# OpenManage Integration for VMware vCenter 버전 5.3

## 보안 구성 가이드

2021년 3월
개정 A00

DELL EMC

## 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

# 그림

# 표

# 1

# 서문

제품군을 개선하기 위한 노력의 일환으로, Dell EMC는 소프트웨어 및 하드웨어에 대한 개정 사항을 주기적으로 릴리스합니다. 이 문서에 설명된 일부 기능은 현재 사용 중인 소프트웨어 또는 하드웨어의 모든 버전에서 지원되지 않을 수 있습니다. 제품 릴리스 노트는 제품 기능에 대한 최신 정보를 제공합니다.

제품이 제대로 작동하지 않거나 이 문서에 설명된 대로 작동하지 않는 경우 Dell EMC 기술 지원 전문가에게 문의하십시오. 이 문서는 발행 시점에 정확했습니다. 이 문서의 최신 버전을 사용하고 있는지 확인하려면 **https://www.dell.com/support**를 방문하십시오.

## 용도

이 문서에는 OMIVV(OpenManage Integration for VMware vCenter)의 보안 기능 및 각종 기능에 대한 정보가 포함되어 있습니다.

## 대상

이 문서는 OMIVV의 보안 관리를 담당하는 개인을 대상으로 합니다.

## 개정 내역

다음 표에는 이 문서의 개정 내역이 나와 있습니다.

**표 1. 개정 내역**

| 개정 | 날짜 | 설명 |
|---|---|---|
| A00_5.2.0 | 2020년 10월 | OpenManage Integration for VMware vCenter 5.2 보안 구성 가이드의 최초 릴리스입니다. |
| A00_5.3.0 | 2021년 3월 | 인증 및 데이터 보안 항목에 RESTful API 관련 정보가 추가되었습니다. |

## 관련 설명서

OMIVV에 대한 전체 문서 세트는 **https://www.dell.com/support**에서 확인할 수 있습니다. **모든 제품 찾아보기**를 클릭한 다음 **소프트웨어** > **가상화 솔루션**을 클릭합니다. 다음 문서에 액세스하려면 **OpenManage Integration for VMware vCenter**를 클릭합니다.

- *OpenManage Integration for VMware vCenter 버전 5.3 사용자 가이드*
- *OpenManage Integration for VMware vCenter 버전 5.3 릴리스 노트*
- *OpenManage Integration for VMware vCenter 버전 5.3 호환성 매트릭스*
- *OpenManage Integration for VMware vCenter 버전 5.3 API 가이드*
- *OpenManage Integration for VMware vCenter 버전 5.3 설치 가이드*

https://www.dell.com/support에서 백서를 포함한 기술 아티팩트를 찾을 수 있습니다.

# 2

# 본 문서에 사용된 용어

**표 2. 본 문서에 사용된 용어**

| 용어 | 설명 |
|---|---|
| OMIVV | OpenManage Integration for VMware vCenter |
| OVF | Open Virtualization Format |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| NFS | Network File System |
| CIFS | Common Internet File System |
| OM MP | OpenManage Management Pack for vRealize Operations |
| CMC | Chassis Management Controller(M1000e, FX, VRTX) |
| OME-M | OpenManage Modular Edition(MX7000) |
| iDRAC | Integrated Dell Remote Access Controller |
| SNMP | Simple Network Management Protocol |
| VM | 가상 시스템 |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| PEM | Privacy-Enhanced Mail |
| RPM | Red Hat Package Manager |
| OS | 운영 체제 |

# 3

# 배포 모델

OMIVV(OpenManage Integration for VMware vCenter)를 VMware vCenter 환경에서 OVF로 배포할 수 있습니다.

**주제:**



## OVF(Open Virtualization Format) 구축

VMware vSphere 가상 시스템 환경을 갖추고 있는 경우, OMIVV를 OVF(Open Virtualization Format)로 구축하는 것이 권장됩니다.

OVF 배포 모델에는 OMIVV 소프트웨어를 비롯하여 OMIVV 소프트웨어가 실행되는 Linux 운영 체제가 사전 구성된 번들이 포함되어 있습니다.

OVF 환경에는 모니터링된 시스템의 OMIVV 통신 요구 사항에 맞게 조정되어 사전 구성된 방화벽도 포함되어 있습니다.

OVF는 OVF 템플릿 파일과 함께 구축됩니다. OMIVV를 OVF로 배포하기에 관한 자세한 내용은 **https://www.dell.com/support**에서 제공되는 *OpenManage Integration for VMware vCenter 5.3 설치 가이드*를 참조하십시오.

## 보안 프로필

OMIVV는 안전한 HTTP 액세스를 위한 기본 보안 프로필을 갖추고 있습니다. 보안 환경 강화를 위해 CA(Certificate Authority) 서명된 인증서를 교체하는 것이 적극 권장됩니다.

# 4

# 제품 및 하위 시스템 보안

**주제:**



## 보안 제어 맵

OMIVV는 iDRAC을 사용하여 PowerEdge 서버의 배포, 인벤토리, 업데이트를 수행하고 iDRAC으로부터 SNMP 트랩을 수신합니다.

OMIVV의 사용자 인터페이스는 어플라이언스 관리 웹 페이지입니다. OMIVV 플러그인 UI는 VMware vCenter Client에서 작동하며 호스트 하드웨어 모니터링 및 관리 기능을 제공합니다.

모든 시스템 자격 증명은 OMIVV 보안 스토리지 내에 저장됩니다.

다음 그림은 OMIVV 보안 제어 맵을 표시합니다.

