Cyber Disaster Recovery Cloud

24.03

Manuale dell'amministratore

REVISIONE:11/04/2024

Sommario

Informazioni su Cyber Disaster Recovery Cloud

Cyber Disaster Recovery Cloud (DR) è un componente di Cyber Protection che fornisce servizi DRaaS (Disaster Recovery as-a-Service). Cyber Disaster Recovery Cloud rappresenta una soluzione rapida e stabile per avviare copie esatte dei sistemi nel sito cloud e per trasferire i carichi di lavoro dai sistemi originali danneggiati ai server di ripristino nel cloud in caso di errore umano o calamità naturale.

È possibile impostare e configurare il disaster recovery secondo le modalità seguenti:

- Creare un piano di protezione che include il modulo di disaster recovery e applicarlo ai dispositivi. Ciò configurerà automaticamente l'infrastruttura di disaster recovery. Vedere Creare un piano di protezione di disaster recovery.
- Configurare manualmente l'infrastruttura cloud di disaster recovery e controllare ogni fase. Vedere "Configurazione dei server di ripristino" (pag. 56).

Funzionalità principali

Nota
Alcune funzionalità possono richiedere licenze aggiuntive, a seconda del modello di licensing applicato.

- Gestisci il servizio Cyber Disaster Recovery Cloud da un'unica console
- Estende al cloud un massimo di 23 reti locali, utilizzando un tunnel VPN sicuro
- Stabilisci la connessione al sito cloud senza distribuire alcuna appliance VPN[1] (modalità solo cloud)
- Stabilisci la connessione da punto a sito ai siti cloud e locale
- Proteggi le macchine utilizzando i server di ripristino nel cloud
- Proteggi applicazioni e appliance utilizzando i server primari nel cloud
- Esegui attività di disaster recovery automatiche per i backup crittografati
- Esegui failover di prova nella rete isolata
- Utilizza i runbook per allestire l'ambiente di produzione nel cloud

[1] Una macchina virtuale speciale che abilita la connessione tra la rete locale e il sito nel cloud tramite un tunnel VPN sicuro. L'appliance VPN viene distribuita nel sito locale.

Requisiti software

Sistemi operativi supportati

La protezione tramite server di ripristino è stata testata con i sistemi operativi seguenti:

- 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 - tutte le opzioni di installazione, ad eccezione di Nano Server
- Windows Server 2019 - tutte le opzioni di installazione, ad eccezione di Nano Server
- Windows Server 2022 - tutte le opzioni di installazione, ad eccezione di Nano Server

Il software può funzionare con altri sistemi operativi Windows e distribuzioni Linux, ma ciò non è garantito.

Nota
La protezione tramite server di ripristino è stata testata per le VM Microsoft Azure che eseguono i sistemi operativi seguenti:

- Windows Server 2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016 - tutte le opzioni di installazione, ad eccezione di Nano Server
- Windows Server 2019 - tutte le opzioni di installazione, ad eccezione di Nano Server
- Windows Server 2022 - tutte le opzioni di installazione, ad eccezione di Nano Server
- Ubuntu Server 20.04 LTS - Gen2 (Canonical) Per ulteriori informazioni su come accedere alla console del server di ripristino, consultare https://kb.acronis.com/content/71616.

Piattaforme di virtualizzazione supportate

La protezione delle macchine virtuali con un server di ripristino è stata testata con le piattaforme di virtualizzazione seguenti:

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

- Windows Server 2016 con Hyper-V - tutte le opzioni di installazione, ad eccezione di Nano Server
- Windows Server 2019 con Hyper-V – tutte le opzioni di installazione, ad eccezione di Nano Server
- Windows Server 2022 con Hyper-V – tutte le opzioni di installazione, ad eccezione di Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016
- Virtual machine basate su Kernel (KVM) – solo guest (HVM) completamente virtualizzati. Non sono supportati i guest paravirtualizzati (PV).
- Red Hat Enterprise Virtualization (RHEV) 3.6
- Red Hat Virtualization (RHV) 4.0
- Citrix XenServer: 6.5, 7.0, 7.1, 7.2

L'appliance VPN è stata testata con le piattaforme di virtualizzazione seguenti:

- VMware ESXi 5.1, 5.5, 6.0, 6.5, 6.7
- Windows Server 2008 R2 con Hyper-V
- Windows Server 2012/2012 R2 con Hyper-V
- Windows Server 2016 con Hyper-V - tutte le opzioni di installazione, ad eccezione di Nano Server
- Windows Server 2019 con Hyper-V – tutte le opzioni di installazione, ad eccezione di Nano Server
- Windows Server 2022 con Hyper-V – tutte le opzioni di installazione, ad eccezione di Nano Server
- Microsoft Hyper-V Server 2012/2012 R2
- Microsoft Hyper-V Server 2016

Il software può funzionare con altre versioni e piattaforme di virtualizzazione, ma ciò non è garantito.

Limitazioni

Cyber Disaster Recovery Cloud non supporta le seguenti piattaforme e configurazioni:

1. Piattaforme non supportate:
   - Agenti per Virtuozzo
   - macOS
   - I sistemi operativi desktop di Windows non sono supportati a causa dei termini del prodotto di Microsoft.
   - Azure Edition per Windows Server
     Azure Edition è una versione speciale di Windows Server progettata specificamente per funzionare sia come virtual machine (VM) IaaS di Azure in Azure, sia come VM su un cluster Azure Stack HCI. A differenza delle edizioni Standard e Datacenter, Azure Edition non dispone della licenza per funzionare su hardware bare metal, Hyper-V client di Windows, Hyper-V server di Windows, hypervisor di terze parti o su cloud di terze parti.

2. Configurazioni non supportate:

   Microsoft Windows

   - I dischi dinamici non sono supportati
   - I sistemi operativi desktop di Windows non sono supportati a causa dei termini del prodotto di Microsoft.
   - Il servizio Active Directory con replica FRS non è supportato
   - I supporti rimovibili senza formattazione GPT o (i cosiddetti "superfloppy") non sono supportati

   Linux

   - File system senza una tabella di partizione
   - I workload Linux il cui backup è stato eseguito con un agente da un SO guest e che hanno volumi con le seguenti configurazioni avanzate di Logical Volume Manager (LVM): volumi con striping, volumi con mirroring, volumi RAID 0, RAID 4, RAID 5, RAID 6 o RAID 10.

   Nota
   I workload con più sistemi operativi installati non sono supportati.

3. Tipi di backup non supportati:
   - I punti di ripristino con protezione continua dei dati (CDP) non sono compatibili.

     Importante
     Se si crea un server di ripristino da un backup dotato di un punto di ripristino CDP, durante il failback o la creazione di un server di ripristino, i dati contenuti nel punto di ripristino CDP andranno perduti.

   - Non è possibile utilizzare backup contenenti dati forensi per la creazione di server di ripristino.

Un server di ripristino è dotato di una sola interfaccia di rete. Se il sistema originale presenta più interfacce di rete, solo una verrà emulata.

I server cloud non sono crittografati.

Versione in trial di Cyber Disaster Recovery Cloud

È possibile utilizzare una versione in trial di Acronis Cyber Disaster Recovery Cloud per un periodo di 30 giorni. In questa versione, Disaster Recovery presenta le seguenti limitazioni per i tenant partner:

- I server di ripristino e primari non possono accedere a una rete Internet pubblica. Non è possibile assegnare indirizzi IP pubblici ai server.
- La VPN IPsec multisito non è disponibile.

Limitazioni durante l'utilizzo di Geo-redundant Cloud Storage

Geo-redundant Cloud Storage fornisce una posizione secondaria per i dati di backup. La posizione secondaria si trova in una regione geograficamente distinta dalla posizione primaria dello storage. La separazione geografica tra le regioni garantisce che, in caso di un'emergenza che colpisca una delle regioni e renda irrecuperabili i dati dei backup, l'altra regione non subisca conseguenze, evitando così interruzioni operative.

Importante
Il servizio Disaster Recovery non è supportato se la posizione dello storage di backup viene trasferita dalla posizione primaria alla posizione secondaria con geo-ridondanza.

Compatibilità di Disaster Recovery con il software di crittografia

Disaster Recovery è compatibile con i seguenti software di crittografia a livello del disco:

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

Nota

- Per i workload con crittografia a livello del disco, si consiglia di installare l'agente di protezione nel sistema operativo guest del workload e di eseguire backup con agente.
- I backup agentless di workload crittografati non supportano le attività di failover e failback.

Per ulteriori informazioni sulla compatibilità con i software di crittografia, consultare il manuale dell'utente del servizio Cyber Protection.

Punti di calcolo

In Disaster Recovery, i punti di calcolo vengono utilizzati per i server primari e per i server di ripristino, durante il failover di prova e il failover di produzione. I punti di calcolo riflettono le risorse di elaborazione utilizzate per l'esecuzione dei server (virtual machine) nel cloud.

Il consumo di punti di calcolo durante il disaster recovery dipende dai parametri del server e dalla durata dell'intervallo di tempo in cui il server è nella condizione di failover. Più è potente il server e più è lungo l'intervallo di tempo, maggiore sarà il volume di punti di calcolo consumati. A un volume più elevato di punti di calcolo consumati corrisponde un prezzo più alto.

L'addebito per tutti i server in esecuzione in Acronis Cloud viene conteggiato in base ai punti di calcolo consumati e alla preferenza configurata e indipendentemente dallo stato in cui si trovano (acceso o spento).

I server di ripristino nello stato Standby non consumano punti di calcolo e il relativo addebito non avviene in base ai punti di calcolo.

Nella tabella sottostante è visualizzato un esempio che mostra otto server nel cloud con diverse preferenze e i corrispondenti punti di calcolo consumati all'ora. È possibile modificare le versioni dei server nella scheda **Dettagli**.

Tipo	CPU	RAM	Punti di calcolo
F1	1 vCPU	2 GB	1
F2	1 vCPU	4 GB	2
F3	2 vCPU	8 GB	4
F4	4 vCPU	16 GB	8
F5	8 vCPU	32 GB	16
F6	16 vCPU	64 GB	32
F7	16 vCPU	128 GB	64
F8	16 vCPU	256 GB	128

Utilizzando le informazioni nella tabella, sarà facile stimare quanti punti di calcolo verranno consumati da un server (virtual machine).

Ad esempio, proteggendo con il modulo Disaster Recovery una virtual machine con 4 vCPU* con 16 GB di RAM e una virtual machine con 2 vCPU con 8 GB di RAM, la prima virtual machine consumerà 8 punti di calcolo l'ora e la seconda virtual machine 4 punti di calcolo l'ora. Se entrambe le virtual machine sono in failover, il consumo totale sarà di 12 punti di calcolo l'ora, ovvero 288 punti di calcolo per l'intera giornata (12 punti di calcolo x 24 ore = 288 punti di calcolo).

*vCPU indica un'unità di elaborazione fisica centrale (CPU) assegnata a una virtual machine; si tratta di un'entità dipendente dal tempo.

Nota

Se viene raggiunto il surplus della quota relativa ai **Punti di calcolo**, tutti i server primari e di ripristino vengono spenti. Non sarà possibile utilizzare questi server fino all'inizio del periodo di fatturazione successivo, o fino a quando non viene incrementata la quota. Per impostazione predefinita, il periodo di fatturazione corrisponde a un mese di calendario.

Creare un piano di protezione di disaster recovery

Creare un piano di protezione che include il modulo Disaster Recovery e applicarlo ai dispositivi.

Per impostazione predefinita, durante la creazione di un nuovo piano di protezione il modulo Disaster Recovery è disabilitato. Dopo aver abilitato la funzionalità di disaster recovery e applicato il piano ai dispositivi, viene creata l'infrastruttura della rete cloud, che include un *server di ripristino* per ogni dispositivo protetto. Il *server di ripristino* è una virtual machine nel cloud che è una copia del dispositivo selezionato. Per ognuno dei dispositivi selezionati, verrà creato un server di ripristino con impostazioni predefinite nello stato Standby (virtual machine non in esecuzione). La dimensione del server di ripristino è automatica e dipende dalla CPU e dalla RAM del dispositivo protetto. Viene creata in modalità automatica anche l'infrastruttura di rete cloud: Reti e gateway VPN nel sito cloud, ai quali verranno connessi i server di ripristino.

Se si revoca, elimina o disabilita il modulo Disaster Recovery di un piano di protezione, i server di ripristino e le reti cloud non vengono automaticamente eliminate. È possibile rimuovere l'infrastruttura di disaster recovery manualmente, se necessario.

Nota

- Dopo aver configurato il disaster recovery, sarà possibile eseguire il failover di prova o di produzione da qualsiasi punto di ripristino generato dopo la creazione del server di ripristino per il dispositivo. I punti di ripristino generati prima che i dispositivi vengano protetti con la funzionalità di disaster recovery (ad esempio prima della creazione del server di ripristino) non possono essere utilizzati per il failover.
- Non è possibile abilitare un piano di protezione di disaster recovery se non è possibile individuare l'indirizzo IP di un dispositivo, come nel caso in cui viene eseguito il backup agentless delle virtual machine e a queste non viene assegnato un indirizzo IP.
- Quando si applica un piano di protezione, nel sito cloud vengono assegnati le stesse reti e gli stessi indirizzi IP. Per la connessione VPN IPsec è necessario che i segmenti di rete del cloud e dei siti locali non si sovrappongano. Se si configura una connessione VPN IPsec multisito, e se il piano di protezione viene applicato a uno o più dispositivi in un secondo momento, sarà anche necessario aggiornare le reti cloud e riassegnare gli indirizzi IP dei server cloud. Per ulteriori informazioni, consultare "Riassegnazione di indirizzi IP" (pag. 45).

Per creare un piano di protezione di disaster recovery

1. Nella console di Cyber Protect, passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare i sistemi da proteggere.
3. Fare clic su **Proteggi**, quindi su **Crea piano**.
   Viene visualizzato il piano di protezione con le impostazioni predefinite.
4. Configurare le opzioni di backup.

Per utilizzare la funzionalità di disaster recovery, il piano deve eseguire il backup dell'intero sistema, o solo dei dischi necessari per l'avvio e per fornire i servizi necessari, in un archivio nel cloud.

5. Abilitare il modulo di Disaster recovery facendo clic sull'interruttore accanto al nome del modulo.
6. Fare clic su **Crea**.
   Il piano viene creato e applicato ai sistemi selezionati.

Passaggi successivi

- È possibile modificare la configurazione predefinita del server di ripristino. Per ulteriori informazioni, consultare "Configurazione dei server di ripristino" (pag. 56).
- È possibile modificare la configurazione di rete predefinita. Per ulteriori informazioni, consultare "Configurazione della connessione" (pag. 18).
- È possibile visualizzare più informazioni sui parametri predefiniti del server di ripristino e sull'infrastruttura di rete cloud. Per ulteriori informazioni, consultare "Modifica dei parametri predefiniti del server di ripristino" (pag. 15) e "Infrastruttura di rete cloud" (pag. 16).

Modifica dei parametri predefiniti del server di ripristino

Quando si crea e applica un piano di protezione di disaster recovery, viene creato un server di ripristino con parametri predefiniti. I parametri predefiniti possono essere modificati in un secondo momento.

Nota
Tale server viene creato solo se non esiste. Eventuali server di ripristino esistenti non vengono né modificati né ricreati.

Per modificare i parametri predefiniti del server di ripristino

1. Passare a **Dispositivi** > **Tutti i dispositivi**.
2. Selezionare un dispositivo e fare clic su **Disaster Recovery**.
3. Modificare i parametri predefiniti del server di ripristino.
   I parametri del server di ripristino sono descritti nella tabella seguente.

Server di ripristino **parametro**	**Impostazione predefinita** **valore**	**Descrizione**
CPU e RAM	auto	Il numero di CPU virtuali e la dimensione della RAM del server di ripristino. Le impostazioni predefinite verranno determinate automaticamente alla configurazione di CPU e RAM del dispositivo originale.

Rete cloud	auto	Specificare la rete cloud alla quale viene connesso il server. Per informazioni su come sono configurate le reti cloud, vedere Infrastruttura di rete cloud.
Indirizzo IP in rete di produzione	auto	L'indirizzo IP che avrà il server nella rete di produzione. Per impostazione predefinita, viene configurato l'indirizzo IP del sistema originale.
Indirizzo IP di prova	disattivato	Il test dell'indirizzo IP consente di eseguire il failover di prova nella rete di prova isolata e di connettersi al server di ripristino tramite RDP o SSH durante un failover di prova. Nella modalità failover di prova, il gateway VPN sostituisce l'indirizzo IP di prova con l'indirizzo IP di produzione utilizzando il protocollo NAT. Se non è specificato un indirizzo IP di prova, per accedere al server durante un failover di prova sarà possibile utilizzare esclusivamente la console.
Accesso Internet	Abilitato	Il server di ripristino potrà accedere a Internet durante un failover reale o di prova. Per impostazione predefinita, la porta TCP 25 non è autorizzata alle connessioni in uscita.
Utilizza indirizzo pubblico	disattivato	Se dispone di un indirizzo IP pubblico, il server di ripristino è disponibile anche da Internet durante un failover reale o di prova. Se non viene utilizzato un indirizzo IP pubblico, il server sarà disponibile solo nella rete di produzione. Per utilizzare un indirizzo IP pubblico, è necessario abilitare l'accesso a Internet. L'indirizzo IP pubblico verrà visualizzato dopo aver completato la configurazione. Per impostazione predefinita, la porta TCP 443 è aperta per le connessioni in entrata.
Imposta soglia RPO	disattivato	La soglia RPO definisce l'intervallo di tempo massimo consentito tra l'ultimo punto di ripristino e l'ora corrente. È possibile impostare il valore tra 15–60 minuti, 1–24 ore, 1–14 giorni.

Infrastruttura di rete cloud

L'infrastruttura di rete cloud è costituita dal gateway VPN nel sito cloud e dalle reti cloud alle quali verranno connessi i server di ripristino.

Nota
L'applicazione di un piano di protezione di disaster recovery creare un'infrastruttura di rete cloud di ripristino solo se non esiste. Le reti cloud esistenti non possono essere modificate o ricreate.

Il sistema controlla gli indirizzi IP dei dispositivi e se non sono presenti reti cloud adatte a un indirizzo IP, crea automaticamente reti cloud idonee. Se sono già disponibili reti cloud per le quali gli indirizzi IP dei server di ripristino sono adatti, le reti cloud esistenti non verranno modificate o ricreate.

- Se non sono presenti reti cloud o se la configurazione di disaster recovery viene impostata per la prima volta, le reti cloud verranno create con gli intervalli massimi raccomandati da IANA per l'uso privato (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) in base all'intervallo di indirizzi IP dei dispositivi in uso. È possibile limitare la rete modificando la maschera di rete.
- Se sono presenti dispositivi su più reti locali, la rete nel sito cloud può diventare un superinsieme di reti locali. È possibile riconfigurare le reti nella sezione **Connessione**. Vedere "Gestione delle reti" (pag. 39).
- Se è necessario configurare la connessione Open VPN da sito a sito, scaricare e configurare l'appliance VPN. Vedere "Configurazione di una Open VPN da sito a sito" (pag. 29).Verificare che gli intervalli delle reti cloud corrispondano agli intervalli della rete locale connessa all'appliance VPN.
- Per modificare la configurazione di rete predefinita fare clic sul collegamento **Vai a Connessione** nel modulo Disaster Recovery del piano di protezione oppure passare a **Disaster Recovery** > **Connessione**.

Configurazione della connessione

In questa sezione vengono illustrati alcuni concetti sulla rete, necessari per comprendere il funzionamento di Cyber Disaster Recovery Cloud. Viene spiegato come configurare diversi tipi di connessione al sito cloud, in base alle diverse esigenze. Infine, viene illustrato come gestire le reti nel cloud, le impostazioni dell'appliance VPN, e il gateway VPN.

Concetti sulla rete

Nota
Alcune funzionalità possono richiedere licenze aggiuntive, a seconda del modello di licensing applicato.

Cyber Disaster Recovery Cloud consente di definire i seguenti tipi di connessione al sito cloud:

- **Modalità solo cloud**

  Questo tipo di connessione non richiede la distribuzione di un'appliance VPN nel sito locale.

  Le reti locali e cloud operano come reti indipendenti. Questo tipo di connessione implica il failover di tutti i server protetti del sito locale o il failover parziale dei server indipendenti che non hanno necessità di comunicare con il sito locale.

  È possibile accedere ai server cloud nel sito cloud tramite VPN da punto a sito e indirizzi IP pubblici, se assegnati.
- **Connessione Open VPN da sito a sito**

  Questo tipo di connessione richiede la distribuzione di un'appliance VPN nel sito locale.

  Una connessione Open VPN da sito a sito consente di estendere le reti al sito cloud, mantenendo gli indirizzi IP.

  Il sito locale viene connesso al cloud tramite un tunnel VPN sicuro. Si tratta di una connessione adatta in presenza di server altamente dipendenti nel sito locale, come un server web e un server per database. In caso di failover parziale, nel momento in cui uno di questi server viene ricreato nel sito site mentre l'altro resta nel sito locale, i server potranno comunque comunicare uno con l'altro tramite il tunnel VPN.

  È possibile accedere ai server cloud nel sito cloud tramite rete locale, VPN da punto a sito e indirizzi IP pubblici, se assegnati.
- **Connessione VPN IPsec multisito**

  Questo tipo di connessione richiede un dispositivo VPN locale che supporti IPsec IKE v2.

  Quando si avvia la configurazione della connessione VPN IPsec multisito, Cyber Disaster Recovery Cloud crea automaticamente un gateway VPN cloud con un indirizzo IP pubblico.

  Con la connessione VPN IPsec multisito, i siti locali vengono connessi al sito cloud tramite un tunnel VPN IPsec sicuro.

  Questo tipo di connessione è adatta agli scenari di Disaster Recovery in cui sono presenti uno o più siti locali che ospitano workload critici o servizi fortemente dipendenti.

In caso di failover parziale di uno dei server, questo server viene ricreato nel sito cloud mentre gli altri restano nel sito locale; i server potranno comunque comunicare uno con l'altro tramite il tunnel VPN IPsec.

In caso di failover parziale di uno dei server, questo server viene ricreato nel sito cloud mentre gli altri restano nel sito locale; i server potranno comunque comunicare uno con l'altro tramite il tunnel VPN IPsec.

- **Accesso VPN remoto da punto a sito**

  Un accesso VPN remoto sicuro da punto a sito al cloud e ai workload del sito locale dall'esterno, utilizzando il dispositivo endpoint.

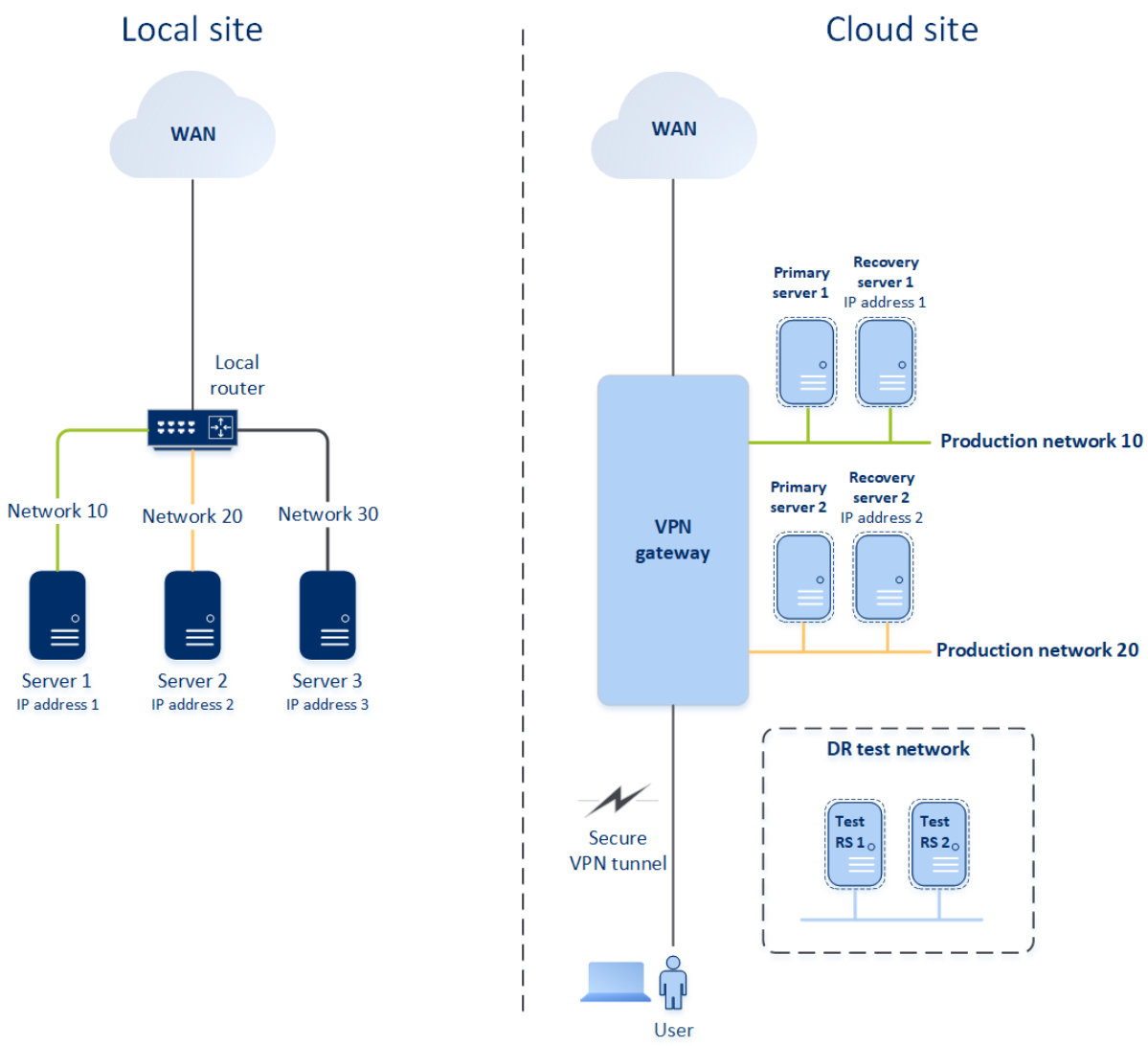
  Per l'accesso al sito locale, questo tipo di connessione richiede la distribuzione di un'appliance VPN nel sito locale.

Modalità solo cloud

La connessione in modalità solo cloud non richiede la distribuzione di un'appliance VPN nel sito locale. Ciò significa che si avranno due reti indipendenti: una nel sito locale e un'altra nel sito cloud. Il routing viene eseguito con il router nel sito cloud.

Come funziona il routing

Nel caso in cui venga stabilita la modalità di connessione solo in cloud, il routing viene eseguito tramite il router sul sito in cloud, in modo che i server di diverse reti cloud possano comunicare fra loro.



