Backup Exec Private Cloud Services

Guida alla distribuzione e alla programmazione

Symantec

Sommario

Capitolo 1

Introduzione a Backup Exec Private Cloud Services

Il capitolo contiene i seguenti argomenti:

Informazioni su Backup Exec Private Cloud Services

Backup Exec Private Cloud Services è pensato per i provider di servizi gestiti (MSP) che desiderano offrire servizi di backup gestiti ai loro clienti. Backup Exec Private Cloud Services consente ai partner di archiviare i backup nei propri datacenter come configurazione "cloud privato".

I provider di servizi gestiti possono fornire servizi di backup su Internet al partner con cloud privato come alternativa alla gestione di copie fuori dall'unità dei nastri. I backup sono crittografati e deduplicati, al fine di rendere la trasmissione dei dati su WAN sicura ed efficiente. I backup locali sono comunque disponibili in sede per un eventuale ripristino veloce. Inoltre Backup Exec Private Cloud Services consente agli utenti di eseguire i backup direttamente nel cloud. Gli utenti possono ripristinare direttamente i dati completi o capillari dal cloud.

Backup Exec Private Cloud Services è pensato anche per i clienti di Backup Exec con reti ampiamente estese. I clienti possono inviare le copie duplicate dei backup dagli uffici remoti all'archiviazione su disco e su nastro all'interno di una posizione cloud privata nel datacenter centrale.

La seguente tabella illustra ulteriormente alcuni termini di Backup Exec importanti per comprendere il funzionamento di Backup Exec Private Cloud Services.

Tabella 1-1 Termini di Backup Exec

Termine	Definizione
Archiviazione su disco per rimozione duplicati	Un dispositivo di archiviazione su disco per rimozione duplicati consente di ottenere una deduplicazione integrata nel server Backup Exec. **Nota:** È possibile utilizzare i dispositivi di archiviazione per rimozione duplicati Symantec NetBackup serie 5000/5020 invece del dispositivo di archiviazione per rimozione duplicati di Backup Exec nel cloud. Un dispositivo può fornire un'opzione più scalabile, specialmente per le grandi configurazioni multi-tenant.
Duplicazione ottimizzata	Un tipo di duplicazione che consente ai dati deduplicati di essere copiati direttamente da un dispositivo OpenStorage a un altro dispositivo OpenStorage dello stesso fornitore.
Tecnologia di recupero capillare (GRT)	Un'opzione di backup che consente di ripristinare i singoli elementi dai backup del database. Un backup separato di singoli elementi non è richiesto per recuperare un elemento.

Vedere "Considerazioni di sicurezza per Backup Exec Private Cloud Services" a pagina 8.

Vedere "Requisiti di sistema per Backup Exec Private Cloud Services" a pagina 10.

Vedere "Configurazione di Backup Exec Private Cloud Services" a pagina 13.

Vedere "Informazioni sulle configurazioni di Backup Exec Private Cloud Services" a pagina 15.

Considerazioni di sicurezza per Backup Exec Private Cloud Services

Backup Exec Private Cloud Services utilizza il modello delle credenziali delle risorse e del processo corrente di Backup Exec per fornire un'esperienza d'uso sicura. Inoltre, Symantec consiglia di utilizzare una connessione di rete sicura

tra la posizione del cliente e il datacenter tramite una soluzione VPN. Sono disponibili diversi IPsec, livelli SSL e altre soluzioni VPN.

È opportuno utilizzare una rete VLAN o restrizioni di routing per mantenere le reti del cliente isolate l'una dall'altra quando viene utilizzata una configurazione che supporta più clienti.

È possibile utilizzare qualsiasi soluzione VPN. Questo manuale fornisce le istruzioni di configurazione per OpenVPN. Il pacchetto open source VPS SSL OpenVPN fornisce una connessione sicura e crittografata tra l'istanza di Backup Exec nel cloud privato e i server Backup Exec locali. Questo componente richiede normalmente che la porta predefinita 1194 sia aperta sul firewall. Tuttavia, OpenVPN consente di configurare qualsiasi altra porta. OpenVPN fornisce metodi di autenticazione in base alla chiave o al certificato. Questo documento fornisce i riferimenti per configurare entrambi i metodi.

Vedere "Informazioni su Backup Exec Private Cloud Services" a pagina 7.

Vedere "Informazioni sulla configurazione di OpenVPN" a pagina 61.

La configurazione di server di Backup Exec multi-tenant ha requisiti di sicurezza aggiuntivi che è necessario tenere in considerazione.

Vedere "Requisiti di sicurezza per la configurazione di server Backup Exec multi-tenant" a pagina 9.

Requisiti di sicurezza per la configurazione di server Backup Exec multi-tenant

È possibile configurare Backup Exec in un cloud privato che consente a un singolo server Backup Exec di supportare più clienti in modo sicuro. È necessario adottare precauzioni di sicurezza aggiuntive quando si utilizza un server Backup Exec per più clienti, poiché ospita contenuti condivisi di più clienti.

Vedere "Informazioni sulla configurazione di server Backup Exec cloud multi-tenant" a pagina 17.

Vedere "Considerazioni di sicurezza per Backup Exec Private Cloud Services" a pagina 8.

È necessario tenere in considerazione i seguenti requisiti di sicurezza quando si configura un server Backup Exec multi-tenant:

- I server Backup Exec gestiti in sede devono essere installati su computer fisici.
- I server Backup Exec gestiti in sede devono avere la funzionalità Microsoft Windows BitLocker attivata sul volume di sistema.

La password di BitLocker non deve essere accessibile a nessun cliente. Come alternativa a BitLocker, è possibile utilizzare una soluzione di crittografia per dischi hardware.

- Il server Backup Exec multi-tenant situato nel cloud privato e i server Backup Exec in sede devono fare parte del dominio del provider di servizi.
  I server Backup Exec non devono consentire l'accesso ai clienti. Per una maggiore sicurezza, si può prendere in considerazione di posizionare il server Backup Exec gestito di ogni cliente in un dominio figlio diverso del provider di servizi.
- Le credenziali del dominio del provider di servizi del server Backup Exec gestito in sede devono corrispondere a quelle di un amministratore locale, ma non di un amministratore di dominio.
- Il dispositivo di archiviazione su disco per rimozione duplicati del server cloud multi-tenant non deve avere la deduplicazione lato client attivata.
- Il server Backup Exec gestito in sede non deve essere installato con l'opzione **Accesso illimitato a cataloghi e set di backup per ripristino**. È necessario installarlo solo con l'opzione **Server Backup Exec gestito centralmente**.
- È possibile utilizzare l'autenticazione a due fattori per i server Backup Exec gestiti in sede, ove applicabile, per fornire un ulteriore livello di sicurezza. Symantec consiglia di utilizzare il servizio di autenticazione VeriSign VIP: http://www.verisign.com/authentication/two-factor-authentication/vip-authentication/index.html

---

Avvertimento: Seguendo questi consigli sulla sicurezza è possibile accedere alla rete e ai dispositivi di archiviazione condivisi di Backup Exec solo fino a un certo punto. Se qualcuno ha accesso fisico a un server Backup Exec gestito e intende eseguire azioni nocive, in teoria potrebbe aggirare queste misure di sicurezza. Potrebbe essere necessario prendere in considerazione l'utilizzo di misure di protezione aggiuntive per i server Backup Exec gestiti in sede.

Requisiti di sistema per Backup Exec Private Cloud Services

La tabella seguente elenca i requisiti minimi di sistema e le raccomandazioni per eseguire Backup Exec Private Cloud Services:

Tabella 1-2 Requisiti di sistema per Backup Exec Private Cloud Services

Requisito	Descrizione
Server Backup Exec	È possibile configurare Backup Exec Private Cloud Services in tre modi differenti. Vedere "Informazioni sulle configurazioni di Backup Exec Private Cloud Services" a pagina 15. Qualsiasi server Backup Exec nel cloud deve includere l'opzione Backup Exec Deduplication Option. L'unico requisito per i server locali è che devono soddisfare i requisiti di Backup Exec 2012. È possibile trovare un elenco dei sistemi operativi, delle piattaforme e delle applicazioni compatibili al seguente URL: http://entsupport.symantec.com/umi/V-269-1
Licenza Deduplication Option	È necessario installare Symantec Backup Exec Deduplication Option sia sul server del cloud privato che sui server Backup Exec locali. Non è necessario creare un dispositivo di archiviazione su disco per rimozione duplicati nel server Backup Exec locale. Tuttavia, è necessario installare Deduplication Option nel server Backup Exec locale per accedere al dispositivo di archiviazione su disco per rimozione duplicati condiviso sul server nel cloud. Tutte le configurazioni richiedono un dispositivo di archiviazione su disco per rimozione duplicati sul server Backup Exec nel cloud.
Licenza Central Admin Server Option	È necessario installare Symantec Backup Exec Enterprise Server Option con Central Admin Server Option nel computer locale o nel cloud se si utilizzano le configurazioni multi-tenant o copia fuori dall'unità.

Requisito	Descrizione
Una connessione attiva ad Internet	È necessario avere una connessione a Internet per trasferire i dati nel dispositivo di archiviazione su disco per rimozione duplicati del cloud privato.
Virtual Private Network (VPN)	Symantec consiglia di utilizzare una connessione di rete sicura tra la posizione del cliente e il datacenter utilizzando una soluzione VPN. Sono disponibili diverse soluzioni IPsec e VPN a livello di SSL. Questa guida fornisce le istruzioni di configurazione per OpenVPN. Il pacchetto open source VPS SSL OpenVPN fornisce una connessione sicura e crittografata tra l'istanza di Backup Exec nel cloud privato e i server Backup Exec locali.

Capitolo 2

Configurazione di Backup Exec Private Cloud Services

Il capitolo contiene i seguenti argomenti:

Configurazione di Backup Exec Private Cloud Services

Per configurare Backup Exec Private Cloud Services, è necessario completare i seguenti passaggi.

Tabella 2-1 Come configurare Backup Exec Private Cloud Services

Passaggio	Descrizione
Passaggio 1	È necessario configurare la rete VPN tra l'istanza del server Backup Exec nel cloud privato e qualsiasi computer in esecuzione nella rete locale. Vedere "Configurazione di OpenVPN" a pagina 62. Vedere "Informazioni sulla configurazione di OpenVPN per client multipli" a pagina 68.

Passaggio	Descrizione
Passaggio 2	Considerare quale configurazione di Backup Exec Private Cloud Services si adatta meglio alle proprie esigenze, quindi selezionarne una. È possibile scegliere una singola configurazione multi-tenant per più clienti. In alternativa è possibile utilizzare una copia fuori dall'unità dedicata alla configurazione del cloud o del backup diretto per ciascun cliente. Vedere "Informazioni sulle configurazioni di Backup Exec Private Cloud Services" a pagina 15. È necessario configurare Backup Exec Private Cloud Services. Vedere "Impostazione delle configurazioni multi-tenant o copia fuori dall'unità nel cloud" a pagina 23. Vedere "Impostazione della configurazione dei backup diretti" a pagina 35.
Passaggio 3	Dopo avere configurato la rete VPN e Backup Exec, è possibile cominciare a lavorare con Backup Exec Private Cloud Services. Vedere "Informazioni su come lavorare con Backup Exec Private Cloud Services per le configurazioni copia fuori dall'unità" a pagina 41. Vedere "Informazioni su come lavorare con Backup Exec Private Cloud Services e la configurazione di backup diretti" a pagina 49.

Passaggio	Descrizione
Passaggio 4	Se si utilizza un gateway VPN con restrizioni per le porte, potrebbe essere necessario definire eccezioni per le porte sui gateway VPN sia in sede, sia nel cloud. Le eccezioni per le porte consentono al server Backup Exec situato nel cloud di comunicare con i server e gli agenti Backup Exec in sede. È anche necessario modificare la porta SQL di Backup Exec CAS da porta assegnata dinamicamente a porta statica. **Nota:** Se si utilizza OpenVPN, potrebbe essere necessario configurare eccezioni per la porta firewall del gateway. OpenVPN è configurato tipicamente per effettuare il tunneling attraverso i firewall. I seguenti articoli di supporto per Backup Exec presentano un elenco di tutti i numeri di porta che Backup Exec richiede e indicano quali devono essere aperti: http://www.symantec.com/business/support/index?page=content&id=HOWTO22990#id-SF700155293 http://www.symantec.com/business/support/index?page=content&id=HOWTO22989 http://www.symantec.com/business/support/index?page=content&id=HOWTO23022 Il seguente articolo di supporto di Backup Exec spiega in modo dettagliato come configurare la porta statica SQL: http://www.symantec.com/business/support/index?page=content&id=HOWTO22985

Informazioni sulle configurazioni di Backup Exec Private Cloud Services

È possibile configurare Backup Exec Private Cloud Services in quattro modi diversi.

Tabella 2-2 Configurazioni specifiche per Backup Exec Private Cloud Services

Tipo di configurazione	Dettagli
Server Backup Exec cloud multi-tenant	La configurazione server Backup Exec cloud multi-tenant invia una copia fuori dall'unità e un backup diretto a un server Backup Exec o a un server di amministrazione centrale situato nel cloud privato. Il singolo server Backup Exec privato nel cloud può essere utilizzato per eseguire il backup dei dati per più clienti. Vedere "Informazioni sulla configurazione di server Backup Exec cloud multi-tenant" a pagina 17.
Copia fuori dall'unità nel server cloud Backup Exec gestito	La configurazione copia fuori dall'unità nel server cloud Backup Exec utilizza un server Backup Exec gestito, un server di amministrazione centrale e un controller di dominio. Questa configurazione consente di copiare i dati fuori dall'unità in un server Backup Exec gestito, situato nel cloud privato. Questa configurazione richiede un server Backup Exec gestito per ciascun cliente. Vedere "Informazioni sulla configurazione copia fuori dall'unità nel server Backup Exec gestito nel cloud" a pagina 20.
Copia fuori dall'unità nel server cloud di amministrazione centrale	La configurazione di copia fuori dall'unità nel server cloud di amministrazione centrale è simile alla prima, tranne per il fatto che le posizioni del server di amministrazione centrale e del server Backup Exec gestito sono invertite. Questa configurazione consente di copiare i dati fuori dall'unità in un server di amministrazione centrale situato nel cloud privato. Questa configurazione richiede un server di amministrazione centrale per ciascun cliente. Vedere "Informazioni sulla copia fuori dall'unità per la configurazione del server di amministrazione centrale del cloud" a pagina 21.

