Dell EMC PowerStore
보안 구성 가이드

1.x

July 2020
개정 A02

참고, 주의 및 경고

노트: 참고"는 제품을 보다 효율적으로 사용하는 데 도움이 되는 중요 정보를 제공합니다.

주의: **주의사항은 하드웨어의 손상 또는 데이터 유실 위험을 설명하며, 이러한 문제를 방지할 수 있는 방법을 알려줍니다.**

경고: **경고는 재산 손실, 신체적 상해 또는 사망 위험이 있음을 알려줍니다.**

목차

서문

제품군을 향상시키기 위한 노력의 일환으로 소프트웨어와 하드웨어의 개정 버전을 정기적으로 릴리즈하고 있습니다. 이 문서에서 설명하는 일부 기능은 현재 사용 중인 소프트웨어 또는 하드웨어의 일부 버전에서 지원되지 않을 수 있습니다. 제품 릴리스 노트에는 제품 기능에 대한 최신 정보가 제공되어 있습니다. 제품이 올바르게 작동하지 않거나 이 문서에 설명된 대로 작동하지 않는 경우 기술 지원 전문가에게 문의하십시오.

지원 정보

지원, 제품 및 라이센스 정보는 다음과 같이 확인할 수 있습니다.

- **제품 정보**

  제품 및 기능 설명서 또는 릴리스 노트를 보려면 www.dell.com/powerstoredocs에서 PowerStore 설명서 페이지를 참조 바랍니다.

- **문제 해결**

  제품, 소프트웨어 업데이트, 라이선스 등록 및 서비스에 대한 자세한 내용은 www.dell.com/support에서 해당 제품 지원 페이지를 참조 바랍니다.

- **기술 지원**

  기술 지원 및 서비스 요청의 경우 www.dell.com/support에서 **Service Requests** 페이지를 참조 바랍니다. 서비스 요청을 개설하려면 유효한 지원 계약이 있어야 합니다. 유효한 지원 계약 체결에 대한 자세한 내용이나 계정 관련 질문에 대한 답을 얻으려면 영업 담당자에게 문의하십시오.

1

인증 및 액세스

이 장에서 다루는 내용은 다음과 같습니다.

주제:

사용자 계정, 역할 및 권한의 인증 및 관리

클러스터에 대한 액세스 인증은 사용자 계정의 자격 증명을 토대로 수행됩니다. 사용자 계정은 PowerStore Manager에서 **Settings** > **Users** > **Users**를 통해 액세스 가능한 **Users** 페이지에서 생성하고 이후 관리할 수 있습니다. 적용되는 인증은 사용자 계정과 연결된 역할에 따라 다릅니다. 웹 브라우저에 클러스터의 네트워크 주소를 URL로 지정하면 로컬 사용자로 인증할 수 있는 로그인 페이지가 표시됩니다. 사용자가 제공하는 자격 증명에 대해 인증이 수행되고 시스템에 세션이 생성됩니다. 이후부터 사용자는 사용자에게 할당된 역할의 기능 내에서 클러스터를 모니터링하고 관리할 수 있습니다.

클러스터는 관리 서버를 사용하는 보안 연결을 통해 사용자 이름 및 암호를 검증하여 사용자를 인증합니다.

공장 출하 기본값 관리

어플라이언스에는 초기 어플라이언스 액세스 및 구성에 사용하는 공장 출하 기본 사용자 계정이 함께 제공됩니다.

노트: 릴리스 1.0.x 버전의 경우 API, CLI, SMI-S 또는 서비스 명령 인터페이스를 사용하는 대신 PowerStore Manager UI를 사용하여 PowerStore를 초기에 구성하는 것이 좋습니다. 이렇게 하면 모든 기본 암호가 변경됩니다.

계정 유형	사용자 이름	암호	권한
시스템 관리	admin	Password123#	기본값 암호를 재설정하고, 어플라이언스 설정을 구성하고, 사용자 계정을 관리하기 위한 관리자 권한입니다.
서비스	서비스	서비스	서비스 작업을 수행하는 데 사용합니다. **노트:** 서비스 사용자는 SSH(secure shell) 액세스를 위해 존재합니다. 하지만 서비스 사용자를 사용하여 PowerStore Manager에 로그인할 수는 없습니다.

세션 규칙

클러스터의 세션에는 다음과 같은 특징이 있습니다.

- 만료 기간이 1시간입니다.
  노트: 세션이 비활성화된 후 사용자가 클러스터에서 자동으로 로그오프됩니다.
- 세션 시간 초과를 구성할 수 없습니다.

사용자 이름 및 암호 사용

시스템 계정 사용자 이름은 다음 요구 사항을 충족해야 합니다.

제한 사항	사용자 이름 요구 사항
구조	영숫자 문자로 시작하고 끝나야 합니다.
사례	모든 사용자 이름은 대/소문자를 구분하지 않습니다.
최소 영숫자 수	1
최대 영숫자 수	64
지원되는 특수 문자	. (dot)

시스템 암호는 다음 요구 사항을 충족해야 합니다.

제한 사항	암호 요구 사항
최소 문자 수	8
최소 대문자 수	1
최소 소문자 수	1
최소 숫자 수	1
최소 특수 문자 수 • 지원되는 문자: ! @ # $ % ^ * _ ~ ? **노트:** 암호에 작은따옴표('), 앰퍼샌드(&) 또는 공백이 포함될 수 없습니다.	1
최대 문자 수	40

노트: 가장 최근의 암호 5개는 다시 사용하지 못하도록 차단됩니다. 이전 암호는 5번째로 설정된 암호 이후부터 순서대로 재사용할 수 있습니다.

ESXi 암호

PowerStore X model 어플라이언스에서 ESXi의 기본 루트 암호는 ***<Service_Tag>_123!*** 형식이며 *<Service_Tag>*는 어플라이언스의 7자리 문자로 이루어진 Dell 서비스 태그입니다.

초기 클러스터 구성이 완료될 때까지 기본 ESXi 암호를 변경하면 안 됩니다. ESXi 암호를 변경하는 방법에 대한 자세한 내용은 VMware ESXi 설명서를 참조 바랍니다.

주의: ESXi 암호를 분실하지 않도록 주의해야 합니다. ESXi가 중단되고 암호가 사라진 경우 어플라이언스를 재초기화해야 합니다. 이 동작은 ESXi에서는 정상이지만 암호를 잃어버려 초기화할 때 데이터 손실이 발생할 수 있습니다.

주의: 기본 ESXi 암호는 각 PowerStore X model 어플라이언스에서 고유하게 구성됩니다. 이 암호는 어플라이언스의 노드가 vCenter 클러스터에 추가될 때 ESXi 호스트에서 인증하는 데 사용됩니다. 클러스터가 완전히 구성되기 전에 기본 암호를 변경하는 경우 어플라이언스를 초기화해야 합니다.

역할 및 권한

역할 기반 액세스 제어를 이용하면 여러 사용자가 서로 다른 권한을 가질 수 있습니다. 이로써 관리 역할이 기술 세트와 책임에 더욱 적절하게 부합하도록 관리 역할을 분리할 수 있습니다.

시스템이 지원하는 역할 및 권한은 다음과 같습니다.

노트: 상자 안의 ✓ 표시는 해당 역할에 대해 지원되는 권한을 나타내며 빈 상자는 해당 역할에 대해 지원되지 않는 권한을 나타냅니다.

작업	연산자	VM 관리자	보안 관리자	스토리지 관리자	관리자
시스템 로컬 암호 변경	✓	✓	✓	✓	✓
시스템 설정, 상태 및 성능 정보 보기	✓		✓	✓	✓
시스템 설정 수정					✓
리소스 및 보호 정책 생성, 수정, 삭제 및 SSH 활성화/비활성화				✓	✓
vCenter에 접속		✓		✓	✓
로컬 계정 목록 보기			✓		✓
로컬 계정 추가, 삭제 또는 수정			✓		✓
시스템의 VASA 공급자에 연결된 vCenter Server를 통해 시스템 스토리지 정보를 보고 VMware CA(certificate authority)/CA 인증서를 등록/다시 등록		✓			✓

파일과 관련된 역할 및 권한

이 시스템은 파일과 관련하여 다음과 같은 역할 및 권한을 지원합니다.

노트: 상자 안의 ✓ 표시는 해당 역할에 대해 지원되는 권한을 나타내며 빈 상자는 해당 역할에 대해 지원되지 않는 권한을 나타냅니다.

작업	연산자	VM 관리자	보안 관리자	스토리지 관리자	관리자
다음을 확인 바랍니다. • 파일 시스템 알림 • NTP 서버 목록 • 파일 시스템 목록 • 파일 사용자 할당량 목록 • 파일 인터페이스 라우트 목록 • 파일 인터페이스 목록 • SMB 공유 목록 • NFS 내보내기 목록	✓		✓	✓	✓
다음을 확인 바랍니다. • 파일 DNS 서버 또는 지정된 DNS 서버 목록	✓		✓	✓	✓

작업	연산자	VM 관리자	보안 관리자	스토리지 관리자	관리자
• 파일 FTP 서버 또는 지정된 FTP 서버 목록 • 파일 인터페이스 또는 지정된 파일 인터페이스 목록 • 파일 인터페이스 라우트 또는 지정된 인터페이스 라우트 목록 • 파일 Kerberos 서버 또는 지정된 Kerberos 서버 목록 • 파일 LDAP 서버 또는 지정된 LDAP 서버 목록 • 파일 NDMP 서버 또는 지정된 NDMP 서버 목록 • 파일 NIS 서버 또는 지정된 NIS 서버 목록 • 파일 시스템 또는 지정된 파일 시스템 목록 • 파일 트리 할당량 또는 지정된 파일 트리 할당량 목록 • 파일 사용자 할당량 또는 지정된 사용자 할당량의 목록 • 파일 바이러스 검사기 또는 지정된 파일 바이러스 검사기 목록 • NAS 서버 또는 지정된 NAS 서버 목록 • NFS 내보내기 또는 지정된 NFS 내보내기의 목록 • NFS 서버 또는 지정된 NFS 서버 목록 • SMB 서버 또는 지정된 SMB 서버 목록 • SMB 공유 또는 지정된 SMB 공유 목록					
지정된 NAS 서버 추가, 수정, 삭제, 핑 또는 지정된 NAS 서버에 암호, 호스트, 그룹 업로드				✓	✓
지정된 NAS 서버의 암호 또는 호스트 보기			✓		✓
기존 NAS 서버에서 파일 시스템 추가 또는 지정된 파일 시스템 수정, 삭제				✓	✓
지정된 파일 시스템에 클론 또는 스냅샷을 추가, 지정된 파일 시스템 새로고침, 복구 지정된 파일 시스템의 할당량 새로고				✓	✓
지정된 파일 트리 할당량 추가, 수정, 삭제, 새로고침				✓	✓
지정된 파일 사용자 할당량 추가, 수정, 삭제, 새로고침				✓	✓
파일 바이러스 검사기 추가 또는 지정된 파일 바이러스 검사기 수정, 삭제 또는 지정된 파일 바이러스 검사기 구성 업로드					✓

작업	연산자	VM 관리자	보안 관리자	스토리지 관리자	관리자
지정된 파일 바이러스 검사기 구성 다운로드			✓		✓
SMB 또는 NFS 서버 추가, 지정된 SMB 또는 NFS 서버 수정, 삭제, 연결, 해제				✓	✓
SMB 공유 추가 또는 지정된 SMB 공유 수정, 삭제				✓	✓
NFS 내보내기 추가 또는 지정된 NFS 내보내기 수정, 삭제				✓	✓
파일 인터페이스 추가 또는 지정된 파일 인터페이스 수정, 삭제				✓	✓
파일 인터페이스 라우트 추가 또는 지정된 파일 인터페이스 라우트 수정, 삭제				✓	✓
파일 DNS, 파일 FTP, 파일 Kerberos, 파일 LDAP, 파일 NDMP, 파일 NIS 서버 추가 또는 지정된 파일 DNS, 파일 FTP, 파일 Kerberos, 파일 LDAP, 파일 NDMP, 파일 NIS 서버 수정, 삭제				✓	✓
Keytab Kerberos 파일 업로드					✓
Keytab 파일 Kerberos 다운로드	✓		✓		✓
파일 LDAP 구성 또는 LDAP 인증서 업로드					✓
파일 LDAP 인증서 다운로드			✓		✓

역할 권한에 따른 사용자 계정 관리

관리자 또는 보안 관리자 역할을 가진 사용자는 사용자 계정 관리와 관련하여 다음과 같은 작업을 수행할 수 있습니다.

- 새 사용자 계정을 생성합니다.
- 기본으로 제공되는 관리자 계정을 제외한 모든 사용자 계정을 삭제합니다.

  노트: 기본으로 제공되는 관리자 계정은 삭제할 수 없습니다.
- 다른 사용자를 임의의 역할로 변경합니다.
- 사용자 암호를 재설정합니다.
- 다른 사용자 계정을 잠그거나 잠금 해제합니다.

  노트: 관리자 또는 보안 관리자 역할을 가진 로그인 사용자는 자신의 계정을 잠글 수 없습니다.

로그인한 사용자는 자신의 사용자 계정을 삭제할 수 없습니다. 또한 보안 관리자 또는 관리자 역할을 가진 사용자를 제외하고 로그인한 사용자는 자신의 암호만 변경할 수 있습니다. 사용자는 암호를 변경하려면 이전 암호를 제공해야 합니다. 로그인한 사용자는 자신의 암호를 재설정하거나 자신의 역할을 변경하거나 자신의 계정을 잠그거나 잠금 해제할 수 없습니다.

기본으로 제공되는 관리자 계정 프로필(관리자 역할)은 편집할 수 없으며 잠글 수 없습니다.

사용자의 역할 또는 잠금 상태가 변경되거나 사용자가 삭제되거나 보안 관리자 또는 관리자에 의해 암호가 변경되면 해당 사용자에 연결된 모든 세션이 무효화됩니다.

노트: 사용자가 세션 내에서 자신의 암호를 업데이트하는 경우 세션은 활성화 상태로 유지됩니다.

관리자 및 서비스 계정 암호 재설정

어플라이언스는 배송 시에 초기 구성을 수행하는 데 사용할 수 있는 기본 관리자 사용자 계정이 함께 제공됩니다. 전문적인 서비스 기능을 수행하는 데 사용할 수 있는 기본 서비스 사용자 계정과 함께 제공됩니다. 초기에 REST API 또는 the CLI와 같은 방법보다는 PowerStore Manager Ui를 사용하여 PowerStore을 구성하는 것이 좋습니다. PowerStore Manager Ui를 사용하면 모든 기본 암호가 변경됩니다. 새 암호를 잊은 경우 다음과 같이 암호를 다시 기본값으로 재설정할 수 있습니다.

암호를 재설정하는 방법은 어플라이언스가 PowerStore T model인지 PowerStore X model인지에 따라 다릅니다. 해당되는 어플라이언스에 알맞은 방법을 사용하여 관리자 암호나 서비스 암호, 또는 두 암호를 모두 재설정합니다.

PowerStore T model 어플라이언스에서 관리자 및 서비스 계정 암호를 기본값으로 재설정

이 작업 정보

PowerStore T model 어플라이언스의 경우, 관리자 또는 서비스 사용자 암호를 재설정하는 기본적인 방법은 USB 드라이브를 사용하는 것입니다. 지원되는 파일 시스템에는 FAT32와 ISO 9660이 포함됩니다.

노트: 어플라이언스가 서비스 모드에 있을 때 암호를 재설정하려면 한 가지 차이점를 가진 다음 단계를 따릅니다. 각 노드에 USB 재설정 절차를 적용합니다. 이 작업을 수행하면 시스템이 정상 모드로 다시 전환되어 PowerStore Manager에 로그인할 때 관리자와 서비스 사용자 모두에 새 암호를 입력하라는 메시지가 표시됩니다.

단계

1. USB 드라이브를 포맷하는 경우 이 다음 단계로 이동합니다. 그렇지 않은 경우에는 `format <d:> /FS:FAT32` 같은 명령 프롬프트를 사용하여 드라이브를 포맷합니다.

   여기서 `d:`는 노트북 또는 PC에 삽입한 USB 드라이브의 드라이브 문자입니다.

2. 다음 명령을 사용하여 레이블을 설정합니다.

   ```
   label d:
   RSTPWD
   ```

   노트: 어플라이언스는 `RSTPWD` 레이블이 없는 USB 드라이브를 탑재하지 않습니다. USB 드라이브에 레이블을 지정하고 나서 재설정하려는 계정 암호에 대한 빈 파일을 삽입합니다. 관리자 계정 또는 서비스 계정의 암호를 재설정하거나 두 가지 모두를 재설정할 수 있습니다.

3. 드라이브에 빈 파일을 생성하려면 필요에 따라 다음 명령 중 하나 또는 둘 다를 사용합니다.

