Backup Exec 개인 클라우드 서비스

계획 및 배포 설명서

Symantec

목차

1 장

Backup Exec 개인 클라우드 서비스 소개

이 장의 내용은 다음과 같습니다.

Backup Exec 개인 클라우드 서비스

Backup Exec 개인 클라우드 서비스는 고객에게 관리형 백업 서비스를 제공하는 데 관심이 있는 관리형 서비스 제공업체(MSP)를 대상으로 합니다. Backup Exec 개인 클라우드 서비스를 통해 파트너는 데이터 센터 내의 백업 저장소를 "개인 클라우드" 구성으로 호스팅할 수 있습니다.

관리형 서비스 제공업체는 오프사이트 테이프 사본 관리를 대체하는 방안으로 인터넷을 통해 파트너 개인 클라우드에 백업 서비스를 제공할 수 있습니다. 백업이 암호화되고 중복 제거되기 때문에 WAN을 통해 안전하고 효율적으로 전송할 수 있습니다. 신속한 복원 기능을 전제로 계속 로컬 백업을 사용할 수 있습니다. 또한 Backup Exec 개인 클라우드 서비스를 통해 사용자는 클라우드로 직접 백업할 수 있습니다. 사용자는 클라우드에서 직접 전체 또는 세분화된 데이터를 복원할 수 있습니다.

또한 Backup Exec 개인 클라우드 서비스는 널리 분산된 네트워크를 보유한 Backup Exec 고객도 대상으로 합니다. 고객이 백업의 중복 사본을 원격 사무실에서 중앙 데이터 센터 개인 클라우드 위치에 있는 디스크 저장소 및 테이프 저장소로 보낼 수 있습니다.

다음 표에서는 Backup Exec 개인 클라우드 서비스를 이해하는 데 중요한 일부 Backup Exec 용어에 대해 설명합니다.

표 1-1 Backup Exec 용어

용어	정의
중복 제거 디스크 저장소	중복 제거 디스크 저장 장치는 Backup Exec 서버에 통합된 중복 제거를 제공합니다. **참고:** 클라우드에서 통합된 Backup Exec 중복 제거 저장 장치 대신 Symantec NetBackup 5000/5020 시리즈 중복 제거 저장 장비를 사용할 수 있습니다. 장비는 특히 큰 멀티테넌트 구성에 대해 확장성이 보다 뛰어난 옵션을 제공합니다.
최적화된 복제	중복 제거된 데이터를 같은 공급업체에서 제공하는 OpenStorage 장치 간에 직접 복사할 수 있는 복제 유형.
GRT(Granular Recovery Technology)	데이터베이스 백업에서 개별 항목을 복원할 수 있는 백업 옵션. 개별 항목을 별도로 백업하기 위해 한 항목을 복구할 필요가 없습니다.

6페이지의 "Backup Exec 개인 클라우드 서비스에 대한 보안 고려 사항" 참조

8페이지의 "Backup Exec 개인 클라우드 서비스에 대한 시스템 요구 사항" 참조

11페이지의 "Backup Exec 개인 클라우드 서비스 구성" 참조

13페이지의 "Backup Exec 개인 클라우드 서비스 구성" 참조

Backup Exec 개인 클라우드 서비스에 대한 보안 고려 사항

Backup Exec 개인 클라우드 서비스는 Backup Exec의 현재 작업 및 리소스 인증 정보 모델을 사용하여 보안 환경을 제공합니다. 또한 VPN 솔루션을 사용하여 고객 위치와 데이터 센터 간에 보안 네트워크 연결을 사용하는 것이 좋습니다. 다양한 IPsec, SSL 계층 및 기타 VPN 솔루션이 제공됩니다.

여러 고객을 지원하는 구성을 사용하는 경우 고객의 네트워크가 서로 분리된 상태를 유지하려면 VLAN 또는 라우팅 제한 사항을 사용해야 합니다.

선호하는 임의의 VPN 솔루션을 사용할 수 있습니다. 이 설명서에서는 OpenVPN에 대한 참조 구성 지침을 제공합니다. OpenVPN SSL VPN 공개 소스 패키지는 개인 클라우드 Backup Exec 인스턴스와 로컬 Backup Exec 서버 간에 암호화된 보안 연결을 제공합니다. 일반적으로 이 구성 요소를 사용하려면 방화벽에서 기본 포트 1194를 열어야 합니다. 하지만 OpenVPN을 통해 다른 포트를 사용하도록 구성할 수 있습니다. OpenVPN은 키 기반 인증 방법과 인증서 기반 인증 방법을 모두 제공합니다. 이 문서에서는 두 가지 방법을 모두 구성할 수 있는 참조를 제공합니다.

5페이지의 "Backup Exec 개인 클라우드 서비스" 참조

49페이지의 "OpenVPN 구성" 참조

멀티테넌트 Backup Exec 서버 구성에는 고려해야 할 추가 보안 요구 사항이 포함됩니다.

7페이지의 "멀티테넌트 Backup Exec 서버 구성 보안 요구 사항" 참조

멀티테넌트 Backup Exec 서버 구성 보안 요구 사항

개인 클라우드에서는 단일 Backup Exec 서버를 통해 여러 고객 또는 테넌트를 안전하게 지원할 수 있도록 Backup Exec을 구성할 수 있습니다. 멀티테넌트 Backup Exec 서버에는 여러 고객의 공유 컨텐츠가 포함되어 있기 때문에 멀티테넌트 Backup Exec 서버를 사용할 때는 추가적인 보안 예방 조치를 취해야 합니다.

15페이지의 "멀티테넌트 클라우드 Backup Exec 서버 구성 정보" 참조

6페이지의 "Backup Exec 개인 클라우드 서비스에 대한 보안 고려 사항" 참조

멀티테넌트 Backup Exec 서버를 구성할 때 고려해야 하는 보안 요구 사항은 다음과 같습니다.

- 관리되는 온사이트 Backup Exec 서버는 실제 시스템에 설치해야 합니다.
- 관리되는 온사이트 Backup Exec 서버에서 Microsoft Windows BitLocker 기능을 시스템 볼륨에 설정하고 활성화해야 합니다.
  BitLocker 암호는 그 어떤 고객에게도 노출되어서는 안 됩니다. BitLocker 대신 하드웨어 디스크 암호화 솔루션을 사용할 수도 있습니다.
- 개인 클라우드에 있는 멀티테넌트 Backup Exec 서버와 온사이트 Backup Exec 서버는 서비스 제공업체 도메인의 구성원이어야 합니다.
  Backup Exec 서버에서 고객의 로그온 액세스를 허용하지 않아야 합니다. 추가적인 격리가 필요한 경우 각 고객의 관리되는 Backup Exec 서버를 서로 다른 서비스 제공업체 하위 도메인에 저장할 수 있습니다.
- 관리되는 온사이트 Backup Exec 서버에 대한 서비스 제공업체 도메인 인증 정보는 도메인 관리자가 아니라 로컬 관리자의 인증 정보여야 합니다.
- 멀티테넌트 클라우드 서버의 중복 제거 디스크 저장 장치에 클라이언트 측 중복 제거 기능이 설정되어 있으면 안 됩니다.
- 관리되는 온사이트 Backup Exec 서버를 설치할 때 **복원할 카탈로그 및 백업 세트에 무제한 액세스** 옵션을 선택하면 안 됩니다. **중앙에서 관리되는 Backup Exec 서버** 옵션만 사용하여 설치해야 합니다.
- 가능한 경우, 관리되는 온사이트 Backup Exec 서버에 대해 2단계 인증을 사용하여 보안을 강화할 수 있습니다.
  다음 VeriSign VIP Authentication Service를 사용하는 것이 좋습니다.
  http://www.verisign.com/authentication/two-factor-authentication/vip-authentication/index.html

경고: 다음과 같은 권장 사항을 따르면 공유 Backup Exec 네트워크 및 저장 장치에 대해 일정 수준의 액세스 보안만 제공됩니다. 관리되는 Backup Exec 서버에 대한 실제 액세스 권한을 가진 사용자가 악의적인 의도로 접근할 경우 이론적으로 이 사용자는 이러한 보안 수단을 뚫을 수 있습니다. 따라서 관리되는 온사이트 Backup Exec 서버에 대해 추가적인 실제 액세스 보호 수단을 사용해야 합니다.

Backup Exec 개인 클라우드 서비스에 대한 시스템 요구 사항

다음 표에서는 Backup Exec 개인 클라우드 서비스를 실행하기 위한 최소 시스템 요구 사항과 권장 사항을 보여 줍니다.

표 1-2 Backup Exec 개인 클라우드 서비스에 대한 시스템 요구 사항

요구 사항	설명
Backup Exec 서버	세 가지 방법 중 하나로 Backup Exec 개인 클라우드 서비스를 구성할 수 있습니다. 13페이지의 "Backup Exec 개인 클라우드 서비스 구성" 참조 클라우드의 모든 Backup Exec 서버에 Backup Exec Deduplication Option이 포함되어야 합니다. 로컬 서버는 Backup Exec 2012에 대한 요구 사항만 준수하면 됩니다. 다음 URL에서 호환되는 운영 체제, 플랫폼 및 응용 프로그램 목록을 확인할 수 있습니다. http://entsupport.symantec.com/umi/V-269-1
Deduplication Option 라이센스	개인 클라우드 서버 및 로컬 Backup Exec 서버에서 모두 Symantec Backup Exec Deduplication Option을 설치해야 합니다. 로컬 Backup Exec 서버에서 중복 제거 디스크 저장 장치를 생성할 필요가 없습니다. 하지만 클라우드의 서버에 있는 공유 중복 제거 디스크 저장 장치에 액세스하려면 로컬 Backup Exec 서버에 Deduplication Option을 설치해야 합니다. 모든 구성에는 클라우드 Backup Exec 서버에 중복 제거 디스크 저장 장치가 있어야 합니다.

표 1-2 Backup Exec 개인 클라우드 서비스에 대한 시스템 요구 사항 (계속)

요구 사항	설명
Central Admin Server Option 라이센스	멀티테넌트 또는 오프사이트 복사 구성 중 하나를 사용하는 경우 로컬 시스템 또는 클라우드 시스템에 Symantec Backup Exec Enterprise Server Option과 Central Admin Server Option을 설치해야 합니다.
활성 인터넷 연결	개인 클라우드 중복 제거 디스크 저장 장치에 데이터를 전송하려면 인터넷에 연결되어 있어야 합니다.
VPN(가상 사설 네트워크)	VPN 솔루션을 사용하여 고객 위치와 데이터 센터 간에 보안 네트워크 연결을 사용하는 것이 좋습니다. 다양한 IPsec 및 SSL 계층 VPN 솔루션을 사용할 수 있습니다. 이 설명서에서는 OpenVPN에 대한 구성 지침을 제공합니다. OpenVPN SSL VPN 공개 소스 패키지는 개인 클라우드 Backup Exec 인스턴스와 로컬 Backup Exec 서버 간에 암호화된 보안 연결을 제공합니다.

2장

Backup Exec 개인 클라우드 서비스 구성

이 장의 내용은 다음과 같습니다.

Backup Exec 개인 클라우드 서비스 구성

Backup Exec 개인 클라우드 서비스를 구성하려면 다음 단계를 완료해야 합니다.

표 2-1 Backup Exec 개인 클라우드 서비스 구성 방법

단계	설명
1단계	개인 클라우드 Backup Exec 서버 인스턴스와 로컬 네트워크에서 실행되는 모든 시스템 간에 VPN을 구성해야 합니다. 49페이지의 "OpenVPN 구성" 참조 55페이지의 "클라이언트에 대해 OpenVPN 구성" 참조

표 2-1 Backup Exec 개인 클라우드 서비스 구성 방법 (계속)

단계	설명
2단계	요구 사항에 가장 적합한 Backup Exec 개인 클라우드 서비스 구성을 고려하여 선택하십시오. 여러 고객을 대상으로 하는 단일 멀티테넌트 구성을 선택할 수 있습니다. 또는 각 고객을 대상으로 하는 클라우드 구성 또는 직접 백업 구성에 대해 전용 오프사이트 복사를 사용하도록 선택할 수 있습니다. 13페이지의 "Backup Exec 개인 클라우드 서비스 구성" 참조 Backup Exec 개인 클라우드 서비스를 구성해야 합니다. 19페이지의 "클라우드에 멀티테넌트 또는 오프사이트 복사 구성 설정" 참조 28페이지의 "직접 백업 구성 설정" 참조
3단계	VPN 및 Backup Exec을 구성한 후 Backup Exec 개인 클라우드 서비스에서 작업을 시작할 수 있습니다. 33페이지의 "오프사이트 복사 구성에 대한 Backup Exec 개인 클라우드 서비스 사용" 참조 39페이지의 "Backup Exec 개인 클라우드 서비스 및 직접 백업 구성 사용" 참조

표 2-1 Backup Exec 개인 클라우드 서비스 구성 방법 (계속)

단계	설명
4단계	포트 제한과 함께 VPN 게이트웨이를 사용할 경우 온사이트 및 클라우드 VPN 게이트웨이 모두에서 포트 예외를 허용해야 할 수 있습니다. 포트 예외를 통해 클라우드에 있는 Backup Exec Backup Exec 서버는 온사이트 Backup Exec 서버 및 에이전트와 통신할 수 있습니다. 또한 동적으로 할당된 포트에서 고정 포트로 CAS Backup Exec SQL 포트를 변경해야 합니다. **참고:** OpenVPN을 사용할 경우 게이트웨이 방화벽 포트 예외를 구성할 필요가 없을 수도 있습니다. OpenVPN은 일반적으로 방화벽을 통해 터널로 구성됩니다. 다음의 Backup Exec 지원 문서는 Backup Exec에 필요한 모든 포트 번호와 열려야 하는 포트 목록이 나와 있습니다. 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 다음 Backup Exec 지원 문서는 SQL 고정 포트의 구성 방법에 대해 자세히 설명합니다. http://www.symantec.com/business/support/index?page=content&id=HOWTO22985

Backup Exec 개인 클라우드 서비스 구성

다음 네 가지 방법 중 하나로 Backup Exec 개인 클라우드 서비스를 구성할 수 있습니다.