Tipo di configurazione	Dettagli
Backup diretto	La configurazione di backup diretto utilizza Backup Exec Agent for Windows o Backup Exec Agent for Linux invece del server Backup Exec gestito o del server di amministrazione centrale. Questa configurazione consente di effettuare backup diretti utilizzando un server Backup Exec situato nel cloud privato. Questa configurazione richiede un server Backup Exec per ciascun cliente. Vedere "Informazioni sulla configurazione diretta del backup" a pagina 22.

Vedere "Informazioni sulla configurazione di OpenVPN" a pagina 61.

Vedere "Impostazione delle configurazioni multi-tenant o copia fuori dall'unità nel cloud" a pagina 23.

Vedere "Impostazione della configurazione dei backup diretti" a pagina 35.

Informazioni sulla configurazione di server Backup Exec cloud multi-tenant

La configurazione di server Backup Exec cloud multi-tenant riguarda più computer.

Tabella 2-3 Configurazione di server Backup Exec cloud multi-tenant

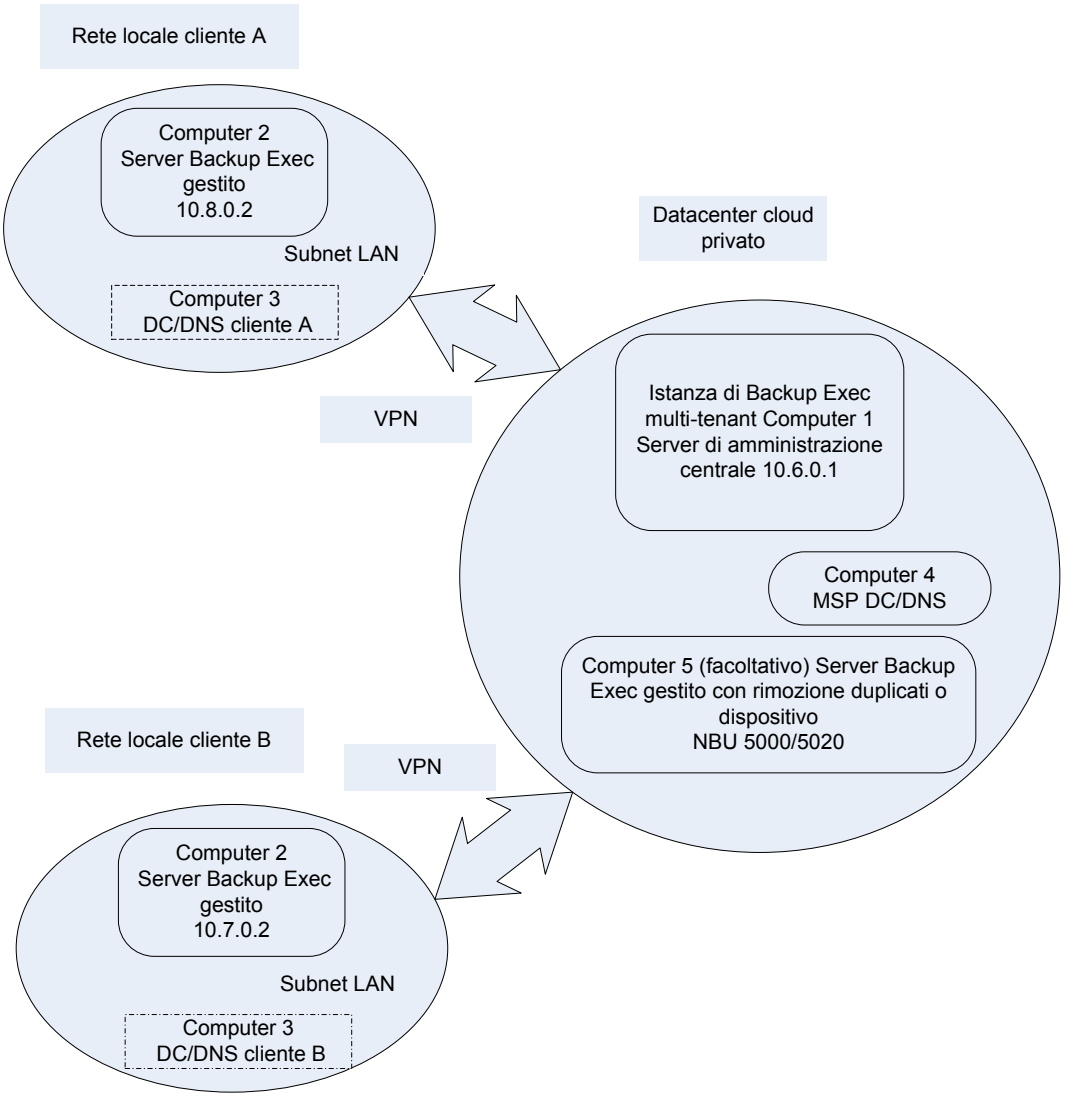
Computer	Ruolo
Computer 1	Il primo computer (C1) è un server a 64 bit di Windows su cui è installato Backup Exec 2012. C1 è configurato come un server di amministrazione centrale ed è situato nel cloud privato.
Computer 2	Il secondo computer (C2) è un server Windows su cui è installato Backup Exec 2012. Il C2 è un server Backup Exec gestito situato sulla rete locale e fa parte del dominio del cloud del provider di servizi (C4). **Nota:** È possibile utilizzare un server Backup Exec locale a 32 bit per C2 se non si desidera utilizzare un dispositivo di archiviazione su disco per rimozione duplicati locale.

Computer	Ruolo
Computer 3	Il terzo computer (C3) è un controller di dominio e DNS. È necessario configurare un computer C3 per ogni posizione del cliente.
Computer 4	Il quarto computer (C4) è un controller di dominio e DNS situato nel cloud privato.
Computer 5 (facoltativo)	Il quinto computer (C5) è un server Backup Exec gestito facoltativo ma consigliato. C5 include una cartella di archiviazione per rimozione duplicati che può essere utilizzata per replicare il dispositivo di archiviazione per rimozione duplicati del computer C1 per aggiungere tolleranza di errore e affidabilità ulteriori. C5 può essere individuato nel cloud privato con C1 o può essere situato in un'ubicazione fisica differente. È possibile configurare un dispositivo di archiviazione per rimozione duplicati NetBackup serie 5000/5020 come dispositivo OST sul server Backup Exec cloud come alternativa a un computer C5 nella stessa ubicazione.

Questa configurazione consente di gestire tutti i processi di Backup Exec all'interno del datacenter del cloud privato. Tuttavia, richiede che le connessioni di rete tra il server di amministrazione centrale e i server Backup Exec gestito siano sempre attive. Le connessioni di rete devono essere attive anche quando si eseguono i processi localmente.

Avvertimento: Se sono supportati più clienti in un singolo server Backup Exec cloud, Symantec richiede che C1, il C2, C4 e C5 siano contenuti in un dominio a cui solo l'amministratore può accedere. Per evitare qualsiasi attività accidentale o nociva che può comportare un rischio per la sicurezza, non è necessario dare ai clienti alcun tipo di credenziale di accesso a C2.

Figura 2-1 Server Backup Exec cloud multi-tenant



Vedere "Informazioni sulle configurazioni di Backup Exec Private Cloud Services" a pagina 15.

Informazioni sulla configurazione copia fuori dall'unità nel server Backup Exec gestito nel cloud

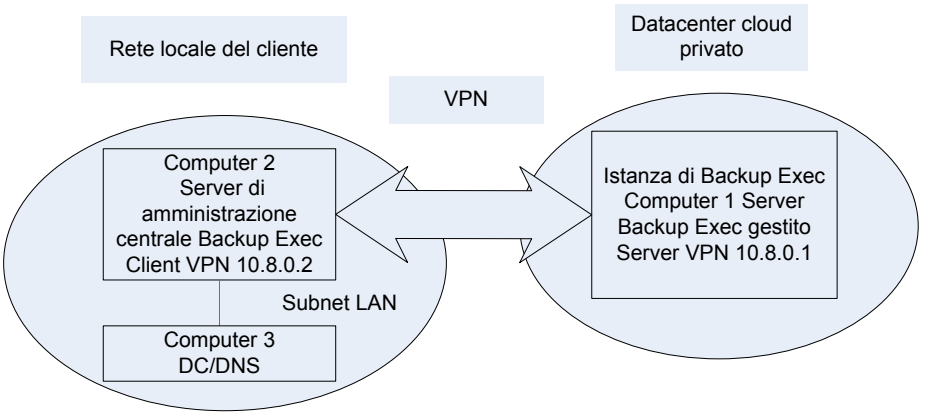
La configurazione copia fuori dall'unità del server Backup Exec gestito comprende tre computer.

Tabella 2-4 Configurazione copia fuori dall'unità su server Backup Exec gestito nel cloud

Computer	Ruolo
Computer 1	Il primo computer (C1) è un server Windows a 64 bit su cui è installato Backup Exec 2012. C1 è configurato come un server Backup Exec gestito ed è situato nel cloud privato.
Computer 2	Il secondo computer (C2) è un server Windows a 64 bit su cui è installato Backup Exec 2012. C2 è un server di amministrazione centrale situato sulla rete locale. **Nota:** Si può utilizzare un server Backup Exec locale a 32 bit per C2 se non si desidera utilizzare un dispositivo di archiviazione su disco per rimozione duplicati locale.
Computer 3	Il terzo computer (C3) è un controller di dominio e DNS.

La connessione di rete tra il server di amministrazione centrale e il server Backup Exec gestito non deve necessariamente essere sempre attiva. La connessione di rete è necessaria solo quando si eseguono processi che coinvolgono il server Backup Exec gestito nel cloud privato. La connessione di rete non deve necessariamente essere sempre attiva per i processi locali.

Figura 2-2 Copia fuori dall'unità nel server cloud Backup Exec gestito



Vedere "Informazioni sulle configurazioni di Backup Exec Private Cloud Services" a pagina 15.

Informazioni sulla copia fuori dall'unità per la configurazione del server di amministrazione centrale del cloud

La copia fuori dall'unità per la configurazione del server di amministrazione centrale del cloud prevede l'utilizzo di tre computer.

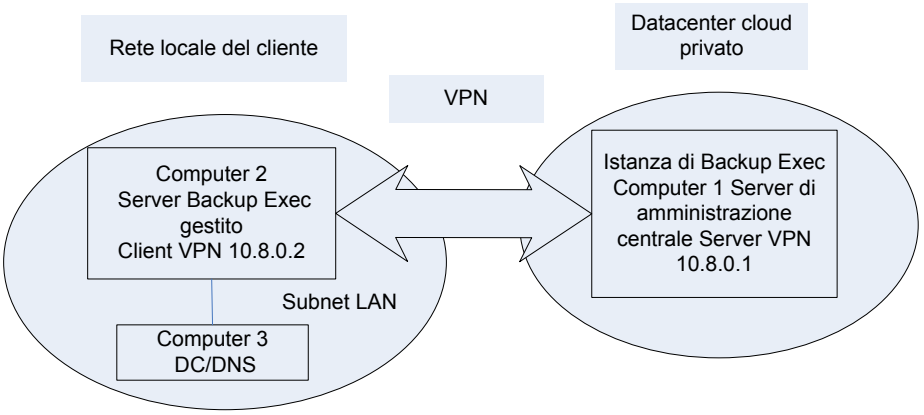
Tabella 2-5 La copia fuori dall'unità per la configurazione del server di amministrazione centrale del cloud

Computer	Ruolo
Computer 1	Il primo computer (C1) è un server Windows a 64 bit su cui è installato Backup Exec 2012. C1 è configurato come un server di amministrazione centrale ed è situato nel cloud privato.
Computer 2	Il secondo computer (C2) è un server Windows a 64 bit su cui è installato Backup Exec 2012. C2 è un server Backup Exec gestito situato sulla rete locale. **Nota:** Si può utilizzare un server Backup Exec locale a 32 bit per C2 se non si desidera utilizzare un dispositivo di archiviazione su disco per rimozione duplicati locale.

Computer	Ruolo
Computer 3	Il terzo computer (C3) è un controller di dominio e DNS.

Questa configurazione consente di gestire tutti i processi di Backup Exec all'interno del datacenter del cloud privato. Tuttavia, richiede che la connessione di rete tra il server di amministrazione centrale e il server Backup Exec gestito sia sempre attiva. La connessione di rete deve essere attiva anche quando si eseguono i processi localmente.

Figura 2-3 Copia fuori dall'unità nel server cloud di amministrazione centrale



Vedere "Informazioni sulle configurazioni di Backup Exec Private Cloud Services" a pagina 15.

Informazioni sulla configurazione diretta del backup

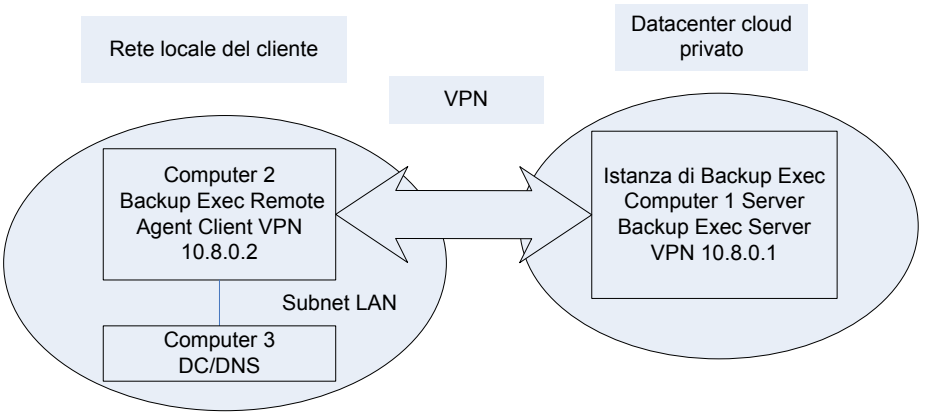
La configurazione diretta del backup prevede l'impiego di minimo tre computer.