   ```
   copy NUL d:\admin
   copy NUL d:\service
   ```

4. USB 드라이브를 어플라이언스의 아무 쪽 노드에 있는 USB 포트에 삽입하고 10초 동안 기다린 후에 분리합니다.
   재설정하려는 각 계정에 대한 암호는 이제 기본값이 됩니다.
5. 클러스터 IP 주소를 사용하여 브라우저를 통해 클러스터에 연결하고 기본값 초기 암호(**`Password123#`**)를 사용하여 admin으로 로그인합니다.
   관리자 또는 서비스 암호를 재설정하라는 프롬프트가 표시될 것입니다. SSH(secure shell)를 사용하여 서비스 암호를 재설정하려는 경우 서비스 계정의 초기 기본값 암호는 **`service`**입니다.
6. 관리자 암호를 기본값에서 사용자 지정 암호로 변경합니다.
7. 서비스 계정 암호를 관리자 암호와 다른 것으로 설정하려면 관련 확인란을 선택 취소합니다.

결과

이 절차를 실행한 후에도 로그인 시도 시 암호를 재설정하라는 프롬프트가 표시되지 않으면 서비스 공급업체에 문의합니다.

PowerStore X model 어플라이언스에서 관리자 및 서비스 계정 암호를 기본값으로 재설정

전제조건

기본 어플라이언스의 기본 노드 이름(예: PSTX-44W1BW2-A PowerStore D6013)을 알고 있어야 합니다. 필요한 경우 `reset.iso` 파일을 생성합니다.

이 작업 정보

PowerStore X model 어플라이언스의 경우 ISO 이미지를 사용하여 vSphere에서 마운트합니다. 미리 생성된 이미지 파일은 www.dell.com/support에서 다운로드할 수 있습니다. 어떤 암호를 재설정해야 하는지에 따라, 다음 터치 명령 중 하나 또는 둘 모두를 사용하여 Linux 시스템으로부터 보유한 이미지를 생성할 수도 있습니다.

```
mkdir iso
touch iso/admin
touch iso/service
mkisofs -V RSTPWD -o reset.iso iso
```

노트: ISO 이미지 `reset.iso`는 데이터 저장소에 상주해야 vSphere에서 가상 CD로 마운트할 수 있습니다.

노트: 어플라이언스가 서비스 모드에 있을 때 암호를 재설정하려면 두 가지 차이점를 가진 다음 단계를 따릅니다. 먼저, 공개 데이터스토어는 사용할 수 없기 때문에 ISO 이미지를 컨트롤러 가상 머신(VM) 자체의 PRIVATE-C9P42W2.A.INTERNAL 데이터스토어에 업로드해야 합니다. 둘째로, 컨트롤러 VM 노드 A와 B 모두에 `reset.iso` 파일을 업로드하고 적용합니다. 이 작업을 수행하면 시스템이 정상 모드로 다시 전환되어 PowerStore Manager에 액세스할 수 있을 때 관리자와 서비스 사용자 모두에 새 암호를 입력하라는 메시지가 표시됩니다.

단계

1. vSphere에서 **Storage** 아래의 PowerStore X model 어플라이언스를 선택합니다.

   예시: **DataCenter-WX-D6013** > **PowerStore D6013**

2. **Files**에서 **ISOs**를 선택합니다.
3. **Upload**를 선택하고 `reset.iso` 파일을 업로드합니다. 이 파일은 www.dell.com/support 또는 Linux 시스템에서 생성한 이미지 파일입니다.
   ISOs 폴더에 `reset.iso` 파일이 나타납니다.
4. vSphere에서 **Host and Clusters** 아래, 클러스터 내 기본 PowerStore X model 어플라이언스의 기본 노드를 선택합니다.

   예시: **DataCenter-WX-D6013** > **Cluster WX-D6013** > **PSTX-44W1BW2-A**

5. **Summary** 아래에서 **CD/DVD drive 1**을 클릭하고 **Connect to datastore ISO file**을 선택합니다.
   Choose an ISO image to mount 창이 나타납니다.
6. **Datastores** 아래, 클러스터 내 기본 PowerStore X model 어플라이언스를 클릭하고 **ISOs** 폴더를 선택합니다.
   `reset.iso` 파일이 **Contents** 아래에 나타나야 합니다.
7. `reset.iso` 파일을 선택하고 **Ok**를를 클릭합니다.
   Summary 아래, **CD/DVD drive 1** 이 약 10초 동안 **Connected**로 나오고 그 후 **Disconnected**로 변경되야 합니다. 이제 클러스터 관리자 암호나 서비스 암호 또는 둘 다가 기본값으로 재설정됩니다.
8. 클러스터 IP 주소를 사용하여 브라우저를 통해 클러스터에 연결하고 기본값 초기 암호(**`Password123#`**)를 사용하여 admin으로 로그인합니다.
   관리자 또는 서비스 암호를 재설정하라는 프롬프트가 표시될 것입니다. SSH를 사용하여 서비스 암호를 재설정하려는 경우 서비스 계정의 초기 기본값 암호는 **`service`**입니다.
9. 관리자 암호를 기본값에서 사용자 지정 암호로 변경합니다.
10. 서비스 계정 암호를 관리자 암호와 다른 것으로 설정하려면 관련 확인란을 선택 취소합니다.

결과

이 절차를 실행한 후에도 로그인 시도 시 암호를 재설정하라는 프롬프트가 표시되지 않으면 서비스 공급업체에 문의합니다.

인증서

PowerStore의 인증서 저장소에 있는 데이터는 영구적입니다. 인증서 저장소에는 다음과 같은 유형의 인증서가 저장됩니다.

- CA(인증 기관) 인증서
- 클라이언트 인증서

- 서버 인증서

인증서 보기

이 작업 정보

어플라이언스에 저장된 각 인증서에 대해 다음과 같은 정보가 PowerStore Manager 에 표시됩니다.

- `Service`
- `Type`
- `Scope`
- `Issued by`
- `Valid`
- `Valid to`
- `Issued to`

노트: REST API 또는 CLI를 사용하여 추가 인증서 정보를 볼 수 있습니다.

인증서 정보를 보려면 다음을 수행합니다.

단계

1. PowerStore Manager를 실행합니다.
2. **Settings**를 클릭하고 **Security**에서 **Certificates**를 클릭합니다.
   어플라이언스에 저장된 인증서에 대한 정보가 표시됩니다.
3. 인증서 및 서비스 관련 정보가 포함된 인증서 체인을 보려면 해당 서비스를 클릭합니다.
   View Certificate Chain이 표시되고 그 인증서를 포함하는 인증서 체인에 대한 정보가 나열됩니다.

클러스터 내 PowerStore 어플라이언스 간의 보안 통신

클러스터를 생성하는 동안 클러스터 마스터 어플라이언스의 기본 노드는 클러스터 CA라고도 불리는 CA(certificate authority) 인증서를 생성합니다. 마스터 어플라이언스는 클러스터에 연결된 어플라이언스로 클러스터의 CA 인증서를 전달합니다.

클러스터의 각 PowerStore 어플라이언스는 CA 인증서에 의해 서명된 고유의 IPsec 인증서를 생성합니다. PowerStore 어플라이언스가 클러스터 네트워크를 통해 전송하는 민감한 데이터는 IPsec 및 TLS에 의해 보호되어 데이터의 보안과 무결성이 보호됩니다.

복제 및 데이터 가져오기에 대한 보안 통신

PowerStore의 인증서 및 자격 증명 인프라스트럭처에서는 서버 및 클라이언트 인증서와 사용자 자격 증명을 교환할 수 있습니다. 이 프로세스에는 다음이 포함됩니다.

- TLS 핸드셰이크 중에 서버 인증서 검색 및 검증
- 원격 시스템의 신뢰할 수 있는 CA 인증서를 자격 증명 저장소에 추가
- 신뢰할 수 있는 서버/클라이언트 인증서를 자격 증명 저장소에 추가
- 신뢰가 수립된 후 보안 연결 수립 지원

PowerStore에서는 다음과 같은 관리 기능이 지원됩니다.

- 복제의 경우, 신뢰할 수 있는 관리 통신을 수립하기 위해 두 PowerStore 클러스터 간에 인증서를 교환합니다. PowerStore 클러스터 간 복제를 용이하게 하려면 복제 REST 제어 요청 발행 시 상호 TLS 인증을 허용하도록 클러스터 간 양방향 신뢰를 수립해야 합니다.
- 데이터 가져오기의 경우, 지속성이 있는 인증서 및 자격 증명을 사용하여 Dell EMC 스토리지 시스템(VNX, Unity, SC(Storage Center) 또는 PS(Peer Storage) 시스템)과 PowerStore 클러스터 간의 보안 연결을 수립합니다.

Storage Awareness 지원에 대한 vSphere Storage API

VASA(vSphere Storage API for Storage Awareness)는 스토리지 지원을 위해 VMware에서 정의한 API로, 특정 공급업체에 구애받지 않는 특성을 가지고 있습니다. VASA Provider는 수신되는 VASA API 요청을 처리하기 위해 서로 협력하는 여러 구성 요소로 이루어져 있

습니다. 수신되는 모든 VASA API를 수신하는 VASA API 게이트웨이는 PowerStore 클러스터에서 기본 어플라이언스(부동 관리 IP를 소유하는 어플라이언스)에 배포됩니다. ESXi 호스트와 vCenter Server는 VASA Provider에 연결하여 사용 가능한 스토리지 토폴로지, 기능 및 상태에 대한 정보를 얻습니다. 이후 vCenter Server는 vSphere 클라이언트에 이 정보를 제공합니다. PowerStore Manager 클라이언트가 아니라 VMware 클라이언트가 VASA를 사용합니다.

vSphere 사용자는 이러한 VASA Provider 인스턴스를 클러스터에 대한 VASA 정보 공급자로 구성해야 합니다. 리드 어플라이언스가 중단될 경우 관련 프로세스는 다음 차례로 기본 어플라이언스가 되는 어플라이언스에서 VASA Provider와 함께 다시 시작됩니다. IP 주소는 자동으로 페일오버됩니다. 내부적으로는 새로운 활성 VASA Provider에서 구성 변경 이벤트를 가져올 때 프로토콜에 장애가 발생하지만 이를 통해 사용자 개입 없이 VASA 객체의 자동 재동기화가 일어납니다.

PowerStore에서는 vSphere 6.5 및 6.7에 대한 VASA 3.0 인터페이스를 제공합니다.

VASA 3.0은 VVol(Virtual Volumes)을 지원합니다. VASA 3.0은 VVol 및 스토리지 컨테이너 같은 스토리지 추상화를 쿼리하기 위한 인터페이스를 지원합니다. 이 정보는 SPBM(storage policy based management)에서 가상 드라이브의 배치와 규정 준수에 대한 결정을 내리는 데 도움이 됩니다. VASA 3.0은 가상 드라이브를 백업하는 데 사용되는 VVol의 수명 주기를 프로비저닝하고 관리할 수 있는 인터페이스도 지원합니다. 이런 인터페이스는 ESXi 호스트에 의해 직접 호출됩니다.

VASA, vSphere 및 VVol과 관련된 자세한 내용은 VMware 설명서 및 PowerStore Manager 온라인 도움말을 참조 바랍니다.

VASA와 관련된 인증

vCenter에서 PowerStore Manager VASA Provider로의 연결을 시작하려면 vSphere 클라이언트를 사용하여 다음 정보를 입력합니다.

- VASA 3.0에 대해 https://<Management IP address>:8443/version.xml 형식을 사용하는 VASA Provider URL.
- PowerStore Manager 사용자의 사용자 이름(역할이 VM 관리자 또는 관리자여야 함).

  노트: VM 관리자 역할은 인증서를 등록하는 수단으로 엄격하게 사용됩니다.
- 이 사용자와 연결된 암호.

여기에서 사용되는 PowerStore Manager 자격 증명은 연결 중 이 초기 단계 동안만 사용됩니다. PowerStore Manager 자격 증명이 타겟 클러스터에 대해 유효한 경우 vCenter Server 인증서가 클러스터에 자동 등록됩니다. 이 인증서는 이후 vCenter로부터의 모든 요청을 인증하는 데 사용됩니다. 이 인증서를 VASA Provider에 설치 또는 업로드하기 위한 수작업은 필요하지 않습니다. 인증서가 만료된 경우 새로운 세션을 지원하려면 vCenter는 새 인증서를 등록해야 합니다. 인증서를 사용자가 취소하는 경우 세션이 무효가 되고 연결이 끊어집니다.

vCenter 세션, 보안 연결 및 자격 증명

vSphere 관리자가 vSphere Client를 사용해 vCenter Server에 VASA Provider URL 및 로그인 자격 증명을 제공하면 vCenter 세션이 시작됩니다. vCenter Server는 VASA Provider의 URL, 자격 증명 및 SSL 인증서를 사용해 VASA Provider와 보안 연결을 설정합니다. 다음 이벤트 중 하나가 발생하면 vCenter 세션이 종료됩니다.

- 관리자가 vSphere Client를 사용해 VASA Provider를 vCenter 구성에서 제거하고 vCenter Server가 연결을 종료합니다.
- vCenter 서버에 장애가 발생하거나 vCenter Server 서비스에 장애가 발생하여 연결이 종료됩니다. vCenter 또는 vCenter Server 서비스는 SSL 연결을 다시 설정할 수 없는 경우 새 서비스를 시작합니다.
- VASA Provider에 장애가 발생하여 연결이 종료됩니다. VASA Provider가 시작되면 vCenter Server로부터의 통신에 응답하여 SSL 연결과 VASA 세션을 다시 설정할 수 있습니다.

vCenter 세션은 vCenter Server와 VASA Provider 사이의 보안 HTTPS 통신을 기반으로 합니다. VASA 3.0에서 vCenter Server는 VMCA(VMware certificate authority)의 역할을 합니다. VASA Provider는 요청을 인증한 후 요청 시 자체 서명 인증서를 전송합니다. VASA Provider는 신뢰 저장소에 인증서를 추가한 후 인증서 서명 요청을 실행하고 자체 서명된 인증서를 VMCA 서명된 인증서로 바꿉니다. 그 이후의 연결은 VASA Provider가 이전에 등록된 루트 서명 인증서에 대해 검증된 클라이언트 SMS(Storage Monitoring Service) 인증서를 사용하여 인증합니다. VASA Provider는 스토리지 엔터티 객체에 대한 고유 식별자를 생성하고 vCenter Server는 이 식별자를 사용하여 특정 엔터티에 대한 데이터를 요청합니다.

VASA Provider는 SSL 인증서와 VASA 세션 식별자를 사용하여 VASA 세션을 검증합니다. 세션이 설정된 후 VASA Provider는 SSL 인증서와 vCenter Server에서의 각 함수 호출과 연결된 VASA 세션 식별자를 모두 검증해야 합니다. VASA Provider는 신뢰 저장소에 저장된 VMCA 인증서를 사용하여 vCenter SMS에서의 함수 호출과 연결된 인증서를 검증합니다. VASA 세션은 여러 SSL 연결에 걸쳐 계속 유지됩니다. SSL 연결이 끊어진 경우 vCenter Server는 VASA Provider와의 SSL 핸드셰이크를 통해 동일한 VASA 세션의 컨텍스트 내에서 SSL 연결을 다시 설정합니다. SSL 인증서가 만료되면 vSphere 관리자는 새 인증서를 생성해야 합니다. vCenter Server는 새 SSL 연결을 설정하고 VASA Provider에 새 인증서를 등록합니다.

주의: SMS는 3.0 VASA Provider에 `unregisterVASACertificate` 함수를 호출하지 않습니다. 따라서 등록 취소 후에도 VASA Provider는 SMS에서 얻은 VMCA 서명 인증서를 계속 사용할 수 있습니다.

CHAP 인증

CHAP(Challenge Handshake Authentication Protocol)는 iSCSI 이니시에이터(호스트) 및 타겟(볼륨 및 스냅샷)을 인증하는 방법입니다. CHAP는 iSCSI 스토리지를 노출하고 동시에 안전한 표준 스토리지 프로토콜을 보장합니다. 인증은 인증자와 피어 모두에게 알려진 비밀 정보(암호와 유사)를 이용합니다. CHAP 프로토콜은 다음과 같은 두 가지 변형이 있습니다.

- 단일 CHAP 인증을 사용하면 iSCSI 타겟이 이니시에이터를 인증할 수 있습니다. 이니시에이터는 타겟에 연결을 시도할 때(일반 모드 또는 검색 모드) 사용자 이름과 암호를 타겟에 제공합니다.
- 단일 CHAP 외에 상호 CHAP 인증도 적용됩니다. 상호 CHAP를 사용하면 iSCSI 타겟과 이니시에이터가 서로 인증할 수 있습니다. 그룹에서 제공하는 각 iSCSI 타겟은 iSCSI 이니시에이터가 인증합니다. 이니시에이터가 타겟에 연결을 시도할 때 타겟은 사용자 이름과 암호를 이니시에이터에 제공합니다. 이니시에이터는 제공된 사용자 이름과 암호를 저장된 정보와 비교합니다. 정보가 일치하는 경우 이니시에이터가 대상에 연결할 수 있습니다.

노트: 사용자 환경에서 CHAP가 사용되는 경우에는 데이터를 수신할 볼륨을 준비하기 전에 CHAP 인증을 설정하고 활성화하는 것이 좋습니다. CHAP 인증을 설정하고 활성화하기 전에 데이터 수신을 위해 드라이브를 준비하면 볼륨에 대한 액세스 권한을 상실할 수 있습니다.

PowerStore에서는 iSCSI CHAP 검색 모드가 지원되지 않습니다. 다음 표에는 iSCSI CHAP 검색 모드와 관련된 PowerStore의 제한 사항이 나와 있습니다.

