Private Backup Exec Cloud-Dienste

Planungs- und Bereitstellungshandbuch

Symantec™

Inhalt

Kapitel 1

Einleitung zu privaten Backup Exec Cloud-Dienste

In diesem Kapitel werden folgende Themen behandelt:

Infos zu Backup Exec-Diensten in der privaten Cloud

Backup Exec-Dienste in der privaten Cloud sind für verwaltete Dienstanbieter (MSP) vorgesehen, die daran interessiert sind, verwaltete Backup-Dienste für ihre Kunden bereitzustellen. Mit Backup Exec-Dienste in der privaten Cloud können Partner Backup-Speicher in ihren Datenzentren als "private Cloud"-Konfiguration hosten.

Verwaltete Dienstanbieter können Backup-Dienste über das Internet für privaten Cloud-Partner als Alternative zum Verwalten von Offsite-Kopien von Bändern anbieten. Die Backups sind verschlüsselt und dedupliziert, wodurch der Transport über WAN sicher und effizient gemacht wird. Lokale Backups sind noch immer vor Ort für schnelle Wiederherstellungsfunktionen verfügbar. Zusätzlich können Benutzer mit privaten Backup Exec Cloud-Dienste Backups direkt auf Cloud durchführen. Benutzer können die vollständige oder granulare Daten direkt von Cloud wiederherstellen.

Private Backup Exec Cloud-Dienste sind außerdem für Backup Exec-Kunden mit weit verteilten Netzwerken bestimmt. Kunden können doppelte Kopien von Backups von standortferne Niederlassungen an Datenträgerspeicher und Bandspeicher innerhalb eines zentralen privaten Cloud-Rechenzentrums senden.

Die folgende Tabelle erklärt einige Backup Exec-Begriffe, die zum Verständnis von Backup Exec-Dienste in der privaten Cloud wichtig sind.

Tabelle 1-1 Backup Exec-Begriffe

Begriff	Definition
Deduplizierungdatenträgerspeicher	Ein Deduplizierungdatenträgerspeichergerät liefert integrierte Deduplizierung auf dem Backup Exec-Server. **Hinweis:** Sie können Deduplizierungspeicherappliances von Symantec NetBackup 5000/5020-Serie statt einem integrierten Backup Exec-Deduplizierungspeichergerät in der Cloud verwenden. Eine Appliance stellt möglicherweise eine skalierbarere Option, besonders für große mandantenfähige Konfigurationen zur Verfügung.
Optimierte Duplizierung	Eine Art von Duplizierung mit der deduplizierte Daten direkt von einem OpenStorage-Gerät auf ein anderes des gleichen Herstellers kopiert werden können.
Granular Recovery Technology (GRT)	Eine Backup-Option, mit der einzelne Elemente von den Datenbank-Backups wiederhergestellt werden können. Ein separates Backup der einzelnen Elemente ist nicht erforderlich, um ein Element wiederherzustellen.

Siehe "Sicherheitsbetrachtungen für private Backup Exec Cloud-Dienste" auf Seite 9.

Siehe "Systemanforderungen für Backup Exec-Dienste in einer privaten Cloud" auf Seite 11.

Siehe "Konfigurieren von Backup Exec-Diensten in einer privaten Cloud" auf Seite 13.

Siehe "Infos zu Backup Exec-Dienstkonfigurationen in der privaten Cloud" auf Seite 15.

Sicherheitsbetrachtungen für private Backup Exec Cloud-Dienste

Private Backup Exec Cloud-Dienste verwendet das aktuelle Auftrags- und Ressourcen-Identifikationsdaten-Modell von Backup Exec, um eine sichere Bedienung bereitzustellen. Symantec empfiehlt außerdem, dass Sie eine sichere Netzwerkverbindung zwischen dem Kundenort und dem Rechenzentrum verwenden, die die VPN-Lösung nutzt. Verschiedene IPsec, SSL-Layer und andere VPN-Lösungen sind verfügbar.

Sie müssen VLAN- oder Route-Einschränkungen verwenden, um Kundennetzwerke voneinander zu isolieren, wenn Sie eine Konfiguration verwenden, die mehrere Kunden unterstützt.

Sie können jede VPN-Lösung verwenden, die Sie bevorzugen. Dieses Handbuch bietet Referenzkonfigurationsanweisungen für OpenVPN. Das OpenVPN-SSL-VPN-Paket bietet eine sichere, verschlüsselte Verbindung zwischen der privaten Cloud Backup Exec-Instanz und dem lokalen Backup Exec-Server. Diese Komponente erfordert normalerweise, dass der Standard-Port 1194 auf der Firewall geöffnet ist. Mit OpenVPN können Sie jedoch nach Belieben auch einen anderen Port dafür vorsehen. OpenVPN arbeitet sowohl mit der schlüsselbasierten als auch mit der zertifikatbasierten Authentifizierungsethode. Dieses Dokument enthält Hinweise für das Konfigurieren beider Methoden.

Siehe "Infos zu Backup Exec-Diensten in der privaten Cloud" auf Seite 7.

Siehe "Info zum Konfigurieren von OpenVPN" auf Seite 63.

Die mandantenfähige Backup Exec-Serverkonfiguration hat zusätzliche Sicherheitsanforderungen, die Sie beachten sollten.

Siehe "Sicherheitsanforderungen für die Konfiguration des mandantenfähigen Backup Exec-Servers" auf Seite 9.

Sicherheitsanforderungen für die Konfiguration des mandantenfähigen Backup Exec-Servers

Sie können Backup Exec in einer privaten Cloud konfigurieren, in der ein einzelner Backup Exec-Server mehrere Kunden oder Mandanten sicher unterstützen kann. Sie müssen zusätzliche Sicherheitsmaßnahmen befolgen, wenn Sie einen mandantenfähigen Backup Exec-Server verwenden, da er den gemeinsam genutzten Inhalt mehrerer Kunden enthält.

Siehe "Info zur Konfiguration des mandantenfähigen Cloud-Backup Exec-Servers" auf Seite 17.

Siehe "Sicherheitsbetrachtungen für private Backup Exec Cloud-Dienste" auf Seite 9.

Beim Konfigurieren eines mandantenfähigen Backup Exec-Servers sollten Sie die folgenden Sicherheitsanforderungen berücksichtigen:

- Die lokalen verwalteten Backup Exec Server müssen auf physischen Computern installiert werden.
- Auf dem Systemdatenträger der lokalen verwalteten Backup Exec-Server muss die Funktion Microsoft Windows BitLocker aktiviert sein.
  Das BitLocker-Kennwort darf keinesfalls an Kunden weitergegeben werden. Als Alternative zu BitLocker können Sie auch eine Hardwaredatenträger-Verschlüsselung verwenden.
- Der mandantenfähige Backup Exec-Server, der sich in der privaten Cloud befindet, und die lokalen Backup Exec-Server müssen Mitglieder der Dienstanbieterdomäne sein.
  Kunden dürfen über keinen Login-Zugriff auf Backup Exec-Server verfügen. Für eine zusätzliche Isolierung empfiehlt es sich, für die verwalteten Backup Exec-Server jedes Kunden eine andere untergeordnete Dienstanbieterdomäne zu verwenden.
- Die Identifikationsdaten der Dienstanbieterdomäne für den lokalen verwalteten Backup Exec-Server sollten die eines lokalen Administrators, jedoch nicht die eines Domänenadministrators sein.
- Für das Deduplizierungsspeichergerät des mandantenfähigen Cloud-Servers darf die Client-seitige Deduplizierung nicht aktiviert sein.
- Der lokale verwaltete Backup Exec-Server darf nicht mit der Option "Uneingeschränkter Zugriff auf Kataloge und Backup-Sätze für Wiederherstellung" installiert werden. Sie sollten ihn nur mit der Option "Zentral verwalteter Backup Exec-Server" installieren.
- Ggf. können Sie die Zwei-Faktor-Authentifizierung für lokale verwaltete Backup Exec-Server verwenden, um zusätzliche Sicherheit zu gewährleisten.
  Symantec empfiehlt, dass Sie den VIP-Authentifizierungsservice von VeriSign verwenden:
  http://www.verisign.com/authentication/two-factor-authentication/vip-authentication/index.html

Warnung: Durch diese Sicherheitsmaßnahmen werden das gemeinsam genutzte Backup Exec-Netzwerk und die zugehörigen Speichergeräte nur bis zu einem gewissen Grad vor unberechtigtem Zugriff geschützt. Wenn jemand physisch auf einen verwalteten Backup Exec-Server zugreifen kann und bösartige Aktivitäten beabsichtigt, könnte diese Person diese Sicherheitsmaßnahmen theoretisch umgehen. Daher sollten Sie zusätzliche Schutzmaßnahmen zum Verhindern des unberechtigten physischen Zugriffs für Ihre lokalen verwalteten Backup Exec-Server erwägen.

Systemanforderungen für Backup Exec-Dienste in einer privaten Cloud

Die folgende Tabelle listet die Mindestsystemvoraussetzungen und Empfehlungen für das Ausführen von Backup Exec-Diensten in einer privaten Cloud auf:

Tabelle 1-2 Systemanforderungen für Backup Exec-Dienste in einer privaten Cloud

Anforderung	Beschreibung
Backup Exec-Server	Sie können Backup Exec-Dienste in einer privaten Cloud auf drei verschiedene Arten konfigurieren. Siehe "Infos zu Backup Exec-Dienstkonfigurationen in der privaten Cloud" auf Seite 15. Alle Backup Exec-Server in der Cloud müssen die Backup Exec Deduplication Option einschließen. Die einzige Anforderung an lokale Server ist, dass sie den Anforderungen für Backup Exec 2012 entsprechen. Eine Liste der kompatiblen Betriebssysteme, Plattformen und Anwendungen finden Sie unter folgender URL: http://entsupport.symantec.com/umi/V-269-1

Anforderung	Beschreibung
Lizenz für Deduplication Option	Sie müssen die Symantec Backup Exec Deduplication Option auf dem privaten Cloud-Server und allen lokalen Backup Exec-Servern installieren. Sie müssen kein Deduplizierungsspeichergerät auf dem lokalen Backup Exec-Server erstellen. Sie müssen jedoch die Deduplication Option auf dem lokalen Backup Exec-Server installieren, um auf das gemeinsam genutzte Deduplizierungsspeichergerät auf dem Server in der Cloud zugreifen zu können. Alle Konfigurationen erfordern ein Deduplizierungsspeichergerät auf dem Cloud-Backup Exec-Server.
Lizenz für Central Admin Server Option	Sie müssen die Symantec Backup Exec Enterprise Server Option mit Central Admin Server Option auf den lokalen Computern oder den Computer in der Cloud installieren, falls Sie entweder die mandantenfähigen oder Offsite-Kopiekonfigurationen verwenden.
Eine aktive Internetverbindung	Es muss eine aktive Internetverbindung bestehen, um Daten an Ihr Deduplizierungsspeichergerät in der privaten Cloud zu übertragen.
Virtual Private Network (VPN)	Symantec empfiehlt, dass Sie eine sichere Netzwerkverbindung zwischen dem Kundenort und dem Rechenzentrum unter Verwendung einer VPN-Lösung verwenden. Verschiedene IPsec- und des SSL-Layer-VPN-Lösungen sind verfügbar. Dieses Handbuch liefert Konfigurationsanweisungen für OpenVPN. Das Open Source-Paket OpenVPN (SSL-VPN) bietet eine sichere, verschlüsselte Verbindung zwischen der Backup Exec-Instanz in der privaten Cloud und dem lokalen Backup Exec-Server.

Kapitel 2

Konfigurieren von privaten Backup Exec Cloud-Dienste

In diesem Kapitel werden folgende Themen behandelt:

- Konfigurieren von Backup Exec-Diensten in einer privaten Cloud
- Infos zu Backup Exec-Dienstkonfigurationen in der privaten Cloud
- Einrichten der mandantenfähigen oder Offsite-Kopie für Cloud-Konfigurationen
- Einrichten der direkten Backup-Konfiguration

Konfigurieren von Backup Exec-Diensten in einer privaten Cloud

Um Backup Exec-Dienste in einer privaten Cloud zu konfigurieren, müssen Sie die folgenden Schritte ausführen.

Tabelle 2-1 Konfigurieren von Backup Exec-Diensten in einer privaten Cloud

Schritt	Beschreibung
Schritt 1	Sie müssen das VPN zwischen der Backup Exec-Serverinstanz in der privaten Cloud und allen Computern im lokalen Netzwerk konfigurieren. Siehe "Konfigurieren von OpenVPN" auf Seite 64. Siehe "Über das Konfigurieren von OpenVPN für mehrere Clients" auf Seite 70.

Schritt	Beschreibung
Schritt 2	Bestimmen Sie, welche der Konfigurationen für Backup Exec-Dienste in der privaten Cloud für Ihre Anforderungen am besten geeignet ist und wählen Sie diese aus. Sie können eine einzelne mandantenfähige Konfiguration für mehrere Kunden auswählen. Oder Sie verwenden für jeden Kunden eine Offsite-Kopie für die Cloud-Konfiguration oder direkte Backup-Konfiguration. Siehe "Infos zu Backup Exec-Dienstkonfigurationen in der privaten Cloud" auf Seite 15. Sie müssen Backup Exec-Dienste in der privaten Cloud konfigurieren. Siehe "Einrichten der mandantenfähigen oder Offsite-Kopie für Cloud-Konfigurationen" auf Seite 24. Siehe "Einrichten der direkten Backup-Konfiguration" auf Seite 36.
Schritt 3	Nachdem Sie das VPN und Backup Exec konfiguriert haben, können Sie mit den Backup Exec-Diensten in der privaten Cloud arbeiten. Siehe "Infos zum Arbeiten mit Backup Exec-Diensten in einer privaten Cloud für die Abseitskopiekonfigurationen" auf Seite 41. Siehe "Infos zum Arbeiten mit Backup Exec-Diensten in einer privaten Cloud und der direkten Backup-Konfiguration" auf Seite 49.

Schritt	Beschreibung
Schritt 4	Wenn Sie ein VPN-Gateway mit Porteinschränkungen verwenden, müssen Sie möglicherweise Portausnahmen auf den lokalen und den Cloud-VPN-Gateways öffnen. Portausnahmen ermöglichen dem Backup Exec-Server, der sich in der Cloud befindet, mit den lokalen Backup Exec-Servern und -Agents zu kommunizieren. Sie sollten außerdem den CAS Backup Exec SQL-Port von einem dynamisch zugewiesenen Port in einen statischen Port ändern. **Hinweis:** Wenn Sie OpenVPN verwenden, müssen Sie die Portausnahmen für die Gateway-Firewall konfigurieren. OpenVPN ist für gewöhnlich so konfiguriert, dass ein Tunnel durch Firewalls geöffnet wird. Die folgenden Backup Exec-Supportartikel führen alle Port-Nummern auf, die Backup Exec benötigt und die geöffnet werden müssen: 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 In den folgenden Backup Exec-Supportartikeln wird beschrieben, wie der statische SQL-Port konfiguriert wird: http://www.symantec.com/business/support/index?page=content&id=HOWTO22985

Infos zu Backup Exec-Dienstkonfigurationen in der privaten Cloud

Sie können Backup Exec-Dienste in der privaten Cloud auf vier verschiedene Möglichkeiten konfigurieren.

Tabelle 2-2 Bestimmte Konfigurationen für Backup Exec-Dienste in der privaten Cloud

Konfigurationstyp	Details
Mandantenfähige Cloud Backup Exec-Server	Die mandantenfähige Cloud Backup Exec-Server-Konfiguration stellt Offsite-Kopien und direkten Backup für einem Backup Exec-Server oder für einen zentralen Administrationsserver bereit, der sich in der privaten Cloud befindet. Der einzelne Backup Exec-Server in der privaten Cloud wird möglicherweise verwendet, um Daten für mehrere Kunden zu sichern. Siehe "Info zur Konfiguration des mandantenfähigen Cloud-Backup Exec-Servers" auf Seite 17.
Offsite-Kopie für verwaltete Backup Exec-Server in der Cloud	Die Offsite-Kopie für die verwaltete Backup Exec-Serverkonfiguration in der Cloud verwendet einen verwalteten Backup Exec-Server, einen zentralen Administrationsserver und einen Domänencontroller. Die Konfiguration stellt Offsite-Kopiefunktionen für einen verwalteten Backup Exec-Server zur Verfügung, der sich in der privaten Cloud befindet. Diese Konfiguration erfordert einen verwalteten Backup Exec-Server pro Kunden. Siehe "Info zur Offsite-Kopie für die Konfiguration verwalteter Cloud-Backup Exec-Server" auf Seite 21.