Tabella 2-6 Configurazione diretta del backup

Computer	Ruolo
Computer 1	Il primo computer (C1) è il server Backup Exec 2012 del server Windows a 64 bit situato nel datacenter del cloud privato.
Computer 2	Il secondo computer (C2) è il client Agent for Windows o Agent for Linux situato sulla rete locale. Si possono configurare più computer client per l'Agent.

Computer	Ruolo
Computer 3	Il terzo computer (C3) è un controller di dominio e DNS.

Figura 2-4 Backup diretto



Vedere "Informazioni sulle configurazioni di Backup Exec Private Cloud Services" a pagina 15.

Impostazione delle configurazioni multi-tenant o copia fuori dall'unità nel cloud

Dopo aver configurato OpenVPN nel server del cloud privato, configurare il server o i server Backup Exec.

Vedere "Configurazione di Backup Exec Private Cloud Services" a pagina 13.

È possibile selezionare una configurazione multi-tenant o una tra due configurazioni copia fuori dall'unità:

Vedere "Informazioni sulla configurazione di server Backup Exec cloud multi-tenant" a pagina 17.

Vedere "Informazioni sulla configurazione copia fuori dall'unità nel server Backup Exec gestito nel cloud" a pagina 20.

Vedere "Informazioni sulla copia fuori dall'unità per la configurazione del server di amministrazione centrale del cloud" a pagina 21.

Tabella 2-7 Come configurare la copia al di fuori delle configurazioni del cloud

Passaggio	Descrizione
Passaggio 1	Installare il server di amministrazione centrale di Backup Exec. Vedere "Installazione del server di amministrazione centrale di Backup Exec" a pagina 24.
Passaggio 2	Installare il server Backup Exec gestito. Vedere "Installazione del server Backup Exec gestito" a pagina 26.
Passaggio 3	Configurare i dispositivi di archiviazione. Vedere "Impostare i dispositivi di archiviazione per le configurazioni multi-tenant e copia fuori dall'unità" a pagina 28.
Passaggio 4	Eseguire il seeding dei dati del dispositivo di archiviazione su disco per rimozione duplicati. Vedere "Informazioni sul seeding del dispositivo di archiviazione su disco per rimozione duplicati per le configurazioni copia fuori dall'unità" a pagina 30.

Installazione del server di amministrazione centrale di Backup Exec

Si deve installare Backup Exec per Windows Server sul computer che funziona da server di amministrazione centrale di Backup Exec.

Vedere "Impostazione delle configurazioni multi-tenant o copia fuori dall'unità nel cloud" a pagina 23.

Se si utilizza la configurazione server cloud Backup Exec per più client, il server cloud Backup Exec deve essere installato come server di amministrazione centrale (computer 1 o C1).

Se si utilizza la configurazione copia fuori dall'unità nel server cloud Backup Exec gestito, il server di amministrazione centrale viene installato su un server Backup Exec dell'ufficio locale (computer 2 o C2). In caso contrario, il server di amministrazione centrale viene installato come server cloud Backup Exec (computer 1 o C1) per la configurazione copia fuori dall'unità nel server di amministrazione centrale nel cloud.

È necessario aggiungere il server di amministrazione centrale a un dominio. Installare l'opzione Enterprise Server con Central Admin Server Option (CASO) nel server di amministrazione centrale.

Tabella 2-8 Modalità di installazione del server di amministrazione centrale di Backup Exec

Passaggio	Descrizione
Passaggio 1	Per configurare un server Backup Exec multi-tenant, aggiungere il server Backup Exec al dominio del cloud. Per qualsiasi configurazione diversa dalla configurazione del server Backup Exec multi-tenant, aggiungere il server Backup Exec al dominio locale completando i seguenti passaggi: ■ Utilizzando la finestra di dialogo Proprietà del computer in Windows, aggiungere il server al dominio. ■ Riavviare il computer quando viene richiesto.
Passaggio 2	Dopo il riavvio del server, accedere con l'account del dominio a cui si desidera assegnare i diritti di amministrazione all'istanza locale di Backup Exec.
Passaggio 3	Utilizzare le chiavi di licenza adeguate per installare Backup Exec 2012. Per ulteriori informazioni sull'installazione di Backup Exec, consultare il *Manuale dell'amministratore di Backup Exec*. I partner Backup Exec possono ottenere le informazioni sulle licenze dal sito Web di Symantec PartnerNet accedendo al collegamento seguente: https://partnernet.symantec.com/Partnercontent/Login.jsp
Passaggio 4	Includere l'opzione Enterprise Server con Central Admin Server Option (CASO) quando si installa Backup Exec. Per ulteriori informazioni sull'installazione di CASO, consultare il *Manuale dell'amministratore di Symantec Backup Exec*. Installare Deduplication Option quando si utilizzano le configurazioni multi-tenant o la copia fuori dall'unità nel server di amministrazione centrale. L'utilizzo del dispositivo locale di archiviazione su disco per rimozione duplicati nel server di amministrazione centrale è facoltativo per la configurazione copia fuori dall'unità su server Backup Exec gestito nel cloud.
Passaggio 5	Utilizzare le credenziali del dominio per l'account di accesso predefinito del sistema quando si installa Backup Exec.

Passaggio	Descrizione
Passaggio 6	Se si desidera eseguire i processi incrementali del backup di duplicazione Exchange GRT nel cloud, impostare il seguente valore di registro su **1** quando l'installazione è completa. Con la modifica del valore di registro viene disattivata la capacità di copia duplicata GRT-to-GRT del dispositivo di archiviazione su disco per rimozione duplicati nel server Backup Exec. dword HKEY LOCAL MACHINE\SOFTWARE\Symantec\Backup Exec for Windows\Backup Exec\Engine\Misc\DisablePDI2PDISetCopy Questo computer è ora il server di amministrazione centrale che controlla il server Backup Exec gestito in tutta la rete WAN. Per ulteriori informazioni sulle limitazioni della Tecnologia di recupero capillare (GRT) per la copia fuori dall'unità, fare riferimento all'argomento seguente: Vedere "Limitazioni sulla tecnologia di recupero capillare con la copia fuori dall'unità" a pagina 59.

Installazione del server Backup Exec gestito

È necessario installare il server Backup Exec gestito. Se si utilizza la configurazione copia fuori dall'unità nel server Backup Exec gestito nel cloud, il server Backup Exec gestito viene installato come server Backup Exec del cloud (computer 1 - C1). In caso contrario, il server Backup Exec gestito viene installato su un server Backup Exec dell'ufficio locale (computer 2 - C2).

Vedere "Impostazione delle configurazioni multi-tenant o copia fuori dall'unità nel cloud" a pagina 23.

Per installare un server Backup Exec gestito

1 Eseguire una delle seguenti operazioni:

Per la configurazione multi-tenant:	Aggiungere il server Backup Exec al dominio del cloud.

Per qualunque altra configurazione:	Aggiungere il server Backup Exec al dominio locale completando i seguenti passaggi: ■ Utilizzando la finestra di dialogo Proprietà del computer in Windows, aggiungere il server al dominio. ■ Riavviare il computer quando viene richiesto.

2. Dopo il riavvio del server, accedere con l'account del dominio con i diritti di amministrazione al server locale di Backup Exec.
3. Installare Backup Exec 2012 sul server e selezionare l'opzione di installazione **Server Backup Exec gestito**.
4. Quando richiesto, inserire le stesse credenziali di account di accesso al sistema utilizzate per installare il server di amministrazione centrale.
5. Se si desidera utilizzare la configurazione copia fuori dall'unità nel server Backup Exec gestito nel cloud, selezionare **Deduplication Option**.

   L'utilizzo del dispositivo locale di archiviazione su disco per rimozione duplicati nel server Backup Exec gestito è facoltativo per la configurazione copia fuori dall'unità su server Backup Exec gestito nel cloud.
6. Quando Backup Exec richiede il server di amministrazione centrale, immettere le informazioni relative al server Backup Exec locale di amministrazione centrale.
7. Selezionare l'opzione **Server Backup Exec gestito centralmente**.

   Non selezionare **Accesso illimitato a cataloghi e set di backup per ripristino** se si utilizza la configurazione multi-tenant.
8. Se si desidera eseguire i processi incrementali del backup di duplicazione Exchange GRT nel cloud, impostare il seguente valore di registro su **1** quando l'installazione è completa.

   dword HKEY LOCAL MACHINE\SOFTWARE\Symantec\Backup Exec for Windows\Backup Exec\Engine\Misc\DisablePDI2PDISetCopy

   Con la modifica del valore di registro viene disattivata la capacità di copia duplicata GRT-to-GRT del dispositivo di archiviazione su disco per rimozione duplicati nel server Backup Exec.
9. Aprire Backup Exec nel server di amministrazione centrale.
10. Selezionare la scheda **Archiviazione**, quindi fare doppio clic sul server Backup Exec situato nel datacenter privato del cloud.

11 Nel riquadro sinistro, fare clic su **Impostazioni**.

12 Nel campo **Cloud server privato**, selezionare **Attivato**.

Impostare i dispositivi di archiviazione per le configurazioni multi-tenant e copia fuori dall'unità

Prima di eseguire i processi di backup al cloud privato, si devono configurare i dispositivi di archiviazione.

Vedere "Impostazione delle configurazioni multi-tenant o copia fuori dall'unità nel cloud" a pagina 23.

Tabella 2-9 Come impostare i dispositivi di archiviazione per le configurazioni della copia fuori dall'unità

Passaggio	Descrizione
Passaggio 1	Creazione di nuovi dispositivi di archiviazione su disco locali nel computer locale 2 (C2). Se lo si desidera, è possibile creare un dispositivo di archiviazione su disco per rimozione duplicati. Per ulteriori informazioni sulla creazione di dispositivi di archiviazione, consultare il *Manuale dell'amministratore di Symantec Backup Exec*.

Passaggio	Descrizione
Passaggio 2	Creare un nuovo dispositivo di archiviazione su disco per rimozione duplicati sull'istanza di Backup Exec nel cloud privato. È possibile configurare il dispositivo di archiviazione NetBackup serie 5000/5020 per la configurazione multi-tenant invece di utilizzare l'archiviazione per rimozione duplicati integrata. Configurare il dispositivo come dispositivo di archiviazione OST nel server di amministrazione centrale multi-tenant. Per ulteriori informazioni su come creare un dispositivo di archiviazione su disco per rimozione duplicati, consultare il *Manuale dell'amministratore di Symantec Backup Exec*. Se si utilizza la configurazione multi-tenant, occorre completare i seguenti passaggi per disattivare la deduplicazione lato client per il dispositivo di archiviazione su disco per rimozione duplicati nel cloud: ■ Fare doppio clic sul dispositivo di archiviazione su disco per rimozione duplicati del server Backup Exec nel cloud privato, nella scheda **Archiviazione**. ■ Selezionare **Proprietà**. ■ Nel campo **Deduplicazione lato client**, selezionare **Disattivata**. ■ Riavviare i servizi del server Backup Exec. Symantec consiglia di utilizzare un volume dedicato per il dispositivo di archiviazione su disco per rimozione duplicati, se possibile. Assegnare al dispositivo di archiviazione su disco per rimozione duplicati un nome univoco per differenziarlo in modo semplice dal dispositivo di archiviazione su disco per rimozione duplicati, se ne è stato creato uno.
Passaggio 3	Se si desidera che i dati a riposo vengano crittografati nel dispositivo di archiviazione su disco per rimozione duplicati del cloud privato, selezionare **Sì, crittografare i dati durante la trasmissione a questo dispositivo di archiviazione su disco per rimozione duplicati e mentre il dispositivo contiene dati** quando si configura un nuovo dispositivo di archiviazione su disco per rimozione duplicati. Per un dispositivo di rimozione duplicati esistente, è possibile modificare il campo **Crittografia** nella proprietà del dispositivo di rimozione duplicati. **Nota:** VPN crittografa i dati in transito tra il server Backup Exec locale e il server Backup Exec nel cloud.

Passaggio	Descrizione
Passaggio 4	Condividere il nuovo dispositivo di archiviazione su disco per rimozione duplicati con il computer locale di Backup Exec. Per ulteriori informazioni sulla condivisione di dispositivi di archiviazione su disco per rimozione duplicati, consultare il *Manuale dell'amministratore di Symantec Backup Exec*.
Passaggio 5	Utilizzare Gestione servizi di Backup Exec per arrestare e riavviare tutti i servizi di Backup Exec sul server Backup Exec locale. Il processo di condivisione del dispositivo di archiviazione su disco per rimozione duplicati del cloud con il server Backup Exec locale è ora completo. Il dispositivo di archiviazione su disco per rimozione duplicati nel cloud privato deve essere essere visibile e accessibile sia da C1 che da C2.
Passaggio 6 (Facoltativo)	Per la configurazione multi-tenant, è possibile installare un ulteriore server Backup Exec gestito con un dispositivo di archiviazione su disco per rimozione duplicati nel cloud. Il server Backup Exec gestito aggiuntivo può essere condiviso con il server Backup Exec primario nel cloud per replicare il dispositivo di archiviazione per rimozione duplicati del server primario. È possibile installare un dispositivo di archiviazione per rimozione duplicati NetBackup 5000/5020 come alternativa al server Backup Exec gestito aggiuntivo. Il dispositivo può essere utilizzato per la replica. Aggiungere il dispositivo come dispositivo di archiviazione OST sul server Backup Exec primario nel cloud. **Avvertimento:** È necessario disattivare la deduplicazione lato client per una o l'altra di queste configurazioni facoltative.

