Cyber Disaster Recovery Cloud

24.03

Anleitung für Administratoren

REVISION: 11.04.2024

Inhaltsverzeichnis

Über Cyber Disaster Recovery Cloud

Cyber Disaster Recovery Cloud (DR) – ein Bestandteil von Cyber Protection, der eine DRaaS-Funktionalität (Disaster Recovery as a Service) bereitstellt. Cyber Disaster Recovery Cloud bietet Ihnen eine schnelle und stabile Lösung, um exakte Kopien Ihrer Maschinen auf einer Cloud-Site zu starten und so Workloads von beschädigten Maschinen zu Recovery-Servern in der Cloud umschalten zu können, falls es zu einem Desaster kommt (egal ob von von Menschen verursacht oder natürlichen Ursprungs).

Sie können die Disaster Recovery-Funktionalität auf folgende Arten einrichten und konfigurieren:

- Erstellen Sie einen Schutzplan, der das Disaster Recovery-Modul enthält, und wenden Sie den Plan auf Ihre Geräte an. Dadurch wird automatisch eine Standard-Disaster-Recovery-Infrastruktur eingerichtet. Siehe auch den Abschnitt 'Einen Disaster Recovery-Schutzplan erstellen'.
- Richten Sie die Disaster Recovery Cloud-Infrastruktur manuell ein, wenn Sie jeden Schritt kontrollieren wollen. Siehe '"Recovery-Server einrichten" (S. 59)'.

Die Kernfunktionalität

Hinweis
In Abhängigkeit davon, welches Lizenzierungsmodell angewendet wird, kann für einige Funktionen eine zusätzliche Lizenzierung erforderlich sein.

- Verwalten Sie den Cyber Disaster Recovery Cloud Service über eine einzelne, zentrale Konsole
- Erweitern Sie bis zu 23 lokale Netzwerke über einen sicheren VPN-Tunnel in die Cloud
- Bauen Sie eine Verbindung zur Cloud-Site auf, ohne dass eine VPN-Appliance[1]-Bereitstellung notwendig ist ('Nur Cloud'-Modus)
- Bauen Sie eine Point-to-Site-Verbindung zur Ihrem lokalen Standort und zur Cloud-Site auf
- Schützen Sie Ihre Maschinen, indem Sie Recovery-Server in der Cloud verwenden
- Schützen Sie Applikationen und Appliances, indem Sie primäre Servern in der Cloud verwenden
- Führen Sie automatische Disaster Recovery-Aktionen für verschlüsselte Backups durch
- Führen Sie einen Test-Failover in einem isolierten Netzwerk aus
- Verwenden Sie Runbooks, um die Produktionsumgebung in die Cloud zu übertragen

[1] Eine spezielle virtuelle Maschine, die eine Verbindung (über einen sicheren VPN-Tunnel) zwischen dem lokalen Netzwerk und der Cloud-Site ermöglicht. Die VPN-Appliance wird am lokalen Standort bereitgestellt.

Software-Anforderungen

Unterstützte Betriebssysteme

Der Schutz mit einem Recovery-Server wurde mit folgenden Betriebssystemen getestet:

- 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 – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows Server 2019 – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows Server 2022 – alle Installationsoptionen, mit Ausnahme des Nano Servers

Eine korrekte Funktion der Software mit anderen Windows-Betriebssystemen und Linux-Distributionen ist möglich, wird jedoch nicht garantiert.

Hinweis
Der Schutz mit einem Recovery-Server wurde für Microsoft Azure-VMs mit den nachfolgenden Betriebssystemen getestet.

- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows Server 2019 – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows Server 2022 – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Ubuntu Server 20.04 LTS - Gen2 (Canonical). Weitere Informationen über den Zugriff auf die Recovery-Server-Konsole finden Sie unter https://kb.acronis.com/content/71616.

Unterstützte Virtualisierungsplattformen

Der Schutz von virtuellen Maschinen mit einem Recovery-Server wurde mit folgenden Virtualisierungsplattformen getestet:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7, 7.0
- Windows Server 2008 R2 mit Hyper-V
- Windows Server 2012/2012 R2 mit Hyper-V

- Windows Server 2016 mit Hyper-V – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows Server 2019 mit Hyper-V – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows Server 2022 mit Hyper-V – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- Kernel-based Virtual Machines (KVM) – nur vollständig virtualisierte Gäste (HVM). Paravirtualisierte Gäste (PV) werden nicht unterstützt.
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2

Die VPN-Appliance wurde mit folgenden Virtualisierungsplattformen getestet:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- Windows Server 2008 R2 mit Hyper-V
- Windows Server 2012/2012 R2 mit Hyper-V
- Windows Server 2016 mit Hyper-V – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows Server 2019 mit Hyper-V – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Windows Server 2022 mit Hyper-V – alle Installationsoptionen, mit Ausnahme des Nano Servers
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016

Eine korrekte Funktion der Software mit anderen Virtualisierungsplattformen und Versionen ist möglich, wird jedoch nicht garantiert.

Einschränkungen

Folgende Plattformen und Konfigurationen werden in Cyber Disaster Recovery Cloud nicht unterstützt:

1. Nicht unterstützte Plattformen:
   - Agenten für Virtuozzo
   - macOS
   - Windows-Desktop-Betriebssysteme werden aufgrund von Microsoft-Produktbedingungen nicht unterstützt.
   - Windows Server Azure Edition

     Die Azure Edition ist eine besondere Version des Windows Servers, die speziell dafür entwickelt wurde, entweder als virtuelle Maschine (VM) in Azure IaaS oder als VM auf einem Azure Stack HCI-Cluster zu laufen. Im Gegensatz zur Standard Edition und der Datacenter Edition ist die Azure Edition nicht für den Betrieb auf farbrikneuer physischer Hardware (Bare-

Metal-Hardware), Windows Client Hyper-V, Windows Server Hyper-V, Drittanbieter-Hypervisoren oder in Drittanbieter-Clouds lizenziert.

2. Nicht unterstützte Konfigurationen:

   Microsoft Windows

   - Dynamische Laufwerke werden nicht unterstützt
   - Windows-Desktop-Betriebssysteme werden (aufgrund von Microsoft-Produktbedingungen) nicht unterstützt
   - Der Active Directory Service mit FRS-Replikation wird nicht unterstützt
   - Wechselmedien ohne GPT- oder MBR-Formatierung (auch „Superfloppy“ genannt) werden nicht unterstützt

   Linux

   - Dateisysteme ohne Partitionstabelle
   - Linux-Workloads, die mit einem Agenten von einem Gastbetriebssystem aus gesichert werden und über Volumes mit folgenden erweiterten LVM-Konfigurationen (Logical Volume Manager) verfügen: Stripeset-Volumes, gespiegelte Volumes sowie Volumes mit RAID 0, RAID 4, RAID 5, RAID 6 oder RAID 10.

   Hinweis
   Workloads, die mehrere Betriebssysteme installiert haben, werden nicht unterstützt.

3. Nicht unterstützte Backup-Typen:
   - Recovery-Punkte aus einer kontinuierlichen Datensicherung (CDP) sind nicht kompatibel.

     Wichtig
     Wenn Sie einen Recovery-Server aus einem Backup mit einem CDP-Recovery-Punkt erstellt haben, werden Sie während des Failbacks – oder wenn Sie ein Backup eines Recovery-Servers erstellen – die im CDP-Recovery-Punkt enthaltenen Daten verlieren.

   - Forensik-Backups können nicht verwendet werden, um Recovery-Server zu erstellen.

Ein Recovery-Server hat eine Netzwerkschnittstelle. Wenn die ursprüngliche mehrere Netzwerkschnittstellen hat, wird nur eine davon emuliert.

Cloud-Server werden nicht verschlüsselt.

Cyber Disaster Recovery Cloud-Testversion

Sie können eine Testversion von Acronis Cyber Disaster Recovery Cloud für einen Zeitraum von 30 Tagen verwenden. In diesem Fall unterliegt die Disaster Recovery-Funktionalität für die Partner-Mandanten folgende Einschränkungen:

- Kein Zugriff auf das öffentliche Internet für primäre Server und Recovery-Server. Sie können den Servern keine öffentlichen IP-Adressen zuweisen.
- Multi-Site-IPsec-VPN ist nicht verfügbar.

Einschränkungen bei der Verwendung des Geo-redundant Cloud Storage

Der Geo-redundant Cloud Storage stellt Ihnen einen zweiten Speicherort für Ihre Backup-Daten zur Verfügung. Der sekundäre Speicherort befindet sich in einer Region, die geografisch vom primären Speicherort entfernt liegt. Durch die geografische Trennung der Regionen wird sichergestellt, dass eine der beiden Regionen jeweils nicht in Mitleidenschaft gezogen wird, wenn der jeweils andere Standort von einem Desaster (wie einer Naturkatastrophe) heimgesucht wird und die entsprechenden Backup-Daten nicht wiederhergestellt werden können. Dank dieser Maßnahme kann der Geschäftsbetrieb dennoch weitergeführt werden.

Wichtig
Der Disaster Recovery Service wird nicht unterstützt, wenn der Backup Storage vom primären Standort zum georedundanten sekundären Standort umgestellt wird.

Disaster Recovery-Kompatibilität mit Verschlüsselungsprogrammen

Die Disaster Recovery-Funktionalität ist mit folgenden laufwerksbasierten Verschlüsselungsprogrammen kompatibel:

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

Hinweis

- Bei Laufwerken mit einer Verschlüsselung auf Festplattenebene empfehlen wir Ihnen, dass Sie den Protection Agent im Gastbetriebssystem des Workloads installieren und agentenbasierte Backups durchführen.
- Für agentenlose Backups von verschlüsselten Workloads werden keine Failover- und Failback-Aktionen unterstützt.

Weitere Informationen über die Kompatibilität mit anderen Verschlüssungsprogrammen finden Sie in der Cyber Protection-Benutzeranleitung.

Berechnungspunkte

Bei Disaster Recovery werden Berechnungspunkte für primäre Server und Recovery-Server bei Test-Failovers und Produktions-Failovers verwendet. Berechnungspunkte spiegeln diejenigen Compute-Ressourcen wider, die für die Ausführung der Server (virtuelle Maschinen) in der Cloud eingesetzt werden.

Der Verbrauch von Berechnungspunkten bei Disaster Recovery-Prozessen hängt von den Parametern des Servers und der Dauer des Zeitraums ab, während dessen sich der Server im Failover-Stadium befindet. Je leistungsfähiger der Server und je länger dieser Zeitraum ist, desto mehr Berechnungspunkte werden verbraucht. Und je mehr Berechnungspunkte verbraucht werden, desto höher ist der Preis, der Ihnen berechnet wird.

Alle Server, die in der Acronis Cloud laufen, werden nach Compute-Punkten berechnet, abhängig von ihrer konfigurierten Ausführung, unabhängig von ihrem Zustand (eingeschaltet oder ausgeschaltet).

Wiederherstellungsserver im Standby-Zustand verbrauchen keine Rechenpunkte und es werden keine Gebühren für Rechenpunkte berechnet.

In der untenstehenden Tabelle sehen Sie ein Beispiel für acht Server in der Cloud mit verschiedenen Ausführungen und die entsprechenden Rechenpunkte, die sie pro Stunde verbrauchen werden. Sie können die Ausführungen der Server im **Details** Tab ändern.

Typ	CPU	RAM	Berechnungspunkte
V1	1 vCPU	2 GB	1
V2	1 vCPU	4 GB	2
V3	2 vCPU	8 GB	4
V4	4 vCPU	16 GB	8
V5	8 vCPU	32 GB	16
V6	16 vCPU	64 GB	32
V7	16 vCPU	128 GB	64
V8	16 vCPU	256 GB	128

Anhand der Informationen in der Tabelle können Sie leicht einschätzen, wie viele Berechnungspunkte ein Server (eine virtuelle Maschine) verbrauchen wird.

Wenn Sie beispielsweise eine virtuelle Maschine mit 4 vCPU* und 16 GB RAM sowie eine virtuelle Maschine mit 2 vCPU und 8 GB RAM per Disaster Recovery schützen wollen, wird die erste virtuelle Maschine 8 Berechnungspunkte pro Stunde verbrauchen und die zweite virtuelle Maschine 4 Berechnungspunkte pro Stunde. Wenn sich beide virtuellen Maschinen im Failover-Stadium befinden, ergibt sich ein Gesamtverbrauch von 12 Berechnungspunkten pro Stunde – oder 288

Berechnungspunkten für den gesamten Tag (12 Berechnungspunkte x 24 Stunden = 288 Berechnungspunkte).

*Eine vCPU bezieht sich auf einen physischen Zentralprozessor (CPU), der einer virtuellen Maschine zugewiesen wurde, und zudem eine zeitabhängige Einheit ist.

Hinweis
Wenn das Limit für die Quota der **Berechnungspunkte** überschritten wird, werden alle primären und Recovery-Server heruntergefahren. Es wird nicht möglich sein, diese Server zu nutzen, bis der nächste Abrechnungszeitraum beginnt oder bis Sie die Quota erhöhen. Der Standardabrechnungszeitraum ist ein voller Kalendermonat.

Einen Disaster Recovery-Schutzplan erstellen

Erstellen Sie einen Schutzplan, der das Disaster Recovery-Modul enthält, und wenden Sie den Plan auf Ihre Geräte an.

Wenn ein neuer Schutzplan erstellt wird, ist das Disaster Recovery-Modul standardmäßig deaktiviert. Wenn Sie die Disaster Recovery-Funktionalität aktivieren und den Plan auf Ihre Geräte anwenden, wird die Cloud-Netzwerkinfrastruktur erstellt – einschließlich eines *Recovery-Servers* für jedes geschütztes Gerät. Ein solcher *Recovery-Server* ist eine virtuelle Maschine in der Cloud, bei der es sich um eine Kopie des ausgewählten Gerätes handelt. Für jedes der ausgewählten Geräte wird ein Recovery-Server mit Standardeinstellungen im Standby-Stadium erstellt (die virtuelle Maschine wird also nicht ausgeführt). Die Größe des Recovery-Servers wird automatisch in Abhängigkeit von der CPU und dem Arbeitsspeicher des geschützten Gerätes festgelegt. Die Standard-Cloud-Netzwerk-Infrastruktur wird ebenfalls automatisch erstellt: das VPN-Gateway und die Netzwerke auf der Cloud-Site, mit denen die Recovery-Server verbunden sind.

Wenn Sie das Disaster Recovery-Modul eines Schutzplanes widerrufen, löschen oder ausschalten, werden die Recovery-Server und Cloud-Netzwerke nicht automatisch gelöscht. Sie können die Disaster Recovery-Infrastruktur bei Bedarf aber manuell entfernen.

Hinweis

- Nachdem Sie die Disaster Recovery-Funktionalität konfiguriert haben, können Sie einen Test- oder Produktions-Failover von jedem Recovery-Punkt aus durchführen, der zu einem Zeitpunkt generiert wurde, nachdem der Recovery-Server für das entsprechende Gerät erstellt wurde. Recovery-Punkte, die generiert wurden, bevor das Gerät per Disaster Recovery geschützt wurde (z.B. bevor der Recovery-Server erstellt wurde), können nicht für ein Failover verwendet werden.
- Ein Disaster Recovery-Schutzplan kann nicht aktiviert werden, wenn die IP-Adresse eines Geräts nicht ermittelt werden kann. Beispielsweise, wenn virtuelle Maschinen agentenlos gesichert werden und ihnen keine IP-Adresse zugewiesen wurde.
- Wenn Sie einen Schutzplan anwenden, werden die gleichen Netzwerke und IP-Adressen in der Cloud-Site zugewiesen. Die IPsec-VPN-Konnektivität setzt voraus, dass sich die Netzwerksegmente der Cloud und der lokalen Standorte nicht überlappen. Wenn eine Multi-Site-IPsec-VPN-Konnektivität konfiguriert wurde und Sie später einen Schutzplan auf ein oder mehrere Geräte anwenden wollen, müssen Sie zusätzlich die Cloud-Netzwerke aktualisieren und die IP-Adressen der Cloud Server neu zuweisen. Weitere Informationen finden Sie im Abschnitt '"IP-Adressen neu zuweisen" (S. 47)'.

So können Sie einen Disaster Recovery-Schutzplan erstellen

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie die Maschinen aus, die Sie sichern wollen.
3. Klicken Sie zuerst auf **Schützen** und dann auf **Plan erstellen**.
   Daraufhin werden die Standardeinstellungen des Schutzplans geöffnet.
4. Konfigurieren Sie die Backup-Optionen.

Wenn Sie die Disaster Recovery-Funktionalität verwenden wollen, muss der Plan die komplette Maschine in den Cloud Storage sichern – oder zumindest diejenigen Laufwerke, die zum Booten und zur Bereitstellung notwendiger Services erforderlich sind.

5. Aktivieren Sie das Disaster Recovery-Modul, indem Sie auf den Schalter neben dem Namen des Moduls klicken.
6. Klicken Sie auf **Erstellen**.
   Der Plan wird erstellt und auf die ausgewählten Maschinen angewendet.

Was ist als nächstes zu tun?

- Sie können die Standardkonfiguration des Recovery-Servers bearbeiten. Weitere Informationen finden Sie im Abschnitt '"Recovery-Server einrichten" (S. 59)'.
- Sie können die Standardnetzwerkkonfiguration bearbeiten. Weitere Informationen finden Sie im Abschnitt '"Verbindungen einrichten" (S. 18)'.
- Sie können mehr über die Standardparameter für die Recovery-Server und die Cloud-Netzwerkinfrastruktur erfahren. Weitere Informationen dazu finden Sie in den Abschnitten '"Die Standardparameter für Recovery-Server bearbeiten" (S. 15)' und '"Cloud-Netzwerk-Infrastruktur" (S. 17)'.

Die Standardparameter für Recovery-Server bearbeiten

Wenn Sie einen Disaster Recovery-Schutzplan erstellen und anwenden, wird ein Recovery-Server mit Standardparametern konfiguriert. Sie können diese Standardparameter auch später noch bearbeiten.

Hinweis
Ein Recovery-Server wird nur dann neu erstellt, wenn er noch nicht vorhanden ist. Bereits vorhandene Recovery-Server werden weder verändert noch neu erstellt.

So können Sie die Standardparameter für Recovery-Server bearbeiten

1. Gehen Sie zu **Geräte** –> **Alle Geräte**.
2. Wählen Sie ein Gerät aus und klicken Sie auf **Disaster Recovery**.
3. Bearbeiten Sie die Standardparameter für Recovery-Server.
   Die Recovery-Server-Parameter werden in der nachfolgenden Tabelle beschrieben.

Recovery-Server Parameter	Standard Wert	Beschreibung
CPU und RAM	auto	Die Anzahl der virtuellen CPUs und die Menge an Arbeitsspeicher (RAM) für den Recovery-Server. Die Standardeinstellungen werden automatisch auf der Grundlage der ursprünglichen Geräte-CPU- und RAM-

		Konfiguration festgelegt.
Cloud-Netzwerk	auto	Das Cloud-Netzwerk, mit dem der Server verbunden sein wird. Weitere Informationen zur Konfiguration von Cloud-Netzwerken finden Sie im Abschnitt Cloud-Netzwerkinfrastruktur.
IP-Adresse im Produktionsnetzwerk	auto	Die IP-Adresse, die der Server im Produktionsnetzwerk haben wird. Standardmäßig ist die IP-Adresse der ursprünglichen Maschine vorgegeben.
Test-IP-Adresse	deaktiviert	Die Test-IP-Adresse gibt Ihnen die Möglichkeit, einen Failover in einem isolierten Testnetzwerk zu testen und sich während eines Test-Failovers per RDP oder SSH mit dem Recovery-Server zu verbinden. Im Test-Failover-Modus wird das VPN-Gateway mithilfe des NAT-Protokolls die Test-IP-Adresse gegen die Produktions-IP-Adresse ersetzen. Wenn keine Test-IP-Adresse spezifiziert wird, ist die Konsole die einzige Möglichkeit, während eines Test-Failovers auf den Server zuzugreifen.
Internetzugriff	aktiviert	Ermöglichen Sie dem Recovery-Server, sich während eines Failovers (im Realbetrieb oder im Testmodus) mit dem Internet zu verbinden. Standardmäßig wird der TCP-Port 25 für ausgehende Verbindungen verweigert.
Öffentliche IP-Adresse verwenden	deaktiviert	Wenn der Recovery-Server über eine öffentliche IP-Adresse verfügt, ist er während eines Failovers (auch im Testmodus) aus dem Internet verfügbar. Wenn Sie keine öffentliche IP-Adresse verwenden, ist der Server nur innerhalb Ihres Produktionsnetzwerks verfügbar. Um eine öffentliche IP-Adresse verwenden zu können, müssen Sie den Zugriff auf das Internet ermöglichen. Die öffentliche IP-Adresse wird angezeigt, nachdem Sie die Konfiguration abgeschlossen haben. Standardmäßig ist der TCP-Port 443 für eingehende Verbindungen geöffnet.
RPO-Grenzwert festlegen	deaktiviert	Der RPO-Grenzwert definiert also das maximal erlaubte Zeitintervall, das zwischen

		dem letzten Recovery-Punkt und dem aktuellen Zeitpunkt (an dem es zu einem Desaster kommen kann) zulässig ist. Der Wert kann zwischen 15–60 Minuten, 1–24 Stunden oder 1–14 Tagen eingestellt werden.

Cloud-Netzwerk-Infrastruktur

Die Cloud-Netzwerkinfrastruktur besteht aus dem VPN-Gateway auf der Cloud-Site und den Cloud-Netzwerken, mit denen die Recovery-Server verbunden sind.

Hinweis
Bei der Anwendung eines Disaster Recovery-Schutzplans wird nur dann eine Disaster-Recovery-Cloud-Netzwerkinfrastruktur erstellt, wenn diese noch nicht vorhanden ist. Bereits vorhandene Cloud-Netzwerke werden weder verändert noch neu erstellt.

Das System überprüft die IP-Adressen der Geräte und erstellt dann automatisch geeignete Cloud-Netzwerke, wenn es noch keine Cloud-Netzwerke gibt, zu denen eine IP-Adresse passen würden. Wenn bei Ihnen bereits Cloud Netzwerke vorhanden sind, zu denen die IP-Adressen der Recovery-Server passen, werden die vorhandenen Cloud-Netzwerke weder geändert noch neu erstellt.

- Wenn noch keine Cloud-Netzwerke vorhanden sind oder Sie die Disaster Recovery-Konfiguration zum ersten Mal einrichten, werden die Cloud-Netzwerke mit den maximalen IP-Bereichen erstellt, die von der IANA für den privaten Gebrauch empfohlen werden (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) – basierend auf dem IP-Adressbereich Ihrer Geräte. Sie können Ihr Netzwerk eingrenzen, indem Sie die Netzwerkmaske bearbeiten.
- Wenn Sie Geräte in mehreren lokalen Netzwerken haben, wird das Netzwerk auf der Cloud-Site zu einer Obermenge der lokalen Netzwerke. Sie können die Netzwerke im Bereich **Verbindung** auch rekonfigurieren. Siehe '"Netzwerke verwalten" (S. 39)'.
- Wenn Sie eine Site-to-Site-OpenVPN-Verbindung einrichten müssen, laden Sie die VPN-Appliance herunter und richten Sie diese ein. Siehe '"Eine Site-to-Site-OpenVPN-Verbindung konfigurieren" (S. 30)'. Stellen Sie sicher, dass die Bereiche Ihrer Cloud-Netzwerke zu den Bereichen Ihres lokalen Netzwerks passen, das mit der VPN-Appliance verbunden ist.
- Wenn Sie die Standard-Netzwerkkonfiguration ändern wollen, müssen Sie im Disaster Recovery-Modul des Schutzplans auf den Link **Zu 'Verbindung' gehen** klicken oder zu **Disaster Recovery** –> **Verbindung** gehen.

Verbindungen einrichten

In diesem Abschnitt werden die erforderlichen Netzwerkkonzepte erläutert, um Ihnen die Funktionsprinzipien von Cyber Disaster Recovery Cloud zu verdeutlichen. Dabei werden Sie lernen, wie Sie – abhängig von Ihren Anforderungen – verschiedene Arten von Verbindungen zur Cloud-Site konfigurieren können. Und abschließend erfahren Sie, wie Sie Ihre Netzwerke in der Cloud sowie die Einstellungen der VPN-Appliance und des VPN-Gateways verwalten können.

Netzwerkkonzepte

Hinweis
In Abhängigkeit davon, welches Lizenzierungsmodell angewendet wird, kann für einige Funktionen eine zusätzliche Lizenzierung erforderlich sein.

Mit Cyber Disaster Recovery Cloud können Sie folgende Verbindungstypen zur Cloud-Site definieren:

- **'Nur Cloud'-Modus**

  Diese Verbindungstyp erfordert keine Bereitstellung der VPN-Appliance am lokalen Standort.

  Die lokalen und Cloud-Netzwerke sind unabhängige Netzwerke. Diese Verbindungstyp bedingt entweder, dass alle geschützten Server des lokalen Standorts per Failover in die Cloud umgeschaltet werden – oder einen partiellen Failover von unabhängigen Servern, die nicht mit dem lokalen Standort kommunizieren müssen.

  Die Cloud Server in der Cloud-Site sind über die Point-to-Site-VPN-Verbindung und über öffentliche IP-Adressen (sofern zugewiesen) zugänglich.
- **Site-to-Site-OpenVPN-Verbindung**

  Diese Verbindungstyp erfordert eine Bereitstellung der VPN-Appliance am lokalen Standort.

  Mit der Site-to-Site-OpenVPN-Verbindung können Sie Ihre Netzwerke in die Cloud erweitern und die IP-Adressen beibehalten.

  Ihr lokaler Standort ist über einen sicheren VPN-Tunnel mit der Cloud-Site verbunden. Diese Verbindungstyp ist geeignet, wenn Sie stark voneinander abhängige Server am lokalen Standort vorliegen haben (wie z.B. ein Webserver und ein Datenbankserver). Bei einem partiellen Failover, wenn beispielsweise einer dieser Server auf der Cloud-Site neu erstellt wird, während der andere am lokalen Standort verbleibt, können diese dennoch weiter über einen VPN-Tunnel miteinander kommunizieren.

  Die Cloud Server in der Cloud-Site sind über das lokale Netzwerk, über die Point-to-Site-VPN-Verbindung und über öffentliche IP-Adressen (sofern zugewiesen) zugänglich.
- **Multi-Site-IPsec-VPN-Verbindung**

  Dieser Verbindungstyp erfordert ein lokales VPN-Gerät, welches den Standard IPsec IKE v2 unterstützt.

Wenn Sie mit der Konfiguration der Multi-Site-IPsec-VPN-Verbindung beginnen, wird Cyber Disaster Recovery Cloud automatisch ein Cloud-VPN-Gateway mit einer öffentlichen IP-Adresse erstellen.

Mit einer Multi-Site-IPsec-VPN-Konnektivität werden Ihre lokalen Standorte über einen sicheren IPsec-VPN-Tunnel mit der Cloud-Site verbunden.

Dieser Verbindungstyp eignet sich für Disaster Recovery-Szenarien, wenn Sie einen oder mehrere lokale Standorte haben, die geschäftskritische Workloads oder stark voneinander abhängige Services hosten.

Bei einem partiellen Failover von einem der Server wird dieser auf der Cloud-Site neu erstellt, während die anderen am lokalen Standort verbleiben. Dabei können die Server weiterhin über einen IPsec-VPN-Tunnel miteinander kommunizieren.

Bei einem partiellen Failover von einem der lokalen Standorte bleiben die übrigen lokalen Standorte weiterhin funktionsfähig und können weiterhin über einen IPsec-VPN-Tunnel miteinander kommunizieren.

- **Point-to-Site-VPN-Remote-Zugriff**

  Ein sicherer Point-to-Site-Remote-VPN-Zugriff auf Ihre Cloud-Site und die Workloads am lokalen Standort von außen über Ihr Endpunkgerät.

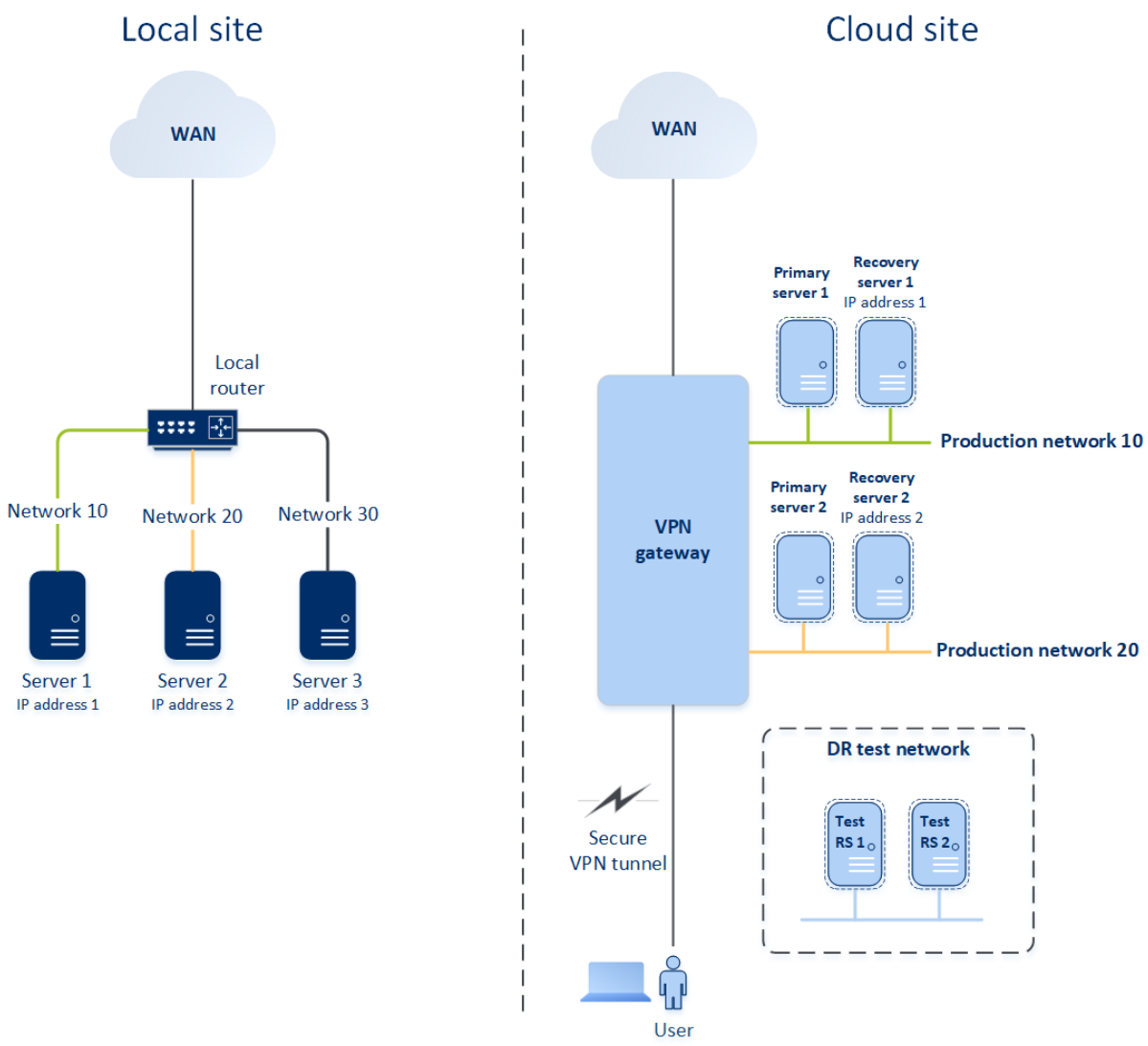
  Für den Zugriff auf einen lokalen Standort erfordert dieser Verbindungstyp eine Bereitstellung der VPN-Appliance am lokalen Standort.

'Nur Cloud'-Modus

Der 'Nur Cloud'-Modus erfordert keine Bereitstellung der VPN-Appliance am lokalen Standort. Er setzt voraus, dass Sie über zwei unabhängige Netzwerke verfügen: eines am lokalen Standort und ein anderes in der Cloud-Site. Das Routing erfolgt mit dem Router in der Cloud-Site.

So funktioniert Routing

Wenn der 'Nur Cloud'-Modus aktiviert ist, wird das Routing mit dem Router auf der Cloud-Site durchgeführt, sodass die Server aus verschiedenen Cloud-Netzwerken miteinander kommunizieren können.