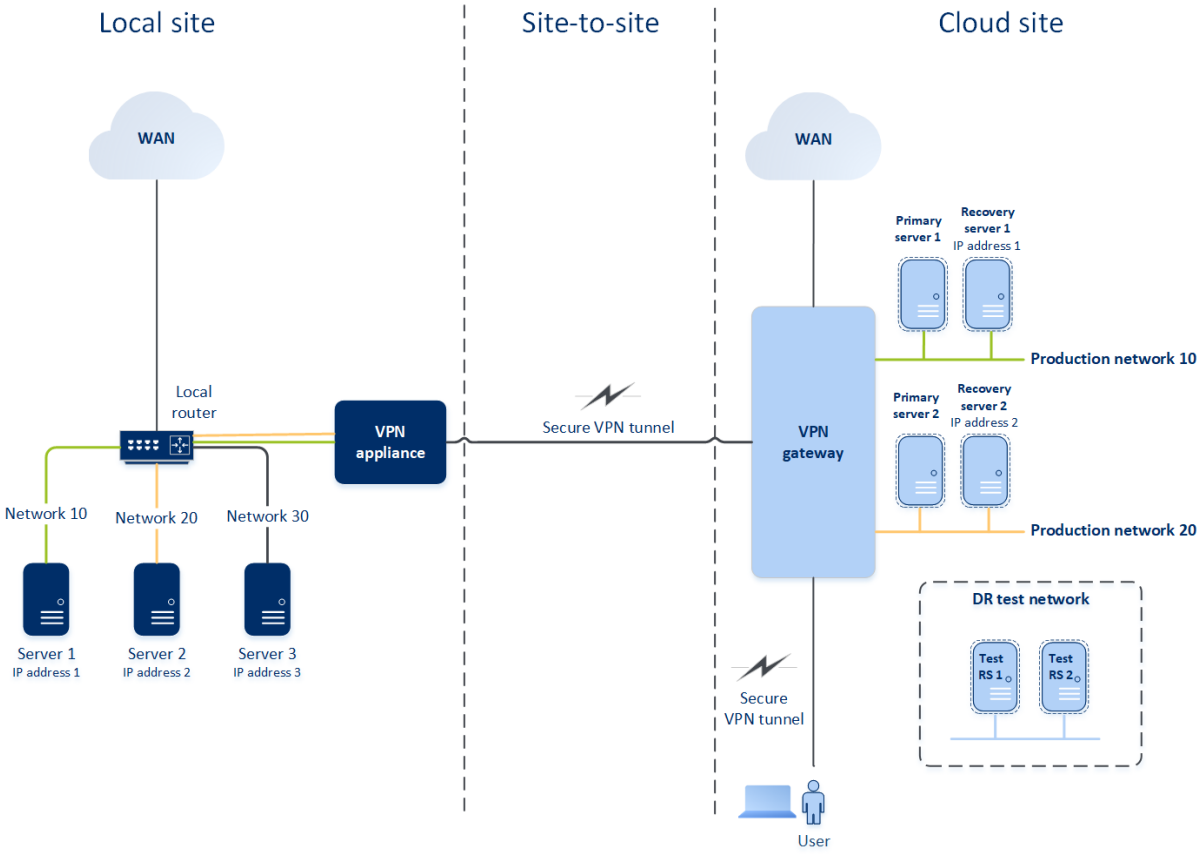
Connessione Open VPN da sito a sito

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Per comprendere il funzionamento della rete in Cyber Disaster Recovery Cloud, verrà considerata una situazione in cui sono presenti tre reti, ognuna con un sistema nel sito locale. Nell'esempio verrà configurata la protezione per le due reti, che denomineremo Rete 10 e Rete 20.

Il diagramma sottostante mostra il sito locale che ospita i sistemi e il sito cloud in cui vengono avviati i server cloud in caso di emergenza.

La soluzione Cyber Disaster Recovery Cloud consente di eseguire il failover di tutti i workload dei sistemi danneggiati nel sito locale sui server cloud nel cloud. È possibile proteggere un massimo di 23 reti con Cyber Disaster Recovery Cloud.



Per stabilire una comunicazione Open VPN da sito a sito tra i siti locali e cloud vengono utilizzati un'**appliance VPN** e un **gateway VPN**. Quando si avvia la configurazione della connessione Open VPN site-to-site nella console di Cyber Protect, il gateway VPN viene distribuito automaticamente nel sito cloud. Successivamente, è necessario distribuire l'appliance VPN nel sito locale, aggiungere le reti da proteggere e registrare l'appliance nel cloud. Cyber Disaster Recovery Cloud crea una replica della rete locale nel cloud. Tra l'appliance VPN e il gateway VPN viene stabilito un tunnel VPN sicuro. che rappresenta l'estensione della rete locale nel cloud. Viene eseguito il bridging tra le reti di produzione nel cloud e le reti locali. I server locali e nel cloud possono comunicare tramite questo tunnel VPN come se fossero tutti nello stesso segmento Ethernet. Viene avviato il routing con il router locale.

È necessario creare un server di ripristino nel sito cloud per ogni macchina di origine da proteggere. Tale server rimane in modalità **Standby** fino a quando non si verifica un evento di failover. In caso di emergenza, se si avvia il processo di failover in **modalità di produzione**, il server di ripristino che rappresenta la copia esatta del sistema protetto viene avviato nel cloud. A tale server può essere assegnato lo stesso indirizzo IP del sistema di origine e potrà essere avviato nello stesso segmento Ethernet. Il server potrà essere utilizzato come sempre, senza che gli utenti notino alcun cambiamento.

È inoltre possibile avviare un processo di failover in **modalità di prova**. In questa modalità, la macchina di origine resta in funzione e al contempo rispettivo il server di ripristino, con lo stesso indirizzo IP, viene avviato nel cloud. Per evitare conflitti tra indirizzi IP, nel cloud viene creata una rete virtuale speciale, definita **rete di prova**. Tale rete è isolata per evitare la duplicazione

dell'indirizzo IP della macchina di origine in un segmento Ethernet. Per accedere al server di ripristino in modalità failover di prova, è necessario assegnare l'**Indirizzo IP di prova** al server di ripristino al momento della sua creazione. Gli altri parametri del server di ripristino che è possibile specificare vengono illustrati nelle rispettive sezioni, più avanti.

Come funziona il routing

Nel caso in cui venga stabilita una connessione da sito a sito, il routing tra le reti cloud viene eseguito con il router locale. Il server VPN non esegue il routing tra i server cloud posizionati in reti cloud diverse. Se il server cloud di una rete deve comunicare con un server di un'altra rete cloud, il traffico passa nel tunnel VPN verso il router locale presso il sito locale. A quel punto, il router locale effettua il routing verso un'altra rete e torna attraverso il tunnel al server di destinazione sul sito in cloud.

Gateway VPN

Il principale componente che consente la comunicazione tra i siti locali e cloud è il **gateway di VPN**. Si tratta di una virtual machine nel cloud, nella quale è installato un software speciale, con una configurazione di rete specifica. Il gateway VPN offre le seguenti funzioni:

- Connette il segmento Ethernet della rete locale e della rete di produzione al cloud, in modalità L2.
- Fornisce le regole iptables e ebtables.
- Funge da router predefinito e da NAT per i sistemi nelle reti di prova e di produzione.
- Funge da server DHCP. Tutti i sistemi nelle reti di produzione e prova ottengono la configurazione di rete (indirizzi IP, impostazioni DNS) tramite DHCP. Un dato server cloud ottiene sempre lo stesso indirizzo IP dal server DHCP. Nel caso in cui sia necessario configurare impostazioni DNS personalizzate, contattare il supporto tecnico.
- Funge da DNS di caching.

Configurazione di rete del gateway VPN

Il gateway VPN presenta diverse interfacce di rete:

- Interfaccia esterna, connessa a Internet
- Interfacce di produzione, connesse alle reti di produzione
- Interfaccia di prova, connessa alla rete di prova

Inoltre, si aggiungono due interfacce virtuali per le connessioni da punto a sito e da sito a sito.

Quando il gateway VPN viene distribuito e inizializzato, vengono creati i bridge: uno per l'interfaccia esterna e uno per le interfacce del client e di produzione. Sebbene il bridge client-produzione e l'interfaccia di prova utilizzino gli stessi indirizzi IP, il gateway VPN può instradare correttamente i pacchetti utilizzando uno specifico metodo.

Appliance VPN

L'**appliance VPN** è una virtual machine nel sito locale, nella quale è installato Linux e un software speciale, con una specifica configurazione di rete. Consente la comunicazione tra i siti locali e cloud.

Server di ripristino

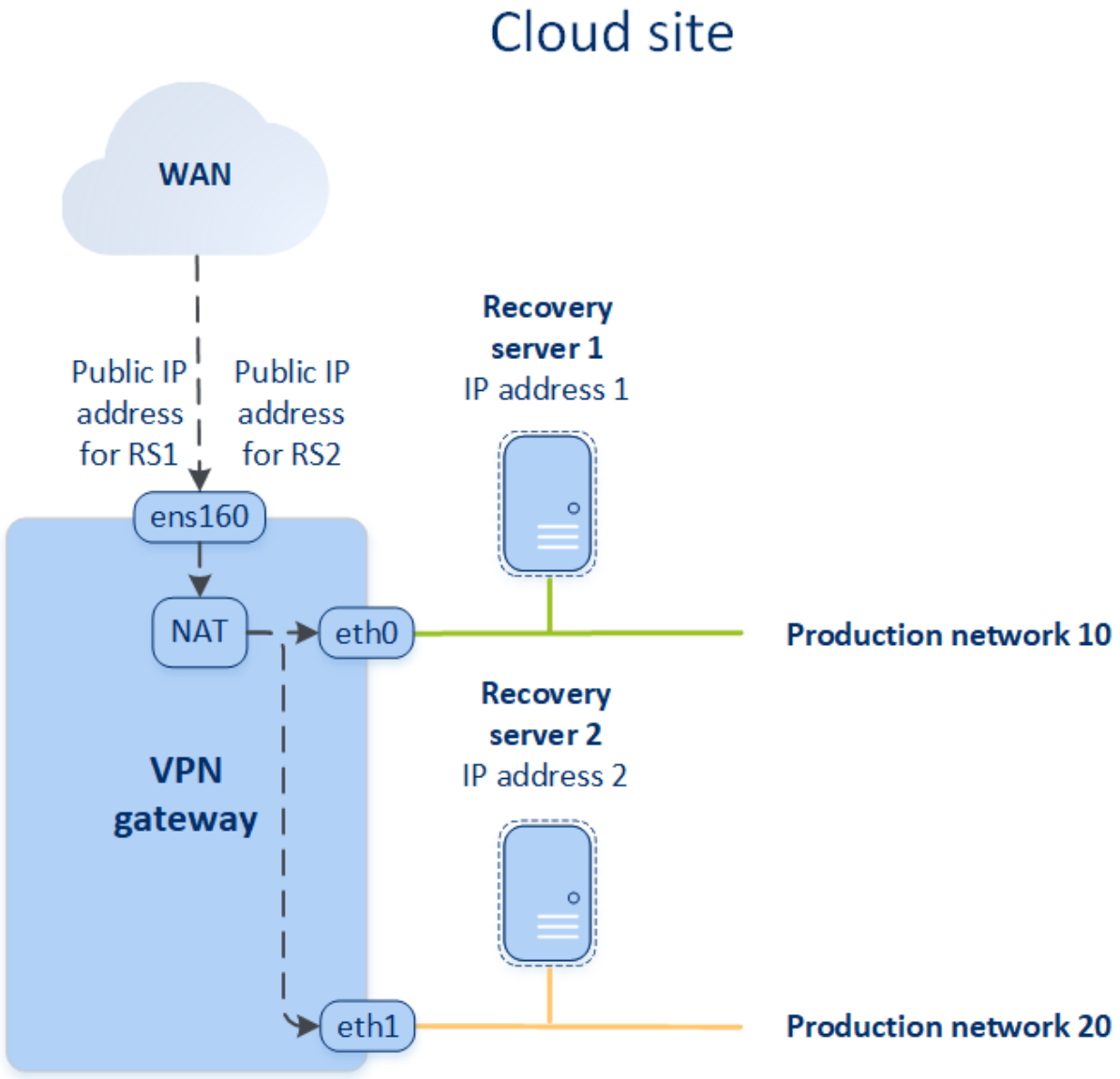
Un **server di ripristino** è una replica virtuale del sistema di origine, basato sui backup dei server protetti archiviati nel cloud. I server di ripristino sono utilizzati per trasferire i carichi di lavoro dai server originali in caso di emergenza.

Durante la creazione di un server di ripristino è necessario specificare i seguenti parametri di rete:

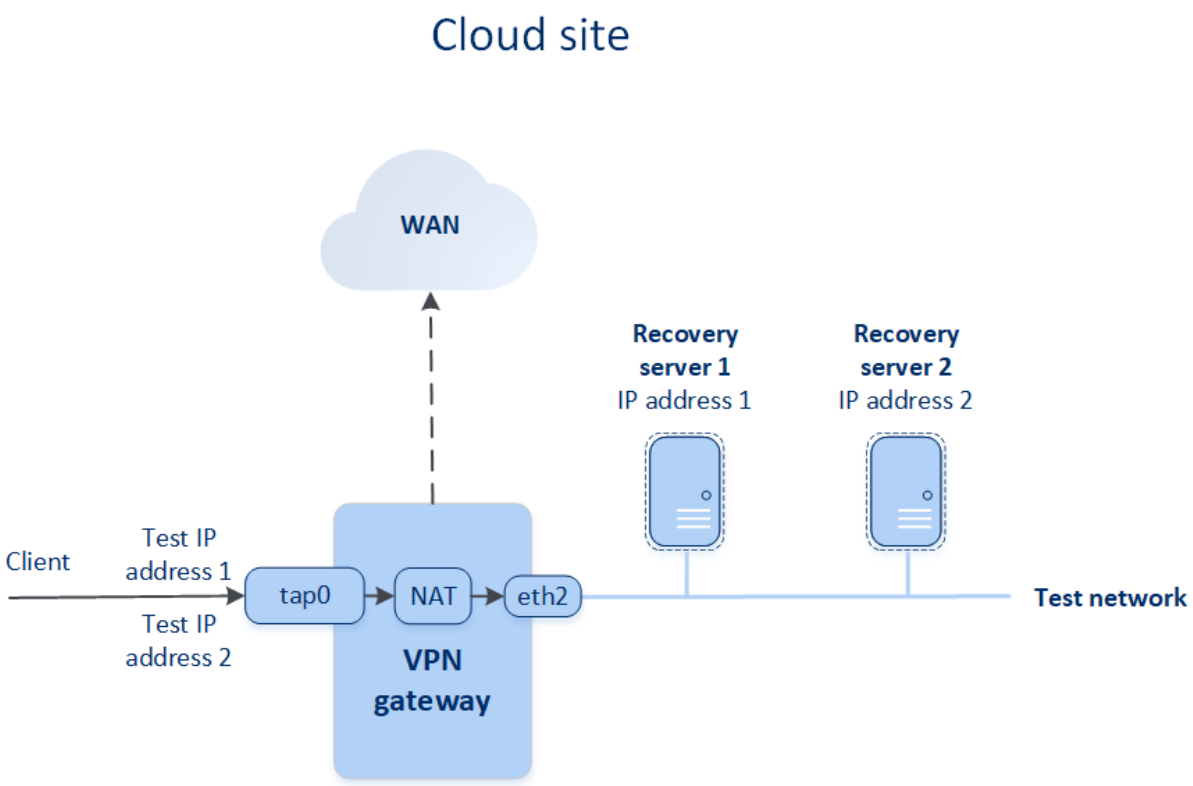
- **Rete cloud** (necessario): una rete cloud alla quale viene connesso il server di ripristino.
- **Indirizzo IP nella rete di produzione** (necessario): un indirizzo IP con il quale viene avviata la macchina virtuale per un server di ripristino. Tale indirizzo è usato sia nella rete di produzione che in quella di prova. Prima dell'avvio, la macchina virtuale viene configurata per l'acquisizione dell'indirizzo IP tramite DHCP.
- **Indirizzo IP di prova** (facoltativo): un indirizzo IP utilizzato per accedere a un server di ripristino dalla rete client-produzione durante il failover di prova, per impedire che l'indirizzo IP di produzione venga duplicato sulla stessa rete. Questo indirizzo IP è diverso da quello della rete di produzione. I server del sito locale possono raggiungere i server di ripristino durante il failover di prova tramite l'indirizzo IP di prova, mentre l'accesso nella direzione contraria non è disponibile. L'accesso a Internet dal server di ripristino della rete di prova è disponibile se l'opzione **Accesso Internet** è stata selezionata durante la creazione del server di ripristino.
- **Indirizzo IP pubblico** (facoltativo): un indirizzo IP utilizzato per accedere a un server di ripristino da Internet. Se il server non dispone di un indirizzo IP pubblico, potrà essere raggiunto solo dalla rete locale.
- **Accesso Internet** (facoltativo): consente a un server di ripristino di accedere a Internet (sia in produzione sia nel failover di prova).

Assegnazione indirizzo IP di prova

Se durante la creazione del server di ripristino viene assegnato un indirizzo IP pubblico, il server di ripristino sarà disponibile da Internet tramite tale indirizzo IP. Quando un pacchetto proveniente da Internet arriva con l'indirizzo IP pubblico di destinazione, il gateway VPN lo associa nuovamente al rispettivo indirizzo IP di produzione utilizzando NAT, quindi lo invia al server di ripristino corrispondente.



Se durante la creazione del server di ripristino viene assegnato un indirizzo IP di prova, il server di ripristino sarà disponibile nella rete di prova tramite tale indirizzo IP. Quando si esegue il failover di prova, il sistema di origine resta in funzione mentre il server di ripristino con lo stesso indirizzo IP viene avviato nella rete di prova nel cloud. Non si verifica alcun conflitto tra indirizzi IP poiché la rete di prova è isolata. I server di ripristino della rete di prova sono raggiungibili tramite i propri indirizzi IP di prova, che vengono riassociati agli indirizzi IP di produzione tramite NAT.



Per ulteriori informazioni sulle reti Open VPN da sito a sito, consultare "Open VPN site-to-site - Informazioni aggiuntive" (pag. 97).

Server primari

Un **server primario** è una virtual machine che, rispetto al server di ripristino, non dispone di un sistema connesso nel sito locale. I server primari sono utilizzati per proteggere un'applicazione tramite replica, o per eseguire diversi servizi ausiliari, ad esempio un server web.

In genere, un server primario viene utilizzato per la replica dei dati in tempo reale tra i server che eseguono le principali applicazioni. La replica viene configurata dall'utente, che a tal fine utilizza gli strumenti propri dell'applicazione. Ad esempio, è possibile configurare la replica di Active Directory o di SQL tra i server locali e il server primario.

In alternativa, è possibile includere un server primario in un gruppo di disponibilità AlwaysOn o in un gruppo di disponibilità dei database.

Entrambi questi metodi richiedono un'approfondita conoscenza dell'applicazione e i diritti di amministrazione sulla stessa. Un server primario consuma costantemente le risorse di elaborazione e lo spazio per l'archivio di ripristino di emergenza rapido. La manutenzione richiesta sul lato utente prevede il monitoraggio della replica, l'installazione degli aggiornamenti software e il backup. Tra i vantaggi, offre la riduzione degli obiettivi RPO e RTO e un carico minimo sull'ambiente di produzione, rispetto al backup dei server completi nel cloud.

I server primari sono avviati sempre ed esclusivamente nella rete di produzione e presentano i seguenti parametri di rete:

- **Rete cloud** (necessario): una rete cloud alla quale viene connesso il server primario.
- **Indirizzo IP nella rete di produzione** (necessario): un indirizzo IP assegnato al server primario nella rete di produzione. Per impostazione predefinita, viene configurato il primo indirizzo IP libero della rete di produzione.
- **Indirizzo IP pubblico** (facoltativo): un indirizzo IP utilizzato per accedere a un server primario da Internet. Se il server non dispone di un indirizzo IP pubblico, potrà essere raggiunto solo dalla rete locale e non da Internet.
- **Accesso Internet** (facoltativo): consente a un server primario di accedere a Internet.

Connessione VPN IPsec multisito

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

La connessione VPN IPsec multisito viene usata per connettere un singolo sito locale o più siti locali a Cyber Disaster Recovery Cloud tramite una connessione VPN IPsec L3.

Si tratta di un tipo di connessione utile per situazioni di Disaster Recovery in presenza di uno dei seguenti scenari d'uso:

- è presente un sito locale che ospita workload critici;
- sono presenti più siti locali che ospitano workload critici, ad esempio uffici in diverse località;
- si utilizzano siti software di terze parti o siti di provider di servizi gestiti, e la connessione a questi avviene tramite un tunnel VPN IPsec.

Per stabilire la comunicazione VPN IPsec multisito tra il sito locale e il sito cloud viene utilizzato il **gateway VPN**. Quando si avvia la configurazione della connessione VPN IPsec multisito nella console di Cyber Protect, il gateway VPN viene distribuito automaticamente nel sito cloud. Configurare i segmenti della rete cloud e verificare non si sovrappongano ai segmenti delle reti locali. Tra i siti locali e il sito cloud viene stabilito un tunnel VPN sicuro. I server locali e nel cloud possono comunicare tramite questo tunnel VPN come se fossero tutti nello stesso segmento Ethernet.

È necessario creare un server di ripristino nel sito cloud per ogni macchina di origine da proteggere. Tale server rimane in modalità **Standby** fino a quando non si verifica un evento di failover. In caso di emergenza, se si avvia il processo di failover in **modalità di produzione**, il server di ripristino che rappresenta la copia esatta del sistema protetto viene avviato nel cloud. Il server potrà essere utilizzato come sempre, senza che gli utenti notino alcun cambiamento.

È inoltre possibile avviare un processo di failover in **modalità di prova**. In questa modalità, il sistema di origine resta in funzione e al contempo il rispettivo il server di ripristino viene avviato nel cloud in una rete virtuale speciale creta nel cloud come **rete di prova**. Tale rete è isolata per evitare la duplicazione degli indirizzi IP del sistema di origine negli altri segmenti della rete cloud.

Gateway VPN

Il principale componente che consente la comunicazione tra i siti locali e il sito cloud è il **gateway VPN**. Si tratta di una macchina virtuale nel cloud, nella quale è installato un software speciale, con una configurazione di rete specifica. Il gateway VPN offre le seguenti funzioni:

- Connette i segmenti Ethernet della rete locale e della rete di produzione al cloud, in modalità IPsec L3.
- Funge da router predefinito e da NAT per i sistemi nelle reti di prova e di produzione.
- Funge da server DHCP. Tutti i sistemi nelle reti di produzione e prova ottengono la configurazione di rete (indirizzi IP, impostazioni DNS) tramite DHCP. Un dato server cloud ottiene sempre lo stesso indirizzo IP dal server DHCP.

  È inoltre possibile impostare una configurazione DNS personalizzata. Per ulteriori informazioni, consultare "Configurazione di server DNS personalizzati" (pag. 46).
- Funge da DNS di caching.

Come funziona il routing

Il routing tra le reti cloud viene eseguito con il router sul sito cloud, in modo che i server di diverse reti cloud possano comunicare fra loro.

Accesso VPN remoto da punto a sito

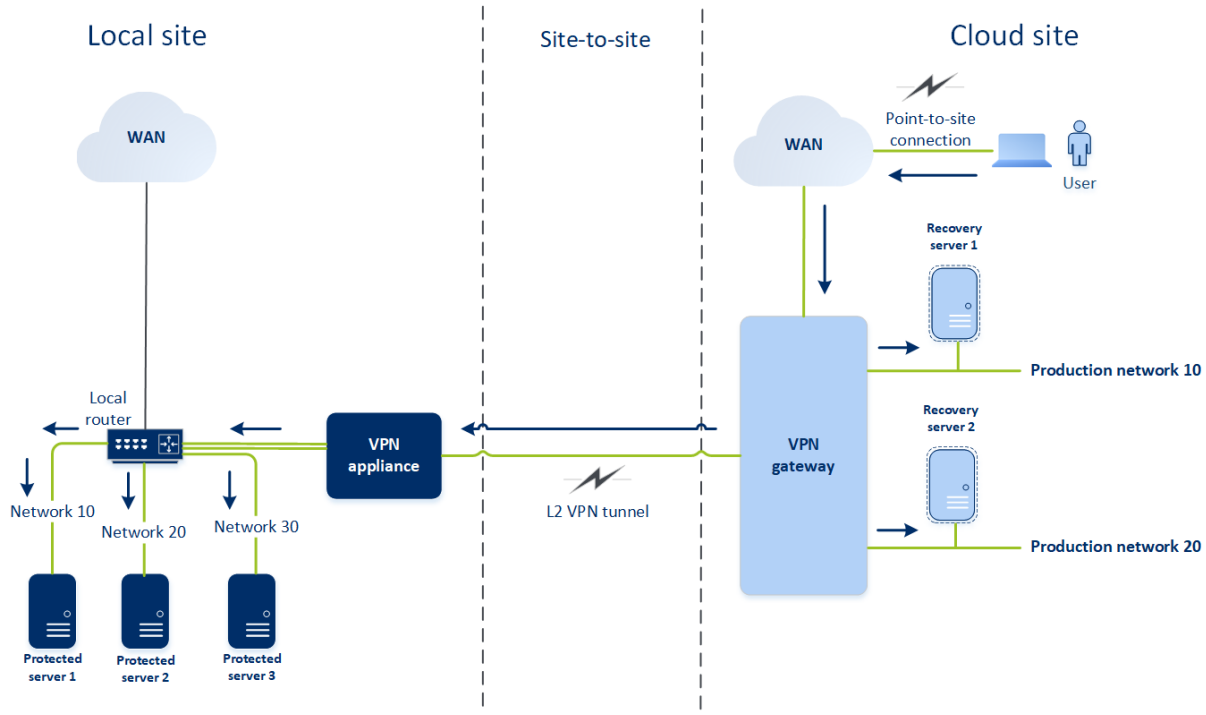
Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Una connessione da punto a sito è una connessione sicura dall'esterno che usa i dispositivi endpoint (ad esempio un computer o laptop) per collegarsi al cloud e ai siti locali tramite una VPN. Sarà disponibile dopo aver stabilito la connessione Open VPN al sito Cyber Disaster Recovery Cloud. Questo tipo di connessione è utile nei seguenti casi:

- In molte aziende, i servizi aziendali e le risorse web sono disponibili solo tramite la rete aziendale. La connessione da punto a sito consente di connettersi in sicurezza al sito locale.
- In caso di emergenza, quando un carico di lavoro viene trasferito al sito cloud e la rete locale non è attiva, potrebbe essere necessario accedere direttamente ai server cloud. Ciò è possibile tramite la connessione da punto a sito al sito cloud.

Per la connessione da punto a sito al sito locale, è necessario installare l'appliance VPN nel sito locale, configurare la connessione da sito a sito, e quindi la connessione da punto a sito al sito locale. Ciò consentirà al personale da remoto di accedere alla rete aziendale tramite la VPN L2.

Lo schema seguente mostra il sito locale, il sito cloud e le comunicazioni tra i server evidenziate in verde. Il tunnel VPN L2 connette i siti cloud e locale. Quando un utente stabilisce una connessione da punto a sito, le comunicazioni al sito locale avvengono tramite il sito cloud.



La configurazione da punto a sito utilizza i certificati per autenticare il client VPN. Per l'autenticazione sono utilizzate credenziali utente aggiuntive. Notare quanto segue relativamente alla connessione da punto a sito al sito locale:

- Gli utenti devono utilizzare le proprie credenziali Cyber Protect Cloud per autenticarsi al client VPN. Devono avere un ruolo utente di "Amministratore dell'azienda" o "Cyber Protection".
- Se la configurazione Open VPN è stata rigenerata, è necessario fornire la configurazione aggiornata a tutti gli utenti che utilizzano la connessione da punto a sito al sito cloud.

Eliminazione automatica degli ambienti del cliente non utilizzati dal sito cloud

Il servizio Disaster Recovery monitora l'utilizzo degli ambienti del cliente creati per il disaster recovery, eliminandoli automaticamente se non utilizzati.

Per stabilire se il tenant del cliente è attivo, vengono applicati i criteri indicati di seguito:

- Al momento, è presente almeno un server cloud o è stato presente uno o più server cloud negli ultimi sette giorni.

  OPPURE

- L'opzione **Accesso VPN al sito locale** è abilitata e il tunnel Open VPN da sito a sito è stabilito, oppure sono presenti dati segnalati dall'appliance VPN per gli ultimi 7 giorni.

Tutti gli altri tenant vengono considerati inattivi. Per questi tenant, il sistema esegue le attività indicate di seguito:

- Elimina il gateway VPN insieme a tutte le risorse cloud correlate al tenant.
- Annulla la registrazione dell'appliance VPN.