표 1. iSCSI CHAP 검색 모드 제한 사항

CHAP 모드	단일 모드(이니시에이터 활성화)	상호 모드(이니시에이터 및 타겟 활성화)
검색	PowerStore은 호스트를 인증(도전)하지 않습니다. 인증을 사용하여 대상의 검색을 배제 시킬 수 없습니다. 이로 인해 사용자 데이터에 의도하지 않은 액세스가 발생 하는 것은 아닙니다.	PowerStore은 호스트의 인증 요청(도전)에 응답하지 않으며 호스트가 PowerStore에 도전하는 경우 검색이 실패합니다.
정상	예상대로 작동합니다. 자격 증명은 PowerStore에 의해 테스트됩니다.	예상대로 작동합니다. 자격 증명은 PowerStore에 의해 전송됩니다.

소스 및 타겟 어플라이언스 간의 원격 복제의 경우, 확인 및 업데이트 프로세스는 로컬 시스템과 원격 시스템의 변경 내용을 감지하고 데이터 연결을 새로 수립하며 CHAP 설정도 고려합니다.

CHAP 구성

PowerStore 클러스터에서 CHAP 단일 인증(이니시에이터 활성화) 또는 상호 인증(이니시에이터 및 타겟)을 활성화할 수 있습니다. CHAP는 하나의 어플라이언스 또는 여러 PowerStore 어플라이언스와 외부 호스트의 클러스터 구현에 사용할 수 있습니다.

단일 인증을 사용하는 경우에는 외부 호스트를 추가할 때 각 이니시에이터에 대한 사용자 이름과 암호를 입력해야 합니다. 상호 인증을 사용하는 경우에는 클러스터에 대한 사용자 이름 및 암호도 입력해야 합니다. 호스트를 추가하고 CHAP가 활성화된 이니시에이터를 추가하는 경우 이니시에이터 암호는 고유해야 하며 호스트의 이니시에이터 간에 동일한 암호를 사용할 수 없습니다. 외부 호스트의 CHAP 구성을 구성하는 방법에 대한 자세한 내용은 상황에 따라 다릅니다. 이 기능을 활용하려면 호스트의 운영 체제와 호스트를 구성하는 방법을 숙지해야 합니다.

노트: 시스템에서 호스트가 구성된 후에 CHAP를 활성화하는 것은 외부 호스트에 대해 운영 중단적인 동작으로 작용합니다. 이 경우 외부 호스트와 어플라이언스 모두에 대한 구성이 설정될 때까지 I/O가 중단됩니다. 구현하고 싶은 CHAP 구성이 있는 경우 어플라이언스에 외부 호스트를 추가하기 전에 그 유형을 결정하는 것이 좋습니다.

호스트가 추가된 후에 CHAP를 활성화하는 경우 각 호스트의 이니시에이터를 업데이트합니다. CHAP가 활성화되면 CHAP 자격 증명이 없는 호스트 그룹에 호스트를 추가할 수 없습니다. CHAP가 활성화되어 있고 나중에 호스트를 추가하는 경우 PowerStore Manager에서 **Compute** 아래 **Hosts & Host Groups**를 선택해 수동으로 호스트를 등록합니다. 인증을 사용하려면 iSCSI 수준에서 자격 증명을 입력해야 합니다. 이 경우 호스트에서 IQN을 복사한 다음 각 이니시에이터에 대한 관련 CHAP 자격 증명을 추가합니다.

다음 중 하나를 통해 클러스터에 대한 CHAP를 구성할 수 있습니다.

- **Chap** - PowerStore Manager (**Settings** 클릭 후 **Security**에서 **CHAP** 선택)에서 액세스할 수 있는 CHAP 설정 페이지.
- REST API 서버 - CHAP 설정을 구성하라는 REST API 요청을 수신할 수 있는 애플리케이션 인터페이스. REST API에 대한 자세한 정보는 *PowerStore REST API Reference Guide* 내용을 참조 바랍니다.

PowerStore Manager에서 CHAP의 상태를 확인하려면 **Settings**를 클릭하고 **Security**에서 **CHAP**를 선택합니다.

외부 SSH 액세스

각 어플라이언스는 어플라이언스 IP 주소의 SSH(secure shell) 포트에 대해 외부 SSH 액세스를 선택적으로 활성화할 수 있습니다. 이 때 사용자는 어플라이언스의 기본 노드에서 서비스 기능으로 이동됩니다. 어플라이언스 IP 주소는 기본 지정 사항이 변경될 때 어플라이언스의 두 노드 간에 변경됩니다. 외부 SSH가 비활성화된 경우, SSH 액세스가 허용되지 않습니다.

어플라이언스가 처음에 실행되고 구성되지 않은 경우에는 SSH가 기본적으로 활성화되어 클러스터에 추가되기 전에 문제가 발생한 경우 어플라이언스를 서비스할 수 있습니다. 새 클러스터가 생성되거나 클러스터 작업에 연결되는 경우 모든 어플라이언스의 SSH는 처음에 비활성화로 설정되어야 합니다.

외부 SSH 액세스 구성

다음 방법 중 하나를 사용하여 클러스터 내에서 외부 SSH 대한 액세스를 구성할 수 있습니다.

- **SSH Management** - PowerStore Manager(**Settings** 클릭 후 **Security**에서 **SSH Management** 선택)에서 액세스할 수 있는 SSH 설정 페이지.
- REST API 서버 – SSH 설정을 구성하도록 REST API 요청을 수신할 수 있는 애플리케이션 인터페이스. REST API에 대한 자세한 정보는 *PowerStore REST API Reference Guide* 내용을 참조 바랍니다.
- `svc_service_config` – 서비스 사용자로서 어플라이언스에 직접 입력할 수 있는 서비스 명령입니다. 이 명령에 대한 자세한 정보는 *PowerStore Service Scripts Guide* 문서를 참조 바랍니다.

PowerStore Manager에서 SSH의 상태를 확인하려면 **Settings**를 클릭하고 **Security**에서 **SSH Management**를 선택합니다. 또한 선택하는 하나 이상의 어플라이언스에서 SSH를 활성화 또는 비활성화할 수 있습니다.

SSH 서비스를 성공적으로 활성화한 후에는 아무 SSH 클라이언트를 사용하여 어플라이언스 IP 주소에 로그인할 수 있습니다. 어플라이언스에 액세스하려면 서비스 사용자 자격 증명이 필요합니다.

서비스 계정을 사용하여 사용자는 다음 기능을 수행할 수 있습니다.

- 어플라이언스 시스템 설정 및 작업을 모니터링하고 문제 해결하는 특수 어플라이언스 서비스 스크립트를 실행할 수 있습니다.
- 제한된 셸 모드에서 권한이 없는 Linux 사용자 계정의 멤버로서 제한적으로 할당된 명령의 집합만을 작동합니다. 이 계정에서는 전용 시스템 파일, 구성 파일 또는 사용자/고객 데이터에 액세스할 수 없습니다.

어플라이언스 보안을 최대화하려면 어플라이언스에서 서비스 작업을 수행하기 위해 특별히 필요하지 않는 한 외부 SSH 서비스 인터페이스를 항상 해제 상태로 두는 것이 좋습니다. 필요한 서비스 작업을 수행한 후 SSH 인터페이스를 해제하여 어플라이언스을 안전한 상태로 유지합니다.

SSH 세션

PowerStore SSH 서비스 인터페이스 세션은 SSH 클라이언트가 구성한 설정에 따라 관리됩니다. 세션의 특징은 SSH 클라이언트 구성 설정에 의해 결정됩니다.

사용자 계정 암호

서비스 계정은 서비스 담당자가 기본 Linux 명령을 수행하는 데 사용할 수 있는 계정입니다.

어플라이언스를 초기 구성하는 동안 기본 서비스 암호를 변경해야 합니다. 서비스 암호 제한 사항은 시스템 관리 계정에 적용되는 제한 사항과 동일합니다(사용자 이름 및 암호 사용 페이지 7 참조).

SSH 인증

서비스 계정 인증은 다음을 기반으로 합니다.

- 애플리케이션 격리 - PowerStore 소프트웨어는 애플리케이션 격리를 제공하는 컨테이너 기술을 사용합니다. 어플라이언스 서비스 액세스는 서비스 컨테이너에 의해 제공되며, 서비스 스크립트 세트 및 Linux 명령 세트만 사용할 수 있습니다. 서비스 계정은 파일 시스템을 제공하는 다른 컨테이너에 액세스하고 사용자에 대한 I/O를 차단할 수 있는 기능이 없습니다.
- Linux 파일 시스템 권한 - 시스템 작업을 수정하는 대부분의 Linux 도구 및 유틸리티는 서비스 사용자가 사용할 수 없으며 슈퍼유저 계정 권한이 필요합니다. 서비스 계정에는 이러한 액세스 권한이 없으므로 Linux 툴 및 유틸리티를 사용할 수 없고, 읽기, 수정 또는 두 작업 모두를 수행하는 데 루트 액세스가 필요한 구성 파일을 편집할 수 없습니다.

- 액세스 제어 - 컨테이너 기술을 통해 제공되는 애플리케이션 격리 외에, 어플라이언스의 ACL(Access Control List) 메커니즘은 서비스 계정의 시스템 리소스 액세스를 명시적으로 부여하거나 거부하기 위한 매우 구체적인 규칙 목록을 사용합니다. 이러한 규칙은 표준 Linux 파일 시스템 권한에 의해 정의되지 않은 기타 어플라이언스 영역에 대한 서비스 계정 권한을 지정합니다.

어플라이언스 서비스 스크립트

어플라이언스의 소프트웨어 버전에 문제 진단, 시스템 구성 및 시스템 복구를 위한 문제 진단 세트가 설치됩니다. 이러한 스크립트는 PowerStore Manager를 통해 사용할 수 있는 것보다 더 심층적인 수준의 정보와 더 하위 레벨의 시스템 제어를 제공합니다. *PowerStore Service Scripts Guide*에서는 이러한 스크립트에 대해 설명하고 일반적인 활용 사례를 보여줍니다.

어플라이언스 노드 이더넷 서비스 포트 및 IPMItool

어플라이언스는 각 노드에 있는 이더넷 서비스 포트를 통해 콘솔 액세스를 제공합니다. 이와 같이 액세스하려면 IPMItool을 사용해야 합니다. IPMItool은 SSH 또는 텔넷과 유사한 네트워크 도구로, IPMI 프로토콜을 사용하는 이더넷 연결을 통해 각 노드와 통신합니다. IPMItool은 어플라이언스의 노드 콘솔을 액세스하기 위해 안전한 통신 채널을 협상하는 Windows 유틸리티입니다. 이 유틸리티를 사용하려면 콘솔을 활성화하기 위해 물리적 액세스가 필요합니다.

노드 이더넷 서비스 포트 인터페이스는 SSH 인터페이스(Service LAN interface)와 동일한 기능을 제공하며 동일한 제한 사항이 적용될 수 있습니다. 하지만 SSH 클라이언트가 아닌 이더넷 포트 연결을 통해 사용자가 인터페이스를 액세스합니다. 이 인터페이스는 네트워크를 방해하지 않고 어플라이언스에 연결할 수 있는 현장 서비스 담당자를 위한 것입니다. 전용 관리 콘솔은 필요하지 않습니다.

이 인터페이스는 라우팅 불가능한 직접 지점 간 연결을 제공합니다. 서비스 담당자는 초기 구성 마법사를 포함한 PowerStore Manager 및 PowerStore 서비스로 컨테이너에 SSH 액세스, 콘솔 출력에 서비스 LAN 인터페이스를 사용할 수 있습니다. 서비스 LAN 인터페이스를 통한 서비스 컨테이너로의 SSH 액세스가 항상 활성화되며 비활성화할 수 없습니다. 하지만 서비스 계정 자격 증명은 직접 관리하셔야 합니다.

서비스 스크립트 목록은 *PowerStore Service Scripts Guide*를 참조 바랍니다.

NFS 보안

NFS 보안은 NFSv3 및 NFSv4를 사용하여 사용자를 인증하기 위해 Kerberos를 사용하는 것입니다. Kerberos는 무결성(서명) 및 개인 정보 보호(암호화) 기능을 제공합니다. 무결성 및 개인 정보 보호를 활성화할 필요가 없습니다. 이들은 NFS 내보내기 옵션입니다.

Kerberos를 사용하지 않으면 서버가 사용자를 인증할 때 클라이언트에 전적으로 의존합니다. 즉, 서버가 클라이언트를 신뢰합니다. Kerberos를 사용하면 서버가 클라이언트를 신뢰하는 것이 아니라, KDC(Key Distribution Center)를 신뢰합니다. 인증을 처리하고 계정(보안 주체)과 암호를 관리하는 것이 바로 KDC입니다. 뿐만 아니라, 어떤 형태의 암호든 회선을 통해 전송되지 않습니다.

Kerberos를 사용하지 않으면 사용자의 자격 증명이 암호화되지 않은 상태로 회선을 통해 전송되므로 쉽게 스푸핑될 수 있습니다. Kerberos를 사용하면 타겟 서버와 KDC만 읽을 수 있는 암호화된 Kerberos 티켓에 사용자의 ID(보안 주체)가 포함됩니다. 타겟 서버와 KDC만이 암호화 키를 인식합니다.

NFS 보안과 함께, Kerberos에서 AES128 및 AES256 암호화가 지원됩니다. NFS 보안과 함께, 이는 SMB와 LDAP에도 영향을 미칩니다. 이제 이런 암호화는 Windows 및 Linux에서 기본적으로 지원됩니다. 이런 새로운 암호화가 훨씬 더 안전하지만, 사용 여부는 클라이언트에 달린 문제입니다. 서버는 해당 사용자 보안 주체에서 활성 UDS(Unix Directory Service)를 쿼리하여 그 사용자의 자격 증명을 빌드합니다. NIS에 보안 설정이 되어 있지 않으므로, NFS 보안과 함께 NIS를 사용하지 않는 것이 좋습니다. LDAP 또는 LDAPS와 함께 Kerberos를 사용하는 것이 좋습니다.

NFS 보안은 PowerStore Manager를 통해 구성할 수 있습니다.

파일 프로토콜 관계

Kerberos를 사용할 때는 다음 사항이 필요합니다.

- DNS - IP 주소 대신 DNS 이름을 사용해야 합니다.
- NTP- PowerStore에 구성된 NTP 서버가 있어야 합니다.

  노트: Kerberos는 네트워크의 클라이언트, 서버 및 KDC 간 시간 동기화가 올바르게 이루어져야 합니다.
- UDS - 자격 증명 배포에 필요합니다.
- 호스트 이름 - Kerberos는 IP 주소가 아니라 이름을 사용하여 작동합니다.

NFS 보안에서는 호스트 이름의 값에 따라 한 개 또는 두 개의 SPN(service principal names)을 사용합니다. 호스트 이름이 FQDN 형식의 호스트 도메인인 경우:

- 짧은 SPN: **nfs/host@REALM**
- 긴 SPN: **nfs/host.domainFQDN@REALM**

호스트 이름이 FQDN 형식이 아닌 경우에는 짧은 SPN만 사용됩니다.

SMB 서버를 도메인에 연결할 수 있는 SMB와 마찬가지로, NFS 서버를 영역(Kerberos에서 도메인과 같은 의미로 사용되는 용어)에 연결할 수 있습니다. 이를 위해 다음 두 가지 옵션이 있습니다.

- 구성된 Windows 도메인 사용(있는 경우)
- UNIX KDC 기반 Kerberos 영역을 완전히 구성

관리자가 구성된 Windows 도메인을 사용하도록 선택하면 따로 해야 할 일은 없습니다. SMB 서버를 연결/연결 해제하면 NFS 서비스에서 사용되는 모든 SPN이 자동으로 KDC에 추가되거나 KDC에서 제거됩니다. NFS 보안이 SMB 구성을 사용하도록 구성된 경우 SMB 서버를 제거할 수 없습니다.

관리자가 UNIX 기반 Kerberos 영역을 사용하도록 선택할 경우 추가적인 구성이 필요합니다.

- 영역 이름: 일반적으로 모든 대문자를 포함하는 Kerberos 영역의 이름입니다.
- UNIX KDC 기반 Kerberos 영역을 완전히 구성합니다.

클라이언트가 특정 보안과 함께 NFS 내보내기를 마운트하도록 보장하기 위해, 어떤 최소 보안이 허용되는지 나타내는 보안 매개변수 sec가 제공됩니다. 다음 4가지 종류의 보안이 있습니다.

- `AUTH_SYS`: Kerberos를 사용하지 않는 표준 기존 보안. 서버가 클라이언트에서 제공되는 자격 증명을 신뢰함
- `KRB5`: Kerberos v5를 사용한 인증.
- `KRB5i`: Kerberos 인증 및 무결성(서명).
- `KRB5p`: Kerberos 인증, 무결성 및 프라이버시(암호화).

NFS 클라이언트가 구성된 최소 보안보다 낮은 보안 수준으로 내보내기 마운트를 시도하는 경우 액세스가 거부됩니다. 예를 들어 최소 액세스가 `KRB5i`인 경우 `AUTH_SYS` 또는 `KRB5`를 사용하는 마운트는 모두 거부됩니다.