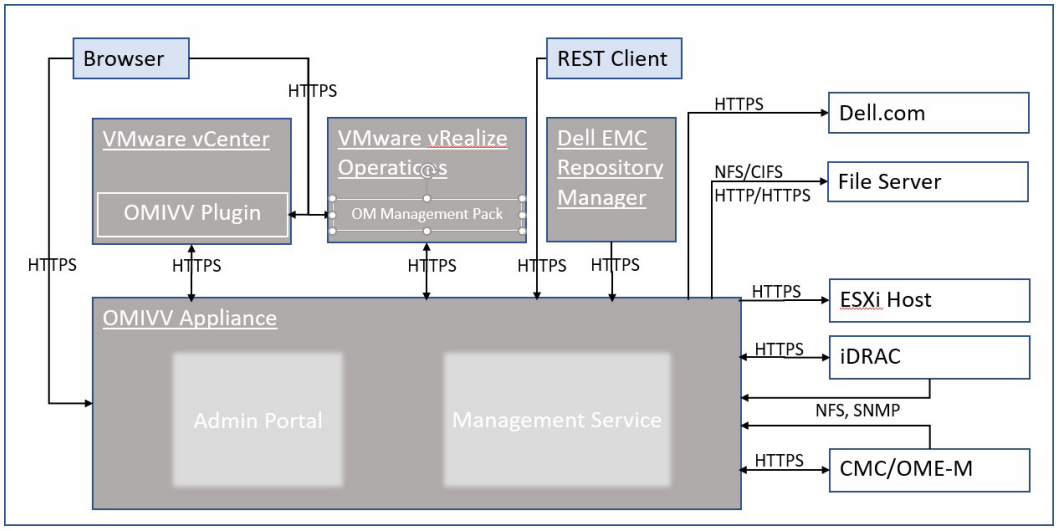


**그림 1. 보안 제어 맵**

# 인증

## 액세스 제어

액세스 제어 설정을 통해 무단 액세스로부터 리소스를 보호할 수 있습니다. OMIVV 플러그인 페이지는 VMware vCenter에 구성된 적절한 역할 및 권한이 있는 VMware vCenter 사용자가 액세스할 수 있습니다. OMIVV 관리 콘솔 및 RESTFul API 액세스 권한은 OMIVV 어플라이언스 관리자 계정에 부여됩니다.

## 기본 사용자 계정

OMIVV에는 다음과 같은 기본 사용자 계정이 포함됩니다.

- 로컬 사용자 계정
- 읽기 전용 사용자 계정
- 루트 계정

### 로컬 사용자 계정

OMIVV는 단일 기본 로컬 관리 사용자 계정을 제공합니다. 이러한 내부 계정의 사용자 이름은 admin입니다.

로컬 관리자는 Dell EMC OMIVV 관리 콘솔에서만 모든 작업에 접속할 수 있습니다.

OMIVV를 최초로 배포할 때, 암호를 설정하라는 프롬프트가 표시됩니다. 화면에 표시되는 지침을 따라 암호를 설정합니다.

### 읽기 전용 사용자 계정

OMIVV는 단일 기본 로컬 읽기 전용 사용자 계정을 제공합니다. 읽기 전용 계정의 사용자 이름은 readonly입니다.

관리자는 VM 원격 콘솔을 사용해서만 OMIVV에 로그인할 수 있습니다.

이 계정은 문제 해결 중에 중요한 어플라이언스 상태 및 로그를 확인하는 데 사용될 수 있습니다.

OMIVV를 최초로 배포할 때, 암호를 설정하라는 프롬프트가 표시됩니다. 화면에 표시되는 지침을 따라 암호를 설정합니다.

### 루트 계정

OMIVV 어플라이언스에는 운영 체제 루트 계정이 있습니다.

이 기본 계정은 접속할 수 없습니다. 기술 지원 팀은 루트 계정을 사용하여 필드 문제를 디버깅합니다.

## 외부 사용자 계정

VMware vCenter 사용자는 vCenter에 대한 적절한 역할 및 권한이 있는 경우 vCenter HTML5 클라이언트에서 OMIVV 플러그인 사용자 인터페이스 요소에 접속할 수 있습니다. 역할 및 권한에 대한 자세한 내용은 관리자가 아닌 사용자의 필수 권한 페이지 13을(를) 참조하십시오.

# 로그인 보안 설정

## 로그인 동작 실패

OMIVV에는 인증 실패가 수차례 발생할 경우에 대비한 보안 설정이 포함되어 있습니다.

# 로컬 사용자 계정 차단

로컬 사용자 계정에 대한 로그인 시도를 6회 연속 실패하면 OMIVV는 사용자를 1분간 일시적으로 차단합니다.

# 자동 세션 시간 초과

## 유휴 브라우저 세션 시간 초과

기본적으로 15분간 활동이 없으면 OMIVV 세션이 시간 초과되어 자동으로 로그아웃됩니다.

# 인증 유형 및 설정 고려 사항

## vCenter 사용자 인증

OMIVV에서는 vCenter 작업을 처리하는 플러그인 페이지 및 RESTful API에 대한 액세스에 vCenter 인증을 사용합니다. vCenter 작업을 처리하는 플러그인 페이지와 RESTful API에는 등록 중에 vCenter에서 Dell EMC가 생성한 권한이 필요합니다.

## 새 vCenter Server 등록

### 전제조건

vCenter 계정에는 사용자를 생성하는 데 필요한 권한이 있어야 합니다. 필요한 권한에 대한 자세한 내용은 관리자가 아닌 사용자의 필수 권한 페이지 13 섹션을 참조하십시오.

### 이 작업 정보

OMIVV를 설치한 후 OMIVV 어플라이언스를 등록할 수 있습니다. OMIVV는 vCenter 운영을 위해 필요한 권한이 포함된 관리자 사용자 계정 또는 비관리자 사용자 계정을 사용합니다. 단일 OMIVV 어플라이언스 인스턴스는 총 15대의 vCenter Server(연결된 모드 포함 또는 제외) 및 최대 2,000대의 ESXi 호스트를 지원할 수 있습니다.

15대가 넘는 vCenter 등록을 시도하면 다음 오류 메시지가 표시됩니다.

라이선스는 <x> vCenter에만 허용되며 모두 이미 등록되어 있습니다.

새 vCenter Server를 등록하려면 다음을 수행합니다.

