OpenManage Integration for VMware vCenter 버전 5.2

사용자 가이드

October 2020
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

1

소개

IT 관리자는 VMware vSphere ESX/ESXi 호스트를 관리하고 모니터링하기 위해 VMware vCenter를 기본 콘솔로 사용합니다. OpenManage Integration for VMware vCenter(OMIVV)는 vSphere 환경에서 Dell EMC 서버 인프라스트럭처의 관리 및 모니터링과 관련된 작업을 간소화함으로써 데이터 센터 관리의 복잡성을 줄입니다.

이 릴리스의 새로운 기능

이 릴리스의 OpenManage Integration for VMware vCenter 5.2에서 제공하는 기능은 다음과 같습니다.

- OMIVV RESTful API 소개

  자세한 내용은 **https://www.dell.com/support/**에서 *OpenManage Integration for VMware vCenter 버전 5.2 API 가이드*를 참조하십시오.
- vSphere 7.0 U1 지원
- XE2420 PowerEdge 서버 지원
- IPv4 범위 기반 운영 체제 미설치 검색 지원
- 보안 향상
- **Dell EMC 섀시** 및 **Dell EMC 호스트** 페이지에서 상태에 따라 호스트 및 섀시를 필터링하는 필터 옵션이 추가되었습니다.
- 다수의 또는 다양한 보증이 있는 호스트의 경우 보증 보고 기능이 향상되었습니다.

OpenManage Integration for VMware vCenter 기능

OpenManage Integration for VMware vCenter(OMIVV) 어플라이언스 기능은 다음과 같습니다.

표 1. OMIVV 기능

기능	설명
인벤토리	인벤토리를 기능은 다음을 제공합니다. 메모리 수량 및 유형, NIC, PSU, 프로세서 및 RAC(Remote Access Controller)와 같은 PowerEdge 서버 세부 정보 서버, 클러스터 및 데이터 센터 수준의 보증 정보 CMC(Chassis Management Controller) 또는 관리 모듈 정보, 섀시 전원 공급 장치, KVM 상태, 팬 또는 열 세부 정보, 보증 정보, 스위치, 서버 및 스토리지 세부 정보와 같은 섀시 세부 정보 MCM(Multi-Chassis Management) 구성에서 MX 섀시 관계에 대한 지원 MX 섀시 MCM 구성에 대한 패브릭 정보 MX 섀시에 대한 QuickSync 하드웨어 정보
알림 모니터링 및 보내기	모니터링 및 알림은 다음 기능을 포함합니다. 주요 하드웨어 결함을 감지하고 가상화 인식 작업 수행 (예: 워크로드 마이그레이션 또는 호스트를 유지 보수 모드로 전환) 인벤토리, 이벤트 및 경보와 같이 서버 및 섀시 문제를 진단하기 위한 지능적인 기능 제공 VMware Proactive HA 기능 지원
펌웨어 업데이트	클러스터 인식 서버 펌웨어 업데이트에는 다음이 포함됩니다.

표 1. OMIVV 기능 (계속)

기능	설명
	지원되는 서버를 최신 버전의 BIOS 및 펌웨어로 업데이트 OMIVV 및 vSphere LifeCycle Manager를 사용하여 펌웨어 업데이트를 수행할 수도 있습니다(vCenter 7.0 이상에 해당).
클러스터에 대한 변경 사항 감지	클러스터에 대한 펌웨어 규정 준수 vSAN 클러스터에 대한 드라이버 규정 준수 하드웨어 규정 준수 **노트:** 섀시 자격 증명 프로필을 사용하여 관리하는 호스트에는 하드웨어 규정 준수가 지원되지 않습니다.
드라이버 업데이트	vSAN 클러스터에 대한 드라이버 업데이트.
배포	배포에는 다음이 포함됩니다. 시스템 프로필 생성 및 배포 PXE를 사용하지 않고 VMware vCenter를 사용하여 운영 체제를 운영 체제 미설치 서버에 원격으로 배포
서비스 정보	Dell의 보증 데이터베이스에서 Dell EMC 서버 및 관련 섀시에 대한 보증 정보를 검색하고 간편한 온라인 보증 업그레이드 가능.
보안 역할 및 권한	보안 역할 및 권한에는 다음 기능이 포함됩니다. 표준 vCenter 인증, 규칙 및 권한과 통합 iDRAC9 기반 서버에서 iDRAC 잠금 모드를 지원합니다. iDRAC9 기반 서버 목록은 호환성 매트릭스를 참조하십시오.
OEM Server 지원	다음과 같은 OMIVV 기능이 지원됩니다. 인벤토리 알림 모니터링 및 보내기 펌웨어 업데이트 배포 서비스 정보 보안 역할 및 권한
MX 섀시 펌웨어 업데이트	MX 섀시에 대한 관리 모듈 펌웨어를 업데이트하는 옵션 제공

노트: OMIVV 5.0 이상부터는 VMware vSphere Client(HTML-5)만 지원되며 vSphere Web Client(FLEX)는 지원되지 않습니다.

2

Dell EMC OMIVV 관리 콘솔 로그인

아래에 나오는 두 관리 포털 중 하나를 사용하여 OpenManage Integration for VMware vCenter 및 해당 가상 환경을 관리할 수 있습니다.

- 웹 기반 Administration Console
- 개별 서버에 대한 콘솔 보기(OMIVV 어플라이언스의 가상 시스템 콘솔)

1. https://<ApplianceIP/hostname/>으로 이동합니다.
   계정 잠금 기간은 1분입니다.
   계정이 잠겨 있으면 새 세션을 시작할 수 없습니다. 하지만 이전 활성 세션이 활성화됩니다.
2. 암호를 입력합니다.
   잘못된 암호를 입력하면 로그인 시도에 실패합니다. 6회 연속 로그인에 실패할 경우 계정이 잠깁니다. 6회 연속 로그인 실패에는 관리 콘솔 또는 REST API에서 실패한 로그인 시도 또는 REST API 액세스를 위한 잘못된 토큰 사용이 포함됩니다.
   계정 잠금 기간은 1분입니다.
   계정 잠금 기간 중에는 세션을 생성할 수 없지만 현재 활성 세션은 활성 상태로 유지됩니다.
   처음 로그인하는 경우 EULA에 동의하라는 메시지가 표시됩니다.
3. **Dell EMC 최종 사용자 라이선스 계약** 페이지에서 사용 약관을 읽은 다음 **라이선스 계약 약관에 동의함** 확인란을 선택합니다.
   텔레메트리 EULA에 대한 자세한 내용을 보려면 **DELL EMC 텔레메트리 EULA**를 클릭합니다.
4. **동의**를 클릭합니다.

새 vCenter Server 등록

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

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 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.

1. https://<ApplianceIP/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.

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.

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: 맞춤 구성 CA(Certificate Authority) 서명된 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 vCenter에서 어플라이언스를 등록 취소한 후 다시 등록합니다.

관리자가 아닌 계정을 사용하여 vCenter 서버 등록

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

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

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.

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

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

기존 역할을 편집하여 Dell 권한을 할당할 수 있습니다.

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 서버를 선택합니다.
4. **역할** 목록에서 **Dell-Operational**을 선택한 후 **권한**을 클릭합니다.
5. Dell 권한을 할당하려면 편집 아이�on [ ]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 보안 역할 및 사용 권한()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.

등록된 vCenter Server의 인증서 업데이트

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

OMIVV로 생성된 CSR은 신뢰할 수 있는 인증 기관에서 디지털 방식으로 서명된 인증서를 받습니다. OMIVV는 보안 통신을 위해 웹 서버에서 디지털 인증서를 사용하여 HTTPS를 활성화합니다.

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

1. https://<ApplianceIP/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.

vCenter 로그인 자격 증명 수정

관리자 권한이 있거나, 관리자가 아닌 사용자라도 필요한 권한이 있으면 vCenter 로그인 자격 증명을 수정할 수 있습니다.

클러스터에 Proactive HA 기능이 활성화된 경우 이와 연결된 사용자를 변경해서는 안 됩니다. 다른 vCenter 사용자를 사용하여 등록을 수정하면 Proactive HA 기능이 중단됩니다. 자격 증명에 수정이 필요하면 기존 자격 증명의 등록을 취소하고 새 자격 증명을 사용하여 등록합니다.

1. https://<ApplianceIP/hostname/>으로 이동합니다.
2. **로그인** 대화 상자에 암호를 입력하고 **로그인**을 클릭합니다.
3. 왼쪽 창에서 **VCENTER 등록**을 클릭합니다.
   등록된 vCenter Server가 작업 창에 표시됩니다.
4. **MODIFY USER ACCT** 창을 열려면 **자격 증명** 아래에서 등록된 vCenter에 대하여 **수정**을 클릭합니다.
5. 잘못된 자격 증명을 입력하면 메시지가 표시됩니다. 올바른 vCenter 사용자 이름, 암호를 입력하고 암호를 재입력하여 확인합니다.
6. 암호를 변경하려면 **적용**을 클릭합니다. 업데이트를 취소하려면 **취소**를 클릭합니다.

OpenManage Integration for VMware vCenter 등록 취소

인벤토리, 보증 또는 배포 작업이 실행 중일 때 vCenter Server에서 OMIVV를 등록 취소하지 마십시오.

클러스터에 Proactive HA를 활성화한 경우, Proactive HA가 클러스터에서 비활성화되었는지 확인합니다. Proactive HA가 비활성화된 경우 **구성** > **서비스** > **vSphere 가용성** 을 선택하여 클러스터의 **Proactive HA 오류 및 응답** 화면에 액세스한 후 **편집**을 클릭합니다. Proactive HA를 비활성화하려면 **Proactive HA 오류 및 응답** 화면에서 **Dell Inc** 공급자의 확인란을 선택 취소합니다.

OpenManage Integration for VMware vCenter를 제거하려면 관리 콘솔을 사용하여 vCenter Server에서 OMIVV 등록을 취소합니다.

1. https://<ApplianceIP/hostname/>으로 이동합니다.
2. **VCENTER 등록** 페이지의 **vCenter Server IP 또는 호스트 이름** 표에서 **등록 취소**를 클릭합니다.

   노트: OMIVV는 둘 이상의 vCenter와 연결될 수 있으므로 올바른 vCenter를 선택해야 합니다.

3. 선택한 vCenter Server의 등록 취소를 확인하려면 **VCENTER 등록 취소** 대화 상자에서 **등록 취소**를 클릭합니다.

   노트: OMIVV를 등록 취소한 후 vSphere Client(HTML-5)에서 로그아웃하고 로그인합니다. OMIVV 아이콘이 계속 표시되면 vSphere Client(HTML-5)와 Web Client(FLEX) 모두에 대한 Client Services를 다시 시작합니다.

OMIVV 관리 콘솔에 라이선스 업로드

https://www.dell.com/support의 Dell Digital Locker에서 라이선스를 다운로드할 준비가 되었는지 확인합니다. 라이선스를 두 개 이상 주문한 경우, 각자 다른 시간에 따로 제공될 수 있습니다. **https://www.dell.com/support**에서 다른 라이선스 항목의 주문 상태를 확인할 수 있습니다. 라이선스 파일은 .XML 형식으로 제공됩니다.

1. https://<ApplianceIP/hostname/>으로 이동합니다.
2. **로그인** 대화 상자에 암호를 입력합니다.
3. 왼쪽 창에서 **VCENTER 등록**을 클릭합니다.
   등록된 vCenter Server가 작업 창에 표시됩니다.
4. **라이선스 업로드**를 클릭합니다.
5. **라이선스 업로드** 대화 상자에서 **찾아보기**를 클릭하여 라이선스 파일로 이동한 후 **업로드**를 클릭합니다.

   노트: 라이선스 파일을 수정하거나 편집하면 라이선스 파일(.XML 파일)을 사용할 수 없습니다. Dell Digital Locker에서 .XML 파일(라이선스 키)을 다운로드할 수 있습니다. 라이선스 키가 다운로드되지 않는 경우 **https://www.dell.com/support**에서 기술 지원 부서에 문의로 이동하여 해당 제품의 지역 Dell 지원 부서 전화 번호를 찾아 Dell 지원 부서에 문의합니다.

OMIVV 어플라이언스 관리

OMIVV 어플라이언스 관리를 사용하면 OpenManage Integration for VMware vCenter 네트워크, NTP 및 HTTPS 정보를 관리할 수 있고 관리자는 다음과 같은 작업을 수행할 수 있습니다.

- OMIVV 어플라이언스 재시작. OMIVV 어플라이언스 재시작 페이지 16을(를) 참조하십시오.
- OMIVV 어플라이언스 업데이트 및 업데이트 리포지토리 위치 구성. 자세한 내용은 OMIVV 어플라이언스 및 리포지토리 위치 업그레이드 페이지 16
- RPM을 사용하여 OMIVV 어플라이언스 업그레이드. RPM을 사용하여 OMIVV 어플라이언스 업그레이드(인터넷 사용) 페이지 17을(를) 참조하십시오.
- 백업 및 복원을 사용하여 OMIVV 어플라이언스 업그레이드. 백업 및 복원을 사용하여 OMIVV 어플라이언스 업그레이드 페이지 18을(를) 참조하십시오.
- 문제 해결 번들 생성 및 다운로드. 문제 해결 번들 생성 및 다운로드 페이지 21을(를) 참조하십시오.
- HTTP 프록시 설정. HTTP 프록시 설정 페이지 21을(를) 참조하십시오.
- Network Time Protocol 서버 설정. NTP(Network Time Protocol) 서버 설정 페이지 21을(를) 참조하십시오.
- 배포 모드 구성. 배포 모드 구성 페이지 21을(를) 참조하십시오.
- 확장된 모니터링. 확장된 모니터링 페이지 22을 참조하십시오.
- CSR(Certificate Signing Request) 생성. 인증서 서명 요청(CSR) 생성 페이지 22을(를) 참조하십시오.
- HTTPS 인증서 업로드. HTTPS 인증서 업로드 페이지 23을(를) 참조하십시오.
- 전역 알림 설정. 전역 알림 설정 페이지 23을(를) 참조하십시오.

어플라이언스 관리에 액세스

OpenManage Integration for VMware vCenter에서 관리 포털을 통해 **어플라이언스 관리** 페이지에 액세스하려면 다음 단계를 수행합니다.

1. https://<ApplianceIP/hostname/>으로 이동합니다.
2. **로그인** 대화 상자에 암호를 입력합니다.
3. 어플라이언스 관리 섹션을 구성하려면 왼쪽 창에서 **어플라이언스 관리**를 클릭합니다.

OMIVV 어플라이언스 재시작

1. **어플라이언스 관리** 페이지에서 **가상 어플라이언스 재시작**을 클릭합니다.
2. OMIVV 어플라이언스를 재시작하려면 **가상 어플라이언스 재시작** 대화 상자에서 **적용**을 클릭합니다.

OMIVV 어플라이언스 및 리포지토리 위치 업그레이드

- 모든 데이터를 보호하려면 OMIVV 어플라이언스 업데이트 이전에 OMIVV 데이터베이스의 백업을 수행합니다. 백업 및 복원 관리 페이지 19을(를) 참조하십시오.

- 사용할 수 있는 업그레이드 메커니즘을 표시하고 RPM 업그레이드를 수행하려면 OMIVV 어플라이언스에 인터넷 연결이 필요합니다. OMIVV 어플라이언스가 인터넷에 연결되었는지 확인합니다. 환경 네트워크 설정에 따라 프록시 네트워크가 필요한 경우 프록시 설정을 활성화하고 프록시 데이터를 입력합니다. (HTTP 프록시 설정)을 참조하십시오.
- **업데이트 리포지토리 경로**가 유효한지 확인합니다.
- 등록된 vCenter 서버에 대한 모든 vSphere Client(HTML-5) 세션에서 로그아웃해야 합니다.
- 등록된 vCenter 서버에 로그인하기 전에 동일한 플랫폼 서비스 컨트롤러(PSC)에서 모든 어플라이언스를 동시에 업데이트해야 합니다. 그렇지 않으면 OMIVV 인스턴스에서 일관성 없는 정보가 표시될 수 있습니다.

1. **어플라이언스 관리** 페이지의 **어플라이언스 업데이트** 섹션에서 현재 및 사용 가능한 OMIVV 버전을 확인합니다.

   사용 가능한 OMIVV 어플라이언스 버전의 경우 적용 가능한 RPM 및 OVF OMIVV 어플라이언스 업그레이드 메커니즘이 눈금 표시 [✔]와 함께 표시됩니다.

   다음은 사용할 수 있는 업그레이드 메커니즘 옵션이며 업그레이드 메커니즘에 대한 작업 중 하나를 수행할 수 있습니다.

옵션	설명
1	RPM에 틱 기호가 있는 경우, 기존 버전에서 사용 가능한 최신 버전으로 RPM을 업그레이드할 수 있습니다. RPM을 사용하여 OMIVV 어플라이언스 업그레이드(인터넷 사용) 페이지 17을(를) 참조하십시오.
2	OVF에 틱 기호가 있는 경우, 기존 버전에서 OMIVV 데이터베이스를 백업한 다음 사용 가능한 최신 어플라이언스 버전에서 복원할 수 있습니다. 백업 및 복원을 사용하여 OMIVV 어플라이언스 업그레이드 페이지 18을(를) 참조하십시오.
3	RPM 및 OVF 모두에 틱 기호가 있는 경우, 언급된 옵션 중 하나를 수행하여 어플라이언스를 업그레이드할 수 있습니다. 이 시나리오에서 권장되는 옵션은 RPM 업그레이드입니다.

2. OMIVV 어플라이언스를 업데이트하려면 OMIVV 버전에서 업그레이드 메커니즘(해당하는 경우)에 언급한 작업을 수행합니다.

OMIVV 업그레이드 옵션

백업 및 복원

OMIVV 5.0에서 최신 버전으로 백업 및 복원을 수행할 수 있습니다(vCenter 6.5 이상).

RPM 업그레이드

OMIVV 5.0에서 최신 버전으로 RPM 업그레이드를 수행할 수 있습니다.

RPM을 사용하여 OMIVV 어플라이언스 업그레이드(인터넷 사용)

현재 버전보다 높은 버전의 어플라이언스로 업그레이드하고 있는지 확인합니다.

OMIVV 어플라이언스를 업그레이드하기 전에 어플라이언스 스냅샷을 생성하는 것이 좋습니다.

1. **어플라이언스 관리** 페이지에서 네트워크 설정에 따라 프록시를 활성화하고 필요한 경우 프록시 설정 데이터를 입력합니다. HTTP 프록시 설정을 참조하십시오.

   사용 가능한 OMIVV 어플라이언스 버전의 경우 적용 가능한 RPM 및 OVF OMIVV 어플라이언스 업그레이드 메커니즘이 눈금 표시 [✔]와 함께 표시됩니다.

2. OMIVV 플러그인을 기존 버전에서 사용 가능한 버전으로 업그레이드하려면 다음 단계 중 하나를 수행합니다.
   - **업데이트 리포지토리 경로**에서 사용할 수 있는 RPM을 사용하여 업그레이드하려면 **업데이트 리포지토리 경로**가 다음 경로로 설정되어 있는지 확인합니다. https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/

   경로가 다른 경우, **어플라이언스 관리** 창의 **어플라이언스 업데이트** 영역에서 **편집**을 클릭하여 경로를 **업데이트 리포지토리 경로** 텍스트 상자의 https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/(으)로 업데이트하고 **적용**을 클릭합니다.

3. 사용 가능한 OMIVV 어플라이언스 버전과 현재 OMIVV 어플라이언스 버전을 비교합니다.
4. 업데이트를 OMIVV 어플라이언스에 적용하려면 **어플라이언스 설정** 아래에서 **가상 어플라이언스 업데이트**를 클릭합니다.
5. **어플라이언스 업데이트** 대화 상자에서 **업데이트**를 클릭합니다.
   업데이트를 클릭하면 **관리 콘솔** 창에서 로그아웃됩니다.

6. 웹 브라우저를 닫습니다.

   업그레이드 프로세스 중에 어플라이언스가 한 번 또는 두 번 다시 시작됩니다. 어플라이언스가 RPM으로 업그레이드되면 Dell 관리 포털에 로그인하기 전에 브라우저 캐시를 지워야 합니다.

   RPM 업그레이드가 완료되면 OMIVV 콘솔에서 로그인 화면을 볼 수 있습니다. 브라우저를 열어 *https:\\<ApplianceIP|hostname>* 링크를 입력하고 **어플라이언스 업데이트** 영역으로 이동합니다. 이용 가능한 어플라이언스 버전과 현재 OMIVV 어플라이언스 버전이 동일한지 확인할 수 있습니다.

   등록된 Dell 알람 및 PHA 클러스터용 Dell 상태 업데이트 공급자에서 수행되는 모든 맞춤 구성은 RPM 업그레이드 후 기본값으로 복원됩니다.

RPM을 사용하여 OMIVV 어플라이언스 업그레이드(인터넷 없음)

HTTP 또는 HTTPS 공유를 생성합니다. HTTP 또는 HTTPS 공유가 ++와 같은 특수 문자나 공백이 포함된 파일 이름을 지원하는지 확인합니다.

OMIVV는 HTTP 및 HTTPS 공유만 지원합니다.

OMIVV는 인터넷에 연결하지 않고 버전 5.1에서 5.2로 업그레이드를 지원합니다.

1. **https://www.dell.com/support**에서 RPM .zip 패키지를 다운로드합니다.
2. RPM .zip 패키지의 압축을 풀고 압축을 푼 위치에서 HTTP 또는 HTTPS 공유로 파일과 폴더를 복사합니다.
3. **어플라이언스 관리** 페이지의 **어플라이언스 업데이트** 영역에서 **편집**을 클릭한 다음 **리포지토리 경로 업데이트**에 공유 위치 경로를 입력합니다.
4. **적용**을 클릭합니다.
5. 사용 가능한 OMIVV 어플라이언스 버전과 현재 OMIVV 어플라이언스 버전을 비교합니다.
6. 업데이트를 OMIVV 어플라이언스에 적용하려면 **어플라이언스 설정** 아래에서 **가상 어플라이언스 업데이트**를 클릭합니다.
7. **어플라이언스 업데이트** 대화 상자에서 **업데이트**를 클릭합니다.
   업데이트를 클릭하면 **OMIVV 관리 콘솔** 창에서 로그아웃됩니다.

   네트워크 속도에 따라 업데이트를 완료하는 데 약 40분 정도 걸릴 수 있습니다.
8. 웹 브라우저를 닫습니다.
   어플라이언스 업그레이드가 완료되면 **OMIVV 관리 콘솔**에 로그인하기 전에 브라우저 캐시를 지워야 합니다.

백업 및 복원을 사용하여 OMIVV 어플라이언스 업그레이드

Dell EMC는 백업 후 및 백업 파일 복원 전에 OMIVV에서 관리하는 클러스터 또는 호스트를 변경 또는 제거하지 않는 것이 좋습니다. OMIVV에서 관리하는 클러스터 또는 호스트가 변경 또는 제거된 경우 복원 후에 해당 클러스터 및 호스트와 연결된 프로필(예: 호스트 자격 증명 프로필, 클러스터 프로필)을 재구성합니다.

vCenter에서 OMIVV 플러그인 등록해제를 하지 마십시오. vCenter에서 플러그인을 등록 취소하면 OMIVV 플러그인으로 vCenter에 등록한 Proactive HA 클러스터에 대한 Dell 상태 업데이트 공급자가 제거됩니다.

OMIVV 어플라이언스를 업그레이드하기 전에 어플라이언스 스냅샷을 생성하는 것이 좋습니다.

OMIVV 어플라이언스를 이전 버전에서 최신 버전으로 업데이트하려면 다음 단계를 수행합니다.

1. 이전 릴리스의 데이터를 백업합니다.
2. vCenter에서 이전 OMIVV 어플라이언스를 끕니다.
3. 새 OpenManage Integration 어플라이언스 OVF를 배포합니다.
4. OpenManage Integration 신규 어플라이언스의 전원을 켭니다.
5. 새 어플라이언스에 대한 네트워크 및 시간대를 설정합니다.

   노트: 새 OMIVV 어플라이언스에 대한 이전 OMIVV 어플라이언스의 ID(IP 또는 FQDN)를 유지하는 것이 좋습니다.

6. OMIVV 어플라이언스는 기본 인증서와 함께 제공됩니다. 어플라이언스에 대한 사용자 정의 인증서를 사용하려면 동일 항목을 업데이트합니다. 인증서 서명 요청(CSR) 생성 페이지 22 및 HTTPS 인증서 업로드 페이지 23의 내용을 참조하십시오. 그렇지 않으면 이 단계를 건너뜁니다.
7. 데이터베이스를 새 OMIVV 어플라이언스에 복원합니다. 백업에서 OMIVV 데이터베이스 복원을 참조하십시오.
8. 어플라이언스를 확인합니다. 자세한 내용은 을(를) 참조하십시오. 설치 가이드의 설치 항목 확인
9. 업그레이드 후 OMIVV 플러그인이 관리하는 모든 호스트에서 인벤토리를 다시 실행하는 것이 좋습니다.

   이벤트 및 알람 설정은 어플라이언스 복원 후 활성화되지 않습니다. **설정** 탭에서 이벤트 및 알람 설정을 다시 활성화할 수 있습니다.

이전 버전의 OMIVV에서 사용 가능한 버전으로 업그레이드하는 경우 예약된 모든 작업이 계속 실행됩니다.

등록된 Dell 알람 및 PHA 클러스터용 Dell 상태 업데이트 공급자에서 수행되는 모든 맞춤 구성은 백업 및 복원을 수행한 후 기본값으로 복원됩니다.

이전 OMIVV 버전에서 이후 OMIVV 버전으로 백업 및 복원한 후 다음 문제가 발생할 경우 다음 작업을 수행합니다.

- 200,000개의 메시지
- Dell EMC 로고 누락
- OMIVV UI가 응답하지 않음
- OMIVV 플러그인은 vCenter에서 제거되지 않음
- SSL 인증서가 유효하지 않음

해상도:

- vCenter Server에서 vSphere Client(HTML-5) 및 vSphere Web Client(FLEX) 모두에 대한 vSphere Client Services를 다시 시작합니다.
- 문제가 지속되면, 다음과 같이 하십시오.
  - VMware vCenter Server 어플라이언스의 경우 `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity`로 이동합니다. Windows vCenter의 경우 vCenter 어플라이언스의 다음 폴더로 이동하여 이전 버전에 해당하는 이전 데이터가 있는지 확인합니다. vCenter 어플라이언스에 `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity` 폴더가 있는지 확인하고 com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX 같은 이전 데이터가 있는지 확인합니다.
  - 이전 OMIVV 버전에 해당하는 폴더를 수동으로 삭제하고 vSphere Client(HTML-5) 및 Web Client(FLEX) 모두에 대한 vSphere Client Services를 다시 시작합니다.

새 어플라이언스의 IP 주소가 이전 어플라이언스의 IP 주소와 다를 경우 다음을 수행합니다.

- Proactive HA 기능이 제대로 작동하지 않을 수 있습니다. 이러한 시나리오에서는 Dell EMC 호스트가 있는 각 클러스터에 대해 Proactive HA를 비활성화하고 활성화합니다.
- SNMP 트랩의 트랩 대상이 새 어플라이언스를 가리키도록 구성합니다. 해당 호스트에서 인벤토리를 실행하면 ID 변경이 고정됩니다. 호스트에서 인벤토리를 실행하는 동안 SNMP 트랩이 새 IP를 가리키지 못하면 이러한 호스트는 비준수로 나열됩니다. 호스트 규정 준수 문제를 해결하려면 의 비준수 호스트 해결 페이지 64을 참조하십시오.

백업 및 복원 관리

관리 콘솔을 사용하여 백업 및 복원 관련 작업을 수행할 수 있습니다.

- 백업 및 복원 구성
- 자동 백업 예약
- 즉시 백업 수행
- 백업에서 데이터베이스 복원
- 백업 및 복원 설정 재설정 페이지 20

OMIVV에서 관리 콘솔을 사용하여 **백업 및 복원 설정** 페이지에 액세스하려면 다음 단계를 수행합니다.

1. `https:\\<ApplianceIP|hostname>`으로 이동합니다.
2. **로그인** 대화 상자에 암호를 입력합니다.
3. 왼쪽 창에서 **백업 및 복원**을 클릭합니다.

백업 및 복원 구성

백업 및 복원 기능은 OMIVV 데이터베이스를 나중에 복원할 수 있는 원격 위치(NFS 및 CIFS)에 백업합니다. 백업에는 프로필, 구성 및 호스트 정보가 포함됩니다. 데이터 손실을 방지하려면 자동 백업을 예약하는 것이 좋습니다.

노트: NTP 설정은 저장 및 복원되지 않습니다.

1. **백업 및 복원 설정** 페이지에서 **편집**을 클릭합니다.
2. 강조 표시된 **설정 및 세부 정보** 영역에서 다음을 수행합니다.
   a. **백업 위치**에 백업 파일 경로를 입력합니다.
   b. **사용자 이름**에 사용자 이름을 입력합니다.
   c. **암호**에 암호를 입력합니다.

d. **백업 암호화에 사용되는 암호 입력** 상자에 암호화된 암호를 입력합니다.
   암호화 암호에는 영숫자와 "!, @, #, $, %, *" 등의 특수 문자를 사용할 수 있습니다.
e. **암호 확인**에 암호화된 암호를 다시 입력합니다.

3. 설정을 저장하려면 **적용**을 클릭합니다.
4. 백업 일정을 구성합니다. 자동 백업 예약을 참조하십시오.

이 절차를 마친 후에는 백업 일정을 구성합니다.

자동 백업 예약

백업 위치 및 자격 증명 구성에 대한 자세한 내용은 백업 및 복원 구성을 참조하십시오.

1. **백업 및 복원 설정** 페이지에서 **자동 예약된 백업 편집**을 클릭합니다.
   관련 필드가 활성화됩니다.
2. 백업을 활성화하려면 **활성화됨**을 클릭합니다.
3. 백업 작업을 실행할 요일의 **백업 날짜** 확인란을 선택합니다.
4. **백업 시간(24시간, HH:mm)**에서 HH: mm 형식으로 시간을 입력합니다.
   다음에 예약된 백업의 날짜와 시간으로 **다음 백업**이 채워집니다.
5. **적용**을 클릭합니다.

즉시 백업 수행

1. **백업 및 복원 설정** 페이지에서 **지금 백업**을 클릭합니다.
2. 백업 설정에서 위치 및 암호화 암호를 사용하려면 **지금 백업** 대화 상자에서 **백업 설정에서 위치 및 암호화 암호를 사용** 확인란을 선택합니다.
3. **백업 위치**, **사용자 이름**, **암호** 및 **암호화 암호** 값을 입력합니다.
   암호화 암호에는 영숫자와 "!, @, #, $, %, *" 등의 특수 문자를 사용할 수 있습니다. 암호를 구성할 때 문자 수 제한은 없습니다.
4. **백업**을 클릭합니다.

백업에서 OMIVV 데이터베이스 복원

이전 버전에서 OMIVV를 복원한 후 다음을 수행합니다.

- 11G 서버는 지원되지 않습니다. 12G 이상 서버만 복원 후 유지됩니다.
- 하드웨어 프로필 및 배포 템플릿은 지원되지 않습니다. 시스템 프로필을 배포에 사용하는 것이 좋습니다.
- 11G 서버에서 예약되거나 하드웨어 프로필 기반 배포 템플릿을 사용하는 배포 작업은 취소됩니다.
- 모든 11G 서버는 자격 증명 프로필에서 제거되며 소비된 라이선스는 해제됩니다.
- 리포지토리 프로필은 64비트 번들만 사용합니다.

  노트: 4.x에서 5.x로 백업 및 복원을 수행하는 경우 OMIVV에서 5.x의 32비트 펌웨어 번들을 지원하지 않기 때문에 클러스터 프로필 이름에 경고 기호가 표시됩니다. 클러스터 프로필에 대한 최신 변경 사항을 사용하려면 클러스터 프로필을 편집합니다.
- 11G 서버에서 예약된 펌웨어 업데이트 작업은 취소됩니다.

복원 작업을 수행하기 전에 올바른 배포 모드가 구성되어 있는지 확인합니다. 배포 모드 구성에 대한 자세한 내용은 배포 모드 구성 페이지 21을(를) 참조하십시오.

1. **백업 및 복원 설정** 페이지에서 **지금 복원**을 클릭합니다.
2. **지금 복원** 대화 상자의 **파일 위치**에 CIFS 또는 NFS 형식의 백업 .gz 파일에 대한 경로를 입력합니다.
3. 백업 파일의 **사용자 이름**, **암호** 및 **암호화 암호**를 입력합니다.
   암호화 암호에는 영숫자와 "!, @, #, $, %, *" 등의 특수 문자를 사용할 수 있습니다.
4. 변경사항을 저장하려면 **적용**을 클릭합니다.
   복원 작업이 완료되면 OMIVV 어플라이언스가 재부팅됩니다. 설치를 확인하려면 설치 가이드의 설치 확인 항목을 참조하십시오.

   복원이 완료되면 브라우저를 닫고 브라우저 캐시를 지운 다음 관리 포털에 로그인합니다.

백업 및 복원 설정 재설정

설정 재설정 기능을 사용하여 설정을 구성되지 않은 상태로 재설정할 수 있습니다.

1. **백업 및 복원 설정** 페이지에서 **설정 재설정**을 클릭합니다.
2. **설정 재설정** 대화 상자에서 **적용**을 클릭합니다.

문제 해결 번들 생성 및 다운로드

문제 해결 번들을 생성하려면 관리 포털에 로그인해야 합니다.

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

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

HTTP 프록시 설정

1. **어플라이언스 관리** 페이지에서 **HTTP 프록시 설정**을 아래로 스크롤한 후 **편집**을 클릭합니다.
2. HTTP 프록시 설정 사용을 활성화하려면 **활성화됨**을 선택합니다.
3. **프록시 서버 주소**에 프록시 서버 주소를 입력합니다.
4. **프록시 서버 포트**에 프록시 서버 포트를 입력합니다.
5. 프록시 자격 증명을 사용하려면 **예**를 선택합니다.
6. 프록시 자격 증명을 사용하는 경우 **사용자 이름**에 사용자 이름을 입력합니다.
7. **암호**에 암호를 입력합니다.
8. **적용**을 클릭합니다.

NTP(Network Time Protocol) 서버 설정

NTP를 사용하여 OMIVV 어플라이언스 시계와 NTP 서버 시계를 동기화할 수 있습니다.

1. 관리 콘솔에서 **어플라이언스 관리** 페이지의 **NTP 설정** 영역에서 **편집**을 클릭합니다.
2. **활성화됨**을 선택합니다. 기본 및 보조 NTP 서버의 호스트 이름 또는 IP 주소를 입력하고 **적용**을 클릭합니다.
3. NTP를 구성한 후 터미널 콘솔을 시작하고 **네트워크에서 날짜 및 시간 동기화** 확인란을 선택합니다.

노트: OMIVV 시계를 NTP 서버와 동기화하는 데 몇 분 정도 걸릴 수 있습니다.

노트: OMIVV 관리 포털에서 정보를 로드하는 데 오랜 시간이 걸리는 경우 NTP 설정이 올바르고 OMIVV 가상 시스템에서 NTP 서버에 연결할 수 있는지 확인합니다.

배포 모드 구성

위에 언급된 배포 모드의 경우 예약을 통해 충분한 양의 메모리 리소스를 OMIVV 어플라이언스에 예약해야 합니다. 메모리 리소스 예약을 위한 단계는 vSphere 설명서를 참조하십시오.

이러한 리소스를 OMIVV가 포함된 VM에 할당하여 필요한 배포 모드에 대한 다음 시스템 요구 사항이 충족되었는지 확인합니다.

표 2. 배포 모드의 시스템 요구 사항

배포 모드	호스트 수	CPU 수	메모리(GB)	최소 저장소
작게	최대 250	2	8	95GB
중간	최대 500	4	16	95GB
크게	최대 1000	8	32	95GB
X 대형 모드	최대 2,000	12	32	95GB

노트: MX 섀시 펌웨어 업데이트 기능은 중형, 대형 및 초대형 배포 모드에서만 지원됩니다.

환경의 노드 수와 일치하도록 OMIVV를 확장하는 적절한 배포 모드를 선택할 수 있습니다.

vROPS(vRealize Operations)용 OpenManage Mangement Pack을 OMIVV와 통합하기 위해 필요한 최소 배포 모드는 **중간**입니다.

1. **어플라이언스 관리** 페이지에서 **배포 모드**까지 아래로 스크롤합니다.
   배포 모드의 구성 값(예: **작게**, **중간**, **크게**, **아주 크게**)이 표시됩니다. 기본적으로 이 모드는 **작게**로 설정됩니다.
2. 환경을 기반으로 배포 모드를 편집하려면 **편집**을 클릭합니다.
3. **편집** 모드에서 필수 구성 요소가 충족되었는지 확인하고 필요한 배포 모드를 선택합니다.
4. **적용**을 클릭합니다.
   설정된 배포 모드에 필요한 CPU 및 메모리 대 할당된 CPU 및 메모리가 확인됩니다.
   - 확인에 실패한 경우 오류 메시지가 표시됩니다.
   - 확인에 성공하면 OMIVV 어플라이언스가 다시 시작되고 변경 확인 후 배포 모드가 변경됩니다.
   - 필요한 배포 모드가 이미 설정된 경우 메시지가 표시됩니다.
5. 배포 모드가 변경되면 변경 사항을 확인한 다음 어플라이언스를 재시작해야 배포 모드를 업데이트할 수 있습니다.

노트: OMIVV 어플라이언스 부팅 중에 설정된 배포 모드에 대해 할당된 시스템 리소스가 확인됩니다. 할당된 시스템 리소스가 설정된 배포 모드보다 적은 경우 OMIVV 어플라이언스가 로그인 페이지로 부팅되지 않습니다. OMIVV 어플라이언스를 부팅하려면 OMIVV 어플라이언스를 종료하고 시스템 리소스를 기존에 설정된 배포 모드로 업데이트한 다음 OMIVV 어플라이언스를 켭니다.

배포 모드 다운그레이드

1. 관리 콘솔에 로그인합니다.
2. 배포 모드를 필요한 수준으로 변경합니다.
3. OMIVV 어플라이언스를 종료하고 시스템 리소스를 필요한 수준으로 변경합니다.
4. OMIVV 어플라이언스의 전원을 켭니다.

배포 모드 업그레이드

1. Dell 관리자 포털에 로그인하기 전에 브라우저 캐시를 지웁니다.
2. OMIVV 어플라이언스의 전원을 켭니다.
3. 관리 콘솔에 로그인합니다.
4. 배포 모드를 필요한 수준으로 변경합니다.

확장된 모니터링

OpenManage Management Pack for vRealize Operations Manager를 지원하도록 확장된 모니터링을 활성화해야 합니다. '중간' 배포 모드를 통해 확장된 모니터링을 수행하는 것이 좋습니다.

OpenManage Management Pack for vRealize Operations Manager에 대한 SNMP 경고를 지원하도록 SNMP 트랩 모니터링을 활성화해야 합니다. 이를 통해 사용자는 서버 또는 섀시의 상태를 실시간으로 모니터링할 수 있습니다.

1. https://<ApplianceIP/hostname/>으로 이동합니다.
2. 왼쪽 창에서 **어플라이언스 관리**를 클릭합니다.
3. **어플라이언스 관리** 페이지에서 **확장된 모니터링**까지 아래로 스크롤합니다.
4. 확장된 모니터링 설정을 편집하려면 **편집**을 클릭합니다.
5. 편집 모드에서 확장 모니터링 및 SNMP 트랩 모니터링을 활성화 또는 비활성화한 다음 **적용**을 클릭합니다.

인증서 서명 요청(CSR) 생성

vCenter에 OMIVV를 등록하기 전에 CSR을 업로드해야 합니다.

새 인증서 서명 요청(CSR)을 생성하면 이전에 생성한 CSR로 만든 인증서가 어플라이언스에 업로드되지 않습니다. CSR을 생성하려면 다음을 수행합니다.

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 공통 이름, 조직, 지역, 구/군/시, 주, 국가 및 이메일 주소 정보를 입력합니다. **계속**을 클릭합니다.
3. **다운로드**를 클릭하고 결과로 생성되는 CSR을 액세스 가능한 위치에 저장합니다.

HTTPS 인증서 업로드

인증서는 PEM 형식을 사용해야 합니다.

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.

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.

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

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

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.

전역 알림 설정

알림 관리를 통해 관리자가 모든 vCenter 인스턴스에 대해 알림이 OMIVV에 저장되는 방법에 대한 전역 설정을 구성할 수 있습니다.

1. https://<ApplianceIP/hostname/>으로 이동합니다.
2. **로그인** 대화 상자에 암호를 입력합니다.
3. 왼쪽 창에서 **알림 관리**를 클릭합니다. 새 vCenter 알림 설정을 입력하려면 **편집**을 클릭합니다.
4. 다음 필드에 숫자 값을 입력합니다.
   기본적으로 현재 알림 수의 개수가 표시됩니다.
   - **최대 알림 수**
   - **알림 보관 일 수**
   - **중복 알림 시간 제한(초)**
5. 설정을 저장하려면 **적용**을 클릭합니다.

OMIVV VM 콘솔 정보

OMIVV VM 콘솔은 VM의 vSphere Client 내에서 사용할 수 있습니다. 콘솔은 관리 콘솔과 밀접하게 작동합니다. 콘솔을 사용하여 다음 작업을 수행할 수 있습니다.

- 네트워크 설정 구성
- OMIVV 어플라이언스 암호 변경
- NTP 구성 및 로컬 시간대 설정
- OMIVV 어플라이언스 재부팅
- OMIVV 어플라이언스를 출하 시 설정으로 재설정
- 읽기 전용 역할을 사용하여 로그인
- 콘솔에서 로그아웃

OMIVV VM 콘솔 열기

OMIVV VM 콘솔을 열려면 OMIVV 어플라이언스의 웹 또는 원격 콘솔을 실행합니다.

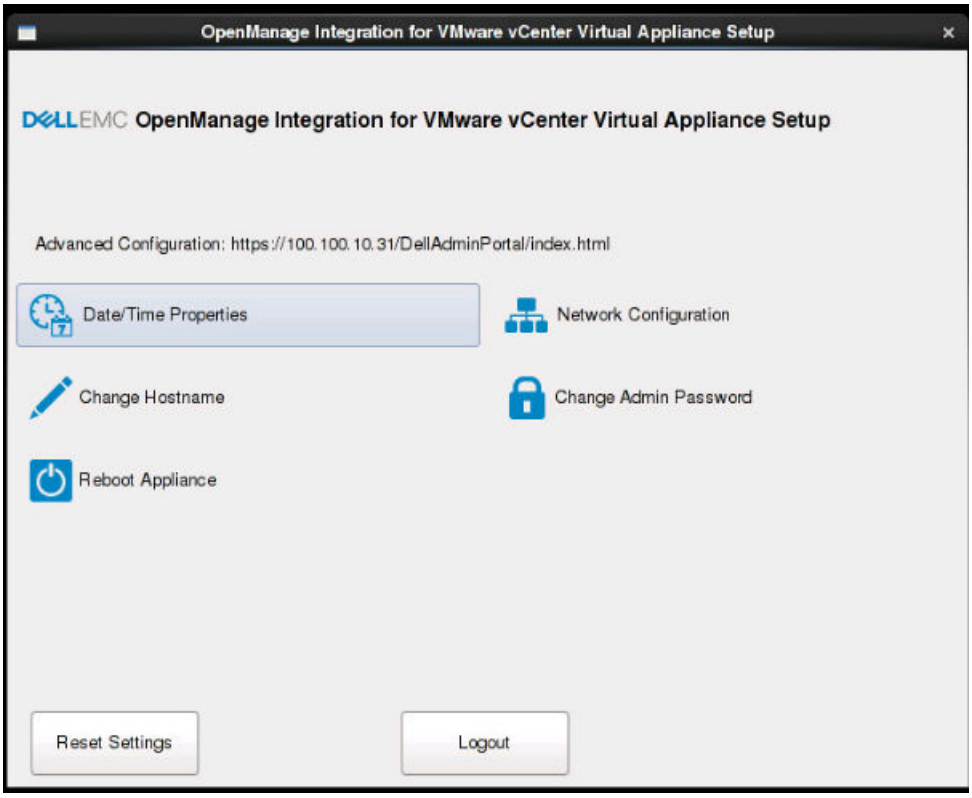
VM 콘솔을 열고 자격 증명(사용자 이름: `admin` 및 암호: 어플라이언스를 배포하는 동안 설정한 암호)을 제공하면 콘솔을 구성할 수 있습니다.