표 2-2 Backup Exec 개인 클라우드 서비스에 대한 특정 구성

구성 유형	세부 정보
멀티테넌트 클라우드 Backup Exec 서버	멀티테넌트 클라우드 Backup Exec 서버 구성은 개인 클라우드에 위치한 Backup Exec 서버 또는 중앙 관리 서버에 오프사이트 복사 및 직접 백업을 제공합니다. 단일 개인 클라우드 Backup Exec 서버를 사용하여 여러 고객을 위해 데이터를 백업할 수 있습니다. 15페이지의 "멀티테넌트 클라우드 Backup Exec 서버 구성 정보" 참조
관리되는 클라우드 Backup Exec 서버에 오프사이트 복사	관리되는 클라우드 Backup Exec 서버에 오프사이트 복사 구성은 관리되는 Backup Exec 서버, 중앙 관리 서버 및 도메인 컨트롤러를 사용합니다. 이 구성은 개인 클라우드 내에 위치한 관리되는 Backup Exec 서버에 오프사이트 복사 기능을 제공합니다. 이 구성을 사용하려면 고객당 하나의 관리되는 Backup Exec 서버가 필요합니다. 17페이지의 "클라우드 관리되는 Backup Exec 서버 구성에 오프사이트 복사" 참조
클라우드 중앙 관리 서버에 오프사이트 복사	클라우드 중앙 관리 서버에 오프사이트 복사 구성은 중앙 관리 서버와 관리되는 Backup Exec 서버의 위치가 반대라는 점을 제외하고 첫 번째 구성과 유사합니다. 이 구성은 개인 클라우드에 있는 중앙 관리 서버에 오프사이트 복사 기능을 제공합니다. 이 구성을 사용하려면 고객당 하나의 중앙 관리 서버가 필요합니다. 18페이지의 "클라우드 중앙 관리 서버에 오프사이트 복사 구성" 참조
직접 백업	직접 백업 구성은 관리되는 Backup Exec 서버 또는 중앙 관리 서버 대신 Backup Exec Agent for Windows 또는 Backup Exec Agent for Linux를 사용합니다. 이 구성은 개인 클라우에 있는 Backup Exec 서버를 사용하여 직접 백업 기능을 제공합니다. 이 구성을 사용하려면 고객당 하나의 Backup Exec 서버가 필요합니다. 19페이지의 "직접 백업 구성" 참조

49페이지의 "OpenVPN 구성" 참조

19페이지의 "클라우드에 멀티테넌트 또는 오프사이트 복사 구성 설정" 참조

28페이지의 "직접 백업 구성 설정" 참조

멀티테넌트 클라우드 Backup Exec 서버 구성 정보

멀티테넌트 클라우드 Backup Exec 서버 구성에는 여러 대의 시스템이 포함됩니다.

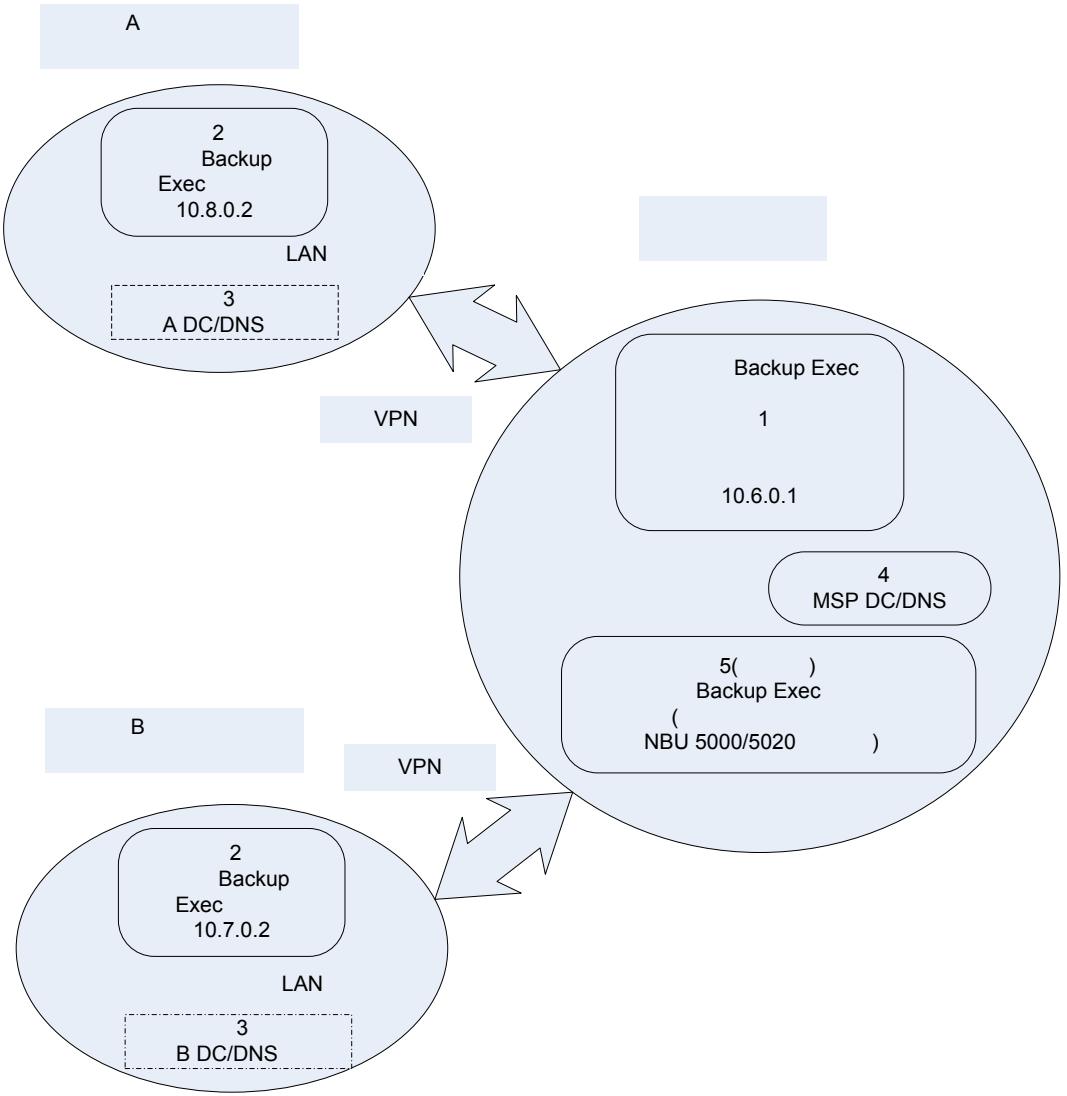
표 2-3 멀티테넌트 클라우드 Backup Exec 서버 구성

시스템	역할
시스템 1	첫 번째 시스템(C1)은 Backup Exec 2012가 설치되어 있는 Windows 64비트 서버입니다. C1은 중앙 관리 서버로 구성되며 개인 클라우드에 있습니다.
시스템 2	두 번째 시스템(C2)은 Backup Exec 2012가 설치된 Windows 서버입니다. C2는 LAN에 있는 관리되는 Backup Exec 서버이며 서비스 제공업체의 클라우드 도메인(C4)의 구성원입니다. **참고:** 로컬 중복 제거 디스크 저장 장치가 필요하지 않을 경우 C2에 32비트 로컬 Backup Exec 서버를 사용할 수 있습니다.
시스템 3	세 번째 시스템(C3)은 도메인 컨트롤러 및 DNS입니다. 각 고객 위치에 C3 시스템을 구성해야 합니다.
시스템 4	네 번째 시스템(C4)은 개인 클라우드에 있는 도메인 컨트롤러 및 DNS입니다.
시스템 5(선택 사항)	다섯 번째 시스템(C5)은 선택 사항이지만 권장되는, 관리되는 Backup Exec 서버입니다. C5에는 추가 내결함성 및 신뢰성을 위해 C1 시스템의 중복 제거 저장 장치를 복제하는 데 사용할 수 있는 중복 제거 저장소 폴더입니다. C5는 C1과 함께 개인 클라우드에 함께 위치할 수 있거나 다른 실제 위치에 있을 수 있습니다. NetBackup 5000/5020 시리즈 중복 제거 저장 장비를 배치된 C5 시스템의 대안인 클라우드 Backup Exec 서버의 OST 장치로 구성할 수 있습니다.

이 구성을 사용하면 개인 클라우드의 데이터 센터 내에서 Backup Exec 작업을 모두 관리할 수 있습니다. 하지만 중앙 관리 서버와 관리되는 Backup Exec 서버 간의 네트워크 연결은 항상 활성 상태여야 합니다. 로컬에서 작업을 실행하는 경우에도 네트워크에 연결되어 있어야 합니다.

경고: 단일 클라우드 Backup Exec 서버로 여러 고객을 지원하려면 C1, C2, C4, C5가 액세스할 수 있는 유일한 도메인에 포함되어야 합니다. 보안 위험을 야기할 수 있는 실수 또는 악성 활동을 방지하려면 고객에게 C2에 대한 모든 로그온 액세스 유형을 허용하면 안 됩니다.

그림 2-1 멀티테넌트 클라우드 Backup Exec 서버



13페이지의 "Backup Exec 개인 클라우드 서비스 구성" 참조

클라우드 관리되는 Backup Exec 서버 구성에 오프사이트 복사

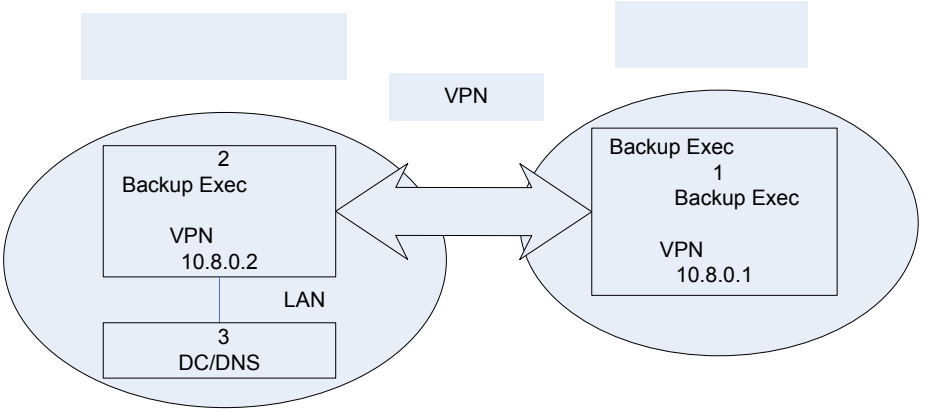
클라우드 관리되는 Backup Exec 서버에 오프사이트 복사 구성에는 3대의 시스템이 포함됩니다.

표 2-4 클라우드 관리되는 Backup Exec 서버 구성에 오프사이트 복사 구성

시스템	역할
시스템 1	첫 번째 시스템(C1)은 Backup Exec 2012가 설치되어 있는 Windows 64비트 서버입니다. C1은 관리되는 Backup Exec 서버로 구성되며 개인 클라우드에 있습니다.
시스템 2	두 번째 시스템(C2)은 Backup Exec 2012가 설치되어 있는 Windows 64비트 서버입니다. C2는 LAN에 있는 중앙 관리 서버입니다. **참고:** 로컬 중복 제거 디스크 저장 장치를 사용하지 않으려는 경우 C2에 대해 32비트 로컬 Backup Exec 서버를 사용할 수 있습니다.
시스템 3	세 번째 시스템(C3)은 도메인 컨트롤러 및 DNS입니다.

중앙 관리 서버와 관리되는 Backup Exec 서버가 항상 네트워크로 연결되어야 하는 것은 아닙니다. 개인 클라우드의 관리되는 Backup Exec 서버와 관련된 작업을 실행하는 경우에만 네트워크 연결이 필요합니다. 로컬 작업을 실행하는 경우에는 네트워크 연결이 필요 없습니다.

그림 2-2 클라우드 관리되는 Backup Exec 서버 구성에 오프사이트 복사



13페이지의 "Backup Exec 개인 클라우드 서비스 구성" 참조

클라우드 중앙 관리 서버에 오프사이트 복사 구성

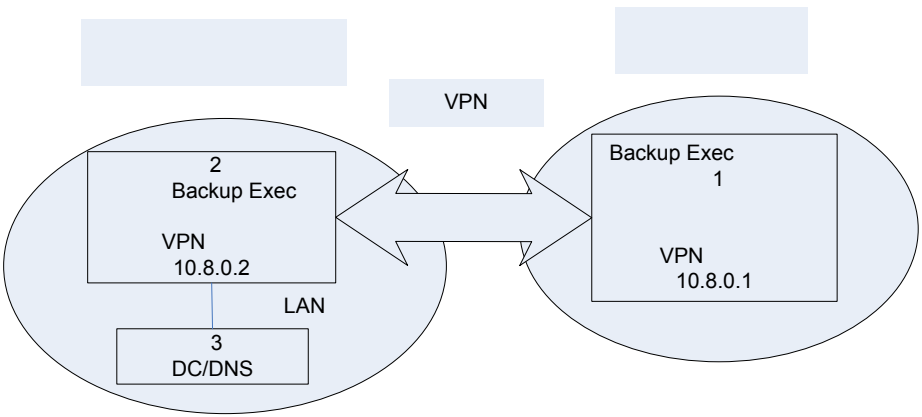
클라우드 중앙 관리 서버에 오프사이트 복사 구성에는 시스템 3대가 포함됩니다.

표 2-5 클라우드 중앙 관리 서버에 오프사이트 복사 구성

시스템	역할
시스템 1	첫 번째 시스템(C1)은 Backup Exec 2012가 설치되어 있는 Windows 64비트 서버입니다. C1은 중앙 관리 서버로 구성되며 개인 클라우드에 있습니다.
시스템 2	두 번째 시스템(C2)은 Backup Exec 2012가 설치되어 있는 Windows 64비트 서버입니다. C2는 LAN에 있는 관리되는 Backup Exec 서버입니다. **참고:** 로컬 중복 제거 디스크 저장 장치를 사용하지 않으려는 경우 C2에 대해 32비트 로컬 Backup Exec 서버를 사용할 수 있습니다.
시스템 3	세 번째 시스템(C3)은 도메인 컨트롤러 및 DNS입니다.

이 구성을 사용하면 개인 클라우드의 데이터 센터 내에서 Backup Exec 작업을 모두 관리할 수 있습니다. 하지만 중앙 관리 서버와 관리되는 Backup Exec 서버 간의 네트워크 연결이 항상 활성 상태여야 합니다. 로컬에서 작업을 실행하는 경우에도 네트워크에 연결되어 있어야 합니다.