Esegue il rollback dei tenant inattivi, riportandoli allo stato precedente alla configurazione della connessione.

Configurazione della connessione iniziale

In questa sezione vengono descritti alcuni scenari di connessione.

Configurazione della modalità solo cloud

Per configurare una connessione in modalità solo cloud

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**.
2. Selezionare **Solo cloud** e fare clic su **Configura**.
   In questo modo, il gateway VPN e la rete cloud con l'indirizzo e la maschera definiti verranno distribuiti nel sito cloud.

Per comprendere come gestire le reti nel cloud e configurare le impostazioni del gateway VPN, fare riferimento a "Gestione di reti cloud".

Configurazione di una Open VPN da sito a sito

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Requisiti per l'appliance VPN

Requisiti di sistema

- 1 CPU
- 1 GB RAM
- 8 GB di spazio su disco

Porte

- TCP 443 (in uscita) - per la connessione VPN
- TCP 80 (in uscita) - per l'aggiornamento automatico dell'appliance

Verificare che i firewall e gli altri componenti del sistema di sicurezza della rete consentano le connessioni attraverso queste porte e qualsiasi indirizzo IP.

Configurazione di una connessione Open VPN da sito a sito

L'appliance VPN estende la rete locale al cloud tramite un tunnel VPN sicuro. Questo tipo di connessione viene spesso definita connessione S2S, ovvero da sito a sito. È possibile attenersi alla procedura seguente o guardare il tutorial video.

Per configurare una connessione tramite l'appliance VPN

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**.
2. Selezionare **Connessione Open VPN da sito a sito** quindi fare clic su **Configura**.
   Il sistema avvia la distribuzione del gateway VPN nel cloud. L'operazione richiede alcuni minuti. Nel frattempo, è possibile procedere al passaggio successivo.

   Nota
   Il gateway VPN viene fornito senza costi aggiuntivi. Verrà eliminato se la funzionalità di disaster recovery non viene utilizzata o se, ad esempio, né il server primario né quello di ripristino saranno presenti nel cloud per sette giorni.

3. Nella sezione **Appliance VPN**, fare clic su **Download e distribuzione**. A seconda della piattaforma di virtualizzazione in uso, scaricare l'appliance VPN per VMware vSphere o per Microsoft Hyper-V.
4. Distribuire l'appliance e connetterla alle reti di produzione.
   In vSphere, verificare che le opzioni **Modalità promiscua** e **Forged Transmits** siano abilitate e impostare su **Accetta** tutti i commutatori virtuali che connettono l'appliance VPN alle reti di produzione. Per accedere a queste impostazioni, nel client vSphere, selezionare l'host > **Riepilogo** > **Rete**, quindi selezionare il commutatore > **Modifica impostazioni...** > **Sicurezza**.
   In Hyper-V, creare una macchina virtuale di tipo **Generation 1** con 1024 MB di memoria. Si consiglia inoltre di abilitare l'opzione **Memoria dinamica** per il sistema. Una volta creata la macchina virtuale, passare a **Impostazioni** > **Hardware** > **Adattatore di rete** > **Funzionalità avanzate** e selezionare la casella di controllo **Abilita lo spoofing degli indirizzi MAC**.
5. Accendere l'appliance.
6. Aprire la console dell'appliance e accedere con il nome utente e la password "admin/admin".
7. [Facoltativo] Modificare la password.
8. [Facoltativo] Modificare le impostazioni di rete se necessario. Definire l'interfaccia che verrà utilizzata come WAN per la connessione Internet.
9. Registrare l'appliance nel servizio Cyber Protection usando le credenziali dell'amministratore dell'azienda.
   Tali credenziali vengono utilizzate solo una volta per recuperare il certificato. L'URL del data center è predefinito.

Nota
Se per l'account è stata configurata l'autenticazione a due fattori, verrà chiesto di inserire il codice TOTP. Se l'autenticazione a due fattori è abilitata ma non configurata per l'account, non è possibile registrare l'appliance VPN. È necessario innanzitutto aprire la pagina di login della console di Cyber Protect e completare la configurazione dell'autenticazione a due fattori per l'account. Per ulteriori dettagli sull'autenticazione a due fattori, consultare il Manuale dell'amministratore del portale di gestione.

Una volta completata la configurazione, l'appliance verrà visualizzata con lo stato **In linea**. L'appliance si connette al gateway VPN e inizia a fornire informazioni sulle reti da tutte le interfacce attive al servizio Cyber Disaster Recovery Cloud. Le interfacce vengono visualizzate nella console di Cyber Protect, in base alle informazioni raccolte dall'appliance VPN.

Configurazione di una connessione VPN IPsec multisito

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

È possibile configurare una connessione VPN IPsec multisito nei due modi seguenti:

- dalla scheda **Disaster Recovery** > **Connessione**;
- applicando un piano di protezione a uno o più dispositivi e quindi passando in modo manuale dalla connessione Open VPN da sito a sito creata automaticamente a una connessione VPN IPsec multisito, quindi configurando le impostazioni VPN IPsec multisito e riassegnando gli indirizzi IP.

Per configurare una connessione VPN IPsec multisito dalla scheda Connessione

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**.
2. Nella sezione **Connessione VPN multisito**, fare clic su **Configura**.
   Il gateway VPN viene distribuito nel sito cloud.
3. Configurare le impostazioni VPN IPsec multisito.

Per configurare una connessione VPN IPsec multisito da un piano di protezione

1. Nella console di Cyber Protect, passare a **Dispositivi**.
2. Applicare un piano di protezione a uno o più dispositivi dell'elenco.
   Le impostazioni del server di ripristino e dell'infrastruttura cloud vengono automaticamente configurate per la connessione Open VPN da sito a sito.
3. Passare a **Disaster Recovery** > **Connessione**.
4. Fare clic su **Mostra proprietà**.
5. Fare clic su **Passa a VPN IPsec multisito**.
6. Configurare le impostazioni VPN IPsec multisito.
7. Riassegnare gli indirizzi IP della rete cloud e dei server cloud.

Configurare le impostazioni di VPN IPsec multisito

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Dopo aver configurato una VPN IPsec multisito, è necessario configurare le impostazioni del sito cloud e dei siti locali nella scheda **Disaster Recovery** > **Connessione**.

Prerequisiti

- La connessione VPN IPsec multisito è configurata. Per ulteriori informazioni su come configurare la connessione VPN IPsec multisito, vedere "Configurazione di una connessione VPN IPsec multisito" (pag. 31).
- Ogni gateway VPN IPsec locale ha un proprio indirizzo IP pubblico.
- La rete cloud deve essere dotata di un numero sufficiente di indirizzi IP per i server cloud che sono copie dei sistemi protetti (nella rete di produzione), e per i server di ripristino (con uno o due indirizzi IP a seconda delle esigenze).
- [Se si utilizza il firewall tra i siti locali e il sito cloud] È necessario consentire i seguenti protocolli IP e porte UDP sui siti locali: Protocollo IP ID 50 (ESP), Porta UDP 500 (IKE) e porta UDP 4500.
- La configurazione NAT-T nei siti locali è disabilitata.

Per configurare una connessione VPN IPsec multisito

1. Aggiungere una o più reti al sito cloud.
   a. Fare clic su **Aggiungi rete**.

      Nota
      Quando si aggiunge una rete cloud, verrà aggiunta automaticamente una rete di test corrispondente, con lo stesso indirizzo e maschera di rete, per l'esecuzione dei failover di prova. I server cloud nella rete di prova avranno gli stessi indirizzi IP della rete di produzione cloud. Se è necessario accedere a un server cloud dalla rete di produzione durante un failover di prova, assegnare un secondo indirizzo IP di prova al momento della creazione del server di ripristino.

   b. Nel campo **Indirizzo di rete**, digitare l'indirizzo IP della rete.
   c. Nel campo **Maschera di rete**, digitare la maschera della rete.
   d. Fare clic su **Aggiungi**.
2. Configurare le impostazioni di ogni sito locale da connettere al sito cloud, seguendo le raccomandazioni per i siti locali. Per ulteriori informazioni su queste raccomandazioni, consultare "Raccomandazioni generiche per i siti locali" (pag. 33).
   a. Fare clic su **Aggiungi Connessione**.
   b. Inserire un nome per il gateway VPN locale.

c. Inserire l'indirizzo IP pubblico del gateway VPN locale.

d. [Facoltativo] Inserire una descrizione per il gateway VPN locale.

e. Fare clic su **Avanti**.

f. Nel campo **Chiave precondivisa**, digitare la chiave precondivisa oppure fare clic su **Genera una chiave precondivisa** per utilizzare un valore generato automaticamente.

Nota
È necessario utilizzare la stessa chiave precondivisa per i gateway VPN locale e cloud.

g. Fare clic su **Impostazioni di sicurezza IPsec/IKE** per configurare tali impostazioni. Per ulteriori informazioni sulle impostazioni che è possibile configurare, vedere "Impostazioni di sicurezza IPsec/IKE" (pag. 34).

Nota
È possibile utilizzare le impostazioni predefinite, che vengono compilate automaticamente, oppure utilizzare valori personalizzati. Sono supportate solo le connessioni con protocollo IKEv2. L'**Azione all'avvio** predefinita quando si stabilisce la VPN è **Aggiungi** (il gateway VPN locale inizializza la connessione), ma è possibile modificarla in **Avvia** (il gateway VPN cloud inizializza la connessione) oppure in **Indirizza** (adatta ai firewall che supportano le opzioni di routing).

h. Configurare i **Criteri di rete**.
I criteri di rete specificano le reti alle quali si connette la VPN IPsec. Digitare l'indirizzo IP e la maschera della rete utilizzando il formato CIDR. I segmenti di rete locali e cloud non devono sovrapporsi.

i. Fare clic su **Salva**.

Raccomandazioni generiche per i siti locali

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Durante la configurazione dei siti locali per la connessione VPN IPsec multisito, tenere conto delle seguenti raccomandazioni:

- Per ogni fase IKE, impostare almeno uno dei valori configurati nel sito cloud per i seguenti parametri: Algoritmo di crittografia, Algoritmo hash, Numeri del gruppo Diffie-Hellman.
- Abilitare Perfect Forward Secrecy con almeno uno dei valori dei numeri del gruppo Diffie-Hellman configurato nel sito cloud per IKE Phase 2.
- Configurare lo stesso valore per la **Permanenza** di IKE Phase 1 e IKE Phase 2, come nel sito cloud.
- Le configurazioni con attraversamento NAT (NAT-T) non sono supportate. Disabilitare la configurazione NAT-T nel sito locale. Altrimenti, non sarà possibile negoziare l'ulteriore incapsulamento UDP.

- Configurando l'**Azione all'avvio** si definisce il lato che inizializza la connessione. Il valore predefinito **Aggiungi** indica che il sito locale inizializza la connessione e che il sito cloud attende l'inizializzazione della connessione. Cambiare il valore in **Avvio** per fare in modo che sia il sito cloud a inizializzare la connessione, oppure in **Indirizza** per fare in modo che entrambi i lati possano inizializzare la connessione (quest'opzione è adatta ai firewall che supportano l'opzione di routing).

Per ulteriori informazioni ed esempi di configurazione per diverse soluzioni, consultare:

- Questa serie di articoli della Knowledge Base
- Questo tutorial video

Impostazioni di sicurezza IPsec/IKE

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

La tabella seguente include informazioni dettagliate sui parametri di sicurezza IPsec/IKE.

Parametro	Descrizione
Algoritmo di crittografia	L'algoritmo di crittografia da utilizzare per garantire che i dati non siano visualizzabili quando in transito. Per impostazione predefinita, tutti gli algoritmi sono selezionati. È necessario configurare almeno uno degli algoritmi selezionati nel dispositivo gateway locale per ogni fase IKE.
Algoritmo di hash	L'algoritmo di hash da utilizzare per verificare l'integrità e l'autenticità dei dati. Per impostazione predefinita, tutti gli algoritmi sono selezionati. È necessario configurare almeno uno degli algoritmi selezionati nel dispositivo gateway locale per ogni fase IKE.
Numeri del gruppo Diffie-Hellman	I numeri del gruppo Diffie-Hellman definiscono la sicurezza delle chiavi utilizzate nel processo IKE (Internet Key Exchange). I numeri di gruppo più elevati sono più sicuri ma richiedono più tempo per l'elaborazione della chiave. Per impostazione predefinita, tutti i gruppi sono selezionati. È necessario configurare almeno uno dei gruppi selezionati nel dispositivo gateway locale per ogni fase IKE.
Permanenza (in secondi)	Il valore della permanenza determina la durata di

Parametro	Descrizione
	un'istanza di connessione con un insieme di chiavi di crittografia/autenticazione per i pacchetti utente, dalla riuscita della negoziazione alla scadenza. Intervallo per la fase 1: 900-28800 secondo con valore predefinito 28800. Intervallo per la fase 2: 900-3600 secondi con valore predefinito 3600. La permanenza nella fase 2 deve essere inferiore alla permanenza nella fase 1. La connessione viene nuovamente negoziata tramite il canale di reimpostazione delle chiavi prima della sua scadenza; consultare **Tempo di margine di reimpostazione di nuova chiave**. Se il lato locale e quello remoto entrano in conflitto sulla durata della permanenza, sul lato con la permanenza più lunga si avrà un accumulo di connessioni sostituite. Vedere anche **Tempo di margine di reimpostazione di nuova chiave** e **Fuzz di reimpostazione della chiave**.
Tempo di margine di reimpostazione della chiave (secondi)	Il tempo di margine in secondi prima della scadenza della connessione o del canale di reimpostazione della chiave, durante il quale il lato locale della connessione VPN tenta di negoziare una sostituzione. Il tempo esatto di reimpostazione della chiave viene selezionato in maniera casuale in base al valore di **Fuzz di reimpostazione della nuova chiave.** È rilevante solo a livello locale, non è necessario che il valore sia concordato con il lato remoto. Intervallo: 900-3600 secondi. Il valore predefinito è 3600.
Intervallo della finestra di riproduzione (pacchetti)	Dimensione della finestra di riproduzione IPsec per questa connessione. Il valore predefinito -1 utilizza il valore configurato con il comando charon.replay_window nel file strongswan.conf. Valori superiori a 32 sono supportati solo quando si utilizza il backend Netlink. Il valore 0 disabilita la protezione della riproduzione IPsec.
Fuzz di reimpostazione della chiave	Valore che indica la percentuale massima di

Parametro	Descrizione
(%)	aumento casuale dei valori di marginbyte, marginpacket e margintime per randomizzare gli intervalli di reimpostazione della chiave (importante per gli host con molte connessioni). Il valore del fuzz di reimpostazione della chiave può superare 100%. Il valore di marginTYPE, dopo l'aumento casuale, non deve superare il valore di lifeTYPE, in cui TYPE indica il tipo di byte, packet o time. Il valore 0% disabilita la randomizzazione. È rilevante solo a livello locale, non è necessario che il valore sia concordato con il lato remoto.
Timeout DPD (secondi)	Il periodo di tempo dopo il quale si verifica un timeout DPD (Dead Peer Detection). È possibile specificare un valore pari a 30 o superiore. Il valore predefinito è 30.
Azione timeout DPD	L'azione da intraprendere dopo il verificarsi del timeout DPD. **Riavvia** - Riavvia la sessione quando si verifica il timeout DPD. **Cancella** - Termina la sessione quando si verifica il timeout DPD. **Nessuna** - Non intraprende nessuna azione quando si verifica il timeout DPD.
Azione all'avvio	Determina il lato che inizializza la connessione e definisce il tunnel della connessione VPN. **Aggiungi** - Il gateway VPN locale che inizializza la connessione. **Avvia** - Il gateway VPN cloud che inizializza la connessione. **Indirizza** - Adatta ai gateway VPN che supportano l'opzione di indirizzamento. Il tunnel viene attivato solo quando c'è traffico inizializzato dal gateway VPN locale o dal gateway VPN cloud.

Raccomandazioni per la disponibilità dei Servizi di dominio Active Directory

Se i workload protetti devono eseguire l'autenticazione in un controller di dominio, è consigliabile disporre di un'istanza del controller di dominio Active Directory nel sito di disaster recovery.

Controller di dominio Active Directory per la connessione Open VPN L2

Con la connessione Open VPN L2, gli indirizzi IP dei workload protetti vengono conservati nel sito cloud durante un failover di prova o un failover di produzione. Pertanto, durante un failover di prova o un failover di produzione, il controller di dominio Active Directory avrà lo stesso indirizzo IP del sito locale.

Un DNS personalizzato consente di definire il proprio server DNS personalizzato per tutti i server cloud. Per ulteriori informazioni, consultare "Configurazione di server DNS personalizzati" (pag. 46).

Controller di dominio Active Directory per la connessione VPN IPsec L3

Con la connessione VPN IPsec L3, gli indirizzi IP dei workload protetti non vengono conservati nel sito cloud. Pertanto, prima di eseguire un failover di produzione, è consigliabile disporre di un'istanza aggiuntiva dedicata del controller di dominio Active Directory come server primario nel sito cloud.

Per un'istanza dedicata del controller di dominio Active Directory, configurato come server primario nel sito cloud, sono raccomandate le operazioni indicate di seguito.

- Disattivare Windows Firewall.
- Registrare il server primario al servizio Active Directory.
- Accertarsi che il server primario disponga dell'accesso a Internet.
- Aggiungere la funzionalità Active Directory.

Un DNS personalizzato consente di definire il proprio server DNS personalizzato per tutti i server cloud. Per ulteriori informazioni, consultare "Configurazione di server DNS personalizzati" (pag. 46).

Configurazione dell'accesso VPN remoto da punto a sito

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Se è necessario connettersi al sito locale da remoto, è possibile configurare la connessione da punto a sito al sito locale. È possibile attenersi alla procedura seguente o guardare il tutorial video.

Prerequisiti

- La connessione Open VPN da sito a sito è configurata.
- L'appliance VPN è installata nel sito locale.

Per configurare la connessione da punto a sito al sito locale

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**.
2. Fare clic su **Mostra proprietà**.
3. Abilitare l'opzione **Accesso VPN al sito locale**.
4. Verificare che l'utente che desidera stabilire la connessione da punto a sito al sito locale disponga di:
   - un account utente in Cyber Protect Cloud. Queste credenziali sono utilizzate per l'autenticazione nel client VPN. In caso contrario, creare un account utente in Cyber Protect Cloud.
   - un ruolo utente di "Amministratore dell'azienda" o "Cyber Protection".
5. Configurazione del cliente OpenVPN:
   a. Scaricare il client OpenVPN versione 2.4.0 o successive dalla posizione seguente https://openvpn.net/community-downloads/.
   b. Installare il client OpenVPN sul sistema dal quale connettersi al sito locale.
   c. Fare clic su **Scarica configurazione per OpenVPN**. Il file di configurazione è valido per gli utenti dell'organizzazione con il ruolo utente "Amministratore società" o "Cyber Protection".
   d. Importare la configurazione scaricata in OpenVPN.
   e. Accedere al client OpenVPN con le credenziali utente Cyber Protect Cloud (vedere il precedente passaggio 4).
   f. [Facoltativo] Se l'autenticazione a due fattori viene abilitata per l'organizzazione, è necessario fornire il codice TOTP temporaneo.

Importante
Se è stata abilitata l'autenticazione a due fattori per l'account, è necessario rigenerare il file di configurazione e rinnovarlo per i client OpenVPN esistenti. Gli utenti devono accedere nuovamente a Cyber Protect Cloud per configurare l'autenticazione a due fattori per i propri account.

Gli utenti potranno collegarsi ai sistemi sul sito locale.

Gestione della rete

In questa sezione vengono descritti alcuni esempi di gestione della rete.

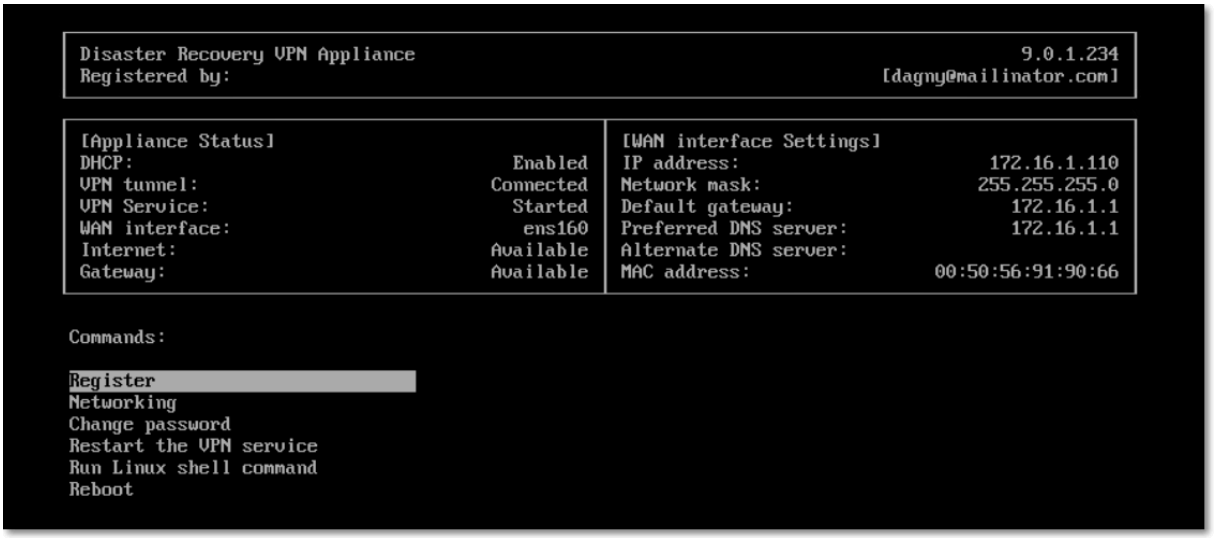
Gestione delle reti

Nota
Alcune funzionalità possono richiedere licenze aggiuntive, a seconda del modello di licensing applicato.

Connessione Open VPN da sito a sito

Per aggiungere una rete al sito locale ed estenderla al cloud

1. Nell'appliance VPN, configurare la nuova interfaccia di rete con la rete locale che si desidera estendere al cloud.
2. Accedere alla console dell'appliance VPN.
3. Nella sezione della **rete**, configurare le impostazioni di rete della nuova interfaccia.



L'appliance VPN inizia a fornire informazioni sulle reti da tutte le interfacce attive al servizio Cyber Disaster Recovery Cloud. Le interfacce vengono visualizzate nella console di Cyber Protect, in base alle informazioni raccolte dall'appliance VPN.

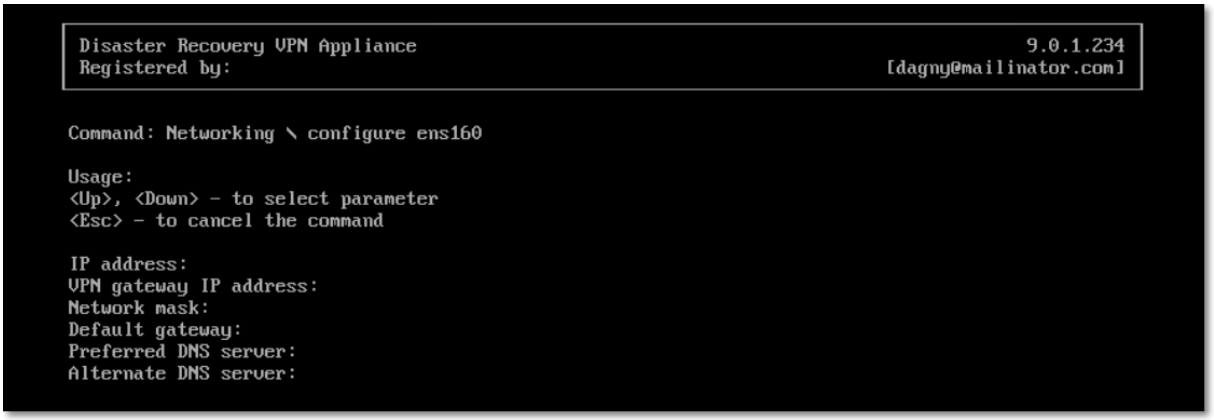
Per eliminare una rete estesa al cloud

1. Accedere alla console dell'appliance VPN.
2. Nella sezione della **rete**, selezionare l'interfaccia da eliminare e quindi fare clic su **Elimina impostazioni di rete**.
3. Confermare l'operazione.

L'estensione della rete locale al cloud tramite un tunnel VPN sicuro verrà eliminata. Tale rete funzionerà come segmento cloud indipendente. Se l'interfaccia è utilizzata per il passaggio del traffico da/verso il sito cloud, tutte le connessioni di rete da/verso il sito cloud verranno disconnesse.

Per modificare i parametri di rete

1. Accedere alla console dell'appliance VPN.
2. Nella sezione della **rete**, selezionare l'interfaccia da modificare.
3. Fare clic su **Modifica impostazioni di rete**.
4. Selezionare una delle due opzioni:
   - Per la configurazione automatica tramite DHCP, fare clic su **Uso del DHCP**. Confermare l'operazione.
   - Per la configurazione manuale della rete, fare clic su **Configurazione dell'indirizzo IP statico**. Le seguenti impostazioni sono disponibili per la modifica:
     - **Indirizzo IP**: l'indirizzo IP dell'interfaccia nella rete locale.
     - **Indirizzo IP del gateway VPN**: lo speciale indirizzo IP riservato al segmento della rete cloud per l'appropriato funzionamento del servizio Cyber Disaster Recovery Cloud.
     - **Maschera di rete**: maschera di rete della rete locale.
     - **Gateway predefinito**: gateway predefinito sul sito locale.
     - **Server DNS preferito**: server DNS primario sul sito locale.
     - **Server DNS alternativo**: server DNS secondario sul sito locale.



- Apportare le modifiche necessarie e confermarle facendo clic su Invio.

Modalità solo cloud

È possibile avere un massimo di 23 reti nel cloud.

Per aggiungere una nuova rete cloud

1. Passare a **Disaster Recovery** > **Connessione**.
2. In **Sito cloud**, fare clic su **Aggiungere una rete cloud**.
3. Definire i parametri della rete cloud: indirizzo e maschera. Al termine, fare clic su **Fine**.

La rete cloud aggiuntiva, con l'indirizzo e la maschera definiti, verranno creati nel sito cloud.

Per eliminare una rete cloud

Nota
Non è possibile eliminare una rete cloud se contiene anche un solo un server cloud. Eliminare innanzitutto il server cloud e quindi eliminare la rete.

1. Passare a **Disaster Recovery** > **Connessione**.
2. In **Sito cloud**, fare clic sull'indirizzo di rete che si desidera eliminare.
3. Fare clic su **Elimina** e confermare l'operazione.

Per modificare i parametri della rete cloud

1. Passare a **Disaster Recovery** > **Connessione**.
2. In **Sito cloud**, fare clic sull'indirizzo di rete che si desidera modificare.
3. Fare clic su **Modifica**.
4. Modificare l'indirizzo e la maschera della rete, quindi fare clic su **Fine**.

Nuova configurazione dell'indirizzo IP

Affinché le prestazioni di disaster recovery siano adeguate, gli indirizzi IP assegnati ai server locale e cloud devono essere coerenti. In caso di incoerenza o mancata corrispondenza tra gli indirizzi IP, in **Disaster Recovery** > **Connessione** verrà visualizzato un punto esclamativo accanto alla rete corrispondente.