OMIVV 어플라이언스 구성

1. VM의 전원을 켭니다.
2. 오른쪽 창에서 **웹 콘솔 시작**을 클릭합니다.
3. 관리자로 로그인합니다(기본 사용자 이름은 `admin`입니다).
4. 처음 로그인하는 경우 화면의 지침에 따라 암호를 설정합니다(Admin 및 ReadOnly 사용자).

   노트: 관리자 암호를 잊어버린 경우 OpenManage Integration for VMware vCenter 어플라이언스에서 복구할 수 없습니다.

5. OMIVV 시간대 정보를 구성하려면 **날짜/시간 속성**을 클릭합니다.



   노트: OMIVV 어플라이언스가 네트워크(DHCP)에서 IP 주소를 검색할 수 없는 경우 IP 주소가 `0.0.0.0`으로 표시됩니다. 이 문제를 해결하려면 정적 IP를 수동으로 구성해야 합니다.

   a. **날짜 및 시간** 탭에서 **네트워크에서 날짜 및 시간 동기화** 확인란을 선택합니다. **네트워크에서 날짜 및 시간 동기화** 확인란은 관리 포털을 사용하여 NTP를 구성해야 활성화됩니다. NTP 구성에 대한 자세한 내용은 NTP(Network Time Protocol) 서버 설정 페이지 21을(를) 참조하십시오.
   b. **시간대**를 클릭하고 해당 시간대를 선택한 다음 **확인**을 클릭합니다.

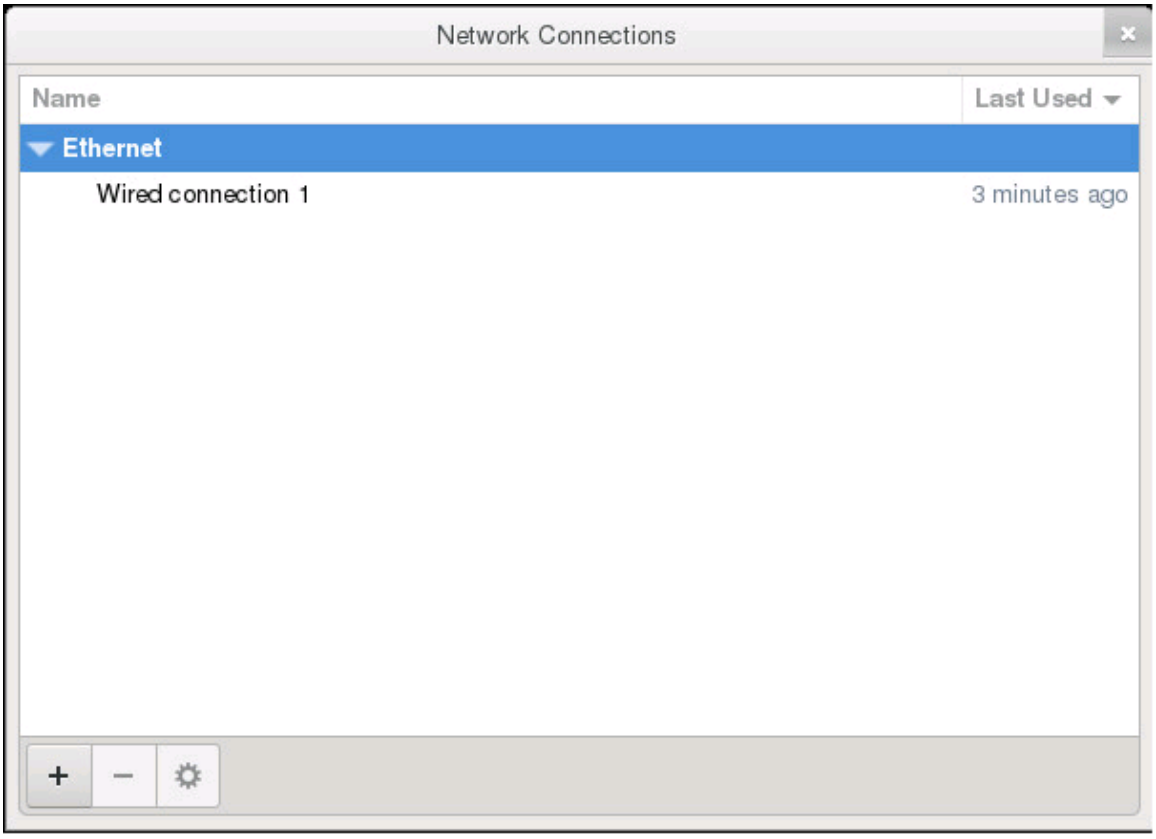
6. OMIVV 어플라이언스의 네트워크를 구성하려면 **네트워크 구성**을 클릭합니다.

   vSphere 환경에서 Dell EMC 서버를 관리하려면 OMIVV에서 vSphere 네트워크(vCenter 및 ESXi 관리 네트워크)와 아웃오브밴드 네트워크(iDRAC, CMC 및 OME-Modular) 모두에 액세스해야 합니다.

   vSphere 네트워크와 아웃오브밴드 네트워크가 사용자 환경에서 별도의 분리된 네트워크로 유지되는 경우 OMIVV는 두 개의 네트워크에 액세스해야 합니다. 이 경우 OMIVV 어플라이언스는 두 개의 네트워크 어댑터로 구성되어야 합니다. 초기 구성의 일부로 두 네트워크를 모두 구성하는 것이 좋습니다.

   vSphere 네트워크를 사용하여 아웃오브밴드 네트워크에 액세스할 수 있는 경우 OMIVV 어플라이언스에 대해 2개의 네트워크 어댑터를 구성하지 마십시오. 두 번째 NIC 구성에 대한 자세한 내용은 2개의 NIC(Network Interface Controller)를 사용하여 OMIVV 어플라이언스 구성 페이지 26을(를) 참조하십시오.

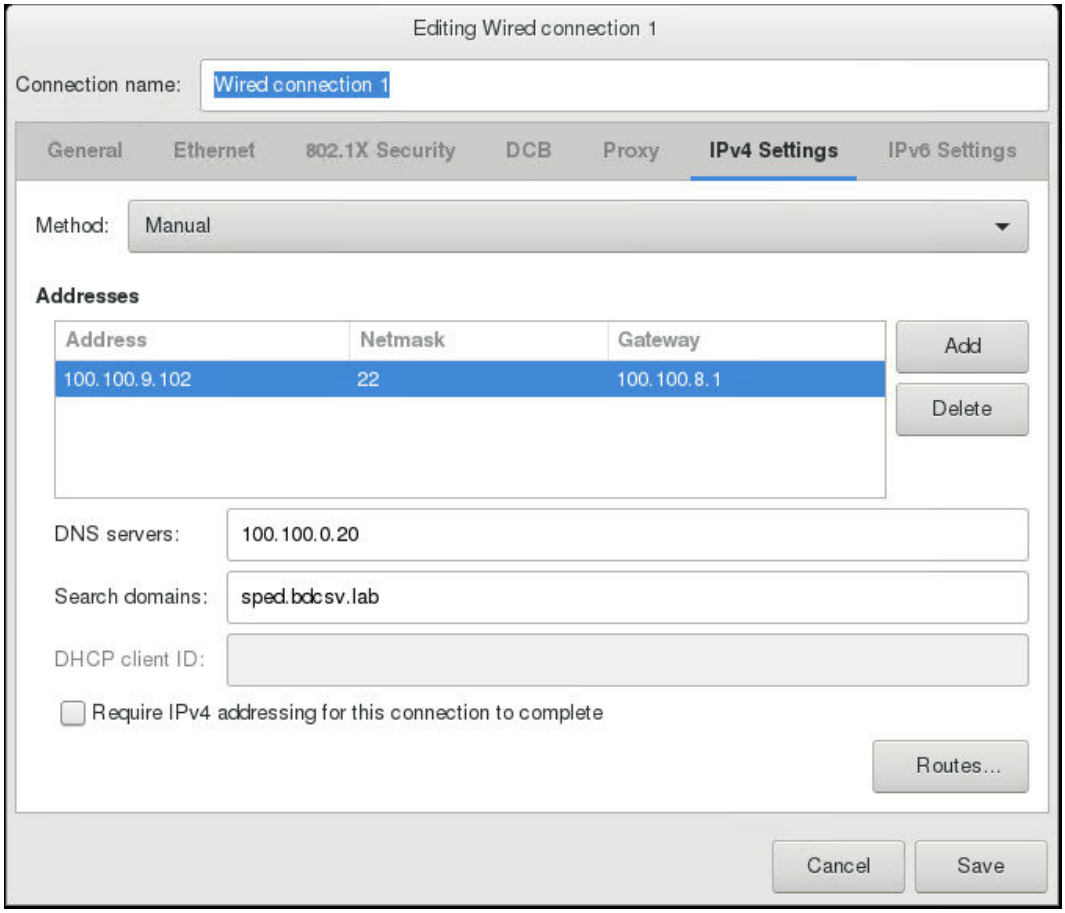
7. **유선 연결 1**을 선택하고  을 클릭합니다.



a. **IPv4 설정** 탭에서 **방법** 드롭다운 목록에 **수동**을 선택하고 **추가**를 클릭합니다.

   노트: 자동(DHCP)을 선택한 경우, 다음 재시작 중에 OMIVV 어플라이언스가 DHCP 서버로부터 IP를 자동으로 수신하므로 IP 주소를 입력하지 마십시오.

b. 올바른 IP, 넷마스크(CIDR(Classless Inter-Domain Routing) 형식) 및 게이트웨이 정보를 입력합니다.
   넷마스크 입력란에 IP 주소를 입력하면 해당하는 CIDR 형식으로 자동 변환됩니다.
c. **DNS 서버** 및 **검색 도메인** 입력란에 검색할 DNS 서버 IP 및 도메인을 각각 입력합니다.
d. **이 연결을 수행하는 데 IPV4 주소 지정 필요** 확인란을 선택하고 **저장**을 클릭합니다.



노트:

OMIVV 어플라이언스를 정적 IP로 구성한 후 OMIVV 터미널 유틸리티 페이지가 즉시 새로 고쳐지지 않고 업데이트된 IP가 표시되지 않을 수 있습니다. 이 문제를 해결하려면 OMIVV 터미널 유틸리티를 종료하고 다시 로그인합니다.

8. OMIVV 어플라이언스의 호스트 이름을 변경하려면 **호스트 이름 변경**을 클릭합니다.
   a. 유효한 호스트 이름을 입력하고 **호스트 이름 업데이트**를 클릭합니다.

      노트: vCenter 서버가 OMIVV 어플라이언스에 이미 등록된 경우 모든 vCenter 인스턴스를 등록 취소하고 다시 등록해야 합니다. 자세한 내용은 설치 가이드의 등록 취소 및 재등록 관리 항목을 참조하십시오.

9. 어플라이언스를 다시 시작합니다.

2개의 NIC(Network Interface Controller)를 사용하여 OMIVV 어플라이언스 구성

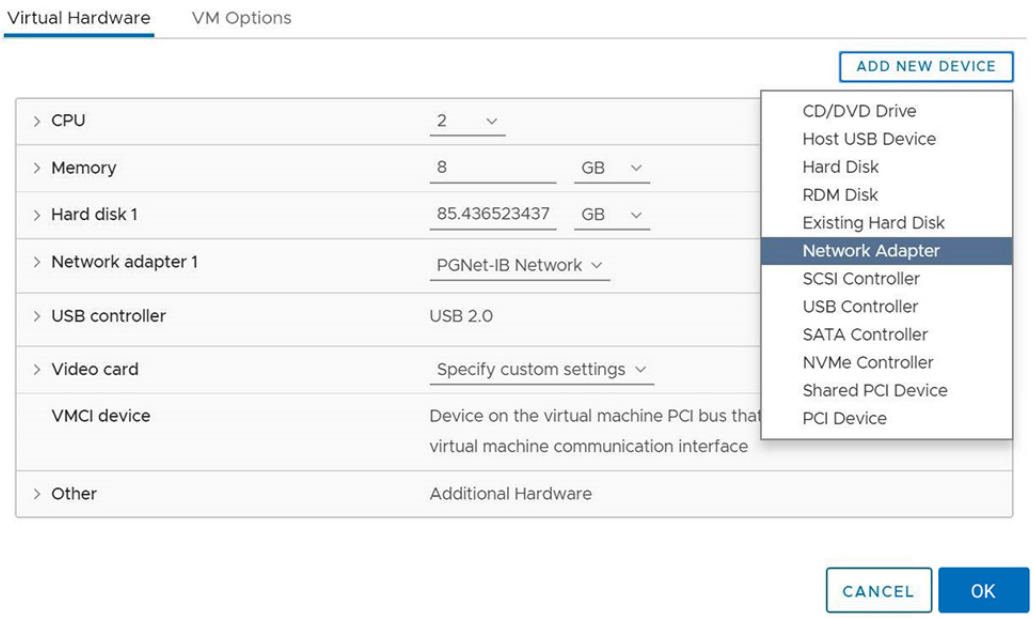
vSphere 환경에서 Dell EMC 서버를 관리하려면 OMIVV에서 vSphere 네트워크(vCenter 및 ESXi 관리 네트워크)와 아웃오브밴드 네트워크(iDRAC, CMC 및 OME-Modular) 모두에 액세스해야 합니다. vSphere 네트워크와 아웃오브밴드 네트워크가 사용자 환경에서 별도의 분리된 네트워크로 유지되는 경우 OMIVV는 두 개의 네트워크에 액세스해야 합니다. 이 경우 OMIVV 어플라이언스는 두 개의 NIC로 구성되어야 합니다. vSphere 네트워크를 사용하여 아웃오브밴드 네트워크에 액세스할 수 있는 경우 OMIVV 어플라이언스에 대해 2개의 NIC를 구성하지 마십시오.

아웃오브밴드 네트워크와 vSphere 네트워크 모두에 대해 다음 정보가 준비되어 있는지 확인하십시오.

- 어플라이언스의 IP 주소, 넷마스크(CIDR 형식) 및 게이트웨이(고정된 경우)
- 기본 게이트웨이 – 인터넷에 연결된 하나의 네트워크에 대해서만 기본 게이트웨이를 구성해야 합니다. vSphere 네트워크를 기본 게이트웨이로 사용하는 것이 좋습니다.
- 라우팅 요구 사항(네트워크 IP, 넷마스크 및 게이트웨이) – 직접 또는 기본 게이트웨이를 통해 연결할 수 없는 다른 외부 네트워크의 경우 고정 경로를 구성합니다.
- DNS 요구 사항 – OMIVV는 하나의 네트워크에 대해서만 DNS 구성만 지원합니다. DNS 구성에 대한 자세한 내용을 보려면 이 항목의 9단계(b)로 이동하십시오.

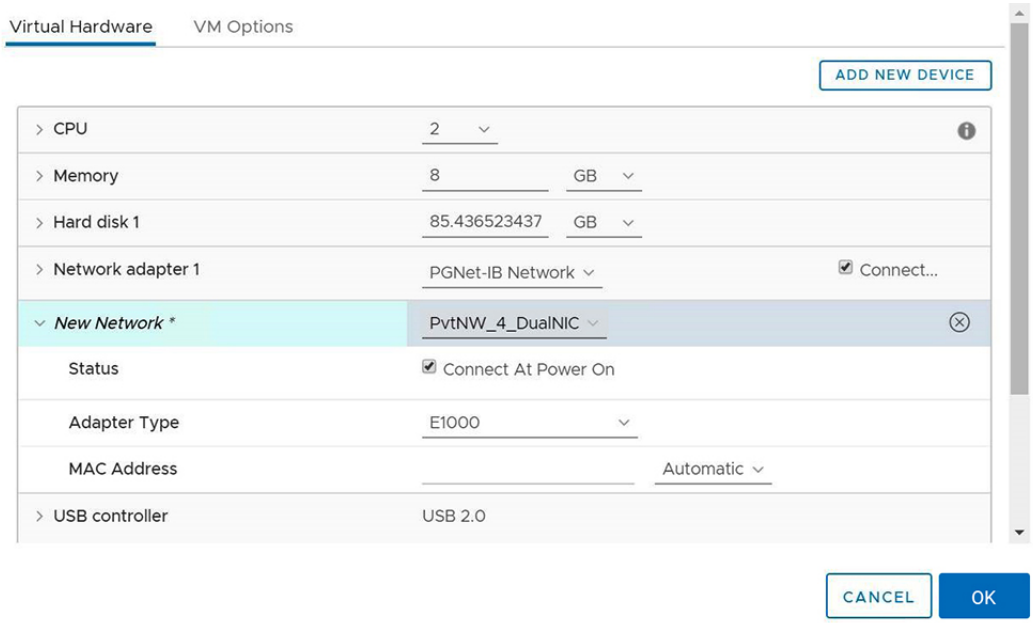
1. OMIVV 어플라이언스의 전원을 끕니다.

2. vSphere Client(HTML-5)를 사용하여 VM 설정을 편집하고 네트워크 어댑터를 추가합니다. VM 설정을 편집하려면 VM을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집** 을 클릭합니다.
3. **새 디바이스 추가**를 클릭하고 **네트워크 어댑터**를 선택합니다.

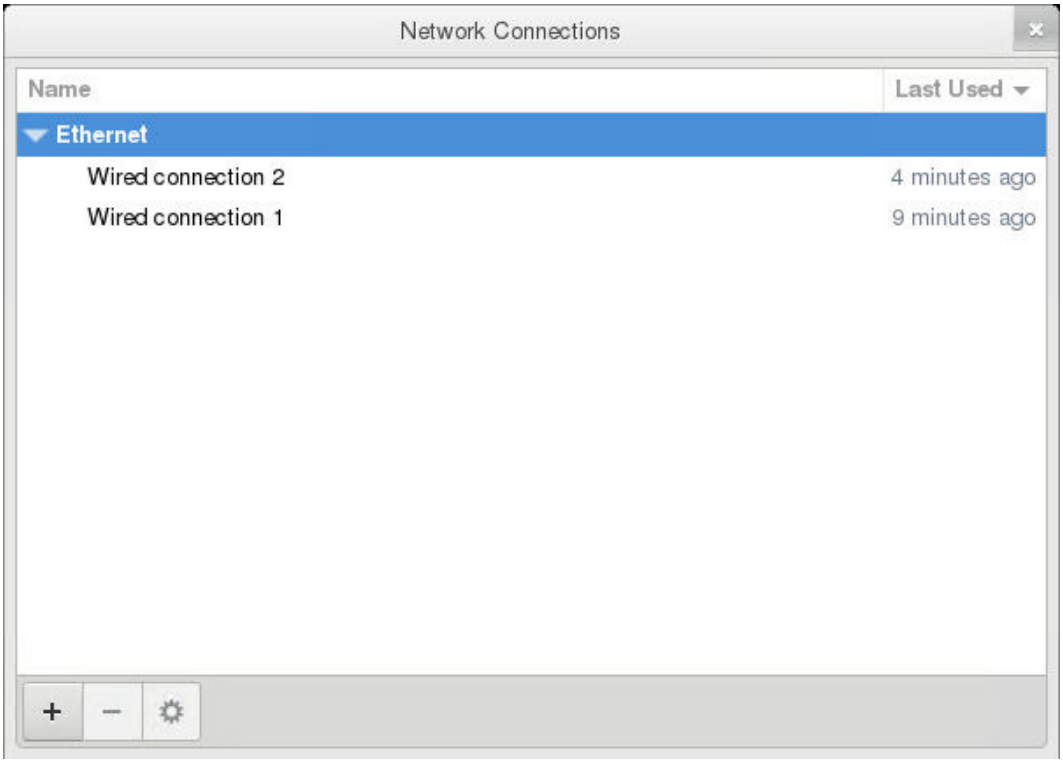


a. NIC에 적합한 네트워크를 선택한 후 **전원을 켤 때 연결** 확인란을 선택합니다.
b. 드롭다운 메뉴에서 **VMXNET3** 어댑터 유형을 선택합니다.

노트: OMIVV는 VMXNET3 유형의 NIC를 지원합니다.

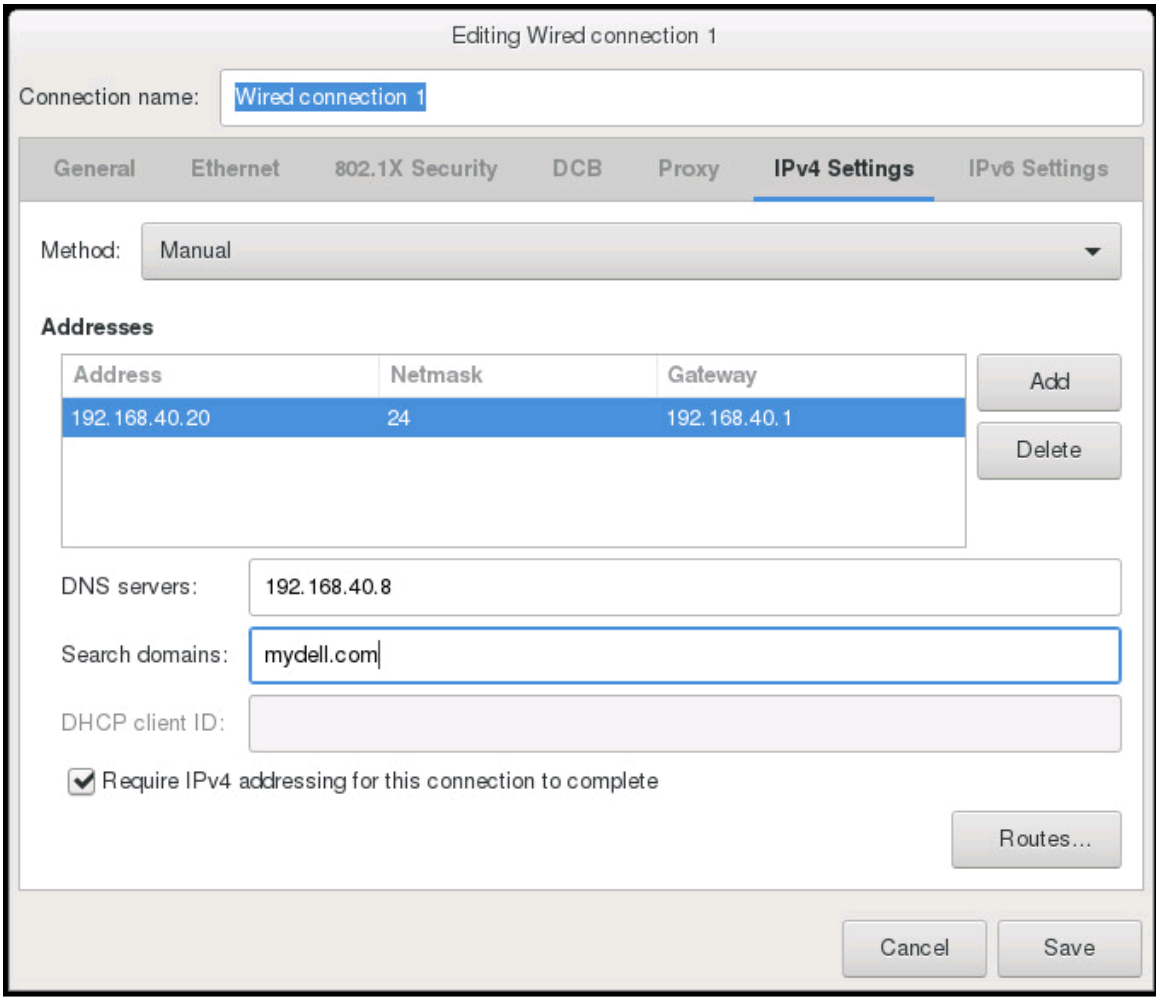


4. OMIVV 어플라이언스의 전원을 켭니다. 관리자(기본 사용자 이름은 Admin)로 로그인한 후 **Enter** 키를 누릅니다.
5. **OpenManage Integration for VMware vCenter 가상 어플라이언스 설정** 페이지에서 **네트워크 구성**을 선택합니다. **네트워크 연결** 페이지에 NIC 2개가 표시됩니다.



경고: "+"를 사용하여 새 네트워크 인터페이스를 추가하지 마십시오. NIC를 추가하려면 vSphere 편집 설정을 사용해야 합니다.

6. 구성하려는 NIC를 선택하고  을 클릭합니다.
7. 올바른 NIC를 식별하려면 **이더넷** 탭에 표시된 MAC ID를 사용한 다음 vSphere Client(HTML-5)에 표시된 MAC ID와 비교합니다. **이더넷** 탭에 나열된 기본 MAC 주소를 변경하지 마십시오.
8. **일반** 탭을 클릭하고**사용 가능한 경우 이 네트워크에 자동으로 연결** 확인란을 선택합니다.
9. **IPv4 설정** 탭을 클릭하고 다음을 수행합니다.



a. **방법** 드롭다운 목록에서 **수동** 또는 **자동(DHCP)**을 선택합니다.
b. **수동** 방법을 선택한 경우 **추가**를 클릭하고 올바른 IP 주소, 넷마스크(CIDR 형식) 및 게이트웨이 세부 정보를 입력합니다. DNS 서버의 우선 순위(기본 및 보조 DNS 항목)를 제어하려면 고정 IP를 사용하는 것이 좋습니다.

   일반적으로 vCenter 및 ESXi 호스트와 같은 데이터 센터의 vSphere 요소는 호스트 이름 또는 FQDN을 사용하여 관리됩니다. iDRAC, CMC 및 OME-Modular는 IP 주소를 사용하여 관리됩니다. 이 경우 vSphere 네트워크에 대해서만 DNS 설정을 구성하는 것이 좋습니다.

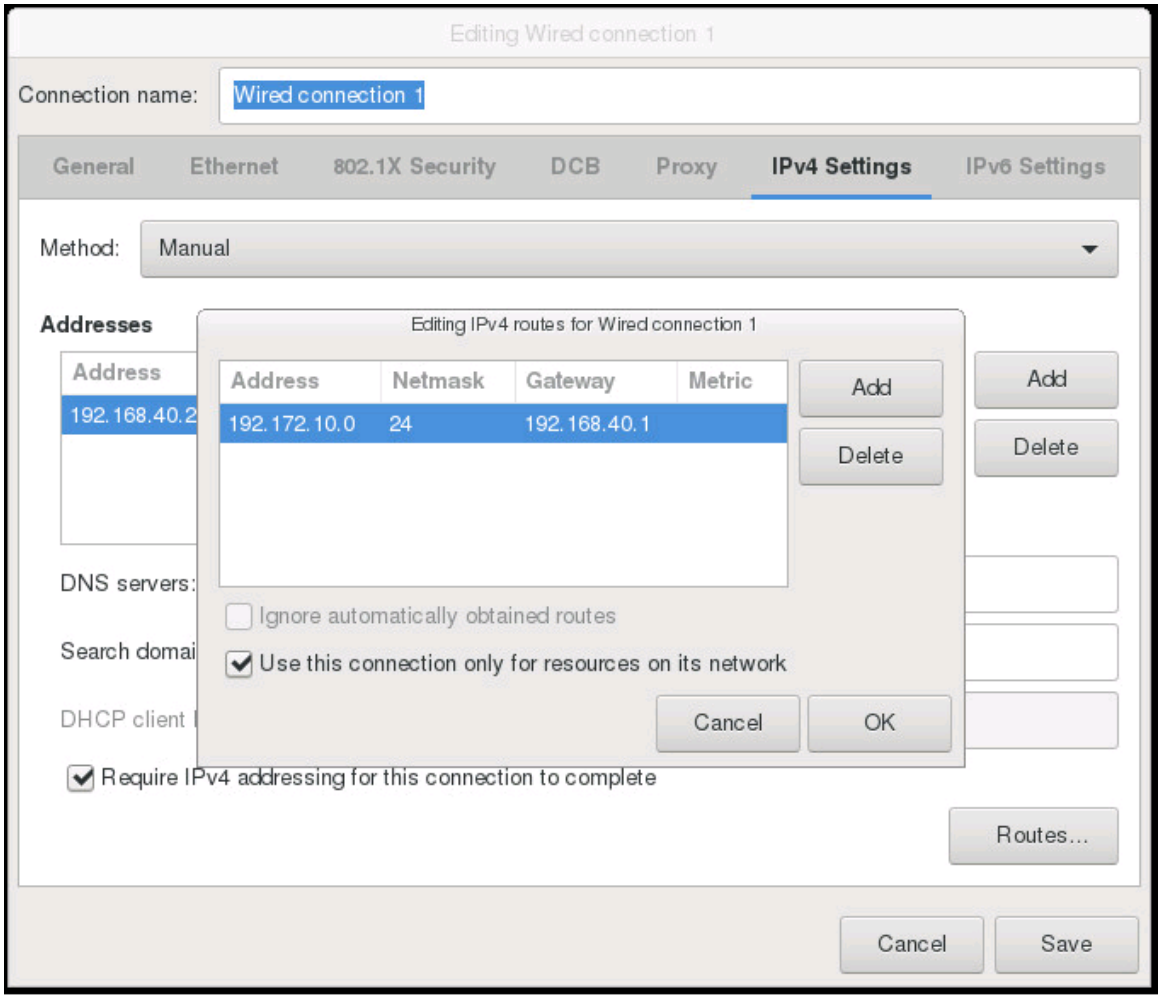
   호스트 이름 또는 FQDN을 사용하여 vSphere 네트워크와 iDRAC 관리 네트워크를 모두 관리하는 경우 DNS 서버가 두 개의 네트워크에 대해 호스트 이름 또는 FQDN을 확인하도록 구성되어야 합니다. 자세한 내용은 CentOS 설명서를 참조하십시오.

   노트: 마지막으로 구성된 DNS 서버는 DNS가 구성된 네트워크와 상관없이 기본 DNS가 됩니다.

c. **DNS 서버** 및**검색 도메인** 상자에 검색할 DNS 서버 IP 및 도메인을 각각 입력합니다.
d. **이 연결을 수행하는 데 IPV4 주소 지정 필요** 확인란을 선택하고 **저장**을 클릭합니다.
e. 이 네트워크를 기본 네트워크(게이트웨이)로 사용하지 않으려면 **루트**를 클릭하고 **이 연결을 해당 네트워크의 리소스에 대해서만 사용** 확인란을 선택합니다.

   노트: 여러 네트워크를 기본 게이트웨이로서 추가하면 네트워크 문제가 발생하고 OMIVV 기능이 영향을 받을 수 있습니다.

f. 알려진 게이트웨이를 사용하여 외부 네트워크에 연결하려는 경우 동일한 페이지에서 **추가**를 클릭하고 네트워크 IP 주소, 넷마스크(CIDR 형식) 및 게이트웨이 세부 정보를 추가합니다.



일반적으로 기본 게이트웨이로서 구성한 네트워크에서는 게이트웨이가 연결성을 제공할 수 있기 때문에 수동 라우팅 구성이 필요하지 않습니다. 그러나 기본 게이트웨이가 구성되지 않은 네트워크의 경우(**이 연결을 해당 네트워크의 리소스에 대해서만 사용** 확인란이 선택됨) 수동 라우팅 구성이 필요할 수 있습니다. 이 네트워크가 외부 네트워크에 도달하도록 기본 게이트웨이가 구성되지 않았으므로 수동 라우팅 구성이 필요합니다.

노트: 라우팅 구성이 잘못되면 네트워크 인터페이스가 갑자기 응답하지 않을 수 있습니다. 라우팅 항목을 적절하게 구성해야 합니다.

g. **확인**을 클릭합니다.

10. **저장**을 클릭합니다. 다른 NIC를 구성하려면 6~10번 작업을 반복합니다.
11. **OpenManage Integration for VMware vCenter 가상 어플라이언스 설정** 유틸리티에서 **어플라이언스 재부팅**을 클릭합니다. 네트워크 구성은 OMIVV 어플라이언스를 재시작해야 완료됩니다.

    어플라이언스가 성공적으로 재시작된 후 NIC가 구성된 대로 작동하기 시작합니다. NIC 상태는 **readonly** 사용자로 로그인하고 `ifconfig`, `ping`, 및 `route -n` 명령을 실행하면 볼 수 있습니다.

OMIVV 어플라이언스 암호 변경

콘솔을 사용하여 vSphere Client에서 OMIVV 어플라이언스 암호를 변경할 수 있습니다.

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.

NTP(Network Time Protocol) 구성 및 현지 시간대 설정

1. OMIVV 웹 콘솔을 엽니다.
2. **OpenManage Integration for VMware vCenter 가상 어플라이언스 설정** 유틸리티에서 **날짜/시간 속성**을 클릭합니다.
   관리 콘솔에 NTP 세부 정보를 입력해야 합니다. 자세한 내용은 NTP(Network Time Protocol) 서버 설정 페이지 21을(를) 참조하십시오.
3. **날짜 및 시간** 탭에서 **네트워크에서 날짜 및 시간 동기화**를 선택합니다.
   NTP 서버 창이 표시됩니다.
4. 다른 NTP 서버 IP 또는 호스트 이름(필요한 경우)을 추가하려면 **추가** 버튼을 클릭한 다음 **TAB** 키를 누릅니다.
5. **시간대**를 클릭하고 해당 시간대를 선택한 다음 **확인**을 클릭합니다.

OMIVV 어플라이언스의 호스트 이름 변경

1. **OpenManage Integration for VMware vCenter 가상 어플라이언스 설정** 유틸리티에서 **호스트 이름 변경**을 클릭합니다.

   노트: vCenter 서버가 OMIVV 어플라이언스에 등록된 경우 모든 vCenter 인스턴스를 등록 취소하고 다시 등록해야 합니다.

2. 업데이트된 호스트 이름을 입력합니다.
   <hostname> 형식으로 도메인 이름을 입력합니다.
3. **호스트 이름 업데이트**를 클릭합니다.
   어플라이언스 호스트 이름이 업데이트되고 메인 메뉴 페이지가 표시됩니다.
4. 어플라이언스를 재부팅하려면 **어플라이언스 재부팅**을 클릭합니다.

노트: iDRAC 및 DRM(Dell EMC Repository Manager)의 프로비저닝 서버와 같은 환경에서는 가상 어플라이언스에 대한 모든 참조를 수동으로 업데이트해야 합니다.

OMIVV 어플라이언스 재부팅

1. OMIVV 웹 콘솔을 엽니다.
2. **OpenManage Integration for VMware vCenter 가상 어플라이언스 설정** 유틸리티에서 **어플라이언스 재부팅**을 클릭합니다.
3. 어플라이언스를 재부팅하려면 **예**를 클릭합니다.

OMIVV 어플라이언스를 출하 시 설정으로 재설정

1. OMIVV 웹 콘솔을 엽니다.
2. **OpenManage Integration for VMware vCenter 가상 어플라이언스 설정** 유틸리티에서 **설정 재설정**을 클릭합니다.
   다음과 같은 메시지가 표시됩니다.

```
All the settings in the appliance will be Reset to Factory Defaults and the appliance will
be rebooted. Do you still wish to continue?
```

3. 어플라이언스 리셋을 확인하려면 **예**를 클릭합니다.
   예를 클릭하면 OMIVV 어플라이언스가 출하 시 기본 설정으로 리셋되고 다른 모든 설정 및 기존 데이터가 삭제됩니다.

   출하 시 설정으로 재설정이 완료되면 vCenter를 OMIVV 어플라이언스에 다시 등록합니다.

노트: OMIVV 어플라이언스를 출하 시 기본 설정으로 재설정해도 네트워크 구성에서 수행한 모든 업데이트는 보존됩니다. 이러한 설정은 리셋되지 않습니다.

읽기 전용 사용자 역할

진단을 위한 셸 액세스 권한이 있는 "읽기 전용"이라고 하는 권한 없는 사용자가 있습니다. 읽기 전용 사용자의 권한은 소수의 명령 실행으로 제한됩니다.

3

대시보드를 사용하여 호스트 및 섀시 모니터링

대시보드는 다음을 표시합니다.

- 호스트 및 섀시의 상태
- 호스트 및 섀시의 보증 상태
- 호스트 및 vCenter의 라이선스 정보
- 호스트의 구성 규정 준수 상태
- OMIVV를 사용하여 예약된 작업의 상태
- 배포에 사용할 수 있는 운영 체제 미설치 서버
- OMIVV 기능에 대한 빠른 참조

상태

상태 섹션에는 모든 OMIVV 관리 호스트 및 섀시의 상태가 표시됩니다. 여기에 표시되는 모든 호스트는 동일한 PSC(Platform Service Controller)를 사용하여 구성됩니다.

호스트 및 섀시에서 상태 메트릭 작업 또는 SNMP 이벤트(특정 호스트 또는 섀시의 상태 메트릭 작업을 트리거함)가 주기적으로 완료된 후 각 호스트 및 섀시의 상태가 새로 고쳐집니다.

기본적으로 상태 메트릭 작업은 매 시간 실행됩니다. 표시된 데이터는 대시보드의 서버 및 섀시에 대한 Proactive HA 상태 및 상태 업데이트를 모니터링하는 데 사용됩니다. 작업 세부 정보는 로그에서 볼 수 있습니다.

다음 목록에서는 호스트 및 섀시의 여러 상태에 대해 설명합니다.

- **정상** - 정상 상태에 있는 호스트 및 섀시의 개수를 표시합니다.
- **경고** - 개선 조치가 필요하지만 시스템에 즉시 영향을 주지 않는 호스트 및 섀시 개수를 표시합니다.
- **위험** - 하나 이상의 구성 요소에 중요한 문제가 있는 호스트 및 섀시 개수를 표시하며 즉시 해결해야 합니다.
- **알 수 없음** - 알 수 없는 상태의 호스트 및 섀시의 개수를 표시합니다. 호스트 또는 섀시에 연결할 수 없거나 상태를 알 수 없는 경우 호스트 또는 섀시가 알 수 없음 상태로 표시됩니다.

호스트에 대한 자세한 내용을 보려면 **대시보드** 페이지의 **상태** 섹션에서 **호스트 보기**를 클릭합니다.

섀시에 대한 자세한 내용을 보려면 **대시보드** 페이지의 **상태** 섹션에서 **섀시 보기**를 클릭합니다.

보증

이 보증 범주에 표시되는 호스트 수는 PSC를 사용하여 구성된 vCenter Server에 속한 호스트를 나타냅니다. 호스트 및 섀시에 대한 보증 정보를 얻으려면 **설정** 페이지에서 보증 만료 알림을 활성화해야 합니다.

다수의 또는 다양한 보증이 있는 호스트(예: NBD(Next Business Day) 및 POW(Parts Only Warranty)와 같은 보증 유형)의 경우 OMIVV는 남은 보증 일수가 가장 적은 보증 유형에 의거해 상태를 표시합니다.

보증 섹션에는 호스트 및 섀시에 대한 다음과 같은 정보가 있습니다.

- **정상** - 남은 보증 일이 경고 임계값을 초과하는 호스트 및 섀시 수를 표시합니다.
- **경고** - 남은 보증 일이 경고 임계값 미만인 호스트 및 섀시 수를 표시합니다.
- **위험** - 남은 보증 일이 위험 임계값 미만인 호스트 및 섀시 수를 표시합니다.
- **알 수 없음** - 보증이 알려지지 않은 호스트 및 섀시 수를 표시합니다.

정상, **경고**, **위험** 및 **알 수 없음** 상태인 호스트를 식별하려면 다음을 수행합니다.

1. **호스트 및 클러스터**로 이동합니다.
2. 클러스터 수준에서 호스트의 상태를 보려면 클러스터를 선택한 다음 **모니터링** > **OMIVV 클러스터 정보** > **보증**을 클릭합니다.
3. 데이터 센터 수준에서 호스트의 상태를 보려면 데이터 센터를 선택한 다음 **모니터링** > **OMIVV 데이터 센터 정보** > **보증**을 클릭합니다.

라이선스

라이선스 섹션에는 다음 정보가 표시됩니다.

- 모든 호스트 및 vCenter 라이선스 수
- 사용 가능한 호스트 및 vCenter 라이선스 수
- 사용 중인 호스트 및 vCenter 라이선스의 수

라이선스를 구매하려면 **대시보드** 페이지의 **라이선스** 섹션에서 **라이선스 구입**을 클릭합니다.

배포 준비

이 섹션에서는 OMIVV를 사용하여 검색된 호환되는 운영 체제 미설치 서버만 다룹니다. 운영 체제 미설치 서버를 배포하려면 **배포**를 클릭합니다.

구성 규정 준수

이 섹션에는 클러스터 프로필과 연결된 클러스터의 일부인 호스트가 표시됩니다. 여기에 표시되는 호스트는 동일한 플랫폼 서비스 컨트롤러(PSC)를 사용하여 구성됩니다.

호스트의 구성 규정 준수 상태를 보려면 **규정 준수 보기**를 클릭합니다.

작업

이 섹션에는 OMIVV를 사용하여 예약된 작업이 표시됩니다. 지난 7일 동안만 작업 세부 정보를 볼 수 있습니다.

원형 차트는 **성공**, **진행 중**, **실패**, **예약됨** 및 **취소됨** 상태의 총 작업 수를 표시합니다. 원형 차트에서 작업 상태를 필터링하려면 작업 상태를 클릭합니다.

성공, **진행 중**, **실패**, **예약됨** 및 **취소됨** 상태의 다음 작업 수를 볼 수 있습니다.

- 배포 작업

  자세한 내용은 배포 작업 페이지 68을(를) 참조하십시오.
- 호스트 펌웨어 업데이트 작업

  자세한 내용은 호스트 펌웨어 업데이트 작업 페이지 70을(를) 참조하십시오.
- 섀시 펌웨어 업데이트 작업

  자세한 내용은 섀시 펌웨어 업데이트 작업 페이지 69을(를) 참조하십시오.
- 시스템 잠금 작업

  자세한 내용은 시스템 잠금 모드 작업 페이지 70을(를) 참조하십시오.

모든 작업의 상태를 보려면 **모든 작업 보기**를 클릭합니다.

빠른 참조

이 섹션에는 다음 기능에 대한 빠른 참조가 나와 있습니다.

- 초기 구성 마법사 시작

  자세한 내용은 다음을 참조하십시오. 초기 구성 페이지 80
- 호스트 자격 증명 프로필

  자세한 내용은 다음을 참조하십시오. 호스트 자격 증명 프로필 페이지 35
- 관리 규정 준수

  자세한 내용은 다음을 참조하십시오. 관리 규정 준수 페이지 63
- 섀시 자격 증명 프로필

자세한 내용은 다음을 참조하십시오. 섀시 자격 증명 프로필 페이지 39

- 클러스터 프로필

  자세한 내용은 다음을 참조하십시오. 클러스터 프로필 페이지 46

- 배포

  자세한 내용은 다음을 참조하십시오. 배포 체크리스트 페이지 58

4

호스트 자격 증명 프로필을 사용하여 호스트 관리

호스트 자격 증명 프로필

호스트 자격 증명 프로필에서는 OMIVV에서 서버와 통신하기 위해 사용하는 iDRAC 및 호스트 자격 증명을 저장합니다. OMIVV는 호스트 자격 증명 프로필과 연결된 호스트를 관리합니다. 하나의 호스트 자격 증명 프로필에 여러 서버를 연결할 수 있습니다.