Informazioni sul seeding del dispositivo di archiviazione su disco per rimozione duplicati per le configurazioni copia fuori dall'unità

Per evitare lunghi tempi di trasferimento su Internet, è possibile effettuare il seeding del dispositivo di archiviazione su disco per rimozione duplicati nel cloud con i dati necessari per l'avvio. Il seeding del dispositivo di archiviazione su disco per rimozione duplicati è il processo di collocazione dei file di configurazione iniziale o dei set di backup nel dispositivo di archiviazione su disco per rimozione duplicati per prepararlo all'uso. I tempi di trasferimento dipendono dalla quantità di dati da copiare e di cui eseguire il backup in un'istanza di Backup Exec nel cloud privato.

Si può eseguire il seeding dei dati iniziali utilizzando due metodi, a seconda del tipo di dati:

- Si può eseguire il seeding del dispositivo di archiviazione su disco per rimozione duplicati con i backup del sistema operativo System State. Eseguire il seeding del dispositivo di archiviazione su disco per rimozione duplicati tramite processi di backup di duplicazione dei dati di System State di altri computer in esecuzione nel cloud privato. Eseguire il backup dei dati dello stato del sistema per i computer che eseguono lo stesso sistema operativo come i computer locali di cui si desidera eseguire il backup.
  Vedere "Esecuzione del seeding dei file di sistema per le configurazioni copia fuori dall'unità." a pagina 31.
- Si può inviare un'unità di trasferimento fisica che contiene i set di backup con i dati pertinenti dal server locale di Backup Exec al datacenter del cloud privato.
  Vedere "Informazioni sull'utilizzo di un'unità di trasferimento per eseguire il seeding del dispositivo di archiviazione su disco per rimozione duplicati per le configurazioni copia fuori dall'unità" a pagina 32.

Esecuzione del seeding dei file di sistema per le configurazioni copia fuori dall'unità.

Per evitare lunghi tempi di trasferimento su Internet, è possibile effettuare il seeding del dispositivo di archiviazione su disco per rimozione duplicati nel cloud con i dati necessari per l'avvio. Un modo per eseguire il seeding del dispositivo di archiviazione su disco per rimozione duplicati è utilizzare i dati del backup di System State provenienti da altri computer nella stessa posizione.

Vedere "Informazioni sul seeding del dispositivo di archiviazione su disco per rimozione duplicati per le configurazioni copia fuori dall'unità" a pagina 30.

Tabella 2-10 Come eseguire il seeding dei file del sistema operativo per le configurazioni fuori dall'unità

Passaggio	Descrizione
Passaggio 1	Installare Agent for Windows o Agent for Linux su qualsiasi computer nella stessa posizione nel cloud privato. Per ulteriori informazioni sull'installazione degli agenti di Backup Exec, consultare il *Manuale dell'amministratore di Backup Exec*. I computer devono utilizzare le stesse versioni del sistema operativo dei server su cui si deve eseguire il backup nelle reti del cliente locale.
Passaggio 2	Creare ed eseguire i processi di backup nel server Backup Exec del cloud privato. Eseguire il backup dei volumi di System State e dei volumi del sistema dei computer nella stessa posizione nel dispositivo di archiviazione su disco per rimozione duplicati nel cloud privato.

Informazioni sull'utilizzo di un'unità di trasferimento per eseguire il seeding del dispositivo di archiviazione su disco per rimozione duplicati per le configurazioni copia fuori dall'unità

Per evitare lunghi tempi di trasferimento su Internet, è possibile effettuare il seeding del dispositivo di archiviazione su disco per rimozione duplicati nel cloud con i dati necessari per l'avvio. Un modo per eseguire il seeding del dispositivo di archiviazione su disco per rimozione duplicati è utilizzare un'unità di trasferimento fisica.

Vedere "Informazioni sul seeding del dispositivo di archiviazione su disco per rimozione duplicati per le configurazioni copia fuori dall'unità" a pagina 30.

Symantec fornisce uno strumento di calcolo che consente di confrontare il tempo necessario per utilizzare un'unità di trasferimento con il tempo necessario per copiare i dati su Internet. È possibile trovare il calcolatore al collegamento seguente:

http://entsupport.symantec.com/umi/V-269-34

Per eseguire il seeding dell'istanza di Backup Exec nel cloud privato utilizzando un'unità di trasferimento, attenersi alla procedura seguente:

Vedere "Seeding del dispositivo di archiviazione su disco per rimozione duplicati con un'unità di trasferimento per le configurazioni copia fuori dall'unità" a pagina 32.

Seeding del dispositivo di archiviazione su disco per rimozione duplicati con un'unità di trasferimento per le configurazioni copia fuori dall'unità

È possibile utilizzare un'unità di trasferimento fisica per eseguire il seeding del dispositivo di archiviazione su disco per rimozione duplicati di Backup Exec nel cloud privato. Il seeding del dispositivo di archiviazione su disco per rimozione duplicati con i file necessari per l'avvio consente di risparmiare tempo durante l'esecuzione di un backup di grandi dimensioni su Internet.

Vedere "Informazioni sull'utilizzo di un'unità di trasferimento per eseguire il seeding del dispositivo di archiviazione su disco per rimozione duplicati per le configurazioni copia fuori dall'unità" a pagina 32.

Per eseguire il seeding del dispositivo di archiviazione su disco per rimozione duplicati tramite un'unità di trasferimento per le configurazioni copia fuori dall'unità

1. Creare l'archiviazione su disco su un'unità portatile nel server locale di Backup Exec, ovvero il computer 2 (C2).
2. Copiare un set di backup nel dispositivo di archiviazione su disco e crittografare i dati con crittografia del software tramite uno dei seguenti metodi:

Se non è stata creata la chiave di registro "DisablePDI2PDISetCopy" durante l'installazione, è possibile duplicare set di backup	Completare i seguenti passaggi: ■ Selezionare per la duplicazione gli ultimi set di backup completi dei dati che si desidera utilizzare per eseguire il seeding del dispositivo di archiviazione su disco con rimozione dei duplicati nel cloud privato. ■ Selezionare il dispositivo di archiviazione su disco creato come destinazione di archiviazione nella finestra di dialogo **Processo di duplicazione**. ■ Configurare la crittografia del software nella finestra di dialogo **Processo di duplicazione**. È necessario creare o selezionare una chiave di crittografia per crittografare il software.

Se è stata creata la chiave di registro "DisablePDI2PDISetCopy" durante l'installazione, è necessario creare un processo di backup completo	Completare i seguenti passaggi: ■ Creare un processo di backup completo che utilizza l'archiviazione su disco per tutte le applicazioni che utilizzano la tecnologia di recupero capillare di Symantec (GRT). ■ Disattivare la GRT per tutte le applicazioni specifiche che la utilizzano e di cui si desidera eseguire il backup. Fare riferimento al seguente argomento per ulteriori informazioni sulle limitazioni alla GRT della copia fuori dall'unità. Vedere "Limitazioni sulla tecnologia di recupero capillare con la copia fuori dall'unità" a pagina 59. ■ Attivare la crittografia del software nella finestra **Archiviazione**. È necessario creare o selezionare una chiave di crittografia per crittografare il software.

3. Eseguire il processo creato nel passaggio precedente.
4. Inviare il disco rimovibile al datacenter del cloud privato.
5. Allegare il disco rimovibile al server Backup Exec nel cloud privato.
6. Creare l'archiviazione su disco sull'unità portatile allegata utilizzando l'archiviazione su disco creata in precedenza sull'unità.
7. Creare ed eseguire un'operazione di inventario di Backup Exec nel dispositivo di archiviazione su disco portatile.
8. Creare ed eseguire un'operazione di catalogo di Backup Exec nel dispositivo di archiviazione portatile su disco.

9 Duplicare i set di backup nel dispositivo di archiviazione su disco e utilizzare il dispositivo di archiviazione su disco per rimozione duplicati del cloud come dispositivo di archiviazione di destinazione.

10 Una volta completata l'operazione, è possibile utilizzare Backup Exec per ritirare ed eliminare i file nell'archiviazione su disco. Utilizzare un'utilità disco per eliminare i dati dall'unità rimovibile.

Al termine del processo di seeding del dispositivo di archiviazione su disco per rimozione duplicati nel cloud privato, il processo di configurazione è completo. Si può procedere all'argomento seguente per iniziare a lavorare in Backup Exec:

Vedere "Informazioni su come lavorare con Backup Exec Private Cloud Services per le configurazioni copia fuori dall'unità" a pagina 41.

Impostazione della configurazione dei backup diretti

Dopo aver configurato OpenVPN sul server del cloud privato, configurare il server o i server di Backup Exec.

Vedere "Configurazione di Backup Exec Private Cloud Services" a pagina 13.

La configurazione diretta del backup prevede l'impiego di minimo tre computer.

Vedere "Informazioni sulla configurazione diretta del backup" a pagina 22.

Tabella 2-11 Come configurare la configurazione diretta del backup

Passaggio	Descrizione
Passaggio 1	Configurare il dispositivo di archiviazione su disco per rimozione duplicati nel cloud privato. Vedere "Configurazione del dispositivo di archiviazione su disco per rimozione duplicati nel cloud privato per la configurazione di backup diretti" a pagina 36.
Passaggio 2	Eseguire il seeding dei dati del dispositivo di archiviazione su disco per rimozione duplicati nel cloud privato. Vedere "Informazioni sul seeding del dispositivo di archiviazione su disco per rimozione duplicati per la configurazione di backup diretti" a pagina 37.

Configurazione del dispositivo di archiviazione su disco per rimozione duplicati nel cloud privato per la configurazione di backup diretti

È necessario creare il dispositivo di archiviazione su disco di Backup Exec e il dispositivo di archiviazione su disco per rimozione duplicati nell'istanza del cloud privato.

Vedere "Impostazione della configurazione dei backup diretti" a pagina 35.

Tabella 2-12 Come configurare l'istanza del dispositivo di archiviazione su disco per rimozione duplicati di Backup Exec

Passaggio	Descrizione
Passaggio 1	Accedere a C1 utilizzando l'account di dominio con i diritti di amministrazione nel server locale.
Passaggio 2	Installare Backup Exec 2012 su C1 e specificare un accesso al sistema.
Passaggio 3	In C1, in Backup Exec, creare un nuovo dispositivo di archiviazione su disco per rimozione duplicati. Se si desidera che i dati a riposo vengano crittografati nel dispositivo di archiviazione su disco per rimozione duplicati del cloud privato, selezionare **Sì, crittografare i dati durante la trasmissione a questo dispositivo di archiviazione su disco per rimozione duplicati e mentre il dispositivo contiene dati** quando si configura un nuovo dispositivo di archiviazione su disco per rimozione duplicati. Per un dispositivo di rimozione duplicati esistente, è possibile modificare il campo **Crittografia** nella proprietà del dispositivo di rimozione duplicati. **Nota:** VPN crittografa i dati in transito tra il server Backup Exec locale e il server Backup Exec nel cloud. Per ulteriori informazioni su come creare un dispositivo di archiviazione su disco per rimozione duplicati, consultare il *Manuale dell'amministratore di Symantec Backup Exec*.
Passaggio 4	Attivare l'impostazione del server nel cloud privato: ■ Aprire Backup Exec nel server Backup Exec. ■ Fare clic sul pulsante Backup Exec, selezionare **Configurazione e impostazioni**, quindi fare clic su **Proprietà server locale**. ■ Nel riquadro sinistro, fare clic su **Impostazioni**. ■ Nel campo **Cloud server privato**, selezionare **Attivato**.

Informazioni sul seeding del dispositivo di archiviazione su disco per rimozione duplicati per la configurazione di backup diretti

Per evitare lunghi tempi di trasferimento su Internet, è possibile effettuare il seeding del dispositivo di archiviazione su disco con rimozione duplicati nel cloud con i dati necessari per l'avvio. Il seeding del dispositivo di archiviazione su disco per rimozione duplicati è il processo di collocazione dei file di configurazione iniziale o dei set di backup nel dispositivo di archiviazione su disco per rimozione duplicati per prepararlo all'uso. I tempi di trasferimento dipendono dalla quantità di dati da copiare e di cui eseguire il backup in un'istanza di Backup Exec nel cloud privato.

Si può eseguire il seeding dei dati iniziali utilizzando due metodi, a seconda del tipo di dati di cui si desidera eseguire il seeding:

- Si può eseguire il seeding del dispositivo di archiviazione su disco per rimozione duplicati con i backup del sistema operativo System State. Eseguire il seeding del dispositivo di archiviazione su disco con rimozione duplicati tramite processi di backup dei dati di System State di altri computer in esecuzione nel cloud privato. Eseguire il backup dei dati dello stato del sistema per i computer che eseguono lo stesso sistema operativo come i computer locali di cui si desidera eseguire il backup.
  Vedere "Seeding dei file del sistema operativo per la configurazione di backup diretti" a pagina 37.
- Si può inviare un'unità di trasferimento fisica che contiene i set di backup con i dati pertinenti dal server locale di Backup Exec al datacenter del cloud privato.
  Vedere "Seeding del dispositivo di archiviazione su disco per rimozione duplicati tramite un'unità di trasferimento per la configurazione dei backup diretti" a pagina 38.

Seeding dei file del sistema operativo per la configurazione di backup diretti

Per evitare lunghi tempi di trasferimento su Internet, è possibile effettuare il seeding del dispositivo di archiviazione su disco con rimozione duplicati nel cloud con i dati necessari per l'avvio. Un modo per eseguire il seeding del dispositivo di archiviazione su disco per rimozione duplicati è utilizzare i dati del backup di System State provenienti da altri computer nella stessa posizione.

Vedere "Informazioni sul seeding del dispositivo di archiviazione su disco per rimozione duplicati per la configurazione di backup diretti" a pagina 37.