### 단계

1. https://<Appliance IP 또는 hostname>으로 이동합니다.
2. **VCENTER 등록** 페이지의 오른쪽 창에서 **새 vCenter Server 등록**을 클릭합니다.
   **새 vCenter 등록** 페이지가 표시됩니다.
3. **새 vCenter 등록** 대화 상자의 **vCenter 이름** 아래에서 다음 작업을 수행합니다.
   a. **vCenter Server IP 또는 호스트 이름** 상자에 vCenter IP 주소 또는 호스트의 FQDN을 입력합니다.
      정규화된 도메인 이름(FQDN)을 사용하여 VMware vCenter에 OMIVV를 등록하는 것이 좋습니다. 모든 등록의 경우, vCenter의 호스트 이름이 DNS 서버에서 제대로 확인되어야 합니다. 다음은 DNS 서버 이용을 위한 권장 관행입니다.
      - 유효한 DNS 등록이 포함된 OMIVV 어플라이언스를 배포할 때 정적 IP 주소 및 호스트 이름을 할당합니다. 정적 IP 주소로 시스템을 다시 시작할 때 OMIVV 어플라이언스의 IP 주소를 동일하게 유지할 수 있습니다.
      - DNS 서버의 정방향 및 역방향 조회 영역 모두에 OMIVV 호스트 이름 정보가 표시되는지 확인합니다.
   b. **설명** 상자에 설명(선택 사항)을 입력합니다.
4. **vCenter 사용자 계정** 아래에서 다음 단계를 수행합니다.
   a. **vCenter 사용자 이름** 상자에 관리자의 사용자 이름 또는 필요한 권한이 있는 관리자가 아닌 사용자 이름을 입력합니다.
   b. **암호** 상자에 암호를 입력합니다.
   c. **암호 확인** 상자에서 암호를 다시 입력합니다.
   d. **vSphere Lifecycle Manager 등록** 확인란을 선택합니다.

**vSphere Lifecycle Manager 등록** 확인란을 선택하면 vCenter 7.0 이상에서 vSphere Lifecycle Manager 기능을 사용할 수 있습니다.

5. **등록**을 클릭합니다.

   vCenter 등록에 실패하면 다음 오류 메시지가 표시됩니다.

   잘못된 자격 증명으로 인해 지정된 vCenter Server <x>에 연결할 수 없습니다. 사용자 이름과 암호를 확인하십시오.

### 결과

vCenter Server를 등록하면 OMIVV가 vCenter 플러그인으로 등록되고 OMIVV 기능에 액세스할 수 있는 vSphere Client에 "Dell EMC OpenManage Integration" 아이콘이 표시됩니다.

**노트:** OMIVV 어플라이언스의 모든 vCenter 작업의 경우, OMIVV는 VMware vCenter 또는 OMIVV 어플라이언스 로컬 계정에 로그인한 사용자의 권한이 아니라 등록된 사용자의 권한을 사용합니다. 예를 들면, 필요한 권한이 있는 사용자 X가 vCenter에 OMIVV를 등록하고 사용자 Y는 Dell 권한만 가지고 있습니다. 사용자 Y는 이제 vCenter에 로그인하여 OMIVV로부터 펌웨어 업데이트 작업을 트리거할 수 있습니다. 펌웨어 업데이트 작업을 수행하는 동안 OMIVV는 사용자 X의 권한을 사용하여 호스트를 유지 보수 모드로 두거나 호스트를 재부팅합니다.

**노트:** CA(Certificate Authority)에서 서명한 맞춤 구성 인증서를 OMIVV로 업로드하려면 vCenter 등록 전에 새로운 인증서를 업로드해야 합니다. vCenter 등록 후에 새로운 맞춤 구성된 인증서를 업로드하면 vSphere Client에 통신 오류가 표시됩니다. 이 문제를 해결하려면 로그아웃하고 vCenter에 로그인하십시오. 문제가 계속되면 vCenter Server에서 vSphere Client 서비스를 재시작하십시오.

# 관리자가 아닌 계정을 사용하여 vCenter 서버 등록

### 전제조건

vCenter 관리자 자격 증명 또는 Dell 권한이 있는 관리자가 아닌 사용자를 사용하여 OMIVV 어플라이언스용 vCenter 서버를 등록할 수 있습니다.

### 이 작업 정보

vCenter 서버를 등록하는 데 필요한 권한이 있는 관리자가 아닌 사용자를 사용하려면 다음 단계를 수행합니다.

### 단계

1. 역할에 필요한 권한으로 역할을 생성하거나 기존 역할을 수정합니다.

   역할에 필요한 권한 목록에 대한 자세한 내용은 관리자가 아닌 사용자의 필수 권한을 참조하십시오.

   역할을 생성하거나 수정하고 vSphere Client(HTML-5)에서 권한을 선택하는 데 필요한 단계는 VMware vSphere 설명서를 참조하십시오.
2. 역할을 정의하고 역할에 대한 권한을 선택한 후 새로 생성된 역할에 사용자를 할당합니다.

   권한에 역할을 할당하기에 대한 자세한 내용은 VMware vSphere 설명서를 참조하십시오.

   필요한 권한을 가진 vCenter 서버 관리자가 아닌 사용자가 이제 vCenter를 등록 또는 등록 해제하거나, 자격 증명을 수정하거나, 인증서를 업데이트할 수 있습니다.
3. 필요한 권한이 있는 관리자가 아닌 사용자를 사용하여 vCenter 서버를 등록합니다.
4. 등록이 완료된 후에 1단계에서 생성했거나 수정한 역할에 Dell 권한을 할당합니다. 기존 역할에 Dell 권한 할당 페이지 14을(를) 참조하십시오.

### 결과

이제 필요한 권한이 있는 관리자가 아닌 사용자는 Dell EMC 호스트를 사용하여 OMIVV 기능을 사용할 수 있습니다.

# 관리자가 아닌 사용자의 필수 권한

OMIVV를 vCenter에 등록하려면 관리자가 아닌 사용자에게 다음 권한이 있어야 합니다.

다음 권한이 할당되지 않으면 관리자가 아닌 사용자가 vCenter를 OMIVV에 등록하는 동안 메시지가 표시됩니다.

- 알람
  - 알람 생성
  - 알람 수정

    - 알람 제거
- 확장명
    - 확장명 등록
    - 확장명 등록 취소
    - 확장명 업데이트
- 전역
    - 작업 취소
    - 이벤트 로그
    - 설정
- 상태 업데이트 공급자
    - 등록
    - 등록 취소
    - 업데이트
- 호스트
    - CIM
        - CIM 상호 작용
- Host.Config
    - 고급 설정
    - 설정 변경
    - 연결
    - 유지 보수
    - 네트워크 구성
    - 쿼리 패치
    - 보안 프로필 및 방화벽
- 인벤토리
    - 클러스터에 호스트 추가
    - 독립 실행형 호스트 추가
    - 클러스터 수정
- Lifecycle Manager: 일반 권한
    - 읽기

    **노트:** Lifecycle Manager 일반 권한은 vCenter 7.0 이상에만 적용됩니다.
- 호스트 프로필
    - 편집
    - 보기
- 권한
    - 권한 수정
    - 역할 수정
- 세션
    - 세션 유효성 검사
- 작업
    - 생성
    - 업데이트

**노트:** 관리자가 아닌 사용자를 사용하여 OMIVV 기능에 액세스하기 위해 vCenter 서버를 등록한 경우 관리자가 아닌 사용자는 Dell 권한이 있어야 합니다. Dell 권한 할당에 대한 자세한 내용은 기존 역할에 Dell 권한 할당 페이지 14을(를) 참조하십시오.