그림 2-3 클라우드 중앙 관리 서버에 오프사이트 복사



13페이지의 "Backup Exec 개인 클라우드 서비스 구성" 참조

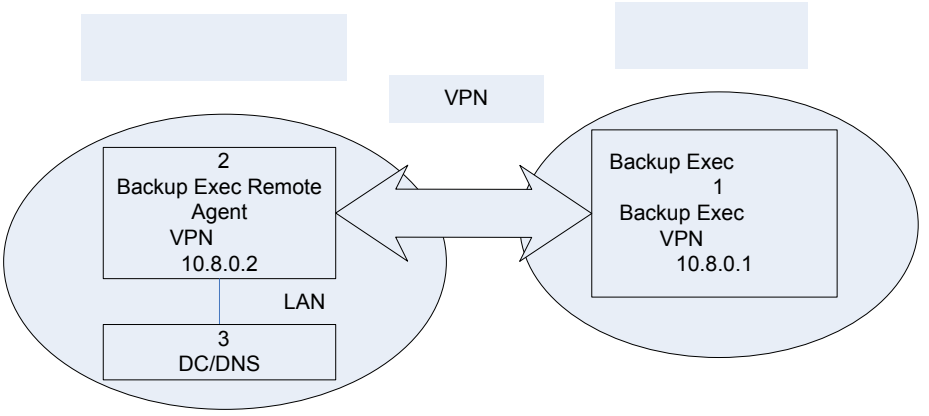
직접 백업 구성

직접 백업 구성을 사용하려면 최소한 시스템 3대가 필요합니다.

표 2-6 직접 백업 구성

시스템	역할
시스템 1	첫 번째 시스템(C1)은 개인 클라우드 데이터 센터에 있는 Windows 64비트 서버 Backup Exec 2012 서버입니다.
시스템 2	두 번째 시스템(C2)은 LAN에 있는 Agent for Windows 또는 Agent for Linux 클라이언트입니다. 에이전트 클라이언트 시스템을 여러 대 구성할 수 있습니다.
시스템 3	세 번째 시스템(C3)은 도메인 컨트롤러 및 DNS입니다.

그림 2-4 직접 백업



13페이지의 "Backup Exec 개인 클라우드 서비스 구성" 참조

클라우드에 멀티테넌트 또는 오프사이트 복사 구성 설정

개인 클라우드 서버에 VPN을 구성한 후 Backup Exec 서버를 구성해야 합니다.

11페이지의 "Backup Exec 개인 클라우드 서비스 구성" 참조

멀티테넌트 구성 또는 클라우드에 오프사이트 복사 구성 두 개 중 하나를 선택할 수 있습니다.

15페이지의 "멀티테넌트 클라우드 Backup Exec 서버 구성 정보" 참조

17페이지의 "클라우드 관리되는 Backup Exec 서버 구성에 오프사이트 복사" 참조

18페이지의 "클라우드 중앙 관리 서버에 오프사이트 복사 구성" 참조

표 2-7 클라우드에 오프사이트 복사 구성을 구성하는 방법

단계	설명
1단계	Backup Exec 중앙 관리 서버를 설치하십시오. 20페이지의 "Backup Exec 중앙 관리 서버 설치" 참조
2단계	관리되는 Backup Exec 서버를 설치하십시오. 22페이지의 "관리되는 Backup Exec 서버 설치" 참조
3단계	저장 장치를 구성하십시오. 23페이지의 "멀티테넌트 및 오프사이트 복사 구성에 대한 저장 장치 설정" 참조
4단계	데이터가 포함된 중복 제거 디스크 저장 장치를 시드하십시오. 25페이지의 "오프사이트 복사 구성에 대한 중복 제거 디스크 저장 장치 시드" 참조

Backup Exec 중앙 관리 서버 설치

Backup Exec 중앙 관리 서버로 사용되는 시스템에 Backup Exec for Windows Servers를 설치해야 합니다.

19페이지의 "클라우드에 멀티테넌트 또는 오프사이트 복사 구성 설정" 참조

멀티테넌트 클라우드 Backup Exec 서버 구성을 사용할 경우 클라우드 Backup Exec 서버는 중앙 관리 서버(시스템 1 또는 C1)로 설치해야 합니다.

관리되는 클라우드 Backup Exec 서버 구성에 오프사이트 복사를 사용하는 경우 중앙 관리 서버는 로컬 사무실 Backup Exec 서버(시스템 2 또는 C2)에 설치됩니다. 그렇지 않으면 중앙 관리 서버는 클라우드 중앙 관리 서버 구성에 오프사이트 복사를 위해 클라우드 Backup Exec 서버(시스템 1 또는 C1)로 설치됩니다.

도메인에 중앙 관리 서버를 추가해야 합니다. 중앙 관리 서버에 CASO(Central Admin Server Option)와 함께 Enterprise Server Option을 설치합니다.

표 2-8 Backup Exec 중앙 관리 서버를 설치하는 방법

단계	설명
1단계	멀티테넌트 Backup Exec 서버를 구성하려면 클라우드 도메인에 Backup Exec 서버를 추가하십시오. 멀티테넌트 Backup Exec 서버 구성을 제외하고 구성하려면 다음 단계를 완료하여 로컬 도메인에 Backup Exec 서버를 추가하십시오. ■ Windows의 시스템 속성 대화 상자를 사용하여 도메인에 서버를 추가하십시오. ■ 확인 메시지가 표시되면 시스템을 재시작하십시오.
2단계	서버가 재시작된 후 로컬 Backup Exec 인스턴스에 대한 관리자 권한을 보유하려는 도메인 계정을 사용하여 로그온하십시오.
3단계	적절한 라이센스 키를 사용하여 Backup Exec 2012를 설치하십시오. Backup Exec 설치에 대한 자세한 내용은 Symantec Backup Exec 관리자 설명서를 참조하십시오. Backup Exec 파트너는 Symantec PartnerNet 웹 사이트의 다음 링크에서 라이센싱 정보를 얻을 수 있습니다. https://partnernet.symantec.com/Partnercontent/Login.jsp
4단계	Backup Exec을 설치할 때 Enterprise Server Option을 CASO(Central Admin Server Option)와 함께 포함하십시오. CASO 설치에 대한 자세한 내용은 Symantec Backup Exec 관리자 설명서를 참조하십시오. 클라우드 중앙 관리 서버 구성에 멀티테넌트 또는 오프사이트 복사를 사용하는 경우 중복 제거 옵션을 설치하십시오. 관리되는 클라우드 Backup Exec 서버에 대한 오프사이트 복사 구성의 경우 중앙 관리 서버에서 로컬 중복 제거 디스크 저장 장치의 사용은 선택 사항입니다.
5단계	Backup Exec을 설치할 때 기본 시스템 로그온 계정에 대해 도메인 인증 정보를 사용하십시오.

표 2-8 Backup Exec 중앙 관리 서버를 설치하는 방법 (계속)

단계	설명
6단계	클라우드에 대한 증분 Exchange GRT 복제 백업 작업을 실행하려면 설치 완료 시 다음 레지스트리 값을 **1**로 설정하십시오. 레지스트리 값을 변경하면 Backup Exec 서버의 중복 제거 디스크 저장 장치의 GRT-to-GRT 복제 복사 기능이 비활성화됩니다. dword HKEY LOCAL MACHINE\SOFTWARE\Symantec\Backup Exec for Windows\Backup Exec\Engine\Misc\DisablePDI2PDISetCopy 이 시스템은 이제 WAN 전체에서 관리되는 Backup Exec 서버를 제어하는 중앙 관리 서버입니다. 오프사이트 복사 GRT(Granular Recovery Technology)의 제한에 대한 자세한 내용은 다음 항목에서 확인하십시오. 47페이지의 "오프사이트 복사의 Granular Recovery Technology 제한" 참조

관리되는 Backup Exec 서버 설치

관리되는 Backup Exec 서버를 설치해야 합니다. 관리되는 클라우드 Backup Exec 서버 구성에 오프사이트 복사를 사용하는 경우 관리되는 Backup Exec 서버는 클라우드 Backup Exec 서버(시스템 1 - C1)로 설치됩니다. 그렇지 않으면 관리되는 Backup Exec 서버는 로컬 사무실 Backup Exec 서버(시스템 2 - C2)에 설치됩니다.

19페이지의 "클라우드에 멀티테넌트 또는 오프사이트 복사 구성 설정" 참조

관리되는 Backup Exec 서버를 설치하려면

1 다음 중 하나를 수행하십시오.

멀티테넌트 구성의 경우	클라우드 도메인에 Backup Exec 서버를 추가하십시오.
다른 구성의 경우	다음 단계를 완료하여 로컬 도메인에 Backup Exec 서버를 추가하십시오. ■ Windows의 시스템 속성 대화 상자를 사용하여 도메인에 서버를 추가하십시오. ■ 확인 메시지가 표시되면 시스템을 재시작하십시오.

2 서버가 재시작된 후 로컬 Backup Exec 서버에 대한 관리자 권한을 가진 도메인 계정을 사용하여 로그온하십시오.

3 서버에 Backup Exec 2012를 설치하고 **관리되는 Backup Exec 서버** 설치 옵션을 선택하십시오.

4 프롬프트에서 중앙 관리 서버를 설치하는 데 사용한 것과 동일한 시스템 로그온 계정 인증 정보를 지정하십시오.

5 관리되는 클라우드 Backup Exec 서버 구성에 오프사이트 복사를 사용하려는 경우 **중복 제거 옵션**을 선택하십시오.

클라우드 중앙 관리 서버에 대한 오프사이트 복사 구성의 경우 관리되는 Backup Exec 서버의 로컬 중복 제거 디스크 저장 장치 사용은 선택 사항입니다.

6 Backup Exec에서 중앙 관리 서버를 묻는 메시지가 표시되면 로컬 Backup Exec 중앙 관리 서버에 대한 정보를 입력하십시오.

7 **중앙에서 관리되는 Backup Exec 서버** 옵션을 선택하십시오.

멀티테넌트 구성을 사용하는 경우 **복원할 카탈로그 및 백업 세트에 무제한 액세스**를 선택하지 마십시오.

8 클라우드에 대한 증분 Exchange GRT 복제 백업 작업을 실행하려면 설치 완료 시 다음 레지스트리 값을 **1**로 설정하십시오.

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

레지스트리 값을 변경하면 Backup Exec 서버의 중복 제거 디스크 저장 장치의 GRT-to-GRT 복제 복사 기능이 비활성화됩니다.

9 중앙 관리 서버에서 Backup Exec을 여십시오.

10 **저장소** 탭을 선택한 다음 개인 클라우드 데이터 센터에 있는 Backup Exec 서버를 두 번 누르십시오.

11 왼쪽 창에서 **설정**을 누르십시오.

12 **개인 클라우드 서버** 필드에서 **실행**을 선택하십시오.

멀티테넌트 및 오프사이트 복사 구성에 대한 저장 장치 설정

개인 클라우드에 백업 작업을 실행하려면 먼저 저장 장치를 구성해야 합니다.

19페이지의 "클라우드에 멀티테넌트 또는 오프사이트 복사 구성 설정" 참조

표 2-9 오프사이트 복사 구성에 대한 저장 장치를 설정하는 방법

단계	설명
1단계	로컬 시스템 2(C2)에 새 로컬 디스크 저장 장치를 생성하십시오. 원할 경우 중복 제거 디스크 저장 장치를 생성할 수 있습니다. 저장 장치 생성에 대한 자세한 내용은 Symantec Backup Exec 관리자 설명서를 참조하십시오.

표 2-9 오프사이트 복사 구성에 대한 저장 장치를 설정하는 방법 (계속)

단계	설명
2단계	개인 클라우드 Backup Exec 인스턴스에 새 중복 제거 디스크 저장 장치를 생성하십시오. 멀티테넌트 구성의 경우 통합 중복 제거 저장소를 사용하는 대신 NetBackup 5000/5020 시리즈 중복 제거 저장 장비를 구성할 수 있습니다. 멀티테넌트 중앙 관리 서버에서 OST 저장 장치로 장비를 구성하십시오. 중복 제거 디스크 저장 장치 생성에 대한 자세한 내용은 Symantec Backup Exec 관리자 설명서를 참조하십시오. 멀티테넌트 구성을 사용하는 경우 다음 단계를 완료하여 개인 클라우드 중복 제거 디스크 저장 장치의 클라이언트 측 중복 제거 실행을 중지해야 합니다. ■ **저장소** 탭에서 개인 클라우드 Backup Exec 서버의 중복 제거 디스크 저장 장치를 두 번 누르십시오. ■ **속성**을 선택하십시오. ■ **클라이언트 측 중복 제거** 필드에서 **실행 중지**를 선택하십시오. ■ Backup Exec 서버의 서비스를 재시작하십시오. 가능한 경우 중복 제거 디스크 저장 장치의 전용 볼륨을 사용하는 것이 좋습니다. 로컬 중복 제거 디스크 저장 장치(생성한 경우)와 쉽게 구분할 수 있도록 중복 제거 디스크 저장 장치에 고유 이름을 지정하십시오.
3단계	개인 클라우드 중복 제거 디스크 저장 장치에서 움직이지 않는 데이터를 암호화하려면 **예를 선택하고 이 중복 제거 디스크 저장 장치로 전송 중에 새로운 중복 제거 디스크 저장 장치를 구성할 경우** 데이터가 해당 위치에 저장되는 동안 데이터를 암호화하십시오. 기존 중복 제거 장치의 경우 중복 제거 장치 속성의 **암호화** 필드를 수정할 수 있습니다. **참고:** VPN은 로컬 Backup Exec 서버와 클라우드 Backup Exec 서버 간에 전송 중인 데이터를 암호화합니다.
4단계	새 클라우드 중복 제거 저장 장치를 로컬 Backup Exec 시스템과 공유하십시오. 중복 제거 디스크 저장 장치 공유에 대한 자세한 내용은 Symantec Backup Exec 관리자 설명서를 참조하십시오.
5단계	Backup Exec 서비스 관리자를 사용하여 로컬 Backup Exec 서버에서 모든 Backup Exec 서비스를 중지하고 재시작하십시오. 이제 클라우드 중복 제거 저장 장치를 로컬 Backup Exec 서버와 공유하는 프로세스가 완료되었습니다. 개인 클라우드 중복 제거 디스크 저장 장치가 표시되고 C1과 C2에서 모두 액세스할 수 있어야 합니다.

