowej.
 - a. Kliknij **Określ**, a następnie wprowadź hasło do zaszyfrowanej kopii zapasowej i zdefiniuj nazwę poświadczeń.

Domyślnie na liście będzie wyświetlana najnowsza kopia zapasowa.
 - b. [Opcjonalnie] Aby wyświetlić wszystkie kopie zapasowe, zaznacz **Pokaż wszystkie kopie zapasowe**.
 - c. Kliknij **Gotowe**.

Uwaga

Wprowadzone określone hasło będzie przechowywane w bezpiecznym magazynie poświadczeń, jednak zapisywanie haseł może być sprzeczne z wymogami dotyczącymi zachowania zgodności z przepisami.

13. [Opcjonalnie] Zmień nazwę serwera odzyskiwania.
14. [Opcjonalnie] Wpisz opis serwera odzyskiwania.
15. [Opcjonalnie] Kliknij kartę **Reguły zapory chmury**, aby edytować domyślne reguły zapory. Aby uzyskać więcej informacji, zobacz "Ustawianie reguł zapory dla serwerów chmurowych" (s. 87).
16. Kliknij **Utwórz**.

Serwer odzyskiwania pojawi się na karcie **Odzyskiwanie po awarii** > **Serwery** > **Serwery odzyskiwania** konsoli Cyber Protect. Aby wyświetlić jego ustawienia, możesz zaznaczyć oryginalny komputer i kliknąć **Odzyskiwanie po awarii**.

Acronis Cyber Protect Cloud Manage account DISASTER RECOVERY Servers Connectivity Runbooks ANTI-MALWARE PROTECTION SOFTWARE MANAGEMENT BACKUP STORAGE REPORTS SETTINGS <small>Powered by Acronis AnyData Engine</small>	Servers					
	RECOVERY SERVERS PRIMARY SERVERS <input type="text" value="Search"/>					
	<input type="checkbox"/>	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

Przebieg przełączania awaryjnego

Produkcyjne przełączanie awaryjne

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Gdy zostanie utworzony serwer odzyskiwania, działa on w **stanie gotowości**. Odpowiadająca mu maszyna wirtualna nie istnieje, dopóki nie zostanie rozpoczęte przełączanie awaryjne. Przed uruchomieniem przełączania awaryjnego trzeba utworzyć co najmniej jedną kopię zapasową obrazu dysku (z woluminem startowym) pierwotnego komputera.

Po rozpoczęciu przełączania awaryjnego wybierz punkt odzyskiwania (kopię zapasową) pierwotnego komputera, na podstawie którego zostanie utworzona maszyna wirtualna o uprzednio zdefiniowanych parametrach. W operacji przełączania awaryjnego używana jest funkcja „Uruchamianie maszyny wirtualnej z kopii zapasowej”. Serwer odzyskiwania wchodzi w stan przejściowy **Finalizacja**. Proces ten polega na przeniesieniu dysków wirtualnych serwera z magazynu kopii zapasowych (pamięci „cold storage”) do magazynu odzyskiwania po awarii (pamięci „hot storage”).

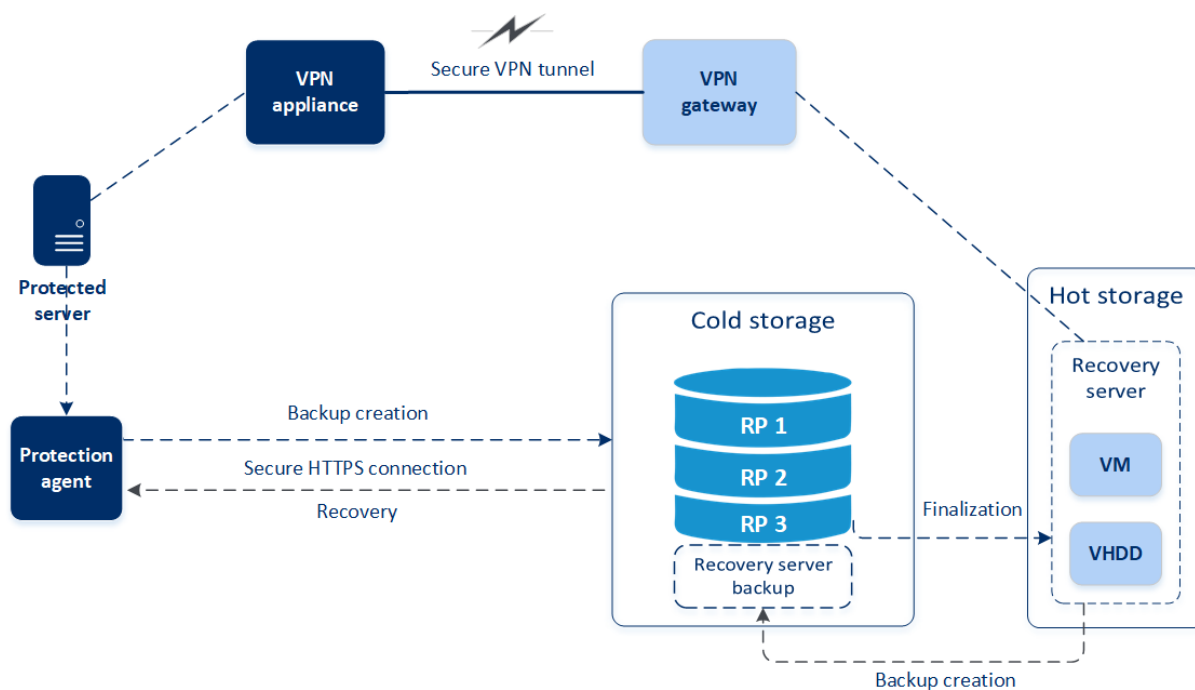
Uwaga

W trakcie procesu **Finalizacja** serwer jest dostępny i może wykonywać operacje, ale jego wydajność jest niższa niż zwykle. Możesz otworzyć konsolę serwera, klikając łącze **Konsola jest gotowa**. Łącze to jest dostępne w kolumnie **Stan maszyny wirtualnej** na ekranie **Odzyskiwanie po awarii > Serwery**, a także w widoku **Szczegóły** serwera.

Gdy **Finalizacja** zostanie ukończona, wydajność serwera osiąga normalną wartość. Stan serwera zmienia się na **Przełączanie awaryjne**. Obciążenie zostaje przełączone z oryginalnego komputera na serwer odzyskiwania w chmurze.

Jeśli na serwerze odzyskiwania znajduje się agent ochrony, usługa tego agenta jest zatrzymywana, aby zapobiec zakłóceniom (takim jak rozpoczęcie tworzenia kopii zapasowej lub zgłoszenie nieaktualnych statusów do komponentu kopii zapasowych).

Na poniższym diagramie przedstawiono zarówno proces przełączania awaryjnego, jak i proces powrotu po awarii.



Testuj przełączenie awaryjne

Podczas **testowego przełączania awaryjnego** maszyna wirtualna nie jest finalizowana. Oznacza to, że agent odczytuje zawartość dysków wirtualnych bezpośrednio z kopii zapasowej, tj. losowo uzyskuje dostęp do różnych części kopii zapasowej, i jego wydajność może być niższa od normalnej. Dodatkowe informacje na temat testowego przełączania awaryjnego można znaleźć w sekcji "Wykonywanie testowego przełączania awaryjnego" (s. 61).

Automatyczne testowe przełączanie awaryjne

Skonfigurowane automatyczne testowe przełączanie awaryjne jest wykonywane raz w miesiącu bez jakichkolwiek ręcznych interakcji. Dodatkowe informacje można znaleźć w sekcjach "Automatyczne testowe przełączanie awaryjne" (s. 64) i "Konfigurowanie automatycznego testowego przełączania awaryjnego" (s. 65).

Wykonywanie testowego przełączania awaryjnego

Wykonanie testu przełączania awaryjnego polega na uruchomieniu serwera odzyskiwania w testowej sieci VLAN odizolowanej od sieci produkcyjnej. Można przetestować kilka serwerów odzyskiwania jednocześnie i sprawdzić interakcje między nimi. W obrębie sieci testowej serwery

komunikują się za pomocą swoich produkcyjnych adresów IP, jednak nie mogą nawiązywać połączeń TCP ani UDP z obciążeniami w sieci lokalnej.

Podczas testowego przełączania awaryjnego maszyna wirtualna (serwer odzyskiwania) nie jest finalizowana. Agent odczytuje zawartość dysków wirtualnych bezpośrednio z kopii zapasowej i losowo uzyskuje dostęp do różnych części kopii zapasowej. Może to spowodować, że wydajność serwera odzyskiwania w stanie testowego przełączania awaryjnego będzie niższa od normalnej.

Wykonanie testu przełączania awaryjnego jest wprawdzie opcjonalne, jednak warto robić go regularnie — tak często, jak się da, biorąc pod uwagę koszty i względy bezpieczeństwa. Dobrą praktyką jest utworzenie runbooka, czyli zestawu instrukcji opisujących sposób uruchamiania środowiska produkcyjnego w chmurze.

Ważne

Trzeba zawczasu [utworzyć serwer odzyskiwania](#), aby chronić swoje urządzenia przed awarią.

Przełączenie awaryjne można wykonać tylko z tych punktów odzyskiwania, które zostały utworzone po utworzeniu serwera odzyskiwania danego urządzenia.

Przed przełączeniem awaryjnym na serwer odzyskiwania musi zostać utworzony co najmniej jeden punkt odzyskiwania. Obsługiwanych jest maksymalnie 100 punktów odzyskiwania.

Aby wykonać testowe przełączenie awaryjne

1. Wybierz pierwotną maszynę lub serwer odzyskiwania, który chcesz przetestować.
2. Kliknij **Odzyskiwanie po awarii**.
Zostanie wyświetlony opis serwera odzyskiwania.
3. Kliknij **Przełączanie awaryjne**.
4. Wybierz typ przełączania awaryjnego **Testuj przełączenie awaryjne**.
5. Wybierz punkt odzyskiwania (kopię zapasową), a następnie kliknij **Rozpocznij**.
6. Jeśli wybrana kopia zapasowa jest zaszyfrowana za pomocą szyfrowania jako właściwość komputera:
 - a. Wprowadź hasło szyfrowania zestawu kopii zapasowych.

Uwaga

Hasło zostanie zapisane tylko tymczasowo i będzie używane tylko w ramach bieżącej operacji testowego przełączania awaryjnego. Jeśli testowe przełączenie awaryjne zostanie zatrzymane lub gdy się zakończy, hasło zostanie automatycznie usunięte z magazynu poświadczeń.

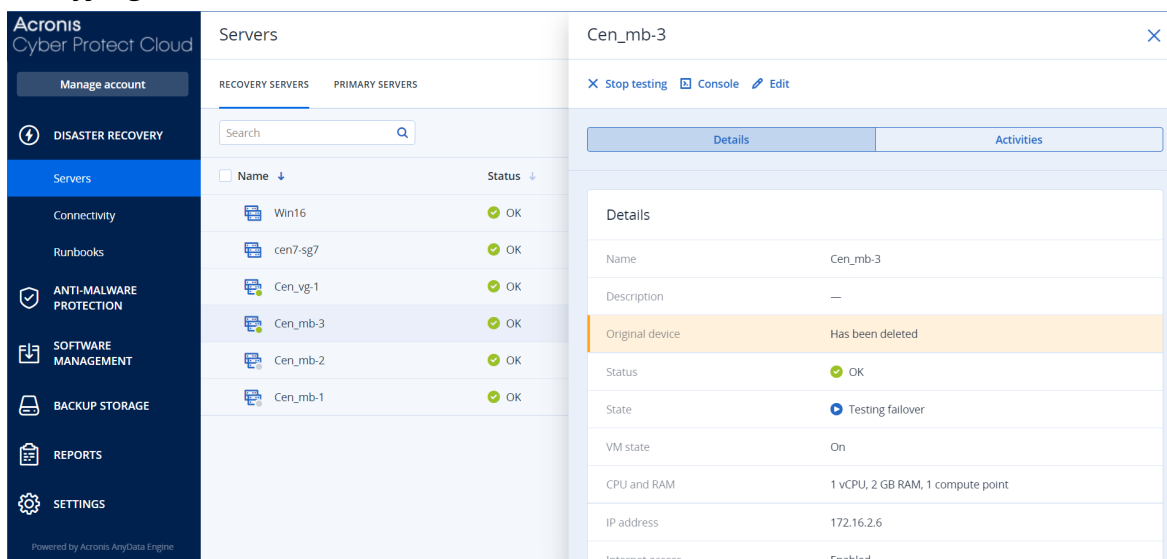
- b. [Opcjonalnie] Aby zapisać hasło do zestawu kopii zapasowych i użyć go w kolejnych operacjach przełączania awaryjnego, zaznacz pole wyboru **Zachowaj hasło w bezpiecznym magazynie poświadczeń**, a następnie w polu **Nazwa poświadczenia** wpisz nazwę tego poświadczenia.

Ważne

Hasło zostanie zapisane w bezpiecznym magazynie poświadczeń i będzie stosowane automatycznie w późniejszych operacjach przełączania awaryjnego. Zapisywanie haseł jednak może być sprzeczne z wymogami dotyczącymi zachowania zgodności z przepisami.

c. Kliknij **Gotowe**.

Po uruchomieniu serwera odzyskiwania jego stan zmieni się na **Testowanie przełączania awaryjnego**.



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

Details	
Name	Cen_mb-3
Description	—
Original device	Has been deleted
Status	OK
State	Testing failover
VM state	On
CPU and RAM	1 vCPU, 2 GB RAM, 1 compute point
IP address	172.16.2.6
Internet access	Enabled

7. Wykonaj dowolne z następujących czynności, aby przetestować serwer odzyskiwania:

- W sekcji **Odzyskiwanie po awarii > Serwery** wybierz serwer odzyskiwania, a następnie kliknij **Konsola**.
- Nawiąż połączenie z serwerem odzyskiwania za pomocą protokołu RDP lub SSH oraz testowego adresu IP podanego podczas tworzenia tego serwera. Sprawdź połączenie zarówno wewnątrz sieci produkcyjnej, jak i poza nią (zgodnie z opisem podanym w sekcji „Połączenie point-to-site”).
- Uruchom skrypt na serwerze odzyskiwania.
Skrypt może sprawdzić ekran logowania, stan uruchomienia aplikacji, połączenie z Internetem oraz możliwość nawiązania połączenia z serwerem odzyskiwania przez pozostałe komputery.
- Jeśli serwer odzyskiwania ma dostęp do Internetu i publiczny adres IP, można skorzystać z programu TeamViewer.

8. Po ukończeniu testu kliknij **Zatrzymaj testowanie**.

Serwer odzyskiwania zostanie zatrzymany. Zmiany wprowadzone na serwerze odzyskiwania podczas testu przełączania awaryjnego nie są zapisywane.