Tabella 2-13 Come eseguire il seeding dei file del sistema operativo per la configurazione diretta del backup

Passaggio	Descrizione
Passaggio 1	Installare Agent for Windows e Agent for Linux su qualsiasi computer di cui si intende eseguire il backup sulle reti locali del cliente. Per ulteriori informazioni sull'installazione degli agenti di Backup Exec, consultare il *Manuale dell'amministratore di Backup Exec*. I computer utilizzati per eseguire il seeding dei dati devono avere le stesse versioni del sistema operativo dei computer su cui si esegue il backup.
Passaggio 2	Creare ed eseguire i processi di backup nel server Backup Exec del cloud privato. Eseguire il backup dei volumi di System State e dei volumi del sistema dei computer nella stessa posizione nel dispositivo di archiviazione su disco per rimozione duplicati nel cloud privato.

Seeding del dispositivo di archiviazione su disco per rimozione duplicati tramite un'unità di trasferimento per la configurazione dei backup diretti

È possibile utilizzare un'unità di trasferimento fisica per eseguire il seeding del dispositivo di archiviazione su disco per rimozione duplicati di Backup Exec nel cloud privato. Il seeding del dispositivo di archiviazione su disco per rimozione duplicati con i file necessari per l'avvio consente di risparmiare tempo durante l'esecuzione di un backup di grandi dimensioni su Internet.

Vedere "Informazioni sul seeding del dispositivo di archiviazione su disco per rimozione duplicati per la configurazione di backup diretti" a pagina 37.

Tabella 2-14 Come eseguire il seeding del dispositivo di archiviazione su disco per rimozione duplicati tramite un'unità di trasferimento per la configurazione dei backup diretti

Passaggio	Descrizione
Passaggio 1	Collegare un'unità portatile al computer (C2).
Passaggio 2	Copiare i file su cui è stato eseguito il seeding da C2 all'unità rimovibile.
Passaggio 3	Crittografare i file sul disco utilizzando lo strumento di crittografia di terzi.
Passaggio 4	Spedire l'unità di trasferimento al datacenter del cloud privato.
Passaggio 5	Connettere l'unità di trasferimento al computer 1 (C1).

Passaggio	Descrizione
Passaggio 6	Temporaneamente decrittografare i dati sull'unità di trasferimento utilizzando lo stesso strumento che è stato utilizzato per crittografare i dati.
Passaggio 7	Creare ed eseguire un processo di backup che esegua il backup dei file non crittografati. Utilizzare il dispositivo di archiviazione su disco per rimozione duplicati nel cloud come destinazione.
Passaggio 8	Al termine del processo di backup, è possibile eliminare i file di origine copiati. Utilizzare un'utilità disco per eliminare i dati dall'unità rimovibile.

Al termine del processo di seeding del dispositivo di archiviazione su disco per rimozione duplicati nel cloud privato, il processo di configurazione è completo.

Si può procedere all'argomento seguente per iniziare a lavorare in Backup Exec.

Vedere "Informazioni su come lavorare con Backup Exec Private Cloud Services e la configurazione di backup diretti" a pagina 49.

Capitolo 3

Lavorare con Backup Exec Private Cloud Services

Il capitolo contiene i seguenti argomenti:

Informazioni su come lavorare con Backup Exec Private Cloud Services per le configurazioni copia fuori dall'unità

Backup Exec Private Cloud Services consente di gestire le definizioni di backup con l'utilizzo di Central Admin Server Option (CASO) e di Deduplication Option.

Symantec fornisce un utile strumento di calcolo che consente di ottenere una stima del tempo necessario per copiare i dati su Internet. Il calcolatore di tempo del backup del cloud può essere utile per pianificare a strategia di backup del

cloud. Si può utilizzare il calcolatore per stabilire se le risorse di sistema sono adeguate per eseguire il backup i dati dei clienti all'interno di una specifica finestra di backup. La stima del tempo può contribuire a decidere la quantità di dati che si riesce a supportare e quanto tempo si dedica ai backup del cloud.

È possibile trovare il calcolatore al collegamento seguente:

http://entsupport.symantec.com/umi/V-269-34

Vedere "Creazione delle definizioni di backup per le configurazioni copia fuori dall'unità" a pagina 42.

Vedere "Informazioni sul ripristino dei dati dal cloud privato utilizzando le configurazioni della copia fuori dall'unità." a pagina 45.

Vedere "Il ripristino dei dati dal cloud privato utilizzando le configurazioni della copia fuori dall'unità" a pagina 45.

Vedere "Ripristino dei dati dal cloud privato con un'unità di trasferimento utilizzando le configurazioni copia fuori dall'unità" a pagina 46.

Creazione delle definizioni di backup per le configurazioni copia fuori dall'unità

È possibile copiare i dati dei backup nell'istanza di Backup Exec nel cloud privato creando una definizione di backup con una fase di duplicazione. La definizione di backup si trova nel server di amministrazione centrale. La definizione contiene i processi di backup che eseguono il backup dei dati nel dispositivo di archiviazione su disco per rimozione duplicati locale. La definizione contiene inoltre una fase di duplicazione che poi copia i set di backup nel dispositivo di archiviazione su disco per rimozione duplicati nel cloud privato.

A scelta, è inoltre possibile aggiungere un'ulteriore fase di duplicazione alla definizione di backup per replicare il set di backup copiato dal dispositivo di archiviazione su disco per rimozione duplicati nel cloud. È possibile duplicare il set di backup su un dispositivo a nastro situato anch'esso nel cloud o su un altro dispositivo di archiviazione per rimozione duplicati su un server Backup Exec gestito. Il server Backup Exec gestito può essere situato nel cloud privato o in un'ubicazione fisica differente.

Nota: Per ulteriori informazioni su come creare le definizioni di backup, consultare il *Manuale dell'amministratore di Symantec Backup Exec*.

Per creare le definizioni di backup per le configurazioni copia fuori dall'unità

1. Nel server di amministrazione centrale, aprire Backup Exec.
2. Nella scheda **Backup e ripristino** eseguire una delle operazioni seguenti:
   - Per eseguire il backup di un singolo server, fare clic con il pulsante destro del mouse sul nome del server.
   - Per eseguire il backup di più server, selezionare i nomi dei server con MAIUSC + clic o CTRL + clic, quindi fare clic con il pulsante destro del mouse su uno dei server selezionati.
3. Nel menu **Backup**, selezionare l'opzione di backup che si desidera utilizzare.
4. Nel campo **Nome**, digitare un nome univoco per la definizione di backup.

Nota: Se viene eseguito il backup di dati di più server, Backup Exec aggiunge il nome del server al testo immesso nel campo **Nome**. Backup Exec usa il nome del server e il testo immesso per creare nomi univoci per ogni definizione di backup.

---

5. Effettuare una delle seguenti operazioni:

Per verificare o modificare le credenziali utilizzate da Backup Exec per accedere alle selezioni di backup	Nella casella **Selezioni** fare clic su **Verifica/Modifica credenziali**.
Per modificare le selezioni di backup	Nella casella **Selezioni** fare clic su **Modifica**.

Per aggiungere una fase alla definizione di backup	Completare i seguenti passaggi: ■ Nella casella **Backup** fare clic su **Aggiungi fase**. ■ Fare clic su **Duplica** per aggiungere la fase di duplicazione. ■ Nella casella **Duplica** fare clic su **Modifica**. ■ Nel riquadro **Archiviazione**, selezionare il dispositivo di archiviazione su disco per rimozione duplicati su cloud privato come archiviazione per l'operazione di duplicazione. ■ Configurare qualsiasi altra impostazione secondo le esigenze. Symantec consiglia di verificare l'operazione di duplicazione come processo separato. Se si seleziona la verifica dell'operazione alla fine del processo, le prestazioni del processo diminuiscono. È possibile configurare l'operazione di verifica nel riquadro **Verifica**. **Nota:** È possibile aggiungere ulteriori fasi di duplicazione alla definizione di backup. Ad esempio, può essere necessario inviare copie aggiuntive a un dispositivo a nastro nella stessa posizione o a un dispositivo di archiviazione per rimozione duplicati su un server Backup Exec gestito remoto.
Per modificare le impostazioni del processo	Completare i seguenti passaggi: ■ Nella casella **Backup**, fare clic su **Modifica**. ■ Nel riquadro **Archiviazione**, selezionare il dispositivo di archiviazione su disco per rimozione duplicati locale come archiviazione per il processo di backup. ■ Configurare qualsiasi altra impostazione secondo le esigenze.

6 Al termine della configurazione della definizione di backup, fare clic su **OK** nella finestra di dialogo **Proprietà di backup**.

Vedere "Informazioni su come lavorare con Backup Exec Private Cloud Services per le configurazioni copia fuori dall'unità" a pagina 41.

Informazioni sul ripristino dei dati dal cloud privato utilizzando le configurazioni della copia fuori dall'unità.

Dopo aver eseguito il backup dei dati nell'istanza di Backup Exec del cloud privato, è possibile ripristinarlo in qualunque momento. Il ripristino dei dati da un dispositivo di archiviazione su disco per rimozione duplicati nel cloud privato è molto simile al normale ripristino dei dati in Backup Exec.

Vedere "Il ripristino dei dati dal cloud privato utilizzando le configurazioni della copia fuori dall'unità" a pagina 45.

Può essere più efficiente ripristinare un gran numero di dati da un'istanza di Backup Exec nel cloud privato utilizzando un'unità fisica di trasferimento. È possibile utilizzare l'unità di trasferimento per trasferire i dati nel server Backup Exec locale. Successivamente, utilizzare il server Backup Exec locale per eseguire il processo di ripristino.

Vedere "Ripristino dei dati dal cloud privato con un'unità di trasferimento utilizzando le configurazioni copia fuori dall'unità" a pagina 46.

Il ripristino dei dati dal cloud privato utilizzando le configurazioni della copia fuori dall'unità

Si può ripristinare i dati dall'istanza di Backup Exec del cloud privato sui computer client locali di Backup Exec.

Vedere "Informazioni sul ripristino dei dati dal cloud privato utilizzando le configurazioni della copia fuori dall'unità." a pagina 45.

Per ripristinare i dati dal cloud privato utilizzando le configurazioni della copia fuori dall'unità

1. Assicurarsi che il server da ripristinare contenga comando route della rete che consente di comunicare con il computer 1 (C1) come descritto nella procedura seguente:

   Vedere "Configurazione del percorso di rete locale" a pagina 65.

2. Aprire Backup Exec nel server di amministrazione centrale.
3. Nella scheda **Backup e ripristino**, fare clic su **Ripristino**.
4. Selezionare i dati che si desidera ripristinare e tutte le altre opzioni di processo necessarie, quindi avviare il processo.

Vedere "Informazioni su come lavorare con Backup Exec Private Cloud Services per le configurazioni copia fuori dall'unità" a pagina 41.

Ripristino dei dati dal cloud privato con un'unità di trasferimento utilizzando le configurazioni copia fuori dall'unità

È possibile copiare i dati dall'istanza di Backup Exec nel cloud privato al server Backup Exec locale utilizzando un'unità di trasferimento. L'utilizzo di un'unità di trasferimento può essere utile se si desidera ripristinare un gran numero di dati contemporaneamente. Un grande processo di ripristino può incidere le risorse del sistema, in base alla quantità di larghezza di banda disponibile e al tempo per completare il processo.

Vedere "Informazioni sul ripristino dei dati dal cloud privato utilizzando le configurazioni della copia fuori dall'unità." a pagina 45.

Per ripristinare i dati dal cloud privato facendo utilizzando un'unità di trasferimento e le configurazioni della copia fuori dall'unità

1. Creare l'archiviazione su disco su un'unità portatile nel computer 1 (C1), l'istanza di Backup Exec nel cloud privato.
2. Duplicare i set di backup che si desidera ripristinare dal dispositivo di archiviazione su disco per rimozione duplicati basato su cloud. Selezionare l'archiviazione su disco creata come dispositivo di archiviazione di destinazione.

   Assicurarsi di selezionare la crittografia dei dati utilizzando la crittografia del software. È necessario creare o selezionare una chiave di crittografia per crittografare il software.

   Per ulteriori informazioni sulla crittografia dei dati, consultare il *Manuale dell'amministratore di Symantec Backup Exec*.
3. Dopo il completamento del processo, inviare l'unità di trasferimento all'ufficio locale.
4. Dopo l'arrivo dell'unità portatile, collegare l'unità al server Backup Exec locale.
5. Creare l'archiviazione su disco nel computer 2 (C2) utilizzando l'unità portatile come percorso.
6. Creare ed eseguire le operazioni di inventario e catalogo di Backup Exec nell'archiviazione su disco.

7 Ripristinare i dati dalla nuova archiviazione su disco alla destinazione appropriata.

8 Cancellare i dati dall'unità di trasferimento.

Vedere "Informazioni su come lavorare con Backup Exec Private Cloud Services per le configurazioni copia fuori dall'unità" a pagina 41.

Ripristino di dati da un server Backup Exec gestito in caso di errore del server di amministrazione centrale

Se un errore di hardware o un'altra emergenza interessa il server di amministrazione centrale, il server Backup Exec gestito non potrà eseguire i processi di backup o di ripristino. È possibile recuperare il server di amministrazione centrale configurando un computer sostitutivo e reinstallando il server di amministrazione centrale di Backup Exec. È anche possibile, tuttavia, convertire un server Backup Exec gestito in server Backup Exec stand-alone per ripristinare il server di amministrazione centrale.

Per convertire un server Backup Exec gestito in un server Backup Exec stand-alone al fine di ripristinare il server di amministrazione centrale

1 Nel server Backup Exec gestito, prendere nota dei nomi e dei percorsi di directory dei dispositivi di archiviazione su disco locale.

Nota: Fare doppio clic sul dispositivo di archiviazione su disco nella scheda **Archiviazione**. Quindi fare clic su **Proprietà** nel riquadro sinistro per visualizzare la proprietà di archiviazione.