하나의 통합 섀시 관리 IP를 사용하여 PowerEdge MX 섀시 호스트를 관리할 수 있습니다. iDRAC IP가 비활성화된 PowerEdge MX 섀시에 존재하는 호스트는 섀시 자격 증명 프로필을 사용하여 관리해야 합니다. 섀시 자격 증명 프로필을 사용하여 PowerEdge MX 섀시를 관리하려면 섀시 자격 증명 프로필 생성 페이지 39을(를) 참조하십시오. 전체 OMIVV 기능을 얻기 위해 호스트 자격 증명 프로필을 사용하여 iDRAC IP로 PowerEdge MX 섀시 호스트를 관리하는 것이 좋습니다.

호스트 자격 증명 프로필 생성

추가된 호스트 수가 라이선스 제한을 초과하는 경우 호스트 자격 증명 프로필을 생성할 수 없습니다.

호스트 자격 증명 프로필과 함께 AD(Active Directory) 자격 증명을 사용하기 전에 다음을 확인합니다.

- AD에 사용자 계정이 있습니다.
- iDRAC 또는 호스트가 AD 기반 인증에 맞게 구성되었습니다.

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **호스트 자격 증명 프로필**을 클릭합니다.
2. **호스트 자격 증명 프로필** 페이지에서 **새 프로필 생성**을 클릭합니다.
3. 마법사의 **호스트 자격 증명 프로필** 페이지에서 지침을 읽고 **시작하기**를 클릭합니다.
4. **이름 및 자격 증명** 페이지에서 다음을 수행합니다.
   a. 프로필 이름과 설명을 입력합니다. 설명 필드는 선택 사항입니다.
   b. **vCenter 이름** 목록에서 호스트 자격 증명 프로필을 생성할 vCenter의 인스턴스를 선택합니다.
   c. **iDRAC 자격 증명** 영역에서 iDRAC 로컬 자격 증명 또는 AD 자격 증명을 입력합니다.
      - iDRAC의 로컬 자격 증명을 입력하려면 다음 작업을 수행합니다.
        - **사용자 이름** 상자에 사용자 이름을 입력합니다. 사용자 이름은 16자로 제한됩니다.

          사용자 이름 정의에 대한 자세한 내용은 **https://www.dell.com/support**에서 제공되는 *iDRAC 사용자 가이드*를 참조하십시오.
        - 암호를 입력합니다.

          사용자 이름 및 암호에 권장되는 문자에 대한 자세한 내용은 **https://www.dell.com/support**에서 제공되는 *iDRAC 사용자 가이드*를 참조하십시오.
      - iDRAC 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화** 확인란을 선택합니다.
      - AD용으로 이미 구성 및 활성화된 iDRAC에 대한 자격 증명을 입력하려면 **Active Directory 사용** 확인란을 선택합니다.

        노트: iDRAC 계정에 관리 권한이 있어야 펌웨어 업데이트, OS(Operating System) 배포를 수행할 수 있습니다.
        - **Active Directory 사용자 이름** 상자에 사용자 이름을 입력합니다.

          `domain\username` 또는 `username@domain`과 같은 형식 중 하나로 사용자 이름을 입력합니다. 사용자 이름은 256자로 제한됩니다. 사용자 이름 제한 사항에 대해서는 **Microsoft Active Directory 설명서**를 참조하십시오.
        - 암호를 입력합니다.

          iDRAC 및 호스트에 대한 AD 자격 증명은 동일하거나 별개일 수 있습니다.

   d. **호스트 루트** 영역에서 로컬 호스트 자격 증명 또는 AD 자격 증명을 입력합니다.

      기본 사용자 이름은 root입니다.

- 로컬 호스트 자격 증명을 입력하려면 다음 단계를 수행합니다.
  - 암호를 입력합니다.

    호스트 암호는 ESXi 6.5 U3 이하 버전을 실행하는 호스트에만 필요합니다.

    ESXi 6.7 이상 버전에 대해 이 단계를 건너뛰려면 **호스트 자격 증명 사용** 확인란의 선택을 취소해야 합니다. ESXi 6.7 이상을 실행하는 호스트에 암호를 입력하면 암호가 무시됩니다.

    ESXi 6.7 이상 버전을 실행하는 호스트의 경우 ESXi 자격 증명을 입력할 필요가 없습니다. OMIVV는 잘못된 호스트 자격 증명을 입력한 경우에도 iDRAC를 ESXi 호스트와 페어링할 수 있습니다.

- AD용으로 이미 구성 및 활성화된 호스트에 대한 자격 증명을 입력하려면 **Active Directory 사용** 확인란을 선택합니다.
  - **Active Directory 사용자 이름** 상자에 사용자 이름을 입력합니다. `domain\username` 또는 `username@domain`과 같은 형식 중 하나로 사용자 이름을 입력합니다. 사용자 이름은 256자로 제한됩니다. 사용자 이름 제한 사항에 대해서는 **Microsoft Active Directory 설명서**를 참조하십시오.
  - 암호를 입력합니다.

- 호스트 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화** 확인란을 선택합니다.

5. **다음**을 클릭합니다.
   호스트 선택 페이지가 표시됩니다.
6. **호스트 선택** 페이지에서 트리 뷰를 확장하고 호스트를 선택한 다음 **확인**을 클릭합니다.
   - **호스트 추가**를 클릭하여 **연결된 호스트** 페이지에서 호스트를 추가 또는 제거합니다.

     노트: iDRAC IPv4가 비활성화된 PowerEdge MX 서버를 호스트 자격 증명 프로필에 추가하지 마십시오. 이러한 서버는 섀시 자격 증명 프로필을 사용하여 관리합니다.

   선택한 호스트가 **연결된 호스트** 페이지에 표시됩니다.
7. 연결을 테스트하려면 하나 이상의 호스트를 선택하고 **테스트 시작**을 클릭합니다.
   구성한 모든 호스트에 대해 연결을 테스트하는 것이 좋습니다.

   연결 테스트 중에 OMIVV는 WBEM 서비스를 활성화하여 ESXi 6.5 이상을 실행하는 호스트의 iDRAC IP를 검색한 다음 WBEM 서비스를 비활성화합니다.

   노트: 유효한 자격 증명을 입력한 후 호스트에 대한 연결 테스트 작업이 실패할 수 있으며, 유효하지 않은 자격 증명을 입력했음을 나타내는 메시지가 표시됩니다. 이 문제는 ESXi에서 액세스를 차단하는 경우 발생합니다. 잘못된 자격 증명을 사용하여 ESXi 연결을 여러 번 시도하면 15분 동안 ESXi에 액세스할 수 없습니다. 15분 정도 기다린 후 작업을 다시 시도하십시오.

   - 연결 테스트 프로세스를 중지하려면 **테스트 중단**을 클릭합니다.

   테스트 결과 섹션에서 연결 테스트 결과를 볼 수 있습니다.
8. **마침**을 클릭합니다.

호스트 자격 증명 프로필 편집

여러 호스트 자격 증명 프로필의 자격 증명을 한 번에 편집할 수 있습니다.

1. **이름 및 자격 증명** 페이지에서 다음을 수행합니다.
   a. 프로필 이름과 설명을 편집합니다.
   b. **iDRAC 자격 증명** 영역에서 iDRAC 로컬 자격 증명 또는 AD 자격 증명을 편집합니다.
      - iDRAC의 로컬 자격 증명을 변경하려면 다음 작업을 수행합니다.
        - **사용자 이름** 상자의 사용자 이름을 변경합니다. 사용자 이름은 16자로 제한됩니다.

          사용자 이름 정의에 대한 자세한 내용은 **dell.com/support**에서 제공되는 *iDRAC 사용자 가이드*를 참조하십시오.
        - 암호를 변경합니다.
        - iDRAC 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화** 확인란을 선택합니다.
      - AD용으로 이미 구성 및 활성화된 iDRAC에 대한 자격 증명을 변경하려면 **Active Directory 사용** 확인란을 선택합니다.

        노트: iDRAC 계정에 관리 권한이 있어야 펌웨어 업데이트, OS(Operating System) 배포를 수행할 수 있습니다.

- **Active Directory 사용자 이름** 상자의 사용자 이름을 변경합니다.

  `domain\username` 또는 `username@domain`과 같은 형식 중 하나로 사용자 이름을 입력합니다. 사용자 이름은 256자로 제한됩니다. 사용자 이름 정의에 대한 자세한 내용은 *Microsoft Active Directory 설명서*를 참조하십시오.
- 암호를 입력합니다.
- iDRAC 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화** 확인란을 선택합니다.

c. **호스트 루트** 영역에서 로컬 호스트 자격 증명 또는 AD 자격 증명을 수정합니다.

- 로컬 호스트 자격 증명을 입력하려면 다음 단계를 수행합니다.

  기본 사용자 이름은 root입니다.
  - 암호를 입력합니다.

    호스트 암호는 ESXi 6.5 U3 이하 버전을 실행하는 호스트에만 필요합니다.

    ESXi 6.7 이상 버전에 대해 이 단계를 건너뛰려면 **호스트 자격 증명 사용** 확인란의 선택을 취소해야 합니다. ESXi 6.7 이상을 실행하는 호스트에 암호를 입력하면 암호가 무시됩니다.

    ESXi 6.7 이상 버전을 실행하는 호스트의 경우 ESXi 자격 증명을 입력할 필요가 없습니다. OMIVV는 잘못된 호스트 자격 증명을 입력한 경우에도 iDRAC을 ESXi 호스트와 페어링할 수 있습니다.
- AD용으로 이미 구성 및 활성화된 호스트에 대한 자격 증명을 변경하려면 **Active Directory 사용** 확인란을 선택합니다.
  - **Active Directory 사용자 이름** 상자의 사용자 이름을 변경합니다.

    `domain\username` 또는 `username@domain`과 같은 형식 중 하나로 사용자 이름을 입력합니다. 사용자 이름은 256자로 제한됩니다. 사용자 이름 제한 사항에 대해서는 *Microsoft Active Directory 설명서*를 참조하십시오.
  - 암호를 변경합니다.
- 호스트 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화** 확인란을 선택합니다.

2. **다음**을 클릭합니다.
   연결된 호스트 페이지가 표시됩니다.
3. 연결된 호스트 목록에서 호스트를 추가 또는 제거하려면 **연결된 호스트** 페이지에서 **호스트 추가**를 클릭합니다.

   노트: iDRAC IPv4가 비활성화된 PowerEdge MX 서버를 호스트 자격 증명 프로필에 추가하지 마십시오. 이러한 서버는 섀시 자격 증명 프로필을 사용하여 관리합니다.

   선택한 호스트가 **연결된 호스트** 페이지에 표시됩니다.
4. 연결을 테스트하려면 하나 이상의 호스트를 선택하고 **테스트 시작**을 클릭합니다. 구성한 모든 호스트에 대해 연결을 테스트하는 것이 좋습니다.

   노트: 유효한 자격 증명을 입력한 후 호스트에 대한 연결 테스트 작업이 실패할 수 있으며, 유효하지 않은 자격 증명을 입력했음을 나타내는 메시지가 표시됩니다. 이 문제는 ESXi에서 액세스를 차단하는 경우 발생합니다. 잘못된 자격 증명을 사용하여 ESXi 연결을 여러 번 시도하면 15분 동안 ESXi에 액세스할 수 없습니다. 15분 정도 기다린 후 작업을 다시 시도하십시오.

   - 연결 테스트를 중지하려면 **테스트 중단**을 클릭합니다.

   테스트 결과 섹션에서 연결 테스트 결과를 볼 수 있습니다.

   연결 테스트 중에 OMIVV는 WBEM 서비스를 활성화하여 ESXi 6.5 이상을 실행하는 호스트의 iDRAC IP를 검색한 다음 WBEM 서비스를 비활성화합니다.
5. **마침**을 클릭합니다.

   노트: 수정 날짜 및 마지막으로 수정한 사람 필드에는 vSphere Client 인터페이스를 사용하여 호스트 자격 증명 프로필에 대해 수행한 변경 사항이 포함되어 있습니다. 해당 호스트 자격 증명 프로필에 대해 OMIVV 어플라이언스가 수행하는 모든 변경 사항은 이러한 두 필드에 영향을 미치지 않습니다.

호스트 자격 증명 프로필 보기

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **호스트 자격 증명 프로필**을 클릭합니다.
   모든 호스트 자격 증명 프로필이 다음 정보와 함께 표에 표시됩니다.

- **프로필 이름** – 호스트 자격 증명 프로필의 이름입니다.
- **설명** – 프로필 설명입니다(제공된 경우).
- **vCenter** – 연결된 vCenter의 FQDN, 호스트 이름 또는 IP 주소입니다.
- **연결된 호스트** – 호스트 자격 증명 프로필과 연결된 호스트입니다. 연결된 호스트가 둘 이상인 경우 확장 아이콘을 사용하여 모두 표시합니다.
- **iDRAC 인증서 확인** – 호스트 자격 증명 프로필을 생성할 때 iDRAC 인증서를 검증했는지 여부를 나타냅니다.
- **호스트 루트 인증서 확인** – 호스트 자격 증명 프로필을 생성할 때 호스트 루트 인증서를 검증했는지 여부를 나타냅니다.
- **생성한 날짜** – 호스트 자격 증명 프로필을 생성한 날짜입니다.
- **수정한 날짜** – 호스트 자격 증명 프로필을 수정한 날짜입니다.
- **마지막으로 수정한 사람** – 호스트 자격 증명 프로필을 수정한 사용자의 세부 정보입니다.

노트: 섀시 자격 증명 프로필을 사용하여 PowerEdge MX 호스트를 관리하는 경우, OMIVV에서는 이를 섀시 자격 증명 프로필에 연결된 것으로 표시합니다. 자세한 내용은 섀시 자격 증명 프로필 보기 페이지 40을(를) 참조하십시오.

2. 마법사에서 열 이름을 제거하거나 추가하려면 아이콘을 클릭합니다.
   기본적으로 **수정한 날짜**와 **마지막으로 수정한 사람** 열은 선택되지 않습니다. 이 열을 선택하려면 을 클릭합니다.
3. 호스트 자격 증명 프로필 정보를 내보내려면 을 클릭합니다.

호스트 자격 증명 프로필 테스트

자격 증명 프로필 테스트 기능을 사용하여 호스트 및 iDRAC 자격 증명을 테스트할 수 있습니다. 모든 호스트를 선택하는 것이 좋습니다.

1. OMIVV 홈 페이지에서 연결된 호스트가 있는 호스트 자격 증명 프로필을 선택하고 **테스트**를 클릭합니다.
   호스트 자격 증명 프로필 테스트 페이지가 표시됩니다.
2. 모든 연결된 호스트를 선택하고 **테스트 시작**을 클릭합니다.
   a. 연결 테스트를 중지하려면 **테스트 중단**을 클릭합니다.
   iDRAC 및 호스트 자격 증명에 대한 연결 테스트 결과가 모두 표시됩니다.

호스트 자격 증명 프로필 삭제

인벤토리, 보증 또는 배포 작업이 실행 중일 때 호스트와 연결된 호스트 자격 증명 프로필을 삭제하지 마십시오.

OMIVV는 삭제한 호스트 자격 증명 프로필에 속하는 호스트가 다른 호스트 자격 증명 프로필에 추가될 때까지 해당 호스트를 관리하지 않습니다.

1. **호스트 자격 증명 프로필** 페이지에서 프로필을 선택하고 **삭제**를 클릭합니다.
2. 확인 메시지가 표시되면 **삭제**를 클릭합니다.
   선택한 프로필이 호스트 자격 증명 프로필 목록에서 제거됩니다.

5

섀시 자격 증명 프로필을 사용하여 섀시 관리

섀시 자격 증명 프로필

섀시 자격 증명 프로필에서는 OMIVV가 섀시와 통신하기 위해 사용하는 섀시 자격 증명을 저장합니다. OMIVV는 섀시 자격 증명 프로필과 연결된 섀시를 관리하고 모니터링합니다. 하나의 섀시 자격 증명 프로필에 여러 개의 섀시를 할당할 수 있습니다.

하나의 통합 섀시 관리 IP를 사용하여 PowerEdge MX 섀시 호스트를 관리할 수 있습니다. iDRAC IP가 비활성화된 PowerEdge MX 섀시에 존재하는 호스트는 섀시 자격 증명 프로필을 사용하여 관리해야 합니다. 전체 OMIVV 기능을 얻기 위해 호스트 자격 증명 프로필을 사용하여 iDRAC IP로 PowerEdge MX 섀시 호스트를 관리하는 것이 좋습니다. MX 섀시 관리에 대한 자세한 내용은 PowerEdge MX 섀시 관리 페이지 103을(를) 참조하십시오.

섀시 자격 증명 프로필 생성

- 섀시 자격 증명 프로필을 생성하려면 다음 권한이 있어야 합니다.
  - M1000e, VRTX 및 FX2 섀시 - SNMP 트랩 대상 읽기 및 설정
  - PowerEdge MX 섀시 - 관리자
- 호스트 자격 증명 프로필과 함께 AD(Active Directory) 자격 증명을 사용하기 전에 다음을 확인합니다.
  - AD에 사용자 계정이 있습니다.
  - CMC 또는 OME-Modular가 AD 기반 인증을 위해 구성되어 있습니다.
- PowerEdge MX 섀시의 경우, 등록된 vCenter에 최소 하나의 MX 호스트가 있는지 확인하여 연결 테스트에 성공했는지 확인해야 합니다.

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **섀시 자격 증명 프로필** > **새 프로필 생성**을 클릭합니다.
2. 마법사의 **섀시 자격 증명 프로필** 페이지에서 지침을 읽고 **시작하기**를 클릭합니다.
3. **이름 및 자격 증명** 페이지에서 다음을 수행합니다.
   a. 프로필 이름과 설명을 입력합니다. 설명은 선택 사항입니다.
   b. **사용자 이름** 텍스트 상자에 일반적으로 CMC(Chassis Management Controller) 또는 OME-Modular(OpenManage Enterprise-Modular)에 로그온할 때 사용되는 관리자 권한이 있는 사용자 이름을 입력합니다.
   c. **암호** 텍스트 상자에 암호를 입력합니다.
   d. **암호 확인** 텍스트 상자에 **암호** 텍스트 상자에 입력한 것과 동일한 암호를 입력합니다. 이 두 암호는 서로 일치해야 합니다.
4. **섀시 선택** 페이지에서 **IP/호스트 이름** 열 옆에 있는 확인란을 사용하여 개별 섀시 또는 여러 섀시를 선택하고 **확인**을 클릭합니다. 선택한 섀시가 **연결된 섀시** 페이지에 표시됩니다. 연결된 섀시 목록에서 섀시를 추가하거나 제거하려면 **섀시 추가**를 클릭합니다.

   선택한 섀시가 이미 섀시 자격 증명 프로필과 연결되어 있는 경우 다음 메시지가 표시됩니다.

   현재 다른 프로필에 연결된 섀시를 선택하면 해당 섀시 자격 증명 프로필에서 섀시가 제거됩니다. 연결된 섀시가 없는 섀시 자격 증명 프로필은 삭제됩니다.

   예를 들어, 섀시 A와 연결된 테스트 프로필이 있습니다. 다른 프로필 테스트 1을 생성하고 섀시 A를 테스트 1에 연결하도록 시도하면 경고 메시지가 표시됩니다.

   연결 테스트는 선택한 섀시에 대해 자동으로 실행됩니다.

   다음과 같은 경우 연결 테스트는 자동으로 실행됩니다.

   - 섀시를 선택한 후 처음인 경우
   - 자격 증명을 변경하는 경우
   - 섀시가 새로 선택된 경우

   테스트 결과가 **테스트 결과** 열에 **통과** 또는 **실패**로 표시됩니다. 섀시 연결을 수동으로 테스트하려면, 섀시를 선택하고 **연결 테스트**를 클릭합니다.

MCM 그룹에 구성된 PowerEdge MX 섀시의 경우 리드 섀시를 사용하여 모든 리드 섀시와 구성원 섀시를 관리하는 것이 좋습니다. 구성원 섀시 연결 테스트 작업이 실패하고 테스트 결과 상태가 **실패**로 표시됩니다. 리드 섀시 IP 링크가 표시됩니다. 전체 MCM 그룹을 검색하려면 리드 섀시 IP 링크를 클릭합니다.

5. **마침**을 클릭합니다.

   마법사에서 작업을 완료하려면 검증된 섀시가 하나 이상 있어야 합니다. 성공적으로 유효성을 검사한 섀시만 섀시 자격 증명 프로필과 연결될 수 있습니다.

   PowerEdge MX 섀시를 추가하려면 PowerEdge MX 섀시 추가 페이지 104을(를) 참조하십시오.

섀시 자격 증명 프로필 편집

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **섀시 자격 증명 프로필**을 클릭합니다.
2. **섀시 자격 증명 프로필** 페이지에서 **편집**을 클릭합니다.
3. **이름 및 자격 증명** 페이지에서 다음을 수행합니다.
   a. 프로필 이름과 설명을 편집합니다. 설명은 선택 사항입니다.
   b. **사용자 이름** 텍스트 상자에 일반적으로 CMC(Chassis Management Controller) 또는 OME-Modular(OpenManage Enterprise-Modular)에 로그온할 때 사용되는 관리자 권한이 있는 사용자 이름을 변경합니다.
   c. **암호** 텍스트 상자에 암호를 입력합니다.

      암호 필드를 비워 두면 OMIVV는 워크플로 생성 중에 입력한 것을 암호로 간주합니다.
   d. **암호 확인** 텍스트 상자에 **암호** 텍스트 상자에 입력한 것과 동일한 암호를 입력합니다. 이 두 암호는 서로 일치해야 합니다.
4. **섀시 선택** 페이지에서 **IP/호스트 이름** 열 옆에 있는 확인란을 사용하여 섀시를 선택 또는 제거하고 **확인**을 클릭합니다.
   선택한 섀시가 **연결된 섀시** 페이지에 표시됩니다. 연결된 섀시 목록에서 섀시를 추가하거나 제거하려면 **섀시 추가**를 클릭합니다.

   선택한 섀시가 이미 호스트 자격 증명 프로필과 연결되어 있는 경우 다음 메시지가 표시됩니다.

   현재 다른 프로필에 연결된 섀시를 선택하면 해당 섀시 자격 증명 프로필에서 섀시가 제거됩니다. 연결된 섀시가 없는 섀시 자격 증명 프로필은 삭제됩니다.

   예를 들어, 섀시 A와 연결된 테스트 프로필이 있습니다. 다른 프로필 테스트 1을 생성하고 섀시 A를 테스트 1에 연결하도록 시도하면 경고 메시지가 표시됩니다.

   연결 테스트는 선택한 섀시에 대해 자동으로 실행됩니다.

   다음과 같은 경우 연결 테스트는 자동으로 실행됩니다.

   - 섀시를 선택한 후 처음인 경우
   - 자격 증명을 변경하는 경우
   - 섀시가 새로 선택된 경우

   테스트 결과가 **테스트 결과** 열에 **통과** 또는 **실패**로 표시됩니다. 섀시 연결을 수동으로 테스트하려면, 섀시를 선택하고 **연결 테스트**를 클릭합니다.

   MCM 그룹에 구성된 PowerEdge MX 섀시의 경우 리드 섀시를 사용하여 모든 리드 섀시와 구성원 섀시를 관리하는 것이 좋습니다. 구성원 섀시 연결 테스트 작업이 실패하고 테스트 결과 상태가 실패로 표시됩니다. 리드 섀시 IP 링크가 표시됩니다. 전체 MCM 그룹을 검색하려면 리드 섀시 IP 링크를 클릭합니다.

   노트: 추가된 PowerEdge MX 섀시에 연결된 등록된 vCenter에 호스트가 표시되지 않는 경우 섀시에 대한 연결 테스트에 실패합니다.
5. **마침**을 클릭합니다.

   마법사에서 작업을 완료하려면 검증된 섀시가 하나 이상 있어야 합니다. 성공적으로 유효성을 검사한 섀시만 섀시 자격 증명 프로필과 연결될 수 있습니다.

   PowerEdge MX 섀시를 추가하려면 PowerEdge MX 섀시 추가 페이지 104을(를) 참조하십시오.

섀시 자격 증명 프로필 보기

하나 이상의 섀시 자격 증명 프로필을 생성한 후 섀시 자격 증명 프로필 페이지에서 섀시 및 연결된 섀시를 볼 수 있습니다.

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **섀시 자격 증명 프로필**을 클릭합니다.

   모든 섀시 자격 증명 프로필이 다음 정보와 함께 표에 표시됩니다.

- **프로필 이름** – 섀시 자격 증명 프로필의 이름입니다.
- **설명** – 프로필 설명입니다.
- **섀시 IP/호스트 이름** – 섀시 IP 또는 호스트 이름 링크.

  MCM(Multi-chassis Management) 그룹의 경우 리드 섀시()와 구성원 섀시()가 계층 구조에 나열됩니다.

  노트: MCM 구성의 PowerEdge MX 섀시의 경우 OMIVV에서 리드 섀시만 사용하여 모든 리드 및 구성원 섀시를 관리합니다. 모든 리드 및 구성원은 리드 섀시가 연결된 동일한 섀시 자격 증명 프로필에 연결됩니다.

  MCM 그룹의 구성원 섀시(IPv4가 비활성화됨)의 경우 리드의 IPv4 주소가 표시됩니다. 구성원 섀시의 서비스 태그도 괄호 안에 표시됩니다.
- **섀시 서비스 태그** – 섀시에 할당된 고유 식별자.
- **수정한 날짜** – 섀시 자격 증명 프로필을 수정한 날짜.

2. 관련 호스트에 대한 다음 정보가 하단 그리드에 표시됩니다.
   - **프로필 이름**
   - **연결된 호스트**
   - **서비스 태그**
   - **섀시 IP/호스트 이름**
   - **섀시 서비스 태그**
3. 섀시 자격 증명 프로필 정보를 내보내려면 을 클릭합니다.

섀시 자격 증명 프로필 테스트

섀시 자격 증명 프로필 테스트 기능을 사용하여 섀시 자격 증명 프로필과 연결된 섀시의 자격 증명을 테스트할 수 있습니다. 모든 섀시를 선택하는 것이 좋습니다.

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **섀시 자격 증명 프로필**을 클릭합니다.
2. 섀시 자격 증명 프로필을 선택하고 **테스트**를 클릭합니다.
3. **섀시 자격 증명 프로필 테스트** 페이지에서 연결된 섀시를 선택하고 **테스트 시작**을 클릭합니다.
   a. 연결 테스트를 중지하려면 **테스트 중단**을 클릭합니다.

   테스트 결과는 **테스트 결과** 열에 표시됩니다.

섀시 자격 증명 프로필 삭제

섀시 자격 증명 프로필을 삭제하기 전에 섀시 인스턴스가 OMIVV가 등록된 다른 vCenter의 일부가 아닌지 확인합니다.

섀시 자격 증명 프로필이 삭제된 경우 OMIVV는 섀시를 다른 섀시 자격 증명 프로필에 추가할 때까지 삭제된 섀시 자격 증명 프로필에 있는 섀시를 모니터링하지 않습니다.

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **섀시 자격 증명 프로필** > **삭제**를 클릭합니다.
2. 삭제할 섀시 자격 증명 프로필을 선택합니다.
3. 확인 메시지가 표시되면 **삭제**를 클릭합니다.

   섀시 자격 증명 프로필에 연결된 모든 섀시가 제거되거나 다른 프로필로 이동되면 삭제 확인 메시지가 표시됩니다. 이 메시지는 섀시 자격 증명 프로필에 연결된 섀시가 없으며 삭제되었음을 나타냅니다.

   섀시 자격 증명 프로필을 삭제하려면 삭제 확인 메시지에서 **확인**을 클릭합니다.

6

리포지토리 프로필을 사용하여 펌웨어 및 드라이버 리포지토리 관리

리포지토리 프로필

리포지토리 프로필을 사용하면 드라이버 또는 펌웨어 리포지토리를 생성하고 관리할 수 있습니다.

펌웨어 및 드라이버 리포지토리 프로필을 사용하여 다음을 수행할 수 있습니다.

- 호스트 펌웨어 업데이트
- vSAN 클러스터에 속한 호스트 드라이버를 업데이트합니다.
- 클러스터 프로필을 생성하고 클러스터 베이스라인을 설정합니다.

기본 OMIVV 펌웨어 카탈로그는 다음과 같습니다.

- **Dell EMC 기본 카탈로그**: Dell EMC 온라인 카탈로그를 사용하여 최신 펌웨어 정보를 가져오는 출하 시 생성된 펌웨어 리포지토리 프로필입니다. 어플라이언스에 인터넷 연결이 없는 경우, 이 리포지토리를 수정하여 로컬 CIFS, NFS 또는 HTTP 또는 HTTPS 기반 공유를 지정합니다. 이 카탈로그의 수정에 대한 자세한 내용은 Dell 기본 카탈로그 편집 또는 맞춤 구성 페이지 43을(를) 참조하십시오.

  Dell EMC 기본 카탈로그를 기본 카탈로그로 선택하여 클러스터 프로필과 연결되지 않은 vSphere 호스트의 펌웨어를 업데이트할 수 있습니다.
- **검증된 MX 스택 카탈로그**: Dell EMC 온라인 카탈로그를 사용하여 MX 섀시 및 해당 슬레드에 대한 검증된 펌웨어 정보를 가져오는 출하 시 생성된 펌웨어 리포지토리 프로필입니다. 이 카탈로그의 수정에 대한 자세한 내용은 유효성을 검사한 MX 스택 카탈로그 편집 페이지 44을(를) 참조하십시오. 검증된 MX 스택 카탈로그에 대한 자세한 내용은 MX7000 펌웨어 업데이트에서 제공하는 기술 백서를 참조하십시오.

  노트: Dell EMC 기본 카탈로그 및 검증된 MX 스택 카탈로그 리포지토리 프로필을 사용하여 vSAN 클러스터 베이스라인을 설정할 수 없습니다.

리포지토리 프로필 생성

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **프로필** > **리포지토리 프로필**을 클릭합니다.
2. 마법사의 **리포지토리 프로필** 페이지에서 지침을 읽고 **시작하기**를 클릭합니다.
3. **프로필 이름 및 설명** 페이지에서 프로필 이름 및 설명을 입력합니다. 설명 필드는 선택 사항이며 255자로 제한됩니다.
4. **다음**을 클릭합니다.
   프로필 설정 페이지가 표시됩니다.
5. **프로필 설정** 페이지에서 **펌웨어** 또는 **드라이버**를 선택합니다.
   드라이버 리포지토리 프로필에는 다음 사항이 적용됩니다.
   - 드라이버 리포지토리 프로필은 최대 10개의 드라이버를 포함할 수 있습니다. 더 많은 파일이 있는 경우 드라이버가 임의로 선택됩니다.
   - 오프라인 드라이버 번들(.zip 파일)만 사용됩니다.
   - 오프라인 드라이버 번들(.zip 파일)을 다운로드하고 추출해 공유 위치의 전체 경로를 제공하여 공유 위치에 저장합니다. OMIVV에서 OMIVV 어플라이언스 내부에 카탈로그를 자동으로 생성합니다. 드라이버 번들은 다음 주소에서 확인할 수 있습니다. https://my.vmware.com/web/vmware/downloads
   - OMIVV에는 CIFS 또는 NFS에 대한 쓰기 액세스 권한이 필요합니다.
   - 하위 폴더 내의 파일은 무시됩니다.
   - 10MB 크기를 초과하는 파일은 무시됩니다.
   - 드라이버 리포지토리는 vSAN 클러스터에만 적용할 수 있습니다.
6. **리포지토리 공유 위치** 영역에서 다음 작업을 수행합니다.

a. 리포지토리 공유 위치(NFS 또는 CIFS)를 입력합니다.
b. CIFS의 경우 자격 증명을 입력합니다.
OMIVV에서는 SMB(Server Message Block) 버전 1.0과 SMB 버전 2.0 기반 CIFS 공유만 지원됩니다.

노트: SMB 1.0 공유가 드라이버 리포지토리에 사용되는 경우 디렉토리 경로 끝에 파일 구분 기호를 추가합니다.

7. 카탈로그 경로 및 자격 증명을 확인하려면 **테스트 시작**을 클릭합니다.
리포지토리 프로필을 계속 생성하려면 이 검증 프로세스를 완료해야 합니다.
연결 테스트 결과가 표시됩니다.
8. **다음**을 클릭합니다.
리포지토리 위치와 동기화 페이지가 표시됩니다.
9. **다음**을 클릭합니다.
리포지토리 프로필에 관한 정보를 제공하는 **요약** 페이지가 표시됩니다.
10. **마침**을 클릭합니다.
카탈로그 생성 후, 다운로드 및 구문 분석이 수행되고 리포지토리 프로필의 홈 페이지에 상태가 표시됩니다.
성공적으로 구문 분석된 리포지토리 프로필은 클러스터 프로필을 작성하는 중에, 그리고 펌웨어를 업데이트하는 중에 사용 가능합니다.

리포지토리 프로필 편집

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **리포지토리 프로필** > **편집**을 클릭합니다.
2. **프로필 이름 및 설명** 페이지에서 프로필 이름 및 설명을 편집한 후 **다음**을 클릭합니다.
3. **프로필 설정** 페이지에서 **펌웨어** 또는 **드라이버**를 선택합니다.
드라이버 리포지토리 프로필에는 다음 사항이 적용됩니다.
   - 드라이버 리포지토리 프로필은 최대 10개의 드라이버를 포함할 수 있습니다. 더 많은 파일이 있는 경우 드라이버가 임의로 선택됩니다.
   - 오프라인 드라이버 번들(.zip 파일)만 사용됩니다.
   - 오프라인 드라이버 번들(.zip 파일)을 다운로드하고 추출해 공유 위치의 전체 경로를 제공하여 공유 위치에 저장합니다. OMIVV에서 OMIVV 어플라이언스 내부에 카탈로그를 자동으로 생성합니다. 드라이버 번들은 다음 주소에서 확인할 수 있습니다. https://my.vmware.com/web/vmware/downloads
   - OMIVV에는 CIFS 또는 NFS에 대한 쓰기 액세스 권한이 필요합니다.
   - 하위 폴더 내의 파일은 무시됩니다.
   - 10MB 크기를 초과하는 파일은 무시됩니다.
   - 드라이버 리포지토리는 vSAN 클러스터에만 적용할 수 있습니다.
4. **리포지토리 공유 위치** 영역에서 다음 작업을 수행합니다.
a. 리포지토리 공유 위치(NFS 또는 CIFS)를 입력합니다.
b. CIFS의 경우 자격 증명을 입력합니다.

노트: OMIVV에서는 SMB(Server Message Block) 버전 1.0과 SMB 버전 2.0 기반 CIFS 공유만 지원됩니다.

5. 카탈로그 경로 및 자격 증명을 확인하려면 **테스트 시작**을 클릭합니다.
계속 진행하려면 이 유효성 검사가 필요합니다.
연결 테스트 결과가 표시됩니다.
6. **다음**을 클릭합니다.
리포지토리 위치와 동기화 페이지가 표시됩니다.
7. **리포지토리 위치와 동기화** 페이지에서 **리포지토리 위치와 동기화** 확인란을 선택하고 **다음**을 클릭합니다.
프로필 이름만 업데이트하거나 정보를 검토하려면 **리포지토리 위치와 동기화** 확인란을 지워 카탈로그가 OMIVV에서 변경되지 않도록 합니다. 리포지토리 위치와 동기화에 대한 자세한 내용은 리포지토리 위치와 동기화 페이지 44을 참조하십시오.
8. **요약** 페이지에서 프로필 정보를 검토한 다음 **마침**을 클릭합니다.

Dell 기본 카탈로그 편집 또는 맞춤 구성

1. **리포지토리 프로필** 페이지에서 **Dell 기본 카탈로그**를 선택합니다.

2. **프로필 이름 및 설명** 페이지에서 프로필 설명을 편집한 후 **다음**을 클릭합니다.
3. **리포지토리 위치 지정** 섹션에서 다음 리포지토리 위치 중에서 선택합니다.
   - **Dell 기본 온라인** – 리포지토리 프로필이 **Dell 온라인**(`https://downloads.dell.com/catalog/Catalog.gz`)으로 설정됩니다. OMIVV에서는 Dell EMC 온라인을 카탈로그 및 업데이트 패키지의 소스로 사용합니다.
   - **맞춤 구성 온라인** - OMIVV에서는 **맞춤 구성 온라인**(HTTP 또는 HTTPS 공유)을 카탈로그 및 업데이트 패키지에 대한 소스로 사용합니다. SUU(Server Update Utility)를 사용하여 맞춤 구성 리포지토리를 생성할 때 카탈로그(`catalog.xml.gz.sign`)의 서명 파일이 카탈로그 파일 폴더에 있는지 확인합니다.
   - **공유 네트워크 폴더** - OMIVV에서는 공유 네트워크 폴더(CIFS 또는 NFS)를 카탈로그 및 업데이트 패키지에 대한 소스로 사용합니다.

   a. **맞춤 구성 온라인**을 선택한 경우 카탈로그 온라인 경로를 입력합니다.
   b. **공유 네트워크 폴더**를 선택한 경우에는 다음과 같은 형식으로 카탈로그 파일 위치(NFS 또는 CIFS)를 입력합니다.
4. 카탈로그 경로 및 자격 증명을 확인하려면 **테스트 시작**을 클릭합니다.
   연결 테스트 결과가 표시됩니다.
5. **리포지토리 위치와 동기화** 페이지에서 **리포지토리 위치와 동기화** 확인란을 선택하고 **다음**을 클릭합니다.
   프로필 이름만 업데이트하거나 정보를 검토하려면 **리포지토리 위치와 동기화** 확인란을 지워 카탈로그가 OMIVV에서 변경되지 않도록 합니다. 리포지토리 위치와 동기화에 대한 자세한 내용은 리포지토리 위치와 동기화 페이지 44을 참조하십시오.
6. **요약** 페이지에서 프로필 정보를 검토한 다음 **마침**을 클릭합니다.

유효성을 검사한 MX 스택 카탈로그 편집

1. **리포지토리 프로필** 페이지에서 **유효성을 검사한 MX 스택 카탈로그**를 선택하고 **편집**을 클릭합니다.
2. 다음 항목만 편집할 수 있습니다.
   a. 카탈로그 설정.
   b. **리포지토리 위치와 동기화** 확인란.
      프로필 이름만 업데이트하거나 정보를 검토하려면 **리포지토리 위치와 동기화** 확인란을 지워 카탈로그가 OMIVV에서 변경되지 않도록 합니다. 리포지토리 위치와 동기화에 대한 자세한 내용은 리포지토리 위치와 동기화 페이지 44을 참조하십시오.

리포지토리 위치와 동기화

Dell 기본 카탈로그 및 검증된 MX 스택 리포지토리 프로필에서는 24시간마다 또는 재부팅 및 업데이트할 때마다 자동으로 변경 사항을 확인합니다.

오프라인 카탈로그를 업데이트하려면 다음 단계를 완료하십시오.

1. DRM(Dell EMC Repository Manager) 또는 SUU(Server Update Utility)를 사용하여 오프라인 위치(CIFS 또는 NFS)에서 카탈로그를 업데이트합니다. 드라이버의 경우 드라이버 번들을 교체합니다.
2. 리포지토리 프로필을 편집하고 **리포지토리 위치와 동기화** 확인란을 선택하여 OMIVV가 참조하는 변경 사항을 캡처합니다. 프로세스를 완료하는 데 몇 분 정도 걸릴 수 있습니다.
3. 구성 규정 준수 기준선으로 펌웨어를 업데이트하려면 해당 클러스터 프로필을 편집하고 저장해야 합니다.

리포지토리 프로필 보기

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **리포지토리 프로필**을 클릭합니다.
   모든 리포지토리 프로필이 다음 정보와 함께 표에 표시됩니다.
   - **프로필 이름** – 리포지토리 프로필의 이름입니다.
   - **설명** – 프로필 설명입니다.
   - **유형** – 리포지토리의 유형(펌웨어 또는 드라이버)입니다.
   - **공유 경로** – NFS 또는 CIFS 또는 HTTP 또는 HTTPS 경로입니다.
   - **마지막 업데이트 시간** – 리포지토리 프로필을 업데이트한 날짜 및 시간입니다.
   - **마지막 새로 고침 상태** – 카탈로그 다운로드 및 구문 분석 상태입니다.
2. 마법사에서 열 이름을 제거하거나 추가하려면 아이콘을 클릭합니다.
3. 리포지토리 프로필 정보를 내보내려면  을 클릭합니다.

리포지토리 프로필 삭제

리포지토리 프로필을 삭제하기 전에 연결된 클러스터 프로필에서 리포지토리 프로필의 연결을 해제해야 합니다.

1. **리포지토리 프로필** 페이지에서 리포지토리 프로필을 선택하고 **삭제**를 클릭합니다.
2. 삭제 확인 대화 상자에서 **삭제**를 클릭합니다.

7

클러스터 프로필을 사용하여 기준 구성 캡처

클러스터 프로필

클러스터 프로필을 사용하면 구성 기준(하드웨어 구성, 펌웨어 또는 드라이버 버전)을 캡처하고, 구성 기준에 대한 변경 사항을 식별하여 클러스터에 필요한 상태를 유지 관리할 수 있습니다.

클러스터 프로필을 생성하려면 시스템 프로필, 펌웨어 리포지토리 프로필, 드라이버 리포지토리 프로필 또는 이들의 조합 중 하나가 있어야 합니다. 기준이 되는 클러스터에 대해 동종 서버(동일한 모델, 동일한 하드웨어 구성 및 동일한 펌웨어 수준)를 사용하는 것이 좋습니다.

- 클러스터 프로필이 생성된 후 펌웨어 및 드라이버 리포지토리 프로필의 구문을 분석해야 클러스터 프로필 생성에 사용할 수 있습니다.
- 클러스터 프로필이 생성된 후에 기준을 위하여 관련된 펌웨어 및 드라이버 리포지토리의 현재 스냅샷이 생성됩니다. 원래 리포지토리에 변경 사항이 있는 경우에는 변경 사항을 반영하기 위해 클러스터 프로필을 다시 업데이트해야 합니다. 그렇지 않으면 원래 리포지토리에 수행되는 업데이트가 클러스터 프로필 스냅샷으로 업데이트되지 않습니다.
- 클러스터 프로필을 생성하면 변경 사항 감지 작업이 트리거됩니다.
- 클러스터가 클러스터 프로필에 연결되면 이전 클러스터 프로필 연결을 덮어씁니다(있을 경우).
- 여러 개의 독립 실행형 vCenter가 OMIVV에 등록된 경우 각 vCenter에 대해 별도의 클러스터 프로필을 생성하는 것이 좋습니다.
- vSAN 클러스터에서만 드라이버의 기준 지정이 지원됩니다.

  노트: OMIVV 외부에 설치된 드라이버는 기준 대상으로 고려하지 않습니다.

클러스터 프로필 생성

다음을 확인합니다.

- 시스템 프로필, 펌웨어 리포지토리 프로필, 드라이버 리포지토리 프로필 또는 이들의 조합 중 하나가 있어야 합니다.
- 클러스터는 vCenter에 있어야 합니다.