Uwaga

Czynności **Uruchom serwer** i **Zatrzymaj serwer** nie mają zastosowania w przypadku operacji przełączania awaryjnego — dotyczy to zarówno runbooków, jak i ręcznego uruchomienia testowego przełączania awaryjnego. Próba wykonania takiej czynności zakończy się niepowodzeniem z następującym komunikatem o błędzie:

Niepowodzenie: Czynność nie ma zastosowania w bieżącym stanie serwera.

Automatyczne testowe przełączanie awaryjne

W przypadku korzystania z funkcji automatycznego testowego przełączania awaryjnego serwer odzyskiwania jest automatycznie testowany raz w miesiącu bez jakichkolwiek ręcznych interakcji.

Proces automatycznego testowego przełączania awaryjnego obejmuje następujące etapy:

1. utworzenie maszyny wirtualnej z ostatniego punktu odzyskiwania
2. wykonanie zrzutu ekranu maszyny wirtualnej
3. przeanalizowanie, czy system operacyjny maszyny wirtualnej pomyślnie się uruchamia
4. wysłanie powiadomienia o statusie testowego przełączania awaryjnego

Uwaga

Podczas automatycznego testowego przełączania awaryjnego wykorzystywane są punkty obliczeniowe.

Automatyczne testowe przełączanie awaryjne można skonfigurować w ustawieniach serwera odzyskiwania. Aby uzyskać więcej informacji, zobacz "Konfigurowanie automatycznego testowego przełączania awaryjnego" (s. 65).

Należy pamiętać, że w bardzo rzadkich przypadkach automatyczne testowe przełączanie awaryjne może zostać pominięte i nie zostać wykonane w zaplanowanym czasie. Może się tak zdarzyć, ponieważ przełączanie awaryjne w środowisku produkcyjnym ma wyższy priorytet niż automatyczne testowe przełączanie awaryjne, więc zasoby sprzętowe (procesor i pamięć RAM) alokowane na potrzeby automatycznego testowego przełączania awaryjnego mogą zostać tymczasowo ograniczone, aby wykonywane równolegle przełączanie awaryjne w środowisku produkcyjnym miało do dyspozycji wystarczające zasoby.

Jeśli automatyczne testowe przełączanie awaryjne zostanie z jakiegoś powodu pominięte, zostanie zgłoszony alert.

Uwaga

Automatyczne testowe przełączanie awaryjne się nie powiedzie, jeśli kopie zapasowe oryginalnego komputera są zaszyfrowane za pomocą szyfrowania jako właściwości komputera, a hasło szyfrowania nie zostało określone podczas tworzenia serwera odzyskiwania. Aby uzyskać więcej informacji na temat określania hasła szyfrowania, zobacz "Tworzenie serwera odzyskiwania" (s. 57).

Konfigurowanie automatycznego testowego przełączania awaryjnego

Dzięki skonfigurowaniu automatycznego testowego przełączania awaryjnego można co miesiąc testować serwer odzyskiwania bez ręcznego wykonywania jakichkolwiek czynności.

Aby skonfigurować automatyczne testowe przełączanie awaryjne

1. W konsoli przejdź do sekcji **Odzyskiwanie po awarii > Serwery > Serwery odzyskiwania** i zaznacz serwer odzyskiwania.
2. Kliknij **Edytuj**.
3. W sekcji **Automatyczne testowe przełączanie awaryjne** w polu **Harmonogram** wybierz **Co miesiąc**.
4. [Opcjonalnie] W polu **Limit czasu zrzutu ekranu** zmień wartość domyślną maksymalnego przedziału czasu (w minutach), w którym system będzie próbował wykonać automatyczne testowe przełączenie awaryjne.
5. [Opcjonalnie] Jeśli chcesz zapisać wartość pola **Limit czasu zrzutu ekranu** jako domyślną, tak aby była automatycznie stosowana, gdy aktywujesz automatyczne testowe przełączanie awaryjne dla innych serwerów odzyskiwania, wybierz **Ustaw jako domyślny limit czasu**.
6. Kliknij **Zapisz**.

Wyświetlanie statusu automatycznego testowego przełączania awaryjnego

Możesz wyświetlić szczegóły zakończonego automatycznego testowego przełączania awaryjnego, takie jak status, godzina rozpoczęcia, godzina zakończenia, czas trwania oraz zrzut ekranu maszyny wirtualnej.

Aby wyświetlić status automatycznego testowego przełączania awaryjnego serwera odzyskiwania

1. W konsoli przejdź do sekcji **Odzyskiwanie po awarii > Serwery > Serwery odzyskiwania** i zaznacz serwer odzyskiwania.
2. W sekcji **Automatyczne testowe przełączanie awaryjne** sprawdź szczegóły ostatniego automatycznego testowego przełączania awaryjnego.
3. [Opcjonalnie] Kliknij **Pokaż zrzut ekranu**, aby wyświetlić zrzut ekranu maszyny wirtualnej.

Wyłączanie automatycznego testowego przełączania awaryjnego

Automatyczne testowe przełączanie awaryjne można wyłączyć, aby oszczędzać zasoby lub jeśli automatyczne testowe przełączanie awaryjne nie musi zostać wykonane w przypadku określonego serwera odzyskiwania.

Aby wyłączyć automatyczne testowe przełączanie awaryjne

1. W konsoli przejdź do sekcji **Odzyskiwanie po awarii > Serwery > Serwery odzyskiwania** i zaznacz serwer odzyskiwania.
2. Kliknij **Edytuj**.

3. W sekcji **Automatyczne testowe przełączanie awaryjne** w polu **Harmonogram** wybierz **Nigdy**.
4. Kliknij **Zapisz**.

Wykonywanie przełączenia awaryjnego

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Przełączenie awaryjne to proces przenoszenia obciążenia z Twojej lokalizacji do chmury oraz stan obecności tego obciążenia w chmurze.

Po rozpoczęciu procesu przełączania awaryjnego serwer odzyskiwania jest uruchamiany w sieci produkcyjnej. Aby uniknąć zakłóceń i niepożądanych problemów, upewnij się, że pierwotne obciążenie nie jest w trybie online i nie ma do niego dostępu przez połączenie VPN.

Aby zapobiec zakłóceniom kopii zapasowych w tym samym archiwum w chmurze, należy ręcznie odwołać plan ochrony z obciążenia będącego aktualnie w stanie **Przełączanie awaryjne**.

Dodatkowe informacje na temat odwoływania planów można znaleźć w sekcji [Odwoływanie planu ochrony](#).

Ważne

Trzeba zawczasu [utworzyć serwer odzyskiwania](#), aby chronić swoje urządzenia przed awarią.

Przełączenie awaryjne można wykonać tylko z tych punktów odzyskiwania, które zostały utworzone po utworzeniu serwera odzyskiwania danego urządzenia.

Przed przełączeniem awaryjnym na serwer odzyskiwania musi zostać utworzony co najmniej jeden punkt odzyskiwania. Obsługiwanych jest maksymalnie 100 punktów odzyskiwania.

Możesz postąpić zgodnie z poniższymi instrukcjami lub obejrzeć [instruktaż wideo](#).

Aby wykonać przełączenie awaryjne

1. Upewnij się, że pierwotna maszyna nie jest dostępna w sieci.
2. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii > Serwery > Serwery odzyskiwania** i zaznacz serwer odzyskiwania.
3. Kliknij **Przełączanie awaryjne**.
4. Wybierz typ przełączania awaryjnego **Produkcyjne przełączanie awaryjne**.
5. Wybierz punkt odzyskiwania (kopię zapasową), a następnie kliknij **Rozpocznij**.
6. [Jeśli wybrana kopia zapasowa jest zaszyfrowana za pomocą szyfrowania jako właściwość komputera]

- a. Wprowadź hasło szyfrowania zestawu kopii zapasowych.

Uwaga

Hasło zostanie zapisane tylko tymczasowo i będzie używane tylko w ramach bieżącej operacji przełączania awaryjnego. Po zakończeniu operacji przełączania awaryjnego i powrocie serwera do stanu **Stan gotowości** hasło zostanie automatycznie usunięte z magazynu poświadczeń.

- b. [Opcjonalnie] Aby zapisać hasło do zestawu kopii zapasowych i użyć go w kolejnych operacjach przełączania awaryjnego, zaznacz pole wyboru **Zachowaj hasło w bezpiecznym magazynie poświadczeń**, a następnie w polu **Nazwa poświadczenia** wpisz nazwę tego poświadczenia.

Ważne

Hasło zostanie zapisane w bezpiecznym magazynie poświadczeń i będzie stosowane automatycznie w późniejszych operacjach przełączania awaryjnego. Zapisywanie haseł jednak może być sprzeczne z wymogami dotyczącymi zachowania zgodności z przepisami.

- c. Kliknij **Gotowe**.

Po uruchomieniu serwera odzyskiwania jego stan zmienia się na **Finalizacja**, a po pewnym czasie na **Przełączanie awaryjne**.

Ważne

Nie wolno zapominać, że serwer jest dostępny zarówno w stanie **Finalizacja**, jak i w stanie **Przełączanie awaryjne**. W stanie **Finalizacja** można uzyskać dostęp do konsoli serwera przez kliknięcie łącza **Konsola jest gotowa**. Łącze to jest dostępne w kolumnie **Stan maszyny wirtualnej** na ekranie **Odzyskiwanie po awarii > Serwery**, a także w widoku **Szczegóły** serwera. Szczegółowe informacje można znaleźć w sekcji "Przebieg przełączania awaryjnego" (s. 60).

The screenshot displays the Acronis Cyber Protect Cloud management console. On the left is a navigation sidebar with options like 'Manage account', 'DISASTER RECOVERY', 'Servers', 'Connectivity', 'Runbooks', 'ANTI-MALWARE PROTECTION', 'SOFTWARE MANAGEMENT', 'BACKUP STORAGE', 'REPORTS', and 'SETTINGS'. The main area is divided into two panels. The left panel, titled 'Servers', shows a list of servers under 'PRIMARY SERVERS' with columns for 'Name' and 'Status'. The servers listed are Win16, cen7-sg7, Cen_vg-1, Cen_mb-3, Cen_mb-2, and Cen_mb-1, all with a status of 'OK'. The right panel shows the 'Details' for the selected server 'Cen_vg-1'. It includes a header with action buttons (Cancel failover, Recovery, Power off, Console, Edit, Delete) and a tabbed interface with 'Details', 'Backup', 'Activities', and 'Failback'. The 'Details' tab is active, showing fields for Name, Description, Original device (cen7-sg), Status (OK), State (Failover), VM state (On), CPU and RAM (1 vCPU, 2 GB RAM, 1 compute point), and IP address (172.16.2.22).

7. Upewnij się, że serwer odzyskiwania został uruchomiony, sprawdzając jego konsolę. Kliknij **Odzyskiwanie po awarii** > **Serwery**, wybierz serwer odzyskiwania, a następnie kliknij **Konsola**.
8. Upewnij się, że do serwera odzyskiwania można uzyskać dostęp za pomocą produkcyjnego adresu IP podanego podczas tworzenia tego serwera.

Po sfinalizowaniu serwera odzyskiwania automatycznie jest tworzony nowy plan ochrony i stosowany na tym serwerze. Ten plan ochrony jest tworzony na podstawie planu, za pomocą którego utworzono serwer odzyskiwania (z pewnymi ograniczeniami). W tym planie możesz zmienić tylko harmonogram oraz reguły przechowywania. Aby uzyskać więcej informacji, zobacz sekcję „[Tworzenie kopii zapasowych serwerów chmurowych](#)”.

Jeśli chcesz anulować przełączenie awaryjne, wybierz serwer odzyskiwania i kliknij **Anuluj przełączenie awaryjne**. Wszystkie zmiany wprowadzone od chwili przełączenia awaryjnego, z wyjątkiem kopii zapasowych serwera odzyskiwania, zostaną utracone. Serwer odzyskiwania wróci do stanu **gotowości**.

Jeśli chcesz wykonać powrót po awarii, wybierz serwer odzyskiwania i kliknij **Powrót po awarii**.

Jak wykonać przełączenie awaryjne serwerów korzystających z lokalnego serwera DNS

Jeśli używasz serwerów DNS w lokalizacji lokalnej do rozpoznawania nazw komputerów, to po przełączeniu awaryjnym na serwery odzyskiwania odpowiadające im komputery korzystające z serwerów DNS nie będą się komunikować, ponieważ w chmurze są używane inne serwery DNS. Domyślnie serwery DNS w lokalizacji chmurze są używane na potrzeby nowo utworzonych serwerów chmurowych. Jeśli trzeba zastosować niestandardowe ustawienia DNS, skontaktuj się z działem pomocy technicznej.

Jak wykonać przełączenie awaryjne serwera DHCP

Lokalna infrastruktura może obejmować serwer DHCP działający na komputerze z systemem Windows lub Linux. W przypadku przełączenia awaryjnego takiego hosta do lokalizacji w chmurze pojawia się problem zdublowania serwera DHCP, ponieważ brama VPN w chmurze pełni również funkcję serwera DHCP. Aby rozwiązać ten problem, wykonaj jedną z następujących czynności:

- Jeśli tylko host DHCP został przełączony awaryjnie do chmury, a pozostałe serwery lokalne nadal działają w lokalizacji lokalnej, zaloguj się na hoście DHCP w chmurze i wyłącz na nim serwer DHCP. W ten sposób zapobiegiesz konfliktom i tylko brama VPN będzie działać jako serwer DHCP.
- Jeśli serwery chmurowe mają już adresy IP z hosta DHCP, trzeba się zalogować na hoście DHCP w chmurze i wyłączyć na nim serwer DHCP. Trzeba też się zalogować na serwerze chmurowe i odnowić dzierżawę DHCP, aby przypisać nowe adresy IP przydzielone z właściwego serwera DHCP (hostowanego na bramie VPN).

Uwaga

Instrukcje te nie mają zastosowania, jeśli serwer DHCP w chmurze jest skonfigurowany z użyciem opcji **Niestandardowy serwer DHCP**, a niektóre serwery odzyskiwania lub podstawowe dostają z niego swoje adresy IP.

Przebieg powrotu po awarii

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Powrót po awarii to proces przenoszenia obciążenia z chmury z powrotem na komputer fizyczny lub maszynę wirtualną w lokalizacji lokalnej. Można wykonać powrót po awarii na serwer odzyskiwania w stanie **Przełączanie awaryjne** i nadal korzystać z tego serwera w lokalizacji lokalnej.

Istnieje możliwość przeprowadzenia automatycznego przełączenia awaryjnego na docelowy komputer fizyczny w lokalizacji lokalnej. Podczas powrotu po awarii można przesłać dane kopii zapasowej do lokalizacji lokalnej, podczas gdy maszyna wirtualna w chmurze nadal działa. Technologia ta pozwala na uzyskanie bardzo krótkiego czasu przestoju, którego oszacowanie jest wyświetlane w konsoli Cyber Protect. Można je sprawdzić i uwzględnić w planach swoich działań, a także ostrzec klientów o zbliżającym się przestoju, jeśli jest taka potrzeba.