2 Se il server Backup Exec gestito ha un proprio dispositivo di archiviazione su disco per rimozione duplicati, prendere nota del nome del dispositivo, del percorso, del'account di accesso e delle proprietà della password.

Nota: Fare doppio clic sul dispositivo di archiviazione su disco per rimozione duplicati nella scheda **Archiviazione**. Quindi fare clic su **Proprietà** nel riquadro sinistro per visualizzare la proprietà di archiviazione.

3 Aprire la finestra di dialogo Programmi e funzionalità (o Installazione applicazioni) oppure la finestra di dialogo Disinstalla un programma dal Pannello di controllo di Windows.

4 Selezionare l'opzione **Modifica** per Symantec Backup Exec.

5 Nel riquadro sinistro, selezionare **Opzioni aggiuntive**, se non risulta già selezionato.

6 Fare clic su **Avanti** finché non si raggiunge la finestra **Configura server Backup Exec gestito**.

7 Selezionare l'opzione **Server Backup Exec gestito localmente**.

8 Fare clic su **Avanti**.

9 Effettuare una delle operazioni seguenti quando si riceve il messaggio "Impossibile contattare {Server di amministrazione centrale}. Verificare che il server di amministrazione centrale sia in esecuzione."

Se il server di amministrazione centrale non è disponibile e si desidera che questo server Backup Exec venga gestito localmente	Fare clic su **OK** per continuare.
Se che si desidera riprovare questa operazione quando il server di amministrazione centrale è in esecuzione	Fare clic su **Annulla** per terminare la procedura.

Quando l'installazione è completa, il computer non sarà più un server Backup Exec gestito centralmente.

10 Fare clic su **Avanti**.

11 Riavviare il computer se viene richiesto.

12 Aprire Backup Exec e selezionare la scheda **Archiviazione**.

Se Backup Exec non riesce a connettersi al server Backup Exec, riavviare i servizi di Backup Exec e poi riprovare.

13 Ricreare qualsiasi dispositivo di archiviazione su disco locale importando il dispositivo di archiviazione su disco originale e utilizzando gli stessi nomi e percorsi annotati nel passaggio 1.

14 Ricreare qualsiasi dispositivo di archiviazione su disco con rimozione duplicati importando i dispositivi di archiviazione su disco con rimozione duplicati originali e utilizzando le stesse informazioni annotate nel passaggio 2.

Nota: Ricreare un dispositivo di archiviazione esistente potrebbe richiedere più tempo rispetto alla creazione di un nuovo dispositivo. Il tempo necessario dipende da quanti set di backup conteneva il dispositivo di archiviazione e se questo server Backup Exec gestito ha accesso ai relativi controller di dominio e DNS.

---

15 Creare ed eseguire le operazioni di inventario e catalogo di Backup Exec su ogni dispositivo di archiviazione ricreato.

   È ora possibile utilizzare il server Backup Exec stand-alone per ripristinare i set di backup presenti nei dispositivi di archiviazione del server Backup Exec.

16 Se si utilizza il server Backup Exec stand-alone per recuperare il server di amministrazione centrale, potrebbe essere necessario eliminare la risorsa attuale del server di amministrazione centrale nel server Backup Exec stand-alone. Successivamente, eseguire l'installazione remota di Agent for Windows nel server di amministrazione centrale prima di ripristinarlo.

   Una volta recuperato il server di amministrazione centrale, è possibile convertire nuovamente il server Backup Exec gestito localmente in un server Backup Exec gestito centralmente, utilizzando nuovamente la finestra di dialogo di modifica dell'installazione di Backup Exec. Selezionare l'opzione Server Backup Exec gestito centralmente per riconfigurare il computer come server Backup Exec gestito.

Informazioni su come lavorare con Backup Exec Private Cloud Services e la configurazione di backup diretti

Backup Exec Private Cloud Services consente di gestire le definizioni di backup con la deduplicazione lato client per la configurazione di backup diretti.

Si può scegliere di avviare e arrestare manualmente la connessione di collegamento dell'istanza VPN di Backup Exec del cloud privato durante l'esecuzione dei processi. Oppure si può scegliere di avere la connessione al VPN e l'istanza continuamente in esecuzione. Si può anche scegliere di automatizzare questo processo pianificando l'avvio e l'arresto del servizio di OpenVPN all'interno della finestra di processo di backup. Si può utilizzare l'utilità Windows Scheduled Tasks per creare una pianificazione del servizio.

Symantec fornisce un utile strumento di calcolo che consente di ottenere una stima del tempo necessario per copiare i dati su Internet. Il calcolatore di tempo del backup del cloud può essere utile per pianificare a strategia di backup del cloud. Si può utilizzare il calcolatore per stabilire se le risorse di sistema sono adeguate per eseguire il backup i dati dei clienti all'interno di una specifica finestra di backup. La stima del tempo può contribuire a decidere la quantità di dati che si riesce a supportare e quanto tempo si dedica ai backup del cloud.

È possibile trovare il calcolatore al collegamento seguente:

http://entsupport.symantec.com/umi/V-269-34

Vedere "Attivare la deduplicazione lato client per la configurazione di backup diretti" a pagina 50.

Vedere "Creazione dei processi di backup per la configurazione dei backup diretti" a pagina 51.

Vedere "Ripristino dei dati dal cloud privato con un'unità di trasferimento utilizzando la configurazione diretta del backup" a pagina 52.

Attivare la deduplicazione lato client per la configurazione di backup diretti

Prima di poter creare ed eseguire i processi di backup diretti nell'istanza di Backup Exec nel cloud privato, è necessario attivare la deduplicazione lato client.

Nota: Se si utilizza la configurazione multi-tenant, non deve essere attivata la deduplicazione lato client per il dispositivo di archiviazione su disco del server di amministrazione centrale.

Per attivare la deduplicazione lato client per la configurazione di backup diretti

1. Nella scheda **Archiviazione**, fare doppio clic sull'archiviazione di cui si desidera modificare le proprietà.
2. Nel riquadro sinistro, fare clic su **Proprietà**.
3. Nel campo **Deduplicazione lato client**, selezionare **Attivata**.
4. Fare clic su **Applica**.
5. Riavviare i servizi di Backup Exec.

   Nota: È necessario arrestare e riavviare i servizi di Backup Exec su C1.

Dopo avere attivato la deduplicazione lato client, è possibile creare ed eseguire i processi di backup diretti.

Per ulteriori informazioni sulla creazione di processi di backup che utilizzano la deduplicazione lato client, consultare il *Manuale dell'amministratore di Symantec Backup Exec*.

Vedere "Creazione dei processi di backup per la configurazione dei backup diretti" a pagina 51.

Vedere "Informazioni su come lavorare con Backup Exec Private Cloud Services e la configurazione di backup diretti" a pagina 49.

Creazione dei processi di backup per la configurazione dei backup diretti

Dopo aver configurato OpenVPN e aggiunto qualsiasi altro computer per la condivisione dell'agente remoto e la deduplicazione lato client, è possibile creare ed eseguire i processi di backup diretti.

Vedere "Attivare la deduplicazione lato client per la configurazione di backup diretti" a pagina 50.

Nota: Per ulteriori informazioni su come creare le definizioni di backup, consultare il *Manuale dell'amministratore di Symantec Backup Exec*.

Seguire la seguente procedura per eseguire il backup dei dati direttamente nell'istanza di Backup Exec del cloud privato.

Per creare processi di backup per la configurazione diretta del backup

1. Sul computer 1 (C1), aprire Backup Exec.
2. Nella scheda **Backup e ripristino** eseguire una delle operazioni seguenti:
   - Per eseguire il backup di un singolo server, fare clic con il pulsante destro del mouse sul nome del server.
   - Per eseguire il backup di più server, selezionare i nomi dei server con MAIUSC + clic o CTRL + clic, quindi fare clic con il pulsante destro del mouse su uno dei server selezionati.
3. Nel menu **Backup**, selezionare l'opzione di backup che si desidera utilizzare.
4. Nel campo **Nome**, digitare un nome univoco per la definizione di backup.

   Nota: Se viene eseguito il backup di dati di più server, Backup Exec aggiunge il nome del server al testo immesso nel campo **Nome**. Backup Exec usa il nome del server e il testo immesso per creare nomi univoci per ogni definizione di backup.

   ---

5. Effettuare una delle seguenti operazioni:

Per verificare o modificare le credenziali utilizzate da Backup Exec per accedere alle selezioni di backup	Nella casella **Selezioni** fare clic su **Verifica/Modifica credenziali**.
Per modificare le selezioni di backup	Nella casella **Selezioni** fare clic su **Modifica**.
Per aggiungere una fase alla definizione di backup	Nella casella **Backup** fare clic su **Aggiungi fase**.
Per modificare le impostazioni del processo	Completare i seguenti passaggi: ■ Nella casella **Backup**, fare clic su **Modifica**. ■ Assicurarsi che l'opzione **Consenti al computer remoto di accedere direttamente al dispositivo di archiviazione e di eseguire la deduplicazione lato client, se supportata** sia selezionata. ■ Configurare qualsiasi altra impostazione secondo le esigenze.

6 Al termine della configurazione della definizione di backup, fare clic su **OK** nella finestra di dialogo **Proprietà di backup**.

Vedere "Informazioni su come lavorare con Backup Exec Private Cloud Services e la configurazione di backup diretti" a pagina 49.

Ripristino dei dati dal cloud privato con un'unità di trasferimento utilizzando la configurazione diretta del backup

Si può creare un processo di ripristino normale per ripristinare i dati dall'istanza di Backup Exec del cloud privato al client locale. Tuttavia, se si desidera ripristinare un gran numero di dati contemporaneamente, è preferibile utilizzare un'unità fisica di trasferimento. Il tempo necessario per il trasferimento di un gran numero di dati dipende dalla larghezza disponibile della banda e dal tempo per completare il processo.

Per ripristinare i dati dal cloud privato con un'unità di trasferimento utilizzando la configurazione diretta del backup

1 Creare ed eseguire un processo di ripristino sul computer 1 (C1) per ripristinare i file in una cartella su un'unità disco rimovibile.

2 Al termine del processo, crittografare i file sul disco utilizzando un qualsiasi strumento di crittografia di terzi.

3 Inviare l'unità rimovibile all'ufficio locale.

4 Quando l'unità rimovibile arriva, decrittografare i file utilizzando lo stesso strumento utilizzato per crittografarli.

5 Trasferire i file non crittografati alla loro destinazione adeguata sul computer 2 (C2).

6 Cancellare o far scomparire del tutto i file dall'unità di trasferimento per assicurarsi che i dati vengano rimossi in modo permanente.

Vedere "Informazioni su come lavorare con Backup Exec Private Cloud Services e la configurazione di backup diretti" a pagina 49.

Informazioni sul servizio di recupero di emergenza nel cloud

Le funzionalità Simplified Disaster Recovery (SDR) e conversione in computer virtuale di Backup Exec 2012 consentono ai provider di servizi o ai clienti di eseguire recuperi di emergenza nel cloud. I dati di backup memorizzati nel cloud possono essere utilizzati per creare server virtuali o fisici temporanei sostitutivi nel cloud privato in caso di emergenza.

Le configurazioni di rete specifiche e gli stati dell'errore possono influire sui passaggi specifici che sono richiesti per il failover e il failback. Questa sezione fornisce solo alcune indicazioni di base per l'utilizzo di SDR e della conversione in computer virtuali all'interno di un ambiente cloud privato di Backup Exec per fornire servizi di recupero di emergenza.

Si possono verificare due scenari principali di recupero di emergenza. Il primo scenario è il failover e il failback del server in cui uno o più server in sede si arrestano, ma la rete locale rimane intatta. Il secondo scenario è il failover e il failback del sito in cui un intero sito smette di funzionare.

Vedere "Recupero di un server o di un sito da un failover" a pagina 53.

Vedere "Recupero di un server o di un sito da un failback" a pagina 56.

Recupero di un server o di un sito da un failover

Per prepararsi a uno scenario di failover del server, è necessario configurare ed eseguire regolarmente le definizioni di backup con Simplified Disaster Recovery (SDR) attivato per tutti i server di importanza critica per l'azienda. Le definizioni di backup devono includere le fasi di duplicazione che copiano i dati di backup nel dispositivo di archiviazione su disco nel cloud privato. Quando si verifica il failover

del server, utilizzare il server Backup Exec nel cloud privato per recuperare i server virtuali o fisici sostitutivi.

Vedere "Informazioni sul servizio di recupero di emergenza nel cloud" a pagina 53.

Per recuperare un server fisico sostitutivo, utilizzare il disco di Simplified Disaster Recovery per eseguire un ripristino bare metal. Utilizzare il backup più recente con SDR sul dispositivo di archiviazione su disco per rimozione duplicati nel cloud privato. È possibile portare il server sostitutivo in sede per sostituire il server con failover. Un failover del sito richiede che un intero gruppo di server di importanza cruciale per l'azienda venga sostituito con computer virtuali in un ambiente hypervisor situato nel cloud.

Per ulteriori informazioni su Simplified Disaster Recovery, consultare il *Manuale dell'amministratore di Symantec Backup Exec*.

Nota: Le configurazioni di rete specifiche e gli stati dell'errore possono influire sui passaggi specifici che sono richiesti per il failback. La seguente procedura fornisce solo alcune indicazioni di base per l'utilizzo di un ambiente cloud privato di Backup Exec per fornire servizi di recupero di emergenza.

Per recuperare un server o un sito dal failover

1. Creare un ambiente hypervisor VMware o Hyper-V ESX nella posizione del cloud.
2. Creare una rete virtuale con priorità per i conflitti per il computer virtuale o computer virtuali sostitutivi in esecuzione sull'hypervisor. I server sostitutivi devono conservare il loro indirizzo IP originale in sede per uno scenario di failover del sito completo.

   Nota: Quando si effettua il recupero di un sito, i server sostitutivi devono conservare il loro indirizzo IP originale in sede. È necessario ripristinare i computer sostitutivi in un ordine logico. Ad esempio, è necessario ripristinare prima tutti i controller di dominio e i server DNS .