Di seguito sono elencate alcune delle cause note di incoerenza tra indirizzi IP:

1. Un server di ripristino è stato migrato da una rete all'altra oppure la maschera di rete della rete cloud è stata modificata. Di conseguenza, i server cloud ottengono gli indirizzi IP da reti alle quali non sono connessi.
2. Il tipo di connessione è stato modificato da Senza Connessione da sito a sito in Connessione da sito a sito. Di conseguenza, un server locale risulta collocato in una rete diversa da quella creata per il sito di ripristino nel sito cloud.
3. Il tipo di connessione è stato modificato da Open VPN da sito a sito in VPN IPsec multisito, o da VPN IPsec multisito in Open VPN da sito a sito. Per ulteriori informazioni su questo scenario, vedere Passaggio da una connessione a un'altra e Riassegnazione di indirizzi IP.
4. Modifica dei seguenti parametri di rete nel sito dell'appliance VPN:
   - Aggiunta di un'interfaccia tramite le impostazioni di rete
   - Modifica manuale della maschera di rete tramite le impostazioni dell'interfaccia
   - Modifica della maschera di rete tramite DHCP
   - Modifica dell'indirizzo e della maschera di rete tramite le impostazioni dell'interfaccia
   - Modifica dell'indirizzo e della maschera di rete tramite DHCP

   Come conseguenza delle azioni sopra elencate, la rete nel sito cloud può diventare un sottoinsieme o soprainsieme della rete locale, oppure l'interfaccia dell'appliance VPN può fornire le stesse impostazioni di rete per diverse interfacce.

Per risolvere i problemi delle impostazioni di rete

1. Fare clic sulla rete che richiede una nuova configurazione dell'indirizzo IP.
   Viene visualizzato l'elenco dei server presenti nella rete selezionata, con il relativo stato e gli indirizzi IP. I server le cui impostazioni di rete non sono coerenti sono contrassegnati da un punto esclamativo.
2. Per modificare le impostazioni di rete per un server fare clic su **Vai al server**. Per modificare le impostazioni di rete per tutti i server contemporaneamente, fare clic su **Modifica** nella sezione di notifica.
3. Modificare gli indirizzi IP come necessario definendoli nei campi **Nuovo IP** e **Nuovo IP di prova**.
4. Al termine, fare clic su **Conferma**.

Spostare i server in una rete adatta

Quando si crea un piano di protezione di disaster recovery e si applica ai dispositivi selezionati, il sistema controlla gli indirizzi IP dei dispositivi e se non sono presenti reti cloud adatte all'indirizzo IP, crea automaticamente reti cloud idonee. Per impostazione predefinita vengono configurate con gli intervalli massimi raccomandati da IANA per l'uso privato (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). È possibile limitare la rete modificando la maschera di rete.

Nel caso in cui i dispositivi selezionati siano presenti su più reti locali, la rete nel sito cloud può diventare un superinsieme di reti locali. In questo caso, per riconfigurare le reti cloud:

1. Fare clic sulla rete cloud che richiede la riconfigurazione della dimensione della rete e quindi su **Modifica**.
2. Riconfigurare la dimensione della rete con le impostazioni corrette.
3. Creare altre le reti necessarie.
4. Fare clic sull'icona della notifica accanto al numero dei dispositivi connessi alla rete.
5. Fare clic su **Passare a una rete adatta**.
6. Selezionare i server da spostare sulle reti adatte, quindi fare clic su **Sposta**.

Gestione delle impostazioni dell'appliance VPN

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Nella console di Cyber Protect (**Disaster Recovery** > **Connessione**) è possibile:

- Scaricare i file di registro.
- Annullare la registrazione dell'appliance (se è necessario ripristinare le impostazioni dell'appliance VPN o passare alla modalità di connessione solo cloud).

Per accedere a queste impostazioni, fare clic sull'**i**cona nella sezione **Appliance VPN**.

Nella console dell'appliance VPN è possibile:

- Modificare la password dell'appliance.
- Visualizzare/modificare le impostazioni di rete e definire l'interfaccia che verrà utilizzata come WAN per la connessione Internet.
- Registrare/modificare l'account di registrazione (ripetendo la registrazione).
- Riavviare il servizio VPN.
- Riavviare l'appliance VPN.
- Eseguire il comando della shell Linux (solo per operazioni avanzate di soluzione dei problemi).

Reinstallazione del gateway VPN

Se si verifica un problema con il gateway VPN che non si riesce a risolvere, è possibile reinstallarlo. I possibili problemi includono:

- Il gateway VPN è nello stato **Errore**.
- Il gateway VPN è nello stato **In sospeso** da molto tempo.
- Lo stato del gateway VPN è impossibile da determinare da molto tempo.

La procedura di reinstallazione del gateway VPN include le seguenti azioni automatiche: eliminazione completa della virtual machine del gateway VPN esistente, installazione di una nuova virtual machine dal modello e applicazione delle impostazioni del gateway VPN precedente sulla nuova virtual machine.

Prerequisiti:

È necessario configurare uno dei tipi di connessione al sito cloud.

Per reinstallare il gateway VPN

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**.
2. Fare clic sull'icona ingranaggio del gateway VPN e selezionare **Reinstalla gateway VPN**.
3. Nella finestra di dialogo **Reinstalla gateway VPN**, inserire il login.
4. Fare clic su **Reinstalla**.

Abilitazione e disabilitazione della connessione da sito a sito

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

È possibile abilitare la connessione da sito a sito nei seguenti casi:

- Se è necessario che i server cloud nel sito cloud comunichino con i server del sito locale.
- Dopo un failover nel cloud, l'infrastruttura locale viene ripristinata e si desidera eseguire il failback dei server nel sito locale.

Per abilitare la connessione da sito a sito

1. Passare a **Disaster Recovery** > **Connessione**.
2. Fare clic su **Mostra proprietà**, quindi abilitare l'opzione **Connessione da sito a sito**.

Viene abilitata la connessione VPN da sito a sito tra i siti locale e cloud. Il servizio Cyber Disaster Recovery Cloud ottiene le impostazioni di rete dall'appliance VPN ed estende le reti locali al sito cloud.

Se non è necessario che i server cloud nel sito cloud comunichino con i server del sito locale, è possibile disabilitare la connessione da sito a sito.

Per disabilitare la connessione da sito a sito

1. Passare a **Disaster Recovery** > **Connessione**.
2. Fare clic su **Mostra proprietà**, quindi disabilitare l'opzione **Connessione da sito a sito**.

Il sito locale verrà scollegato dal sito cloud.

Passaggio al tipo di connessione da sito a sito

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

È possibile passare con facilità da una connessione Open VPN da sito a sito a una connessione VPN IPsec multisito, e viceversa.

Quando si modifica il tipo di connessione, le connessioni VPN attive vengono eliminate, mentre vengono conservate le configurazioni della rete e dei server cloud. È tuttavia necessario riassegnare gli indirizzi IP delle reti e dei server cloud.

La tabella seguente confronta le caratteristiche di base della connessione Open VPN da sito a sito e della connessione VPN IPsec multisito.

	Open VPN da sito a sito	**VPN IPsec multisito**
Supporto per il sito locale	Singolo	Singolo, multiplo
Modalità Gateway VPN	L2 Open VPN	L3 IPsec VPN
Segmenti di rete	Estende la rete locale alla rete cloud	I segmenti delle reti locali e delle reti cloud non devono sovrapporsi
Supporta l'accesso da punto a sito al sito locale	Sì	No
Supporta l'accesso da punto a sito al sito cloud	Sì	Sì
Richiede un elemento dell'offerta IP pubblico	No	Sì

Per passare da una connessione Open VPN da sito a sito a una connessione VPN IPsec multisito

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**.
2. Fare clic su **Mostra proprietà**.
3. Fare clic su **Passa a VPN IPsec multisito**.
4. Fare clic su **Riconfigura**.
5. Riassegnare gli indirizzi IP della rete cloud e dei server cloud.
6. Configurare le impostazioni della connessione IPsec multisito.

Per passare da una connessione VPN IPsec multisito a una connessione Open VPN da sito a sito

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**.
2. Fare clic su **Mostra proprietà**.
3. Fare clic su **Passa a Open VPN da sito a sito**.
4. Fare clic su **Riconfigura**.
5. Riassegnare gli indirizzi IP della rete cloud e dei server cloud.
6. Configurare le impostazioni della connessione da sito a sito.

Riassegnazione di indirizzi IP

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

È necessario riassegnare gli indirizzi IP delle reti cloud e dei server cloud per poter completare la configurazione nei casi indicati di seguito:

- Il tipo di connessione è stato modificato da Open VPN da sito a sito in VPN IPsec multisito, o al contrario.
- Dopo aver applicato un piano di protezione (se la connessione VPN IPsec multisito è configurata).

Per riassegnare l'indirizzo IP di una rete cloud

1. Nella scheda **Connessione**, fare clic sull'indirizzo IP della rete cloud.
2. Nel menu a comparsa **Rete**, fare clic su **Modifica**.
3. Digitare il nuovo indirizzo e la nuova maschera di rete.
4. Fare clic su **Fine**.

Dopo aver riassegnato l'indirizzo IP di una rete cloud, è necessario riassegnare i server cloud che appartengono alla rete cloud riassegnata.

Per riassegnare l'indirizzo IP di un server

1. Nella scheda **Connessione**, fare clic sull'indirizzo IP del server nella rete cloud.
2. Nel menu a comparsa **Server**, fare clic su **Modifica indirizzo IP**.
3. Nel menu a comparsa **Modifica indirizzo IP**, digitare il nuovo indirizzo IP del server, o utilizzare l'indirizzo IP generato automaticamente che fa parte della rete cloud riassegnata.

   Nota
   Cyber Disaster Recovery Cloud assegna automaticamente gli indirizzi IP dalla rete cloud a tutti i server cloud che erano parte della rete cloud prima della riassegnazione dell'indirizzo IP di rete. È possibile utilizzare gli indirizzi IP suggeriti per riassegnare in una sola volta gli indirizzi IP di tutti i server cloud.

4. Fare clic su **Conferma**.

Configurazione di server DNS personalizzati

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Quando si configura una connessione, Cyber Disaster Recovery Cloud crea l'infrastruttura della rete cloud. Il server DHCP cloud assegna automaticamente i server DNS predefiniti ai server di ripristino e ai server primari; è tuttavia possibile modificare le impostazioni predefinite e configurare server DNS personalizzati. Le nuove impostazioni DNS verranno applicate al momento della successiva richiesta inviata al server DHCP.

Prerequisiti:

È necessario configurare uno dei tipi di connessione al sito cloud.

Per configurare un server DNS personalizzato

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**.
2. Fare clic su **Mostra proprietà**.
3. Fare clic su **Impostazioni predefinite (fornite dal sito cloud)**.
4. Selezionare **Server personalizzati**.
5. Digitare l'indirizzo IP del server DNS.
6. [Facoltativo] Se si desidera aggiungere un altro server DNS, fare clic su **Aggiungi** e digitare l'indirizzo IP del server DNS.

   Nota
   Dopo aver aggiunto i server DNS personalizzati, è possibile aggiungere anche i server DNS predefiniti. In questo modo, se i server DNS non sono disponibili Cyber Disaster Recovery Cloud utilizzerà i server DNS predefiniti.

7. Fare clic su **Fine**.

Eliminazione di server DNS personalizzati

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

È possibile eliminare i server DNS dall'elenco dei server DNS personalizzati.

Prerequisiti:

I server DNS personalizzati sono configurati.

Per eliminare un server DNS personalizzato

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**.
2. Fare clic su **Mostra proprietà**.
3. Fare clic su **Server personalizzati**.
4. Fare clic sull'icona di eliminazione accanto al server DNS.

   Nota
   L'operazione di eliminazione è disabitata quando è disponibile un solo server DNS personalizzato. Per eliminare tutti i server DNS personalizzati, selezionare **Impostazioni predefinite (fornite dal sito cloud)**.

5. Fare clic su **Fine**.

Download degli indirizzi MAC

È possibile scaricare un elenco di indirizzi MAC e quindi estrarli e importarli nella configurazione del server DHCP personalizzato.

Prerequisiti:

- È necessario configurare uno dei tipi di connessione al sito cloud.
- È necessario configurare almeno un server primario o di ripristino con un indirizzo MAC.

Per scaricare l'elenco degli indirizzi MAC

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**.
2. Fare clic su **Mostra proprietà**.
3. Fare clic su **Scarica l'elenco degli indirizzi MAC**, quindi salvare il file CSV.

Configurazione del routing locale

Oltre alle reti locali estese al cloud tramite l'appliance VPN, possono essere presenti altre reti locali non registrate nell'appliance VPN ma contenenti server che devono comunicare con i server cloud. Per stabilire la connessione tra questi server locali e i server cloud, è necessario configurare le impostazioni del routing locale.

Per configurare il routing locale

1. Passare a **Disaster Recovery**>**Connessione**.
2. Fare clic su **Mostra proprietà**, quindi su **Routing locale**.
3. Specificare le reti locali nella notazione CIDR.
4. Fare clic su **Salva**.

I server delle reti locali specificate potranno ora comunicare con i server cloud.

Consentire il traffico DHCP su L2 VPN

Se i dispositivi nel sito locale dell'utente ottengono i propri indirizzi IP da un server DHCP, è possibile proteggere tale server DHCP con la funzionalità di Disaster Recovery, eseguirne il failover nel cloud e quindi consentire che il traffico DHCP venga eseguito su L2 VPN. In questo modo, il server DHCP verrà eseguito nel cloud, ma continuerà ad assegnare gli indirizzi IP ai dispositivi locali.

Prerequisiti:

È necessario configurare il tipo di connessione al sito cloud Site-to-site L2 VPN.

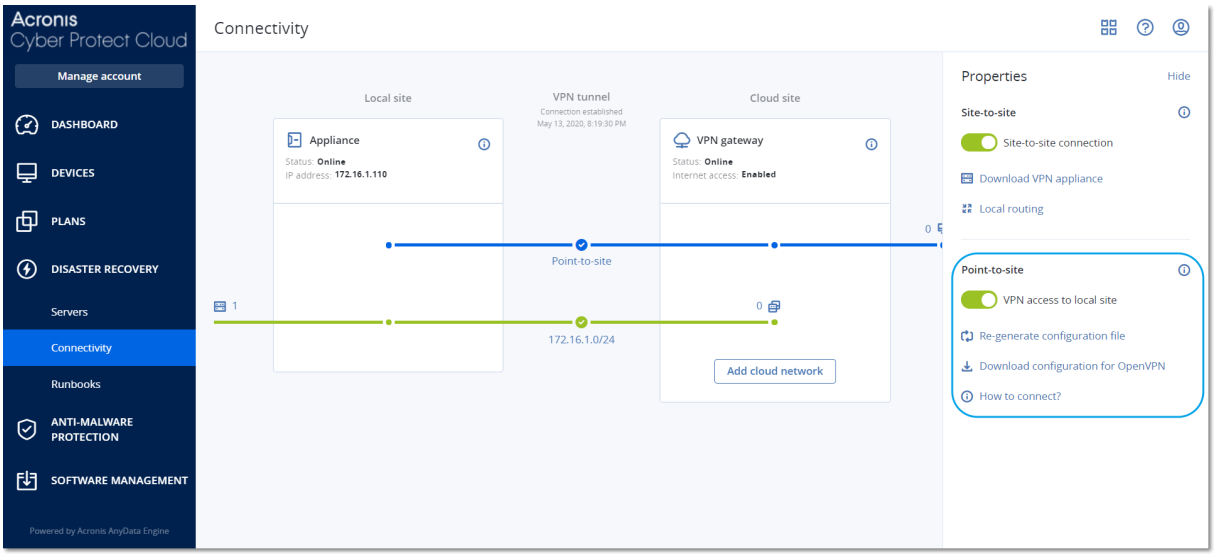
Per consentire il traffico DHCP tramite la connessione L2 VPN

1. Passare alla scheda **Disaster Recovery** > **Connessione**.
2. Fare clic su **Mostra proprietà**.
3. Abilitare l'opzione **Consente il traffico DHCP su L2 VPN**.

Gestione delle impostazioni di connessioni da punto a sito

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**, quindi fare clic su **Mostra proprietà** nell'angolo in alto a destra.



Accesso VPN al sito locale

Questa opzione viene utilizzata per gestire l'accesso VPN al sito locale. È abilitata per impostazione predefinita. Se viene disabilitata, l'accesso da punto a sito al sito locale non verrà consentito.

Scarica configurazione per OpenVPN

Questa opzione consente di scaricare il file di configurazione del client OpenVPN. Il file è necessario per stabilire una connessione da punto a sito con il sito cloud.

Rigenera file di configurazione

Questa opzione consente di rigenerare il file di configurazione del client OpenVPN.

L'operazione è necessaria nei seguenti casi:

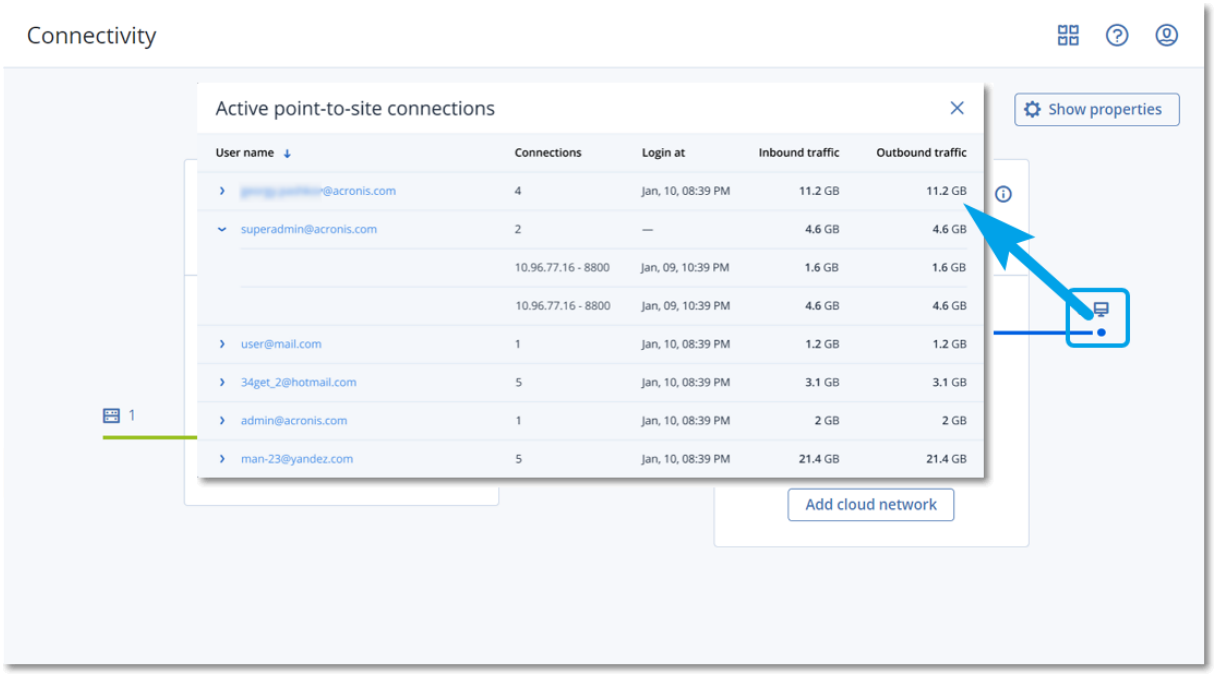
- Se si sospetta che il file di configurazione sia danneggiato.
- Se l'autenticazione a due fattori è stata abilitata per l'account dell'utente.

Non appena completato l'aggiornamento del file di configurazione, non sarà più possibile connettersi utilizzando il file di configurazione precedente. Accertarsi di distribuire il nuovo file agli utenti autorizzati all'uso della connessione da punto a sito.

Connessioni da punto a sito attive

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Tutte le connessioni attive da punto a sito sono visualizzate in **Disaster Recovery** > **Connessione**. Fare clic sull'icona del sistema sulla linea blu **Da punto a sito** per visualizzare informazioni dettagliate sulle connessioni attive da punto a sito raggruppate in base al nome dell'utente.



Lavorare con i registri

Disaster Recovery acquisisce i registri dall'appliance VPN e dal gateway VPN. Questi registri vengono salvati come file txt e quindi compressi in un archivio zip. È possibile scaricare ed estrarre l'archivio e utilizzare le informazioni per attività di soluzione dei problemi o di monitoraggio.

L'elenco seguente descrive i file di registro contenuti nell'archivio zip e le informazioni che contengono.

`dnsmasq.config.txt` - Il file contiene informazioni sulla configurazione del servizio che fornisce gli indirizzi DNS e DHCP.

`dnsmsq.leases.txt` - Il file contiene informazioni sulle assegnazioni dell'indirizzo DHCP corrente.

`dnsmasq_log.txt` - Il file contiene i registri del servizio dnsmasq.

`ebtables.txt` - Il file contiene informazioni sulle tabelle del firewall.

`free.txt` - Il file contiene informazioni sulla memoria disponibile.

`ip.txt` - Il file contiene i registri derivanti dalla configurazione delle interfacce di rete, inclusi i nomi che possono essere utilizzati nella configurazione delle impostazioni di **Acquisizione pacchetti di rete**.

`NetworkManager_log.txt` - Il file contiene i registri derivanti dal servizio NetworkManager.

`NetworkManager_status.txt` - Il file contiene informazioni sullo stato del servizio NetworkManager.

`openvpn@p2s_log.txt` - Il file contiene i registri derivanti dal servizio OpenVPN.

`openvpn@p2s_status.txt` - Il file contiene informazioni sullo stato dei tunnel VPN.

`ps.txt` - Il file contiene informazioni sui processi attualmente in esecuzione nel gateway VPN o nell'appliance VPN.

`resolf.conf.txt` - Il file contiene informazioni sulla configurazione dei server DNS.

`routes.txt` - Il file contiene informazioni sulle route di networking.

`uname.txt` - Il file contiene informazioni sulla versione corrente del kernel del sistema operativo.

`uptime.txt` - Il file contiene informazioni sulla lunghezza del periodo durante il quale non è avvenuto alcun riavvio del sistema operativo.

`vpnserver_log.txt` - Il file contiene registri derivanti dal servizio VPN.

`vpnserver_status.txt` - Il file contiene informazioni sullo stato del server VPN.

Per ulteriori informazioni sui file di registro specifici per la connessione VPN IPsec, vedere "File di registro della VPN IPsec multisito" (pag. 55).

Scaricare i registri dell'appliance VPN

È possibile scaricare ed estrarre l'archivio che contiene i registri dell'appliance VPN, e utilizzare le informazioni per attività di soluzione dei problemi o di monitoraggio.

Per scaricare i registri dell'appliance VPN

1. Nella pagina **Connessione**, fare clic sull'icona ingranaggio accanto all'appliance VPN.
2. Fare clic su **Scarica registro**.
3. [Facoltativo] Selezionare **Acquisizione pacchetti di rete** e configurare le impostazioni. Per ulteriori informazioni, consultare "Acquisizione di pacchetti di rete" (pag. 52).
4. Fare clic su **Fine**.
5. Non appena l'archivio zip è pronto per il download, fare clic su **Scarica registro** e salvarlo in locale.

Scaricare i registri del gateway VPN

È possibile scaricare ed estrarre l'archivio che contiene i registri del gateway VPN, e utilizzare le informazioni per attività di soluzione dei problemi o di monitoraggio.

Per scaricare i registri del gateway VPN

1. Nella pagina **Connessione**, fare clic sull'icona ingranaggio accanto al gateway VPN.
2. Fare clic su **Scarica registro**.
3. [Facoltativo] Selezionare **Acquisizione pacchetti di rete** e quindi configurare le impostazioni. Per ulteriori informazioni, consultare "Acquisizione di pacchetti di rete" (pag. 52).
4. Fare clic su **Fine**.
5. Non appena l'archivio zip è pronto per il download, fare clic su **Scarica registro** e salvarlo in locale.

Acquisizione di pacchetti di rete

Per risolvere i problemi e analizzare la comunicazione tra il sito di produzione locale e un server primario o di ripristino, è possibile scegliere di acquisire i pacchetti di rete dal gateway VPN o dall'appliance VPN.

Dopo aver raccolto 32.000 pacchetti di rete o raggiunto il limite temporale, l'acquisizione dei pacchetti di rete si arresta e i risultati vengono scritti in un file .libpcap che viene aggiunto all'archivio zip dei registri.

La tabella seguente fornisce più informazioni sulle impostazioni configurabili dall'utente di **Acquisizione pacchetti di rete**.

Impostazione	Descrizione
Nome interfaccia di rete	L'interfaccia di rete sulla quale acquisire i pacchetti di rete. Se si desidera acquisire i pacchetti di rete su tutte le interfacce di rete, selezionare **Qualsiasi**.
Limite di tempo (in secondi)	Il limite di tempo per l'acquisizione dei pacchetti di rete. È possibile impostare un valore massimo di 1.800.
Filtro	Un filtro ulteriore da applicare ai pacchetti di rete acquisiti. È possibile inserire una stringa contenente protocolli, porte, direzioni e le rispettive combinazioni, separate da uno spazio, come: "and", "or", "not", " (", ") ", "src", "dst", "net", "host", "port", "ip", "tcp", "udp", "icmp", "arp" e "esp". Per utilizzare le parentesi, circoscriverle entro spazi. È anche possibile inserire indirizzi IP e indirizzi di rete, ad esempio "icmp or arp" e "port 67 or 68". Per ulteriori informazioni sui valori che è possibile inserire, vedere la guida in linea di Linux tpcdump.

Soluzione dei problemi della configurazione VPN IPsec

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Durante la configurazione o l'utilizzo della connessione VPN IPsec possono verificarsi alcuni problemi.

Ulteriori informazioni sui problemi riscontrati sono disponibili nel file di registro IPsec; è anche possibile consultare l'argomento Soluzione dei problemi di configurazione di VPN IPsec per possibili soluzioni ad alcuni dei problemi più comuni.

Soluzione dei problemi di configurazione di VPN IPsec

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

La tabella seguente illustra i problemi più comuni riscontrati durante la configurazione di VPN IPsec, e indica come risolverli.

Problema	Possibile soluzione
Viene visualizzato il seguente messaggio di errore: **Errore di negoziazione IKE Phase 1. Verificare le impostazioni di IPsec IKE nel cloud e nei siti locali.**	Fare clic su **Riprova** e verificare se viene visualizzato un messaggio di errore più specifico. Ad esempio, un messaggio di errore più specifico può indicare una mancata corrispondenza di un algoritmo o una chiave precondivisa errata. **Nota** Per ragioni di sicurezza, alla connessione VPN IPsec si applicano le seguenti limitazioni: • IKEv1 è stato deprecato in RFC8247 e non è più supportato a causa di rischi alla sicurezza. Sono supportate solo le connessioni con protocollo IKEv2. • I seguenti algoritmi di crittografia non sono considerati sicuri e pertanto non sono supportati: DES e 3DES. • I seguenti algoritmi di hash non sono considerati sicuri e pertanto non sono supportati: SHA1 e MD5. • Il numero 2 dei numeri del gruppo Diffie-Hellman non è considerato sicuro pertanto non è supportato.
La connessione tra il sito locale personale e il sito cloud permane nello stato **Connessione in corso**.	Verificare quanto segue: • Che la porta UDP 500 sia aperta (quando è in uso un firewall). • La connessione tra il sito locale e il sito cloud. • La correttezza dell'indirizzo IP del sito locale.
La connessione tra il sito locale personale e il sito cloud permane nello stato **In attesa di connessione**.	Questo stato è visualizzato quando l'**Azione all'avvio** del sito cloud è impostata su **Aggiungi**, indicando che il sito cloud è in attesa che il sito locale inizializzi la connessione. Inizializzare la connessione dal sito locale.