Konfigurationstyp	Details
Offsite-Kopie für zentrale Cloud-Administrationsserver-Konfiguration	Die Offsite-Kopie für die zentrale Cloud-Administrationsserverkonfiguration ist der ersten ähnlich, außer dass die Standorte des zentralen Administrationsservers und des verwalteten Backup Exec-Servers ausgetauscht sind. Die Konfiguration stellt Offsite-Kopienfunktionen zu einem zentralen Administrationsserver zur Verfügung, der sich in der privaten Cloud befindet. Diese Konfiguration erfordert einen zentralen Administrationsserver pro Kunden. Siehe "Über die Offsite-Kopie für die zentrale Cloud-Administrationsserver-Konfiguration" auf Seite 22.
Direktes Backup	Die direkte Backup-Konfiguration verwendet Backup Exec Agent for Windows oder Backup Exec Agent for Linux anstelle des verwalteten Backup Exec-Servers oder des zentralen Administrationsservers. Die Konfiguration stellt direkte Backup-Funktionen unter Verwendung eines Backup Exec-Servers zur Verfügung, der sich in der privaten Cloud befindet. Diese Konfiguration erfordert einen Backup Exec-Server pro Kunden. Siehe "Über die direkte Backup-Konfiguration" auf Seite 23.

Siehe "Info zum Konfigurieren von OpenVPN" auf Seite 63.

Siehe "Einrichten der mandantenfähigen oder Offsite-Kopie für Cloud-Konfigurationen" auf Seite 24.

Siehe "Einrichten der direkten Backup-Konfiguration" auf Seite 36.

Info zur Konfiguration des mandantenfähigen Cloud-Backup Exec-Servers

Die Konfiguration des mandantenfähigen Cloud-Backup Exec-Servers umfasst mehrere Computer.

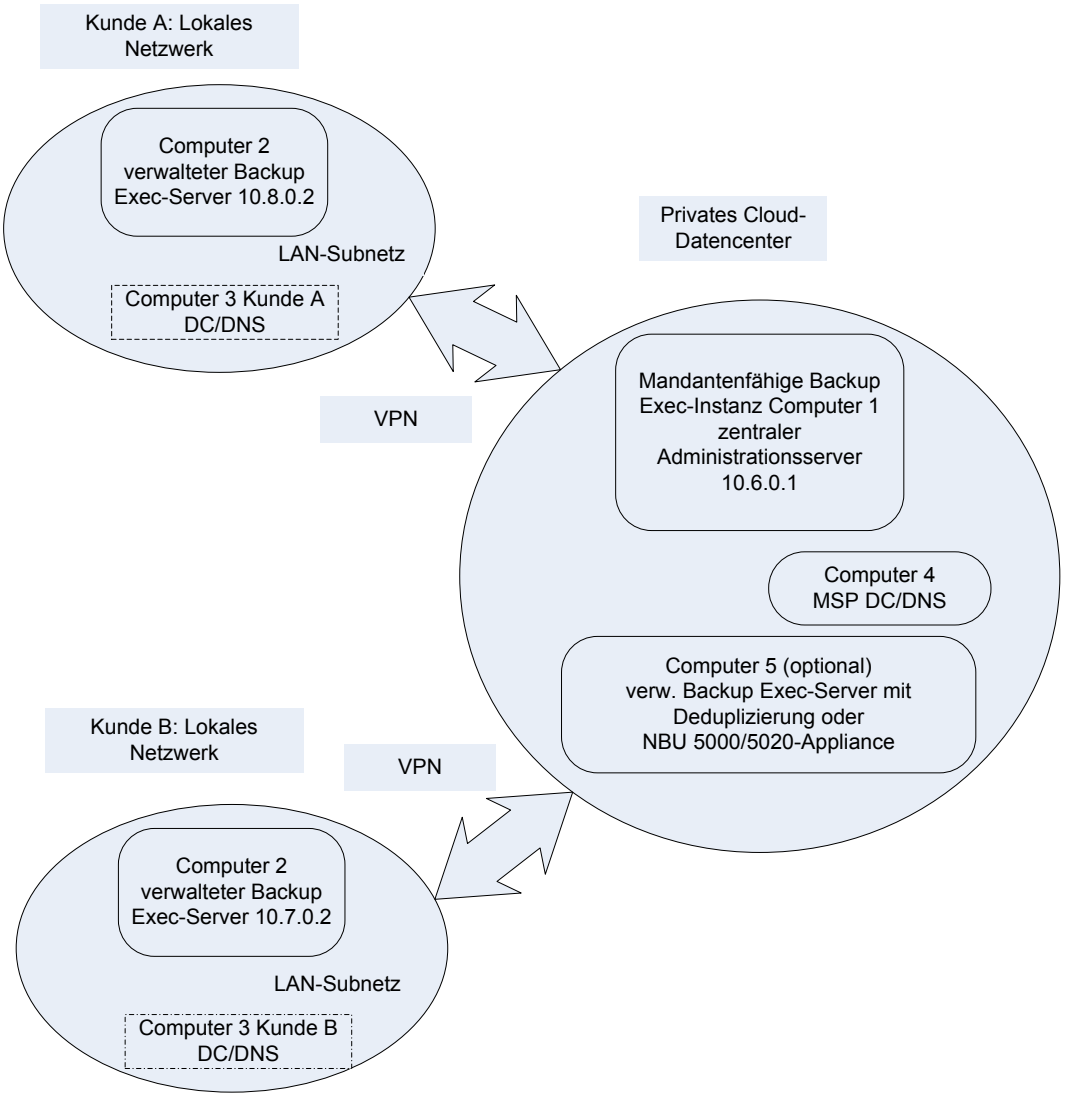
Tabelle 2-3 Konfiguration des mandantenfähigen Cloud-Backup Exec-Servers

Computer	Rolle
Computer 1	Der erste Computer (C1) ist ein Windows-64-Bit-Server, auf dem Backup Exec 2012 installiert ist. C1 ist als ein zentraler Administrationsserver konfiguriert und befindet sich in der privaten Cloud.
Computer 2	Der zweite Computer (C2) ist ein Windows-Server, auf dem Backup Exec 2012 installiert ist. C2 ist ein verwalteter Backup Exec-Server, der sich im LAN befindet und ein Mitglied der Clouddomäne des Dienstanbieters (C4) ist. **Hinweis:** Sie können einen lokalen 32-Bit-Backup Exec-Server für C2 verwenden, wenn Sie kein lokales Deduplizierungsspeichergerät benötigen.
Computer 3	Der dritte Computer (C3) ist ein Domänencontroller und ein DNS. Sie müssen einen C3-Computer für jeden Kundenstandort konfigurieren.
Computer 4	Der vierte Computer (C4) ist ein Domänencontroller und ein DNS, der sich in der privaten Cloud befindet.
Computer 5 (optional)	Der fünfte Computer (C5) ist ein optionaler, aber empfohlener verwalteter Backup Exec-Server. C5 enthält einen Deduplizierungsspeicherordner, der verwendet werden kann, um das Deduplizierungsspeichergerät des Computers C1 für zusätzliche Fehlertoleranz und Zuverlässigkeit zu replizieren. C5 kann sich in der privaten Cloud zusammen mit C1 oder an einem anderen physischen Standort befinden. Sie können ein Deduplizierungsspeichergerät der NetBackup 5000/5020-Serie als OST-Gerät auf dem Cloud-Backup Exec-Server als Alternative zu einem gemeinsam installierten C5-Computer konfigurieren.

Diese Konfiguration ermöglicht die Verwaltung aller Backup Exec-Aufträge innerhalb des Rechenzentrums der privaten Cloud. Es ist jedoch erforderlich, dass die Netzwerkverbindungen zwischen dem zentralen Administrationsserver und den verwalteten Backup Exec-Servern jederzeit aktiv sind. Die Netzwerkverbindungen müssen selbst dann aktiv sein, wenn Sie Aufträge lokal ausführen.

Warnung: Wenn Sie mehrere Kunden mit einem einzelnen Cloud-Backup Exec-Server unterstützen, müssen C1, C2, C4 und C5 in einer Domäne enthalten sein, auf die nur Sie zugreifen können. Um versehentliche oder bösartige Aktivitäten, die ein Sicherheitsrisiko darstellen können, zu vermeiden, dürfen Sie Kunden keinesfalls Zugriff auf C2 geben.

Abbildung 2-1 Mandantenfähiger Cloud-Backup Exec-Server



Siehe "Infos zu Backup Exec-Dienstkonfigurationen in der privaten Cloud" auf Seite 15.

Info zur Offsite-Kopie für die Konfiguration verwalteter Cloud-Backup Exec-Server

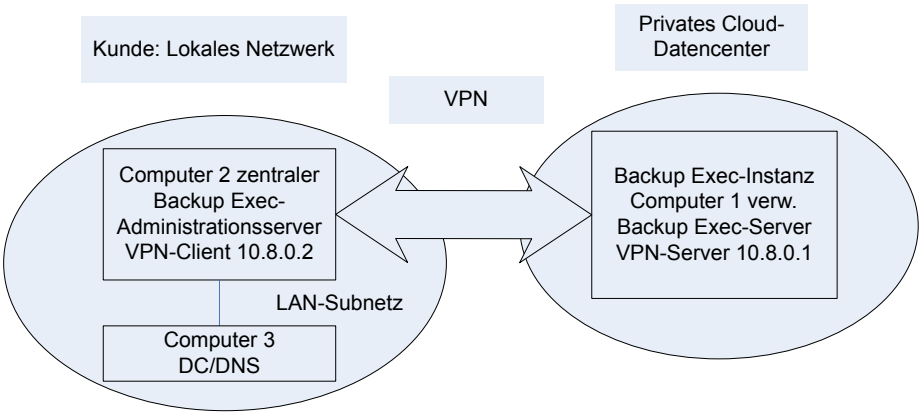
Die Offsite-Kopie für die Konfiguration verwalteter Cloud-Backup Exec-Server umfasst drei Computer.

Tabelle 2-4 Offsite-Kopie für die Konfiguration verwalteter Cloud-Backup Exec-Server

Computer	Rolle
Computer 1	Der erste Computer (C1) ist ein Windows-64-Bit-Server, auf dem Backup Exec 2012 installiert ist. C1 ist als verwalteter Backup Exec-Server konfiguriert und befindet sich in der privaten Cloud.
Computer 2	Der zweite Computer (C2) ist ein Windows-64-Bit-Server, auf dem Backup Exec 2012 installiert ist. C2 ist ein zentraler Administrationsserver, der sich im LAN befindet. **Hinweis:** Sie können einen lokalen 32-Bit-Backup Exec-Server für C2 verwenden, wenn Sie kein lokales Deduplizierungsspeichergerät verwenden möchten.
Computer 3	Der dritte Computer (C3) ist ein Domänencontroller und ein DNS.

Die Netzwerkverbindung zwischen dem zentralen Administrationsserver und dem verwalteten Backup Exec-Server muss nicht immer aktiv sein. Die Netzwerkverbindung ist nur erforderlich, wenn Sie einen Auftrag ausführen, der den verwalteten Backup Exec-Server in der privaten Cloud einschließt. Die Netzwerkverbindung muss für lokale Aufträge nicht aktiv sein.

Abbildung 2-2 Offsite-Kopie für verwaltete Cloud-Backup Exec-Server



Siehe "Infos zu Backup Exec-Dienstkonfigurationen in der privaten Cloud" auf Seite 15.

Über die Offsite-Kopie für die zentrale Cloud-Administrationsserver-Konfiguration

Die Offsite-Kopie bezieht drei Computer mit ein.

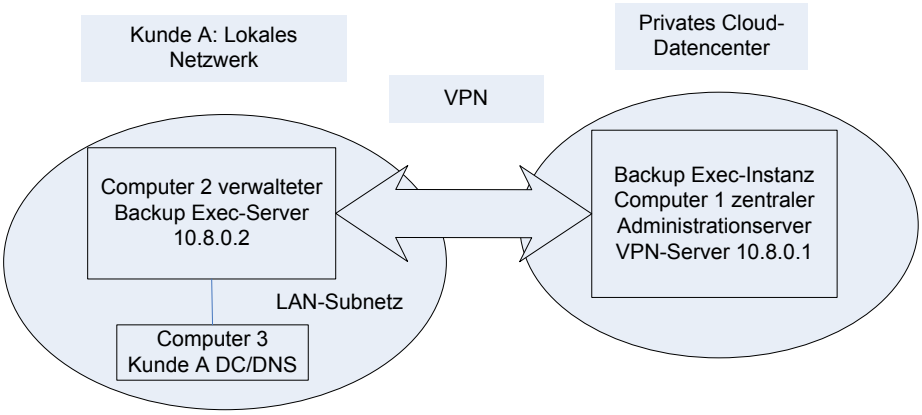
Tabelle 2-5 Offsite-Kopie für zentrale Cloud-Administrationsserver-Konfiguration

Computer	Rolle
Computer 1	Der erste Computer (C1) ist ein Windows-64-Bit-Server, auf dem Backup Exec 2012 installiert ist. C1 ist als ein zentraler Administrationsserver konfiguriert und befindet sich in der privaten Cloud.
Computer 2	Der zweite Computer (C2) ist ein Windows-64-Bit-Server, auf dem Backup Exec 2012 installiert ist. C2 ist ein verwalteter Backup Exec-Server, der sich im LAN befindet. **Hinweis:** Sie können einen lokalen 32-Bit-Backup Exec-Server für C2 verwenden, wenn Sie kein lokales Deduplizierungsspeichergerät verwenden möchten.

Computer	Rolle
Computer 3	Der dritte Computer (C3) ist ein Domänencontroller und ein DNS.

Diese Konfiguration ermöglicht die Verwaltung aller Backup Exec-Aufträge innerhalb des Rechenzentrums der privaten Cloud. Sie erfordert jedoch, dass die Netzwerkverbindung zwischen dem zentralen Administrationsserver und dem verwalteten Backup Exec-Server jederzeit aktiv ist. Die Netzwerkverbindung muss selbst dann aktiv sein, wenn Sie Aufträge lokal ausführen.

Abbildung 2-3 Offsite-Kopie für zentrale Cloud-Administrationsserver



Siehe "Infos zu Backup Exec-Dienstkonfigurationen in der privaten Cloud" auf Seite 15.

Über die direkte Backup-Konfiguration

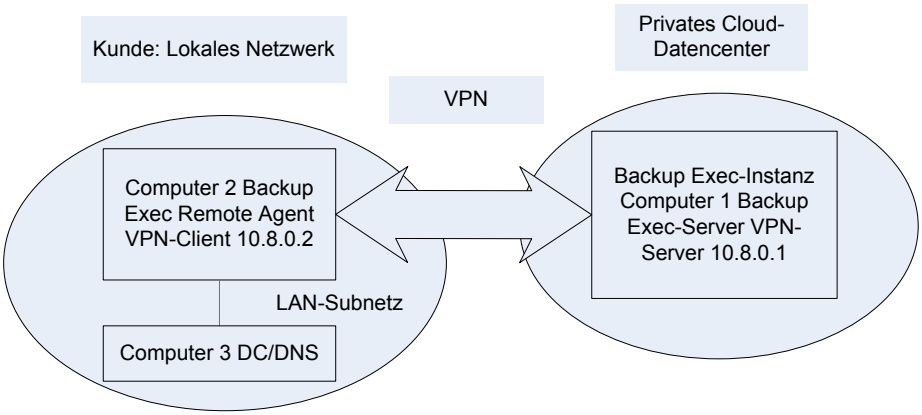
Die direkte Backup-Konfiguration bezieht mindestens drei Computer mit ein.