   ---

3. Eseguire una delle seguenti operazioni:

Per eseguire il failover da un computer fisico	Completare i seguenti passaggi: ■ Creare ed eseguire una conversione a un computer virtuale. Convertire il volume di sistema SDR in una data e i dati dello stato del sistema in computer virtuali per tutti i computer sostitutivi. I computer virtuali devono puntare all'hypervisor. Non selezionare risorse di applicazione in questo momento. ■ Configurare tutti gli indirizzi IP fissi per i computer virtuali sostitutivi, se necessario. ■ Stabilire la connettività di rete tra il computer o computer virtuali sostitutivi e il server o i server Backup Exec nel cloud privato. ■ Creare ed eseguire i processi di ripristino dagli stessi backup SDR con data e ora specifiche per ciascuno dei server sostituiti. Selezionare tutte le risorse disponibili nel computer per quella data e ora specifiche. Reindirizzare i dati di ripristino al server o ai server sostitutivi.
Per eseguire il failover da un computer virtuale	Creare ed eseguire un processo di ripristino reindirizzato dai backup SDR di ciascuno dei server sostitutivi con data e ora specifiche più recenti. Lo stesso tipo di hypervisor deve essere utilizzato sia per i server in sede, sia per quelli nel cloud.

4 Per recuperare solo un singolo server, stabilire la connettività VPN tra il server virtuale sostitutivo e la rete in sede e configurare tutte le voci DNS in sede per gli indirizzi IP dei computer virtuali sostitutivi.

5 Esporre tutti i nuovi indirizzi esterni dalla rete del cloud e modificare tutti i record DNS esterni se il server o i server bloccati sono stati esposti tramite indirizzi IP esterni (un server di posta di Exchange, ad esempio).

6 Configurare ed eseguire le definizioni di backup host hypervisor regolarmente pianificate per il computer o i computer virtuali sostitutivi. Utilizzare il dispositivo di archiviazione su disco per rimozione duplicati del cloud privato come destinazione di backup.

Se il server o i server di Backup Exec in sede hanno un dispositivo di archiviazione su disco con rimozione duplicati, le definizioni di backup devono includere una fase di duplicazione che copia i backup nel dispositivo di archiviazione su disco per rimozione duplicati in sede.

Recupero di un server o di un sito da un failback

È possibile recuperare un server o un sito in caso di failback. Uno scenario di failback del sito richiede che un intero gruppo di server di importanza cruciale per l'azienda venga ripristinato su server fisici in sede o su computer virtuali.

Vedere "Informazioni sul servizio di recupero di emergenza nel cloud" a pagina 53.

Potrebbe essere necessario recuperare gradualmente i server in sede invece di recuperarli tutti contemporaneamente. È possibile recuperare inizialmente alcuni server e recuperare gli altri in modo graduale nel corso di alcuni giorni o settimane. Questa strategia richiede modifiche alla connettività VPN e all'indirizzo IP per la sostituzione dei server cloud rimanenti collegati alla rete in sede.

Per ulteriori informazioni su Simplified Disaster Recovery, consultare il *Manuale dell'amministratore di Symantec Backup Exec*.

Nota: Le configurazioni di rete specifiche e gli stati dell'errore possono influire sui passaggi specifici che sono richiesti per il failback. La seguente procedura fornisce solo alcune indicazioni di base per l'utilizzo di un ambiente cloud privato di Backup Exec per fornire servizi di recupero di emergenza.

Per recuperare un server o un sito dal failback

1 Eseguire un backup con Simplified Disaster Recovery (SDR) attivato e includere tutte le fasi di duplicazione.

2 Spegnere il computer o i computer virtuali sostitutivi.

3 Se la definizione di backup con SDR attiva non comprendeva una fase di duplicazione con invio dei set di backup all'archiviazione su disco con rimozione duplicati, completare i seguenti passaggi:

- Aggiungere un dispositivo di archiviazione su disco portatile a Backup Exec sul server o sui server Backup Exec nel cloud privato.
- Duplicare i set di backup dal backup finale in una data e ora specifiche relativi a tutti i dati del computer o dei computer sostitutivi. Utilizzare il dispositivo di archiviazione su disco portatile come destinazione.
- Inviare il dispositivo di archiviazione su disco portatile all'ubicazione in sede.
- Aggiungere il dispositivo di archiviazione su disco portatile a Backup Exec sul server o sui server di Backup Exec in sede.
- Inventariare e catalogare il dispositivo di archiviazione su disco sul server o sui server di Backup Exec in sede.

4 Effettuare una delle seguenti operazioni:

Per eseguire il failback su un server o su più server fisici in sede	Completare i seguenti passaggi: ■ Utilizzare il disco di Simplified Disaster Recovery per eseguire un ripristino bare metal. Selezionare i backup con SDR più recenti nel server o nei server Backup Exec in sede. ■ Configurare un indirizzo IP fisso per i computer recuperati, se necessario. ■ Configurare tutte le voci DNS in sede per i computer recuperati o i relativi indirizzi IP, se necessario.
Per eseguire il failback su un server o su più server virtuali in sede	Completare i seguenti passaggi: ■ Creare ed eseguire un processo di ripristino reindirizzato dal server sostitutivo o dai backup dei server con data e ora specifiche più recenti. Lo stesso tipo di hypervisor deve essere utilizzato sia per i server in sede, sia per quelli nel cloud. ■ Configurare un indirizzo IP fisso per i computer virtuali recuperati, se necessario. ■ Configurare tutte le voci DNS in sede per i computer virtuali recuperati o i relativi indirizzi IP, se necessario.

5 Se il server o i server bloccati sono stati esposti attraverso un indirizzo IP esterno (un server di posta di Exchange, ad esempio), ripristinare l'indirizzo o gli indirizzi originali nei registri DNS esterni.

6 Eliminare il server sostitutivo o le definizioni di backup dei server nel cloud.

7 Riprendere l'esecuzione della definizione o delle definizioni di backup originali per qualsiasi computer ripristinato in sede.

Requisiti del dispositivo di archiviazione su disco per rimozione duplicati di Backup Exec

I requisiti del dispositivo di archiviazione su disco per rimozione duplicati di Backup Exec si applicano a tutte le configurazioni del cloud privato. Se si raggiunge il limite della condivisione su un determinato server di Backup Exec nel cloud, occorre aggiungere ulteriori server Backup Exec cloud.

Per ulteriori informazioni sui requisiti dei dispositivi di archiviazione su disco per rimozione duplicati, consultare il *Manuale dell'amministratore di Symantec Backup Exec*.

Limitazioni di latenza WAN

Se la rete presenta alti livelli di latenza, può avere un impatto negativo sulle prestazioni del processo di backup diretto iniziale del cloud. La latenza può influenzare anche alcuni processi di backup di duplicazione che trasferiscono i dati tra l'ufficio locale e il server Backup Exec nel cloud privato. È possibile riscontrare problemi di prestazioni anche se è stato eseguito il seeding del dispositivo di archiviazione su disco per rimozione duplicati con un'unità di trasferimento, sebbene le prestazioni risultino sempre migliorate con il seeding. Durante il processo di backup iniziale, Backup Exec identifica e memorizza nella cache le informazioni su i segmenti di dati, consentendo di ottenere prestazioni più efficienti per i processi successivi.

Nota: I valori di latenza possono essere considerati alti se superano i 30 millisecondi di latenza andata e ritorno media. Più alta è la latenza, più vengono influenzate le prestazioni di Backup Exec.

Questa limitazione non si applica ai processi di backup di duplicazione, quando sia il dispositivo di origine che il dispositivo di destinazione sono dispositivi di archiviazione su disco per rimozione duplicati.

Qui di seguito vengono elencate le limitazioni all'utilizzo di Backup Exec Private Cloud Services negli ambienti ad alta latenza:

- I processi di backup di duplicazione che utilizzano un dispositivo di origine diverso da un dispositivo di archiviazione su disco per rimozione duplicati e da un dispositivo di archiviazione su disco per rimozione duplicati in un cloud privato come destinazione potrebbero riscontrare problemi di prestazioni. Tali problemi di prestazioni possono essere evitati utilizzando un dispositivo di archiviazione su disco per rimozione duplicati come dispositivo di archiviazione di origine locale.
- È possibile riscontrare che la configurazione di backup diretto sul cloud non è idonea all'esecuzione di backup per grandi quantità di dati.
- Se si desidera eliminare e ricreare le definizioni di backup per le stesse risorse, Backup Exec deve nuovamente memorizzare nella cache le impronte dei dati. In questo modo è possibile riscontrare gli stessi problemi di prestazioni del processo di backup diretto iniziale su cloud.

Limitazioni sulla tecnologia di recupero capillare con la copia fuori dall'unità

Di seguito le limitazioni per utilizzare l 'opzione della tecnologia di recupero capillare (GRT) di Backup Exec con la configurazione della copia fuori dall'unità:

- L'esecuzione di set di backup Exchange locali incrementali con opzione GRT attivata in un dispositivo di archiviazione su disco per rimozione duplicati nel cloud privato crea dati di backup in un formato a nastro MTF. È possibile ripristinare i dati capillari da questi set di backup, tuttavia ciò richiede l'organizzazione del set di backup sul server Backup Exec nel cloud durante il processo di ripristino. Questa limitazione non esiste per il backup diretto dei set di backup con opzione GRT attivata nel dispositivo di archiviazione su disco con rimozione duplicati nel cloud.
- Non è consigliato copiare i set duplicati con opzione GRT attivata da dispositivi locali a nastro direttamente nel dispositivo di archiviazione su disco per rimozione duplicati, poiché ciò può implicare una durata eccessiva.
- L'esecuzione di set di backup con opzione GRT attivata direttamente nel server Backup Exec nel cloud può determinare tempi di prestazione minori in ambienti ad alta latenza. È possibile avvertire una riduzione nelle prestazioni anche dopo il backup iniziale. Se le prestazioni continuano a essere un problema, è possibile disattivare il GRT per i backup diretti.

Limitazioni di Windows Small Business Server (SBS) e della configurazione di server Backup Exec multi-tenant

La configurazione di server Backup Exec multi-tenant richiede che tutti i server Backup Exec gestiti localmente facciano parte del dominio del cloud privato. Di conseguenza, non è possibile configurare il server SBS di un cliente come server Backup Exec gestito se fa parte del dominio del cliente. Il server Backup Exec gestito deve essere installato come server separato.

Capitolo 4

Configurazione di OpenVPN

Il capitolo contiene i seguenti argomenti:

Informazioni sulla configurazione di OpenVPN

Il pacchetto open source VPS SSL OpenVPN fornisce una connessione sicura e crittografata tra l'istanza di Backup Exec nel cloud privato e i server Backup Exec locali. È necessario configurare SSL VPN tra l'istanza del server Backup Exec nel cloud privato e qualsiasi computer in esecuzione nella rete locale.

La configurazione di Backup Exec Private Cloud Services ha le seguenti restrizioni di rete per questo esempio di OpenVPN per client singolo:

- La rete locale deve essere contenuta all'interno di una singola subnet.
- Il controller di dominio locale e il DNS devono essere contenuti sullo stesso server.

Vedere "Configurazione di OpenVPN" a pagina 62.

Le istruzioni per la configurazione base di OpenVPN per Backup Exec Private Cloud Services utilizzano un client singolo. Le istruzioni possono essere utilizzare per supportare uno o più computer client locali se i client tutti sono contenuti sulla stessa subnet. Tutti i dati intesi per l'istanza del cloud privata sono instradati attraverso un singolo client di OpenVPN. Per una rete più complessa o per utilizzare l'autenticazione basata su certificato, si può utilizzare la configurazione facoltativa OpenVPN per più client.

Vedere "Informazioni sulla configurazione di OpenVPN per client multipli" a pagina 68.

Configurazione di OpenVPN

Il pacchetto open source VPS SSL OpenVPN fornisce una connessione sicura e crittografata tra l'istanza di Backup Exec nel cloud privato e i server Backup Exec locali. È necessario configurare SSL VPN tra l'istanza del server Backup Exec nel cloud privato e qualsiasi computer in esecuzione nella rete locale.

Vedere "Informazioni sulla configurazione di OpenVPN" a pagina 61.

Tabella 4-1 Come configurare OpenVPN

Passaggio	Descrizione
Passaggio 1	Configurare OpenVPN sull'istanza di Backup Exec del cloud privato Vedere "Configurazione di OpenVPN sull'istanza di Backup Exec del cloud privato" a pagina 62.
Passaggio 2	Configurare di OpenVPN sul computer 2 Vedere "Configurazione di OpenVPN sul computer 2" a pagina 64.
Passaggio 3	Configurare il percorso di rete locale Vedere "Configurazione del percorso di rete locale" a pagina 65.
Passaggio 4	Configurare il firewall, se necessario. Vedere "Informazioni sulla configurazione dei firewall" a pagina 65.
Passaggio 5	Verificare la connessione di OpenVPN Vedere "Verifica della connessione di OpenVPN" a pagina 66.

Configurazione di OpenVPN sull'istanza di Backup Exec del cloud privato

Per garantire una connessione sicura e crittografata, è necessario configurare OpenVPN sull'istanza i Backup Exec del cloud privato.

Vedere "Informazioni sulla configurazione di OpenVPN" a pagina 61.

Per configurare di OpenVPN sull'istanza di Backup Exec del cloud privato

1. Scaricare OpenVPN 2.1.4 dal seguente collegamento e installarlo sul computer 1 (C1) nella posizione predefinita:

   http://swupdate.openvpn.net/community/releases/openvpn-2.1.4-install.exe

2. Su C1, aprire una finestra di Windows Explorer nella cartella di configurazione di OpenVPN selezionando:

   Start > Tutti i programmi > OpenVPN > Shortcuts > OpenVPN Configuration File Directory

3. Generare la chiave statica OpenVPN eseguendo il seguente comando da un prompt di comandi in \Programmi (x86)\OpenVPN\cartella cestino:

   ```
   c:\Programmi (x86)\Open VPN\bin\openvpn --genkey --secret
   static.key
   ```

4. Creare il file di configurazione del server nella cartella aperta in C1 e salvare il file come “server.ovpn":

   Il file “server.ovpn" assomiglia all'esempio seguente:

   ```
   dev tun

   ifconfig 10.8.0.1 10.8.0.2

   secret static.key

   keepalive 10 120
   ```

   Nota: Se la subnet 10.8.x.x è in uso sulla rete locale, utilizzare un intervallo di subnet differente nel comando **ifconfig**.