Problema	Possibile soluzione
La connessione tra il sito locale personale e il sito cloud permane nello stato **In attesa di traffico**.	Questo stato è visualizzato quando l'**Azione all'avvio** del sito cloud è impostata su **Indirizza**. Se si è in attesa della connessione dal sito locale, attenersi alla seguente procedura: • Dal sito locale, provare a effettuare il ping della virtual machine nel sito cloud. Si tratta di un comportamento standard necessario per stabilire un tunnel per alcuni servizi, ad esempio Cisco ASA. Modalità Indirizza • Verificare che il sito locale stabilisca un tunnel impostando l'**Azione all'avvio** del sito locale su **Avvia**.
La connessione tra il sito locale personale e il sito cloud è stabilita, ma uno o più dei criteri di rete non sono attivi.	Questo problema può essere dovuto ai seguenti motivi: • Il mapping di rete nel sito IPsec cloud è differente dal mapping di rete del sito locale. Verificare che i mapping di rete e la sequenza dei criteri di rete nei siti locale e cloud corrispondano in modo esatto. • Questo stato è corretto quando l'**Azione all'avvio** del sito locale e/o del sito cloud è impostata su **Indirizza** (ad esempio, nei dispositivi Cisco ASA), e al momento non è presente alcun traffico. È possibile provare a effettuare il ping per verificare che il tunnel sia stato stabilito. Se il ping non funziona, controllare il mapping di rete nel sito locale e nel sito cloud.
Desidero riavviare una connessione IPsec specifica.	Per riavviare una connessione IPsec specifica: 1. Nella schermata **Disaster Recovery** > **Connessione**, fare clic sulla connessione IPsec. 2. Fare clic su **Disabilita connessione**. 3. Fare di nuovo clic sulla connessione IPsec. 4. Fare clic su **Abilita connessione**.

Download dei file di registro della connessione VPN IPsec

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Ulteriori informazioni sulla connessione IPsec sono disponibili nel file di registro nel server VPN. I file di registro sono compressi in un archivio .zip che è possibile scaricare e decomprimere.

Prerequisiti

La connessione VPN IPsec multisito è configurata.

Per scaricare l'archivio .zip con i file di registro

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Connessione**.
2. Fare clic sull'icona ingranaggio accanto al gateway VPN del sito cloud.
3. Fare clic su **Scarica registro**.
4. Fare clic su **Fine**.
5. Non appena l'archivio zip è pronto per il download, fare clic su **Scarica registro** e salvarlo in locale.

File di registro della VPN IPsec multisito

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

L'elenco seguente descrive i file di registro della VPN IPsec contenuti nell'archivio zip e le informazioni che contengono.

- `ip.txt` - Il file contiene i registri derivanti dalla configurazione delle interfacce di rete. Devono essere visualizzati due indirizzi IP: l'indirizzo IP pubblico e l'indirizzo IP locale. Se nel registro non sono visibili questi due indirizzi IP, c'è un problema. Contattare il team di supporto.

  Nota
  La maschera dell'indirizzo IP pubblico deve essere 32.

- `swanctl-list-loaded-config.txt` - Il file contiene informazioni su tutti i siti IPsec.
  Se nel file non è presente uno dei siti, la configurazione IPsec non è stata applicata. Provare ad aggiornare e a salvare la configurazione, oppure contattare il team di supporto.
- `swanctl-list-active-sas.txt` - Il file contiene le connessioni e i criteri che sono nello stato attivo o in connessione.

Configurazione dei server di ripristino

In questa sezione vengono descritti i concetti di failover e failback, la creazione di un server di ripristino e le operazioni di disaster recovery.

Creazione di un server di ripristino

Per creare un server di ripristino che sarà una copia del workload dell'utente, seguire la procedura descritta di seguito. È anche possibile guardare il video tutorial che mostra il processo.

Importante
Quando si esegue un failover, è possibile selezionare solo punti di ripristino creati dopo la creazione del server di ripristino.

Prerequisiti

- Al sistema originale da proteggere deve essere applicato un piano di protezione. Questo piano deve eseguire il backup dell'intero sistema, o solo dei dischi necessari per l'avvio e per fornire i servizi necessari, in un archivio nel cloud.
- È necessario configurare uno dei tipi di connessione al sito cloud.

Per creare un server di ripristino

1. Nella scheda **Tutti i dispositivi** selezionare il sistema da proteggere.
2. Fare clic su **Disaster Recovery** e quindi su **Crea server di ripristino**.
3. Selezionare il numero di core virtuali e la dimensione della RAM.

   Nota
   Sono visibili i punti di calcolo per ogni opzione. Questo numero riflette il costo orario dell'esecuzione del server di ripristino. Per ulteriori informazioni, consultare "Punti di calcolo" (pag. 12).

4. Specificare la rete cloud alla quale viene connesso il server.
5. Selezionare l'opzione **DHCP**.

Opzione DHCP	Descrizione
Fornito dal sito cloud	Impostazione predefinita. L'indirizzo IP del server verrà fornito da un server DHCP configurato automaticamente nel cloud.
Personalizzato	L'indirizzo IP del server verrà fornito dal server DHCP dell'utente nel cloud.

6. [Facoltativo] Specificare l'**indirizzo MAC**.
   L'indirizzo MAC è un identificatore univoco assegnato alla scheda di rete del server. Se si utilizza un DHCP personalizzato, è possibile configurarlo in modo che assegni sempre uno specifico

indirizzo IP a uno specifico indirizzo MAC. Ciò garantisce che il server di ripristino disponga sempre dello stesso indirizzo IP. È possibile eseguire applicazioni che hanno licenze che sono state registrate con l'indirizzo MAC.

7. Specificare l'indirizzo IP che avrà il server nella rete di produzione. Per impostazione predefinita, viene configurato l'indirizzo IP del sistema originale.

   Nota
   Se si utilizza un server DHCP, aggiungere questo indirizzo IP all'elenco di esclusione del server per evitare che l'indirizzo IP entri in conflitto.
   Se si utilizza un server DHCP personalizzato, è necessario specificare lo stesso indirizzo IP specificato in **Indirizzo IP in rete di produzione** nella configurazione del server DHCP. In caso contrario, il failover di prova non funzionerà correttamente e il server non sarà raggiungibile tramite un indirizzo IP pubblico.

8. [Facoltativo] Selezionare la casella di controllo **Indirizzo IP di prova** e quindi specificare l'indirizzo IP.
   In questo modo sarà possibile eseguire il failover di prova nella rete di prova isolata e connettersi al server di ripristino tramite RDP o SSH durante un failover di prova. Nella modalità failover di prova, il gateway VPN sostituisce l'indirizzo IP di prova con l'indirizzo IP di produzione utilizzando il protocollo NAT.
   Se la casella di controllo non è selezionata, per accedere al server durante un failover di prova sarà possibile utilizzare esclusivamente la console.

   Nota
   Se si utilizza un server DHCP, aggiungere questo indirizzo IP all'elenco di esclusione del server per evitare che l'indirizzo IP entri in conflitto.

   È possibile selezionare uno degli indirizzi IP proposti oppure digitarne uno differente.

9. [Facoltativo] Selezionare la casella di controllo **Accesso Internet**.
   In questo modo il server di ripristino potrà accedere a Internet durante un failover reale o di prova. Per impostazione predefinita, la porta TCP 25 è aperta per le connessioni in uscita verso gli indirizzi IP pubblici.
10. [Facoltativo] Impostare la **Soglia RPO**.
    La soglia RPO definisce l'intervallo di tempo massimo consentito tra l'ultimo punto di ripristino idoneo per un failover e l'ora corrente. È possibile impostare il valore tra 15–60 minuti, 1–24 ore, 1–14 giorni.
11. [Facoltativo] Selezionare la casella di controllo **Utilizza indirizzo IP pubblico**.
    Se dispone di un indirizzo IP pubblico, il server di ripristino è disponibile anche da Internet durante un failover reale o di prova. Se la casella di controllo non è selezionata, il server sarà disponibile solo nella rete di produzione.
    L'opzione **Utilizza indirizzo IP pubblico** richiede l'abilitazione dell'opzione **Accesso Internet**.

L'indirizzo IP pubblico verrà visualizzato dopo aver completato la configurazione. Per impostazione predefinita, la porta TCP 443 è aperta per le connessioni in entrata verso gli indirizzi IP pubblici.

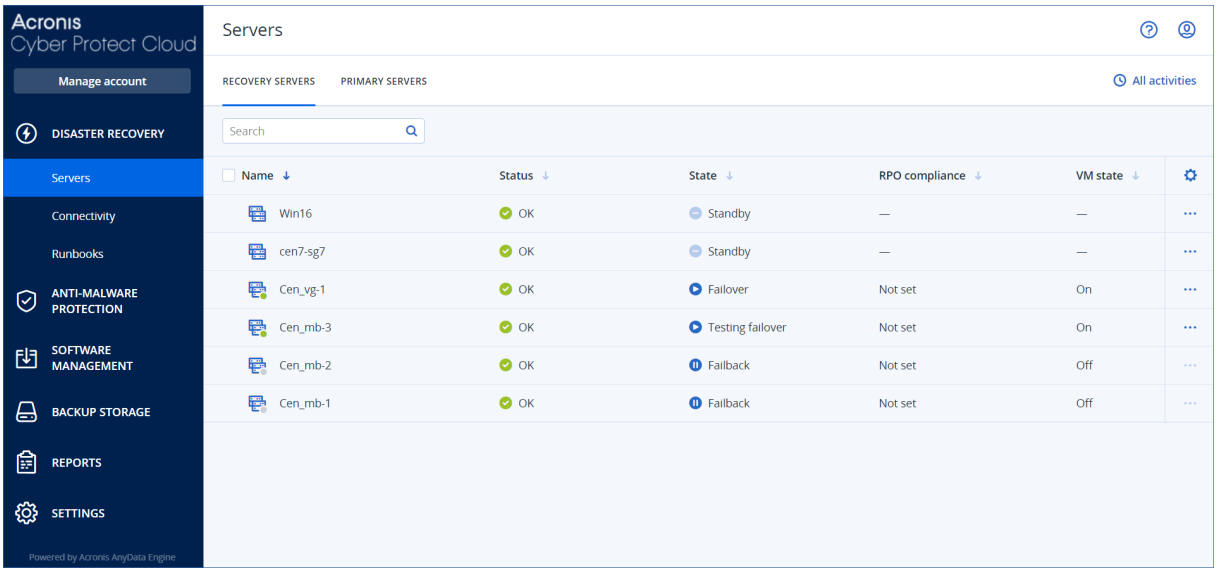
Nota
Se si deseleziona la cartella di controllo **Utilizza indirizzo IP pubblico** o si elimina il server di ripristino, il relativo indirizzo IP pubblico non viene riservato.

12. [Facoltativo] [Se i backup del sistema selezionato sono crittografati utilizzando la crittografia come proprietà del sistema], specificare la password che verrà automaticamente utilizzata al momento della creazione della virtual machine per il server di ripristino a partire dal backup crittografato.
    a. Fare clic su **Specificare**, quindi inserire la password per il backup crittografato e definire un nome per le credenziali.
       Per impostazione predefinita nell'elenco viene visualizzato il backup più recente.
    b. [Facoltativo] Per visualizzare tutti i backup, selezionare **Mostra tutti i backup**.
    c. Fare clic su **Fine**.

Nota
Poiché la password specificata viene archiviata in un archivio di credenziali sicuro, il salvataggio delle password potrebbe generare un conflitto con gli obblighi di conformità.

13. [Facoltativo] Modificare il nome del server di ripristino.
14. [Facoltativo] Immettere una descrizione per il server di ripristino.
15. [Facoltativo] Fare clic sulla scheda **Regole del firewall cloud** per modificare le regole predefinite del firewall. Per ulteriori informazioni, consultare "Impostazione delle regole del firewall per server cloud" (pag. 85).
16. Fare clic su **Crea**.

Il server di ripristino viene visualizzato nella scheda **Disaster Recovery** > **Server** > **Server di ripristino** della console di Cyber Protect. È anche possibile visualizzarne le impostazioni selezionando il sistema originale e facendo clic su **Disaster Recovery**.



Funzionamento del processo di failover

Failover di produzione

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Dal momento della creazione, un server di ripristino rimane in modalità **Standby**. La virtual machine corrispondente non esiste fino a quando non viene avviato il failover. Prima di avviare un processo di failover, è necessario creare almeno un backup dell'immagine del disco (con volume avviabile) del sistema originale.

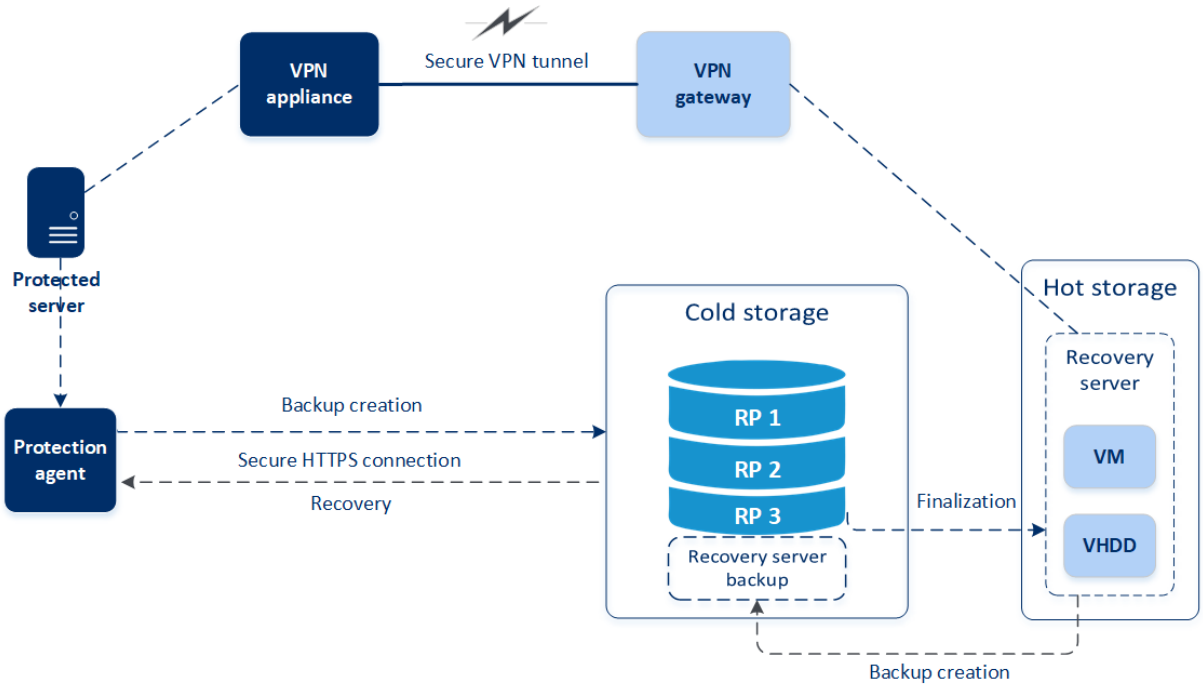
All'avvio del processo di failover, selezionare il punto di ripristino (backup) del sistema originale dal quale verrà creata la virtual machine con i parametri predefiniti. L'operazione di failover utilizza la funzionalità di esecuzione della macchina virtuale da un backup. Il server di ripristino entra nello stato di transizione denominato **Finalizzazione**. Il processo implica il trasferimento dei dischi virtuali del server dallo storage di backup (storage ad accesso infrequente) allo storage di disaster recovery (storage ad accesso frequente).

Nota
Durante la **Finalizzazione**, il server è accessibile e funzionale, sebbene con prestazioni inferiori al normale. È possibile aprire la console del server facendo clic sul link **La console è pronta**. Il link è disponibile nella colonna **Stato VM** della schermata **Disaster Recovery** > **Server**, e nella vista **Dettagli** del server.

Una volta completata la **Finalizzazione**, le prestazioni del server torneranno alla normalità. Lo stato del server passa a **Failover**. Il workload viene trasferito dal sistema originale al server di ripristino nel sito cloud.

Se il server di ripristino include un agente di protezione, il servizio agente viene arrestato per evitare interferenze, ad esempio l'avvio di un backup o la creazione di report di stato non aggiornati nel componente di backup.

Il diagramma sottostante mostra i processi di failover e failback.



Prova failover

Durante un **failover di prova**, la macchina virtuale non viene finalizzata. Ciò significa che l'agente legge il contenuto dei dischi virtuali direttamente dal backup, ovvero accede in modo casuale alle varie parti del backup; per questa ragione le prestazioni dell'agente potrebbero essere inferiori rispetto a quelle normali. Per ulteriori informazioni sul processo di failover di prova, fare riferimento a "Esecuzione di un failover di prova" (pag. 60).

Failover di prova automatizzato

Quando è configurato il failover di prova automatizzato, questo viene eseguito una volta al mese, senza interazione manuale. Per ulteriori informazioni, consultare "Failover di prova automatizzato" (pag. 63) e "Configurazione del failover di prova automatizzato" (pag. 63).

Esecuzione di un failover di prova

Eseguire un failover di prova significa avviare un server di ripristino in una VLAN di prova che è isolata rispetto alla rete di produzione. È possibile sottoporre a prova diversi server di ripristino alla volta e controllarne le interazioni. Nella rete di prova, i server comunicano tramite i propri indirizzi IP di produzione, ma non possono inizializzare le connessioni TCP o UDP ai workload della rete locale.

Durante un failover di prova, la virtual machine (server di ripristino) non viene finalizzata. L'agente legge il contenuto dei dischi virtuali direttamente dal backup e accede in modo casuale alle varie componenti del backup. Ciò può rallentare le prestazioni del server di ripristino nello stato di failover di prova rispetto alle prestazioni normali.

Sebbene il failover di prova sia un'attività facoltativa, è consigliabile eseguirla con regolarità, scegliendo la frequenza più idonea in termini di costi e sicurezza. Una procedura raccomandata è la creazione di un runbook, ovvero un insieme di istruzioni che descrive come allestire l'ambiente di produzione nel cloud.

Importante
È necessario creare un server di ripristino in anticipo, per proteggere i dispositivi da situazioni di emergenza.

È possibile eseguire il failover solo da punti di ripristino creati dopo la creazione del server di ripristino del dispositivo.

È necessario creare almeno un punto di ripristino prima che sia possibile eseguire il failover su un server di ripristino. Il numero massimo di punti di ripristino supportati è 100.

Per eseguire un failover di prova

1. Selezionare il sistema originale o il server di ripristino da sottoporre a prova.
2. Fare clic su **Disaster Recovery**.
   Viene visualizzata la descrizione del server di ripristino.
3. Fare clic su **Failover**.
4. Selezionare il tipo di failover **Prova failover**.
5. Selezionare il punto di ripristino (backup) e fare clic su **Avvia**.
6. Se il backup selezionato è crittografato utilizzando la crittografia come proprietà del sistema:
   a. Inserire la password di crittografia per il set di backup.

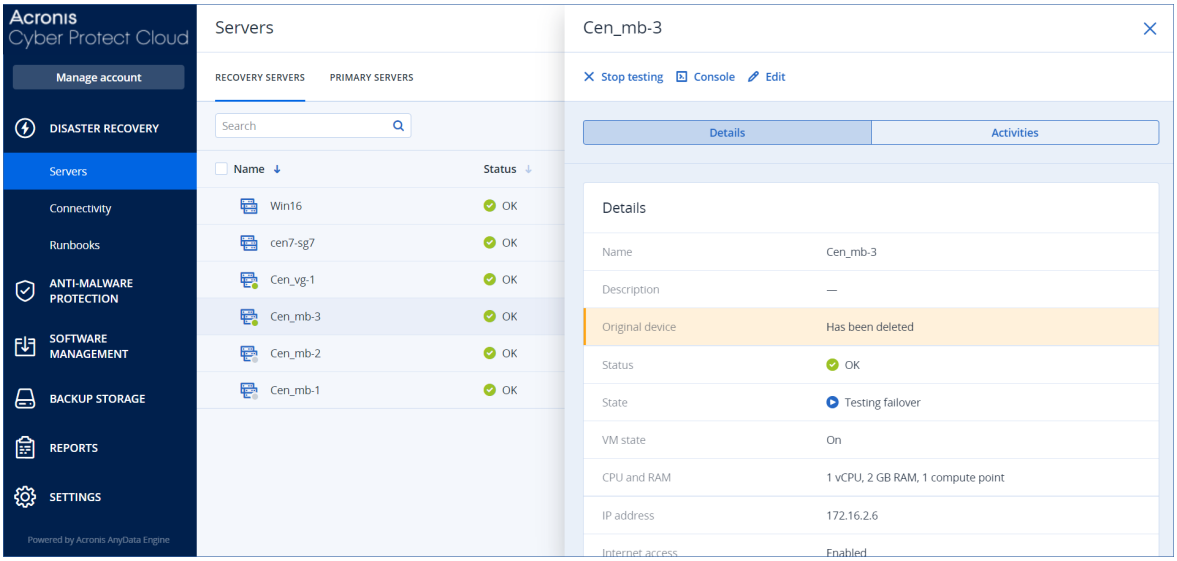
      Nota
      La password viene salvata solo temporaneamente e utilizzata solo per l'operazione di failover di prova corrente. La password viene automaticamente eliminata dall'archivio delle credenziali se il failover di prova viene interrotto o completato.

   b. [Facoltativo] Per salvare la password per il set di backup e utilizzarla nelle operazioni di failover successive, selezionare la casella di controllo **Archivia la password in un archivio delle credenziali protetto...** e, nel campo **Nome credenziali**, inserire un nome per le credenziali.

Importante
La password verrà archiviata in un archivio delle credenziali protetto e verrà applicata automaticamente nelle successive operazioni di failover. Tenere presente che il salvataggio delle password potrebbe generare un conflitto con gli obblighi di conformità.

c. Fare clic su **Fine**.

All'avvio del server di ripristino, lo stato passa a **Prova failover in corso**.



7. Verificare il funzionamento del server di ripristino con uno dei metodi seguenti:
   - In **Disaster Recovery** > **Server**, selezionare il server di ripristino e quindi fare clic su **Console**.
   - Eseguire la connessione al server di ripristino tramite RDP o SSH e l'indirizzo IP di prova specificato al momento della creazione del server stesso. Provare la connessione dall'interno e dall'esterno della rete di produzione, come descritto in "Connessione da punto a sito".
   - Eseguire uno script nel server di ripristino.
     Lo script può verificare la schermata di accesso, l'avvio corretto delle applicazioni, la connessione a Internet e la capacità degli altri sistemi di connettersi al server di ripristino.
   - Se il server di ripristino può accedere a Internet e a un indirizzo IP pubblico, è possibile utilizzare TeamViewer.
8. Una volta completata la prova, fare clic su **Interrompi test**.
   Il server di ripristino si arresta. Tutte le modifiche apportare al server di ripristino durante il failover di prova non vengono conservate.

Nota
Le azioni **Avvia server** e **Arresta server** non sono applicabili alle operazioni di failover di prova, sia nei runbook sia quando si avvia manualmente un failover di prova. Se si tenta di eseguire questo tipo di azione, questa non avrà esito positivo e si riceverà il seguente messaggio di errore:
Non riuscita: L'azione non è applicabile allo stato del server corrente.

Failover di prova automatizzato

Con il failover di prova automatizzato, il server di ripristino viene testato automaticamente una volta al mese, senza interazione manuale.

Il failover di prova automatizzato consiste delle parti seguenti:

1. creare una virtual machine dall'ultimo punto di ripristino
2. acquisire uno screenshot della virtual machine
3. analizzare se il sistema operativo della virtual machine si avvia in modo corretto
4. inviare una notifica sullo stato del failover di prova

Nota
Il failover di prova automatizzato consuma dei punti di calcolo.

È possibile configurare il failover di prova automatizzato nelle impostazioni del server di ripristino. Per ulteriori informazioni, consultare "Configurazione del failover di prova automatizzato" (pag. 63).

Tenere presente che in rari casi, il failover di prova automatizzato può essere ignorato e potrebbe non essere come pianificato. Ciò accade perché il failover di produzione ha una priorità più elevata rispetto al failover di prova automatizzato, perciò le risorse hardware (CPU e RAM) allocate al failover di prova potrebbero essere temporaneamente limitate per garantire che ci siano sufficienti risorse per eseguire simultaneamente un failover di produzione.

Se, per qualsiasi motivo, un failover di prova viene ignorato, viene visualizzato un avviso.

Nota
Il failover del test automatizzato non riesce se i backup del sistema originale sono crittografati utilizzando la crittografia come proprietà del sistema, e la password di crittografia non è specificata durante la creazione del server di ripristino. Per ulteriori informazioni su come specificare la password di crittografia, consultare "Creazione di un server di ripristino" (pag. 56).

Configurazione del failover di prova automatizzato

Configurando un failover di prova automatizzato è possibile provare il server di ripristino ogni mese, senza eseguire alcuna azione manuale.

Per configurare il failover di prova automatizzato

1. Nella console, passare a **Disaster Recovery** > **Server** > **Server di ripristino** e selezionare il server di ripristino.
2. Fare clic su **Modifica**.
3. Nella sezione **Failover di prova automatizzato**, nel campo **Pianificazione**, selezionare **Ogni mese**.

4. [Facoltativo] In **Timeout screenshot**, modificare il valore predefinito del periodo di tempo massimo (in minuti) entro il quale il sistema tenta l'esecuzione del failover di prova automatizzato.
5. [Facoltativo] Per salvare il valore **Timeout screenshot** come predefinito e compilarlo in modo automatico quando viene abilitato il failover di prova automatizzato per gli altri server di ripristino, selezionare **Imposta come timeout predefinito**.
6. Fare clic su **Salva**.

Visualizzazione dello stato del failover di prova automatizzato

È possibile visualizzare i dettagli di un failover di prova automatizzato completato, come stato, ora di inizio, ora di fine, durata, e lo screenshot della virtual machine.

Per visualizzare lo stato del failover di prova automatizzato di un server di ripristino

1. Nella console, passare a **Disaster Recovery** > **Server** > **Server di ripristino** e selezionare il server di ripristino.
2. Nella sezione **Failover di prova automatizzato**, controllare i dettagli dell'ultimo failover di prova automatizzato.
3. [Facoltativo] Dare clic su **Mostra screenshot** per visualizzare lo screenshot della virtual machine.

Disabilitazione del failover di prova automatizzato

È possibile disabilitare il failover di prova automatizzato per risparmiare risorse o se non è necessario eseguire il failover di prova automatizzato per un determinato server di ripristino.

Per disabilitare il failover di prova automatizzato

1. Nella console, passare a **Disaster Recovery** > **Server** > **Server di ripristino** e selezionare il server di ripristino.
2. Fare clic su **Modifica**.
3. Nella sezione **Failover di prova automatizzato**, nel campo **Pianificazione**, selezionare **Mai**.
4. Fare clic su **Salva**.

Esecuzione di un failover

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Il failover è il processo tramite il quale un carico di lavoro locale viene archiviato nel cloud. Il termine definisce anche lo stato del carico di lavoro che rimane nel cloud.

Quando si avvia un failover, il server di ripristino viene avviato nella rete di produzione. Per evitare interferenze e problemi imprevisti, verificare che il workload originale non sia online e che non sia possibile accedervi tramite VPN.

Per evitare l'interferenza del backup nello stesso archivio cloud, revocare manualmente il piano di protezione dal workload che è attualmente nello stato **Failover**. Per ulteriori informazioni su come revocare i piani, vedere Revoca di un piano di protezione.

Importante
È necessario creare un server di ripristino in anticipo, per proteggere i dispositivi da situazioni di emergenza.

È possibile eseguire il failover solo da punti di ripristino creati dopo la creazione del server di ripristino del dispositivo.

È necessario creare almeno un punto di ripristino prima che sia possibile eseguire il failover su un server di ripristino. Il numero massimo di punti di ripristino supportati è 100.

È possibile attenersi alle istruzioni seguenti o guardare il tutorial video.

Per eseguire un failover

1. Verificare che il sistema originale non sia disponibile in rete.
2. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Server** > **Server di ripristino** e selezionare il server di ripristino.
3. Fare clic su **Failover**.
4. Selezionare il tipo di failover **Failover di produzione**.
5. Selezionare il punto di ripristino (backup) e fare clic su **Avvia**.
6. [Se il backup selezionato è crittografato utilizzando la crittografia come proprietà del sistema]
   a. Inserire la password di crittografia per il set di backup.