표 2-9 오프사이트 복사 구성에 대한 저장 장치를 설정하는 방법 (계속)

단계	설명
6단계(선택 사항)	멀티테넌트 구성의 경우 클라우드의 관리되는 Backup Exec 서버를 중복 제거 저장 장치와 함께 추가로 설치할 수 있습니다. 추가 관리되는 Backup Exec 서버는 주 클라우드 Backup Exec 서버와 공유하여 주 서버의 중복 제거 저장 장치를 복제할 수 있습니다. NetBackup 5000/5020 시리즈 중복 제거 저장 장비를 추가 관리되는 Backup Exec 서버의 대안으로 설치할 수 있습니다. 장비를 복제에 사용할 수 있습니다. 주 클라우드 Backup Exec 서버의 OST 저장 장치로 장비를 추가하십시오. **경고:** 이 선택적 구성 중 하나에 대해 클라이언트 측 중복 제거를 실행 중지해야 합니다.

오프사이트 복사 구성에 대한 중복 제거 디스크 저장 장치 시드

인터넷을 통한 긴 전송 시간을 방지하기 위해 시작하는 데 필요한 데이터가 포함된 중복 제거 디스크 저장 장치를 클라우드에 시드할 수 있습니다. 중복 제거 디스크 저장 장치 시드는 초기 구성 파일이나 백업 세트를 중복 제거 디스크 저장 장치에 배치하여 사용 준비를 하는 프로세스입니다. 전송 시간은 복사하여 개인 클라우드 Backup Exec 인스턴스로 백업할 데이터 양에 따라 달라집니다.

데이터 유형에 따라 다음 두 가지 방법 중 하나를 사용하여 초기 데이터를 시드할 수 있습니다.

- 시스템 상태 운영 체제 백업을 사용하여 중복 제거 디스크 저장 장치를 시드할 수 있습니다. 개인 클라우드에서 실행 중인 다른 시스템의 시스템 상태 데이터에 대해 복제 백업 작업을 실행하여 중복 제거 디스크 저장 장치를 시드합니다. 백업하려는 로컬 시스템과 동일한 운영 체제를 실행하는 시스템에 대한 시스템 상태 데이터를 백업합니다.
  25페이지의 “오프사이트 복사 구성에 대한 운영 체제 파일 시드” 참조
- 로컬 Backup Exec 서버의 관련 데이터와 함께 백업 세트가 포함된 실제 전송 드라이브를 개인 클라우드 데이터 센터로 보낼 수 있습니다.
  26페이지의 “전송 드라이브를 사용하여 오프사이트 복사 구성에 대한 중복 제거 디스크 저장 장치 시드” 참조

오프사이트 복사 구성에 대한 운영 체제 파일 시드

인터넷을 통한 긴 전송 시간을 방지하기 위해 시작하는 데 필요한 데이터가 포함된 중복 제거 디스크 저장 장치를 클라우드에 시드할 수 있습니다. 중복 제거 디스크 저장 장치를 시드하는 한 가지 방법은 다른 배치된 시스템의 시스템 상태 백업 데이터를 사용하는 것입니다.

25페이지의 “오프사이트 복사 구성에 대한 중복 제거 디스크 저장 장치 시드” 참조

표 2-10 오프사이트 복사 구성에 대한 운영 체제 파일을 시드하는 방법

단계	설명
1단계	개인 클라우드에 배치된 시스템에 Agent for Windows 또는 Agent for Linux를 설치하십시오. Backup Exec Agent 설치에 대한 자세한 내용은 Symantec Backup Exec 관리자 설명서에서 확인하십시오. 시스템이 로컬 고객 네트워크에 백업할 서버와 동일한 운영 체제 버전을 실행해야 합니다.
2단계	개인 클라우드 Backup Exec 서버에서 백업 작업을 생성하고 실행하십시오. 이러한 배치된 시스템의 시스템 상태 및 시스템 볼륨을 개인 클라우드 중복 제거 디스크 저장 장치로 백업하십시오.

전송 드라이브를 사용하여 오프사이트 복사 구성에 대한 중복 제거 디스크 저장 장치 시드

인터넷을 통한 긴 전송 시간을 방지하기 위해 시작하는 데 필요한 데이터가 포함된 중복 제거 디스크 저장 장치를 클라우드에 시드할 수 있습니다. 중복 제거 디스크 저장 장치를 시드하는 한 가지 방법은 실제 전송 드라이브를 사용하는 것입니다.

25페이지의 “오프사이트 복사 구성에 대한 중복 제거 디스크 저장 장치 시드” 참조

Symantec에서 제공하는 계산기 도구를 사용하면 전송 드라이브를 사용하는 데 필요한 시간과 인터넷을 통해 데이터를 복사하는 데 필요한 시간을 비교할 수 있습니다. 계산기는 다음 링크에 있습니다.

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

전송 드라이브를 사용하여 개인 클라우드 Backup Exec 인스턴스를 시드하려면 다음 절차를 완료하십시오.

26페이지의 “전송 드라이브를 사용하여 오프사이트 복사 구성에 대한 중복 제거 디스크 저장 장치 시드” 참조

전송 드라이브를 사용하여 오프사이트 복사 구성에 대한 중복 제거 디스크 저장 장치 시드

실제 전송 드라이브를 사용하여 개인 클라우드 Backup Exec 중복 제거 디스크 저장 장치를 시드할 수 있습니다. 시작하는 데 필요한 파일이 포함된 중복 제거 디스크 저장 장치를 시드하면 인터넷을 통해 대용량 백업을 수행하는 시간을 줄일 수 있습니다.

26페이지의 “전송 드라이브를 사용하여 오프사이트 복사 구성에 대한 중복 제거 디스크 저장 장치 시드” 참조

전송 드라이브를 사용하여 오프사이트 복사 구성에 대한 중복 제거 디스크 저장 장치를 시드하려면 다음과 같이 하십시오.

1 시스템 2(C2)인 로컬 Backup Exec 서버에서 이동식 드라이브에 디스크 저장소를 생성하십시오.

2 다음 방법 중 하나를 사용하여 백업 세트를 디스크 저장소에 복사하고 소프트웨어 암호화를 통해 데이터를 암호화하십시오.

설치하는 동안 "DisablePDI2PDISetCopy" 레지스트리 키를 생성하지 않았다면 백업 세트를 복제할 수 있습니다.	다음 단계를 완료하십시오. ■ 개인 클라우드 중복 제거 디스크 저장 장치를 시드하는 데 사용할 데이터의 최신 전체 백업 세트를 복제하도록 선택하십시오. ■ **복제 작업** 대화 상자에서 저장소 대상으로 생성한 디스크 저장소를 선택하십시오. ■ **복제 작업** 대화 상자에서 소프트웨어 암호화를 구성하십시오. 소프트웨어 암호화를 위한 암호화 키를 생성하거나 선택해야 합니다.
설치하는 동안 "DisablePDI2PDISetCopy" 레지스트리 키를 생성했다면 전체 백업 작업을 생성해야 합니다.	다음 단계를 완료하십시오. ■ Symantec의 GRT(Granular Recovery Technology)를 지원하는 응용 프로그램에 대해 해당 디스크 저장소를 사용하는 전체 백업 작업을 생성하십시오. ■ 백업할 특정 GRT 지원 응용 프로그램에 대해 GRT를 실행 중지하십시오. 오프사이트 복사 GRT의 제한에 대한 자세한 내용은 다음 항목에서 확인하십시오. 47페이지의 "오프사이트 복사의 Granular Recovery Technology 제한" 참조 ■ **저장소** 패널에서 소프트웨어 암호화를 실행하십시오. 소프트웨어 암호화를 위한 암호화 키를 생성하거나 선택해야 합니다.

3 이전 단계에서 생성한 작업을 실행하십시오.

4 이동식 디스크를 개인 클라우드 데이터 센터로 보내십시오.

5 이동식 디스크를 개인 클라우드 Backup Exec 서버에 연결하십시오.

6 해당 드라이브에 원래 생성한 디스크 저장소를 사용하여 연결된 이동식 드라이브에 디스크 저장소를 생성하십시오.

7 이동식 디스크 저장 장치에서 Backup Exec 인벤토리 작업을 생성하고 실행하십시오.

8 이동식 디스크 저장 장치에서 Backup Exec 카탈로그 작업을 생성하고 실행하십시오.

9 디스크 저장 장치에서 백업 세트를 복제하고 클라우드 중복 제거 디스크 저장 장치를 대상 저장 장치로 사용하십시오.

10 복제 작업이 완료되면 Backup Exec을 사용하여 디스크 저장소에 있는 파일을 사용 중지하고 삭제하십시오. 디스크 유틸리티를 사용하여 이동식 드라이브를 완전히 지우십시오.

개인 클라우드 중복 제거 디스크 저장 장치를 성공적으로 시드했으면 구성 프로세스가 완료된 것입니다. 다음 항목으로 진행하여 Backup Exec에서 작업을 시작할 수 있습니다.

33페이지의 "오프사이트 복사 구성에 대한 Backup Exec 개인 클라우드 서비스 사용" 참조

직접 백업 구성 설정

개인 클라우드 서버에 OpenVPN을 구성한 후 Backup Exec 서버를 구성해야 합니다.

11페이지의 "Backup Exec 개인 클라우드 서비스 구성" 참조

직접 백업 구성을 사용하려면 최소한 시스템 3대가 필요합니다.

19페이지의 "직접 백업 구성" 참조

표 2-11 직접 백업 구성을 구성하는 방법

단계	설명
1단계	개인 클라우드 중복 제거 디스크 저장 장치를 구성하십시오. 28페이지의 "직접 백업 구성을 위한 개인 클라우드 중복 제거 디스크 저장 장치 구성" 참조
2단계	데이터가 포함된 개인 클라우드 중복 제거 디스크 저장 장치를 시드하십시오. 29페이지의 "직접 백업 구성에 대한 중복 제거 디스크 저장 장치 시드" 참조

직접 백업 구성을 위한 개인 클라우드 중복 제거 디스크 저장 장치 구성

개인 클라우드 인스턴스에 Backup Exec 디스크 저장 장치와 중복 제거 디스크 저장 장치를 생성해야 합니다.

28페이지의 "직접 백업 구성 설정" 참조

표 2-12 개인 클라우드 Backup Exec 인스턴스 중복 제거 디스크 저장 장치를 구성하는 방법

단계	설명
1단계	로컬 서버에 대한 관리자 권한을 가진 도메인 계정을 사용하여 C1에 로그온하십시오.
2단계	C1에 Backup Exec 2012를 설치하고 시스템 로그온을 지정하십시오.
3단계	C1의 Backup Exec에서 새로운 중복 제거 디스크 저장 장치를 생성하십시오. 개인 클라우드 중복 제거 디스크 저장 장치에서 움직이지 않는 데이터를 암호화하려면 **예를 선택하고 이 중복 제거 디스크 저장 장치로 전송 중에 새로운 중복 제거 디스크 저장 장치를 구성할 경우** 데이터가 해당 위치에 저장되는 동안 데이터를 암호화하십시오. 기존 중복 제거 장치의 경우 중복 제거 장치 속성의 **암호화** 필드를 수정할 수 있습니다. **참고:** VPN은 로컬 Backup Exec 서버와 클라우드 Backup Exec 서버 간에 전송 중인 데이터를 암호화합니다. 중복 제거 디스크 저장 장치 생성에 대한 자세한 내용은 Symantec Backup Exec 관리자 설명서를 참조하십시오.
4단계	개인 클라우드 서버 설정 실행: ■ Backup Exec 서버에서 Backup Exec을 여십시오. ■ Backup Exec 버튼을 누르고 **구성 및 설정**을 선택한 다음 **로컬 서버 속성**을 누르십시오. ■ 왼쪽 창에서 **설정**을 누르십시오. ■ **개인 클라우드 서버** 필드에서 **실행**을 선택하십시오.

직접 백업 구성에 대한 중복 제거 디스크 저장 장치 시드

인터넷을 통한 긴 전송 시간을 방지하기 위해 시작하는 데 필요한 데이터가 포함된 중복 제거 디스크 저장 장치를 클라우드에 시드할 수 있습니다. 중복 제거 디스크 저장 장치 시드는 초기 구성 파일이나 백업 세트를 중복 제거 디스크 저장 장치에 배치하여 사용 준비를 하는 프로세스입니다. 전송 시간은 복사하여 개인 클라우드 Backup Exec 인스턴스로 백업할 데이터 양에 따라 달라집니다.

시드할 데이터 유형에 따라 다음 두 가지 방법 중 하나를 사용하여 초기 데이터를 시드할 수 있습니다.

- 시스템 상태 운영 체제 백업을 사용하여 중복 제거 디스크 저장 장치를 시드할 수 있습니다. 개인 클라우드에서 실행 중인 다른 시스템의 시스템 상태 데이터에 대해 백업 작업을 실행하여 중복 제거 디스크 저장 장치를 시드합니다. 백업하려는 로컬 시스템과 동일한 운영 체제를 실행하는 시스템에 대한 시스템 상태 데이터를 백업합니다.
30페이지의 “직접 백업 구성에 대한 운영 체제 파일 시드” 참조

- 로컬 Backup Exec 서버의 관련 데이터와 함께 백업 세트가 포함된 실제 전송 드라이브를 개인 클라우드 데이터 센터로 보낼 수 있습니다.
  30페이지의 "전송 드라이브를 사용하여 직접 백업 구성에 대한 중복 제거 디스크 저장 장치 시드" 참조

직접 백업 구성에 대한 운영 체제 파일 시드

인터넷을 통한 긴 전송 시간을 방지하기 위해 시작하는 데 필요한 데이터가 포함된 중복 제거 디스크 저장 장치를 클라우드에 시드할 수 있습니다. 중복 제거 디스크 저장 장치를 시드하는 한 가지 방법은 다른 배치된 시스템의 시스템 상태 백업 데이터를 사용하는 것입니다.

29페이지의 "직접 백업 구성에 대한 중복 제거 디스크 저장 장치 시드" 참조

표 2-13 직접 백업 구성에 대한 운영 체제 파일을 시드하는 방법

단계	설명
1단계	로컬 고객 네트워크에서 백업하려는 시스템에 Agent for Windows 및 Agent for Linux를 설치하십시오. Backup Exec Agent 설치에 대한 자세한 내용은 Symantec Backup Exec 관리자 설명서에서 확인하십시오. 데이터를 시드하는 데 사용하는 시스템이 백업할 시스템과 동일한 운영 체제 버전을 실행해야 합니다.
2단계	개인 클라우드 Backup Exec 서버에서 백업 작업을 생성하고 실행하십시오. 이러한 배치된 시스템의 시스템 상태 및 시스템 볼륨을 개인 클라우드 중복 제거 디스크 저장 장치로 백업하십시오.