자격 증명 빌드

사용자가 시스템에 연결할 때는 Kerberos 티켓에서 추출되는 사용자의 보안 주체인 **user@REALM**만 표시됩니다. `AUTH_SYS` 보안과는 달리, NFS 요청에 자격 증명이 포함되지 않습니다. 보안 주체에서 사용자에 해당하는 부부(@ 앞)이 추출되어 해당 uid에 대한 UDS를 조회하는 데 사용됩니다. 이 uid에서 자격 증명은 확장 NFS 자격 증명을 사용하는 경우와 유사하게 시스템이 액티브 UDS를 사용하여 배포합니다. 단, Kerberos 없이는 요청에 의해 직접 uid가 제공된다는 점이 다릅니다.

보안 주체가 UDS에서 매핑되지 않으면 구성된 기본 UNIX 사용자 자격 증명이 대신 사용됩니다. 기본 UNIX 사용자가 설정되어 있지 않으면 사용되는 자격 증명은 아무도 없음이 됩니다.

파일 시스템 객체의 보안

멀티 프로토콜 환경에서 보안 정책은 파일 시스템 레벨에서 설정되며 각 파일 시스템에 대해 독립적입니다. 각 파일 시스템은 고유의 액세스 정책을 사용하여 NFS와 SMB의 액세스 제어 의미 체계 간 차이를 조정하는 방법을 결정합니다. 액세스 정책을 선택하면 특정 파일 시스템에 파일 보안을 적용할 때 사용되는 메커니즘이 결정됩니다.

노트: 환경에서 이전 SMB1 프로토콜이 지원되야 하는 경우 `svc_nas_cifssupport` 서비스 명령을 사용하여 활성화할 수 있습니다. 이 서비스 명령에 대한 자세한 정보는 *PowerStore Service Scripts Guide*를 참조 바랍니다.

UNIX 보안 모델

UNIX 정책을 선택하면 SMB 프로토콜에서 파일 레벨 보안을 변경하려는 시도, 즉 ACL(Access Control List)에 대한 변경이 무시됩니다. UNIX 액세스 권한을 파일 시스템 객체의 모드 비트 또는 NFSv4 ACL라고도 합니다. 모드 비트는 비트 문자열로 표현됩니다. 각 비트는 파일 소유자, 파일 시스템 객체에 연결된 그룹 및 기타 모든 사용자에게 부여되는 액세스 모드 또는 권한을 나타냅니다. UNIX 모드 비트는 각 사용자 범주(사용자, 그룹 또는 기타)에 지정되는 3개의 rwx(read, write, execute) 트리플릿 세트를 하나로 연결한 것입니다. ACL은 서비스에 대한 액세스 및 거부를 제어하는 사용자 및 사용자 그룹의 목록입니다.

Windows 보안 모델

Windows 보안 모델은 기본적으로 SD(Security Descriptor) 및 그에 따른 ACL을 사용한 객체별 권한을 기반으로 합니다. SMB 정책을 선택하면 NFS 프로토콜의 모드 비트 변경이 무시됩니다.

파일 시스템 객체에 대한 액세스는 보안 설명자를 통해 사용 권한이 '허용'으로 설정되었는지 또는 '거부'로 설정되었는지에 따라 결정됩니다. SD는 해당 ACL과 함께 객체의 소유자 및 객체의 그룹 SID를 기술합니다. ACL은 각 객체의 보안 설명자에 포함됩니다. 각 ACL에는 ACE(Access Control Entry)가 포함됩니다. 또한 ACE에는 사용자, 그룹 또는 컴퓨터를 식별하는 SID 한 개 및 해당 SID에 대해 거부되거나 허용되는 권한 목록이 포함됩니다.

멀티 프로토콜 환경의 파일 시스템 액세스

파일 액세스는 NAS 서버를 통해 제공됩니다. NAS 서버는 데이터가 저장되는 파일 시스템 세트를 포함합니다. NAS 서버는 SMB 공유 및 NFS 공유를 통해 파일 시스템을 공유하여 NFS 및 SMB 파일 프로토콜에서 이 데이터에 액세스할 수 있도록 합니다. NAS 서버의 멀티 프로토콜 공유 모드를 사용하면 SMB와 NFS 간에 동일한 데이터를 공유할 수 있습니다. 멀티 프로토콜 공유 모드는 파일 시스템에 대한 SMB 액세스와 NFS 액세스를 동시에 제공하므로, Windows 사용자를 UNIX 사용자에 매핑하고 사용할 보안 규칙(모드 비트, ACL 및 사용자 자격 증명)을 적절하게 정의하여 멀티 프로토콜 공유를 적절히 구성해야 합니다.

노트: 멀티 프로토콜 공유, 사용자 매핑, 액세스 정책 및 사용자 자격 증명과 관련된 NAS 서버 구성 및 관리 방법에 대한 자세한 내용은 PowerStore Manager 온라인 도움말을 참조하십시오.

사용자 매핑

멀티 프로토콜 컨텍스트에서는 Windows 사용자가 UNIX 사용자와 일치해야 합니다. 그러나 UNIX 사용자를 Windows 사용자에 매핑하는 작업은 액세스 정책이 Windows일 때만 필요합니다. 파일 시스템 보안을 적용하려면 이 일치가 필요하며 프로토콜에 기본이 아닌 경우에도 마찬가지입니다. 사용자 매핑에 관여하는 구성 요소는 다음과 같습니다.

- UNIX Directory Service, 로컬 파일 또는 둘 다
- Windows Resolver
- 보안 매핑(secmap) - NAS 서버가 사용하는 SID와 UID 또는 GID 간의 모든 매핑이 포함된 캐시
- ntxmap

노트: 사용자 매핑은 SMB 서버에 로컬인 사용자 또는 그룹에 영향을 미치지 않습니다.

UNIX Directory Service 및 로컬 파일

UDS(UNIX Directory Service) 및 로컬 파일은 다음과 같은 작업을 처리합니다.

- 특정 UID(User Identifier)에 해당하는 UNIX 계정 이름을 반환합니다.
- 특정 UNIX 계정 이름에 해당하는 UID 및 기본 GID(Group Identifier)를 반환합니다.

지원되는 서비스는 다음과 같습니다.

- LDAP
- NIS
- 로컬 파일
- 없음(기본 사용자를 통한 매핑만 가능)

멀티 프로토콜 공유가 활성화된 경우 NAS 서버에 대해 UDS 1개가 활성화되거나, 로컬 파일이 활성화되거나, 로컬 파일과 UDS 둘 다가 활성화되어야 합니다. 사용자 매핑에 사용할 항목은 NAS 서버의 Unix Directory Service 속성에 의해 결정됩니다.

Windows Resolver

Windows Resolver는 사용자 매핑의 다음과 같은 작업을 처리합니다.

- 특정 SID(Security Identifier)에 해당하는 Windows 계정 이름을 반환합니다.
- 특정 Windows 계정 이름에 대해 해당하는 SID 반환

Windows Resolver는 다음과 같습니다.

- 도메인의 DC(Domain Controller)
- SMB 서버의 LGDB(Local Group Database)

secmap

secmap의 기능은 모든 SID-UID, 기본 GID 및 UID-SID 매핑을 저장하여 NAS 서버의 모든 파일 시스템 전체에서 일관성을 보장하는 것입니다.

ntxmap

ntxmap은 이름이 서로 다른 Windows 계정을 UNIX 계정에 연결하는 데 사용됩니다. 예를 들어 같은 사용자가 Windows에서는 Gerald라는 계정을, UNIX에서는 Gerry라는 계정을 사용하는 경우 ntxmap으로 두 계정 사이의 상관 관계를 설정할 수 있습니다.

SID-UID, 기본 GID 매핑

다음 순서는 SID-UID, 기본 GID 매핑을 확인하는 데 사용되는 프로세스입니다.

1. secmap을 검색하여 SID를 찾습니다. SID가 검색되면 UID 및 GID 매핑이 확인됩니다.
2. secmap에서 SID가 검색되지 않으면 SID와 관련된 Windows 이름을 찾아야 합니다.
   a. NAS SMB 서버의 로컬 그룹 데이터베이스를 검색하여 SID를 찾습니다. SID가 검색되는 경우 관련된 Windows 이름은 로컬 사용자 이름과 SMB 서버 이름입니다.
   b. 로컬 그룹 데이터베이스에서 SID가 검색되지 않으면 도메인의 DC를 검색합니다. SID가 검색되는 경우 관련된 Windows 이름은 사용자 이름입니다. SID를 확인할 수 없는 경우 액세스가 거부됩니다.
3. Windows 이름은 UNIX 이름으로 변환됩니다. ntxmap은 이 용도로 사용됩니다.
   a. ntxmap에서 Windows 이름이 검색되면 해당 항목이 UNIX 이름으로 사용됩니다.
   b. ntxmap에서 Windows 이름이 검색되지 않으면 Windows 이름이 UNIX 이름으로 사용됩니다.
4. UNIX 이름을 사용하여 UDS(NIS 서버, LDAP 서버 또는 로컬 파일)를 검색합니다.
   a. UDS에서 UNIX 사용자 이름이 검색되면 UID 및 GID 매핑이 확인됩니다.
   b. UNIX 이름을 찾을 수 없지만 매핑되지 않은 Windows 계정에 대한 자동 매핑 기능이 활성화되어 있으면 자동으로 UID가 할당됩니다.
   c. UDS에서 UNIX 사용자 이름이 검색되지 않지만 기본 UNIX 계정이 있는 경우 UID 및 GID 매핑은 기본 UNIX 계정의 매핑으로 확인됩니다.
   d. SID를 확인할 수 없는 경우 액세스가 거부됩니다.

매핑이 검색되면 영구 secmap 데이터베이스에 추가됩니다. 매핑이 검색되지 않으면 실패한 매핑이 영구 secmap 데이터베이스에 추가됩니다.

다음 다이어그램은 기본 GID 매핑인 SID-UID 매핑을 확인하는 데 사용되는 프로세스입니다.

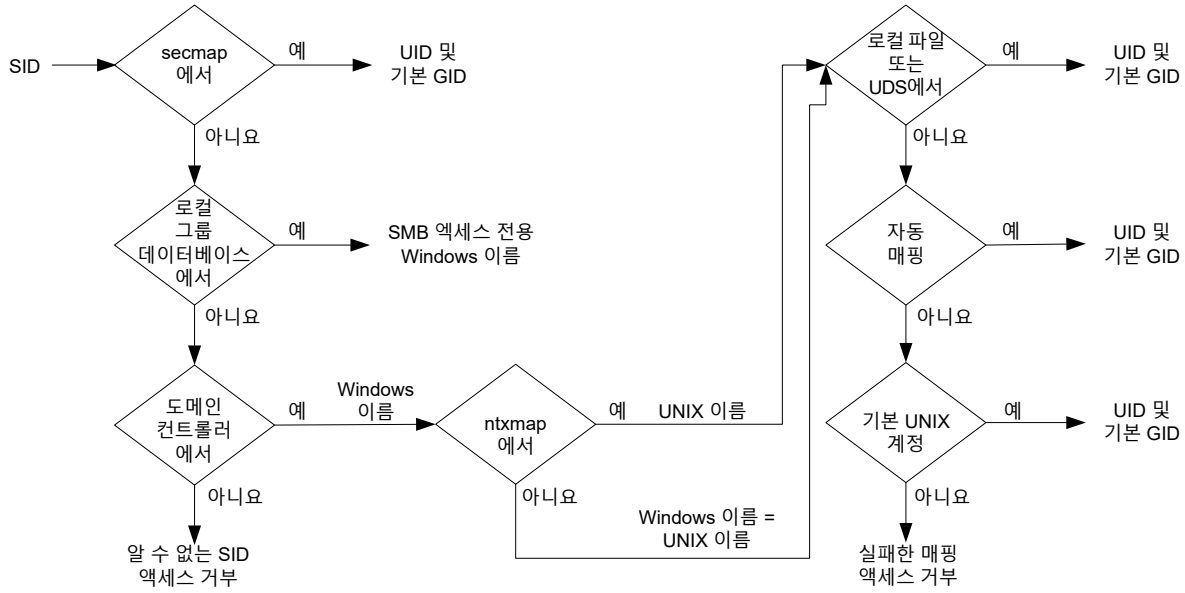

그림 1 . 기본 GID 매핑인 SID-UID를 확인하는 프로세스

UID-SID 매핑

다음 순서는 UID-SID 매핑을 확인하는 데 사용되는 프로세스입니다.

1. secmap을 검색하여 UID를 찾습니다. UID가 검색되면 SID 매핑이 확인됩니다.
2. secmap에서 UID가 검색되지 않으면 UID와 관련된 UNIX 이름을 찾아야 합니다.
   a. UID를 사용하여 UDS(NIS 서버, LDAP 서버 또는 로컬 파일)를 검색합니다. UID가 검색되는 경우 관련된 UNIX 이름은 사용자 이름입니다.
   b. UDS에서 UID가 검색되지 않지만 기본 Windows 계정이 있는 경우 UID가 기본 Windows 계정의 SID에 매핑됩니다.
3. 기본 Windows 계정 정보가 사용되지 않는 경우 UNIX 이름이 Windows 이름으로 변환됩니다. ntxmap은 이 용도로 사용됩니다.
   a. ntxmap에서 UNIX 이름이 검색되면 해당 항목이 Windows 이름으로 사용됩니다.
   b. ntxmap에서 UNIX 이름이 검색되지 않으면 UNIX 이름이 Windows 이름으로 사용됩니다.
4. Windows 이름을 사용하여 Windows DC 또는 로컬 그룹 데이터베이스를 검색합니다.
   a. Windows 이름이 검색되면 SID 매핑이 확인됩니다.
   b. Windows 이름에 마침표가 포함되어 있고 마지막 마침표(.) 뒤의 이름이 SMB 서버 이름과 일치하는 경우 해당 SMB 서버의 로컬 그룹 데이터베이스를 검색하여 SID 매핑을 확인합니다.
   c. Windows 이름이 검색되지 않지만 기본 Windows 계정이 있는 경우 SID가 기본 Windows 계정의 이름에 매핑됩니다.
   d. SID를 확인할 수 없는 경우 액세스가 거부됩니다.

매핑이 검색되면 영구 secmap 데이터베이스에 추가됩니다. 매핑이 검색되지 않으면 실패한 매핑이 영구 secmap 데이터베이스에 추가됩니다.

다음 다이어그램은 UID-SID 매핑을 확인하는 데 사용되는 프로세스입니다.

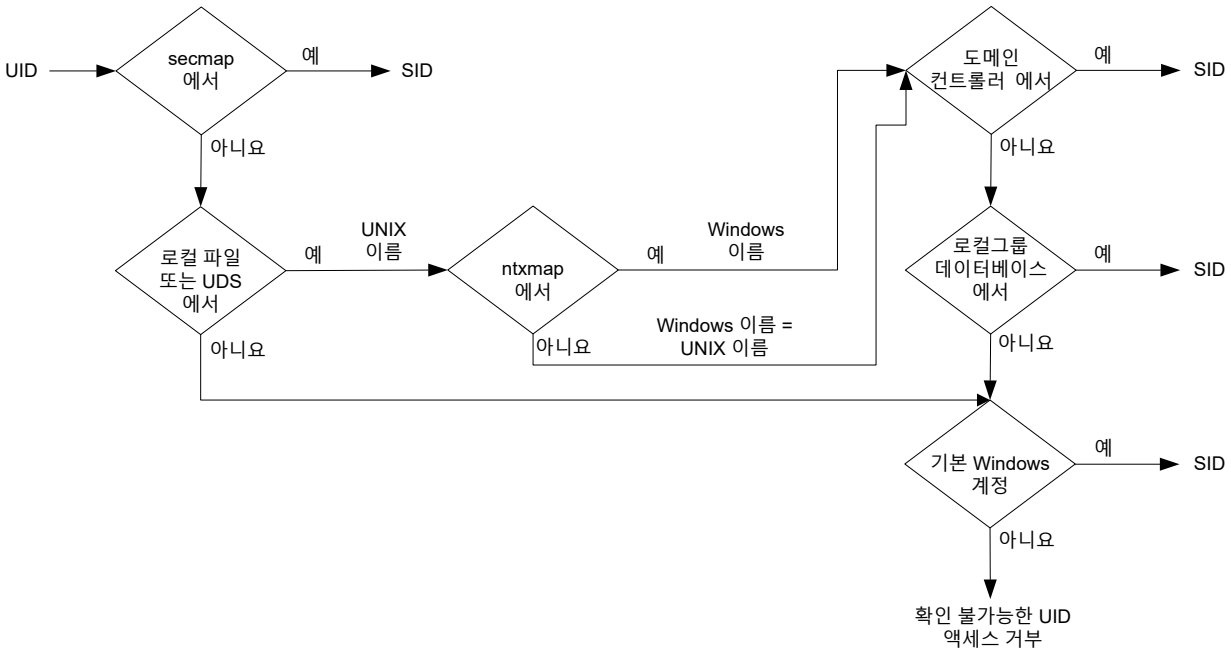

그림 2 . UID-SID 매핑을 확인하는 데 사용되는 프로세스

NFS, SMB 및 FTP의 액세스 정책

멀티 프로토콜 환경에서 스토리지 시스템은 파일 시스템 액세스 정책을 사용하여 파일 시스템의 사용자 액세스 제어를 관리합니다. 보안에는 UNIX와 Windows의 두 가지 종류가 있습니다.