      Nota
      La password viene salvata temporaneamente e utilizzata solo per l'operazione di failover corrente. La password viene automaticamente eliminata dall'archivio delle credenziali una volta completata l'operazione di failover e non appena il server torna nello stato di **standby**.

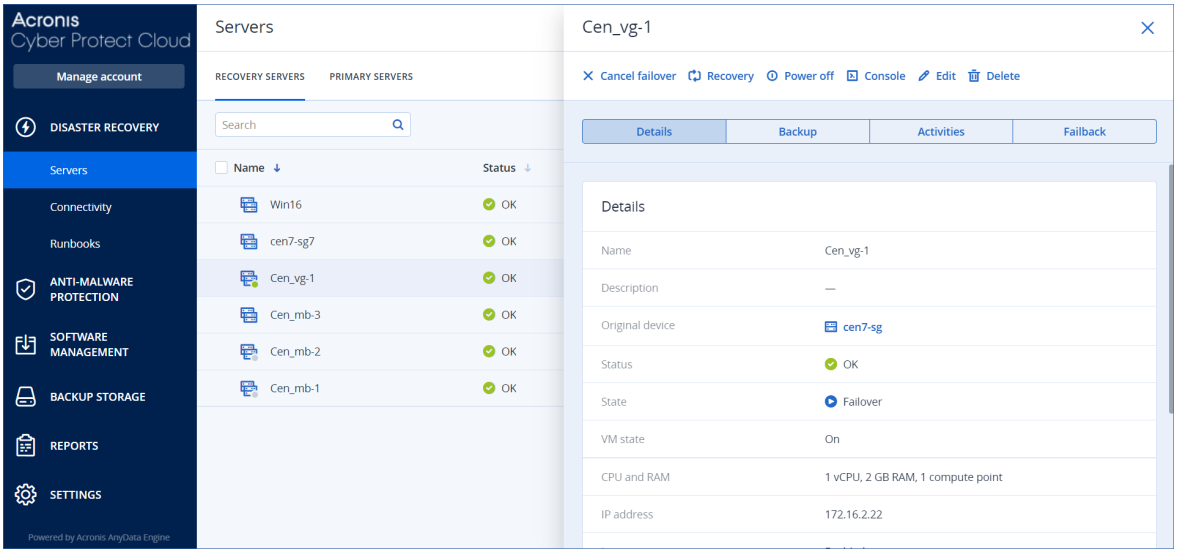
   b. [Facoltativo] Per salvare la password per il set di backup e utilizzarla nelle operazioni di failover successive, selezionare la casella di controllo **Archivia la password in un archivio delle credenziali protetto...** e, nel campo **Nome credenziali**, inserire un nome per le credenziali.

      Importante
      La password verrà archiviata in un archivio delle credenziali protetto e verrà applicata automaticamente nelle successive operazioni di failover. Tenere presente che il salvataggio delle password potrebbe generare un conflitto con gli obblighi di conformità.

   c. Fare clic su **Fine**.

   All'avvio del server di ripristino, lo stato passa a **Finalizzazione**, e dopo qualche tempo a **Failover**.

Importante
È fondamentale comprendere che il server è disponibile sia nello stato **Finalizzazione** che nello stato **Failover**. Durante la **Finalizzazione**, il server è accessibile facendo clic sul link **La console è pronta**. Il link è disponibile nella colonna **Stato VM** della schermata **Disaster Recovery** > **Server**, e nella vista **Dettagli** del server. Per ulteriori dettagli, consultare "Funzionamento del processo di failover" (pag. 59).



7. Verificare che il server di ripristino sia avviato visualizzandone la console. Fare clic su **Disaster Recovery** > **Server**, selezionare il server di ripristino e quindi fare clic su **Console**.
8. Verificare che sia possibile accedere al server di ripristino utilizzando l'indirizzo IP di produzione specificato al momento della creazione del server stesso.

Dopo la finalizzazione del server di ripristino, viene automaticamente creato un nuovo piano di protezione, che sarà applicato al server. Tale piano di protezione si basa sul piano di protezione utilizzato per la creazione del server di ripristino, pur se con alcune limitazioni: Del piano, ad esempio, è possibile modificare solo la pianificazione e le regole di conservazione. Per ulteriori informazioni, fare riferimento a "Backup dei server cloud".

Se si desidera annullare il failover, selezionare il server di ripristino e fare clic su **Annulla failover**. Tutte le modifiche apportate a partire dal momento del failover andranno perse, ad eccezione dei backup del server di ripristino. Il server di ripristino ritornerà in stato di **Standby**.

Se si desidera eseguire il failback, selezionare il server di ripristino e fare clic su **Failback**.

Come eseguire il failover di server utilizzando il server DNS locale

Se nel sito locale vengono utilizzati i server DNS per la risoluzione dei nomi dei sistemi, successivamente a un failover i server di ripristino corrispondenti ai sistemi che si affidano al server DNS non riusciranno a comunicare, perché i server DNS utilizzati nel cloud sono diversi. Per impostazione predefinita, i server DNS del sito cloud vengono utilizzati per i server cloud appena

creati. Nel caso in cui sia necessario applicare impostazioni DNS personalizzate, contattare il supporto tecnico.

Come eseguire il failover di un server DHCP

Nell'infrastruttura locale, il server DHCP può essere collocato su un host Windows o Linux. Quando viene eseguito il failover di questo host nel sito cloud, si verifica un problema di duplicazione del server DHCP, perché anche il gateway VPN nel cloud esegue il ruolo DHCP. Per risolvere il problema, eseguire una delle seguenti operazioni:

- Se è stato eseguito solo il failover dell'host DHCP nel cloud, mentre i server locali rimanenti sono ancora nel sito locale, è necessario accedere all'host DHCP nel cloud e disattivare il server DHCP ospitato. In questo modo non si avranno conflitti e solo il gateway VPN funzionerà come server DHCP.
- Se i server cloud hanno già ottenuto gli indirizzi IP dall'host DHCP, è necessario accedere all'host DHCP nel cloud e disattivare il server DHCP ospitato.È necessario accedere ai server cloud e rinnovare l'assegnazione DHCP per assegnare i nuovi indirizzi IP allocati dal server DHCP corretto ospitato nel gateway VPN.

Nota
Le istruzioni non sono valide quando il server DHCP nel cloud è configurato con l'opzione **DHCP personalizzato** e alcuni dei server di ripristino o primari ottengono il proprio indirizzo IP da questo server DHCP.

Funzionamento del processo di failback

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Il failback è il processo con il quale un workload archiviato nel cloud viene riportato in un sistema fisico o in una virtual machine nel sito locale. È possibile eseguire il failback in un server di ripristino nello stato di **Failover**, e continuare a utilizzare il server nel sito locale.

È possibile eseguire il failover automatizzato in un sistema di destinazione fisico o virtuale nel sito locale. Durante il processo di failback, è possibile trasferire i dati di backup nel sito locale mentre la virtual machine nel cloud resta in esecuzione. Questa tecnologia aiuta a ridurre nettamente l'interruzione operativa, la cui durata prevista è visualizzata nella console di Cyber Protect. L'informazione può essere visualizzata e utilizzata per pianificare le tempistiche e, se necessario, per avvisare i clienti del previsto e imminente periodo di inattività.

I processi di failback su un sistema fisico di destinazione e su una virtual machine di destinazione sono lievemente differenti. Per ulteriori informazioni sulle fasi del processo di failback, fare riferimento a "Failback in una virtual machine di destinazione" (pag. 68) e "Failback in un sistema fisico di destinazione" (pag. 73).

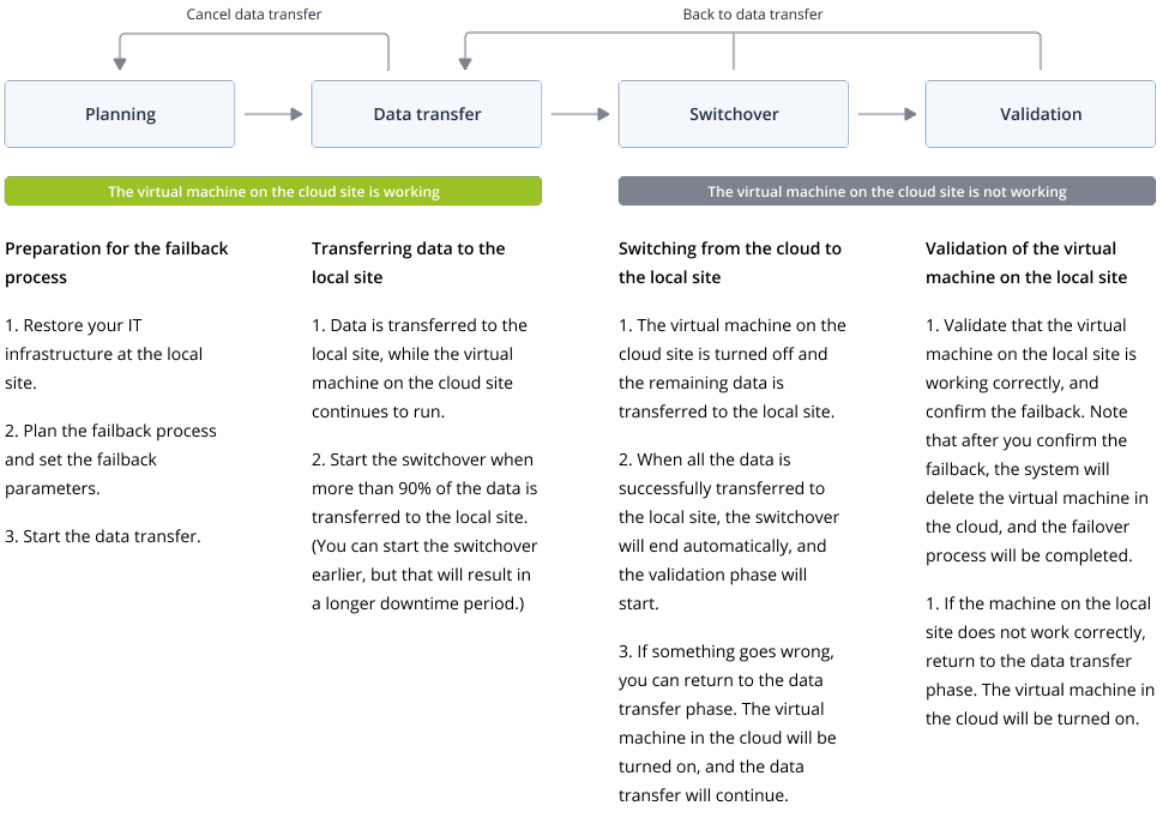
In alcuni casi specifici in cui non è possibile utilizzare la procedura di failback automatizzato, è possibile eseguire un failback manuale. Per ulteriori informazioni, consultare "Failback manuale" (pag. 76).

Nota
Le operazioni runbook supportano solo il failback in modalità manuale. Ciò significa che se si avvia il processo di failback eseguendo un runbook che include il passaggio **Esegui il failback del server**, la procedura richiederà un'interazione manuale: sarà necessario ripristinare manualmente il sistema, e confermare o annullare il processo di failback dalla scheda **Disaster Recovery** > **Server**.

Failback in una virtual machine di destinazione

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Il processo di failback in una virtual machine di destinazione è costituito da quattro fasi.



1. **Pianificazione**. Durante questa fase si esegue il ripristino dell'infrastruttura IT nel sito locale, ad esempio degli host e delle configurazioni di rete, si configurano i parametri di failback e si pianifica quando avviare il trasferimento dei dati.

Nota
Per ridurre al minimo il tempo totale del processo di failback, si consiglia di avviare la fase di trasferimento dei dati subito dopo aver configurato i server locali, e di proseguire quindi con la configurazione della rete e del resto dell'infrastruttura locale nel corso della fase di trasferimento dei dati.

2. **Trasferimento dei dati**. Durante questa fase i dati vengono trasferiti dal sito cloud al sito locale, mentre la virtual machine nel cloud resta in esecuzione. È possibile avviare la fase successiva (lo switchover) in qualsiasi momento durante la fase del trasferimento dei dati, ma occorre tenere presente quanto segue.

   Più tempo si rimane nella fase di trasferimento dei dati,
   - più a lungo la virtual machine nel cloud resta in esecuzione;
   - più dati verranno trasferiti nel sito locale;
   - più elevato sarà il costo che verrà addebitato (si consumano infatti più punti di calcolo);
   - minore il periodo di interruzione operativa che si sperimenta durante la fase di switchover.

   Per ridurre al minimo l'interruzione operativa, avviare la fase di switchover dopo aver trasferito oltre il 90% dei dati nel sito locale.

   Se è possibile tollerare un periodo di interruzione operativa più lungo e non si desidera utilizzare ulteriori punti di calcolo per l'esecuzione della virtual machine nel cloud, è possibile anticipare la fase di switchover.

   Se il processo di failback viene annullato durante la fase di trasferimento dei dati, i dati trasferiti non verranno eliminati dal sito locale. Per evitare potenziali problemi, cancellare manualmente i dati trasferiti prima di avviare un nuovo processo di failback. Il successivo processo di trasferimento dei dati si avvierà dall'inizio.
3. **Switchover**. Durante questa fase la virtual machine nel cloud viene disattivata e i dati rimanenti, incluso l'ultimo incremento di backup, vengono trasferiti nel sito locale. Se al server di ripristino non è stato applicato alcun piano di backup, verrà automaticamente eseguito un backup durante la fase di switchover; ciò potrebbe rallentare il processo.

   Nella console di Cyber Protect è visibile il tempo stimato (periodo di interruzione operativa) prima del termine di questa fase. Quando tutti i dati sono stati trasferiti nel sito locale (non c'è alcuna perdita di dati e la virtual machine nel sito locale è una copia esatta della virtual machine nel cloud) la fase di switchover è considerata completa. La virtual machine nel sito locale viene ripristinata e la fase di convalida si avvia in automatico.
4. **Convalida**. Durante questa fase, la virtual machine nel sito locale è pronta e viene avviata automaticamente. È possibile verificare il corretto funzionamento della virtual machine e:
   - Se tutto funziona come previsto, confermare il failback. Dopo la conferma, la virtual machine nel cloud viene eliminata e il server di ripristino torna nello stato di **Standby**. Questa è l'ultima fase del processo di failback.
   - Se qualcosa non ha funzionato come previsto, è possibile annullare lo switchover e tornare alla fase di trasferimento dei dati.

Esecuzione del failback in una virtual machine

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

È possibile eseguire il failback in una virtual machine di destinazione nel sito locale.

Prerequisiti

- L'agente che verrà utilizzato per eseguire il failback è online e al momento non è impiegato in un'altra operazione di failback.
- La connessione Internet è stabile.
- Nel cloud è presente almeno un backup completo della virtual machine.

Per eseguire il failback in una virtual machine

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Server**.
2. Selezionare il server di ripristino che si trova nello stato di **Failover**.
3. Fare clic sulla scheda **Failback**.
4. Nella sezione **Parametri di failback**, selezionare **Macchina virtuale** come **Destinazione** e configurare gli altri parametri.
   Per impostazione predefinita, alcuni dei **Parametri di failback** vengono compilati automaticamente con i valori suggeriti, ma è possibile modificarli.
   La tabella seguente fornisce più informazioni sui **Parametri di failback**.

Parametro	Descrizione
Dimensioni backup	La quantità di dati che verranno trasferiti al sito locale durante il processo di failback. Dopo l'avvio del processo di failback in una virtual machine di destinazione, la **Dimensioni backup** aumenterà durante la fase di trasferimento dei dati, perché la virtual machine nel cloud resta in esecuzione e continua a generare nuovi dati. Per calcolare il periodo stimato di interruzione operativa durante il processo di failback in una virtual machine di destinazione, prendere il 10% del valore della **Dimensioni backup** (come già raccomandato, la fase di switchover deve essere avviata dopo che il 90% dei dati è stato trasferito al sito locale), e dividerlo per il valore della velocità di Internet. **Nota** Il valore della velocità di Internet diminuisce quando vengono eseguiti più processi di failback alla volta.
Destinazione	Il tipo di workload nel sito locale nel quale verrà ripristinato il server cloud: **Macchina virtuale** o **Macchina fisica**.

Parametro	Descrizione
Posizione del sistema di destinazione	Posizione del failback: un host VMware ESXi o un host Microsoft Hyper-V. È possibile scegliere tra tutti gli host che dispongono di un agente registrato nel servizio Cyber Protection.
Agente	L'agente che eseguirà l'operazione di failback. È possibile utilizzare un agente per eseguire un'operazione di failback a volta. L'agente selezionato non deve essere impiegato da un altro processo di failback, deve essere online, far parte di una versione che supporta la funzionalità di failback e disporre dei permessi di accesso al backup. È possibile installare più agenti sugli host VMware ESXi e avviare un processo di failback distinto utilizzando ognuno di essi. Questi processi di failback possono essere eseguiti in contemporanea.
Impostazioni del sistema di destinazione	Impostazioni della virtual machine: • **Processori virtuali**. Selezionare il numero di processori virtuali. • **Memoria**. Selezionare la quantità di memoria di cui disporrà la virtual machine. • **Unità**. Selezionare le unità per la memoria. • [Facoltativo] **Schede di rete**. Per aggiungere una scheda di rete, fare clic su **Aggiungi** e selezionare una rete nel campo **Rete**. Dopo aver completato la modifica, fare clic su **Fine**.
Percorso	(Per gli host Microsoft Hyper-V) La cartella nell'host in cui verrà archiviato il sistema. Verificare che lo spazio di memoria disponibile sull'host sia sufficiente per il sistema.
Datastore	(Per gli host VMware ESXi) Il datastore nell'host in cui verrà archiviato il sistema. Verificare che lo spazio di memoria disponibile sull'host sia sufficiente per il sistema.
Modalità di provisioning	Metodo di allocazione del disco virtuale. Per host Microsoft Hyper-V: • **Espansione dinamica** (valore predefinito). • **Dimensione fissa**. Per host Microsoft Hyper-V: • **Thin** (valore predefinito). • **Thick**.
Nome del sistema di destinazione	Nome del sistema di destinazione. Per impostazione predefinita, il nome del sistema di destinazione è lo stesso del nome del server di ripristino. Il nome del sistema di destinazione deve essere univoco per la **Posizione del sistema di destinazione** selezionata.

5. Fare clic su **Avvia trasferimento dei dati**, e nella finestra di conferma fare clic di nuovo su **Avvia**.

   Nota
   Se nel cloud non esiste un backup della virtual machine, il sistema esegue automaticamente un backup prima della fase di trasferimento dei dati.

   Viene avviata la fase di **Trasferimento dei dati**. La console visualizza le seguenti informazioni:

Campo	Descrizione
Avanzamento	Questo parametro mostra quanti dati sono stati già trasferiti nel sito locale, e la quantità totale di dati che devono essere ancora trasferiti. La quantità totale di dati include i dati dell'ultimo backup eseguito prima dell'avvio della fase di trasferimento dei dati, e i backup dei dati generati di recente (incrementi di backup), perché la virtual machine resta in esecuzione durante la fase di trasferimento dei dati. Per questa ragione, entrambi i valori del parametro **Avanzamento** aumentano nel tempo.
Stima del tempo di inattività	Questo parametro mostra per quanto tempo la virtual machine nel cloud non sarà disponibile se la fase di switchover viene avviata immediatamente. Il valore è calcolato in base ai valori del parametro **Avanzamento**, e diminuisce con il tempo.

6. Fare clic su **Switchover** e, nella finestra di conferma, fare clic di nuovo su **Switchover**.
   Sia avvia la fase di switchover. La console visualizza le seguenti informazioni:

Campo	Descrizione
Avanzamento	Questo parametro mostra l'avanzamento del ripristino del sistema nel sito locale.
Tempo stimato al termine	Questo parametro mostra il tempo stimato per il completamento della fase di switchover, dopo la quale sarà possibile avviare il sistema nel sito locale.

   Nota
   Se alla virtual machine nel cloud non è stato applicato alcun piano di backup, verrà automaticamente eseguito un backup durante la fase di switchover, e ciò potrebbe causare un'interruzione operativa più lunga.

7. Al completamento della fase di **switchover** la virtual machine nel sito locale viene avviata automaticamente. Verificare che funzioni come previsto.
8. Fare clic su **Conferma failback**, e nella finestra di conferma fare clic di nuovo su **Conferma** per finalizzare il processo.
   La virtual machine nel cloud viene eliminata e il server di ripristino torna nello stato di **Standby**.

Nota
L'operazione di applicazione di un piano di protezione al server ripristinato non fa parte del processo di failback. Una volta completato il processo di failback, applicare un piano di protezione al server ripristinato per assicurarsi che sia di nuovo protetto. È possibile applicare lo stesso piano di protezione che è stato applicato al server originario, oppure un nuovo piano di protezione per il quale sia abilitato il modulo **Disaster Recovery**.

Failback in un sistema fisico di destinazione

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Il processo di failback automatizzato in un sistema fisico di destinazione consiste delle fasi seguenti:

1. **Pianificazione**. Durante questa fase si esegue il ripristino dell'infrastruttura IT nel sito locale, ad esempio degli host e delle configurazioni di rete, si configurano i parametri di failback e si pianifica quando avviare il trasferimento dei dati.
2. **Trasferimento dei dati**. Durante questa fase i dati vengono trasferiti dal sito cloud al sito locale, mentre la virtual machine nel cloud resta in esecuzione. È possibile avviare la fase successiva (lo switchover) in qualsiasi momento durante la fase del trasferimento dei dati, ma occorre tenere presente quanto segue.

   Più tempo si rimane nella fase di trasferimento dei dati,
   - più a lungo la virtual machine nel cloud resta in esecuzione;
   - più dati verranno trasferiti nel sito locale;
   - più elevato sarà il costo che verrà addebitato (si consumano infatti più punti di calcolo);
   - minore il periodo di interruzione operativa che si sperimenta durante la fase di switchover.

   Per ridurre al minimo l'interruzione operativa, avviare la fase di switchover dopo aver trasferito oltre il 90% dei dati nel sito locale.

   Se è possibile tollerare un periodo di interruzione operativa più lungo e non si desidera utilizzare ulteriori punti di calcolo per l'esecuzione della virtual machine nel cloud, è possibile anticipare la fase di switchover.

   Nota
   Il processo di trasferimento dei dati si avvale di una tecnologia flashback. Tale tecnologia confronta i dati disponibili sul sistema di destinazione con quelli della virtual machine nel cloud. Se parte dei dati è già disponibile nel sistema di destinazione, tali dati non verranno trasferiti di nuovo. La tecnologia accelera quindi la fase di trasferimento dei dati.

   Per questo motivo si consiglia di ripristinare il server nel sistema originale nel sito locale.

3. **Switchover**. Durante questa fase la virtual machine nel cloud viene disattivata e i dati rimanenti, incluso l'ultimo incremento di backup, vengono trasferiti nel sito locale. Se al server di ripristino

non è stato applicato alcun piano di backup, verrà automaticamente eseguito un backup durante la fase di switchover; ciò potrebbe rallentare il processo.

4. **Convalida**. Durante questa fase, il sistema fisico nel sito locale è pronto ed è possibile riavviarlo utilizzando un supporto di avvio Linux. È possibile verificare il corretto funzionamento della virtual machine e:
   - Se tutto funziona come previsto, confermare il failback. Dopo la conferma, la virtual machine nel cloud viene eliminata e il server di ripristino torna nello stato di **Standby**. Questa è l'ultima fase del processo di failback.
   - Se qualcosa non ha funzionato come previsto, è possibile annullare il failover e tornare alla fase di pianificazione.

   Nota
   Una volta riavviato il supporto di avvio, non sarà possibile utilizzarlo di nuovo. Se, dopo la fase di convalida, il funzionamento è diverso dal previsto, è necessario registrare un nuovo supporto di avvio e avviare nuovamente il processo di failback.

   Poiché verrà utilizzata la tecnologia flashback, i dati che si trovano già sul sito locale non verranno trasferiti di nuovo, e il processo di failback sarà più rapido.

Esecuzione del failback in un sistema fisico

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

È possibile eseguire il failback automatizzato in un sistema fisico di destinazione nel sito locale.

Nota
Il processo di trasferimento dei dati si avvale di una tecnologia flashback. Tale tecnologia confronta i dati disponibili sul sistema di destinazione con quelli della virtual machine nel cloud. Se parte dei dati è già disponibile nel sistema di destinazione, tali dati non verranno trasferiti di nuovo. La tecnologia accelera quindi la fase di trasferimento dei dati.

Per questo motivo si consiglia di ripristinare il server nel sistema originale nel sito locale.

Prerequisiti

- L'agente che verrà utilizzato per eseguire il failback è online e al momento non è impiegato in un'altra operazione di failback.
- La connessione Internet è stabile.
- È disponibile un supporto di avvio registrato. Per ulteriori informazioni, consultare "Creazione di un supporto di avvio per recuperare i sistemi operativi" nel Manuale dell'utente di Cyber Protection.
- Il sistema fisico di destinazione è il sistema originale nel sito locale, o presenta lo stesso firmware del sistema originale.
- Nel cloud è presente almeno un backup completo della virtual machine.

Per eseguire il failback in un sistema fisico

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Server**.
2. Selezionare il server di ripristino che si trova nello stato di **Failover**.
3. Fare clic sulla scheda **Failback**.
4. Nel campo **Destinazione**, scegliere **Sistema fisico**.
5. Nel campo **Supporto di avvio di destinazione**, fare clic su **Specificare**, selezionare il supporto di avvio, quindi fare clic su **Fine**.

   Nota
   Si consiglia l'utilizzo di un supporto di avvio pronto all'uso, perché è già configurato. Per ulteriori informazioni, consultare "Creazione di un supporto di avvio per recuperare i sistemi operativi" nel Manuale dell'utente di Cyber Protection.

6. [Facoltativo] Per modificare il mapping al disco predefinito, nel campo **Mappatura disco** fare clic su **Specificare**, mappare i dischi del backup ai dischi del sistema di destinazione, quindi fare clic su **Fine**.
7. Fare clic su **Avvia trasferimento dei dati**, e nella finestra di conferma fare clic su **Avvia**.

   Nota
   Se nel cloud non esiste un backup della virtual machine, il sistema esegue automaticamente un backup prima della fase di trasferimento dei dati.

   Viene avviata la fase di trasferimento dei dati. La console visualizza le seguenti informazioni:

Campo	Descrizione
Avanzamento	Questo parametro mostra quanti dati sono stati già trasferiti nel sito locale, e la quantità totale di dati che devono essere ancora trasferiti. La quantità totale di dati include i dati dell'ultimo backup eseguito prima dell'avvio della fase di trasferimento dei dati, e i backup dei dati generati di recente (incrementi di backup), perché la virtual machine resta in esecuzione durante la fase di trasferimento dei dati. Per questa ragione, entrambi i valori del parametro **Avanzamento** aumentano nel tempo. Poiché durante il trasferimento dei dati il sistema utilizza una tecnologia flashback che evita il trasferimento dei dati che sono già disponibili nel sistema di destinazione, l'avanzamento potrebbe essere più veloce di quanto calcolato inizialmente dalla console.
Stima del tempo di inattività	Questo parametro mostra per quanto tempo la virtual machine nel cloud non sarà disponibile se la fase di switchover viene avviata immediatamente. Il valore è calcolato in base ai valori del parametro **Avanzamento**, e diminuisce con il tempo. Poiché durante il trasferimento dei dati il sistema utilizza una tecnologia flashback che evita il trasferimento dei dati che sono già disponibili nel

Campo	Descrizione
	sistema di destinazione, l'interruzione operativa potrebbe essere più breve rispetto al valore visualizzato inizialmente nella console.

8. Fare clic su **Switchover** e, nella finestra di conferma, fare clic di nuovo su **Switchover**.
   Sia avvia la fase di switchover. La console visualizza le seguenti informazioni:

Campo	Descrizione
Avanzamento	Questo parametro mostra l'avanzamento del ripristino del sistema nel sito locale.
Tempo stimato al termine	Questo parametro mostra il tempo stimato per il completamento della fase di switchover, dopo la quale sarà possibile avviare il sistema nel sito locale.