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **프로필** > **클러스터 프로필** > **새 프로필 생성**을 선택합니다.
2. 마법사의 **클러스터 프로필** 페이지에서 지침을 읽고 **시작하기**를 클릭합니다.
3. **프로필 이름 및 설명** 페이지에서 프로필 이름 및 설명을 입력하고 **다음**을 클릭합니다.
   프로필 이름은 최대 200자까지 가능하고 설명은 최대 400자까지 가능합니다.
4. **프로필 연결** 페이지에서 다음 프로필 중 하나 또는 이들의 조합을 선택합니다.
   - 시스템 프로필 – 시스템 프로필을 선택하면 클러스터의 호스트에 대한 구성 기준이 설정됩니다. 기본 및 고급 시스템 프로필 유형의 경우 시스템 프로필 이름이 Basic_<system profile name>, Advanced_<system profile name> 형식으로 표시됩니다.
   - 펌웨어 리포지토리 프로필 – 펌웨어 리포지토리를 선택하면 클러스터의 호스트에 대해 펌웨어 또는 BIOS 기준이 생성됩니다. 온라인 리포지토리는 vSAN 클러스터의 기준을 지정하는 데 지원되지 않습니다.
   - 드라이버 리포지토리 프로필 – 드라이버 리포지토리를 선택하면 클러스터의 호스트에 대한 드라이버 기준이 생성됩니다. 한 번에 최대 10개의 드라이버를 기준에 연결할 수 있습니다. vSAN 클러스터에서만 드라이버의 기준 지정이 지원됩니다.
5. **다음**을 클릭합니다.
   클러스터 연결 페이지가 표시됩니다.
6. **클러스터 연결** 페이지에서 다음 작업을 수행합니다.
   a. 등록된 vCenter Server의 인스턴스를 선택합니다.
   b. 클러스터를 연결하려면 **찾아보기**를 클릭합니다.
   c. 기준을 지정하려는 클러스터를 선택합니다.
   d. **확인**을 클릭합니다.
      선택한 클러스터가 **클러스터 연결** 페이지에 표시됩니다.
   e. **다음**을 클릭합니다.
7. **변경 사항 감지 예약** 페이지에서 날짜 및 시간을 선택하고 **다음**을 클릭합니다.
   클러스터 프로필에 관한 정보를 제공하는 **요약** 페이지가 표시됩니다.

8. **마침**을 클릭합니다.
   변경 사항 감지 작업은 클러스터 프로필을 저장한 직후 실행되고 이후에는 예약된 시간 동안 실행됩니다. 작업 페이지에서 작업 완료 상태를 봅니다.
   노트: 클러스터에 대한 클러스터 프로필을 생성한 후 OMIVV에서 관리하는 노드의 수가 수정되면 이후의 변경 사항 감지 작업 중에 컬렉션 크기가 자동으로 업데이트됩니다.

클러스터 프로필 편집

클러스터 프로필을 편집하면 기준이 변경되며 그에 따라 규정 준수 수준이 재계산될 수 있습니다.

연결된 드라이버 리포지토리, 펌웨어 리포지토리 또는 시스템 프로필이 변경되고 클러스터 프로필에 대한 최신 변경 사항을 사용하려면 클러스터 프로필을 선택하고 **편집**을 클릭하고 마법사에서 **다음**을 클릭한 다음 **마침**을 클릭합니다.

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **프로필** > **클러스터 프로필**을 클릭합니다.
2. 클러스터 프로필을 선택하고 **편집**을 클릭합니다.
3. **프로필 이름 및 설명** 페이지에서 설명을 편집한 후 **다음**을 클릭합니다.
4. **프로필 연결** 대화 상자에서 프로필 조합을 변경할 수 있습니다.
5. **클러스터 연결** 대화 상자에서 vCenter 인스턴스 및 연결된 클러스터를 변경할 수 있습니다.
6. **변경 사항 감지 예약** 페이지에서 변경 사항 감지 일정을 변경할 수 있습니다.
7. **요약** 페이지에서 업데이트된 정보를 검토하고 **마침**을 클릭합니다.
   변경 사항 감지 작업은 클러스터 프로필을 저장한 직후 실행되고 이후에는 예약된 시간 동안 실행됩니다.

클러스터 프로필 보기

1. OMIVV 페이지에서 **규정 준수 및 배포** > **프로필** > **클러스터 프로필**을 클릭합니다.
   모든 클러스터 프로필이 다음 정보와 함께 표에 표시됩니다.
   - **프로필 이름** – 클러스터 프로필의 이름입니다.
   - **설명** – 프로필 설명입니다.
   - **연결된 시스템 프로필** - 기본 및 고급 시스템 프로필 유형과 관련된 시스템 프로필 이름으로 Basic_<system profile name>, Advanced_<system profile name> 형식으로 표시됩니다.
   - **연결된 펌웨어 리포지토리 프로필** – 연결된 펌웨어 리포지토리 프로필 이름입니다.
   - **연결된 드라이버 리포지토리 프로필** – 연결된 드라이버 리포지토리 프로필 이름입니다.
     노트: 섀시 자격 증명 프로필을 사용하여 관리되는 PowerEdge MX 호스트의 경우 구성 변경 사항이 계산되지 않습니다.
   - **vCenter** - 클러스터 프로필과 연결된 vCenter 인스턴스입니다.
   - **마지막 업데이트 시간** – 클러스터 프로필이 업데이트된 날짜 및 시간입니다.

   노트: 연결된 리포지토리 프로필(펌웨어 또는 드라이버) 또는 시스템 프로필이 수정되면 프로필 이름에 경고 기호가 표시됩니다. 기준 변경 사항을 업데이트하도록 리포지토리 또는 시스템 프로필을 수정한 후 클러스터 프로필을 업데이트해야 합니다. 클러스터 프로필 업데이트에 대한 자세한 내용은 클러스터 프로필 업데이트 페이지 47을(를) 참조하십시오.
2. 마법사에서 열 이름을 제거하거나 추가하려면 을 클릭합니다.
3. 클러스터 프로필 정보를 내보내려면 을 클릭합니다.

클러스터 프로필 업데이트

리포지토리 프로필(펌웨어 또는 드라이버) 및 시스템 프로필을 업데이트하는 경우 클러스터 프로필 페이지에 프로필 이름에 대한 경고 기호가 표시됩니다. 프로필을 업데이트하면 클러스터 프로필의 연결된 클러스터와 vSphere Lifecycle Manager의 펌웨어 규정 준수 상태에 대한 구성 규정 준수에 영향을 미칠 수 있습니다. **프로필 업데이트** 기능을 사용하여 클러스터 프로필을 업데이트하거나 기준을 다시 지정할 수 있습니다.

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **프로필** > **클러스터 프로필**을 클릭합니다.
2. 프로필 이름에 대한 경고 기호가 있는 클러스터 프로필을 선택합니다.
3. **프로필 업데이트**를 클릭합니다.
4. 연결된 프로필을 최신 버전으로 업데이트하려면 **확인**을 클릭합니다.
   프로필을 업데이트한 후에는 기준을 되돌릴 수 없습니다.

클러스터 프로필이 업데이트된 리포지토리 프로필 또는 시스템 프로필과 동기화되면 경고 기호가 사라집니다.

클러스터 프로필 삭제

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **프로필** > **클러스터 프로필**을 클릭합니다.
2. 클러스터 프로필을 선택한 다음 **삭제**를 클릭합니다.
3. **삭제 확인** 대화 상자에서 **삭제**를 클릭합니다.
   클러스터 프로필을 삭제하면 해당 변경 사항 감지 작업도 삭제됩니다.

8

운영 체제 미설치 서버 관리

운영 체제 미설치 서버 보기

운영 체제 미설치 서버 페이지에서 다음을 수행할 수 있습니다.

- 자동 검색 및 수동 검색을 사용하여 검색된 운영 체제 미설치 서버를 봅니다.

  서비스 태그, **모델 이름**, **iDRAC IP**, **서버 상태**, **시스템 잠금 모드**, **규정 준수 상태** 및 **iDRAC 라이선스 상태** 등의 정보가 표시됩니다.

  다음은 다양한 운영 체제 미설치 서버의 상태입니다.

  - **구성되지 않음** - 서버가 OMIVV에 추가되고 구성 대기 중입니다.
  - **구성됨** - 서버에 성공적인 운영 체제 배포에 필요한 모든 하드웨어 정보가 구성되어 있습니다.
  - **격리됨** - 서버가 OMIVV 작업에서 제외되므로 서버가 운영 체제 배포 및 펌웨어 업데이트와 같은 작업을 수행할 수 없습니다.
- 운영 체제 미설치 서버의 규정 준수 상태를 봅니다.

  다음과 같은 경우 운영 체제 미설치 서버가 규정을 준수하지 않습니다.

  - 지원되는 서버가 아닌 경우.
  - 지원되는 iDRAC 라이선스가 없는 경우(iDRAC Express가 최소 요구 사항).
  - 지원되는 버전의 iDRAC, BIOS 또는 LC가 설치되지 않은 경우.
  - LOM 또는 NIC가 없는 경우.
  - 시스템 잠금 모드가 설정되었습니다.
- 규정 준수 문제에 대한 자세한 내용을 보려면 아래 수평 창에서 **세부 정보**를 클릭하십시오.

운영 체제 미설치 서버 페이지에서 다음 작업을 수행할 수도 있습니다.

- 운영 체제 미설치 서버 수동 검색
- 운영 체제 미설치 서버 제거
- 시스템 프로필 및 ISO 프로필 배포
- 운영 체제 미설치 서버 새로 고침
- iDRAC 라이선스 구입 또는 갱신

디바이스 검색

검색은 지원되는 운영 체제 미설치 서버를 추가하는 과정입니다. 서버를 검색한 후 시스템 프로필과 iso 프로필 배포에 사용할 수 있습니다. 지원되는 서버의 목록에 대한 자세한 내용은 *OpenManage Integration for VMware vCenter 호환성 매트릭스*를 참조하십시오.

사전 요구 사항:

- 운영 체제 미설치 서버의 iDRAC에서 OMIVV 가상 시스템에 대한 네트워크 연결이 필요합니다.
- 기존 운영 체제가 있는 호스트가 OMIVV에 검색되지 않아야 하며, 대신 이러한 vCenter에 추가되어야 합니다. 호스트 자격 증명 프로필에 추가합니다.
- SD 카드에 운영 체제를 배포하고 12세대 및 13세대 PowerEdge 서버의 시스템 프로필 기능을 사용하려면 iDRAC 2.50.50.50 이상이 설치되어 있어야 합니다.

자동 검색

자동 검색은 운영 체제 미설치 서버를 추가하는 과정입니다. 서버가 검색된 후에는 운영 체제 및 하드웨어 배포에 사용합니다. 자동 검색은 iDRAC의 기능으로 이 기능을 사용하면 OMIVV를 사용하여 운영 체제 미설치 서버를 수동으로 검색할 필요가 없습니다.

자동 검색 사전 요구 사항

PowerEdge 운영 체제 미설치 서버를 검색하기 전에 OMIVV가 설치되었는지 확인하십시오. iDRAC Express 또는 iDRAC Enterprise의 Dell PowerEdge 서버는 운영 체제 미설치 서버 풀에서 검색할 수 있습니다. Dell EMC 운영 체제 미설치 서버의 iDRAC에서 OMIVV 어플라이언스로 네트워크가 연결되어 있는지 확인하십시오.

노트: 기존 운영 체제가 있는 호스트는 OMIVV를 사용하여 검색되지 않으므로 호스트 자격 증명 프로필에 운영 체제를 추가해야 합니다.

자동 검색을 수행하려면 다음 조건을 충족해야 합니다.

- 전원 - 서버를 콘센트에 연결하십시오. 서버의 전원을 켤 필요가 없습니다.
- 네트워크 연결 - 서버의 iDRAC에 네트워크가 연결되어 있고 포트 4433을 통해 프로비저닝 서버와 통신하는지 확인합니다. DHCP 서버를 사용하여 프로비저닝 서버의 IP 주소를 가져오거나 iDRAC 구성 유틸리티에서 수동으로 지정할 수 있습니다.
- 추가 네트워크 설정 - DNS 이름을 확인하기 위해 DHCP 설정에서 DNS 서버 주소 가져오기를 활성화합니다.
- 프로비저닝 서비스 위치 - iDRAC이 프로비저닝 서비스 서버의 IP 주소 또는 호스트 이름을 아는지 확인합니다. 프로비저닝 서비스 위치를 참조하십시오.
- 계정 액세스 비활성화됨 - 관리자 권한이 있는 iDRAC 계정이 있는 경우 먼저 iDRAC 웹 콘솔에서 계정을 비활성화합니다. 자동 검색이 완료되면 **설정** 페이지에 입력된 배포 자격 증명을 사용하여 관리 iDRAC 계정이 다시 활성화됩니다. 배포 자격 증명에 대한 자세한 내용은 배포 자격 증명 구성 페이지 77을(를) 참조하십시오.
- 자동 검색 활성화 - 자동 검색 프로세스가 시작될 수 있도록 서버의 iDRAC에 자동 검색이 활성화되어 있는지 확인합니다. 자세한 내용은 iDRAC에서 관리 계정 활성화 또는 비활성화 페이지 50을(를) 참조하십시오.

프로비저닝 서비스 위치

다음 옵션을 사용하여 자동 검색 중 iDRAC에 의한 프로비저닝 서비스 위치를 가져옵니다.

- iDRAC에서 수동 지정 - LAN 사용자 구성, 프로비저닝 서버의 iDRAC 구성 유틸리티에 위치를 수동으로 지정합니다.
- DHCP 범위 옵션 - DHCP 범위 옵션을 사용하여 위치를 지정합니다.
- DNS 서비스 레코드 - DNS 서비스 레코드를 사용하여 위치를 지정합니다.
- DNS 알려진 이름 - DNS 서버는 알려진 이름인 DCIMCredentialServer를 사용하여 서버에 대한 IP 주소를 지정합니다.

프로비저닝 서비스 값을 iDRAC 구성 유틸리티에서 수동으로 지정하지 않으면 iDRAC에서 DHCP 범위 옵션 값을 사용하려고 합니다. DHCP 범위 옵션이 없으면 iDRAC이 DNS에서 서비스 레코드 값을 사용하려고 합니다.

DHCP 범위 옵션 및 DNS 서비스 레코드를 구성하는 방법은 https://www.dell.com/support의 Dell 자동 검색 네트워크 설정 사양을 참조하십시오.

iDRAC에서 관리 계정 활성화 또는 비활성화

자동 검색을 설정하기 전에 관리자 액세스 권한이 없는 iDRAC 계정을 제외한 모든 iDRAC 계정을 비활성화합니다. 자동 검색 후에 루트 계정을 제외한 모든 계정을 활성화할 수 있습니다.

노트: 관리자 권한을 비활성화하기 전에 iDRAC에 관리자가 아닌 사용자 계정을 만드는 것이 좋습니다.

1. 브라우저에 **iDRAC IP 주소**를 입력합니다.
2. **Integrated Dell Remote Access Controller GUI**에 로그인합니다.
3. 다음 중 하나를 실행하십시오.
   - iDRAC7의 경우: 왼쪽 창에서 **iDRAC 설정** > **사용자 인증** > **사용자** 탭을 선택합니다.
   - iDRAC8의 경우: 왼쪽 창에서 **iDRAC 설정** > **사용자 인증** > **사용자** 탭을 선택합니다.
   - iDRAC9: **iDRAC 설정** > **사용자** > **로컬 사용자**로 이동합니다.
4. **로컬 사용자** 탭에서 루트 이외의 관리 계정을 모두 찾습니다.
5. 계정을 비활성화하려면 사용자 ID에서 **ID**를 선택합니다.
6. **다음**을 클릭합니다.
7. **사용자 구성** 페이지의 **일반**에서 **사용자 활성화** 확인란을 선택 해제합니다.
8. **적용**을 클릭합니다.
9. 각 관리 계정을 다시 활성화하려면 자동 검색을 설정한 후 1~8단계를 반복합니다. 하지만 이제는 **사용자 활성화** 확인란을 선택하고 **적용**을 클릭합니다.

수동으로 PowerEdge 서버 자동 검색 구성

iDRAC 주소가 있는지 확인합니다.

Dell EMC에서 서버를 주문할 경우 프로비저닝 서버 IP 주소를 제공한 후에 서버에서 자동 검색 기능을 활성화해 달라고 요청할 수 있습니다. 프로비저닝 서버 IP 주소는 OMIVV의 IP 주소입니다. Dell EMC에서 서버를 받은 후에 iDRAC 케이블을 마운팅 및 연결한 후 서버의 전원을 켜면 서버가 자동으로 검색되고 **운영 체제 미설치 서버** 페이지에 나열됩니다.

노트: 자동으로 검색된 서버의 경우 **설정** > **어플라이언스 설정** > **배포 자격 증명**에 제공된 자격 증명이 관리자 자격 증명으로 설정되며 운영 체제 배포가 완료될 때까지 서버와의 추가 통신에 사용됩니다. 운영 체제가 배포된 후에는 연결된 호스트 자격 증명 프로필에 제공된 iDRAC 자격 증명이 설정됩니다.

타겟 시스템에서 자동 검색을 수동으로 활성화하려면 12세대 이후의 PowerEdge 서버에서 다음 단계를 수행합니다.

1. 타겟 시스템에서 초기 부팅 중에 F2 키를 누릅니다.
2. **iDRAC 설정** > **사용자 구성**으로 이동한 다음 루트 사용자를 비활성화합니다. 루트 사용자를 비활성화할 때에는 해당 iDRAC 주소에서 관리자 권한이 있고 활성 상태인 다른 사용자가 없어야 합니다.
3. **뒤로**를 클릭하고 **원격 활성화**를 클릭합니다.
4. **자동 검색 활성화**를 **활성화**로 설정하고 **프로비저닝 서버**를 OMIVV의 IP 주소로 설정합니다.
5. 설정을 저장합니다.
   서버는 다음 서버 부팅 때 자동으로 검색됩니다. 성공적인 자동 검색 후에 루트 사용자가 활성화되고 **자동 검색 활성화** 플래그가 자동으로 비활성화됩니다.

운영 체제 미설치 서버 수동 검색

검색에 관리자 권한이 있는 iDRAC 사용자가 사용되는지 확인합니다.

OMIVV를 사용하면 IPv4 범위를 기준으로 서버를 수동으로 검색할 수 있습니다. IPv4 기반 범위 검색 방법을 사용하여 단일 IP 또는 IP 그룹을 검색할 수 있습니다.

운영 체제 미설치 서버가 추가되면 **운영 체제 미설치 서버** 페이지의 서버 목록에 표시됩니다.

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **배포** > **검색**을 클릭합니다.
   운영 체제 미설치 서버 검색 페이지가 표시됩니다.
2. **운영 체제 미설치 서버 검색** 페이지에서 다음 작업을 수행합니다.
   a. **작업 이름 검색** 필드에 작업 이름을 입력합니다.
   b. 작업 설명을 입력합니다(선택 사항).
   c. IP 범위를 입력하려면 **범위 데이터 추가**를 클릭합니다.

      각 검색 작업에 여러 범위를 언급할 수 있습니다. 최대 1024개의 IP가 지원됩니다. 범위에서 구성할 수 있는 최대 IP 수는 256개입니다.

      한 범위의 제외 목록에 특정 IP 세트를 추가한 다음 다른 범위의 포함 목록에 동일한 IP를 추가할 때 포함된 IP가 우선합니다.
   d. **시작 IP**를 입력합니다.
      시작 IP는 IPv4 주소 형식이어야 합니다.
   e. **종료 IP**를 입력합니다.
      종료 IP는 IP의 마지막 옥텟이고 시작 IP보다 커야 합니다.
   f. **제외 목록**을 입력합니다.
      제외 목록은 목록에서 제외할 IP 목록입니다.

      제외 목록에 입력한 값은 **시작 IP** 및 **종료 IP** 범위 내에 있어야 합니다. 값은 쉼표로 구분해야 하며, 각 값은 마지막 옥텟 값이거나 - 로 구분된 마지막 옥텟 값의 범위일 수 있습니다.

      예:

      100.100.100.25~100.100.100.30과 100.100.100.40~100.100.100.45를 제외한 100.100.100.1~100.100.100.50 사이의 모든 IP를 검색하려면 **시작 IP**, **종료 IP** 및 **제외 목록**에 다음을 입력합니다.

      시작 IP: 100.100.100.1

      종료 IP: 50

      제외 목록: 25~30, 40~45
   g. **배포 자격 증명** 페이지에 입력한 iDRAC 자격 증명을 사용하려면 **배포 자격 증명 사용** 확인란을 선택합니다.

배포 자격 증명에 대한 자세한 내용은 배포 자격 증명 구성 페이지 77을(를) 참조하십시오.

h. 배포 자격 증명이 설정되지 않은 경우 사용자 이름과 암호를 입력합니다.

기본적으로 배포 자격 증명이 설정되어 있습니다. 배포 자격 증명 이외의 다른 자격 증명을 사용하려면 iDRAC 사용자 이름 및 암호를 입력합니다. 각 범위에 대해 별도의 자격 증명 세트를 가질 수 있습니다.

사용자 이름 길이는 1~16자 범위여야 합니다. 특수 문자 /, \, ~, '는 지원되지 않습니다.

암호는 최대 42자까지 입력할 수 있습니다.

3. 다음 옵션 중에서 선택합니다.
   - **지금 실행** - 작업을 실행하면 지정된 범위 내에서 언급된 모든 IP가 검색됩니다.
   - **나중에 실행** - 나중에 실행되도록 작업을 예약하면 지정된 범위 내의 IP가 검색됩니다.
4. **적용**을 클릭합니다.
   검색 작업의 상태가 **검색 작업** 페이지에 표시됩니다. 자세한 내용은 검색 작업 페이지 69을(를) 참조하십시오.

운영 체제 미설치 서버 제거

자동으로 검색되거나 수동으로 추가된 서버를 수동으로 제거할 수 있습니다.

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **배포** > **삭제**를 클릭합니다.
2. 운영 체제 미설치 서버를 선택한 다음 **확인** 을 클릭합니다.

운영 체제 미설치 서버 새로 고침

새로 고침 작업은 iDRAC에 연결하고 기본 인벤토리를 수집하여 운영 체제 미설치 서버를 다시 검색합니다.

노트: "구성된" 운영 체제 미설치 서버에서 새로 고침 작업을 수행하는 경우 새로 고침 작업에서 서버를 다시 검색하기 때문에 서버 상태가 "구성되지 않은" 상태로 변경됩니다.

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **배포** > **새로 고침**을 클릭합니다.
2. **운영 체제 미설치 서버 새로 고침** 페이지에서 서버를 선택하고 **확인**을 클릭합니다.
   운영 체제 미설치 서버의 데이터 새로 고침은 몇 분 정도 걸릴 수 있습니다. 작업이 진행되는 동안 **운영 체제 미설치 서버 새로 고침** 페이지를 닫을 수 있습니다. 다시 검색 프로세스가 백그라운드에서 진행됩니다. 다시 검색된 서버가 **운영 체제 미설치 서버** 페이지에 표시됩니다.

iDRAC 라이선스 구입 또는 갱신

운영 체제 미설치 서버의 상태는 호환되는 iDRAC 라이선스가 없는 경우 비준수로 표시됩니다. 표에 iDRAC 라이선스 상태가 표시되어 있습니다. iDRAC 라이선스에 대한 자세한 내용을 보려면 비준수 운영 체제 미설치 서버를 선택합니다.

1. iDRAC 라이선스를 갱신하려면 OMIVV 홈 페이지에서 **규정 준수 및 배포** > **배포**를 클릭합니다.
2. iDRAC 라이선스가 규정을 준수하지 않는 운영 체제 미설치 서버를 선택하고 **IDRAC 라이선스 구매/갱신**을 클릭합니다.
3. Dell Digital Locker에 로그인하여 라이선스를 업데이트하거나 새 iDRAC 라이선스를 구입합니다.
4. iDRAC 라이선스를 설치한 후 **새로 고침**을 클릭합니다.

9

배포 프로필 관리

시스템 프로필

시스템 프로필은 iDRAC, BIOS, RAID, 이벤트 필터, FC 및 NIC의 구성 요소 수준 설정 및 구성을 캡처합니다. 운영 체제 미설치 서버에 운영 체제를 배포하는 동안 이러한 구성을 다른 동일한 서버에 적용할 수 있습니다. 시스템 프로필을 클러스터 프로필에 사용하여 구성에 대한 기준을 유지할 수도 있습니다.

사전 요구 사항

시스템 프로필을 생성하거나 편집하기 전에 다음을 확인하십시오.

- CSIOR 기능은 참조 서버에서 활성화됩니다. iDRAC에서 반환된 데이터를 최신 상태로 유지하려면 CSIOR을 활성화한 후에 참조 서버를 재시작해야 합니다.
- vCenter에서 관리되는 각 참조 호스트에 대해 인벤토리가 성공적으로 수행되었습니다.
- 운영 체제 미설치 서버에 최소한으로 요구되는 BIOS 및 펌웨어 버전이 설치되어 있습니다. 자세한 내용은 지원 사이트에서 *OMIVV 호환성 매트릭스*를 참조하십시오.
- 참조 서버 및 대상 서버는 동일합니다(동일한 모델, 동일한 하드웨어 구성 및 동일한 펌웨어 수준).
- 하드웨어(예: FC, NIC 및 RAID 컨트롤러)가 참조 서버 및 대상 서버의 동일한 슬롯에 있습니다.
- 기본 선택에서 특성을 제외하거나 포함하기 전에 특성 이름 위에 커서를 올려서 특성 세부 정보를 이해하십시오.
- iDRAC를 검색하는 데 사용되는 iDRAC 사용자는 시스템 프로필에서 iDRAC 사용자를 구성할 때 선택됩니다.

  노트: 운영 체제 미설치 검색에 사용되는 iDRAC 사용자와 연결된 특성을 지우지 마십시오. 그렇지 않으면 시스템 프로필 배포 작업이 실패합니다.
- iDRAC를 검색하는 데 사용된 iDRAC 사용자의 사용자 이름은 변경하지 않습니다. 이로 인해 iDRAC에 대한 연결 문제가 발생하여 시스템 프로필 배포 작업에 실패하고 특성이 적용되지 않습니다.

시스템 프로필을 생성하기 전에 필요한 경우 참조 서버 특성과 값을 구성하는 것이 좋습니다. 필요한 모든 타겟 호스트에 참조 특성 및 값을 적용합니다.

시스템 프로필은 랙 서버(동일함)에서 성공적으로 작동하지만 모듈형 서버에서는 제한사항이 거의 없는 프로필을 적용하는 동안 정확한 인스턴스(FQDD)를 검색합니다. 예를 들어 FC640의 경우, 한 모듈형 서버에서 생성된 시스템 프로필은 NIC 레벨 제한사항으로 인해 동일한 FX 섀시에 있는 다른 모듈형 서버에는 적용할 수 없습니다. 이 경우 섀시의 각 슬롯에서 참조 시스템 프로필을 사용하는 것이 좋습니다. 해당 슬롯에 대해서만 섀시에 이러한 시스템 프로필을 적용합니다.

노트: 시스템 프로필은 부팅 옵션의 활성화 및 비활성화를 지원하지 않습니다.

노트:

- 시스템 프로필을 사용하는 동안에는 Enterprise 라이선스를 사용하여 시스템 프로필을 내보내고 Express 라이선스를 사용하여 동일한 시스템 프로필을 서버로 가져올 수 없습니다.
- iDRAC9 펌웨어 3.00.00.00의 Express 라이선스를 사용하여 시스템 프로필을 가져올 수 없습니다. Enterprise 라이선스가 있어야 합니다.

시스템 프로필 생성

시스템 프로필을 만들거나 편집하려면 Google Chrome을 사용하는 것이 좋습니다.

슬림라인 케이블을 사용하여 HBA, BOSS(Boot Optimized Storage Subsystem) 및 PERC가 연결된 PowerEdge R6515, R7515, R65125, R7525 및 C6515 서버입니다. iDRAC 버전이 4.30.30.30 이하인 OMIVV에서 생성된 시스템 프로필은 iDRAC 4.30.30.30 이상 버전에 사용할 수 없습니다. iDRAC 4.30.30.30 이상으로 새 시스템 프로필을 만들고 필요한 경우 사용합니다.

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **프로필** > **시스템 프로필** > **새 프로필 생성**을 클릭합니다.
2. 마법사의 **시스템 프로필 생성** 페이지에서 지침을 읽고 **시작하기**를 클릭합니다.
3. **이름 및 설명** 페이지에서 다음을 수행합니다.

a. 프로필 이름과 설명을 입력합니다. 설명 필드는 선택적인 필드입니다.
b. 다음 시스템 프로필 유형 중에서 선택합니다.
   - **기본** - iDRAC, BIOS, RAID, NIC 및 FC에 대한 특성의 최소 집합을 표시합니다.
   - **고급** - iDRAC, BIOS, RAID, NIC, FC 및 EventFilters에 대한 특성을 모두 표시합니다.

4. 호스트 또는 운영 체제 미설치인 참조 서버를 선택하려면 **참조 서버** 페이지에서 **선택**을 클릭합니다.
   다음과 같은 이유로 인해 서버 선택이 비활성화될 수 있습니다.
   - 서버가 비준수 호스트 또는 비준수 운영 체제 미설치 서버입니다.
   - 배포 작업이 예약되어 있거나 서버에서 실행 중입니다.
   - 서버는 섀시 자격 증명 프로필을 사용하여 관리됩니다.

   추출 확인 대화 상자가 표시됩니다.
5. 참조 서버에서 시스템 구성을 추출하려면 **확인**을 클릭합니다.
   참조 서버에서 시스템 구성을 추출하는 데 몇 분 정도 걸릴 수 있습니다.
6. 참조 서버 세부 정보를 검토하고 **다음**을 클릭합니다.
   - **참조 서버 선택** 페이지에서 참조 서버를 변경하려면 **찾아보기**를 클릭합니다.

     참조 서버가 운영 체제 미설치 유형인 경우 해당 iDRAC IP만 표시됩니다. 참조 서버 자체가 호스트 서버인 경우 iDRAC 및 호스트(FQDN) IP가 모두 표시됩니다.

   프로필 설정 페이지가 표시됩니다.
7. **프로필 설정** 페이지에서 참조 서버의 구성을 기반으로 iDRAC, BIOS, RAID, NIC, CNA, FCoE 및 EvenFilters와 같은 구성 요소의 프로필 설정을 보거나 수정할 수 있습니다.
   기본적으로 플랫폼별 특성 및 읽기 전용 특성은 나열되지 않습니다. 플랫폼별 특성에 대한 자세한 내용은 시스템별 특성 페이지 155을 참조하십시오.
   의사 특성은 시스템 프로필에 표시되지 않습니다. 자세한 내용은 서버 구성 XML 파일 문서를 참조하십시오.
   기본으로 선택된 특성 이외의 특성을 선택하기 전에 특성, 종속성 및 기타 세부 정보의 특성을 확인하십시오.
   기본으로 선택된 특성 이외의 특성을 선택하면 다음 메시지가 표시됩니다.
   이러한 특성은 다른 종속 특성에 영향을 미치거나 본질적으로 파괴적이거나 서버 ID를 해소하거나 대상 서버의 보안에 영향을 미칠 수 있습니다.

   노트: 12세대 및 13세대 PowerEdge 서버의 경우 일부 특성이 OMIVV에 종속성을 적절하게 매핑하지 못할 수 있습니다. 예를 들어 **시스템 BIOS 설정**에서 시스템 프로필을 **맞춤 구성**으로 설정하지 않는 한 BIOS의 메모리 작동 전압 구성 요소는 읽기 전용입니다.

   a. 각 구성 요소를 확장하여 **인스턴스**, **특성 이름**, **값**, **파괴적**, **종속성** 및 **그룹**과 같은 설정 옵션을 봅니다.
      종속성 텍스트를 사용할 수 없으면 빈 필드가 표시됩니다.
      노트: **검색** 필드를 사용하여 **값**을 제외한 모든 열에 특정한 데이터로 필터링할 수 있습니다.
   b. 빨간색 느낌표로 표시된 특성은 값을 반드시 설정해야 합니다. 이 옵션은 유효한 사용자 이름이 있는 iDRAC 사용 가능 사용자에 대해서만 사용할 수 있습니다.
8. **다음**을 클릭합니다.
   요약 페이지에 시스템 구성의 특성 통계와 프로필 세부 정보에 관한 정보가 표시됩니다.
   총 특성 수, 활성화된 총 특성 수 및 총 파괴적 특성 수가 특성 통계에 표시됩니다.
9. **마침**을 클릭합니다.
   저장된 프로필이 **시스템 프로필** 페이지에 표시됩니다.
   OMIVV가 작동하기 위해 일부 시스템 프로필 특성은 무시됩니다. 맞춤 구성 특성에 대한 자세한 내용은 사용자 지정 특성 페이지 160을 참조하십시오. 시스템 프로필 구성 템플릿, 특성 및 워크플로에 대한 자세한 내용은 추가 정보 페이지 159를 참조하십시오.

시스템 프로필 편집

시스템 프로필을 만들거나 편집하려면 Google Chrome을 사용하는 것이 좋습니다.

1. **시스템 프로필 생성** 페이지에서 프로필을 선택하고 **편집**을 클릭합니다.
2. **이름 및 설명** 페이지에서 프로필 이름 및 설명을 변경합니다. 설명은 선택 사항입니다.

노트: 기본 또는 고급 시스템 프로필을 생성한 후에는 프로필을 수정할 수 없습니다.

3. 호스트 또는 운영 체제 미설치인 참조 서버를 변경하려면 **참조 서버** 페이지에서 **선택**을 클릭합니다.
   다음과 같은 이유로 인해 서버 선택이 비활성화될 수 있습니다.
   - 서버가 비준수 호스트 또는 운영 체제 미설치 서버입니다.
   - 배포 작업이 예약되어 있거나 서버에서 실행 중입니다.
   - 서버는 섀시 자격 증명 프로필을 사용하여 관리됩니다.

   추출 확인 대화 상자가 표시됩니다.
4. 참조 서버에서 시스템 구성을 추출하려면 **확인**을 클릭합니다.
   참조 서버에서 시스템 구성을 추출하는 데 몇 분 정도 걸릴 수 있습니다.
5. 참조 서버 세부 정보를 검토하고 **다음**을 클릭합니다.
   - **참조 서버 선택** 페이지에서 참조 서버를 변경하려면 **찾아보기**를 클릭합니다. 참조 서버가 운영 체제 미설치 유형인 경우 해당 iDRAC IP만 표시됩니다. 참조 서버 자체가 호스트 서버인 경우 iDRAC 및 호스트(FQDN) IP가 모두 표시됩니다.

   프로필 설정 페이지가 표시됩니다.
6. **프로필 설정** 페이지에서 참조 서버의 구성을 기반으로 iDRAC, BIOS, RAID, NIC, CNA, FCoE 및 EvenFilters와 같은 구성 요소의 프로필 설정을 보거나 수정할 수 있습니다.
   기본적으로 플랫폼별 특성 및 읽기 전용 특성은 나열되지 않습니다. 플랫폼별 특성에 대한 자세한 내용은 시스템별 특성 페이지 155을 참조하십시오.

   몇 가지 속성을 수정하려고 할 경우 다음 경고 메시지가 표시됩니다.

   이러한 특성은 다른 종속 특성에 영향을 미치거나 본질적으로 파괴적이거나 서버 ID를 해소하거나 대상 서버의 보안에 영향을 미칠 수 있습니다.

   노트: 시스템 프로필을 편집한 후 운영 체제 미설치 서버를 검색하는 데 사용되는 iDRAC 사용자의 암호가 수정되면 업데이트된 암호가 무시됩니다. 업데이트된 암호는 운영 체제 미설치 서버를 검색하는 데 사용되는 암호로 대체됩니다.

   a. 각 구성 요소를 확장하여 인스턴스, 특성 이름, 값, 파괴적, 종속성 및 그룹과 같은 설정 옵션을 봅니다.
      종속성 텍스트를 사용할 수 없으면 빈 필드가 표시됩니다.
   b. 빨간색 느낌표로 표시된 특성은 값을 반드시 설정해야 합니다. 이 옵션은 유효한 사용자 이름이 있는 iDRAC 사용 가능 사용자에 대해서만 사용할 수 있습니다.
7. **다음**을 클릭합니다.
   요약 페이지에 시스템 구성의 특성 통계와 프로필 세부 정보에 관한 정보가 표시됩니다.

   총 특성 수, 활성화된 총 특성 수 및 총 파괴적 특성 수가 특성 통계에 표시됩니다.
8. **마침**을 클릭합니다.
   저장된 프로필이 **시스템 프로필** 페이지에 표시됩니다.

   OMIVV가 작동하기 위해 일부 시스템 프로필 특성은 무시됩니다. 맞춤 구성 특성에 대한 자세한 내용은 사용자 지정 특성 페이지 160을 참조하십시오. 시스템 프로필 구성 템플릿, 특성 및 워크플로에 대한 자세한 내용은 추가 정보 페이지 159를 참조하십시오.

시스템 프로필 보기

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **시스템 프로필**을 클릭합니다.
   모든 시스템 프로필이 다음 정보와 함께 표에 표시됩니다.
   - **프로필 이름** – 시스템 프로필의 이름입니다.
   - **설명** – 프로필 설명입니다.
   - **참조 서버** – 시스템 구성 세부 정보가 추출되는 iDRAC IP입니다.
   - **서버 모델** – 참조 서버의 모델 이름입니다.
2. 마법사에서 열 이름을 제거하거나 추가하려면 ▮을 클릭합니다.
3. 시스템 프로필 정보를 내보내려면 을 클릭합니다.

시스템 프로필 삭제

실행 중인 배포 작업의 일부인 시스템 프로필을 삭제하면 삭제 작업에 오류가 발생할 수 있습니다.

1. **시스템 프로필** 페이지에서 시스템 프로필을 선택하고 **삭제**를 클릭합니다.
2. 삭제 확인 대화 상자에서 **삭제**를 클릭합니다.

ISO 프로필

ISO 프로필에는 NFS 또는 CIFS 폴더에 저장된 Dell EMC 맞춤 구성 ESXi ISO 이미지 파일의 폴더 경로가 포함되어 있습니다. ISO 프로필은 배포 마법사에서 사용됩니다.

ISO 프로필 생성

ISO 프로필은 NFS 또는 CIFS에 있는 Dell EMC 맞춤 구성 ISO 파일 위치를 필요로 합니다.

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **프로필** > **ISO 프로필** > **새 프로필 생성**을 클릭합니다.
2. 마법사의 **ISO 프로필** 페이지에서 지침을 읽고 **시작하기**를 클릭합니다.
3. **프로필 이름 및 설명** 페이지에서 프로필 이름 및 설명을 입력합니다. 설명은 선택적인 필드입니다.
4. **설치 소스(ISO)** 상자에 ISO 파일 위치(NFS 또는 CIFS)를 입력합니다.
   OMIVV에서는 SMB(Server Message Block) 버전 1.0과 SMB 버전 2.0 기반 CIFS 공유만 지원됩니다.
   a. CIFS를 사용하는 경우 자격 증명을 입력합니다.
5. **ESXi 버전** 드롭다운 목록에서 ESXi 버전을 선택합니다.
   적절한 설치 부팅 스크립트가 사용되도록 올바른 ESXi 버전을 선택합니다. 잘못된 ESXi 버전을 선택하는 경우 배포에 실패할 수 있습니다.
6. ISO 파일 경로 접근성 및 자격 증명을 확인하려면 **테스트 시작**을 클릭합니다.
   테스트 결과가 표시됩니다.
7. **마침**을 클릭합니다.

ISO 프로필 편집

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **프로필** > **ISO 프로필**을 클릭합니다.
2. ISO 프로필을 선택하고 **편집**을 클릭합니다.
3. **프로필 이름 및 설명** 페이지에서 프로필 이름 및 설명을 편집합니다. 설명은 선택적인 필드입니다.
4. **설치 소스(ISO)** 상자의 ISO 파일 위치(NFS 또는 CIFS)를 변경합니다.
   OMIVV에서는 SMB(Server Message Block) 버전 1.0과 SMB 버전 2.0 기반 CIFS 공유만 지원됩니다.
   a. CIFS를 사용하는 경우 자격 증명을 입력합니다.
5. **ESXi 버전** 드롭다운 목록에서 ESXi 버전을 선택합니다.
   적절한 설치 부팅 스크립트가 사용되도록 올바른 ESXi 버전을 선택합니다. 잘못된 ESXi 버전을 선택하는 경우 배포가 실패할 수 있습니다.
6. ISO 파일 경로 및 인증을 확인하려면 **테스트 시작**을 클릭합니다.
   테스트 결과가 표시됩니다.
7. **마침**을 클릭합니다.

ISO 프로필 보기

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **ISO 프로필**을 클릭합니다.
   모든 ISO 프로필이 다음 정보와 함께 표에 표시됩니다.
   - **프로필 이름** – 프로필 이름입니다.
   - **설명** – 프로필 설명입니다.
   - **설치 소스** – ISO 파일 위치(NFS 또는 CIFS)입니다.
   - **ESXi 기본 버전** – ESXi 기본 버전입니다.

2. 마법사에서 열 이름을 제거하거나 추가하려면 을 클릭하십시오.
3. ISO 프로필 정보를 내보내려면 을 클릭하십시오.

ISO 프로필 삭제

실행 중인 배포 작업의 일부인 ISO 프로필을 삭제하면 배포 작업에 오류가 발생합니다.

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **프로필** > **ISO 프로필**을 클릭합니다.
2. ISO 프로필을 선택하고 **삭제**를 클릭합니다.
3. 확인 대화 상자에서 **삭제**를 클릭합니다.

맞춤 구성 Dell EMC ISO 이미지 다운로드

배포하려면 모든 Dell EMC 드라이버가 포함되어 있는 맞춤 구성 ESXi 이미지가 필요합니다.

1. 브라우저를 열고 **support.dell.com**으로 이동합니다.
2. **모든 제품 찾아보기** > **서버** > **PowerEdge**를 클릭합니다.
3. PowerEdge 서버 모델을 클릭합니다.
4. 서버 모델의 **드라이버 및 다운로드** 페이지를 클릭합니다.
5. **운영 체제** 드롭다운에서 ESXi 버전을 선택합니다.
6. **범주** 드롭다운 메뉴에서 **엔터프라이즈 솔루션**을 선택합니다.
7. **엔터프라이즈 솔루션** 목록에서 필요한 ISO 버전을 선택하고 **다운로드**를 클릭합니다.

10

시스템 프로필 및 ISO 프로필 배포

시스템 프로필 및 ISO 프로필을 배포하려면 모든 서버가 사용자 환경에서 다음 요구 사항을 충족하는지 확인합니다.

- 모든 서버가 **시스템 프로필 및 ISO 프로필 배포** 마법사에 표시됩니다.
- *OpenManage Integration for VMware vCenter 호환성 매트릭스*에 언급된 특정 하드웨어 지원 정보를 확인하십시오.
- 지원되는 최소 버전의 iDRAC 펌웨어 및 BIOS를 사용할 수 있는지 확인하십시오.

  특정 펌웨어 지원 정보의 경우 *OpenManage Integration for VMware vCenter 호환성 매트릭스*를 확인하십시오.
- IDSDM 스토리지 사양을 사용할 수 있습니다.

  IDSDM의 스토리지 사양을 알아보려면 VMware 설명서를 참조하십시오.
- OMIVV로 OS를 배포하기 전에 BIOS에서 IDSDM이 활성화되었습니다.

  OMIVV를 사용하면 IDSDM 또는 로컬 하드 드라이브 또는 BOSS 카드에서 배포할 수 있습니다.
- vCenter, OMIVV 및 iDRAC이 서로 다른 네트워크에 연결된 경우 vCenter, OMIVV 및 iDRAC 네트워크 사이에 라우트가 있습니다.