# 기존 역할에 Dell 권한 할당

**이 작업 정보**

로그인한 사용자에게 할당된 Dell 권한 없이 OMIVV의 특정 페이지에 액세스하는 경우 2000000 오류가 표시됩니다.

기존 역할을 편집하여 Dell 권한을 할당할 수 있습니다.

**단계**

1. 관리 권한을 사용하여 vSphere Client(HTML-5)에 로그인합니다.
2. vSphere Client(HTML-5)에서 **메뉴**를 확장하고 **관리→ 역할**을 클릭합니다.

3. **역할 공급자** 드롭다운 목록에서 vCenter Server를 선택합니다.
4. **역할** 목록에서 **Dell-Operational**을 선택한 후 **권한**을 클릭합니다.
5. Dell 권한을 할당하려면 편집 아이콘 [ ]을 클릭합니다.
   **역할 편집** 페이지가 표시됩니다.
6. 왼쪽 창에서 **Dell**을 클릭하고 선택한 역할에 대해 다음 Dell 권한을 선택한 후 **다음**을 클릭합니다.
   - Dell.Configuration
   - Dell.Deploy-Provisioning
   - Dell.Inventory
   - Dell.Monitoring
   - Dell.Reporting

   vCenter 내에서 사용 가능한 OMIVV 역할에 대한 자세한 내용은 Dell 운영 역할 페이지 16()을 참조하십시오.
7. 필요한 경우 역할 이름을 편집하고 선택한 역할에 대한 설명을 입력합니다.
8. **마침**을 클릭합니다.
   로그아웃한 다음 vCenter에서 로그인합니다. 이제 필요한 권한이 있는 사용자가 OMIVV 작업을 수행할 수 있습니다.

# vCenter 사용자 보안

## 보안 역할 및 권한

OpenManage Integration for VMware vCenter는 암호화된 형식으로 사용자 자격 증명을 저장합니다. 그리고 부적절한 요청을 막기 위해 클라이언트 애플리케이션에 암호를 제공하지 않습니다. 백업 데이터베이스는 맞춤 구성된 보안 구문을 사용하여 완전히 암호화되므로 데이터가 오용되지 않습니다.

기본적으로 관리자 그룹의 사용자는 모든 권한을 가지고 있습니다. 관리자는 VMware vSphere 웹 클라이언트 내에서 OpenManage Integration for VMware vCenter의 모든 기능을 사용할 수 있습니다. 필요한 권한을 가진 사용자가 제품을 관리하도록 하려면 다음을 수행하십시오.

1. 필요한 권한의 역할을 만듭니다
2. 사용자를 사용하여 vCenter Server를 등록합니다
3. Dell 운영 역할 및 Dell 인프라 배포 역할을 모두 포함합니다.

### 데이터 무결성

OpenManage Integration for VMware vCenter, 관리 콘솔 및 vCenter 사이의 통신은 HTTPS를 사용하여 수행합니다. OpenManage Integration for VMware vCenter는 vCenter와 어플라이언스 간 신뢰할 수 있는 통신에 사용되는 인증서를 만듭니다. 또한 통신 및 OpenManage Integration for VMware vCenter 등록 전에 vCenter Server의 인증서를 확인하고 신뢰합니다.

보안 관리 콘솔 세션은 15분의 유휴 시간 제한이 있으며 이 세션은 현재 브라우저 창 및/또는 탭에서만 유효합니다. 새 창 또는 탭에서 세션을 열려고 하면 유효한 세션을 요청하는 보안 오류 메시지가 표시됩니다. 또한 이 작업 덕분에 사용자는 관리 콘솔 세션을 공격할 수 있는 악성 URL을 클릭하지 않게 됩니다.

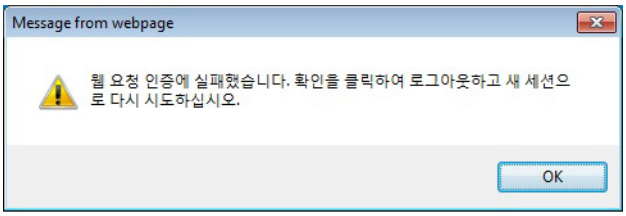


그림 2 . 보안 오류 메시지

## 액세스 제어 인증, 권한 부여 및 역할

OpenManage Integration for VMware vCenter에서는 vCenter 작업을 수행하기 위해 vSphere Client의 현재 사용자 세션과 OpenManage Integration에 대하여 저장된 관리 자격 증명을 사용합니다. OpenManage Integration for VMware vCenter에서는 vCenter Server의 내장된 역할 및 권한 모델을 사용하여 OpenManage Integration 및 vCenter의 관리되는 개체(호스트 및 클러스터)를 사용하는 사용자 작업에 대한 권한을 부여합니다.

## Dell 운영 역할

이 역할에는 펌웨어 업데이트, 하드웨어 인벤토리, 호스트 재시작, 유지 보수 모드에 호스트 배치 또는 vCenter Server 작업 생성을 비롯하여 어플라이언스 및 vCenter Server 작업을 수행하기 위한 권한/그룹이 포함됩니다.

이 역할에 다음 권한 그룹이 포함됩니다.

### 표 3. 권한 그룹

| 그룹 이름 | 설명 |
|---|---|
| 권한 그룹 - Dell.Configuration | 호스트 관련 작업 수행, vCenter 관련 작업 수행, SelLog 구성, ConnectionProfile 구성, ClearLed 구성 및 펌웨어 업데이트 |
| 권한 그룹 - Dell.Inventory | 인벤토리 구성, 보증 검색 구성 및 읽기 전용 구성 |
| 권한 그룹 - Dell.Monitoring | 모니터링 구성, 모니터 |
| 권한 그룹 - Dell Reporting(사용되지 않음) | 보고서 생성, 보고서 실행 |

## Dell 인프라 배포 역할

이 역할에는 하이퍼바이저 배포 기능과 관련된 권한이 포함되어 있습니다.