Tabelle 2-6 Direkte Backup-Konfiguration

Computer	Rolle
Computer 1	Der erste Computer (C1) ist der Windows 64-Bit-Backup Exec 2012-Server, der sich im Rechenzentrum der privaten Cloud befindet.
Computer 2	Der zweite Computer (C2) ist der Agent for Windows- oder Agent for Linux-Client, der sich im LAN befindet. Sie können mehrere Agent-Clientcomputer konfigurieren.

Computer	Rolle
Computer 3	Der dritte Computer (C3) ist ein Domänencontroller und ein DNS.

Abbildung 2-4 Direktes Backup



Siehe "Infos zu Backup Exec-Dienstkonfigurationen in der privaten Cloud" auf Seite 15.

Einrichten der mandantenfähigen oder Offsite-Kopie für Cloud-Konfigurationen

Nachdem Sie das VPN auf dem privaten Cloud-Server konfiguriert haben, sollten Sie die Backup Exec-Server konfigurieren.

Siehe "Konfigurieren von Backup Exec-Diensten in einer privaten Cloud" auf Seite 13.

Sie können entweder eine mandantenfähige Konfiguration oder eine von zwei Offsite-Kopien für Cloud-Konfigurationen auswählen:

Siehe "Info zur Konfiguration des mandantenfähigen Cloud-Backup Exec-Servers" auf Seite 17.

Siehe "Info zur Offsite-Kopie für die Konfiguration verwalteter Cloud-Backup Exec-Server" auf Seite 21.

Siehe "Über die Offsite-Kopie für die zentrale Cloud-Administrationsserver-Konfiguration" auf Seite 22.

Tabelle 2-7 Wie man die Offsite-Kopie für Cloud-Konfigurationen konfiguriert

Schritt	Beschreibung
Schritt 1	Installieren Sie den zentralen Backup Exec-Administrationsserver. Siehe "Installieren des zentralen Backup Exec-Administrationsservers" auf Seite 25.
Schritt 2	Installieren Sie den verwalteten Backup Exec-Server. Siehe "Installation des verwalteten Backup Exec-Servers" auf Seite 27.
Schritt 3	Konfigurieren Sie Speichergeräte. Siehe "Einrichten von Speichergeräten für die mandatenfähigen und Offsite-Kopiekonfigurationen" auf Seite 29.
Schritt 4	Befüllen Sie das Deduplizierungsspeichergerät mit Daten. Siehe "Infos zum Befüllen des Deduplizierungdatenträgerspeichergeräts für die Offsite-Kopiekonfigurationen" auf Seite 31.

Installieren des zentralen Backup Exec-Administrationsservers

Sie müssen "Backup Exec for Windows Servers" auf dem Computer installieren, der als der Backup Exec-zentrale Administrationsserver dient.

Siehe "Einrichten der mandantenfähigen oder Offsite-Kopie für Cloud-Konfigurationen" auf Seite 24.

Wenn Sie die mandantenfähige Cloud Backup Exec-Server-Konfiguration verwenden, muss der Cloud Backup Exec-Server als der zentrale Administrationsserver (Computer 1 oder C1) installiert werden.

Wenn Sie die Offsite-Kopie für die von der Cloud verwaltete Backup Exec-Serverkonfiguration verwenden, wird der zentrale Administrationsserver auf einem Backup Exec-Server der regionalen Niederlassung installiert (Computer 2 oder C2). Andernfalls wird der zentrale Administrationsserver als ein Cloud-Backup Exec-Server (Computer 1 oder C1) für die Offsite-Kopie der zentralen Administrationsserverkonfiguration installiert.

Sie müssen den zentralen Administrationsserver einer Domäne hinzufügen. Installieren Sie die Enterprise Server-Option mit Central Admin Server Option (CASO) auf dem zentralen Administrationsserver.

Tabelle 2-8 Wie man den Backup Exec-zentralen Administrationsserver installiert

Schritt	Beschreibung
Schritt 1	Um einen mandantenfähigen Backup Exec-Server zu konfigurieren, fügen Sie den Backup Exec-Server der Cloud-Domäne hinzu. Um alles andere als die mandantenfähige Backup Exec-Serverkonfiguration zu konfigurieren, fügen Sie den Backup Exec-Server Ihrer lokalen Domäne hinzu, indem Sie die folgenden Schritte durchführen: ■ Unter Verwendung des Dialogfelds "Computereigenschaften" unter Windows fügen Sie den Server der Domäne hinzu. ■ Starten Sie den Computer neu, wenn Sie dazu aufgefordert werden.
Schritt 2	Nachdem der Server neu gestartet hat, loggen Sie mit dem Domänen-Konto ein, dem Sie Administratorrechte für Ihre lokale Backup Exec-Instanz gewähren möchten.
Schritt 3	Verwenden Sie die richtigen Lizenzschlüssel, um Backup Exec 2012 zu installieren. Weitere Informationen zum Installieren von Backup Exec finden Sie im *Administratorhandbuch für Symantec Backup Exec.* Backup Exec-Partner können Lizenzierungsinformationen von der Symantec PartnerNet-Website über den folgenden Link beziehen: https://partnernet.symantec.com/Partnercontent/Login.jsp
Schritt 4	Schließen Sie die Enterprise Server-Option in der Central Admin Server Option (CASO) ein, wenn Sie Backup Exec installieren. Weitere Informationen zzur Installation von CASO finden Sie im *Symantec Backup Exec-Administratorhandbuch.* Installieren Sie die Deduplizierungsoption, wenn Sie die mandantenfähige oder Offsite-Kopie für die zentralen Administrationsserverkonfigurationen verwenden. Die Verwendung eines lokalen Deduplizierungdatenträgerspeichergeräts auf dem zentralen Administrationsserver ist optional für die Offsite-Kopie für verwaltete Cloud Backup Exec-Server-Konfiguration.
Schritt 5	Verwenden Sie Domäneidentifikationsdaten für das Standardsystemslogin-Konto, wenn Sie Backup Exec installieren.

Schritt	Beschreibung
Schritt 6	Wenn Sie inkrementelle Exchange GRT duplizierte Backup-Aufträge auf der Cloud ausführen, legen Sie den folgenden Registrierungswert auf 1 fest, wenn die Installation abgeschlossen ist. Wenn der Registrierungswert geändert wird, wird die Funktion der GRT-zu-GRT-Kopie des Deduplizierungdatenträgerspeichergeräts auf dem Backup Exec-Server deaktiviert. dword HKEY LOCAL MACHINE\SOFTWARE\Symantec\Backup Exec for Windows\Backup Exec\Engine\Misc\DisablePDI2PDISetCopy Dieser Computer ist jetzt der zentrale Administrationsserver, der den verwalteten Backup Exec-Server über WAN steuert. Für nähere Informationen über die Beschränkungen der Offsite-Kopie mit Granular Recovery Technology (GRT) lesen Sie dieses Thema: Siehe "Beschränkungen der Granular Recovery Technology mit Offsite-Kopie" auf Seite 60.

Installation des verwalteten Backup Exec-Servers

Sie müssen den verwalteten Backup Exec-Server installieren. Wenn Sie die Offsite-Kopie für die verwaltete Cloud Backup Exec-Serverkonfiguration verwenden, wird der verwaltete Backup Exec-Server als der Cloud Backup Exec-Server installiert (Computer 1 - C1). Andernfalls wird der verwaltete Backup Exec-Server auf einem Backup Exec-Server der regionalen Niederlassung installiert (Computer 2 - C2).

Siehe "Einrichten der mandantenfähigen oder Offsite-Kopie für Cloud-Konfigurationen" auf Seite 24.

So installieren Sie den verwalteten Backup Exec-Server

1 Sie haben folgende Möglichkeiten:

Für die mandantenfähige Konfiguration:	Fügen Sie der Clouddomäne den Backup Exec-Server hinzu.

Für eine andere Konfiguration:	Fügen Sie Ihrer lokalen Domäne den Backup Exec-Server hinzu, indem Sie die folgenden Schritte durchführen: ■ Verwenden Sie das Dialogfeld "Computereigenschaften" unter Windows, um den Server der lokalen Domäne hinzuzufügen. ■ Starten Sie den Computer neu, wenn Sie dazu aufgefordert werden.

2. Nachdem der Server neu gestartet wurde, loggen Sie sich mit dem Domänenkonto ein, das Administratorrechte für Ihren lokalen Backup Exec-Server hat.
3. Installieren Sie Backup Exec 2012 auf dem Server und wählen Sie die Installationsoption Verwalteter Backup Exec-Server.
4. An der Eingabeaufforderung geben Sie die gleichen System-Login-Konto-Daten an, die Sie zur Installation des zentralen Administrationsservers verwendet haben.
5. Wenn Sie die Offsite-Kopie für die verwaltete Cloud Backup Exec-Serverkonfiguration zu verwenden, wählen Sie die Deduplizierungsoption.

   Die Verwendung eines lokalen Deduplizierungdatenträgerspeichergeräts auf dem verwalteten Backup Exec-Server ist optional für die Offsite-Kopie für die zentrale Coud-Administrationsserverkonfiguration.
6. Wenn Backup Exec Sie nach dem zentralen Administrationsserver fragt, geben Sie die Informationen für Ihren lokalen zentralen Backup Exec-Administrationsserver ein.
7. Wählen Sie die Option "Zentral verwalteter Backup Exec-Server" aus.

   Wählen Sie nicht Uneingeschränkter Zugriff auf Kataloge und Backup-Sätze für Wiederherstellung, wenn Sie die mandantenfähige Konfiguration verwenden.

8 Wenn Sie inkrementelle Exchange GRT-Duplizierungs-Backup-Aufträge für Cloud ausführen möchten, legen Sie den folgenden Registrierungswert auf 1 fest, wenn die Installation abgeschlossen ist.

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

Das Ändern des Registrierungswerts deaktiviert die GRT-zu-GRT-Duplikationskopierfunktion des Deduplizierungdatenträgerspeichergeräts auf dem Backup Exec-Server.

9 Öffnen Sie Backup Exec auf dem zentralen Administrationsserver.

10 Wählen Sie die Registerkarte Speicher und doppelklicken Sie dann auf den Backup Exec-Server, der sich im privaten Cloudrechenzentrum befindet.

11 Klicken Sie im linken Teilfenster auf "Einstellungen".

12 Wählen Sie im Feld "Private Cloud-Server" die Option "Aktiviert".

Einrichten von Speichergeräten für die mandatenfähigen und Offsite-Kopiekonfigurationen

Bevor Sie Backup-Jobs zur privaten Cloud ausführen können, müssen Sie Speichergeräte konfigurieren.

Siehe "Einrichten der mandantenfähigen oder Offsite-Kopie für Cloud-Konfigurationen" auf Seite 24.

Tabelle 2-9 Wie man Speichergeräte für die Offsite-Kopienkonfigurationen einrichtet

Schritt	Beschreibung
Schritt 1	Erstellen Sie neue lokale Datenträgerspeichergeräte auf dem lokalen Computer 2 (C2). Sie können bei Bedarf ein Deduplizierungsspeichergerät erstellen. Weitere Informationen zum Erstellen von Speichergeräten erhalten Sie im *Symantec Backup Exec-Administratorhandbuch*.

Schritt	Beschreibung
Schritt 2	Erstellen Sie ein neues Deduplizierungsspeichergerät auf Ihrer Backup Exec-Instanz in der privaten Cloud. Sie können ein Deduplizierungsspeichergerät der NetBackup 5000/5020-Serie für eine mandantenfähige Konfiguration als Alternative zu einem integriertem Deduplizierungsspeicher konfigurieren. Konfigurieren Sie die Appliance als OST-Speichergerät auf dem mandantenfähigen zentralen Administrationsserver. Weitere Informationen zum Erstellen von Deduplizierungsspeichergeräten finden Sie im *Symantec Backup Exec-Administratorhandbuch*. Falls Sie die mandantenfähige Konfiguration verwenden, müssen Sie die folgenden Schritte durchführen, um Client-seitige Deduplizierung für das Deduplizierungsspeichergerät in der privaten Cloud zu deaktivieren: ■ Doppelklicken Sie auf der Registerkarte "Speicher" auf das Deduplizierungsspeichergerät des Backup Exec-Servers in der privaten Cloud. ■ Wählen Sie "Eigenschaften" aus. ■ Wählen Sie im Fenster "Clientseitige Deduplizierung" die Option "Deaktiviert". ■ Starten Sie die Dienste des Backup Exec-Servers neu. Symantec empfiehlt, falls möglich, einen dedizierten Datenträger für das Deduplizierungsspeichergerät zu verwenden. Geben Sie dem Deduplizierungsspeichergerät einen eindeutigen Namen, um es vom lokalen Deduplizierungsspeichergerät zu unterscheiden, falls Sie eines erstellt haben.
Schritt 3	Falls die gespeicherten Daten auf Ihrem Deduplizierungsspeichergerät in der privaten Cloud verschlüsselt werden sollen, wählen Sie "Ja, Daten während der Übertragung auf dieses Deduplizierungsspeichergerät und während der Speicherung der Daten auf dem Gerät verschlüsseln", wenn Sie ein neues Deduplizierungsspeichergerät konfigurieren. Bei einem vorhandenen Deduplizierungsgerät können Sie in den Eigenschaften des Deduplizierungsgeräts das Feld "Verschlüsselung" ändern. **Hinweis:** Das VPN verschlüsselt die Daten, die zwischen dem lokalen Backup Exec-Server und dem Backup Exec-Server in der Cloud übertragen werden.

Schritt	Beschreibung
Schritt 4	Nutzen Sie das neue Deduplizierungsspeichergerät in der Cloud gemeinsam mit den lokalen Backup Exec-Computern. Weitere Informationen zum gemeinsamen Nutzen von Deduplizierungsspeichergeräten finden Sie im *Symantec Backup Exec-Administratorhandbuch*.
Schritt 5	Verwenden Sie den Backup Exec-Dienstmanager, um alle Backup Exec-Dienste auf dem lokalen Backup Exec-Server zu beenden und zu starten. Die Freigabe des Deduplizierungsspeichergeräts in der Cloud für Ihre lokalen Backup Exec-Server ist nun abgeschlossen. Das Deduplizierungsspeichergerät in der privaten Cloud sollte nun auf C1 und C2 angezeigt werden und von beiden Computern aus zugänglich sein.
Schritt 6 (Optional)	Für die mandantenfähige Konfiguration können Sie einen zusätzlichen verwalteten Backup Exec-Server mit einem Deduplizierungspeichergerät in der Cloud installieren. Der zusätzliche verwaltete Backup Exec-Server kann mit dem primären Backup Exec-Server in der Cloud gemeinsam genutzt werden, um das Deduplizierungspeichergerät des Primärservers zu replizieren. Sie können ein Deduplizierungsspeichergerät der NetBackup 5000/5020-Serie als Alternative zu dem zusätzlichen verwalteten Backup Exec-Server installieren. Die Appliance kann für die Replikation verwendet werden. Fügen Sie die Appliance als OST-Speichergerät auf dem primären Backup Exec-Server in der Cloud hinzu. **Warnung:** Sie müssen Client-seitige Deduplizierung für eine dieser optionalen Konfigurationen deaktivieren.

Infos zum Befüllen des Deduplizierungdatenträgerspeichergeräts für die Offsite-Kopiekonfigurationen

Um lange Übertragungszeiten über das Internet zu vermeiden, können Sie Ihr Deduplizierungsspeichergerät in der Cloud mit den Daten befüllen, die Sie für den Anfang benötigen. Beim Befüllen des Deduplizierungsspeichergeräts werden anfängliche Konfigurationsdateien oder Backup-Sätze in das Deduplizierungsspeichergerät platziert, um ihn zur Verwendung vorzubereiten. Die Übertragungszeiten hängen von der Datenmenge ab, die kopiert und auf der privaten Cloud Backup Exec-Instanz gesichert werden soll.

