Backup Exec プライベートクラウドサービス

計画と配備ガイド

Symantec

目次

1

Backup Exec プライベートクラウドサービスの概要

この章では以下の項目について説明しています。

Backup Exec プライベートクラウドサービスについて

Backup Exec プライベートクラウドサービスは、管理対象バックアップサービスをお客様に提供しようとしている管理対象サービスプロバイダ (MSP) 向けのものです。Backup Exec プライベートクラウドサービスは、「プライベートクラウド」設定としてパートナーのデータセンター内のバックアップストレージをパートナーがホストすることを可能にします。

管理対象サービスプロバイダは、テープのオフサイトコピーを管理する代替方法として、パートナープライベートクラウドへのインターネット経由バックアップサービスを提供できます。WAN 上の移送を安全および効率的にして、バックアップは暗号化され重複排除されます。ローカルバックアップは速いリストア機能のために社内において利用可能なままです。さらに、Backup Exec プライベートクラウドサービスはユーザーがクラウドにバックアップを直接実行することを可能にします。ユーザーはクラウドから完全または個別データを直接リストアできます。

また、Backup Exec プライベートクラウドサービスは、広く分散したネットワークを持つ Backup Exec のお客様向けでもあります。お客様はリモートオフィスから、中央データセンターのプライベートクラウドの場所内のディスクストレージやテープストレージに、バックアップの複製コピーを送ることができます。

次の表は Backup Exec プライベートクラウドサービスを理解するために重要な Backup Exec のいくつかの用語をさらに説明したものです。

表 1-1 Backup Exec の用語

用語	定義
重複排除用ディスクストレージ	重複排除用ディスクストレージデバイスはBackup Execサーバーでの統合された重複排除を提供します。 **メモ:** クラウドの統合型 Backup Exec 重複排除用ストレージデバイスの代りに、Symantec NetBackup 5000/5020 シリーズの重複排除ストレージアプライアンスを使うことができます。特に大きなマルチテナント設定に対して、アプライアンスはより拡張可能なオプションを提供できます。
最適化された複製	重複排除されたデータを、同じ製造元の 1 つの OpenStorage デバイスから別の OpenStorage デバイスに直接コピーできる複製のタイプ。
Granular Recovery Technology (GRT)	データベースのバックアップから個別の項目をリストアできるバックアップオプション。1 つの項目をリカバリする場合、個別の項目の個別のバックアップは不要です。

p.6 の「Backup Exec プライベートクラウドサービスのセキュリティに関する考慮事項」を参照してください。

p.8 の「Backup Exec のプライベートクラウドサービスのシステム必要条件」を参照してください。

p.11 の「Backup Exec プライベートクラウドサービスの設定」を参照してください。

p.13 の「Backup Exec プライベートクラウドサービスの設定について」を参照してください。

Backup Exec プライベートクラウドサービスのセキュリティに関する考慮事項

Backup Exec プライベートクラウドサービスは Backup Exec の現在のジョブとリソースクレデンシャルのモデルを使用して、安全なエクスペリエンスを提供します。また、シマンテック社は VPN ソリューションを使って、お客様の場所とデータセンター間の安全なネットワーク接続を使うことを推奨します。各種の IPsec、SSL Layer、その他の VPN ソリューションが利用可能です。

複数のお客様をサポートする設定を使用するとき、お客様のネットワークを互いから隔離しておくのに VLAN またはルーティングの制限を使ってください。

お好みの VPN ソリューションを使用できます。このガイドでは OpenVPN の参照設定の手順について説明します。OpenVPN SSL VPN のオープンソースパッケージは、プライベートクラウドの Backup Exec インスタンスとローカルの Backup Exec サーバー間で安全に暗号化された接続を提供します。このコンポーネントでは、通常はデフォルトポート 1194 がファイアウォールで開いている必要があります。ただし、OpenVPN は他のどのポートでも代わりに使用して設定できます。OpenVPN はキーベースと証明書ベースの両方の認証方法を提供します。このドキュメントは両方の方法を設定するためのリファレンスを提供します。

p.5 の「Backup Exec プライベートクラウドサービスについて」を参照してください。

p.53 の「OpenVPN の設定について」を参照してください。

マルチテナント型の Backup Exec サーバー設定には、考慮する必要がある追加のセキュリティの必要条件があります。

p.7 の「マルチテナント Backup Exec サーバー設定のセキュリティの必要条件」を参照してください。

マルチテナント Backup Exec サーバー設定のセキュリティの必要条件

単一の Backup Exec サーバーが複数のお客様またはテナントを安全にサポートできるように、Backup Exec をプライベートクラウドに設定できます。マルチテナント Backup Exec サーバーには複数のお客様の共有コンテンツが含まれるため、これを使用する場合は、さらにいくつかのセキュリティ上の予防策を講じる必要があります。

p.15 の「複数テナントクラウドの Backup Exec サーバーの設定について」を参照してください。

p.6 の「Backup Exec プライベートクラウドサービスのセキュリティに関する考慮事項」を参照してください。

マルチテナント Backup Exec サーバーを設定するときは、次のセキュリティ必要条件を考慮する必要があります。

- オンプレミスの管理対象 Backup Exec サーバーは、物理コンピュータにインストールする必要があります。
- オンプレミスの管理対象 Backup Exec サーバーで、Microsoft Windows BitLocker 機能が有効になっており、システムボリュームでアクティブ化されている必要があります。

  BitLocker のパスワードは、どのお客様にも開示してはなりません。BitLocker の代替として、何らかのハードウェアディスク暗号化ソリューションを使用することもできます。
- プライベートクラウドに配置されているマルチテナント Backup Exec サーバーとオンプレミスの Backup Exec サーバーは、サービスプロバイダのドメインのメンバーである必要があります。

Backup Exec サーバーで、お客様にログオンアクセス権限を許可してはなりません。分離性を高めるために、お客様の管理対象 Backup Exec サーバーをそれぞれ別のサービスプロバイダの子ドメインに配置することを検討することもできます。

- オンプレミスの管理対象 Backup Exec サーバー用のサービスプロバイダのドメインクレデンシャルは、ドメイン管理者ではなく、ローカル管理者のクレデンシャルである必要があります。
- マルチテナントクラウドサーバーの重複排除用ディスクストレージデバイスでは、クライアント側の重複排除を有効にしてはなりません。
- オンプレミスの管理対象 Backup Exec サーバーは、[リストアするカタログとバックアップセットに無制限のアクセス権を持ちます]オプションを設定してインストールしないでください。[集中管理される **Backup Exec** サーバー]オプションを設定したインストールのみを行ってください。
- 必要であれば、オンプレミスの管理対象 Backup Exec サーバーに 2 要素認証を使用して、セキュリティをさらに高めることができます。
  VeriSign VIP 認証サービスを使用することをお勧めします。
  http://www.verisign.com/authentication/two-factor-authentication/vip-authentication/index.html

警告: これらのセキュリティ上の推奨事項に従うことで、共有の Backup Exec ネットワークとストレージデバイスに、ある程度のアクセス保護は得られます。何者かが管理対象 Backup Exec サーバーに物理的にアクセスし、悪意のある操作を実行しようとした場合、理論上はこれらのセキュリティ対策が回避されてしまう可能性はあります。オンプレミスの管理対象 Backup Exec サーバーに、物理的なアクセス保護対策をさらに講じるように検討することもできます。

Backup Exec のプライベートクラウドサービスのシステム必要条件

次の表は、Backup Exec のプライベートクラウドサービスの実行に必要な、システムの最小必要条件と推奨事項を示しています。

表 1-2 Backup Exec のプライベートクラウドサービスのシステム必要条件

必要条件	説明
Backup Exec サーバー	3 つの異なる方法のいずれかで、Backup Exec のプライベートクラウドサービスを設定できます。 p.13 の「Backup Exec プライベートクラウドサービスの設定について」を参照してください。 クラウドのどの Backup Exec サーバーにも、Backup Exec の Deduplication Option が含まれている必要があります。ローカルサーバーの唯一の必要条件は、それらが Backup Exec 2012 の必要条件に準拠することです。 互換性があるオペレーティングシステム、プラットフォーム、アプリケーションのリストは、次の URL で参照できます。 http://entsupport.symantec.com/umi/V-269-1
Deduplication Option のライセンス	プライベートクラウドのサーバーとすべてのローカルの Backup Exec サーバーに、Symantec Backup Exec Deduplication Option をインストールする必要があります。 ローカルの Backup Exec サーバー上に重複排除用ディスクストレージデバイスを作成する必要はありません。ただし、クラウドのサーバーにある共有重複排除用ディスクストレージデバイスにアクセスするには、ローカルの Backup Exec サーバーに Deduplication Option をインストールする必要があります。すべての設定で、クラウドの Backup Exec サーバー上に重複排除用ディスクストレージデバイスが必要です。
Central Admin Server Option のライセンス	マルチテナントまたはオフサイトのいずれかのコピー設定を使用する場合は、ローカルコンピュータまたはクラウドコンピュータに Symantec Backup Exec Enterprise Server Option を Central Admin Server Option とともにインストールする必要があります。
有効なインターネット接続	プライベートクラウドの重複排除用ディスクストレージデバイスにデータを転送するには、有効なインターネット接続が必要です。

必要条件	説明
Virtual private network (VPN)	シマンテック社はVPNソリューションを使用して、お客様の場所とデータセンター間の安全なネットワーク接続の使用を推奨します。各種のIPsecとSSL LayerのVPNソリューションが利用可能です。 このガイドではOpenVPNの設定の手順について説明します。OpenVPN SSL VPNのオープンソースパッケージは、プライベートクラウドのBackup Execインスタンスとローカルの Backup Execサーバー間で安全に暗号化された接続を提供します。

2

Backup Exec プライベートクラウドサービスの設定

この章では以下の項目について説明しています。

Backup Exec プライベートクラウドサービスの設定

Backup Exec のプライベートクラウドサービスを設定するには、次の手順を実行します。

表 2-1 Backup Exec のプライベートクラウドサービスの設定方法

手順	説明
手順 1	プライベートクラウドの Backup Exec サーバーインスタンスと、ローカルネットワークで動作しているすべてのコンピュータ間の VPN を設定する必要があります。 p.53 の「OpenVPN の設定」を参照してください。 p.60 の「複数のクライアントの OpenVPN の設定について」を参照してください。

手順	説明
手順 2	目的に最も適した Backup Exec プライベートクラウドサービス設定を検討して、選択します。複数のお客様用に単一のマルチテナント設定を選択できます。または、クラウドへの専用オフサイトコピー設定、またはお客様ごとの直接バックアップ設定を使用することもできます。 p.13 の「Backup Exec プライベートクラウドサービスの設定について」を参照してください。 Backup Exec プライベートクラウドサービスを設定する必要があります。 p.20 の「クラウドへのマルチテナントまたはオフサイトコピー設定のセットアップ」を参照してください。 p.30 の「直接バックアップ設定のセットアップ」を参照してください。
手順 3	Backup Exec プライベートクラウドサービスの操作を開始するには、VPN と Backup Exec を設定する必要があります。 p.35 の「オフサイトコピー設定の Backup Exec プライベートクラウドサービスの操作について」を参照してください。 p.42 の「Backup Exec プライベートクラウドサービスと直接バックアップ設定の操作について」を参照してください。

手順	説明
手順 4	ポート制限付きの VPN ゲートウェイを使用する場合、オンプレミスとクラウド VPN ゲートウェイの両方で、ポート例外を開く必要が生じることがあります。ポート例外により、クラウドに配置されている Backup Exec サーバーはオンプレミス Backup Exec サーバーおよびエージェントと通信できるようになります。 また、CAS Backup Exec SQL ポートを動的に割り当てられたポートから静的ポートに変更する必要もあります。 **メモ:** OpenVPN を使用すれば、ゲートウェイファイアウォールのポート例外を設定しなくて済む場合があります。通常、OpenVPN はファイアウォールを通るように設定されます。 次の Backup Exec サポート技術情報には、Backup Exec に必要なすべてのポート番号と、開く必要のあるポート番号が記載されています。 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 次の Backup Exec サポート技術情報には、SQL 静的ポートの設定方法が説明されています。 http://www.symantec.com/business/support/index?page=content&id=HOWTO22985