Procesy powrotu po awarii na docelowe maszyny wirtualne nieco się różnią od procesów powrotu po awarii na docelowe komputery fizyczne. Dodatkowe informacje na temat faz procesu powrotu po awarii można znaleźć w sekcjach "Powrót po awarii na docelową maszynę wirtualną" (s. 69) i "Powrót po awarii na docelowy komputer fizyczny" (s. 74).

W szczególnych przypadkach, gdy nie można zastosować procedury automatycznego powrotu po awarii, można wykonać tę operację ręcznie. Aby uzyskać więcej informacji, zobacz "Ręczny powrót po awarii" (s. 78).

Uwaga

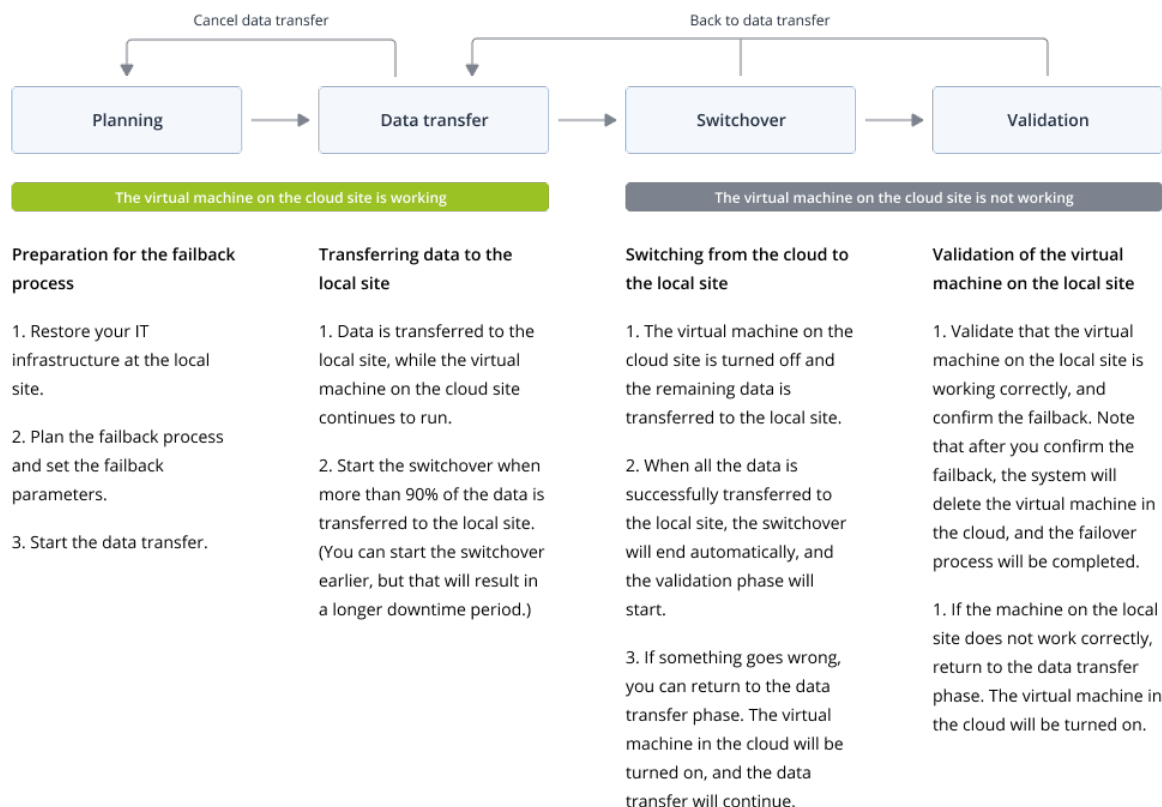
W przypadku wykonywania operacji przy użyciu runbooków jest obsługiwany tylko ręczny tryb powrotu po awarii. Oznacza to, że po rozpoczęciu powrotu po awarii przez wykonanie runbooka obejmującego krok **Powrót po awarii serwera** procedura będzie wymagała ręcznych interakcji: trzeba będzie ręcznie odzyskać komputer, a następnie potwierdzić lub anulować proces powrotu po awarii na karcie **Odzyskiwanie po awarii > Serwery**.

Powrót po awarii na docelową maszynę wirtualną

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Proces powrotu po awarii na docelową maszynę wirtualną obejmuje cztery fazy.



1. **Planowanie.** W tej fazie jest przywracana infrastruktura IT w lokalizacji lokalnej (taka jak hosty i konfiguracje sieci), są konfigurowane parametry powrotu po awarii i jest planowany czas rozpoczęcia przesyłania danych.

Uwaga

Aby zminimalizować czas trwania procesu powrotu po awarii, warto rozpocząć fazę przesyłania danych zaraz po skonfigurowaniu serwerów lokalnych i kontynuować konfigurowanie sieci oraz pozostałej infrastruktury lokalnej w trakcie fazy przesyłania danych.

2. **Przesyłanie danych.** W tej fazie dane są przesyłane z lokalizacji w chmurze do lokalizacji lokalnej, a maszyna wirtualna w chmurze nadal działa. W fazie przesyłania danych można w każdej chwili rozpocząć następną fazę, czyli przełączanie, ale warto wziąć pod uwagę następujące zależności:

Im dłużej trwa faza przesyłania danych,

- tym dłużej działa maszyna wirtualna w chmurze.
- tym więcej danych zostanie przesłanych do lokalizacji lokalnej.
- tym wyższe będą koszty (poświęcisz więcej punktów obliczeniowych).
- tym krótszy będzie przestój w fazie przełączania.

Jeśli chcesz maksymalnie skrócić czas przestoju, rozpocznij fazę przełączania, gdy do lokalizacji lokalnej zostanie przesłanych ponad 90% danych.

Jeśli możesz sobie pozwolić na dłuższy przestój, a nie chcesz wykorzystywać kolejnych punktów obliczeniowych na działanie maszyny wirtualnej w chmurze, możesz rozpocząć fazę przełączanie wcześniej.

Jeśli anulujesz proces powrotu po awarii w fazie przesyłania danych, to przesłane dane nie zostaną usunięte z lokalizacji lokalnej. Aby uniknąć ewentualnych problemów, ręcznie usuń przeniesione dane, zanim rozpoczniesz nowy proces powrotu po awarii. Kolejny proces przesyłania danych zacznie się od nowa.

3. **Przełączanie.** W tej fazie jest wyłączana maszyna wirtualna w chmurze, i pozostałe dane, w tym ostatni przyrost kopii zapasowej, są przesyłane do lokalizacji lokalnej. Jeśli na serwerze odzyskiwania nie zastosowano żadnego planu tworzenia kopii zapasowych, kopia zapasowa zostanie utworzona automatycznie w fazie przełączania, a to spowolni proces.

Szacowany czas do zakończenia tej fazy (czas przestoju) można sprawdzić w konsoli Cyber Protect. Z chwilą przesłania wszystkich danych do lokalizacji lokalnej (nie wystąpi żadna utrata danych, a maszyna wirtualna w lokalizacji lokalnej będzie dokładną kopią maszyny wirtualnej z chmury) faza przełączania zostaje zakończona. Maszyna wirtualna w lokalnej lokalizacji będzie odzyskana i automatycznie się rozpocznie faza sprawdzania poprawności.

4. **Sprawdzenie poprawności.** W tej fazie maszyna wirtualna w lokalizacji lokalnej jest gotowa i zostaje automatycznie uruchomiona. Możesz sprawdzić, czy maszyna wirtualna działa poprawnie, a ponadto:
- Jeśli wszystko działa zgodnie z oczekiwaniami, można potwierdzić wykonanie powrotu po awarii. Po potwierdzeniu wykonania powrotu po awarii zostaje usunięta maszyna wirtualna w chmurze, a serwer odzyskiwania wraca do stanu **Stan gotowości**. Na tym proces powrotu po awarii się kończy.
 - Jeśli coś będzie nie tak, można anulować przełączanie i wrócić do fazy przesyłania danych.

Wykonywanie powrotu po awarii na maszynę wirtualną

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Istnieje możliwość przeprowadzenia powrotu po awarii na docelową maszynę wirtualną w lokalizacji lokalnej.

Wymagania wstępne

- Agent, który zostanie użyty do wykonania powrotu po awarii, jest w trybie online i nie jest aktualnie używany do żadnej innej operacji powrotu po awarii.
- Masz stabilne połączenie z Internetem.
- Istnieje co najmniej jedna pełna kopia zapasowa maszyny wirtualnej w chmurze.

Aby wykonać powrót po awarii na maszynę wirtualną

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii > Serwery**.
2. Wybierz serwer odzyskiwania znajdujący się w stanie **przełączania awaryjnego**.
3. Kliknij kartę **Powrót po awarii**.
4. W sekcji **Parametry powrotu po awarii** wybierz opcję **Maszyna wirtualna** w polu **Miejsce docelowe** i skonfiguruj pozostałe parametry.

Uwaga: domyślnie niektóre **Parametry powrotu po awarii** mają automatycznie ustawione proponowane wartości, ale można je zmienić.

Poniższa tabela zawiera dodatkowe informacje na temat ustawień dostępnych w sekcji **Parametry powrotu po awarii**.

Parametr	Opis
Rozmiar kopii zapasowej	<p>Ilość danych, które zostaną przesłane do lokalizacji lokalnej podczas procesu powrotu po awarii.</p> <p>Po rozpoczęciu procesu powrotu po awarii na docelową maszynę wirtualną wartość Rozmiar kopii zapasowej będzie się zwiększać w fazie przesyłania danych, ponieważ maszyna wirtualna w chmurze nadal będzie działać i generować nowe dane.</p> <p>Aby oszacować czas przestoju podczas procesu powrotu po awarii na docelową maszynę wirtualną, podziel 10% wartości Rozmiar kopii zapasowej (ponieważ zalecamy rozpoczęcie fazy przełączania po przesłaniu 90% danych do lokalizacji lokalnej) przez wartość szybkości połączenia z Internetem.</p> <hr/> <p>Uwaga W przypadku jednoczesnego wykonywania kilku procesów powrotu po awarii wartość szybkości połączenia z Internetem będzie mniejsza.</p>
Miejsce docelowe	Typ obciążenia w lokalizacji lokalnej, na które będzie odzyskiwany serwer chmurowy: Maszyna wirtualna lub Komputer fizyczny .
Lokalizacja komputera docelowego	<p>Lokalizacja na potrzeby powrotu po awarii: host VMware ESXi lub Microsoft Hyper-V.</p> <p>Możesz wybrać dowolny z hostów, które mają agenta zarejestrowanego w usłudze Cyber Protection.</p>
Agent	<p>Agent, który będzie wykonywać operację powrotu po awarii.</p> <p>Wybranego agenta można używać w danym czasie w ramach tylko jednej operacji powrotu po awarii.</p> <p>Można wybrać agenta, który jest w trybie online i nie jest aktualnie używany na potrzeby innego procesu powrotu po awarii, jest w wersji obsługującej funkcję powrotu po awarii oraz ma prawa dostępu do kopii zapasowej.</p> <p>Uwaga: można zainstalować na hostach VMware ESXi kilka agentów i uruchomić osobny proces powrotu po awarii przy użyciu każdego z nich. W ten sposób można wykonywać kilka procesów powrotu po awarii naraz.</p>

Parametr	Opis
Ustawienia komputera docelowego	<p>Ustawienia maszyny wirtualnej:</p> <ul style="list-style-type: none"> • Procesory wirtualne. Wybierz liczbę procesorów wirtualnych. • Pamięć. Wybierz wielkość pamięci maszyny wirtualnej. • Jednostki. Wybierz jednostki pamięci. • [Opcjonalnie] Karty sieciowe. Aby dodać kartę sieciową, kliknij Dodaj i w polu Sieć wybierz sieć. <p>Po wprowadzeniu pożądanych zmian kliknij Gotowe.</p>
Ścieżka	<p>(W przypadku hostów Microsoft Hyper-V) Folder na hoście, na którym będzie rezydować maszyna.</p> <p>Upewnij się, że w pamięci hosta jest wystarczająco dużo wolnego miejsca na maszynę.</p>
Magazyn danych	<p>(W przypadku hostów VMware ESXi) Magazyn danych na hoście, na którym będzie rezydować maszyna.</p> <p>Upewnij się, że w pamięci hosta jest wystarczająco dużo wolnego miejsca na maszynę.</p>
Tryb alokowania	<p>Metoda alokacji dysku wirtualnego.</p> <p>W przypadku hostów Microsoft Hyper-V:</p> <ul style="list-style-type: none"> • Powiększający się dynamicznie (wartość domyślna). • Stały rozmiar. <p>W przypadku hostów VMware ESXi:</p> <ul style="list-style-type: none"> • Elastyczne (wartość domyślna). • Nieelastyczne.
Nazwa komputera docelowego	<p>Nazwa komputera docelowego. Domyślnie komputer docelowy ma taką samą nazwę jak serwer odzyskiwania.</p> <p>Nazwa komputera docelowego musi być unikatowa w ramach lokalizacji wybranej w polu Lokalizacja komputera docelowego.</p>

5. Kliknij **Rozpocznij przesyłanie danych**, a następnie w oknie potwierdzenia kliknij **Rozpocznij**.

Uwaga

Jeżeli w chmurze nie ma kopii zapasowej maszyny wirtualnej, system automatycznie wykona kopię zapasową przed fazą przesyłania danych.

Rozpocznie się faza **Przesyłanie danych**. W konsoli będą wyświetlane następujące informacje:

Pole	Opis
Postęp	<p>Ten parametr odzwierciedla ilość danych już przesłanych do lokalizacji lokalnej oraz całkowitą ilość danych do przesłania.</p> <p>Całkowita ilość danych obejmuje dane z ostatniej kopii zapasowej sprzed rozpoczęcia fazy przesyłania danych oraz kopie zapasowe nowo</p>

Pole	Opis
	wygenerowanych danych (przyrosty kopii zapasowych), ponieważ maszyna wirtualna nadal działa podczas fazy przesyłania danych. Dlatego obie wartości parametru Postęp rosną w miarę upływu czasu.
Oszacowanie przestoju	Ten parametr wskazuje, jak długo maszyna wirtualna w chmurze będzie niedostępna w przypadku rozpoczęcia fazy przełączania w danej chwili. Wartość ta jest obliczana na podstawie wartości parametru Postęp i maleje w miarę upływu czasu.

6. Kliknij **Przełączanie**, a następnie w oknie potwierdzenia ponownie kliknij **Przełączanie**. Rozpocznie się faza przełączania. W konsoli będą wyświetlane następujące informacje:

Pole	Opis
Postęp	Ten parametr ilustruje postęp przywracania maszyny w lokalizacji lokalnej.
Szacowany czas do końca	Ten parametr ilustruje przybliżony czas zakończenia fazy przełączania, kiedy to będzie można włączyć komputer w lokalizacji lokalnej.

Uwaga

Jeśli do maszyny wirtualnej w chmurze nie zastosowano żadnego planu tworzenia kopii zapasowych, kopia zapasowa zostanie utworzona automatycznie w fazie przełączania, co spowoduje dłuższy przestój.