전송 드라이브를 사용하여 직접 백업 구성에 대한 중복 제거 디스크 저장 장치 시드

실제 전송 드라이브를 사용하여 개인 클라우드 Backup Exec 중복 제거 디스크 저장 장치를 시드할 수 있습니다. 시작하는 데 필요한 파일이 포함된 중복 제거 디스크 저장 장치를 시드하면 인터넷을 통해 대용량 백업을 수행하는 시간을 줄일 수 있습니다.

29페이지의 "직접 백업 구성에 대한 중복 제거 디스크 저장 장치 시드" 참조

표 2-14 전송 드라이브를 사용하여 직접 백업 구성에 대한 중복 제거 디스크 저장 장치 시드 방법

단계	설명
1단계	시스템(C2)에 이동식 드라이브를 연결하십시오.
2단계	시드 파일을 C2에서 이동식 드라이브로 복사하십시오.

표 2-14 전송 드라이브를 사용하여 직접 백업 구성에 대한 중복 제거 디스크 저장 장치 시드 방법 (계속)

단계	설명
3단계	타사 암호화 도구를 사용하여 디스크의 파일을 암호화하십시오.
4단계	전송 드라이브를 개인 클라우드 데이터 센터로 보내십시오.
5단계	전송 드라이브를 시스템 1(C1)에 연결하십시오.
6단계	데이터 암호화에 사용된 것과 동일한 도구를 사용하여 전송 드라이브의 데이터를 일시적으로 해독하십시오.
7단계	해독된 파일을 백업하는 백업 작업을 생성하고 실행하십시오. 클라우드에서 중복 제거 디스크 저장 장치를 대상으로 사용하십시오.
8단계	백업 작업이 완료되면 복사한 원본 파일을 삭제할 수 있습니다. 디스크 유틸리티를 사용하여 이동식 드라이브를 완전히 지우십시오.

개인 클라우드 중복 제거 디스크 저장 장치를 성공적으로 시드했으면 구성 프로세스가 완료된 것입니다.

다음 항목으로 진행하여 Backup Exec에서 작업을 시작할 수 있습니다.

39페이지의 "Backup Exec 개인 클라우드 서비스 및 직접 백업 구성 사용" 참조

3장

Backup Exec 개인 클라우드 서비스로 작업

이 장의 내용은 다음과 같습니다.

오프사이트 복사 구성에 대한 Backup Exec 개인 클라우드 서비스 사용

Backup Exec 개인 클라우드 서비스를 사용하면 CASO(Central Admin Server Option) 및 Deduplication Option을 통해 백업 정의를 관리할 수 있습니다.

Symantec에서 제공하는 유용한 계산기 도구를 사용하면 인터넷을 통해 데이터를 복사하는 데 필요한 시간을 예측할 수 있습니다. 클라우드 백업 시간 계산기는 클라우드 백업 전략을 계획하는 데 유용할 수 있습니다. 계산기를 사용하여 시스템 리소스가 할당된 백업 실행 시간대 내에 고객 데이터를 백업하기에 충분한지 확인할 수 있습니다. 시간 예측은 지원할 수 있는 데이터 양과 클라우드 백업에 사용해야 하는 시간을 결정하는 데 도움이 됩니다.

계산기는 다음 링크에 있습니다.

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

34페이지의 "오프사이트 복사 구성에 대한 백업 정의 생성" 참조

35페이지의 "오프사이트 복사 구성을 사용하여 개인 클라우드에서 데이터 복원" 참조

36페이지의 "오프사이트 복사 구성을 사용하여 개인 클라우드에서 데이터 복원" 참조

36페이지의 "전송 드라이브와 오프사이트 복사 구성을 사용하여 개인 클라우드에서 데이터 복원" 참조

오프사이트 복사 구성에 대한 백업 정의 생성

복제 단계를 통해 백업 정의를 생성하여 백업 데이터를 개인 클라우드 Backup Exec 인스턴스에 복사할 수 있습니다. 백업 정의는 중앙 관리 서버에 위치합니다. 백업 정의에는 데이터를 로컬 중복 제거 디스크 저장 장치로 백업하는 백업 작업이 포함됩니다. 또한 백업 정의에는 이후에 해당 백업 세트를 개인 클라우드 중복 제거 디스크 저장 장치로 복사하는 복제 단계도 포함됩니다.

선택적으로 추가 복제 단계를 백업 정의에 추가하여 클라우드 중복 제거 저장 장치에서 복사된 백업 세트를 복제할 수 있습니다. 백업 세트를 해당 클라우드에 위치한 테이프 장치 또는 관리되는 Backup Exec 서버의 다른 중복 제거 저장 장치로 복제할 수 있습니다. 관리되는 Backup Exec 서버는 개인 클라우드 또는 다른 실제 위치에 있을 수 있습니다.

참고: 백업 정의 생성에 대한 자세한 내용은 Symantec Backup Exec 관리자 설명서에서 확인하십시오.

오프사이트 복사 구성에 대한 백업 정의를 생성하려면

1. 중앙 관리 서버에서 Backup Exec을 여십시오.
2. **백업 및 복원** 탭에서 다음 작업 중 하나를 수행하십시오.
   - 단일 서버를 백업하려면 서버 이름을 마우스 오른쪽 버튼으로 누르십시오.
   - 여러 서버를 백업하려면 Shift 키 또는 Ctrl 키를 누른 상태로 서버 이름을 누르고 선택한 서버 중 하나를 마우스 오른쪽 버튼으로 누르십시오.
3. **백업** 메뉴에서 사용할 백업 옵션을 선택하십시오.
4. **이름** 필드에서 백업 정의에 사용할 고유한 이름을 입력하십시오.

   참고: 여러 서버에서 데이터를 백업하는 경우 Backup Exec은 **이름** 필드에 입력하는 텍스트에 서버 이름을 추가합니다. Backup Exec은 각 백업 정의에 대해 고유한 이름이 생성될 수 있도록 서버 이름과 사용자가 입력한 텍스트를 사용합니다.

   ---

5. 다음을 수행하십시오.

Backup Exec이 백업 선택 항목에 액세스하는 데 사용하는 인증 정보를 테스트 또는 편집하는 경우	**선택** 상자에서 **인증 정보 테스트/편집**을 누르십시오.
백업 선택 항목을 변경하는 경우	**선택** 상자에서 **편집**을 누르십시오.
백업 정의에 단계를 추가하는 경우	다음 단계를 완료하십시오. ■ **백업** 상자에서 **단계 추가**를 누르십시오. ■ **복제**를 눌러서 복제 단계를 추가하십시오. ■ **복제** 상자에서 **편집**을 누르십시오. ■ **저장소** 창에서 개인 클라우드 중복 제거 디스크 저장 장치를 복제 작업에 대한 저장소로 선택하십시오. ■ 필요한 경우 다른 설정을 완료하십시오. 복제 작업을 별도의 작업으로 확인하는 것이 좋습니다. 작업 완료 시 작업을 확인하도록 선택하면 해당 작업 성능이 저하됩니다. **확인** 창에서 확인 작업을 구성할 수 있습니다. **참고:** 추가 복제 단계를 백업 정의에 추가할 수 있습니다. 예를 들어, 추가 사본을 원격으로 관리되는 Backup Exec 서버의 배치된 테이프 장치 또는 중복 제거 저장 장치에 보낼 수 있습니다.
작업 설정을 수정하는 경우	다음 단계를 완료하십시오. ■ **백업** 상자에서 **편집**을 누르십시오. ■ **저장소** 창에서 로컬 중복 제거 디스크 저장 장치를 백업 작업에 대한 저장소로 선택하십시오. ■ 필요한 경우 다른 설정을 완료하십시오.

6 백업 정의 구성을 마쳤으면 **백업 속성** 대화 상자에서 **확인**을 누르십시오.

33페이지의 "오프사이트 복사 구성에 대한 Backup Exec 개인 클라우드 서비스 사용" 참조

오프사이트 복사 구성을 사용하여 개인 클라우드에서 데이터 복원

개인 클라우드 Backup Exec 인스턴스에 데이터를 백업한 후 언제든지 복원할 수 있습니다. 개인 클라우드 Backup Exec 중복 제거 디스크 저장 장치에서 데이터를 복원하는 과정은 Backup Exec에서 정상적으로 데이터를 복원하는 과정과 매우 유사합니다.

36페이지의 "오프사이트 복사 구성을 사용하여 개인 클라우드에서 데이터 복원" 참조

실제 전송 드라이브를 사용하여 Backup Exec 개인 클라우드 인스턴스에서 대량 데이터를 복원하는 것이 훨씬 효율적일 수도 있습니다. 전송 드라이브를 사용하여 데이터를 로컬 Backup Exec 서버로 전송할 수 있습니다. 그런 다음 로컬 Backup Exec 서버를 사용하여 복원 작업을 실행합니다.

36페이지의 "전송 드라이브와 오프사이트 복사 구성을 사용하여 개인 클라우드에서 데이터 복원" 참조

오프사이트 복사 구성을 사용하여 개인 클라우드에서 데이터 복원

개인 클라우드 Backup Exec 인스턴스의 데이터를 로컬 Backup Exec 클라이언트 시스템으로 복원할 수 있습니다.

35페이지의 "오프사이트 복사 구성을 사용하여 개인 클라우드에서 데이터 복원" 참조

오프사이트 복사 구성을 사용하여 개인 클라우드에서 데이터를 복원하려면 다음과 같이 하십시오.

1. 다음 절차에 설명된 대로 복원하는 서버에 시스템 1(C1)과 통신하는 데 사용할 수 있는 네트워크 경로 명령이 있는지 확인하십시오.

   52페이지의 "로컬 네트워크 라우팅 구성" 참조

2. 중앙 관리 서버에서 Backup Exec을 여십시오.
3. **백업 및 복원** 탭에서 **복원**을 누르십시오.
4. 복원하려는 데이터와 기타 필요한 작업 옵션을 선택한 후 작업을 제출하십시오.

33페이지의 "오프사이트 복사 구성에 대한 Backup Exec 개인 클라우드 서비스 사용" 참조

전송 드라이브와 오프사이트 복사 구성을 사용하여 개인 클라우드에서 데이터 복원

전송 드라이브를 사용하여 개인 클라우드 Backup Exec 인스턴스의 데이터를 로컬 Backup Exec 서버로 복사할 수 있습니다. 한 번에 대량 데이터를 복원하려는 경우 전송 드라이브를 사용하면 도움이 될 수 있습니다. 사용 가능한 대역폭과 작업 완료 시간에 따라 큰 복원 작업은 시스템 리소스에 영향을 줄 수 있습니다.

35페이지의 "오프사이트 복사 구성을 사용하여 개인 클라우드에서 데이터 복원" 참조

전송 드라이브와 오프사이트 복사 구성을 사용하여 개인 클라우드에서 데이터를 복원하려면 다음과 같이 하십시오.

1 개인 클라우드 Backup Exec 인스턴스인 시스템 1(C1)에서 이동식 드라이브에 디스크 저장소를 생성하십시오.

2 클라우드 기반 중복 제거 디스크 저장 장치에서 복원하려는 백업 세트를 복제하십시오. 대상 저장 장치로 생성한 디스크 저장소를 선택하십시오.

소프트웨어 암호화를 사용하여 데이터를 암호화하도록 선택해야 합니다. 소프트웨어 암호화를 위한 암호화 키를 생성하거나 선택해야 합니다.

데이터 암호화에 대한 자세한 내용은 Symantec Backup Exec 관리자 설명서에서 확인하십시오.

3 작업이 완료된 후 전송 드라이브를 로컬 사무실로 보내십시오.

4 이동식 드라이브가 도착하면 해당 드라이브를 로컬 Backup Exec 서버에 연결하십시오.

5 이동식 드라이브를 경로로 사용하여 시스템 2(C2)에 디스크 저장소를 생성하십시오.

6 해당 디스크 저장소에서 Backup Exec 인벤토리 및 카탈로그 작업을 생성하고 실행하십시오.

7 새로운 디스크 저장소에서 적합한 대상으로 데이터를 복원하십시오.

8 전송 드라이브에서 데이터를 지우십시오.

33페이지의 “오프사이트 복사 구성에 대한 Backup Exec 개인 클라우드 서비스 사용” 참조

중앙 관리 서버 오류가 발생할 경우 관리되는 Backup Exec 서버에서 데이터 복원

하드웨어 오류 또는 기타 재해가 중앙 관리 서버에 영향을 미치면 관리되는 Backup Exec 서버에서 백업을 실행하거나 작업을 복원할 수 없습니다. 대체 시스템을 구성하고 Backup Exec 중앙 관리 서버를 재설치하여 중앙 관리 서버를 복구할 수 있습니다. 그러나 관리되는 Backup Exec 서버를 독립 실행형 Backup Exec 서버로 변환하여 중앙 관리 서버를 복원할 수도 있습니다.

관리되는 Backup Exec 서버를 독립 실행형 Backup Exec 서버로 변환하여 중앙 관리 서버를 복원하려면

1 관리되는 Backup Exec 서버에서 로컬 디스크 저장소의 이름 및 디렉터리 경로를 기록하십시오.

참고: 저장소 탭의 디스크 저장소를 두 번 누르십시오. 그런 다음 왼쪽 창의 **속성**을 눌러 저장소 속성을 확인하십시오.

2 관리되는 Backup Exec 서버에 자체 중복 제거 디스크 저장 장치가 있을 경우 장치의 이름, 경로, 로그온 계정 및 암호 속성을 기록하십시오.

참고: 저장소 탭의 중복 제거 디스크 저장 장치를 두 번 누르십시오. 그런 다음 왼쪽 창의 **속성**을 눌러 저장소 속성을 확인하십시오.

3 Windows 제어판에서 프로그램 및 기능(또는 프로그램 추가/제거) 대화 상자 또는 프로그램 제거 대화 상자를 여십시오.

4 Symantec Backup Exec의 **변경** 옵션을 선택하십시오.

5 왼쪽 창에서 아직 선택하지 않은 경우 **추가 옵션**을 선택하십시오.

6 **관리되는 Backup Exec 서버 구성** 창이 나타날 때까지 **다음**을 누르십시오.

7 **로컬로 관리되는 Backup Exec 서버** 옵션을 선택하십시오.

8 **다음**을 누르십시오.