Backup Exec プライベートクラウドサービスの設定について

4 つの方法のいずれかで、Backup Exec プライベートクラウドサービスを設定できます。

表 2-2 Backup Exec プライベートクラウドサービスの特定の設定

設定の種類	詳細
マルチテナント型のクラウド Backup Exec サーバー	マルチテナント型のクラウド Backup Exec サーバー設定によって、プライベートクラウドにある Backup Exec サーバーまたは集中管理サーバーへのオフサイトコピーおよび直接バックアップが提供されます。単一のプライベートクラウド Backup Exec サーバーを複数のお客様のデータをバックアップするのに使用できます。 p.15 の「複数テナントクラウドの Backup Exec サーバーの設定について」を参照してください。
クラウドの管理対象 Backup Exec サーバーへのオフサイトコピー	クラウドの管理対象 Backup Exec サーバーへのオフサイトコピー設定には、管理対象 Backup Exec サーバー、集中管理サーバー、ドメインコントローラを使用します。この設定によって、プライベートクラウドにある管理対象 Backup Exec サーバーへのオフサイトコピー機能が提供されます。この設定は、お客様ごとに 1 台の管理対象 Backup Exec サーバーを必要とします。 p.17 の「クラウドの管理対象 Backup Exec サーバーへのオフサイトコピー設定について」を参照してください。
クラウドの集中管理サーバーへのオフサイトコピー	クラウドの集中管理サーバーへのオフサイトコピー設定は、集中管理サーバーと管理対象 Backup Exec サーバーの場所が逆であること以外は、1 番目と似ています。この設定によって、プライベートクラウドにある集中管理サーバーへのオフサイトコピー機能が提供されます。この設定は、お客様ごとに 1 台の集中管理サーバーを必要とします。 p.18 の「クラウドの集中管理サーバーへのオフサイトコピー設定について」を参照してください。

設定の種類	詳細
直接バックアップ	直接バックアップ設定は、管理対象 Backup Exec サーバーまたは集中管理サーバーの代りに、Backup Exec Agent for Windows または Backup Exec Agent for Linux を使います。この設定によって、プライベートクラウドにある Backup Exec サーバーを使って直接バックアップ機能が提供されます。この設定は、お客様ごとに 1 台の Backup Exec サーバーを必要とします。 p.19 の「直接バックアップ設定について」を参照してください。

p.53 の「OpenVPN の設定について」を参照してください。

p.20 の「クラウドへのマルチテナントまたはオフサイトコピー設定のセットアップ」を参照してください。

p.30 の「直接バックアップ設定のセットアップ」を参照してください。

複数テナントクラウドの Backup Exec サーバーの設定について

複数テナントクラウドの Backup Exec サーバー設定には複数のコンピュータが含まれます。

表 2-3　複数テナントクラウドの Backup Exec サーバー設定

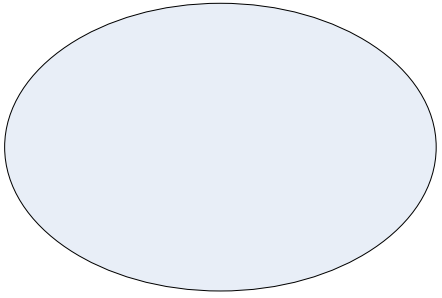
コンピュータ	役割
コンピュータ 1	1 台目のコンピュータ(C1)は、Backup Exec 2012 がインストールされている 64 ビット版の Windows サーバーです。C1 は集中管理サーバーとして設定され、プライベートクラウドに配置されます。
コンピュータ 2	2 台目のコンピュータ(C2)は、Backup Exec 2012 がインストールされている Windows サーバーです。C2 は、ローカルエリアネットワーク上にあり、サービスプロバイダのクラウドドメイン(C4)のメンバーである管理対象 Backup Exec サーバーです。 **メモ:** ローカルの重複排除用ディスクストレージデバイスが必要ない場合は、C2 に 32 ビットのローカル Backup Exec サーバーを使用できます。

コンピュータ	役割
コンピュータ 3	3 台目のコンピュータ（C3）は、ドメインコントローラと DNS です。C3 コンピュータはお客様の場所ごとに設定する必要があります。
コンピュータ 4	4 台目のコンピュータ（C4）は、プライベートクラウド内にあるドメインコントローラと DNS です。
コンピュータ 5（省略可能）	5 台目のコンピュータ（C5）は省略可能ですが、設置が推奨される管理対象 Backup Exec サーバーです。C5 には重複排除用ストレージフォルダが含まれており、耐障害性と信頼性を強化するための C1 コンピュータの重複排除用ストレージデバイスの複製に使用できます。C5 は C1 と同じプライベートクラウドにも、別の物理的な場所にも配置できます。 同じ場所に配置する C5 コンピュータの代わりに、NetBackup 5000/5020 シリーズの重複排除用ストレージアプライアンスを OST デバイスとしてクラウドの Backup Exec サーバー上に設定できます。

この設定によって、プライベートクラウドデータセンター内のすべての Backup Exec ジョブを管理できます。ただし、この場合、集中管理サーバーと管理対象 Backup Exec サーバー間のネットワーク接続が常にアクティブである必要があります。ジョブをローカルで実行する場合でも、ネットワーク接続はアクティブである必要があります。

警告: クラウドの単一の Backup Exec サーバーで複数のお客様をサポートする場合、C1、C2、C4、および C5 を管理者のみがアクセス可能なドメインに含める必要があります。セキュリティリスクの原因となりかねない偶発的または悪質な活動を避けるために、お客様にはどのような C2 へのログオンアクセス権も付与しないでください。

図 2-1 **複数テナントクラウドの Backup Exec サーバー**



p.13 の「Backup Exec プライベートクラウドサービスの設定について」を参照してください。

クラウドの管理対象 Backup Exec サーバーへのオフサイトコピー設定について

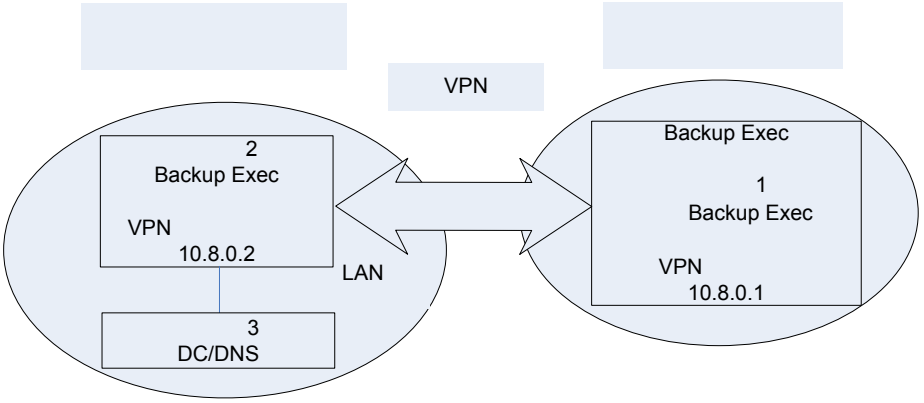
クラウドの管理対象 Backup Exec サーバーへのオフサイトコピー設定には、3 台のコンピュータが必要です。

表 2-4　クラウドの管理対象 Backup Exec サーバーへのオフサイトコピー設定

コンピュータ	役割
コンピュータ 1	1 台目のコンピュータ(C1)は、Backup Exec 2012 がインストールされている 64 ビット版の Windows サーバーです。C1 は管理対象 Backup Exec サーバーとして設定され、プライベートクラウドに配置されます。
コンピュータ 2	2 台目のコンピュータ(C2)は、Backup Exec 2012 がインストールされている 64 ビット版の Windows サーバーです。C2 はローカルエリアネットワークに配置される集中管理サーバーです。 **メモ:** ローカルの重複排除用ディスクストレージデバイスを使用しない場合は、C2 に 32 ビットのローカル Backup Exec サーバーを使用できます。
コンピュータ 3	3 台目のコンピュータ(C3)は、ドメインコントローラと DNS です。

集中管理サーバーと管理対象 Backup Exec サーバー間のネットワーク接続は、常に有効である必要はありません。ネットワーク接続は、プライベートクラウドの管理対象 Backup Exec サーバーを必要とするジョブを実行する場合のみ必要です。ネットワーク接続は、ローカルジョブのために有効である必要はありません。

図 2-2 クラウドの管理対象 Backup Exec サーバーへのオフサイトコピー



p.13 の「Backup Exec プライベートクラウドサービスの設定について」を参照してください。

クラウドの集中管理サーバーへのオフサイトコピー設定について

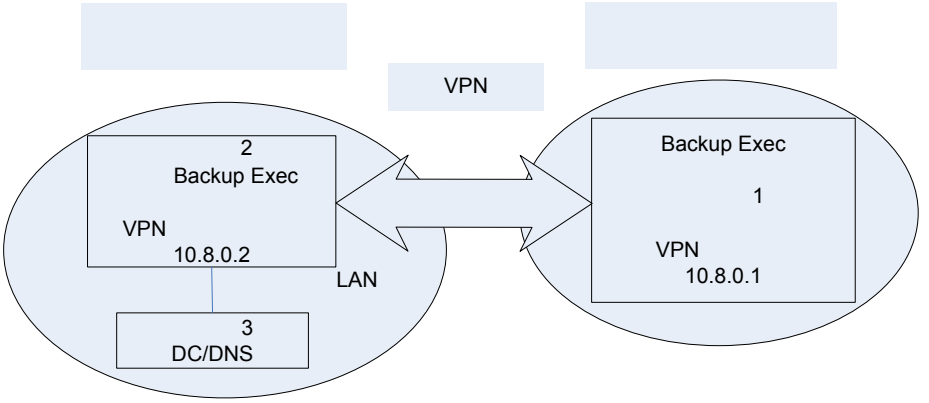
クラウドの集中管理サーバーへのオフサイトコピー設定には、3 台のコンピュータを必要とします。

表 2-5 クラウドの集中管理サーバーへのオフサイトコピー設定

コンピュータ	役割
コンピュータ 1	1 台目のコンピュータ(C1)は、Backup Exec 2012 がインストールされている 64 ビット版の Windows サーバーです。C1 は集中管理サーバーとして設定され、プライベートクラウドに配置されます。
コンピュータ 2	2 台目のコンピュータ(C2)は、Backup Exec 2012 がインストールされている 64 ビット版の Windows サーバーです。C2 は、ローカルエリアネットワークに配置される管理対象 Backup Exec サーバーです。 **メモ:** ローカルの重複排除用ディスクストレージデバイスを使用しない場合は、C2 に 32 ビットのローカル Backup Exec サーバーを使用できます。
コンピュータ 3	3 台目のコンピュータ(C3)は、ドメインコントローラと DNS です。

この設定によって、プライベートクラウドのデータセンター内ですべての Backup Exec ジョブを管理できます。ただし、集中管理サーバーと管理対象 Backup Exec サーバー間のネットワーク接続が、常に有効である必要があります。ジョブをローカルで実行する場合でも、ネットワーク接続は有効である必要があります。

図 2-3　　クラウドの集中管理サーバーへのオフサイトコピー



p.13 の「Backup Exec プライベートクラウドサービスの設定について」を参照してください。

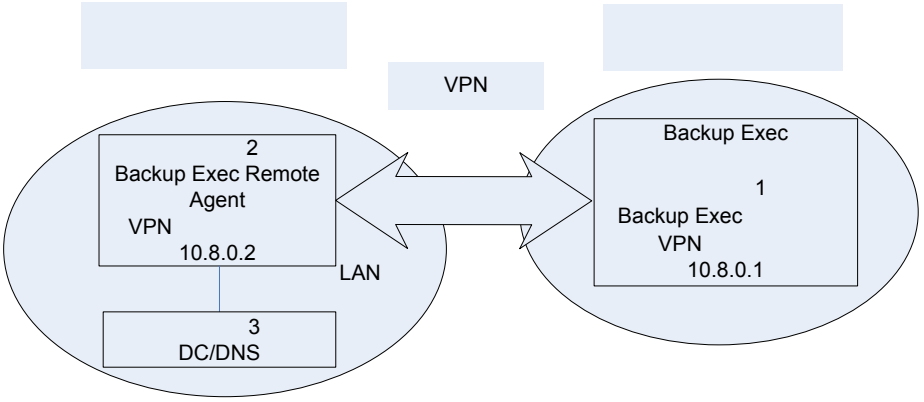
直接バックアップ設定について

直接バックアップ設定には、最低 3 台のコンピュータを必要とします。

表 2-6　　直接バックアップ設定

コンピュータ	役割
コンピュータ 1	1 台目のコンピュータ(C1)は、プライベートクラウドのデータセンターに配置される、64 ビット版の Windows サーバーの Backup Exec 2012 サーバーです。
コンピュータ 2	2 台目のコンピュータ(C2)は、ローカルエリアネットワークに配置される、Agent for Windows または Agent for Linux クライアントです。複数のエージェントクライアントのコンピュータを設定できます。
コンピュータ 3	3 台目のコンピュータ(C3)は、ドメインコントローラと DNS です。