  이 요구 사항은 OMIVV 어플라이언스가 두 네트워크 인터페이스 컨트롤러로 구성되지 않은 경우에만 해당합니다.
- CSIOR(Collect System Inventory on Reboot)이 활성화되었습니다.
- 검색된 데이터는 자동 또는 수동 검색을 시작하기 전에 서버에서 하드 재부팅을 수행하여 최신 상태를 유지합니다.
- 운영 체제 미설치 서버를 자동 검색하는 경우 공장에서 미리 구성된 자동 검색 또는 핸드셰이크 옵션이 있는 Dell EMC 서버를 주문합니다. 서버에 이러한 옵션이 미리 구성되어 있지 않을 경우 OMIVV IP 주소를 수동으로 입력하거나 로컬 네트워크를 구성하여 이 정보를 제공하십시오.
- 하드웨어 구성에 OMIVV를 사용하지 않은 경우 운영 체제를 배포하기 전에 다음 조건이 충족되는지 확인해야 합니다.
  - BIOS에서 VT(가상화 기술) 플래그를 활성화합니다.
  - 가상 드라이버, IDSDM 및 BOSS는 첫 번째 부팅 디스크로 설정됩니다.
- 하드웨어 구성에 OMIVV가 사용되는 경우 BIOS 구성이 시스템 프로필에 속하지 않아도 VT에 대한 BIOS 설정이 자동으로 활성화되어 있는지 확인합니다. 가상 드라이브가 타겟 시스템에 구성되어 있지 않으면 Express 또는 Clone RAID 구성이 필요합니다.
- 모든 Dell EMC 드라이버를 포함하는 맞춤 구성 ESXi 이미지를 배포에 사용할 수 있습니다.

  support.dell.com에서 이용 가능한 **드라이버 및 다운로드** 섹션에서 올바른 이미지를 다운로드합니다. 맞춤 구성 Dell EMC ISO 이미지 다운로드에 대한 자세한 내용은 맞춤 구성 Dell EMC ISO 이미지 다운로드 페이지 57을(를) 참조하십시오.
- 배포 프로세스 중에 OMIVV가 액세스할 수 있는 CIFS 또는 NFS 공유 위치에 맞춤 구성 이미지를 저장합니다.

  이 릴리스에서 지원되는 ESXi 버전의 최신 목록은 *OpenManage Integration for VMware vCenter 호환성 매트릭스*를 참조하십시오.

  이중 NIC가 있는 호스트 배포에 적용할 수 있는 사항은 다음과 같습니다.

- 동일한 네트워크 또는 두 개의 별도 네트워크에 호스트의 iDRAC 및 vCenter 관리 NIC가 있을 수 있습니다.
- ISO 이미지를 어떤 네트워크에도 저장할 수 있습니다.
- 환경에 적합한 올바른 vCenter 네트워크 및 OMIVV 네트워크를 선택해야 합니다. OS 배포 마법사에는 양쪽 OMIVV 네트워크가 모두 표시됩니다.

배포 체크리스트

시스템 프로필 및 ISO 프로필을 배포하기 전에 다음을 사용할 수 있는지 확인합니다.

- 호스트 자격 증명 프로필

  호스트 자격 증명 프로필을 생성하려면 **생성**을 클릭합니다. 호스트 자격 증명 프로필 생성에 대한 자세한 내용은 호스트 자격 증명 프로필 생성 페이지 35을(를) 참조하십시오.
- 운영 체제 미설치 서버

  운영 체제 미설치 서버를 검색하려면 **검색**을 클릭합니다. 운영 체제 미설치 서버 검색에 대한 자세한 내용은 운영 체제 미설치 서버 수동 검색 페이지 51을(를) 참조하십시오.

- 시스템 프로필

  시스템 프로필을 생성하려면 **생성**을 클릭합니다. 시스템 프로필 생성에 대한 자세한 내용은 시스템 프로필 생성 페이지 53을(를) 참조하십시오.

- ISO 프로필

  ISO 프로필을 생성하려면 **생성**을 클릭합니다. ISO 프로필 생성에 대한 자세한 내용은 ISO 프로필 생성 페이지 56을(를) 참조하십시오.

시스템 프로필 및 ISO 프로필 배포 마법사를 사용하여 다음을 수행할 수 있습니다.

- 시스템 프로필 배포

  자세한 내용은 시스템 프로필(하드웨어 구성) 배포 페이지 59을(를) 참조하십시오.

- ISO 프로필 배포

  자세한 내용은 ISO 프로필 배포(ESXi 설치) 페이지 59을(를) 참조하십시오.

- 시스템 프로필 및 ISO 프로필 배포

  자세한 내용은 시스템 프로필 및 ISO 프로필 배포 페이지 61을(를) 참조하십시오.

시스템 프로필(하드웨어 구성) 배포

1. 배포 마법사를 실행하려면 **규정 준수 및 배포** > **배포** > **배포**로 이동합니다.
2. 배포 마법사의 **시스템 프로필 및 ISO 프로필 배포 체크리스트** 페이지에서 배포 체크리스트를 확인한 다음 **시작하기**를 클릭합니다.

   규정을 준수하는 운영 체제 미설치 서버에서만 배포를 수행할 수 있습니다. 자세한 내용은 운영 체제 미설치 서버 보기 페이지 49을(를) 참조하십시오.
3. **서버 선택** 페이지에서 하나 이상의 서버를 선택합니다.
   배포 옵션 선택 페이지가 표시됩니다.
4. **배포 옵션 선택** 페이지에서 **시스템 프로필(하드웨어 구성)**을 선택합니다.
5. **시스템 프로필** 드롭다운 메뉴에서 적절한 시스템 프로필을 선택한 후 **다음**을 클릭합니다.

   기본 및 고급 시스템 프로필 유형의 경우 시스템 프로필 이름이 Basic_<system profile name>, Advanced_<system profile name> 형식으로 표시됩니다.

   구성 미리 보기 작업은 선택한 호스트와 선택한 시스템 프로필의 호환성을 비교하거나 확인합니다.
6. iDRAC에서 미리 보기 작업을 생성하려면 **구성 미리 보기** 페이지에서 iDRAC IP를 선택한 다음 **미리 보기**를 클릭합니다. 구성 미리 보기는 선택적 작업입니다.
   시스템 프로필 미리 보기 작업을 완료하는 데 몇 분이 걸릴 수 있습니다. 비교 상태가 **결과** 열에 표시됩니다.

   다음은 비교 결과입니다.

   - **완료됨** - 미리 보기 작업이 성공적으로 실행되었습니다. 비교 결과에 대한 자세한 내용을 보려면 **세부 정보** 열에서 **세부 정보 보기**를 클릭하십시오.
   - **완료되지 않음** - iDRAC에서 미리 보기 작업이 성공적으로 실행되지 않았습니다. 필요한 경우 iDRAC에 액세스할 수 있는지 확인하고 iDRAC을 재설정합니다. 작업에 대한 자세한 내용은 OMIVV 로그 및 iDRAC 콘솔의 로그를 참조하십시오.
7. **배포 작업 예약** 페이지에서 다음을 수행합니다.
   a. 배포 작업 이름과 설명을 입력합니다. 설명은 선택적인 필드입니다.
   b. 배포 작업을 즉시 실행하려면 **지금 실행**을 클릭합니다.
   c. 나중에 실행할 작업을 예약하려면 **나중에 예약**을 클릭한 다음 날짜와 시간을 선택합니다.
   d. **작업 제출 후 작업 페이지로 이동** 확인란을 선택합니다.
   작업 페이지에서 작업 상태를 추적할 수 있습니다. 자세한 내용은 배포 작업 페이지 68을(를) 참조하십시오.
8. **마침**을 클릭합니다.

ISO 프로필 배포(ESXi 설치)

규정을 준수하는 운영 체제 미설치 서버에서만 배포를 수행할 수 있습니다. 자세한 내용은 운영 체제 미설치 서버 보기 페이지 49을(를) 참조하십시오.

1. 배포 마법사를 실행하려면 **규정 준수 및 배포** > **배포** > **배포**로 이동합니다.

2. 배포 마법사의 **시스템 프로필 및 ISO 프로필 배포 체크리스트** 페이지에서 배포 체크리스트를 확인한 다음 **시작하기**를 클릭합니다.
3. **서버 선택** 페이지에서 하나 이상의 서버를 선택합니다.
   배포 옵션 선택 페이지가 표시됩니다.
4. **배포 옵션 선택** 페이지에서 **ISO 프로필(ESXi 설치)**을 선택합니다.
5. **vCenter 이름** 드롭다운 메뉴에서 vCenter의 인스턴스를 선택합니다.
6. vCenter 대상 컨테이너를 선택하려면 **찾아보기**를 클릭하고 운영 체제를 배포하려는 적절한 데이터 센터 또는 클러스터를 선택합니다.
7. **ISO 프로필** 드롭다운 메뉴에서 적절한 ISO 프로필을 선택합니다.
8. **설치 대상** 아래에서 다음 옵션 중 하나를 선택합니다.
   - **첫 번째 부팅 디스크** - 하드 드라이브, SSD(Solid State Drive) 또는 RAID 컨트롤러에 의해 생성된 가상 드라이브에 운영 체제를 배포합니다.
   - **IDSDM(Internal Dual SD Module)** - IDSDM에 운영 체제를 배포합니다. 선택된 서버 중 하나 이상에서 IDSDM을 사용할 수 있는 경우 내장 이중 SD 모듈 옵션이 활성화됩니다. 그렇지 않을 경우에는 **첫 번째 부팅 디스크** 옵션만 사용할 수 있습니다.
     - 선택한 서버 중 하나라도 IDSDM 또는 BOSS 모듈을 지원하지 않거나 배포 중에 IDSDM 또는 BOSS가 서버에 설치되지 않은 경우 해당 서버의 배포 작업을 건너뜁니다.

       서버의 첫 번째 부팅 디스크에 운영 체제를 배포하려면 **사용 가능한 내부 이중 SD 모듈이 없는 서버의 첫 번째 부팅 디스크에 하이퍼바이저 배포** 확인란을 선택합니다.

     노트: 첫 번째 부팅 디스크 설치 대상이 BIOS 하드 드라이브 순서 또는 UEFI 부트 순서의 첫 번째 항목과 일치하지 않습니다. 이 옵션은 ESXi 사전 OS 환경에서 식별되는 첫 번째 디스크에 운영 체제를 배포합니다. **첫 번째 부팅 디스크** 옵션을 선택한 경우 하드 디스크 페일오버 또는 부트 순서 재시도 옵션이 활성화되어 있는지 확인합니다.
   - **BOSS** - BOSS 카드에 운영 체제를 배포합니다. 선택된 서버 중 하나 이상에서 BOSS를 사용할 수 있는 경우 BOSS 옵션이 활성화됩니다. 그렇지 않을 경우에는 **첫 번째 부팅 디스크** 옵션만 사용할 수 있습니다.

     OMIVV를 사용하여 BOSS 컨트롤러에 운영 체제를 배포하는 경우 BOSS VD 구성과 함께 참조 서버에서 시스템 프로필을 캡처하고 대상 서버에 유사한 구성의 BOSS가 있어야 합니다. VD 생성에 대한 자세한 내용은 www.dell.com/support의 *Dell EMC 부팅 최적화 서버 스토리지-S1 사용자 가이드*를 참조하십시오.

9. **호스트 자격 증명 프로필 선택** 페이지에서 다음 작업을 수행합니다.
   a. 모든 호스트에 동일한 호스트 자격 증명 프로필을 사용하려면 **예**를 클릭한 후 다음 작업을 수행합니다.
      i. 드롭다운 메뉴에서 호스트 자격 증명 프로필을 선택합니다.
      ii. 암호를 입력합니다.

      배포 중에 루트 사용자에게 적용되는 사항은 다음과 같습니다.
      - ESXi 6.5 이하 버전의 경우 호스트 자격 증명 프로필에 입력된 암호가 사용됩니다.
      - ESXi 6.7 이상 버전의 경우 배포 마법사에서 입력한 암호가 사용됩니다.
      - ESXi 6.5 이하 버전의 경우 호스트 자격 증명 프로필에 암호가 입력되지 않으면, 배포 마법사에 입력된 암호가 사용됩니다. OS(Operating System) 배포 후 인벤토리가 성공적으로 실행되도록 호스트 자격 증명 프로필에서 ESXi 자격 증명을 업데이트합니다.

   b. 각 서버에 대한 개별 호스트 자격 증명 프로필을 선택하려면 **아니요**를 클릭한 후 다음 작업을 수행합니다.
      i. 드롭다운 메뉴에서 호스트 자격 증명 프로필을 선택합니다.
      ii. 루트 암호를 입력합니다. 입력한 암호를 보려면 눈 아이콘을 클릭합니다.

      암호 확인 옵션을 사용할 수 없으므로 올바른 암호를 입력했는지 확인하십시오.

   노트: 호스트 자격 증명 프로필에서 iDRAC 또는 ESXi에 AD 자격 증명을 사용하는 경우 이러한 프로필은 운영 체제 배포에 고려되지 않습니다.

   노트: 호스트 자격 증명 프로필에서는 운영 체제 미설치 검색에 사용되는 사용자를 연결하는 것이 좋습니다. 그렇지 않으면 운영 체제 배포 후 iDRAC에서 검색된 사용자가 비활성화됩니다.
10. **네트워크 설정 구성** 페이지에서 다음 작업을 수행합니다.
    a. 서버의 FQDN(Fully Qualified Host Name)을 입력합니다. 호스트 이름의 정규화된 도메인 이름은 필수입니다. FQDN에 *localhost*를 사용할 수 없습니다. FQDN은 호스트를 vCenter에 추가할 때 사용됩니다. FQDN에 대한 IP 주소를 확인하는 DNS 레코드를 생성합니다. 역방향 조회 요청을 지원하도록 DNS 서버를 구성합니다. 배포 작업 실행을 예약하려면 DHCP 예약 및 DNS 호스트 이름이 있고 확인되어야 합니다.

노트: vCenter가 FQDN을 사용하여 OMIVV에 등록된 경우 ESXi 호스트에서 DNS 확인을 사용하여 FQDN을 해결할 수 있는지 확인합니다.

b. 관리 네트워크에 사용되는 NIC를 선택합니다. NIC가 연결된 상태인지 확인합니다.

노트: OMIVV에 대한 네트워크 연결을 기반으로 관리 NIC를 선택해야 합니다. **모든 서버에 설정 적용** 옵션은 관리 NIC 선택에 적용할 수 없습니다.

c. vCenter에 액세스할 수 있는 OMIVV 네트워크 인스턴스를 선택합니다. 자세한 내용은 시스템 프로필 및 ISO 프로필 배포 페이지 58을(를) 참조하십시오.

d. 다음 네트워킹 옵션 중 하나를 선택합니다.

- 정적인 경우 기본 DNS 서버, 대체 DNS 서버, IP 주소, 서브넷 마스크 및 기본 게이트웨이를 입력합니다.
- **VLAN 사용** - VLAN ID를 입력하면, 이것이 배포 중에 운영 체제의 관리 인터페이스에 적용되고 모든 트래픽에 VLAN ID가 태깅됩니다. 서버 식별은 배포된 서버에 새 이름과 네트워크 식별을 할당합니다. 자세한 내용은 VLAN 지원 페이지 62을(를) 참조하십시오.
- **DHCP 사용** - 호스트를 vCenter에 추가하면 DHCP 할당 IP 주소가 사용됩니다. DHCP를 사용할 때는 선택된 NIC MAC 주소에 IP 예약을 사용하는 것이 좋습니다.

11. **배포 작업 예약** 페이지에서 다음을 수행합니다.
    a. 배포 작업 이름과 설명을 입력합니다.
    b. 배포 작업을 즉시 실행하려면 **지금 실행**을 클릭합니다.
    c. 나중에 실행할 작업을 예약하려면 **나중에 예약**을 클릭한 다음 날짜와 시간을 선택합니다.
    d. **작업 제출 후 작업 페이지로 이동** 확인란을 선택합니다.
    작업 페이지에서 작업 상태를 추적할 수 있습니다. 자세한 내용은 배포 작업 페이지 68을(를) 참조하십시오.
12. **마침**을 클릭합니다.

노트: 운영 체제 미설치 서버에서 운영 체제 배포를 수행한 후 OMIVV에서 모든 iDRAC 작업을 지웁니다.

이전 버전의 OMIVV로 예약된 ISO 프로필 배포 작업이 최신 버전의 OMIVV에서 유효하지 않습니다. 예약된 작업을 취소하고 필요에 따라 배포 작업을 만듭니다.

예약된 작업이 취소되지 않으면 배포 작업에 오류가 발생합니다. 이러한 경우 서버를 운영 체제 미설치로 검색하고 ISO 프로필 배포 작업을 만듭니다.

시스템 프로필 및 ISO 프로필 배포

규정을 준수하는 운영 체제 미설치 서버에서만 배포를 수행할 수 있습니다. 자세한 내용은 운영 체제 미설치 서버 보기 페이지 49을(를) 참조하십시오.

1. 배포 마법사를 실행하려면 **규정 준수 및 배포** > **배포** > **배포**로 이동합니다.
2. 배포 마법사의 **시스템 프로필 및 ISO 프로필 배포 체크리스트** 페이지에서 배포 체크리스트를 확인한 다음 **시작하기**를 클릭합니다.
3. **서버 선택** 페이지에서 하나 이상의 서버를 선택합니다.
   배포 옵션 선택 페이지가 표시됩니다.
4. **배포 옵션 선택** 페이지에서 **시스템 프로필(하드웨어 구성)** 및 **ISO 프로필(ESXi 설치)**을 선택합니다.
5. **vCenter 이름** 드롭다운 메뉴에서 vCenter의 인스턴스를 선택합니다.
6. vCenter 대상 컨테이너를 선택하려면 **찾아보기**를 클릭하고 운영 체제를 배포하려는 적절한 데이터 센터 또는 클러스터를 선택합니다.
7. 선택한 클러스터와 연결된 클러스터 프로필에 연결된 시스템 프로필을 사용하려면 **확인**을 클릭합니다.
   - 다른 시스템 프로필을 선택하려면 **다른 항목 선택**을 클릭합니다. 구성 규정 준수 변경 사항을 방지하기 위해 클러스터와 연결된 시스템 프로필을 선택하는 것이 좋습니다.
8. **ISO 프로필** 드롭다운 메뉴에서 적절한 ISO 프로필을 선택하고 **다음**을 클릭합니다.
9. iDRAC에서 미리 보기 작업을 생성하려면 **구성 미리 보기** 페이지에서 iDRAC IP를 선택한 다음 **미리 보기**를 클릭합니다. 구성 미리 보기는 선택적 작업입니다.
   시스템 프로필 미리 보기 작업을 완료하는 데 몇 분이 걸릴 수 있습니다. 비교 상태가 **결과** 열에 표시됩니다.

   다음은 비교 결과입니다.

   - **완료됨** - 미리 보기 작업이 성공적으로 실행되었습니다. 비교 결과에 대한 자세한 내용을 보려면 **세부 정보** 열에서 **세부 정보 보기**를 클릭하십시오.

- **완료되지 않음** - iDRAC에서 미리 보기 작업이 성공적으로 실행되지 않았습니다. 필요한 경우 iDRAC에 액세스할 수 있는지 확인하고 iDRAC을 재설정합니다. 작업에 대한 자세한 내용은 OMIVV 로그 및 iDRAC 콘솔의 로그를 참조하십시오.

10. ISO 프로필 배포(ESXi 설치) 페이지 59 항목에 나열된 작업 7~10을 완료합니다.

VLAN 지원

OMIVV에서는 라우팅 가능 VLAN에 대한 운영 체제 배포를 지원하기 때문에 배포 마법사에서 VLAN 지원을 구성할 수 있습니다. 배포 마법사의 이 부분에는 VLAN ID를 사용하여 VLAN을 지정할 수 있는 옵션이 있습니다. VLAN ID를 입력하면 배포 중 운영 체제의 관리 인터페이스에 적용되고 모든 트래픽에 VLAN ID를 태깅합니다.

배포 중에 제공된 VLAN이 OMIVV 어플라이언스 및 vCenter 서버와 양쪽 모두 통신하는지 확인합니다. 이러한 대상 중 하나 또는 양쪽 모두에 통신할 수 없는 VLAN에 운영 체제를 배포하면 배포에 실패합니다.

단일 배포 작업에서 복수의 운영 체제 미설치 서버를 선택하고 같은 VLAN ID를 모든 서버에 적용하고 싶으면 배포 마법사의 서버 식별 부분에서 **모든 서버에 설정 적용**을 사용합니다. 이 옵션을 사용하면 다른 네트워크 설정과 함께 같은 VLAN ID를 해당 배포 작업의 모든 서버에 적용할 수 있습니다.

노트: OMIVV에 대한 네트워크 연결을 기반으로 관리 NIC를 선택해야 합니다. **모든 서버에 설정 적용** 옵션은 관리 NIC 선택에 적용할 수 없습니다.

배포 작업 타이밍

여러 요인에 따라 시스템 프로필 및 ISO 프로필 배포를 완료하는 데 30분에서 몇 시간이 걸릴 수 있습니다. 배포 작업을 시작할 때는 제공된 지침에 따라 배포 시간을 계획하는 것이 좋습니다. 시스템 프로필 및 ISO 프로필 배포를 완료하는 데 걸리는 시간은 배포 유형, 복잡성, 동시에 실행되는 배포 작업 수에 따라 다릅니다. 배포 작업은 전체 배포 작업 시간을 개선하기 위해 최대 5개의 동시 서버로 구성된 일괄 작업으로 실행합니다. 정확한 동시 작업 수는 사용 가능한 리소스에 따라 다릅니다.

다음 표에는 평균값이 나와 있으며 서버 구성, 서버 세대, 그리고 배포에 대하여 예약된 운영 체제 미설치 서버의 수와 같은 요인에 따라 달라질 수 있습니다.

표 3. 단일 서버의 대략적인 배포 시간

배포 유형	배포 당 예상 소요 시간
ISO 프로필만	30~130분 사이
시스템 프로필만	5 - 6분
시스템 프로필 및 ISO 프로필	30~130분

배포 시퀀스 내의 서버 상태

자동 검색 또는 수동 검색 중에 발견된 서버는 서버가 데이터 센터에 새로운 서버인지 예약된 배포 작업이 보류 중인지 결정하는 데 도움을 주기 위해 여러 가지 상태로 분류됩니다. 관리자는 이러한 상태를 사용하여 하드웨어 구성 상태를 확인할 수 있습니다.

표 4. 배포 시퀀스의 서버 상태

서버 상태	설명
구성되지 않음	서버가 OMIVV에 추가되고 구성을 기다리는 중입니다.
구성됨	서버에 성공적인 운영 체제 배포에 필요한 모든 하드웨어 정보가 구성되어 있습니다.

11

규정 준수

관리 규정 준수

OMIVV에서 호스트를 보고 관리하려면 각 호스트가 특정 기준을 충족해야 합니다. 호스트가 규정 준수 기준을 충족하지 않는 경우 OMIVV는 호스트를 관리하고 모니터링하지 않습니다. OMIVV에서 비준수 호스트에 대한 세부 정보를 표시하고 해당하는 경우 비준수를 수정할 수 있습니다.

호스트는 다음과 같은 경우 기준을 준수하지 않습니다.

- 호스트가 호스트 자격 증명 프로필과 연결되어 있지 않습니다.
- CSIOR(Collect System Inventory on Reboot) 기능을 사용하지 않도록 설정되어 있거나 실행되지 않은 경우, 수동으로 재부팅해야 합니다.

  노트: 섀시를 사용하여 호스트를 관리하면 CSIOR 상태가 결정되지 않습니다.
- 호스트의 SNMP 트랩 대상이 OMIVV 어플라이언스 IP 주소에 구성되어 있지 않습니다. SNMP 트랩 대상 설정의 오류는 호스트 자격 증명 프로필에 제공된 iDRAC 또는 호스트 자격 증명이 유효하지 않은 경우에 발생할 수 있습니다. 또는 iDRAC에 사용 가능한 슬롯이 없거나 iDRAC 잠금 모드(iDRAC9 기반 서버에서만)가 켜져 있습니다. iDRAC9 기반 서버 목록은 호환성 매트릭스를 참조하십시오.
- OMIVV에서 ESXi 6.5 이상을 실행하는 호스트에서 WBEM 서비스를 활성화하는 데 실패했습니다.
- iDRAC 펌웨어 버전이 2.50.50.50 이하입니다. iDRAC 버전 2.50.50.50 이상은 시스템 프로필 기능을 사용하는 경우에만 필요합니다.
- iDRAC 라이선스가 호환되지 않습니다(iDRAC Express가 최소 요구 사항). 호환되는 iDRAC 라이선스가 없는 서버는 펌웨어 업데이트와 모니터링에 사용할 수 없습니다.

주의: 잠금 모드의 호스트는 비준수의 경우에도 규정 준수 테스트에 표시되지 않습니다. 규정 준수 수준을 수동으로 확인해야 합니다. 수동으로 확인하면 메시지가 표시됩니다. 메시지를 무시하십시오. 해당 규정 준수 상태를 파악할 수 없기 때문에 표시되지 않습니다. 이러한 시스템의 규정 준수 여부는 수동으로 확인해야 합니다. 이러한 시나리오에서는 경고 메시지가 표시됩니다.

관리 규정 준수 페이지에서 다음 작업을 수행할 수 있습니다.

- 규정 준수 문제를 해결합니다. 자세한 내용은 비준수 호스트 해결 페이지 64을(를) 참조하십시오.
- 인벤토리를 실행합니다. 호스트 자격 증명 프로필과 관련된 호스트 중에서 iDRAC 상태가 **비준수** 또는 **알 수 없음**인 경우 인벤토리 작업 실행 링크가 활성화됩니다.
- iDRAC 라이선스를 갱신합니다. 자세한 내용은 iDRAC 라이선스 규정 준수 수정 페이지 65을(를) 참조하십시오.
- OEM 호스트를 추가합니다. OEM 호스트 추가에 대한 자세한 내용은 OEM 호스트 추가 페이지 65을(를) 참조하십시오.

비준수 호스트 보기

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **관리 규정 준수**를 클릭합니다.

모든 비준수 호스트가 다음 정보와 함께 표에 표시됩니다.

- **호스트** – 호스트의 FQDN 또는 IP 주소입니다.
- **모델** – 서버의 모델 이름입니다.
- **자격 증명 프로필** – 호스트 자격 증명 프로필 이름입니다.
- **CSIOR 상태** – CSIOR 상태(**켜짐** 또는 **꺼짐**)를 나타냅니다. CSIOR 상태에서는 섀시를 사용하여 관리되는 호스트가 **결정되지 않음**으로 표시됩니다.
- **SNMP 트랩 상태** – SNMP 트랩 상태(**구성됨** 또는 **구성되지 않음**)를 나타냅니다.
- **하이퍼바이저** - 하이퍼바이저 이름 및 버전입니다.
- **WBEM 상태** – WBEM 상태(**준수** 또는 **비준수**)를 나타냅니다. CSIOR 상태에서는 섀시를 사용하여 관리되는 호스트가 **해당 없음**으로 표시됩니다.
- **iDRAC 펌웨어 버전** – iDRAC 펌웨어 버전입니다.
- **iDRAC 라이선스 상태** – iDRAC 라이선스 상태(**준수** 또는 **비준수**)를 나타냅니다.

노트: 섀시 자격 증명 프로필을 사용하여 PowerEdge MX 호스트를 관리하는 경우 iDRAC 펌웨어 버전이 **관리 규정 준수** 페이지에 **해당 없음**으로 표시됩니다. iDRAC 펌웨어 규정 준수가 iDRAC9 기반 서버에 적용되지 않기 때문입니다. iDRAC9 기반 서버 목록은 호환성 매트릭스를 참조하십시오.

비준수 호스트 해결

호스트는 다음과 같은 경우 기준을 준수하지 않습니다.

- 호스트가 호스트 자격 증명 프로필과 연결되어 있지 않습니다.
- CSIOR(Collect System Inventory on Reboot) 기능을 사용하지 않도록 설정되어 있거나 실행되지 않은 경우, 수동으로 재부팅해야 합니다.

  노트: 섀시를 사용하여 호스트를 관리하면 CSIOR 상태가 결정되지 않습니다.
- 호스트의 SNMP 트랩 대상이 OMIVV 어플라이언스 IP 주소에 구성되어 있지 않습니다. SNMP 트랩 대상 설정의 오류는 호스트 자격 증명 프로필에 제공된 iDRAC 또는 호스트 자격 증명이 유효하지 않은 경우에 발생할 수 있습니다. 또는 iDRAC에 사용 가능한 슬롯이 없거나 iDRAC 잠금 모드(iDRAC9 기반 서버에서만)가 켜져 있습니다. iDRAC9 기반 서버 목록은 호환성 매트릭스를 참조하십시오.
- OMIVV에서 ESXi 6.5 이상을 실행하는 호스트에서 WBEM 서비스를 활성화하는 데 실패했습니다.
- iDRAC 펌웨어 버전이 2.50.50.50 이하입니다. iDRAC 버전 2.50.50.50 이상은 시스템 프로필 기능을 사용하는 경우에만 필요합니다.
- iDRAC 라이선스가 호환되지 않습니다(iDRAC Express가 최소 요구 사항). 호환되는 iDRAC 라이선스가 없는 서버는 펌웨어 업데이트와 모니터링에 사용할 수 없습니다.

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **관리 규정 준수**를 클릭합니다.
2. 비준수 호스트를 선택하고 **규정 준수 해결**을 클릭합니다.
3. 마법사의 시작 페이지에서 지침을 읽고 **시작하기**를 클릭합니다.
4. **호스트 선택** 페이지에서 하나 이상의 비준수 호스트를 선택하고 **다음**을 클릭합니다.
   - 호스트가 호스트 자격 증명 프로필에 연결되지 않은 경우 다음 경고 메시지가 표시됩니다.

     선택된 호스트 중 자격 증명 프로필에 연결되지 않은 호스트가 있습니다. OMIVV에서 규정 준수 검사를 실행하도록 하려면 호스트 자격 증명 프로필에 이러한 호스트를 추가해야 합니다.

     호스트 자격 증명 프로필에 할당되지 않은 호스트를 제외하려면 **계속**을 클릭합니다.

     호스트 자격 증명 프로필 페이지에 호스트를 추가하려면 **취소**를 클릭하고 호스트 자격 증명 프로필 페이지로 이동합니다. 호스트 자격 증명 프로필 생성에 대한 자세한 내용은 호스트 자격 증명 프로필 생성 페이지 35을(를) 참조하십시오.

     iDRAC IPv4가 비활성화된 MX 섀시에 있는 호스트는 섀시 자격 증명 프로필을 사용하여 관리해야 합니다. 이러한 호스트를 섀시 자격 증명 프로필에 연결하려면 **Dell EMC 섀시** 페이지의 MX 섀시 추가를 사용하여 섀시를 추가하고 섀시를 섀시 자격 증명 프로필에 연결해야 합니다.

   iDRAC 펌웨어 및 BIOS 버전을 업데이트하려면 다음을 수행합니다.

   a. **iDRAC 펌웨어 및 BIOS 버전 업데이트** 페이지에서 펌웨어 버전을 업데이트할 호스트를 하나 이상 선택합니다.
   b. **다음**을 클릭합니다.
   c. **호스트 재부팅** 페이지에서 재시작해야 하는 ESXi 호스트를 확인합니다.
   d. 호스트를 유지 보수 모드로 자동 전환하고 필요할 때 재부팅하려면 확인란을 선택한 후 **다음**을 클릭합니다.
   e. **요약** 페이지에서 작업 요약을 검토하고 **마침**을 클릭합니다.

   CSIOR을 켜려면 다음을 수행합니다.

   a. **호스트 선택** 페이지에서 하나 이상의 비준수 호스트를 선택하고 **다음**을 클릭합니다.
   b. **CSIOR 켜기** 페이지에서 CSIOR을 켤 호스트를 하나 이상 선택하고 **다음**을 클릭합니다.
   c. **요약** 페이지에서 작업 요약을 검토하고 **마침**을 클릭합니다.

   호스트 자격 증명 프로필에 유효한 정보를 제공하여 iDRAC 또는 호스트 자격 증명을 수정하거나, 처음 4개의 슬롯 중 iDRAC 트랩 대상에서 사용할 수 있게 하거나, iDRAC에서 시스템 잠금 모드를 비활성화한 후에 마법사가 SNMP 트랩 대상 상태를 **구성됨**으로 구성합니다.

   노트: 시스템 잠금 모드는 iDRAC9 기반 서버에만 적용할 수 있습니다.

   WBEM 비준수 호스트가 존재하는 경우 WBEM 서비스 활성화 실패로 이어지는 해당 호스트의 조건을 수동으로 수정할 수 있는지 확인합니다. 사용자 로그에서 오류 조건을 보고 수정할 수 있습니다. OMIVV를 활성화하여 인벤토리 중에 해당 호스트에 대한 WBEM 서비스를 활성화합니다.

iDRAC 라이선스 규정 준수 수정

호환되는 iDRAC 라이선스는 호스트의 규정 준수 기준 중 하나입니다. 호스트에 호환되는 iDRAC 라이선스가 없는 경우 해당 호스트는 **관리 규정 준수** 페이지에 비준수 호스트로 표시됩니다.

비준수 호스트를 클릭하여 iDRAC 만료 날짜, 라이선스 유형 및 라이선스 설명 등의 세부 정보를 볼 수 있습니다. 호스트 자격 증명 프로필과 관련된 호스트에 대한 iDRAC 규정 준수 상태가 **비준수** 또는 **알 수 없음**인 경우 **인벤토리 실행**이 활성화됩니다.

1. iDRAC 라이선스 규정 준수 문제를 해결하려면 OMIVV 홈 페이지에서 **규정 준수 및 배포** > **규정 준수** > **관리 규정 준수**를 클릭합니다.
2. iDRAC 라이선스가 규정을 준수하지 않는 호스트를 선택하고 **iDRAC 라이선스 갱신**을 클릭합니다.
3. Dell Digital Locker에 로그인하여 라이선스를 업데이트하거나 새 iDRAC 라이선스를 구입합니다.
   iDRAC 라이선스를 설치한 후, 호스트에 대한 인벤토리 작업을 실행하고 인벤토리 작업이 완료된 후 이 페이지로 돌아옵니다.

OEM 서버에 대한 지원

OEM 서버는 Dell EMC 파트너가 공급하며 PowerEdge 서버와 비슷한 기능 또는 포트폴리오를 제공합니다.

- OMIVV 4.3 이후부터 OEM 랙 서버가 지원됩니다.
- **OEM 호스트 추가** 마법사를 사용하여 OEM 서버를 추가합니다. OEM 호스트 추가에 대한 자세한 내용은 OEM 호스트 추가 페이지 65을(를) 참조하십시오.

  노트: WBEM 서비스가 이미 OEM 호스트에서 활성화되어 있고 vCenter에 추가되어 있는 경우에는 기본적으로 OMIVV에서 이러한 OEM 서버를 OMIVV 관리 목록에 추가합니다. 이러한 서버를 관리하려면 호스트 자격 증명 프로필에 호스트를 연결합니다. 호스트 자격 증명 프로필 생성에 대한 자세한 내용은 호스트 자격 증명 프로필 생성 페이지 35을(를) 참조하십시오.
- OEM 서버를 추가한 후에 모든 호스트 관리 프로세스는 Dell EMC PowerEdge 서버가 관리되는 방식과 비슷합니다.
- 운영 체제 미설치 및 배포 기능도 iDRAC를 사용하여 OEM 서버에서 지원됩니다.

OEM 호스트 추가

Dell EMC PowerEdge 서버와 함께 OMIVV에서도 리브랜딩 및 디브랜딩된 서버를 지원합니다. OEM에 대한 자세한 내용은 https://www.dellemc.com를 참조하십시오.

WBEM 서비스가 이미 활성화되어 있으면 OMIVV가 호스트의 iDRAC 연결을 확인합니다. 연결이 가능한 경우 OMIVV가 호스트를 관리 목록에 추가합니다.

OMIVV가 확인할 수 없는 경우 호스트가 OMIVV 관리 목록에 추가되도록 **OEM 호스트 추가** 마법사에서 호스트를 수동으로 선택해야 합니다.

WBEM 서비스가 비활성화되어 있거나 iDRAC에 연결할 수 없는 경우에는 **OEM 호스트 추가** 마법사를 사용하여 호스트를 OMIVV 관리 목록에 추가합니다.

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **규정 준수** > **관리 규정 준수** > **OEM 호스트 추가**를 클릭합니다.
2. **OEM 호스트 추가** 창의 **vCenter 인스턴스** 드롭다운 목록에서 vCenter의 인스턴스를 선택합니다.
3. **호스트 자격 증명 프로필** 드롭다운 목록에서 적절한 호스트 자격 증명 프로필을 선택합니다.
4. 연결된 호스트를 추가하거나 제거하려면 **호스트 추가**를 클릭합니다.
   호스트 선택 창이 표시됩니다.
5. **호스트 선택** 창에서 호스트를 선택하고 **예**를 클릭합니다.

   노트: OMIVV에서 관리하지 않는 호스트만 **호스트 선택** 창에 표시됩니다.

   OMIVV에서는 연결을 자동으로 테스트하고 연결 테스트 결과는 **OEM 호스트 추가** 창에 표시됩니다.

   iDRAC 테스트 및 **호스트 테스트** 열에는 **iDRAC 자격 증명** 및 **호스트 자격 증명**에 대한 연결 테스트 결과가 표시됩니다.

   모든 연결 테스트를 중지하려면 **테스트 중단**을 클릭합니다.
6. **확인**을 클릭합니다.
   선택한 호스트 자격 증명 프로필에 선택한 호스트가 추가되고 인벤토리가 트리거됩니다.

구성 규정 준수

구성 규정 준수 페이지에는 클러스터 프로필에 연결된 모든 클러스터에 대한 변경 사항 감지를 기반으로 한 규정 준수 상태가 표시됩니다. 여러 vCenter Server가 있는 PSC 환경의 구성 규정 준수 페이지에는 동일한 어플라이언스에 등록된 동일한 PSC에 속하는 모든 vCenter의 모든 클러스터가 나열됩니다.

- 하드웨어 구성 규정 준수 - 클러스터 프로필에 사용된 시스템 프로필과 클러스터에 속하는 연결된 호스트 사이의 특성 변경 사항을 표시합니다.
- 펌웨어 규정 준수 - 클러스터 프로필에 사용된 펌웨어 리포지토리 프로필과 클러스터에 속하는 연결된 호스트 사이의 펌웨어 버전 변경 사항을 표시합니다.
- 드라이버 규정 준수 - 클러스터 프로필에 사용된 드라이버 리포지토리 프로필과 클러스터에 속하는 연결된 vSAN 호스트 사이의 드라이버 버전 변경 사항을 표시합니다.

구성 규정 준수 보기

1. OMIVV 홈 페이지에서 **규정 준수 및 배포** > **규정 준수** > **구성 규정 준수**를 클릭합니다.
   표에는 연결된 클러스터 프로필, 시스템 프로필, 펌웨어 리포지토리 프로필, 드라이버 리포지토리 프로필과 함께 클러스터가 표시됩니다.

   기본 및 고급 시스템 프로필 유형의 경우 시스템 프로필 이름이 Basic_<system profile name>, Advanced_<system profile name> 형식으로 표시됩니다.
2. **구성 규정 준수** 페이지에서 클러스터를 선택합니다.
   구성 규정 준수 정보 및 규정 준수 상태가 표시됩니다.

   구성 규정 준수 섹션에 다음과 같은 정보가 표시됩니다.

   - **클러스터 이름** – 클러스터의 이름입니다.
   - **규정 준수 상태** – 규정 준수 상태(규정 준수 또는 비준수)를 표시합니다. 클러스터의 호스트 중 하나라도 비준수 상태인 경우 상태는 비준수로 표시됩니다.
   - **호스트 수** - 클러스터에 있는 호스트의 전체 개수입니다.
   - **일정** - 다음 변경 사항 감지 작업이 예약된 날짜와 시간입니다.
   - **마지막 변경 사항 감지 시간** - 마지막 변경 사항 감지 작업이 완료된 날짜 및 시간입니다.

   규정 준수 상태 섹션에는 하드웨어, 펌웨어 및 드라이버 구성 요소의 규정 준수 상태가 표시됩니다. 다른 규정 준수 상태는 다음과 같습니다.

   - **준수** - 관련 하드웨어, 펌웨어 및 드라이버 구성 요소와 호환되는 호스트의 수를 표시합니다.
   - **비준수** - 관련 하드웨어, 펌웨어 및 드라이버 구성 요소와 호환되지 않는 호스트의 수를 표시합니다.
   - **해당 없음** - 적용할 수 없는 호스트 수를 표시합니다.

     섀시 자격 증명 프로필을 사용하여 관리하는 호스트에는 하드웨어 변경 사항을 적용할 수 없습니다.

     vSphere 클러스터의 일부인 호스트에는 드라이버 변경 사항을 적용할 수 없습니다.

     온라인 카탈로그를 사용하여 클러스터 프로필을 생성한 경우 vSAN 클러스터에 펌웨어 규정 준수를 적용할 수 없습니다.
3. 변경 사항을 자세히 보려면 **변경 사항 보고서 보기**를 클릭합니다. 이 링크는 비준수 클러스터에 대해서만 활성화됩니다. 변경 사항 보고서 보기에 대한 자세한 내용은 변경 사항 보고서 보기 페이지 66을(를) 참조하십시오.

변경 사항 보고서 보기

구성 규정 준수 보고서 페이지에는 하드웨어, 펌웨어 및 드라이버 구성 요소의 변경 사항 세부 정보가 표시됩니다.

변경 사항 감지 작업 상태가 **요약** 섹션에 표시됩니다.

하드웨어의 경우

- 호스트 이름 또는 IP - 호스트 IP 또는 호스트 이름을 나타냅니다.
- 서비스 태그 - 호스트의 서비스 태그를 나타냅니다.
- 변경 사항 상태 - 변경 사항 상태(규정 준수 위반 또는 실패)를 나타냅니다.
- 인스턴스 - 하드웨어 구성 요소 이름을 나타냅니다.
- 그룹 - 특성의 그룹 이름을 나타냅니다.
- 특성 이름 - 특성 이름을 나타냅니다.
- 현재 값 - 호스트에 있는 특성의 현재 값을 나타냅니다.
- 기준 값 - 기준 값을 나타냅니다.
- 변경 사항 유형/오류 - 규정 비준수의 이유를 나타냅니다. 변경 사항 유형에 대한 자세한 내용은 구성 요소와 기준선 버전 비교 매트릭스 페이지 161을(를) 참조하십시오.

노트: 변경 사항 감지 작업은 호스트 또는 iDRAC에 연결할 수 없는 경우에만 실패합니다. 호스트 또는 iDRAC이 성공적으로 인벤토리되는 경우 변경 사항 감지 작업이 성공으로 표시됩니다. 다른 변경 사항 감지 작업 실패 이유를 확인하려면 변경 사항 보고서의 **변경 사항 유형/오류** 열을 참조하십시오.

펌웨어 및 드라이버의 경우:

- 호스트 이름 또는 IP - 호스트 IP 또는 호스트 이름을 나타냅니다.
- 서비스 태그 - 호스트의 서비스 태그를 나타냅니다.
- 변경 사항 상태 - 변경 사항 상태를 나타냅니다.
- 구성 요소 이름 - 구성 요소의 이름을 나타냅니다.
- 현재 값 - 호스트에 있는 특성의 현재 값을 나타냅니다.
- 기준 값 - 기준 값을 나타냅니다.
- 변경 사항 유형/오류 - 규정 비준수의 이유를 나타냅니다. 변경 사항 유형에 대한 자세한 내용은 구성 요소와 기준선 버전 비교 매트릭스 페이지 161을(를) 참조하십시오.
- 임계성(펌웨어의 경우) - 식별된 구성 요소 버전의 업데이트에 대한 중요도 수준을 나타냅니다.
- 권장 사항(드라이버의 경우) - 드라이버 구성 요소의 업데이트 권장 사항을 나타냅니다.

노트: 둘 이상의 펌웨어 버전을 사용할 수 있는 경우, 항상 가장 최근의 펌웨어 버전이 규정 준수 비교에 사용됩니다.

필터 옵션을 사용하여 변경 사항 상태에 따라 변경 사항 세부 정보를 확인할 수 있습니다.