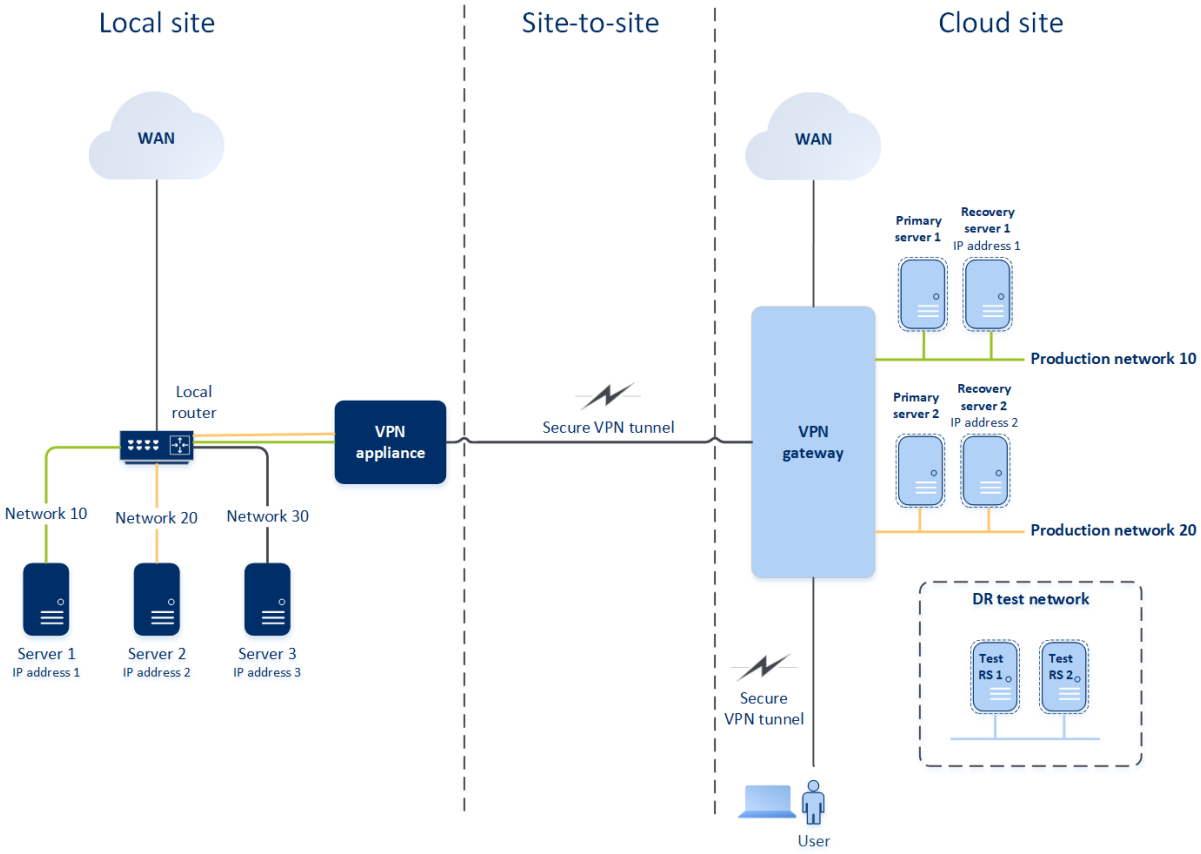
Site-to-Site-OpenVPN-Verbindung

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Um zu verstehen, wie die Vernetzung in Cyber Disaster Recovery Cloud funktioniert, werden wir einen Anwendungsfall betrachten, bei dem Sie drei Netzwerke mit jeweils einer Maschine am lokalen Standort verwenden. Sie werden für zwei Netzwerke – Netzwerk 10 und Netzwerk 20 genannt – einen Schutz vor Desastern konfigurieren.

In der nachfolgenden Abbildung sehen Sie den lokalen Standort, wo Ihre Maschinen gehostet werden, sowie die Cloud-Site, wo die Cloud Server gestartet werden, falls es zu einem Desaster kommt.

Die Cyber Disaster Recovery Cloud-Lösung ermöglicht es Ihnen, alle Workloads von beschädigten Maschinen, die sich an Ihrem lokalen Standort befinden, per Failover zu Cloud Servern in der Cloud umzuschalten. Sie können bis zu 23 Netzwerke mit Cyber Disaster Recovery Cloud schützen.



Um eine Site-to-Site-OpenVPN-Kommunikation zwischen dem lokalen Standort und der Cloud-Site aufzubauen, werden eine **VPN-Appliance** und ein **VPN-Gateway** verwendet. Wenn Sie mit der Konfiguration der Site-to-Site-OpenVPN-Verbindung in der Cyber Protect-Konsole beginnen, wird das VPN-Gateway automatisch in der Cloud-Site bereitgestellt. Anschließend müssen Sie die VPN-Appliance an Ihrem lokalen Standort bereitstellen, die zu schützenden Netzwerke hinzufügen und die Appliance in der Cloud registrieren. Cyber Disaster Recovery Cloud erstellt dann ein Replikat Ihres lokalen Netzwerks in der Cloud. Es wird ein sicherer VPN-Tunnel zwischen der VPN-Appliance und dem VPN-Gateway aufgebaut. Dadurch wird die Erweiterung Ihres lokalen Netzwerks in die Cloud bereitgestellt. Die Produktionsnetzwerke in der Cloud werden mit Ihren lokalen Netzwerken verknüpft. Die lokalen Server und Cloud Server können über den VPN-Tunnel so kommunizieren, als würden sie sich alle im selben Ethernet-Segment befinden. Das Routing erfolgt mit Ihrem lokalen Router.

Für jede zu schützende Quellmaschine müssen Sie einen Recovery-Server in der Cloud-Site erstellen. Dieser verbleibt solange im **Standby**-Stadium, bis es zu einem Failover-Ereignis kommt. Wenn es zu einem Desaster kommt und Sie einen Failover-Prozess starten (im **Produktionsmodus**), wird der Recovery-Server, der eine exakte Kopie Ihrer geschützten Maschine darstellt, in der Cloud ausgeführt. Ihm kann die gleiche IP-Adresse zugewiesen werden, die die Quellmaschine hat, und er

kann im selben Ethernet-Segment ausgeführt werden. Ihre Clients können wie gewohnt weiter mit dem Server arbeiten, ohne irgendwelche der im Hintergrund erfolgten Änderungen zu bemerken.

Sie können einen Failover-Prozess auch im **Testmodus** starten. Das bedeutet, dass die Quellmaschine weiter arbeitet und gleichzeitig der entsprechende Recovery-Server mit der gleichen IP-Adresse in der Cloud gestartet wird. Um IP-Adresskonflikte zu vermeiden, wird in der Cloud ein spezielles virtuelles Netzwerk erstellt – **Testnetzwerk** genannt. Das Testnetzwerk ist isoliert, um zu verhindern, dass die IP-Adresse der Quellmaschine im selben Ethernet-Segment doppelt vorkommt. Um auf den Recovery-Server im Test-Failover-Modus zugreifen zu können, müssen Sie dem Recovery-Server bei dessen Erstellung eine **Test-IP-Adresse** zuweisen. Weitere Parameter, die Sie für den Recovery-Server spezifizieren können, werden in entsprechenden Abschnitten weiter unten betrachtet.

So funktioniert Routing

Bei einer Site-to-Site-Verbindung wird das Routing zwischen den Cloud-Netzwerken mit Ihrem lokalen Router durchgeführt. Der VPN-Server führt kein Routing zwischen den Cloud-Servern durch, die sich in verschiedenen Cloud-Netzwerken befinden. Wenn ein Cloud-Server aus einem Netzwerk mit einem Server aus einem anderen Cloud-Netzwerk kommunizieren möchte, geht der Datenverkehr durch den VPN-Tunnel zum lokalen Router am lokalen Standort. Anschließend wird der Datenverkehr vom lokalen Router in ein anderes Netzwerk weitergeleitet und geht durch den Tunnel zurück zum Zielserver auf der Cloud-Site.

VPN-Gateway

Die Hauptkomponente, die die Kommunikation zwischen dem lokalen Standort und der Cloud-Site ermöglicht, ist das **VPN-Gateway**. Dabei handelt sich um eine virtuelle Maschine in der Cloud, auf welcher eine spezielle Software installiert und das Netzwerk in spezieller Weise konfiguriert ist. Das VPN-Gateway hat folgende Funktionen:

- Es verbindet die Ethernet-Segmente Ihres lokalen Netzwerks und des Produktionsnetzwerks in der Cloud im L2-Modus.
- Es stellt iptables- und ebtables-Regeln bereit.
- Es fungiert als Standardrouter und NAT für die Maschinen in den Test- und Produktionsnetzwerken.
- Es fungiert als DHCP-Server. Alle Maschinen in den Produktions- und Testnetzwerken erhalten ihre Netzwerkkonfiguration (IP-Adressen, DNS-Einstellungen) per DHCP. Ein Cloud-Server erhält jedes Mal die gleiche IP-Adresse vom DHCP-Server. Wenn Sie die benutzerdefinierte DNS-Konfiguration einrichten müssen, sollten Sie sich an Ihr Support-Team wenden.
- Es fungiert als DNS-Cache.

Netzwerkkonfiguration des VPN-Gateways

Das VPN-Gateway hat mehrere Netzwerkschnittstellen:

- Eine externe Schnittstelle, die mit dem Internet verbunden ist
- Produktionsschnittstellen, die mit den Produktionsnetzwerken verbunden sind
- Eine Testschnittstelle, die mit dem Testnetzwerk verbunden ist

Darüber hinaus werden zwei virtuelle Schnittstellen für Point-to-Site- und Site-to-Site-Verbindungen hinzugefügt.

Wenn das VPN-Gateway bereitgestellt und initialisiert wird, werden die Brücken erstellt: eine für die externe Schnittstelle und eine für die Client- und Produktionsschnittstellen. Obwohl die Client-Produktionsbrücke und die Testschnittstelle die gleichen IP-Adressen verwenden, kann das VPN-Gateway die Datenpakete mithilfe einer bestimmten Technik korrekt weiterleiten.

VPN-Appliance

Die **VPN-Appliance** ist eine virtuelle Maschine am lokalen Standort, auf der Linux und eine spezielle Software installiert ist und die über eine spezielle Netzwerkkonfiguration verfügt. Sie ermöglicht die Kommunikation zwischen dem lokalen Standort und der Cloud-Site.

Recovery-Server

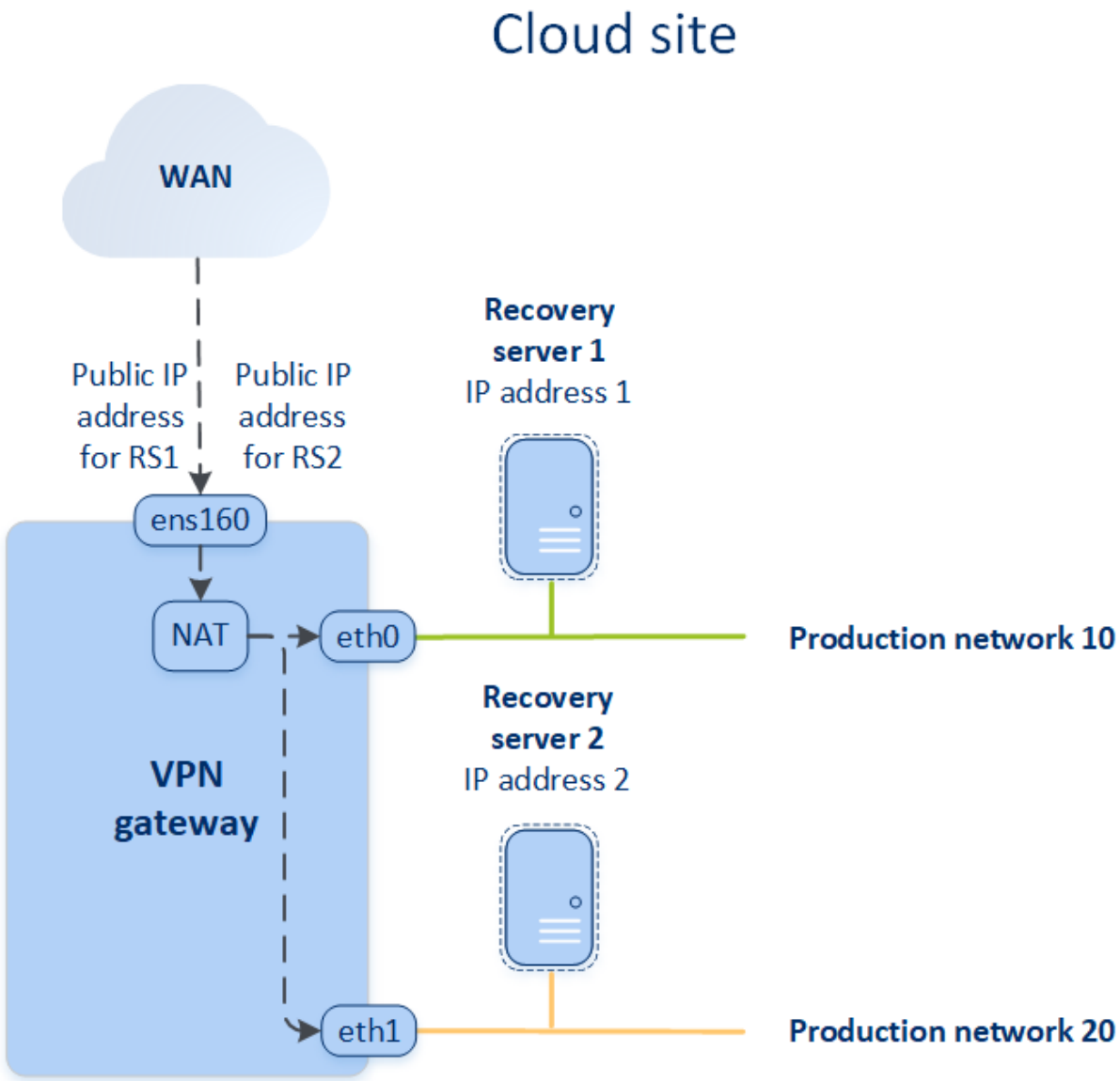
Ein **Recovery-Server** – ist das VM-Replikat einer ursprünglichen Maschine, das auf den (in der Cloud gespeicherten) Backups eines geschützten Servers basiert. Recovery-Server werden verwendet, um bei einem Desaster die Workloads der ursprünglichen Server in die Cloud umschalten zu können.

Wenn Sie einen Recovery-Server erstellen, müssen Sie folgende Netzwerkparameter spezifizieren:

- **Cloud-Netzwerk** (erforderlich): das Cloud-Netzwerk, mit dem der Recovery-Server verbunden wird.
- **IP-Adresse im Produktionsnetzwerk** (erforderlich): die IP-Adresse, mit der die virtuelle Maschine des Recovery-Servers gestartet wird. Diese Adresse wird in den Produktions- und Testnetzwerken verwendet. Die virtuelle Maschine wird vor dem Starten so konfiguriert, dass sie ihre IP-Adresse per DHCP erhält.
- **Test-IP-Adresse** (optional): eine IP-Adresse, um beim Test-Failover vom Client-Produktionsnetzwerk aus auf den Recovery-Server zugreifen zu können. Dadurch wird verhindert, dass die Produktions-IP-Adresse innerhalb desselben Netzwerks doppelt verwendet wird. Diese IP-Adresse unterscheidet sich von der IP-Adresse im Produktionsnetzwerk. Die Server am lokalen Standort können den Recovery-Server während des Test-Failovers über die Test-IP-Adresse erreichen, während in umgekehrter Richtung jedoch kein Zugriff nicht möglich ist. Der Recovery-Server im Testnetzwerk kann auf das Internet zugreifen, wenn bei der Erstellung des Recovery-Servers die Option **Internetzugriff** ausgewählt wurde.
- **Öffentliche IP-Adresse** (optional): eine IP-Adresse, um aus dem Internet auf den Recovery-Server zugreifen zu können. Wenn ein Server keine öffentliche IP-Adresse hat, ist er nur aus dem lokalen Netzwerk erreichbar.
- **Internetzugriff** (optional): diese Option ermöglicht dem Recovery-Server, auf das Internet zuzugreifen (gilt bei Produktions- und Test-Failovers).

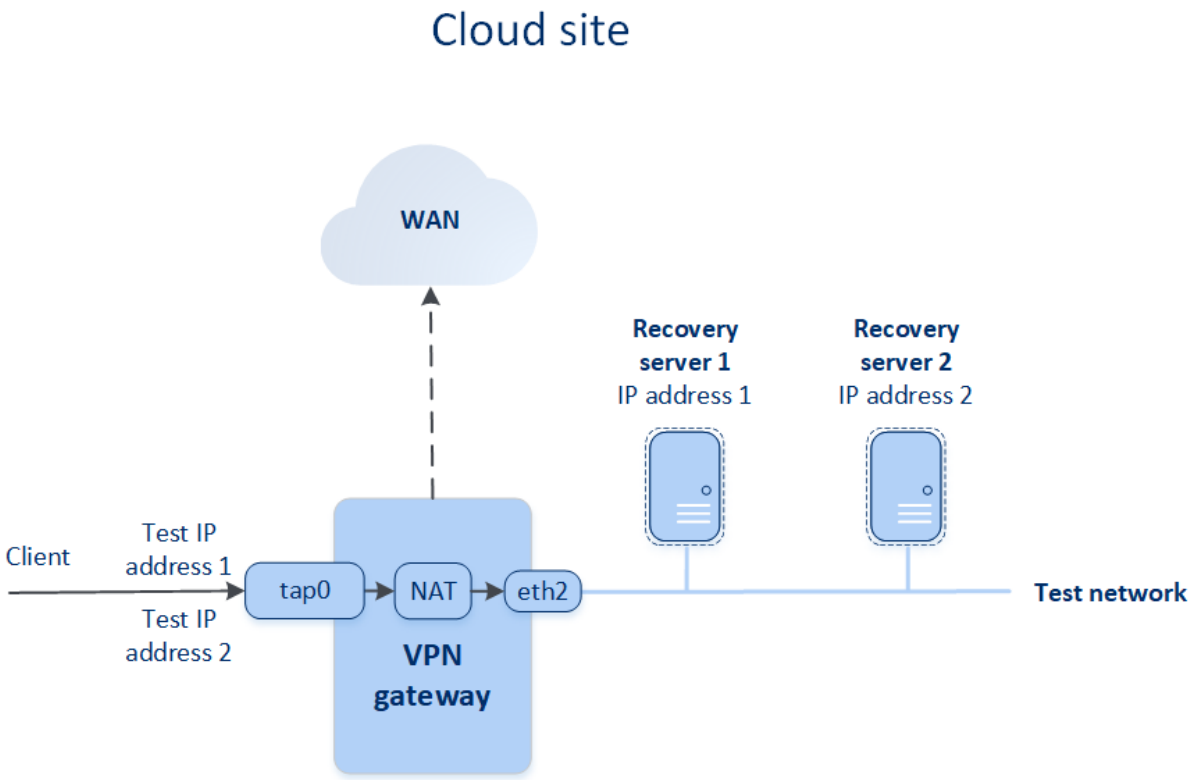
Öffentliche und Test-IP-Adresse

Wenn Sie einem Recovery-Server bei dessen Erstellung eine öffentliche IP-Adresse zuweisen, kann auf den Server über diese IP-Adresse aus dem Internet zugriffen werden. Wenn ein Datenpaket aus dem Internet mit der öffentlichen Ziel-IP-Adresse ankommt, wird das VPN-Gateway das Datenpaket per NAT der jeweiligen Produktions-IP-Adresse zuordnen und es dann an den entsprechenden Recovery-Server weitersenden.



Wenn Sie einem Recovery-Server bei dessen Erstellung eine Test-IP-Adresse zuweisen, kann auf den Server innerhalb des Testnetzwerks über diese IP-Adresse zugriffen werden. Wenn Sie den Test-Failover durchführen, wird die ursprüngliche Maschine weiter ausgeführt – während der Recovery-Server mit der gleichen IP-Adresse im Testnetzwerk in der Cloud gestartet wird. Es kommt jedoch zu keinem IP-Adresskonflikt, weil das Testnetzwerk isoliert ist. Die Recovery-Server im Testnetzwerk

sind über ihre Test-IP-Adressen erreichbar, die per NAT den Produktions-IP-Adressen zugeordnet werden.



Weitere Informationen zu Site-to-Site-OpenVPN finden Sie unter '"Site-to-Site-OpenVPN – Zusätzliche Informationen" (S. 102)'.

Primäre Server

Ein **primärer Server** ist eine virtuelle Maschine, die (im Vergleich zu einem Recovery-Server) keine verknüpfte Maschine am lokalen Standort hat. Primäre Server werden zum Schutz einer Applikation durch Replikation oder zur Ausführung verschiedener Hilfsdienste (z.B. als Webserver) verwendet.

Ein primärer Server wird üblicherweise verwendet, um Echtzeit-Datenreplikationen zwischen Servern durchzuführen, die wichtige Applikationen ausführen. Sie richten die Replikation selbst ein, indem Sie die internen Tools der jeweiligen Applikation verwenden. Beispielsweise kann eine Active Directory- oder SQL-Replikation zwischen lokalen Servern und dem primären Server konfiguriert werden.

Alternativ kann ein primärer Server auch in eine AlwaysOn-Verfügbarkeitsgruppe (AAG) oder Datenbankverfügbarkeitsgruppen (DAG) aufgenommen werden.

Beide Methoden erfordern weitreichende Kenntnisse der jeweiligen Applikation und Administratorrechte. Ein primärer Server verbraucht fortlaufend Computing-Ressourcen (Berechnungspunkte) und benötigt Speicherplatz im schnellen Disaster Recovery Storage. Zudem sind gewisse Wartungsaktivitäten auf Ihrer Seite erforderlich: Überwachung der Replikation, Installation von Software-Updates und Durchführung von Backups. Die Vorteile sind minimale RPOs

und RTOs bei minimaler Belastung der Produktionsumgebung (im Vergleich zum Backup kompletter Server in der Cloud).

Primäre Server werden immer nur im Produktionsnetzwerk gestartet. Sie verfügen über folgende Netzwerkparameter:

- **Cloud-Netzwerk** (erforderlich): das Cloud-Netzwerk, mit dem ein primärer Server verbunden wird.
- **IP-Adresse im Produktionsnetzwerk** (erforderlich): die IP-Adresse, die der primäre Server im Produktionsnetzwerk haben wird. Als Standardeinstellung wird die erste freie IP-Adresse aus Ihrem Produktionsnetzwerk verwendet.
- **Öffentliche IP-Adresse** (optional): eine IP-Adresse, um aus dem Internet auf einen primären Server zugreifen zu können. Wenn ein Server keine öffentliche IP-Adresse hat, ist er nur aus dem lokalen Netzwerk und nicht über das Internet erreichbar.
- **Internetzugriff** (optional): diese Option ermöglicht es einem primären Server, auf das Internet zuzugreifen.

Multi-Site-IPsec-VPN-Verbindung

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Sie können die Multi-Site-IPsec-VPN-Konnektivität verwenden, um einen einzelnen oder mehrere lokale Standorte über eine sichere L3-IPsec-VPN-Verbindung mit der Cyber Disaster Recovery Cloud zu verbinden.

Dieser Verbindungstyp ist für Disaster Recovery-Szenarien nützlich, wenn Sie einen der folgenden Anwendungsfälle haben:

- Sie haben einen lokalen Standort, der geschäftskritische Workloads hostet.
- Sie haben mehrere lokale Standorte, die geschäftskritische Workloads hosten (z.B. Büros an verschiedenen Standorten).
- Sie verwenden Stand- bzw. Speicherorte, die auf Software von Drittanbietern basieren, oder Stand- bzw. Speicherorte von Managed Service Providern – und sind mit diesen über einen IPsec-VPN-Tunnel verbunden.

Um eine Multi-Site-IPsec-VPN-Kommunikation zwischen den lokalen Standorten und der Cloud-Site aufzubauen, wird ein **VPN-Gateway** verwendet. Wenn Sie mit der Konfiguration der Multi-Site-IPsec-VPN-Verbindung in der Cyber Protect-Konsole beginnen, wird das VPN-Gateway automatisch in der Cloud-Site bereitgestellt. Sie sollten die Cloud-Netzwerksegmente konfigurieren und dabei sicherstellen, dass sich diese nicht mit den lokalen Netzwerksegmenten überlappen. Ein sicherer VPN-Tunnel wird zwischen den lokalen Standorten und der Cloud-Site aufgebaut. Die lokalen Server und Cloud Server können über den VPN-Tunnel so kommunizieren, als würden sie sich alle im selben Ethernet-Segment befinden.

Für jede zu schützende Quellmaschine müssen Sie einen Recovery-Server in der Cloud-Site erstellen. Dieser verbleibt solange im **Standby**-Stadium, bis es zu einem Failover-Ereignis kommt. Wenn es zu einem Desaster kommt und Sie einen Failover-Prozess starten (im **Produktionsmodus**), wird der Recovery-Server, der eine exakte Kopie Ihrer geschützten Maschine darstellt, in der Cloud ausgeführt. Ihre Clients können wie gewohnt weiter mit dem Server arbeiten, ohne irgendwelche der im Hintergrund erfolgten Änderungen zu bemerken.

Sie können einen Failover-Prozess auch im **Testmodus** starten. Das bedeutet, dass die Quellmaschine weiterhin arbeitet und gleichzeitig der entsprechende Recovery-Server in der Cloud in einem speziellen virtuellen Netzwerk gestartet wird, welches in der Cloud erstellt wird – ein **Testnetzwerk**. Das Testnetzwerk ist isoliert, um die Duplizierung von IP-Adressen in den anderen Cloud-Netzwerksegmenten zu verhindern.

VPN-Gateway

Die Hauptkomponente, die die Kommunikation zwischen den lokalen Standorten und der Cloud-Site ermöglicht, ist das **VPN-Gateway**. Dabei handelt sich um eine virtuelle Maschine in der Cloud, auf welcher eine spezielle Software installiert und das Netzwerk in spezieller Weise konfiguriert ist. Das VPN-Gateway stellt folgende Funktionen bereit:

- Es verbindet die Ethernet-Segmente Ihres lokalen Netzwerks und des Produktionsnetzwerks in der Cloud im L3-IPsec-Modus.
- Es fungiert als Standardrouter und NAT für die Maschinen in den Test- und Produktionsnetzwerken.
- Es fungiert als DHCP-Server. Alle Maschinen in den Produktions- und Testnetzwerken erhalten ihre Netzwerkkonfiguration (IP-Adressen, DNS-Einstellungen) per DHCP. Ein Cloud-Server erhält jedes Mal die gleiche IP-Adresse vom DHCP-Server.

  Wenn Sie es bevorzugen, können Sie auch eine benutzerdefinierte DNS-Konfiguration einrichten. Weitere Informationen finden Sie im Abschnitt '"Benutzerdefinierte DNS-Server konfigurieren" (S. 48)'.
- Es fungiert als DNS-Cache.

So funktioniert Routing

Das Routing zwischen den Cloud-Netzwerken wird mit dem Router auf der Cloud-Site durchgeführt, sodass die Server aus verschiedenen Cloud-Netzwerken miteinander kommunizieren können.

Point-to-Site-VPN-Remote-Zugriff

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

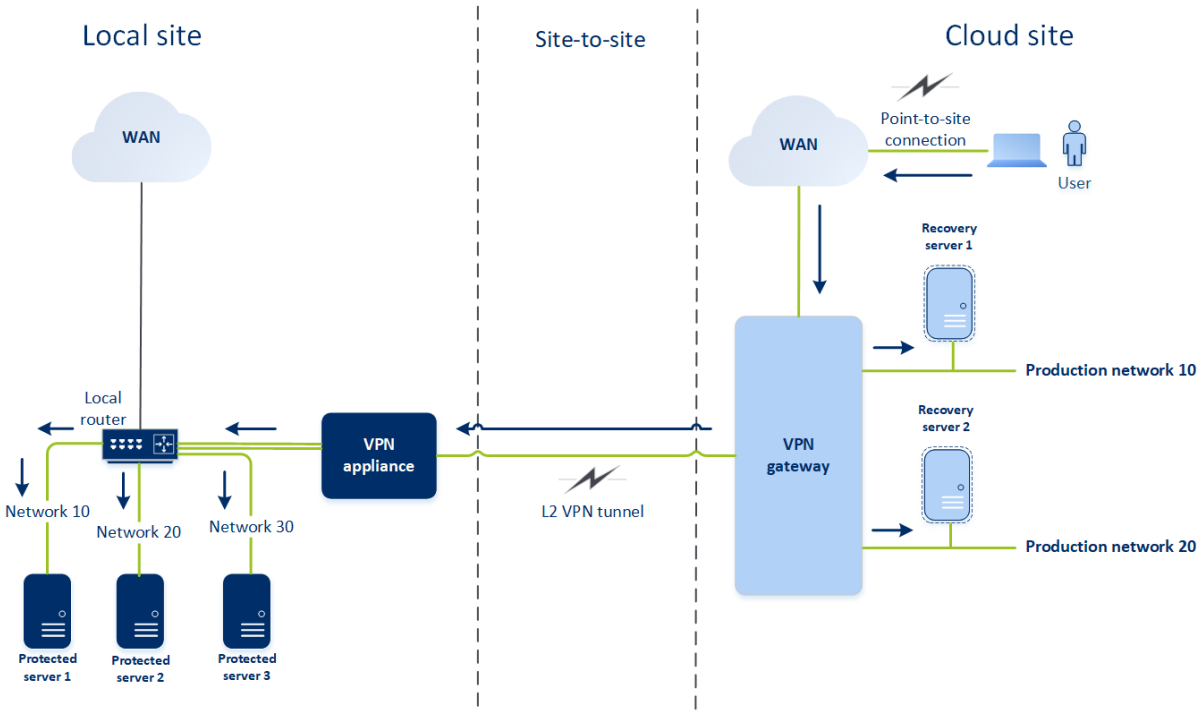
Die Point-to-Site-Verbindung ist eine sichere, von außen kommende Verbindung von einem Ihrer Endgeräte (z.B. einem Desktop-Computer oder Laptop) über ein VPN zu einem lokalen Standort und

einer Cloud-Site. Sie ist verfügbar, nachdem Sie eine Site-to-Site-OpenVPN-Verbindung zur Cyber Disaster Recovery Cloud-Site aufgebaut haben. Diese Art der Verbindung ist in folgenden Fällen nützlich:

- In vielen Unternehmen sind die Unternehmensdienste und Webressourcen nur über das Unternehmensnetzwerk verfügbar. Sie können die Point-to-Site-Verbindung verwenden, um sich sicher mit dem lokalen Standort zu verbinden.
- Bei einem Desaster, wenn Workloads in die Cloud-Site umgeschaltet werden und Ihr lokales Netzwerk ausgefallen ist, benötigen Sie möglicherweise direkten Zugriff auf Ihre Cloud Server. Die ist über die Point-to-Site-Verbindung zur Cloud-Site möglich.

Für die Point-to-Site-Verbindung zum lokalen Standort müssen Sie die VPN-Appliance am lokalen Standort installieren, dann die Site-to-Site-Verbindung konfigurieren und anschließend die Point-to-Site-Verbindung zum lokalen Standort. Auf diese Weise haben Ihre Remote-Mitarbeiter über ein Layer-2-VPN (L2-VPN) Zugriff auf das Unternehmensnetzwerk.

Das unten stehende Schema zeigt den lokalen Standort, die Cloud-Site und die Kommunikationen zwischen den Servern (grün markiert). Der L2-VPN-Tunnel verbindet Ihren lokalen Standort und die Cloud-Site. Wenn ein Benutzer eine Point-to-Site-Verbindung aufbaut, erfolgen die Kommunikationen mit dem lokalen Standort über die Cloud-Site.



Eine Point-to-Site-Konfiguration verwendet Zertifikate zur Authentifizierung gegenüber dem VPN-Client. Und zudem werden auch noch Anmeldedaten für die Authentifizierung verwendet. Beachten Sie folgende Hinweise zu Point-to-Site-Verbindungen mit dem lokalen Standort:

- Die Benutzer sollten Ihre Cyber Protect Cloud-Anmeldedaten verwenden, um sich im VPN-Client zu authentifizieren. Sie müssen entweder die Rolle 'Firmenadministrator' oder 'Cyber Protection' haben.

- Wenn Sie die OpenVPN-Konfiguration neu generieren, müssen Sie die aktualisierte Konfiguration allen Benutzern zur Verfügung stellen, die die Point-to-Site-Verbindung zur Cloud-Site verwenden.

Automatisches Löschen einer ungenutzten Kundenumgebung auf der Cloud-Site

Der Disaster Recovery Service überwacht die Nutzung der Kundenumgebungen, die für Disaster Recovery-Zwecke erstellt wurden, und löscht diese automatisch, wenn sie nicht verwendet werden.

Folgende Kriterien werden verwendet, um zu definieren, ob ein Kunden-Mandant aktiv ist:

- Es gibt aktuell mindestens einen Cloud Server – oder es gab einen (oder mehrere) Cloud Server in den letzten sieben Tagen.
  ODER
- Die Option **VPN-Zugriff auf den lokalen Standort** aktiviert und entweder ist der Site-to-Site-OpenVPN-Tunnel aufgebaut oder von der VPN-Appliance werden Daten für die letzten 7 Tage gemeldet.

Alle übrigen Mandanten werden als inaktive Mandanten betrachtet. Für solche Mandanten führt das System folgende Aktionen aus:

- Das VPN-Gateway wird gelöscht und alle Cloud-Ressourcen, die zu dem Mandanten gehören.
- Die Registrierung der VPN-Appliance wird aufgehoben.

Die inaktiven Mandanten werden auf ihr Stadium zurückversetzt, bevor die Verbindung konfiguriert wurde.

Grundsätzliche Verbindungskonfiguration

In diesem Abschnitt werden verschiedene Szenarien für die Verbindungskonfiguration beschrieben.

Den 'Nur Cloud'-Modus konfigurieren

So können Sie eine Verbindung im 'Nur Cloud'-Modus konfigurieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Wählen Sie **Nur Cloud** und klicken Sie dann auf **Konfigurieren**.
   Als Ergebnis wird das VPN-Gateway und Cloud-Netzwerk mit der definierten Adresse und Netzwerkmaske auf der Cloud-Site bereitgestellt.

Informationen zur Verwaltung Ihrer Netzwerke in der Cloud und zur Konfiguration der VPN-Gateway-Einstellungen finden Sie im Abschnitt 'Cloud-Netzwerke verwalten'.

Eine Site-to-Site-OpenVPN-Verbindung konfigurieren

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Anforderungen für die VPN-Appliance

Systemanforderungen

- 1 CPUs
- 1 GB RAM
- 8 GB Festplattenspeicherplatz

Ports

- TCP 443 (ausgehend) – für VPN-Verbindungen
- TCP 80 (ausgehend) – für automatische Updates der Appliance

Stellen Sie sicher, dass Ihre Firewalls und anderen Komponenten des Netzwerk-Sicherheitssystems Verbindungen zu allen IP-Adressen über diese Ports zulassen.

Eine Site-to-Site-OpenVPN-Verbindung konfigurieren

Die VPN-Appliance erweitert Ihr lokales Netzwerk (LAN) über einen sicheren VPN-Tunnel in die Cloud. Eine solche Verbindung wird oft auch als Site-to-Site-Verbindung (S2S) bezeichnet. Sie können die nachfolgende Prozedur befolgen oder sich das Video-Tutorial ansehen.