Sie können die ersten Daten je nach Datentyp mit einer von zwei Methoden befüllen:

- Sie können das Deduplizierungsspeichergerät mit Systemstatusbetriebssystembackups befüllen. Befüllen Sie das Deduplizierungsspeichergerät durch Ausführen von Duplizierungs-Backup-Aufträgen von Systemstatusdaten anderer Computer, die in der privaten Cloud ausgeführt werden. Sichern Sie Systemstatusdaten für die Computer, die auf dem gleichen Betriebssystem laufen wie die lokalen Computer, die Sie sichern möchten.
  Siehe "Befüllen von Betriebssystemdateien für die Offsite-Kopiekonfigurationen" auf Seite 32.
- Sie können ein physisches Übergangslaufwerk senden, das Backup-Sätze mit den relevanten Daten vom lokalen Backup Exec-Server zum privaten Cloud-Rechenzentrum enthält.
  Siehe "Infos zur Anwendung eines Übergangslaufwerks zum Befüllen des Deduplizierungsspeichergeräts für die Offsite-Kopiekonfigurationen" auf Seite 33.

Befüllen von Betriebssystemdateien für die Offsite-Kopiekonfigurationen

Um lange Übertragungszeiten über das Internet zu vermeiden, können Sie Ihr Deduplizierungsspeichergerät in der Cloud mit den Daten befüllen, die Sie für den Anfang benötigen. Eine Möglichkeit, das Deduplizierungsspeichergerät zu befüllen, ist die Verwendung der Systemstatus-Backup-Daten von anderen gemeinsam installierten Computern zu verwenden.

Siehe "Infos zum Befüllen des Deduplizierungdatenträgerspeichergeräts für die Offsite-Kopiekonfigurationen" auf Seite 31.

Tabelle 2-10 Wie man Betriebssystemdateien für die Offsite-Kopienkonfigurationen einfüllt

Schritt	Beschreibung
Schritt 1	Installieren Sie den Agent for Windows oder den Agent for Linux auf allen Computern, die in der privaten Cloud gemeinsam installiert sind. Weitere Informationen zur Installation von Backup Exec-Agents finden Sie im *Symantec Backup Exec-Administratorhandbuch*. Die Computer sollten die gleichen Betriebssystemversionen wie die Server ausführen, die auf den lokalen Kundennetzwerken gesichert werden sollen.

Schritt	Beschreibung
Schritt 2	Erstellen Sie Backup-Aufträge auf dem privaten Cloud Backup Exec-Server und führen Sie diese aus. Sichern Sie die Systemstatus- und Systemdatenträger dieser gemeinsam installierten Computer auf dem privaten Cloud-Deduplizierungsspeichergerät.

Infos zur Anwendung eines Übergangslaufwerks zum Befüllen des Deduplizierungsspeichergeräts für die Offsite-Kopiekonfigurationen

Um lange Übertragungszeiten über das Internet zu vermeiden, können Sie Ihr Deduplizierungsspeichergerät in der Cloud mit den Daten befüllen, die Sie für den Anfang benötigen. Eine Möglichkeit, das Deduplizierungsspeichergerät zu befüllen, ist die Verwendung eines physischen Übertragungslaufwerks.

Siehe "Infos zum Befüllen des Deduplizierungdatenträgerspeichergeräts für die Offsite-Kopiekonfigurationen" auf Seite 31.

Symantec stellt ein Taschenrechnertool bereit, mit dem die Zeit, die bei Verwendung eines Übertragungslaufwerks erforderlich ist, mit der Zeit, die für das Kopieren von Daten über das Internet erforderlich ist, verglichen werden kann. Den Taschenrechner finden Sie hier:

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

Um Ihre private Cloud Backup Exec-Instanz mit einem Übergangslaufwerk zu befüllen, gehen Sie wie folgt vor:

Siehe "Befüllen des Deduplizierungsspeichergeräts unter Verwendung eines Übertragungslaufwerks für die Offsite-Kopiekonfigurationen" auf Seite 33.

Befüllen des Deduplizierungsspeichergeräts unter Verwendung eines Übertragungslaufwerks für die Offsite-Kopiekonfigurationen

Sie können ein physisches Übergangslaufwerk verwenden, um Ihren privaten Cloud Backup Exec-Deduplizierungsspeicherordner zu füllen. Sie sparen durch das Befüllen Ihres Deduplizierungsspeichergeräts mit den Dateien, die für den Anfang erforderlich sind, Zeit, die Sie für die der Ausführung eines großen Backups über das Internet gebraucht hätten.

Siehe "Infos zur Anwendung eines Übergangslaufwerks zum Befüllen des Deduplizierungsspeichergeräts für die Offsite-Kopiekonfigurationen" auf Seite 33.

So befüllen Sie Ihr Deduplizierungsspeichergerät unter Verwendung eines Übertragungslaufwerks für die Offsite-Kopiekonfigurationen

1. Erstellen Sie Datenträgerspeicher auf einem tragbaren Laufwerk auf dem lokalen Backup Exec-Server, der Computer 2 (C2) ist.
2. Kopieren Sie einen Backup-Satz auf den Datenträgerspeicher und verschlüsseln Sie die Daten mit Software-Verschlüsselung unter Verwendung einer der folgenden Methoden:

Wenn Sie den Registrierungsschlüssel "DisablePDI2PDISetCopy" nicht während der Installation erstellt haben, dann können Sie Backup-Sätze kopieren	Führen Sie die folgenden Schritte aus: ■ Wählen Sie Option zum Kopieren der neuesten Sätze des vollständigen Backups der Daten, die Sie verwenden möchten, um Ihr privates Cloud-Deduplizierungspeichergerät zu befüllen. ■ Wählen Sie den Datenträgerspeicher aus, den Sie als das Speicherziel im Dialogfeld "Auftrag duplizieren" erstellt haben. ■ Konfigurieren Sie Software-Verschlüsselung im Dialogfeld "Auftrag duplizieren". Sie müssen einen Verschlüsselungsschlüssel für Software-Verschlüsselung erstellen oder auswählen.

Wenn Sie den Registrierungsschlüssel "DisablePDI2PDISetCopy" während der Installation erstellt haben, dann müssen Sie einen vollständigen Backup-Auftrag erstellen	Führen Sie die folgenden Schritte durch: ■ Erstellen Sie einen vollständigen Backup-Auftrag, der den Datenträgerspeicher für alle Anwendungen verwendet, die mit Symantecs Granular Recovery Technology (GRT) kompatibel sind. ■ Deaktivieren Sie GRT für alle bestimmten GRT-fähigen Anwendungen, die Sie sichern möchten. Weitere Informationen zu Beschränkungen der Offsite-Kopie an GRT finden Sie in folgendem Thema. Siehe "Beschränkungen der Granular Recovery Technology mit Offsite-Kopie" auf Seite 60. ■ Aktivieren Sie Software-Verschlüsselung im Teilfenster "Speicher". Sie müssen einen Verschlüsselungsschlüssel für Software-Verschlüsselung erstellen oder auswählen.

3 Führen Sie den Job aus, den Sie im vorherigen Schritt erstellt haben.

4 Versenden Sie den tragbare Datenträger zum privaten Cloud-Rechenzentrum.

5 Hängen Sie den tragbaren Datenträger an den privaten Cloud Backup Exec-Server an.

6 Erstellen Sie Datenträgerspeicher auf dem angehängten tragbaren Laufwerk unter Verwendung des Datenträgerspeichers, den Sie ursprünglich auf dem Laufwerk erstellt haben.

7 Erstellen Sie einen Backup Exec-Inventarvorgang auf dem tragbaren Datenträgerspeichergerät und führen Sie ihn aus.

8 Erstellen Sie einen Backup Exec-Katalogvorgang auf dem tragbaren Datenträgerspeichergerät und führen Sie ihn aus.

9 Kopieren Sie die Backup-Sätze auf dem Datenträgerspeichergerät und verwenden Sie das Cloud-Deduplizierungsspeichergerät als das Zielspeichergerät.

10 Wenn der Duplizierugnsvorgang abgeschlossen ist, können Sie Backup Exec verwenden, um die Dateien im Datenträgerspeicher auszurangieren und zu löschen. Verwenden Sie ein Datenträgerdienstprogramm, um das tragbare Laufwerk zu bereinigen.

Wenn Sie erfolgreich Ihr privates Cloud-Deduplizierungsspeichergerät befüllt haben, ist der Konfigurationsprozess abgeschlossen. Sie können zum folgenden Thema übergehen, um die Arbeit mit Backup Exec aufzunehmen:

Siehe "Infos zum Arbeiten mit Backup Exec-Diensten in einer privaten Cloud für die Abseitskopiekonfigurationen" auf Seite 41.

Einrichten der direkten Backup-Konfiguration

Nachdem Sie OpenVPN auf dem privaten Cloud-Server konfiguriert haben, sollten Sie die Backup Exec-Server konfigurieren.

Siehe "Konfigurieren von Backup Exec-Diensten in einer privaten Cloud" auf Seite 13.

Die direkte Backup-Konfiguration bezieht mindestens drei Computer mit ein.

Siehe "Über die direkte Backup-Konfiguration" auf Seite 23.

Tabelle 2-11 Wie man die direkte Backup-Konfiguration konfiguriert

Schritt	Beschreibung
Schritt 1	Konfigurieren Sie das Deduplizierungsspeichergerät in der privaten Cloud. Siehe "DKonfigurieren des privaten Cloud-Deduplizierungsspeichergeräts für die direkte Backup-Konfiguration" auf Seite 37.
Schritt 2	Befüllen Sie das Deduplizierungsspeichergerät in der privaten Cloud mit Daten. Siehe "Infos zum Befüllen des Deduplizierungsspeichergeräts für die direkte Backup-Konfiguration" auf Seite 38.

DKonfigurieren des privaten Cloud-Deduplizierungsspeichergeräts für die direkte Backup-Konfiguration

Sie müssen das Backup Exec-Datenträgerspeichergerät und das Deduplizierungspeichergerät auf der privaten Cloud-Instanz erstellen.

Siehe "Einrichten der direkten Backup-Konfiguration" auf Seite 36.

Tabelle 2-12 Konfigurierung des privaten Cloud Backup Exec-Instanzdeduplizierungsspeichergeräts

Schritt	Beschreibung
Schritt 1	Loggen Sie sich bei C1 unter Verwendung des Domänenkontos ein, das Administratorrechte für Ihren lokalen Server hat.
Schritt 2	Installieren Sie Backup Exec 2012 auf C1 und geben Sie ein System-Login an.
Schritt 3	Erstellen Sie auf C1 in Backup Exec ein neues Deduplizierungsspeichergerät. Wenn Sie die Leerlaufdaten auf Ihrem privaten Clouddeduplizierungsspeichergerät verschlüsseln möchten, wählen Sie "Ja, Daten während der Übertragung auf dieses Deduplizierungsspeichergerät und während der Speicherung der Daten auf dem Gerät verschlüsseln", wenn Sie ein neues Deduplizierungsspeichergerät konfigurieren. Für ein vorhandenes Deduplizierungsgerät können Sie das Feld Verschlüsselung in den Eigenschaften des Deduplizierungsgeräts ändern. **Hinweis:** VPN verschlüsselt die Daten bei dem Transport zwischen dem lokalen Backup Exec-Server und dem Cloud Backup Exec-Server. Weitere Informationen zum Erstellen eines Deduplizierungsspeichergeräts finden Sie im *Symantec Backup Exec-Administratorhandbuch*.
Schritt 4	Aktivieren Sie die private Cloud-Servereinstellung: ■ Öffnen Sie Backup Exec auf dem Backup Exec-Server. ■ Klicken Sie auf die Backup Exec-Schaltfläche, wählen Sie "Konfiguration und Einstellungen" und klicken Sie dann auf "Eigenschaften des lokalen Servers". ■ Klicken Sie im linken Teilfenster auf "Einstellungen". ■ Wählen Sie im Teilfenster "Privater Cloud-Server" die Option "Aktiviert".

Infos zum Befüllen des Deduplizierungsspeichergeräts für die direkte Backup-Konfiguration

Um lange Übertragungszeiten über das Internet zu vermeiden, können Sie Ihr Deduplizierungsspeichergerät in der Cloud mit den Daten befüllen, die Sie für den Anfang benötigen. Beim Befüllen des Deduplizierungsspeichergeräts werden anfängliche Konfigurationsdateien oder Backup-Sätze in das Deduplizierungsspeichergerät platziert, um ihn zur Verwendung vorzubereiten. Die Übertragungszeiten hängen von der Datenmenge ab, die kopiert und auf der Cloud Backup Exec-Instanz gesichert werden muss.

Sie können die anfänglichen Daten unter Verwendung von zwei Methoden befüllen, je nach dem Typ von Daten, den Sie befüllen wollen:

- Sie können das Deduplizierungsspeichergerät mit Systemstatusbetriebssystem-Backups befüllen. Befüllen Sie das Deduplizierungsspeichergerät, indem Sie Backup-Aufträge von Systemstatusdaten anderer Computer ausführen, die in der privaten Cloud ausgeführt werden. Sichern Sie Systemstatusdaten für die Computer, die auf dem gleichen Betriebssystem laufen wie die lokalen Computer, die Sie sichern möchten.
  Siehe "Befüllen von Betriebssystemdateien für die direkte Backup-Konfiguration" auf Seite 38.
- Sie können ein physisches Übergangslaufwerk senden, das Backup-Sätze mit den relevanten Daten vom lokalen Backup Exec-Server zum privaten Cloud-Rechenzentrum enthält.
  Siehe "Befüllen des Deduplizierungsspeichergeräts unter Verwendung eines Übertragungslaufwerks für die direkte Backup-Konfiguration" auf Seite 39.

Befüllen von Betriebssystemdateien für die direkte Backup-Konfiguration

Um lange Übertragungszeiten über das Internet zu vermeiden, können Sie Ihr Deduplizierungsspeichergerät in der Cloud mit den Daten befüllen, die Sie für den Anfang benötigen. Eine Möglichkeit, das Deduplizierungsspeichergerätist zu befüllen, ist die Verwendung der Systemstatus-Backup-Daten von anderen gemeinsam installierten Computern zu verwenden.

Siehe "Infos zum Befüllen des Deduplizierungsspeichergeräts für die direkte Backup-Konfiguration" auf Seite 38.

Tabelle 2-13 Wie man Betriebssystemdateien für die direkte Backup-Konfiguration füllt

Schritt	Beschreibung
Schritt 1	Installieren Sie den Agent for Windows und den Agent for Linux auf allen Computern, auf denen Sie auf den lokalen Kundennetzwerken sichern möchten. Weitere Informationen zum Installieren von Backup Exec-Agents finden Sie im *Symantec Backup Exec-Administratorhandbuch*. Die Computer, denen Sie verwenden, um die Daten einzufüllen, sollten die gleichen Betriebssystemversionen verwendet werden wie die der Computer, die gesichert werden sollen.
Schritt 2	Erstellen Sie Backup-Aufträge auf dem privaten Cloud Backup Exec-Server und führen Sie sie aus. Sichern Sie die Systemstatus- und Systemdatenträger dieser gemeinsam installierten Computer auf dem privaten Cloud-Deduplizierungsspeichergerät.

Befüllen des Deduplizierungsspeichergeräts unter Verwendung eines Übertragungslaufwerks für die direkte Backup-Konfiguration

Sie können ein physisches Übertragungslaufwerk verwenden, um Ihr privates Cloud Backup Exec-Deduplizierungsspeichergerät zu befüllen. Das Befüllen Ihres Deduplizierungsspeichergeräts mit den Dateien, die für den Anfang erforderlich sind, kann Ihnen Zeit bei der Ausführung eines großen Backups über das Internet sparen.

Siehe "Infos zum Befüllen des Deduplizierungsspeichergeräts für die direkte Backup-Konfiguration" auf Seite 38.