노트: 32비트 펌웨어 번들은 5.x에서 지원되지 않습니다. 클러스터 프로필이 4.x 버전에서 32비트 펌웨어 번들과 연결되어 있는 경우 4.x에서 5.x로 백업 및 복원을 수행할 때 변경 사항 상태가 실패로 표시됩니다. 64비트 펌웨어 번들을 클러스터 프로필과 함께 사용하고 변경 사항 감지 작업을 다시 실행합니다.

노트: OMIVV 및 vSphere Lifecycle Manager 변경 사항 보고서 간에 불일치가 발생할 수 있습니다. 이는 vSphere Lifecycle Manager에는 항상 실시간 변경 사항 보고서가 표시되고 OMIVV에는 예약 날짜 및 시간을 기준으로 변경 사항 보고서가 표시되기 때문입니다. 변경 사항 보고서 간에 불일치가 발생하는 경우 **변경 사항 감지 작업** 페이지에서 변경 사항 감지 작업을 온디맨드로 실행합니다.

12

OMIVV 작업 관리

작업 페이지에는 다음과 같은 작업이 표시됩니다.

- 배포
- 검색
- 펌웨어 업데이트
- 시스템 잠금 모드
- 드리프트 감지
- 인벤토리
- 보증

OMIVV는 사용자가 만든 작업(예: 배포 작업) 및 OMIVV가 만든 작업(예: 상태 메트릭 수집 작업)을 포함하는 총 작업 수가 500개에 도달하면 이전 작업을 지웁니다. 작업 수가 500개를 초과하면 이전 500개 작업이 삭제됩니다.

배포 작업

배포 작업이 완료되면 **배포 작업** 페이지에서 배포 작업 상태를 추적할 수 있습니다.

1. OMIVV 홈 페이지에서 **작업** > **배포 작업**을 클릭합니다.
   모든 배포 작업이 다음 정보와 함께 표에 표시됩니다.
   - **이름** - 배포 작업 이름입니다.
   - **설명** – 작업 설명입니다.
   - **예약된 시간** - 작업이 예약된 날짜와 시간입니다.
   - **상태** - 배포 작업의 상태입니다.
   - **컬렉션 크기** - 배포 작업의 서버 수입니다.
   - **진행률 요약** - 배포 작업의 작업 진행률 세부 정보입니다.
2. 배포 작업의 서버에 대한 자세한 정보를 보려면 배포 작업을 선택합니다.
   하단 창에 다음과 같은 정보가 표시됩니다.
   - **서비스 태그**
   - **iDRAC IP**
   - **상태**
   - **경고**
   - **세부 정보**
   - **시작 날짜 및 시간**
   - **종료 날짜 및 시간**
   - **추가 세부 정보**

   a. 배포 작업에 대한 자세한 정보를 보려면 작업을 선택하고 **세부 정보** 열에서 포인터를 일시 중지합니다.
   b. 시스템 프로필 기반 작업 실패에 대한 자세한 내용을 보려면 **자세히 보기**를 클릭하십시오.
   다음 정보가 표시됩니다.
      - 구성 요소의 FQDD
      - 특성의 값
      - 이전 값
      - 새 값
      - 오류 메시지 및 메시지 ID(몇 가지 유형의 오류에 대해서는 표시되지 않음)

      시스템 프로필 적용-오류 세부 정보 창의 **특성 이름** 아래 표시되는 일부 특성은 **자세히 보기**를 클릭할 때 나타나는 시스템 프로필의 특성 이름과 같지 않습니다.
3. 배포 작업을 중지하려면 **중지**를 클릭합니다.
4. 배포 작업을 제거하려면 **완료된 항목 지우기**를 클릭하고 **이전 날짜 및 작업 상태**를 선택한 다음 **적용**을 클릭합니다.
   그러면 선택한 작업이 **배포 작업** 페이지에서 지워집니다.

검색 작업

검색 작업이 생성되면 **검색 작업** 페이지에서 작업 상태를 추적할 수 있습니다.

1. OMIVV 홈 페이지에서 **작업** > **검색 작업**을 클릭합니다.
   모든 검색 작업이 다음 정보와 함께 표에 표시됩니다.
   - **이름** - 검색 작업 이름입니다.
   - **설명** – 작업 설명입니다.
   - **예약된 시간** - 작업이 예약된 날짜와 시간입니다.
   - **상태** - 검색 작업의 상태입니다.

     서버가 성공적으로 검색되면 작업 상태가 성공으로 표시됩니다.

     작업이 실패하는 경우 실패의 이유가 표시됩니다.
   - **컬렉션 크기** - 검색 작업의 서버 수입니다.
   - **진행률 요약** - 검색 작업의 작업 진행률 세부 정보입니다.
2. 자세한 내용을 보려면 검색 작업을 선택합니다.
   하단 창에 다음과 같은 정보가 표시됩니다.
   - **iDRAC IP**
   - **상태**
   - **세부 정보**
   - **시작 날짜 및 시간**
   - **종료 날짜 및 시간**
3. 검색 작업 대기열을 제거하려면 **완료된 항목 지우기**를 클릭합니다.
   a. 날짜를 선택합니다.
      선택한 날짜 이전의 작업이 삭제됩니다.
   b. 작업의 상태를 선택합니다.
   c. **적용**을 클릭합니다.

섀시 펌웨어 업데이트 작업

섀시 펌웨어 업데이트 작업이 완료되면 **섀시 펌웨어 업데이트 작업** 페이지에서 펌웨어 업데이트 작업 상태를 볼 수 있습니다.

1. OMIVV 홈 페이지에서 **작업** > **펌웨어 업데이트** > **섀시 펌웨어 업데이트**를 클릭합니다.
2. 최신 로그 정보를 보려면 새로 고침 아이콘을 클릭합니다.
   모든 섀시 펌웨어 업데이트 작업이 다음 정보와 함께 표에 표시됩니다.
   - **상태** - 펌웨어 업데이트 작업의 상태입니다.
   - **예약된 시간** - 펌웨어 업데이트 작업이 예약된 시간입니다.
   - **이름** - 작업 이름입니다.
   - **설명** - 펌웨어 업데이트 작업 설명입니다.
   - **vCenter** - vCenter 이름입니다.
   - **컬렉션 크기** - 펌웨어 업데이트 작업의 섀시 수입니다.

     총 섀시 수에는 리드 및 독립형 섀시만 포함됩니다. 구성원 섀시는 영향을 받지 않습니다.
   - **진행률 요약** - 펌웨어 업데이트 작업의 진행률 세부 정보입니다.
3. 특정 작업에 대한 자세한 내용을 보려면 작업을 선택합니다.
   하단 그리드에 다음 정보가 표시됩니다.
   - **섀시 서비스 태그** - 섀시의 서비스 태그입니다.
   - **상태** - 작업의 상태입니다.
   - **시작 시간** - 펌웨어 업데이트 작업 시작 시간입니다.
   - **종료 시간** - 펌웨어 업데이트 작업 종료 시간입니다.
4. 실행 중이지 않은 예약된 펌웨어 업데이트를 중지하려면 중지하려는 작업을 선택하고 **중지**를 클릭합니다.

   경고: 이미 MX 섀시에 제출된 펌웨어 업데이트 작업을 중지할 경우 호스트에서는 펌웨어가 업데이트될 수 있습니다. OMIVV에서 작업이 취소된 것으로 보고합니다.

5. 이전 펌웨어 업데이트 작업 또는 예약된 펌웨어 업데이트를 제거하려면 **완료된 항목 지우기**를 클릭합니다.
펌웨어 업데이트 작업 제거 대화 상자가 표시됩니다. 취소, 성공 또는 실패한 작업만 제거할 수 있으며 예약된 또는 활성 작업은 제거할 수 없습니다.
6. **펌웨어 업데이트 작업 제거** 대화 상자에서 **이전 날짜 및 작업 상태**를 선택하고 **확인**을 클릭합니다.
그러면 **섀시 펌웨어 업데이트** 작업 목록에서 선택한 작업이 제거됩니다.

호스트 펌웨어 업데이트 작업

섀시 펌웨어 업데이트 작업이 완료되면 **호스트 펌웨어 업데이트 작업** 페이지에서 펌웨어 업데이트 작업의 상태를 볼 수 있습니다.

1. OMIVV 홈 페이지에서 **작업** > **펌웨어 업데이트** > **호스트 펌웨어 업데이트**를 클릭합니다.
2. 최신 로그 정보를 보려면 새로 고침 아이콘을 클릭합니다.
모든 호스트 펌웨어 업데이트 작업이 다음 정보와 함께 표에 표시됩니다.
   - **상태** - 펌웨어 업데이트 작업의 상태입니다.
   - **예약된 시간** - 펌웨어 업데이트 작업이 예약된 시간입니다.
   - **이름** - 작업 이름입니다.
   - **설명** - 펌웨어 업데이트 작업 설명입니다.
   - **vCenter** - vCenter 이름입니다.
   - **컬렉션 크기** - 펌웨어 업데이트 작업의 서버 수입니다.
   - **진행률 요약** - 펌웨어 업데이트 작업의 진행률 세부 정보입니다.
3. 특정 작업에 대한 자세한 내용을 보려면 작업을 선택합니다.
하단 그리드에 다음 정보가 표시됩니다.
   - **호스트 이름** - 호스트의 서비스 태그입니다.
   - **상태** - 작업의 상태입니다.
   - **시작 시간** - 펌웨어 업데이트 작업 시작 시간입니다.
   - **종료 시간** - 펌웨어 업데이트 작업 종료 시간입니다.

   노트: 여러 Dell Update Packages로 펌웨어 업데이트 작업이 예약되고 OMIVV가 선택한 업데이트 패키지 중 일부를 다운로드하지 못하면 OMIVV는 다운로드에 성공한 패키지를 계속 업데이트합니다. 작업 페이지에는 다운로드한 패키지의 상태가 표시됩니다.
4. 실행 중이지 않은 예약된 펌웨어 업데이트를 중지하려면 중지하려는 작업을 선택하고 **중지**를 클릭합니다.
   경고: 이미 iDRAC에 제출된 펌웨어 업데이트 작업을 중지할 경우 호스트에서는 펌웨어가 업데이트될 수 있습니다. OMIVV에서 작업이 취소된 것으로 보고합니다.
5. 이전 펌웨어 업데이트 작업 또는 예약된 펌웨어 업데이트를 제거하려면 **완료된 항목 지우기**를 클릭합니다.
펌웨어 업데이트 작업 제거 대화 상자가 표시됩니다. 취소, 성공 또는 실패한 작업만 제거할 수 있으며 예약된 또는 활성 작업은 제거할 수 없습니다.
6. **펌웨어 업데이트 작업 제거** 대화 상자에서 **이전 날짜 및 작업 상태**를 선택하고 **확인**을 클릭합니다.
그러면 선택한 작업이 **호스트 펌웨어 업데이트** 작업 목록에서 지워집니다.

시스템 잠금 모드 작업

시스템 잠금 모드 설정은 iDRAC9 기반 서버에서만 지원됩니다. 설정을 켜면 펌웨어 업데이트를 포함하여 시스템 구성이 잠깁니다. 이 설정은 의도하지 않은 변경으로부터 시스템을 보호하기 위해 사용됩니다. OMIVV 어플라이언스를 사용하거나 iDRAC 콘솔에서 관리되는 호스트에 대한 시스템 잠금 모드를 켜거나 끌 수 있습니다. OMIVV 버전 4.1 이상에서 서버의 iDRAC 잠금 모드를 구성하고 모니터링할 수 있습니다. 또한 iDRAC에 Enterprise 라이선스가 있어야 잠금 모드를 활성화할 수 있습니다.

노트: 섀시 자격 증명 프로필을 사용하여 관리하는 호스트는 시스템 잠금 모드를 변경할 수 없습니다.

시스템 잠금 구성이 완료되면 **시스템 잠금 모드 작업** 페이지에서 잠금 모드의 업데이트된 상태를 볼 수 있습니다.

1. OMIVV 홈 페이지에서 **작업** > **시스템 잠금 모드**를 클릭합니다.
모든 시스템 잠금 모드 작업이 다음 정보와 함께 표에 표시됩니다.
   - **이름** - 시스템 잠금 모드 작업 이름입니다.
   - **설명** – 작업 설명입니다.
   - **예약 시간** - 시스템 잠금 모드 작업이 예약된 날짜 및 시간입니다.
   - **vCenter** - vCenter 이름입니다.
   - **상태** - 시스템 잠금 모드 작업의 상태입니다.

- **컬렉션 크기** - 시스템 잠금 모드 작업의 서버 수입니다.
- **진행률 요약** - 시스템 잠금 모드 작업의 작업 진행률 세부 정보입니다.

2. 시스템 잠금 모드 작업의 서버에 대한 자세한 내용을 보려면 시스템 잠금 모드 작업을 선택하십시오.
하단 그리드에 다음 정보가 표시됩니다.
   - **서비스 태그**
   - **iDRAC IP**
   - **호스트 이름**
   - **상태**
   - **세부 정보**
   - **시작 날짜 및 시간**
   - **종료 날짜 및 시간**

   시스템 잠금 모드 작업에 대한 자세한 내용을 보려면 작업을 선택하고 **세부 정보** 열에서 포인터를 일시 중지하십시오.
3. 시스템 잠금 모드 작업을 제거하려면 **완료된 항목 지우기**를 클릭하고 **이전 날짜 및 작업 상태**를 선택한 후 **적용**을 클릭합니다.
그러면 선택한 작업이 **시스템 잠금 모드** 작업 페이지에서 제거됩니다.

변경 사항 감지 작업

유효성 검사된 기준과 하드웨어 구성, 펌웨어 및 드라이버 버전이 포함된 서버 구성 사이의 비교 결과를 찾기 위해 변경 사항 감지 작업이 실행됩니다.

노트: 변경 사항 감지 작업은 호스트 또는 iDRAC에 연결할 수 없는 경우에만 실패합니다. 호스트 또는 iDRAC가 성공적으로 인벤토리되는 경우, 변경 사항 감지 작업이 성공적으로 실행되고 변경 사항 보고서에서 변경 사항 세부 정보를 볼 수 있습니다. 변경 사항 보고서에 대한 자세한 내용은 변경 사항 보고서 보기 페이지 66을(를) 참조하십시오.

1. OMIVV 홈 페이지에서 **작업** > **변경 사항 감지**를 클릭합니다.
모든 변경 사항 감지 작업이 다음 정보와 함께 표에 표시됩니다.
   - **이름** - 변경 사항 감지 작업의 이름입니다.
   - **마지막 실행** - 마지막으로 변경 사항 감지 작업을 실행한 날짜 및 시간입니다.
   - **다음 실행** - 다음 변경 사항 감지 작업이 예약된 날짜 및 시간입니다.
   - **상태** - 변경 사항 감지 작업의 상태입니다.
   - **컬렉션 크기** - 변경 사항 감지 작업의 서버 수입니다.
   - **진행률 요약** - 변경 사항 감지 작업의 진행률 세부 정보입니다.
2. 업데이트된 변경 사항 감지 작업 세부 사항을 보려면 **새로 고침**을 클릭합니다.
3. 변경 사항 감지 작업의 서버에 대한 자세한 정보를 보려면 변경 사항 감지 작업을 선택합니다. 다음 정보가 표시됩니다.
   - 서비스 태그
   - iDRAC IP
   - 호스트 이름
   - 클러스터
   - vCenter
   - 상태
   - 시작 날짜 및 시간
   - 종료 날짜 및 시간
4. **변경 사항 감지** 작업을 온디맨드로 실행하려면 **지금 실행** 버튼을 클릭합니다.
   기준이 지정된 클러스터에서 호스트 자격 증명 프로필 또는 섀시 자격 증명 프로필에 호스트를 추가하고 나면 새로 추가된 호스트에 대해 변경 사항 감지 작업이 자동으로 실행됩니다.

호스트 인벤토리 작업 보기

호스트 인벤토리 페이지에는 호스트 자격 증명 프로필에 연결된 호스트에서 실행되는 최신 인벤토리 작업에 대한 정보가 표시됩니다.

1. OMIVV 홈 페이지에서 **작업** > **인벤토리** > **호스트 인벤토리**를 클릭합니다.
2. 연결된 모든 호스트 인벤토리 작업 정보를 보려면 vCenter를 선택합니다.
   - **vCenter** - vCenter FQDN 또는 IP 주소입니다.
   - **통과한 호스트** - 인벤토리에 성공한 호스트의 수입니다.

- **마지막 인벤토리** - 마지막 인벤토리를 실행한 날짜 및 시간입니다.
- **다음 인벤토리** - 다음 인벤토리가 예약된 날짜 및 시간입니다.

연결된 호스트 세부 정보가 하단 창에 표시됩니다.

- **호스트** - 호스트의 FQDN 또는 IP 주소입니다.
- **상태** - 호스트의 인벤토리 상태입니다. 옵션은 다음과 같습니다.
  - **성공**
  - **실패**
  - **진행 중**
- **기간(MM:SS)** - 분 및 초 단위의 인벤토리 작업 기간입니다.
- **시작 날짜 및 시간** - 인벤토리 작업이 시작된 날짜 및 시간입니다.
- **종료 날짜 및 시간** - 인벤토리 작업이 완료된 날짜 및 시간입니다.

인벤토리 작업 실행

초기 구성이 완료되면 호스트 자격 증명 프로필에 추가된 모든 호스트에 대해 인벤토리가 자동으로 트리거됩니다.

1. 온디맨드 인벤토리를 실행하려면 **작업** > **인벤토리** > **호스트 인벤토리**를 클릭합니다.
2. **지금 실행**을 클릭합니다.
3. 인벤토리 작업 상태를 확인하려면 **새로 고침**을 클릭합니다.
   인벤토리 작업이 완료되면 **OMIVV 호스트 정보** 페이지에서 호스트 정보를 볼 수 있습니다.
4. OMIVV 호스트 정보를 보려면 **메뉴**를 확장한 다음 **호스트 및 클러스터**를 선택합니다.
5. 왼쪽 창에서 아무 호스트나 선택합니다.
6. 오른쪽 창에서 **모니터링**을 선택한 다음 **OMIVV 호스트 정보**를 확장합니다.
   다음 정보가 표시됩니다.
   - 하드웨어 인벤토리
   - 스토리지
   - 펌웨어
   - 전원 모니터링
   - 보증
   - 시스템 이벤트 로그

   섀시 자격 증명 프로필을 사용하여 호스트를 관리하는 경우 펌웨어 인벤토리 데이터는 Lifecycle Controller 및 소프트웨어 RAID와 같은 몇 가지 추가 구성 요소를 보여줍니다.

   노트: 라이선스 한도를 초과하는 호스트의 인벤토리 작업은 건너뛰며 실패로 표시됩니다.
7. **요약** 페이지의 **OMIVV 호스트 정보** 섹션에서 다음 작업을 수행할 수도 있습니다.
   - iDRAC(Remote Access Console) 실행
   - 서버 LED 깜박임 표시등
   - 시스템 잠금 모드 구성

     섀시를 사용하여 호스트를 관리하는 경우에는 시스템 잠금 모드 구성이 지원되지 않습니다.
   - 펌웨어 마법사 실행

호스트 인벤토리 작업 수정

호스트를 호스트 자격 증명 프로필에 연결하면 호스트의 인벤토리 정보가 최신 상태로 유지될 수 있도록 인벤토리를 정기적으로 예약해야 합니다. 인벤토리 작업은 호스트에서 실행하는 인벤토리 작업의 상태를 표시합니다.

설정 > **데이터 검색 일정** > **인벤토리 검색** 페이지에서 인벤토리 일정을 수정할 수도 있습니다.

1. **작업** 페이지에서 vCenter 인스턴스를 선택하고 **일정 편집**을 클릭합니다.
   인벤토리 데이터 검색 대화 상자가 표시됩니다.
2. **인벤토리 데이터** 섹션에서 다음을 수행합니다.
   a. **인벤토리 데이터 검색 활성화**(권장) 확인란을 선택합니다.

b. 인벤토리 데이터 검색 날짜와 시간을 선택하고 **적용**을 클릭합니다.
c. 설정을 리셋하려면 **지우기**를 클릭합니다.
d. 인벤토리 작업을 지금 실행하려면 **작업** 페이지에서 **지금 실행**을 클릭합니다.

노트: iDRAC Express 또는 Enterprise 라이선스가 없는 서버의 경우 iDRAC에 대한 라이선스 업그레이드가 필요하므로 인벤토리가 실패합니다.

노트: 모듈형 호스트 인벤토리를 실행하면 해당 섀시가 자동으로 검색됩니다. 섀시가 섀시 자격 증명 프로필의 일부인 경우 호스트 인벤토리 후 섀시 인벤토리가 자동으로 실행됩니다.

섀시 인벤토리 작업 보기

섀시 인벤토리 페이지에는 섀시 자격 증명 프로필에 연결된 섀시에서 실행되는 최신 인벤토리 작업에 대한 정보가 표시됩니다.

1. OMIVV 홈 페이지에서 **작업** > **인벤토리** > **섀시 인벤토리**를 클릭합니다.
2. 섀시 인벤토리 정보를 보려면 섀시를 선택합니다.
   - **섀시 IP/호스트 이름** - 섀시의 IP 주소입니다.
   - **서비스 태그** - 섀시 서비스 태그입니다. 서비스 태그는 지원 및 유지 보수를 위해 제조업체에서 제공하는 고유한 식별자입니다.
   - **상태** - 섀시의 상태입니다.
   - **기간(MM:SS)** - 분 및 초 단위로 표시된 작업 기간입니다.
   - **시작 날짜 및 시간** - 인벤토리 작업이 시작된 날짜 및 시간입니다.
   - **종료 날짜 및 시간** - 인벤토리 작업이 완료된 날짜 및 시간입니다.

   MCM 그룹에서 인벤토리는 리드 섀시에서만 실행됩니다. 인벤토리 정보는 리드 섀시 및 구성원 섀시 모두에 대한 데이터를 제공합니다.

   노트: PowerEdge 서버 중 C6320P, C6320, C4130 및 C6420에서는 섀시 인벤토리 작업이 지원되지 않습니다.

   노트: MX 섀시 블레이드 서버는 ESXi 6.5U2 버전 이상에서만 지원됩니다. 이러한 호스트에 이전 버전의 ESXi가 구축된 경우 OMIVV에서는 인벤토리 작업이 실행되지 않습니다.

섀시 인벤토리 작업 실행

1. OMIVV 홈 페이지에서 **작업** > **섀시 인벤토리**를 클릭합니다.
2. 섀시를 선택하고 **지금 실행**을 클릭합니다.
   섀시 인벤토리가 완료되면 **호스트 및 섀시** > **섀시** 페이지에서 섀시 정보를 볼 수 있습니다.
3. 섀시 정보를 보려면 **섀시** 페이지에서 섀시를 선택하고 **보기**를 클릭합니다.

   노트: 인벤토리 중 트랩 대상 및 알림 정책은 MCM 그룹에 있는 리드 섀시의 OMIVV가 구성합니다.

   노트: 섀시를 사용하여 호스트를 관리하는 경우에 섀시 인벤토리를 실행하면 호스트에 대한 호스트 인벤토리도 트리거됩니다. 호스트 인벤토리를 실행하는 경우에도 섀시 인벤토리가 트리거됩니다.

호스트 보증 보기

보증 작업은 모든 시스템의 www.dell.com/support에서 보증 정보를 가져오도록 예약된 작업입니다. OMIVV 어플라이언스가 보증 정보를 추출하려면 인터넷이 연결되어 있어야 합니다. 네트워크 설정에 따라 OMIVV가 인터넷에 연결하려면 프록시 정보가 필요할 수 있고 보증 정보를 가져올 수 있습니다. 관리 콘솔에서 프록시 세부 정보를 업데이트할 수 있습니다.

1. OMIVV 홈 페이지에서 **작업** > **보증** > **호스트 보증**을 클릭합니다.
2. 연결된 호스트 정보를 보려면 vCenter를 선택합니다.
   - **vCenter** - vCenter의 목록입니다.
   - **통과된 호스트** - 통과된 vCenter 호스트의 수입니다.
   - **마지막 보증** - 마지막 보증 작업을 실행한 날짜 및 시간입니다.
   - **다음 보증** - 다음 보증 작업을 실행할 날짜 및 시간입니다.

연결된 호스트 정보가 하단 창에 표시됩니다.

- **호스트** - 호스트 IP 주소입니다.
- **상태** - 보증 작업의 상태입니다. 옵션은 다음과 같습니다.
  - 성공
  - 실패
  - 진행 중
  - 예약됨
- **기간(MM:SS)** - MM:SS 단위로 표시된 보증 작업 기간입니다.
- **시작 날짜 및 시간** - 보증 작업이 시작된 날짜 및 시간입니다.
- **종료 날짜 및 시간** - 보증 작업이 종료된 시간입니다.

3. 온디맨드 호스트 보증을 실행하려면 **지금 실행**을 클릭합니다.

호스트 보증 작업 수정

보증 작업은 원래 **초기 구성 마법사**에서 구성됩니다. **설정** > **데이터 검색 일정** > **보증 검색** 페이지에서 보증 작업 일정을 수정할 수도 있습니다.

1. **작업** 페이지에서 **보증**을 확장한 다음 **호스트 보증**을 선택합니다.
2. vCenter를 선택하고 **일정 편집**을 클릭합니다.
3. **보증 데이터** 섹션에서 다음을 수행합니다.
   a. **보증 데이터 검색 활성화(권장)** 확인란을 선택합니다.
   b. 보증 데이터 검색 날짜와 시간을 선택하고 **적용**을 클릭합니다.
   c. 설정을 리셋하려면 **지우기**를 클릭합니다.

섀시 보증 보기

보증 작업은 모든 시스템의 Support.dell.com에서 보증 정보를 가져오도록 예약된 작업입니다. OMIVV 어플라이언스가 보증 정보를 추출하려면 인터넷 연결이 필요합니다. OMIVV 어플라이언스가 인터넷에 연결되었는지 확인합니다. 네트워크 설정에 따라 OMIVV가 인터넷에 연결하려면 프록시 정보가 필요할 수 있고 보증 정보를 가져올 수 있습니다. 관리 콘솔에서 프록시 세부 정보를 업데이트할 수 있습니다.

1. OMIVV 홈 페이지에서 **작업** > **보증** > **섀시 보증**을 클릭합니다.
   표에는 모든 섀시 보증 작업 정보가 표시됩니다.
   - **섀시 IP/호스트 이름** - 호스트 IP 주소입니다.
   - **서비스 태그** - 섀시의 서비스 태그입니다.
   - **상태** - 보증 작업의 상태입니다. 옵션은 다음과 같습니다.
     - 성공
     - 실패
     - 진행 중
     - 예약됨
   - **기간(MM:SS)** - MM:SS 단위로 표시된 보증 작업 기간입니다.
   - **시작 날짜 및 시간** - 보증 작업이 시작된 날짜 및 시간입니다.
   - **종료 날짜 및 시간** - 보증 작업이 종료된 시간입니다.
2. 온디맨드로 섀시 보증 작업을 실행하려면 **지금 실행**을 클릭합니다.

13

로그 관리

로그 내역 보기

1. **OpenManage Integration for VMware vCenter** 페이지에서 모든 로그를 보려면 **로그**를 클릭합니다.
   OMIVV 로그 검색 프로세스에서는 데이터베이스에서 모든 로그를 검색합니다. 로그 크기에 따라 몇 초 정도 걸릴 수 있습니다.

   - 로그 데이터를 내보내려면  을 클릭합니다.
   - 그리드에서 데이터를 정렬하려면 열 머리글을 클릭합니다.
   - 페이지 간을 이동하려면 이전 및 다음 아이콘을 클릭합니다.
   - 로그를 새로 고치려면 왼쪽 상단 모서리에 있는 새로 고침 아이콘을 클릭합니다.

2. 다음과 같은 범주 및/또는 날짜 범위를 기준으로 로그를 필터링하려면 ▼을 클릭합니다.
   범주:

   - **모든 범주**
   - **정보**
   - **경고**
   - **오류**

   날짜:

   - **지난 주**
   - **지난 달**
   - **작년**
   - **맞춤 구성 범위**: 이 옵션을 선택한 경우 달력 아이콘을 클릭하여 시작 및 종료 날짜를 지정합니다.

3. 필요한 범주 및 날짜를 선택한 후 **적용**을 클릭합니다.
   선택한 범주 및/또는 날짜 범위와 관련된 로그를 볼 수 있습니다. 로그 데이터 테이블에는 한 페이지에 100개의 로그가 표시됩니다.
4. 필터링된 데이터를 지우려면 **필터 지우기**를 클릭합니다.

14

OMIVV 어플라이언스 설정 관리

설정 페이지에서 다음 작업을 수행할 수 있습니다.

- 보증 만료 알림 설정을 구성합니다. 자세한 내용은 보증 만료 알림 구성 페이지 76을(를) 참조하십시오.
- 최신 어플라이언스 버전 알림을 구성합니다. 자세한 내용은 최신 어플라이언스 버전 알림 구성 페이지 76을(를) 참조하십시오.
- Proactive HA 경고의 심각도를 재정의합니다. 자세한 내용은 상태 업데이트 알림의 심각도 재정의 페이지 80을(를) 참조하십시오.
- 초기 구성. 자세한 내용은 다음을 참조하십시오. 초기 구성 페이지 80
- 이벤트 및 알람을 구성하고 봅니다. 자세한 내용은 이벤트 및 알람 구성 페이지 86을(를) 참조하십시오.
- 인벤토리 및 보증 데이터 검색 일정을 예약하거나 수정합니다. 자세한 내용은 인벤토리 작업 예약 페이지 95 및 보증 검색 작업 예약 페이지 95을(를) 참조하십시오.

다중 어플라이언스 관리

여러 vCenter 인스턴스에서 동일한 PSC를 공유하고 둘 이상의 OMIVV 어플라이언스 인스턴스에 등록되어 있는 경우 스위치 어플라이언스 마법사를 사용하여 OMIVV 인스턴스 사이를 전환할 수 있습니다.

홈 페이지에서 OMIVV의 현재 인스턴스를 볼 수 있습니다.

1. **OMIVV** 홈 페이지에서 **변경**을 클릭합니다.
   - **IP/이름** - OMIVV 어플라이언스 FQDN 또는 IP.
   - **버전** - OMIVV 어플라이언스의 현재 버전.
   - **규정 준수 상태** - 버전을 기준으로 하는 OMIVV 어플라이언스의 상태(**준수** 또는 **비준수**).
   - **가용성 상태** - OMIVV 서비스의 실행 여부에 따라 달라지는 OMIVV 어플라이언스의 가용성 상태. OMIVV의 작동 상태를 나타내는 **정상** 또는 **오류**가 표시됩니다.
   - **등록된 vCenter Server** - 등록된 vCenter Server FQDN 또는 IP.
   - **작업** - 작업 이름(**선택** 또는 **선택됨**).
2. **OMIVV 어플라이언스 전환** 페이지에서 **선택**을 클릭합니다.
3. 확인하려면 **예**를 클릭합니다.
   홈 페이지에서 어플라이언스 IP의 변경 사항을 볼 수 있습니다.

보증 만료 알림 구성

호스트에 대한 보증이 거의 만료되는 경우 알림을 받으려면 보증 만료 알림을 활성화합니다.

1. OMIVV 홈 페이지에서 **설정** > **알림** > **보증 만료 알림**을 클릭합니다.
2. **호스트의 보증 만료 알림 활성화**를 선택합니다.
3. 보증이 만료되기 전에 알림을 받을 일 수를 선택합니다.
4. **적용**을 클릭합니다.

최신 어플라이언스 버전 알림 구성

새 OMIVV 버전의 가용성에 대한 알림을 받으려면 **최신 버전 알림 활성화(권장)** 확인란을 선택합니다. 매주 확인하는 것이 좋습니다. OMIVV의 최신 어플라이언스 버전 알림 기능을 사용하려면 인터넷에 연결되어 있어야 합니다. 인터넷 연결에 프록시가 필요한 환경에서는 관리 포털에서 프록시 설정을 구성해야 합니다.

최신 버전의 OMIVV(RPM, OVF, RPM/OVF)의 가용성에 대해 주기적으로 알림을 받으려면 다음 단계를 수행하여 최신 버전 알림을 구성합니다.

1. OMIVV 홈 페이지에서 **설정** > **어플라이언스 설정** > **알림** > **최신 버전 알림**을 클릭합니다.

2. **최신 버전 알림 활성화**(권장) 확인란을 선택합니다.
3. 최신 어플라이언스 버전 알림을 수신하려면 날짜 및 시간을 선택합니다.
4. **적용**을 클릭합니다.

배포 자격 증명 구성

OMIVV는 프로비저닝 서버 역할을 합니다. 배포 자격 증명을 사용하면 자동 검색 프로세스에서 프로비저닝 서버로 OMIVV 플러그인을 사용하는 iDRAC와 통신할 수 있습니다. 배포 자격 증명을 사용하면 운영 체제 배포가 완료될 때까지 자동 검색을 사용하여 검색되는 운영 체제 미설치 서버와 안전하게 통신하기 위한 iDRAC 자격 증명을 설정할 수 있습니다.

운영 체제 배포 프로세스가 완료되면 OMIVV에서 호스트 자격 증명 프로필에 제공된 것처럼 iDRAC 자격 증명을 변경합니다. 배포 자격 증명을 변경하면 해당 시점부터 자동 검색을 사용하는 모든 새로 검색된 시스템은 새 iDRAC 자격 증명으로 프로비저닝됩니다. 하지만 배포 자격 증명을 변경하기 전에 검색된 서버의 자격 증명은 이 변경의 영향을 받지 않습니다.

1. OMIVV 홈 페이지에서 **설정** > **어플라이언스 설정** > **배포 자격 증명**을 클릭합니다.
2. 사용자 이름과 암호를 입력합니다. 기본 사용자 이름은 **root**이고 암호는 **calvin**입니다.
   iDRAC에서 설정한 iDRAC 사용자 암호 정책에 따라 암호를 입력해야 합니다. 또한 iDRAC 지원 문자를 사용해야 합니다.
3. **적용**을 클릭합니다.

하드웨어 구성 요소 중복 상태 - Proactive HA

Proactive HA는 OMIVV에서 작동하는 vCenter 기능입니다. Proactive HA를 활성화하면 호스트에서 지원되는 구성 요소의 중복 상태 저하를 기준으로 사전 조치를 취해 워크로드를 보호합니다.

지원되는 호스트 구성 요소의 중복 상태를 평가한 후 OMIVV 어플라이언스는 vCenter Server에 상태 변경 사항을 업데이트합니다. 지원되는 구성 요소(전원 공급 장치, 팬 및 IDSDM)에 대한 중복 상태의 사용 가능한 상태는 다음과 같습니다.

- 정상(정보) - 구성 요소가 정상적으로 작동하고 있습니다.
- 경고(보통으로 저하) - 구성 요소에 위험하지 않은 오류가 있습니다. 보통으로 저하 상태는 **이벤트** 페이지의 **유형** 열에서 *경고*로 표시됩니다.
- 위험(심각하게 저하) - 구성 요소에 위험한 오류가 있습니다.

노트: *알 수 없음* 상태는 Dell Inc 공급자에서 Proactive HA 상태 업데이트를 사용할 수 없음을 나타냅니다. 다음 경우에 알 수 없음 상태가 발생할 수 있습니다.

- OMIVV에서 적절한 상태로 초기화할 때까지 Proactive HA 클러스터에 추가된 모든 호스트는 알 수 없음 상태가 몇 분 동안 유지될 수 있습니다.
- vCenter Server를 다시 시작하면 OMIVV에서 적절한 상태로 다시 초기화할 때까지 Proactive HA 클러스터의 호스트가 알 수 없음 상태가 될 수 있습니다.

OMIVV가 지원되는 구성 요소의 중복 상태가 변경되었음을 감지하는 경우(트랩 또는 폴링을 통해), 구성 요소의 상태 업데이트 알림을 vCenter Server로 보냅니다. 폴링은 한 시간마다 실행되며 트랩 손실 가능성을 대비해 유사시 대기 메커니즘으로 사용할 수 있습니다.

노트:

- 이벤트를 구성할 때 모든 이벤트 게시 옵션을 이벤트 게시 수준으로 선택하는 것이 좋습니다. 구성 이벤트에 대한 자세한 내용은 이벤트 및 알람 구성 페이지 86을(를) 참조하십시오.
- Proactive HA는 전원, 팬, IDSDM의 중복성을 지원하는 플랫폼에서만 사용할 수 있습니다.
- Proactive HA 기능은 중복성을 구성할 수 없는 PSU에 지원되지 않습니다(예: 케이블로 연결된 PSU).

Proactive HA 이벤트

Proactive HA에 대해 VMware에서 지원되는 구성 요소에 따라 Dell Inc 공급자는 vCenter에 등록 중 다음 이벤트를 등록합니다.

표 5. Dell Proactive HA 이벤트

Dell Inc 공급자 이벤트	구성 요소 유형	설명
DellFanRedundancy	팬	팬 중복성 이벤트
DellPowerRedundancy	전원 공급 장치(PSU)	전원 중복성 이벤트
DellIDSDMRedundancy	스토리지	IDSDM 중복성 이벤트 **노트:** 호스트가 Proactive HA가 활성화된 클러스터에 추가되고 IDSDM 구성 요소가 존재하면 iDRAC 설정에서 내부 SD 카드 이중화를 **미러**로 구성하였는지 확인합니다.

Proactive HA 사용 가능 호스트의 경우 구성 요소의 중복 상태를 판단하기 위해 OMIVV에서 트리거로 다음 트랩을 사용합니다.

표 6. Proactive HA 이벤트

이벤트 이름	설명	심각도
팬 정보	팬 정보	정보
팬 경고	팬 경고	경고
팬 오류	팬 오류	위험
전원 공급 장치 정상	전원 공급 장치가 정상으로 돌아옴	정보
전원 공급 장치 경고	전원 공급 장치에서 경고를 감지함	경고
전원 공급 장치 오류	전원 공급 장치에서 장애를 감지함	위험
전원 공급 장치 없음	전원 공급 장치가 없음	위험
중복성 정보	중복성 정보	정보
중복성 저하	중복성이 저하됨	경고
중복성 손실	중복성이 손실됨	위험
통합 듀얼 SD 모듈 정보	통합 듀얼 SD 모듈(IDSDM) 정보	정보
통합 듀얼 SD 모듈 경고	통합 듀얼 SD 모듈 경고	경고
통합 듀얼 SD 모듈 오류	통합 듀얼 SD 모듈 오류	위험
통합 듀얼 SD 모듈 없음	통합 듀얼 SD 모듈이 없음	위험
통합 듀얼 SD 모듈 중복성 정보	통합 듀얼 SD 모듈 중복성 정보	정보
통합 듀얼 SD 모듈 중복성 저하	통합 듀얼 SD 모듈 중복성이 저하됨	경고
통합 듀얼 SD 모듈 중복성 손실	통합 듀얼 SD 모듈 중복성이 손실됨	위험
섀시 이벤트		
팬 정보	팬 정보	정보
팬 경고	팬 경고	경고
팬 오류	팬 오류	위험
전원 공급 장치 정상	전원 공급 장치가 정상으로 돌아옴	정보
전원 공급 장치 경고	전원 공급 장치에서 경고를 감지함	경고
전원 공급 장치 오류	전원 공급 장치에서 장애를 감지함	위험
중복성 정보	중복성 정보	정보

표 6. Proactive HA 이벤트 (계속)

이벤트 이름	설명	심각도
중복성 저하	중복성이 저하됨	경고
중복성 손실	중복성이 손실됨	위험

랙 및 타워 서버에 대한 Proactive HA 구성

세 개의 지원되는 중복 구성 요소(전원 공급 장치, 팬 및 IDSDM) 모두의 중복성에 대해 모든 호스트가 구성되었는지 확인합니다.

1. 호스트 자격 증명 프로필을 생성하고 호스트를 호스트 자격 증명 프로필에 연결합니다. 호스트 자격 증명 프로필 생성 페이지 35을(를) 참조하십시오.
2. 호스트 인벤토리가 성공적으로 완료되었는지 확인합니다. 호스트 인벤토리 작업 보기 페이지 71을(를) 참조하십시오.
3. iDRAC에서 SNMP 트랩 대상이 OMIVV 어플라이언스 IP 주소로 설정되었는지 확인합니다.
   노트: 로그 데이터에서 Proactive HA 클러스터에 대한 호스트의 가용성을 확인합니다.
4. 클러스터에서 Proactive HA를 활성화합니다. 클러스터에서 Proactive HA 활성화를 참조하십시오.

모듈형 서버에 대한 Proactive HA 구성

모듈형 서버에 대한 Proactive HA를 구성하기 전에 다음 조건이 충족되는지 확인하십시오.

- 세 개의 호스트 서버 중복 구성 요소(전원 공급 장치, 팬 및 IDSDM) 모두의 중복성에 대해 모든 호스트가 올바르게 구성되었습니다.
- 호스트 및 섀시 인벤토리가 성공적으로 완료되었습니다.

노트: 섀시 구성 요소(PSU 및 팬) 오류는 모든 연결된 서버에 영향을 미치므로 Proactive HA 클러스터의 모든 모듈형 호스트를 동일한 섀시에 두지 않는 것이 좋습니다.

1. 호스트 자격 증명 프로필을 생성하고 호스트를 호스트 자격 증명 프로필에 연결합니다. 호스트 자격 증명 프로필 생성 페이지 35을(를) 참조하십시오.
2. 호스트 인벤토리가 성공적으로 완료되었는지 확인합니다. 호스트 인벤토리 작업 보기 페이지 71을(를) 참조하십시오.
   노트: 로그 데이터에서 Proactive HA 클러스터에 대한 호스트의 가용성을 확인합니다.
3. 연결된 섀시에 대한 섀시 자격 증명 프로필을 생성합니다. 섀시 자격 증명 프로필 생성 페이지 39을(를) 참조하십시오.
4. 섀시 인벤토리가 성공적으로 완료되었는지 확인합니다. 섀시 인벤토리 작업 보기 페이지 73을(를) 참조하십시오.
5. CMC 또는 OME-Modular를 실행하고 섀시의 트랩 대상이 OMIVV 어플라이언스 IP 주소로 설정되어 있는지 확인합니다. 트랩 구성에 대한 자세한 내용은 **dell.com/support**에서 제공되는 CMC 및 OME-Modular 사용자 가이드를 참조하십시오.
6. 클러스터에서 Proactive HA를 활성화합니다. 클러스터에서 Proactive HA 활성화를 참조하십시오.

클러스터에서 Proactive HA 활성화

클러스터에서 Proactive HA를 활성화하기 전에 다음 조건이 충족되는지 확인하십시오.

- DRS가 활성화된 클러스터가 vCenter 콘솔에 활성화되고 구성되었습니다. 클러스터에서 DRS를 활성화하려면 VMware 설명서를 참조하십시오.
- 클러스터의 일부인 모든 호스트는 호스트 자격 증명 프로필의 일부이어야 하고 성공적으로 인벤토리되어야 합니다.
- 모듈형 서버의 경우 해당 섀시를 섀시 자격 증명 프로필에 추가하고 성공적으로 인벤토리되어야 합니다.

1. vSphere Client에서 **메뉴**를 확장한 후 **호스트 및 클러스터**를 선택합니다.
   모든 호스트 및 클러스터가 왼쪽 창에 표시됩니다.
2. 클러스터를 선택하고 오른쪽 창에서 **vSphere DRS** > **편집**을 클릭합니다.
3. **vSphere DRS**를 선택합니다(선택하지 않은 경우).
4. **구성** > **vSphere 가용성** > **Proactive HA** > **편집**을 선택합니다.
   클러스터 설정 편집 페이지가 표시됩니다.
5. **클러스터 설정 편집** 페이지에서 **Proactive HA**를 선택합니다.
6. **실패 및 응답** 섹션의 드롭다운 메뉴에서 **수동** 또는 **자동** 자동화 수준을 선택합니다.