So können Sie eine Verbindung über die VPN-Appliance konfigurieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Wählen Sie **Site-to-Site-OpenVPN-Verbindung** aus und klicken Sie dann auf **Konfigurieren**.
   Das System beginnt damit, das VPN-Gateway in der Cloud bereitzustellen. Dies wird einige Zeit benötigen. Währenddessen können Sie zum nächsten Schritt weitergehen.

   Hinweis
   Das VPN-Gateway wird kostenlos bereitgestellt. Er wird gelöscht, wenn die Disaster Recovery-Funktionalität nicht verwendet wird (d.h., wenn sieben Tage lang kein primärer oder Recovery-Server in der Cloud vorhanden ist).

3. Klicken Sie im Block **VPN-Appliance** auf den Befehl **Herunterladen und bereitstellen**. Laden Sie je nach der von Ihnen verwendeten Virtualisierungsplattform die entsprechende VPN-Appliance für VMware vSphere oder Microsoft Hyper-V herunter.
4. Stellen Sie die Appliance bereit und verbinden Sie diese mit den Produktionsnetzwerken.

Überprüfen Sie in vSphere, dass für alle virtuellen Switche, die die VPN-Appliance mit den Produktionsnetzwerken verbinden, die Optionen **Promiscuous-Modus** und **Gefälschte Übertragungen** aktiviert sind und auf **Akzeptieren** eingestellt ist. Sie können im vSphere Client mit folgender Befehlssequenz auf diese Einstellungen zugreifen: Host auswählen –> **Übersicht** –> **Netzwerk** –> den Switch auswählen –> **Einstellungen bearbeiten...** > **Sicherheit**.

Erstellen Sie in Hyper-V eine virtuelle Maschine der **Generation 1** mit 1,024 MB Arbeitsspeicher. Wir empfehlen außerdem, dass Sie für diese Maschine die Option **Dynamischer Arbeitsspeicher** aktivieren. Gehen Sie, sobald die Maschine erstellt wurde, zu **Einstellungen** –> **Hardware** –> **Netzwerkkarte** –> **Erweiterte Features** – und aktivieren Sie dort das Kontrollkästchen **Spoofing von MAC-Adressen aktivieren**.

5. Schalten Sie die Appliance ein.
6. Öffnen Sie die Appliance-Konsole und melden Sie sich mit der Benutzernamen-/Kennwort-Kombination 'admin/admin' an.
7. [Optional] Ändern Sie das Kennwort.
8. [Optional] Ändern Sie bei Bedarf die Netzwerkeinstellungen. Definieren Sie, welche Schnittstelle als WAN-Schnittstelle für die Internetverbindung verwendet werden soll.
9. Registrieren Sie die Appliance im Cyber Protection Service, indem Sie die Anmeldedaten des Firmenadministrators verwenden.

   Diese Anmeldedaten werden nur einmal verwendet, um das Zertifikat abzurufen. Die Datacenter-URL ist vordefiniert.

   Hinweis
   Wenn für Ihr Konto eine Zwei-Faktor-Authentifizierung konfiguriert ist, werden Sie auch aufgefordert, den TOTP-Code einzugeben. Wenn die Zwei-Faktor-Authentifizierung aktiviert, aber für Ihr Konto nicht konfiguriert ist, können Sie die VPN-Appliance nicht registrieren. Zuerst müssen Sie zur Anmeldeseite der Cyber Protect-Konsole gehen und die Konfiguration der Zwei-Faktor-Authentifizierung für Ihr Konto abschließen. Weitere Informationen zur Zwei-Faktor-Authentifizierung finden Sie in der Management-Portal-Administrator-Anleitung.

Wenn die Konfiguration abgeschlossen wurde, zeigt die Appliance als Status '**Online**' an. Die Appliance verbindet sich mit dem VPN-Gateway und beginnt, Informationen über die Netzwerke von allen aktiven Schnittstellen an den Cyber Disaster Recovery Cloud Service zu melden. Die Cyber Protect-Konsole zeigt die Schnittstellen basierend auf den Informationen der VPN-Appliance an.

Multi-Site-IPsec-VPN konfigurieren

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Sie können eine Multi-Site-IPsec-VPN-Verbindung auf die folgenden zwei Arten konfigurieren:

- über die Registerkarte **Disaster Recovery** –> **Verbindung**.
- indem Sie einen Schutzplan auf ein oder mehrere Geräte anwenden und dann manuell von der automatisch erstellten Site-to-Site-OpenVPN-Verbindung zu einer Multi-Site-IPsec-VPN-Verbindung wechseln, anschließend die Multi-Site-IPsec-VPN-Einstellungen konfigurieren und abschließend die IP-Adressen neu zuweisen.

So können Sie eine Multi-Site-IPsec-VPN-Verbindung über die Registerkarte Verbindung konfigurieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie im Bereich **Multi-Site-VPN-Verbindung** auf den Befehl **Konfigurieren**.
   Ein VPN-Gateway wird in der Cloud-Site bereitgestellt.
3. Konfigurieren Sie die Multi-Site-IPsec-VPN-Einstellungen.

So können Sie eine Multi-Site-IPsec-VPN-Verbindung über einen Schutzplan konfigurieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Geräte**.
2. Wenden Sie einen Schutzplan auf ein oder mehrere Geräte aus der Liste an.
   Der Recovery-Server und die Cloud-Infrastruktur-Einstellungen werden automatisch für die Site-to-Site-OpenVPN-Verbindung konfiguriert.
3. Gehen Sie zu **Disaster Recovery** –> **Verbindung**.
4. Klicken Sie auf **Eigenschaften anzeigen**.
5. Klicken Sie auf **Zu Multi-Site-IPsec-VPN wechseln**.
6. Konfigurieren Sie die Multi-Site-IPsec-VPN-Einstellungen.
7. Weisen Sie die IP-Adressen des Cloud-Netzwerks und der Cloud Server neu zu.

Die Multi-Site-IPsec-VPN-Einstellungen konfigurieren

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Wenn Sie eine Multi-Site-IPsec-VPN-Verbindung konfiguriert haben, müssen Sie anschließend die Einstellungen für die Cloud-Site und die lokalen Standorte auf der Registerkarte **Disaster Recovery** –> **Verbindung** konfigurieren.

Voraussetzungen

- Die Multi-Site-IPsec-VPN-Konnektivität ist konfiguriert. Weitere Informationen zur Konfiguration der Multi-Site-IPsec-VPN-Konnektivität finden Sie im Abschnitt '"Multi-Site-IPsec-VPN konfigurieren" (S. 31)'.
- Jedes lokale IPsec-VPN-Gateway hat eine öffentliche IP-Adresse.

- Ihr Cloud-Netzwerk hat genügend IP-Adressen für die Cloud Server, die Kopien Ihrer geschützten Maschinen sind (im Produktionsnetzwerk), und für die Recovery-Server (mit einer oder zwei IP-Adressen, je nach Ihren Anforderungen).
- [Wenn Sie eine Firewall zwischen den lokalen Standorten und der Cloud-Site verwenden] Die folgenden IP-Protokolle und UDP-Ports sind an den lokalen Standorten zugelassen: IP-Protokoll ID 50 (ESP), UDP-Port 500 (IKE) und UDP-Port 4500.
- Die NAT-T-Konfiguration am lokalen Standort ist deaktiviert.

So können Sie eine Multi-Site-IPsec-VPN-Verbindung konfigurieren

1. Fügen Sie ein oder mehrere Netzwerke zur Cloud-Site hinzu.
   a. Klicken Sie auf **Netzwerk hinzufügen**.

   Hinweis
   Wenn Sie ein Cloud-Netzwerk hinzufügen, wird automatisch ein entsprechendes Testnetzwerk mit der gleichen Netzwerkadresse und Maske hinzugefügt, um Test-Failover durchführen zu können. Die Cloud Server im Testnetzwerk haben die gleichen IP-Adressen wie die im Cloud-Produktionsnetzwerk. Wenn Sie während eines Test-Failover vom Produktionsnetzwerk aus auf einen Cloud Server zugreifen müssen, sollten Sie beim Erstellen eines Recovery-Servers diesem eine zweite Test-IP-Adresse zuweisen.

   b. Geben Sie im Feld **Netzwerkadresse** die IP-Adresse des Netzwerks ein.
   c. Geben Sie im Feld **Netzwerkmaske** die Maske des Netzwerkes ein.
   d. Klicken Sie auf **Hinzufügen**.
2. Konfigurieren Sie die Einstellungen für jeden lokalen Standort, den Sie mit der Cloud-Site verbinden wollen, gemäß den Empfehlungen für lokale Standorte. Weitere Informationen zu diesen Empfehlungen finden Sie in Abschnitt '"Allgemeine Empfehlungen für lokale Standorte" (S. 34)'.
   a. Klicken Sie auf **Verbindung hinzufügen**.
   b. Geben Sie einen Namen für das lokale VPN-Gateway ein.
   c. Geben Sie die öffentliche IP-Adresse des lokalen VPN-Gateways ein.
   d. [Optional] Geben Sie eine Beschreibung für das lokale VPN-Gateway ein.
   e. Klicken Sie auf **Weiter**.
   f. Geben Sie im Feld **Vorinstallierter Schlüssel (PSK)** den „Pre-Shared Key“ ein – oder klicken Sie auf **Einen neuen vorinstallierten Schlüssel (PSK) generieren**, um einen automatisch generierten Wert zu verwenden.

   Hinweis
   Sie müssen den gleichen vorinstallierten Schlüssel (Pre-Shared Key, PSK) für das lokale und das Cloud-VPN-Gateway verwenden.

g. Klicken Sie auf **IPsec/IKE-Sicherheitseinstellungen**, um die Einstellungen zu konfigurieren. Weitere Informationen zu den Einstellungen, die Sie konfigurieren können, finden Sie im Abschnitt '"IPsec/IKE-Sicherheitseinstellungen" (S. 35)'.

Hinweis
Sie können die Standardeinstellungen verwenden, die automatisch ausgefüllt werden, oder eigene Werte verwenden. Es werden nur Verbindungen mit dem IKEv2-Protokoll unterstützt. Die vorgegebene **Aktion bei Start** bei Aufbau der VPN-Verbindung ist **Hinzufügen** (bedeutet: Ihr lokales VPN-Gateway initiiert die Verbindung). Sie können den Wert aber auch auf **Start** (bedeutet: das Cloud-VPN-Gateway initiiert die Verbindung) oder **Route** (geeignet für Firewalls, die die Route-Option unterstützen) ändern.

h. Konfigurieren Sie die **Netzwerkrichtlinien**.
Die Netzwerkrichtlinien spezifizieren diejenigen Netzwerke, mit denen sich das IPsec-VPN verbindet. Geben Sie die IP-Adresse und Maske des Netzwerks im CIDR-Format ein. Die lokalen und Cloud-Netzwerksegmente sollten sich nicht überlappen.

i. Klicken Sie auf **Speichern**.

Allgemeine Empfehlungen für lokale Standorte

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Wenn Sie die lokalen Standorte für Ihre Multi-Site-IPsec-VPN-Konnektivität konfigurieren, sollten Sie folgende Empfehlungen beachten:

- Legen Sie für jede IKE-Phase mindestens einen der Werte fest, die in der Cloud-Site für folgende Parameter konfiguriert sind: Verschlüsselungsalgorithmus, Hash-Algorithmus und Diffie-Hellman-Gruppennummern.
- Aktivieren Sie 'Perfect Forward Secrecy' (PFS, perfekte vorwärts gerichtete Geheimhaltung) mit mindestens einem der Werte für Diffie-Hellman-Gruppennummern, der in der Cloud-Site für die IKE-Phase 2 konfiguriert ist.
- Konfigurieren Sie für die IKE-Phase 1 und IKE-Phase 2 denselben **Lebensdauer**-Wert wie in der Cloud-Site.
- Konfigurationen mit NAT-Traversal (NAT-T) werden nicht unterstützt. Deaktivieren Sie die NAT-T-Konfiguration am lokalen Standort. Anderenfalls kann die zusätzliche UDP-Kapselung nicht ausgehandelt werden.
- Die Konfiguration von **Aktion bei Start** definiert, welche Seite die Verbindung initiiert. Der Standardwert **Hinzufügen** bedeutet, dass der lokale Standort die Verbindung einleitet und die Cloud-Site auf die Initiierung der Verbindung wartet. Ändern Sie den Wert auf **Start**, wenn die Cloud-Site die Verbindung initiieren soll – oder auf **Route**, wenn Sie wollen, dass beide Seiten die Verbindung initiieren können (geeignet für Firewalls, die die Route-Option unterstützen).

Weitere Informationen und Konfigurationsbeispiele für verschiedene Lösungen finden Sie unter:

- Diese Serie von Knowledge Base-Artikeln
- Dieses Video-Beispiel

IPsec/IKE-Sicherheitseinstellungen

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Die folgende Tabelle gibt weitere Informationen über die IPsec-/IKE-Sicherheitsparameter.

Parameter	Beschreibung
Verschlüsselungsalgorithmus	Der Verschlüsselungsalgorithmus, durch den sichergestellt wird, dass die Daten während der Übertragung nicht einsehbar sind. Standardmäßig sind alle Algorithmen ausgewählt. Sie müssen mindestens einen der ausgewählten Algorithmen auf Ihrem lokalen Gateway-Gerät für jede IKE-Phase konfigurieren.
Hash-Algorithmus	Der Hash-Algorithmus, der verwendet wird, um die Integrität und Authentizität der Daten überprüfen zu können. Standardmäßig sind alle Algorithmen ausgewählt. Sie müssen mindestens einen der ausgewählten Algorithmen auf Ihrem lokalen Gateway-Gerät für jede IKE-Phase konfigurieren.
Diffie-Hellman-Gruppennummern	Die Diffie-Hellman-Gruppennummern definieren die Stärke des Schlüssels, der beim IKE-Prozess (Internet Key Exchange, Internetschlüsselaustausch) verwendet wird. Höhere Gruppennummern sind sicherer, erfordern jedoch mehr Zeit für die Berechnung des Schlüssels. Standardmäßig sind alle Gruppen ausgewählt. Sie müssen mindestens eine der ausgewählten Gruppen auf Ihrem lokalen Gateway-Gerät für jede IKE-Phase konfigurieren.
Lebensdauer (Sekunden)	Der Wert 'Lebensdauer' bestimmt die Zeitspanne einer Verbindungsinstanz mit einem Satz von Verschlüsselungs-/Authentifizierungsschlüsseln für Benutzerpakete, von der erfolgreichen Aushandlung bis zum Ablaufzeitpunkt. Bereich für Phase 1: 900-28800 Sekunden

Parameter	Beschreibung
	(Vorgabe: 28800). Bereich für Phase 2: 900-3600 Sekunden (Vorgabe: 3600). Die Lebensdauer für Phase 2 muss kleiner sein als die Lebensdauer für Phase 1. Die Verbindung wird, bevor sie abläuft, über den Schlüsselkanal neu ausgehandelt. Vergleiche den Abschnitt '**Grenzzeit bis zur Schlüsselerneuerung**'. Wenn sich die lokale und die Remote-Seite nicht über die Lebensdauer einig sind, kommt es auf der Seite mit der längeren Lebensdauer zu einem Wust von überflüssigen Verbindungen. Siehe außerdem die Abschnitte '**Grenzzeit bis zur Schlüsselerneuerung** und '**Schlüsselerneuerungsvarianz**'.
Grenzzeit bis zur Schlüsselerneuerung (Sekunden)	Die Grenzzeit (Englisch: Rekey Margin Time) bevor die Verbindung oder der Schlüsselkanal abläuft, während der die lokale Seite der VPN-Verbindung versucht, einen Ersatzschlüssel auszuhandeln. Die Schlüsselerneuerungszeit (Englisch: Rekey Time) wird zufällig variiert und zwar nach dem Wert für die **Schlüsselerneuerungsvarianz**. Ist nur lokal relevant. Die Remote-Seite (Gegenstelle) muss dem nicht zustimmen. Bereich: 900-3600 Sekunden. Der Standardwert ist 3600.
Replay-Fenstergröße (Paket)	Die IPsec-Replay-Fenstergröße (Replay = Wiedereinspielung von übertragenen Daten) für diese Verbindung. Der Standardwert -1 verwendet den Wert, der mit 'charon.replay_window' in der Datei 'strongswan.conf' konfiguriert wurde. Werte größer als 32 werden nur unterstützt, wenn das Netlink-Backend verwendet wird. Ein Wert von 0 deaktiviert den IPsec-Replay-Schutz.
Schlüsselerneuerungsvarianz (%)	Der maximale Prozentsatz, um den die Werte für 'marginbytes', 'marginpackets' und 'margintime' zufällig erhöht werden, um die Schlüsselerneuerungsintervalle zufällig zu variieren (wichtig für Hosts mit vielen gleichzeitigen Verbindungen).

Parameter	Beschreibung
	Diese Wert für die Schlüsselerneuerungsvarianz (Englisch: Rekey Fuzz) kann 100% überschreiten. Der Wert von 'marginTYPE' darf nach der zufälligen Erhöhung 'lifeTYPE' nicht überschreiten, wobei 'TYPE' für Bytes, Pakete oder Zeit steht. Ein Wert von 0% deaktiviert die Zufallsverteilung. Ist nur lokal relevant. Die Remote-Seite (Gegenstelle) muss dem nicht zustimmen.
DPD-Timeout (Sekunden)	Die Zeit, nach der ein DPD-Zeitüberschreitung (Dead Peer Detection) auftritt. Sie können einen Wert von 30 oder höher spezifizieren. Der Standardwert ist 30.
Aktion bei DPD-Timeout	Die Aktion, die ausgeführt werden soll, wenn eine DPD-Zeitüberschreitung (Dead Peer Detection) auftritt. **Neustart** – Die Sitzung wird neu gestartet, wenn es zu einer DPD-Zeitüberschreitung kommt. **Löschen** – Die Sitzung wird gelöscht, wenn es zu einer DPD-Zeitüberschreitung kommt. **Ohne** – Keine Aktion durchführen, wenn es zu einer DPD-Zeitüberschreitung kommt
Aktion bei Start	Bestimmt, welche Seite die Verbindung initiiert und den Tunnel für die VPN-Verbindung aufbaut. **Hinzufügen** – Ihr lokales VPN-Gateway initiiert die Verbindung. **Start** – das Cloud-VPN-Gateway initiiert die Verbindung. **Route** – eignet sich für VPN-Gateways, die die Route-Option unterstützen. Der Tunnel ist nur dann aktiv, wenn ein Datenverkehr vom lokalen VPN-Gateway oder vom Cloud VPN-Gateway initiiert wird.

Empfehlungen für die Verfügbarkeit der Active Directory-Domänendienste

Wenn sich Ihre geschützten Workloads an einem Domain Controller authentifizieren müssen, empfehlen wir, dass Sie eine Active Directory Domain Controller (AD DC)-Instanz auf der Disaster Recovery-Site haben.

Active Directory Domain Controller für L2-OpenVPN-Konnektivität

Mit der L2-OpenVPN-Konnektivität bleiben die IP-Adressen der geschützten Workloads bei einem Test- oder Produktions-Failover in der Cloud-Site erhalten. Daher hat der AD DC während eines Test- oder Produktions-Failovers die gleiche IP-Adresse wie am lokalen Standort.

Mit einer benutzerdefinierten DNS-Konfiguration können Sie Ihren eigenen benutzerdefinierten DNS-Server für alle Cloud Server festlegen. Weitere Informationen finden Sie im Abschnitt '"Benutzerdefinierte DNS-Server konfigurieren" (S. 48)'.

Active Directory Domain Controller für L3-IPsec-VPN-Konnektivität

Mit der L3-IPsec-VPN-Konnektivität bleiben die IP-Adressen der geschützten Workloads nicht in der Cloud-Site erhalten. Daher empfehlen wir, dass Sie eine zusätzliche dedizierte AD DC-Instanz als primären Server in der Cloud-Site haben, bevor Sie einen Produktions-Failover durchführen.

Die Empfehlungen für eine dedizierte AD DC-Instanz, die als primärer Server in der Cloud-Site konfiguriert wird, sehen folgendermaßen aus:

- Schalten Sie die Windows-Firewall aus.
- Verknüpfen Sie den primären Server mit dem Active Directory-Dienst.
- Stellen Sie sicher, dass der primäre Server auf das Internet zugreifen kann.
- Fügen Sie die Active Directory-Funktion hinzu.

Mit einer benutzerdefinierten DNS-Konfiguration können Sie Ihren eigenen benutzerdefinierten DNS-Server für alle Cloud Server festlegen. Weitere Informationen finden Sie im Abschnitt '"Benutzerdefinierte DNS-Server konfigurieren" (S. 48)'.

Einen Point-to-Site-VPN-Remote-Zugriff konfigurieren

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Wenn Sie eine Remote-Verbindung zu Ihrem lokalen Standort aufbauen müssen, können Sie die Point-to-Site-Verbindung zum lokalen Standort konfigurieren. Sie können die nachfolgende Prozedur befolgen oder sich das Video-Tutorial ansehen.

Voraussetzungen

- Es wurde eine Site-to-Site-OpenVPN-Konnektivität konfiguriert.
- Die VPN-Appliance wurde am lokalen Standort installiert.

So können Sie eine Point-to-Site-Verbindung zum lokalen Standort konfigurieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie auf **Eigenschaften anzeigen**.
3. Aktivieren Sie die Option **VPN-Zugriff auf den lokalen Standort**.
4. Stellen Sie sicher, dass Ihr Benutzer, der die Point-to-Site-Verbindung zum lokalen Standort aufbauen muss, Folgendes hat:
   - ein Benutzerkonto in Cyber Protect Cloud. Diese Anmeldedaten werden für die Authentifizierung im VPN-Client verwendet. Ansonsten müssen Sie ein Benutzerkonto in Cyber Protect Cloud erstellen.
   - eine Benutzerrolle 'Firmenadministrator' oder 'Cyber Protection'.
5. Den OpenVPN-Client konfigurieren:
   a. Sie können den OpenVPN-Client v2.4.0 oder höher von dieser Adresse herunterladen: https://openvpn.net/community-downloads/.
   b. Installieren Sie den OpenVPN-Client auf derjenigen Maschine, von der aus Sie sich mit dem lokalen Standort verbinden wollen.
   c. Klicken Sie auf **Konfiguration für OpenVPN herunterladen**. Die Konfigurationsdatei ist auf Benutzer in Ihrer Organisation anwendbar, die die Benutzerrolle 'Firmenadministrator' oder 'Cyber Protection' haben.
   d. Importieren Sie die heruntergeladene Konfiguration in die OpenVPN-Einstellungen.
   e. Melden Sie mit Ihren Benutzeranmeldedaten von Cyber Protect Cloud am OpenVPN-Client an (siehe Schritt 4 weiter oben).
   f. [Optional] Wenn für Ihre Organisation eine Zwei-Faktor-Authentifizierung aktiviert ist, müssen Sie den einmaligen TOTP-Code (Einmalkennwort) bereitstellen.

Wichtig
Wenn Sie die Zwei-Faktor-Authentifizierung für Ihr Konto aktiviert haben, müssen Sie die Konfigurationsdatei neu generieren und für Ihre vorhandenen OpenVPN-Clients erneuern. Die Benutzer müssen sich erneut an Cyber Protect Cloud anmelden, um die Zwei-Faktor-Authentifizierung für ihre Konten einzurichten.

Anschließend kann sich Ihr Benutzer mit Maschinen am lokalen Standort verbinden.

Netzwerkverwaltung

In diesem Abschnitt werden verschiedene Szenarien für die Netzwerkverwaltung beschrieben.

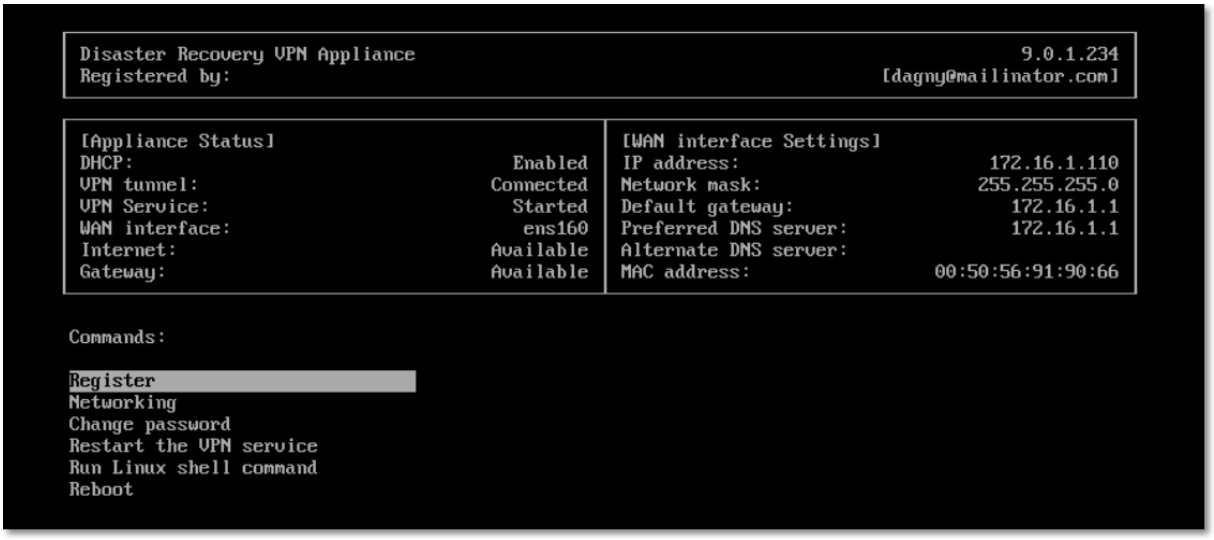
Netzwerke verwalten

Hinweis
In Abhängigkeit davon, welches Lizenzierungsmodell angewendet wird, kann für einige Funktionen eine zusätzliche Lizenzierung erforderlich sein.

Site-to-Site-OpenVPN-Verbindung

So können Sie ein Netzwerk am lokalen Standort hinzufügen und dieses in die Cloud erweitern

1. Richten Sie auf der VPN-Appliance eine neue Netzwerkschnittstelle mit dem lokalen Netzwerk ein, welches Sie in die Cloud erweitern wollen.
2. Melden Sie sich an der Konsole der VPN-Appliance an.
3. Konfigurieren Sie im Bereich **Netzwerk** die Netzwerkeinstellungen für die neue Schnittstelle.



Die Appliance beginnt, Informationen über die Netzwerke von allen aktiven Schnittstellen an Cyber Disaster Recovery Cloud zu melden. Die Cyber Protect-Konsole zeigt die Schnittstellen basierend auf den Informationen der VPN-Appliance an.

So können Sie ein Netzwerk, das in die Cloud erweitert ist, löschen

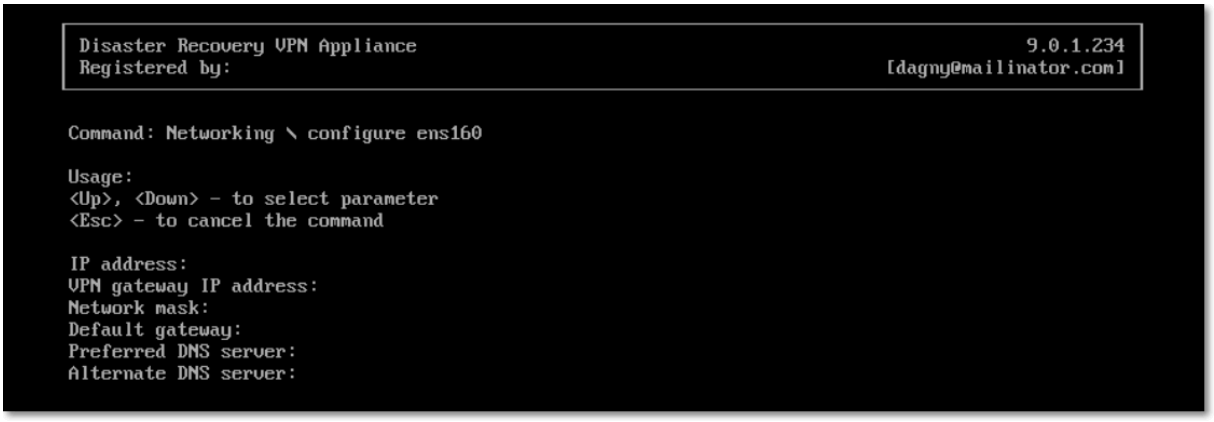
1. Melden Sie sich an der Konsole der VPN-Appliance an.
2. Wählen Sie im Bereich **Netzwerk** die Schnittstelle, die Sie löschen wollen, und klicken Sie dann auf **Netzwerkeinstellungen bereinigen**.
3. Bestätigen Sie die Aktion.

Als Ergebnis wird die lokale Netzwerkerweiterung in die Cloud über einen sicheren VPN-Tunnel gestoppt. Dieses Netzwerk wird als unabhängiges Cloud-Segment arbeiten. Wenn diese Schnittstelle verwendet wird, um den Datenverkehr von der/zur Cloud-Site durchzuleiten, werden alle Ihre Netzwerkverbindungen von der/zur Cloud-Site getrennt.

So können Sie die Netzwerkparameter ändern

1. Melden Sie sich an der Konsole der VPN-Appliance an.
2. Wählen Sie im Bereich **Netzwerk** die Schnittstelle, die Sie bearbeiten wollen.
3. Klicken Sie auf **Netzwerkeinstellungen bearbeiten**.
4. Wählen Sie eine der zwei möglichen Optionen:

- Bei einer automatischen Netzwerkkonfiguration per DHCP: klicken Sie auf **DHCP verwenden**. Bestätigen Sie die Aktion.
- Bei einer manuellen Netzwerkkonfiguration: klicken Sie auf **Statische IP-Adresse festlegen**. Folgende Einstellungen können bearbeitet werden:
  - **IP-Adresse**: die IP-Adresse der Schnittstelle im lokalen Netzwerk.
  - **IP-Adresse des VPN-Gateway**: die spezielle IP-Adresse, die für das Cloud-Segment des Netzwerks reserviert ist, damit der Cyber Disaster Recovery Cloud Service ordnungsgemäß funktionieren kann.
  - **Netzwerk-Maske**: die Netzwerk-Maske des lokalen Netzwerks.
  - **Standard-Gateway**: das Standard-Gateway am lokalen Standort.
  - **Bevorzugter DNS-Server**: der primäre DNS-Server am lokalen Standort.
  - **Alternativer DNS-Server**: der sekundäre DNS-Server am lokalen Standort.



- Nehmen Sie die erforderlichen Änderungen vor und bestätigen Sie diese durch Drücken der Eingabetaste.

'Nur Cloud'-Modus

Sie können bis zu 23 Netzwerke in der Cloud haben.

So können Sie ein neues Cloud-Netzwerk hinzufügen

1. Gehen Sie zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie bei **Cloud-Site** auf **Cloud-Netzwerk hinzufügen**.
3. Definieren Sie die Parameter des Cloud-Netzwerks: die Netzwerkadresse und Netzwerkmaske. Wenn Sie dies abgeschlossen haben, klicken Sie auf **Fertig**.

Anschließend wird das zusätzliche Cloud-Netzwerk mit der definierten Adresse und Netzwerkmaske auf der Cloud-Site bereitgestellt.

So können Sie ein Cloud-Netzwerk löschen

Hinweis
Sie können ein Cloud-Netzwerk nicht löschen, solange sich noch wenigstens ein Cloud Server darin befindet. Löschen Sie dann zuerst den Cloud Server und anschließend das Netzwerk.

1. Gehen Sie zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie bei **Cloud-Site** auf die Netzwerkadresse, die Sie löschen wollen.
3. Klicken Sie auf **Löschen** und bestätigen Sie die Aktion.

So können Sie die Cloud-Netzwerkparameter ändern

1. Gehen Sie zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie bei **Cloud-Site** auf die Netzwerkadresse, die Sie bearbeiten wollen.
3. Klicken Sie auf **Bearbeiten**.
4. Definieren Sie die Netzwerkadresse und Netzwerkmaske und klicken Sie dann auf **Fertig**.

Rekonfiguration der IP-Adresse

Für eine optimale Disaster Recovery-Performance müssen die IP-Adressen, die den lokalen und Cloud-Servern zugewiesen werden, konsistent sein. Wenn Inkonsistenzen oder Unstimmigkeiten bei den IP-Adressen vorliegen, sehen Sie ein Ausrufezeichen neben dem entsprechenden Netzwerk bei **Disaster Recovery** –> **Verbindung**.

Nachfolgend sind einige gängige Gründe für Inkonsistenzen mit IP-Adressen aufgeführt:

1. Ein Recovery-Server wurde von einem Netzwerk in ein anderes migriert oder die Netzwerkmaske des Cloud-Netzwerks wurde geändert. Infolgedessen haben Cloud-Server die IP-Adressen aus Netzwerken, mit denen sie nicht verbunden sind.
2. Der Verbindungstyp wurde von einer 'Ohne Site-to-Site'-Verbindung zu einer Site-to-Site-Verbindung umgestellt. Dadurch wird ein lokaler Server in ein anderes Netzwerk platziert als das, welches für den Recovery-Server in der Cloud-Site erstellt wurde.
3. Der Verbindungstyp wurde von Site-to-Site-OpenVPN zu Multi-Site-IPsec-VPN umgestellt – oder von Multi-Site-IPsec-VPN zu Site-to-Site-OpenVPN. Weitere Informationen zu diesem Szenario finden Sie in den Abschnitten 'Verbindungen wechseln' und 'IP-Adressen neu zuweisen'.
4. Bearbeiten der folgenden Netzwerkparameter auf der VPN-Appliance-Site:
   - Hinzufügen einer Schnittstelle über die Netzwerkeinstellungen
   - Manuelles Bearbeiten der Netzwerkmaske über die Schnittstelleneinstellungen
   - Bearbeiten der Netzwerkmaske über DHCP
   - Manuelles Bearbeiten der Netzwerkadresse und Netzwerkmaske über die Schnittstelleneinstellungen
   - Bearbeiten der Netzwerkmaske und Netzwerkadresse über DHCP

Als Ergebnis dieser aufgeführten Aktionen kann das Netzwerk in der Cloud-Site eine Teilmenge oder Obermenge des lokalen Netzwerks werden – oder die VPN-Appliance-Schnittstelle kann die gleichen Netzwerkeinstellungen für verschiedene Schnittstellen melden.