Tabelle 2-14 Befüllen des Deduplizierungsspeichergeräts unter Verwendung eines Übertragungslaufwerks für die direkte Backup-Konfiguration

Schritt	Beschreibung
Schritt 1	Hängen Sie ein tragbares Laufwerk an Computer (C2) an.
Schritt 2	Kopieren Sie die Befüllungs-Dateien von C2 auf das tragbare Laufwerk.
Schritt 3	Verschlüsseln Sie die Dateien auf dem Datenträger unter Verwendung eines beliebigen Verschlüsselungtools eines Fremdherstellers.
Schritt 4	Versenden Sie das Übergangslaufwerk zum privaten Cloud-Rechenzentrum.

Schritt	Beschreibung
Schritt 5	Verbinden Sie das Übergangslaufwerk zu Computer 1 (C1).
Schritt 6	Entschlüsseln Sie die Daten auf dem Übergangslaufwerk vorübergehend, indem sie das gleiche Tool verwenden, das auch verwendet wurde, um die Daten zu verschlüsseln.
Schritt 7	Erstellen Sie und führen Sie einen Backup-Job aus, der die unverschlüsselten Dateien sichert. Verwenden Sie das Deduplizierungsspeichergerät in der Cloud als das Ziel.
Schritt 8	Wenn der Backup-Job vollständig ist, können Sie die kopierten Quelldateien löschen. Verwenden Sie ein Datenträgerdienstprogramm, um die das tragbare Laufwerk zu bereinigen.

Wenn Sie erfolgreich Ihr privates Cloud-Deduplizierungsgerät befüllt haben, ist der Konfigurationsprozess abgeschlossen.

Sie können zum folgenden Thema übergehen, um die Arbeit mit Backup Exec aufzunehmen.

Siehe "Infos zum Arbeiten mit Backup Exec-Diensten in einer privaten Cloud und der direkten Backup-Konfiguration" auf Seite 49.

Kapitel 3

Arbeiten mit privaten Backup Exec Cloud-Dienste

In diesem Kapitel werden folgende Themen behandelt:

Infos zum Arbeiten mit Backup Exec-Diensten in einer privaten Cloud für die Abseitskopiekonfigurationen

Mit Backup Exec-Diensten in einer privaten Cloud können Sie Backup-Definitionen unter Verwendung von Central Admin Server Options (CASO) und der Deduplizierungsoption verwalten.

Symantec stellt ein Taschenrechnertool bereit, mit dem Sie die Zeit schätzen können, die erforderlich ist, um Daten über das Internet zu kopieren. Der Cloud-Backup-Zeittaschenrechner kann für die Planung Ihrer Cloud-Backup-Strategie nützlich sein. Sie können den Taschenrechner verwenden,

um zu ermitteln, ob Ihre Systemressourcen für das Sichern von Kundendaten innerhalb eines zugeteilten Backup-Zeitrahmens ausreichen. Die Zeitschätzungen können Ihnen helfen, zu entscheiden, wie viel Daten Sie angemessen unterstützen können und wie viel Zeit Sie für die Cloud-Backups einsetzen sollten.

Den Taschenrechner finden Sie hier:

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

Siehe "Erstellen von Backup-Definitionen für die Offsite-Kopiekonfigurationen" auf Seite 42.

Siehe "Wiederherstellen von Daten von der privaten Cloud unter Verwendung der Offsite-Kopienkonfigurationen" auf Seite 45.

Siehe "Wiederherstellen von Daten von der privaten Cloud unter Verwendung der Offsite-Kopienkonfigurationen" auf Seite 45.

Siehe "Wiederherstellen von Daten von der privaten Cloud mit einem Übertragungslaufwerk unter Verwendung der Offsite-Kopiekonfiguration" auf Seite 46.

Erstellen von Backup-Definitionen für die Offsite-Kopiekonfigurationen

Sie können Backup-Daten in Ihre Backup Exec-Instanz der privaten Cloud kopieren, indem Sie eine Backup-Definition mit einer Duplizierungsstufe erstellen. Die Backup-Definition befindet sich auf dem zentralen Administrationsserver. Die Definition enthält Backup-Aufträge, die Daten auf dem lokalen Deduplizierungsspeichergerät sichern. Die Definition enthält auch eine Duplizierungsstufe, die dann die Backup-Sätze auf das Deduplizierungsspeichergerät der privaten Cloud kopiert.

Optional können Sie eine zusätzliche Duplizierungsstufe der Backup-Definition hinzufügen, um den kopierten Backup-Satz vom Duplizierungspeichergerät der privaten Cloud zu replizieren. Sie können den Backup-Satz auf ein Bandgerät kopieren, das sich auch in der Cloud befinden, oder auf ein anderes Deduplizierungsspeichergerät auf einem verwalteten Backup Exec-Server. Der verwaltete Backup Exec-Server kann sich in der privaten Cloud oder an einem anderen physischen Standort befinden.

Hinweis: Weitere Informationen zum Erstellen von Backup-Definitionen finden Sie im *Symantec Backup Exec-Administratorhandbuch*.

So erstellen Sie Backup-Definitionen für die Abseitskopiekonfigurationen

1. Öffnen Sie auf dem zentralen Administrationsserver Backup Exec.
2. Auf der Registerkarte "Backup und Wiederherstellung" haben Sie folgende Möglichkeiten:
   - Um einen einzelnen Server zu sichern, klicken Sie mit der rechten Maustaste auf den Servernamen.
   - Um mehrere Server zu sichern, klicken Sie bei gedrückter Umschalttaste oder Strg-Taste auf die Servernamen und klicken Sie dann mit der rechten Maustaste auf einen der ausgewählten Server.
3. Wählen Sie im Menü "Backup" die Backup-Option, die Sie verwenden möchten.
4. Geben Sie im Feld "Name" einen eindeutigen Namen für die Backup-Definition ein.

Hinweis: Wenn Sie Daten von mehreren Servern sichern, hängt Backup Exec den Servernamen an den Text an, den Sie im Feld "Name" eingeben. Backup Exec verwendet den Servernamen und den Text, die Sie eingegeben haben, um eindeutige Namen für jede Backup-Definition zu erstellen.

---

5. Führen Sie einen der folgenden Schritte aus:

So testen oder bearbeiten Sie die Identifikationsdaten, die Backup Exec für den Zugriff auf die Backup-Auswahl verwendet	Klicken Sie im Dialogfeld "Auswahl" auf "Identifikationsdaten testen/bearbeiten".
So ändern Sie die Backup-Auswahl	Klicken Sie im Dialogfeld "Auswahl" auf "Bearbeiten".

So fügen Sie der Backup-Definition eine Stufe hinzu	führen Sie die folgenden Schritte durch: ■ Klicken Sie im Dialogfeld "Backup" auf "Stufe hinzufügen". ■ Klicken Sie auf "Duplizieren", um die Duplizierungsstufe hinzuzufügen. ■ Klicken Sie im Dialogfeld "Duplizieren" auf "Bearbeiten". ■ Wählen Sie im Teilfenster "Speicher" das Deduplizierungsspeichergerät der privaten Cloud als Speicher für den Duplizierungsvorgang. ■ Nehmen Sie anderen Einstellungen, falls erforderlich, vor. Symantec empfiehlt, dass Sie den Duplizierungsvorgang als separater Auftrag verifizieren. Wenn Sie den Vorgang am Ende des Auftrags verifizieren, wird die Auftragsleistung herabgesetzt. Sie können den Verifizierungsvorgang im Teilfenster "Überprüfen" konfigurieren. **Hinweis:** Sie können zusätzliche Duplizierungsstufen der Backup-Definition hinzufügen. Sie müssen beispielsweise zusätzliche Kopien an ein gemeinsam installiertes Bandgerät oder an ein Deduplizierungspeichergerät auf einem standortfernen verwalteten Backup Exec-Server schicken.
So ändern Sie die Auftragseinstellungen	Führen Sie die folgenden Schritte durch: ■ Klicken Sie im Dialogfeld "Backup" auf "Bearbeiten". ■ Wählen Sie im Teilfenster "Speicher" das lokale Deduplizierungssspeichergerät als Speicher für den Backup-Auftrag aus. ■ Legen Sie beliebige anderen Einstellungen, falls erforderlich, fest.

6 Wenn Sie mit der Konfiguration der Backup-Definition fertig sind, klicken Sie im Dialogfeld "Backup-Eigenschaften" auf "OK".

Siehe "Infos zum Arbeiten mit Backup Exec-Diensten in einer privaten Cloud für die Abseitskopiekonfigurationen" auf Seite 41.

Wiederherstellen von Daten von der privaten Cloud unter Verwendung der Offsite-Kopienkonfigurationen

Nachdem Sie die Daten zur privaten Cloud Backup Exec-Instanz gesichert haben, können Sie sie jederzeit wiederherstellen. Das Wiederherstellen von Daten von einem Backup Exec-Deduplizierungsspeichergerät auf einer privaten Cloud verläuft ganz ähnlich wie das Wiederherstellen von Daten in Backup Exec.

Siehe "Wiederherstellen von Daten von der privaten Cloud unter Verwendung der Offsite-Kopienkonfigurationen" auf Seite 45.

Es ist möglicherweise effizienter, eine große Menge Daten von einer Backup Exec-Instanz einer privaten Cloud unter Verwendung eines physischen Übertragungslaufwerks wiederherzustellen. Sie können das Übertragungslaufwerk verwenden, um die Daten an den lokalen Backup Exec-Server zu übertragen. Verwenden Sie dann den lokalen Backup Exec-Server, um den Wiederherstellungsauftrag auszuführen.

Siehe "Wiederherstellen von Daten von der privaten Cloud mit einem Übertragungslaufwerk unter Verwendung der Offsite-Kopiekonfiguration" auf Seite 46.

Wiederherstellen von Daten von der privaten Cloud unter Verwendung der Offsite-Kopienkonfigurationen

Sie können Daten von der privaten Cloud Backup Exec-Instanz zu den lokalen Backup Exec-Clientcomputern wiederherstellen.

Siehe "Wiederherstellen von Daten von der privaten Cloud unter Verwendung der Offsite-Kopienkonfigurationen" auf Seite 45.

Wiederherstellen von Daten von der privaten Cloud unter Verwendung der Offsite-Kopienkonfigurationen

1. Stellen Sie sicher, dass der Server, den Sie wiederherstellen, den Netzwerk-Routenbefehl enthält, damit er mit Computer 1 (C1) wie im folgenden Verfahren beschrieben kommunizieren kann.

   Siehe "Konfigurieren der lokalen Netzwerk-Route" auf Seite 67.

2. Öffnen Sie Backup Exec auf dem zentralen Administrationsserver.

3 Klicken Sie auf der Registerkarte "Backup und Wiederherstellung" auf "Wiederherstellen".

4 Wählen Sie die Daten, die Sie wiederherstellen möchten und alle anderen notwendigen Auftragsoptionen, und reichen Sie dann den Auftrag ein.

Siehe "Infos zum Arbeiten mit Backup Exec-Diensten in einer privaten Cloud für die Abseitskopiekonfigurationen" auf Seite 41.

Wiederherstellen von Daten von der privaten Cloud mit einem Übertragungslaufwerk unter Verwendung der Offsite-Kopiekonfiguration

Sie können Daten von der Backup Exec-Instanz der privaten Cloud auf den lokalen Backup Exec-Server unter Verwendung eines Übertragungslaufwerks kopieren. Mit einem Übertragungslaufwerk können Sie eine große Menge Daten auf einmal wiederherstellen. Ein großer Wiederherstellungsjob kann sich auf Ihre Systemressourcen auswirken. Dies ist abhängig von der Menge der verfügbaren Bandbreite und der Zeit für die Abarbeitung des Jobs.

Siehe "Wiederherstellen von Daten von der privaten Cloud unter Verwendung der Offsite-Kopienkonfigurationen" auf Seite 45.

So stellen Sie Daten von der privaten Cloud unter Verwendung eines Übergangslaufwerks und der Offsite-Kopienkonfiguration wieder her

1 Erstellen Sie Datenträgerspeicher auf einem tragbaren Laufwerk auf Computer 1 (C1), der Backup Exec-Instanz der privaten Cloud.

2 Kopieren Sie die Backup-Sätze, die Sie vom Cloud-basierten Deduplizierungsspeichergerät wiederherstellen möchten. Wählen Sie den Datenträgerspeicher aus, den Sie als das Zielspeichergerät erstellt haben.

   Stellen Sie sicher, dass Sie die Daten mit Software-Verschlüsselung verschlüsseln. Sie müssen einen Verschlüsselungsschlüssel für Software-Verschlüsselung erstellen oder auswählen.

   Weitere Informationen zum Verschlüsseln von Daten finden Sie im *Symantec Backup Exec-Administratorhandbuch*.

3 Nachdem der Auftrag abgeschlossen ist, versenden Sie das Übertragungslaufwerk an die regionalen Niederlassung.

4 Nachdem das tragbare Laufwerk angekommen ist, verbinden Sie das Laufwerk mit dem lokalen Backup Exec-Server.

5 Erstellen Sie Datenträgerspeicher auf Computer 2 (C2) unter Verwendung des tragbaren Laufwerks als Pfad.

6 Erstellen Sie Backup Exec-Inventar- und -Katalogvorgänge auf dem Datenträgerspeicher und führen Sie sie aus.

7 Stellen Sie die Daten vom neuen Datenträgerspeicher auf dem entsprechenden Ziel wieder her.

8 Löschen Sie die Daten vom Übertragungslaufwerk.

Siehe "Infos zum Arbeiten mit Backup Exec-Diensten in einer privaten Cloud für die Abseitskopiekonfigurationen" auf Seite 41.

Wiederherstellen von Daten von einem verwalteten Backup Exec-Server im Falle eines Ausfalls des zentralen Administrationsservers

Wenn Ihr zentraler Administrationsserver von einem Hardwareausfall oder anderen Systemausfall betroffen ist, kann der verwaltete Backup Exec-Server keine Backup- oder Wiederherstellungsaufträge ausführen. Sie können den zentralen Administrationsserver wiederherstellen, indem Sie einen Ersatzcomputer konfigurieren und den zentralen Backup Exec-Administrationsserver neu installieren. Sie können jedoch auch einen verwalteten Backup Exec-Server in einen eigenständigen Backup Exec-Server umwandeln, um den zentralen Administrationsserver wiederherzustellen.

So wandeln Sie einen verwalteten Backup Exec-Server in einen eigenständigen Backup Exec-Server um, um den zentralen Administrationsserver wiederherzustellen

1 Notieren Sie sich für den verwalteten Backup Exec-Server die Namen und Verzeichnispfade aller lokaler Datenträgerspeicher.

Hinweis: Doppelklicken Sie auf der Registerkarte "Speicher" auf den Datenträgerspeicher. Klicken Sie dann im linken Teilfenster auf "Eigenschaften", um die Speichereigenschaften anzuzeigen.

2 Wenn der verwaltete Backup Exec-Server über ein eigenes Deduplizierungsspeichergerät verfügt, notieren Sie für das Gerät Name, Pfad, Login-Account und Kennworteigenschaften.

Hinweis: Doppelklicken Sie auf der Registerkarte "Speicher" auf das Deduplizierungsspeichergerät. Klicken Sie dann im linken Teilfenster auf "Eigenschaften", um die Speichereigenschaften anzuzeigen.

3 Öffnen Sie in der Windows-Systemsteuerung das Dialogfeld "Programme und Funktionen" (oder "Software") oder "Programm deinstallieren".

4. Wählen Sie die Option "Ändern" für Symantec Backup Exec aus.
5. Wählen Sie im linken Teilfenster "Zusätzliche Optionen", wenn es nicht bereits ausgewählt ist.
6. Klicken Sie auf "Weiter", bis Sie das Fenster "Verwalteten Backup Exec-Server konfigurieren" erreichen.
7. Wählen Sie die Option "Lokal verwalteter Backup Exec-Server" aus.
8. Klicken Sie auf "Weiter".
9. Führen Sie einen der folgenden Schritte aus, wenn die folgende Meldung angezeigt wird: "Verbindung mit {zentraler Administrationsserver} konnte nicht hergestellt werden. Stellen Sie sicher, dass der zentrale Administrationsserver ausgeführt wird."