이 역할이 제공하는 권한은 호스트 자격 증명 프로필 구성, ID 할당 및 배포입니다.

**권한 그룹 — Dell.Deploy-Provisioning**

호스트 자격 증명 프로필 구성, ID 할당, 배포.

## 권한 정보

OpenManage Integration for VMware vCenter에서 수행하는 모든 작업은 권한과 관련이 있습니다. 다음 섹션에는 사용 가능한 작업 및 연관된 권한이 나열되어 있습니다.

- Dell.Configuration.Perform vCenter 관련 작업
  - 유지 보수 모드 종료 및 시작
  - 권한을 쿼리하기 위해 vCenter 사용자 그룹 가져오기
  - 알람 등록 및 구성(예: 이벤트 설정 페이지에서 알람 활성화/비활성화)
  - vCenter에 이벤트/알림 게시
  - 이벤트 설정 페이지에 이벤트 설정 구성
  - 이벤트 설정 페이지에서 기본 알림 복원
  - 알림/이벤트 설정을 구성하는 동안 클러스터에 대한 DRS 상태 확인
  - 업데이트 또는 기타 구성 작업을 수행한 후 호스트 재부팅
  - vCenter 작업 상태/진행률 모니터
  - vCenter 작업 생성(예: 펌웨어 업데이트 작업, 호스트 구성 작업 및 인벤토리 작업)
  - vCenter 작업 상태/진행률 업데이트
  - 호스트 프로필 가져오기
  - 데이터 센터에 호스트 추가
  - 클러스터에 호스트 추가
  - 호스트에 프로필 적용
  - CIM 자격 증명 가져오기
  - 규정 준수를 위해 호스트 구성
  - 규정 준수 작업 상태 가져오기
- Dell.Inventory.Configure 읽기 전용
  - 연결 프로필을 구성하는 동안 vCenter 트리를 구성하기 위해 모든 vCenter 호스트 가져오기
  - 탭을 선택할 때 호스트가 Dell 서버인지 확인
  - vCenter의 주소/IP 가져오기
  - 호스트 IP/주소 가져오기
  - vSphere Client 세션 ID를 기반으로 현재 vCenter 세션 사용자 가져오기
  - 트리 구조에 vCenter 인벤토리를 표시하기 위해 vCenter 인벤토리 트리 가져오기
- Dell.Monitoring.Monitor

- 이벤트를 게시하기 위한 호스트 이름 가져오기
- 이벤트 로그 작업 수행(예: 이벤트 개수 가져오기 또는 이벤트 로그 설정 변경)
- 이벤트/알림 등록, 등록 취소 및 구성 – SNMP 트랩 수신 및 이벤트 게시

- Dell.Configuration.Firmware 업데이트
  - 펌웨어 업데이트 수행
  - 펌웨어 업데이트 마법사 페이지에서 펌웨어 리포지토리 및 DUP 파일 정보 로드
  - 펌웨어 인벤토리 쿼리
  - 펌웨어 리포지토리 설정 구성
  - 준비 기능을 사용하여 준비 폴더 구성 및 업데이트 수행
  - 네트워크 및 리포지토리 연결 테스트
- Dell.Deploy-Provisioning.Create Template
  - HW 구성 프로필 구성
  - 하이퍼바이저 배포 프로필 구성
  - 연결 프로필 구성
  - ID 할당
  - 배포
- Dell.Configuration.Perform 호스트 관련 작업
  - 점멸 LED, 점등 LED
  - iDRAC 콘솔 실행
  - SEL 로그 표시 및 지우기
- Dell.Inventory.Configure Inventory
  - Dell 서버 관리 탭에 시스템 인벤토리 표시
  - 스토리지 상세정보 가져오기
  - 전원 모니터링 상세정보 가져오기
  - 연결 프로필 페이지에 연결 프로필 생성, 표시, 편집, 삭제 및 테스트
  - 인벤토리 스케줄 예약, 업데이트 및 삭제
  - 호스트에서 인벤토리 실행

# 사용자 및 자격 증명 관리

## 사전 로드된 계정

다음 표는 사전 로드된 OMIVV 계정을 설명합니다.

### 표 4. 사전 로드된 계정

| 사용자 계정 | 설명 |
|---|---|
| OpenManage Integration for VMware vCenter 관리자 | OMIVV 웹 애플리케이션 관리를 위한 기본 사용자입니다. |
| 읽기 전용 사용자입니다. | OMIVV는 단일 기본 로컬 읽기 전용 사용자 계정을 제공합니다.<br>관리자는 VM 원격 콘솔을 사용해서만 OMIVV에 로그인할 수 있습니다.<br>이 계정은 문제 해결 중에 중요한 어플라이언스 상태 및 로그를 확인하는 데 사용될 수 있습니다. |
| Linux 운영 체제 루트 | 루트 운영 체제 계정은 접속할 수 없습니다. 기술 지원 팀은 루트 계정을 사용하여 필드 문제를 디버깅합니다. |

## 기본 자격 증명

다음 표에서는 사전 로드된 OMIVV 계정의 기본 자격 증명을 설명합니다.

### 표 5. 기본 자격 증명

**표 5. 기본 자격 증명**

| 계정 | 사용자 | 암호 |
|---|---|---|
| OpenManage Integration for VMware vCenter 관리자 | 관리자 | 배포 후 첫 번째 부팅에서 설정합니다. 관리자 암호 변경에 대한 자세한 내용은 OMIVV 어플라이언스 암호 변경 페이지 18를 참조하십시오. |
| 읽기 전용 사용자 | 읽기 전용 | 배포 후 첫 번째 부팅에서 설정합니다. 읽기 전용 사용자 암호는 표준 Linux 암호 변경 명령을 사용하여 읽기 전용 사용자로 로그인한 후 재구성될 수 있습니다. |
| Linux 운영 체제 루트 | 루트 | OS 루트 암호는 OMIVV가 배포될 때 설정됩니다. |

# 자격 증명 관리

Dell EMC 관리 콘솔에 최초로 로그인하는 경우 관리자로 로그인합니다(기본 사용자 이름은 admin).