So können Sie das Problem mit den Netzwerkeinstellungen lösen

1. Klicken Sie auf das Netzwerk, dessen IP-Adresse rekonfiguriert werden muss.
   Sie sehen eine Liste der Server in dem ausgewählten Netzwerk, deren Status und IP-Adressen. Server, deren Netzwerkeinstellungen inkonsistent sind, sind mit einem Ausrufezeichen gekennzeichnet.
2. Wenn Sie die Netzwerkeinstellungen eines Servers ändern wollen, müssen Sie auf **Zu Server gehen** klicken. Wenn Sie die Netzwerkeinstellungen für alle Server gemeinsam ändern wollen, müssen Sie im Benachrichtigungsblock auf **Ändern** klicken.
3. Ändern Sie die IP-Adressen nach Bedarf, indem Sie diese in den Feldern **Neue IP** und **Neue Test-IP** definieren.
4. Wenn Sie dies abgeschlossen haben, klicken Sie auf **Bestätigen**.

Server zu einem geeigneten Netzwerk verschieben

Wenn Sie einen Disaster Recovery-Schutzplan erstellen und diesen auf ausgewählte Geräte anwenden, überprüft das System die entsprechenden IP-Adressen der Geräte und erstellt dann automatisch Cloud-Netzwerke, wenn es noch keine Cloud-Netzwerke gibt, zu denen die IP-Adresse passen würden. Standardmäßig sind die Cloud-Netze mit den maximalen Bereichen konfiguriert, die von der IANA für den privaten Gebrauch empfohlen werden (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Sie können Ihr Netzwerk eingrenzen, indem Sie die Netzwerkmaske bearbeiten.

Falls sich die ausgewählten Geräte in mehreren lokalen Netzwerken befinden, kann das Netzwerk auf der Cloud-Site zu einer Obermenge der lokalen Netzwerke werden. Gehen Sie in diesem Fall folgendermaßen vor, um die Cloud-Netzwerke zu rekonfigurieren:

1. Klicken Sie zuerst auf das Cloud-Netzwerk, das eine Rekonfiguration der Netzwerkgröße erfordert, und klicken Sie dann auf **Bearbeiten**.
2. Rekonfigurieren Sie die Netzwerkgröße mit den passenden Einstellungen.
3. Erstellen Sie bei Bedarf weitere Netzwerke.
4. Klicken Sie neben der Anzahl der Geräte, die mit dem Netzwerk verbunden sind, auf das Benachrichtigungssymbol.
5. Klicken Sie auf **Zu einem geeigneten Netzwerk verschieben**.
6. Wählen Sie die Server aus, die Sie in die geeigneten Netzwerke verschieben wollen, und klicken Sie dann auf **Verschieben**.

Die Einstellungen der VPN-Appliance verwalten

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

In der Cyber Protect-Konsole (**Disaster Recovery** –> **Verbindung**) können Sie:

- Die Protokolldateien herunterladen.
- Die Registrierung der Appliance aufheben (wenn Sie die Einstellungen der VPN-Appliance zurücksetzen oder zum 'Nur Cloud'-Modus wechseln müssen).

Wenn Sie auf diese Einstellungen zugreifen wollen, klicken Sie im Block **VPN-Appliance** auf das **i**-Symbol.

In der VPN-Appliance-Konsole können Sie:

- Das Kennwort für die Appliance ändern.
- Die Netzwerkeinstellungen einsehen/ändern und definieren, welche Schnittstelle als WAN-Schnittstelle für die Internetverbindung verwendet werden soll.
- Das Registrierungskonto registrieren/ändern (durch Wiederholung der Registrierung).
- Den VPN-Dienst neu starten.
- Die VPN-Appliance neu booten.
- Einen Linux-Shell-Befehl ausführen (nur für fortgeschrittene Fehlerbehebungsfälle).

Das VPN-Gateway neu installieren

Wenn es ein nicht behebbares Problem mit dem VPN-Gateway gibt, wollen Sie das VPN-Gateway möglicherweise neu installieren. Zu den möglichen Problemen, die dabei auftauchen können, gehören:

- Das VPN-Gateway befindet sich im Status **Fehler**.
- Das VPN-Gateway befindet sich für längere Zeit im Status **Ausstehend**.
- Der Status des VPN-Gateways bleibt für längere Zeit unbestimmt.

Der Prozess zur Neuinstallation des VPN-Gateways umfasst folgende automatische Aktionen: die vorhandene virtuelle Maschine des VPN-Gateways vollständig löschen, eine neue virtuelle Maschine aus der Vorlage installieren sowie die Einstellungen des vorherigen VPN-Gateways auf die neue virtuelle Maschine anwenden.

Voraussetzungen:

Einer der Verbindungstypen zur Cloud-Site muss festgelegt sein.

So können Sie das VPN-Gateway neu installieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie auf das Zahnradsymbol des VPN-Gateways und wählen Sie den Befehl **VPN-Gateway neu installieren**.
3. Geben Sie im Dialog **VPN-Gateway neu installieren** Ihre Anmeldedaten ein.
4. Klicken Sie auf **Neu installieren**.

Die Site-to-Site-Verbindung (de)aktivieren

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

In folgenden Fällen können Sie die Site-zu-Site-Verbindung aktivieren:

- Wenn die Cloud Server in der Cloud-Site mit den Servern am lokalen Standort kommunizieren müssen.
- Nach einem Failover in die Cloud wurde die lokale Infrastruktur wiederhergestellt – und Sie wollen Ihre Server per Failback wieder zum lokalen Standort zurücksetzen.

So können Sie die Site-to-Site-Verbindung aktivieren

1. Gehen Sie zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie auf **Eigenschaften anzeigen** und aktivieren Sie die Option **Site-to-Site-Verbindung**.

Infolgedessen wird die Site-to-Site-VPN-Verbindung zwischen dem lokalen Standort und der Cloud-Site aktiviert. Der Cyber Disaster Recovery Cloud Service ruft die Netzwerkeinstellungen von der VPN-Appliance ab und erweitert die lokalen Netzwerke in die Cloud-Site.

Wenn Ihre Cloud Server in der Cloud-Site nicht mit den Servern am lokalen Standort kommunizieren müssen, können Sie die Site-to-Site Verbindung deaktivieren.

So können Sie die Site-to-Site-Verbindung deaktivieren

1. Gehen Sie zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie zuer auf **Eigenschaften anzeigen** und deaktivieren Sie dann die Option **Site-to-Site-Verbindung**.

Als Ergebnis wird die Verbindung vom lokalen Standort zur Cloud-Site getrennt.

Den Site-to-Site-Verbindungstyp wechseln

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Sie können einfach von einer Site-to-Site-OpenVPN- zu einer Multi-Site-IPsec-VPN-Verbindung wechseln – oder von einer Multi-Site-IPsec-VPN- zu einer Site-to-Site-OpenVPN-Verbindung.

Wenn Sie den Verbindungstyp wechseln, werden gerade aktive VPN-Verbindungen gelöscht, aber die Cloud Server und Netzwerkkonfigurationen bleiben erhalten. Sie müssen jedoch noch die IP-Adressen der Cloud-Netzwerke und Cloud Server neu zuweisen.

Die folgende Tabelle vergleicht die grundlegenden Eigenschaften der Site-to-Site-OpenVPN- und der Multi-Site-IPsec-VPN-Verbindung.

	Site-to-Site-OpenVPN	**Multi-Site-IPsec-VPN**
Unterstützung für lokalen Standort	Einzel	Einzel, Mehrere
VPN-Gateway-Modus	L2 Open VPN	L3 IPsec VPN
Netzwerksegmente	Erweitert das lokale Netzwerk in das Cloud-Netzwerk	Lokale und Cloud-Netzwerksegmente sollten sich nicht überlappen
Unterstützt Point-to-Site-Zugriffe auf den lokalen Standort	Ja	Nein
Unterstützt Point-to-Site-Zugriffe auf die Cloud-Site	Ja	Ja
Erfordert ein Angebotselement 'Öffentliche IP'	Nein	Ja

So können Sie von einer Site-to-Site-OpenVPN- zu einer Multi-Site-IPsec-VPN-Verbindung wechseln

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie auf **Eigenschaften anzeigen**.
3. Klicken Sie auf **Zu Multi-Site-IPsec-VPN wechseln**.
4. Klicken Sie auf **Rekonfigurieren**.
5. Weisen Sie die IP-Adressen des Cloud-Netzwerks und der Cloud Server neu zu.
6. Konfigurieren Sie die Multi-Site-IPsec-Verbindungseinstellungen.

So können Sie von einer Multi-Site-IPsec-VPN- zu einer Site-to-Site-OpenVPN-Verbindung wechseln

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie auf **Eigenschaften anzeigen**.
3. Klicken Sie auf **Zu Site-to-Site-OpenVPN wechseln**.

4. Klicken Sie auf **Rekonfigurieren**.
5. Weisen Sie die IP-Adressen des Cloud-Netzwerks und der Cloud Server neu zu.
6. Konfigurieren Sie die Site-to-Site-Verbindungseinstellungen.

IP-Adressen neu zuweisen

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Sie müssen die IP-Adressen der Cloud-Netzwerke und der Cloud Server neu zuweisen, um die Konfiguration in folgenden Fällen abschließen zu können:

- Nachdem Sie von einer Site-to-Site-OpenVPN- zu einer Multi-Site-IPsec-VPN-Konnektivität umgestellt haben – oder umgekehrt.
- Nachdem Sie einen Schutzplan angewendet haben (wenn die Multi-Site-IPsec-VPN-Konnektivität konfiguriert wurde).

So können Sie die IP-Adresse eines Cloud-Netzwerks neu zuweisen

1. Klicken Sie in der Registerkarte **Verbindung** auf die IP-Adresse des Cloud-Netzwerks.
2. Klicken Sie im sich öffnenden Dialogfenster **Netzwerk** auf den Befehl **Bearbeiten**.
3. Geben Sie die neue Netzwerkadresse und Netzwerkmaske ein.
4. Klicken Sie auf **Fertig**.

Nachdem Sie die IP-Adresse eines Cloud-Netzwerks neu zugewiesen haben, müssen Sie auch die Cloud Server neu zuweisen, die zu dem neu zugewiesenen Cloud-Netzwerk gehören.

So können Sie die IP-Adresse eines Servers neu zuweisen

1. Klicken Sie in der Registerkarte **Verbindung** auf die IP-Adresse des Servers im Cloud-Netzwerk.
2. Klicken Sie im sich öffnenden Dialogfenster **Server** auf den Befehl **IP-Adresse ändern**.
3. Geben Sie im sich öffnenden Dialogfenster **IP-Adresse ändern** die neue IP-Adresse des Servers ein – oder verwenden Sie die automatisch generierte IP-Adresse, die zum neu zugewiesenen Cloud-Netzwerk gehört.

   Hinweis
   Cyber Disaster Recovery Cloud weist allen Cloud Servern, die vor der Neuzuweisung der Netzwerk-IP-Adresse zum Cloud-Netzwerk gehörten, automatisch IP-Adressen aus dem Cloud-Netzwerk zu. Sie können die vorgeschlagenen IP-Adressen verwenden, um die IP-Adressen aller Cloud Server gemeinsam neu zuzuweisen.

4. Klicken Sie auf **Bestätigen**.

Benutzerdefinierte DNS-Server konfigurieren

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Wenn Sie eine Verbindung (Konnektivität) konfigurieren, erstellt Cyber Disaster Recovery Cloud Ihre Cloud-Netzwerkinfrastruktur. Der Cloud-DHCP-Server weist den Recovery-Servern und den primären Servern automatisch Standard-DNS-Server zu. Sie können diese Standardeinstellungen aber jederzeit ändern und eigene DNS-Server konfigurieren. Die neuen DNS-Einstellungen werden bei der nächsten Anfrage an den DHCP-Server angewendet.

Voraussetzungen:

Einer der Verbindungstypen zur Cloud-Site muss festgelegt sein.

So können Sie einen benutzerdefinierten DNS-Server konfigurieren

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie auf **Eigenschaften anzeigen**.
3. Klicken Sie auf **Standard (von der Cloud-Site bereitgestellt)**.
4. Wählen Sie **Benutzerdefinierte Server**.
5. Geben Sie die IP-Adresse des DNS-Servers ein.
6. [Optional] Wenn Sie einen weiteren DNS-Server hinzufügen wollen, klicken Sie auf **Hinzufügen** und geben Sie dann die IP-Adresse dieses DNS-Servers ein.

   Hinweis
   Wenn Sie die benutzerdefinierten DNS-Server hinzugefügt haben, können Sie auch noch die Standard-DNS-Server hinzufügen. Dadurch wird Cyber Disaster Recovery Cloud auf die Standard-DNS-Server zurückgreifen können, wenn die benutzerdefinierten DNS-Server einmal nicht verfügbar sein sollten.

7. Klicken Sie auf **Fertig**.

Benutzerdefinierte DNS-Server löschen

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Sie können DNS-Server aus der benutzerdefinierten DNS-Liste löschen.

Voraussetzungen:

Benutzerdefinierte DNS-Server sind konfiguriert.

So können Sie einen benutzerdefinierten DNS-Server löschen

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie auf **Eigenschaften anzeigen**.
3. Klicken Sie auf **Benutzerdefinierte Server**.
4. Klicken Sie neben dem DNS-Server auf das Symbol 'Löschen'.

   Hinweis
   Die Löschaktion ist deaktiviert, wenn nur ein benutzerdefinierter DNS-Server verfügbar ist. Wenn Sie alle benutzerdefinierten DNS-Server löschen wollen, müssen Sie **Standard (von der Cloud-Site bereitgestellt)** auswählen.

5. Klicken Sie auf **Fertig**.

MAC-Adressen herunterladen

Sie können eine Liste von MAC-Adressen herunterladen, diese dann extrahieren und anschießend in die Konfiguration Ihres benutzerdefinierten DHCP-Servers importieren.

Voraussetzungen:

- Einer der Verbindungstypen zur Cloud-Site muss festgelegt sein.
- Es muss mindestens ein primärer Server oder Recovery-Server mit einer MAC-Adresse konfiguriert werden.

So können Sie die Liste der MAC-Adressen herunterladen

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie auf **Eigenschaften anzeigen**.
3. Klicken Sie auf **Die Liste der MAC-Adressen herunterladen** und speichern Sie dann die CSV-Datei.

Lokales Routing konfigurieren

Neben Ihren lokalen Netzwerken, die über die VPN-Appliance in die Cloud erweitert sind, haben Sie möglicherweise noch andere lokale Netzwerke, die nicht in der VPN-Appliance registriert sind, aber deren Server dennoch mit den Cloud Servern kommunizieren müssen. Um eine Verbindung zwischen solchen lokalen Servern und den Cloud Servern herzustellen, müssen Sie die Einstellungen für das lokale Routing konfigurieren.

So können Sie ein lokales Routing konfigurieren

1. Gehen Sie zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie auf **Eigenschaften anzeigen** und anschließend auf **Lokales Routing**.
3. Spezifizieren Sie die lokalen Netzwerke in der CIDR-Notation.
4. Klicken Sie auf **Speichern**.

Als Ergebnis können die Server aus den spezifizierten lokalen Netzwerken mit den Cloud Servern kommunizieren.

DHCP-Traffic über L2-VPN zulassen

Wenn Geräte an Ihrem lokalen Standort ihre IP-Adresse von einem DHCP-Server beziehen, können Sie diesen DHCP-Server per Disaster Recovery schützen, indem Sie ihn per Failover in die Cloud verlagern und dann den DHCP-Datenverkehr über ein L2-VPN laufen lassen. Auf diese Weise wird Ihr DHCP-Server in der Cloud ausgeführt, von wo er aber weiterhin Ihren lokalen Geräten deren IP-Adressen zuweisen kann.

Voraussetzungen:

Es muss ein Site-to-Site-L2-VPN-Verbindungstyp zur Cloud-Site festgelegt werden.

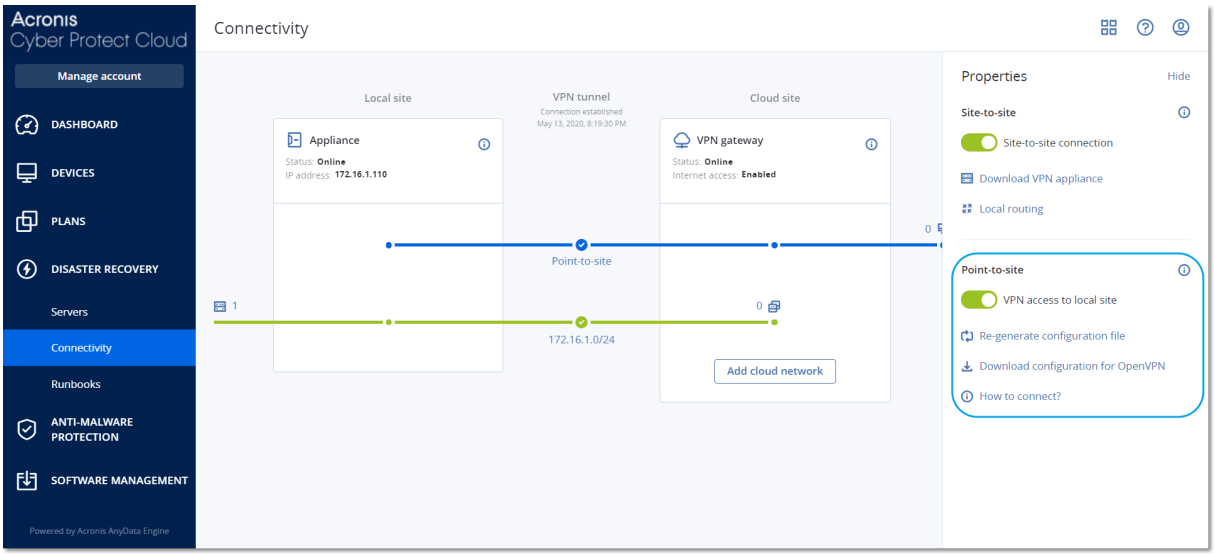
So können Sie den DHCP-Traffic über die L2-VPN-Verbindung zulassen

1. Gehen Sie zu Registerkarte **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie auf **Eigenschaften anzeigen**.
3. Aktivieren Sie den Schalter **DHCP-Traffic über L2-VPN zulassen**.

Einstellungen der Point-to-Site-Verbindung verwalten

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung** und klicken Sie dann in der rechten oberen Ecke auf **Eigenschaften anzeigen**.



VPN-Zugriff auf den lokalen Standort

Diese Option wird verwendet, um den VPN-Zugriff auf den lokalen Standort zu verwalten. Die Option ist standardmäßig aktiviert. Wenn sie deaktiviert ist, wird kein Point-to-Site-Zugriff auf den lokalen Standort erlaubt.

Konfiguration für OpenVPN herunterladen

Mit diesem Befehl wird die Konfigurationsdatei für den OpenVPN-Client heruntergeladen. Diese Datei ist erforderlich, um eine Point-to-Site-Verbindung zur Cloud-Site aufzubauen.

Konfigurationsdatei neu generieren

Sie können die Konfigurationsdatei für den OpenVPN-Client neu generieren.

Dies ist in folgenden Fällen erforderlich:

- Wenn Sie annehmen, dass die Konfigurationsdatei kompromittiert sein könnte.
- Wenn die Zwei-Faktor-Authentifizierung für Ihr Konto aktiviert wurde.

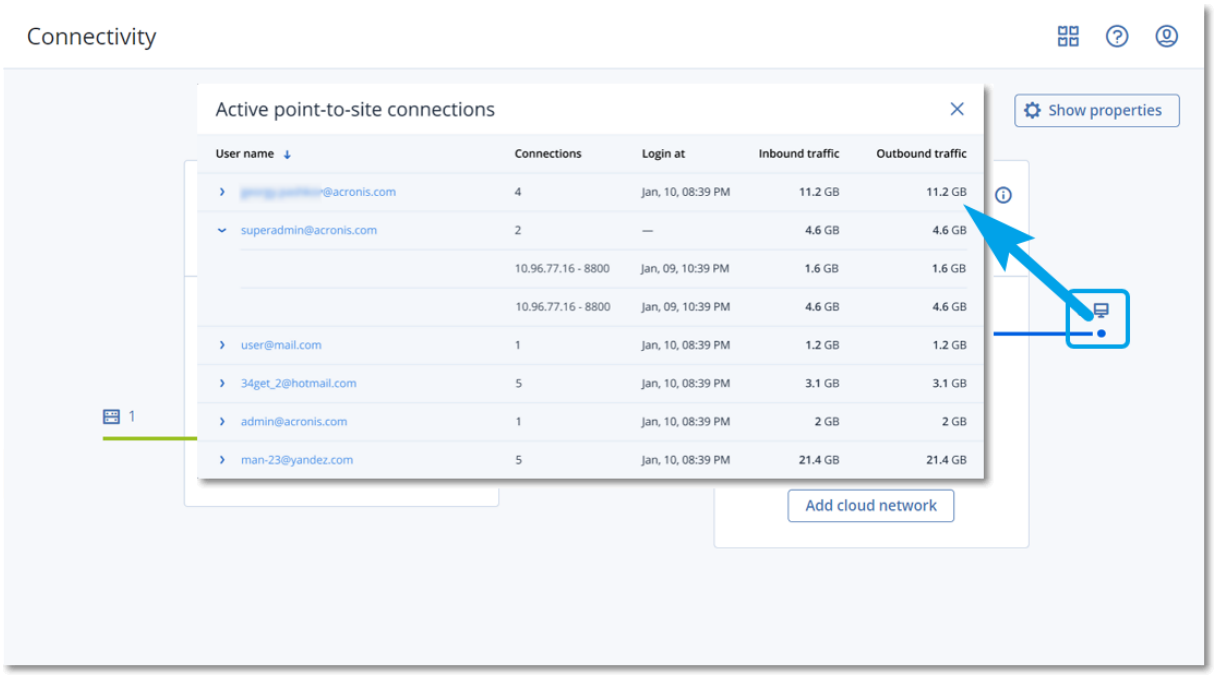
Sobald die Konfigurationsdatei aktualisiert wurde, ist keine Verbindung mehr über die alte Konfigurationsdatei möglich. Stellen Sie sicher, dass die neue Datei an alle Benutzer verteilt wird, die die Point-to-Site-Verbindung verwenden dürfen.

Aktive Point-to-Site-Verbindungen

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Sie können alle aktiven Point-to-Site-Verbindungen im Bereich **Disaster Recovery** –> **Verbindung** einsehen. Klicken Sie in der blauen **Point-to-Site**-Linie auf das Maschinen-Symbole und Ihnen

werden ausführliche Informationen über die aktiven Point-to-Site-Verbindungen (nach Benutzernamen gruppiert) angezeigt.



Mit Protokollen arbeiten

Die Disaster Recovery-Funktionalität sammelt Protokolle für die VPN-Appliance und das VPN-Gateway. Die Protokolle werden als .txt-Dateien gespeichert, die dann in einem .zip-Archiv komprimiert werden. Sie können das Archiv herunterladen, anschließend extrahieren und die Informationen zur Fehlerbehebung oder zum Monitoring verwenden.

Die folgende Liste beschreibt die Protokolldateien, die Teil des .zip-Archivs sind, und die darin enthaltenen Informationen.

`dnsmasq.config.txt` – Die Datei enthält Informationen über die Konfiguration des Dienstes, der DNS- und DHCP-Adressen bereitstellt.

`dnsmsq.leases.txt` – Die Datei enthält Informationen über die aktuellen DHCP-Adressleases.

`dnsmasq_log.txt` – Die Datei enthält Protokolle des dnsmasq-Dienstes.

`ebtables.txt` – Die Datei enthält Informationen über die Firewall-Tabellen.

`free.txt` – Die Datei enthält Informationen über den freien Arbeitsspeicher.

`ip.txt` – Die Datei enthält die Protokolle über die Konfiguration der Netzwerkschnittstellen, einschließlich ihrer Namen, die bei der Konfiguration der **Netzwerkpakete erfassen**-Einstellungen verwendet werden können.

`NetworkManager_log.txt` – Die Datei enthält Protokolle vom NetworkManager-Dienst.

`NetworkManager_status.txt` – Die Datei enthält Informationen über den Status des NetworkManager-Dienstes.

`openvpn@p2s_log.txt` – Die Datei enthält Protokolle vom OpenVPN-Dienst.

`openvpn@p2s_status.txt` – Die Datei enthält Informationen über den Status der VPN-Tunnel.

`ps.txt` – Die Datei enthält Informationen über die Prozesse, die gerade auf dem VPN-Gateway oder der VPN-Appliance ausgeführt werden.

`resolf.conf.txt` – Die Datei enthält Informationen über die Konfiguration der DNS-Server.

`routes.txt` – Die Datei enthält Informationen über die Netzwerk-Routen.

`uname.txt` – Die Datei enthält Informationen über die aktuelle Kernel-Version des Betriebssystems.

`uptime.txt` – Die Datei enthält Informationen über den Zeitraum, in dem das Betriebssystem nicht neu gestartet worden ist.

`vpnserver_log.txt` – Die Datei enthält Protokolle vom VPN-Dienst.

`vpnserver_status.txt` – Die Datei enthält Informationen über den Status des VPN-Servers.

Weitere Informationen zu den Protokolldateien, die für die IPsec-VPN-Konnektivität spezifisch sind, finden Sie im Abschnitt '"Multi-Site-IPSec-VPN-Protokolldateien" (S. 57)'.

Die Protokolle der VPN-Appliance herunterladen

Sie können das Archiv, das die Protokolle der VPN-Appliance enthält, herunterladen, dann extrahieren und die Informationen zur Fehlerbehebung oder zum Monitoring verwenden.

So können Sie die Protokolle der VPN-Appliance herunterladen

1. Klicken Sie auf der Seite **Verbindung** auf das Zahnradsymbol neben der VPN-Appliance.
2. Klicken Sie auf **Protokoll herunterladen**.
3. [Optional] Wählen Sie **Netzwerkpakete erfassen** und konfigurieren Sie die Einstellungen. Weitere Informationen finden Sie im Abschnitt '"Netzwerkpakete erfassen" (S. 54)'.
4. Klicken Sie auf **Fertig**.
5. Wenn das .zip-Archiv zum Herunterladen bereit ist, klicken Sie auf **Protokoll herunterladen** und speichern Sie es lokal.

Die Protokolle des VPN-Gateways herunterladen

Sie können das Archiv, das die Protokolle des VPN-Gateways enthält, herunterladen, dann extrahieren und die Informationen zur Fehlerbehebung oder zum Monitoring verwenden.

So können Sie die Protokolle des VPN-Gateways herunterladen

1. Klicken Sie auf der Seite **Verbindung** auf das Zahnradsymbol neben dem VPN-Gateway.
2. Klicken Sie auf **Protokoll herunterladen**.
3. [Optional] Wählen Sie **Netzwerkpakete erfassen** und konfigurieren Sie dann die Einstellungen. Weitere Informationen finden Sie im Abschnitt '"Netzwerkpakete erfassen" (S. 54)'.
4. Klicken Sie auf **Fertig**.

5. Wenn das .zip-Archiv zum Herunterladen bereit ist, klicken Sie auf **Protokoll herunterladen** und speichern Sie es lokal.

Netzwerkpakete erfassen

Wenn Sie die Kommunikation zwischen dem lokalen Produktionsstandort und einem primären Server oder Recovery-Server analysieren bzw. zwischen diesen auftretende Probleme beheben wollen, können Sie Netzwerkpakete auf dem VPN-Gateway oder der VPN-Appliance sammeln lassen.

Nachdem 32000 Netzwerkpakete gesammelt wurden oder das Zeitlimit erreicht wurde, wird die Netzwerkpaket-Erfassung beendet und die Ergebnisse werden in eine .libpcap-Datei geschrieben, die in das .zip-Archiv der Protokolle aufgenommen wird.

n der nachfolgenden Tabelle finden Sie weitere Informationen zu den **Netzwerkpakete erfassen**-Einstellungen, die Sie konfigurieren können.

Einstellung	Beschreibung
Netzwerkschnittstellenname	Die Netzwerkschnittstelle, über die Netzwerkpakete erfasst werden sollen. Wenn Sie Netzwerkpakete auf allen Netzwerkschnittstellen erfassen wollen, wählen Sie die Option **Alle**.
Zeitlimit (in Sekunden)	as Zeitlimit für die Erfassung von Netzwerkpaketen. Der Höchstwert, den Sie festlegen können, ist 1800.
Filterung	Ein zusätzlicher Filter, der auf die erfassten Netzwerkpakete angewendet wird. Sie können eine Zeichenfolge eingeben, die Protokolle, Ports, Richtungen sowie deren Kombinationen enthält, durch Leerzeichen getrennt – beispielsweise: "and", "or", "not", " (", ") ", "src", "dst", "net", "host", "port", "ip", "tcp", "udp", "icmp", "arp", "esp". Wenn Sie Klammern verwenden wollen, müssen Sie diese mit Leerzeichen umschließen. Sie können außerdem IP-Adressen und Netzwerkadressen eingeben. Beispielsweise: "icmp or arp" und "port 67 or 68". Weitere Informationen über die Werte, die Sie eingeben können, finden Sie in der Linux-Hilfe für tcpdump.

Probleme mit der IPsec-VPN-Konfiguration beheben

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Wenn Sie die IPsec-VPN-Verbindung konfigurieren oder verwenden, kann es gelegentlich auch zu Problemen kommen.

Wenn Sie auf Probleme stoßen, können Sie die IPsec-Protokolldateien auswerten und im Abschnitt 'IPsec-VPN-Konfigurationsprobleme beheben' nach möglichen Lösungen für gängige Probleme suchen.

IPsec-VPN-Konfigurationsprobleme beheben

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Die nachfolgende Tabelle beschreibt häufig auftretende IPsec-VPN-Konfigurationsprobleme und erläutert, wie Sie diese beheben können.

Problem	Mögliche Lösung
Ich sehe folgende Fehlermeldung: **IKE-Phase-1-Aushandlungsfehler. Überprüfen Sie die IPsec-IKE-Einstellungen auf den Cloud- und den lokalen Sites.**	Klicken Sie zuerst auf **Wiederholen** und überprüfen Sie, ob eine spezifischere Fehlermeldung erscheint. Eine solche spezifischere Fehlermeldung kann z.B. Angaben zu einer Algorithmus-Diskrepanz oder einem falschen vorinstallierten Schlüssel (PSK) enthalten. **Hinweis** Aus Sicherheitsgründen gelten für IPsec-VPN-Verbindungen folgende Einschränkungen: • IKEv1 wird in RFC8247 als nicht mehr zeitgemäß bezeichnet und aufgrund von Sicherheitsrisiken daher nicht mehr unterstützt. Es werden nur Verbindungen mit dem IKEv2-Protokoll unterstützt. • Folgende Verschlüsselungsalgorithmen gelten mittlerweile als unsicher und werden daher nicht mehr unterstützt: DES und 3DES. • Folgende Hash-Algorithmen gelten mittlerweile als unsicher und werden daher nicht mehr unterstützt: SHA1 und MD5. • Die Diffie-Hellman-Gruppennummer 2 gilt als unsicher und wird daher nicht unterstützt.
Die Verbindung zwischen meinem lokalen Standort und der Cloud-Site bleibt im Status **Verbindungsaufbau** hängen.	Überprüfen Sie: • Falls der UDP-Port 500 offen ist (wenn Sie eine Firewall verwenden). • Die Konnektivität zwischen dem lokalen

Problem	Mögliche Lösung
	Standort und der Cloud-Site. • Falls die IP-Adresse des lokalen Standorts korrekt ist.
Die Verbindung zwischen meinem lokalen Standort und der Cloud-Site bleibt im Status **Auf eine Verbindung warten** hängen.	Dieser Status wird angezeigt, wenn die **Aktion bei Start** für die Cloud-Site mit **Hinzufügen** festgelegt wurde, was bedeutet, dass die Cloud-Site darauf wartet, dass der lokale Standort die Verbindung initiiert. Die Verbindung vom lokalen Standort aus initiieren.
Die Verbindung zwischen meinem lokalen Standort und der Cloud-Site bleibt im Status **Auf Datenverkehr warten** hängen.	Dieser Zustand wird angezeigt, wenn die **Aktion bei Start** für die Cloud-Site mit **Route** festgelegt wurde. Gehen Sie wie folgt vor, wenn Sie eine Verbindung vom lokalen Standort aus erwarten: • Versuchen Sie vom lokalen Standort aus die virtuelle Maschine in der Cloud-Site anzupingen. Dies ist ein Standardverhalten, das bei einigen Geräten (z.B. Cisco ASA) zum Aufbau eines VPN-Tunnels notwendig ist. (Route-Modus) • Stellen Sie sicher, dass der lokale Standort einen VPN-Tunnel eingerichtet hat, indem Sie die **Aktion bei Start** für den lokalen Standort mit **Start** festlegen.
Die Verbindung zwischen meinem lokalen Standort und der Cloud-Site ist hergestellt, aber ich kann sehen, dass eine oder mehrere Netzwerkrichtlinien nicht funktionieren.	Dieses Problem kann folgende Ursachen haben: • Die Netzwerkzuordnung in der IPsec-Cloud-Site unterscheidet sich von der Netzwerkzuordnung am lokalen Standort. Stellen Sie sicher, dass die Netzwerk-Zuordnungen und die Abfolge der Netzwerk-Richtlinien am lokalen Standort und in der Cloud-Site genau übereinstimmen. • Dieses Stadium ist korrekt, wenn die **Aktion bei Start** des lokalen Standorts und/oder der Cloud-Site auf **Route** eingestellt ist (z.B. auf Cisco ASA-Geräten) und derzeit kein Datenverkehr stattfindet. Sie können einen Ping-Test durchführen, um sicherzustellen, dass der Tunnel korrekt aufgebaut wurde. Wenn der Ping-Test nicht funktioniert, prüfen Sie die Netzwerkzuordnung am lokalen Standort und in

Problem	Mögliche Lösung
	der Cloud-Site.
Ich möchte eine bestimmte IPsec-Verbindung neu starten.	So können Sie eine bestimmte IPsec-Verbindung neu starten: 1. Klicken Sie in der Anzeige **Disaster Recovery** –> **Verbindung** auf die gewünschte IPsec-Verbindung. 2. Klicken Sie auf **Verbindung deaktivieren**. 3. Klicken Sie erneut auf die IPsec-Verbindung. 4. Klicken Sie auf **Verbindung aktivieren**.