Wenn der zentrale Administrationsserver nicht verfügbar ist und dieser verwaltete Backup Exec-Server lokal verwaltet werden soll	Klicken Sie zum Fortfahren auf "OK".
Wenn Sie diesen Vorgang wiederholen möchten, wenn der zentrale Administrationsserver ausgeführt wird	Klicken Sie auf "Abbrechen", um das Verfahren zu beenden.

   Wenn die Installation abgeschlossen ist, ist der Computer nicht mehr ein zentral verwalteter Backup Exec-Server.

10. Klicken Sie auf "Weiter".
11. Starten Sie den Computer neu, wenn Sie dazu aufgefordert werden.
12. Öffnen Sie Backup Exec und wählen Sie die Registerkarte "Speicher" aus.

    Wenn Backup Exec zum Backup Exec-Server keine Verbindung herstellen kann, starten Sie die Backup Exec-Dienste neu und versuchen Sie es erneut.

13. Erstellen Sie alle lokalen Datenträgerspeicher neu, indem Sie den Original-Datenträgerspeicher unter Verwendung der Namen und Pfade, die Sie in Schritt 1 notiert haben, importieren.

14 Erstellen Sie alle Deduplizierungsspeichergeräte neu, indem Sie die Original-Deduplizierungsspeichergeräte unter Verwendung der Informationen, die Sie in Schritt 2 notiert haben, importieren.

Hinweis: Er dauerte möglicherweise viel länger, ein bestehendes Speichergerät neu zu erstellen, als ein neues Speichergerät zu erstellen. Die Dauer hängt davon ab, wie viele Backup-Sätze das Speichergerät enthalten hat und ob dieser verwaltete Backup Exec-Server Zugriff auf Domänencontroller und DNS hat.

15 Erstellen Sie Backup Exec-Inventarisierungs- und -Katalogisierungsvorgänge auf jedem Speichergerät, das Sie wieder erstellt haben, und führen Sie sie aus.

Sie können jetzt den eigenständigen Backup Exec-Server verwenden, um alle Backup-Sätze wiederherzustellen, die auf den Speichergeräten des Backup Exec-Servers gespeichert waren.

16 Wenn Sie den eigenständigen Backup Exec-Server verwenden, um den zentralen Administrationsserver wiederherzustellen, müssen Sie möglicherweise die vorhandene Ressource des zentralen Administrationsservers auf dem eigenständigen Backup Exec-Server löschen. Installieren Sie anschließend Agent for Windows über eine Push-Installation auf dem zentralen Administrationsserver, bevor Sie ihn wiederherstellen.

Sobald der zentrale Administrationsserver wiederhergestellt wurde, können Sie über das Dialogfeld zum Ändern der Backup Exec-Installation den lokal verwalteten Backup Exec-Server zurück in einen zentral verwalteten Backup Exec-Server umwandeln. Wählen Sie die zentral verwaltete Backup Exec-Server-Option aus, um den Computer als verwalteten Backup Exec-Server neu zu konfigurieren.

Infos zum Arbeiten mit Backup Exec-Diensten in einer privaten Cloud und der direkten Backup-Konfiguration

Mit Backup Exec-Diensten in einer privaten Cloud können Sie Backup-Definitionen mit Client-seitiger Deduplizierung für die direkte Backup-Konfiguration verwalten.

Möglicherweise entscheiden Sie sich, die private Cloud Backup Exec-Instanz- und VPNlink-Verbindung manuell zu starten und zu beenden, wenn Sie Jobs ausführen. Oder Sie lassen die VPN-Link permanent stehen, so dass die Instanz ununterbrochen läuft. Sie können diesen Prozess aber auch automatisieren, indem Sie den OpenVPN-Dienst so planen, dass er um das Backup-Job-Fenster startet

und endet. Sie können das "Windows Scheduled Tasks"-Dienstprogramm verwenden, um einen Zeitplan für den Dienst zu erstellen.

Symantec stellt ein hilfreiches Taschenrechnertool bereit, mit dem Sie die Zeit schätzen können, die erforderlich ist, um Daten über das Internet zu kopieren. Der Cloud-Backup-Zeittaschenrechner kann für die Planung Ihrer Cloud-Backup-Strategie nützlich sein. Sie können den Taschenrechner verwenden, um zu ermitteln, ob Ihre Systemressourcen für das Sichern von Kundendaten innerhalb eines zugeteilten Backup-Zeitrahmens ausreichen. Die Zeitschätzungen können Ihnen helfen, zu entscheiden, wie viel Daten Sie angemessen unterstützen können und wie viel Zeit Sie für die Cloud-Backups einsetzen sollten.

Den Taschenrechner finden Sie hier:

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

Siehe "Aktivieren der Client-seitige Deduplizierung für die direkte Backup-Konfiguration" auf Seite 50.

Siehe "Erstellen von Backup-Definitionen für die direkte Backup-Konfiguration" auf Seite 51.

Siehe "Wiederherstellen von Daten von der privaten Cloud mit einem Übergangslaufwerk unter Verwendung der direkten Backup-Konfiguration" auf Seite 53.

Aktivieren der Client-seitige Deduplizierung für die direkte Backup-Konfiguration

Bevor Sie direkte Backup-Aufträge für die private Cloud Backup Exec-Instanz erstellen und ausführen können, müssen Sie Client-seitige Deduplizierung aktivieren.

Hinweis: Wenn Sie die mandantenfähigen Konfiguration verwenden, dürfen Sie Client-seitige Deduplizierung für das Deduplizierungsspeichergerät des zentralen Administrationsservers nicht aktivieren.

So aktivieren Sie Client-seitige Deduplizierung für die direkte Backup-Konfiguration

1. Doppelklicken Sie auf der Registerkarte "Speicher" auf den Speicher, dessen Eigenschaften Sie anzeigen möchten.
2. Klicken Sie im linken Teilfenster auf "Eigenschaften".
3. Wählen Sie im Teilfenster "Client-seitige Deduplizierung" die Option "Aktiviert" aus.

4 Klicken Sie auf "Anwenden".

5 Starten Sie die Backup Exec-Dienste neu.

Hinweis: Sie müssen Backup Exec-Dienste auf C1 beenden und neu starten.

Nachdem Sie Client-seitige Deduplizierung aktiviert haben, können Sie direkte Backup-Aufträge erstellen und ausführen.

Weitere Informationen zum Erstellen von Backup-Aufträgen mit Client-seitiger Deduplizierung, finden Sie im *Symantec Backup Exec-Administratorhandbuch*.

Siehe "Erstellen von Backup-Definitionen für die direkte Backup-Konfiguration" auf Seite 51.

Siehe "Infos zum Arbeiten mit Backup Exec-Diensten in einer privaten Cloud und der direkten Backup-Konfiguration" auf Seite 49.

Erstellen von Backup-Definitionen für die direkte Backup-Konfiguration

Nachdem Sie OpenVPN konfiguriert und alle zusätzlichen Computer für das Remote Agent Sharing und die Client-seitige Deduplizierung aktiviert haben, können Sie direkte Backup-Aufträge erstellen und ausführen.

Siehe "Aktivieren der Client-seitige Deduplizierung für die direkte Backup-Konfiguration" auf Seite 50.

Hinweis: Weitere Informationen zum Erstellen von Backup-Definitionen finden Sie im *Symantec Backup Exec-Administratorhandbuch*.

Verwenden Sie folgendes Verfahren, um Daten direkt zur privaten Cloud Backup Exec-Instanz zu sichern.

Backup-Jobs für die direkte Backup-Konfiguration erstellen

1 Auf Computer 1 (C1) öffnen Sie Backup Exec.

2 Auf der Registerkarte "Backup und Wiederherstellung" haben Sie folgende Möglichkeiten:

- Um einen einzelnen Server zu sichern, klicken Sie mit der rechten Maustaste auf den Servernamen.
- Um mehrere Server zu sichern, klicken Sie bei gedrückter Umschalttaste oder Strg-Taste auf die Servernamen und klicken Sie dann mit der rechten Maustaste auf einen der ausgewählten Server.

3 Wählen Sie im Menü "Backup" die Backup-Option, die Sie verwenden möchten.

4 Geben Sie im Feld "Name" einen eindeutigen Namen für die Backup-Definition ein.

Hinweis: Wenn Sie Daten von mehreren Servern sichern, hängt Backup Exec den Servernamen an den Text an, den Sie im Feld "Name" eingeben. Backup Exec verwendet den Servernamen und den Text, die Sie eingegeben haben, um eindeutige Namen für jede Backup-Definition zu erstellen.

5 Führen Sie einen der folgenden Schritte aus:

So testen oder bearbeiten Sie die Identifikationsdaten, die Backup Exec für den Zugriff auf die Backup-Auswahl verwendet	Klicken Sie im Dialogfeld "Auswahl" auf "Identifikationsdaten testen/bearbeiten".
So ändern Sie die Backup-Auswahl	Klicken Sie im Dialogfeld "Auswahl" auf "Bearbeiten".
So fügen Sie der Backup-Definition eine Stufe hinzu	Klicken Sie im Dialogfeld "Backup" auf "Stufe hinzufügen".
So ändern Sie die Auftragseinstellungen	Führen Sie die folgenden Schritte durch: ■ Klicken Sie im Dialogfeld "Backup" auf "Bearbeiten". ■ Stellen Sie sicher, dass die Option "Dem Remote-Computer ermöglichen, direkt auf das Speichergerät zuzugreifen und eine Client-seitige Deduplizierung durchzuführen, falls diese unterstützt wird" ausgewählt ist. ■ Legen Sie beliebige anderen Einstellungen, falls erforderlich, fest.

6 Wenn Sie mit der Konfiguration der Backup-Definition fertig sind, klicken Sie im Dialogfeld "Backup-Eigenschaften" auf "OK".

Siehe "Infos zum Arbeiten mit Backup Exec-Diensten in einer privaten Cloud und der direkten Backup-Konfiguration" auf Seite 49.

Wiederherstellen von Daten von der privaten Cloud mit einem Übergangslaufwerk unter Verwendung der direkten Backup-Konfiguration

Sie können einen normalen Wiederherstellungsjob erstellen, um Daten von der privaten Cloud Backup Exec-Instanz zum lokalen Client wiederherzustellen. Wenn Sie hingegen eine große Menge Daten auf einmal wiederherstellen möchten, ist möglicherweise sinnvoll, ein physisches Übergangslaufwerk zu verwenden. Die Zeit, die zur Übertragung einer großen Menge von Daten erforderlich ist, hängt von verfügbaren Bandbreite und der Zeit zur Ausführung des Jobs ab.

Wiederherstellen von Daten von der privaten Cloud mit einem Übergangslaufwerk unter Verwendung der direkten Backup-Konfiguration

1. Erstellen Sie einen Wiederherstellungsauftrag auf Computer 1 (C1) und führen Sie ihn aus, um die Dateien in einem Ordner auf einem tragbaren Laufwerk wiederherzustellen.
2. Nachdem der Auftrag abgeschlossen ist, verschlüsseln Sie die Dateien auf dem Datenträger unter Verwendung eines beliebigen Verschlüsselungs-Tools eines anderen Herstellers.
3. Versenden Sie das tragbare Laufwerk an die regionale Niederlassung.
4. Wenn das tragbare Laufwerk angekommen ist, entschlüsseln Sie die Dateien unter Verwendung des gleichen Tools, das zur Verschlüsselung eingesetzt wurde.
5. Übertragen Sie die unverschlüsselten Dateien zu ihrem richtigen Ziel auf Computer 2 (C2).
6. Löschen oder entfernen Sie die Dateien vom Übergangslaufwerk vollständig, um sicherzustellen, dass die Daten unwiderbringlich entfernt werden.

Siehe "Infos zum Arbeiten mit Backup Exec-Diensten in einer privaten Cloud und der direkten Backup-Konfiguration" auf Seite 49.

Info zum Cloud-Notfallwiederherstellungsdienst

Mit der Backup Exec 2012-Funktion "Simplified Disaster Recovery" 2012 (SDR) und der Funktion zur Konvertierung in einen virtuellen Computer können Dienstanbieter oder Kunden Cloud-Notfallwiederherstellungsdienste bereitstellen. Mit Backup-Daten, die in der Cloud gespeichert sind, können im Falle eines Systemausfalls temporäre virtuelle oder physische Ersatzserver in der privaten Cloud erstellt werden.

Bestimmte Netzwerkkonfigurationen und Ausfallbedingungen können die bei einem Failover und Failback notwendigen Schritte bestimmen. Dieser Abschnitt

beschreibt nur grundlegende Richtlinien für die Verwendung von SDR-Funktionen und Funktionen zur Konvertierung in virtuelle Computer innerhalb einer privaten Backup Exec-Cloud-Umgebung für die Bereitstellung von Notfallwiederherstellungsdiensten.

Es gibt zwei mögliche Hauptszenarien der Notfallwiederherstellung. Beim ersten Szenario handelt es sich um den Server-Failover und -Failback, wobei mindestens ein lokaler Server ausfällt, das lokale Netzwerk jedoch intakt bleibt. Beim zweiten Szenario handelt es sich um den Standort-Failover und -Failback, bei dem der gesamte Standort ausfällt.

Siehe "Wiederherstellen eines Servers oder eines Standorts bei einem Failover" auf Seite 54.

Siehe "Wiederherstellen eines Servers oder eines Standorts bei einem Failback" auf Seite 57.

Wiederherstellen eines Servers oder eines Standorts bei einem Failover

Um für einen Server-Failover vorbereitet zu sein, sollten Sie regelmäßig geplante Backup-Definitionen mit aktivierter Simplified Disaster Recovery(SDR)-Option für alle unternehmenskritischen Server konfigurieren und ausführen. Die Backup-Definitionen müssen Duplizierungsstufen enthalten, die die Backup-Daten auf das Deduplizierungsspeichergerät in der privaten Cloud kopieren. Wenn ein Server-Failover auftritt, verwenden Sie den privaten Cloud-Backup Exec-Server, um virtuelle oder physische Ersatzserver wiederherzustellen.

Siehe "Info zum Cloud-Notfallwiederherstellungsdienst" auf Seite 53.

Um einen physischen Ersatzserver wiederherzustellen, führen Sie mithilfe der Simplified Disaster Recovery Disk eine Bare Metal Restore aus. Verwenden Sie das neueste SDR-aktivierte Backup auf dem Deduplizierungsspeichergerät in der privaten Cloud. Sie können den Ersatzserver zum lokalen Standort transportieren, um den ausgefallenen Server zu ersetzen. Bei einem Standort-Failover muss eine ganze Gruppe unternehmenskritische Server durch virtuelle Computer in einer Hypervisor-Umgebung in der Cloud ersetzt werden.

Weitere Informationen zu Simplified Disaster Recovery finden Sie im *Symantec Backup Exec-Administratorhandbuch*.

Hinweis: Bestimmte Netzwerkkonfigurationen und Ausfallbedingungen können die bei einem Failback notwendigen Schritte bestimmen. Das folgende Verfahren bietet nur grundlegende Richtlinien für die Verwendung einer privaten Backup Exec-Cloud-Umgebung zur Bereitstellung von Notfallwiederherstellungsdiensten.

So stellen Sie einen Server oder einen Standort bei einem Failover wieder her

1. Erstellen Sie am Cloud-Standort eine Hyper-V- oder VMWare ESX-Hypervisor-Umgebung.
2. Erstellen Sie für die virtuellen Ersatzcomputer, die auf dem Hypervisor ausgeführt werden, ein virtuelles Netzwerk mit Fencing. Die Ersatzserver sollten ihre ursprünglichen lokalen IP-Adressen für ein gesamtes Standort-Failover-Szenario beibehalten.

   Hinweis: Wenn Sie einen Standort wiederherstellen, sollten die Ersatzserver ihre ursprünglichen lokalen IP-Adresse beibehalten. Sie sollten die Ersatzcomputer in einer logischen Reihenfolge wiederherstellen. Beispielsweise sollten Sie alle Domänencontroller und DNS-Server zuerst wiederherstellen.