UNIX 보안 인증에서는 호스트 클라이언트가 자격 증명을 제공하는 비보안 NFS 액세스를 제외하고 UDS(UNIX Directory Service)에서 자격 증명이 생성됩니다. 사용자 권한은 모드 비트 및 NFSv4 ACL로 지정됩니다. 사용자 및 그룹 ID(각각 UID 및 GID)가 인증에 사용됩니다. UNIX 보안에는 별도의 권한이 관련되지 않습니다.

Windows 보안 인증에서는 자격 증명이 Windows DC(Domain Controller) 및 SMB 서버의 LGDB(Local Group Database)에서 생성됩니다. 사용자 권한은 SMB ACL로 지정됩니다. SID(Security Identifier)가 인증에 사용됩니다. Windows 보안에는 SMB 서버의 LGDB 또는 GPO(Group Policy Object)에서 부여하는 TakeOwnership, Backup 및 Restore 등의 권한이 관련됩니다.

다음 표에 각 프로토콜에서 사용할 보안을 정의하는 액세스 정책이 설명되어 있습니다.

액세스 정책	설명
기본 인증(기본값)	• 각 프로토콜이 기본 보안을 사용하여 액세스를 관리합니다. • NFS 공유의 보안은 요청에 연결된 UNIX 자격 증명을 사용하여 NFSv3 UNIX 모드 비트 또는 NFSv4 ACL을 확인합니다. 그런 다음 액세스를 허용하거나 거부합니다. • SMB 공유의 보안은 요청에 연결된 Windows 자격 증명을 사용하며 SMB ACL을 확인합니다. 그런 다음 액세스를 허용하거나 거부합니다. • NFSv3 UNIX 모드 비트와 NFSv4 ACL 사용 권한 변경은 서로 동기화됩니다. • Unix와 Windows 사용 권한은 서로 동기화되지 않습니다.
Windows	• Windows 보안을 사용하여 Windows와 UNIX의 파일 레벨 액세스에 대한 보안을 유지합니다. • Windows 자격 증명을 사용하여 SMB ACL을 확인합니다. • 새로 생성된 된 파일에 대한 사용 권한은 SMB ACL 변환에 의해 결정됩니다. SMB ACL 사용 권한 변경은 NFSv3 UNIX 모드 비트 또는 NFSv4 ACL에 동기화됩니다. • NFSv3 모드 비트 및 NFSv4 ACL 사용 권한 변경은 거부됩니다.
UNIX	• UNIX 보안을 사용하여 Windows와 UNIX의 파일 레벨 액세스에 대한 보안을 유지합니다. • SMB 액세스 요청이 발생하면 로컬 파일 또는 UDS의 UNIX 자격 증명을 사용하여 NFSv3 모드 비트 또는 NFSv4 ACL의 사용 권한을 확인합니다. • 새로 생성된 파일에 대한 권한은 UMASK에 의해 결정됩니다. • NFSv3 UNIX 모드 비트 또는 NFSv4 ACL 사용 권한 변경은 SMB ACL에 동기화됩니다. • SMB ACL 사용 권한 변경은 중단 방지를 위해 허용되지만 이러한 사용 권한은 유지되지 않습니다.

FTP의 경우 NAS 서버 인증에 사용되는 사용자 이름 형식에 따라 Windows나 UNIX 인증이 달라집니다. Windows 인증을 사용하는 경우 FTP 액세스 제어는 SMB의 액세스 제어와 유사하며, 다른 인증을 사용하는 경우는 NFS의 액세스 제어와 유사합니다. FTP 및 SFTP 클라이언트는 NAS 서버에 연결될 때 인증됩니다. 이때 SMB 인증(사용자 이름 형식이 `domain\user` 또는 `user@domain`인 경우) 또는 UNIX 인증(기타 단일 사용자 이름 형식)이 사용될 수 있습니다. SMB 인증은 NAS 서버에서 정의된 도메인의 Windows DC에 의해 보장됩니다. UNIX 인증은 원격 LDAP 서버, 원격 NIS 서버 또는 NAS 서버의 로컬 암호 파일 중 하나에 저장된 암호화된 암호에 따라 NAS 서버에 의해 보장됩니다.

파일 레벨 보안 자격 증명

파일 레벨 보안을 적용하려면 처리되는 중인 SMB 또는 NFS 요청에 연결되는 자격 증명을 스토리지 시스템에서 생성해야 합니다. 자격 증명에는 Windows와 UNIX의 두 가지 종류가 있습니다. 다음 활용 사례의 경우 UNIX 및 Windows 자격 증명은 NAS 서버에서 생성됩니다.

- NFS 요청에 대해 16개 그룹을 초과하는 UNIX 자격 증명을 생성하는 경우. 이 기능을 제공하려면 NAS 서버의 확장 자격 증명 속성을 설정해야 합니다.
- 파일 시스템의 액세스 정책이 UNIX일 때 SMB 요청에 대한 UNIX 자격 증명을 생성하는 경우.
- SMB 요청에 대한 Windows 자격 증명을 생성하는 경우.
- 파일 시스템의 액세스 정책이 Windows일 때 NFS 요청에 대한 Windows 자격 증명을 생성하는 경우.

노트: 확장 자격 증명 속성이 설정되지 않은 NFS 요청의 경우 NFS 요청의 UNIX 자격 증명이 사용됩니다. SMB 요청에 Kerberos 인증을 사용할 때는 세션 설정 요청에 대한 Kerberos 티켓에 도메인 사용자의 Windows 사용자 자격 증명이 포함되어 있습니다.

다음과 같은 경우 영구 자격 증명 캐시가 사용됩니다.

- Windows 액세스 정책을 사용하는 파일 시스템 액세스를 위해 생성된 Windows 자격 증명.

- 확장 자격 증명 옵션이 설정된 경우 NFS를 통한 액세스용 Unix 자격 증명.

NAS 서버마다 하나의 캐시 인스턴스가 있습니다.

매핑되지 않은 사용자의 액세스 허용

멀티 프로토콜의 필수 조건은 다음과 같습니다.

- Windows 사용자는 UNIX 사용자에 매핑되어야 합니다.
- UNIX 사용자는 Windows 사용자에 매핑되어야 합니다. 그래야만 사용자가 Windows 액세스 정책을 사용하는 파일 시스템을 액세스할 때 Windows 자격 증명을 생성할 수 있습니다.

매핑되지 않은 사용자의 경우 두 가지 속성이 NAS 서버에 연결됩니다.

- 기본 UNIX 사용자.
- 기본 Windows 사용자.

매핑되지 않은 Windows 사용자가 멀티 프로토콜 파일 시스템에 연결을 시도하고 NAS 서버에 대해 기본 UNIX 사용자 계정이 구성된 경우 기본 UNIX 사용자의 UID(User Identifier) 및 기본 GID(Group Identifier)가 Windows 자격 증명에 사용됩니다. 마찬가지로, 매핑되지 않은 UNIX 사용자가 멀티 프로토콜 파일 시스템에 연결을 시도하고 NAS 서버에 대해 기본 Windows 사용자 계정이 구성된 경우 기본 Windows 사용자의 Windows 자격 증명이 사용됩니다.

노트: UDS(UNIX Directory Service)에 기본 UNIX 사용자가 설정되어 있지 않은 경우 매핑되지 않은 사용자의 SMB 액세스가 거부됩니다. Windows DC 또는 LGDB에 기본 Windows 사용자가 없는 경우 Windows 액세스 정책을 사용하는 파일 시스템에서 매핑되지 않은 사용자의 NFS 액세스가 거부됩니다.

노트: 기본 UNIX 사용자는 기존의 유효한 UNIX 계정 이름이거나 새로운 형식인 `@uid=xxxx,gid=yyyy@`를 따릅니다. 이 형식에서 *xxxx* 및 *yyyy*는 각각 UID 및 기본 GID의 10진수 숫자 값이며 PowerStore Manager를 통해 시스템에서 구성할 수 있습니다.

NFS 요청에 대한 UNIX 자격 증명

UNIX 또는 기본 액세스 정책을 사용하는 NFS 전용 또는 멀티 프로토콜 파일 시스템에 대한 NFS 요청을 처리하려면 UNIX 자격 증명을 사용해야 합니다. 각 요청에는 항상 UNIX 자격 증명이 포함되지만 자격 증명의 추가 그룹은 16개로 제한됩니다. NFS 서버의 `extendedUnixCredEnabled` 속성을 통해 그룹 수가 16개가 넘는 자격 증명을 생성할 수 있습니다. 이 속성을 설정하면 활성 UDS에 UID를 쿼리하여 기본 GID 및 모든 소속 그룹의 GID를 가져옵니다. UDS에 UID가 없는 경우 요청에 포함된 UNIX 자격 증명이 사용됩니다.

노트: NFS 보안 액세스의 경우 항상 UDS를 사용하여 자격 증명이 생성됩니다.

SMB 요청에 대한 UNIX 자격 증명

UNIX 액세스 정책을 사용하는 멀티 프로토콜 파일 시스템에 대한 SMB 요청을 처리하려면 세션을 설정할 때 SMB 사용자에 대한 Windows 자격 증명을 먼저 생성해야 합니다. Windows 사용자의 SID는 AD에서 이름을 찾는 데 사용됩니다. 이 이름은 UDS 또는 로컬 파일(passwd 파일)에서 Unix UID 및 GID를 찾는 데 사용(필요한 경우 ntxmap를 통해)됩니다. 사용자의 소유자 UID는 Windows 자격 증명에 포함됩니다. UNIX 액세스 정책을 사용하는 파일 시스템을 액세스할 경우 사용자의 UID로 UDS를 쿼리하여 UNIX 자격 증명을 생성할 수 있습니다. 이는 NFS용 확장 자격 증명을 생성하는 경우와 비슷합니다. UID는 할당량 관리에 필요합니다.

SMB 요청에 대한 Windows 자격 증명

Windows 또는 기본 액세스 정책을 사용하는 SMB 전용 또는 멀티 프로토콜 파일 시스템에 대한 SMB 요청을 처리하려면 Windows 자격 증명을 사용해야 합니다. SMB에 대한 Windows 자격 증명은 사용자가 연결할 때 세션 설정 요청 시에 한 번만 생성하면 됩니다.

Kerberos 인증을 사용할 때는 NTLM(NT LAN Manager)을 사용할 때와 달리 세션 설정 요청에 대한 Kerberos 티켓에 사용자 자격 증명이 포함되어 있습니다. 기타 정보는 Windows DC 또는 LGDB에서 쿼리하여 가져옵니다. Kerberos의 경우 추가 그룹 SID 목록은 Kerberos 티켓 및 추가 로컬 그룹 SID 목록에서 가져옵니다. 권한 목록은 LGDB에서 가져옵니다. NTLM의 경우 추가 그룹 SID 목록은 Windows DC 및 로컬 그룹 SID 목록에서 가져옵니다. 권한 목록은 LGDB에서 가져옵니다.

또한 사용자 매핑 구성 요소에서 해당 UID 및 기본 GID가 검색됩니다. 기본 그룹 SID는 액세스 확인에 사용되지 않으므로 UNIX 기본 GID가 대신 사용됩니다.

노트: NTLM은 인증, 무결성 및 기밀성을 제공하는 독점적 보안 프로토콜의 이전 제품군입니다. Kerberos는 티켓 생성 시스템을 사용하여 더 빠른 인증을 제공하는 개방형 표준 프로토콜입니다. Kerberos는 네트워크의 시스템에 NTLM보다 개선된 보안을 제공합니다.

NFS 요청에 대한 Windows 자격 증명

사용자가 NFS 요청을 통해 Windows 액세스 정책을 사용하는 파일 시스템에 액세스를 시도할 때만 Windows 자격 증명이 생성되거나 검색됩니다. UID는 NFS 요청에서 추출됩니다. 관련된 보존시간이 지정된 각 NFS 요청에 대해 자격 증명을 일일이 생성할 필요가 없도록 전역 Windows 자격 증명 캐시가 운용됩니다. 이 캐시에 Windows 자격 증명이 있는 경우 별도의 작업이 필요하지 않습니다. Windows 자격 증명을 찾을 수 없는 경우 UDS 또는 로컬 파일을 쿼리하여 UID 이름을 찾습니다. 그런 다음 필요한 경우 ntxmap를 통해 이 이름을 사용하여 Windows 사용자를 찾고 Windows DC 또는 LGDB에서 자격 증명을 검색합니다. 매핑이 발견되지 않으면 기본 Windows 사용자의 Windows 자격 증명이 대신 사용되거나 액세스가 거부됩니다.

CAVA(Common AntiVirus Agent)의 이해

CAVA(Common AntiVirus Agent)는 NAS 서버를 사용하는 클라이언트에 안티바이러스 솔루션을 제공합니다. Microsoft Windows Server 환경에서 산업 표준 SMB 프로토콜을 사용합니다. CAVA는 타사 안티바이러스 소프트웨어를 사용하여 바이러스가 스토리지 시스템의 파일에 감염되기 전에 알려진 바이러스를 제거합니다.

안티바이러스가 중요한 이유

이 스토리지 시스템은 자체 아키텍처 덕분에 바이러스 침입으로부터 안전합니다. NAS 서버는 내장된 운영 체제를 사용하여 실시간으로 데이터 액세스를 실행합니다. 타사는 이 운영 체제에서 바이러스가 포함된 프로그램을 실행할 수 없습니다. 이 운영 체제 소프트웨어는 바이러스로부터 안전하지만 스토리지 시스템에 액세스하는 Windows 클라이언트에는 바이러스 방지 기능이 필요합니다. 클라이언트에서 바이러스 방지 기능을 사용하면 클라이언트가 서버에 감염된 파일을 저장할 가능성이 낮아지며 감염된 파일을 열더라도 클라이언트가 안전하게 보호됩니다. 이 안티바이러스 솔루션은 운영 체제 소프트웨어, CAVA 에이전트, 타사 안티바이러스 엔진의 조합으로 구성됩니다. 도메인에 있는 Windows Server에는 CAVA 소프트웨어와 타사 안티바이러스 엔진을 설치해야 합니다.

CEE(Common Event Enabler)의 일부인 CAVA에 대한 추가 정보는 *Using the Common Event Enabler on Windows Platforms*www.dell.com/powerstoredocs 문서를 참조 바랍니다.

코드 서명

PowerStore는 새 릴리스 및 패치 릴리스 모두에 대한 소프트웨어 업그레이드를 수용하도록 설계 되었습니다. 마스터 GPG(GNU Privacy Guard) 키는 모든 PowerStore 소프트웨어 패키지를 서명하고 Dell EMC가 이 GPG 키를 제어합니다. PowerStore 소프트웨어 업그레이드 프로세스는 소프트웨어 패키지의 서명을 확인하고 훼손 또는 손상 가능성을 나타내는 유효하지 않은 서명을 거부합니다. 검증 단계는 업그레이드 프로세스에서 기본적으로 제공되며 설치 전 단계에서 소프트웨어 패키지의 서명이 자동으로 확인됩니다.

2

통신 보안 설정

이 섹션에서 다루는 내용은 다음과 같습니다.

주제:

- 포트 사용

포트 사용

다음 섹션은 어플라이언스에서 볼 수 있는 여러 네트워크 포트와 그 관련 서비스에 대해 설명합니다. 어플라이언스는 vCenter Server와 통신하는 경우를 비롯한 여러 가지 환경에서 네트워크 클라이언트의 역할을 합니다. 이러한 경우 어플라이언스가 통신을 시작하며 네트워크 인프라스트럭처는 해당 연결을 지원해야 합니다.

노트: 포트에 대한 자세한 내용은 기술 자료 문서 542240, *PowerStore: 고객 네트워크 방화벽 규칙 - TCP/UDP 포트*를 참조 바랍니다. https://www.dell.com/support/kbdoc/en-us/542240로 이동합니다. 고객 네트워크 방화벽 규칙 도구를 사용하면 PowerStore 배포와 관련된 방화벽 규칙 및 포트 목록을 필터링하고 검토할 수 있습니다.

어플라이언스 네트워크 포트

다음 표는 어플라이언스에서 볼 수 있는 여러 네트워크 포트와 그 관련 서비스에 대해 설명한 것입니다.