9 "{중앙 관리 서버}에 연결할 수 없습니다. 중앙 관리 서버가 실행 중인지 확인하십시오."라는 메시지가 표시될 경우 다음 중 하나를 수행하십시오.

중앙 관리 서버를 사용할 수 없고 이 관리되는 Backup Exec 서버가 로컬로 관리되기를 원할 경우	계속하려면 **확인**을 누르십시오.
중앙 관리 서버가 실행 중일 때 이 작업을 다시 시도하려는 경우	**취소**를 눌러 절차를 종료하십시오.

설치가 완료되면 시스템은 더 이상 중앙에서 관리되는 Backup Exec 서버가 아닙니다.

10 **다음**을 누르십시오.

11 확인 메시지가 표시되면 시스템을 재시작하십시오.

12 Backup Exec을 열고 **저장소** 탭을 선택하십시오.

Backup Exec이 Backup Exec 서버에 연결되지 못하면 Backup Exec 서비스를 재시작한 다음 다시 시도하십시오.

13 1단계에서 기록한 이름 및 경로를 동일하게 사용하여 원래 디스크 저장소를 가져오는 방법으로 로컬 디스크 저장소를 재생성하십시오.

14 2단계에서 기록한 동일한 정보를 사용하여 원래 중복 제거 디스크 저장 장치를 가져오는 방법으로 모든 중복 제거 디스크 저장 장치를 재생성하십시오.

참고: 새 저장 장치를 생성하는 경우보다 기존 저장 장치를 재생성하는 경우가 훨씬 더 오랜 시간이 소요될 수 있습니다. 이러한 시간은 저장 장치에 포함된 백업 세트 수와 이 관리되는 Backup Exec 서버가 도메인 컨트롤러 및 DNS에 액세스할 수 있는지 여부에 따라 달라집니다.

---

15 재생성한 각 저장 장치에서 Backup Exec 인벤토리 및 카탈로그 작업을 생성 및 실행하십시오.

이제 독립 실행형 Backup Exec 서버를 사용하여 Backup Exec 서버의 저장 장치에 저장된 모든 백업 세트를 복원할 수 있습니다.

16 독립 실행형 Backup Exec 서버를 사용하여 중앙 관리 서버를 복구하는 경우 독립 실행형 Backup Exec 서버의 기존 중앙 관리 서버 리소스를 삭제해야 할 수 있습니다. 그런 다음 Agent for Windows를 중앙 관리 서버로 강제 설치하여 복원하십시오.

중앙 관리 서버가 복구되었으면 Backup Exec 변경 설치 대화 상자를 다시 사용하여 로컬로 관리되는 Backup Exec 서버를 중앙에서 관리되는 Backup Exec 서버로 다시 변환할 수 있습니다. 중앙에서 관리되는 Backup Exec 서버 옵션을 선택하여 관리되는 Backup Exec 서버로 시스템을 재구성하십시오.

Backup Exec 개인 클라우드 서비스 및 직접 백업 구성 사용

Backup Exec 개인 클라우드 서비스를 사용하면 직접 백업 구성에 대한 클라이언트 측 중복 제거를 통해 백업 정의를 관리할 수 있습니다.

작업을 실행할 때 개인 클라우드 Backup Exec 인스턴스 및 VPN 링크 연결을 수동으로 시작하고 중지할 수 있습니다. 또는 VPN 링크가 연결되고 인스턴스가 영구적으로 실행되게 할 수도 있습니다. 대략 백업 작업 실행 시간대에 시작 및 중지되도록 OpenVPN 서비스를 예약하여 이 프로세스를 자동화할 수도 있습니다. Windows 예약된 태스크 유틸리티를 사용하여 서비스 예약을 생성할 수 있습니다.

Symantec에서 제공하는 유용한 계산기 도구를 사용하면 인터넷을 통해 데이터를 복사하는 데 필요한 시간을 예측할 수 있습니다. 클라우드 백업 시간 계산기는 클라우드 백업 전

략을 계획하는 데 유용할 수 있습니다. 계산기를 사용하여 시스템 리소스가 할당된 백업 실행 시간대 내에 고객 데이터를 백업하기에 충분한지 확인할 수 있습니다. 시간 예측은 지원할 수 있는 데이터 양과 클라우드 백업에 사용해야 하는 시간을 결정하는 데 도움이 됩니다.

계산기는 다음 링크에 있습니다.

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

40페이지의 "직접 백업 구성을 위한 클라이언트 측 중복 제거 실행" 참조

41페이지의 "직접 백업 구성에 대한 백업 정의 생성" 참조

42페이지의 "전송 드라이브와 직접 백업 구성을 사용하여 개인 클라우드에서 데이터 복원" 참조

직접 백업 구성을 위한 클라이언트 측 중복 제거 실행

개인 클라우드 Backup Exec 인스턴스로 직접 백업 작업을 생성하고 실행하려면 먼저 클라이언트 측 중복 제거를 실행해야 합니다.

참고: 멀티테넌트 구성을 사용하는 경우 중앙 관리 서버의 중복 제거 디스크 저장 장치의 경우 클라이언트 측 중복 제거를 실행하지 말아야 합니다.

직접 백업 구성을 위한 클라이언트 측 중복 제거를 실행하려면

1. **저장소** 탭에서 속성을 편집하려는 저장소를 두 번 누르십시오.
2. 왼쪽 창에서 **속성**을 누르십시오.
3. **클라이언트 측 중복 제거** 필드에서 **실행**을 선택하십시오.
4. **적용**을 누르십시오.
5. Backup Exec 서비스를 재시작하십시오.

   참고: C1에서 Backup Exec 서비스를 중지하고 재시작해야 합니다.

클라이언트 측 중복 제거를 실행한 후 직접 백업 작업을 생성하고 실행할 수 있습니다.

클라이언트 측 중복 제거를 사용하는 백업 작업 생성에 대한 자세한 내용은 Symantec Backup Exec 관리자 설명서를 참조하십시오.

41페이지의 "직접 백업 구성에 대한 백업 정의 생성" 참조

39페이지의 "Backup Exec 개인 클라우드 서비스 및 직접 백업 구성 사용" 참조

직접 백업 구성에 대한 백업 정의 생성

Remote Agent 공유 및 클라이언트 측 중복 제거에 대해 VPN을 구성하고 추가 시스템을 실행한 후 직접 백업 작업을 생성하고 실행할 수 있습니다.

40페이지의 "직접 백업 구성을 위한 클라이언트 측 중복 제거 실행" 참조

참고: 백업 정의 생성에 대한 자세한 내용은 Symantec Backup Exec 관리자 설명서에서 확인하십시오.

개인 클라우드 Backup Exec 인스턴스로 직접 데이터를 백업하려면 다음 절차를 따르십시오.

직접 백업 구성에 대한 백업 작업을 생성하려면 다음과 같이 하십시오.

1 시스템 1(C1)에서 Backup Exec을 여십시오.

2 **백업 및 복원** 탭에서 다음 작업 중 하나를 수행하십시오.

- 단일 서버를 백업하려면 서버 이름을 마우스 오른쪽 버튼으로 누르십시오.
- 여러 서버를 백업하려면 Shift 키 또는 Ctrl 키를 누른 상태로 서버 이름을 누르고 선택한 서버 중 하나를 마우스 오른쪽 버튼으로 누르십시오.

3 **백업** 메뉴에서 사용할 백업 옵션을 선택하십시오.

4 **이름** 필드에서 백업 정의에 사용할 고유한 이름을 입력하십시오.

참고: 여러 서버에서 데이터를 백업하는 경우 Backup Exec은 **이름** 필드에 입력하는 텍스트에 서버 이름을 추가합니다. Backup Exec은 각 백업 정의에 대해 고유한 이름이 생성될 수 있도록 서버 이름과 사용자가 입력한 텍스트를 사용합니다.

---

5 다음을 수행하십시오.

Backup Exec이 백업 선택 항목에 액세스하는 데 사용하는 인증 정보를 테스트 또는 편집하는 경우	**선택** 상자에서 **인증 정보 테스트/편집**을 누르십시오.
백업 선택 항목을 변경하는 경우	**선택** 상자에서 **편집**을 누르십시오.
백업 정의에 단계를 추가하는 경우	**백업** 상자에서 **단계 추가**를 누르십시오.

작업 설정을 수정하는 경우	다음 단계를 완료하십시오. ■ **백업** 상자에서 **편집**을 누르십시오. ■ **원격 시스템에서 저장 장치에 직접 액세스하고 클라이언트 측 중복 제거 수행(지원되는 경우)** 옵션이 선택되어 있는지 확인하십시오. ■ 필요한 경우 다른 설정을 완료하십시오.

6 백업 정의 구성을 마쳤으면 **백업 속성** 대화 상자에서 **확인**을 누르십시오.

39페이지의 "Backup Exec 개인 클라우드 서비스 및 직접 백업 구성 사용" 참조

전송 드라이브와 직접 백업 구성을 사용하여 개인 클라우드에서 데이터 복원

일반 복원 작업을 생성하여 개인 클라우드 Backup Exec 인스턴스의 데이터를 로컬 클라이언트로 복원할 수 있습니다. 하지만 한 번에 대량 데이터를 복원하려는 경우 실제 전송 드라이브를 사용하는 것이 더 효율적일 수도 있습니다. 대량 데이터를 전송하는 데 걸리는 시간은 사용 가능한 대역폭과 작업 완료 시간에 따라 달라집니다.

전송 드라이브와 직접 백업 구성을 사용하여 개인 클라우드에서 데이터를 복원하려면 다음과 같이 하십시오.

1 시스템 1(C1)에서 복원 작업을 생성하고 실행하여 파일을 이동식 디스크 드라이브의 폴더로 복원하십시오.

2 작업이 완료된 후 타사 암호화 도구를 사용하여 디스크의 파일을 암호화하십시오.

3 이동식 드라이브를 로컬 사무실로 보내십시오.

4 이동식 드라이브가 도착하면 암호화에 사용된 것과 동일한 도구를 사용하여 파일을 해독하십시오.

5 해독된 파일을 시스템 2(C2)의 적절한 대상으로 전송하십시오.

6 전송 드라이브의 파일을 완전히 지우거나 정리하여 데이터를 영구적으로 제거하십시오.

39페이지의 "Backup Exec 개인 클라우드 서비스 및 직접 백업 구성 사용" 참조

클라우드 재해 복구 서비스 정보

Backup Exec 2012 SDR(Simplified Disaster Recovery) 기능과 가상 시스템 기능으로의 변환을 통해 서비스 제공업체 또는 고객은 클라우드 재해 복구 서비스를 제공할 수 있습니다. 클라우드에 저장된 백업 데이터를 사용하여 재해 발생 시 개인 클라우드의 임시 교체 가상 또는 실제 서버를 생성할 수 있습니다.

특정 네트워크 구성 및 오류 조건이 장애 조치 및 장애 복구에 필요한 특정 단계에 영향을 미칠 수 있습니다. 이 섹션은 Backup Exec 개인 클라우드 환경 내에서 SDR 및 가상 시스템 기능으로의 변환을 통해 재해 복구 서비스를 제공하는 기본 지침에 대해서만 설명합니다.

주요 재해 복구 시나리오는 두 가지가 있습니다. 첫 번째 시나리오는 하나 이상의 온사이트 서버에 오류가 발생하지만 사이트에 있는 네트워크는 그대로 유지되는 서버 장애 조치 및 장애 복구입니다. 두 번째 시나리오는 전체 사이트에 오류가 발생한 사이트 장애 조치 및 장애 복구입니다.

43페이지의 "장애 조치로부터 서버 또는 사이트 복구" 참조

45페이지의 "장애 복구로부터 서버 또는 사이트 복구" 참조

장애 조치로부터 서버 또는 사이트 복구

서버 장애 조치 시나리오를 준비하려면 모든 중요한 비즈니스 서버에 대해 SDR(Simplified Disaster Recovery) 실행 백업 정의를 구성하고 정기적으로 실행해야 합니다. 백업 정의에는 백업 데이터를 개인 클라우드 중복 제거 디스크 저장 장치에 복사하는 복제 단계가 포함되어야 합니다. 서버 장애 조치가 발생하면 개인 클라우드 Backup Exec 서버를 사용하여 대체 가상 또는 실제 서버를 복구합니다.

42페이지의 "클라우드 재해 복구 서비스 정보" 참조

대체 실제 서버를 복구하려면 Simplified Disaster Recovery 디스크를 사용하여 베어 메탈 복구를 수행하십시오. 개인 클라우드 중복 제거 디스크 저장 장치의 최근 SDR 실행 백업을 사용하십시오. 대체 서버를 온사이트 사이트로 전송하여 장애가 발생한 서버를 대체할 수 있습니다. 사이트 장애 조치에서는 중요한 비즈니스 서버의 전체 그룹을 클라우드에 있는 하이퍼바이저 환경의 가상 시스템으로 대체해야 합니다.

Simplified Disaster Recovery에 대한 자세한 내용은 Symantec Backup Exec 관리자 설명서를 참조하십시오.

참고: 특정 네트워크 구성 및 오류 조건이 장애 복구에 필요한 특정 단계에 영향을 미칠 수 있습니다. 다음 절차는 Backup Exec 개인 클라우드 환경에서 재해 복구 서비스를 제공하는 기본 지침만 제공합니다.

장애 조치로부터 서버 또는 사이트를 복구하려면

1 클라우드 위치에서 Hyper-V 또는 VMWare ESX 하이퍼바이저 환경을 생성하십시오.

2 하이퍼바이저에서 실행될 대체 가상 시스템 또는 가상 시스템에 대해 차단 장치가 있는 가상 네트워크를 생성하십시오. 전체 사이트 장애 조치 시나리오에서 대체 서버는 원래의 온사이트 IP 주소를 유지해야 합니다.

참고: 사이트를 복구할 경우 대체 서버는 원래의 온사이트 IP 주소를 유지해야 합니다. 논리적 순서로 대체 시스템을 복원해야 합니다. 예를 들어, 도메인 컨트롤러 및 DNS 서버를 먼저 복원해야 합니다.

---

3 다음 중 하나를 수행하십시오.