図 2-4 直接バックアップ



p.13 の「Backup Exec プライベートクラウドサービスの設定について」を参照してください。

クラウドへのマルチテナントまたはオフサイトコピー設定のセットアップ

プライベートクラウドサーバーで VPN を設定した後、1 台または複数の Backup Exec サーバーを設定する必要があります。

p.11 の「Backup Exec プライベートクラウドサービスの設定」を参照してください。

マルチテナント設定、または クラウドへの 2 つのオフサイトコピー設定のうちの 1 つを選択できます。

p.15 の「複数テナントクラウドの Backup Exec サーバーの設定について」を参照してください。

p.17 の「クラウドの管理対象 Backup Exec サーバーへのオフサイトコピー設定について」を参照してください。

p.18 の「クラウドの集中管理サーバーへのオフサイトコピー設定について」を参照してください。

表 2-7 クラウドへのオフサイトコピー設定を行う方法

手順	説明
手順 1	Backup Exec の集中管理サーバーのをインストールします。 p.21 の「Backup Exec の集中管理サーバーのインストール」を参照してください。

手順	説明
手順 2	管理対象 Backup Exec サーバーをインストールします。 p.23 の「管理対象 Backup Exec サーバーのインストール」を参照してください。
手順 3	ストレージデバイスを設定します。 p.24 の「マルチテナントおよびオフサイトコピー設定でのストレージデバイスの設定」を参照してください。
手順 4	データを重複排除用ディスクストレージデバイスにシードします。 p.26 の「オフサイトコピー設定の重複排除用ディスクストレージデバイスのシーディングについて」を参照してください。

Backup Exec の集中管理サーバーのインストール

Backup Exec の集中管理サーバーとして動作するコンピュータに Backup Exec for Windows Servers をインストールする必要があります。

p.20 の「クラウドへのマルチテナントまたはオフサイトコピー設定のセットアップ」を参照してください。

マルチテナントクラウドの Backup Exec サーバー設定を使用する場合、クラウドの Backup Exec サーバーは集中管理サーバー（コンピュータ 1、つまり C1）としてインストールする必要があります。

クラウドの管理対象 Backup Exec サーバーへのオフサイトコピー設定を使用する場合は、集中管理サーバーはローカルオフィスの Backup Exec サーバー（コンピュータ 2、つまり C2）としてインストールされます。それ以外の場合、集中管理サーバーはクラウドの集中管理サーバー設定へのオフサイトコピー用のクラウドの Backup Exec サーバー（コンピュータ 1、つまり C1）としてインストールされます。

ドメインに集中管理サーバーを追加する必要があります。集中管理サーバーに Enterprise Server Option を Central Admin Server Option（CASO）とともにインストールします。

表 2-8 Backup Exec の集中管理サーバーをインストールする方法

手順	説明
手順 1	マルチテナント Backup Exec サーバーを設定するには、Backup Exec サーバーをクラウドドメインに追加します。 マルチテナント Backup Exec サーバー設定以外を設定する場合は、次の手順を実行して、Backup Exec サーバーをローカルドメインに追加します。 ■ Windows の[コンピュータのプロパティ]ダイアログボックスを使用して、ドメインにサーバーを追加します。 ■ コンピュータの再起動を要求するメッセージが表示されたら、再起動します。
手順 2	サーバーが再起動したら、ローカルの Backup Exec インスタンスの管理者権限を持つドメインのアカウントでログオンします。
手順 3	適切なライセンスキーを使用して Backup Exec 2012 をインストールします。 Backup Exec のインストールについて詳しくは、『Symantec Backup Exec 管理者ガイド』を参照してください。 Backup Exec パートナーは次のリンクで、シマンテック社の PartnerNet の Web サイトからライセンス情報を入手できます。 https://partnernet.symantec.com/Partnercontent/Login.jsp
手順 4	Backup Exec をインストールするときは、Enterprise Server Option と Central Admin Server Option (CASO)を含めてください。 CASO のインストールについて詳しくは、『Symantec Backup Exec 管理者ガイド』を参照してください。 クラウドの集中管理サーバー設定にマルチテナントまたはオフサイトコピーを使用する場合は、Deduplication Option をインストールします。集中管理サーバーでのローカルの重複排除用ディスクストレージデバイスの使用は、クラウドの管理対象 Backup Exec サーバーへのオフサイトコピー設定のオプションです。
手順 5	Backup Exec をインストールするときには、デフォルトのシステムログオンアカウント用のドメインクレデンシャルを使用してください。

手順	説明
手順 6	クラウドに増分 Exchange GRT 複製バックアップジョブを実行する場合は、インストールの完了時に次のレジストリ値を1に設定します。このレジストリ値を変更すると、Backup Exec サーバーでの重複排除ディスクストレージデバイスの GRT-to-GRT 重複コピー機能が無効になります。 dword HKEY LOCAL MACHINE¥SOFTWARE¥Symantec¥Backup Exec for Windows¥Backup Exec¥Engine¥Misc¥DisablePDI2PDISetCopy これで、コンピュータは WAN 経由で管理対象 Backup Exec サーバーを制御する集中管理サーバーになります。 オフサイトコピー Granular Recovery Technology (GRT) の制限事項について、詳しくは次のトピックを参照してください。 p.50 の「オフサイトコピーでの Granular Recovery Technology の制限事項」を参照してください。

管理対象 Backup Exec サーバーのインストール

管理対象 Backup Exec サーバーをインストールする必要があります。クラウドの管理対象 Backup Exec サーバーへのオフサイトコピー設定を使用する場合は、管理対象 Backup Exec サーバーはクラウドの Backup Exec サーバー(コンピュータ 1、つまり C1)としてインストールされます。それ以外の場合は、管理対象 Backup Exec サーバーはローカルオフィスの Backup Exec サーバー(コンピュータ 2、つまり C2)にインストールされます。

p.20 の「クラウドへのマルチテナントまたはオフサイトコピー設定のセットアップ」を参照してください。

管理対象 Backup Exec サーバーをインストールする方法

1 次のいずれかを実行します。

マルチテナント設定の場合	Backup Exec サーバーをクラウドドメインに追加します。
その他の設定の場合	次の手順を実行して、Backup Exec サーバーをローカルドメインに追加します。 ■ Windows の[コンピュータのプロパティ]ダイアログボックスを使用して、ドメインにサーバーを追加します。 ■ コンピュータの再起動を要求するメッセージが表示されたら、再起動します。

2 サーバーが再起動したら、ローカルの Backup Exec サーバーの管理者権限を持つドメインのアカウントでログオンします。

3 Backup Exec 2012 をサーバーにインストールし、[管理対象 Backup Exec サーバー]インストールオプションを選択します。

4 プロンプトで、集中管理サーバーのインストールに使用したのと同じシステムログオンアカウントのクレデンシャルを指定します。

5 クラウドの管理対象 Backup Exec サーバーへのオフサイトコピー設定を使用する場合は、[Deduplication Option]を選択します。

管理対象 Backup Exec サーバーでのローカル重複排除用ディスクストレージデバイスの使用は、クラウドの集中管理サーバーへのオフサイトコピー設定のオプションです。

6 Backup Exec によって集中管理サーバーの情報の入力を求められる場合は、ローカルの Backup Exec 集中管理サーバーの情報を入力します。

7 [集中管理 Backup Exec サーバー]オプションを選択します。

マルチテナント設定を使用する場合は、[リストアするカタログとバックアップセットに無制限のアクセス権を持ちます]を選択しないでください。

8 クラウドに増分 Exchange GRT 複製バックアップジョブを実行する場合は、インストールの完了時に次のレジストリ値を 1 に設定します。

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

このレジストリ値を変更すると、Backup Exec サーバーでの重複排除ディスクストレージデバイスの GRT-to-GRT 重複コピー機能が無効になります。

9 集中管理サーバーで Backup Exec を開きます。

10 [ストレージ]タブを選択して、プライベートクラウドのデータセンターに配置されている Backup Exec サーバーをダブルクリックします。

11 左側のペインで、[設定]をクリックします。

12 [プライベートクラウドサーバー]フィールドで、[有効]を選択します。

マルチテナントおよびオフサイトコピー設定でのストレージデバイスの設定

プライベートクラウドにバックアップジョブを実行する前に、ストレージデバイスを設定します。

p.20 の「クラウドへのマルチテナントまたはオフサイトコピー設定のセットアップ」を参照してください。

表 2-9 オフサイトコピー設定にストレージデバイスを設定する方法

手順	説明
手順 1	ローカルコンピュータ 2（C2）に新しいローカルディスクのストレージデバイスを作成します。必要に応じて、重複排除用ディスクストレージデバイスを作成できます。 ストレージデバイスの作成について詳しくは、『Symantec Backup Exec 管理者ガイド』を参照してください。
手順 2	プライベートクラウドの Backup Exec インスタンスに、新しい重複排除用ディスクストレージデバイスを作成します。 統合された重複排除ストレージを使用するのではなく、マルチテナント設定用の NetBackup 5000/5020 シリーズ重複排除用ストレージアプライアンスを設定できます。マルチテナント集中管理サーバー上の OST ストレージデバイスとしてアプライアンスを設定します。 重複排除用ディスクストレージデバイスの作成について詳しくは、『Symantec Backup Exec 管理者ガイド』を参照してください。 マルチテナント設定を使用する場合は、次の手順を実行して、プライベートクラウドの重複排除用ディスクストレージデバイスのクライアント側の重複排除を無効にする必要があります。 ■ [ストレージ]タブで、プライベートクラウドの Backup Exec サーバーの重複排除用ディスクストレージデバイスをダブルクリックします。 ■ [プロパティ]を選択します。 ■ [クライアント側重複排除]フィールドで、[使用不可]を選択します。 ■ Backup Exec サーバーのサービスを再起動します。 可能な場合は、重複排除用ディスクストレージデバイス専用のボリュームを使用することを推奨します。ローカルの重複排除用ディスクストレージデバイスから簡単に区別できるように、重複排除用ディスクストレージデバイスを 1 つ作成したら、それに一意の名前をつけてください。
手順 3	プライベートクラウドの重複排除用ディスクストレージデバイスで保存データを暗号化する場合は、新しい重複排除用ディスクストレージデバイスを作成するときに、[はい。この重複排除用ディスクストレージデバイスに転送中、データがそのデバイスに格納されている間に、データを暗号化します]を選択します。既存の重複排除用デバイスの場合、重複排除用デバイスのプロパティで[暗号化]フィールドを変更できます。 **メモ:** VPN はローカル Backup Exec サーバーとクラウドの Backup Exec サーバー間でデータを送信しているときに、データを暗号化します。
手順 4	ローカルの Backup Exec のコンピュータと、新しいクラウドの重複排除用ディスクストレージデバイスを共有します。 重複排除用ディスクストレージデバイスの共有について詳しくは、『Symantec Backup Exec 管理者ガイド』を参照してください。

手順	説明
手順 5	Backup Exec Services Manager を使用して、ローカル Backup Exec サーバーのすべての Backup Exec サービスを停止し、再起動します。 ローカルの Backup Exec サーバーと、クラウドの重複排除用ディスクストレージデバイスを共有する処理はこれで完了しました。プライベートクラウドの重複排除用ディスクストレージデバイスが表示され、C1 と C2 の両方からアクセスできるようになります。
手順 6（省略可能）	マルチテナント設定の場合、追加の管理対象 Backup Exec サーバーをクラウドの重複排除用ストレージデバイスとともにインストールできます。追加の管理対象 Backup Exec サーバーをプライマリクラウドの Backup Exec サーバーと共有して、プライマリサーバーの重複排除用ストレージデバイスを複製できます。 NetBackup 5000/5020 シリーズの重複排除用ストレージアプライアンスを、追加の管理対象 Backup Exec サーバーの代替としてインストールできます。アプライアンスは、複製用に使用できます。アプライアンスを OST ストレージデバイスとしてプライマリクラウドの Backup Exec サーバーに追加します。 **警告:** これらのいずれのオプション設定の場合も、クライアント側の重複排除を無効にする必要があります。

オフサイトコピー設定の重複排除用ディスクストレージデバイスのシーディングについて

インターネット上の長い転送時間を避けるために、開始するデータをクラウドの重複排除用ディスクストレージデバイスにシードできます。重複排除用ディスクストレージデバイスのシーディングは、使用の準備のために重複排除用ディスクストレージデバイスに初期設定ファイルやバックアップセットを配置する処理です。転送時間は、プライベートクラウドの Backup Exec インスタンスにコピーされバックアップされるデータの量によって決まります。