**노트:** 관리자 암호를 잊어버린 경우 OMIVV 어플라이언스에서 복구할 수 없습니다.

## OMIVV 어플라이언스 암호 변경

**이 작업 정보**

콘솔을 사용하여 vSphere Client에서 OMIVV 어플라이언스 암호를 변경할 수 있습니다.

**단계**

1. OMIVV 웹 콘솔을 엽니다.
2. **OpenManage Integration for VMware vCenter 가상 어플라이언스 설정** 유틸리티에서 **관리자 암호 변경**을 클릭합니다. 화면의 지시 사항에 따라 암호 설정을 완료합니다.
3. **현재 암호** 텍스트 상자에서 현재 관리자 암호를 입력합니다.
4. **새 암호** 텍스트 상자에 새 암호를 입력합니다.
5. **새 암호 확인** 텍스트 상자에 새 암호를 다시 입력합니다.
6. **관리자 암호 변경**을 클릭합니다.

# 인증

OMIVV 어플라이언스는 단일 관리 사용자를 지원합니다.

OMIVV에 로그인한 후, 관리자는 다음과 같은 OMIVV 어플라이언스 구성 기능만 이용할 수 있습니다.

- 새 vCenter Server 등록
- 어플라이언스 구성
- RPM과 백업 및 복원을 사용하여 OMIVV 어플라이언스 업그레이드
- Network Time Protocol 서버 설정
- 배포 모드 구성
- 인증서 서명 요청(CSR) 생성
- HTTPS 인증서 업로드
- 전역 알림 설정
- 문제 해결 번들 생성 및 다운로드

# 네트워크 보안

OMIVV 어플라이언스는 TCP 및 UDP 포트로 인바운드 및 아웃바운드 네트워크 트래픽을 제한함으로써 보안을 강화하기 위해 사전 구성된 방화벽을 사용합니다. 이 섹션의 표에는 OMIVV에서 사용하는 인바운드 및 아웃바운드 포트가 나열되어 있습니다.

## 네트워크 노출

OpenManage Integration for VMware vCenter는 원격 시스템과 통신할 때 인바운드 및 아웃바운드 포트를 사용합니다.

## 아웃바운드 포트

원격 시스템에 연결할 때 OMIVV에서 아웃바운드 포트를 사용할 수 있습니다.

다음 표에 나열된 포트는 OMIVV 아웃바운드 포트입니다.

**표 6. 아웃바운드 포트**

| 포트 번호 | 계층 4 프로토콜 | 서비스 |
|---|---|---|
| 7 | TCP, UDP | ECHO |
| 22 | TCP | SSH |
| 25 | TCP | SMTP |
| 53 | UDP, TCP | DNS |
| 67,68 | TCP | DHCP |
| 80 | TCP | HTTP |
| 88 | TCP, UDP | Kerberos |
| 111 | TCP, UDP | ONC RPC |
| 123 | TCP, UDP | NTP |
| 161-163 | TCP, UDP | SNMP |
| 389 | TCP, UDP | LDAP |
| 443 | TCP | HTTPS |
| 448 | TCP | Data Protection Search 관리자 REST API |
| 464 | TCP, UDP | Kerberos |
| 514 | TCP, UDP | rsh |
| 587 | TCP | SMTP |
| 636 | TCP, UDP | LDAPS |
| 902 | TCP | VMware ESXi |
| 2049 | TCP, UDP | NFS |
| 2052 | TCP, UDP | mountd, clearvisn |
| 3009 | TCP | Data Domain REST API |
| 5672 | TCP | amqp를 통한 RabbitMQ |
| 8443 | TCP | MCSDK 8443은 443의 대체재 |
| 9002 | TCP | Data Protection Advisor REST API |
| 9443 | TCP | Avamar 관리 콘솔 웹 서비스 |

# 인바운드 포트

OMIVV에 연결할 때 원격 시스템에서 사용될 수 있는 인바운드 포트입니다.

다음 표에 나열된 포트는 OMIVV 인바운드 포트입니다.

**표 7. 인바운드 포트**

| 포트 번호 | 계층 4 프로토콜 | 서비스 |
|---|---|---|
| 22 | TCP | SSH |
| 80 | TCP | HTTP |
| 443 | TCP | HTTPS |
| 5671 | TCP | amqp를 통한 RabbitMQ |

# 데이터 보안

OMIVV에서 유지 관리하는 데이터는 어플라이언스 내의 내부 데이터베이스에서 저장 및 보안 처리되며 외부에서 액세스할 수 없습니다.

OMIVV를 통해 전송되는 데이터는 보안 통신 채널에서 보안 처리됩니다.

**노트:** RESTful API 사용자는 환경 제한에 따라 안전하게 검색된 자격 증명과 데이터를 저장하는 것이 좋습니다.

# 암호화

OMIVV는 다음 구성 요소에 암호화를 사용합니다.

- 액세스 제어
- 인증
- 디지털 시그너처

# 인증서 관리

OMIVV는 안전한 HTTP 액세스(HTTPS)용 인증서를 사용합니다.

기본적으로 OMIVV는 HTTPS 보안 트랜잭션용 자체 서명된 인증서를 설치 및 사용합니다.

보안 강화를 위해 CA(Certificate Authority) 서명되거나 맞춤 구성된 인증서 사용이 권장됩니다.

자체 서명된 인증서만으로 웹 브라우저와 서버 간에 암호화된 채널을 설정할 수 있습니다. 자체 서명된 인증서는 인증용으로는 사용될 수 없습니다.

다음 유형의 인증서를 OMIVV 인증용으로 사용할 수 있습니다.

- 자체 서명된 인증서

  OMIVV는 어플라이언스의 호스트 이름이 변경되면 자체 서명된 인증서를 생성합니다.
- 신뢰할 수 있는 CA(Certificate Authority) 공급업체에서 서명하는 인증서입니다.

**노트:** 인증서를 생성할 때 사규를 고려하십시오.

## 등록된 vCenter Server의 인증서 업데이트

**이 작업 정보**

OpenManage Integration for VMware vCenter는 키 길이가 2,048비트인 RSA 암호화 표준을 이용하여 CSR(인증서 서명 요청)을 생성하기 위해 OpenSSL API를 사용합니다.

vCenter Server에서 인증서가 변경된 경우 다음 작업을 수행하여 OMIVV를 위한 새 인증서를 가져옵니다.