7. **문제 해결**의 경우 심각도 상태(혼합 모드)에 따라 격리 모드, 유지 보수 모드 또는 격리 모드와 유지 보수 모드를 모두 선택합니다. 자세한 내용은 VMware 설명서를 참조하십시오.
8. **공급자**를 클릭하고 클러스터에 대한 공급자로 **Dell Inc**를 선택합니다.
9. **저장**을 클릭합니다.

클러스터에서 Proactive HA가 활성화되면 OMIVV에서 Proactive HA 상태 및 중복성 상태를 초기화하고 vCenter에 보고합니다. vCenter Server는 OMIVV의 상태 업데이트 알림에 따라 **문제 해결**을 위해 선택한 수동 또는 자동 작업을 수행합니다.

기존 심각도를 재정의하려면 상태 업데이트 알림의 심각도 재정의 페이지 80를 참조하십시오.

등록된 PHA 클러스터용 Dell 상태 업데이트 공급자에서 수행되는 모든 맞춤 구성은 RPM 업그레이드 및 백업 및 복원 작업 후에 기본값으로 복원됩니다.

상태 업데이트 알림의 심각도 재정의

사용자 환경에 적합하게 맞춤 구성된 심각도로 Dell EMC 호스트 및 구성 요소에 대해 Dell Proactive HA 이벤트의 기존 심각도를 재정의하도록 구성할 수 있습니다.

각 Proactive HA 이벤트에 해당하는 심각도 수준은 다음과 같습니다.

- **정보**
- **보통으로 저하**
- **심각하게 저하**

노트: 정보 심각도 수준으로 Proactive HA 구성 요소의 심각도를 사용자 정의할 수 없습니다.

1. OpenManage Integration for VMware vCenter에서 **설정** > **Proactive HA의 심각도 재정의**를 클릭합니다.
   데이터 그리드는 지원되는 모든 Proactive HA 이벤트를 표시합니다. 데이터 그리드 열에는 호스트 및 구성 요소의 심각도를 맞춤 구성하기 위한 이벤트 ID, 이벤트 설명, 구성 요소 유형, 기본 심각도, 심각도 재정의 열이 포함됩니다.
2. 호스트 또는 구성 요소의 심각도를 변경하려면 **심각도 재정의** 열의 드롭다운 목록에서 필요한 상태를 선택합니다.
   이 정책은 OMIVV에 등록된 모든 vCenter 서버의 모든 Proactive HA 호스트에 적용됩니다.
3. 맞춤 구성해야 하는 모든 이벤트에 대해 2단계를 반복합니다.
4. 다음 작업 중 하나를 수행합니다.
   a. 맞춤 구성 사항을 저장하려면 **적용**을 클릭합니다.
   b. 심각도 설정 재정의를 취소하려면 **취소**를 클릭합니다.

   심각도 설정 재정의를 기본값으로 재설정하려면 **기본값으로 재설정**을 클릭합니다.

초기 구성

OMIVV의 기본 설치와 vCenter 등록을 완료한 후에 vCenter에서 OMIVV를 실행하면 초기 구성 마법사가 자동으로 처음 표시됩니다.

나중에 초기 구성 마법사를 실행하려면 다음으로 이동하십시오.

- **설정** > **초기 구성 마법사** > **초기 구성 마법사 시작**
- **대시보드** > **빠른 참조** > **초기 구성 마법사 시작**

1. **시작** 페이지에서 지침을 읽은 후 **시작하기**를 클릭합니다.
2. **vCenter 선택** 페이지의 **vCenters** 드롭다운 메뉴에서 특정 vCenter 또는 **등록된 모든 vCenter**를 선택한 후 **다음**을 클릭합니다.
   노트: 같은 OMIVV 어플라이언스로 등록된 동일한 PSC에 속하는 vCenter Server가 여러 개 있고 단일 vCenter Server를 선택하여 구성하는 경우 각 vCenter를 구성할 때까지 2단계를 반복합니다.
3. **호스트 자격 증명 프로필 생성** 페이지에서 **호스트 자격 증명 프로필 생성**을 클릭합니다.
   호스트 자격 증명 프로필 생성에 대한 자세한 내용은 호스트 자격 증명 프로필 생성 페이지 35을(를) 참조하십시오.

   호스트 자격 증명 프로필에 호스트를 추가하면 OMIVV의 IP 주소가 호스트의 iDRAC에 대한 SNMP 트랩 대상으로 자동 설정됩니다. OMIVV는 WBEM 서비스를 활성화하여 ESXi 6.5 이상을 실행하는 호스트의 iDRAC IP를 검색한 다음 WBEM 서비스를 비활성화합니다.

   OMIVV는 WBEM 서비스를 사용하여 ESXi 호스트 및 iDRAC 관계를 적절하게 동기화합니다. 특정 호스트에 대한 SNMP 트랩 대상 구성에 실패하거나 특정 호스트에 대한 WBEM 서비스 활성화에 실패하면 이러한 호스트는 비준수로 나열됩니다. 비준수 항목을 보고 해결하려면 비준수 호스트 해결 페이지 64의 을 참조하십시오.
4. **추가 설정 구성** 페이지에서 다음을 수행합니다.
   a. 인벤토리 작업을 예약합니다. 인벤토리 작업 예약에 대한 자세한 내용은 인벤토리 작업 예약 페이지 95을(를) 참조하십시오.

b. 보증 검색 작업을 예약합니다. 보증 검색 작업 예약에 대한 자세한 내용은 보증 검색 작업 예약 페이지 95을(를) 참조하십시오.

   인벤토리 작업 일정을 수정하려면 **설정** > **vCenter 설정** > **데이터 검색 일정** > **인벤토리 검색** 또는 **작업** > **인벤토리** > **호스트 인벤토리**로 이동합니다.

   보증 검색 작업 일정을 수정하려면 **설정** > **vCenter 설정** > **데이터 검색 일정** > **보증 검색** 또는 **작업** > **보증**으로 이동합니다.

c. 이벤트 및 알람을 구성합니다. 이벤트 및 알람 구성에 대한 자세한 내용은 이벤트 및 알람 구성 페이지 86을(를) 참조하십시오.

d. 개별 설정을 적용하려면 **적용** 버튼을 따로 클릭한 후 **다음**을 클릭합니다.

   모든 추가 설정을 활성화하는 것이 좋습니다. 추가 설정 중 하나라도 적용되지 않으면 모든 추가 설정이 필수임을 나타내는 메시지가 표시됩니다.

5. **다음 단계** 페이지에서 지침을 읽은 후 **마침**을 클릭합니다.

   OMIVV 호스트를 사용하면 호스트 및 연결된 클러스터에서 발생하는 구성 변경 사항을 면밀히 모니터링할 수 있기 때문에 OMIVV 호스트를 구성 기준선과 연결하는 것이 좋습니다. OMIVV에서 호스트를 성공적으로 관리하면 모든 클러스터에 대해 구성 기준선을 생성할 수 있습니다. 구성 기준선을 만들려면 다음을 수행합니다.

   - 펌웨어 및 드라이버용 리포지토리 프로필을 생성하면 기본 펌웨어 및 드라이버 버전을 정의할 수 있습니다.
   - 시스템 프로필을 생성하면 호스트의 기본 하드웨어 구성을 정의할 수 있습니다.
   - 클러스터 프로필 생성 - 기본값을 생성하려면 클러스터를 선택하여 펌웨어, 드라이버 및 하드웨어 구성에 연결하십시오.
   - iDRAC IPv4를 비활성화한 PowerEdge MX 섀시에 있는 호스트는 섀시 자격 증명 프로필을 사용하여 관리해야 합니다.

초기 구성 상태 보기

초기 구성 마법사 페이지에서 다음을 수행할 수 있습니다.

- 초기 구성 상태 보기

  초기 구성 상태는 모든 vCenter가 호스트 자격 증명 프로필, 이벤트 및 알람, 인벤토리 및 보증 작업으로 구성된 경우에만 완료됨으로 표시됩니다.

- 초기 구성 마법사 시작

펌웨어 업데이트 설정

iDRAC 작업 지우기 및 iDRAC 재설정 확인란을 선택하면, 호스트에서 펌웨어를 업데이트하기 전에 iDRAC 재설정 이전 **작업 대기열**에 있는 모든 iDRAC 작업을 지웁니다.

iDRAC 작업 지우기 및 iDRAC 재설정 설정은 다음 작업을 수행할 때 사용됩니다.

- OMIVV를 사용하여 펌웨어 업데이트

  이 설정은 OMIVV를 사용하여 펌웨어를 업데이트하는 동안 재정의될 수 있습니다. 하지만 설정을 재정의하더라도 **펌웨어 업데이트 설정** 페이지에서 수행하는 설정에는 영향을 주지 않습니다.

- vSphere Lifecycle Manager를 사용하여 펌웨어 문제 해결

  펌웨어 문제 해결 작업을 수행하는 동안에는 이 설정을 재정의할 수 없습니다.

1. **iDRAC 작업 지우기 및 iDRAC 재설정** 확인란을 선택합니다.
2. **적용**을 클릭합니다.

라이선스 정보 보기

OMIVV 라이선스를 업로드하면 다수의 지원되는 호스트 및 vCenter Server가 이 탭에 표시됩니다.

소프트웨어 라이선스를 구매하려면 **소프트웨어 라이선스** 옆에 있는 **라이선스 구입**을 클릭합니다. 자세한 내용은 소프트웨어 라이선스 구입 페이지 82을(를) 참조하십시오.

라이선스 페이지에 다음과 같은 정보가 표시됩니다.

라이선스 유형	설명
호스트 라이선스	• 사용 가능한 라이선스 사용 가능한 라이선스 수 표시 • 사용 중인 라이선스 사용 중인 라이선스 수 표시
vCenter 라이선스	• 사용 가능한 라이선스 사용 가능한 라이선스 수 표시 • 사용 중인 라이선스 사용 중인 라이선스 수 표시

라이선스 관리 섹션에는 다음에 대한 링크가 표시됩니다.

- 제품 라이선싱 포털(Digital Locker)
- 관리 콘솔

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.

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/support**의 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 문의**로 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 프로필에 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.

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.

소프트웨어 라이선스 구입

1. **설정** > **라이선싱** > **라이선스 구입** 또는 **대시보드** > **라이선스 구입** 또는 **관리 포털** > **vCenter 등록** > **라이선싱** > **지금 구입**으로 이동합니다.
   DellEMC 지원 페이지가 표시됩니다.
2. 라이선스 파일을 다운로드하여 알려진 위치에 저장합니다.

라이선스 파일이 .zip 파일 내에 압축되어 있을 수 있습니다. zip 파일의 압축을 풀고 라이선스 .xml 파일만 업로드해야 합니다. 라이선스 파일의 이름은 주문 번호를 기준으로 지정될 것입니다(예: 123456789.xml).

액세스 지원 정보

표 7. 지원 페이지 정보

이름	설명
문서 지원	다음과 같은 설명서 링크를 제공합니다. • PowerEdge 서버 • OMIVV 매뉴얼 • LifeCycle Controller가 포함된 iDRAC
관리 콘솔	Administration Console에 대한 링크를 제공합니다.
일반 도움말	Dell EMC 지원 사이트에 대한 링크를 제공합니다.
iDRAC 재설정	iDRAC이 응답하지 않을 때 사용할 수 있는 iDRAC을 재설정하기 위한 링크를 제공합니다. 이를 사용하면 iDRAC이 정상적으로 재부팅됩니다. iDRAC 재설정에 대한 자세한 내용은 iDRAC 재설정 페이지 83을(를) 참조하십시오.
기술 지원에 전화하기 전에	Dell EMC 지원 부서에 연락하고 통화를 올바르게 연결하는 방법에 대한 팁을 제공합니다.
문제 해결 번들	문제 해결 번들을 생성하고 다운로드할 수 있는 링크를 제공합니다. 기술 지원에 문의할 때 이 번들을 제공하거나 볼 수 있습니다. 자세한 내용은 문제 해결 번들 생성 및 다운로드 페이지 83을(를) 참조하십시오.
Dell EMC 권장 사항	DRM(Dell EMC Repository Manager) 지원 페이지에 대한 링크를 제공합니다. DRM은 펌웨어 및 변경 사항 감지를 업데이트하는 데 사용할 수 있는 사용자 지정 카탈로그를 생성하는 데에 사용됩니다.

문제 해결 번들 생성 및 다운로드

문제 해결 번들을 생성하려면 관리 포털에 로그인해야 합니다.

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.

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.

iDRAC 재설정

iDRAC을 재설정하면 iDRAC이 정상적으로 다시 부팅됩니다. iDRAC을 재설정한 후에 iDRAC은 일반적으로 다시 시작되지만 호스트는 다시 시작되지 않습니다. 재설정한 후 몇 분이 지나야만 iDRAC을 사용할 수 있습니다. OMIVV 어플라이언스에서 iDRAC이 응답하지 않는 경우에만 재설정합니다.

- 한 번 이상 인벤토리 작업이 수행되었고 호스트 자격 증명 프로필의 일부인 호스트에서만 이 재설정 작업을 적용할 수 있습니다.
- Dell EMC에서는 호스트를 유지 보수 모드로 전환한 다음 iDRAC을 재설정할 것을 권장합니다.
- iDRAC을 재설정한 후 iDRAC을 사용할 수 없거나 응답을 멈추는 경우 iDRAC을 하드 리셋하십시오. 하드 리셋에 대한 자세한 내용은 https://www.dell.com/support/에서 제공되는 iDRAC 사용자 가이드를 참조하십시오.

iDRAC이 다시 부팅되는 동안에 다음과 같은 상황이 발생할 수 있습니다.

- OMIVV가 호스트 상태를 검색하는 동안 통신이 지연됩니다.

- 현재 iDRAC에 대해 열려 있는 모든 세션이 종료됩니다.
- iDRAC의 DHCP 주소 변경. iDRAC에서 DHCP를 사용하여 IP 주소를 생성하는 경우 iDRAC IP 주소가 변경될 수 있습니다. 이 경우에는 호스트 인벤토리 작업을 다시 실행하여 인벤토리 데이터에서 새로운 iDRAC IP 주소를 구하십시오.

1. **지원** 페이지에서 **iDRAC 재설정**을 클릭합니다.
2. **iDRAC 재설정** 페이지에서 호스트 이름 또는 IP 주소를 입력합니다.
3. iDRAC 재설정 프로세스를 이해하였다는 것을 확인하려면 **iDRAC 재설정의 영향을 이해합니다**를 선택합니다. **선택한 호스트에서 계속 iDRAC 재설정** 확인란.
4. **iDRAC 재설정**을 클릭합니다.

15

vCenter 설정 관리

이벤트 및 알람 정보

설정 페이지에서 호스트 및 섀시에 대한 이벤트 및 알람을 활성화하고 이벤트 게시 수준을 선택하고 기본 알람을 복원할 수 있습니다. 각 vCenter에 대해 또는 등록된 모든 vCenter에 대해 이벤트 및 알람을 구성할 수 있습니다. 섀시에 해당하는 이벤트 및 알람은 vCenter와 연결되어 있습니다.

4개의 이벤트 게시 수준은 다음과 같습니다.

표 8. 이벤트 게시 수준

이벤트	설명
이벤트 게시하지 않음	OMIVV가 이벤트나 알림을 연결된 vCenter에 전달하지 못하게 하십시오.
모든 이벤트 게시	비공식적인 이벤트를 포함하여 OMIVV 호스트가 관리되는 Dell EMC 호스트로부터 수신하는 모든 이벤트를 연결된 vCenter에 게시합니다. **모든 이벤트 게시** 옵션을 이벤트 게시 수준으로 선택할 것을 권장합니다.
위험 및 경고 이벤트만 게시	위험 또는 경고 수준의 이벤트만 연결된 vCenter에 게시합니다.
가상화 관련 위험 및 경고 이벤트만 게시	호스트에서 수신한 가상화 관련 이벤트를 관련 vCenter에 게시합니다. 가상화 관련 이벤트는 가상 시스템을 실행 중인 호스트에 가장 위험한 수준으로 분류된 이벤트입니다.

이벤트 및 알람을 구성할 때 위험 수준의 하드웨어 알람은 OMIVV 어플라이언스를 트리거하여 호스트 시스템을 유지 보수 모드로 전환할 수 있습니다. 특정한 경우 가상 시스템을 다른 호스트 시스템으로 마이그레이션합니다. OMIVV는 관리되는 호스트에서 vCenter로 수신된 이벤트를 전달하고 해당 이벤트에 대해 알람을 생성합니다. 이러한 알람은 다시 부팅, 유지 보수 모드 또는 마이그레이션 등과 같은 조치를 vCenter로부터 트리거하기 위해 사용됩니다.

예를 들어, 전원 공급 장치에서 오류가 발생하여 알람이 생성되면 후속 조치로 시스템을 유지 보수 모드로 전환합니다. 즉, 워크로드가 클러스터에 있는 다른 호스트로 마이그레이션됩니다.

클러스터 외부에 있거나 VMware DRS(Distributed Resource Scheduling)가 사용되지 않는 클러스터 내부에 있는 모든 호스트에서는 위험 이벤트로 인해 가상 시스템이 종료될 수 있습니다. Dell EMC는 Dell 알람을 활성화하기 전에 DRS를 활성화하는 것을 권장합니다. 자세한 내용은 VMware 설명서를 참조하십시오.

DRS는 리소스 풀에서의 사용량을 지속적으로 모니터링하고 비즈니스 필요에 따라 가상 시스템 간에 사용 가능한 리소스를 지능적으로 할당합니다. 중요 하드웨어 이벤트에서 가상 시스템이 자동으로 마이그레이션되는지 확인하려면 DRS가 구성된 Dell 알람을 사용하십시오. 화면 메시지 세부 정보는 영향을 받을 수 있는 vCenter 인스턴스의 클러스터를 나열합니다. 이벤트 및 알람을 활성화하기 전에 클러스터에 영향이 있는지 확인하십시오.

기본 알람 설정을 복원하려면 **알람 복원** 옵션을 선택합니다. 이 옵션은 제품을 제거하거나 재설치하지 않고도 기본 알람 구성을 복원하는 데 유용한 옵션입니다. 설치 후 Dell EMC 알람 구성이 변경된 경우 **알람 복원** 옵션을 사용하면 해당 변경 사항을 되돌릴 수 있습니다.

노트: Dell 이벤트를 수신하려면 iDRAC, CMC 및 관리 컨트롤러에서 필수 이벤트를 활성화해야 합니다.

노트: OMIVV는 호스트에서 가상 시스템을 성공적으로 실행하는 데 필수인 가상화 관련 이벤트를 미리 선택합니다. 기본적으로 Dell 호스트 알람은 비활성화되어 있습니다. Dell EMC 알람이 활성화된 경우 클러스터에서 DRS를 사용하여 중요 이벤트를 보내는 가상 시스템이 자동으로 마이그레이션되도록 해야 합니다.

이벤트 및 알람 구성

서버에서 이벤트를 수신하려면 iDRAC에서 SNMP 트랩 대상이 설정되었는지 확인합니다. OMIVV는 SNMP v1 및 v2 알림을 지원합니다.

1. OMIVV 홈 페이지에서 **설정** > **vCenter 설정** > **이벤트 및 알람**을 클릭합니다.
2. 모든 호스트 및 섀시에 대한 알람을 활성화하려면 **모든 호스트 및 섀시 알람 활성화**를 클릭합니다.
   Dell EMC 알람 경고 활성화 페이지에는 Dell EMC 알람을 활성화한 후 영향을 받을 수 있는 클러스터와 클러스터링되지 않은 호스트가 표시됩니다.

   노트: 알람이 활성화된 Dell EMC 호스트가 유지 보수 모드로 전환되어 일부 특정 위험 이벤트에 대응합니다. 필요한 경우 알람을 수정할 수 있습니다.

   노트: vCenter 6.7 U1 및 6.7 U2 버전에서 편집 옵션이 실패합니다. 알람 정의를 편집하려면 웹 클라이언트(FLEX)를 사용하는 것이 좋습니다.

   노트: BMC 트랩에 메시지 ID가 없어 알림에 OMIVV의 자세한 내용이 포함되지 않습니다.
3. 변경을 수락하려면 **계속**을 클릭합니다.
   모든 호스트 및 섀시에 대한 알람이 활성화됩니다.
4. 다음 이벤트 게시 수준 중 하나를 선택합니다.
   - **이벤트 게시하지 않음** – 이벤트나 알림을 연결된 vCenter에 전달하지 않습니다.
   - **모든 이벤트 게시** – 정보 제공 이벤트를 포함한 모든 이벤트와 관리되는 호스트 및 섀시에서 수신되는 이벤트를 관련 vCenter에 게시합니다. 모든 이벤트 게시 옵션을 이벤트 게시 수준으로 선택하는 것이 좋습니다.
   - **위험 및 경고 이벤트만 게시** – 위험 및 경고 수준 이벤트만 연결된 vCenter에 게시합니다.
   - **가상화 관련 이벤트만 게시** – 호스트에서 수신한 가상화 관련 이벤트를 연결된 vCenter에 게시합니다. 가상화 관련 이벤트는 VM을 실행하는 호스트에 가장 중요한 이벤트입니다.
5. 변경 사항을 저장하려면 **적용**을 클릭합니다.
   관리되는 모든 호스트 및 섀시에서 기본 vCenter 알람 설정을 복원하려면 **알람 복원**을 클릭합니다. 변경이 적용되는 데 1분 정도 걸릴 수 있습니다.

   경고 복원 옵션은 제품을 제거하거나 다시 설치하지 않고도 기본 알람 구성을 복원하는 데 편리한 방법입니다. 설치 후 Dell EMC 알람 구성이 변경된 경우 **알람 복원** 옵션을 사용하면 변경사항이 되돌려집니다.

   노트: 이벤트 및 알람 설정은 어플라이언스 복원 후 활성화되지 않습니다. 설정 탭에서 이벤트 및 알람 설정을 다시 활성화할 수 있습니다.

섀시 이벤트 보기

1. vSphere Client에서 **메뉴**를 확장한 후 **호스트 및 클러스터**를 선택합니다.
2. 왼쪽 창에서 vCenter의 인스턴스를 선택합니다.
3. 오른쪽 창에서 **모니터링** > **작업 및 이벤트** > **이벤트**를 클릭합니다.
4. 자세한 내용을 보려면 특정 이벤트를 선택합니다.

   노트: MCM 구성이 있는 PowerEdge MX 섀시에서 이벤트의 소스는 리드 섀시로 표시되지만 메시지 세부 정보에는 식별을 위해 구성원 섀시의 서비스 태그가 포함됩니다.

섀시 알람 보기

1. vSphere Client에서 **메뉴**를 확장한 후 **호스트 및 클러스터**를 선택합니다.
2. 왼쪽 창에서 vCenter의 인스턴스를 선택합니다.
3. 오른쪽 창에서 **모니터** > **문제 및 알람** > **트리거된 알람**을 클릭합니다.
4. **트리거된 알람**에서 알람 이름을 클릭하여 알람 정의를 봅니다.

알람 및 이벤트 설정 보기

알람 및 이벤트를 구성한 후에 설정 탭에서 호스트에 vCenter 알람이 활성화되어 있는지 여부와 선택된 이벤트 게시 수준을 볼 수 있습니다.

1. OMIVV 홈 페이지에서 **설정** > **이벤트 및 알람**을 클릭합니다.
   다음과 같은 세부 사항이 표시됩니다.
   - Dell EMC 호스트의 vCenter 알람 - **활성화됨** 또는 **비활성화됨**으로 표시됩니다.
   - 이벤트 게시 수준
2. 이벤트 및 알람을 구성합니다. 이벤트 및 알람 구성 페이지 86을(를) 참조하십시오.

이벤트 게시 수준을 보려면 이벤트 및 알람 정보 페이지 85을(를) 참조하십시오.

가상화 관련 이벤트

다음 표에는 가상화와 관련된 위험 및 경고 이벤트와 이벤트 이름, 설명, 심각도 수준, 권장 작업이 나와 있습니다.

가상화 관련 이벤트는 다음 형식으로 표시됩니다.

Dell-Message ID:<ID number>, 메시지:<Message Description>.

섀시 이벤트는 다음 형식으로 표시됩니다.

Dell-메시지:<Message description>, 섀시 이름:<name of the chassis>, 섀시 서비스 태그:<chassis Service Tag>, 섀시 위치:<chassis location>

표 9. 가상화 이벤트

이벤트 이름	설명	심각도	권장 작업
Dell-alertHWCAuditWarning	하드웨어 구성 경고	경고	작업 안 함
Dell-alertHWCAuditInformation	하드웨어 구성 정보	정보	작업 안 함
Dell-alertLiquidCoolingLeakInformational	디바이스에서 이전에 탐지되었던 소량 누출이 해결되었음	정보	작업 안 함
Dell-alertLiquidCoolingLeakWarning	디바이스에서 소량 누출이 탐지됨	경고	작업 안 함
Dell-alertLiquidCoolingLeakFailure	디바이스에서 대량 누출이 탐지됨	위험	입력 전원을 분리한 다음, 서비스 공급업체에 즉시 문의하십시오.
Dell-alertStorageSoftwareDefinedSubSystemFailure	소프트웨어 정의 스토리지 하위 시스템 오류	위험	메시지에서 식별된 하드 드라이브의 상태를 확인하고 작업을 재시도합니다. iDRAC GUI의 상태를 확인하려면 iDRAC 대시보드에서 **스토리지** > **물리적 디스크**를 클릭합니다. CLI(Command Line Interface)에서 다음 RACADM 명령을 실행합니다. `racadm raid get pdisks -o -p status` 스토리지 풀에 물리적 드라이브를 더 추가하고 작업을 재시도합니다.
Dell-alertStorageSoftwareDefinedSubSystemWarning	소프트웨어 정의 스토리지 하위 시스템 경고	경고	작업 안 함
Dell-alertTemperatureProbeReadWarning	온도 센서를 읽을 수 없음	경고	작업 안 함
Dell-alertTemperatureProbeChangeFailure	온도 상승 오류	위험	섀시 이벤트 로그에서 팬 이슈를 확인하고 발생한 이슈를 해결합니다. 팬 이슈가 탐지되지 않으면, 섀시 주변 온도를 확인하고 온도가 작동 범위 내에 있는지 확인합니다. 섀시 주변 온도를 확인하려면 다음 RACADM

표 9. 가상화 이벤트 (계속)

이벤트 이름	설명	심각도	권장 작업
			명령을 실행합니다. `racadm getsensorinfo`
Dell-전류 센서가 경고 값을 감지함	지정된 시스템의 전류 센서가 경고 임계값을 초과했습니다.	경고	작업 안 함
Dell-전류 센서가 고장 값을 감지함	지정된 시스템의 전류 센서가 오류 임계값을 초과했습니다.	오류	시스템을 유지 보수 모두에 배치
Dell-전류 센서가 복구할 수 없는 값을 감지함	지정된 시스템의 전류 센서가 복구할 수 없는 오류를 감지함	오류	작업 안 함
Dell-중복성이 반환됨	정상 값으로 반환된 센서	정보	작업 안 함
Dell-중복성이 저하됨	지정된 시스템의 중복성 센서가 중복 단위의 구성 요소 중 하나가 실패하지만 장치가 계속해서 중복됨을 감지했습니다.	경고	작업 안 함
Dell-중복성이 없음	지정된 시스템의 중복성 센서가 중복 단위의 구성 요소 중 하나의 연결이 해제되고 오류가 발생했거나 현재 없음을 감지했습니다.	오류	시스템을 유지 보수 모두에 배치
Dell-전원 공급 장치가 정상으로 돌아옴	정상 값으로 반환된 센서	정보	작업 안 함
Dell-전원 공급 장치가 경고를 감지함	지정된 시스템에서 전원 공급 장치 센서 수치가 사용자 정의 가능한 경고 임계값을 초과했습니다.	경고	작업 안 함
Dell-전원 공급 장치가 고장을 감지함	전원 공급 장치의 연결이 해제되었거나 오류가 발생했습니다.	오류	시스템을 유지 보수 모두에 배치
Dell-전원 공급 장치 센서가 복구할 수 없는 값을 감지함	지정된 시스템의 전원 공급 장치가 복구할 수 없는 오류를 감지했습니다.	오류	작업 안 함
Dell-메모리 디바이스 상태 경고	메모리 디바이스 수정 등급이 적정 값을 초과했습니다.	경고	작업 안 함
Dell-메모리 디바이스 오류	메모리 디바이스 수정 등급이 적정 수준을 초과했거나 메모리 스패어 뱅크가 활성화되었거나 멀티비트 ECC 오류가 발생했습니다.	오류	시스템을 유지 보수 모두에 배치
Dell-팬 인클로저가 시스템에 삽입됨	정상 값으로 반환된 센서	정보	작업 안 함

표 9. 가상화 이벤트 (계속)

이벤트 이름	설명	심각도	권장 작업
Dell-팬 인클로저가 시스템에서 제거됨	지정된 시스템에서 팬 인클로저가 제거됨	경고	작업 안 함
Dell-팬 인클로저가 연장된 시간 동안 시스템에서 제거됨	사용자 정의 가능한 기간 동안 지정된 시스템에서 팬 인클로저가 제거됨	오류	작업 안 함
Dell-팬 인클로저 센서가 복구할 수 없는 값을 감지함	지정된 시스템의 팬 인클로저 센서가 복구할 수 없는 오류를 감지함	오류	작업 안 함
Dell-AC 전원이 복원됨	정상 값으로 반환된 센서	정보	작업 안 함
Dell-AC 전원 손실됨 경고	AC 전원 코드에서 전원이 손실되었지만 경고로 분류될 만큼 중복됩니다.	경고	작업 안 함
Dell-AC 전원 코드에서 전원이 손실됨	AC 전원 코드에서 전원이 손실되고 오류로 분리되기에는 중복성이 부족합니다.	오류	작업 안 함
Dell-프로세서 센서가 정상 값으로 반환됨	정상 값으로 반환된 센서	정보	작업 안 함
Dell-프로세서 센서가 경고 값을 감지함	지정된 시스템의 프로세서 센서가 정체 상태입니다.	경고	작업 안 함
Dell-프로세서 센서가 오류 값을 감지함	지정된 시스템의 프로세서 센서가 비활성화되고 구성 오류가 발생했거나 가열 트립이 발생했습니다.	오류	작업 안 함
Dell-프로세서 센서가 복구할 수 없는 값을 감지함	지정된 시스템의 프로세서 센서에 오류가 발생했습니다.	오류	작업 안 함
Dell-디바이스 구성 오류	지정된 시스템의 플러그형 디바이스에 대한 구성 오류가 감지되었습니다.	오류	작업 안 함
Dell-배터리 센서가 정상 값으로 반환됨	정상 값으로 반환된 센서	정보	작업 안 함
Dell-배터리 센서가 경고 값을 감지함	지정된 시스템의 배터리 센서가 배터리의 예상 오류 상태에 있음을 감지했습니다.	경고	작업 안 함
Dell-배터리 센서가 오류 값을 감지함	지정된 시스템의 배터리 센서가 배터리에 오류가 있음을 감지했습니다.	오류	작업 안 함
Dell-배터리 센서가 복구할 수 없는 값을 감지함	지정된 시스템의 배터리 센서가 배터리	오류	작업 안 함

표 9. 가상화 이벤트 (계속)

이벤트 이름	설명	심각도	권장 작업
	에 오류가 있음을 감지했습니다.		
Dell-가열 종료 보호가 시작됨	오류 이벤트로 인해 시스템에 가열 종료가 구성된 경우 이 메시지가 생성됩니다. 온도 센서 수치가 시스템에 구성된 오류 임계값을 초과하는 경우 운영 체제가 종료되고 시스템의 전원이 꺼집니다. 연장된 기간 동안 시스템에서 팬 인클로저가 제거된 경우 특정 시스템에서 이 이벤트가 시작될 수도 있음	오류	작업 안 함
Dell-온도 센서가 정상 값으로 반환됨	정상 값으로 반환된 센서	정보	작업 안 함
Dell-온도 센서가 경고 값을 감지함	지정된 시스템에 있는 백플레인 보드, 시스템 보드, CPU 또는 드라이브 이동 장치의 온도 센서가 경고 임계값을 초과했습니다.	경고	작업 안 함
Dell-온도 센서가 오류 값을 감지함	지정된 시스템에 있는 백플레인 보드, 시스템 보드, 또는 드라이브 이동 장치의 온도 센서가 오류 임계값을 초과했습니다.	오류	시스템을 유지 보수 모두에 배치
Dell-온도 센서가 복구할 수 없는 값을 감지함	지정된 시스템에 있는 백플레인 보드, 시스템 보드 또는 드라이브 이동 장치의 온도 센서가 복구할 수 없는 오류를 감지했습니다.	오류	작업 안 함
Dell-팬 센서가 정상 값으로 반환됨	정상 값으로 반환된 센서	정보	작업 안 함
Dell-팬 센서가 경고 값을 감지함	호스트 <x>의 팬 센서 수치가 경고 임계값을 초과했습니다.	경고	작업 안 함
Dell-팬 센서가 오류 값을 감지함	지정된 시스템의 팬 센서가 하나 이상의 팬에서 오류를 감지했습니다.	오류	시스템을 유지 보수 모두에 배치
Dell-팬 센서가 복구할 수 없는 값을 감지함	팬 센서가 복구할 수 없는 오류를 감지했습니다.	오류	작업 안 함
Dell-전압 센서가 정상 값으로 반환됨	정상 값으로 반환된 센서	정보	작업 안 함

표 9. 가상화 이벤트 (계속)

이벤트 이름	설명	심각도	권장 작업
Dell-전압 센서가 경고 값을 감지함	지정된 시스템의 전압 센서가 경고 임계값을 초과했습니다.	경고	작업 안 함
Dell-전압 센서가 오류 값을 감지함	지정된 시스템의 전압 센서가 오류 임계값을 초과했습니다.	오류	시스템을 유지 보수 모두에 배치
Dell-전압 센서가 복구할 수 없는 값을 감지함	지정된 시스템의 전압 센서가 복구할 수 없는 오류를 감지했습니다.	오류	작업 안 함
Dell-전류 센서가 정상 값으로 반환됨	정상 값으로 반환된 센서	정보	작업 안 함
Dell-스토리지: 스토리지 관리 오류	스토리지 관리에서 디바이스에 종속되지 않는 오류 상태를 감지했습니다.	오류	시스템을 유지 보수 모두에 배치
Dell-스토리지: 컨트롤러 경고	물리적 디스크의 일부가 손상되었습니다.	경고	작업 안 함
Dell-스토리지: 컨트롤러 오류	물리적 디스크의 일부가 손상되었습니다.	오류	시스템을 유지 보수 모두에 배치
Dell-스토리지: 채널 오류	채널 오류	오류	시스템을 유지 보수 모두에 배치
Dell-스토리지: 인클로저 하드웨어 정보	인클로저 하드웨어 정보	정보	작업 안 함
Dell-스토리지: 인클로저 하드웨어 경고	인클로저 하드웨어 경고	경고	작업 안 함
Dell-스토리지: 인클로저 하드웨어 오류	인클로저 하드웨어 오류	오류	시스템을 유지 보수 모두에 배치
Dell-스토리지: 어레이 디스크 장애	어레이 디스크 장애	오류	시스템을 유지 보수 모두에 배치
Dell-스토리지: EMM 오류	EMM 오류	오류	시스템을 유지 보수 모두에 배치
Dell-스토리지: 전원 공급 장치 오류	전원 공급 장치 오류	오류	시스템을 유지 보수 모두에 배치
Dell-스토리지: 온도 센서 경고	너무 차갑거나 너무 뜨거운 물리적 디스크 온도 센서 경고입니다.	경고	작업 안 함
Dell-스토리지: 온도 센서 오류	너무 차갑거나 너무 뜨거운 물리적 디스크 온도 센서 오류입니다.	오류	시스템을 유지 보수 모두에 배치
Dell-스토리지: 팬 오류	팬 오류	오류	시스템을 유지 보수 모두에 배치
Dell-스토리지: 배터리 경고	배터리 경고	경고	작업 안 함
Dell-스토리지: 가상 디스크 성능이 저하됨 경고	가상 디스크 성능이 저하됨 경고	경고	작업 안 함
Dell-스토리지: 가상 디스크 성능 저하 오류	가상 디스크 성능 저하 오류	오류	시스템을 유지 보수 모두에 배치
Dell-스토리지: 온도 센서 정보	온도 센서 정보	정보	작업 안 함

표 9. 가상화 이벤트 (계속)

이벤트 이름	설명	심각도	권장 작업
Dell-스토리지: 어레이 디스크 경고	어레이 디스크 경고	경고	작업 안 함
Dell-스토리지: 어레이 디스크 정보	어레이 디스크 정보	정보	작업 안 함
Dell-스토리지: 전원 공급 장치 경고	전원 공급 장치 경고	경고	작업 안 함
Dell-Fluid Cache 디스크 장애	Fluid Cache 디스크 장애	오류	시스템을 유지 보수 모두에 배치
Dell-케이블 연결 실패 또는 위험 이벤트	케이블 연결 실패 또는 위험 이벤트	오류	시스템을 유지 보수 모두에 배치
Dell-Chassis Management Controller가 경고 감지	Chassis Management Controller가 경고 감지	경고	작업 안 함
Dell-Chassis Management Controller가 오류 감지	Chassis Management Controller가 오류 감지	오류	시스템을 유지 보수 모두에 배치
Dell-IO 가상화 실패 또는 위험 이벤트	IO 가상화 실패 또는 위험 이벤트	오류	시스템을 유지 보수 모두에 배치
Dell-링크 상태 경고	링크 상태 경고	경고	작업 안 함
Dell-링크 상태 실패 또는 위험 이벤트	링크 상태 실패 또는 위험 이벤트	오류	시스템을 유지 보수 모두에 배치
Dell-보안 경고	보안 경고	경고	작업 안 함
Dell-시스템: 소프트웨어 구성 경고	시스템: 소프트웨어 구성 경고	경고	작업 안 함
Dell-시스템: 소프트웨어 구성 오류	시스템: 소프트웨어 구성 오류.	오류	시스템을 유지 보수 모두에 배치
Dell-스토리지 보안 경고	스토리지 보안 경고	경고	작업 안 함
Dell-스토리지 보안 실패 또는 위험 이벤트	스토리지 보안 실패 또는 위험 이벤트	오류	시스템을 유지 보수 모두에 배치
Dell-소프트웨어 변경사항 업데이트 경고	소프트웨어 변경사항 업데이트 경고	경고	작업 안 함
Dell-Chassis Management Controller 감사 경고	Chassis Management Controller 감사 경고	경고	작업 안 함
Dell-Chassis Management Controller 감사 실패 또는 위험 이벤트	Chassis Management Controller 감사 실패 또는 위험 이벤트	오류	시스템을 유지 보수 모두에 배치
Dell-PCI 디바이스 감사 경고	PCI 디바이스 감사 경고	경고	작업 안 함
Dell 전원 공급 장치 감사 경고	전원 공급 장치 감사 경고	경고	작업 안 함
Dell-전원 공급 장치 감사 실패 또는 위험 이벤트	전원 공급 장치 감사 실패 또는 위험 이벤트	오류	시스템을 유지 보수 모두에 배치
Dell-전원 사용 감사 경고	전원 사용 감사 경고	경고	작업 안 함
Dell-전원 사용 감사 실패 또는 위험 이벤트	전원 사용 감사 실패 또는 위험 이벤트	오류	시스템을 유지 보수 모두에 배치
Dell-보안 구성 경고	보안 구성 경고	경고	작업 안 함

표 9. 가상화 이벤트 (계속)

이벤트 이름	설명	심각도	권장 작업
Dell-구성: 소프트웨어 구성 경고	구성: 소프트웨어 구성 경고	경고	작업 안 함
Dell-구성: 소프트웨어 구성 오류	구성: 소프트웨어 구성 오류	오류	시스템을 유지 보수 모두에 배치
Dell-가상 디스크 파티션 실패	가상 디스크 파티션 실패	오류	시스템을 유지 보수 모두에 배치
Dell-가상 디스크 파티션 경고	가상 디스크 파티션 경고	경고	작업 안 함
iDRAC 이벤트 **노트:** 클러스터에 속한 모든 Proactive HA 사용 가능 호스트의 경우, 다음과 같은 가상화 이벤트가 Proactive HA 이벤트에 매핑됩니다. "팬이 중복되지 않음" 및 "전원 공급 장치가 중복되지 않음"과 같은 이벤트는 매핑되지 않습니다.			
팬이 중복됩니다.	없음	정보	작업 안 함
팬 중복성이 손실되었습니다.	팬 중 하나에 문제가 발생했거나 팬을 제거했거나 추가 팬이 필요한 구성 변경이 발생했습니다.	위험	오류가 있는 팬을 분리한 후 다시 설치하거나 다른 팬을 설치합니다.
팬 중복성이 저하되었습니다.	팬 중 하나에 문제가 발생했거나 팬을 제거했거나 추가 팬이 필요한 구성 변경이 발생했습니다.	경고	오류가 있는 팬을 분리한 후 다시 설치하거나 다른 팬을 설치합니다.
팬이 중복되지 않습니다.	팬 중 하나에 문제가 발생했거나 팬을 제거했거나 추가 팬이 필요한 구성 변경이 발생했습니다.	정보	오류가 있는 팬을 분리한 후 다시 설치하거나 다른 팬을 설치합니다.
팬이 중복되지 않습니다. 리소스가 부족하여 정상적인 작동을 유지할 수 없습니다.	팬 중 하나에 문제가 발생했거나 팬을 제거했거나 추가 팬이 필요한 구성 변경이 발생했습니다.	위험	오류가 있는 팬을 분리한 후 다시 설치하거나 다른 팬을 설치합니다.
전원 공급 장치가 중복됩니다.	없음	정보	작업 안 함
전원 공급 장치 중복성이 손실되었습니다.	전원 공급 장치 예외, 전원 공급 장치 인벤토리 변경 또는 시스템 전원 인벤토리 변경 때문에 현재의 전원 작동 모드가 중복되지 않습니다. 시스템은 이전에 전원 중복 모드였습니다.	위험	이벤트 로그에서 전원 공급 장치 오류를 확인합니다. 시스템 구성 및 소비 전력을 검토하십시오.
전원 공급 장치 중복성이 저하되었습니다.	전원 공급 장치 예외, 전원 공급 장치 인벤토리 변경 또는 시스템 전원 인벤토리 변경 때문에 현재의 전원 작동 모드가 중복되지 않습니다. 시스템은 이전에 전원 중복 모드였습니다.	경고	이벤트 로그에서 전원 공급 장치 오류를 확인합니다. 시스템 구성 및 소비 전력을 검토하십시오.