7. Po zakończeniu fazy **Przełączanie** i automatycznym uruchomieniu maszyny wirtualnej w lokalizacji lokalnej sprawdź, czy działa ona zgodnie z oczekiwaniami.
8. Kliknij **Potwierdź powrót po awarii**, a następnie w oknie potwierdzenia kliknij **Potwierdź**, aby sfinalizować proces.

Maszyna wirtualna w chmurze zostaje usunięta, a serwer odzyskiwania wraca do stanu **Stan gotowości**.

Uwaga

Zastosowanie planu ochrony na odzyskiwanym serwerze nie jest częścią procesu powrotu po awarii. Po zakończeniu procesu powrotu po awarii zastosuj plan ochrony na odzyskanym serwerze, aby wznowić jego ochronę. Możesz wykorzystać ten sam plan ochrony, który został zastosowany na pierwotnym serwerze, lub nowy plan ochrony z włączonym modulem

Odzyskiwanie po awarii.

Powrót po awarii na docelowy komputer fizyczny

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Proces automatycznego powrotu po awarii na docelowy komputer fizyczny obejmuje następujące fazy:

1. **Planowanie.** W tej fazie jest przywracana infrastruktura IT w lokalizacji lokalnej (taka jak hosty i konfiguracje sieci), są konfigurowane parametry powrotu po awarii i jest planowany czas rozpoczęcia przesyłania danych.
2. **Przesyłanie danych.** W tej fazie dane są przesyłane z lokalizacji w chmurze do lokalizacji lokalnej, a maszyna wirtualna w chmurze nadal działa. W fazie przesyłania danych można w każdej chwili rozpocząć następną fazę, czyli przełączanie, ale warto wziąć pod uwagę następujące zależności:

Im dłużej trwa faza przesyłania danych,

- tym dłużej działa maszyna wirtualna w chmurze.
- tym więcej danych zostanie przesłanych do lokalizacji lokalnej.
- tym wyższe będą koszty (poświęcisz więcej punktów obliczeniowych).
- tym krótszy będzie przestój w fazie przełączania.

Jeśli chcesz maksymalnie skrócić czas przestoju, rozpocznij fazę przełączania, gdy do lokalizacji lokalnej zostanie przesłanych ponad 90% danych.

Jeśli możesz sobie pozwolić na dłuższy przestój, a nie chcesz wykorzystywać kolejnych punktów obliczeniowych na działanie maszyny wirtualnej w chmurze, możesz rozpocząć fazę przełączania wcześniej.

Uwaga

Proces przesyłania danych wykorzystuje technologię flashback. Technologia ta obsługuje porównanie danych dostępnych na komputerze docelowym z danymi na maszynie wirtualnej w chmurze. Jeśli część tych danych jest już dostępna na komputerze docelowym, nie zostaną one przesłane ponownie. Technologia ta przyspiesza realizację fazy Przesyłanie danych.

Dlatego zalecamy przywrócenie serwera na pierwotną maszynę w lokalizacji lokalnej.

3. **Przełączanie.** W tej fazie jest wyłączana maszyna wirtualna w chmurze, i pozostałe dane, w tym ostatni przyrost kopii zapasowej, są przesyłane do lokalizacji lokalnej. Jeśli na serwerze odzyskiwania nie zastosowano żadnego planu tworzenia kopii zapasowych, kopia zapasowa zostanie utworzona automatycznie w fazie przełączania, a to spowolni proces.
4. **Sprawdzanie poprawności.** Podczas tej fazy komputer fizyczny w lokalizacji lokalnej jest gotowy i można go uruchomić ponownie przy użyciu nośnika startowego opartego na systemie Linux. Można sprawdzić, czy maszyna wirtualna działa poprawnie, oraz:
 - Jeśli wszystko działa zgodnie z oczekiwaniami, można potwierdzić wykonanie powrotu po awarii. Po potwierdzeniu wykonania powrotu po awarii zostaje usunięta maszyna wirtualna w chmurze, a serwer odzyskiwania wraca do stanu **Stan gotowości**. Na tym proces powrotu po awarii się kończy.
 - Jeśli coś będzie nie tak, można anulować przełączanie awaryjne i wrócić do fazy planowania.

Uwaga

Po ponownym uruchomieniu nośnika startowego nie będzie można go ponownie użyć. Jeśli w fazie sprawdzania poprawności zostanie wykryty jakiś błąd, trzeba będzie zarejestrować nowy nośnik startowy i ponownie rozpocząć proces powrotu po awarii.

Ponieważ jednak będzie używana technologia flashback, dane, które już się znajdują w lokalizacji lokalnej, nie będą ponownie przesyłane, a proces powrotu po awarii będzie znacznie szybszy.

Wykonywanie powrotu po awarii na komputer fizyczny

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Istnieje możliwość automatycznego przeprowadzenia powrotu po awarii na docelowy komputer fizyczny w lokalizacji lokalnej.

Uwaga

Proces przesyłania danych wykorzystuje technologię flashback. Technologia ta obsługuje porównanie danych dostępnych na komputerze docelowym z danymi na maszynie wirtualnej w chmurze. Jeśli część tych danych jest już dostępna na komputerze docelowym, nie zostaną one przesłane ponownie. Technologia ta przyspiesza realizację fazy Przesyłanie danych.

Dlatego zalecamy przywrócenie serwera na pierwotną maszynę w lokalizacji lokalnej.

Wymagania wstępne

- Agent, który zostanie użyty do wykonania powrotu po awarii, jest w trybie online i nie jest aktualnie używany do żadnej innej operacji powrotu po awarii.
- Masz stabilne połączenie z Internetem.
- Jest dostępny zarejestrowany nośnik startowy. Dodatkowe informacje można znaleźć w sekcji „Tworzenie nośników startowych do odzyskiwania systemów operacyjnych” w Podręczniku użytkownika programu Cyber Protection.
- Docelowy komputer fizyczny jest pierwotnym komputerem w lokalizacji lokalnej lub ma takie samo oprogramowanie układowe jak pierwotny komputer.
- Istnieje co najmniej jedna pełna kopia zapasowa maszyny wirtualnej w chmurze.

Aby wykonać powrót po awarii na komputer fizyczny

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii > Serwery**.
2. Wybierz serwer odzyskiwania znajdujący się w stanie **przełączania awaryjnego**.
3. Kliknij kartę **Powrót po awarii**.
4. W polu **Miejsce docelowe** wybierz **Komputer fizyczny**.
5. W polu **Docelowy nośnik startowy** kliknij **Określ**, wybierz nośnik startowy, a następnie kliknij **Gotowe**.

Uwaga

Zalecamy korzystanie z gotowych nośników startowych, ponieważ są one już skonfigurowane. Dodatkowe informacje można znaleźć w sekcji „Tworzenie nośników startowych do odzyskiwania systemów operacyjnych” w Podręczniku użytkownika programu Cyber Protection.

6. [Opcjonalnie] Aby zmienić domyślne mapowanie dysków, w polu **Mapowanie dysków** kliknij **Określ**, zamapuj dyski z kopii zapasowej na dyski komputera docelowego, a następnie kliknij **Gotowe**.
 7. Kliknij **Rozpocznij przesyłanie danych**, a następnie w oknie potwierdzenia kliknij **Rozpocznij**.
-

Uwaga

Jeżeli w chmurze nie ma kopii zapasowej maszyny wirtualnej, system automatycznie wykona kopię zapasową przed fazą przesyłania danych.

Rozpocznie się faza przesyłania danych. W konsoli będą wyświetlane następujące informacje:

Pole	Opis
Postęp	Ten parametr odzwierciedla ilość danych już przesłanych do lokalizacji lokalnej oraz całkowitą ilość danych do przesłania. Całkowita ilość danych obejmuje dane z ostatniej kopii zapasowej sprzed rozpoczęcia fazy przesyłania danych oraz kopie zapasowe nowo wygenerowanych danych (przyrosty kopii zapasowych), ponieważ maszyna wirtualna nadal działa podczas fazy przesyłania danych. Dlatego wartości parametru Postęp rosną w miarę upływu czasu. Ponieważ system używa technologii flashback podczas przesyłania danych i nie przesyła danych, które już są dostępne na komputerze docelowym, postęp może być szybszy niż ten, który został na początku obliczony przez konsolę.
Oszacowanie przestoju	Ten parametr wskazuje, jak długo maszyna wirtualna w chmurze będzie niedostępna w przypadku rozpoczęcia fazy przełączania w danej chwili. Wartość ta jest obliczana na podstawie wartości parametru Postęp i maleje w miarę upływu czasu. Ponieważ system używa technologii flashback podczas przesyłania danych i nie przesyła danych, które już są dostępne na komputerze docelowym, czas przestoju może być znacznie krótszy niż ten, który został na początku wyświetlony w konsoli.

8. Kliknij **Przełączanie**, a następnie w oknie potwierdzenia ponownie kliknij **Przełączanie**.
Rozpocznie się faza przełączania. W konsoli będą wyświetlane następujące informacje:

Pole	Opis
Postęp	Ten parametr ilustruje postęp przywracania maszyny w lokalizacji lokalnej.
Szacowany	Ten parametr ilustruje przybliżony czas zakończenia fazy przełączania,

Pole	Opis
czas do końca	kiedy to będzie można włączyć komputer w lokalizacji lokalnej.

Uwaga

Jeśli do maszyny wirtualnej w chmurze nie zastosowano żadnego planu tworzenia kopii zapasowych, kopia zapasowa zostanie utworzona automatycznie w fazie przełączania, co spowoduje dłuższy przestój.

- Po zakończeniu fazy **Przełączanie** uruchom ponownie nośnik startowy, a następnie sprawdź, czy komputer fizyczny w lokalizacji lokalnej działa zgodnie z oczekiwaniami.

Dodatkowe informacje można znaleźć w sekcji „Odzyskiwanie dysków przy użyciu nośnika startowego” w Podręczniku użytkownika programu Cyber Protection.

- Kliknij **Potwierdź powrót po awarii**, a następnie w oknie potwierdzenia kliknij **Potwierdź**, aby sfinalizować proces.

Maszyna wirtualna w chmurze zostaje usunięta, a serwer odzyskiwania wraca do stanu **Stan gotowości**.

Uwaga

Zastosowanie planu ochrony na odzyskiwanym serwerze nie jest częścią procesu powrotu po awarii. Po zakończeniu procesu powrotu po awarii zastosuj plan ochrony na odzyskanym serwerze, aby wznowić jego ochronę. Możesz wykorzystać ten sam plan ochrony, który został zastosowany na pierwotnym serwerze, lub nowy plan ochrony z włączonym modulem

Odzyskiwanie po awarii.

Ręczny powrót po awarii

Uwaga

Zalecamy korzystanie z ręcznego trybu powrotu po awarii tylko wtedy, gdy zaleci to zespół pomocy technicznej.

Proces powrotu po awarii można też uruchomić w trybie ręcznym. W takim przypadku przesłanie danych z kopii zapasowej w chmurze do lokalizacji lokalnej nie zostanie wykonane automatycznie. Trzeba to zrobić ręcznie po wyłączeniu maszyny wirtualnej w chmurze. Skutkuje to znacznym spowolnieniem procesu powrotu po awarii w trybie ręcznym i można się spodziewać dłuższego przestoju.

Proces powrotu po awarii w trybie ręcznym obejmuje następujące fazy:

- Planowanie.** W tej fazie jest przywracana infrastruktura IT w lokalizacji lokalnej (taka jak hosty i konfiguracje sieci), są konfigurowane parametry powrotu po awarii i jest planowany czas rozpoczęcia przesyłania danych.

2. **Przełączanie.** W tej fazie jest wyłączana maszyna wirtualna w chmurze i tworzona kopia zapasowa nowo wygenerowanych danych. Jeśli na serwerze odzyskiwania nie zastosowano żadnego planu tworzenia kopii zapasowych, kopia zapasowa zostanie utworzona automatycznie w fazie przełączania, a to spowolni proces. Po utworzeniu kopii zapasowej należy ręcznie odzyskać komputer w lokalizacji lokalnej. Można odzyskać dysk przy użyciu nośnika startowego lub odzyskać cały komputer z kopii zapasowej w chmurze.
3. **Sprawdzanie poprawności.** W tej fazie należy sprawdzić, czy komputer fizyczny lub maszyna wirtualna w lokalizacji lokalnej działa poprawnie, i potwierdzić wykonanie powrotu po awarii. Po potwierdzeniu zostaje usunięta maszyna wirtualna w lokalizacji w chmurze, a serwer odzyskiwania wraca do stanu **Stan gotowości**.

Wykonywanie ręcznego powrotu po awarii

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Istnieje możliwość przeprowadzenia ręcznego powrotu po awarii na docelowy komputer fizyczny lub maszynę wirtualną w lokalizacji lokalnej.

Aby wykonać ręczny powrót po awarii

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii > Serwery**.
2. Wybierz serwer odzyskiwania znajdujący się w stanie **przełączania awaryjnego**.
3. Kliknij kartę **Powrót po awarii**.
4. W polu **Miejsce docelowe** wybierz **Komputer fizyczny**.
5. Kliknij ikonę koła zębatego, a następnie włącz przełącznik **Użyj trybu ręcznego**.
6. [Opcjonalnie] Oszacuj czas przestoju podczas procesu powrotu po awarii: podziel wartość **Rozmiar kopii zapasowej** przez wartość szybkości połączenia z Internetem.

Uwaga

W przypadku jednoczesnego wykonywania kilku procesów powrotu po awarii wartość szybkości połączenia z Internetem będzie mniejsza.

7. Kliknij **Przełączanie**, a następnie w oknie potwierdzenia ponownie kliknij **Przełączanie**. Maszyna wirtualna w lokalizacji w chmurze zostaje wyłączona.

Uwaga

Jeśli do maszyny wirtualnej w chmurze nie zastosowano żadnego planu tworzenia kopii zapasowych, kopia zapasowa zostanie utworzona automatycznie w fazie przełączania, co spowoduje dłuższy przestój.

8. Odzyskaj serwer z kopii zapasowej w chmurze na komputer fizyczny lub maszynę wirtualną w lokalizacji lokalnej. Dodatkowe informacje można znaleźć w sekcji „Odzyskiwanie komputera” w Podręczniku użytkownika programu Cyber Protection.

9. Upewnij się, że proces odzyskiwania został ukończony i odzyskany komputer działa prawidłowo, a następnie kliknij **Przywrócono maszynę**.
10. Jeśli wszystko działa zgodnie z oczekiwaniami, kliknij **Potwierdź powrót po awarii**, a następnie w oknie potwierdzenia kliknij **Potwierdź**.
Serwer odzyskiwania i punkty odzyskiwania będą gotowe do następnego przełączenia awaryjnego. Aby utworzyć nowe punkty odzyskiwania, zastosuj plan ochrony do nowego serwera lokalnego.

Uwaga

Zastosowanie planu ochrony na odzyskiwanym serwerze nie jest częścią procesu powrotu po awarii. Po zakończeniu procesu powrotu po awarii zastosuj plan ochrony na odzyskanym serwerze, aby wznowić jego ochronę. Możesz wykorzystać ten sam plan ochrony, który został zastosowany na pierwotnym serwerze, lub nowy plan ochrony z włączonym modulem

Odzyskiwanie po awarii.