データの種類によって、2 つの方法のいずれかを使って初期データをシードできます。

- ［システム状態］のオペレーティングシステムバックアップを、重複排除用ディスクストレージデバイスにシードできます。プライベートクラウドで動作する他のコンピュータの［システム状態］データのバックアップ複製ジョブを実行することによって、重複排除用ディスクストレージデバイスをシードします。バックアップするローカルコンピュータと同じオペレーティングシステムを実行するコンピュータの［システム状態］データをバックアップします。
  p.27 の「オフサイトコピー設定のオペレーティングシステムファイルのシーディング」を参照してください。
- ローカル Backup Exec サーバーからプライベートクラウドのデータセンターへ、関連したデータとバックアップセットを含む物理転送ドライブを送ることができます。

p.27 の「オフサイトコピー設定の重複排除用ディスクストレージデバイスのシーディングに転送ドライブを使用することについて」を参照してください。

オフサイトコピー設定のオペレーティングシステムファイルのシーディング

インターネット上の長い転送時間を避けるために、開始するデータをクラウドの重複排除用ディスクストレージデバイスにシードできます。重複排除用ディスクストレージデバイスをシードする方法の 1 つは、同じ場所に配置された他のコンピュータからの[システム状態]のバックアップデータを使用することです。

p.26 の「オフサイトコピー設定の重複排除用ディスクストレージデバイスのシーディングについて」を参照してください。

表 2-10　オフサイトコピー設定のオペレーティングシステムファイルをシードする方法

手順	説明
手順 1	プライベートクラウドで同じ場所に配置されている任意のコンピュータに Agent for Windows または Agent for Linux をインストールします。 Backup Exec エージェントのインストールの詳細については『Symantec Backup Exec 管理者ガイド』を参照してください。 コンピュータは、お客様のローカルネットワークでバックアップ対象のサーバーと同じオペレーティングシステムのバージョンを実行する必要があります。
手順 2	プライベートクラウドの Backup Exec サーバーでバックアップジョブを作成し、実行します。プライベートクラウドの重複排除用ディスクストレージデバイスに、これらの同じ場所に配置されたコンピュータの[システム状態]とシステムボリュームをバックアップします。

オフサイトコピー設定の重複排除用ディスクストレージデバイスのシーディングに転送ドライブを使用することについて

インターネット上の長い転送時間を避けるために、開始するデータをクラウドの重複排除用ディスクストレージデバイスにシードできます。重複排除用ディスクストレージデバイスにシードする方法の 1 つは、物理転送ドライブを使うことです。

p.26 の「オフサイトコピー設定の重複排除用ディスクストレージデバイスのシーディングについて」を参照してください。

シマンテック社は、インターネット上のデータをコピーするために必要な時間と、転送ドライブを使うのに必要な時間を比較できる計算ツールを提供しています。次のリンクで計算ツールを入手できます。

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

転送ドライブを使用してプライベートクラウドの Backup Exec インスタンスをシードするには、次の手順を実行します。

p.28 の「オフサイトコピー設定のための、転送ドライブを使用した重複排除用ディスクストレージデバイスのシーディング」を参照してください。

オフサイトコピー設定のための、転送ドライブを使用した重複排除用ディスクストレージデバイスのシーディング

プライベートクラウドの Backup Exec の重複排除用ディスクストレージデバイスをシードするために、物理転送ドライブを使用できます。起動するファイルを重複排除用ディスクストレージデバイスにシードすれば、インターネットでの大容量のバックアップの実行時間を節約できます。

p.27 の「オフサイトコピー設定の重複排除用ディスクストレージデバイスのシーディングに転送ドライブを使用することについて」を参照してください。

オフサイトコピー設定のための、転送ドライブを使用した重複排除用ディスクストレージデバイスをシードする方法

1 コンピュータ 2 (C2) のローカル Backup Exec サーバー上で、ポータブルドライブのディスクストレージを作成します。

2 次の方法のいずれかを使って、ディスクストレージにバックアップセットをコピーし、ソフトウェア暗号化を使用してデータを暗号化します。

インストール時に「DisablePDI2PDISetCopy」レジストリキーを作成しなかった場合は、バックアップセットを複製できます	次の手順を実行します。 ■ プライベートクラウドの重複排除用ディスクストレージデバイスのシーディングに使用するデータの最新の完全バックアップセットを複製するように選択します。 ■ [ジョブを複製する]ダイアログボックスで宛先ストレージとして作成したディスクストレージを選択します。 ■ [ジョブを複製する]ダイアログボックスでソフトウェア暗号化を設定します。 ソフトウェア暗号化の暗号化キーを作成するか、または選択します。

インストール時に「DisablePDI2PDISetCopy」レジストリキーを作成した場合は、完全バックアップジョブを作成する必要があります。

次の手順を実行します。

- シマンテック社の Granular Recovery Technology (GRT) 対応のアプリケーションでは、ディスクストレージを使用する完全バックアップジョブを作成します。
- バックアップする特定の GRT 対応のアプリケーションでは GRT を無効にしてください。
  GRT へのオフサイトコピーの制限事項について、詳しくは次のトピックを参照してください。
  p.50 の「オフサイトコピーでの Granular Recovery Technology の制限事項」を参照してください。
- [ストレージ]パネルでソフトウェア暗号化を有効にします。
  ソフトウェア暗号化の暗号化キーを作成するか、または選択します。

3 前の手順で作成したジョブを実行します。

4 プライベートクラウドのデータセンターにポータブルディスクを送ります。

5 プライベートクラウドの Backup Exec サーバーにポータブルディスクを接続します。

6 ドライブで最初に作成したディスクストレージを使って、接続されたポータブルドライブでディスクストレージを作成します。

7 ポータブルディスクストレージデバイスで Backup Exec のインベントリ操作を作成し、実行します。

8 ポータブルディスクストレージデバイスで Backup Exec のカタログ操作を作成し、実行します。

9 ディスクストレージデバイスでバックアップセットを複製し、宛先ストレージデバイスとしてクラウドの重複排除用ディスクストレージデバイスを使用します。

10 複製操作が完了したら、Backup Exec を使用してディスクストレージのファイルを廃棄して削除できます。ディスクユーティリティを使用してポータブルドライブをきれいに消去します。

プライベートクラウドの重複排除用ディスクストレージデバイスのシーディングが正常に終了したら、設定の処理は完了です。次のトピックで Backup Exec での操作を開始できます。

p.35 の「オフサイトコピー設定の Backup Exec プライベートクラウドサービスの操作について」を参照してください。

直接バックアップ設定のセットアップ

プライベートクラウドサーバーで OpenVPN を設定した後、1 台または複数の Backup Exec サーバーを設定する必要があります。

p.11 の「Backup Exec プライベートクラウドサービスの設定」を参照してください。

直接バックアップ設定には、最低 3 台のコンピュータを必要とします。

p.19 の「直接バックアップ設定について」を参照してください。

表 2-11　直接バックアップ設定をセットアップする方法

手順	説明
手順 1	プライベートクラウドの重複排除用ディスクストレージデバイスを設定します。 p.30 の「直接バックアップ設定のプライベートクラウドの重複排除用ディスクストレージデバイスの設定」を参照してください。
手順 2	プライベートクラウドの重複排除用ディスクストレージデバイスにデータをシードします。 p.31 の「直接バックアップ設定の重複排除用ディスクストレージデバイスのシーディングについて」を参照してください。

直接バックアップ設定のプライベートクラウドの重複排除用ディスクストレージデバイスの設定

Backup Exec ディスクストレージデバイスと重複排除用ディスクストレージデバイスをプライベートクラウドのインスタンスに作成する必要があります。

p.30 の「直接バックアップ設定のセットアップ」を参照してください。

表 2-12　プライベートクラウドの Backup Exec インスタンスの重複排除用ディスクストレージデバイスを設定する方法

手順	説明
手順 1	ローカルサーバーに管理者権限を持つドメインアカウントを使用して C1 にログオンします。
手順 2	Backup Exec 2012 を C1 にインストールし、システムログオンを指定します。

手順	説明
手順 3	C1 の Backup Exec で、新しい重複排除用ディスクストレージデバイスを作成します。 プライベートクラウドの重複排除用ディスクストレージデバイスで保存データを暗号化する場合は、新しい重複排除用ディスクストレージデバイスを作成するときに、[はい。この重複排除用ディスクストレージデバイスに転送中、データがそのデバイスに格納されている間に、データを暗号化します]を選択します。既存の重複排除用デバイスの場合、重複排除用デバイスのプロパティで[暗号化]フィールドを変更できます。 **メモ:** VPN はローカル Backup Exec サーバーとクラウドの Backup Exec サーバー間でデータを送信しているときに、データを暗号化します。 重複排除用ディスクストレージデバイスの作成について詳しくは、『Symantec Backup Exec 管理者ガイド』を参照してください。
手順 4	次の手順を実行して、プライベートクラウドサーバーの設定を有効にします。 ■ Backup Exec サーバーで Backup Exec を開きます。 ■ [Backup Exec]ボタンをクリックして[構成と設定]を選択し、[ローカルサーバーのプロパティ]をクリックします。 ■ 左側のペインで、[設定]をクリックします。 ■ [プライベートクラウドサーバー]フィールドで、[有効]を選択します。

直接バックアップ設定の重複排除用ディスクストレージデバイスのシーディングについて

インターネット上の長い転送時間を避けるために、開始するデータをクラウドの重複排除用ディスクストレージデバイスにシードできます。重複排除用ディスクストレージデバイスのシーディングは、使用の準備のために重複排除用ディスクストレージデバイスに初期設定ファイルやバックアップセットを配置する処理です。転送時間は、プライベートクラウドの Backup Exec インスタンスにコピーされバックアップされるデータの量によって決まります。

シードするデータの種類によって、2 つの方法のいずれかを使って初期データをシードできます。

■ [システム状態]のオペレーティングシステムバックアップを、重複排除用ディスクストレージデバイスにシードできます。プライベートクラウドで動作する他のコンピュータの[システム状態]データのバックアップジョブを実行することによって、重複排除用ディスクストレージデバイスをシードします。バックアップするローカルコンピュータと同じオペレーティングシステムを実行するコンピュータの[システム状態]データをバックアップします。
p.32 の「直接バックアップ設定のオペレーティングシステムファイルのシーディング」を参照してください。

- ローカル Backup Exec サーバーからプライベートクラウドのデータセンターへ、関連したデータとバックアップセットを含む物理転送ドライブを送ることができます。
p.32 の「直接バックアップ設定のための、転送ドライブを使用した重複排除用ディスクストレージデバイスのシーディング」を参照してください。

直接バックアップ設定のオペレーティングシステムファイルのシーディング

インターネット上の長い転送時間を避けるために、開始するデータをクラウドの重複排除用ディスクストレージデバイスにシードできます。重複排除用ディスクストレージデバイスをシードする方法の 1 つは、同じ場所に配置された他のコンピュータからの[システム状態]のバックアップデータを使用することです。

p.31 の「直接バックアップ設定の重複排除用ディスクストレージデバイスのシーディングについて」を参照してください。

表 2-13　直接バックアップ設定のオペレーティングシステムファイルをシードする方法

手順	説明
手順 1	お客様のローカルネットワークでバックアップするコンピュータに、Agent for Windows と Agent for Linux をインストールします。 Backup Exec エージェントのインストールの詳細については『Symantec Backup Exec 管理者ガイド』を参照してください。 データのシーディングに使用するコンピュータは、バックアップ対象のコンピュータと同じオペレーティングシステムのバージョンを実行する必要があります。
手順 2	プライベートクラウドの Backup Exec サーバーでバックアップジョブを作成し、実行します。プライベートクラウドの重複排除用ディスクストレージデバイスに、これらの同じ場所に配置されたコンピュータの[システム状態]とシステムボリュームをバックアップします。

直接バックアップ設定のための、転送ドライブを使用した重複排除用ディスクストレージデバイスのシーディング

プライベートクラウドの Backup Exec の重複排除用ディスクストレージデバイスをシードするために、物理転送ドライブを使用できます。起動するファイルを重複排除用ディスクストレージデバイスにシードすれば、インターネットでの大容量のバックアップの実行時間を節約できます。

p.31 の「直接バックアップ設定の重複排除用ディスクストレージデバイスのシーディングについて」を参照してください。

表 2-14　直接バックアップ設定のための、転送ドライブを使用した重複排除用ディスクストレージデバイスをシードする方法

手順	説明
手順 1	コンピュータ (C2) にポータブルドライブを接続します。
手順 2	C2 からポータブルドライブにシードファイルをコピーします。
手順 3	サードパーティの暗号化ツールを使ってディスクのファイルを暗号化します。
手順 4	プライベートクラウドのデータセンターに転送ドライブを送ります。
手順 5	コンピュータ 1 (C1) に転送ドライブを接続します。
手順 6	データの暗号化に使用した同じツールを使用して、転送ドライブのデータを一時的に暗号解除します。
手順 7	暗号化されていないファイルをバックアップするバックアップジョブを作成し、実行します。宛先としてクラウドの重複排除用ディスクストレージデバイスを使用してください。
手順 8	バックアップジョブが完了すると、コピーされたソースファイルを削除できます。ディスクユーティリティを使用してポータブルドライブをきれいに消去します。