실제 시스템에서 장애 조치하려면	다음 단계를 완료하십시오. ■ 가상 시스템으로의 변환을 생성 및 실행하십시오. 모든 대체 시스템에서 SDR 지정 시점 시스템 볼륨과 시스템 상태 데이터를 가상 시스템으로 변환하십시오. 가상 시스템은 하이퍼바이저를 대상으로 해야 합니다. 이 경우 응용 프로그램 리소스를 선택하지 마십시오. ■ 필요할 경우 대체 가상 시스템의 고정 IP 주소를 구성하십시오. ■ 대체 가상 시스템 또는 가상 시스템과 개인 클라우드 Backup Exec 서버 사이에 네트워크 연결을 설정하십시오. ■ 각 대체 서버에 대해 동일한 SDR 실행 지정 시점 백업에서 복원 작업을 생성 및 실행하십시오. 해당 지정 시점에 사용 가능한 시스템 리소스를 모두 선택하십시오. 복원 데이터를 대체 서버로 재연결하십시오.
가상 시스템에서 장애 조치하려면	대체 서버의 최근 SDR 지정 시점 백업 각각에서 재연결된 복원 작업을 생성 및 실행하십시오. 동일한 하이퍼바이저 유형을 온사이트 및 클라우드 서버 모두에 대해 사용해야 합니다.

4 단일 서버만 복구하려면 대체 가상 서버와 온사이트 네트워크 사이의 VPN 연결을 설정하고 대체 가상 시스템의 IP 주소에 대한 온사이트 DNS 항목을 구성하십시오.

5 장애가 발생한 서버가 외부 IP 주소(예: Exchange 메일 서버)를 통해 노출된 경우 클라우드 네트워크에서 새로운 외부 주소를 노출시키고 외부 DNS 레코드를 변경하십시오.

6 대체 가상 시스템 또는 가상 시스템에 대해 정기적으로 예약된 하이퍼바이저 호스트 백업 정의를 구성 및 실행하십시오. 개인 클라우드 중복 제거 디스크 저장 장치를 백업 저장소로 사용하십시오.

온사이트 Backup Exec 서버에 로컬 중복 제거 디스크 저장소가 있을 경우 백업 정의에는 백업을 온사이트 중복 제거 디스크 저장 장치로 복사하는 복제 단계가 포함되어야 합니다.

장애 복구로부터 서버 또는 사이트 복구

장애 복구 시 서버 또는 사이트를 복구할 수 있습니다. 사이트 장애 복구 시나리오에서는 중요한 비즈니스 서버의 전체 그룹을 온사이트 실제 서버 또는 가상 서버로 복원해야 합니다.

42페이지의 "클라우드 재해 복구 서비스 정보" 참조

온사이트 서버를 한 번에 모두 복구하기보다 서서히 복구할 수도 있습니다. 처음에는 일부 서버를 복구하고 며칠 또는 몇 주에 걸쳐 나머지가 복구되도록 할 수 있습니다. 이 전략에서도 온사이트 네트워크에 연결된 나머지 교체 클라우드 서버의 VPN 연결 및 IP 주소를 변경해야 합니다.

Simplified Disaster Recovery에 대한 자세한 내용은 Symantec Backup Exec 관리자 설명서를 참조하십시오.

참고: 특정 네트워크 구성 및 오류 조건이 장애 복구에 필요한 특정 단계에 영향을 미칠 수 있습니다. 다음 절차는 Backup Exec 개인 클라우드 환경에서 재해 복구 서비스를 제공하는 기본 지침만 제공합니다.

장애 복구로부터 서버 또는 사이트를 복구하려면

1 SDR(Simplified Disaster Recovery) 실행 백업을 실행하고 복제 단계를 포함시키십시오.

2 대체 가상 시스템 또는 가상 시스템의 실행을 중지하십시오.

3 SDR 실행 백업 정의에 백업 세트를 온사이트 중복 제거 디스크 저장소에 보내는 복제 단계가 포함되지 않은 경우 다음 단계를 완료하십시오.

- 개인 클라우드 Backup Exec 서버의 Backup Exec에 이동식 디스크 저장 장치를 추가하십시오.
- 대체 시스템 또는 시스템 데이터 모두의 최종 지정 시점 백업으로부터 백업 세트를 복제하십시오. 이동식 디스크 저장 장치를 대상으로 사용하십시오.
- 이동식 디스크 저장 장치를 온사이트 위치로 보내십시오.

- 온사이트 Backup Exec 서버의 Backup Exec에 이동식 디스크 저장 장치를 추가하십시오.
- 온사이트 Backup Exec 서버의 디스크 저장 장치의 인벤토리 및 카탈로그를 만드십시오.

4 다음 중 한 가지 작업을 수행하십시오.

온사이트 실제 서버로 장애를 복구하려면	다음 단계를 완료하십시오. ■ SDR(Simplified Disaster Recovery) 디스크를 사용하여 베어 메탈 복구를 수행하십시오. 온사이트 Backup Exec 서버에서 최근 SDR 실행 백업을 선택하십시오. ■ 필요할 경우 복구된 시스템의 고정 IP 주소를 구성하십시오. ■ 필요할 경우 복구된 시스템의 온사이트 DNS 항목 또는 복구된 시스템의 IP 주소를 구성하십시오.
온사이트 가상 서버에 대한 장애를 복구하려면	다음 단계를 완료하십시오. ■ 대체 서버 또는 서버의 최근 지정 시점 백업으로부터 재연결된 복원 작업을 생성 및 실행하십시오. 동일한 하이퍼바이저 유형을 온사이트 및 클라우드 서버 모두에 대해 사용해야 합니다. ■ 필요할 경우 복구된 가상 시스템의 고정 IP 주소를 구성하십시오. ■ 필요할 경우 복구된 가상 시스템의 온사이트 DNS 항목 또는 복구된 가상 시스템의 IP 주소를 구성하십시오.

5 실패한 서버가 외부 IP 주소(예: Exchange 메일 서버)를 통해 노출된 경우 원래 주소 또는 외부 DNS 레코드의 주소를 복원하십시오.

6 대체 클라우드 서버 또는 서버의 백업 정의를 삭제하십시오.

7 원래 백업 정의 또는 모든 복원된 온사이트 시스템 정의의 실행을 재시작하십시오.

Backup Exec 중복 제거 디스크 저장 장치 요구 사항

Backup Exec 중복 제거 디스크 저장 장치 요구 사항은 모든 개인 클라우드 구성에 적용됩니다. 특정 클라우드 Backup Exec 서버의 공유 한계에 도달하면 클라우드 Backup Exec 서버를 추가해야 합니다.

중복 제거 디스크 저장 장치 요구 사항에 대한 자세한 내용은 Symantec Backup Exec 관리자 설명서를 참조하십시오.

WAN 대기 시간 제한 사항

네트워크의 대기 시간이 긴 경우 초기의 직접 클라우드 백업 작업 성능에 부정적인 영향을 미칠 수 있습니다. 대기 시간은 로컬 사무실과 개인 클라우드 Backup Exec 서버 간에 데이터를 전송하는 일부 복제 백업 작업에 영향을 미칠 수도 있습니다. 장치 시드를 통해 항상 성능을 개선할 수 있지만 중복 제거 디스크 저장 장치를 시드한 경우에도 성능 문제가 발생할 수 있습니다. 초기 백업 작업을 수행하는 동안 Backup Exec은 이후 작업의 성능 효율성을 높여 주는 데이터 세그먼트 정보를 식별하고 캐시합니다.

참고: 대기 시간 값이 높은 경우 평균 왕복 대기 시간이 30밀리초 이상인 것으로 간주할 수 있습니다. 대기 시간이 길수록 Backup Exec 성능에 미치는 영향이 큽니다.

이러한 제한은 원본 장치와 대상 장치가 모두 중복 제거 디스크 저장 장치인 경우에만 복제 백업 작업에 적용됩니다

다음은 대기 시간이 긴 환경에서 Backup Exec 개인 클라우드 서비스를 사용할 경우의 제한 사항입니다.

- 중복 제거 디스크 저장 장치와 개인 클라우드 중복 제거 디스크 저장 장치 이외의 다른 원본 장치를 대상으로 사용하는 복제 백업 작업에서는 성능 문제가 발생할 수 있습니다. 중복 제거 디스크 저장 장치를 로컬 원본 저장 장치로 사용하면 이러한 성능 문제를 방지할 수 있습니다.
- 클라우드로 직접 백업하는 구성은 대량의 데이터를 백업하는 데 적합하지 않을 수 있습니다.
- 동일한 리소스에 대해 백업 정의를 삭제하고 재생성하면 Backup Exec가 데이터 핑거프린트를 처음부터 다시 캐시해야 합니다. 따라서 초기의 직접 클라우드 백업 작업과 마찬가지로 성능 문제가 발생할 수 있습니다.

오프사이트 복사의 Granular Recovery Technology 제한

다음은 오프사이트 복사 구성에서 Backup Exec GRT(Granular Recovery Technology) 옵션을 사용할 경우의 제한 사항입니다.

- 로컬 Exchange 증분 GRT 실행 백업 세트를 개인 클라우드 중복 제거 디스크 저장 장치로 백업하면 MTF 테이프 형식의 백업 데이터가 생성됩니다. 이러한 백업 세트에서 세부 데이터를 복원할 수 있지만 이 경우 복원 작업을 수행하는 동안 클라우드 Backup Exec 서버에서 백업 세트를 준비해야 합니다. 클라우드 중복 제거 디스크 저장 장치에 GRT 실행 백업 세트를 직접 백업하는 경우에는 이러한 제한이 적용되지 않습니다.

- 로컬 테이프 장치에서 클라우드 중복 제거 디스크 저장 장치로 중복 GRT 실행 세트를 복사하지 않는 것이 좋으며, 이렇게 할 경우 작업 실행 시간이 너무 길어질 수 있습니다.
- GRT 실행 세트를 클라우드 Backup Exec 서버에 직접 백업하면 대기 시간이 긴 환경에서 성능이 저하될 수 있습니다. 초기 백업 이후에도 성능이 저하될 수 있습니다. 성능 문제가 계속 발생하는 경우에는 직접 백업에 대해 GRT를 해제해야 할 수 있습니다.

Windows Small Business Server(SBS) 및 멀티테넌트 Backup Exec 서버 구성에 대한 제한 사항

멀티테넌트 Backup Exec 서버를 구성하려면 관리되는 모든 로컬 Backup Exec 서버가 개인 클라우드 도메인의 구성원이어야 합니다. 따라서 관리되는 Backup Exec 서버가 고객 도메인에 속해 있는 경우에는 고객의 SBS 서버를 관리되는 Backup Exec 서버로 구성할 수 없습니다. 관리되는 Backup Exec 서버는 개별 서버로 설치해야 합니다.

4장

OpenVPN 구성

이 장의 내용은 다음과 같습니다.

OpenVPN 구성

OpenVPN SSL VPN 공개 소스 패키지는 개인 클라우드 Backup Exec 인스턴스와 로컬 Backup Exec 서버 간에 암호화된 보안 연결을 제공합니다. 개인 클라우드 Backup Exec 서버 인스턴스와 로컬 네트워크에서 실행 중인 모든 시스템 간에 SSL VPN을 구성해야 합니다.

Backup Exec 개인 클라우드 서비스 구성에는 이 단일 클라이언트 OpenVPN 예제에 대해 다음과 같은 네트워크 제한 사항이 포함됩니다.

- 로컬 네트워크가 서브넷 하나에 포함되어야 합니다.
- 로컬 도메인 컨트롤러와 DNS가 같은 서버에 포함되어야 합니다.

49페이지의 “OpenVPN 구성” 참조

Backup Exec 개인 클라우드 서비스에 대한 기본 OpenVPN 구성 지침은 단일 클라이언트를 사용합니다. 모든 클라이언트가 같은 서브넷에 포함되어 있는 경우 이러한 지침을 사용하여 하나 이상의 로컬 클라이언트 시스템을 지원할 수 있습니다. 개인 클라우드 인스턴스를 대상으로 하는 모든 데이터가 OpenVPN 클라이언트 하나를 통해 라우팅됩니다. 보다 복잡한 네트워크의 경우 또는 인증서 기반 인증을 사용하려는 경우 선택적 OpenVPN 다중 클라이언트 구성을 사용할 수 있습니다.

55페이지의 “클라이언트에 대해 OpenVPN 구성” 참조

OpenVPN 구성

OpenVPN SSL VPN 공개 소스 패키지는 개인 클라우드 Backup Exec 인스턴스와 로컬 Backup Exec 서버 간에 암호화된 보안 연결을 제공합니다. 개인 클라우드 Backup Exec 서

버 인스턴스와 로컬 네트워크에서 실행 중인 모든 시스템 간에 SSL VPN을 구성해야 합니다.

49페이지의 "OpenVPN 구성" 참조

표 4-1 OpenVPN 구성 방법

단계	설명
1단계	개인 클라우드 Backup Exec 인스턴스에서 OpenVPN을 구성하십시오. 50페이지의 "개인 클라우드 Backup Exec 인스턴스에서 OpenVPN 구성" 참조
2단계	시스템 2에서 OpenVPN을 구성하십시오. 51페이지의 "시스템 2에서 OpenVPN 구성" 참조
3단계	로컬 네트워크 라우팅을 구성하십시오. 52페이지의 "로컬 네트워크 라우팅 구성" 참조
4단계	필요한 경우 방화벽을 구성하십시오. 53페이지의 "방화벽 구성" 참조
5단계	OpenVPN 연결을 확인하십시오. 54페이지의 "OpenVPN 연결 확인" 참조

개인 클라우드 Backup Exec 인스턴스에서 OpenVPN 구성

암호화된 보안 연결을 사용하려면 개인 클라우드 Backup Exec 인스턴스에서 OpenVPN을 구성해야 합니다.

49페이지의 "OpenVPN 구성" 참조

개인 클라우드 Backup Exec 인스턴스에서 OpenVPN을 구성하려면 다음과 같이 하십시오.

1 다음 링크에서 OpenVPN 2.1.4를 다운로드하여 시스템 1(C1)의 기본 위치에 설치하십시오.

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

2 C1에서 다음을 선택하여 OpenVPN 구성 폴더에서 Windows 탐색기 창을 여십시오.

시작 > 모든 프로그램 > OpenVPN > 바로 가기 > OpenVPN 구성 파일 디렉터리

3 \Program Files (x86)\OpenVPN\bin 폴더의 명령 프롬프트에서 다음 명령을 실행하여 OpenVPN 정적 키를 생성하십시오.