표 2. 어플라이언스 네트워크 포트

포트	서비스	프로토콜	액세스 방향	설명
22	SSH 클라이언트, SupportAssist Connect Home	TCP	양방향	• SSH 액세스 허용(활성화된 경우). • SupportAssist Connect Home에 필요합니다. 이 포트가 닫힌 경우 SSH를 통한 관리 연결을 사용할 수 없습니다.
25	SMTP	TCP	아웃바운드	어플라이언스가 이메일을 보내도록 허용합니다. 이 포트가 닫힌 경우 e-메일 알림을 사용할 수 없습니다.
26	SSH 클라이언트	TCP	양방향	포트 22에 대한 SSH 액세스가 이 포트로 리디렉션됩니다. 이 포트가 닫힌 경우 SSH를 통한 관리 연결을 사용할 수 없습니다.
53	DNS	TCP/UDP	아웃바운드	DNS 서버로 DNS 쿼리를 전송하는 데 사용됩니다. 이 포트가 닫힌 경우 DNS 이름 확인이 수행되지 않습니다.
80, 8080, 8128	SupportAssist	TCP	아웃바운드	SupportAssist 프록시 연결에 사용됩니다.
123	NTP	TCP/UDP	아웃바운드	NTP 시간 동기화. 이 포트가 닫힌 경우 어플라이언스 간에 시간이 동기화되지 않습니다.
443	HTTPS	TCP	양방향	PowerStore Manager에 대한 HTTP 트래픽을 보호합니다. 이 포트가 닫힌 경우 어플라이언스와의 통신이 불가능합니다.
500	IPsec(IKEv2)	UDP	양방향	IPSec이 방화벽을 통과하도록 하려면 UDP 포트 500을 열고 인바운드와 아웃바운드 방

표 2. 어플라이언스 네트워크 포트 (계속)

포트	서비스	프로토콜	액세스 방향	설명
				화벽 필터 모두에서 IP 프로토콜 번호 50 및 51을 허용합니다. ISAKMP(Internet Security Association and Key Management Protocol) 트래픽이 방화벽을 통과하여 전달될 수 있도록 하려면 UDP 포트 500을 열어야 합니다. IPSec ESP(Encapsulating Security Protocol) 트래픽이 전달될 수 있도록 하려면 IP 프로토콜 ID 50을 설정해야 합니다. AH(Authentication Header) 트래픽이 전달될 수 있도록 하려면 IP 프로토콜 ID 51을 설정해야 합니다. 이 포트가 닫힌 경우 PowerStore 어플라이언스 간의 IPsec 연결을 사용할 수 없습니다.
587	SMTP	TCP	아웃바운드	어플라이언스가 이메일을 보내도록 허용합니다. 이 포트가 닫힌 경우 e-메일 알림을 사용할 수 없습니다.
3033	가져오기	TCP/UDP	아웃바운드	레거시 EqualLogic 피어 스토리지 및 Compellent 스토리지 센터 시스템에서 스토리지를 가져오는 데 필요합니다.
3260	iSCSI	TCP	• 호스트 및 ESXi 호스트 액세스에 대한 인바운드 • 양방향 복제 • 스토리지 가져오기에 대한 아웃바운드	iSCSI 서비스에 액세스를 제공하기 위해 필요합니다. • 외부 호스트 iSCSI 액세스 • 외부 또는 PowerStore 임베디드 ESXi 호스트 iSCSI 액세스 • 복제를 위한 클러스터 간 액세스 • 레거시 EqualLogic 피어 스토리지, Compellent Storage Center, Unity 및 VNX2 시스템에서 스토리지 가져오기 액세스 닫힌 경우 iSCSI 서비스를 사용할 수 없습니다. 레이턴시가 낮은 연결에서 적합한 복제 성능을 지원하기 위해 데이터 이동성에 사용됩니다.
3261	데이터 이동성	TCP	양방향	레이턴시가 높은 연결에서 적합한 복제 성능을 지원하기 위해 데이터 이동성에 사용됩니다.
5353	mDNS(Multicast DNS)	UDP	양방향	멀티캐스트 DNS 쿼리입니다. 이 포트가 닫힌 경우 mDNS 이름 확인이 수행되지 않습니다.
8443	VASA, SupportAssist	TCP	• VASA 인바운드 • SupportAssist 아웃바운드	• VASA 3.0의 VASA 공급업체에 필요합니다. • SupportAssist Connect Home 기능에 관련하여 필요합니다.
8443, 50443, 55443 또는 60443	Windows 가져오기 호스트 에이전트, Linux 가져오기 호스트 에이전트 또는 VMware 가져오기 호스트 에이전트	TCP	아웃바운드	기존 스토리지 시스템에서 데이터 스토리지를 가져올 때 이러한 포트 중 하나를 열어야 합니다.
9443	SupportAssist	TCP	아웃바운드	Connect Home 관련 SupportAssist REST API에 필요합니다.

파일과 관련된 어플라이언스 네트워크 포트

다음 표에는 파일에 관련된 어플라이언스에서 찾을 수 있는 여러 네트워크 포트 및 해당 서비스가 정리되어 있습니다.

노트: 아웃바운드 포트는 사용 후 삭제됩니다.

표 3. 파일과 관련된 어플라이언스 네트워크 포트

포트	서비스	프로토콜	액세스 방향	설명
20	FTP	TCP	아웃바운드	FTP 데이터 전송에 사용되는 포트. 이 포트는 FTP를 활성화하여 열 수 있습니다. 인증은 포트 21에서 수행되고 FTP 프로토콜에 의해 정의됩니다.
21	FTP	TCP	인바운드	포트 21은 FTP 서비스가 들어오는 FTP 요청을 수신 대기하는 제어 포트입니다.
22	SFTP	TCP	인바운드	SFTP(FTP over SSH)를 통한 알림을 허용합니다. SFTP는 클라이언트/서버 프로토콜입니다. 사용자는 SFTP를 사용하여 로컬 서브넷에 있는 어플라이언스에서 파일을 전송할 수 있습니다. 송신 FTP 제어 연결도 제공합니다. 이 포트가 닫힌 경우 FTP를 사용할 수 없습니다.
53	DNS	TCP/UDP	아웃바운드	DNS 서버로 DNS 쿼리를 전송하는 데 사용됩니다. 이 포트가 닫힌 경우 DNS 이름 확인이 수행되지 않습니다. SMB v1에 필요합니다.
88	Kerberos	TCP/UDP	아웃바운드	Kerberos 인증 서비스에 필요합니다.
111	RPC 바인드(SDNAS 네임 스페이스의 경우; 외의 경우는 호스트 서비스)	TCP/UDP	양방향	표준 portmapper 또는 rpcbind 서비스에 의해 포트가 열리는 보조 어플라이언스 네트워크 서비스입니다. 이 서비스는 중지할 수 없습니다. 정의에 따라, 클라이언트 시스템이 네트워크를 통해 이 포트에 연결된 경우 클라이언트가 포트를 쿼리할 수 있습니다. 인증 프로세스는 실행되지 않습니다.
123	NTP	UDP	아웃바운드	NTP 시간 동기화. 이 포트가 닫힌 경우 어플라이언스 간에 시간이 동기화되지 않습니다.
135	Microsoft RPC	TCP	인바운드	MicroSoft 클라이언트에서 여러 가지 용도로 사용됩니다. NDMP에도 사용됩니다.
137	Microsoft Netbios WINS	UDP; TCP/UDP	Inbound; Outbound	NETBIOS 이름 서비스는 어플라이언스 SMB 파일 공유 서비스와 연결되며, 이 기능(Wins)의 핵심 구성 요소입니다. 이 포트가 비활성화되면 모든 SMB 관련 서비스도 비활성화됩니다.
138	Microsoft Netbios BROWSE	UDP	아웃바운드	NETBIOS 데이터그램 서비스는 어플라이언스 SMB 파일 공유 서비스와 연결되며, 이 기능의 핵심 구성 요소입니다. 탐색 서비스만 사용됩니다. 해제된 경우 이 포트는 탐색 기능을 해제합니다.
139	Microsoft CIFS	TCP	양방향	NETBIOS 세션 서비스는 어플라이언스 SMB 파일 공유 서비스와 연결되며, 이 기능의 핵심 구성 요소입니다. SMB 서비스를 활성화하면 이 포트가 열립니다. 특히 SMB v1에 필요합니다.
389	LDAP	TCP/UDP	아웃바운드	비보안 LDAP 쿼리입니다. 이 포트가 닫힌 경우 비보안 LDAP 인증 쿼리를 사용할 수

표 3. 파일과 관련된 어플라이언스 네트워크 포트 (계속)

포트	서비스	프로토콜	액세스 방향	설명
				없습니다. 대안 수단으로 보안 LDAP를 구성할 수 있습니다.
445	Microsoft SMB	TCP	인바운드	Windows 2000 이상 클라이언트를 위한 SMB(도메인 컨트롤러에 있음) 및 SMB 연결 포트입니다. 지속적인 작업을 위해서는 어플라이언스 SMB 서비스에 적합한 액세스 권한이 있는 클라이언트가 네트워크를 통해 포트에 연결되어야 합니다. 이 포트를 비활성화하면 모든 SMB 관련 서비스가 비활성화됩니다. 포트 139도 비활성화하면 SMB 파일 공유가 비활성화됩니다.
464	Kerberos	TCP/UDP	아웃바운드	Kerberos 인증 서비스 및 SMB에 필요합니다.
500	IPsec(IKEv2)	UDP	양방향	IPSec이 방화벽을 통과하도록 하려면 UDP 포트 500을 열고 인바운드와 아웃바운드 방화벽 필터 모두에서 IP 프로토콜 번호 50 및 51을 허용합니다. ISAKMP(Internet Security Association and Key Management Protocol) 트래픽이 방화벽을 통과하여 전달될 수 있도록 하려면 UDP 포트 500을 열어야 합니다. IPSec ESP(Encapsulating Security Protocol) 트래픽이 전달될 수 있도록 하려면 IP 프로토콜 ID 50을 설정해야 합니다. AH(Authentication Header) 트래픽이 전달될 수 있도록 하려면 IP 프로토콜 ID 51을 설정해야 합니다. 이 포트가 닫힌 경우 PowerStore 어플라이언스 간의 IPsec 연결을 사용할 수 없습니다.
636	LDAPS	TCP/UDP	아웃바운드	보안 LDAP 쿼리입니다. 이 포트가 닫힌 경우 보안 LDAP 인증을 사용할 수 없습니다.
1234	NFS mountd	TCP/UDP	양방향	마운트 서비스에 사용되며, NFS 서비스(버전 2, 3 및 4)의 핵심 구성 요소입니다.
2000	SSHD	TCP	인바운드	서비스 가용성을 위한 SSHD(선택 사항)
2049	NFS I/O	TCP/UDP	양방향	NFS 서비스를 제공하는 데 사용됩니다.
3268	LDAP	UDP	아웃바운드	비보안 LDAP 쿼리입니다. 이 포트가 닫힌 경우 비보안 LDAP 인증 쿼리를 사용할 수 없습니다.
4000	NFSv3에 대한 STATD	TCP/UDP	양방향	NFS statd 서비스를 제공하는 데 사용됩니다. statd는 NFS 파일 잠금 상태 모니터이며 lockd와 함께 NFS에 충돌 및 복구 기능을 제공합니다. 이 포트가 닫힌 경우 NAS statd 서비스를 사용할 수 없습니다.
4001	NFSv3에 대한 NLMD	TCP/UDP	양방향	NFS lockd 서비스를 제공하는 데 사용됩니다. lockd는 NFS 파일 잠금 데몬입니다. 이 서비스는 NFS 클라이언트의 잠금 요청을 처리하며 statd 데몬과 함께 작동합니다. 이 포트가 닫힌 경우 NAS lockd 서비스를 사용할 수 없습니다.
4002	RQUOTAD for NFSv3	TCP/UDP; UDP	Inbound; Outbound	NFS rquotad 서비스를 제공하는 데 사용됩니다. rquotad 데몬은 파일 시스템을 마운트한 NFS 클라이언트에 할당량 정보를 제공합니다. 이 포트가 닫힌 경우 NAS rquotad 서비스를 사용할 수 없습니다.

표 3. 파일과 관련된 어플라이언스 네트워크 포트 (계속)

포트	서비스	프로토콜	액세스 방향	설명
4003	XATTRPD(확장된 파일 속성)	TCP/UDP	인바운드	멀티 프로토콜 환경에서 파일 특성을 관리하는 데 필요합니다.
4658	PAX(NAS 서버 아카이브)	TCP	인바운드	PAX는 표준 UNIX 테이프 형식에서 작동하는 어플라이언스 아카이브 프로토콜입니다.
8888	RCPD(복제 데이터 경로)	TCP	인바운드	Replicator(보조측)에서 사용됩니다. 복제할 데이터가 있다면 즉시 Replicator가 이 서비스를 열어둡니다. 서비스가 시작되면 중지할 수 있는 방법이 없습니다.
10000	NDMP	TCP	인바운드	• 서버에 타사 소프트웨어를 설치할 필요 없이 네트워크 백업 애플리케이션을 사용하여 NDMP(Network Data Management Protocol) 서버의 백업 및 복구를 제어할 수 있습니다. 어플라이언스에서는 NAS 서버가 NDMP 서버의 역할을 합니다. • NDMP 테이프 백업을 사용하지 않는 경우에는 NDMP 서비스를 비활성화할 수 있습니다. • NDMP 서비스 인증에는 사용자 이름/암호 쌍이 사용됩니다. 사용자 이름은 구성이 가능합니다. NDMP 문서에 다양한 환경에서 암호를 구성하는 방법이 설명되어 있습니다.
[10500,10531]	NDMP 동적 포트에 대해 NDMP 예약된 범위	TCP	인바운드	3-way 백업/복원 세션의 경우 NAS 서버는 10500 포트에서 10531 포트까지 사용합니다.
12228	안티바이러스 검사기 서비스	TCP	아웃바운드	안티바이러스 검사기 서비스에 필요합니다.

PowerStore X 모델 어플라이언스와 관련된 네트워크 포트

다음 표에는 PowerStore X model 어플라이언스에서 찾을 수 있는 여러 네트워크 포트 및 해당 서비스가 정리되어 있습니다.

표 4. PowerStore X model 어플라이언스와 관련된 네트워크 포트

포트	서비스	프로토콜	액세스 방향	설명
22	SSH 서버	TCP	인바운드	SSH 액세스 허용(활성화된 경우). 닫힌 경우 SSH를 통한 관리 연결을 사용할 수 없습니다.
80, 9000	vSphere Web Access	TCP	인바운드	vSphere Web Client용 vSphere Update Manager Web Client 플러그인 액세스.
427	CIM SLP(Service Location Protocol)	TCP/UDP	양방향	CIM 클라이언트는 SLPv2(Service Location Protocol, version 2)를 사용하여 CIM 서버를 찾습니다.
443	vSphere Web Client	TCP	인바운드	클라이언트 연결에 사용됩니다.
902	NFC(Network File Copy), VMware vCenter, vSphere Web Client	TCP	• NFC 양방향 • VMware vCenter 아웃바운드 • vSphere Web Client 인바운드	• NFC는 vSphere 구성 요소에 대한 파일 형식 인식 FTP 서비스를 제공합니다. ESXi는기본적으로 데이터 저장소 간에 데이터를 복사하고 이동하는 등의 작업을 위해 NFC를 사용합니다. • VMware vCenter 에이전트

표 4. PowerStore X model 어플라이언스와 관련된 네트워크 포트 (계속)

포트	서비스	프로토콜	액세스 방향	설명
				• vSphere Web Client의 경우 클라이언트 연결에 사용됩니다.
5900, 5901, 5902, 5903, 5904	RFB 프로토콜	TCP	인바운드	VNC와 같은 그래픽 사용자 인터페이스에 대한 원격 액세스.
5988	Common Information Model (CIM) Server	TCP	인바운드	CIM용 서버.
5989	CIM 보안 서버	TCP	인바운드	CIM용 서버.
6999	NSX Virtual Distributed Logical Router, rabbitmqproxy	UDP	• NSX Virtual Distributed Router 서비스용 양방향 • Rabbitmqproxy 아웃바운드	• NSX Virtual Distributed Router 서비스의 경우, NSX VIB가 설치되고 VDR 모듈이 생성될 때 이 서비스와 연관된 방화벽 포트가 열립니다. 호스트와 연관된 VDR 인스턴스가 없는 경우 포트가 열려 있지 않아도 됩니다. • Rabbitmqproxy의 경우 ESXi 호스트에서 실행되는 프록시입니다. 이 프록시는 가상 머신 내에서 실행 중인 애플리케이션이 vCenter 네트워크 도메인에서 실행되는 AMQP 브로커와 통신할 수 있게 합니다. 가상 머신이 네트워크에 있을 필요는 없습니다. 즉, NIC가 필요하지 않습니다. 송신 연결 IP 주소에 최소한 현재 또는 향후의 브로커가 포함되어 있는지 확인합니다. 나중에 브로커를 추가하여 크기를 늘릴 수 있습니다.
8000	vMotion	TCP	양방향	vMotion를 사용한 가상 머신 마이그레이션에 필요합니다. ESXi 호스트는 포트 8000에서 vMotion 트래픽에 대해 원격 ESXi 호스트로부터 TCP 연결을 수신 대기합니다.
8100, 8200, 8300	내결함성	TCP/UDP	양방향	vSphere 내결함성(FT)을 위한 호스트 간의 트래픽에 사용됩니다.
8301, 8302	DVSSync	UDP	양방향	DVSSync 포트는 VMware FT 레코드/리플레이을 활성화한 호스트 간에 분산된 가상 포트의 상태를 동기화하는 데 사용됩니다. 기본 또는 백업 가상 머신을 실행하는 호스트에만 이러한 포트가 열려 있어야 합니다. VMware FT를 사용하지 않는 호스트에서 이러한 포트는 열 필요가 없습니다.
9080	I/O 필터	TCP	아웃바운드	I/O 필터 스토리지 기능에 사용됩니다.
31031	vSphere Replication, VMware 사이트 복구 관리자	TCP	아웃바운드	vSphere Replication 및 VMware Site Recovery Manager에 의해 송출되는 복제 트래픽에 사용됩니다.
44046	vSphere Replication, VMware 사이트 복구 관리자	TCP	아웃바운드	vSphere Replication 및 Vmware Site Recovery Manager에 의해 송출되는 복제 트래픽에 사용됩니다.