Praca z zaszyfrowanymi kopiami zapasowymi

Istnieje możliwość tworzenia serwerów odzyskiwania z zaszyfrowanych kopii zapasowych. Dla wygody można skonfigurować automatyczne stosowanie hasła do zaszyfrowanej kopii zapasowej podczas przełączania awaryjnego na serwer odzyskiwania.

Tworząc serwer odzyskiwania, można [podać hasło, które ma być używane do automatycznych operacji odzyskiwania po awarii](#). Zostanie ono zapisane w Magazynie poświadczeń, bezpiecznym repozytorium poświadczeń dostępnym w sekcji **Ustawienia > Poświadczenia**.

Jedno poświadczenie można powiązać z kilkoma kopiami zapasowymi.

Aby zarządzać hasłami zapisanymi w Magazynie poświadczeń

1. Przejdź do sekcji **Ustawienia > Poświadczenia**.
2. Aby zarządzać określonym poświadczeniem, kliknij ikonę w ostatniej kolumnie. Możesz wyświetlić elementy powiązane z tym poświadczeniem.
 - Aby usunąć powiązanie kopii zapasowej z wybranym poświadczeniem, kliknij ikonę kosza obok tej kopii. W rezultacie podczas przełączania awaryjnego na serwer odzyskiwania hasło trzeba będzie podać ręcznie.
 - Aby edytować poświadczenie, kliknij **Edytuj** i określ nazwę użytkownika lub hasło.
 - Aby usunąć poświadczenie, kliknij **Usuń**. Uwaga: podczas przełączania awaryjnego na serwer odzyskiwania hasło trzeba będzie podać ręcznie.

Operacje dotyczące maszyn wirtualnych Microsoft Azure

Uwaga

Niektóre funkcje mogą wymagać dodatkowego licencjonowania — w zależności od stosowanego modelu licencjonowania.

Można przeprowadzić przełączanie awaryjne maszyn wirtualnych Microsoft Azure na środowisko Acronis Cyber Protect Cloud. Aby uzyskać więcej informacji, zobacz "Wykonywanie przełączenia awaryjnego" (s. 66).

Potem można wykonać powrót po awarii ze środowiska Acronis Cyber Protect Cloud z powrotem na maszyny wirtualne Azure. Ten proces powrotu po awarii wygląda tak samo jak powrót po awarii na komputer fizyczny. Aby uzyskać więcej informacji, zobacz "Wykonywanie powrotu po awarii na komputer fizyczny" (s. 76).

Uwaga

Aby zarejestrować nową maszynę wirtualną Azure w celu wykonania powrotu po awarii, można użyć rozszerzenia Acronis Backup VM dostępnego na platformie Azure.

Można skonfigurować połączenie IPsec VPN multi-site między środowiskiem Acronis Cyber Protect Cloud a bramą VPN Azure. Aby uzyskać więcej informacji, zobacz "Konfigurowanie połączenia IPsec VPN multi-site" (s. 31).

Konfigurowanie serwerów podstawowych

W tej sekcji opisano, jak można utworzyć serwery podstawowe i nimi zarządzać.

Tworzenie serwera podstawowego

Wymagania wstępne

- Trzeba ustawić typ łączności z lokalizacją w chmurze.

Aby utworzyć serwer podstawowy

1. Przejdź do karty **Odzyskiwanie po awarii** > **Serwery** > **Serwery podstawowe**.
2. Kliknij **Utwórz**.
3. Wybierz szablon dla nowej maszyny wirtualnej.
4. Wybierz wariant konfiguracji (liczbę rdzeni wirtualnych i wielkość pamięci RAM). W poniższej tabeli przedstawiono maksymalną łączną ilość miejsca na dysku (GB) w przypadku każdego wariantu.

Typ	vCPU	RAM (GB)	Maksymalna łączna ilość miejsca na dysku (GB)
W1	1	2	500
F2	1	4	1000
W3	2	8	2000
W4	4	16	4000
W5	8	32	8000
W6	16	64	16000
W7	16	128	32000
W8	16	256	64000

Uwaga

Podano liczbę punktów obliczeniowych wykorzystywanych w przypadku każdej opcji. Liczba punktów obliczeniowych odzwierciedla koszt działania serwera podstawowego przez godzinę. Aby uzyskać więcej informacji, zobacz "Punkty obliczeniowe" (s. 12).

5. [Opcjonalnie] Zmień rozmiar dysku wirtualnego. Jeśli potrzebujesz więcej niż jednego dysku twardego, kliknij **Dodaj dysk**, a następnie określ rozmiar nowego dysku. Obecnie można dodać maksymalnie 10 dysków serwera podstawowego.
6. Wskaż sieć w chmurze, do której będzie należeć serwer podstawowy.
7. Wybierz **DHCP**.

Opcja DHCP	Opis
Dostępne w lokalizacji w chmurze	Ustawienie domyślne. Adres IP serwera zostanie udostępniony przez automatycznie skonfigurowany serwer DHCP w chmurze.
Niestandardowe	Adres IP serwera zostanie udostępniony przez Twój własny serwer DHCP w chmurze.

8. [Opcjonalnie] Podaj **adres MAC**.

Adres MAC jest unikatowym identyfikatorem przypisanym do karty sieciowej serwera. W przypadku korzystania z niestandardowego serwera DHCP można go skonfigurować tak, aby zawsze przypisywał określone adresy IP do określonych adresów MAC. Dzięki temu serwer podstawowy zawsze otrzymuje ten sam adres IP. Można uruchamiać aplikacje, które mają licencje zarejestrowane na adres MAC.

9. Określ adres IP, który będzie znajdował się w sieci produkcyjnej serwera. Domyślnie wybierany jest pierwszy niezajęty adres IP w Twojej sieci produkcyjnej.

Uwaga

Jeśli korzystasz z serwera DHCP, dodaj ten adres IP do listy elementów wykluczonych serwera, aby uniknąć konfliktu adresów IP.

W przypadku korzystania z niestandardowego serwera DHCP trzeba w polu **Adres IP w sieci produkcyjnej** podać ten sam adres, który został skonfigurowany na serwerze DHCP. W przeciwnym razie testowe przełączanie awaryjne nie będzie działać prawidłowo i nie będzie można się komunikować z serwerem przy użyciu publicznego adresu IP.

10. [Opcjonalnie] Zaznacz pole wyboru **Dostęp do Internetu**.

Opcja ta pozwala serwerowi podstawowemu na dostęp do Internetu. Domyślnie port TCP 25 jest otwarty dla połączeń wychodzących do publicznych adresów IP.

11. [Opcjonalnie] Zaznacz pole wyboru **Użyj publicznego adresu IP**.

Publiczny adres IP serwera podstawowego umożliwia uzyskiwanie do niego dostępu z Internetu. Jeśli pole wyboru pozostanie niezaznaczone, serwer będzie dostępny wyłącznie w Twojej sieci produkcyjnej.

Publiczny adres IP zostanie wyświetlony po zakończeniu konfiguracji. Domyślnie port TCP 443 jest otwarty dla połączeń przychodzących do publicznych adresów IP.

Uwaga

Jeśli wyczyścisz pole wyboru **Użyj publicznego adresu IP** lub usuniesz serwer odzyskiwania, jego publiczny adres IP nie zostanie zastrzeżony.

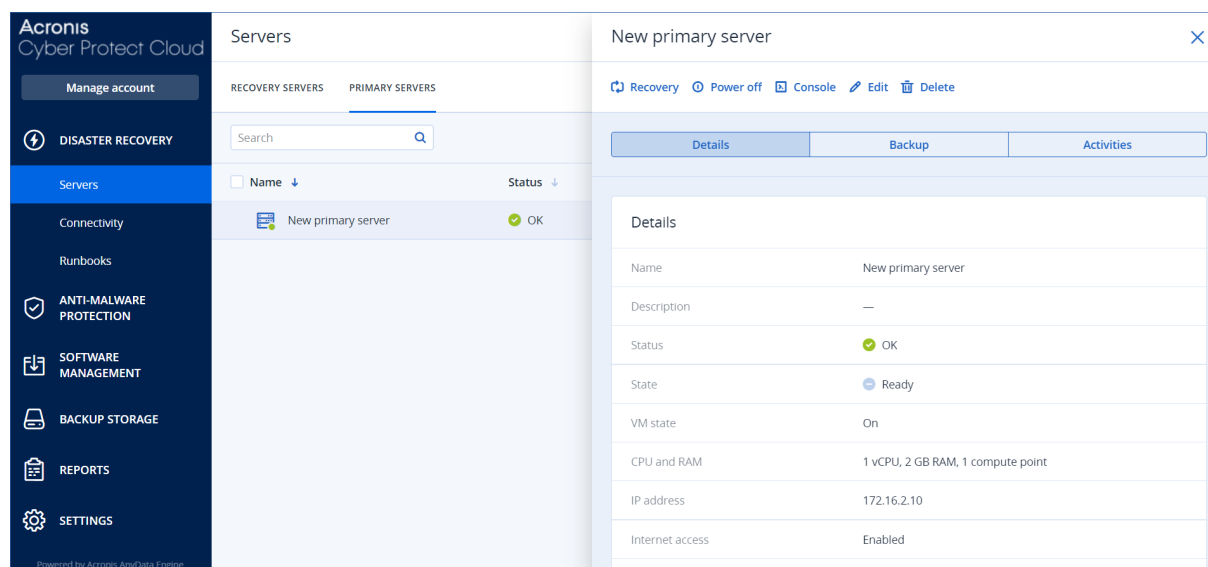
12. [Opcjonalnie] Wybierz **Ustaw próg RPO**.

Próg RPO określa maksymalny dozwolony odstęp czasu między ostatnim punktem odzyskiwania a czasem bieżącym. Można ustawić wartość z przedziałów: 15– 60 minut, 1–24 godz., 1–14 dni.

13. Podaj nazwę serwera podstawowego.

14. [Opcjonalnie] Podaj opis serwera podstawowego.
15. [Opcjonalnie] Kliknij kartę **Reguły zapory chmury**, aby edytować domyślne reguły zapory. Aby uzyskać więcej informacji, zobacz "Ustawianie reguł zapory dla serwerów chmurowych" (s. 87).
16. Kliknij **Utwórz**.

Serwer podstawowy zostanie udostępniony w sieci produkcyjnej. Możesz zarządzać serwerem za pomocą jego konsoli, funkcji RDP, połączenia SSH lub programu TeamViewer.



Działania na serwerze podstawowym

Serwer podstawowy pojawi się na karcie **Odzyskiwanie po awarii > Serwery > Serwery podstawowe** w konsoli Cyber Protect.

Aby uruchomić lub zatrzymać serwer, kliknij **Włącz** lub **Wyłącz** na panelu serwera podstawowego.

Aby edytować ustawienia serwera podstawowego, zatrzymaj serwer, a następnie kliknij **Edytuj**.

Aby zastosować plan ochrony do serwera podstawowego, zaznacz go i na karcie **Plan** kliknij **Utwórz**. Zostanie wyświetlony wstępnie zdefiniowany plan ochrony, w którym możesz zmienić tylko harmonogram oraz reguły przechowywania. Aby uzyskać więcej informacji, zobacz sekcję „[Tworzenie kopii zapasowych serwerów chmurowych](#)”.

Zarządzanie serwerami chmurowymi

Aby zarządzać serwerami chmurowymi, wybierz **Odzyskiwanie po awarii > Serwery**. Są tam dostępne dwie karty: **Serwery odzyskiwania** i **Serwery podstawowe**. Aby wyświetlić wszystkie opcjonalne kolumny w tabeli, kliknij ikonę koła zębatego.

Zaznaczając serwer chmurowy, można wyświetlić następujące informacje na jego temat.

Nazwa kolumny	Opis
Nazwa	Zdefiniowana przez Ciebie nazwa serwera chmurowego
Status	Status odzwierciedlający największy problem z danym serwerem chmurowym (na podstawie aktywnych alertów)
Stan	Stan serwera chmurowego
Stan maszyny wirtualnej	Stan zasilania maszyny wirtualnej powiązanej z serwerem chmurowym
Aktywna lokalizacja	Lokalizacja, w której jest hostowany serwer chmurowy. Na przykład Chmura .
Próg RPO	Maksymalny dozwolony odstęp czasu między ostatnim punktem odzyskiwania nadającym się do wykorzystania do przełączenia awaryjnego a czasem bieżącym. Dopuszczalne są wartości z następujących przedziałów: 15–60 minut, 1–24 godz., 1–14 dni.
Zgodność z wymogami RPO	<p>Zgodność z wymogami RPO to stosunek między rzeczywistym wskaźnikiem RPO a progiem RPO. Zgodność z wymogami RPO jest pokazywana tylko wtedy, gdy został zdefiniowany próg RPO.</p> <p>Oblicza się ją następująco:</p> $\text{Zgodność z wymogami RPO} = \frac{\text{rzeczywisty wskaźnik RPO}}{\text{próg RPO}}$ <p>gdzie</p> $\text{Rzeczywisty wskaźnik RPO} = \text{czas bieżący} - \text{czas ostatniego punktu odzyskiwania}$ <p>Statusy zgodności z wymogami RPO</p> <p>Zależnie od wartości wskaźnika stosunku rzeczywistego wskaźnika RPO do progu RPO używane są następujące statusy:</p> <ul style="list-style-type: none">• Zgodność. Zgodność z wymogami RPO < 1x. Serwer mieści się w progu RPO.• Przekroczenie. Zgodność z wymogami RPO ≤ 2x. Serwer narusza próg RPO.• Znaczne przekroczenie. Zgodność z wymogami RPO ≤ 4x. Serwer ponad dwukrotnie przekracza próg RPO.• Krytyczne przekroczenie. Zgodność z wymogami RPO > 4x. Serwer ponad czterokrotnie przekracza próg RPO.

	<ul style="list-style-type: none"> • Oczekujące (brak kopii zapasowych). Serwer jest chroniony przy użyciu planu ochrony, ale kopia zapasowa dopiero jest tworzona i nie została jeszcze ukończona.
Rzeczywisty wskaźnik RPO	Czas, jaki upłynął od utworzenia ostatniego punktu odzyskiwania
Ostatni punkt odzyskiwania	Data i godzina utworzenia ostatniego punktu odzyskiwania

Reguły zapory dotyczące serwerów chmurowych

Reguły zapory można skonfigurować tak, aby kontrolować ruch przychodzący i wychodzący serwera podstawowego oraz serwera odzyskiwania w lokalizacji w chmurze.

Reguły dotyczące połączeń przychodzących można skonfigurować po przydzieleniu serwerowi chmurowego publicznego adresu IP. Domyślnie dozwolony jest port TCP 443, a w przypadku pozostałych połączeń przychodzących jest aktywna odmowa dostępu. Można zmienić domyślne reguły zapory sieciowej oraz dodać lub usunąć wyjątki dotyczące połączeń przychodzących. Jeśli publiczny adres IP nie zostanie przydzielony, można jedynie przeglądać reguły dotyczące połączeń przychodzących, ale nie można ich konfigurować.