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

4 C1에서 연 폴더에 서버 구성 파일을 생성하고 파일을 "server.ovpn"으로 저장하십시오.

"server.ovpn" 파일은 다음 예와 같이 나타납니다.

```
dev tun

ifconfig 10.8.0.1 10.8.0.2

secret static.key

keepalive 10 120
```

참고: 로컬 네트워크에서 10.8.x.x 서브넷이 사용되고 있는 경우 **ifconfig** 명령에 다른 서브넷 범위를 사용하십시오.

참고: OpenVPN은 기본적으로 UDP 포트 1194를 사용합니다. 필요한 경우 OpenVPN 서버 및 클라이언트 구성 파일에 Port 명령을 추가하여 다른 포트 번호를 지정할 수 있습니다.

5 Windows 서비스 유틸리티를 사용하여 OpenVPN 서비스 시작 유형 속성을 **자동**으로 변경하십시오.

6 C1에서 명령 프롬프트를 열고 로컬 DNS(시스템 3)의 서브넷 주소와 DNS 서브넷 마스크를 대체하여 다음을 입력하십시오.

참고: 꺾쇠 괄호는 포함하지 마십시오.

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

시스템 2에서 OpenVPN 구성

암호화된 보안 연결을 사용하려면 시스템 1(C1)에서 OpenVPN을 구성한 후 시스템 2(C2)에서 OpenVPN을 구성해야 합니다.

49페이지의 "OpenVPN 구성" 참조

시스템 2에서 OpenVPN을 구성하려면 다음과 같이 하십시오.

1 다음 링크에서 OpenVPN 2.1.4를 다운로드하여 C2의 기본 위치에 설치하십시오.

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

2 다음 절차의 2단계에서 생성된 정적 키를 복사하십시오.

개인 클라우드 Backup Exec 인스턴스에서 OpenVPN 구성

3 C2의 다음 위치에 키를 붙여 넣으십시오.

\Program Files (x86)\OpenVPN\config

4 C2의 다음 위치에 클라이언트 구성 파일을 생성하고 파일을 "client.ovpn"으로 저장하십시오.

\Program Files (x86)\OpenVPN\config

"client.ovpn" 파일은 다음 예와 같이 나타납니다.

```
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** 문에 개인 클라우드 Backup Exec 시스템의 고정 IP 주소를 입력하십시오.

참고: 꺾쇠 괄호는 포함하지 마십시오.

---

6 로컬 네트워크에서 10.8.x.x 서브넷이 사용되고 있는 경우 파일을 편집하여 **ifconfig** 문에 다른 서브넷 범위를 사용하십시오.

7 Windows 서비스 유틸리티를 사용하여 OpenVPN 서비스 시작 유형 속성을 **자동**으로 변경하십시오.

로컬 네트워크 라우팅 구성

로컬 네트워크 라우팅을 구성하려면 TAP-Win32 Adapter V9 및 실제 네트워크 인터페이스에서 모두 IP 전달을 실행해야 합니다.

49페이지의 "OpenVPN 구성" 참조

로컬 네트워크 라우팅을 구성하려면 다음과 같이 하십시오.

1 시스템 2(C2)에서 레지스트리 편집기를 시작하고 다음 키를 찾으십시오.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

2 다음 레지스트리 값을 설정하십시오.

값 이름: **IPEnableRouter**

값 유형: **REG_DWORD**

값 데이터: **1**

참고: 값이 1이면 시스템에 설치되어 사용되는 모든 네트워크 연결에 대해 TCP/IP 전달이 실행됩니다.

---

3 C2를 재시작하십시오.

4 시스템 3(C3)의 명령 창에서 C2의 로컬 IP 주소를 대체하여 다음 명령을 입력하십시오.

참고: IP 주소를 입력할 때 꺾쇠 괄호는 포함하지 마십시오.

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

참고: 클라우드의 OpenVPN Server 시스템과 통신해야 하는 모든 로컬 네트워크 시스템에서 이 명령을 실행해야 합니다. Backup Exec Agent를 실행하고 개인 클라우드 Backup Exec 서버에서 작업을 복원할 대상이 되는 모든 서버에서 명령을 실행해야 합니다.

방화벽 구성

로컬 서버와 클라우드 서버 간에 통신이 제대로 수행되려면 표에 설명된 대로 네트워크 방화벽을 구성해야 합니다.

표 4-2 방화벽 구성

방화벽 인스턴스	조치
시스템 1(C1)	OpenVPN 네트워크 어댑터에 대해 Windows 방화벽을 실행 중지해야 합니다. OpenVPN이 사용하도록 구성된 포트에서 인바운드 트래픽을 허용하도록 Windows 방화벽을 구성해야 합니다. OpenVPN은 기본적으로 UDP 포트 1194를 사용합니다.
시스템 2(C2)	OpenVPN TAP 네트워크 어댑터에 대해 로컬 Windows 방화벽을 실행 중지해야 합니다.
로컬 네트워크	외부 로컬 또는 회사 방화벽이 있는 경우 OpenVPN이 사용하도록 구성된 포트에서 아웃바운드 트래픽을 허용하도록 방화벽을 구성해야 합니다. OpenVPN은 기본적으로 UDP 포트 1194를 사용합니다.

49페이지의 "OpenVPN 구성" 참조

OpenVPN 연결 확인

OpenVPN 구성을 마쳤으면 테스트하여 OpenVPN 서버와 클라이언트를 성공적으로 연결할 수 있는지 확인해야 합니다.

49페이지의 "OpenVPN 구성" 참조

OpenVPN 연결을 확인하려면 다음과 같이 하십시오.

1 Windows 서비스 유틸리티를 사용하여 시스템 1(C1)과 시스템 2(C2) 모두에서 OpenVPN 서비스를 시작하십시오.

2 C1과 C2의 다음 디렉터리에 있는 OpenVPN 로그 파일을 여십시오.

C:\Program Files (x86)\OpenVPN\log

3 두 파일에 모두 "Initialization Sequence Completed" 텍스트가 있는지 확인하십시오.

4 C1에서 기본 DNS 서버로 로컬 도메인의 DNS 서버를 가리키도록 TAP-Win32 네트워크 어댑터를 구성하십시오.

55페이지의 "TAP-Win32 네트워크 어댑터 구성" 참조

작업을 실행할 때 개인 클라우드 Backup Exec 인스턴스 VPN 링크 연결을 수동으로 시작하고 중지할 수 있습니다. 또는 VPN 링크 연결 상태를 유지하고 해당 인스턴스가 영구적으로 실행되도록 할 수 있습니다. 예약한 백업 작업을 시작하고 중지하려면 OpenVPN 서비스를 예약하여 프로세스를 자동화할 수 있습니다. 또한 Windows 예약된 태스크 유틸리티를 사용하여 해당 서비스에 대한 예약을 생성할 수 있습니다.

TAP-Win32 네트워크 어댑터 구성

OpenVPN 연결을 확인하려면 기본 DNS 서버로 로컬 도메인의 DNS 서버를 가리키도록 TAP-Win32 네트워크 어댑터를 구성해야 합니다.

54페이지의 "OpenVPN 연결 확인" 참조

TAP-Win32 네트워크 어댑터를 구성하려면 다음과 같이 하십시오.

1 **TAP 네트워크 어댑터 속성**을 여십시오.

2 **IPv4 속성**을 누르십시오.

3 **고급**을 누르십시오.

4 **DNS** 탭에서 로컬 네트워크 DNS 서버의 IP 주소를 입력하십시오.

5 **접미사** 필드에서 도메인 FQDN 접미사를 추가하고 접미사 목록의 맨 위로 이동하십시오.

6 **확인**을 눌러 모든 대화 상자를 종료하십시오.

7 시스템 1(C1)의 명령 프롬프트에서 다음 명령을 입력하십시오.

```
ipconfig /flushdns

ipconfig /registerdns
```

OpenVPN 연결 확인을 마쳤으면 Backup Exec 서버를 구성할 수 있습니다.

19페이지의 "클라우드에 멀티테넌트 또는 오프사이트 복사 구성 설정" 참조

28페이지의 "직접 백업 구성 설정" 참조

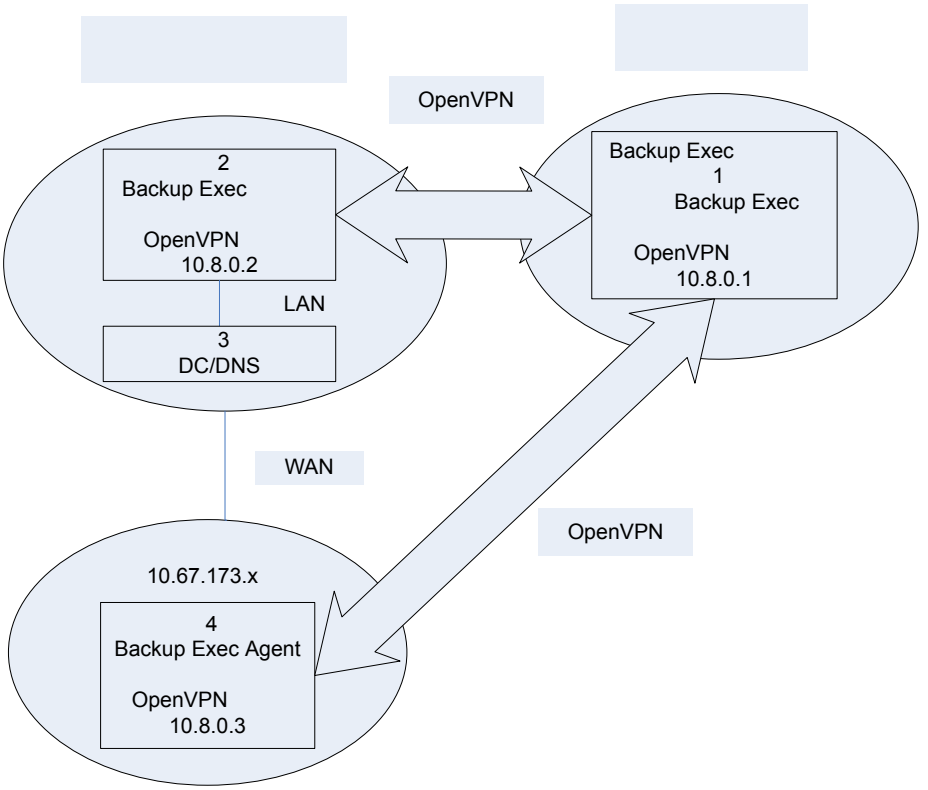
클라이언트에 대해 OpenVPN 구성

여러 클라이언트에서 사용되도록 OpenVPN을 구성할 수 있습니다. 복잡한 로컬 네트워크가 있는 경우 다중 클라이언트 VPN 구성을 사용해야 할 수도 있습니다. 예를 들어 로컬 서브넷을 여러 개 사용하는 경우 다중 클라이언트 VPN 구성이 유용할 수 있습니다.

49페이지의 "OpenVPN 구성" 참조

경고: 도메인 컨트롤러에 OpenVPN을 설치하면 안 됩니다. 다중 홈 도메인 컨트롤러 구성은 Backup Exec 개인 클라우드 서비스에서 지원되지 않습니다.

그림 4-1 다중 클라이언트 VPN 구성



OpenVPN 서버는 개인 클라우드 인스턴스입니다. 클라이언트는 로컬 LAN의 시스템입니다. OpenVPN 클라이언트를 여러 개 사용하려면 단일 클라이언트 구성에 사용하는 공유 키 텍스트 파일 대신 보안 인증서를 사용해야 합니다. 다중 클라이언트 구성에서는 각 OpenVPN 클라이언트에 고유한 키와 인증서가 있습니다.

참고: 키 파일이 중요합니다. 키 파일이 손상된 경우 다시 생성해야 합니다. CA(인증 기관) 키 파일이 손상된 경우 해당 CA를 기반으로 하는 모든 키를 다시 생성해야 합니다.

여러 클라이언트에 대해 OpenVPN을 구성하려면 공개적으로 사용 가능한 예를 참조하여 절차를 완료하십시오. 다음 사이트는 OpenVPN 인증서 및 여러 OpenVPN 클라이언트 구성에 대한 전체 지침을 제공합니다.

http://www.runpcrun.com

http://openvpn.net

복잡한 네트워크를 위한 또 다른 옵션은 로컬 네트워크 게이트웨이 라우터에서 OpenVPN을 사용하는 것입니다. 로컬 네트워크 게이트웨이 라우터는 지점 간 OpenVPN 연결을 제공합니다. OpenVPN 클라이언트와 시스템 네트워크 경로를 더 추가하지 않아도 다른 로컬 시스템이 VPN에 라우팅될 수 있습니다. OpenVPN 지원에 대한 자세한 내용은 라우터 제조업체 및 설명서에서 확인하십시오.

타사 소프트웨어 조직은 OpenVPN 지원이 포함된 라우터 펌웨어 업데이트도 제공합니다. 다음 사이트에서 예를 제공합니다.

http://www.dd-wrt.com

여러 클라이언트에 대해 OpenVPN을 구성한 후에는 클라이언트 데이터를 백업하는 직접 백업 작업을 생성하고 실행할 수 있습니다. 개인 클라우드 인스턴스를 직접 백업 작업 또는 중복 백업 작업의 백업 저장소로 사용할 수 있습니다.

네트워크 문제 해결

Backup Exec 개인 클라우드 서비스에 네트워크 문제가 있는 경우 OpenVPN 서버와 클라이언트를 성공적으로 연결할 수 있는지 확인해야 합니다.

네트워크 문제를 해결하려면 다음과 같이 하십시오.

1. Backup Exec 개인 클라우드 서비스 구성의 모든 시스템에 대해 Windows 방화벽을 일시적으로 해제하거나 적절한 ICMP 방화벽 예외를 추가하십시오.
2. Windows 서비스 유틸리티를 사용하여 시스템 1(C1)과 시스템 2(C2)에서 모두 OpenVPN 서비스를 시작하십시오.
3. C1과 C2의 다음 디렉터리에서 OpenVPN 로그 파일을 열고 각 파일에 "Initialization Sequence Completed" 텍스트가 있는지 확인하십시오.

   C:\Program Files (X86)\OpenVPN\log
4. C1, C2 및 시스템 3(C3)에서 10.8.0.1 및 10.8.0.2에 대해 ping을 수행하여 연결을 테스트하십시오.
5. C1에서 C2의 로컬 IP 주소와 C3의 로컬 IP 주소에 대해 ping을 수행하십시오.

   OpenVPN이 연결된 경우 OpenVPN 로컬 네트워크 어댑터 DNS 속성에 로컬 도메인 접미사가 포함되어 있는지 확인하십시오.