Die IPsec-VPN-Protokolldateien herunterladen

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Sie können zusätzliche Informationen über die IPsec-Konnektivität in den Protokolldateien auf dem VPN-Server finden. Die Protokolldateien befinden sich komprimiert in einem .zip-Archiv, welches Sie herunterladen und entpacken können.

Voraussetzungen

Die Multi-Site-IPsec-VPN-Konnektivität ist konfiguriert.

So können Sie das .zip-Archiv mit den Protokolldateien herunterladen

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Verbindung**.
2. Klicken Sie neben dem VPN-Gateway der Cloud-Site auf das Zahnradsymbol.
3. Klicken Sie auf **Protokoll herunterladen**.
4. Klicken Sie auf **Fertig**.
5. Wenn das .zip-Archiv zum Herunterladen bereit ist, klicken Sie auf **Protokoll herunterladen** und speichern Sie es lokal.

Multi-Site-IPSec-VPN-Protokolldateien

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Die folgende Liste beschreibt die IPsec-VPN-Protokolldateien, die Teil des .zip-Archivs sind, und die darin enthaltenen Informationen.

- `ip.txt` – Diese Datei enthält die Protokolle über die Konfiguration der Netzwerkschnittstellen. Sie müssen zwei IP-Adressen sehen: eine öffentliche IP-Adresse und eine lokale IP-Adresse. Wenn Sie diese IP-Adressen nicht im Protokoll sehen, liegt ein Problem vor. Kontaktieren Sie dann den Support.

  Hinweis
  Die Netzwerkmaske für die öffentliche IP-Adresse muss 32 sein.

- `swanctl-list-loaded-config.txt` – Diese Datei enthält Informationen über alle IPsec-Standorte (Sites).

  Wenn Sie in der Datei keinen Standort sehen, wurde die IPsec-Konfiguration nicht angewendet. Versuchen Sie, die Konfiguration zu aktualisieren und zu speichern – oder wenden Sie sich an den Support.
- `swanctl-list-active-sas.txt` – Diese Datei enthält Verbindungen und Richtlinien, die sich im Status 'aktiv' oder 'Verbindungsaufbau' befinden.

Recovery-Server einrichten

Dieser Abschnitt beschreibt die Konzepte von Failover und Failback, die Erstellung eines Recovery-Servers und die entsprechenden Disaster Recovery-Aktionen.

Einen Recovery-Server erstellen

Wenn Sie einen Recovery-Server erstellen wollen, der eine Kopie Ihres Workloads ist, gehen Sie wie nachfolgend beschrieben vor. Sie können sich außerdem das Video-Tutorial ansehen, in dem der Prozess demonstriert wird.

Wichtig
Wenn Sie einen Failover durchführen, können Sie nur Recovery-Punkte auswählen, die erst nach dem Erstellen des Recovery-Servers erstellt wurden.

Voraussetzungen

- Sie müssen einer ursprünglichen Maschine, die Sie sichern wollen, einen Schutzplan zuweisen. Dieser Plan muss die komplette Maschine in den Cloud Storage sichern – oder nur diejenigen Laufwerke, die zum Booten und zur Bereitstellung notwendiger Dienste erforderlich sind.
- Einer der Verbindungstypen zur Cloud-Site muss festgelegt sein.

So können Sie einen Recovery-Server erstellen

1. Wählen Sie in der Registerkarte **Alle Geräte** diejenige Maschine aus, den Sie schützen wollen.
2. Klicken Sie zuerst auf **Disaster Recovery** und dann auf **Recovery-Server erstellen**.
3. Bestimmen Sie die Anzahl der virtuellen CPU-Kerne und die Größe des Arbeitsspeichers.

   Hinweis
   Sie können die Berechnungspunkte für jede Option sehen. Die Anzahl der Berechnungspunkte spiegelt wieder, wie viel die Ausführung des Recovery-Servers pro Stunde kostet. Weitere Informationen finden Sie im Abschnitt '"Berechnungspunkte" (S. 12)'.

4. Spezifizieren Sie das Cloud-Netzwerk, mit dem der Server verbunden werden soll.
5. Wählen Sie die **DHCP**-Option.

DHCP-Option	Beschreibung
Von der Cloud-Site bereitgestellt	Standardeinstellung. Die IP-Adresse des Servers wird von einem automatisch konfigurierten DHCP-Server in der Cloud bereitgestellt.
Benutzerdefiniert	Die IP-Adresse des Servers wird von Ihrem eigenen DHCP-Server in der Cloud bereitgestellt.

6. [Optional] Spezifizieren Sie die **MAC-Adresse**.

Die MAC-Adresse ist eine eindeutige Kennung, die dem Netzwerkadapter des Servers zugewiesen wird. Wenn Sie benutzerdefiniertes DHCP verwenden, können Sie es so konfigurieren, dass einer bestimmten MAC-Adresse immer eine bestimmte IP-Adresse zugewiesen wird. Auf diese Weise können Sie sicherstellen, dass der Recovery-Server immer die gleiche IP-Adresse erhält. Dadurch können Sie Applikationen ausführen, die Lizenzen haben, die wiederum auf die MAC-Adresse registriert sind.

7. Spezifizieren Sie die IP-Adresse, die der Server im Produktionsnetzwerk haben wird. Standardmäßig ist die IP-Adresse der ursprünglichen Maschine vorgegeben.

   Hinweis
   Falls Sie einen DHCP-Server verwenden, fügen Sie dessen IP-Adresse zu der Server-Ausschlussliste hinzu, um IP-Adressen-Konflikte zu vermeiden.
   Wenn Sie einen benutzerdefinierten DHCP-Server verwenden, müssen Sie unter **IP-Adresse im Produktionsnetzwerk** dieselbe IP-Adresse spezifizieren, die im DHCP-Server konfiguriert ist. Ansonsten wird der Test-Failover nicht richtig funktionieren und der Server wird nicht über eine öffentliche IP-Adresse erreichbar sein.

8. [Optional] Aktivieren Sie das Kontrollkästchen **Test-IP-Adresse** und spezifizieren Sie dann die IP-Adresse.
   Dies gibt Ihnen die Möglichkeit, einen Failover im isolierten Testnetzwerk zu testen und sich während eines Test-Failovers per RDP oder SSH mit dem Recovery-Server zu verbinden. Im Test-Failover-Modus wird das VPN-Gateway mithilfe des NAT-Protokolls die Test-IP-Adresse gegen die Produktions-IP-Adresse ersetzen.
   Wenn Sie das Kontrollkästchen deaktiviert lassen, können Sie sich während eines Test-Failovers nur über die Konsole mit dem Server verbinden.

   Hinweis
   Falls Sie einen DHCP-Server verwenden, fügen Sie dessen IP-Adresse zu der Server-Ausschlussliste hinzu, um IP-Adressen-Konflikte zu vermeiden.

   Sie können eine der vorgeschlagenen IP-Adressen verwenden oder eine andere eingeben.

9. [Optional] Aktivieren Sie das Kontrollkästchen **Internetzugriff**.
   Dies ermöglicht es dem Recovery-Server, sich während eines Failovers (auch im Testmodus) mit dem Internet zu verbinden. Standardmäßig ist der TCP-Port 25 für ausgehende Verbindungen zu öffentlichen IP-Adressen geöffnet.
10. [Optional] Legen Sie einen **RPO-Grenzwert** fest.
    Der RPO-Grenzwert definiert also das maximale Zeitintervall, das zwischen dem letzten (für einen Failover verwendbaren) Recovery-Punkt und dem aktuellen Zeitpunkt (an dem es zu einem Desaster kommen kann) zulässig ist. Der Wert kann zwischen 15–60 Minuten, 1–24 Stunden oder 1–14 Tagen eingestellt werden.
11. [Optional] Aktivieren Sie das Kontrollkästchen **Öffentliche IP-Adresse verwenden**.

Wenn der Recovery-Server über eine öffentliche IP-Adresse verfügt, ist er während eines Failovers (auch im Testmodus) aus dem Internet verfügbar. Wenn Sie das Kontrollkästchen deaktiviert lassen, wird der Server nur in Ihrem Produktionsnetzwerk verfügbar sein.

Die Option **Öffentliche IP-Adresse verwenden** erfordert, dass die Option **Internetzugriff** ebenfalls aktiviert ist.

Die öffentliche IP-Adresse wird angezeigt, nachdem Sie die Konfiguration abgeschlossen haben. Standardmäßig ist der TCP-Port 443 für eingehende Verbindungen zu öffentlichen IP-Adressen geöffnet.

Hinweis
Wenn Sie das Kontrollkästchen **Öffentliche IP-Adresse verwenden** deaktivieren oder den Recovery-Server löschen, wird dessen öffentliche IP-Adresse nicht reserviert.

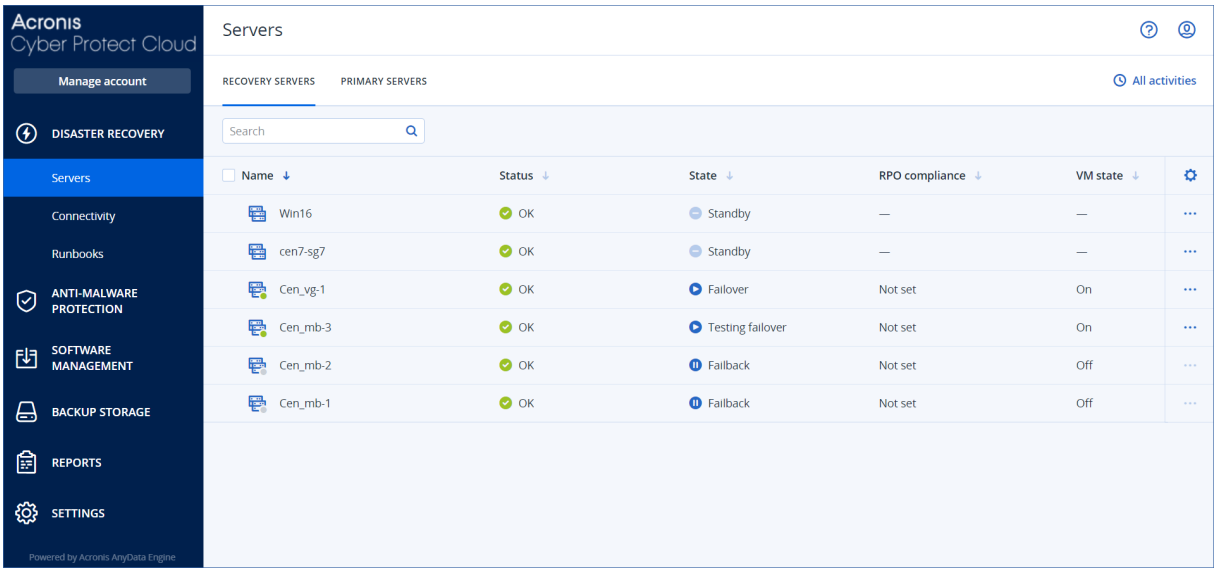
12. [Optional] [Wenn die Backups für die ausgewählte Maschine verschlüsselt sind, indem die Verschlüsselung als Maschineneigenschaft verwendet wird] Spezifizieren Sie das Kennwort, das automatisch verwendet wird, wenn eine virtuelle Maschine für den Recovery-Server aus dem verschlüsselten Backup erstellt wird.
    a. Klicken Sie zuerst auf **Spezifizieren**, geben Sie dann das Kennwort für das verschlüsselte Backup ein und definieren Sie dann einen Namen für die Anmeldedaten.

       Standardmäßig wird Ihnen das neueste Backup in der Liste angezeigt.
    b. [Optional] Wenn Sie alle Backups sehen wollen, müssen Sie auf **Alle Backups anzeigen** klicken.
    c. Klicken Sie auf **Fertig**.

Hinweis
Obwohl das von Ihnen spezifizierte Kennwort in einem sicheren Anmeldedatenspeicher hinterlegt wird, kann es dennoch sein, dass das Speichern von Kennwörtern gegen Ihre Compliance-Auflagen verstößt.

13. [Optional] Ändern Sie den Namen des Recovery-Servers.
14. [Optional] Geben Sie eine Beschreibung für den Recovery-Server ein.
15. [Optional] Klicken Sie auf die Registerkarte **Cloud-Firewall-Regeln**, um die Standard-Firewall-Regeln zu bearbeiten. Weitere Informationen finden Sie im Abschnitt '"Firewall-Regeln für Cloud Server einrichten" (S. 90)'.
16. Klicken Sie auf **Erstellen**.

Der Recovery-Server wird in der Cyber Protect-Konsole in der Registerkarte **Disaster Recovery** –> **Server** –> **Recovery-Server** angezeigt. Sie können dessen Einstellungen einsehen, wenn Sie die ursprüngliche Maschine auswählen und dann auf **Disaster Recovery** klicken.



Wie ein Failover funktioniert

Produktions-Failover

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Wenn ein Recovery-Server erstellt wird, verbleibt er zunächst im **Standby**-Stadium. Die entsprechende virtuelle Maschine existiert erst, wenn Sie den Failover starten. Bevor Sie einen Failover-Prozess starten, müssen Sie mindestens ein Disk-Image-Backup (mit bootfähigem Volume) von der ursprünglichen Maschine erstellen.

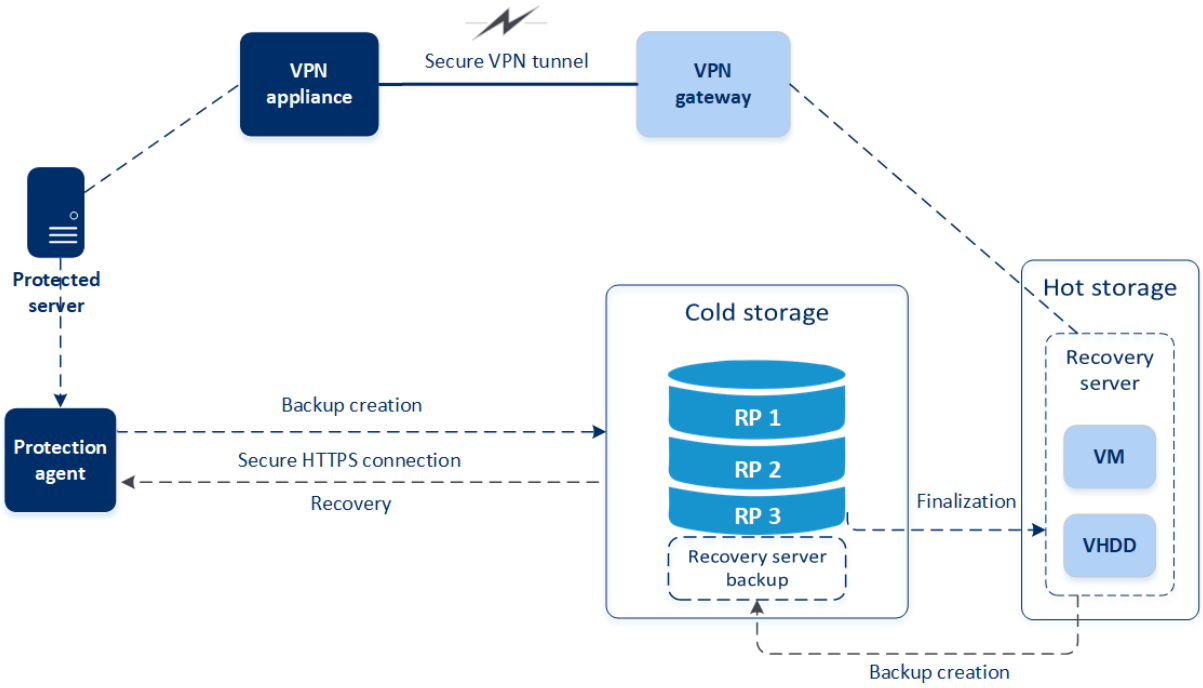
Wenn Sie den Failover-Prozess starten, wählen Sie den Recovery-Punkt (das Backup) der ursprünglichen Maschine, aus der dann eine virtuelle Maschine mit vordefinierten Parametern erstellt wird. Eine Failover-Aktion basiert auf der Funktion „VM von Backup ausführen“. Der Recovery-Server erhält das Übergangsstadium **Finalisierung**. Dieser Prozess beinhaltet die Übertragung der virtuellen Laufwerke des Servers aus dem Backup Storage („Cold Storage“) zum Disaster Recovery Storage („Hot Storage“).

Hinweis
Der Server bleibt während der **Finalisierung** verfügbar und betriebsbereit. Die Performance ist gegenüber dem Normalzustand jedoch herabgesetzt. Sie können die Server-Konsole öffnen, indem Sie auf den Link **Konsole ist bereit** klicken. Der Link ist in der Spalte **VM-Stadium** auf der Anzeige **Disaster Recovery** –> **Server** sowie in der Ansicht **Details** des Servers verfügbar.

Wenn die **Finalisierung** abgeschlossen ist, erreicht der Server wieder eine normale Performance. Das Server-Stadium wird auf **Failover** geändert. Der Workload wird nun von der ursprünglichen Maschine zum Recovery-Server in der Cloud-Site umgeschaltet (übertragen).

Wenn auf dem Recovery-Server ein Protection Agent ist, wird der Agenten-Dienst gestoppt, um Störungen (wie Backup-Starts oder das Senden veralteter Statusmeldungen an die Backup-Komponente) zu vermeiden.

Die untere Abbildung verdeutlicht die Failover- und Failback-Prozesse.



Failover testen

Bei einem **Test-Failover** wird die virtuelle Maschine nicht finalisiert. Das bedeutet, dass der Agent die Inhalte der virtuellen Laufwerke direkt aus dem Backup auslesen kann, also die verschiedenen Bereiche des Backups per wahlfreien Zugriff verfügbar sind und dass dessen Performance unter Umständen langsamer als normal ist. Weitere Informationen über den Failover-Prozess finden Sie im Abschnitt '"Einen Test-Failover durchführen" (S. 63)'.

Automatisierter Test-Failover

Wenn der automatisierte Failover-Test konfiguriert ist, wird er einmal im Monat durchgeführt, ohne dass ein manuelles Eingreifen erforderlich ist. Weitere Informationen dazu finden Sie in den Abschnitten '"Automatisierter Test-Failover" (S. 66)' und '"Automatisierte Test-Failover konfigurieren" (S. 67)'.

Einen Test-Failover durchführen

Einen Test-Failover durchzuführen bedeutet, einen Recovery-Server in einem Test-VLAN zu starten, welches von Ihrem Produktionsnetzwerk isoliert ist. Sie können mehrere Recovery-Server gleichzeitig testen und deren Interaktion überprüfen. Innerhalb des Testnetzwerks kommunizieren die Server über ihre Produktions-IP-Adressen. Die Server können jedoch keine TCP- oder UDP-Verbindungen zu den Workloads in Ihrem lokalen Netzwerk (LAN) aufbauen.

Bei einem Test-Failover wird die virtuelle Maschine (der Recovery-Server) nicht finalisiert. Der Agent liest die Inhalte der virtuellen Laufwerke direkt aus dem Backup aus und hat dabei wahlfreien Zugriff auf die verschiedenen Bereiche des Backups. Dies kann dazu führen, dass die Performance des Recovery-Servers im Test-Failover-Stadium langsamer ist als seine normale Performance.

Obwohl die Durchführung eines Test-Failovers optional ist, empfehlen wir Ihnen, einen solchen doch so häufig durchzuführen, wie Sie es unter Berücksichtigung der Faktoren Kosten und Sicherheit passend finden. Bewährt hat sich die Erstellung eines sogenannten Runbooks. Das ist eine Zusammenstellung von Anweisungen, die beschreibt, wie die Produktionsumgebung in die Cloud übertragen wird.

Wichtig
Sie müssen bereits im Vorfeld einen Recovery-Server erstellen, um Ihre Geräte vor einem möglicherweise auftretenden Desaster schützen zu können.

Sie können einen Failover nur aus Recovery-Punkten durchführen, die erstellt wurden, nachdem der Recovery-Server des Gerätes erstellt wurde.

Es muss mindestens ein Recovery-Punkt erstellt worden sein, bevor ein Failover-Prozess zu einem Recovery-Server durchgeführt werden kann. Die maximale Anzahl der unterstützten Recovery-Punkte beträgt 100.

So können Sie einen Test-Failover durchführen

1. Wählen Sie die ursprüngliche Maschine oder den Recovery-Server aus, für die/den Sie den Test durchführen wollen.
2. Klicken Sie auf **Disaster Recovery**.
   Die Beschreibung des Recovery-Servers wird angezeigt.
3. Klicken Sie auf **Failover**.
4. Wählen Sie **Failover testen** als Art des durchzuführenden Failovers aus.
5. Wählen Sie den gewünschten Recovery-Punkt (das Backup) und klicken Sie dann auf **Start**.
6. Wenn das von Ihnen ausgewählte Backup verschlüsselt ist, wobei die Verschlüsselung über die Maschineneigenschaften festgelegt ist:
   a. Geben Sie das Verschlüsselungskennwort für den Backup-Satz ein.

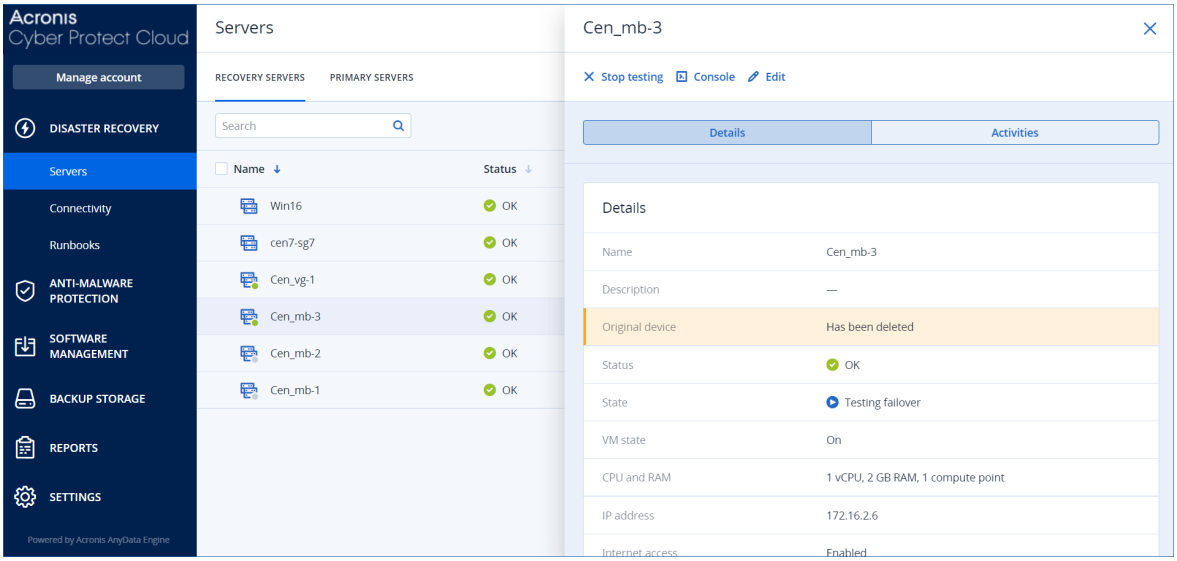
      Hinweis
      Das Kennwort wird nur temporär gespeichert und nur für die aktuelle Test-Failover-Aktion verwendet. Das Kennwort wird automatisch aus dem Anmeldedatenspeicher gelöscht, wenn der Test-Failover-Prozess gestoppt wird oder abgeschlossen wurde.

   b. [Optional] Wenn Sie das Kennwort für den Backup-Satz speichern und für nachfolgende Failover-Aktionen verwenden wollen, müssen Sie das Kontrollkästchen **Das Kennwort in einem sicheren Anmeldedatenspeicher speichern...** aktivieren und dann im Feld **Anmeldedatenname** einen Namen für die Anmeldedaten eingeben.

Wichtig
Das Kennwort wird in einem sicheren Anmeldedatenspeicher hinterlegt und bei späteren Failover-Aktionen automatisch angewendet. Es kann jedoch sein, dass das Speichern von Kennwörtern im Konflikt mit Ihren Compliance-Verpflichtungen steht.

c. Klicken Sie auf **Fertig**.

Wenn der Recovery-Server gestartet ist, ändert sich dessen Stadium auf '**Failover wird getestet**'.



7. Testen Sie den Recovery-Server mit einer der nachfolgenden Methoden:
   - Wählen Sie bei **Disaster Recovery** –> **Server** den gewünschten Recovery-Server aus und klicken Sie dann auf **Konsole**.
   - Verbinden Sie sich per RDP oder SSH mit dem Recovery-Server und verwenden Sie dabei die Test-IP-Adresse, die Sie bei der Erstellung des Recovery-Servers spezifiziert haben. Testen Sie die Verbindung sowohl innerhalb als auch außerhalb des Produktionsnetzwerks (wie im Abschnitt 'Point-to-Site-Verbindung' beschrieben).
   - Führen Sie ein Skript im Recovery-Server aus.

     Dieses Skript kann beispielsweise den Anmeldebildschirm überprüfen, ob Applikationen gestartet wurden, ob eine Internetverbindung besteht oder ob sich andere Maschinen mit dem Recovery-Server verbinden können.
   - Wenn der Recovery-Server auf das Internet zugreifen kann und eine öffentliche IP-Adresse hat, können Sie auch TeamViewer verwenden.
8. Klicken Sie nach Abschluss der Installation auf **Test stoppen**.

   Der Recovery-Server wird gestoppt. Alle Änderungen am Recovery-Server, die während des Test-Failovers erfolgten, gehen verloren.

Hinweis
Die Aktionen **Server starten** und **Server stoppen** sind für Test-Failover-Aktionen nicht anwendbar, egal ob in Runbooks oder beim manuellen Starten eines Test-Failovers. Wenn Sie versuchen, eine solche Aktion auszuführen, wird diese mit folgender Fehlermeldung fehlschlagen: Fehlgeschlagen: Die Aktion ist auf das aktuelle Server-Stadium nicht anwendbar.

Automatisierter Test-Failover

Mit einem automatisierten Test-Failover kann der Recovery-Server einmal im Monat automatisch getestet werden, ohne dass manuelle Eingriffe erforderlich sind.

Der automatisierte Test-Failover-Prozess besteht aus folgenden Abschnitten:

1. Es wird eine virtuelle Maschine aus dem jüngsten Recovery-Punkt erstellt
2. Es wird ein Screenshot von der virtuellen Maschine aufgenommen
3. Es wird analysiert, ob das Betriebssystem der virtuellen Maschine erfolgreich startet
4. Sie werden über den Status des Failover-Tests benachrichtigt

Hinweis
Automatisierte Test-Failover verbrauchen Berechnungspunkte.

Sie können die automatisierten Test-Failover in den Einstellungen des Recovery-Servers konfigurieren. Weitere Informationen finden Sie im Abschnitt '"Automatisierte Test-Failover konfigurieren" (S. 67)'.

Beachten Sie, dass es in sehr seltenen Fällen vorkommen kann, dass ein automatisierter Test-Failover übersprungen und nicht zum geplanten Zeitpunkt durchgeführt wird. Weil ein Produktions-Failover eine höhere Priorität als ein automatisierter Test-Failover hat, werden die Hardware-Ressourcen (CPU und RAM), die dem automatisierten Test-Failover zugeordnet wurden, möglicherweise vorübergehend eingeschränkt, um sicherzustellen, dass für einen gleichzeitig stattfindenden Produktions-Failover genügend Ressourcen vorhanden sind.

Wenn ein automatisierter Test-Failover aus irgendeinem Grund übersprungen wird, wird eine entsprechende Alarmmeldung ausgelöst.

Hinweis
Der automatisierte Failover-Test wird fehlschlagen, wenn die Backups der ursprünglichen Maschine verschlüsselt sind (wobei die Verschlüsselung als Maschinen-Eigenschaft festgelegt wurde) und das Verschlüsselungskennwort beim Erstellen des Recovery-Servers nicht spezifiziert wurde. Weitere Informationen über das Spezifizieren des Verschlüsselungskennworts finden Sie im Abschnitt '"Einen Recovery-Server erstellen" (S. 59)'.

Automatisierte Test-Failover konfigurieren

Durch die Konfiguration eines automatisierten Test-Failovers können Sie Ihren Recovery-Server jeden Monat automatisiert testen lassen, ohne dabei manuell eingreifen zu müssen.

So können Sie einen automatisierten Test-Failover konfigurieren

1. Gehen Sie in der Konsole zu **Disaster Recovery** –> **Server** –> **Recovery-Server** und wählen Sie den gewünschten Recovery-Server aus.
2. Klicken Sie auf **Bearbeiten**.
3. Wählen Sie im Bereich **Automatisierter Test-Failover** im Feld **Planung** die Option **Monatlich**.
4. [Optional] Ändern Sie bei **Screenshot-Zeitlimit** den Standardwert für den maximalen Zeitraum (in Minuten), in dem das System versuchen soll, einen automatisierten Test-Failover durchzuführen.
5. [Optional] Wenn Sie den Wert für das **Screenshot-Zeitlimit** als Standard speichern und automatisch eintragen lassen wollen, wenn Sie einen automatisierten Test-Failover für andere Recovery-Server aktivieren, wählen Sie **Als Standard-Zeitlimit speichern**.
6. Klicken Sie auf **Speichern**.

Den Status des automatisierten Test-Failovers einsehen

Sie können sich die Details eines abgeschlossenen automatisierten Test-Failovers anzeigen lassen, z.B. den Status, die Startzeit, die Endzeit, die Dauer sowie einen Screenshot der virtuellen Maschine.

So können Sie sich den automatisierten Test-Failover-Status eines Recovery-Servers anzeigen lassen

1. Gehen Sie in der Konsole zu **Disaster Recovery** –> **Server** –> **Recovery-Server** und wählen Sie den gewünschten Recovery-Server aus.
2. Überprüfen Sie im Bereich **Automatisierter Test-Failover** die angezeigten Details des letzten automatisierten Test-Failovers.
3. [Optional] Klicken Sie auf **Screenshot anzeigen**, um sich den Screenshot der virtuellen Maschine anzusehen.

Automatisierte Test-Failover deaktivieren

Sie können einen automatisierten Test-Failover deaktivieren, wenn Sie Ressourcen einsparen wollen oder für einen bestimmten Recovery-Server keinen automatisierten Test-Failover durchführen müssen.

So können Sie einen automatisierten Test-Failover deaktivieren

1. Gehen Sie in der Konsole zu **Disaster Recovery** –> **Server** –> **Recovery-Server** und wählen Sie den gewünschten Recovery-Server aus.
2. Klicken Sie auf **Bearbeiten**.

3. Wählen Sie im Bereich **Automatisierter Test-Failover** im Feld **Planung** die Option **Nie**.
4. Klicken Sie auf **Speichern**.

Einen Failover durchführen

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Ein Failover ist ein Prozess, bei dem ein Workload von Ihren lokalen Systemen (on-premise) in die Cloud verschoben wird. Der Begriff wird außerdem auch für das Stadium verwendet, wenn der Workload in der Cloud bleibt.

Wenn Sie einen Failover-Prozess starten, wird der Recovery-Server im Produktionsnetzwerk gestartet. Um Störungen und unerwünschte Problemen zu vermeiden, sollten Sie sicherstellen, dass der ursprüngliche Workload nicht mehr online ist und nicht per VPN zugänglich ist.

Um zu vermeiden, dass Backups, die in dasselbe Cloud-Archiv durchgeführt werden, gestört werden, sollten Sie den Schutzplan vom Workload, der sich gerade im **Failover**-Stadium befindet, manuell widerrufen. Weitere Informationen über das Widerrufen von Plänen finden Sie im Abschnitt Einen Schutzplan widerrufen.

Wichtig
Sie müssen bereits im Vorfeld einen Recovery-Server erstellen, um Ihre Geräte vor einem möglicherweise auftretenden Desaster schützen zu können.

Sie können einen Failover nur aus Recovery-Punkten durchführen, die erstellt wurden, nachdem der Recovery-Server des Gerätes erstellt wurde.

Es muss mindestens ein Recovery-Punkt erstellt worden sein, bevor ein Failover-Prozess zu einem Recovery-Server durchgeführt werden kann. Die maximale Anzahl der unterstützten Recovery-Punkte beträgt 100.

Sie können die nachfolgenden Anleitungen befolgen oder sich das Video-Tutorial ansehen.

So können Sie einen Failover durchführen

1. Überprüfen Sie, dass die ursprüngliche Maschine nicht mehr im Netzwerk verfügbar ist.
2. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Server** –> **Recovery-Server** und wählen Sie den gewünschten Recovery-Server aus.
3. Klicken Sie auf **Failover**.
4. Wählen Sie **Produktions-Failover** als Art des durchzuführenden Failovers aus.
5. Wählen Sie den gewünschten Recovery-Punkt (das Backup) und klicken Sie dann auf **Start**.
6. [Wenn das von Ihnen ausgewählte Backup verschlüsselt ist, wobei die Verschlüsselung über die Maschineneigenschaften festgelegt ist]

a. Geben Sie das Verschlüsselungskennwort für den Backup-Satz ein.