プライベートクラウドの重複排除用ディスクストレージデバイスのシーディングが正常に終了したら、設定の処理は完了です。

次のトピックで Backup Exec の操作を開始できます。

p.42 の「Backup Exec プライベートクラウドサービスと直接バックアップ設定の操作について」を参照してください。

3

Backup Exec プライベートクラウドサービスの操作

この章では以下の項目について説明しています。

オフサイトコピー設定の Backup Exec プライベートクラウドサービスの操作について

Backup Exec プライベートクラウドサービスでは、Central Admin Server Option (CASO) と Deduplication Option を使用して、バックアップ定義を管理できます。

シマンテック社は、インターネットでのデータのコピーにかかる時間を推定するのに役立つ計算ツールを提供しています。クラウドバックアップ時間の計算ツールは、クラウドバックアップ戦略を計画するのに役立ちます。割り当てられたバックアップ時間帯内にお客様のデータをバックアップするのに、システムリソースが十分であるかどうか判断するために、計算ツールを使用できます。見積もり時間は、どの位のデータを適切にサポートでき、どの位の時間をクラウドバックアップに割り当てる必要があるかを判断するうえで役立ちます。

次のリンクで計算ツールを入手できます。

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

p.36 の「オフサイトコピー設定のバックアップ定義の作成」を参照してください。

p.38 の「オフサイトコピー設定を使用したプライベートクラウドからのデータのリストアについて」を参照してください。

p.38 の「オフサイトコピー設定を使用したプライベートクラウドからのデータのリストア」を参照してください。

p.39 の「オフサイトコピー設定を使用した、プライベートクラウドからの転送ドライブを用いたデータのリストア」を参照してください。

オフサイトコピー設定のバックアップ定義の作成

複製ステージを使用してバックアップ定義を作成することで、プライベートクラウドの Backup Exec インスタンスにバックアップデータをコピーできます。バックアップ定義は集中管理サーバーに存在します。定義は、ローカルの重複排除用ディスクストレージデバイスにデータをバックアップするバックアップジョブを含んでいます。また定義は、プライベートクラウドの重複排除用ディスクストレージデバイスにそれらのバックアップセットをコピーする複製ステージも含んでいます。

必要に応じて、バックアップ定義に追加の複製ステージを加えて、クラウドの重複排除用ディスクストレージデバイスからコピーされたバックアップセットをレプリケートできます。同様にクラウドに存在するテープデバイス、または管理対象 Backup Exec サーバー上の他の重複排除用ストレージデバイスに、バックアップセットを複製できます。管理対象 Backup Exec サーバーは、プライベートクラウドまたは異なる物理的な場所に存在する場合もあります。

メモ: バックアップ定義の作成の詳細については『Symantec Backup Exec 管理者ガイド』を参照してください。

オフサイトコピー設定のバックアップ定義を作成する方法

1. 集中管理サーバーで、Backup Exec を開いてください。
2. [バックアップとリストア]タブで、次のいずれかを実行します。
   - 単一のサーバーをバックアップするには、サーバー名を右クリックしてください。
   - 複数のサーバーをバックアップするには、Shift キーまたは Ctrl キーを押しながらサーバー名をクリックし、選択したいずれかのサーバーを右クリックします。
3. [バックアップ]メニューで、使用するバックアップオプションを選択します。

4 [名前]フィールドで、バックアップ定義の一意の名前を入力してください。

メモ: 複数のサーバーからのデータをバックアップする場合、Backup Exec は[名前]フィールドに入力したテキストにサーバー名を追記します。Backup Exec は、ユーザーが入力したサーバー名とテキストを使用して、各バックアップ定義の一意の名前を作成します。

5 次のいずれかを実行します。

バックアップ選択項目にアクセスするのに Backup Exec が使用するクレデンシャルを編集またはテストするには	[**Selections**]のボックスで、[クレデンシャルのテストと編集]をクリックしてください。
バックアップの選択項目を変更する方法	[**Selections**]のボックスで、[編集]をクリックしてください。
ステージをバックアップ定義に追加する方法	次の手順を実行します。 ■ [バックアップ]ボックスで[ステージを追加]をクリックします。 ■ [複製]をクリックして、複製ステージを追加します。 ■ [複製]ボックスで、[編集]をクリックします。 ■ [ストレージ]ペインで、複製操作のストレージとして、プライベートクラウドの重複排除用ディスクストレージデバイスを選択します。 ■ 必要に応じて他の設定を設定します。個別のジョブとして複製操作を検証することをお勧めします。ジョブの終わりに操作を検証することを選択すると、ジョブのパフォーマンスが低下します。[検証]ペインで検証操作を設定できます。 **メモ:** バックアップ定義に追加の複製ステージを加えることができます。例えば、同じ場所に配置されたテープデバイスまたはリモートの管理対象 Backup Exec サーバー上の重複排除用ストレージデバイスに、追加コピーを送ることもできます。

ジョブ設定を変更するには	次の手順を実行します。 ■ [バックアップ]ボックスで、[編集]をクリックします。 ■ [ストレージ]ペインで、バックアップジョブのストレージとして、ローカルの重複排除用ディスクストレージデバイスを選択します。 ■ 必要に応じて他の設定を設定します。

6 バックアップ定義の設定を終了するときは、[バックアップのプロパティ]ダイアログボックスで[OK]をクリックします。

p.35 の「オフサイトコピー設定の Backup Exec プライベートクラウドサービスの操作について」を参照してください。

オフサイトコピー設定を使用したプライベートクラウドからのデータのリストアについて

プライベートクラウドの Backup Exec インスタンスにデータをバックアップすれば、それをいつでもリストアできます。プライベートクラウドの Backup Exec の重複排除用ディスクストレージデバイスからデータをリストアすることは、Backup Exec でデータを通常どおりリストアすることに非常に似ています。

p.38 の「オフサイトコピー設定を使用したプライベートクラウドからのデータのリストア」を参照してください。

物理転送ドライブを使用して Backup Exec のプライベートクラウドのインスタンスから大量のデータをリストアすると、より効率的な場合があります。転送ドライブを使用して、ローカルの Backup Exec サーバーにデータを転送できます。その後ローカルの Backup Exec サーバーを使用して、リストアジョブを実行します。

p.39 の「オフサイトコピー設定を使用した、プライベートクラウドからの転送ドライブを用いたデータのリストア」を参照してください。

オフサイトコピー設定を使用したプライベートクラウドからのデータのリストア

プライベートクラウドの Backup Exec インスタンスから、ローカルの Backup Exec クライアントのコンピュータにデータをリストアできます。

p.38 の「オフサイトコピー設定を使用したプライベートクラウドからのデータのリストアについて」を参照してください。

オフサイトコピー設定を使用したプライベートクラウドからデータをリストアする方法

1. リストアするサーバーが、次の手順で説明するように、コンピュータ 1 (C1) と通信可能なネットワークルートコマンドを含んでいることを確認します。

   p.56 の「ローカルネットワークのルーティングの設定」を参照してください。

2. 集中管理サーバーで Backup Exec を開きます。
3. [バックアップとリストア]タブで、[リストア]をクリックします。
4. リストアするデータを選択して、他の必要なジョブオプションも選択します。次にジョブをサブミットします。

p.35 の「オフサイトコピー設定の Backup Exec プライベートクラウドサービスの操作について」を参照してください。

オフサイトコピー設定を使用した、プライベートクラウドからの転送ドライブを用いたデータのリストア

転送ドライブを使用して、プライベートクラウドの Backup Exec インスタンスからローカルの Backup Exec サーバーにデータをコピーできます。転送ドライブを使用すると、多量のデータを一度にリストアする場合に便利です。大きいリストアジョブは、利用可能な帯域幅とジョブの完了までの時間によって、システムリソースに影響を与えることがあります。

p.38 の「オフサイトコピー設定を使用したプライベートクラウドからのデータのリストアについて」を参照してください。

転送ドライブとオフサイトコピー設定を使用して、プライベートクラウドからデータをリストアする方法

1. プライベートクラウドの Backup Exec インスタンスのコンピュータ 1 (C1) のポータブルドライブでディスクストレージを作成します。
2. クラウドベースの重複排除用ディスクストレージデバイスから、リストアするバックアップセットを複製します。宛先ストレージデバイスとして作成した、ディスクストレージを選択します。

   ソフトウェア暗号化を使用してデータを暗号化することを選択することを確認してください。ソフトウェア暗号化の暗号化キーを作成するか、または選択します。

   データの暗号化の詳細については『Symantec Backup Exec 管理者ガイド』を参照してください。
3. ジョブが完了したら、ローカルオフィスに転送ドライブを送ってください。
4. ポータブルドライブが到着したら、ローカルの Backup Exec サーバーにドライブを接続します。
5. パスとしてポータブルドライブを使用して、コンピュータ 2 (C2) でディスクストレージを作成します。

6 ディスクストレージで Backup Exec のインベントリおよびカタログ操作を作成し、実行します。

7 新しいディスクストレージから適切な宛先にデータをリストアします。

8 転送ドライブからデータを消去します。

p.35 の「オフサイトコピー設定の Backup Exec プライベートクラウドサービスの操作について」を参照してください。

集中管理サーバーエラー時の管理対象 Backup Exec サーバーからのデータリストア

ハードウェアエラーやその他の災害によって集中管理サーバーが影響を受けると、管理対象 Backup Exec サーバーがバックアップジョブやリストアジョブを実行できなくなります。代替コンピュータを設定し、Backup Exec 集中管理サーバーを再インストールすることによって、集中管理サーバーを回復することができます。また、管理対象 Backup Exec サーバーをスタンドアロン Backup Exec サーバーに変換して集中管理サーバーをリストアすることもできます。

管理対象 Backup Exec サーバーをスタンドアロン Backup Exec サーバーに変換して集中管理サーバーをリストアするには

1 管理対象 Backup Exec サーバーで、ローカルディスクストレージの名前とディレクトリパスをメモします。

メモ: [ストレージ]タブでディスクストレージをダブルクリックします。次に、左ペインの[プロパティ]をクリックして、ストレージのプロパティを表示します。

2 管理対象 Backup Exec サーバーに独自の重複排除用ディスクストレージデバイスがある場合、そのデバイスの名前、パス、ログオンアカウント、およびパスワードプロパティをメモします。

メモ: [ストレージ]タブで重複排除用ディスクストレージデバイスをダブルクリックします。次に、左ペインの[プロパティ]をクリックして、ストレージのプロパティを表示します。

3 Windows のコントロールパネルから、[プログラムと機能]（または[プログラムの追加と削除]）ダイアログか、[プログラムのアンインストール]ダイアログを開きます。

4 Symantec Backup Exec の[変更]オプションを選択します。

5 左ペインで、[追加オプション]がまだ選択されていない場合は選択します。

6 [**Managed Backup Exec Server** の設定]パネルに達するまで[次へ]をクリックします。

7 [ローカルに管理された Backup Exec サーバー]オプションを選択します。

8 [次へ]をクリックします。

9 「{集中管理サーバー}に接続できません。集中管理サーバーが実行されていることを確認してください。」というメッセージが表示されたら、次のいずれかを実行します。

集中管理サーバーが使用不可で、この管理対象 Backup Exec サーバーをローカルに管理する場合	[OK]をクリックして続行します。
集中管理サーバーの稼働時にこの操作を再試行する場合	[キャンセル]をクリックしてこの手順を終了します。

インストールが完了すると、コンピュータは中央管理 Backup Exec サーバーではなくなります。

10 [次へ]をクリックします。

11 コンピュータの再起動を要求するメッセージが表示されたら、再起動します。

12 Backup Exec を開き、[ストレージ]タブを選択します。

Backup Exec が Backup Exec サーバーに接続できない場合、Backup Exec サービスを再起動してから再試行してください。

13 手順1でメモしたものと同じ名前とパスを使用して元のディスクストレージをインポートし、ローカルディスクストレージを再作成します。

14 手順2でメモしたものと同じ情報を使用して元の重複排除用ディスクストレージデバイスをインポートし、重複排除用ディスクストレージデバイスを再作成します。

メモ: 既存のストレージデバイスの再作成には、新しいストレージデバイスを作成するよりはるかに長い時間がかかる場合があります。かかる時間は、ストレージデバイスに含まれていたバックアップセットの数、その管理対象 Backup Exec サーバーにドメインコントローラと DNS へのアクセス権があるかどうかによって異なります。