3

감사

이 장에서 다루는 내용은 다음과 같습니다.

주제:

- 감사

감사

감사는 시스템에서의 사용자 활동에 대한 과거 내역 보기를 제공합니다. 관리자, 보안 관리자 또는 스토리지 관리자 역할을 가진 사용자는 REST API를 사용하여 시스템에서 구성 변경 이벤트를 검색하고 볼 수 있습니다. 감사되는 이벤트는 보안과 관련된 것이 아니며, 모든 세트 작업(POST/PATCH/DELETE)은 감사 로그에 기록됩니다.

PowerStore Manager UI 및 CLI와 같은 다른 인터페이스를 사용하여 감사 이벤트를 검색하고 볼 수 있습니다.

4

데이터 보안 설정

이 섹션에서 다루는 내용은 다음과 같습니다.

주제:

저장된 데이터 암호화

PowerStore의 D@RE(Data at Rest Encryption)는 기본 스토리지(NVMe SSD, NVMe SCM, SAS SSD)에 대해 FIPS 140-2로 검증된 SED(Self-Encrypting Drive)를 사용합니다. NVRAM 캐싱 디바이스는 암호화되었지만 현재 FIPS 140-2로 검증되지 않았습니다.

데이터를 미디어에 쓰기 전에 각 드라이브 내에서 암호화가 수행됩니다. 이는 드라이브의 데이터가 도난 또는 손실되지 않도록 보호하고 드라이브가 물리적으로 제거되어 직접 읽히지 못하도록 방지합니다. 또한, 암호화는 드라이브에서 정보를 빠르고 안전하게 삭제하여 정보를 복구할 수 없도록 하는 수단을 제공합니다. 이를 통해 미디어의 물리적 제거와 관련한 위협으로부터 데이터를 보호할 수 있을 뿐만 아니라, 이전에 해당 미디어에 저장된 데이터를 보호하는 데 사용된 암호화 키를 제거하여 미디어의 용도를 즉시 변경할 수도 있습니다.

암호화된 데이터를 읽으려면 드라이브 잠금을 해제할 SED 인증 키가 필요합니다. 인증된 SED만 잠금 해제되어 액세스할 수 있습니다. 데이터 잠금이 해제되면 SED 드라이브가 암호화된 데이터를 다시 원래 형태로 암호 해독합니다.

PowerStore 어플라이언스는 모든 SED를 포함해야 합니다. SED(Self-Encrypting Drive) 이외의 드라이브를 어플라이언스에 추가하려고 하면 어플라이언스에서 오류가 발생합니다. 또한, 암호화된 클러스터에서는 암호화되지 않은 어플라이언스가 지원되지 않습니다.

암호화 활성화

PowerStore 어플라이언스의 저장된 데이터 암호화 기능은 공장에서 설정됩니다. 암호화를 지원하는 어플라이언스를 가져올 수 있는 모든 국가에서는 기본값으로 암호화가 활성화되어 있습니다. 활성화된 암호화는 비활성화할 수 없습니다. 암호화를 지원하는 어플라이언스의 가져오기를 허용하지 않는 모든 국가에서는 저장된 데이터 암호화 기능이 비활성화됩니다.

노트: 저장된 데이터 암호화를 지원하지 않는 어플라이언스는 암호화된 어플라이언스와 클러스터링할 수 없습니다.

암호화 상태

어플라이언스의 암호화 상태는 다음과 같은 수준에서 보고됩니다.

- 클러스터 수준
- 어플라이언스 수준
- 드라이브 수준

클러스터 수준 암호화 상태는 단순히 어플라이언스의 암호화 활성화 여부를 나타냅니다. 이는 드라이브 상태와 관련이 없습니다.

어플라이언스의 암호화 상태는 다음 중 하나로 표시됩니다.

- 암호화됨 - 어플라이언스에서 암호화 기능이 활성화되어 있습니다.
- 암호화되지 않음 – 어플라이언스에서 암호화 기능이 지원되지 않습니다.

- 암호화 중 – 암호화 활성화 프로세스 중에 표시됩니다. 암호화 프로세스가 성공적으로 완료되면 클러스터 수준의 암호화 상태가 암호화됨으로 표시됩니다.

드라이브 수준의 암호화 상태는 어플라이언스의 각 드라이브에 대해 제공되며 다음 중 하나로 표시됩니다.

- 암호화됨 - 드라이브가 암호화되어 있습니다. 이는 암호화가 가능한 어플라이언스에 있는 드라이브의 일반적인 상태입니다.
- 암호화 중 - 어플라이언스가 드라이브에 암호화를 활성화하는 중입니다. 이 상태는 어플라이언스에서 암호화를 처음 활성화는 중이거나 이미 구성된 어플라이언스에 새 드라이브를 추가하는 동안에 표시될 수 있습니다.
- 비활성화됨 - 국가별 가져오기 제한 사항으로 인해 드라이브에서 암호화를 사용할 수 없습니다. 어느 하나의 드라이브라도 이 상태를 보고하는 경우 클러스터의 모든 드라이브도 동일한 상태를 보고합니다.
- 알 수 없음 - 아직은 어플라이언스가 드라이브에서 암호화를 활성화하려고 시도하지 않았습니다. 이 상태는 어플라이언스에서 암호화를 처음 활성화는 중이거나 이미 구성된 어플라이언스에 새 드라이브를 추가하는 동안에 표시될 수 있습니다.
- 지원되지 않음 – 드라이브가 암호화를 지원하지 않습니다.
- 외부 – 드라이브가 지원되지만 다른 어플라이언스에 의해 잠겨 있습니다. 이 경우 잠김을 해제해야 사용할 수 있습니다.

키 관리

임베디드 KMS(key manager service)는 각 PowerStore 어플라이언스의 액티브 노드에서 실행됩니다. 이 서비스는 로컬 키 저장소 파일 Lockbox 스토리지를 관리하여 시스템 및 부팅 드라이브에 대한 자동 암호화 키 백업을 지원합니다. 또한, 어플라이언스에서 SED(Self-Encrypting Drive) 잠금 및 잠금 해제 프로세스를 제어하며 어플라이언스의 로컬 키 저장소 콘텐츠를 관리하는 역할을 담당합니다. 로컬 키 저장소 파일은 RSA BSAFE 기술을 사용하는 256비트 AES 키로 암호화되어 키 저장소 파일 Lockbox 스토리지에 저장됩니다.

KMS는 어플라이언스를 초기화하는 동안 SED에 대한 무작위 인증 키를 자동으로 생성합니다. 각 드라이브에는 나중에 어플라이언스에 추가되는 인증서를 비롯해 SED 잠금 및 잠금 해제 프로세스에 사용되는 고유의 인증 키가 있습니다. 핵심 암호화 키는 파일 스토리지와 어플라이언스 내 플라이트에서 인증 및 암호화 키를 암호화합니다. 미디어 암호화 키는 SED의 전용 하드웨어에 저장되며 액세스할 수 없습니다. 암호화가 활성화되면 모든 인증 키가 어플라이언스 내에 저장됩니다.

키 저장소 백업 파일

KMS는 키 저장소 아카이브 파일에 대해 어플라이언스 밖에서 백업을 생성하고 다운로드하는 기능을 지원합니다. 어플라이언스 밖에서 백업을 실행하면 어플라이언스 또는 클러스터를 사용할 수 없게 만들 수 있는 심각한 키 손실 가능성을 줄여줍니다. 클러스터 키 저장소 백업이 시작될 때 특정 어플라이언스를 사용할 수 없게 되는 경우, 전체 작업은 성공적으로 완료되지만 클러스터 내 모든 어플라이언스에 대한 키 저장소 파일이 백업에 포함된 것은 아니며 오프라인 어플라이언스를 사용할 수 있는 경우 작업을 다시 시도해야 한다는 경고가 발생합니다.

노트: 클러스터의 기본 어플라이언스에는 클러스터 키 저장소 아카이브 파일이 포함되어 있습니다. 이 파일에는 기본 어플라이언스를 비롯해 그 클러스터에서 확인되는 각 어플라이언스에 대한 키 저장소 백업 복사본이 들어 있습니다.

클러스터 내에서 시스템 구성을 변경하여 키 저장소가 변경되는 경우에는 다운로드할 수 있는 새로운 키 저장소 아카이브 파일을 생성하는 것이 좋습니다. 키 저장소 아카이브 파일의 백업은 한 번에 하나씩만 다운로드할 수 있습니다.

노트: 새로 생성한 키 저장소 아카이브 파일은 외부의 안전한 위치에 다운로드하는 것이 적극 권장됩니다. 시스템의 키 저장소 파일이 손상되어 액세스할 수 없게 되면 해당 시스템이 서비스 모드로 전환됩니다. 이 경우, 백업 키 저장소 파일과 서비스 부서의 도움을 통해 문제를 해결해야 합니다.

키 저장소 파일을 백업하려면 관리자 또는 스토리지 관리자에 해당하는 사용자 역할이 필요합니다. 키 저장소 아카이브 파일을 백업하려면 **Settings**를 클릭하고 **Security**에서 **Encryption**을 선택합니다. 그리고 **Encryption** 페이지의 **Lockbox Backup**에서 **Download Keystore Backup**을 선택합니다.

노트: 장애가 발생한 경우 키 저장소 백업을 복원하려면 서비스 공급업체에 문의합니다.

암호화가 활성화된 어플라이언스의 드라이브 용도 변경

이 작업 정보

SED(self-encrypting drive) 어플라이언스는 초기화되거나 이미 초기화된 어플라이언스에 삽입될 때 잠깁니다. 이 드라이브를 먼저 잠금 해제하지 않으면 다른 시스템에서 사용할 수 없습니다. 잠겨 있는 드라이브를 다른 어플라이언스에 삽입하면 해당 드라이브를 사용할 수 없게 되고 암호화 상태는 새 어플라이언스에 `Foreign`으로 표시됩니다. 드라이브의 용도를 새 어플라이언스에 맞게 변경할 수는 있지만 이 경우 드라이브에 있는 모든 기존 데이터가 손실됩니다.

암호화 상태가 `Foreign`인 드라이브의 용도를 변경하려면 다음을 수행합니다.

단계

1. 드라이브 후면의 레이블에 있는 PSID(Physical Security ID)를 기록해 둡니다. PSID는 용도 변경 프로세스 중에 제공해야 합니다.
2. PowerStore Manager에서 **Hardware**를 클릭하고 어플라이언스를 선택한 뒤 **Hardware** 카드를 선택합니다.
3. 용도를 변경할 드라이브를 선택합니다.
   드라이브의 **Encryption Status**가 `Foreign`으로 나타날 것입니다.
4. **Repurpose Drive**를 클릭합니다.
   Repurpose Drive 슬라이드 아웃이 표시됩니다.
5. 드라이브의 PSID를 입력하고 **Apply**를 클릭합니다.

결과

용도 변경 프로세스가 완료되면 드라이브가 어플라이언스에서 새 드라이브로 용도 변경되며 암호화 상태는 `Encrypted`로 변경됩니다.

암호화가 활성화된 시스템에서 베이스 인클로저 및 노드 교체

암호화가 활성화된 어플라이언스에서 base enclosure 및 nodes를 교체하려면 서비스 계약이 필요합니다.

어플라이언스를 공장 출하 설정으로 재설정

`svc_factory_reset` 서비스 스크립트는 어플라이언스를 공장 출고 상태로 되돌리고 모든 사용자 데이터와 지속되는 구성을 삭제합니다.

다중 어플라이언스 클러스터의 경우 `svc_factory_reset` 명령이 보조 어플라이언스에서 실행될 수 없습니다. 대신 `svc_remove_appliance` 서비스 스크립트를 실행해야 합니다. 이 스크립트는 시스템을 공장 출고 상태로 되돌리고, 모든 사용자 데이터와 지속되는 구성을 삭제합니다. 기본 어플라이언스만 클러스터에 남아 있는 경우 `svc_factory_reset` 명령을 실행하여 해당 어플라이언스를 초기화할 수 있습니다.

노트: 이러한 스크립트는 검증된 서비스 공급업체만 실행하는 것이 좋습니다.

이 스크립트에 대한 자세한 정보는 *PowerStore Service Scripts Guide* 문서를 참조 바랍니다.

5

보안 서비스 기능 설정

이 장에서 다루는 내용은 다음과 같습니다.

주제:

운영에 대한 설명: SupportAssist™

SupportAssist 기능은 Dell EMC 지원 부서에서 사용자의 어플라이언스로부터 오류 파일 및 알림 메시지를 받아 원격으로 문제 해결 절차를 수행하여 문제를 빠르고 효율적으로 해결할 수 있도록 IP 기반 연결을 제공합니다.

노트: 문제 진단 및 문제 해결 속도를 높여 문제를 빠르게 해결하려면 SupportAssist 기능을 활성화하는 것이 매우 좋습니다. SupportAssist을 활성화하지 않으면 Dell EMC 지원 부서가 어플라이언스의 문제를 해결하도록 하기 위해 어플라이언스 정보를 수동으로 수집해야 할 수 있습니다. 데이터를 CloudIQ로 전송하려면 어플라이언스에 SupportAssist 기능을 활성화해야 합니다. CloudIQ에 대한 자세한 내용은 www.dell.com/support를 참조 바랍니다. 로그인한 후 CloudIQ **제품 지원** 페이지를 찾습니다.

SupportAssist 및 보안

SupportAssist 기능은 원격 연결 프로세스의 각 단계 전반에서 다층적인 보안 기능을 적용하므로 고객과 Dell EMC가 안심하고 솔루션을 이용할 수 있습니다.

- Dell EMC로 전달되는 모든 알림은 외부 소스가 아닌 고객 사이트에서 생성되며 AES(Advanced Encryption Standard) 256비트 암호화를 통해 안전하게 보호됩니다.
- IP 기반 아키텍처가 기존 인프라스트럭처와 완벽하게 통합되어 고객 환경의 보안을 유지합니다.
- 고객 사이트와 Dell EMC 간의 통신은 RSA® 디지털 인증서를 사용하여 양쪽에서 인증됩니다.
- 2단계 인증 방식을 통해 확인된 Dell EMC 공인 고객 서비스 담당자만이 적절한 디지털 인증서를 다운로드하여 고객 사이트에서 전송된 알림을 조회할 수 있습니다.
- SupportAssist v3 정책 관리자 애플리케이션은 고객이 자체 지침 및 요건에 따라 Dell EMC 지원 부서에 액세스 권한을 부여하거나 제한하기 위해 사용할 수 있는 옵션이며 자세한 감사 로그를 제공합니다.

SupportAssist 관리

PowerStore Manager 또는 REST API를 사용하여 SupportAssist 기능을 관리할 수 있습니다. 서비스를 활성화 또는 비활성화할 수 있으며, 선택하는 SupportAssist 옵션에 필요한 관련 정보를 제공할 수 있습니다.

노트: 중앙 집중식 SupportAssist에 대한 **Gateway Connect with remote assist** 및 **Gateway Connect without remote assist** 옵션은 고가용성을 지원하지 않습니다. 이 옵션은 활성화된 고가용의 SupportAssist 클러스터에 페일오버 기능을 제공하지 않습니다. PowerStore 어플라이언스가 단일 HA 게이트웨이 클러스터 서버(사용 가능한 유일한 구성 옵션)에 배포된 경우 클러스터 내에서 장애가 발생하지 않은 게이트웨이 서버에 대해 페일오버 기능이 없습니다. 어플라이언스에 연결된 HA 게이트웨이 서버의 작동이 중지될 경우 Call Home 및 CloudIQ 파일과 같은 아웃바운드 파일을 Dell EMC 지원 부서에 전송하는 작업이 중지됩니다. 어플라이언스에 대한 SupportAssist 인바운드 연결 구성(원격 액세스)은 클러스터 내에서 HA 장애가 발생하지 않은 HA 게이트웨

이 서버를 사용하여 계속 작동합니다. 또한, SupportAssist **Gateway Connect with remote assist** 및 **Gateway Connect without remote assist** 옵션은 시스템의 지정된 기본 어플라이언스에만 구성해야 합니다.

어플라이언스 자체는 어떠한 정책도 구현하지 않습니다. 어플라이언스에 대한 원격 액세스를 더 세밀하게 제어해야 한다면 정책 관리자를 사용하여 인증 사용 권한을 설정할 수 있습니다. 정책 관리자 소프트웨어 구성 요소는 고객이 제공한 서버에 설치됩니다. 디바이스에 대한 원격 액세스를 제어하고 원격 연결의 감사 로그를 유지 관리하며 파일 전송 작업을 지원합니다. 어플라이언스에 액세스할 수 있는 사용자, 액세스하는 내용 및 시기를 제어할 수 있습니다. 정책 관리자에 대한 자세한 내용은 www.dell.com/support를 참조하십시오. 웹사이트에 로그인한 후 해당하는 **Support by Product** 페이지로 이동하여 원하는 SupportAssist 제품 기술 설명서에 대한 링크를 검색합니다.

SupportAssist 통신

노트: 관리 네트워크에 IPv6를 사용하여 구성된 PowerStore 모델에서는 SupportAssist를 활성화할 수 없습니다. SupportAssist는 IPv6에서 지원되지 않습니다. 또한 클러스터에 SupportAssist를 구성하는 경우 IPv4에서 IPv6로의 관리 네트워크 재구성이 허용되지 않습니다.