Hinweis
Das Kennwort wird nur temporär gespeichert und nur für die aktuelle Failover-Aktion verwendet. Das Kennwort wird automatisch aus dem Anmeldedatenspeicher gelöscht, nachdem die Failover-Aktion abgeschlossen wurde und der Server in das Stadium **Standby** zurückgesetzt wurde.

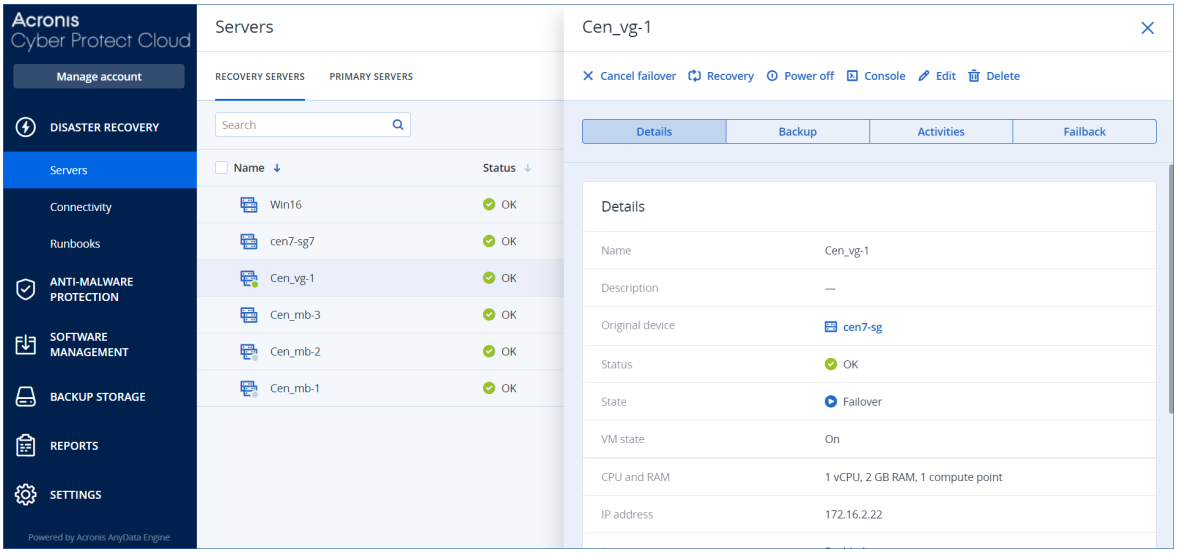
b. [Optional] Wenn Sie das Kennwort für den Backup-Satz speichern und für nachfolgende Failover-Aktionen verwenden wollen, müssen Sie das Kontrollkästchen **Das Kennwort in einem sicheren Anmeldedatenspeicher speichern...** aktivieren und dann im Feld **Anmeldedatenname** einen Namen für die Anmeldedaten eingeben.

Wichtig
Das Kennwort wird in einem sicheren Anmeldedatenspeicher hinterlegt und bei späteren Failover-Aktionen automatisch angewendet. Es kann jedoch sein, dass das Speichern von Kennwörtern im Konflikt mit Ihren Compliance-Verpflichtungen steht.

c. Klicken Sie auf **Fertig**.

Wenn der Recovery-Server gestartet ist, ändert sich dessen Stadium auf **Finalisierung** und nach einer gewissen Zeit auf **Failover.**

Wichtig
Es ist wichtig zu verstehen, dass der Server sowohl im Stadium **Finalisierung** also auch **Failover** verfügbar ist. Im Stadium **Finalisierung** können Sie auf die Server-Konsole zugreifen, indem Sie auf den Link **Konsole ist bereit** klicken. Der Link ist in der Spalte **VM-Stadium** auf der Anzeige **Disaster Recovery** –> **Server** sowie in der Ansicht **Details** des Servers verfügbar. Weitere Informationen finden Sie unter '"Wie ein Failover funktioniert" (S. 62)'.



7. Überprüfen Sie, dass der Recovery-Server gestartet ist, indem Sie sich dessen Konsole anzeigen lassen. Klicken Sie auf **Disaster Recovery** –> **Server**, wählen Sie den Recovery-Server aus und klicken Sie dann auf **Konsole**.
8. Stellen Sie sicher, dass der Recovery-Server über die Produktions-IP-Adresse verfügbar ist, die Sie bei Erstellung des Recovery-Servers spezifiziert haben.

Sobald der Recovery-Server finalisiert ist, wird automatisch ein neuer Schutzplan erstellt und dem Recovery-Server zugewiesen. Bis auf einige Einschränkungen basiert dieser Schutzplan auf demjenigen Schutzplan, der zu Erstellung des Recovery-Servers verwendet wurde. Sie können in diesem Plan nur die Planung und Aufbewahrungsregeln ändern. Weitere Informationen dazu finden Sie im Abschnitt 'Backup der Cloud-Server'.

Wenn Sie den Failover-Prozess abbrechen wollen, müssen Sie den Recovery-Server auswählen und dann auf **Failover abbrechen** klicken. Alle Änderungen, die ab dem Zeitpunkt des Failover beginnen, mit Ausnahme der Backups des Recovery-Servers, werden verloren gehen. Der Recovery-Server wird in das Stadium **Standby** zurückkehren.

Wenn Sie einen Failback-Prozess durchführen wollen, müssen Sie zuerst den Recovery-Server auswählen und dann auf **Failback** klicken.

So können Sie einen Failover von Servern mit einem lokalem DNS durchführen

Wenn Sie die Maschinennamen am lokalen Standort über DNS-Server auflösen, können die Recovery-Server, die den Maschinen entsprechen, die auf die DNS-Server zurückgreifen, nach einem Failover nicht mehr kommunizieren, da in der Cloud andere DNS-Server verwendet werden. Standardmäßig werden die DNS-Server der Cloud-Site für neu erstellte Cloud Server verwendet. Wenn Sie benutzerdefinierte DNS-Einstellungen anwenden müssen, sollten Sie das Support-Team kontaktieren.

So können Sie einen Failover für einen DHCP-Server durchführen

In Ihrer lokalen Infrastruktur kann sich der DHCP-Server auf einem Windows- oder Linux-Host befinden. Wenn ein solcher Host per Failover in die Cloud-Site umgeschaltet wird, kommt es zu einem DHCP-Server-Duplizierungsproblem, weil das VPN-Gateway in der Cloud ebenfalls die DHCP-Rolle übernimmt. Führen Sie einen der folgenden Schritte aus, um dieses Problem zu beheben:

- Wenn nur der DHCP-Host per Failover in die Cloud umgeschaltet wurde, während sich die restlichen lokalen Server weiterhin am lokalen Standort befinden, müssen Sie sich beim DHCP-Host in der Cloud anmelden und den dort laufenden DHCP-Server ausschalten. Somit gibt es keine Konflikte mehr und nur das VPN-Gateway wird als DHCP-Server fungieren.
- Wenn Ihre Cloud Server bereits ihre IP-Adressen vom DHCP-Host erhalten haben, müssen Sie sich beim DHCP-Host in der Cloud anmelden und den dort laufenden DHCP-Server ausschalten. Sie müssen sich auch bei den Cloud Servern anmelden und die DHCP-IP-Vergabe erneuern, damit neue IP-Adressen vom richtigen (auf dem VPN-Gateway gehosteten) DHCP-Server zugewiesen werden.

Hinweis
Diese Anweisungen sind nicht gültig, wenn Ihr Cloud-DHCP-Server mit der Option **Benutzerdefiniertes DHCP** konfiguriert wurde – und einige der primären oder Recovery-Server ihre IP-Adresse von diesem DHCP-Server beziehen.

Wie ein Failback funktioniert

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Ein Failback ist ein Prozess, bei dem ein Workload aus der Cloud zurück zu einer physischen oder virtuellen Maschine am lokalen Standort des entsprechenden Unternehmens/Kunden verschoben wird. Sie können einen Failback-Prozess auf einen Recovery-Server im **Failover**-Stadium anwenden – und den entsprechenden Server dann an Ihrem lokalen Standort weiter verwenden.

Sie können einen automatisierten Failback zu einer virtuellen oder physischen Zielmaschine durchführen, die sich an Ihrem lokalen Standort befindet. Während des Failback-Prozesses können Sie die Backup-Daten zu Ihrem lokalen Standort übertragen, während die virtuelle Maschine weiter in der Cloud ausgeführt wird. Mit dieser Technologie können Sie eine sehr kurze Ausfallzeit erreichen, die in der Cyber Protect-Konsole auch entsprechend prognostiziert und angezeigt wird. Sie können diese Informationen einsehen und verwenden, um Ihre Aktivitäten zu planen – und (falls nötig) Ihre Kunden vor einer anstehenden Ausfallzeit zu warnen.

Die Failback-Prozesse zu virtuellen Zielmaschinen und physischen Zielmaschinen unterscheiden sich leicht. Weitere Informationen zu den verschiedenen Phasen eines Failback-Prozesses finden Sie in den Abschnitten '"Failback zu einer virtuellen Zielmaschine" (S. 72)' und '"Failback zu einer physischen Zielmaschine" (S. 77)'.

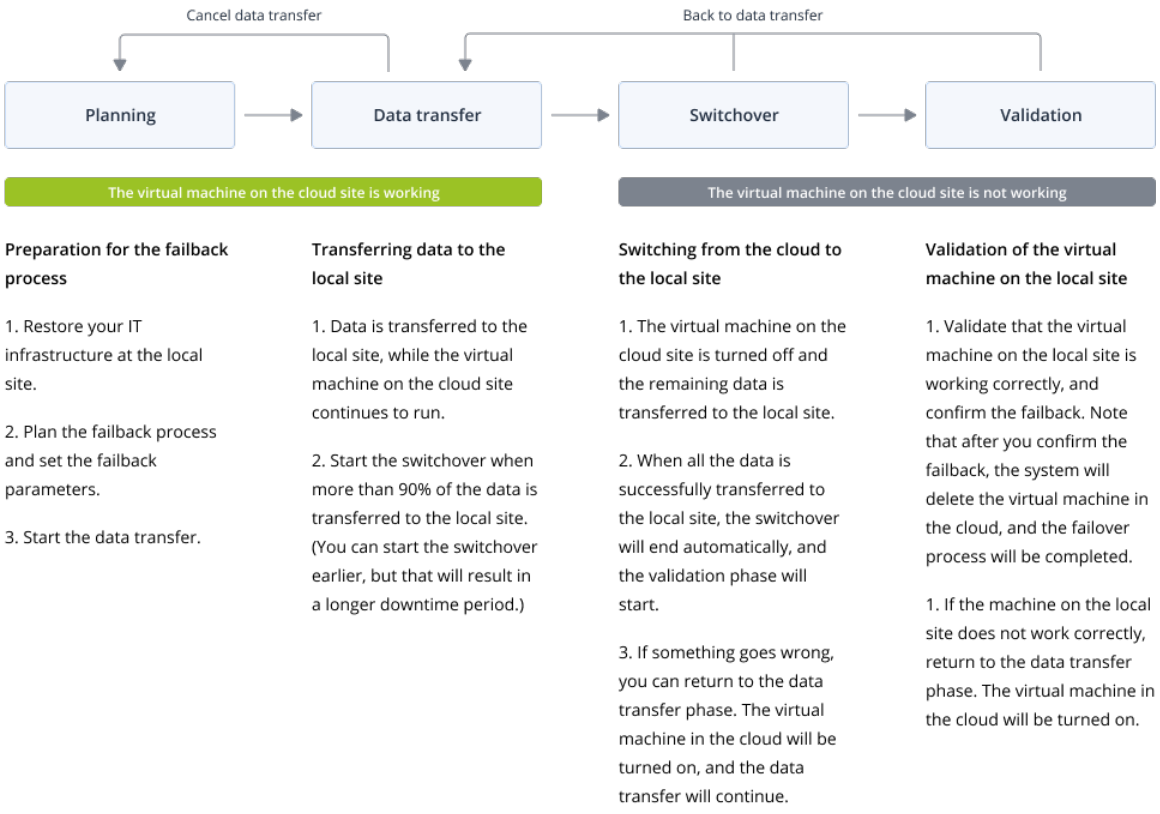
Wenn Sie die automatisierte Failback-Prozedur aus bestimmten Gründen nicht verwenden können, können Sie auch einen manuellen Failback-Prozess durchführen. Weitere Informationen finden Sie im Abschnitt '"Manueller Failback-Prozess" (S. 81)'.

Hinweis
Runbook-Aktionen unterstützen Failbacks nur im manuellen Modus. Das heißt, wenn Sie den Failback-Prozess durch die Ausführung eines Runbooks starten, in dem ein **Server-Failback ausführen**-Schritt enthalten ist, erfordert die Prozedur eine manuelle Interaktion: Sie müssen die Maschine zuerst manuell wiederherstellen und dann den Failback-Prozess über die Registerkarte **Disaster Recovery** –> **Server** bestätigen oder abbrechen.

Failback zu einer virtuellen Zielmaschine

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Der Failback-Prozess zu einer virtuellen Maschine umfasst vier Phasen:



1. **Planung**. In dieser Phase stellen Sie die IT-Infrastruktur (z.B. die Hosts und Netzwerkkonfigurationen) an Ihrem lokalen Standort wieder her, konfigurieren Sie die Failback-Parameter und planen Sie, wann die Datenübertragung beginnen soll.

   Hinweis
   Um die Gesamtzeit für den Failback-Prozess möglichst kurz zu halten, empfehlen wir, dass Sie die Datenübertragungsphase direkt nach der Einrichtung Ihrer lokalen Server starten und während dieser Datenübertragungsphase dann mit der Konfiguration des Netzwerks und der restlichen lokalen Infrastruktur fortfahren.

2. **Datenübertragung**. In dieser Phase werden die Daten von der Cloud-Site zum lokalen Standort übertragen, während die virtuelle Maschine in der Cloud weiter ausgeführt wird. Sie können die nächste Phase (die Switchover-Phase) jederzeit während der Datenübertragungsphase starten.

Dabei sollten Sie jedoch folgende Zusammenhänge beachten.

Je länger Sie in der Datenübertragungsphase verbleiben,

- desto länger wird die virtuelle Maschine in der Cloud weiter ausgeführt.
- desto mehr Daten werden zu Ihrem lokalen Standort übertragen.
- desto höher werden die Kosten sein, die Sie zahlen müssen (Sie werden mehr Berechnungspunkte verbrauchen).
- desto kürzer wird die Ausfallzeit sein, die Sie während der Switchover-Phase erleben werden.

Wenn Sie die Ausfallzeit minimieren wollen, starten Sie die Switchover-Phase, nachdem mehr als 90% der Daten an den lokalen Standort übertragen wurden.

Wenn Sie eine längere Ausfallzeit in Kauf nehmen können und nicht mehr Berechnungspunkte für den Betrieb der virtuellen Maschine in der Cloud ausgeben wollen, können Sie die Switchover-Phase früher starten.

Wenn Sie den Failback-Prozess während der Datenübertragungsphase abbrechen, werden die bisher zum lokalen Standort übertragenen Daten nicht gelöscht. Bevor Sie einen neuen Failback-Prozess starten, sollten Sie die übertragenen Daten manuell löschen, um mögliche Probleme zu vermeiden. Der nachfolgenden Datenübertragungsprozess wird ganz neu gestartet.

3. **Switchover**. In dieser Phase wird die virtuelle Maschine in der Cloud ausgeschaltet und die verbleibenden Daten (einschließlich des letzten Backup-Inkrements) werden zum lokalen Standort übertragen. Wenn auf den Recovery-Server kein Backup-Plan angewendet wurde, wird automatisch während der Switchover-Phase ein Backup durchgeführt, was jedoch den Prozess verlangsamt.

   Sie können die geschätzte Zeit bis zur Fertigstellung (entspricht der Ausfallzeit) für diese Phase in der Cyber Protect-Konsole einsehen Wenn alle Daten zum lokalen Standort übertragen wurden (es gehen keine Daten verloren und die virtuelle Maschine am lokalen Standort ist eine exakte Kopie der virtuellen Maschine in der Cloud), ist die Switchover-Phase abgeschlossen. Die virtuelle Maschine am lokalen Standort wird wiederhergestellt und die Validierungsphase beginnt automatisch.
4. **Validierung**.Während dieser Phase ist die virtuelle Maschine am lokalen Standort bereits verfügbar und automatisch gestartet. Sie können überprüfen, ob die virtuelle Maschine korrekt funktioniert – und können Folgendes tun:
   - Falls alles wie erwartet funktioniert, bestätigen Sie das Failback. Nach der Failback-Bestätigung wird die virtuelle Maschine in der Cloud gelöscht und der Recovery-Server in das Stadium Standby **Standby** zurückversetzt. Damit ist der Failback-Prozess beendet.
   - Wenn etwas nicht stimmt, können Sie den Switchover-Prozess abbrechen und zur Datenübertragungsphase zurückkehren.

Einen Failback zu einer virtuellen Maschine durchführen

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Sie können einen Failback zu einer virtuellen Zielmaschine durchführen, die sich an Ihrem lokalen Standort befindet.

Voraussetzungen

- Der Agent, den Sie zur Durchführung des Failbacks verwenden wollen, ist online und wird aktuell für keine andere Failback-Aktion verwendet.
- Ihre Internetverbindung ist stabil.
- Es gibt mindestens ein vollständiges Backup der virtuellen Maschine in der Cloud.

So können Sie einen Failback zu einer virtuellen Maschine durchführen

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Server**.
2. Wählen Sie den Recovery-Server aus, der sich im **Failover**-Stadium befindet.
3. Klicken Sie auf die Registerkarte **Failback**.
4. Wählen Sie im Bereich **Failback-Parameter** den Eintrag **Virtuelle Maschine** als **Ziel** aus und konfigurieren Sie dann die Parameter.
   Beachten Sie, dass standardmäßig einige der **Failback-Parameter** automatisch mit vorgeschlagenen Werten ausgefüllt werden. Sie können diese Werte aber ändern.
   Die nachfolgende Tabelle gibt Ihnen weitere Informationen über die **Failback-Parameter**.

Parameter	Beschreibung
Backup-Größe	Die Datenmenge, die während des Failback-Prozesses zu Ihrem lokalen Standort übertragen wird. Nach dem der Start des Failback-Prozesses zu einer virtuellen Zielmaschine nimmt die **Backup-Größe** während der Datenübertragungsphase zu, weil die virtuelle Maschine in der Cloud weiter ausgeführt wird und dabei neue Daten generiert. Wenn Sie die geschätzte Ausfallzeit während des Failback-Prozesses zu einer virtuellen Zielmaschine berechnen wollen, nehmen Sie 10% des Wertes für die **Backup-Größe** (da wir empfehlen, die Switchover-Phase zu starten, nachdem 90% der Daten zum lokalen Standort übertragen wurden) und teilen Sie diesen Wert dann durch Ihre Internet-Geschwindigkeit. **Hinweis** Der Wert für die Internet-Geschwindigkeit wird kleiner, wenn Sie mehrere Failback-Prozesse gleichzeitig durchführen.
Ziel	Die Art des Workloads an Ihrem lokalen Standort, zu dem Sie den Cloud Server wiederherstellen wollen: **Virtuelle Maschine** oder **Physische Maschine**.
Speicherort der Zielmaschine	Failback-Speicherort: ein VMware ESXi- oder ein Microsoft Hyper-V-Host.

Parameter	Beschreibung
	Sie können aus allen Hosts wählen, die einen Agent haben, welcher wiederum im Cyber Protection Service registriert ist.
Agent	Der Agent, der die Failback-Aktion durchführen wird. Sie können einen (1) Agenten verwenden, um eine (1) Failback-Aktion gleichzeitig durchzuführen. Sie können einen Agenten auswählen, der online ist und aktuell für keinen anderen Failback-Prozess verwendet wird. Außerdem muss die Agenten-Version die Failback-Funktionalität unterstützen sowie über die Berechtigung verfügen, um auf das Backup zugreifen zu können. Beachten Sie, dass Sie mehrere Agenten auf VMware ESXi-Hosts installieren können und mit jedem von diesen einen separaten Failback-Prozess starten können. Diese Failback-Prozesse können auch gleichzeitig ausgeführt werden.
Einstellungen der Zielmachine	Einstellungen der virtuellen Maschine: • **Virtuelle Prozessoren**. Bestimmen Sie die Anzahl der virtuellen Prozessoren (CPUs). • **Arbeitsspeicher**. Bestimmen Sie, wie viel Arbeitsspeicher die virtuelle Maschine erhalten soll. • **Abteilungen**. Wählen Sie die Abteilungen für den Arbeitsspeicher. • [Optional] **Netzwerkadapter**. Wenn Sie einen Netzwerkadapter hinzufügen wollen, klicken Sie zuerst auf **Hinzufügen** und wählen Sie dann ein Netzwerk im Feld **Netzwerk** aus. Klicken Sie auf **Fertig**, wenn Sie die Änderungen abgeschlossen haben.
Pfad	(Für Microsoft Hyper-V-Hosts) Ordner auf dem Host, wo Ihre Maschine gespeichert werden soll. Sorgen Sie dafür, dass auf dem Host genügend freier Speicherplatz für die Maschine vorhanden ist.
Datenspeicher	(Für VMware ESXi-Hosts) Datenspeicher auf dem Host, wo Ihre Maschine gespeichert werden soll. Sorgen Sie dafür, dass auf dem Host genügend freier Speicherplatz für die Maschine vorhanden ist.
Provisioning-Modus	Zuordnungsmethode für das virtuelle Laufwerk. Für Microsoft Hyper-V-Hosts: • **Dynamisch erweiterbar** (Standardwert). • **Feste Größe**. Für Microsoft Hyper-V-Hosts: • **Thin** (Standardwert). • **Thick**.
Name der	Name der Zielmaschine. Standardmäßig ist der Name der Zielmaschine

Parameter	Beschreibung
Zielmaschine	identisch mit dem Namen des Recovery-Servers. Der Name der Zielmaschine muss für den gewählten **Speicherort der Zielmaschine** eindeutig (einmalig) sein.

5. Klicken Sie zuerst auf **Datenübertragung starten** und klicken Sie dann im Bestätigungsfenster auf **Start**.

Hinweis
Wenn es kein Backup der virtuellen Maschine in der Cloud gibt, führt das System automatisch ein Backup durch, bevor die Datenübertragungsphase beginnt.

Die **Datenübertragungs**phase wird gestartet. In der Konsole werden folgende Informationen angezeigt:

Feld	Beschreibung
Fortschritt	Dieser Parameter zeigt an, wie viele Daten bereits zum lokalen Standort übertragen wurden und wie viele Daten insgesamt noch übertragen werden müssen. Die Gesamtmenge der Daten setzt sich folgendermaßen zusammen: Die Daten des letzten Backups, bevor die Datenübertragungsphase gestartet wurde, sowie die Backups von neu generierten Daten (also Backup-Inkremente), während die virtuelle Maschine in der Datenübertragungsphase weiter ausgeführt wird. Aus diesem Grund werden beide Werte des Parameters **Fortschritt** mit der Zeit größer.
Schätzung der Ausfallzeit	Dieser Parameter gibt an, wie lange die virtuelle Maschine in der Cloud nicht verfügbar sein wird, wenn Sie die Switchover-Phase zum jetzigen Zeitpunkt starten. Dieser Wert wird aus den Werten des Parameters **Fortschritt** berechnet – und wird mit der Zeit kleiner.

6. Klicken Sie zuerst auf **Switchover** und dann im Bestätigungsfenster erneut auf **Switchover**.
Die Switchover-Phase wird gestartet. In der Konsole werden folgende Informationen angezeigt:

Feld	Beschreibung
Fortschritt	Dieser Parameter zeigt an, wie die Wiederherstellung der Maschine am lokalen Standort fortschreitet.
Geschätzte Zeit bis zur Fertigstellung	Dieser Parameter gibt an, wann die Switchover-Phase ungefähr abgeschlossen sein wird und wann Sie die Maschine am lokalen Standort starten können.

Hinweis
Wenn kein Backup-Plan auf die virtuelle Maschine in der Cloud angewendet wurde, wird automatisch während der Switchover-Phase ein Backup durchgeführt, was jedoch zu einer längeren Ausfallzeit führt.

7. Nachdem die **Switchover**-Phase abgeschlossen und die virtuelle Maschine an Ihrem lokalen Standort automatisch gestartet wurde, sollten Sie überprüfen, ob diese wie erwartet funktioniert.
8. Klicken Sie zuerst auf **Failback bestätigen** und dann im Bestätigungsfenster auf **Bestätigen**, um den Prozess abzuschließen.
   Die virtuelle Maschine wird daraufhin in der Cloud gelöscht und der Recovery-Server in das Stadium Standby **Standby** zurückversetzt.

Hinweis
Das Anwenden eines Schutzplans auf den wiederhergestellten Server ist kein Bestandteil des Failback-Prozesses. Nach Abschluss des Failback-Prozesses können Sie aber einen Schutzplan auf den wiederhergestellten Server anwenden, damit dieser wieder geschützt ist. Sie können den gleichen Schutzplan anwenden, der auf den ursprünglichen Server angewendet wurde – oder einen neuen Schutzplan, bei dem das **Disaster Recovery**-Modul aktiviert ist.

Failback zu einer physischen Zielmaschine

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Der automatische Failback-Prozess zu einer physischen Maschine umfasst folgende Phasen:

1. **Planung**. In dieser Phase stellen Sie die IT-Infrastruktur (z.B. die Hosts und Netzwerkkonfigurationen) an Ihrem lokalen Standort wieder her, konfigurieren Sie die Failback-Parameter und planen Sie, wann die Datenübertragung beginnen soll.
2. **Datenübertragung**. In dieser Phase werden die Daten von der Cloud-Site zum lokalen Standort übertragen, während die virtuelle Maschine in der Cloud weiter ausgeführt wird. Sie können die nächste Phase (die Switchover-Phase) jederzeit während der Datenübertragungsphase starten. Dabei sollten Sie jedoch folgende Zusammenhänge beachten.
   Je länger Sie in der Datenübertragungsphase verbleiben,
   - desto länger wird die virtuelle Maschine in der Cloud weiter ausgeführt.
   - desto mehr Daten werden zu Ihrem lokalen Standort übertragen.
   - desto höher werden die Kosten sein, die Sie zahlen müssen (Sie werden mehr Berechnungspunkte verbrauchen).
   - desto kürzer wird die Ausfallzeit sein, die Sie während der Switchover-Phase erleben werden.

Wenn Sie die Ausfallzeit minimieren wollen, starten Sie die Switchover-Phase, nachdem mehr als 90% der Daten an den lokalen Standort übertragen wurden.

Wenn Sie eine längere Ausfallzeit in Kauf nehmen können und nicht mehr Berechnungspunkte für den Betrieb der virtuellen Maschine in der Cloud ausgeben wollen, können Sie die Switchover-Phase früher starten.

Hinweis

Der Datenübertragungsprozess verwendet eine Flashback-Technologie. Diese Technologie vergleicht die Daten, die auf der Zielmaschine vorhanden sind, mit den Daten der virtuellen Maschine in der Cloud. Wenn bereits ein Teil der Daten auf der Maschine vorhanden ist, werden diese nicht erneut übertragen. Durch diese Technologie wird die Datenübertragungsphase beschleunigt.

Aus diesem Grund empfehlen wir Ihnen, dass Sie den Server an Ihrem lokalen Standort zu der ursprünglichen Maschine wiederherstellen.

3. **Switchover**. In dieser Phase wird die virtuelle Maschine in der Cloud ausgeschaltet und die verbleibenden Daten (einschließlich des letzten Backup-Inkrements) werden zum lokalen Standort übertragen. Wenn auf den Recovery-Server kein Backup-Plan angewendet wurde, wird automatisch während der Switchover-Phase ein Backup durchgeführt, was jedoch den Prozess verlangsamt.
4. **Validierung**. In dieser Phase ist die physische Maschine am lokalen Standort betriebsbereit und Sie können sie mit einem Linux-basierten Boot-Medium neu starten. Sie können überprüfen, ob die virtuelle Maschine korrekt funktioniert – und können Folgendes tun:
   - Falls alles wie erwartet funktioniert, bestätigen Sie das Failback. Nach der Failback-Bestätigung wird die virtuelle Maschine in der Cloud gelöscht und der Recovery-Server in das Stadium Standby **Standby** zurückversetzt. Damit ist der Failback-Prozess beendet.
   - Wenn etwas nicht stimmt, können Sie den Failover-Prozess abbrechen und zur Planungsphase zurückkehren.

Hinweis

Nachdem das Boot-Medium neu gestartet worden ist, können Sie es nicht mehr verwenden. Wenn Sie während der Validierungsphase einen Fehler feststellen, müssen Sie ein neues Boot-Medium registrieren und den Failback-Prozess neu starten.

Aufgrund der verwendeten Flashback-Technologie müssen jedoch die Daten, die sich bereits am lokalen Standort befinden, nicht noch einmal übertragen werden, sodass der Failback-Prozess wesentlich schneller verläuft.

Einen Failback zu einer physischen Maschine durchführen

Hinweis

Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Sie können einen automatischen Failback zu einer physischen Zielmaschine durchführen, die sich an Ihrem lokalen Standort befindet.

Hinweis
Der Datenübertragungsprozess verwendet eine Flashback-Technologie. Diese Technologie vergleicht die Daten, die auf der Zielmaschine vorhanden sind, mit den Daten der virtuellen Maschine in der Cloud. Wenn bereits ein Teil der Daten auf der Maschine vorhanden ist, werden diese nicht erneut übertragen. Durch diese Technologie wird die Datenübertragungsphase beschleunigt.

Aus diesem Grund empfehlen wir Ihnen, dass Sie den Server an Ihrem lokalen Standort zu der ursprünglichen Maschine wiederherstellen.

Voraussetzungen

- Der Agent, den Sie zur Durchführung des Failbacks verwenden wollen, ist online und wird aktuell für keine andere Failback-Aktion verwendet.
- Ihre Internetverbindung ist stabil.
- Es ist ein registriertes Boot-Medium verfügbar. Für weitere Informationen lesen Sie den Abschnitt 'Ein Boot-Medium zur Wiederherstellung von Betriebssystemen erstellen' in der Benutzeranleitung von Cyber Protection.
- Die physische Zielmaschine ist die ursprüngliche Maschine an Ihrem lokalen Standort oder hat die gleiche Firmware wie die ursprüngliche Maschine.
- Es gibt mindestens ein vollständiges Backup der virtuellen Maschine in der Cloud.

So können Sie einen Failback zu einer physischen Maschine durchführen

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Server**.
2. Wählen Sie den Recovery-Server aus, der sich im **Failover**-Stadium befindet.
3. Klicken Sie auf die Registerkarte **Failback**.
4. Wählen Sie im Feld **Ziel** den Eintrag **Physische Maschine**.
5. Klicken Sie im Feld **Boot-Medium für das Ziel** auf **Spezifizieren**, wählen Sie das Boot-Medium aus und klicken Sie auf **Fertig**.

   Hinweis
   Wir empfehlen Ihnen, dass Sie ein vorgefertigtes Boot-Medium verwenden, weil dieses bereits vorkonfiguriert ist. Für weitere Informationen lesen Sie den Abschnitt 'Ein Boot-Medium zur Wiederherstellung von Betriebssystemen erstellen' in der Benutzeranleitung für Cyber Protection.

6. [Optional] Wenn Sie die standardmäßige Laufwerkzuordnung ändern wollen, klicken Sie im Feld **Laufwerkszuordnung** auf **Spezifizieren**, ordnen Sie dann die Laufwerke im Backup den Laufwerken der Zielmaschine zu und klicken Sie anschließend auf **Fertig**.
7. Klicken Sie zuerst auf **Datenübertragung starten** und dann im Bestätigungsfenster auf **Start**.

Hinweis
Wenn es kein Backup der virtuellen Maschine in der Cloud gibt, führt das System automatisch ein Backup durch, bevor die Datenübertragungsphase beginnt.

Die Datenübertragungsphase wird gestartet. In der Konsole werden folgende Informationen angezeigt:

Feld	Beschreibung
Fortschritt	Dieser Parameter zeigt an, wie viele Daten bereits zum lokalen Standort übertragen wurden und wie viele Daten insgesamt noch übertragen werden müssen. Die Gesamtmenge der Daten setzt sich folgendermaßen zusammen: Die Daten des letzten Backups, bevor die Datenübertragungsphase gestartet wurde, sowie die Backups von neu generierten Daten (also Backup-Inkremente), während die virtuelle Maschine in der Datenübertragungsphase weiter ausgeführt wird. Aus diesem Grund nehmen die **Fortschritt**-Werte mit der Zeit zu. Da das System während der Datenübertragung eine Flashback-Technologie verwendet und keine Daten mehr übertragen muss, die bereits auf der Zielmaschine vorhanden sind, kann der Fortschritt schneller sein, als von der Konsole anfänglich berechnet wurde.
Schätzung der Ausfallzeit	Dieser Parameter gibt an, wie lange die virtuelle Maschine in der Cloud nicht verfügbar sein wird, wenn Sie die Switchover-Phase zum jetzigen Zeitpunkt starten. Dieser Wert wird aus den Werten des Parameters **Fortschritt** berechnet – und wird mit der Zeit kleiner. Da das System während der Datenübertragung eine Flashback-Technologie verwendet und keine Daten mehr übertragen muss, die bereits auf der Zielmaschine vorhanden sind, kann die Ausfallzeit viel kürzer sein als der Wert, der anfänglich auf der Konsole angezeigt wird.

8. Klicken Sie zuerst auf **Switchover** und dann im Bestätigungsfenster erneut auf **Switchover**.
   Die Switchover-Phase wird gestartet. In der Konsole werden folgende Informationen angezeigt:

Feld	Beschreibung
Fortschritt	Dieser Parameter zeigt an, wie die Wiederherstellung der Maschine am lokalen Standort fortschreitet.
Geschätzte Zeit bis zur Fertigstellung	Dieser Parameter gibt an, wann die Switchover-Phase ungefähr abgeschlossen sein wird und wann Sie die Maschine am lokalen Standort starten können.