### 단계

1. https://<Appliance IP 또는 hostname>으로 이동합니다.
2. 왼쪽 창에서 **VCENTER 등록**을 클릭합니다.
   등록된 vCenter Server가 작업 창에 표시됩니다.
3. vCenter Server IP 또는 호스트 이름에 대한 인증서를 업데이트하려면 **업데이트**를 클릭합니다.

## CSR(Certificate Signing Request) 생성

### 전제조건

기본적으로 OMIVV에는 자체 서명된 인증서가 있습니다. OMIVV에 대해 CA(Certificate Authority)에서 서명한 맞춤 구성 인증서가 필요한 경우 vCenter 등록 전에 새 인증서를 업로드하는 것이 좋습니다.

### 이 작업 정보

새 인증서 CSR를 생성하면 이전에 생성한 CSR로 만든 인증서가 어플라이언스에 업로드되지 않습니다. CSR을 생성하려면 다음을 수행합니다.

### 단계

1. **어플라이언스 관리** 페이지의 **HTTPS 인증서** 영역에서 **인증서 서명 요청 생성**을 클릭합니다.
   새 요청을 생성하면 이전 CSR을 사용하여 생성한 인증서를 더는 어플라이언스에 업로드할 수 없다는 메시지가 표시됩니다. 요청을 계속하려면 **계속**을 클릭합니다.
2. 요청을 계속할 경우 **인증서 서명 요청 생성** 대화 상자에서 일반 이름, 조직 이름, 지역, 주, 국가, 이메일 주소 및 SAN(Subject Alternate Name)에 대한 정보를 입력한 다음 **계속**을 클릭합니다.

   **노트:** OMIVV는 SAN에 대해 여러 개의 값을 지원하지 않습니다.

3. **다운로드**를 클릭하고 결과로 생성되는 CSR을 액세스 가능한 위치에 저장합니다.

## HTTPS 인증서 업로드

### 전제조건

인증서는 PEM 형식을 사용해야 합니다.

### 이 작업 정보

OMIVV 어플라이언스와 호스트 시스템 또는 vCenter와의 보안 통신을 위해 HTTPS 인증서를 사용할 수 있습니다. 이 유형의 보안 통신을 설정하려면 CSR 인증서를 서명 기관에 보낸 후, 받은 CSR을 관리 콘솔을 사용하여 업로드합니다. 자체 서명된 기본 인증서를 보안 통신에 사용할 수도 있습니다. 이 인증서는 모든 설치에서 고유합니다.

### 단계

1. **어플라이언스 관리** 페이지의 **HTTPS 인증서** 영역에서 **인증서 업로드**를 클릭합니다.
2. **인증서 업로드** 대화 상자에서 **확인**을 클릭합니다.
3. 인증서를 업로드하려면 **찾아보기**를 클릭한 후 **업로드**를 클릭합니다.
   상태를 확인하려면 등록된 vCenter의 vSphere Client에서 **이벤트 콘솔**로 이동합니다.

### 결과

인증서를 업로드하는 동안 OMIVV 관리 콘솔이 최대 3분 동안 응답하지 않습니다. HTTPs 인증서 업로드 작업이 완료되면 브라우저 세션을 닫고 새 브라우저 세션에서 관리 포털에 액세스합니다.

## 기본 HTTPS 인증서 복원

### 단계

1. **어플라이언스 관리** 페이지의 **HTTPS 인증서** 영역에서 **기본 인증서 복원**을 클릭합니다.
2. **기본 인증서 복원** 대화 상자에서 **적용**을 클릭합니다.

**결과**

인증서를 복원하는 동안 OMIVV 관리 콘솔이 최대 3분 동안 응답하지 않습니다. 기본 HTTPs 인증서 복원 작업이 완료된 후 브라우저 세션을 닫고 새 브라우저 세션에서 관리 포털에 액세스합니다.

# 감사 및 로깅

관리자는 OMIVV 관리 콘솔을 사용하여 모든 관련 로그가 포함된 문제 해결 번들을 생성할 수 있습니다.

자세한 내용은 문제 해결 번들 생성 및 다운로드 페이지 22 섹션을 참조하십시오.

읽기 전용 계정은 사용자가 런타임에 어플라이언스의 다양한 매개변수를 읽을 수 있도록 하여 어플라이언스 문제 해결을 지원합니다. 고급 문제 해결은 기술 지원 부서에서 특정 매개변수를 확인하도록 안내합니다.

**노트:** OMIVV 관리자만 어플라이언스에서 쓰기 작업을 수행할 수 있습니다. OMIVV 로그에서는 사용자 감사를 사용할 수 없습니다. vCenter 플러그인에서 수행되는 vCenter 작업에 대한 자세한 내용은 vCenter 감사 로그를 참조하십시오. RESTful API의 경우 클라이언트가 감사 로깅을 처리할 수 있어야 합니다.

## 문제 해결 번들 생성 및 다운로드

**이 작업 정보**

문제 해결 번들에는 문제 해결을 지원하거나 기술 지원 부서로 전송하는 데 사용할 수 있는 OMIVV 어플라이언스 로깅 정보가 포함되어 있습니다. OMIVV는 사용자 기밀 데이터를 기록하지 않습니다.

**단계**

1. **지원** 페이지에서 **문제 해결 번들 생성 및 다운로드**를 클릭합니다.
   **문제 해결 번들** 대화 상자가 표시됩니다.
2. **문제 해결 번들** 대화 상자에서 **생성**을 클릭합니다.
   로그 크기에 따라 번들을 생성하는 데 다소 시간이 걸릴 수 있습니다.
3. 파일을 저장하려면 **다운로드**를 클릭합니다.
   Dell EMC OMIVV 관리 콘솔 로그인 페이지가 표시됩니다.
4. Dell EMC OMIVV 관리 콘솔에 로그인합니다.
5. 문제 해결 번들을 다운로드합니다. 자세한 내용은 문제 해결 번들 생성 및 다운로드 페이지 22 섹션을 참조하십시오.

## 문제 해결 번들 생성 및 다운로드

**전제조건**

문제 해결 번들을 생성하려면 관리 포털에 로그인해야 합니다.

**이 작업 정보**

문제 해결 번들에는 문제 해결을 지원하거나 기술 지원 부서로 전송하는 데 사용할 수 있는 OMIVV 로깅 정보가 포함되어 있습니다.

**단계**

1. **어플라이언스 관리** 페이지에서 **문제 해결 번들 생성**을 클릭합니다.
2. **문제 해결 번들 다운로드**를 클릭합니다.