---

15 再作成したストレージデバイスごとに、Backup Exec インベントリ操作およびカタログ操作を作成して実行します。

これで、スタンドアロン Backup Exec サーバーを使用して、Backup Exec サーバーのストレージデバイスに保存されていたバックアップセットをリストアできます。

16 集中管理サーバーの回復にスタンドアロン Backup Exec サーバーを使用する場合、スタンドアロン Backup Exec サーバーにある既存の集中管理サーバーリソースの削除が必要になる場合があります。続いて、リストア前に集中管理サーバーに Agent for Windows をプッシュインストールします。

集中管理サーバーが回復したら、再び Backup Exec 変更インストールダイアログを使用して、ローカルに管理された Backup Exec サーバーを中央管理 Backup Exec サーバーに変換できます。中央管理 Backup Exec サーバーオプションを選択して、コンピュータを管理対象 Backup Exec サーバーとして再設定します。

Backup Exec プライベートクラウドサービスと直接バックアップ設定の操作について

Backup Exec プライベートクラウドサービスでは、直接バックアップ設定のクライアント側の重複排除で、バックアップ定義を管理できます。

ジョブを実行するとき、プライベートクラウドの Backup Exec インスタンスと VPN リンク接続を手動で開始し、停止することを選択できます。あるいは、VPN リンクを接続してインスタンスを永続的に実行させることも選択できます。また、OpenVPN サービスをスケジュール設定することで、この処理を自動化して、バックアップジョブの時間帯に開始したり停止したりすることも選択できます。サービスのスケジュールを作成するために Windows の Scheduled Tasks ユーティリティを使用できます。

シマンテック社は、インターネットでのデータのコピーにかかる時間を推定するのに役立つ計算ツールを提供しています。クラウドバックアップ時間の計算ツールは、クラウドバックアップ戦略を計画するのに役立ちます。割り当てられたバックアップ時間帯内にお客様のデータをバックアップするのに、システムリソースが十分であるかどうか判断するために、計算ツールを使用できます。見積もり時間は、どの位のデータを適切にサポートでき、どの位の時間をクラウドバックアップに割り当てる必要があるかを判断するうえで役立ちます。

次のリンクで計算ツールを入手できます。

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

p.43 の「直接バックアップ設定のクライアント側の重複排除の有効化」を参照してください。

p.43 の「直接バックアップ設定のバック定義の作成」を参照してください。

p.45 の「直接バックアップ設定を使用した、プライベートクラウドからの転送ドライブによるデータのリストア」を参照してください。

直接バックアップ設定のクライアント側の重複排除の有効化

プライベートクラウドの Backup Exec インスタンスへの直接バックアップジョブを作成して実行するには、クライアント側の重複排除を有効にしておく必要があります。

メモ: マルチテナント設定を使用する場合は、集中管理サーバーの重複排除用ディスクストレージデバイスのクライアント側の重複排除を有効にしないでください。

直接バックアップ設定のクライアント側の重複排除を有効にする方法

1. [ストレージ]タブで、プロパティを編集するストレージをダブルクリックします。
2. 左ペインで、[プロパティ]をクリックします。
3. [クライアント側重複排除]フィールドで、[有効]を選択します。
4. [適用]をクリックします。
5. Backup Exec サービスを再起動します。

メモ: C1 の Backup Exec サービスを停止し、再起動します。

直接バックアップジョブを作成して実行するには、クライアント側の重複排除を有効にする必要があります。

クライアント側の重複排除を使用するバックアップジョブの作成について詳しくは、『Symantec Backup Exec 管理者ガイド』を参照してください。

p.43 の「直接バックアップ設定のバック定義の作成」を参照してください。

p.42 の「Backup Exec プライベートクラウドサービスと直接バックアップ設定の操作について」を参照してください。

直接バックアップ設定のバック定義の作成

VPNを設定して、Remote Agent 共有とクライアント側の重複排除用の他のコンピュータを有効にした後、直接バックアップジョブを作成し、実行できます。

p.43 の「直接バックアップ設定のクライアント側の重複排除の有効化」を参照してください。

メモ: バックアップ定義の作成の詳細については『Symantec Backup Exec 管理者ガイド』を参照してください。

次の手順を使用して、プライベートクラウドの Backup Exec インスタンスにデータを直接バックアップします。

直接バックアップ設定のバックアップジョブを作成する方法

1. コンピュータ 1 (C1) で、Backup Exec を開いてください。
2. [バックアップとリストア]タブで、次のいずれかを実行します。
   - 単一のサーバーをバックアップするには、サーバー名を右クリックしてください。
   - 複数のサーバーをバックアップするには、Shift キーまたは Ctrl キーを押しながらサーバー名をクリックし、選択したいずれかのサーバーを右クリックします。
3. [バックアップ]メニューで、使用するバックアップオプションを選択します。
4. [名前]フィールドで、バックアップ定義の一意の名前を入力してください。

メモ: 複数のサーバーからのデータをバックアップする場合、Backup Exec は[名前]フィールドに入力したテキストにサーバー名を追記します。Backup Exec は、ユーザーが入力したサーバー名とテキストを使用して、各バックアップ定義の一意の名前を作成します。

---

5. 次のいずれかを実行します。

バックアップ選択項目にアクセスするのに Backup Exec が使用するクレデンシャルを編集またはテストするには	[**Selections**]のボックスで、[クレデンシャルのテストと編集]をクリックしてください。
バックアップの選択項目を変更する方法	[**Selections**]のボックスで、[編集]をクリックしてください。
ステージをバックアップ定義に追加する方法	[バックアップ]ボックスで[ステージを追加]をクリックします。
ジョブ設定を変更するには	次の手順を実行します。 ■ [バックアップ]ボックスで、[編集]をクリックします。 ■ [リモートコンピュータのストレージデバイスへの直接アクセスとクライアント側の重複排除の実行がサポートされている場合には、それらを有効にする]オプションが選択されていることを確認します。 ■ 必要に応じて他の設定を設定します。

6. バックアップ定義の設定を終了するときは、[バックアップのプロパティ]ダイアログボックスで[OK]をクリックします。

p.42 の「Backup Exec プライベートクラウドサービスと直接バックアップ設定の操作について」を参照してください。

直接バックアップ設定を使用した、プライベートクラウドからの転送ドライブによるデータのリストア

プライベートクラウドの Backup Exec インスタンスからローカルクライアントにデータをリストアするために、通常のリストアジョブを作成できます。ただし、多量のデータを一度にリストアするには、物理転送ドライブを使用することが賢明な場合があります。多量のデータの転送にかかる時間は、利用可能な帯域幅とジョブの完了時間によって決まります。

直接バックアップ設定を使用し、プライベートクラウドから転送ドライブを用いてデータをリストアする方法

1. コンピュータ 1 (C1) にリストアジョブを作成し実行して、ポータブルディスクドライブのフォルダにファイルをリストアします。
2. ジョブの完了後、サードパーティの暗号化ツールを使用してディスクのファイルを暗号化します。
3. ローカルオフィスにポータブルドライブを送ります。
4. ポータブルドライブが到着したら、暗号化に使用したのと同じツールを使用して、ファイルを暗号解除します。
5. コンピュータ 2 (C2) の適切な宛先に、暗号化されていないファイルを転送します。
6. 転送ドライブからファイルを完全に削除または消去して、データが永久に削除されたことを確認します。

p.42 の「Backup Exec プライベートクラウドサービスと直接バックアップ設定の操作について」を参照してください。

クラウドディザスタリカバリサービスについて

Backup Exec 2012 Simplified Disaster Recovery（SDR）機能および仮想マシンへの変換機能を使用すると、サービスプロバイダやお客様はクラウドディザスタリカバリサービスを実現できます。災害の際には、クラウドに格納されているバックアップデータを使用して、一時的な代替仮想または物理サーバーをプライベートクラウド内に作成できます。

特定のネットワーク設定およびエラー状況によって、フェールオーバーおよびフェールバックに必要な特定の手順の変更が必要になる場合があります。ここでは、Backup Exec プライベートクラウド環境内で SDR および仮想マシンへの変換機能を使用してディザスタリカバリサービスを実現するための基本的なガイドラインのみを示します。

主なディザスタリカバリシナリオとして次の 2 つが考えられます。1 つ目のシナリオは、1 台以上のオンプレミスサーバーに障害が発生したが、オンサイトネットワークは影響を受けていない場合のサーバーのフェールオーバーおよびフェールバックです。2 つ目のシナリオは、サイト全体に障害が発生した場合のサイトのフェールオーバーおよびフェールバックです。

p.46 の「フェールオーバーからのサーバーまたはサイトの回復」を参照してください。

p.48 の「フェールバックからのサーバーまたはサイトの回復」を参照してください。

フェールオーバーからのサーバーまたはサイトの回復

サーバーフェールオーバーシナリオの準備をするには、業務上重要なサーバーについて、定例のスケジュール済み Simplified Disaster Recovery（SDR）対応バックアップ定義を設定して実行する必要があります。バックアップ定義には、バックアップデータをプライベートクラウドの重複排除用ディスクストレージデバイスにコピーする複製ステージを含める必要があります。サーバーのフェールオーバーが発生したら、プライベートクラウドの Backup Exec サーバーを使用して代替仮想または物理サーバーを回復します。

p.45 の「クラウドディザスタリカバリサービスについて」を参照してください。

代替物理サーバーを回復するには、Simplified Disaster Recovery ディスクを使用して Bare Metal Restore を実行します。プライベートクラウドの重複排除用ディスクストレージデバイスにある最新の SDR 対応バックアップを使用します。代替サーバーをオンプレミスサイトにトランスポートして障害が発生したサーバーを置き換えることができます。サイトのフェールオーバーでは、業務上重要なサーバーのグループ全体を、クラウド内にあるハイパーバイザ環境の仮想マシンで置き換える必要があります。

Simplified Disaster Recovery について詳しくは『Symantec Backup Exec 管理者ガイド』を参照して下さい。

メモ: 特定のネットワーク設定およびエラー状況によって、フェールオーバーに必要な特定の手順の変更が必要になる場合があります。次の手順では、Backup Exec プライベートクラウド環境を使用してディザスタリカバリサービスを実現するための基本的なガイドラインのみを示します。

フェールオーバーからサーバーまたはサイトを回復するには

1. クラウドの場所に Hyper-V または VMWare ESX ハイパーバイザ環境を作成します。
2. ハイパーバイザ上で稼動する代替仮想マシン用にフェンスを設定した仮想ネットワークを作成します。サイト全体のフェールオーバーシナリオの場合、代替サーバーに元のオンプレミス IP アドレスを維持する必要があります。

   メモ: サイトを回復する場合、代替サーバーに元のオンプレミス IP アドレスを維持する必要があります。代替コンピュータは論理的な順序でリストアする必要があります。たとえば、ドメインコントローラおよび DNS サーバーを最初にリストアする必要があります。

   ---

3. 次のいずれかを実行します。

物理コンピュータからフェールオーバーするには	次の手順を実行します。 ■ 仮想マシンへの変換を作成して実行します。すべての代替コンピュータについて、特定の時点の SDR システムボリュームとシステム状態データを仮想マシンに変換します。仮想マシンのターゲットはハイパーバイザにする必要があります。この時点では、どのアプリケーションリソースも選択しないで下さい。 ■ 必要に応じて、代替仮想マシンに固定 IP アドレスを設定します。 ■ 代替仮想マシンとプライベートクラウドの Backup Exec サーバー間のネットワーク接続を確立します。 ■ 代替元サーバーのそれぞれについて、同じ特定の時点の SDR 対応バックアップからのリストアジョブを作成して実行します。その特定の時点で使用可能なコンピュータのリソースをすべて選択します。データのリストア先を代替サーバーに変更します。
仮想マシンからフェールオーバーするには	代替サーバーの最新時点の SDR バックアップからリストア先を変更したリストアジョブを作成して実行します。オンプレミスサーバーとクラウドサーバーの両方に同じタイプのハイパーバイザを使用する必要があります。

4 単一サーバーのみを回復するには、代替サーバーとオンプレミスネットワーク間の VPN 接続を確立し、代替仮想マシンの IP アドレスについてオンプレミス DNS エントリを設定します。