Nota
Se alla virtual machine nel cloud non è stato applicato alcun piano di backup, verrà automaticamente eseguito un backup durante la fase di switchover, e ciò potrebbe causare un'interruzione operativa più lunga.

9. Al completamento della fase di **switchover**, riavviare il supporto di avvio e verificare che il sistema fisico nel sito locale funzioni come previsto.
   Per ulteriori informazioni, consultare la sezione relativa al ripristino di dischi con supporto di avvio nel Manuale dell'utente di Cyber Protection.
10. Fare clic su **Conferma failback**, e nella finestra di conferma fare clic di nuovo su **Conferma** per completare il processo.
    La virtual machine nel cloud viene eliminata e il server di ripristino torna nello stato di **Standby**.

Nota
L'operazione di applicazione di un piano di protezione al server ripristinato non fa parte del processo di failback. Una volta completato il processo di failback, applicare un piano di protezione al server ripristinato per assicurarsi che sia di nuovo protetto. È possibile applicare lo stesso piano di protezione che è stato applicato al server originario, oppure un nuovo piano di protezione per il quale sia abilitato il modulo **Disaster Recovery**.

Failback manuale

Nota
Si consiglia di utilizzare il processo di failback in modalità manuale solo se l'operazione è suggerita dal team di supporto.

È anche possibile avviare un processo di failback in modalità manuale. In questo caso, il trasferimento dei dati dal backup nel cloud al sito locale non viene eseguito automaticamente, ma deve essere avviato manualmente dopo aver spento la virtual machine nel cloud. Ciò rende il

processo di failback in modalità manuale più lento e di conseguenza occorre prevedere un periodo di interruzione operativa più lungo.

Il processo di failback in modalità manuale consiste delle fasi seguenti:

1. **Pianificazione**. Durante questa fase si esegue il ripristino dell'infrastruttura IT nel sito locale, ad esempio degli host e delle configurazioni di rete, si configurano i parametri di failback e si pianifica quando avviare il trasferimento dei dati.
2. **Switchover**. Durante questa fase la virtual machine nel cloud viene disattivata e viene eseguito il backup dei dati generati più di recente. Se al server di ripristino non è stato applicato alcun piano di backup, verrà automaticamente eseguito un backup durante la fase di switchover; ciò potrebbe rallentare il processo. Al termine del backup, il sistema viene ripristinato nel sito locale manualmente. È possibile ripristinare il disco utilizzando il supporto di avvio o l'intero sistema dallo storage di backup nel cloud.
3. **Convalida**. Durante questa fase viene verificato il corretto funzionamento del sistema fisico o della virtual machine nel sito locale, e viene confermato il failback. Dopo la conferma, la virtual machine nel sito cloud viene eliminata e il server di ripristino torna nello stato di **standby**.

Esecuzione di un failback manuale

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

È possibile eseguire il failback manuale in un sistema fisico o una virtual machine di destinazione nel sito locale.

Per eseguire un failback manuale

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Server**.
2. Selezionare il server di ripristino che si trova nello stato di **Failover**.
3. Fare clic sulla scheda **Failback**.
4. Nel campo **Destinazione**, scegliere **Sistema fisico**.
5. Fare clic sull'icona ingranaggio e quindi abilitare l'interruttore **Utilizzare la modalità manuale**.
6. [Facoltativo] Per calcolare il periodo stimato di inattività durante il processo di failback, dividere il valore della **dimensioni del backup** per il valore della velocità di Internet.

   Nota
   Il valore della velocità di Internet diminuisce quando vengono eseguiti più processi di failback alla volta.

7. Fare clic su **Switchover**, e nella finestra di conferma fare clic di nuovo su **Switchover**.
   La virtual machine nel sito cloud viene disattivata.

Nota
Se alla virtual machine nel cloud non è stato applicato alcun piano di backup, verrà automaticamente eseguito un backup durante la fase di switchover, e ciò potrebbe causare un'interruzione operativa più lunga.

8. Ripristinare il server dal backup cloud al sistema fisico o alla virtual machine nel sito locale. Per ulteriori informazioni, consultare la sezione relativa al ripristino di un sistema nel Manuale dell'utente di Cyber Protection.
9. Accertarsi che il ripristino sia completato e che il sistema ripristinato funzioni correttamente, quindi fare clic su **Sistema ripristinato**.
10. Se tutto funziona come previsto, fare clic su **Conferma failback**, e nella finestra di conferma fare clic di nuovo su **Conferma**.
    Il server di ripristino e i punti di ripristino sono pronti per il successivo failover. Per creare nuovi punti di ripristino, applicare un piano di protezione al nuovo server locale.

Nota
L'operazione di applicazione di un piano di protezione al server ripristinato non fa parte del processo di failback. Una volta completato il processo di failback, applicare un piano di protezione al server ripristinato per assicurarsi che sia di nuovo protetto. È possibile applicare lo stesso piano di protezione che è stato applicato al server originario, oppure un nuovo piano di protezione per il quale sia abilitato il modulo **Disaster Recovery**.

Operare con backup crittografati

È possibile creare server di ripristino dai backup crittografati. Per praticità, configurare l'applicazione di una password automatica a un backup crittografato durante il failover su un server di ripristino.

Durante la creazione di un server di ripristino, è possibile specificare la password da utilizzare per le operazioni di disaster recovery automatico. Tali password vengono salvate nell'archivio delle credenziali, un archivio sicuro reperibile nella sezione **Impostazioni** > **Credenziali**.

Più backup possono condividere la stessa credenziale.

Per gestire le password salvate in Archivio credenziali

1. Passare a **Impostazioni** > **Credenziali**.
2. Per gestire una credenziale specifica, fare clic sull'icona nell'ultima colonna. È possibile visualizzare gli elementi collegati alla credenziale selezionata.
   - Per scollegare il backup dalla credenziale selezionata, fare clic sull'icona cestino accanto al backup. Sarà necessario specificare manualmente la password durante il failover nel server di ripristino.
   - Per modificare le credenziali, fare clic su **Modifica** e quindi specificare il nome e la password.
   - Per eliminare la credenziale, fare clic su **Elimina**. Tenere presente che sarà necessario specificare manualmente la password durante il failover nel server di ripristino.

Operazioni con virtual machine di Microsoft Azure

Nota
Alcune funzionalità possono richiedere licenze aggiuntive, a seconda del modello di licensing applicato.

È possibile eseguire il failover di virtual machine di Microsoft Azure in Acronis Cyber Protect Cloud. Per ulteriori informazioni, consultare "Esecuzione di un failover" (pag. 64).

Dopo di ciò, sarà possibile eseguire il failback da Acronis Cyber Protect Cloud alle virtual machine di Azure. Il processo di failback è uguale al processo di failback in un sistema fisico. Per ulteriori informazioni, consultare "Esecuzione del failback in un sistema fisico" (pag. 74).

Nota
Per registrare una nuova virtual machine di Azure per il failback, utilizzare l'estensione Acronis Backup VM disponibile in Azure.

È inoltre possibile configurare una connessione VPN IPsec multisito tra Acronis Cyber Protect Cloud e il gateway VPN di Azure. Per ulteriori informazioni, consultare "Configurazione di una connessione VPN IPsec multisito" (pag. 31).

Configurazione dei server primari

In questa sezione viene descritto come trovare e gestire i server primari.

Creazione di un server primario

Prerequisiti

- È necessario configurare uno dei tipi di connessione al sito cloud.

Per creare un server primario

1. Passare alla scheda **Disaster Recovery** > **Server** > **Server primari**.
2. Fare clic su **Crea**.
3. Selezionare il modello per la nuova macchina virtuale.
4. Selezionare la versione della configurazione (numero di core virtuali e dimensione della RAM). La tabella seguente mostra la quantità massima totale di spazio su disco (GB) per ogni versione.

Tipo	vCPU	RAM (GB)	Quantità massima totale di spazio su disco (GB)
F1	1	2	500
F2	1	4	1000
F3	2	8	2000
F4	4	16	4000
F5	8	32	8000
F6	16	64	16000
F7	16	128	32000
F8	16	256	64000

Nota
Sono visibili i punti di calcolo per ogni opzione. Questo numero riflette il costo orario dell'esecuzione del server primario. Per ulteriori informazioni, consultare "Punti di calcolo" (pag. 12).

5. [Facoltativo] Modificare la dimensione del disco virtuale. Se è necessario più di un disco rigido, fare clic su **Aggiungi disco** e quindi specificare la dimensione del nuovo disco. Al momento non è possibile aggiungere più di 10 dischi a un server primario.
6. Specificare la rete cloud nella quale viene incluso il server primario.
7. Selezionare l'opzione **DHCP**.

Opzione DHCP	Descrizione
Fornito dal sito cloud	Impostazione predefinita. L'indirizzo IP del server verrà fornito da un server DHCP configurato automaticamente nel cloud.
Personalizzato	L'indirizzo IP del server verrà fornito dal server DHCP dell'utente nel cloud.

8. [Facoltativo] Specificare l'**indirizzo MAC**.

   L'indirizzo MAC è un identificatore univoco assegnato alla scheda di rete del server. Se si utilizza un DHCP personalizzato, è possibile configurarlo in modo che assegni sempre uno specifico indirizzo IP a uno specifico indirizzo MAC. Ciò garantisce che il server primario disponga sempre dello stesso indirizzo IP. È possibile eseguire applicazioni che hanno licenze che sono state registrate con l'indirizzo MAC.
9. Specificare l'indirizzo IP che avrà il server nella rete di produzione. Per impostazione predefinita, viene configurato il primo indirizzo IP libero della rete di produzione.

   Nota

   Se si utilizza un server DHCP, aggiungere questo indirizzo IP all'elenco di esclusione del server per evitare che l'indirizzo IP entri in conflitto.

   Se si utilizza un server DHCP personalizzato, è necessario specificare lo stesso indirizzo IP specificato in **Indirizzo IP in rete di produzione** nella configurazione del server DHCP. In caso contrario, il failover di prova non funzionerà correttamente e il server non sarà raggiungibile tramite un indirizzo IP pubblico.
10. [Facoltativo] Selezionare la casella di controllo **Accesso Internet**.

    Viene così abilitato l'accesso a Internet per il server primario. Per impostazione predefinita, la porta TCP 25 è aperta per le connessioni in uscita verso gli indirizzi IP pubblici.
11. [Facoltativo] Selezionare la casella di controllo **Utilizza indirizzo IP pubblico**.

    Se dispone di un indirizzo IP pubblico, il server primario è disponibile anche da Internet. Se la casella di controllo non è selezionata, il server sarà disponibile solo nella rete di produzione.

    L'indirizzo IP pubblico verrà visualizzato dopo aver completato la configurazione. Per impostazione predefinita, la porta TCP 443 è aperta per le connessioni in entrata verso gli indirizzi IP pubblici.

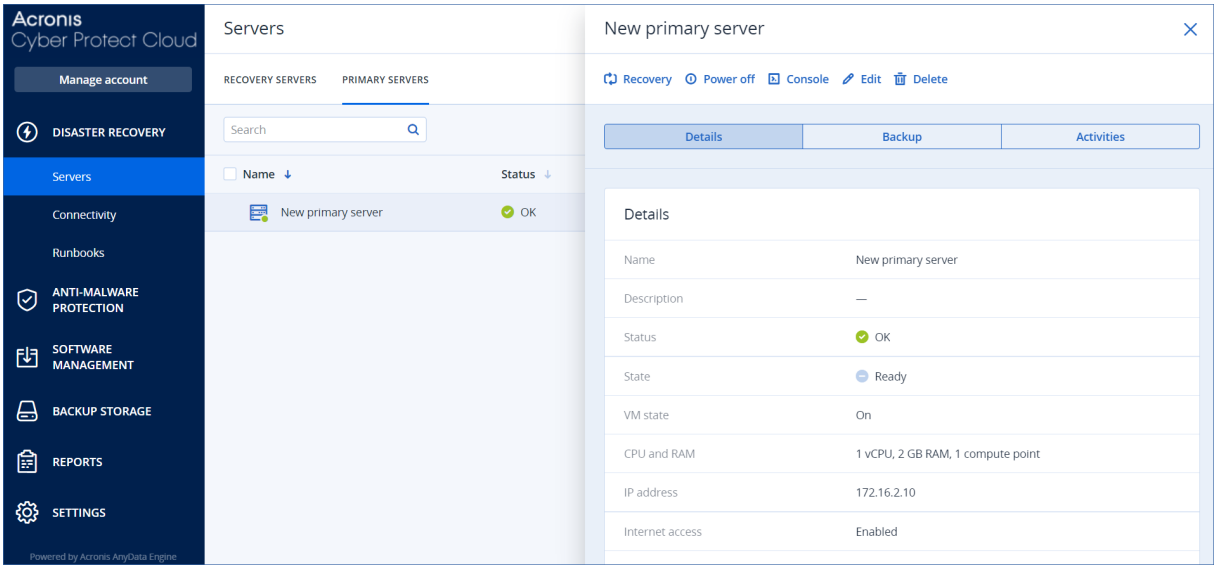
    Nota

    Se si deseleziona la cartella di controllo **Utilizza indirizzo IP pubblico** o si elimina il server di ripristino, il relativo indirizzo IP pubblico non viene riservato.
12. [Facoltativo] Selezionare **Imposta soglia RPO**.

    La soglia RPO definisce l'intervallo di tempo massimo consentito tra l'ultimo punto di ripristino e l'ora corrente. È possibile impostare il valore tra 15–60 minuti, 1–24 ore, 1–14 giorni.
13. Definire il nome del server primario.
14. [Facoltativo] Specificare una descrizione per il server primario.

15. [Facoltativo] Fare clic sulla scheda **Regole del firewall cloud** per modificare le regole predefinite del firewall. Per ulteriori informazioni, consultare "Impostazione delle regole del firewall per server cloud" (pag. 85).
16. Fare clic su **Crea**.

Il server primario è ora disponibile nella rete di produzione. È possibile gestire il server utilizzando la relativa console, RDP, SSH o TeamViewer.



Operazioni con un server primario

Il server primario viene visualizzato nella scheda **Disaster Recovery** > **Server** > **Server primari** della console di Cyber Protect.

Per avviare o arrestare il server, fare clic su **Avvia** o **Arresta** nel riquadro del server primario.

Per modificare le impostazioni del server primario, arrestare il server e fare clic su **Modifica**.

Per applicare un piano di protezione al server primario, selezionarlo e fare clic su **Crea** nella scheda **Piano**. Verrà visualizzato un piano di protezione predefinito del quale è possibile modificare solo la pianificazione e le regole di conservazione. Per ulteriori informazioni, fare riferimento a "Backup dei server cloud".

Gestione dei server cloud

Per gestire i server cloud, passare a **Disaster Recovery** > **Server**. Sono disponibili due schede: **Server di ripristino** e **Server primari**. Per visualizzare tutte le colonne facoltative della tabella, fare clic sull'icona ingranaggio.

Selezionando ciascun server cloud saranno disponibili le seguenti informazioni.

Nome colonna	Descrizione
Nome	Il nome del server cloud definito dall'utente
Stato	Lo stato che riflette il problema più grave riscontrato in un server cloud (in base agli avvisi attivi)
Condizione	Una condizione di server cloud
Stato VM	Lo stato di alimentazione della macchina virtuale associata a un server cloud
Posizione attiva	La posizione in cui è ospitato il server cloud. Ad esempio, **Cloud**.
Soglia RPO	L'intervallo di tempo massimo consentito tra l'ultimo punto di ripristino idoneo per un failover e l'ora corrente. Il valore può essere impostato tra 15-60 minuti, 1-24 ore, 1-14 giorni.
Conformità RPO	La conformità RPO è il rapporto tra la soglia RPO effettiva e la soglia RPO definita. L'opzione Conformità RPO viene visualizzata se è stata definita la soglia RPO. Viene calcolata come indicato di seguito: **Conformità RPO = RPO effettiva/soglia RPO** dove **RPO effettiva = ora corrente – ora dell'ultimo punto di ripristino** **Stati di conformità RPO** In funzione del valore del rapporto tra la soglia RPO effettiva e la soglia RPO definita, vengono utilizzati gli stati seguenti: • **Conforme**. Conformità RPO < 1x. Un server rispetta la soglia RPO. • **Superato**. Conformità RPO <= 2x. Un server viola la soglia RPO. • **Gravemente superato**. Conformità RPO <= 4x. Un server viola la soglia RPO di un valore superiore al doppio consentito. • **Criticamente superato**. Conformità RPO > 4x. Un server viola la soglia RPO di un valore superiore al quadruplo consentito. • **In sospeso (nessun backup)**. Il server è protetto con il piano di protezione, tuttavia il backup creato non è stato ancora completato.
RPO effettivo	Tempo trascorso dalla creazione dell'ultimo punto di ripristino

Ultimo punto di ripristino	Data e ora in cui si è stato creato l'ultimo punto di ripristino

Regole del firewall per i server cloud

È possibile configurare le regole del firewall per controllare il traffico in entrata e in uscita dei server primario e di ripristino nel sito cloud.

È possibile configurare le regole in entrata dopo aver fornito un indirizzo IP pubblico al server cloud. Per impostazione predefinita, è consentita la porta TCP 443, mentre tutte le altre connessioni in entrata non vengono autorizzate. È possibile modificare le regole predefinite del firewall e aggiungere o rimuovere eccezioni in entrata. Se non è stato fornito un indirizzo IP pubblico, sarà possibile soltanto visualizzare le regole in entrata, ma non configurarle.

È possibile configurare le regole in uscita dopo aver fornito l'accesso a Internet per il server cloud. Per impostazione predefinita, è consentita la porta TCP 25, mentre tutte le altre connessioni in uscita sono autorizzate. È possibile modificare le regole predefinite del firewall e aggiungere o rimuovere eccezioni in uscita. Se non è stato fornito un accesso a Internet, sarà possibile soltanto visualizzare le regole in uscita, ma non configurarle.

Nota
Per motivi di sicurezza, sono presenti regole del firewall predefinite che non è possibile modificare.

Per le connessioni in entrata e in uscita:

- Consenti ping: ICMP echo-request (type 8, code 0) and ICMP echo-reply (type 0, code 0)
- Consenti ICMP need-to-frag (type 3, code 4)
- Consenti TTL exceeded (type 11, code 0)

Solo per le connessioni in entrata:

- Parte non configurabile: Nega tutto

Solo per le connessioni in uscita:

- Parte non configurabile: Rifiuta tutto

Impostazione delle regole del firewall per server cloud

È possibile modificare le regole predefinite del firewall per i server primario e di ripristino nel cloud.

Per modificare le regole del firewall di un server nel sito cloud

1. Nella console di Cyber Protect, passare a **Disaster Recovery** > **Server**.
2. Per modificare le regole del firewall di un server di ripristino, fare clic sulla scheda **Server di ripristino**. In alternativa, per modificare le regole del firewall di un server primario, fare clic sulla scheda **Server primari**.
3. Fare clic sul server, quindi scegliere **Modifica**.
4. Fare clic sulla scheda **Regole del firewall cloud**.
5. Per cambiare l'azione predefinita per le connessioni in entrata:

a. Nel campo a discesa **In entrata**, selezionare l'azione predefinita.

Azione	Descrizione
Nega tutto	Nega tutto il traffico in entrata. È possibile aggiungere eccezioni e consentire il traffico proveniente da indirizzi IP, protocolli e porte specifici.
Consenti tutto	Consente tutto il traffico TCP e UDP in entrata. È possibile aggiungere eccezioni e negare il traffico proveniente da indirizzi IP, protocolli e porte specifici.

Nota
La modifica dell'azione predefinita annulla e rimuove la configurazione delle regole in entrata esistenti.

b. [Facoltativo] Per salvare le eccezioni esistenti, nella finestra di conferma selezionare **Salvare le eccezioni compilate**.

c. Fare clic su **Conferma**.

6. Per aggiungere un'eccezione:

a. Fare clic su **Aggiungi eccezione**.

b. Specificare i parametri del firewall.

Parametro del firewall	Descrizione
Protocollo	Selezionare il protocollo di connessione. Sono supportate le seguenti opzioni: • **TCP** • **UDP** • **TCP+UDP**
Porta del server	Selezionare le porte alle quali applicare la regola. È possibile specificare quanto segue: • un numero di porta specifico (ad esempio `2298`) • un intervallo di numeri di porta (ad esempio `6000-6700`) • qualsiasi numero di porta. Utilizzare `*` per applicare la regola a qualsiasi numero di porta.
Indirizzo IP del client	Selezionare gli indirizzi IP ai quali applicare la regola. È possibile specificare quanto segue: • un indirizzo IP specifico (ad esempio `192.168.0.0`) • un intervallo di indirizzi IP mediante la notazione CIDR (ad esempio `192.168.0.0/24`) • qualsiasi indirizzo IP. Utilizzare `*` per applicare la regola a qualsiasi indirizzo IP.

7. Per rimuovere un'eccezione in entrata esistente, fare clic sull'icona del cestino accanto all'eccezione.
8. Per cambiare l'azione predefinita per le connessioni in uscita:
   a. Nel campo a discesa **In uscita**, selezionare l'azione predefinita.

Azione	Descrizione
Nega tutto	Nega tutto il traffico in uscita. È possibile aggiungere eccezioni e consentire il traffico verso indirizzi IP, protocolli e porte specifici.
Consenti tutto	Consente tutto il traffico in uscita. È possibile aggiungere eccezioni e negare il traffico proveniente da indirizzi IP, protocolli e porte specifici.

Nota
La modifica dell'azione predefinita annulla e rimuove la configurazione delle regole in uscita esistenti.

   b. [Facoltativo] Per salvare le eccezioni esistenti, nella finestra di conferma selezionare **Salvare le eccezioni compilate**.
   c. Fare clic su **Conferma**.
9. Per aggiungere un'eccezione:
   a. Fare clic su **Aggiungi eccezione**.
   b. Specificare i parametri del firewall.

Parametro del firewall	Descrizione
Protocollo	Selezionare il protocollo di connessione. Sono supportate le seguenti opzioni: • **TCP** • **UDP** • **TCP+UDP**
Porta del server	Selezionare le porte alle quali applicare la regola. È possibile specificare quanto segue: • un numero di porta specifico (ad esempio `2298`) • un intervallo di numeri di porta (ad esempio `6000-6700`) • qualsiasi numero di porta. Utilizzare `*` per applicare la regola a qualsiasi numero di porta.
Indirizzo IP del client	Selezionare gli indirizzi IP ai quali applicare la regola. È possibile specificare quanto segue: • un indirizzo IP specifico (ad esempio `192.168.0.0`) • un intervallo di indirizzi IP mediante la notazione CIDR (ad

Parametro del firewall	Descrizione
	esempio `192.168.0.0/24`) • qualsiasi indirizzo IP. Utilizzare * per applicare la regola a qualsiasi indirizzo IP.

10. Per rimuovere un'eccezione in uscita esistente, fare clic sull'icona del cestino accanto all'eccezione.
11. Fare clic su **Salva**.

Controllo delle attività del firewall cloud

Dopo un aggiornamento della configurazione delle regole del firewall di un server cloud, il registro dell'attività aggiornata è disponibile nella console di Cyber Protect. È possibile visualizzare il registro e verificare le seguenti informazioni:

- nome utente dell'utente che ha aggiornato la configurazione
- data e ora dell'aggiornamento
- impostazioni del firewall per le connessioni in entrata e in uscita
- azioni predefinite per le connessioni in entrata e in uscita
- protocolli, porte e indirizzi IP delle eccezioni per le connessioni in entrata e in uscita

Per visualizzare i dettagli delle modifiche alle configurazioni delle regole del firewall cloud

1. Nella console di Cyber Protect, fare clic su **Monitoraggio** > **Attività**.
2. Fare clic sull'attività corrispondente e quindi su **Tutte le proprietà**.
   La descrizione dell'attività dovrebbe essere **Aggiornamento configurazione del server cloud**.
3. Verificare le informazioni di interesse nel campo **Contesto**.

Backup dei server cloud

Il backup dei server primari e di ripristino viene eseguito in modalità agentless nel sito cloud. Questo tipo di backup presenta alcune limitazioni specifiche.

- L'unica posizione di backup possibile è l'archivio del cloud. Il backup dei server primari viene eseguito sullo storage di **backup dei server primari**.

  Nota
  Non sono supportate le posizioni di backup di Microsoft Azure.

- Non è possibile applicare un piano di backup a più server. Ogni server deve quindi disporre del proprio piano di backup, anche se tutti i piani di backup presentano le stesse impostazioni.
- A un server può essere applicato un solo piano di backup.
- Non è supportato il backup compatibile con le applicazioni.
- La crittografia non è disponibile.
- Non sono disponibili opzioni di backup.

Quando si elimina un server primario vengono eliminati anche i rispettivi backup.

Il backup di un server di ripristino viene eseguito solo in condizioni di failover. Tale backup prosegue la sequenza di backup del server originario. All'esecuzione del failback, il server originario potrà continuare questa sequenza di backup. Ne consegue che i backup del server di ripristino possano essere eliminati solo manualmente o come risultato dell'applicazione delle regole di conservazione. Quando viene eliminato un server di ripristino, i relativi backup vengono sempre conservati.

Nota
I piani di backup per i server cloud vengono eseguiti in base al fuso orario UTC.

Orchestrazione (runbook)

Nota
Alcune funzionalità possono richiedere licenze aggiuntive, a seconda del modello di licensing applicato.

Un runbook è un insieme di istruzioni che descrive come allestire l'ambiente di produzione nel cloud. I runbook vengono creati nella console di Cyber Protect. Per accedere alla schermata **Runbooks**, selezionare **Disaster Recovery** > **Runbooks**.

Perché utilizzare i runbook?

Con i runbooks è possibile:

- Rendere automatico il failover di uno o più server
- Controllare automaticamente il risultato del failover eseguendo il ping dell'indirizzo IP del server e controllando la connessione alla porta specificata
- Impostando la sequenza di operazioni per i server che eseguono applicazioni distribuite
- Includere operazioni manuali nel flusso di lavoro
- Verificare l'integrità della soluzione di disaster recovery eseguendo i runbook in modalità di prova.

Creazione di runbook

Un runbook è costituito da passaggi che vengono eseguiti consecutivamente. Un passaggio è costituito da azioni il cui avvio è simultaneo.

È possibile attenersi alle istruzioni seguenti o guardare il tutorial video.