Reguły dotyczące połączeń wychodzących można skonfigurować po przydzieleniu serwerowi chmurowego dostępu do Internetu. Domyślnie skonfigurowana jest odmowa dostępu w przypadku portu TCP 25, a pozostałe połączenia wychodzące są dozwolone. Można zmienić domyślne reguły zapory sieciowej oraz dodać lub usunąć wyjątki dotyczące połączeń wychodzących. Jeśli dostęp do Internetu nie zostanie przydzielony, można jedynie przeglądać reguły dotyczące połączeń wychodzących, ale nie można ich konfigurować.

Uwaga

Ze względów bezpieczeństwa istnieją pewne gotowe reguły zapory, których nie można zmienić.

W przypadku połączeń przychodzących i wychodzących:

- Zezwolenie na obsługę poleceń ping: ICMP echo-request (type 8, code 0) and ICMP echo-reply (type 0, code 0)
- Permit ICMP need-to-frag (type 3, code 4)
- Permit TTL exceeded (type 11, code 0)

Tylko w przypadku połączeń przychodzących:

- Część, której nie można konfigurować: Odmawiaj w przypadku wszystkich

Tylko w przypadku połączeń wychodzących:

- Część, której nie można konfigurować: Odrzucaj wszystkie
-

Ustawianie reguł zapory dla serwerów chmurowych

Istnieje możliwość edycji domyślnych reguł zapory dla serwera podstawowego i serwera odzyskiwania w chmurze.

Aby edytować reguły zapory serwera w lokalizacji w chmurze

1. W konsoli Cyber Protect przejdź do sekcji **Odzyskiwanie po awarii > Serwery**.
2. Jeśli chcesz edytować reguły zapory serwera odzyskiwania, kliknij kartę **Serwery odzyskiwania**. Jeśli zaś chcesz edytować reguły zapory serwera podstawowego, kliknij kartę **Serwery podstawowe**.
3. Kliknij serwer, a następnie kliknij **Edytuj**.
4. Kliknij kartę **Reguły zapory chmury**.
5. Jeśli chcesz zmienić czynność domyślną dotyczącą połączeń przychodzących:
 - a. W polu rozwijanym **Przychodzące** wybierz czynność domyślną.

Czynność	Opis
Odmawiaj w przypadku wszystkich	Powoduje odmowę obsługi ruchu przychodzącego. Można dodawać wyjątki i zezwalać na ruch z określonych adresów IP, protokołów i portów.
Zezwalaj w przypadku wszystkich	Umożliwia zezwolenie na cały przychodzący ruch TCP i UDP. Można dodawać wyjątki i odmawiać obsługi ruchu z określonych adresów IP, protokołów i portów.

Uwaga

Zmiana czynności domyślnej powoduje unieważnienie i usunięcie konfiguracji istniejących reguł dotyczących połączeń przychodzących.

- b. [Opcjonalnie] Jeśli chcesz zapisać już dodane wyjątki, w oknie potwierdzenia wybierz **Zapisz wypełnione wyjątki**.
 - c. Kliknij **Potwierdź**.
6. Jeśli chcesz dodać wyjątek:
 - a. Kliknij **Dodaj wyjątek**.
 - b. Określ parametry zapory.

Parametr zapory	Opis
Protokół	Wybierz protokół połączenia. Obsługiwane są następujące opcje: <ul style="list-style-type: none"> • TCP • UDP • TCP+UDP
Port serwera	Wybierz porty, których dotyczy reguła. Możesz określić: <ul style="list-style-type: none"> • Konkretny numer portu (na przykład 2298) • Zakres numerów portów (na przykład 6000-6700) • Dowolny numer portu Użyj symbolu *, jeśli reguła ma dotyczyć każdego numeru portu.
Adres IP	Wybierz adresy IP, których dotyczy reguła. Możesz określić:

Parametr zapory	Opis
klienta	<ul style="list-style-type: none"> Konkretny adres IP (na przykład 192.168.0.0) Zakres adresów IP w notacji CIDR (na przykład 192.168.0.0/24) Dowolny adres IP Użyj symbolu *, jeśli reguła ma dotyczyć każdego adresu IP.

7. Jeśli chcesz usunąć jakiś wyjątek dotyczący połączeń przychodzących, kliknij znajdującą się obok niego ikonę kosza.

8. Jeśli chcesz zmienić czynność domyślną dotyczącą połączeń wychodzących:

a. W polu rozwijanym **Wychodzące** wybierz czynność domyślną.

Czynność	Opis
Odmawiaj w przypadku wszystkich	Powoduje odmowę obsługi ruchu wychodzącego. Można dodawać wyjątki i zezwalać na ruch do określonych adresów IP, protokołów i portów.
Zezwalaj w przypadku wszystkich	Powoduje zezwolenie na wszelki ruch wychodzący. Można dodawać wyjątki i odmawiać obsługi ruchu z określonych adresów IP, protokołów i portów.

Uwaga

Zmiana czynności domyślnej powoduje unieważnienie i usunięcie konfiguracji istniejących reguł dotyczących połączeń wychodzących.

b. [Opcjonalnie] Jeśli chcesz zapisać już dodane wyjątki, w oknie potwierdzenia wybierz **Zapisz wypełnione wyjątki**.

c. Kliknij **Potwierdź**.

9. Jeśli chcesz dodać wyjątek:

a. Kliknij **Dodaj wyjątek**.

b. Określ parametry zapory.

Parametr zapory	Opis
Protokół	Wybierz protokół połączenia. Obsługiwane są następujące opcje: <ul style="list-style-type: none"> TCP UDP TCP+UDP
Port serwera	Wybierz porty, których dotyczy reguła. Możesz określić: <ul style="list-style-type: none"> Konkretny numer portu (na przykład 2298) Zakres numerów portów (na przykład 6000-6700) Dowolny numer portu Użyj symbolu *, jeśli reguła ma dotyczyć

Parametr zapory	Opis
	każdego numeru portu.
Adres IP klienta	Wybierz adresy IP, których dotyczy reguła. Możesz określić: <ul style="list-style-type: none"> Konkretny adres IP (na przykład 192.168.0.0) Zakres adresów IP w notacji CIDR (na przykład 192.168.0.0/24) Dowolny adres IP Użyj symbolu *, jeśli reguła ma dotyczyć każdego adresu IP.

- Jeśli chcesz usunąć jakiś wyjątek dotyczący połączeń wychodzących, kliknij znajdującą się obok niego ikonę kosza.
- Kliknij **Zapisz**.

Sprawdzanie działań dotyczących zapory chmury

Po zaktualizowaniu konfiguracji reguł zapory serwera chmurowego w konsoli Cyber Protect będzie dostępny dziennik działań dotyczących aktualizacji. Można przejrzeć dziennik i sprawdzić takie informacje jak:

- nazwa użytkownika, który zaktualizował konfigurację
- data i godzina aktualizacji
- ustawienia zapory dla połączeń przychodzących i wychodzących
- domyślne czynności dotyczące połączeń przychodzących i wychodzących
- protokoły, porty i adresy IP wyjątków dotyczących połączeń przychodzących i wychodzących

Aby wyświetlić szczegóły zmian konfiguracji reguł zapory chmury

- W konsoli Cyber Protect kliknij **Monitorowanie > Działania**.
- Kliknij odpowiednie działanie, a następnie kliknij **Wszystkie właściwości**.
Działanie powinno być opisane jako **Aktualizowanie konfiguracji serwera w chmurze**.
- W polu **kontekst** sprawdź interesujące Cię informacje.

Tworzenie kopii zapasowych serwerów chmurowych

Kopie zapasowe serwerów podstawowych i serwerów odzyskiwania są tworzone bezagentowo w chmurze. Te kopie zapasowe mają następujące ograniczenia.

- Jediną możliwą lokalizacją kopii zapasowej jest chmura. Kopie zapasowe serwerów podstawowych są tworzone w magazynie **Kopia zapasowa serwerów podstawowych**.

Uwaga

Lokalizacje kopii zapasowych na platformie Microsoft Azure nie są obsługiwane.

- Nie można zastosować jednego planu tworzenia kopii zapasowych do wielu serwerów. Każdy serwer musi mieć własny plan tworzenia kopii zapasowych, nawet jeśli wszystkie te plany mają takie same ustawienia.
- Do serwera można zastosować tylko jeden plan tworzenia kopii zapasowych.
- Tworzenie kopii zapasowych uwzględniające aplikacje nie jest obsługiwane.
- Szyfrowanie jest niedostępne.
- Opcje tworzenia kopii zapasowych są niedostępne.

W wyniku usunięcia serwera podstawowego zostają usunięte również jego kopie zapasowe.

Kopia zapasowa serwera odzyskiwania jest tworzona tylko w stanie przełączania awaryjnego. Kopie zapasowe serwera odzyskiwania kontynuują tworzenie kopii zapasowych zgodnie z pierwotną kolejnością. W razie wykonania powrotu po awarii pierwotny serwer może kontynuować tę sekwencję tworzenia kopii zapasowych. Kopie zapasowe serwera odzyskiwania można zatem usuwać ręcznie lub poprzez zastosowanie reguł przechowywania. Kopie zapasowe serwera odzyskiwania są zawsze zachowywane po jego usunięciu.

Uwaga

Plany tworzenia kopii zapasowych dotyczące serwerów chmurowych są wykonywane według czasu UTC.

Orkiestracja (runbooki)

Uwaga

Niektóre funkcje mogą wymagać dodatkowego licencjonowania — w zależności od stosowanego modelu licencjonowania.

Runbook to zestaw instrukcji opisujących sposób uruchamiania środowiska produkcyjnego w chmurze. Runbooki można tworzyć z poziomu konsoli Cyber Protect. Aby otworzyć ekran **Runbooki**, wybierz **Odzyskiwanie po awarii > Runbooki**.

Dlaczego warto korzystać z runbooków?

Za pomocą runbooków można:

- Automatyzację przełączania awaryjnego jednego lub wielu serwerów
- Automatyczne sprawdzanie wyników operacji przełączania awaryjnego przez wysłanie sondy ping na adres IP serwera i sprawdzanie połączenia określonego portu
- Określanie sekwencji operacji dla serwerów z uruchomionymi aplikacjami rozproszonymi
- Uwzględnienie czynności manualnych w toku pracy
- Weryfikację integralności stosowanego rozwiązania do odzyskiwania po awarii przez uruchomienie runbooków w trybie testowania

Tworzenie runbooka

Runbook składa się z wykonywanych kolejno kroków. Krok składa się z rozpoczynanych jednocześnie czynności.

Możesz postąpić zgodnie z poniższą instrukcją lub obejrzeć [instruktaż wideo](#).

Aby utworzyć runbook

1. W konsoli Cyber Protection przejdź do sekcji **Odzyskiwanie po awarii > Runbooki**.
2. Kliknij **Utwórz runbook**.
3. Kliknij **Dodaj krok**.
4. Kliknij **Dodaj czynność**, a następnie wybierz czynność, którą chcesz dodać do kroku.

Czynność	Opis
Przełączenie awaryjne serwera	Wykonuje przełączenie awaryjne serwera chmurowego. Aby zdefiniować tę czynność, trzeba wybrać serwer chmurowy i skonfigurować dostępne dla danej czynności parametry runbooka. Aby uzyskać więcej informacji na temat tych parametrów, zobacz sekcję "Parametry runbooka" (s. 95).

Czynność	Opis
	<p>Uwaga</p> <p>Jeśli wybrana kopia zapasowa serwera jest zaszyfrowana za pomocą szyfrowania jako właściwość komputera, czynność Przełączenie awaryjne serwera zostanie wstrzymana i automatycznie zmieniona na Wymagane działanie. Aby kontynuować wykonywanie runbooka, musisz podać hasło do zaszyfrowanej kopii zapasowej.</p>
Wykonaj powrót po awarii serwera	<p>Przeprowadza powrót po awarii serwera chmurowego. Aby zdefiniować to działanie, musisz wybrać serwer chmurowy i skonfigurować dostępne dla tego działania parametry runbooka. Aby uzyskać więcej informacji na temat tych ustawień, zobacz sekcję "Parametry runbooka" (s. 95).</p> <p>Uwaga</p> <p>W przypadku wykonywania operacji przy użyciu runbooków jest obsługiwany tylko ręczny tryb powrotu po awarii. Oznacza to, że po rozpoczęciu powrotu po awarii przez wykonanie runbooka obejmującego krok Wykonaj powrót po awarii serwera procedura będzie wymagała ręcznych interakcji: trzeba będzie ręcznie odzyskać komputer, a następnie potwierdzić lub anulować proces powrotu po awarii na karcie Odzyskiwanie po awarii > Serwery.</p>
Uruchom serwer	<p>Uruchamia serwer chmurowy. Aby zdefiniować to działanie, musisz wybrać serwer chmurowy i skonfigurować dostępne w przypadku tej czynności parametry runbooka. Aby uzyskać więcej informacji na temat tych ustawień, zobacz sekcję "Parametry runbooka" (s. 95).</p> <p>Uwaga</p> <p>Czynność Uruchom serwer nie może być stosowana w przypadku operacji testowego przełączania awaryjnego w runbookach. Jeśli spróbujesz wykonać taką czynność, zakończy się ona niepowodzeniem z następującym komunikatem o błędzie: Niepowodzenie: Czynność nie ma zastosowania w bieżącym stanie serwera.</p>
Zatrzymaj serwer	<p>Zatrzymuje serwer chmurowy. Aby zdefiniować tę czynność, musisz wybrać serwer chmurowy i skonfigurować dostępne w przypadku tej czynności parametry runbooka. Aby uzyskać więcej informacji na temat tych ustawień, zobacz sekcję "Parametry runbooka" (s. 95).</p> <p>Uwaga</p> <p>Czynność Zatrzymaj serwer nie może być stosowana w przypadku operacji testowego przełączania awaryjnego w runbookach. Jeśli spróbujesz wykonać taką czynność, zakończy się ona niepowodzeniem z następującym komunikatem o błędzie: Niepowodzenie: Czynność nie ma zastosowania w bieżącym stanie serwera.</p>
Operacja ręczna	<p>Operacja ręczna wymaga działań ze strony użytkownika. Aby zdefiniować tę czynność, trzeba wprowadzić opis.</p>

Czynność	Opis
	Gdy sekwencja runbooka dojdzie do operacji ręcznej, runbook zostanie wstrzymany i nie będzie kontynuowany, dopóki użytkownik nie wykona wymaganej operacji ręcznej, na przykład nie kliknie przycisku potwierdzenia.
Wykonaj runbook	Powoduje wykonanie kolejnego runbooka. Aby zdefiniować tę czynność, musisz wybrać runbook. Runbook może zawierać tylko jedno wykonanie danego runbooka. Na przykład jeśli dodałeś czynność "wykonaj Runbook A", możesz dodać czynność "wykonaj Runbook B", ale nie możesz dodać kolejnej czynności "wykonaj Runbook A".