Hinweis
Wenn kein Backup-Plan auf die virtuelle Maschine in der Cloud angewendet wurde, wird automatisch während der Switchover-Phase ein Backup durchgeführt, was jedoch zu einer längeren Ausfallzeit führt.

9. Wenn die **Switchover**-Phase abgeschlossen wurde, starten Sie das Boot-Medium neu und überprüfen Sie dann, ob die physische Maschine an Ihrem lokalen Standort wie erwartet funktioniert.
   Für weitere Informationen lesen Sie den Abschnitt 'Laufwerke mithilfe eines Boot-Mediums wiederherstellen' in der Benutzeranleitung von Cyber Protection.
10. Klicken Sie zuerst auf **Failback bestätigen** und dann im Bestätigungsfenster auf **Bestätigen**, um den Prozess abzuschließen.
    Die virtuelle Maschine wird daraufhin in der Cloud gelöscht und der Recovery-Server in das Stadium Standby **Standby** zurückversetzt.

Hinweis
Das Anwenden eines Schutzplans auf den wiederhergestellten Server ist kein Bestandteil des Failback-Prozesses. Nach Abschluss des Failback-Prozesses können Sie aber einen Schutzplan auf den wiederhergestellten Server anwenden, damit dieser wieder geschützt ist. Sie können den gleichen Schutzplan anwenden, der auf den ursprünglichen Server angewendet wurde – oder einen neuen Schutzplan, bei dem das **Disaster Recovery**-Modul aktiviert ist.

Manueller Failback-Prozess

Hinweis
Wir empfehlen Ihnen, den Failback-Prozess nur dann im Handbetrieb zu verwenden, wenn Sie vom Support-Team dazu aufgefordert werden.

Sie können einen Failback-Prozess auch im manuellen Modus starten. In diesem Fall wird die Datenübertragung vom Backup in der Cloud zum lokalen Standort nicht automatisch durchgeführt. Dies muss manuell erfolgen, nachdem die virtuelle Maschine in der Cloud ausgeschaltet wurde. Dadurch wird der Failback-Prozess im manuellen Modus deutlich langsamer, sodass Sie mit einer längeren Ausfallzeit rechnen sollten.

Ein Failback-Prozess im manuellen Modus umfasst folgende Phasen:

1. **Planung**. In dieser Phase stellen Sie die IT-Infrastruktur (z.B. die Hosts und Netzwerkkonfigurationen) an Ihrem lokalen Standort wieder her, konfigurieren Sie die Failback-Parameter und planen Sie, wann die Datenübertragung beginnen soll.
2. **Switchover**. In dieser Phase wird die virtuelle Maschine in der Cloud ausgeschaltet und die neu generierten Daten werden gesichert. Wenn auf den Recovery-Server kein Backup-Plan angewendet wurde, wird automatisch während der Switchover-Phase ein Backup durchgeführt, was jedoch den Prozess verlangsamt. Wenn das Backup abgeschlossen wurde, stellen Sie die

Maschine zum lokalen Standort manuell wieder her. Sie können das Laufwerk entweder mithilfe eines Boot-Mediums wiederherstellen – oder die gesamte Maschine aus dem Cloud Backup Storage wiederherstellen.

3. **Validierung**. In dieser Phase überprüfen Sie, ob die physische oder virtuelle Maschine am lokalen Standort korrekt funktioniert, und bestätigen Sie den Failback-Prozess. Nach der Bestätigung wird die virtuelle Maschine in der Cloud-Site gelöscht und der Recovery-Server in das Stadium Standby **Standby** zurückversetzt.

Einen manuellen Failback-Prozess durchführen

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Sie können einen manuellen Failback-Prozess zu einer physischen oder virtuellen Zielmaschine durchführen, die sich an Ihrem lokalen Standort befindet.

So können Sie einen manuellen Failback-Prozess durchführen

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Server**.
2. Wählen Sie den Recovery-Server aus, der sich im **Failover**-Stadium befindet.
3. Klicken Sie auf die Registerkarte **Failback**.
4. Wählen Sie im Feld **Ziel** den Eintrag **Physische Maschine**.
5. Klicken Sie auf das Zahnradsymbol und aktivieren Sie dann den Schalter **Manuellen Modus verwenden**.
6. [Optional] Berechnen Sie die geschätzte Ausfallzeit während des Failback-Prozesses, indem Sie den Wert für die **Backup-Größe** durch den Wert für Ihre Internet-Geschwindigkeit teilen.

   Hinweis
   Der Wert für die Internet-Geschwindigkeit wird kleiner, wenn Sie mehrere Failback-Prozesse gleichzeitig durchführen.

7. Klicken Sie zuerst auf **Switchover** und dann im Bestätigungsfenster erneut auf **Switchover**. Die virtuelle Maschine in der Cloud-Site wird ausgeschaltet.

   Hinweis
   Wenn kein Backup-Plan auf die virtuelle Maschine in der Cloud angewendet wurde, wird automatisch während der Switchover-Phase ein Backup durchgeführt, was jedoch zu einer längeren Ausfallzeit führt.

8. Stellen Sie den Server aus einem Cloud Backup zur physischen oder virtuellen Zielmaschine an Ihrem lokalen Standort wieder her. Für weitere Informationen lesen Sie den Abschnitt 'Eine Maschine wiederherstellen' in der Benutzeranleitung von Cyber Protection.

9. Überprüfen Sie, dass die Wiederherstellung abgeschlossen wurde und die wiederhergestellte Maschine korrekt funktioniert, und klicken Sie dann auf **Die Maschine wurde wiederhergestellt**.
10. Wenn alles wie erwartet funktioniert, können Sie auf **Failback bestätigen** und dann im Bestätigungsfenster noch einmal auf **Bestätigen** klicken.

    Der Recovery-Server und die Recovery-Punkte werden für den nächsten Failover bereit sein. Wenn Sie neue Recovery-Punkte erstellen wollen, müssen Sie dem neuen lokalen Server einen Schutzplan zuweisen.

Hinweis
Das Anwenden eines Schutzplans auf den wiederhergestellten Server ist kein Bestandteil des Failback-Prozesses. Nach Abschluss des Failback-Prozesses können Sie aber einen Schutzplan auf den wiederhergestellten Server anwenden, damit dieser wieder geschützt ist. Sie können den gleichen Schutzplan anwenden, der auf den ursprünglichen Server angewendet wurde – oder einen neuen Schutzplan, bei dem das **Disaster Recovery**-Modul aktiviert ist.

Mit verschlüsselten Backups arbeiten

Sie können Recovery-Server aus verschlüsselten Backups erstellen. Zu Ihrer Bequemlichkeit können Sie eine automatische Kennwort-Applikation für verschlüsselte Backups während des Failovers zu einem Recovery-Server einrichten.

Sie können bei der Erstellung eines Recovery-Servers das Kennwort spezifizieren, das für automatische Disaster-Recovery-Aktionen verwendet werden soll. Es wird im Anmeldedatenspeicher gespeichert, einem sicheren Storage für Anmeldedaten, der im Bereich **Einstellungen** –> **Anmeldedaten** gefunden werden kann.

Anmeldedaten können mit mehreren Backups verknüpft werden.

So können Sie die gespeicherten Kennwörter im Anmeldedatenspeicher verwalten

1. Gehen Sie zu **Einstellungen** –> **Anmeldedaten**.
2. Wenn Sie bestimmte Anmeldedaten verwalten wollen, klicken Sie auf das Symbol in der letzten Spalte. Sie können die Elemente sehen, die mit diesen Anmeldedaten verknüpft sind.
   - Wenn Sie die Verknüpfung des Backups mit den ausgewählten Anmeldedaten aufheben wollen, müssen Sie auf das Papierkorb-Symbol neben dem Backup klicken. Als Ergebnis dieser Aktion müssen Sie beim Failover zum Recovery-Server das Kennwort wieder manuell eingeben.
   - Um die Anmeldedaten zu bearbeiten, klicken Sie auf **Bearbeiten** und spezifizeiren Sie den Namen oder das Kennwort.
   - Um die Anmeldedaten zu verwerfen, klicken Sie auf **Löschen**. Beachten Sie, dass Sie dann das Kennwort beim Failover zum Recovery-Server wieder manuell eingeben müssen.

Aktionen mit virtuellen Microsoft Azure-Maschinen

Hinweis
In Abhängigkeit davon, welches Lizenzierungsmodell angewendet wird, kann für einige Funktionen eine zusätzliche Lizenzierung erforderlich sein.

Sie können Failover von virtuellen Microsoft Azure-Maschinen in die Acronis Cyber Protect Cloud durchführen. Weitere Informationen finden Sie im Abschnitt '"Einen Failover durchführen" (S. 68)'.

Anschließend können Sie einen Failback aus der Acronis Cyber Protect Cloud zurück zu virtuellen Azure-Maschinen durchführen. Ein solcher Failback-Prozess verläuft ebenso wie ein Failback-Prozess zu einer physischen Maschine. Weitere Informationen finden Sie im Abschnitt '"Einen Failback zu einer physischen Maschine durchführen" (S. 78)'.

Hinweis
Wenn Sie eine neue virtuelle Azure-Maschine für Failbacks registrieren wollen, können Sie die Acronis Backup VM-Erweiterung verwenden, die in Azure verfügbar ist.

Sie können eine Multi-Site-IPsec-VPN-Konnektivität zwischen Acronis Cyber Protect Cloud und dem Azure VPN-Gateway konfigurieren. Weitere Informationen finden Sie im Abschnitt '"Multi-Site-IPsec-VPN konfigurieren" (S. 31)'.

Primäre Server einrichten

In diesem Abschnitt wird beschrieben, wie Sie Ihre primären Server erstellen und verwalten können.

Einen primären Server erstellen

Voraussetzungen

- Einer der Verbindungstypen zur Cloud-Site muss festgelegt sein.

So können Sie einen primären Server erstellen

1. Gehen Sie zur Registerkarte **Disaster Recovery** –> **Server** –> **Primäre Server**.
2. Klicken Sie auf **Erstellen**.
3. Wählen Sie eine Vorlage für die neue virtuelle Maschine aus.
4. Bestimmen Sie die Variante („Flavor“) der Konfiguration (die Anzahl der virtuellen Kerne und die Größe des RAMs). Die folgende Tabelle zeigt den maximalen Gesamtspeicherplatz (in GB) für jede Variante.

Typ	vCPU	RAM (GB)	Maximaler Gesamtspeicherplatz (GB)
V1	1	2	500
V2	1	4	1000
V3	2	8	2000
V4	4	16	4000
V5	8	32	8000
V6	16	64	16000
V7	16	128	32000
V8	16	256	64000

Hinweis
Sie können die Berechnungspunkte für jede Option sehen. Die Anzahl der Berechnungspunkte spiegelt wieder, wie viel die Ausführung des primären Servers pro Stunde kostet. Weitere Informationen finden Sie im Abschnitt '"Berechnungspunkte" (S. 12)'.

5. [Optional] Ändern Sie die Größe der virtuellen Festplatte. Wenn Sie mehr als eine Festplatte benötigen, müssen Sie auf **Laufwerk hinzufügen** klicken und dann die Größe des neuen Laufwerks festlegen. Sie können derzeit nicht mehr als 10 Laufwerke für einen primären Server hinzufügen.
6. Spezifizieren Sie das Cloud-Netzwerk, mit dem der primäre Server eingebunden werden soll.

7. Wählen Sie die **DHCP**-Option.

DHCP-Option	Beschreibung
Von der Cloud-Site bereitgestellt	Standardeinstellung. Die IP-Adresse des Servers wird von einem automatisch konfigurierten DHCP-Server in der Cloud bereitgestellt.
Benutzerdefiniert	Die IP-Adresse des Servers wird von Ihrem eigenen DHCP-Server in der Cloud bereitgestellt.

8. [Optional] Spezifizieren Sie die **MAC-Adresse**.
   Die MAC-Adresse ist eine eindeutige Kennung, die dem Netzwerkadapter des Servers zugewiesen wird. Wenn Sie benutzerdefiniertes DHCP verwenden, können Sie es so konfigurieren, dass einer bestimmten MAC-Adresse immer eine bestimmte IP-Adresse zugewiesen wird. Dadurch wird sichergestellt, dass der primäre Server immer dieselbe IP-Adresse erhält. Dadurch können Sie Applikationen ausführen, die Lizenzen haben, die wiederum auf die MAC-Adresse registriert sind.
9. Spezifizieren Sie die IP-Adresse, die der Server im Produktionsnetzwerk haben wird. Als Standardeinstellung wird die erste freie IP-Adresse aus Ihrem Produktionsnetzwerk verwendet.

   Hinweis
   Falls Sie einen DHCP-Server verwenden, fügen Sie dessen IP-Adresse zu der Server-Ausschlussliste hinzu, um IP-Adressen-Konflikte zu vermeiden.
   Wenn Sie einen benutzerdefinierten DHCP-Server verwenden, müssen Sie unter **IP-Adresse im Produktionsnetzwerk** dieselbe IP-Adresse spezifizieren, die im DHCP-Server konfiguriert ist. Ansonsten wird der Test-Failover nicht richtig funktionieren und der Server wird nicht über eine öffentliche IP-Adresse erreichbar sein.

10. [Optional] Aktivieren Sie das Kontrollkästchen **Internetzugriff**.
    Dadurch wird dem primären Server ermöglicht, auf das Internet zuzugreifen. Standardmäßig ist der TCP-Port 25 für ausgehende Verbindungen zu öffentlichen IP-Adressen geöffnet.
11. [Optional] Aktivieren Sie das Kontrollkästchen **Öffentliche IP-Adresse verwenden**.
    Wenn der primäre Server über eine öffentliche IP-Adresse verfügt, ist er aus dem Internet verfügbar. Wenn Sie das Kontrollkästchen deaktiviert lassen, wird der Server nur in Ihrem Produktionsnetzwerk verfügbar sein.
    Die öffentliche IP-Adresse wird angezeigt, nachdem Sie die Konfiguration abgeschlossen haben. Standardmäßig ist der TCP-Port 443 für eingehende Verbindungen zu öffentlichen IP-Adressen geöffnet.

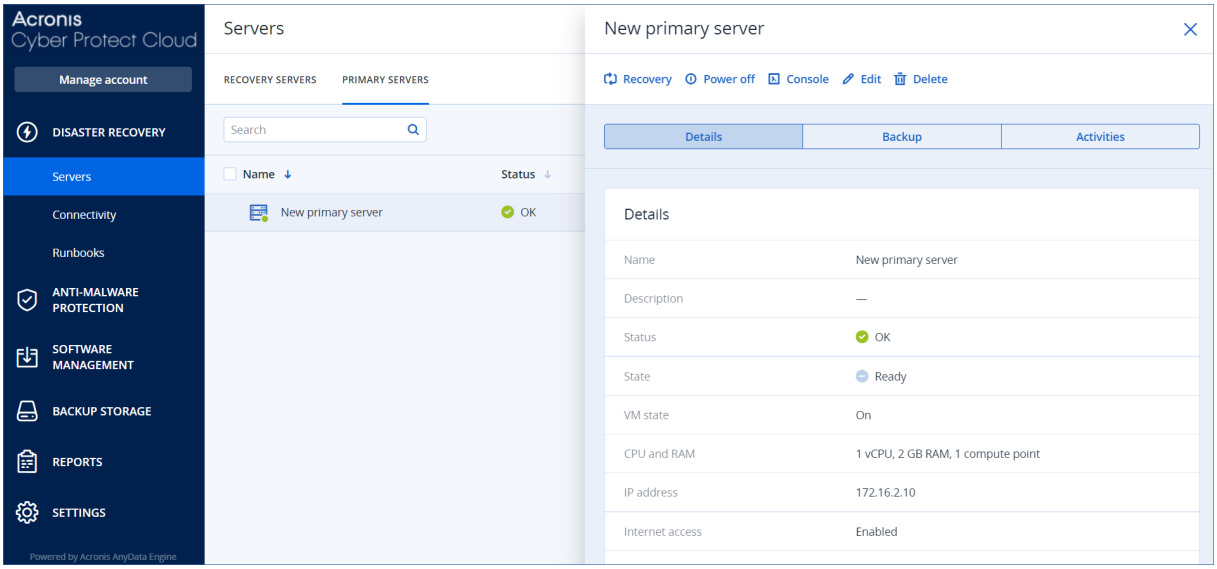
    Hinweis
    Wenn Sie das Kontrollkästchen **Öffentliche IP-Adresse verwenden** deaktivieren oder den Recovery-Server löschen, wird dessen öffentliche IP-Adresse nicht reserviert.

12. [Optional] Wählen Sie **RPO-Grenzwert festlegen**.

Der RPO-Grenzwert definiert also das maximal erlaubte Zeitintervall, das zwischen dem letzten Recovery-Punkt und dem aktuellen Zeitpunkt (an dem es zu einem Desaster kommen kann) zulässig ist. Der Wert kann zwischen 15–60 Minuten, 1–24 Stunden oder 1–14 Tagen eingestellt werden.

13. Definieren Sie einen Namen für den primären Server.
14. [Optional] Spezifizieren Sie eine Beschreibung für den primären Server.
15. [Optional] Klicken Sie auf die Registerkarte **Cloud-Firewall-Regeln**, um die Standard-Firewall-Regeln zu bearbeiten. Weitere Informationen finden Sie im Abschnitt '"Firewall-Regeln für Cloud Server einrichten" (S. 90)'.
16. Klicken Sie auf **Erstellen**.

Der primäre Server wird im Produktionsnetzwerk verfügbar gemacht. Sie können den Server über seine Konsole, über RDP, SSH oder den TeamViewer verwalten.



Aktionen mit einem primären Server

Der primäre Server wird in der -Konsole in der Registerkarte **Disaster Recovery** –> **Server** –> **Primäre Server** angezeigt.

Wenn Sie den Server starten oder stoppen wollen, müssen Sie im Fensterbereich des primären Servers auf **Einschalten** oder **Ausschalten** klicken.

Wenn Sie die primären Server-Einstellungen bearbeiten wollen, müssen Sie zuerst den Server stoppen und dann auf **Bearbeiten** klicken.

Wenn Sie dem primären Server einen Schutzplan zuweisen wollen, müssen Sie diesen auswählen und dann in der Registerkarte **Plan** auf **Erstellen** klicken. Daraufhin wird Ihnen ein vordefinierter Schutzplan angezeigt, indem Sie nur die Planung und Aufbewahrungsregeln ändern können. Weitere Informationen dazu finden Sie im Abschnitt 'Backup der Cloud-Server'.

Die Cloud Server verwalten

Wenn Sie die Cloud Server verwalten wollen, gehen Sie zu **Disaster Recovery** –> **Server**. Es gibt hier zwei Registerkarten: **Recovery-Server** und **Primäre Server**. Klicken Sie auf das Zahnradsymbol, damit alle optionalen Spalten in der Tabelle angezeigt werden.

Wenn Sie einen Cloud Server auswählen, können Sie die nachfolgenden Informationen finden.

Spaltenname	Beschreibung
Name	Ein von Ihnen definierter Cloud Server-Name
Status	Der Status, der das schwerwiegendste Problem mit einem Cloud Server anzeigt (basierend auf den aktiven Warnmeldungen).
Stadium	Ein Cloud Server-Stadium
VM-Zustand	Der Betriebszustand einer virtuellen Maschine, die mit einem Cloud Server assoziiert ist.
Aktiver Speicherort	Der Ort, wo ein Cloud Server gehostet wird. Beispiel: **Cloud**.
RPO-Grenzwert	Das maximal zulässige Zeitintervall zwischen dem letzten Recovery-Punkt, der für Failover geeignet ist, und der aktuellen Zeit. Der Wert kann zwischen 15–60 Minuten, 1–24 Stunden oder 1–14 Tagen eingestellt werden.
RPO-Compliance	Die RPO-Compliance ist das Verhältnis zwischen dem tatsächlichen RPO-Wert und dem RPO-Grenzwert. Die RPO-Compliance wird angezeigt, wenn der RPO-Grenzwert definiert ist. Sie wird folgendermaßen berechnet: **RPO-Compliance = Aktueller RPO-Wert / RPO-Grenzwert** wobei gilt: **Aktueller RPO-Wert = aktuelle Zeit – Zeit des letzten Recovery-Punkts** **RPO-Compliance-Statuszustände** Abhängig vom Verhältnis zwischen dem tatsächlichen RPO-Wert und dem RPO-Grenzwert werden folgende Statuszustände verwendet: • **Konform**. Die RPO-Compliance < 1x. Ein Server hält den RPO-Grenzwert ein. • **Überschritten**. Die RPO-Compliance <= 2x. Ein Server verstößt gegen den RPO-Grenzwert. • **Stark überschritten**. Die RPO-Compliance <= 4x. Ein Server überschreitet den RPO-Grenzwert um mehr als das Zweifache. • **Kritisch überschritten**. Die RPO-Compliance > 4x. Ein Server überschreitet den RPO-Grenzwert um mehr als das Vierfache. • **Ausstehend (keine Backups)**. Der Server ist durch den Schutzplan abgesichert, aber das Backup wird gerade erstellt und wurde noch nicht abgeschlossen.

Aktuelle RPO	Die Zeit, die seit Erstellung des letzten Recovery-Punktes vergangen ist
Neuester Recovery-Punkt	Datum und Uhrzeit, an dem der letzte Recovery-Punkt erstellt wurde.

Firewall-Regeln für Cloud Server

Sie können Firewall-Regeln konfigurieren, um den ein- und ausgehenden Datenverkehr der primären Server und Recovery-Server auf Ihrer Cloud-Site zu kontrollieren.

Sie können eingehende Regeln konfigurieren, nachdem Sie eine öffentliche IP-Adresse für den Cloud Server bereitgestellt haben. Standardmäßig ist der TCP-Port 443 erlaubt, während alle anderen eingehenden Verbindungen verweigert werden. Sie können die Standard-Firewall-Regeln ändern und eingehende Ausnahmen hinzufügen oder entfernen. Wenn keine öffentliche IP-Adresse bereitgestellt wurde, können Sie die eingehenden Regeln nur einsehen, aber nicht konfigurieren.

Sie können ausgehende Regeln konfigurieren, wenn Sie den Internet-Zugriff für den Cloud Server bereitgestellt haben. Standardmäßig wird der TCP-Port 25 verweigert, während alle anderen ausgehenden Verbindungen erlaubt sind. Sie können die Standard-Firewall-Regeln ändern und ausgehende Ausnahmen hinzufügen oder entfernen. Wenn kein Internetzugriff bereitgestellt wurde, können Sie die ausgehenden Regeln nur einsehen, aber nicht konfigurieren.

Hinweis
Aus Sicherheitsgründen gibt es vordefinierte Firewall-Regeln, die Sie nicht ändern können.

Für ein- und ausgehende Verbindungen:

- Ping zulassen: ICMP-Echo-Anforderung (Typ 8, Code 0) und ICMP-Echo-Antwort (Typ 0, Code 0)
- ICMP-Antwort 'Fragmentierung erforderlich' zulassen (Typ 3, Code 4)
- 'TTL überschritten' zulassen (Typ 11, Code 0)

Nur für eingehende Verbindungen:

- Nicht konfigurierbarer Teil: Alle verweigern

Nur für ausgehende Verbindungen:

- Nicht konfigurierbarer Teil: Alle ablehnen

Firewall-Regeln für Cloud Server einrichten

Sie können die Standard-Firewall-Regeln für die primären Server und Recovery-Server in der Cloud bearbeiten.

So können Sie die Firewall-Regeln für einen Server auf Ihrer Cloud-Site bearbeiten

1. Gehen Sie in der Cyber Protect-Konsole zu **Disaster Recovery** –> **Server**.
2. Wenn Sie die Firewall-Regeln eines Recovery-Servers bearbeiten wollen, klicken Sie auf die Registerkarte **Recovery-Server**. Wenn Sie stattdessen die Firewall-Regeln eines primären Servers bearbeiten wollen, klicken Sie auf die Registerkarte **Primäre Server**.
3. Klicken Sie zuerst auf den Server und anschließend auf **Bearbeiten**.
4. Klicken Sie auf die Registerkarte **Cloud-Firewall-Regeln**.

5. Wenn Sie die Standardaktion für die eingehenden Verbindungen ändern wollen:
   a. Wählen Sie im Listenfeld **Eingehend** die Standardaktion.

Aktion	Beschreibung
Alle verweigern	Verweigert jeden eingehenden Datenverkehr. Sie können Ausnahmen hinzufügen und Datenverkehr von bestimmten IP-Adressen, Protokollen und Ports zulassen.
Alle erlauben	Erlaubt jeden eingehenden TCP- und UDP-Datenverkehr. Sie können Ausnahmen hinzufügen und den Datenverkehr von bestimmten IP-Adressen, Protokollen und Ports verbieten.

Hinweis
Wenn Sie die Standardaktion ändern, wird die Konfiguration der vorhandenen Eingangsregeln ungültig und entfernt.

   b. [Optional] Wenn Sie die vorhandenen Ausnahmen speichern wollen, müssen Sie im Bestätigungsfenster den Befehl **Eingegebene Ausnahmen speichern** auswählen.
   c. Klicken Sie auf **Bestätigen**.
6. Wenn Sie eine Ausnahme hinzufügen wollen, dann:
   a. Klicken Sie auf **Ausnahme hinzufügen**.
   b. Spezifizieren Sie die Firewall-Parameter.

Firewall-Parameter	Beschreibung
Protokoll	Wählen Sie das Protokoll für die Verbindung aus. Folgende Optionen werden unterstützt: • **TCP** • **UDP:** • **TCP+UDP**
Server-Port	Wählen Sie die Ports aus, für die die Regel gelten soll. Sie können Folgendes spezifizieren: • eine bestimmte Port-Nummer (z.B. `2298`) • einen Port-Nummernbereich (z.B. `6000-6700`) • eine beliebige Portnummer. Verwenden Sie `*`, wenn die Regel auf jede Port-Nummer angewendet werden soll.
Client-IP-Adresse	Wählen Sie die IP-Adressen aus, für die die Regel gelten soll. Sie können Folgendes spezifizieren: • eine bestimmte IP-Adresse (z.B. `192.168.0.0`) • einen Bereich von IP-Adressen im CIDR-Format (z.B. `192.168.0.0/24`) • eine beliebige IP-Adresse. Verwenden Sie `*`, wenn die Regel auf jede IP-Adresse angewendet werden soll.

7. Wenn Sie eine vorhandene Eingangsausnahme entfernen wollen, klicken Sie auf das Papierkorb-Symbol neben der Ausnahme.
8. Wenn Sie die Standardaktion für die ausgehenden Verbindungen ändern wollen:
   a. Wählen Sie im Listenfeld **Ausgehend** die Standardaktion.

Aktion	Beschreibung
Alle verweigern	Verweigert jeden ausgehenden Datenverkehr. Sie können Ausnahmen hinzufügen und Datenverkehr zu bestimmten IP-Adressen, Protokollen und Ports zulassen.
Alle erlauben	Erlaubt jeden ausgehenden Datenverkehr. Sie können Ausnahmen hinzufügen und den Datenverkehr von bestimmten IP-Adressen, Protokollen und Ports verbieten.

Hinweis
Wenn Sie die Standardaktion ändern, wird die Konfiguration der vorhandenen Ausgangsregeln ungültig und entfernt.

   b. [Optional] Wenn Sie die vorhandenen Ausnahmen speichern wollen, müssen Sie im Bestätigungsfenster den Befehl **Eingegebene Ausnahmen speichern** auswählen.
   c. Klicken Sie auf **Bestätigen**.
9. Wenn Sie eine Ausnahme hinzufügen wollen, dann:
   a. Klicken Sie auf **Ausnahme hinzufügen**.
   b. Spezifizieren Sie die Firewall-Parameter.

Firewall-Parameter	Beschreibung
Protokoll	Wählen Sie das Protokoll für die Verbindung aus. Folgende Optionen werden unterstützt: • **TCP** • **UDP:** • **TCP+UDP**
Server-Port	Wählen Sie die Ports aus, für die die Regel gelten soll. Sie können Folgendes spezifizieren: • eine bestimmte Port-Nummer (z.B. `2298`) • einen Port-Nummernbereich (z.B. `6000-6700`) • eine beliebige Portnummer. Verwenden Sie `*`, wenn die Regel auf jede Port-Nummer angewendet werden soll.
Client-IP-Adresse	Wählen Sie die IP-Adressen aus, für die die Regel gelten soll. Sie können Folgendes spezifizieren: • eine bestimmte IP-Adresse (z.B. `192.168.0.0`) • einen Bereich von IP-Adressen im CIDR-Format (z.B. `192.168.0.0/24`)

Firewall-Parameter	Beschreibung
	• eine beliebige IP-Adresse. Verwenden Sie *, wenn die Regel auf jede IP-Adresse angewendet werden soll.

10. Wenn Sie eine vorhandene Ausgangsausnahme entfernen wollen, klicken Sie auf das Papierkorb-Symbol neben der Ausnahme.
11. Klicken Sie auf **Speichern**.

Die Aktivitäten der Cloud-Firewall prüfen

Wenn die Konfiguration der Firewall-Regeln eines Cloud Servers aktualisiert werden, ist anschließend in der Cyber Protect-Konsole ein Protokoll der Update-Aktivität verfügbar. Sie können das Protokoll einsehen und dabei folgende Informationen überprüfen:

- den Benutzernamen desjenigen Benutzers, der die Konfiguration aktualisiert hat
- den Zeitpunkt (Datum, Uhrzeit) des Updates
- die Firewall-Einstellungen für ein- und ausgehende Verbindungen
- die Standardaktionen für ein- und ausgehende Verbindungen
- die Protokolle, Ports und IP-Adressen der Ausnahmen für ein- und ausgehende Verbindungen

So können Sie die Details zu einer Konfigurationsänderung der Cloud-Firewall-Regeln einsehen

1. Klicken Sie in der Cyber Protect-Konsole auf **Monitoring** –> **Aktivitäten**.
2. Klicken Sie zuerst auf die entsprechende Aktivität und dann auf **Alle Eigenschaften**.
   Die Beschreibung der Aktivität sollte **Cloud Server-Konfiguration wird aktualisiert** lauten.
3. Überprüfen Sie im Feld **Kontext** die Informationen, für die Sie sich interessieren.

Backup der Cloud Server

Die primären Server und Recovery-Server werden agentenlos auf der Cloud-Site gesichert. Für diese Backups gelten die nachfolgenden Einschränkungen.

- Der einzig mögliche Backup-Speicherort ist der Cloud Storage. Primäre Server werden zum Storage **Backup der primären Server** gesichert.

  Hinweis
  Microsoft Azure-Backup-Speicherorte werden nicht unterstützt.

- Ein Backup-Plan kann nicht auf mehrere Server gleichzeitig angewendet werden. Jeder Server muss seinen eigenen Backup-Plan haben, auch wenn alle Backup-Pläne ansonsten die gleichen Einstellungen haben.
- Auf einen Server kann nur je ein Backup-Plan angewendet werden.
- Applikationskonforme Backups werden nicht unterstützt.
- Es ist keine Verschlüsselung verfügbar.
- Es sind keine Backup-Optionen verfügbar.

Wenn Sie einen primären Server löschen, werden auch dessen Backups gelöscht.

Ein Recovery-Server wird nur im Failover-Stadium per Backup gesichert. Seine Backups setzen die Backup-Sequenz des ursprünglichen Servers fort. Wenn ein Failback durchgeführt wird, kann der ursprüngliche Server diese Backup-Sequenz fortsetzen. Die Backups des Recovery-Servers können also nur manuell gelöscht werden – oder weil Aufbewahrungsregeln angewendet werden. Wenn ein Recovery-Server gelöscht wird, werden seine Backups immer aufbewahrt.

Hinweis
Die Backup-Pläne für Cloud Server werden nach UTC-Zeit durchgeführt.

Orchestrierung (Runbooks)

Hinweis
In Abhängigkeit davon, welches Lizenzierungsmodell angewendet wird, kann für einige Funktionen eine zusätzliche Lizenzierung erforderlich sein.

Ein Runbook ist eine Zusammenstellung von Anweisungen, die beschreibt, wie die Produktionsumgebung in die Cloud übertragen wird. Sie können Runbooks in der Cyber Protect-Konsole erstellen. Wenn Sie auf die Anzeige **Runbooks** zugreifen wollen, wählen Sie die Befehle **Disaster Recovery** –> **Runbooks**.

Warum sollte ich Runbooks verwenden?

Mit Runbooks können Sie Folgendes tun:

- Ein Failover von einem oder mehreren Servern automatisieren
- Das Failover-Ergebnis automatisch überprüfen, indem Sie die Server-IP-Adresse anpingen und die Verbindung zu dem von Ihnen spezifizierten Port überprüfen
- Die Reihenfolge der Aktionen mit den Servern festlegen, die verteilte Applikationen ausführen
- Manuelle Aktionen in den Workflow einbinden
- Die Integrität Ihrer Disaster Recovery-Lösung überprüfen, indem Sie die entsprechenden Runbooks im Testmodus ausführen.

Ein Runbook erstellen

Ein Runbook besteht aus Schritten, die nacheinander ausgeführt werden. Ein Schritt besteht aus Aktionen, die gleichzeitig gestartet werden.

Sie können die nachfolgende Anleitung befolgen oder sich das Video-Tutorial ansehen.