   Nota: Per impostazione predefinita OpenVPN utilizza la porta UDP 1194. Se necessario, si può specificare un altro numero di porta aggiungendo il comando Porta al server OpenVPN e ai file di configurazione del client.

5. Utilizzando l'utilità di Windows Services, cambiare la proprietà del tipo di avvio del servizio di OpenVPN in **Automatico**.

6. Aprire un prompt di comandi su C1 e digitare quanto segue sostituendo l'indirizzo della subnet del DNS locale (computer 3) e la subnet mask DNS:

   Nota: Non includere le parentesi angolari.

   ```
   route add -p <DNS subnet> mask <DNS subnet mask> 10.8.0.2
   ```

Configurazione di OpenVPN sul computer 2

Per assicurare una connessione sicura e crittografata, configurare OpenVPN sul computer 2 (C2) dopo aver configurato OpenVPN sul computer 1 (C1).

Vedere "Informazioni sulla configurazione di OpenVPN" a pagina 61.

Per configurare OpenVPN sul computer 2

1. Scaricare OpenVPN 2.1.4 dal seguente collegamento e installarlo su C2 nella posizione predefinita:

   http://swupdate.openvpn.net/community/releases/openvpn-2.1.4-install.exe

2. Copiare la chiave statica generata nel passaggio 2 della procedura seguente:

   Configurazione di OpenVPN sull'istanza di Backup Exec del cloud privato

3. Incollare la chiave nella posizione seguente su C2:

   \Programmi (x86)\OpenVPN\config

4. Creare il file di configurazione del client nella posizione seguente su C2 e salvare il file come “client.ovpn":

   \Programmi (x86)\OpenVPN\config

   Il file “client.ovpn" assomiglia all'esempio seguente:

   ```
   dev tun

   remote <The Static IP address of computer 1>

   ifconfig 10.8.0.2 10.8.0.1

   keepalive 10 120

   secret static.key
   ```

5. Immettere l'indirizzo IP statico del computer di Backup Exec del Cloud privato nell'istruzione **remota**.

   Nota: Non includere le parentesi angolari.

6. Se la subnet 10.8.x.x è in uso sulla rete locale, modificare il file per utilizzare un intervallo differente di subnet nell'istruzione **ifconfig**.

7. Utilizzando l'utilità di Windows Services, cambiare la proprietà del tipo di avvio del servizio di OpenVPN in **Automatico**.

Configurazione del percorso di rete locale

Per configurare il percorso di rete locale, si deve attivare l'IP che trasmette sia sul TAP-Win32 Adapter V9 che sull'interfaccia di rete fisica.

Vedere "Informazioni sulla configurazione di OpenVPN" a pagina 61.

Per configurare il percorso di rete locale

1. Sul computer 2 (C2), avviare l'editor del registro di sistema e individuare il tasto seguente:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

2. Impostare i seguenti valori del registro:

   Nome valore: **IPEnableRouter**

   Tipo di valore: **REG_DWORD**

   Dati Valori: **1**

   Nota: Un valore di 1 attiva l'inoltro di TCP/IP per tutte le connessioni di rete installate e utilizzate dal computer.

3. Riavvia C2.

4. Digitare il seguente comando in una finestra di comando sul computer 3 (C3), sostituendo l'indirizzo IP locale di C2:

   Nota: Non includere le parentesi angolari quando si inserisce l'indirizzo IP.

   ```
   Route add -p 10.8.0.0 mask 255.255.255.0 <local IP address of
   computer 2>
   ```

   Nota: È necessario eseguire questo comando su ogni computer di rete locale che deve comunicare con il computer del server OpenVPN Server nel cloud. È necessario eseguire il comando su tutti i server in cui è in esecuzione un agente Backup Exec e che sarebbero coinvolti nei processi di ripristino dal server Backup Exec nel cloud privato.

Informazioni sulla configurazione dei firewall

È necessario configurare i firewall di rete come descritto nella tabella per assicurare una comunicazione adeguata tra il server locale e il server del cloud.

Tabella 4-2 Informazioni sulla configurazione dei firewall

Istanza di Firewall	Azione
Computer 1 (C1)	Si deve disattivare il firewall di Windows per la scheda di rete di OpenVPN. Si deve configurare il firewall di Windows per consentire il traffico in entrata su qualsiasi porta OpenVPN configurata per l'utilizzo. Per impostazione predefinita, OpenVPN utilizza UDP 1194 della porta.
Computer 2 (C2)	Si deve disattivare il firewall di Windows locale per la scheda di rete di OpenVPN TAP.
Rete locale	Se si possiede un firewell locale esterno o aziendale, si deve configurare il firewall per consentire il traffico in uscita su qualsiasi porta OpenVPN configurata per l'utilizzo. Per impostazione predefinita, OpenVPN utilizza UDP 1194 della porta.

Vedere "Informazioni sulla configurazione di OpenVPN" a pagina 61.

Verifica della connessione di OpenVPN

Quando si è finito di configurare OpenVPN, si deve provarlo per assicurarsi che il server e il client di OpenVPN riescano a connettersi.

Vedere "Informazioni sulla configurazione di OpenVPN" a pagina 61.

Per verificare la connessione di OpenVPN

1. Utilizzando l'utilità di Windows Services, avviare i servizi di OpenVPN sia sul computer 1 (C1) che sul computer 2 (C2).
2. Aprire i file di registro di OpenVPN situati su C1 e su C2 nella directory seguente:

   C:\Programmi (x86)\OpenVPN\registro

3 Verificare che il testo “Sequenza inizializzazione completata" sia presente in entrambi i file.

4 Su C1, configurare la scheda di rete TAP-Win32 in modo che indichi il server DNS del dominio locale come server DNS preferito.

Vedere "Configurazione della scheda di rete TAP-Win32" a pagina 67.

Si può scegliere di avviare e arrestare manualmente la connessione di collegamento dell'istanza VPN di Backup Exec nel cloud privato durante l'esecuzione dei processi. In alternativa, è possibile mantenere il collegamento VPN e consentire all'istanza di rimanere sempre in esecuzione. È possibile automatizzare il processo pianificando il servizio OpenVPN in modo che venga avviato e arrestato insieme ai processi di backup pianificati. È possibile utilizzare l'utilità Windows Scheduled Tasks per creare una pianificazione per questo servizio.

Configurazione della scheda di rete TAP-Win32

Per verificare la connessione di OpenVPN, si deve configurare la scheda di rete TAP-Win32 per indicare il server DNS del dominio locale come server DNS preferito.

Vedere "Verifica della connessione di OpenVPN" a pagina 66.

Per configurare la scheda di rete TAP-Win32

1 Aprire **Proprietà scheda di rete TAP**.

2 Fare clic su **Proprietà IPv4**.

3 Fare clic su **Avanzate**.

4 Nella scheda **DNS**, immettere l'indirizzo IP del server DNS della rete locale.

5 Nel campo **Suffissi**, aggiungere i suffissi del dominio FQDN e spostarli all'interno dell'elenco dei suffissi.

6 Fare clic su **OK** per uscire da tutte le finestre di dialogo.

7 Nel prompt dei comandi sul computer 1 (C1), immettere i comandi seguenti:

```
ipconfig /flushdns

ipconfig /registerdns
```

Dopo aver verificato la connessione di OpenVPN, è possibile configurare i server di Backup Exec.

Vedere "Impostazione delle configurazioni multi-tenant o copia fuori dall'unità nel cloud" a pagina 23.

Vedere "Impostazione della configurazione dei backup diretti" a pagina 35.

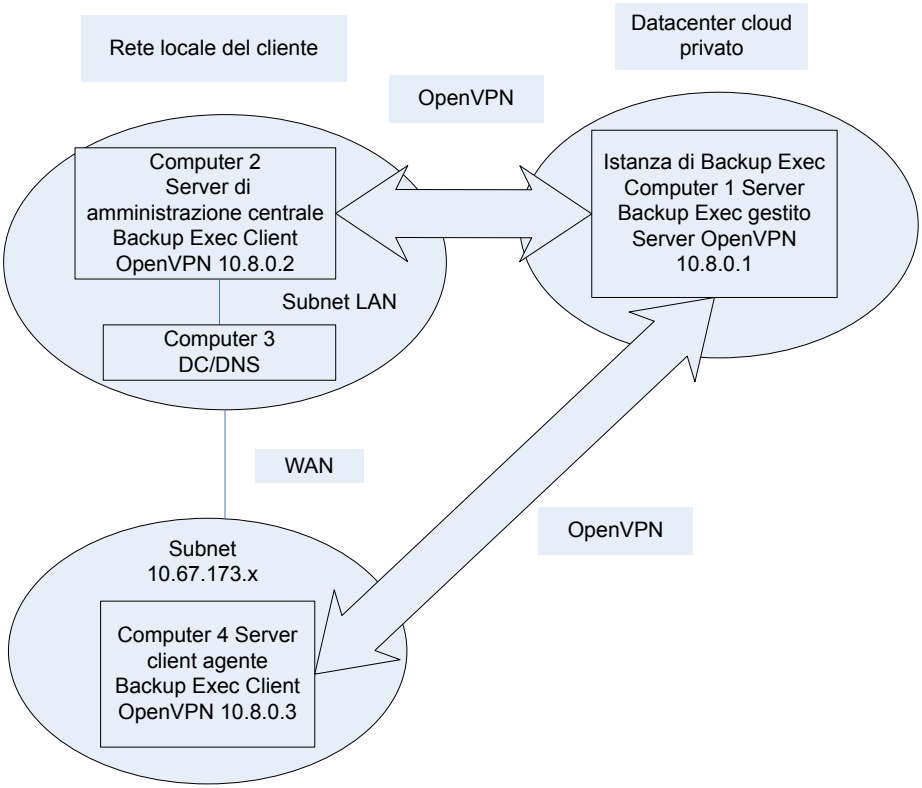
Informazioni sulla configurazione di OpenVPN per client multipli

Si può configurare OpenVPN per utilizzarlo con client multipli. Può essere necessario utilizzare una configurazione VPN del client multiplo se si possiede una rete locale complessa. Ad esempio, se si utilizzano le subnet locali multiple, si può beneficiare di una configurazione VPN di client multipli.

Vedere "Informazioni sulla configurazione di OpenVPN" a pagina 61.

Avvertimento: OpenVPN non deve essere installato su un controller di dominio. Le configurazioni multihomed del controller di dominio non sono supportate per Backup Exec Private Cloud Services.

Figura 4-1 Configurazione di VPN client multipli



Il server OpenVPN è l'istanza del cloud privato. I client sono i computer sulla LAN locale. L'utilizzo di client OpenVPN multipli richiede l'utilizzo di certificati di sicurezza piuttosto che di file di testo della chiave condivisa da utilizzare per le

configurazioni del client singolo. Nella configurazione client multipli, ogni client OpenVPN ha la propria chiave e il proprio certificato.

Nota: I file chiave sono importanti. Se un file chiave viene compromesso, si deve rigenerarlo. Se le file chiave (CA) dell'autorità di certificazione è compromesso, si devono rigenerare tutte le chiavi basate su quel CA.

Per configurare OpenVPN per i client multipli, attenersi alla procedura utilizzando gli esempi pubblicamente disponibili. I siti seguenti forniscono le istruzioni complete per configurare i certificati e i client multipli OpenVPN:

http://www.runpcrun.com

http://openvpn.net

Un'altra opzione per le reti più complesse è di utilizzare OpenVPN su un router di gateway della rete locale. Un router di gateway della rete locale fornisce una connessione point-to-point di OpenVPN. Altri computer locali possono dirigersi al VPN senza dovere aggiungere ulteriori client di OpenVPN e router di rete del computer. Consultare il produttore e la documentazione del router per maggiori dettagli circa il loro supporto per OpenVPN.

Le organizzazioni software di terzi inoltre forniscono gli aggiornamenti del firmware del router che includono il supporto di OpenVPN. Il sito seguente fornisce un esempio:

http://www.dd-wrt.com

Una volta configurato OpenVPN per più client, è possibile creare ed eseguire i processi di backup diretti per eseguire il backup dei dati del client. È possibile utilizzare l'istanza nel cloud privato come destinazione di backup per i processi di backup diretti o le operazioni di backup di duplicazione.

Risoluzione di problemi di rete

Se si riscontrano problemi di rete con Backup Exec Private Cloud Services, è necessario verificare che il server e il client di OpenVPN riescano a collegarsi tra di loro.

Per risolvere i problemi di rete

1. Disattivare temporaneamente i firewall di Windows o aggiungere le eccezioni appropriate di firewall ICMP per tutti i computer nella configurazione di Backup Exec Private Cloud Services.
2. Su entrambi i computer 1 (C1)e 2 (C2), avviare i servizi di OpenVPN utilizzando l'utilità di Windows Services.

3. Su entrambi i computer C1 e C2, aprire i file di registro di OpenVPN nella seguente directory e verificare che ogni file contenga il testo "Sequenza di inizializzazione completata":

   C:\Programmi (X86)\OpenVPN\registro

4. Ping 10.8.0.1 e 10.8.0.2 da C1, C2 e computer 3 (C3) per verificare la connettività.

5. Da C1, ping indirizzo IP locale di C2 e indirizzo IP locale di C3.

   Assicurarsi che la proprietà DNS della scheda della rete locale di OpenVPN contenga il suffisso di dominio locale quando OpenVPN è connesso.