5. Zdefiniuj parametry runbooka na potrzeby danej czynności. Aby uzyskać więcej informacji na temat tych parametrów, zobacz sekcję "Parametry runbooka" (s. 95).
6. [Opcjonalnie] Aby dodać opis kroku:
 - a. Kliknij ikonę wielokropka, a następnie kliknij **Opis**.
 - b. Wprowadź opis kroku.
 - c. Kliknij **Gotowe**.
7. Powtarzaj kroki 3–6, dopóki nie utworzysz pożądanej sekwencji kroków i czynności.
8. [Opcjonalnie] Aby zmienić domyślną nazwę runbooka:
 - a. Kliknij ikonę wielokropka.
 - b. Wprowadź nazwę runbooka.
 - c. Wprowadź opis runbooka.
 - d. Kliknij **Gotowe**.
9. Kliknij **Zapisz**.
10. Kliknij **Zamknij**.

New runbook

...
Close
Save

Step 1

Add action

Failover server
recovery
Continue if already done

Add step

Action
Failover server

☒ Continue if already done
☐ Continue if failed

Server
- rec...

Completion check
☒ Ping IP address
10.0.3.35
☒ Connect to port
10.0.3.35: 443

Timeout in minutes
10

Parametry runbooka

Parametry runbooka to specyficzne ustawienia, które trzeba skonfigurować, aby zdefiniować działanie runbooka. Istnieją dwie kategorie parametrów runbooka — parametry czynności i parametry sprawdzania ukończenia.

Parametry czynności definiują zachowanie runbooka w zależności od początkowego stanu lub wyniku czynności.

Parametry sprawdzania ukończenia zapewniają, że serwer jest dostępny i świadczy niezbędne usługi. Jeśli sprawdzenie ukończenia się nie powiedzie, czynność jest uznawana za zakończoną niepowodzeniem.

W poniższej tabeli opisano konfigurowalne parametry runbooka dla każdej czynności.

Parametr runbooka	Kategoria	Dostępny na potrzeby czynności	Opis
Kontynuuj, jeśli już wykonano	Parametr czynności	<ul style="list-style-type: none"> Przełączenie awaryjne serwera Uruchom serwer Zatrzymaj serwer Wykonaj powrót po awarii serwera 	Ten parametr definiuje zachowanie runbooka, gdy żądana czynność jest już wykonana (na przykład przełączanie awaryjne zostało już przeprowadzone lub serwer już działa). Włączenie tego parametru oznacza, że runbook wyśle ostrzeżenie i będzie kontynuował działanie. Wyłączenie tego parametru oznacza, że czynność się nie powiedzie, a

Parametr runbooka	Kategoria	Dostępny na potrzeby czynności	Opis
			wówczas runbook również przestanie działać. Domyślnie ten parametr jest włączony.
Kontynuuj, jeśli czynność się nie powiodła	Parametr czynności	<ul style="list-style-type: none"> • Przełączenie awaryjne serwera • Uruchom serwer • Zatrzymaj serwer • Wykonaj powrót po awarii serwera 	Ten parametr definiuje zachowanie runbooka, gdy żądana czynność się nie powiedzie. Włączenie tego parametru oznacza, że runbook wyśle ostrzeżenie i będzie kontynuował czynność. Wyłączenie tego parametru oznacza, że czynność się nie powiedzie, a wówczas runbook również przestanie działać. Domyślnie ten parametr jest wyłączony.
Wysyłanie sondy ping na adres IP	Kontrola ukończenia	<ul style="list-style-type: none"> • Uruchom serwer 	Oprogramowanie będzie wysyłać sondę ping na produkcyjny adres IP serwera w chmurze, dopóki serwer nie odpowie lub nie zostanie przekroczony limit czasu, w zależności od tego, które z tych zdarzeń nastąpi jako pierwsze.
Połącz z portem (domyślnie 443)	Kontrola ukończenia	<ul style="list-style-type: none"> • Przełączenie awaryjne serwera • Uruchom serwer 	Oprogramowanie będzie próbować połączyć się z serwerem w chmurze, korzystając z produkcyjnego adresu IP oraz wskazanego portu, dopóki połączenie nie zostanie nawiązane lub nie zostanie przekroczony limit czasu, w zależności od tego, które z tych zdarzeń nastąpi jako pierwsze. W ten sposób możesz sprawdzić, czy aplikacja nasłuchująca dany port działa.
Limit czasu w minutach	Kontrola ukończenia	<ul style="list-style-type: none"> • Przełączenie awaryjne serwera • Uruchom serwer 	Domyślny limit czasu wynosi 10 minut.

Operacje przy użyciu runbooków

Uwaga

Dostępność tej funkcji zależy od limitów usług włączonych dla danego konta.

Aby uzyskać dostęp do listy operacji, najedź kursorem na runbook i kliknij ikonę wielokropka. Gdy runbook nie działa, dostępne są następujące operacje:

- **Wykonaj**
- **Edytuj**
- **Klonuj**
- **Usuń**

Wykonywanie runbooka

Za każdym razem gdy klikniesz **Wykonaj**, wyświetlona zostanie prośba o podanie parametrów wykonania. Parametry te będą zastosowane do wszystkich operacji przełączania awaryjnego i powrotu po awarii zawartych w runbooku. Runbooki wyszczególnione w operacjach **Wykonaj runbook** dziedziczą te parametry z głównego runbooka.

- **Tryb przełączania awaryjnego i powrotu po awarii**

Wybierz, czy chcesz wykonać testowe przełączanie awaryjne (domyślnie) czy prawdziwe (produkcyjne) przełączanie awaryjne. Tryb przywracania po awarii będzie powiązany z wybranym trybem przełączania awaryjnego.

- **Punkt odzyskiwania po awarii**

Wybierz ostatni punkt odzyskiwania (domyślnie) lub wybierz żądany punkt w przeszłości. W tym drugim przypadku dla każdego serwera zostaną wybrane punkty odzyskiwania stworzone najbliżej przed określoną datą i godziną.

Zatrzymywanie wykonywania runbooka

Podczas wykonywania runbooka możesz na liście operacji wybrać pozycję **Stop**. Oprogramowanie dokończy wszystkie rozpoczęte działania z wyjątkiem tych, które wymagają działania użytkownika.

Wyświetlanie historii wykonania

Gdy na karcie **Runbooki** wybierzesz runbooka, oprogramowanie wyświetli szczegóły na jego temat oraz historię wykonania. Kliknij wiersz odpowiadający konkretnemu wykonaniu, aby wyświetlić jego dziennik.

Runbooks

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.

Rb0 000

Execute

Edit

Clone

Delete

Details

Name

Rb0 000

Description

-

Execution history

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

Połączenie Open VPN site-to-site — dodatkowe informacje

Tworząc serwer odzyskiwania, konfiguruje się jego **Adres IP w sieci produkcyjnej** oraz jego **testowy adres IP**.

Po przeprowadzeniu przełączania awaryjnego (uruchomieniu maszyny wirtualnej w chmurze) i zalogowaniu się do maszyny wirtualnej w celu sprawdzenia adresu IP serwera pojawia się sekcja **Adres IP w sieci produkcyjnej**.

Po wykonaniu testowego przełączania awaryjnego komunikacja z serwerem testowym jest możliwa tylko wtedy, gdy się poda **Testowy adres IP**, który jest widoczny tylko w konfiguracji serwera odzyskiwania.

Aby uzyskać dostęp do serwera testowego z lokalizacji lokalnej, trzeba zastosować **Testowy adres IP**.

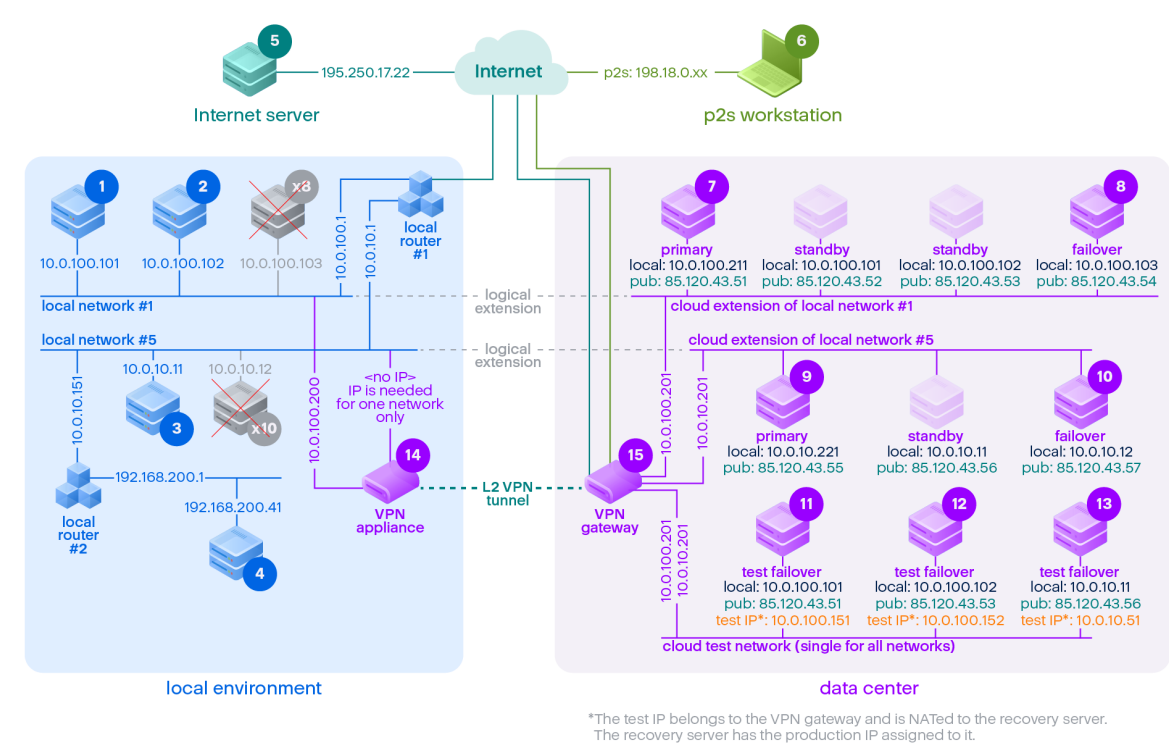
Uwaga

Konfiguracja sieci na serwerze zawsze zawiera **Adres IP w sieci produkcyjnej** (ponieważ serwer testowy odzwierciedla serwer produkcyjny). Jest tak, ponieważ testowy adres IP należy nie do serwera testowego, tylko do bramy VPN, i jest zmieniany na produkcyjny adres IP za pomocą translatora adresów sieciowych.

Poniższy diagram przedstawia przykładową konfigurację połączenia Open VPN site-to-site. Część serwerów znajdujących się w środowisku lokalnym jest odzyskiwanych w chmurze metodą przełączania awaryjnego (gdy infrastruktura sieci jest poprawna).

1. Klient włączył usługę Odzyskiwanie po awarii przez:
 - a. skonfigurowanie urządzenia VPN (14) i podłączenie go do specjalnego chmurowego serwera VPN (15)
 - b. objęcie wybranych serwerów lokalnych ochroną w ramach usługi Odzyskiwanie po awarii (1, 2, 3, x8 i x10)
Niektóre serwery w lokalizacji lokalnej (np. 4) są podłączone do sieci, które nie są podłączone do urządzenia VPN. Takie serwery nie są chronione przy użyciu usługi Odzyskiwanie po awarii.
2. Część tych serwerów (podłączonych do różnych sieci) działa w lokalizacji lokalnej: (1, 2, 3 i 4)
3. Chronione serwery (1, 2 i 3) są poddawane testom w ramach testowego przełączania awaryjnego (11, 12 i 13)
4. Niektóre serwery w lokalizacji lokalnej są niedostępne (x8, x10). Po przełączeniu awaryjnym stają się one dostępne w chmurze (8 i 10)

- Niektóre serwery podstawowe (7 i 9), połączone do różnych sieci, są dostępne w środowisku chmurowym
- (5) to serwer w Internecie z publicznym adresem IP
- (6) to stacja robocza połączona do chmury za pośrednictwem połączenia VPN point-to-site (p2s)



W tym przykładzie dostępna jest następująca konfiguracja połączenia (na przykład „ping”) od serwera w wierszu **Od:** do serwera w kolumnie **Do:**.

	Do:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
O		lokalny	lokalny	lokal	lokal	Inter	p2	podstaw	przełącz	podstaw	przełącz	testowe	testowe	testowe	urządze	serwe

	Do:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
d:				ny	ny	net	s	owe	anie awaryjne	owe	anie awaryjne	przełączanie awaryjne	przełączanie awaryjne	przełączanie awaryjne	nie VPN	r VPN
1	lokalny		bezpośrednio	przez router lokalny 1	przez router lokalny 2	przez router lokalny 1 i Internet	nie	przez tunel: lokalny przez router lokalny 1 i Internet: publiczny	przez tunel: lokalny przez router lokalny 1 i Internet: publiczny	przez tunel: lokalny przez router lokalny 1 i Internet: publiczny	przez tunel: lokalny przez router lokalny 1 i Internet: publiczny	przez tunel: NAT (serwer VPN) przez router lokalny 1 i Internet: publiczny	przez tunel: NAT (serwer VPN) przez router lokalny 1 i Internet: publiczny	przez router lokalny 1 i tunel: NAT (serwer VPN) przez router lokalny 1 i Internet: publiczny	bezpośrednio	nie
2	lokalny	bezpośrednio		przez router lokalny 1	przez router lokalny 2	przez router lokalny 1 i Internet	nie	przez tunel: lokalny przez router	przez tunel: lokalny przez router	przez tunel: lokalny przez router	przez tunel: lokalny przez router	przez tunel: NAT (serwer VPN)	przez tunel: NAT (serwer VPN)	przez router lokalny 1 i tunel: NAT	bezpośrednio	nie

	Do:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
						net		lokalny 1 i Internet: publiczny	lokalny 1 i Internet: publiczny	lokalny 1 i Internet: publiczny	lokalny 1 i Internet: publiczny	przez router lokalny 1 i Internet: publiczny	przez router lokalny 1 i Internet: publiczny	(serwer VPN) przez router lokalny 1 i Internet: publiczny		
3	lokalny	przez router lokalny 1	przez router lokalny 1		przez router lokalny 2	przez router lokalny 1 i Internet	nie	przez tunel: lokalny przez router lokalny 1 i Internet: publiczny	przez tunel: lokalny przez router lokalny 1 i Internet: publiczny	przez tunel: lokalny przez router lokalny 1 i Internet: publiczny	przez tunel: lokalny przez router lokalny 1 i Internet: publiczny	przez tunel: NAT (serwer VPN) przez router lokalny 1 i Internet: publiczny	przez tunel: NAT (serwer VPN) przez router lokalny 1 i Internet: publiczny	przez router lokalny 1 i tunel: NAT (serwer VPN) przez router lokalny 1 i Internet: publiczny	przez router lokalny	nie