So können Sie ein Runbook erstellen

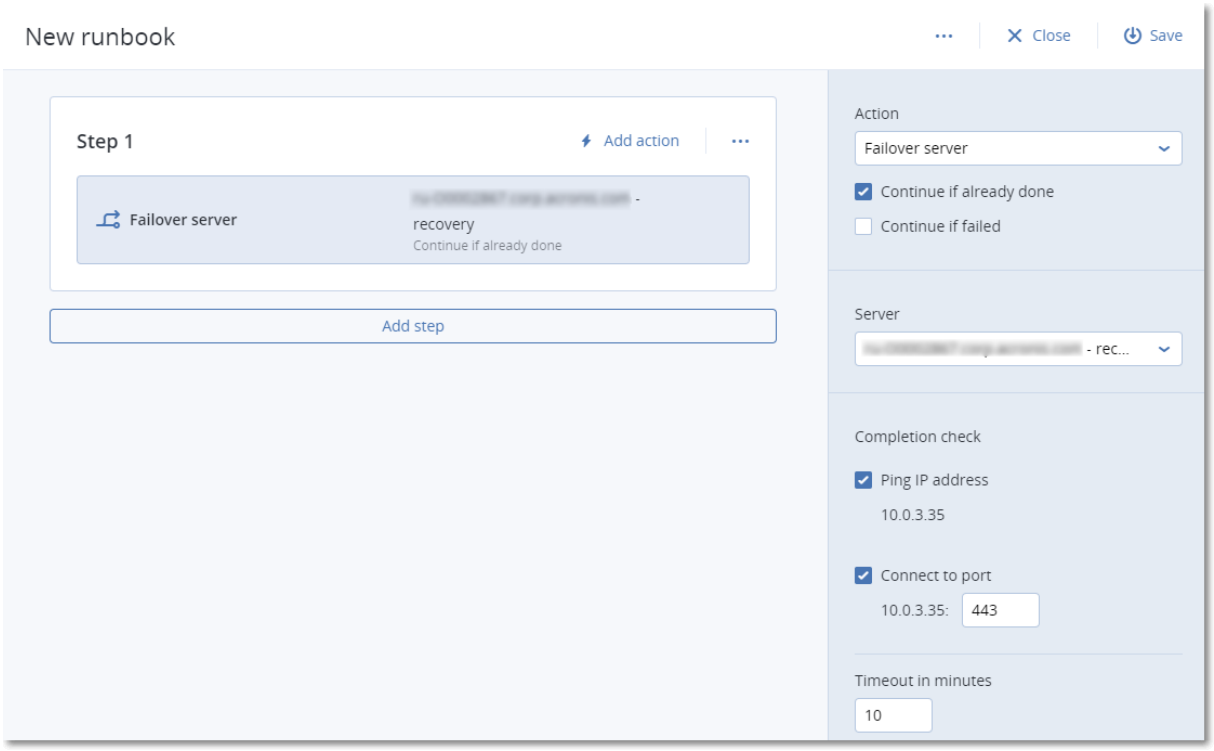
1. Gehen Sie in der Cyber Protection-Konsole zu **Disaster Recovery** –> **Runbooks**.
2. Klicken Sie auf **Runbook erstellen**.
3. Klicken Sie auf **Schritt hinzufügen**.
4. Klicken Sie zuerst auf **Aktion hinzufügen** und wählen Sie dann die Aktion aus, die Sie dem Schritt hinzufügen wollen.

Aktion	Beschreibung
Server-Failover ausführen	Führt eine Failover-Aktion mit einem Cloud Server durch. Wenn Sie diese Aktion definieren wollen, müssen Sie einen Cloud Server auswählen und die Runbook-Parameter konfigurieren, die für diese Aktion verfügbar sind. Weitere Informationen zu diesen Parametern finden Sie im Abschnitt '"Runbook-

Aktion	Beschreibung
	Parameter" (S. 98)'. **Hinweis** Wenn das Backup des von Ihnen ausgewählten Servers über die Maschinen-Eigenschaften verschlüsselt wurde, wird die Aktion **Server-Failover ausführen** pausiert und automatisch zu **Benutzereingriff erforderlich** geändert. Um mit der Ausführung des Runbooks fortfahren zu können, müssen Sie das Kennwort für das verschlüsselte Backup angeben.
Server-Failback ausführen	Führt eine Failback-Aktion mit einem Cloud Server durch. Wenn Sie diese Aktion definieren wollen, müssen Sie einen Cloud Server auswählen und die Runbook-Parameter konfigurieren, die für diese Aktion verfügbar sind. Weitere Informationen zu diese Einstellungen finden Sie im Abschnitt '"Runbook-Parameter" (S. 98)'. **Hinweis** Runbook-Aktionen unterstützen Failbacks nur im manuellen Modus. Das heißt, wenn Sie den Failback-Prozess durch die Ausführung eines Runbooks starten, in dem ein **Server-Failback ausführen**-Schritt enthalten ist, erfordert die Prozedur eine manuelle Interaktion: Sie müssen die Maschine zuerst manuell wiederherstellen und dann den Failback-Prozess über die Registerkarte **Disaster Recovery** –> **Server** bestätigen oder abbrechen.
Server starten	Startet einen Cloud Server. Wenn Sie diese Aktion definieren wollen, müssen Sie einen Cloud Server auswählen und die Runbook-Parameter konfigurieren, die für diese Aktion verfügbar sind. Weitere Informationen zu diese Einstellungen finden Sie im Abschnitt '"Runbook-Parameter" (S. 98)'. **Hinweis** Die Aktion **Server starten** ist bei Test-Failover-Aktionen in Runbooks nicht verfügbar. Wenn Sie versuchen, eine solche Aktion auszuführen, wird diese mit folgender Fehlermeldung fehlschlagen: Fehlgeschlagen: Die Aktion ist auf das aktuelle Server-Stadium nicht anwendbar.
Server stoppen	Stoppt einen Cloud Server. Wenn Sie diese Aktion definieren wollen, müssen Sie einen Cloud Server auswählen und die Runbook-Parameter konfigurieren, die für diese Aktion verfügbar sind. Weitere Informationen zu diese Einstellungen finden Sie im Abschnitt '"Runbook-Parameter" (S. 98)'. **Hinweis** Die Aktion **Server stoppen** ist bei Test-Failover-Aktionen in Runbooks nicht verfügbar. Wenn Sie versuchen, eine solche Aktion auszuführen, wird diese mit folgender Fehlermeldung fehlschlagen: Fehlgeschlagen: Die Aktion ist auf das aktuelle Server-Stadium nicht anwendbar.
Manuelle Aktion	Eine manuelle Aktion erfordert das Eingreifen eines Benutzers. Wenn Sie diese

Aktion	Beschreibung
	Aktion definieren wollen, müssen Sie eine Beschreibung eingeben. Wenn eine Runbook-Sequenz eine manuelle Aktion erreicht, wird das Runbook solange pausiert, bis ein Benutzer die erforderliche manuelle Aktion durchführt, z.B. durch Klicken auf die Bestätigungsschaltfläche.
Runbook ausführen	Führt ein anderes Runbook aus. Wenn Sie diese Aktion definieren wollen, müssen Sie ein Runbook auswählen. Ein Runbook kann nur eine (1) Ausführung eines bestimmten Runbooks enthalten. Wenn Sie beispielsweise die Aktion 'Runbook A ausführen' hinzugefügt haben, können Sie zwar die Aktion 'Runbook B ausführen' hinzufügen, aber keine weitere Aktion 'Runbook A ausführen'.

5. Definieren Sie die Runbook-Parameter für die Aktion. Weitere Informationen zu diesen Parametern finden Sie im Abschnitt '"Runbook-Parameter" (S. 98)'.
6. [Optional] So können Sie eine Beschreibung für den Schritt hinzufügen:
   a. Klicken Sie auf das Drei-Punkte-Symbol und anschließend auf **Beschreibung**.
   b. Geben Sie eine Beschreibung für den Schritt ein.
   c. Klicken Sie auf **Fertig**.
7. Wiederholen Sie die Schritte 3–6, bis Sie die gewünschte Abfolge von Schritten und Aktionen erstellt haben.
8. [Optional] So können Sie den Standardnamen des Runbooks ändern:
   a. Klicken Sie auf das Drei-Punkte-Symbol.
   b. Geben Sie den Namen des Runbooks ein.
   c. Geben Sie eine Beschreibung für das Runbook ein.
   d. Klicken Sie auf **Fertig**.
9. Klicken Sie auf **Speichern**.
10. Klicken Sie auf **Schließen**.



Runbook-Parameter

Runbook-Parameter sind spezifische Einstellungen, die Sie konfigurieren müssen, um eine Runbook-Aktion zu definieren. Es gibt zwei Kategorien von Runbook-Parametern: für Aktionen und für die Fertigstellungsprüfung.

Aktionsparameter definieren das Verhalten des Runbooks in Abhängigkeit vom anfänglichen Stadium oder dem Ergebnis einer Aktion.

Parameter für die Fertigstellungsprüfung stellen sicher, dass der Server verfügbar ist und die notwendigen Dienste bereitstellt. Wenn eine Fertigstellungsprüfung scheitert, wird die Aktion als fehlgeschlagen betrachtet.

Die folgende Tabelle beschreibt die konfigurierbaren Runbook-Parameter für jede Aktion.

Runbook-Parameter	Kategorie	Für Aktion verfügbar	Beschreibung
Fortsetzen, wenn bereits durchgeführt	Aktionsparameter	• **Server-Failover ausführen** • **Server starten** • **Server stoppen** • **Server-Failback ausführen**	Dieser Parameter definiert das Runbook-Verhalten, wenn die erforderliche Aktion bereits durchgeführt wurde (weil beispielsweise ein Failover bereits durchgeführt wurde oder ein Server bereits ausgeführt wird). Wenn dieser Parameter aktiviert ist, gibt das Runbook eine

Runbook-Parameter	Kategorie	Für Aktion verfügbar	Beschreibung
			Warnung aus und fährt mit der Ausführung fort. Wenn der Parameter deaktiviert wurde, schlägt die Aktion und damit dann auch das Runbook fehl. Dieser Parameter ist standardmäßig aktiviert.
Fortsetzen, wenn fehlgeschlagen	Aktionsparameter	• **Server-Failover ausführen** • **Server starten** • **Server stoppen** • **Server-Failback ausführen**	Dieser Parameter definiert das Runbook-Verhalten, wenn die erforderliche Aktion fehlschlägt. Wenn dieser Parameter aktiviert ist, gibt das Runbook eine Warnung aus und fährt mit der Ausführung fort. Wenn der Parameter deaktiviert wurde, schlägt die Aktion und damit dann auch das Runbook fehl. Dieser Parameter ist standardmäßig deaktiviert.
IP-Adresse anpingen	Fertigstellungsprüfung	• **Server starten**	Die Software wird die Produktions-IP-Adresse des Cloud Servers solange anpingen, bis der Server antwortet oder es zu einem Timeout kommt (je nachdem, was zuerst eintritt).
Mit Port verbinden (standardmäßig 443)	Fertigstellungsprüfung	• **Server-Failover ausführen** • **Server starten**	Die Software wird versuchen, sich über die Produktions-IP-Adresse und den von Ihnen spezifizierten Port mit dem Cloud Server zu verbinden, bis die Verbindung hergestellt ist oder es zu einem Timeout kommt (je nachdem, was zuerst eintritt). Auf diese Weise können Sie überprüfen, ob die Applikation, die auf dem angegebenen Port lauscht, auch ausgeführt wird.
Zeitlimit in Minuten	Fertigstellungsprüfung	• **Server-Failover ausführen** • **Server starten**	Der vorgegebene Timeout-Wert beträgt 10 Minuten.

Aktionen mit Runbooks

Hinweis
Die Verfügbarkeit dieser Funktion hängt von den Service-Quotas ab, die für Ihr Konto aktiviert wurden.

Um auf die Liste der Aktionen zuzugreifen, bewegen Sie den Mauszeiger auf ein Runbook und klicken Sie auf das Drei-Punkte-Symbol. Wenn ein Runbook nicht ausgeführt wird, sind folgenden Aktionen verfügbar:

- **Ausführen**
- **Bearbeiten**
- **Klonen**
- **Löschen**

Ein Runbook ausführen

Jedes Mal, wenn Sie auf **Ausführen** klicken, werden Sie zur Eingabe von Ausführungsparametern aufgefordert. Diese Parameter gelten für alle Failover- und Failback-Operationen, die im Runbook enthalten sind. Diejenigen Runbooks, die mit der Operation **Runbook ausführen** spezifiziert werden, erben diese Parameter vom Haupt-Runbook.

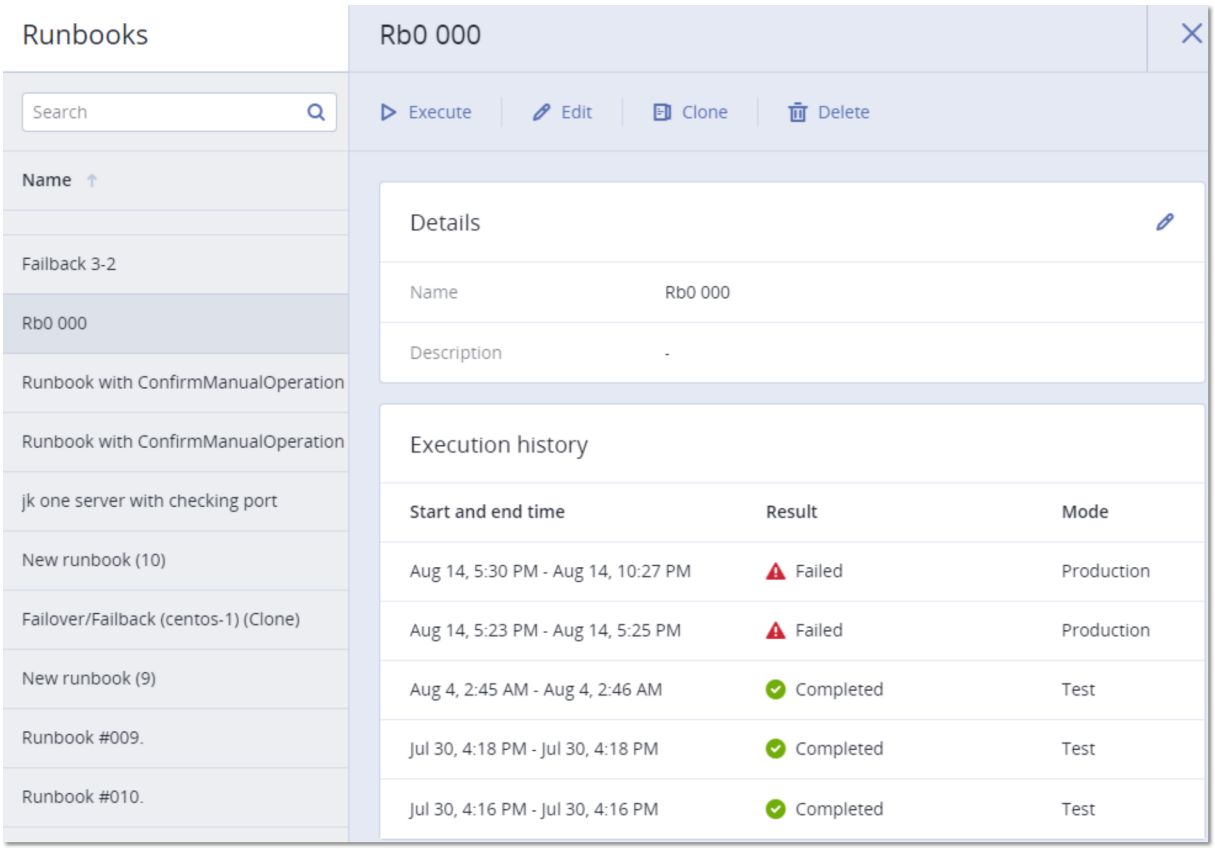
- **Failover- und Failback-Modus**
  Wählen Sie, ob Sie einen Test-Failover (Standardvorgabe) oder einen tatsächlichen (Produktions-)Failover ausführen möchten. Der Failback-Modus entspricht dem gewählten Failover-Modus.
- **Failover-Recovery-Punkt**
  Wählen Sie den neuesten Recovery-Punkt (Standardvorgabe) oder wählen Sie einen bestimmten Zeitpunkt in der Vergangenheit. Bei letzterem werden für jeden Server diejenigen Recovery-Punkte ausgewählt, die dem spezifizierten Zeitpunkt am nächsten liegen.

Eine Runbook-Ausführung stoppen

Sie können während einer Runbook-Ausführung den Befehl **Stopp** aus der Liste der verfügbaren Aktionen wählen. Die Software wird alle bereits gestarteten Aktionen abschließen – außer solche Aktionen, die eine Benutzerinteraktion erfordern.

Den Ausführungsverlauf anzeigen

Wenn Sie ein Runbook in der Registerkarte **Runbooks** auswählen, wird Ihnen die Software Details und einen Ausführungsverlauf zu diesem Runbook anzeigen. Klicken Sie auf eine Zeile, die zu einer bestimmten Ausführung gehört, um das entsprechende Ausführungsprotokoll einzusehen.


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
Failed
Production
Aug 14, 5:23 PM - Aug 14, 5:25 PM
Failed
Production
Aug 4, 2:45 AM - Aug 4, 2:46 AM
Completed
Test
Jul 30, 4:18 PM - Jul 30, 4:18 PM
Completed
Test
Jul 30, 4:16 PM - Jul 30, 4:16 PM
Completed
Test

Site-to-Site-OpenVPN – Zusätzliche Informationen

Wenn Sie einen Recovery-Server erstellen, konfigurieren Sie dessen **IP-Adresse im Produktionsnetzwerk** und dessen **Test-IP-Adresse**.

Nachdem Sie einen Failover durchgeführt (die virtuelle Maschine in der Cloud ausgeführt) und sich an der virtuellen Maschine angemeldet haben, um die IP-Adresse des Servers zu überprüfen, sehen Sie die **IP-Adresse im Produktionsnetzwerk**.

Wenn Sie einen Test-Failover durchführen, können Sie den Test-Server nur über die **Test-IP-Adresse** erreichen, die wiederum nur in der Konfiguration des Recovery-Servers sichtbar ist.

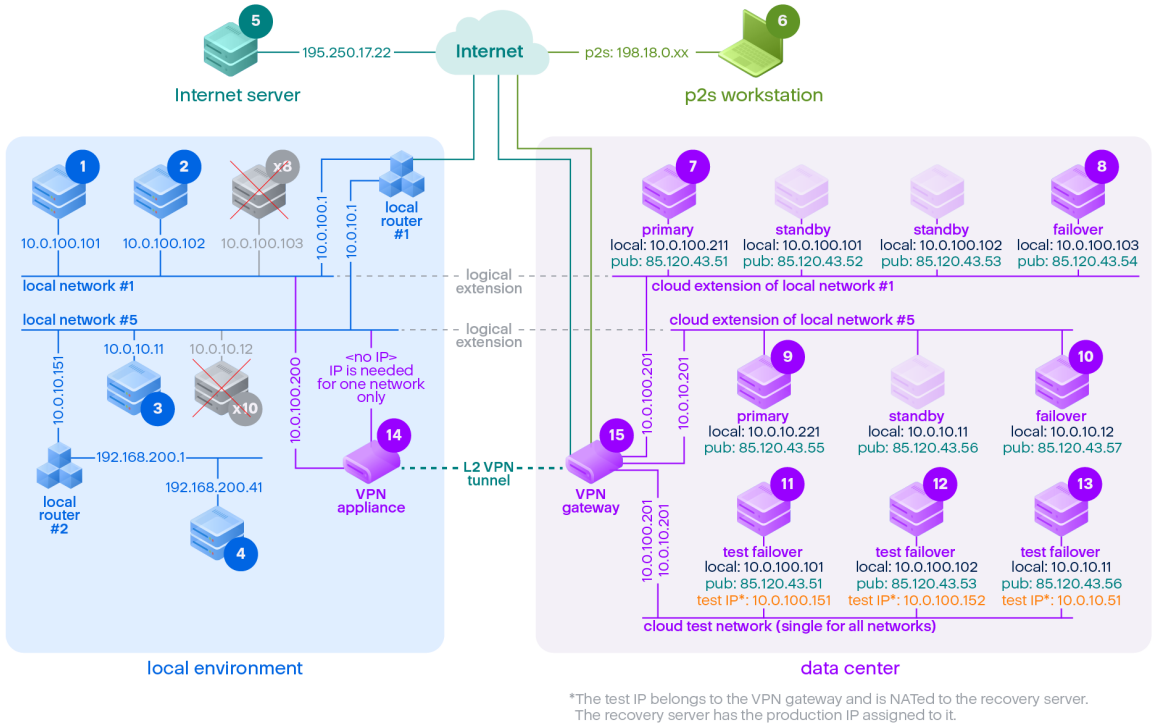
Wenn Sie einen Test-Server von Ihrem lokalen Standort aus erreichen wollen, müssen Sie die **Test-IP-Adresse** verwenden.

Hinweis
Die Netzwerkkonfiguration des Servers zeigt immer die **IP-Adresse im Produktionsnetzwerk** an (weil der Test-Server spiegelt, wie der Produktionsserver aussehen würde). Dies geschieht, weil die Test-IP-Adresse nicht zum Test-Server, sondern zum VPN-Gateway gehört und per NAT in die Produktions-IP-Adresse übersetzt wird.

Das untere Diagramm zeigt ein Beispiel für eine Site-to-Site-OpenVPN-Konfiguration. Einige der Server in der lokalen Umgebung werden per Failover zur Cloud wiederhergestellt (während die Netzwerkinfrastruktur in Ordnung ist).

1. Der Kunde hat das Disaster Recovery durch folgende Maßnahmen aktiviert:
   a. er hat die VPN-Appliance (14) konfiguriert und sie mit dem dedizierten Cloud VPN-Server (15) verbunden
   b. er hat einige der lokalen Server per Disaster Recovery geschützt (1, 2, 3, x8 und x10)
      Einige Server am lokalen Standort (wie 4) sind mit Netzwerken verbunden, die nicht mit der VPN-Appliance verbunden sind. Solche Server sind nicht per Disaster Recovery geschützt.
2. Ein Teil der Server (die mit verschiedenen Netzwerken verbunden sind) arbeitet am lokalen Standort: (1, 2, 3 und 4)
3. Die geschützten Server (1, 2 und 3) werden per Test-Failover (11, 12 und 13) getestet
4. Einige Server am lokalen Standort sind nicht verfügbar (x8, x10). Nach der Durchführung des Failovers werden sie in der Cloud verfügbar (8 und 10)

5. Einige primäre Server (7 und 9), die mit verschiedenen Netzwerken verbunden sind, sind in der Cloud-Umgebung verfügbar
6. (5) ist ein Server im Internet mit einer öffentlichen IP-Adresse
7. (6) ist eine Workstation, die über eine Point-to-Site-Verbindung (P2S) mit der Cloud verbunden ist



In diesem Beispiel sind folgende Verbindungen von einem Server in der Zeile **Von:** zu einem Server in der Spalte **Zu:** möglich.

	Zu:	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Von:		lokal	lokal	lokal	lokal	Interne	P2S	primär	Failover	primär	Failover	Test-	Test-	Test-	VPN-	VPN-

	Zu:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
						t						Failover	Failover	Failover	Applianc e	Server
1	lokal		direkt	über lokale n Router 1	über lokale n Router 2	über lokalen Router 1 und Interne t	nein	über Tunnel: lokal über lokalen Router 1 und Interne t: pub	über Tunnel: lokal über lokalen Router 1 und Interne t: pub	über Tunnel: lokal über lokalen Router 1 und Interne t: pub	über Tunnel: lokal über lokalen Router 1 und Interne t: pub	über Tunnel: NAT (VPN-Server) über lokalen Router 1 und Interne t: pub	über Tunnel: NAT (VPN-Server) über lokalen Router 1 und Interne t: pub	über lokalen Router 1 und Tunnel: NAT (VPN-Server) über lokalen Router 1 und Interne t: pub	direkt	nein
2	lokal	direkt		über lokale n Router 1	über lokale n Router 2	über lokalen Router 1 und Interne t	nein	über Tunnel: lokal über lokalen Router 1 und Interne t: pub	über Tunnel: lokal über lokalen Router 1 und Interne t: pub	über Tunnel: lokal über lokalen Router 1 und Interne t: pub	über Tunnel: lokal über lokalen Router 1 und Interne t: pub	über Tunnel: NAT (VPN-Server) über lokalen Router 1 und Interne	über Tunnel: NAT (VPN-Server) über lokalen Router 1 und Interne	über lokalen Router 1 und Tunnel: NAT (VPN-Server) über	direkt	nein

	Zu:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
												t: pub	t: pub	lokalen Router 1 und Internet: pub		
3	lokal	über lokalen Router 1	über lokalen Router 1		über lokalen Router 2	über lokalen Router 1 und Internet	nein	über Tunnel: lokal über lokalen Router 1 und Internet: pub	über Tunnel: lokal über lokalen Router 1 und Internet: pub	über Tunnel: lokal über lokalen Router 1 und Internet: pub	über Tunnel: lokal über lokalen Router 1 und Internet: pub	über Tunnel: NAT (VPN-Server) über lokalen Router 1 und Internet: pub	über Tunnel: NAT (VPN-Server) über lokalen Router 1 und Internet: pub	über lokalen Router 1 und Tunnel: NAT (VPN-Server) über lokalen Router 1 und Internet: pub	über lokalen Router	nein
4	lokal	über lokalen Router 2 und Router 1	über lokalen Router 2 und Router 1	über lokalen Router 2		über lokalen Router 2 und Router 1 und Interne	nein	über lokalen Router 2 und Tunnel: lokal	über lokalen Router 2 und Tunnel: lokal	über lokalen Router 2 und Tunnel: lokal	über lokalen Router 2 und Tunnel: lokal	über Tunnel: NAT (VPN-Server) über	über Tunnel: NAT (VPN-Server) über	über Tunnel: NAT (VPN-Server) über	über lokalen Router 2	nein

	Zu:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
						t		über lokalen Router 2 und lokalen Router 1 und Internet: pub	über lokalen Router 2 und lokalen Router 1 und Internet: pub	über lokalen Router 2 und lokalen Router 1 und Internet: pub	über lokalen Router 2 und lokalen Router 1 und Internet: pub	lokalen Router 2 und Router 1 und Internet: pub	lokalen Router 2 und Router 1 und Internet: pub	lokalen Router 2 und Router 1 und Internet: pub		
5	Internet	nein	nein	nein	nein		n/a	über Internet: pub	über Internet: pub	über Internet: pub	über Internet: pub	über Internet: pub	über Internet: pub	über Internet: pub	nein	nein
6	P2S	nein	nein	nein	nein	über Internet		über P2S-VPN (VPN-Server): lokal über Internet: pub	über P2S-VPN (VPN-Server): lokal über Internet: pub	über P2S-VPN (VPN-Server): lokal über Internet: pub	über P2S-VPN (VPN-Server): lokal über Internet: pub	über P2S-VPN – NAT (VPN-Server) über Internet: pub	über P2S-VPN – NAT (VPN-Server) über Internet: pub	über P2S-VPN – NAT (VPN-Server) über Internet: pub	nein	nein
7	primär	über Tunnel	über Tunnel	über Tunnel und lokale	über Tunnel und lokale	über Internet (über VPN-Server)	nein		direkt in der Cloud: lokal	über Tunnel und lokalen	über Tunnel und lokalen	über VPN-Server: NAT	über VPN-Server: NAT	über Tunnel und lokalen	nein	Nur DHCP- und DNS-

	Zu:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
				n Router 1	n Router 1 und 2					Router 1: lokal	Router 1: lokal			Router 1: NAT		Protokolle
8	Failover	über Tunnel	über Tunnel	über Tunnel und lokalen Router 1	über Tunnel und lokalen Router 1 und 2	über Internet (über VPN-Server)	nein	direkt in der Cloud: lokal		über Tunnel und lokalen Router 1: lokal	über Tunnel und lokalen Router 1: lokal	über VPN-Server: NAT	über VPN-Server: NAT	über Tunnel und lokalen Router 1: NAT	nein	Nur DHCP- und DNS-Protokolle
9	primär	über Tunnel und lokalen Router 1	über Tunnel und lokalen Router 1	über Tunnel	über Tunnel	über Internet (über VPN-Server)	nein	über Tunnel und lokalen Router 1: lokal	über Tunnel und lokalen Router 1: lokal		direkt in der Cloud: lokal	über Tunnel und lokalen Router 1: NAT	über Tunnel und lokalen Router 1: NAT	über VPN-Server: NAT	nein	Nur DHCP- und DNS-Protokolle
10	Failover	über Tunnel und lokalen Router 1	über Tunnel und lokalen Router 1	über Tunnel	über Tunnel	über Internet (über VPN-Server)	nein	über Tunnel und lokalen Router 1: lokal	über Tunnel und lokalen Router 1: lokal	direkt in der Cloud: lokal		über Tunnel und lokalen Router 1: NAT	über Tunnel und lokalen Router 1: NAT	über VPN-Server: NAT	nein	Nur DHCP- und DNS-Protokolle

	Zu:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
11	Test-Failover	nein	nein	nein	nein	über Internet (über VPN-Server)	nein	nein	nein	nein	nein		direkt in der Cloud: lokal	über VPN-Server: lokal (Routing)	nein	Nur DHCP- und DNS-Protokolle
12	Test-Failover	nein	nein	nein	nein	über Internet (über VPN-Server)	nein	nein	nein	nein	nein	direkt in der Cloud: lokal		über VPN-Server: lokal (Routing)	nein	Nur DHCP- und DNS-Protokolle
13	Test-Failover	nein	nein	nein	nein	über Internet (über VPN-Server)	nein	nein	nein	nein	nein	über VPN-Server: lokal (Routing)	über VPN-Server: lokal (Routing)		nein	Nur DHCP- und DNS-Protokolle
14	VPN-Appliance	direkt	direkt	über lokalen Router 1	über lokalen Router 2	über Internet (lokaler Router 1)	nein	nein	nein	nein	nein	nein	nein	nein		nein
15	VPN-Server	nein	nein	nein	nein	nein	nein	nein	nein	nein	nein	nein	nein	nein	nein	

Glossar

C

Cloud-Site (oder DR-Site)

Ein in der Cloud gehosteter Remote-Standort, der dazu verwendet wird, im Desasterfall eine Recovery-Infrastruktur auszuführen.

Cloud Server

Allgemeiner Begriff für eine primären Server oder Recovery- Server (auch Wiederherstellungsserver genannt).

F

Failback

Ein Prozess, der Server am ihrem ursprünglichen lokalen Standort wiederherstellt, nachdem diese zuvor per Failover in die Cloud-Site verschoben worden waren.

Failover

Umschalten von Workloads oder Applikationen in die Cloud- Site, wenn/weil es am lokalen Standort zu einem (natürlichen oder von Menschen verursachten) Desaster gekommen ist.

Finalisierung

Ein Zwischenstadium beim Produktions-Failover oder Wiederherstellungsprozess des Cloud Servers. Dieser Prozess beinhaltet die Übertragung der virtuellen Laufwerke des Servers aus dem Backup Storage („Cold Storage“) zum Disaster Recovery Storage („Hot Storage“). Der Server bleibt während der Finalisierung verfügbar und betriebsbereit. Die Performance ist gegenüber dem Normalzustand jedoch herabgesetzt.

G

Geschützter Server

Eine physische oder virtuelle Maschine, die einem bestimmten Kunden gehört und durch den Service geschützt wird.

L

Lokaler Standort

Die lokale Infrastruktur, die „on-premise“ (auf den lokalen Systemen/am lokalen Standort) Ihres Unternehmens bereitgestellt wird.

O

Öffentliche IP-Adresse

Eine IP-Adresse, die erforderlich ist, um Cloud Server aus dem Internet verfügbar zu machen.

P

Point-to-Site-Verbindung (P2S)

Eine sichere VPN-Verbindung von außen zur Cloud-Site und Ihrem lokalen Standort über Ihre Endgeräte (z.B. einen Desktop-Computer oder Laptop).

Primärer Server

Eine virtuelle Maschine, die keine verknüpfte Maschine am lokalen Standort hat (wie etwa einen Recovery-Server). Primäre Server werden zum Schutz einer Applikation oder zur Ausführung verschiedener Hilfsdienste (z.B. als Webserver) verwendet.

Produktionsnetzwerk

Das per VPN-Tunneling erweiterte interne Netzwerk, das sowohl den lokale Standort als auch die Cloud-Site umfasst. Lokale Server und Cloud Server können im Produktionsnetzwerk miteinander kommunizieren.

R

Recovery-Server

Das VM-Replikat einer ursprünglichen Maschine, das auf den (in der Cloud gespeicherten) Backups eines geschützten Servers basiert. Recovery-Server werden verwendet, um bei einem Desaster die Workloads der ursprünglichen Server in die Cloud umschalten zu können.

RPO (Recovery Point Objective)

Auf Deutsch etwas „Wiederherstellungspunktvorgabe“. Bestimmt, welche Datenmenge bei einem Ausfall höchstens verloren gehen darf. Wird an der Zeitspanne bemessen, die nach einem geplanten Ausfall oder einem zufälligen Desasterereignis höchstens verstreichen darf. Der RPO-Grenzwert definiert also das maximale Zeitintervall, das zwischen dem letzten (für ein Failover verwendbaren) Recovery-Punkt und dem aktuellen Zeitpunkt (an dem es zu einem Desaster kommen kann) zulässig ist.

Runbook

Ein geplantes Szenario, das aus konfigurierbaren Schritten besteht, um Disaster Recovery-Aktionen zu automatisieren.

S

Site-to-Site-Verbindung (S2)

Eine Verbindung zur Erweiterung des lokalen Netzwerks über einen sicheren VPN-Tunnel in die Cloud.

T

Test-IP-Adresse

Eine IP-Adresse, die bei einem Test-Failover benötigt wird, um die Duplizierung der Produktions-IP-Adresse zu vermeiden.

Testnetzwerk

Isoliertes virtuelles Netzwerk, das zum Testen des Failover-Prozesses verwendet wird.

V

VPN-Appliance

Eine spezielle virtuelle Maschine, die eine Verbindung (über einen sicheren VPN-Tunnel) zwischen dem lokalen Netzwerk und der Cloud-Site ermöglicht. Die VPN-Appliance wird am lokalen Standort bereitgestellt.

VPN-Gateway (früher auch VPN-Server oder Verbindungsgateway genannt)

Eine spezielle virtuelle Maschine, die eine Verbindung (über einen sicheren VPN-Tunnel) zwischen dem lokalen Standort und den Cloud-Site-Netzwerken bereitstellt. Das VPN-Gateway wird in der Cloud-Site bereitgestellt.

Index