3. Sie haben folgende Möglichkeiten:

Failover von einem physischen Computer aus	Führen Sie die folgenden Schritte aus: ■ Erstellen Sie einen Auftrag zur Konvertierung zu einem virtuellen Computer und führen Sie ihn aus. Konvertieren Sie den SDR-Point-in-Time-Systemdatenträger und die Systemstatusdaten in virtuelle Computer für alle Ersatzcomputer. Die virtuellen Computer sollten den Hypervisor zum Ziel haben. Wählen Sie zu diesem Zeitpunkt keine Anwendungsressourcen aus. ■ Konfigurieren Sie bei Bedarf feste IP-Adressen für die virtuellen Ersatzcomputer. ■ Stellen Sie zwischen dem virtuellen Ersatzcomputer oder den virtuellen Computern und den privaten Cloud-Backup Exec-Servern eine Netzwerkkonnektivität her. ■ Erstellen Sie Wiederherstellungsaufträge aus denselben SDR-aktivierten Point-In-Time-Backups für jeden der ersetzten Server und führen Sie sie aus. Wählen Sie alle Ressourcen des Computers aus, die für diesen Zeitpunkt verfügbar sind. Leiten Sie die Wiederherstellungsdaten an die Ersatzserver um.
Failover von einem virtuellen Computer aus	Erstellen Sie einen umgeleiteten Wiederherstellungsauftrag aus den neuesten SDR-Point-In-Time-Backups der Ersatzserver und führen Sie ihn aus. Für die lokalen und die Cloud-Server sollte derselbe Hypervisor-Typ verwendet werden.

4 Um nur einen einzelnen Server wiederherzustellen, stellen Sie eine VPN-Konnektivität zwischen dem virtuellen Ersatzserver und dem lokalen Netzwerk her und konfigurieren Sie alle lokalen DNS-Einträge für die IP-Adressen der virtuellen Ersatzcomputer.

5 Machen Sie alle neuen externen Adressen aus dem Cloud-Netzwerk verfügbar und ändern Sie alle externen DNS-Datensätze, wenn die ausgefallenen Server über externe IP-Adressen (z. B. einen Exchange-E-Mail-Server) verfügbar gemacht wurden.

6 Konfigurieren Sie regelmäßig geplante Hypervisor-Host-Backup-Definitionen für die virtuellen Ersatzcomputer und führen Sie sie aus. Verwenden Sie das Deduplizierungsspeichergerät in der privaten Cloud als Backup-Ziel.

Wenn die lokalen Backup Exec-Server über einen lokalen Deduplizierungsspeicher verfügen, müssen die Backup-Definitionen eine Duplizierungsstufe enthalten, die die Backups auf das lokale Deduplizierungsspeichergerät kopiert.

Wiederherstellen eines Servers oder eines Standorts bei einem Failback

Sie können einen Server oder einen Standort im Falle eines Failbacks wiederherstellen. Bei einem Standort-Failback-Szenario muss eine ganze Gruppe unternehmenskritischer Server auf lokalen physischen Servern oder virtuellen Computern wiederhergestellt werden.

Siehe "Info zum Cloud-Notfallwiederherstellungsdienst" auf Seite 53.

Sie sollten lokale Server nacheinander wiederherstellen, anstatt sie alle gleichzeitig wiederherzustellen. Sie können einige Server zuerst und andere erst nach einigen Tagen oder Wochen wiederherstellen. Bei dieser Strategie sind wahrscheinlich VPN-Konnektivität und IP-Adressen-Änderungen für die übrigen Ersatz-Cloud-Server, die eine Verbindung zum lokalen Netzwerk herstellen, erforderlich.

Weitere Informationen zu Simplified Disaster Recovery finden Sie im *Symantec Backup Exec-Administratorhandbuch*.

Hinweis: Bestimmte Netzwerkkonfigurationen und Ausfallbedingungen können die bei einem Failback notwendigen Schritte bestimmen. Das folgende Verfahren bietet nur grundlegende Richtlinien für die Verwendung einer privaten Backup Exec-Cloud-Umgebung zur Bereitstellung von Notfallwiederherstellungsdiensten.

So stellen Sie einen Server oder einen Standort bei einem Failback wieder her

1 Führen Sie ein Backup mit aktivierter Simplified Disaster Recovery(SDR)-Option aus und schließen Sie alle Duplizierungsstufen ein.

2 Schalten Sie die virtuellen Ersatzcomputer aus.

3 Wenn die SDR-aktivierte Backup-Definition keine Duplizierungsstufe umfasst hat, die Backup-Sätze an das lokale Deduplizierungsspeichergerät gesendet hat, führen Sie die folgenden Schritte aus:

- Fügen Sie ein tragbares Datenträgerspeichergerät zu Backup Exec auf den privaten Cloud-Backup Exec-Servern hinzu.
- Duplizieren Sie die Backup-Sätze aus dem letzten Point-In-Time-Backup der Daten aller Ersatzcomputer. Verwenden Sie das tragbare Datenträgerspeichergerät als Ziel.
- Schicken Sie das tragbare Datenträgerspeichergerät zum lokalen Standort.
- Fügen Sie das tragbare Datenträgerspeichergerät zu Backup Exec auf den lokalen Backup Exec-Servern hinzu.
- Inventarisieren und katalogisieren Sie das Datenträgerspeichergerät auf den lokalen Backup Exec-Servern.

4 Sie haben folgende Möglichkeiten:

So führen Sie einen Failback auf lokale physische Server aus	Führen Sie die folgenden Schritte aus: ■ Verwenden Sie die Simplified Disaster Recovery Disk, um eine Bare Metal Restore auszuführen. Wählen Sie die neuesten SDR-aktivierten Backups auf den lokalen Backup Exec-Servern aus. ■ Konfigurieren Sie bei Bedarf eine feste IP-Adresse für die wiederhergestellten Computer. ■ Konfigurieren Sie bei Bedarf alle lokalen DNS-Einträge für die IP-Adressen der wiederhergestellten Computer.

So führen Sie einen Failback auf lokale virtuelle Server aus	Führen Sie die folgenden Schritte aus: ■ Erstellen Sie einen umgeleiteten Wiederherstellungsauftrag aus den neuesten Point-In-Time-Backups der Ersatzserver und führen Sie ihn aus. Für die lokalen und die Cloud-Server sollte derselbe Hypervisor-Typ verwendet werden. ■ Konfigurieren Sie bei Bedarf eine feste IP-Adresse für die wiederhergestellten virtuellen Computer. ■ Konfigurieren Sie bei Bedarf alle lokalen DNS-Einträge für die IP-Adressen der virtuellen Computer.

5 Wenn die ausgefallenen Server über eine externe IP-Adresse (z. B. einen Exchange-E-Mail-Server) verfügbar gemacht wurden, stellen Sie die ursprünglichen Adressen in den externen DNS-Datensätzen wieder her.

6 Löschen Sie die Backup-Definitionen der Ersatz-Cloud-Server.

7 Führen Sie die ursprünglichen Backup-Definitionen für alle wiederhergestellten lokalen Computer wieder aus.

Anforderungen für Backup Exec-Deduplizierungsspeichergeräte

Die Anforderungen für Backup Exec-Deduplizierungsspeichergeräte gelten für alle Konfigurationen der privaten Cloud. Wenn Sie das Freigabenlimit auf einem bestimmten Cloud-Backup Exec-Server erreichen, müssen Sie zusätzliche Cloud-Backup Exec-Server hinzufügen.

Weitere Informationen zu Anforderungen für Deduplizierungsspeichergeräte finden Sie im *Symantec Backup Exec-Administratorhandbuch*.

Einschränkungen der WAN-Latenz

Eine hohe Netzwerklatenz in Ihrem Netzwerk kann sich negativ auf die Leistung des ersten direkten Cloud-Backup-Auftrags auswirken. Latenz kann sich außerdem auch auf einige Duplizierungs-Backup-Aufträge auswirken, die Daten zwischen der regionalen Niederlassung und dem privaten Cloud-Backup Exec-Server übertragen. Es können auch dann Probleme mit der Leistung auftreten, wenn Sie für das Deduplizierungsspeichergerät ein Übertragungslaufwerk bereitstellen,

obwohl Sie die Leistung üblicherweise durch das Bereitstellen von Geräten steigern. Während des ersten Backup-Auftrags identifiziert Backup Exec Informationen zu Datensegmenten und legt sie im Cache-Speicher ab, was die Leistung bei folgenden Aufträgen steigert.

Hinweis: Als hoher Latenzwert wird eine durchschnittliche Übertragungslatenz von über 30 Millisekunden angesehen. Je größer die Latenz, umso mehr wirkt sie sich auf die Leistung von Backup Exec aus.

Diese Einschränkung trifft nicht auf Duplizierungs-Backup-Aufträge zu, wenn sowohl das Quellgerät als auch das Zielgerät Deduplizierungsspeichergeräte sind.

Im Folgenden sind Einschränkungen bei der Verwendung von Backup Exec-Diensten in einer privaten Cloud bei hohen Latenzwerten aufgeführt:

- Bei Duplizierungs-Backup-Aufträgen, die ein anderes Quellgerät als ein Deduplizierungsspeichergerät und ein Deduplizierungsspeichergerät in der privaten Cloud als Ziel verwenden, können Leistungsprobleme auftreten. Sie vermeiden diese Leistungsprobleme, indem Sie ein Deduplizierungsspeichergerät als lokales Quellspeichergerät verwenden.
- Möglicherweise ist die Konfiguration für direkte Backups in die Cloud nicht zum Sichern großer Datenmengen geeignet.
- Wenn Sie Backup-Definitionen für dieselben Ressourcen löschen und neu erstellen, muss Backup Exec die Datenfingerabdrücke von Neuem zwischenspeichern. Daher können dieselben Leistungsprobleme wie beim ersten direkten Cloud-Backup-Auftrag auftreten.

Beschränkungen der Granular Recovery Technology mit Offsite-Kopie

Im Folgenden sehen Sie Beschränkungen bei der Anwendung der Backup Exec Granular Recovery Option (GRT) mit der Offsite-Kopienkonfiguration:

- Beim Sichern von lokalen, inkrementellen Exchange-Backup-Sätzen mit GRT auf ein Deduplizierungsspeichergerät in der privaten Cloud werden Backup-Daten im MTF-Format erstellt. Sie können granulare Daten aus diesen Backup-Sätzen wiederherstellen. Dies erfordert jedoch das Staffeln des Backup-Satzes auf dem Cloud-Backup Exec-Server während des Wiederherstellungsauftrags. Diese Beschränkung gilt nicht bei direktem Sichern von GRT-aktivierten Backup-Sätzen auf das Cloud-Deduplizierungspeichergerät.

- Das direkte Kopieren duplizierter Sätzen mit aktivierter GRT-Option von lokalen Bandgeräten auf ein Cloud-Deduplizierungspeichergerät wird nicht empfohlen und kann zu übermäßig langen Auftragslaufzeiten führen.
- Das direkte Sichern von GRT-aktivierten Sätzen auf den Cloud-Backup Exec-Server verursacht möglicherweise verringerte Leistungszeiten bei hohen Latenzwerten. Die Leistung ist möglicherweise selbst nach dem ersten Backup beeinträchtigt. Besteht weiterhin ein Leistungsproblem, sollten Sie die GRT-Option für direkte Backups deaktivieren.

Einschränkungen für Windows Small Business Server (SBS) und die Konfiguration von mandantenfähigen Backup Exec-Servern

In der Konfiguration eines mandantenfähigen Backup Exec-Servers müssen alle lokal verwalteten Backup Exec-Server Mitglied der privaten Clouddomäne sein. Daher können Sie den SBS-Server eines Kunden nicht als verwalteten Backup Exec-Server konfigurieren, wenn er Teil der Domäne des Kunden ist. Der verwaltete Backup Exec-Server muss als separater Server installiert werden.

Kapitel 4

Konfigurieren von OpenVPN

In diesem Kapitel werden folgende Themen behandelt:

- Info zum Konfigurieren von OpenVPN
- Fehlerbehebung bei Netzwerkproblemen

Info zum Konfigurieren von OpenVPN

Das OpenVPN-SSL-VPN-Paket bietet eine sichere, verschlüsselte Verbindung zwischen der Backup Exec-Instanz in der privaten Cloud und dem lokalen Backup Exec-Server. Sie müssen das SSL-VPN zwischen der Backup Exec-Serverinstanz in der privaten Cloud und allen Computern konfigurieren, die auf dem lokalen Netzwerk laufen.

Die Backup Exec-Dienstkonfiguration der privaten Cloud hat die folgenden Netzwerkeinschränkungen für dieses einzelne Client OpenVPN-Beispiel:

- Das lokale Netzwerk muss innerhalb eines einzelnen Subnetzes enthalten sein.
- Der lokale Domänencontroller und die DNS müssen auf dem gleichen Server enthalten sein.

Siehe "Konfigurieren von OpenVPN" auf Seite 64.

Die grundlegenden OpenVPN-Konfigurationsanweisungen für Backup Exec-Dienste in der privaten Cloud verwenden einen einzelnen Client. Die Anweisungen können verwendet werden, um eine oder mehrere lokalen Clientcomputer zu unterstützen, wenn Ihre Clients alle auf dem gleichen Subnetz enthalten sind. Alle Daten, die für die private Cloud-Instanz gedacht sind, werden durch einen einzelnen OpenVPN-Client geroutet. Für ein komplizierteres Netzwerk oder Zertifikatbasierte Authentifizierung können Sie die optionale OpenVPN-Mehrfachverbindungsstellenclient-Konfiguration verwenden.

Siehe "Über das Konfigurieren von OpenVPN für mehrere Clients" auf Seite 70.

Konfigurieren von OpenVPN

Das Open Source-Paket OpenVPN (SSL-VPN) bietet eine sichere, verschlüsselte Verbindung zwischen der Backup Exec-Instanz in der privaten Cloud und dem lokalen Backup Exec-Server. Sie müssen das SSL-VPN zwischen der Backup Exec-Serverinstanz in der privaten Cloud und allen Computern im lokalen Netzwerk konfigurieren.

Siehe "Info zum Konfigurieren von OpenVPN" auf Seite 63.

Tabelle 4-1 Wie man OpenVPN konfiguriert

Schritt	Beschreibung
Schritt 1	Konfigurieren von OpenVPN auf der privaten Cloud Backup Exec-Instanz Siehe "Konfigurieren Sie OpenVPN auf der privaten Cloud Backup Exec-Instanz." auf Seite 64.
Schritt 2	Konfigurieren von OpenVPN auf Computer 2 Siehe "Konfigurieren von OpenVPN auf Computer 2" auf Seite 66.
Schritt 3	Konfigurieren der lokalen Netzwerk-Route Siehe "Konfigurieren der lokalen Netzwerk-Route" auf Seite 67.
Schritt 4	Konfigurieren Sie ggf. Ihre Firewall. Siehe "Über das Konfigurieren von Firewalls" auf Seite 68.
Schritt 5	Überprüfen Sie die OpenVPN-Verbindung. Siehe "Überprüfen der OpenVPN-Verbindung" auf Seite 69.

Konfigurieren Sie OpenVPN auf der privaten Cloud Backup Exec-Instanz.

Um eine sichere und verschlüsselte Verbindung sicherzustellen, müssen Sie OpenVPN auf der privaten Cloud Backup Exec-Instanz konfigurieren.

Siehe "Info zum Konfigurieren von OpenVPN" auf Seite 63.

Konfigurieren von OpenVPN auf der privaten Cloud Backup Exec-Instanz.

1. Laden Sie OpenVPN 2.1.4 vom folgenden Link herunter und installieren Sie es auf C1 am Standardort:

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

2. Auf C1 öffnen Sie ein Windows-Explorer-Fenster im OpenVPN-Konfigurationsordner, indem Sie auswählen:

   Start > Programme > OpenVPN > Verknüpfungen> OpenVPN Configuration File Directory

3. Generieren Sie den OpenVPN Static-Schlüssel durch Ausführen des folgenden Befehls von einer Eingabeaufforderung in \Programme (x86)\OpenVPN\bin-Ordner:

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

4. Erstellen Sie die Serverkonfigurationsdatei im Ordner, den Sie auf C1 geöffnet haben und speichern Sie die Datei als "server.ovpn":

   Die "server.ovpn-" Datei sieht wie folgendes Beispiel aus:

   ```
   dev tun

   ifconfig 10.8.0.2 10.8.0.1

   secret static.key

   Keepalive 10 120
   ```

Hinweis: Wenn Subnetz 10.8.x.x auf Ihrem lokalen Netzwerk in Gebrauch ist, verwenden Sie einen anderen Subnetzbereich im ifconfig -Befehl.