# 서비스 가용성

지원 웹사이트 **https://www.dell.com/support**에서 라이선스 정보, 제품 설명서, 권장 사항, 다운로드, 문제 해결 정보를 이용할 수 있습니다. 이러한 정보는 지원 팀에 문의하기 전에 제품 문제를 해결하는 데 도움이 됩니다.

서비스 직원용 OMIVV에 대한 특별 로그인이 필요하지 않습니다. 문제 해결 번들이 충분하지 않은 경우, 직원이 루트 사용자가 추가 정보를 수집하도록 지원할 수 있습니다.

보안 패치 및 기타 업데이트가 제공되는 경우 설치해야 합니다(OMIVV vCenter 운영 체제 업데이트 등).

## 보안 패치

보안 업데이트를 포함하는 주기적인 OMIVV 업데이트 및 필요에 따라 릴리스되는 보안 전용 업데이트입니다.

업데이트는 누적되어 지원에 게시되며 OMIVV 사용자는 vCenter에서 동일한 알림을 받게 됩니다.

# OMIVV OS 업데이트

주기적으로 OMIVV OS에 대한 보안 패치 및 수정 사항이 릴리스됩니다.

이러한 수정 사항은 RPM 업데이트 패키지를 통해 OMIVV의 기존 OVF 배포에 설치되어야 합니다. 이용 가능한 경우 RPM 업데이트를 통해 이러한 보안 패치 및 수정 사항을 OMIVV 서버에 설치하는 것이 적극 권장됩니다.

# 제품 코드 무결성

OMIVV 소프트웨어 설치 프로그램은 Dell에서 서명했습니다. OMIVV 설치 프로그램 서명의 신뢰성을 검증하는 것이 권장됩니다.

# 5

# 기타 구성 및 관리

**주제:**



## OMIVV(OpenManage Integration for VMware vCenter) 라이선스

OMIVV는 두 가지 유형의 라이선스를 제공합니다.

- 평가판 라이선스 - OMIVV 어플라이언스의 전원을 처음 켜면, 평가판 라이선스가 자동으로 설치됩니다. 평가 버전에는 OMIVV에서 관리되는 호스트(서버) 5개에 대한 평가판 라이선스가 포함되어 있습니다. 이 90일 평가 버전은 배송 시 제공되는 기본 라이선스입니다.
- 표준 라이선스 - OMIVV에서 관리하는 호스트 라이선스를 원하는 수만큼 구매할 수 있습니다. 이 라이선스에는 제품 지원 및 OMIVV 어플라이언스 업데이트가 포함됩니다. 표준 라이선스는 3년 또는 5년 동안 사용할 수 있습니다. 추가 라이선스를 구매하면 기존 라이선스 기간이 연장됩니다. 표준 라이선스는 평가판 라이선스를 덮어씁니다.

단일 XML 키에 대한 라이선스 기간은 원래 주문의 판매 날짜를 기준으로 계산됩니다. 업로드된 새 라이선스는 이전에 만료된 라이선스에 대한 90일 유예 기간이 종료된 후 개수에 반영됩니다.

OMIVV에서는 최대 15개의 vCenter 인스턴스를 지원합니다. 평가판 라이선스를 정식 표준 라이선스로 업그레이드하면, 이메일로 주문 확인서가 전송되며 Dell Digital Locker에서 라이선스 파일을 다운로드할 수 있습니다. 라이선스 .XML 파일을 로컬 시스템에 저장하고 **관리 콘솔**을 사용하여 새 라이선스 파일을 업로드합니다.

라이선스를 구매하면 https://www.dell.com/support의 Dell Digital Locker에서 .XML 파일(라이선스 키)을 다운로드할 수 있습니다. 라이선스 키가 다운로드되지 않는 경우 **https://www.dell.com/support**에서 주문 지원 부서에 문의로 이동하여 해당 제품의 지역 Dell 지원 부서 전화 번호를 찾아 Dell 지원 부서에 문의합니다.

라이선스의 OMIVV 관리 콘솔에서는 다음과 같은 정보가 제공됩니다.

- 최대 vCenter 연결 라이선스 수 - 등록되어 사용 중인 vCenter 연결은 최대 15개까지 활성화됩니다.
- 최대 호스트 연결 라이선스 - 구매한 호스트 연결 수입니다(단일 OMIVV 인스턴스에 대해 최대 2000개의 호스트가 지원됨).
- 사용 중 - 사용 중인 vCenter 연결 또는 호스트 연결 라이선스 수입니다. 호스트 연결에서 이 숫자는 인벤토리로 작성된 호스트(또는 서버) 수를 나타냅니다.
- 사용 가능 - 나중에 사용할 수 있는 vCenter 연결 또는 호스트 연결 라이선스의 수입니다.

호스트 자격 증명 프로파일에 호스트를 추가하는 경우 라이선스가 부여된 호스트 수가 라이선스 수를 초과하면 호스트를 더 추가할 수 없습니다. OMIVV에서는 사용 가능한 호스트 라이선스 수보다 많은 호스트 수를 관리하는 것을 지원하지 않습니다.

라이선스에 대한 자세한 내용을 보려면 OMIVV RESTful API를 사용하십시오. 자세한 내용은 https://www.dell.com/support에서 *OpenManage Integration for VMware API 가이드*를 참조하십시오.

**노트:** 모든 활성 라이선스는 OMIVV 5.x 버전에 사용할 수 있습니다. 이전 OMIVV 인스턴스에서 백업되거나 Digital Locker에서 다시 다운로드한 라이선스는 현재 OMIVV 인스턴스에 사용할 수 있습니다.

## 신뢰성 및 무결성 보호

제품 무결성을 보장하기 위해 OMIVV 설치 및 업데이트 구성 요소가 서명됩니다.

통신 무결성을 보장하기 위해 CA 서명된 인증서를 사용하는 것이 권장됩니다.

# OMIVV에서 백업 및 복원 관리

재해 시나리오에서 OMIVV를 보호하려면 OMIVV의 백업을 수행하는 것이 권장됩니다. 필요한 경우 이러한 백업에서 OMIVV를 복원할 수 있습니다. 백업 및 복원에 대한 자세한 내용은 **https://www.dell.com/support**에서 제공되는 OMIVV 사용자 가이드를 참조하십시오.