5 障害が発生したサーバーが外部 IP アドレスを通じて公開されていた場合（Exchange メールサーバーなど）、新しい外部アドレスをクラウドネットワークから公開し、外部 DNS レコードを変更します。

6 代替仮想マシン用に定例のスケジュール済みハイパーバイザホストバックアップ定義を設定して実行します。バックアップ先としてプライベートクラウドの重複排除用ディスクストレージデバイスを使用します。

オンプレミス Backup Exec サーバーにローカルの重複排除用ディスクストレージがある場合、バックアップ定義には、バックアップをオンプレミスの重複排除用ディスクストレージデバイスにコピーする複製ステージを含める必要があります。

フェールバックからのサーバーまたはサイトの回復

フェールバックの際には、サーバーまたはサイトを回復できます。サイトのフェールバックシナリオでは、業務上重要なサーバーのグループ全体をオンプレミスの物理サーバーまたは仮想マシンにリストアする必要があります。

p.45 の「クラウドディザスタリカバリサービスについて」を参照してください。

すべてのオンプレミスサーバーを一度に回復するのではなく、サーバーの段階的な回復が必要な場合もあります。一部のサーバーを最初に回復し、残りのサーバーを数日間または数週間かけて回復することができます。この方法では、オンプレミスネットワークに接続する残りの代替クラウドサーバーで VPN 接続と IP アドレスの変更が必要になる可能性があります。

Simplified Disaster Recovery について詳しくは『Symantec Backup Exec 管理者ガイド』を参照して下さい。

メモ: 特定のネットワーク設定およびエラー状況によって、フェールオーバーに必要な特定の手順の変更が必要になる場合があります。次の手順では、Backup Exec プライベートクラウド環境を使用してディザスタリカバリサービスを実現するための基本的なガイドラインのみを示します。

フェールバックからサーバーまたはサイトを回復するには

1. Simplified Disaster Recovery（SDR）対応バックアップを実行し、複製ステージを含めます。
2. 代替仮想マシンをオフにします。
3. バックアップセットをオンプレミス重複排除用ディスクストレージに送信する複製ステージが SDR 対応バックアップ定義に含まれていなかった場合、次の手順を実行します。
   - プライベートクラウドの Backup Exec サーバーの Backup Exec にポータブルディスクストレージデバイスを追加します。
   - すべての代替コンピュータの最終バックアップデータからバックアップセットを複製します。複製先としてポータブルディスクストレージデバイスを使用します。
   - ポータブルディスクストレージデバイスをオンプレミスの場所に送付します。
   - オンプレミス Backup Exec サーバーの Backup Exec にポータブルディスクストレージデバイスを追加します。
   - オンプレミス Backup Exec サーバーでディスクストレージデバイスのインベントリおよびカタログ操作を実行します。
4. 次のいずれかを実行します。

オンプレミス物理サーバーにフェールバックするには	次の手順を実行します。 ■ Simplified Disaster Recovery ディスクを使用して Bare Metal Restore を実行します。オンプレミス Backup Exec サーバーで最新の SDR 対応バックアップを選択します。 ■ 必要に応じて、回復したコンピュータに固定 IP アドレスを設定します。 ■ 必要に応じて、回復したコンピュータの IP アドレスについてオンプレミス DNS エントリを設定します。
オンプレミス仮想サーバーにフェールバックするには	次の手順を実行します。 ■ 代替サーバーの最新時点のバックアップからリストア先を変更したリストアジョブを作成して実行します。オンプレミスサーバーとクラウドサーバーの両方に同じタイプのハイパーバイザを使用する必要があります。 ■ 必要に応じて、回復した仮想マシンに固定 IP アドレスを設定します。 ■ 必要に応じて、回復した仮想マシンの IP アドレスについてオンプレミス DNS エントリを設定します。

5 障害が発生したサーバーが外部 IP アドレスを通じて公開されていた場合（Exchange メールサーバーなど）、外部 DNS レコードに元のアドレスをリストアします。

6 代替クラウドサーバーのバックアップ定義を削除します。

7 リストアしたオンプレミスコンピュータで元のバックアップ定義の実行を再開します。

Backup Exec 重複排除用ディスクストレージデバイスの必要条件

Backup Exec 重複排除用ディスクストレージデバイスの必要条件は、すべてのプライベートクラウド設定に適用されます。特定のクラウドの Backup Exec サーバーに設定された共有制限に到達した場合は、クラウドの Backup Exec サーバーをさらに追加する必要があります。

重複排除用ディスクストレージデバイスの必要条件について詳しくは、『Symantec Backup Exec 管理者ガイド』を参照してください。

WAN 待機時間の制限

ネットワーク待機時間が長いネットワークの場合、初回の直接クラウドバックアップジョブのパフォーマンスに悪影響が及ぼされる可能性があります。待機時間は、ローカルオフィスとプライベートクラウドの Backup Exec サーバー間でデータを転送する一部の複製バックアップジョブにも影響を及ぼす場合があります。通常はデバイスをシードすることでパフォーマンスは向上しますが、転送ドライブを使用して重複排除用ディスクストレージデバイスをシードした場合でも、パフォーマンスの問題が生じることがあります。初回のバックアップジョブ中に、Backup Exec はデータセグメントに関する情報を特定してキャッシュします。これにより、後続のジョブのパフォーマンス効率が高まります。

メモ: 平均往復待機時間が 30 ミリ秒を超える場合、待機時間の値が高いと見なすことができます。待機時間が長くなるほど、Backup Exec のパフォーマンスに及ぼされる影響は大きくなります。

ソースデバイスとターゲットデバイスの両方が重複排除用ディスクストレージデバイスである場合は、この制限事項は複製バックアップジョブに適用されません。

待機時間が長い環境で Backup Exec のプライベートクラウドサービスを使用する場合の制限事項を以下に示します。

- 複製バックアップジョブで、宛先として重複排除用ディスクストレージデバイスとプライベートクラウド重複排除用ディスクストレージデバイス以外のソースデバイスを使用する場合、パフォーマンスの問題が生じることがあります。ローカルソースストレージデバイスとして重複排除用ディスクストレージデバイスを使用することで、これらのパフォーマンス問題を回避します。
- クラウド設定に直接バックアップを使用することは、大量のデータのバックアップには適していない場合があります。
- 同じリソースのバックアップ定義を削除して再作成すると、Backup Exec はデータのフィンガープリントを最初からキャッシュしなくてはなりません。このため、初回の直接クラウドバックアップジョブの場合と同様に、何らかのパフォーマンス問題が生じる可能性があります。

オフサイトコピーでの Granular Recovery Technology の制限事項

オフサイトコピー設定での、Backup Exec の Granular Recovery Technology (GRT) オプションを使用する際の制限事項は、次のとおりです。

- ローカル Exchange の増分的な GRT 対応バックアップセットをプライベートクラウドの重複排除用ディスクストレージデバイスにバックアップすると、MTF テープ形式でバックアップデータが作成されます。これらのバックアップセットから個別データをリス

トアすることはできますが、リストアジョブの実行中に、クラウドの Backup Exec サーバーにバックアップセットをステージングする必要があります。GRT 対応バックアップセットをクラウドの重複排除用ディスクストレージデバイスに直接バックアップする場合には、この制限はありません。

- GRT 対応の複製セットをローカルテープデバイスからクラウドの重複排除用ディスクストレージデバイスに直接コピーすることは、できるだけ避けてください。ジョブの実行時間が過度にかかる場合があります。
- GRT 対応のセットをクラウドの Backup Exec サーバーに直接バックアップすると、待機時間の長い環境ではパフォーマンスが低下する可能性があります。初回バックアップの後でも、パフォーマンスが低下する場合があります。パフォーマンスの問題が解決されない場合は、直接バックアップで GRT を無効に設定してください。

Windows Small Business Server（SBS）およびマルチテナント Backup Exec サーバー設定の制限事項

マルチテナント Backup Exec サーバー設定では、すべてのローカルの管理対象 Backup Exec サーバーがプライベートクラウドドメインのメンバーである必要があります。したがって、管理対象 Backup Exec サーバーがお客様のドメインの一部である場合は、お客様の SBS サーバーを管理対象 Backup Exec サーバーとして設定することはできません。管理対象 Backup Exec サーバーは、別個のサーバーとしてインストールする必要があります。

4

OpenVPN の設定

この章では以下の項目について説明しています。

OpenVPN の設定について

OpenVPN SSL VPN のオープンソースパッケージは、プライベートクラウドの Backup Exec インスタンスとローカルの Backup Exec サーバー間で安全に暗号化された接続を提供します。プライベートクラウドの Backup Exec サーバーインスタンスと、ローカルネットワークで動作しているすべてのコンピュータ間の SSL VPN を設定する必要があります。

Backup Exec プライベートクラウドサービスの設定には、この単一のクライアント OpenVPN サンプルに対して、次のネットワーク制限があります。

- ローカルネットワークは単一のサブネット内に含まれている必要があります。
- ローカルドメインコントローラと DNS は同じサーバーに含まれている必要があります。

p.53 の「OpenVPN の設定」を参照してください。

Backup Exec プライベートクラウドサービスでの基本の OpenVPN 設定の手順では、単一のクライアントを使います。クライアントがすべて同じサブネットに含まれていれば、この手順を使用して、1 つ以上のローカルクライアントコンピュータをサポートできます。プライベートクラウドのインスタンスで使用されるすべてのデータは、OpenVPN の単一のクライアントを通して転送されます。より複雑なネットワークのために、または証明書ベースの認証を使うために、オプションで OpenVPN の複数のクライアント設定を使用できます。

p.60 の「複数のクライアントの OpenVPN の設定について」を参照してください。

OpenVPN の設定

OpenVPN SSL VPN のオープンソースパッケージは、プライベートクラウドの Backup Exec インスタンスとローカルの Backup Exec サーバー間で安全に暗号化された接続を

提供します。プライベートクラウドの Backup Exec サーバーインスタンスと、ローカルネットワークで動作しているすべてのコンピュータ間の SSL VPN を設定する必要があります。

p.53 の「OpenVPN の設定について」を参照してください。

表 4-1 OpenVPN を設定する方法

手順	説明
手順 1	プライベートクラウドの Backup Exec インスタンス上に OpenVPN を設定します。 p.54 の「プライベートクラウドの Backup Exec インスタンス上の OpenVPN の設定」を参照してください。
手順 2	コンピュータ 2 に OpenVPN を設定します。 p.55 の「コンピュータ 2 での OpenVPN の設定」を参照してください。
手順 3	ローカルネットワークのルーティングを設定します。 p.56 の「ローカルネットワークのルーティングの設定」を参照してください。
手順 4	必要に応じて、ファイアウォールを設定します。 p.57 の「ファイアウォールの設定について」を参照してください。
手順 5	OpenVPN の接続を検証します。 p.58 の「OpenVPN の接続の検証」を参照してください。

プライベートクラウドの Backup Exec インスタンス上の OpenVPN の設定

安全で暗号化された接続をするには、プライベートクラウドの Backup Exec インスタンス上に OpenVPN を設定します。

p.53 の「OpenVPN の設定について」を参照してください。

プライベートクラウドの Backup Exec インスタンス上に OpenVPN を設定する方法

1. OpenVPN 2.1.4 を次のリンクからダウンロードし、コンピュータ 1 (C1) でデフォルトの場所にインストールします。

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

2. C1 で、次のように選択して OpenVPN 設定フォルダの Windows Explorer のウィンドウを開いてください。

   [スタート]>[すべてのプログラム]>[OpenVPN]>[ショートカット]> OpenVPN の設定ファイルのディレクトリ

3 ¥Program Files (x86)¥OpenVPN¥bin フォルダのコマンドプロンプトから次のコマンドを実行して、OpenVPN の静的なキーを生成します。

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

4 C1 で開いたフォルダでサーバーの設定ファイルを作成し、「server.ovpn」としてファイルを保存します。

「server.ovpn」ファイルは次の例のように表示されます。

```
dev tun

ifconfig 10.8.0.1 10.8.0.2

secret static.key

keepalive 10 120
```

メモ: サブネット 10.8.x.x がローカルネットワークで使用中の場合、**ifconfig** コマンドで異なるサブネットの範囲を使ってください。

メモ: OpenVPN はデフォルトでは UDP ポート 1194 を使います。必要に応じて、OpenVPN のサーバーとクライアントの設定ファイルにポートコマンドを追加することで、別のポート番号を指定できます。