	Do:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
4	lokalny	przez router lokalny 2 i router 1	przez router lokalny 2 i router 1	przez router lokalny 2		przez router lokalny 2, router 1 i Internet	nie	przez router lokalny 2 i tunel: lokalny przez router lokalny 2, router lokalny 1 i Internet: publiczny	przez router lokalny 2 i tunel: lokalny przez router lokalny 2, router lokalny 1 i Internet: publiczny	przez router lokalny 2 i tunel: lokalny przez router lokalny 2, router lokalny 1 i Internet: publiczny	przez router lokalny 2 i tunel: lokalny przez router lokalny 2, router lokalny 1 i Internet: publiczny	przez tunel: NAT (serwer VPN) przez router lokalny 2, router 1 i Internet: publiczny	przez tunel: NAT (serwer VPN) przez router lokalny 2, router 1 i Internet: publiczny	przez tunel: NAT (serwer VPN) przez router lokalny 2, router 1 i Internet: publiczny	przez router lokalny 2	nie
5	Internet	nie	nie	nie	nie		n/d	przez Internet: publiczny	przez Internet: publiczny	przez Internet: publiczny	przez Internet: publiczny	przez Internet: publiczny	przez Internet: publiczny	przez Internet: publiczny	nie	nie
6	p2s	nie	nie	nie	nie	przez Internet		przez VPN p2s (serwer VPN); lokalny przez	przez VPN p2s (serwer VPN); lokalny przez	przez VPN p2s (serwer VPN); lokalny przez	przez VPN p2s (serwer VPN); lokalny przez	przez VPN p2s — NAT (serwer VPN) przez	przez VPN p2s — NAT (serwer VPN) przez	przez VPN p2s — NAT (serwer VPN) przez	nie	nie

	Do:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								Internet: publiczn y	Internet: publiczn y	Internet: publiczn y	Internet: publiczn y	Internet: publiczn y	Internet: publiczn y	przez Interne t: publiczn y		
7	podsta wowe	przez tunel	przez tunel	prze z tune li rout er lokal ny 1	prze z tune li rout er lokal ny 1 oraz 2	przez Inter net (prze z serw er VPN)	ni e		bezpośr ednio w chmurz e: lokalny	przez tunel i router lokalny 1: lokalny	przez tunel i router lokalny 1: lokalny	przez serwer VPN: NAT	przez serwer VPN: NAT	przez tunel i router lokalny 1: NAT	nie	Tylko proto koły DHCP i DNS
8	przełąc zanie awaryjn e	przez tunel	przez tunel	prze z tune li rout er lokal ny 1	prze z tune li rout er lokal ny 1 oraz 2	przez Inter net (prze z serw er VPN)	ni e	bezpośr ednio w chmurz e: lokalny		przez tunel i router lokalny 1: lokalny	przez tunel i router lokalny 1: lokalny	przez serwer VPN: NAT	przez serwer VPN: NAT	przez tunel i router lokalny 1: NAT	nie	Tylko proto koły DHCP i DNS
9	podsta	przez	przez	prze	prze	przez	ni	przez	przez		bezpośr	przez	przez	przez	nie	Tylko

	Do:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	wowe	tunel i router lokalny 1	tunel i router lokalny 1	z tune l	z tune l	Inter net (prze z serw er VPN)	e	tunel i router lokalny 1: lokalny	tunel i router lokalny 1: lokalny		ednio w chmurz e: lokalny	tunel i router lokalny 1: NAT	tunel i router lokalny 1: NAT	serwer VPN: NAT		proto koły DHCP i DNS
10	przełącz anie awaryjn e	przez tunel i router lokalny 1	przez tunel i router lokalny 1	prze z tune l	prze z tune l	przez Inter net (prze z serw er VPN)	ni e	przez tunel i router lokalny 1: lokalny	przez tunel i router lokalny 1: lokalny	bezpośr ednio w chmurz e: lokalny		przez tunel i router lokalny 1: NAT	przez tunel i router lokalny 1: NAT	przez serwer VPN: NAT	nie	Tylko proto koły DHCP i DNS
11	testuj przełącz anie awaryjn e	nie	nie	nie	nie	przez Inter net (prze z serw er VPN)	ni e	nie	nie	nie	nie		bezpośr ednio w chmurz e: lokalny	przez serwer VPN: lokalny (routin g)	nie	Tylko proto koły DHCP i DNS
12	testuj przełącz anie	nie	nie	nie	nie	przez Inter net	ni e	nie	nie	nie	nie	bezpośr ednio w chmurz		przez serwer VPN:	nie	Tylko proto koły

	Do:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	awaryjne					(przez serwer VPN)						e: lokalny		lokalny (routing)		DHCP i DNS
13	testuj przełączenie awaryjne	nie	nie	nie	nie	przez Internet (przez serwer VPN)	nie	nie	nie	nie	nie	przez serwer VPN: lokalny (routing)	przez serwer VPN: lokalny (routing)		nie	Tylko protokoły DHCP i DNS
14	urządzenie VPN	bezpośrednio	bezpośrednio	przez router lokalny 1	przez router lokalny 2	przez Internet (router lokalny 1)	nie	nie	nie	nie	nie	nie	nie	nie		nie
15	serwer VPN	nie	nie	nie	nie	nie	nie	nie	nie	nie	nie	nie	nie	nie	nie	

Słownik

B

Brama VPN (dawniej nazywana serwerem VPN lub bramą łączności)

Specjalna maszyna wirtualna zapewniająca połączenie między lokalizacją lokalną a lokalizacją w chmurze przez bezpieczny tunel VPN. Brama VPN jest wdrażana w lokalizacji w chmurze.

C

Chroniony serwer

Komputer fizyczny lub maszyna wirtualna klienta objęte ochroną przez usługę.

D

Docelowy punkt odzyskiwania (RPO)

Ilość danych utraconych w wyniku przestoju mierzona ilością czasu, który upłynął od zaplanowanego przestoju lub awarii. Próg RPO określa maksymalny dozwolony odstęp czasu między ostatnim punktem odzyskiwania nadającym się do wykorzystania w celu przełączenia awaryjnego a czasem bieżącym.

F

Finalizacja

Stan pośredni w procesie przełączania awaryjnego ze środowiska produkcyjnego lub odzyskiwania serwera chmurowego. Proces ten polega na przeniesieniu dysków wirtualnych serwera z magazynu kopii zapasowych do magazynu odzyskiwania po awarii. Podczas finalizacji serwer jest dostępny i wykonuje wszystkie operacje, ale jego wydajność jest niższa niż zwykle.

L

Lokalizacja lokalna

Lokalna infrastruktura zainstalowana w obiekcie danej firmy.

Lokalizacja w chmurze (lub lokalizacja odzyskiwania po awarii)

Lokalizacja zdalna w chmurze używana do obsługi infrastruktury odzyskiwania w razie wystąpienia awarii.

P

Połączenie point-to-site (P2S)

Bezpieczne połączenie VPN z zewnątrz do lokalizacji w chmurze i lokalizacji lokalnej nawiązywane z urządzeń końcowych (np. komputera stacjonarnego lub laptopa).

Połączenie site-to-site (S2S)

Połączenie rozszerzające sieć lokalną o chmurę przy użyciu bezpiecznego tunelu VPN.

Powrót po awarii

Proces przywracania serwerów do lokalizacji lokalnej po przeniesieniu ich do lokalizacji w chmurze wskutek awarii.

Przełączanie awaryjne

Przełączenie obciążenia lub aplikacji do lokalizacji w chmurze w razie katastrofy naturalnej lub poważnych szkód spowodowanych przez człowieka w lokalizacji lokalnej.

Publiczny adres IP

Adres IP przypisywany serwerowi chmurowemu, aby był on dostępny z Internetu.

R

Runbook

Planowany scenariusz obejmujący konfigurowalne czynności automatyzujące operacje związane z odzyskiwaniem po awarii.

S

Serwer chmurowy

Ogólne pojęcie oznaczające serwer odzyskiwania lub serwer podstawowy.

Serwer odzyskiwania

Replika oryginalnego komputera utworzona w formie maszyny wirtualnej na podstawie przechowywanych w chmurze kopii zapasowych chronionego serwera. Serwery odzyskiwania służą do przełączania obciążeń z oryginalnych serwerów w razie wystąpienia awarii.

Serwer podstawowy

Maszyna wirtualna, z którą nie jest powiązana żadna maszyna w lokalizacji lokalnej (np. serwer odzyskiwania). Serwery podstawowe służą do ochrony aplikacji lub obsługi różnych usług pomocniczych (np. serwera internetowego).

Sieć produkcyjna

Sieć wewnętrzna rozszerzona przy użyciu tunelowania VPN i obejmująca zarówno lokalizację lokalną, jak i lokalizację w chmurze. Serwery lokalne i chmurowe mogą

komunikować się ze sobą w ramach sieci produkcyjnej.

Sieć testowa

Odizolowana sieć wirtualna służąca do testowania przełączania awaryjnego.

T

Testowy adres IP

Adres IP potrzebny do testów przełączania awaryjnego, aby zapobiec zdublowaniu adresu IP ze środowiska produkcyjnego.

U

Urządzenie VPN

Specjalna maszyna wirtualna umożliwiająca połączenie między siecią lokalną a lokalizacją w chmurze przez bezpieczny tunel VPN. Urządzenie VPN jest wdrażane w lokalizacji lokalnej.

Indeks

A

Aktywne połączenia point-to-site 50

Automatyczne testowe przełączanie awaryjne 61, 64

Automatyczne usuwanie nieużywanych środowisk klientów w lokalizacji w chmurze 28

B

Brama VPN 22, 27

C

Co dalej 15

Cyber Disaster Recovery Cloud — informacje 5

D

Dlaczego warto korzystać z runbooków? 92

Dostęp VPN do lokalizacji lokalnej 49

Działania na serwerze podstawowym 84

E

Edytowanie domyślnych parametrów serwera odzyskiwania 15

I

Infrastruktura sieci w chmurze 16

J

Jak działa routing 19, 22, 27

Jak wykonać przełączenie awaryjne serwera DHCP 68

Jak wykonać przełączenie awaryjne serwerów korzystających z lokalnego serwera DNS 68

K

Kompatybilność modułu Odzyskiwanie po awarii z programami szyfrującymi 11

Konfiguracja sieci bramy VPN 22

Konfigurowanie automatycznego testowego przełączania awaryjnego 65

Konfigurowanie łączności 18

Konfigurowanie niestandardowych serwerów DNS 46

Konfigurowanie połączenia IPsec VPN multi-site 31

Konfigurowanie połączenia Open VPN site-to-site 29-30

Konfigurowanie routingu lokalnego 48

Konfigurowanie serwerów odzyskiwania 57

Konfigurowanie serwerów podstawowych 82

Konfigurowanie trybu Tylko chmura 29

Konfigurowanie ustawień połączenia IPsec VPN multi-site 32

Konfigurowanie zdalnego dostępu VPN point-to-site 37

Kontroler domeny usługi Active Directory na potrzeby łączności L2 Open VPN 37

Kontroler domeny usługi Active Directory na potrzeby łączności L3 IPsec VPN 37

N

Najważniejsze funkcje 5

O

Obsługiwane platformy wirtualizacji 6
Obsługiwane systemy operacyjne 6
Ogólne zalecenia dotyczące lokalizacji lokalnych 33
Ograniczenia 7
Ograniczenia w przypadku korzystania z magazynu Geo-redundant Cloud Storage 10
Operacje dotyczące maszyn wirtualnych Microsoft Azure 80
Operacje przy użyciu runbooków 96
Orkiestracja (runbooki) 92

P

Parametry runbooka 95
Pliki dziennika IPsec VPN multi-site 55
Pobieranie adresów MAC 47
Pobieranie dzienników bramy VPN 51
Pobieranie dzienników urządzenia VPN 51
Pobieranie plików dziennika IPsec VPN 55
Pobierz konfigurację dla pakietu OpenVPN 49
Początkowa konfiguracja łączności 29
Pojęcia dotyczące sieci 18
Połączenie IPsec VPN multi-site 26
Połączenie Open VPN site-to-site 20, 39
Połączenie Open VPN site-to-site — dodatkowe informacje 99
Ponowne generowanie konfiguracji 49
Ponowne instalowanie bramy VPN 43
Porty 30

Powrót po awarii na docelową maszynę wirtualną 69

Powrót po awarii na docelowy komputer fizyczny 74

Praca z dziennikami 50

Praca z zaszyfrowanymi kopiami zapasowymi 80

Produkcyjne przełączanie awaryjne 60

Przebieg powrotu po awarii 69

Przebieg przełączania awaryjnego 60

Przechwytywanie pakietów sieciowych 52

Publiczny i testowy adres IP 23

Punkty obliczeniowe 12

R

Reguły zapory dotyczące serwerów chmurowych 87

Ręczny powrót po awarii 78

Rozwiązywanie napotkanych problemów z konfiguracją IPsec VPN 53

Rozwiązywanie problemów z konfiguracją IPsec VPN 52

S

Serwery odzyskiwania 23

Serwery podstawowe 25

Sprawdzanie działań dotyczących zapory chmury 90

T

Testuj przełączenie awaryjne 61

Tryb Tylko chmura 19, 40

Tworzenie kopii zapasowych serwerów chmurowych 91

Tworzenie planu ochrony na potrzeby odzyskiwania po awarii 14

Tworzenie runbooka 92

Tworzenie serwera odzyskiwania 57

Tworzenie serwera podstawowego 82

U

Urządzenie VPN 23

Ustawianie reguł zapory dla serwerów chmurowych 87

Ustawienia zabezpieczeń IPsec/IKE 34

Usuwanie niestandardowych serwerów DNS 47

W

Wersja próbna rozwiązania Cyber Disaster Recovery Cloud 9

Włączanie i wyłączanie połączenia site-to-site 43

Wykonywanie powrotu po awarii na komputer fizyczny 76

Wykonywanie powrotu po awarii na maszynę wirtualną 71

Wykonywanie przełączenia awaryjnego 66

Wykonywanie ręcznego powrotu po awarii 79

Wykonywanie runbooka 97

Wykonywanie testowego przełączenia awaryjnego 61

Wyłączanie automatycznego testowego przełączania awaryjnego 65

Wymagania dotyczące oprogramowania 6

Wymagania systemowe 29

Wymagania urządzenia VPN 29

Wymagania wstępne 32, 38, 43, 46-48, 55, 57,

71, 76, 82

Wyświetlanie historii wykonania 97

Wyświetlanie statusu automatycznego testowego przełączania awaryjnego 65

Z

Zalecenia dotyczące dostępności usług Active Directory Domain Services 37

Zarządzanie serwerami chmurowymi 85

Zarządzanie sieciami 38-39

Zarządzanie ustawieniami połączenia point-to-site 49

Zarządzanie ustawieniami urządzenia VPN 42

Zatrzymywanie wykonywania runbooka 97

Zdalny dostęp VPN point-to-site 27

Zezwalanie na ruch DHCP przez połączenie L2 VPN 48

Zmienianie konfiguracji adresu IP 41

Zmienianie przypisania adresów IP 45

Zmienianie typu łączności na site-to-site 44