Per creare un runbook

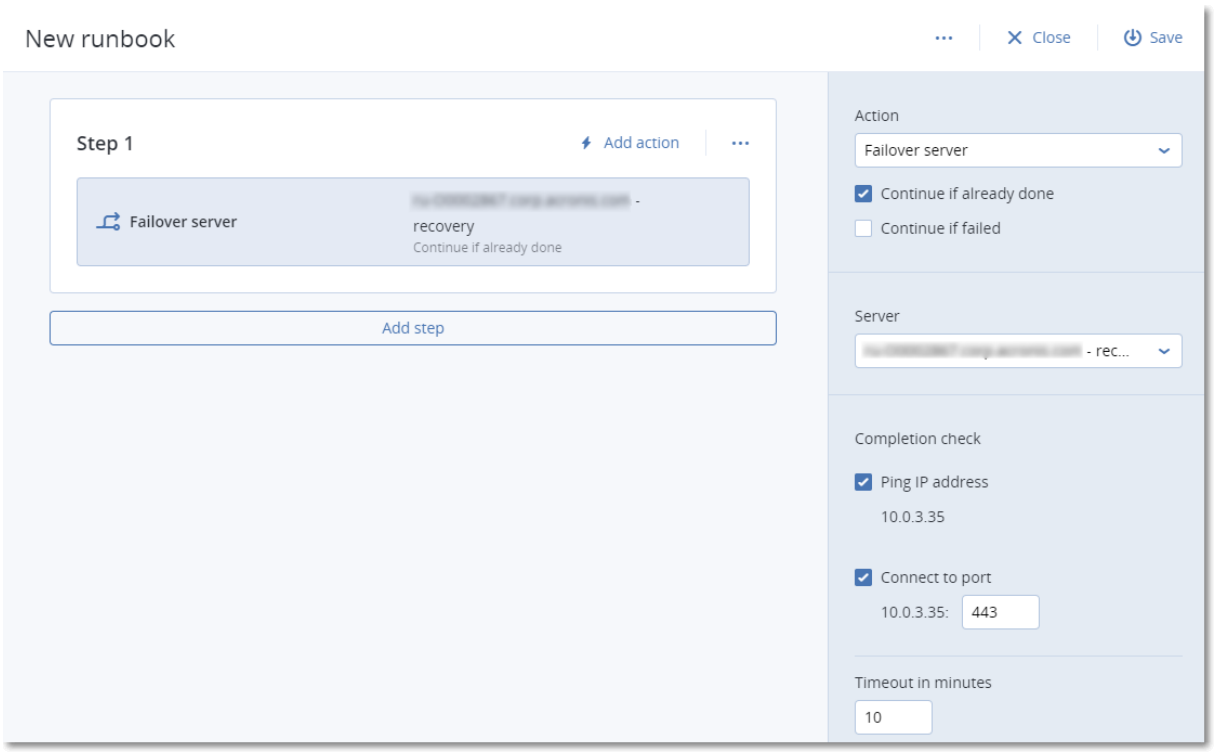
1. Nella console di Cyber Protection, passare a **Disaster Recovery** > **Runbooks**.
2. Fare clic su **Crea runbook**.
3. Fare clic su **Aggiungi passaggio**.
4. Fare clic su **Aggiungi azione**, quindi selezionare l'azione da aggiungere al passaggio.

Azione	Descrizione
Esegui il failover del server	Esegue il failover di un server cloud. Per definire questa azione, è necessario selezionare un server cloud e configurare i parametri del runbook disponibili per questa azione. Per ulteriori informazioni su questi parametri, consultare "Parametri del runbook" (pag. 93).

Azione	Descrizione
	Nota Se il backup del server selezionato è stato crittografato utilizzando la crittografia come proprietà del sistema, l'azione **Esegui il failover del server** viene sospesa e modificata automaticamente in **Richiesta interazione**. Per procedere con l'esecuzione del runbook, fornire la password del backup crittografato.
Esegui il failback del server	Esegue il failback di un server cloud. Per definire questa azione, è necessario selezionare un server cloud e configurare i parametri del runbook disponibili per questa azione. Per ulteriori informazioni su queste impostazioni, consultare "Parametri del runbook" (pag. 93). **Nota** Le operazioni runbook supportano solo il failback in modalità manuale. Ciò significa che se si avvia il processo di failback eseguendo un runbook che include il passaggio **Esegui il failback del server**, la procedura richiederà un'interazione manuale: sarà necessario ripristinare manualmente il sistema, e confermare o annullare il processo di failback dalla scheda **Disaster Recovery** > **Server**.
Avvia server	Avvia un server cloud. Per definire questa azione, è necessario selezionare un server cloud e configurare i parametri del runbook disponibili per questa azione. Per ulteriori informazioni su queste impostazioni, consultare "Parametri del runbook" (pag. 93). **Nota** L'azione **Avvia server** non è applicabile alle operazioni di failover di prova nei runbook. Il tentativo di esecuzione di questa azione non riesce e restituisce il seguente messaggio di errore: Non riuscita: L'azione non è applicabile allo stato del server corrente.
Arresta server	Arresta un server cloud. Per definire questa azione, è necessario selezionare un server cloud e configurare i parametri del runbook disponibili per questa azione. Per ulteriori informazioni su queste impostazioni, consultare "Parametri del runbook" (pag. 93). **Nota** L'azione **Arresta server** non è applicabile alle operazioni di failover di prova nei runbook. Il tentativo di esecuzione di questa azione non riesce e restituisce il seguente messaggio di errore: Non riuscita: L'azione non è applicabile allo stato del server corrente.
Operazione manuale	Un'operazione manuale richiede un'interazione da parte di un utente. Per definire questa azione, è necessario inserire una descrizione. Quando una sequenza di runbook raggiunge un'operazione manuale, il runbook viene sospeso e non procede fino a quando un utente non esegue l'operazione manuale necessaria, ad esempio fare clic sul pulsante di conferma.

Azione	Descrizione
Esegui runbook	Esegue un altro runbook. Per definire questa azione, è necessario scegliere un runbook. Un runbook può includere solo un'esecuzione di un determinato runbook. Se, ad esempio, è stata aggiunta l'azione "Esegui Runbook A", è possibile aggiungere l'azione "Esegui Runbook B", ma non è possibile aggiungere un'altra azione "Esegui Runbook A".

5. Definire i parametri del runbook per l'azione. Per ulteriori informazioni su questi parametri, consultare "Parametri del runbook" (pag. 93).
6. [Facoltativo] Per aggiungere una descrizione del passaggio:
   a. Fare clic sull'icona dei puntini di sospensione, quindi su **Descrizione**.
   b. Inserire una descrizione del passaggio.
   c. Fare clic su **Fine**.
7. Ripetere i passaggi da 3 a 6 fino a quando non si ottiene la sequenza desiderata di passaggi e azioni.
8. [Facoltativo] Per modificare il nome predefinito del runbook:
   a. Fare clic sull'icona dei puntini di sospensione.
   b. Inserire il nome del runbook.
   c. Inserire una descrizione del runbook.
   d. Fare clic su **Fine**.
9. Fare clic su **Salva**.
10. Fare clic su **Chiudi**.



Parametri del runbook

I parametri del runbook sono impostazioni specifiche che devono essere configurate per definire un'azione del runbook. Esistono due categorie di parametri dei runbook: i parametri di azione e parametri di controllo della completezza.

I parametri di azione definiscono il comportamento del runbook in base allo stato iniziale o al risultato dell'azione.

I parametri di controllo della completezza verificano che il server sia disponibile e in grado di fornire i servizi necessari. Se un controllo di completezza non ha esito positivo, l'intera azione viene considerata non riuscita.

La tabella seguente descrive i parametri del runbook configurabili per ogni azione.

Parametro del runbook	Categoria	Disponibile per l'azione	Descrizione
Continuare se già completata	Parametro dell'azione	• **Esegui il failover del server** • **Avvia server** • **Arresta server** • **Esegui il failback del server**	Questo parametro definisce il comportamento del runbook quando l'azione richiesta è già stata completata (ad esempio, un failover è già stato eseguito o un server è già in esecuzione). Quando è attivo, il runbook invia un avviso e procede. Quando non è attivo, l'azione e il runbook non hanno esito positivo.

Parametro del runbook	Categoria	Disponibile per l'azione	Descrizione
			Per impostazione predefinita, questo parametro è abilitato.
Continuare se non riuscita	Parametro dell'azione	• **Esegui il failover del server** • **Avvia server** • **Arresta server** • **Esegui il failback del server**	Questo parametro definisce il comportamento del runbook quando l'azione richiesta non riesce. Quando è attivo, il runbook invia un avviso e procede. Quando non è attivo, l'azione e il runbook non hanno esito positivo. Per impostazione predefinita, questo parametro è disabilitato.
Indirizzo IP del ping	Controllo del completamento	• **Avvia server**	Il software esegue il ping dell'indirizzo IP di produzione del server cloud fino a quando il server risponde o il timeout scade, a seconda della condizione che si verifica per prima.
Connetti alla porta (443 per impostazione predefinita)	Controllo del completamento	• **Esegui il failover del server** • **Avvia server**	Il software tenta di connettersi al server cloud usando l'indirizzo IP di produzione e la porta specificata, fino a quando la connessione viene stabilita o il timeout scade, a seconda della condizione che si verifica per prima. In questo modo è possibile controllare che l'applicazione in ascolto sulla porta specificata sia in esecuzione.
Timeout in minuti	Controllo del completamento	• **Esegui il failover del server** • **Avvia server**	Il timeout predefinito è di 10 minuti.

Operazioni con i runbook

Nota
La disponibilità della funzionalità dipende dalle quote di servizio abilitate per l'account.

Per accedere all'elenco delle operazioni, al passaggio del mouse sul runbook fare clic sull'icona con i puntini di sospensione. Se il runbook non è in esecuzione, sono disponibili le seguenti operazioni:

- **Esegui**
- **Modifica**

- **Clona**
- **Elimina**

Esecuzione di un runbook

Ogni volta che l'utente fa clic su **Esegui**, vengono richiesti i parametri di esecuzione. Tali parametri si applicano a tutte le operazioni di failover e failback incluse nel runbook. I runbook specificati nelle operazioni **Esegui runbook** ereditano tali parametri dal runbook principale.

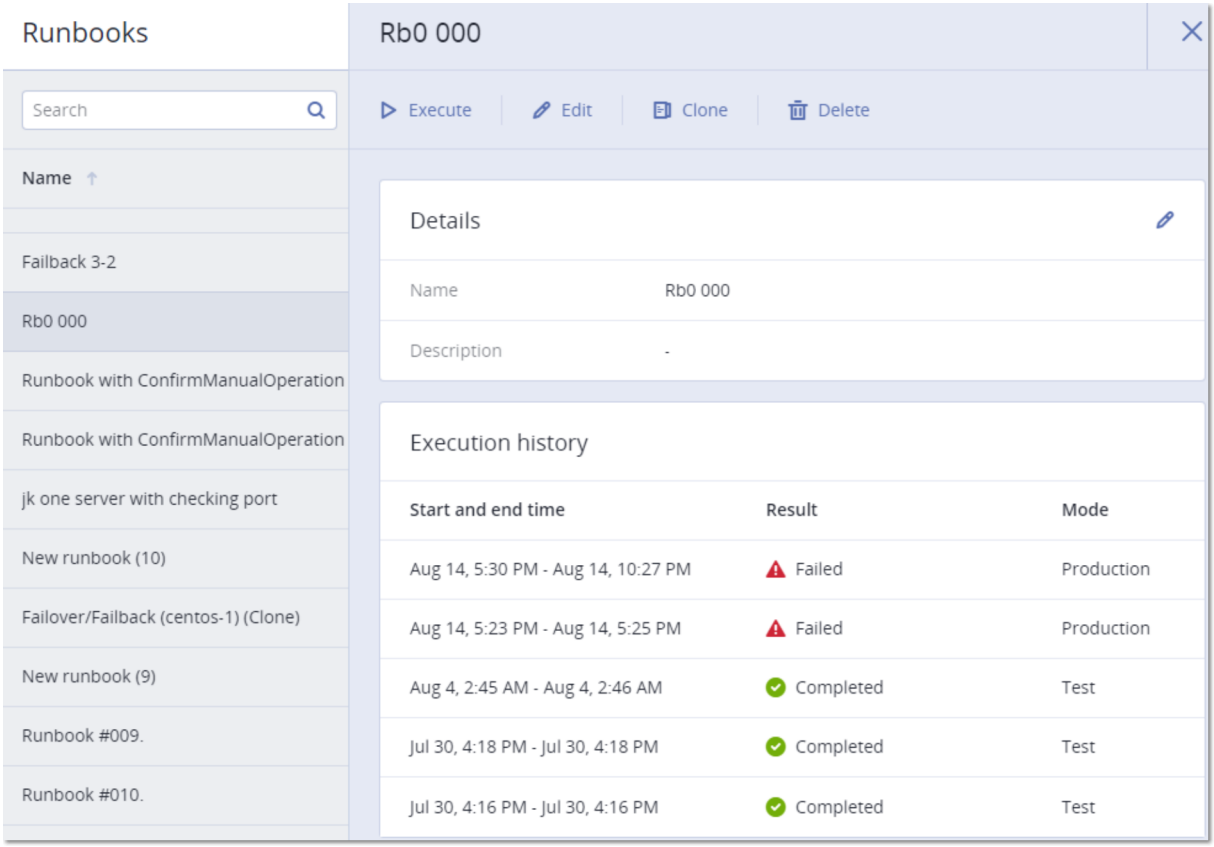
- **Modalità di failover e failback**
  Selezionare se si desidera eseguire un failover di prova (impostazione predefinita) o un failover reale (produzione). La modalità di failback corrisponderà alla modalità di failover scelta.
- **Punto di ripristino di failover**
  Scegliere il punto di ripristino di failover più recente (impostazione predefinita) o selezionare un punto temporizzato passato. Nell'ultimo caso, per ogni server vengono selezionati i punti di ripristino più vicini precedenti alla data e all'ora specificate.

Arresto dell'esecuzione di un runbook

Durante l'esecuzione di un runbook è possibile selezionare l'opzione **Arresta** nell'elenco delle operazioni. Il software porterà a termine tutte le azioni già avviate ad eccezione di quelle che richiedono l'interazione dell'utente.

Visualizzazione della cronologia dell'esecuzione

Quando si seleziona un runbook nella scheda **Runbooks**, il software visualizza informazioni sul runbook e la cronologia di esecuzione. Fare clic sulla riga corrispondente a un'esecuzione specifica per visualizzare il log dell'esecuzione.


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

Open VPN site-to-site - Informazioni aggiuntive

Durante la configurazione di un server di ripristino, vengono configurati l'**indirizzo IP nella rete produttiva** e l'**indirizzo IP di prova**.

Successivamente all'esecuzione del failover (esecuzione della virtual machine nel cloud) e all'accesso alla virtual machine per controllare l'indirizzo IP del server, viene visualizzato l'**indirizzo IP nella rete produttiva**.

Durante l'esecuzione del failover di prova, è possibile raggiungere il server di prova solo utilizzando l'**indirizzo IP di prova**, visibile soltanto nella configurazione del server di ripristino.

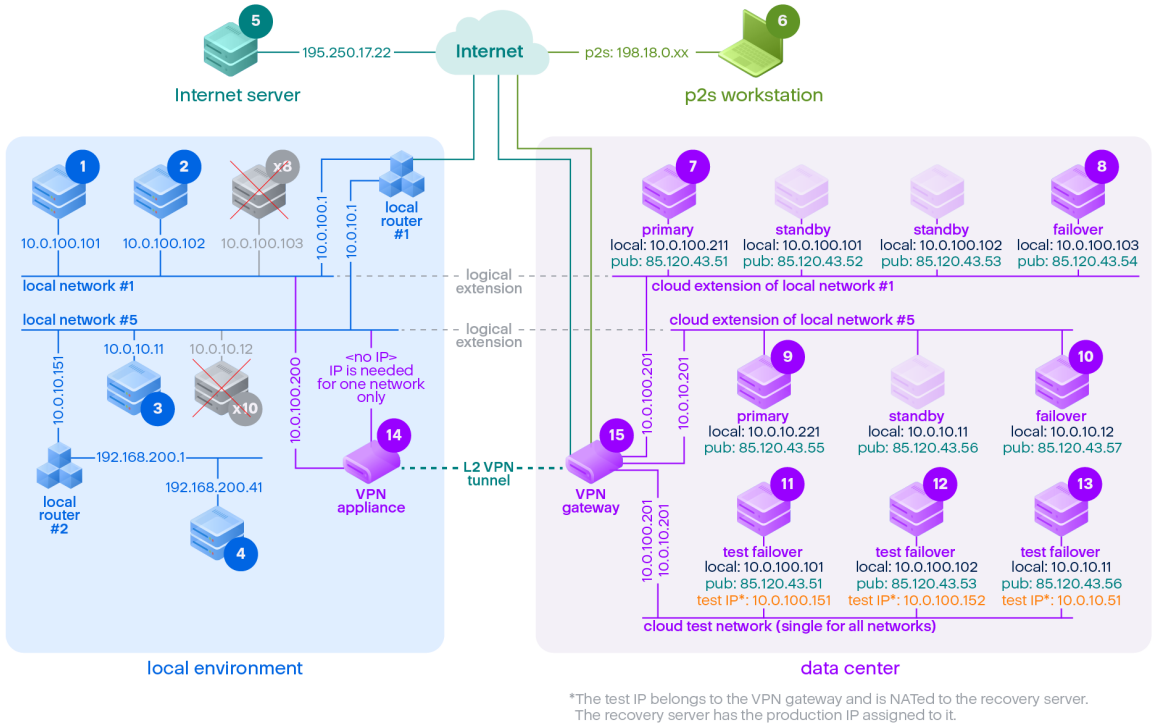
Per raggiungere un server di prova dal sito locale, è necessario utilizzare l'**indirizzo IP di prova**.

Nota
La configurazione di rete del server mostra sempre l'**indirizzo IP nella rete produttiva**, perché il server di prova rispecchia la configurazione del server di produzione. Ciò accade perché l'indirizzo IP di prova non appartiene al server di prova ma al gateway VPN, e viene tradotto nell'indirizzo IP di produzione tramite NAT.

Il diagramma seguente illustra un esempio di configurazione di Open VPN da sito a sito. Alcuni dei server nell'ambiente locale vengono ripristinati nel cloud tramite il failover (mentre l'infrastruttura di rete non presenta problema).

1. Il cliente ha abilitato il Disaster Recovery nei seguenti modi:
   a. configurando l'appliance VPN (14) e connettendola al server VPN cloud dedicato (15)
   b. proteggendo alcuni dei server locali con il Disaster Recovery (1, 2, 3, x8 e x10)
      Alcuni server nel sito locale (come il 4) sono collegati a reti non connesse all'appliance VPN. Questi server non sono protetti con Disaster Recovery.
2. Parte dei server (connessi a reti differenti) funzionano nel sito locale: (1, 2, 3 e 4)
3. Questi server protetti (1, 2 e 3) vengono sottoposti a test con il failover di prova (11, 12 e 13)
4. Alcuni server del sito locale non sono disponibili (x8, x10). Dopo l'esecuzione del failover, diventano disponibili nel cloud (8 e 10)
5. Alcuni server primari (7 e 9), connessi a reti differenti, sono disponibili nell'ambiente cloud

6. (5) è un server in Internet con un indirizzo IP pubblico
7. (6) è una workstation connessa al cloud tramite una connessione VPN da punto a sito (p2s)



In questo esempio, è disponibile la seguente configurazione di connessione (ad esempio, "ping") da un server nella riga **Da:** a un server nella colonna **A:**.

	A:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Da:		locale	locale	locale	locale	internet	p2s	primario	failover	primario	failover	failover di prova	failover di prova	failover di prova	appliance VPN	server VPN

	A:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	locale		diretto	tramite router locale 1	tramite router locale 2	tramite router locale 1 e Internet	no	tramite tunnel: locale tramite router locale 1 e Internet: pub	tramite tunnel: locale tramite router locale 1 e Internet: pub	tramite tunnel: locale tramite router locale 1 e Internet: pub	tramite tunnel: locale tramite router locale 1 e Internet: pub	tramite tunnel: NAT (server VPN) tramite router locale 1 e Internet: pub	tramite tunnel: NAT (server VPN) tramite router locale 1 e Internet: pub	tramite router locale 1 e tunnel: NAT (server VPN) tramite router locale 1 e Internet: pub	diretto	no
2	locale	diretto		tramite router locale 1	tramite router locale 2	tramite router locale 1 e Internet	no	tramite tunnel: locale tramite router locale 1 e Internet: pub	tramite tunnel: locale tramite router locale 1 e Internet: pub	tramite tunnel: locale tramite router locale 1 e Internet: pub	tramite tunnel: locale tramite router locale 1 e Internet: pub	tramite tunnel: NAT (server VPN) tramite router locale 1 e Internet: pub	tramite tunnel: NAT (server VPN) tramite router locale 1 e Internet: pub	tramite router locale 1 e tunnel: NAT (server VPN) tramite router locale 1 e	diretto	no

	A:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
														Internet: pub		
3	locale	tramite router locale 1	tramite router locale 1		tramite router locale 2	tramite router locale 1 e Internet	no	tramite tunnel: locale tramite router locale 1 e Internet: pub	tramite tunnel: locale tramite router locale 1 e Internet: pub	tramite tunnel: locale tramite router locale 1 e Internet: pub	tramite tunnel: locale tramite router locale 1 e Internet: pub	tramite tunnel: NAT (server VPN) tramite router locale 1 e Internet: pub	tramite tunnel: NAT (server VPN) tramite router locale 1 e Internet: pub	tramite router locale 1 e tunnel: NAT (server VPN) tramite router locale 1 e Internet: pub	tramite router locale	no
4	locale	tramite router locale 2 e router 1	tramite router locale 2 e router 1	tramite router locale 2		tramite router locale 2, router 1 e Internet	no	tramite router locale 2 e tunnel: locale tramite router locale 2,	tramite router locale 2 e tunnel: locale tramite router locale 2,	tramite router locale 2 e tunnel: locale tramite router locale 2,	tramite router locale 2 e tunnel: locale tramite router locale 2,	tramite tunnel: NAT (server VPN) tramite router locale 2, router 1 e	tramite tunnel: NAT (server VPN) tramite router locale 2, router 1 e	tramite tunnel: NAT (server VPN) tramite router locale 2, router 1 e	tramite router locale 2	no

	A:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
								router locale 1 e Internet: pub	router locale 1 e Internet: pub	router locale 1 e Internet: pub	router locale 1 e Internet: pub	Internet: pub	Internet: pub	Internet: pub		
5	internet	no	no	no	no		n/d	tramite Internet: pub	tramite Internet: pub	tramite Internet: pub	tramite Internet: pub	tramite Internet: pub	tramite Internet: pub	tramite Internet: pub	no	no
6	p2s	no	no	no	no	tramite Internet		tramite VPN p2s (server VPN): locale tramite Internet: pub	tramite VPN p2s (server VPN): locale tramite Internet: pub	tramite VPN p2s (server VPN): locale tramite Internet: pub	tramite VPN p2s (server VPN): locale tramite Internet: pub	tramite VPN p2s - NAT (server VPN) tramite Internet: pub	tramite VPN p2s - NAT (server VPN) tramite Internet: pub	tramite VPN p2s - NAT (server VPN) tramite Internet: pub	no	no
7	primario	tramite tunnel	tramite tunnel	tramite tunnel e router locale 1	tramite tunnel e router locale 1 e 2	tramite Internet (tramite server VPN)	no		diretto in cloud: locale	tramite tunnel e router locale 1: locale	tramite tunnel e router locale 1: locale	tramite server VPN: NAT	tramite server VPN: NAT	tramite tunnel e router locale 1: NAT	no	Solo protocolli DHCP e DNS
8	failover	tramit	tramit	tramit	tramit	tramite	no	diretto		tramite	tramite	tramite	tramite	tramite	no	Solo

	A:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		e tunnel	e tunnel	e tunnel e router locale 1	e tunnel e router locale 1 e 2	Internet (tramite server VPN)		in cloud: locale		tunnel e router locale 1: locale	tunnel e router locale 1: locale	server VPN: NAT	server VPN: NAT	tunnel e router locale 1: NAT		protocolli DHCP e DNS
9	primario	tramite tunnel e router locale 1	tramite tunnel e router locale 1	tramite tunnel	tramite tunnel	tramite Internet (tramite server VPN)	no	tramite tunnel e router locale 1: locale	tramite tunnel e router locale 1: locale		diretto in cloud: locale	tramite tunnel e router locale 1: NAT	tramite tunnel e router locale 1: NAT	tramite server VPN: NAT	no	Solo protocolli DHCP e DNS
10	failover	tramite tunnel e router locale 1	tramite tunnel e router locale 1	tramite tunnel	tramite tunnel	tramite Internet (tramite server VPN)	no	tramite tunnel e router locale 1: locale	tramite tunnel e router locale 1: locale	diretto in cloud: locale		tramite tunnel e router locale 1: NAT	tramite tunnel e router locale 1: NAT	tramite server VPN: NAT	no	Solo protocolli DHCP e DNS
11	failover di prova	no	no	no	no	tramite Internet (tramite server	no	no	no	no	no		diretto in cloud: locale	tramite server VPN: locale (routing)	no	Solo protocolli DHCP e DNS

	A:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
						VPN)										
12	failover di prova	no	no	no	no	tramite Internet (tramite server VPN)	no	no	no	no	no	diretto in cloud: locale		tramite server VPN: locale (routing)	no	Solo protocolli DHCP e DNS
13	failover di prova	no	no	no	no	tramite Internet (tramite server VPN)	no	no	no	no	no	tramite server VPN: locale (routing)	tramite server VPN: locale (routing)		no	Solo protocolli DHCP e DNS
14	appliance VPN	diretto	diretto	tramite router locale 1	tramite router locale 2	tramite Internet (router locale 1)	no	no	no	no	no	no	no	no		no
15	server VPN	no	no	no	no	no	no	no	no	no	no	no	no	no	no	

Glossario

A

Appliance VPN

Una macchina virtuale speciale che abilita la connessione tra la rete locale e il sito nel cloud tramite un tunnel VPN sicuro. L'appliance VPN viene distribuita nel sito locale.

C

Connessione da punto a sito (P2S)

Una connessione VPN sicura dall'esterno che usa i dispositivi endpoint (ad esempio un computer o laptop) per collegarsi al cloud e ai siti locali.

Connessione da sito a sito (S2S)

Una connessione che estende la rete locale nel cloud tramite un tunnel VPN sicuro.

F

Failback

Il processo di ripristino dei server nel sito locale dopo lo spostamento dei server nel sito cloud durante il failover.

Failover

Lo spostamento di un carico di lavoro o di un'applicazione nel sito cloud in caso di calamità naturale o provocata dall'uomo nel sito locale.

Finalizzazione

Lo stato intermedio del failover di produzione o del processo di ripristino del server cloud. Il processo implica il trasferimento dei dischi virtuali del server dall'archivio di backup (archivio cold) all'archivio di disaster recovery (archivio hot). Durante la finalizzazione il server è accessibile e funzionale, sebbene con prestazioni inferiori al normale.

G

Gateway VPN (in precedenza noto come server VPN o gateway di connessione)

Una macchina virtuale speciale che fornisce la connessione tra il sito locale e il sito nel cloud tramite un tunnel VPN sicuro. Il gateway VPN viene distribuito nel sito cloud.

I

Indirizzo IP di prova

Un indirizzo IP necessario in caso di prova del failover, per impedire la duplicazione dell'indirizzo IP di produzione.

Indirizzo IP pubblico

Un indirizzo IP necessario per rendere i server cloud disponibili da Internet.

O

Obiettivo punto di ripristino (RPO)

Quantità di dati perduta a causa di un'interruzione, misurata come la quantità di tempo a partire da un'interruzione pianificata o da un'emergenza. La soglia RPO definisce l'intervallo di tempo massimo consentito tra l'ultimo punto di ripristino idoneo per un failover e l'ora corrente.

R

Rete di produzione

La rete interna estesa per mezzo di un tunnel VPN, a copertura dei siti locali e cloud. I server locali e i server cloud possono comunicare tra loro nella rete di produzione.

Rete di prova

Rete virtuale isolata utilizzata per testare il processo di failover.

Runbook

Uno scenario pianificato costituito da passaggi configurabili che automatizzano le azioni da intraprendere in caso di disaster recovery.

S

Server cloud

Riferimenti generali per il ripristino di un server primario.

Server di ripristino

Una replica virtuale della macchina di origine, basata sui backup dei server protetti archiviati nel cloud. I server di ripristino sono utilizzati per trasferire i carichi di lavoro dai server originali in caso di emergenza.

Server primario

Una macchina virtuale che non dispone di una macchina collegata nel sito locale (ad esempio un server di ripristino). I server primari sono utilizzati per proteggere un'applicazione o per eseguire diversi servizi ausiliari, ad esempio un server web.

Server protetto

Un sistema fisico o virtual machine di proprietà di un cliente protetto dal servizio.

Sito cloud (o sito DR)

Sito remoto con hosting nel cloud, utilizzato per l'esecuzione dell'infrastruttura di ripristino in caso di emergenza.

Sito locale

L'infrastruttura locale distribuita nella sede dell'azienda.

Indice