SupportAssist 기능이 작동하려면 DNS 서버에 액세스할 수 있어야 합니다.

SupportAssist의 **Connection Status**는 PowerStore 및 Dell EMC 백엔드 지원 서비스의 연결 상태와 연결의 서비스 품질을 보여줍니다. 연결 상태는 5분 기준으로 결정되며 연결의 서비스 품질이 24시간 이내에 결정 됩니다. **Connection Status**는 클러스터에 있는 어플라이언스를 기준으로 다음 중 하나로 나타날 수 있습니다.

- `Unavailable` – 연결 데이터를 사용할 수 없습니다. 어플라이언스와 연결이 끊기거나 SupportAssist이 활성화된지 얼마되지 않아 상태를 결정할 데이터가 부족한 경우입니다.
- `Disabled` – SupportAssist이 활성화되지 않았습니다.
- `Not connected` – 연결이 끊어졌습니다. 5번 연속 keepalive 페일오버가 감지되었습니다.
- `Reconnecting` – 연결 손실 후 PowerStore에서 재연결을 시도하는 중입니다. 연결된 상태로 다시 전환되려면 5번 연속 keepalive 요청이 필요합니다.

Connection Status는 PowerStore이 Dell EMC 백엔드 지원 서비스에 연결된 경우 클러스터에 있는 모든 어플라이언스의 평균에 따라 다음 중 하나로 표시될 수 있습니다.

- `Evaluating` – 연결 서비스 품질은 SupportAssist가 처음으로 시작된 후 처음 24시간 동안은 확인되지 않습니다.
- `Good` – 연속 keepalive 요청이 80% 이상 성공했습니다.
- `Fair` - 연속 keepalive 요청의 50%~80% 성공했습니다.
- `Poor` - 연속 keepalive 요청의 50% 미만으로 성공했습니다.

SupportAssist 옵션

SupportAssist 기능은 Dell EMC 지원 부서에서 사용자의 시스템으로부터 오류 파일 및 알림 메시지를 받아 원격으로 문제 해결 절차를 수행하여 문제를 빠르고 효율적으로 해결할 수 있도록 IP 기반 연결을 제공합니다.

원격 문제 해결을 위해 어플라이언스 정보를 Dell EMC 지원 부서에 보낼 때는 다음과 같은 세 가지 SupportAssist 옵션을 사용할 수 있습니다.

- Gateway Connect without remote access - 양방향 파일 전송을 통해 고객이 제공한 게이트웨이 서버에서 실행되며 중앙 집중식 SupportAssist으로 다음을 포함합니다.
  - Call Home
  - CloudIQ 지원
  - 소프트웨어 알림
  - Dell EMC 지원 부서에서 클러스터로 운영 환경/펌웨어 다운로드

  SupportAssist 게이트웨이 서버는 게이트 웨이와 연관된 어플라이언스에 대한 모든 IP 기반 SupportAssist 활동의 시작 및 종료 단일 지점입니다.
- Gateway Connect with remote access – 원격 액세스 및 Dell EMC 지원 담당자를 위한 원격 액세스 없이, Direct Connect와 동일하게 2 방향 파일 전송을 이용해 실행되는 SupportAssist을 위한 옵션입니다.
- Direct Connect without remote access — 원격 액세스가 없는 Gateway Connect로 동일하게 양방향 파일 전송을 이용해 개별 어플라이언스에서 실행되는 분산형 SupportAssist을 위한 옵션입니다.
- Direct Connect with remote access — 원격 액세스 및 Dell EMC 지원 담당자를 위한 원격 액세스 없이, Direct Connect와 동일하게 2 방향 파일 전송을 이용해 개별 어플라이언스에서 실행되는 분산형 SupportAssist을 위한 옵션입니다.

또 다른 옵션인 비활성화됨은 사용할 수 있지만 권장되지 않습니다. 이 옵션을 선택하는 경우 Dell EMC 지원 부서가 어플라이언스의 문제에 대한 알림 메시지를 받지 않습니다. 따라서 지원 담당자가 어플라이언스의 문제를 해결하는 데 도움을 주기 위해 어플라이언스 정보를 수동으로 수집해야 할 수 있습니다.

SupportAssist Direct Connect 옵션

SupportAssist Gateway Connect는 게이트웨이 서버에서 실행됩니다. **Gateway Connect without remote access** 옵션 또는 **Gateway Connect with remote access** 옵션을 선택하면 해당 어플라이언스가 SupportAssist 클러스터의 다른 어플라이언스에 추가됩니다. 클러스터는 Dell EMC 지원 서버와 오프 어레이 게이트웨이 서버 간 단일 공통(중앙 집중식) 보안 연결 뒤에 상주합니다. 게이트웨이 서버는 게이트웨이에 연결된 어플라이언스에 대한 모든 IP 기반 Dell EMC SupportAssist 활동의 단일 시작 및 종료 지점입니다.

게이트웨이 서버는 고객이 제공한 하나 이상의 전용 서버에 설치되는 원격 지원 솔루션 애플리케이션입니다. 게이트웨이 서버는 연결된 어플라이언스와 Dell EMC 엔터프라이즈 간 통신 브로커 기능을 수행합니다.

SupportAssist 게이트웨이 및 정책 관리자에 대한 자세한 내용은 Dell 지원 웹사이트(www.dell.com/support)의 SupportAssist 제품 페이지에서 확인할 수 있습니다.

어플라이언스가 SupportAssist에 대해 **Gateway Connect without remote access** 옵션 또는 **Gateway Connect with remote access** 옵션을 사용하도록 구성하려면, 게이트웨이 서버의 IP 주소 및 포트 넘버(기본값 9443)를 제공해야 합니다. 또한 게이트웨이 서버와 어플라이언스 사이에 포트가 열려 있는지 확인합니다.

노트: 어플라이언스에서 이 게이트웨이 서버를 사용하도록 구성하기 전에 게이트웨이 서버가 준비되어 있고 실행 중이어야 합니다. PowerStore Manager에서만 어플라이언스를 게이트웨이에 추가할 수 있습니다. 어플라이언스를 게이트웨이 서버에서 추가한 경우에는 어플라이언스가 연결된 것으로 나타나지만 시스템 정보가 성공적으로 전송되지 않습니다.

SupportAssist Direct Connect 옵션

SupportAssist Direct Connect는 각 어플라이언스의 기본 노드에서 직접 실행됩니다. 클러스터에서 각 어플라이언스는 Dell EMC 지원 부서에 대한 자체 연결을 수립합니다. 트래픽은 클러스터의 기본 어플라이언스를 통해 라우팅되지 않습니다. 하지만 SupportAssist는 클러스터 수준에서만 관리할 수 있습니다. 즉, 모든 변경 내용이 클러스터의 모든 어플라이언스에 적용됩니다.

PowerStore Manager에서 **Support** 아래의 **Settings**으로 이동하여 **Support Assist** 페이지에서 SupportAssist Direct Connect를 활성화 및 구성합니다. 이러한 작업을 통해 어플라이언스를 설정하여 어플라이언스와 Dell EMC 지원 간에 보안 연결을 사용합니다. SupportAssist Direct Connect에는 다음 원격 서비스 연결 옵션 중 하나를 선택할 수 있습니다.

- **Direct Connect without remote access**
- **Direct Connect with remote access**

Direct Connect without remote access 옵션을 선택하고 EULA(End User License Agreement)에 동의하는 경우, 어플라이언스가 Dell EMC 지원 부서와의 보안 연결을 설정합니다. 이 옵션을 사용하면 Dell EMC 지원 부서와의 양방향 파일 전송 연결이 가능합니다. 해당하는 경우 어플라이언스와 그 연결된 프록시 서버(선택 사항) 간의 연결을 구성할 수 있습니다. 필요에 따라 나중에 원격 액세스 구성 설정을 이용해 Direct Connect로 업그레이드할 수 있습니다.

Direct Connect with Remote Access 옵션을 선택하고 EULA(End User License Agreement)에 동의하는 경우, 어플라이언스가 Dell EMC 지원 부서와의 보안 연결을 설정합니다. 이 옵션을 사용하면 어플라이언스와 Dell EMC 지원 부서 간에 양방향 파일 전송과 함께 원격 액세스 서비스 연결이 가능합니다. 해당하는 경우 PowerStore Manager를 통해 어플라이언스와 정책 관리자 및 모든 연결된 프록시 서버(선택 사항) 간의 연결을 구성할 수 있습니다.

기존 클러스터에 새 어플라이언스를 추가하는 경우 새 어플라이언스는 클러스터 SupportAssist 설정을 감지하고 새 어플라이언스를 일치되도록 자동 구성합니다. 현재 SupportAssist Direct Connect가 활성화되어 있으면 새 어플라이언스에서도 자동으로 활성화됩니다. 추가 작업은 필요하지 않습니다. SupportAssist Direct Connect를 활성화할 수 없더라도 어플라이언스 추가 프로세스에 지장을 주지는 않습니다.

SupportAssist Gateway Connect 요구 사항

Gateway Connect without remote access 및 **Gateway Connect with remote access**에 SupportAssist 구현 시 모두 다음 요구 사항이 적용됩니다.

- 포트 9443(또는 다른 경우 고객이 지정한 포트)에서 어플라이언스와 SupportAssist 게이트웨이 서버 간의 네트워크 트래픽(HTTPS)이 허용되어야 합니다.
- SupportAssist 버전이 4.0.5 또는 3.38이어야 합니다.

노트: 절대 게이트웨이 서버에서 어플라이언스를 수동으로 추가 또는 제거해서는 안 됩니다. PowerStore Manager SupportAssist 구성 마법사를 사용하는 방법으로만 게이트웨이 서버에서 어플라이언스를 추가 또는 제거합니다.

SupportAssist Direct Connect에 대한 요구 사항

Direct Connect without remote access 및 **Direct Connect with remote access** SupportAssist 구현 시 모두 다음 요구 사항이 적용됩니다.

- 포트 443 및 8443(아웃바운드)에서 Dell EMC 지원 부서로의 네트워크 트래픽(HTTPS)이 허용되어야 합니다. 포트 8443이 열리지 않으면 성능에 심각한 영향(30~45%)을 미칩니다. 두 포트 모두 열리지 않으면 엔드 디바이스 관련 문제 해결이 지연될 수 있습니다.

다음 요구 사항은 원격 액세스 **Direct Connect with Remote Access** SupportAssist 구현 시에만 적용됩니다.

- 어플라이언스에 대한 원격 액세스를 더 효율적으로 제어할 수 있도록 구현 시 정책 관리자를 포함하려는 경우 SupportAssist 기능 구성 과정에서 이를 지정해야 합니다.

SupportAssist 구성

다음 방법 중 하나를 사용하여 어플라이언스에 대한 SupportAssist를 구성할 수 있습니다.

- 초기 구성 마법사 - PowerStore Manager 초기 설정을 돕고 시스템을 준비하는 데 도움을 주는 사용자 인터페이스.
- **Suppoprt Assist** – PowerStore Manager(**Settings** 클릭 후 **Support**에서 **SupportAssist** 선택)에서 액세스할 수 있는 설정 페이지.
- REST API 서버 - SupportAssist 설정을 구성하라는 REST API 요청을 수신할 수 있는 애플리케이션 인터페이스. REST API에 대한 자세한 정보는 PowerStore REST API Reference Guide를 참조 바랍니다.

SupportAssist 기능의 상태를 확인하려면 PowerStore Manager에서 **Support** 아래의 **Settings**를 클릭하고 Support에서 **SupportAssist**를 선택합니다.

SupportAssist 구성

이 작업 정보

PowerStore Manager를 사용하여 SupportAssist을 구성하려면 다음을 수행합니다.

노트: **Direct Connect with remote access** 옵션을 **Direct Connect without remote access** 또는 **Gateway Connect** 옵션 중 하나로 변경하려면 Dell EMC 서비스 담당자의 도움이 필요합니다.

단계

1. **Support**에서 **Settings**를 클릭하고 **SupportAssist**를 선택합니다.
2. SupportAssist의 상태가 비활성으로 표시되는 경우 **SupportAssist** 제어 아이콘을 클릭하여 SupportAssist를 활성화합니다.
   SupportAssist 기능은 비활성화하는 것이 가능하지만 그렇게 하지 않는 것이 좋습니다.
   버튼이 오른쪽으로 이동하고 표시를 `Enabled`로 변경해야 합니다. 하지만 필요한 구성 정보를 입력하고 **Apply**를 클릭한 후에만 **Connection Status**가 변경됩니다.
3. 기본값으로, **SupportAssist**에서 **Connect to CloudIQ** 확인란이 선택되어 있습니다. 파일을 CloudIQ 보내지 않으려면 해당 확인란을 선택 취소합니다. 그렇지 않은 경우에는 확인란을 선택된 상태로 둡니다.
4. 사용할 SupportAssist 옵션의 **Type**을 목록에서 선택합니다.
5. 선택하는 SupportAssist 옵션의 유형에 따라 다음 중 하나를 수행합니다.
   - **Gateway Connect without remote access** 또는 **Gateway Connect with remote access** 옵션의 경우:
     - 게이트웨이 서버의 IP 주소를 지정합니다.
       노트: 어플라이언스에서 이 게이트웨이 서버를 사용하도록 구성하기 전에 게이트웨이 서버가 준비되어 있고 실행 중이어야 합니다.
     - 게이트웨이 서버에 연결하는 데 사용할 포트가 기본값(9443)과 다른 경우 컨트롤을 이용해 네트워크에 사용될 포트의 번호를 선택합니다.
   - **Direct Connect without remote access** 옵션:

- 네트워크 연결에서 프록시 서버를 사용하는 경우 프록시 서버의 IP 주소를 지정합니다.
  노트: 시스템에서 이 프록시 서버를 사용하도록 구성하기 전에 프록시 서버가 준비되어 있고 실행 중이어야 합니다.
- 컨트롤을 이용해, 네트워크의 프록시 서버에 연결하는 데 사용할 포트 번호를 선택합니다.

- **Direct Connect with Remote Access** 옵션:
  - 네트워크 연결에서 프록시 서버를 사용하는 경우 프록시 서버의 IP 주소를 지정합니다.
    노트: 어플라이언스에서 이 프록시 서버를 사용하도록 구성하기 전에 프록시 서버가 준비되어 있고 실행 중이어야 합니다.
  - 컨트롤을 이용해, 네트워크의 프록시 서버에 연결하는 데 사용할 포트 번호를 선택합니다.
  - 정책 관리자를 사용하여 시스템에 대한 원격 액세스를 제어하려는 경우 정책 관리자의 IP 주소를 지정합니다.
    노트: 어플라이언스에서 이 정책 관리자를 사용하도록 구성하기 전에 정책 관리자가 준비되어 있고 실행 중이어야 합니다.
  - 정책 관리자에 연결하는 데 사용할 포트가 기본값(9443)과 다른 경우 컨트롤을 이용해 네트워크에 사용될 포트의 번호를 선택합니다.

6. 선택하는 SupportAssist 옵션의 유형에 따라 다음 중 하나를 수행합니다.
   - **Direct Connect without remote access** 또는 **Direct Connect with Remote Access** 옵션의 경우 다음 단계로 이동합니다.
   - **Gateway Connect without remote access** 또는 **Gateway Connect with Remote Access** 옵션의 경우, **Test Connection**을 선택해 게이트웨이 서버의 연결 상태를 확인합니다.

   노트: 연결 상태가 계속 `Transitioning`으로 나타나고 몇 분(연결성 테스트 시 소요 시간) 후에도 바뀌지 않으면 온라인 고객 서비스에 문의합니다.

7. 확실한 연결성을 확인하려면 테스트 알림을 Dell EMC 지원 부서에 전송할 수 있도록 **Send Test Alert**를 선택합니다.
8. 표시된 연락처 정보가 정확한지 확인합니다. 잘못되었거나 오래된 것으로 표시되는 모든 정보를 수정합니다.
   SupportAssist 연락처 정보는 문제에 신속하게 대응하는 데 중요하며 정확하고 최신이어야 합니다.
9. SupportAssist 구성 정보를 보존하려면 **Apply**를 선택합니다.

A

TLS 암호 그룹

이 부록에서 다루는 내용은 다음과 같습니다.

주제:

- 지원되는 TLS 암호 그룹

지원되는 TLS 암호 그룹

암호 그룹은 TLS 통신 보안을 유지하는 기술 집합을 정의합니다.

- 키 교환 알고리즘(클라이언트에서 서버로 전송되는 데이터의 암호화에 암호 키를 사용하는 방법). 예: RSA 키 또는 DH(Diffie-Hellman)
- 인증 방법(호스트가 원격 호스트의 ID를 인증하는 방법). 예: RSA 인증서, DSS 인증서, 또는 인증하지 않음
- 암호화(데이터 암호화 방법). 예: AES(256 또는 128비트)
- 해시 알고리즘(데이터의 수정 여부를 확인하는 방법을 제공하여 데이터 보안 유지). 예: SHA-2 또는 SHA-1

지원되는 암호 그룹에는 이 모든 항목이 결합됩니다.

다음은 어플라이언스 및 그 연결되는 포트에 사용할 수 있는 TLS 암호 그룹의 OpenSSL 이름 목록입니다.

표 5. 어플라이언스에서 지원되는 기본값/지원 TLS 암호 그룹

암호 그룹	프로토콜	포트
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443, 8443