Hinweis: OpenVPN verwendet UDP-Port 1194 standardmäßig. Bei Bedarf können Sie eine andere Port-Nummer angeben, indem Sie den Befehl "Port" zu OpenVPN-Server und zu den Client-Konfigurations-Dateien hinzufügen.

---

5 Unter Verwendung des Windows-Dienst-Dienstprogramms ändern Sie die OpenVPN-Dienst-Starttypeigenschaft zu Automatisch.

6 Öffnen Sie eine Eingabeaufforderung auf C1 und geben Sie Folgendes ein, um die Subnetzadresse des Einheimischen DNS (Computer 3) und die DNS-Subnetzmaske zu ersetzen:

Hinweis: Die spitzen Klammern sind wegzulassen.

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

Konfigurieren von OpenVPN auf Computer 2

Um eine sichere und verschlüsselte Verbindung sicherzustellen, müssen Sie OpenVPN auf Computer 2 (C2) konfigurieren, nachdem Sie OpenVPN auf Computer 1 (C1) konfiguriert haben.

Siehe "Info zum Konfigurieren von OpenVPN" auf Seite 63.

So konfigurieren Sie OpenVPN auf Computer 2

1 Laden Sie OpenVPN 2.1.4 vom folgenden Link herunter und installieren Sie es auf C2 am Standardort:

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

2 Kopieren Sie den statischen Schlüssel, der in Schritt 2 des folgenden Verfahrens generiert wird:

Konfigurieren Sie OpenVPN auf der privaten Cloud Backup Exec-Instanz.

3 Fügen Sie den Schlüssel am folgenden Ort auf C2 ein:

\Program Files (x86)\OpenVPN\config

4 Erstellen Sie die Client-Konfigurations-Datei am folgenden Speicherort auf C2 und speichern Sie die Datei als "client.ovpn":

\Program Files (x86)\OpenVPN\config

Die "client.ovpn-" Datei sieht wie folgendes Beispiel aus:

```
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 Geben Sie die statische IP-Adresse Ihres privaten Cloud Backup Exec-Computers in der Remote Anweisung ein.

Hinweis: Die spitzen Klammern sind wegzulassen.

6 Wenn Subnetz 10.8.x.x auf dem lokalen Netzwerk in Gebrauch ist, bearbeiten Sie die Datei, um einen anderen Subnetzbereich in der ifconfig -Anweisung zu verwenden.

7 Unter Verwendung des Windows-Dienst-Dienstprogramms ändern Sie die OpenVPN-Dienst-Starttypeigenschaft zu Automatisch.

Konfigurieren der lokalen Netzwerk-Route

Für die Konfiguration des lokalen Netzwerk-Routing müssen Sie IP-Weiterleitung sowohl auf dem TAP-Win32 Adapter V9 als auch der physischen Netzwerkschnittstelle aktivieren.

Siehe "Info zum Konfigurieren von OpenVPN" auf Seite 63.

So konfigurieren Sie das Routing des lokalen Netzwerks

1 Auf Computer 2 (C2) starten Sie den Registrierungseditor und suchen Sie den folgenden Schlüssel:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

2 Legen Sie die folgenden Registrierungswerte fest:

Wertname: IPEnableRouter

Werttyp: REG_DWORD

Wertdaten: 1

Hinweis: Ein Wert von 1 aktiviert TCP/IP-Weiterleitung für alle Netzwerkverbindungen, die auf dem Computer installiert und verwendet werden.

3 Neustart C2.

4 Geben Sie den folgenden Befehl in einem Befehlsfenster auf dem Computer 3 (C3) ein, um und die lokale IP-Adresse von C2 zu ersetzen:

Hinweis: Geben Sie die IP-Adresse ohne die spitzen Klammern ein.

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

Hinweis: Sie müssen diesen Befehl auf Computer auf allen lokalen Netzwerk-Computern ausführen, die mit dem OpenVPN-Servercomputer in der Cloud kommunizieren müssen. Sie müssen den Befehl auf allen Servern ausführen, auf denen ein Backup Exec Agent ausgeführt wird und die für Wiederherstellungsaufträge vom Backup Exec-Server in der privaten Cloud vorgesehen sind.

Über das Konfigurieren von Firewalls

Sie sollten Ihre Netzfirewälle gemäß der Tabelle konfigurieren, um eine ordnungsgemäße Kommunikation zwischen Ihrem lokalen Server und dem Cloud-Server sicherzustellen.

Tabelle 4-2 Über das Konfigurieren von Firewalls

Firewallinstanz	Aktion
Computer 1 (C1)	Sie sollten die Windows-Firewall für den OpenVPN-Netzwerkadapter deaktivieren. Sie sollten die Windows-Firewall so konfigurieren, dass der Datenverkehr über jeden Port hereinkommen kann, der für OpenVPN vorgesehen ist. Standardmäßig verwendet OpenVPN Port UDP 1194.
Computer 2 (C2)	Sie sollten die Windows-Firewall für den OpenVPN-TAP-Netzwerkadapter deaktivieren.

Firewallinstanz	Aktion
Lokales Netzwerk	Wenn Sie eine externe lokale- oder Corporatefirewall haben, sollten Sie die Firewall so konfigurieren, dass Datenverkehr über jeden Port herausgehen kann, der für OpenVPN vorgesehen ist. Standardmäßig verwendet OpenVPN Port UDP 1194.

Siehe "Info zum Konfigurieren von OpenVPN" auf Seite 63.

Überprüfen der OpenVPN-Verbindung

Wenn Sie OpenVPN-Konfiguration abgeschlossen haben, sollten Sie sie prüfen, um sicherzustellen, dass der OpenVPN-Server und der Client erfolgreich eine Verbindung herstellen können.

Siehe "Info zum Konfigurieren von OpenVPN" auf Seite 63.

So überprüfen Sie die OpenVPN-Verbindung

1. Unter Verwendung des Windows-Dienst-Dienstprogramms starten Sie die OpenVPN-Dienste auf Computer 1 (C1) und Computer 2 (C2).
2. Öffnen Sie die OpenVPN-Protokolldateien, die sich auf C1 und C2 im folgenden Verzeichnis befinden:

   C:\Program Files (x86)\OpenVPN\log
3. Überprüfen Sie, dass der Text "Initialization Sequence Completed" in beiden Dateien vorhanden ist.
4. Auf C1 konfigurieren Sie Ihren TAP-Win32 Netzwerkadapter TAP-Win32 so, dass er auf den DNS-Server Ihrer lokalen Domäne als seinem bevorzugten DNS-Server zeigt.

   Siehe "Ihren TAP-Win32-Netzwerkadapter konfigurieren" auf Seite 70.

   Sie können die private Cloud Backup Exec-Instanz- und VPNlink-Verbindung manuell starten und beenden, wenn Sie Aufträge ausführen. Oder, Sie können den verbundenen VPN-Link beibehalten und die Instanz permanent ausführen. Sie können den Prozess automatisieren, indem Sie den OpenVPN-Dienst planen, damit er mit Ihren geplanten Backup-Aufträgen startet und beendet wird. Sie können das "Windows Scheduled Tasks"-Dienstprogramm verwenden, um einen Zeitplan für den Dienst zu erstellen.

Ihren TAP-Win32-Netzwerkadapter konfigurieren

Um die OpenVPN-Verbindung zu überprüfen, müssen Sie Ihren Netzwerkadapter TAP-Win32 konfigurieren , damit der auf den DNS-Server Ihrer lokalen Domäne als den bevorzugten DNS-Server zeigt.

Siehe "Überprüfen der OpenVPN-Verbindung" auf Seite 69.

Ihren TAP-Win32-Netzwerkadapter konfigurieren

1. Öffnen Sie TAP Netzwerkadaptereigenschaften.
2. Klicken Sie auf Eigenschaften IPv4.
3. Klicken Sie auf Erweitert.
4. Auf der Registerkarte DNS geben Sie die IP-Adresse des DNS-Servers des lokalen Netzwerks ein.
5. Im Feld Suffixe fügen Sie die Domäne FQDN-Suffixe hinzu und verschieben Sie sie an den Anfang der Suffixliste.
6. Klicken Sie auf OK, um alle Dialogfelder zu schließen.
7. In einer Eingabeaufforderung auf Computer 1 (C1) geben Sie die folgenden Befehle ein:

   ```
   ipconfig /flushdns
   ```

   ```
   ipconfig /registerdns
   ```

   Wenn Sie mit der Überprüfung der OpenVPN-Verbindung fertig sind, können Sie die Backup Exec-Server konfigurieren.

   Siehe "Einrichten der mandantenfähigen oder Offsite-Kopie für Cloud-Konfigurationen" auf Seite 24.

   Siehe "Einrichten der direkten Backup-Konfiguration" auf Seite 36.

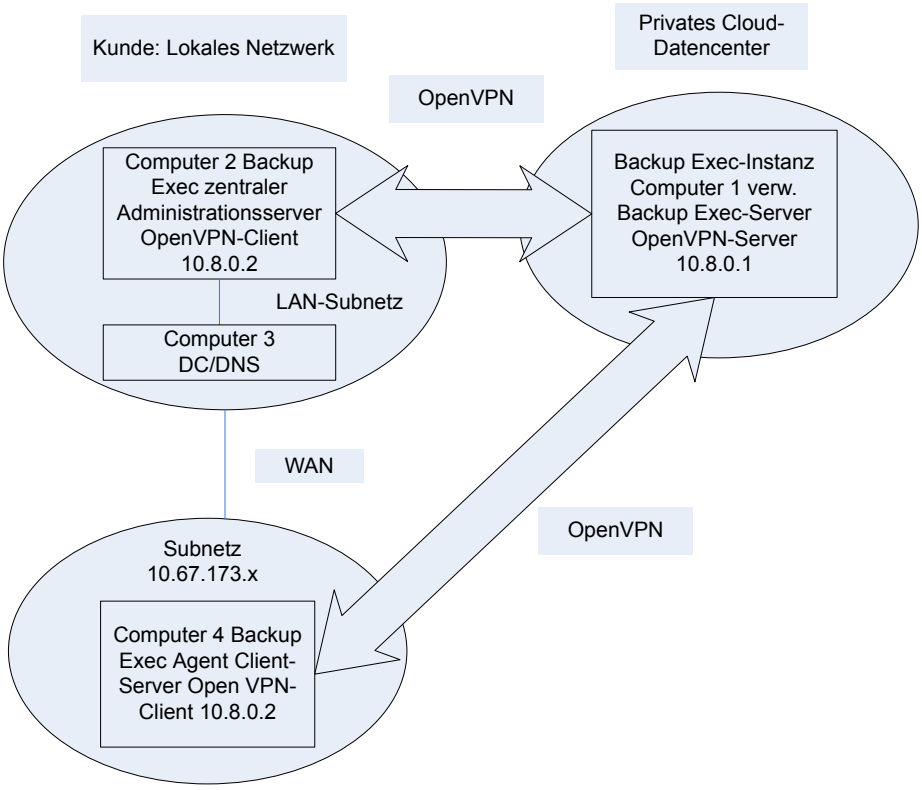
Über das Konfigurieren von OpenVPN für mehrere Clients

Sie können OpenVPN für die Verwendung mit mehreren Clients konfigurieren. Es ist möglicherweise notwendig, eine Mehrfachverbindungsstellenclient-VPN-Konfiguration zu verwenden, wenn Sie ein komplexes lokales Netzwerk haben. Wenn Sie beispielsweise mehrere lokale Subnetzwerke verwenden, profitieren Sie möglicherweise von einer Mehrfachverbindungsstellenclient-VPN-Konfiguration.

Siehe "Info zum Konfigurieren von OpenVPN" auf Seite 63.

Warnung: OpenVPN sollte nicht auf einem Domänencontroller installiert werden. Mehrnetzige Domänencontrollerkonfigurationen werden nicht für Backup Exec-Dienste in einer privaten Cloud unterstützt.

Abbildung 4-1 Mehrfach-Client-VPN-Konfiguration



Der OpenVPN-Server ist die private Cloud-Instanz. Die Clients sind die Computer auf dem LAN. Bei Verwendung mehrerer OpenVPN-Clients erfordert die Verwendung von Sicherheitszertifikaten statt der gemeinsam genutzten Schlüssel-Textdatei, die Sie für die einzelnen Client-Konfigurationen verwenden. In der MultiClient Konfiguration hat jeder OpenVPN-Client seinen eigenen Schlüssel und Zertifikat.

Hinweis: Schlüsseldateien sind wichtig. Wenn eine Schlüsseldatei defekt ist, sollten Sie sie regenerieren. Wenn die Zertifizierungsstelle (CA) Schlüsseldatei defekt ist, sollten Sie alle Schlüssel regenerieren, die auf dieser Zertifizierungsstelle basieren.

Um OpenVPN für mehrere Clients zu konfigurieren, schließen Sie das Verfahren unter Verwendung der öffentlich verfügbaren Beispiele ab. Die folgenden Sites liefern vollständige Anweisungen für das Konfigurieren von OpenVPN-Zertifikaten und von mehreren OpenVPN-Clients:

http://www.runpcrun.com

http://openvpn.net

Eine Alternative für komplexere Netzwerke ist die Verwendung von OpenVPN auf einem Gatewayrouter des lokalen Netzwerks. Ein Gatewayrouter des lokalen Netzwerks stellt eine Punkt-zu-Punkt--OpenVPN-Verbindung zur Verfügung. Andere lokale Computer können zum VPN führen, ohne zusätzliche OpenVPN-Client- und Computernetzpfade hinzuzufügen. Konsultieren Sie Ihren Routerhersteller und die Dokumentation für weitere Einzelheiten über ihren Support für OpenVPN.

Drittanbietersoftwareorganisationen liefern auch Routerfirmwareupdates, die OpenVPN-Support enthalten. Die folgende Site liefert ein Beispiel:

http://www.dd-wrt.com

Sobald Sie OpenVPN für mehrere Clients konfiguriert haben, können Sie direkte Backup-Aufträge erstellen und ausführen, um die Daten der Clients zu sichern. Sie können die private Cloud-Instanz als das Backup-Ziel für direkte Backup-Aufträge oder doppelte Backup-Vorgänge verwenden.

Fehlerbehebung bei Netzwerkproblemen

Bei Netzwerkproblemen mit Backup Exec-Diensten in einer privaten Cloud sollten Sie überprüfen, ob der OpenVPN-Server und -Client eine Verbindung herstellen können.

So beheben Sie Netzwerkprobleme

1. Schalten Sie vorübergehend die Windows-Firewalls aus oder fügen Sie die entsprechenden ICMP-Firewallausnahmen für alle Computer in Ihrer Konfiguration für Backup Exec-Dienste in der privaten Cloud hinzu.
2. Auf Computer 1 (C1) und Computer 2 (C2) starten Sie die OpenVPN-Dienstleistungen, indem Sie die Windows-Dienste verwenden.
3. Auf C1 und C2 öffnen Sie die OpenVPN-Protokolldateien im folgenden Verzeichnis und überprüfen, dass jede Datei den Text "Initialization Sequence Completed" enthält:

   C:\Program Files (X86)\OpenVPN\log

4 Senden Sie einen Ping-Befehl an 10.8.0.1 und 10.8.0.2 von C1, C2 und Computer 3 (C3), um auf Konnektivität zu prüfen.

5 Von C1 senden Sie an die lokale IP-Adresse von C2 und die lokale IP-Adresse von C3 einen ping-Befehl.

   Stellen Sie sicher, dass die Eigenschaften des Adapters OpenVPN-lokalen Netzwerks DNS das lokale Domänesuffix enthalten, wenn OpenVPN verbunden ist.