5 Windows サービスユーティリティを使って、OpenVPN サービスのスタートアップの種類プロパティを[自動]に変更します。

6 C1 のコマンドプロンプトを開いて、次のように入力し、ローカル DNS (コンピュータ 3) のサブネットアドレスと DNS のサブネットマスクを代入します。

メモ: 三角カッコを含めないでください。

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

コンピュータ 2 での OpenVPN の設定

安全で暗号化された接続を行うには、コンピュータ 1 (C1) に OpenVPN を設定した後、コンピュータ 2 (C2) に OpenVPN を設定する必要があります。

p.53 の「OpenVPN の設定について」を参照してください。

コンピュータ 2 に OpenVPN を設定する方法

1. 次のリンクから OpenVPN 2.1.4 をダウンロードし、C2 のデフォルトの場所にインストールします。

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

2. 次の手順の手順 2 で生成された静的なキーをコピーします。

   「プライベートクラウドの Backup Exec インスタンス上の OpenVPN の設定」

3. C2 の次の場所にキーを貼り付けてください。

   ¥Program Files (x86)¥OpenVPN¥config

4. C2 の次の場所にクライアントの設定ファイルを作成し、「client.ovpn」としてファイルを保存します。

   ¥Program Files (x86)¥OpenVPN¥config

   「client.ovpn」ファイルは次の例のように表示されます。

   ```
   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. **remote** 文にプライベートクラウド Backup Exec のコンピュータの固定 IP アドレスを入力します。

   メモ: 三角カッコを含めないでください。

6. サブネット 10.8.x.x がローカルネットワークで使用中の場合、ファイルを編集して **ifconfig** 文で異なるサブネットの範囲を使ってください。
7. Windows サービスユーティリティを使用して、OpenVPN サービスの[スタートアップの種類]のプロパティを[自動]に変更します。

ローカルネットワークのルーティングの設定

ローカルネットワークのルーティングを設定するには、TAP-Win32 Adapter V9 と物理的なネットワークインターフェースの両方の IP の転送を有効にする必要があります。

p.53 の「OpenVPN の設定について」を参照してください。

ローカルネットワークのルーティングを設定する方法

1. コンピュータ 2 (C2) で、レジストリエディタを開始し、次のキーを検索します。

   HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Tcpip¥Parameters

2. 次のレジストリ値を設定します。

   値の名前: IPEnableRouter

   値の種類: REG_DWORD

   値のデータ: 1

   メモ: 1 の値は、コンピュータにインストールされ、使用されるすべてのネットワーク接続の TCP/IP の転送を有効にします。

3. C2 を再起動します。
4. コンピュータ 3 (C3) のコマンドウィンドウで次のコマンドを入力して、C2 のローカル IP アドレスを代入します。

   メモ: IP アドレスを入力するときに、三角カッコを含めないでください。

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

   メモ: クラウドの OpenVPN サーバーコンピュータと通信が必要なすべてのローカルネットワークのコンピュータで、このコマンドを実行する必要があります。Backup Exec エージェントを実行するすべてのサーバーでコマンドを実行する必要があります。これは、プライベートクラウド Backup Exec サーバーからのリストアジョブの対象になります。

ファイアウォールの設定について

ローカルサーバーとクラウドサーバー間で正常な通信をするためには、表で説明されているようにネットワークのファイアウォールを設定する必要があります。

表 4-2 ファイアウォールの設定について

ファイアウォールのインスタンス	処理
コンピュータ 1 (C1)	OpenVPN のネットワークアダプタの Windows ファイアウォールを無効にする必要があります。 OpenVPN を使用するように設定されたどのポートでも、受信トラフィックを許可するように Windows ファイアウォールを設定する必要があります。デフォルトでは、OpenVPN はポート 1194 UDP を使用します。
コンピュータ 2 (C2)	OpenVPN の TAP ネットワークアダプタに対してローカルの Windows ファイアウォールを無効にする必要があります。
ローカルネットワーク	外部ローカルまたは企業のファイアウォールがある場合は、OpenVPN を使用するように設定されたどのポートでも、送信トラフィックを許可するように Windows ファイアウォールを設定する必要があります。デフォルトでは、OpenVPN はポート 1194 UDP を使用します。

p.53 の「OpenVPN の設定について」を参照してください。

OpenVPN の接続の検証

OpenVPN の設定を終了するとき、OpenVPN のサーバーとクライアントが正常に接続できることを確認するために、テストする必要があります。

p.53 の「OpenVPN の設定について」を参照してください。

OpenVPN の接続を検証する方法

1 Windows サービスユーティリティを使って、コンピュータ 1 (C1) とコンピュータ 2 (C2) の両方で OpenVPN サービスを起動します。

2 次のディレクトリで C1 と C2 にある OpenVPN のログファイルを開きます。

C:¥Program Files (x86)¥OpenVPN¥log

3 テキスト「Initialization Sequence Completed」が両方のファイルにあることを確認します。

4 C1 で、TAP-Win32 ネットワークアダプタを設定し、優先 DNS サーバーとしてローカルドメインの DNS サーバーにポイントします。

p.59 の「TAP-Win32 ネットワークアダプタの設定」を参照してください。

ジョブを実行するとき、プライベートクラウドの Backup Exec インスタンスと VPN リンク接続を手動で開始し、停止できます。あるいは、VPN リンクを接続してインスタンスを永続的に実行させることもできます。OpenVPN サービスをスケジュール設定することで、この処理を自動化して、スケジュール済みバックアップジョブで開始したり停止したりできます。また、サービスのスケジュールを作成するために Windows の Scheduled Tasks ユーティリティも使用できます。

TAP-Win32 ネットワークアダプタの設定

OpenVPN の接続を検証するには、ローカルドメインの DNS サーバーを優先 DNS サーバーとして示すように、TAP-Win32 ネットワークアダプタを設定します。

p.58 の「OpenVPN の接続の検証」を参照してください。

TAP-Win32 ネットワークアダプタを設定する方法

1 [**TAP Network Adapter properties**]を開きます。

2 [IPv4 properties]をクリックします。

3 [詳細]をクリックします。

4 [**DNS**]タブで、ローカルネットワークの DNS サーバーの IP アドレスを入力します。

5 [接尾辞]フィールドでは、ドメイン FQDN の接尾辞を追加し、接尾辞リストの最上位に移動させます。

6 [OK]をクリックして、すべてのダイアログボックスを終了します。

7 コンピュータ 1 (C1) のコマンドプロンプトでは、次のコマンドを入力します。

```
ipconfig /flushdns
```

```
ipconfig /registerdns
```

OpenVPN 接続の検証が終了したら、Backup Exec サーバーを設定できます。

p.20 の「クラウドへのマルチテナントまたはオフサイトコピー設定のセットアップ」を参照してください。

p.30 の「直接バックアップ設定のセットアップ」を参照してください。

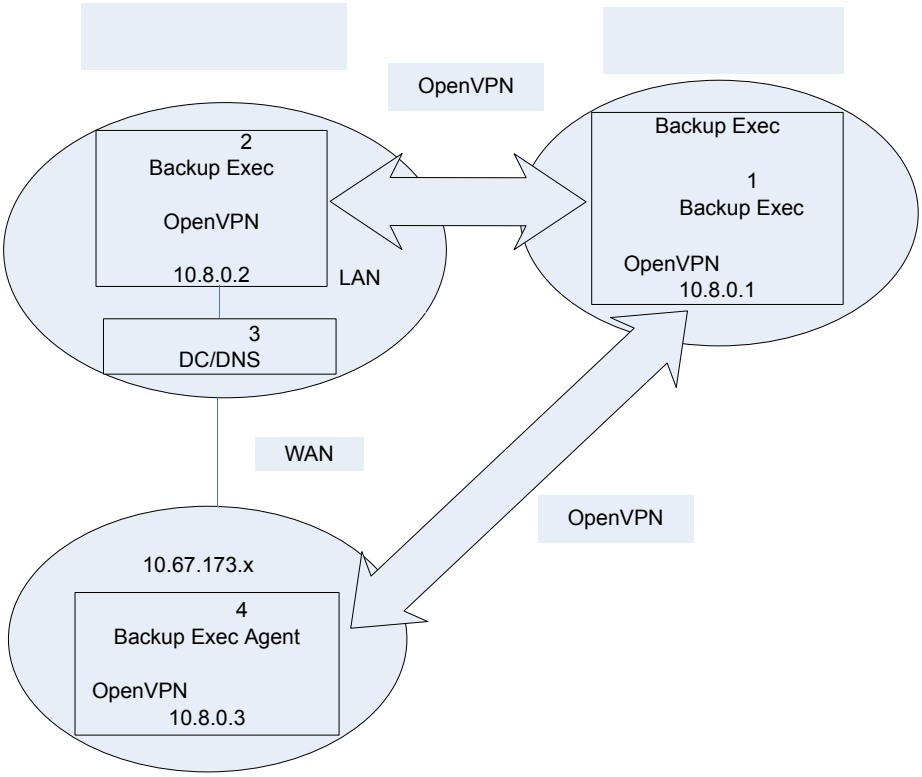
複数のクライアントの OpenVPN の設定について

複数のクライアントで使用する OpenVPN を設定できます。複雑なローカルネットワークがあるときは、複数のクライアントの VPN 設定を使用することが必要な場合があります。たとえば、複数のローカルサブネットを使用するとき、複数のクライアントの VPN 設定が有益な場合があります。

p.53 の「OpenVPN の設定について」を参照してください。

警告: OpenVPN はドメインコントローラにインストールしないでください。マルチホームドメインコントローラの設定は、Backup Exec のプライベートクラウドサービスではサポートされていません。

図 4-1　　複数のクライアントの VPN 設定



OpenVPN サーバーはプライベートクラウドのインスタンスです。クライアントはローカル LAN のコンピュータです。複数の OpenVPN のクライアントを使用する場合は、単一のクライアント設定に使用する共有キーのテキストファイルではなく、セキュリティ証明書を

使用する必要があります。複数クライアントの設定では、OpenVPN の各クライアントは個別のキーと証明書を持っています。

メモ: キーファイルは重要です。キーファイルが危害を受けた場合は、それを再生成する必要があります。証明機関 (CA) のキーファイルが危害を受けた場合は、その CA に基づいているすべてのキーを再生成する必要があります。

複数のクライアントの OpenVPN を設定するには、公開され利用可能な例を使って手順を実行します。次のサイトでは、OpenVPN の証明書と、複数の OpenVPN クライアントを設定するための完全な説明が提供されています。

http://www.runpcrun.com

http://openvpn.net

より複雑なネットワークのもう 1 つのオプションは、ローカルネットワークのゲートウェイのルーターで OpenVPN を使うことです。ローカルネットワークのゲートウェイのルーターは、OpenVPN のポイント間接続を提供します。他のローカルコンピュータは、追加の OpenVPN クライアントとコンピュータネットワークのルートを追加しないで、VPN に送信できます。OpenVPN のサポートについて詳しくは、ルーターの製造元にお問い合わせいただくか、マニュアルを参照してください。

またサードパーティ製ソフトウェアの組織は、OpenVPN のサポートを含むルーターのファームウェアの更新を提供しています。次のサイトで例を示します。

http://www.dd-wrt.com

複数のクライアントに OpenVPN を設定すれば、直接バックアップジョブを作成して実行し、それらのクライアントのデータをバックアップできます。直接バックアップジョブまたはバックアップ複製操作のバックアップ先として、プライベートクラウドのインスタンスを使うことができます。

ネットワーク上の問題のトラブルシューティング

Backup Exec のプライベートクラウドサービスでネットワーク上の問題がある場合は、OpenVPN のサーバーとクライアントが正常に接続できることを確認する必要があります。

ネットワーク上の問題をトラブルシューティングする方法

1. 一時的に Windows のファイアウォールをオフにするか、または Backup Exec のプライベートクラウドサービス設定のすべてのコンピュータに、適切な ICMP のファイアウォールの例外を追加します。
2. コンピュータ 1 (C1) とコンピュータ 2 (C2) の両方で、Windows サービスユーティリティを使用して、OpenVPN サービスを開始します。

3 C1 と C2 両方で、次のディレクトリの OpenVPN のログファイルを開き、各ファイルにテキスト「Initialization Sequence Completed」が含まれていることを確認します。

C:¥Program Files (X86)¥OpenVPN¥log

4 接続性をテストするために、C1、C2 とコンピュータ 3 (C3) から ping 10.8.0.1 と 10.8.0.2 を実行します。

5 C1 から、C2 のローカル IP アドレスと C3 のローカル IP アドレスに ping を実行します。

OpenVPN が接続されているとき、OpenVPN のローカルネットワークアダプタの DNS プロパティが、ローカルドメインの接尾辞を含んでいることを確認します。