표 9. 가상화 이벤트 (계속)

이벤트 이름	설명	심각도	권장 작업
전원 공급 장치가 중복되지 않습니다.	현재의 전원 공급 장치 구성이 중복성을 보장하기 위한 플랫폼 요구 사항을 충족하지 못합니다. 전원 공급 장치에 오류가 발생하면 시스템이 종료될 수 있습니다.	정보	이 문제가 의도치 않게 발생한 경우라면 시스템 구성 및 소비 전력을 검토하고 그에 따라 전원 공급 장치를 설치합니다. 전원 공급 장치 상태를 점검하여 오류가 없는지 확인하십시오.
전원 공급 장치가 중복되지 않습니다. 리소스가 부족하여 정상적인 작동을 유지할 수 없습니다.	시스템 전원이 꺼지거나 시스템이 성능 저하 상태에서 작동할 수 있습니다.	위험	이벤트 로그에서 전원 공급 장치 오류를 확인합니다. 시스템 구성 및 소비 전력을 검토하고 그에 따라 전원 공급 장치를 업그레이드하거나 설치하십시오.
내부 듀얼 SD 모듈이 중복됨	없음	정보	작업 안 함
내부 이중 SD 모듈 중복성이 손실되었습니다.	SD 카드 중 하나 또는 SD 카드 두 개 모두 올바로 작동하지 않습니다.	위험	오류가 발생한 SD 카드를 교체하십시오.
내부 이중 SD 모듈 중복성이 저하되었습니다.	SD 카드 중 하나 또는 SD 카드 두 개 모두 올바로 작동하지 않습니다.	경고	오류가 발생한 SD 카드를 교체하십시오.
내부 듀얼 SD 모듈이 중복되지 않음	없음	정보	중복이 필요하면 SD 카드를 추가로 설치하고 구성하여 중복되도록 하십시오.
섀시 이벤트			
전원 공급 장치 중복성이 손실되었습니다.	전원 공급 장치 예외, 전원 공급 장치 인벤토리 변경 또는 시스템 전원 인벤토리 변경 때문에 현재의 전원 작동 모드가 중복되지 않습니다. 시스템은 이전에 전원 중복 모드였습니다.	위험	이벤트 로그에서 전원 공급 장치 오류를 확인합니다. 시스템 구성 및 소비 전력을 검토하십시오.
전원 공급 장치 중복성이 저하되었습니다.	전원 공급 장치 예외, 전원 공급 장치 인벤토리 변경 또는 시스템 전원 인벤토리 변경 때문에 현재의 전원 작동 모드가 중복되지 않습니다. 시스템은 이전에 전원 중복 모드였습니다.	경고	이벤트 로그에서 전원 공급 장치 오류를 확인합니다. 시스템 구성 및 소비 전력을 검토하십시오.
전원 공급 장치가 중복됩니다.	없음	정보	작업 안 함
전원 공급 장치가 중복되지 않습니다.	현재의 전원 공급 장치 구성이 중복성을 보장하기 위한 플랫폼 요구 사항을 충족하지 못합니다. 전원 공급 장치에 오류가 발생하면 시스템이 종료될 수 있습니다.	정보	이 문제가 의도치 않게 발생한 경우라면 시스템 구성 및 소비 전력을 검토하고 그에 따라 전원 공급 장치를 설치합니다. 전원 공급 장치 상태를 점검하여 오류가 없는지 확인하십시오.
전원 공급 장치가 중복되지 않습니다. 리소스가 부족하여 정상적인 작동을 유지할 수 없습니다.	시스템 전원이 꺼지거나 시스템이 성능	위험	이벤트 로그에서 전원 공급 장치 오류를 확인합니다. 시스템 구성 및 소비 전력을 검토

표 9. 가상화 이벤트 (계속)

이벤트 이름	설명	심각도	권장 작업
	저하 상태에서 작동할 수 있습니다.		하고 그에 따라 전원 공급 장치를 업그레이드하거나 설치하십시오.
팬 중복성이 손실되었습니다.	팬 중 하나에 문제가 발생했거나 팬을 제거했거나 추가 팬이 필요한 구성 변경이 발생했습니다.	위험	오류가 있는 팬을 분리한 후 다시 설치하거나 다른 팬을 설치합니다.
팬 중복성이 저하되었습니다.	팬 중 하나에 문제가 발생했거나 팬을 제거했거나 추가 팬이 필요한 구성 변경이 발생했습니다.	경고	오류가 있는 팬을 분리한 후 다시 설치하거나 다른 팬을 설치합니다.
팬이 중복됩니다.	없음	정보	작업 안 함
팬이 중복되지 않습니다.	팬 중 하나에 문제가 발생했거나 팬을 제거했거나 추가 팬이 필요한 구성 변경이 발생했습니다.	정보	오류가 있는 팬을 분리한 후 다시 설치하거나 다른 팬을 설치합니다.
팬이 중복되지 않습니다. 리소스가 부족하여 정상적인 작동을 유지할 수 없습니다.	팬 중 하나에 문제가 발생했거나 팬을 제거했거나 추가 팬이 필요한 구성 변경이 발생했습니다.	위험	오류가 있는 팬을 분리한 후 다시 설치하거나 다른 팬을 설치합니다.

데이터 검색 일정 관리

인벤토리 작업 예약

OMIVV에서 최신 인벤토리 데이터를 보려면 정기적으로 실행되도록 인벤토리 작업을 예약하여 호스트 또는 섀시의 인벤토리 정보를 최신 상태로 유지해야 합니다. 인벤토리 작업은 매주 실행하는 것이 좋습니다.

노트: 섀시는 OMIVV 컨텍스트로 관리됩니다. 섀시 관리에는 vCenter의 컨텍스트가 없습니다. 예약된 호스트 인벤토리가 완료되면 OMIVV를 사용하여 관리되는 모든 섀시에 대해 섀시 인벤토리가 트리거됩니다.

노트: 이 페이지의 설정은 구성 마법사가 호출될 때마다 기본값으로 재설정됩니다. 이전에 인벤토리에 대한 일정을 구성한 경우 마법사 기능을 완료하기 전에 이전 일정이 기본 설정으로 재정의되지 않도록 이 페이지의 이전 일정을 복제해야 합니다.

1. OMIVV 홈 페이지에서 **설정** > **vCenter 설정** > **데이터 검색 일정** > **인벤토리 검색**을 클릭합니다.
2. **인벤토리 데이터 검색 활성화**(권장) 확인란을 선택합니다.

   vCenter 서버가 여러 개인 PSC 환경에서 개별 vCenter의 일정이 다르며 인벤토리 일정을 업데이트하기 위해 **모든 등록된 vCenter** 옵션을 선택하는 경우 인벤토리 일정 설정 페이지에 기본 일정이 표시됩니다.
3. 인벤토리 데이터 검색 날짜와 시간을 선택하고 **적용**을 클릭합니다.

   노트: vCenter 서버가 여러 개인 PSC 환경에서 **모든 등록된 vCenter**의 인벤토리 일정을 업데이트하는 경우 업데이트가 개별 vCenter 인벤토리 일정 설정보다 우선 적용됩니다.

보증 검색 작업 예약

1. 인증 키를 업데이트하려면 인덱스 카탈로그(`https://downloads.dell.com/catalog/CatalogIndex.gz`)에 대한 액세스 권한이 있는지 확인하십시오.
2. 보증 보고서를 받으려면 `https://apigtwb2c.us.dell.com`에 대한 액세스 권한이 있는지 확인하십시오.

3. 호스트 및 섀시에서 인벤토리가 올바르게 실행되는지 확인합니다.
4. OMIVV의 보증 기능을 사용하려면 인터넷에 연결되어 있어야 합니다. 인터넷 연결에 프록시가 필요한 환경에서는 관리 포털에서 프록시 설정을 구성해야 합니다.

하드웨어 보증 정보는 Dell 온라인에서 검색하고 OMIVV에서 표시합니다. 서비스 태그만 전송되고 Dell 온라인에 저장되지 않습니다.

여러 개의 vCenter 서버가 있는 PSC 환경에서는 vCenter에 대한 보증이 실행되면 모든 vCenter에 대하여 섀시 보증이 자동으로 실행됩니다. 하지만 보증은 섀시 자격 증명 프로필에 추가되지 않을 경우 자동으로 실행되지 않습니다.

노트: 이 페이지의 설정은 구성 마법사가 호출될 때마다 기본값으로 재설정됩니다. 이전에 보증 검색 작업을 구성한 경우에는 이전 보증 검색이 기본 설정으로 재정의되지 않도록 마법사 기능을 완료하기 전에 이 페이지에서 해당하는 보증 검색 작업 예약을 복제해야 합니다.

1. OMIVV 홈 페이지에서 **설정** > **vCenter 설정** > **데이터 검색 일정** > **보증 검색**을 클릭합니다.
2. **보증 데이터 검색 활성화(권장)** 확인란을 선택합니다.

   vCenter 서버가 여러 개인 PSC 환경에서 개별 vCenter의 일정이 다르며 보증 일정을 업데이트하기 위해 **모든 등록된 vCenter** 옵션을 선택하는 경우 보증 일정 설정 페이지에 기본 일정이 표시됩니다.
3. 보증 데이터 검색 날짜와 시간을 선택하고 **적용**을 클릭합니다.

   노트: vCenter 서버가 여러 개인 PSC 환경에서 **모든 등록된 vCenter**의 보증 일정을 업데이트하는 경우 업데이트가 개별 vCenter 보증 일정 설정보다 우선 적용됩니다.

16

섀시 관리

Dell EMC 섀시 정보 보기

OMIVV를 사용하여 검색하고 인벤토리 작업을 수행한 섀시 정보를 볼 수 있습니다. Dell EMC 섀시에는 OMIVV를 사용하여 관리하는 모든 섀시가 나열됩니다.

1. OMIVV 홈 페이지에서 **호스트 및 섀시** > **섀시** > **섀시 목록**을 클릭합니다.
   다음 정보가 표시됩니다.
   - **이름** - 각 Dell EMC 섀시의 IP 주소 링크를 표시합니다.
   - **상태** - 섀시의 상태를 표시합니다.

     각 Dell EMC 섀시의 상태별로 필터링하려면 검색에 대해 나타나는 필터 아이콘을 클릭합니다.
   - **IP 주소/FQDN** - vCenter IP 주소 또는 FQDN을 표시합니다.
   - **서비스 태그** - 섀시의 서비스 태그를 표시합니다.
   - **섀시 URL** - 섀시 URL을 표시합니다.
   - **모델** - 모델 이름을 표시합니다.
   - **역할** - MX 섀시에만 해당합니다. 섀시의 역할(리드 또는 구성원)을 표시합니다.
   - **마지막 인벤토리** - 마지막 인벤토리 정보를 표시합니다.
   - **사용 가능한 슬롯** - 섀시에서 사용할 수 있는 슬롯을 표시합니다.
   - **프로필 이름** - 섀시가 연결되어 있는 섀시 자격 증명 프로필 이름을 표시합니다.
   - **위치** - 섀시의 위치를 표시합니다.

   인벤토리를 실행하지 않으면 **이름**, **마지막 인벤토리**, **사용 가능한 슬롯**, **프로필 이름**, **위치** 및 섀시 인벤토리 정보가 표시되지 않습니다.

   노트: MCM 구성의 PowerEdge MX 섀시의 경우에는 리드 섀시를 사용하여 전체 MCM 인프라를 관리합니다. 구성원 섀시 IP 및 iDRAC IP가 비활성화되거나 섀시 역할이 변경되는 경우 Dell EMC는 기존 리드 섀시를 제거하고 새 리드 섀시 IP를 다시 추가한 다음 섀시 자격 증명 프로필에 연결할 것을 권장합니다.
2. 펌웨어, 라이선스 유형 및 보증 관련 정보를 보려면 섀시를 선택합니다.
   인벤토리를 실행하지 않으면 **이름**, **펌웨어**, **라이선스 유형** 및 **보증** 정보가 표시되지 않습니다.

섀시 인벤토리 정보 보기

1. **Dell EMC 섀시** 페이지에서 섀시를 선택하거나 서비스 태그를 클릭합니다.
2. **섀시 정보** 섹션에서 **보기**를 클릭합니다.
   개요 페이지에는 섀시 상태, 활성 오류, 섀시의 구성 요소 수준 상태, 하드웨어 개요 및 섀시 관계(MX 섀시에만 해당)가 표시됩니다.

   노트: M1000e 버전 4.3 및 이전 버전에서는 활성 오류가 표시되지 않습니다.

   기본 창에는 섀시의 전반적 상태가 표시됩니다. 유효한 상태 표시등은 **정상**, **경고**, **위험** 및 **알 수 없음**입니다. 섀시 상태 그리드 보기에 각 구성 요소의 상태가 표시됩니다. 이들 섀시 상태 매개변수는 VRTX 버전 1.0 이상과 M1000e 버전 4.4 이상에 적용됩니다. 4.3 이전의 M1000e 펌웨어 버전에서는 정상과 경고 또는 위험처럼 두 가지 상태 표시등만 표시됩니다.

   전체적인 상태에는 상태 매개변수가 가장 낮은 섀시를 기초로 하여 상태가 표시됩니다. 예를 들어, 정상 기호가 5개 있고 경고 기호가 1개 있는 경우 전체적인 상태는 경고로 표시됩니다.

섀시의 하드웨어 인벤토리 정보 보기

선택한 섀시에 대해 하드웨어 인벤토리에 관한 정보를 볼 수 있습니다.

1. OMIVV 홈 페이지에서 **호스트 및 섀시** > **섀시** > **섀시 목록**을 클릭합니다.
   Dell EMC 섀시 페이지가 표시됩니다.
2. 섀시를 선택하고 서비스 태그 링크를 클릭합니다.
   개요 페이지가 표시됩니다.
3. **개요** 페이지에서 **하드웨어**를 클릭합니다.

표 10. 하드웨어 인벤토리 정보

하드웨어 인벤토리: 구성 요소	OMIVV 탐색	정보

팬	• **Dell EMC 섀시** 페이지에서 **섀시** > **섀시 목록**을 클릭하고 서비스 태그 링크를 클릭합니다.
	• **개요** 페이지의 왼쪽 창에서 **하드웨어**를 선택합니다.
	• 오른쪽 창에서 **팬**을 확장합니다.
	또는
	• **개요** 페이지에서 **팬**을 클릭합니다.
		팬 정보:
		• 이름
		• 표시
		• 식별자(MX 섀시에만 적용)
		• 전원 상태
		• 판독값(RPM)
		• 경고 임계값(MX 섀시에는 적용되지 않음)
		• 중요 임계값(MX 섀시에는 적용되지 않음)
		  ○ 최소
		  ○ 최대
		• Pulse 너비 변조(MX 섀시에만 해당)
		노트: PowerEdge MX 섀시에서 팬을 제거한 경우에도 팬이 있는지의 여부가 '예'로 표시됩니다. 그러나 팬 상태는 **요약** 페이지에 활성 오류와 함께 **위험**으로 표시됩니다.

전원 공급 장치	• **Dell EMC 섀시** 페이지에서 **섀시** > **섀시 목록**을 클릭하고 서비스 태그 링크를 클릭합니다. • **개요** 페이지의 왼쪽 창에서 **하드웨어**를 선택합니다. • 오른쪽 창에서 **전원 공급 장치**를 확장합니다. **또는** • **개요** 페이지에서 **전원 공급 장치**를 클릭합니다.	전원 공급 장치 정보: • 이름 • 용량 • 표시 • 전원 상태 • 입력 전압(PowerEdge MX 섀시에만 해당)

온도 센서	• **Dell EMC 섀시** 페이지에서 **섀시** > **섀시 목록**을 클릭하고 서비스 태그 링크를 클릭합니다.
	• **개요** 페이지의 왼쪽 창에서 **하드웨어**를 선택합니다.
	• 오른쪽 창에서 **온도 센서**를 확장합니다.
	또는
	• **개요** 페이지에서 **온도 센서**를 클릭합니다.
		온도 센서 정보:
		• 위치
		• 판독값
		• 경고 임계값
		  ○ 최대
		  ○ 최소
		• 중요 임계값
		  ○ 최대
		  ○ 최소
		노트: PowerEdge M1000e 섀시의 섀시 온도 정보가 표시됩니다. 다른 섀시는 섀시 및 연결된 모듈형 서버의 온도 센서에 대한 정보가 표시됩니다.

I/O 모듈	• **Dell EMC 섀시** 페이지에서 **섀시** > **섀시 목록**을 클릭하고 서비스 태그 링크를 클릭합니다. • **개요** 페이지의 왼쪽 창에서 **하드웨어**를 선택합니다.	I/O 모듈 정보: • 슬롯/위치 • 표시 • 이름 • 패브릭 • 서비스 태그

표 10. 하드웨어 인벤토리 정보 (계속)

하드웨어 인벤토리: 구성 요소	OMIVV 탐색	정보
	• 오른쪽 창에서 **I/O 모듈**을 확장합니다. **또는** • **개요** 페이지에서 **I/O 모듈**을 클릭합니다.	• 전원 상태 • 역할 • 펌웨어 버전 • 하드웨어 버전 • IP 주소 • 서브넷 마스크 • 게이트웨이 • MAC 주소 • DHCP 활성화
패브릭(PowerEdge MX 섀시만 해당)	• **Dell EMC 섀시** 페이지에서 **섀시** > **섀시 목록**을 클릭하고 서비스 태그 링크를 클릭합니다. • **개요** 페이지의 왼쪽 창에서 **하드웨어**를 선택합니다. • 오른쪽 창에서 **패브릭**을 확장합니다. **또는** • **개요** 페이지에서 **패브릭**을 클릭합니다.	패브릭 구성 요소 정보: • 상태 • 패브릭 • 설명 • 스위치 개수 • 연산 개수 • 업링크 개수 패브릭에 연결된 스위치를 보기 위해 패브릭 구성 요소를 선택하면 하단 그리드에 다음 정보가 표시됩니다. • 스위치 • 섀시 • 슬롯 • 섀시 역할 • 스위치 모델

PCIe	• **Dell EMC 섀시** 페이지에서 **섀시** > **섀시 목록**을 클릭하고 서비스 태그 링크를 클릭합니다.
	• **개요** 페이지의 왼쪽 창에서 **하드웨어**를 선택합니다.
	• 오른쪽 창에서 **PCIe**를 확장합니다.
	또는
	• **개요** 페이지에서 **PCIe**를 클릭합니다.
		PCIe 정보:
		• PCIe 슬롯
		  ○ 슬롯
		  ○ 이름
		  ○ 전원 상태
		  ○ 패브릭
		• 서버 슬롯
		  ○ 이름
		  ○ 번호
		• 슬롯 유형
		• 서버 매핑
		• 할당 상태
		• 할당된 슬롯 전원
		• PCI ID
		• 벤더 ID
		노트: PCIe 정보는 M1000e 섀시에는 해당되지 않습니다.

iKVM(PowerEdge M1000e에만 해당)	• **Dell EMC 섀시** 페이지에서 **섀시** > **섀시 목록**을 클릭하고 서비스 태그 링크를 클릭합니다. • **개요** 페이지의 왼쪽 창에서 **하드웨어**를 선택하고 오른쪽 창에서 **iKVM**을 확장합니다. **또는**	iKVM 정보: • iKVM 이름 • 표시 • 펌웨어 버전 • 전면 패널 USB/비디오 활성화 • CMC CLI에 대한 액세스 허용 **노트:** iKVM 탭은 섀시에 iKVM 모듈이 포함되어 있는 경우에만 표시됩니다.

표 10. 하드웨어 인벤토리 정보 (계속)

하드웨어 인벤토리: 구성 요소	OMIVV 탐색	정보
	• **개요** 페이지에서 **iKVM**을 클릭합니다.	

펌웨어 인벤토리 정보 보기

선택한 섀시의 펌웨어 관련 정보를 볼 수 있습니다.

1. OMIVV 홈 페이지에서 **호스트 및 섀시** > **섀시** > **섀시 목록**을 클릭합니다.
   Dell EMC 섀시 페이지가 표시됩니다.
2. 섀시를 선택하고 서비스 태그 링크를 클릭합니다.
   개요 페이지가 표시됩니다.
3. **개요** 페이지에서 **펌웨어**를 클릭합니다.
   펌웨어에 대해 다음 정보가 표시됩니다.
   - 구성 요소
   - 현재 버전

   이 페이지에서 OpenManage Enterprise Modular 및 CMC를 실행할 수도 있습니다.

관리 컨트롤러 정보 보기

선택한 섀시에 대한 관리 컨트롤러 관련 정보를 볼 수 있습니다.

1. OMIVV 홈 페이지에서 **호스트 및 섀시** > **섀시** > **섀시 목록**을 클릭합니다.
   Dell EMC 섀시 페이지가 표시됩니다.
2. 섀시를 선택하고 서비스 태그 링크를 클릭합니다.
   개요 페이지가 표시됩니다.
3. **개요** 페이지에서 **관리 컨트롤러**를 클릭합니다.
   관리 컨트롤러에 대한 다음과 같은 정보가 표시됩니다.
   - 일반
     - 이름
     - 펌웨어 버전
     - 마지막 업데이트 시간
     - 섀시 위치
     - 하드웨어 버전
   - 공용 네트워크
     - DNS 도메인 이름
     - DNS의 DHCP 사용
     - MAC 주소
     - 중복 모드
     - 하드웨어 버전
   - IPv4 정보
     - IPv4 활성화
     - DHCP 활성화
     - IP 주소
     - 서브넷 마스크
     - 게이트웨이
     - 기본 DNS 서버
     - 대체 DNS 서버
   - IPv6 정보

- IPv6 활성화
- DHCP 활성화
- IP 주소
- 링크 로컬 주소
- 게이트웨이
- 기본 DNS 서버
- 대체 DNS 서버

- 로컬 액세스 구성
  - Quick Sync 하드웨어 있음
  - LCD 있음
  - LED 있음
  - KVM 활성화됨

노트: MCM 구성에 포함된 구성원 섀시의 네트워크 관련 정보 중 일부 속성은 **관리 컨트롤러** 섹션에 표시되지 않습니다.

스토리지 인벤토리 정보 보기

선택한 섀시의 스토리지 관련 정보를 볼 수 있습니다.

1. OMIVV 홈 페이지에서 **호스트 및 섀시** > **섀시** > **섀시 목록**을 클릭합니다.
   Dell EMC 섀시 페이지가 표시됩니다.
2. 섀시를 선택하고 서비스 태그 링크를 클릭합니다.
   개요 페이지가 표시됩니다.
3. **개요** 페이지에서 **스토리지**를 클릭합니다.

   스토리지에 대한 다음 정보가 표시됩니다.

   - 가상 디스크
   - 물리 디스크
   - 컨트롤러
   - 인클로저
   - 핫 스페어

   MX 섀시에 대해 다음과 같은 정보가 표시됩니다.

   - 슬롯 번호
   - 슬롯 이름
   - 모델
   - 서비스 태그
   - 펌웨어 버전
   - 자산 태그
   - 전원 상태
   - 할당 모드

   MX 섀시의 경우 드라이브에 대한 정보를 보려면 스토리지 슬레드를 클릭합니다. 하단 창에 다음의 드라이브 정보가 표시됩니다.

   - 상태
   - 상태
   - 슬롯
   - 슬롯 할당
   - 디스크 이름
   - 용량
   - 버스 프로토콜
   - 미디어

   PowerEdge MX 섀시의 디스크가 할당되지 않은 경우 슬롯 할당이 **NA**로 표시됩니다.

   M1000e 섀시의 경우, 스토리지 모듈이 있다면 다른 추가 정보 없이 다음과 같은 스토리지 세부 사항이 격자 형태로 표시됩니다.

   - 이름
   - 모델

- 서비스 태그
- IP 주소(스토리지로 연결되는 링크)
- 패브릭
- 그룹 이름
- 그룹 IP 주소(스토리지 그룹으로 연결되는 링크)

노트: 스토리지 아래의 강조 표시된 각 링크를 클릭하면 **보기** 표에 강조 표시된 각 항목에 대한 세부 정보가 표시됩니다. 보기 표에서 각 라인 항목을 클릭하면 강조 표시된 각 항목에 대한 세부 정보가 표시됩니다.

보증 정보 보기

선택한 섀시에 대한 보증 관련 정보를 볼 수 있습니다.

1. OMIVV 홈 페이지에서 **호스트 및 섀시** > **섀시** > **섀시 목록**을 클릭합니다.
   Dell EMC 섀시 페이지가 표시됩니다.
2. 섀시를 선택하고 서비스 태그 링크를 클릭합니다.
   개요 페이지가 표시됩니다.
3. **개요** 페이지에서 **보증**을 클릭합니다.

   보증 정보:

   - 공급자
   - 설명
   - 상태
   - 권리 유형
   - 시작 날짜
   - 종료 날짜
   - 남은 일 수
   - 마지막으로 업데이트한 날짜

   노트: 보증 상태를 보려면 보증 작업을 실행해야 합니다. 보증 검색 작업 예약 페이지 95을(를) 참조하십시오.

섀시 관련 호스트 보기

선택한 섀시 관련 호스트 정보를 볼 수 있습니다.

1. OMIVV 홈 페이지에서 **호스트 및 섀시** > **섀시** > **섀시 목록**을 클릭합니다.
   Dell EMC 섀시 페이지가 표시됩니다.
2. 섀시를 선택하고 서비스 태그 링크를 클릭합니다.
   개요 페이지가 표시됩니다.
3. **개요** 페이지에서 **관련 호스트**를 클릭합니다.
   연결된 호스트에 대해 다음과 같은 정보가 표시됩니다.

   - Hostname(호스트 이름)
   - 서비스 태그
   - 모델
   - iDRAC IP
   - 위치
   - 슬롯 위치
   - 마지막 인벤토리

4. 호스트에 대한 자세한 내용을 보려면 호스트를 선택하십시오.

관련 섀시 정보 보기

섀시 관계 섹션에 MCM 모드로 배포되는 MX 섀시의 섀시 간 관계가 표시됩니다.

노트: 관련 섀시 정보는 MCM 그룹에서 구성된 PowerEdge MX 섀시에만 해당됩니다.

1. OMIVV 홈 페이지에서 **호스트 및 섀시** > **섀시** > **섀시 목록**을 클릭합니다.
   Dell EMC 섀시 페이지가 표시됩니다.
2. 섀시를 선택하고 서비스 태그 링크를 클릭합니다.
   개요 페이지가 표시됩니다.

   개요 페이지의 **섀시 관계** 섹션에 리드 및 구성원 섀시와 관련된 모든 섀시 정보가 표시됩니다.

PowerEdge MX 섀시 관리

MX7000X 섀시를 관리하는 방식은 M1000e, VRTX 및 FX2과 같은 Dell EMC 섀시의 관리와 다릅니다.

관리 모듈 및 iDRAC IP에 대한 공용 IP가 있는 독립 실행형 모드로 MX 섀시를 관리할 수 있습니다. 또한 1개의 리드 및 다중 구성원이 있는MCM(Multi-Chassis Management) 모드에서 MX 섀시를 구성할 수 있습니다.

Dell EMC OpenManage Enterprise-Modular에서는 유선 MCM 그룹을 지원합니다. 유선 유형에서 섀시는 관리 모듈의 중복 포트를 통해 데이지 체인 방식 또는 유선으로 연결됩니다. 그룹을 생성하기 위해 선택한 섀시는 한 개 이상의 섀시에 데이지 체인 방식으로 연결되어야 합니다. 섀시 그룹 생성에 대한 자세한 내용은 dell.com/support의 *PowerEdge MX7000 사용자 가이드용 Dell EMC OpenManage Enterprise-Modular*를 참조하십시오.

다음과 같은 두 가지 방법으로 MX 섀시에 있는 서버를 관리할 수 있습니다.

1. **호스트 자격 증명 프로필을 사용하여 서버 관리**: 모든 기능이 지원되는 서버를 관리하는 표준 및 권장 방법입니다. 이 경우에 섀시는 MX 호스트 인벤토리가 완료된 후에만 검색됩니다. 호스트 자격 증명 프로필 생성에 대한 자세한 내용은 호스트 자격 증명 프로필 생성 페이지 35을(를) 참조하십시오.
2. **섀시 자격 증명 프로필을 사용하여 서버 관리**: 섀시 자격 증명 프로필을 사용하여 호스트를 관리하도록 선택하면 인벤토리, 모니터링, 펌웨어 및 드라이버 업데이트와 같은 OMIVV 기능이 지원됩니다. 섀시 자격 증명 프로필을 이용한 섀시 및 호스트 관리에 대한 자세한 내용은 섀시 자격 증명 프로필 생성 페이지 39을(를) 참조하십시오.

노트: OMIVV는 백업 리드 구성을 사용한 PowerEdge MX 섀시 관리를 지원하지 않습니다.

노트: iDRAC의 IPv4 주소가 비활성화되어 있는 경우에는 섀시 자격 증명 프로필을 사용하여 서버를 관리하도록 선택할 수 있습니다. 섀시 자격 증명 프로필을 사용하여 서버를 관리하는 경우에는 다음과 같은 OMIVV 기능이 지원되지 않습니다.

- iDRAC 잠금 모드
- 이 서버를 참조 서버로 사용하여 시스템 프로필을 캡처하는 기능
- OS 배포
- CSIOR 상태 얻기 또는 업데이트
- 서버 구성 규정 준수
- 소수의 재고 관련 정보

노트: 공용 IPv4 iDRAC IP를 사용하는 호스트는 섀시 자격 증명 프로필을 사용하여 관리할 수도 있습니다. 그러나 위에 나열된 기능이 지원되지 않으므로 이 방법은 권장하지 않습니다.

통합 섀시 관리 IP를 이용한 섀시 및 호스트 관리

호스트 자격 증명 프로필을 사용하여 관리하는 호스트에 대해 iDRAC IPv4가 비활성화되어 있으면 호스트 인벤토리가 실패하고 섀시가 검색되지 않습니다. 이 경우 섀시 및 관련 호스트를 관리하기 위해 섀시를 수동으로 추가하고 섀시 자격 증명 프로필에 연결해야 합니다.

통합 섀시 관리 IP를 사용하여 호스트를 관리하도록 선택하면 인벤토리, 모니터링, 펌웨어 및 드라이버 업데이트와 같은 OMIVV 기능이 지원됩니다. 다음은 통합 섀시 관리 IP를 사용하여 호스트 및 섀시를 관리하는 작업에 대한 높은 수준의 설명입니다.

1. MX 섀시를 추가합니다.

   MX 섀시 추가에 대한 자세한 내용은 PowerEdge MX 섀시 추가 페이지 104을(를) 참조하십시오.
2. 섀시 자격 증명 프로필을 생성하고 호스트를 연결합니다.

   섀시 자격 증명 프로필 생성에 대한 자세한 내용은 섀시 자격 증명 프로필 생성 페이지 39을(를) 참조하십시오.
3. 섀시 자격 증명 프로필을 사용하여 관리하는 섀시와 호스트 양쪽 모두에 대한 작업을 봅니다.
4. 섀시 및 호스트 인벤토리를 봅니다.

호스트 및 섀시 인벤토리에 대한 자세한 내용은 호스트 인벤토리 작업 보기 페이지 71 및 섀시 인벤토리 작업 보기 페이지 73을(를) 참조하십시오.

5. 섀시를 사용하여 관리하는 호스트에 대한 펌웨어 업데이트를 수행합니다.

   펌웨어 업데이트에 대한 자세한 내용은 펌웨어 업데이트 페이지 118을(를) 참조하십시오.

   노트: 섀시를 사용하여 호스트를 관리하는 경우에는 운영 체제 미설치 워크플로가 지원되지 않습니다.

PowerEdge MX 섀시 추가

유효한 IPv4 iDRAC IP를 가진 호스트를 호스트 자격 증명 프로필에 추가할 수 있으며, 호스트 인벤토리 중에는 관련 MX 섀시가 자동으로 검색되어 **Dell EMC 섀시** 페이지에 표시됩니다.

호스트에 대한 iDRAC IPv4가 비활성화된 경우 호스트 인벤토리가 실패하고 섀시가 검색되지 않습니다. 이 경우 섀시 및 관련 호스트를 관리하기 위해 MX 섀시를 수동으로 추가하고 섀시 자격 증명 프로필에 연결해야 합니다.

MX 섀시를 수동으로 추가하려면 다음을 수행하십시오.

1. **OMIVV** 홈 페이지에서 **호스트 및 섀시** > **섀시**를 클릭합니다.
2. **Dell EMC 섀시** 페이지에서 **MX 섀시 추가**를 클릭합니다.
3. 관리 모듈 IPv4 또는 FQDN 또는 호스트 이름을 입력하고 **확인**을 클릭합니다.

   IP를 입력하면 OMIVV가 해당 IP를 관리하고 있는지 확인합니다.

   노트: 호스트 이름 또는 FQDN을 사용하여 섀시를 추가하기 전에 DNS에 유효한 정방향 및 역방향 조회 항목이 생성되는지 확인합니다.

   노트: FQDN을 입력하면 섀시 URL이 FQDN과 함께 표시됩니다.

   해당 섀시가 **Dell EMC 섀시** 페이지에 추가됩니다.

4. 섀시 자격 증명 프로필을 생성하여 호스트를 섀시 자격 증명 프로필에 연결합니다. 섀시 자격 증명 프로필 생성에 대한 자세한 내용은 섀시 자격 증명 프로필 생성 페이지 39을(를) 참조하십시오.

노트: MX 섀시 IP 이외의 IP를 입력하면 테스트 연결이 실행되지 않으며 잘못된 입력 내용이 **Dell EMC 섀시** 페이지에 남아 있게 됩니다. 성공적으로 유효성을 검사한 섀시만 섀시 자격 증명 프로필과 연결됩니다.

노트: 추가된 MX 섀시에 연결되어 있는 등록된 vCenter에 호스트가 없으면 테스트 연결이 실패합니다.

노트: MCM 구성에서 구성된 PowerEdge MX 섀시의 경우 리드와 구성원이 동일한 자격 증명이 있어야 합니다.

MX 섀시 펌웨어 업데이트

펌웨어 업데이트를 예약하기 전에 다음 조건이 환경에서 충족되는지 확인합니다.

- MX 섀시가 섀시 자격 증명 프로필에 속하고 성공적으로 인벤토리에 포함되는지 확인합니다.
- 펌웨어 업데이트를 진행 중인 호스트가 있는 경우 섀시 펌웨어를 업데이트할 수 없습니다.

노트: MX 섀시 펌웨어 업데이트 기능을 사용하는 경우 관리 모듈 펌웨어만 업데이트할 수 있습니다.

1. OMIVV 홈 페이지에서 **호스트 및 섀시** > **섀시** > **섀시 목록** > **MX 섀시 펌웨어 업데이트**를 클릭합니다.
2. 마법사의 **섀시 펌웨어 업데이트** 페이지에서 지침을 읽은 후 **시작하기**를 클릭합니다.
3. **MX 섀시 목록**에서 하나 이상의 MX 섀시를 선택한 후 **다음**을 클릭합니다.
   다음 조건 중 하나가 환경에서 충족되지 않으면 섀시가 표시되지 않습니다.
   - OMIVV에서 섀시 펌웨어 업데이트가 진행 중입니다.
   - 섀시에 대해 섀시 자격 증명 프로필이 생성되지 않았습니다.
   - 섀시가 성공적으로 인벤토리되지 않았습니다.

   MCM 구성이 포함된 PowerEdge MX 섀시의 경우 리드 섀시만 선택할 수 있습니다. 구성원 섀시가 자동으로 선택됩니다.
4. **업데이트 소스 선택** 페이지에서 다음을 수행합니다.
   a. 드롭다운 메뉴에서 적절한 펌웨어 리포지토리 프로필을 선택합니다.

b. 선택한 섀시 및 펌웨어 리포지토리 프로필을 기반으로 식별된 시스템 카테고리에서 적절한 번들을 선택하십시오.

5. **펌웨어 구성 요소 선택** 페이지에서 업데이트가 필요한 펌웨어 구성 요소를 선택한 후 **다음**을 클릭합니다.

   카탈로그에서 사용 가능한 버전보다 낮은 버전 또는 같은 수준(최신)의 구성 요소는 선택할 수 없습니다. 다운그레이드 상태로 나열된 구성 요소를 선택하려면 **펌웨어 다운그레이드 허용**을 클릭합니다.

   MCM 구성과 연결된 PowerEdge MX 섀시에서 **펌웨어 다운그레이드 허용** 확인란이 선택되지 않은 경우에도 펌웨어 버전을 다운그레이드할 수 있습니다.

   업데이트 또는 다운그레이드하는 경우 구성원 섀시만 선택할 수 없습니다. 리드 섀시를 선택하면 구성원 섀시가 자동으로 선택됩니다.

   모든 페이지에서 모든 펌웨어 구성 요소를 선택하려면 을 클릭합니다.

   모든 페이지에서 모든 펌웨어 구성 요소를 지우려면 을 클릭합니다.

6. **작업 예약** 페이지에서 다음을 수행합니다.
   a. 펌웨어 업데이트 작업 이름 및 설명을 입력합니다. 설명은 선택적인 필드입니다.

      펌웨어 업데이트 작업 이름은 필수이며 이미 사용 중인 이름은 사용하지 말아야 합니다. 펌웨어 업데이트 작업 이름을 제거한 경우 작업 이름을 재사용할 수 있습니다.

   b. 업데이트를 적용할 적절한 예약 옵션을 선택합니다.

7. **요약 검토** 페이지에서 펌웨어 업데이트 세부 정보를 검토한 후 **마침**을 클릭합니다.

표 11. 각 배포 모드에서 동시에 실행되는 MX 섀시 펌웨어 업데이트의 총 수

배포 모드	동시에 실행되는 섀시 펌웨어 업데이트 수
작게	1
중간	1
크게	2
아주 크게	2

17

호스트 관리

OMIVV 호스트 보기

OMIVV 호스트 페이지에서 모든 OMIVV 관리 호스트를 볼 수 있습니다.

1. OMIVV 홈 페이지에서 **호스트 및 섀시** > **호스트**를 클릭합니다.
2. **OMIVV 호스트** 탭에서 다음과 같은 정보를 볼 수 있습니다.
   - **호스트 이름** – 호스트의 IP 주소를 표시합니다. 호스트 정보를 보려면 호스트를 선택합니다.
   - **상태** - 호스트의 상태를 표시합니다.

     각 Dell EMC 호스트의 상태별로 필터링하려면 검색에 대해 나타나는 필터 아이콘을 클릭합니다.
   - **vCenter** - 호스트의 vCenter IP 주소를 표시합니다.
   - **클러스터** - Dell EMC 호스트가 클러스터에 있는 경우 클러스터 이름을 표시합니다.
   - **호스트 자격 증명 프로필** - 호스트 자격 증명 프로필 이름을 표시합니다.

단일 호스트 모니터링

OMIVV에서 단일 호스트의 세부 정보를 볼 수 있습니다. **호스트 및 클러스터** 페이지에서 모든 OMIVV 호스트를 볼 수 있습니다. 자세한 내용을 보려면 특정 OMIVV 관리 호스트를 선택한 다음 **모니터링** > **OMIVV 호스트 정보**로 이동합니다.

호스트 요약 정보 보기

다양한 포틀릿이 표시되는 **요약** 페이지에서 개별 호스트의 호스트 요약 세부 정보를 볼 수 있습니다. 포틀릿 중 2개를 OMIVV에 적용할 수 있습니다. 2개 포틀릿은 다음과 같습니다.

- **OMIVV 호스트 상태**
- **OMIVV 호스트 정보**

2개의 포틀릿을 원하는 위치에 끌어 놓을 수 있으며 다른 포틀릿과 마찬가지로 요구 사항에 따라 이 2개의 포틀릿을 포맷하고 사용자 지정할 수 있습니다. 호스트 요약 세부 정보를 보려면 다음을 수행합니다.

1. OMIVV 홈 페이지에서 **메뉴**를 확장한 다음 **호스트 및 클러스터**를 선택합니다.
2. 왼쪽 창에서 특정 호스트를 선택합니다.
3. 오른쪽 창에서 **요약**을 클릭합니다.
4. 아래로 스크롤하여 OMIVV 서버 관리 포틀릿을 봅니다.

   OMIVV 호스트 정보 및 **OMIVV 호스트 상태** 섹션에서 다음 정보를 볼 수 있습니다.

표 12. OMIVV 호스트 정보

정보	설명
서비스 태그	서버의 서비스 태그를 표시합니다. 지원 부서에 전화로 문의할 때 이 ID를 사용하십시오.
모델 이름	서버의 모델 이름을 표시합니다.
결함 복원 메모리	BIOS 특성 상태를 표시합니다. BIOS 특성은 서버 초기 설치 중에 BIOS에서 활성화되고 서버의 메모리 작동 모드를 표시합니다. 메모리 작동 모드 값을 변경한 경우 시스템을 다시 시작합니다. 이는 FRM(Fault Resilient Memory)을 지원하고 ESXi 5.5

표 12. OMIVV 호스트 정보 (계속)

정보	설명
	이상 버전을 실행하는 PowerEdge 서버에 적용됩니다. BIOS 특성의 4가지 값은 다음과 같습니다. • 사용되고 보호됨: 이 값은 시스템이 지원되고 운영 체제 버전이 ESXi 5.5 이상이며 BIOS의 메모리 작동 모드가 FRM으로 설정되어 있음을 나타냅니다. • NUMA 사용되고 보호됨: 이 값은 시스템이 지원되고 운영 체제 버전이 ESXi 5.5 이상이며 BIOS의 메모리 작동 모드가 NUMA으로 설정되어 있음을 나타냅니다. • 활성화되고 보호되지 않음: 이 값은 ESXi 5.5 이하의 운영 체제 버전으로 시스템을 지원함을 나타냅니다. • 사용 안 함: 이 값은 아무 운영 체제 버전으로나 유효한 시스템을 지원함을 나타내며, 여기서 BIOS의 메모리 작동 모드는 FRM으로 설정되지 않습니다. • 비어 있음: BIOS의 메모리 작동 모드가 지원되지 않으면 FRM 특성이 표시되지 않습니다.
시스템 잠금 모드	iDRAC 8 이상의 서버에 대한 iDRAC 잠금 모드의 상태를 표시합니다. 닫힌 자물쇠는 iDRAC 잠금 모드가 켜져 있는 것을 나타내고 열린 자물쇠는 iDRAC 잠금 모드가 꺼져 있는 것을 나타냅니다.
식별	다음을 표시합니다. • 호스트 이름 — OMIVV 관리 호스트의 이름을 표시 • 전원 상태 - 전원이 켜져 있는지 아니면 꺼져 있는지 여부 표시 • iDRAC IP - iDRAC IP 주소 표시 • 관리 IP - 관리 IP 주소 표시 • 호스트 자격 증명 프로필 - 이 호스트에 대한 호스트 자격 증명 프로필 이름 표시 • 모델 - Dell EMC 서버 모델 표시 • 서비스 태그 - 서버에 대한 서비스 태그 표시 • 자산 태그 - 자산 태그 표시 • 남은 보증 기간 - 남은 보증 일 수 표시 • 마지막 인벤토리 검색 - 마지막 인벤토리 검색의 날짜와 시간 표시
하이퍼바이저 및 펌웨어	다음을 표시합니다. • 하이퍼바이저 - 하이퍼바이저 버전 표시 • BIOS 버전 - BIOS 버전 표시 • 원격 액세스 카드 버전 - 원격 액세스 카드 버전 표시
관리 콘솔	iDRAC(Remote Access Console)를 실행할 링크를 표시합니다.
호스트 조치	다양한 시간 간격으로 깜빡이도록 하려면 실제 서버가 다양한 시간 간격으로 깜빡이도록 설정합니다. 깜박임 표시등 설정 페이지 133을(를) 참조하십시오.

표 13. OMIVV 호스트 상태

정보	설명
OMIVV 호스트 상태	구성 요소 상태는 호스트 서버의 모든 주요 구성 요소들의 상태를 그림으로 나타낸 것으로, 서버의 전반적인 상태, 서버, 전원 공급 장치, 온도, 전압, 프로세서, 배터리, 침입, 하드웨어 로그, 전력 관리, 전원 및 메모리 등으로 구성됩니다. 이들 섀시 상태 매개변수는 VRTX 버전 1.0 이상과 M1000e 버전 4.4 이상에 적용됩니다. 4.3 이전 버전의 경우, 양호 및 경고 또는 치명적 결함(느낌표가 있는 주황색 역삼각형)의 두 가지 상태 표시등만이

표 13. OMIVV 호스트 상태

정보	설명
	표시됩니다. 전체적인 상태에는 상태 매개변수가 가장 낮은 섀시를 기초로 하여 상태가 표시됩니다. 다음과 같은 옵션을 사용할 수 있습니다. • 정상(녹색 확인 표시) - 구성 요소가 정상적으로 작동하고 있음. • 경고(느낌표가 있는 노란색 삼각형) - 구성 요소에 위험하지 않은 오류가 있습니다. • 위험(빨간색 X) - 구성 요소에 위험한 오류가 있습니다. • 알 수 없음(물음표) - 구성 요소의 상태를 알 수 없습니다.

예를 들어, 정상 기호가 5개 있고 경고 기호가 1개 있는 경우 전체적인 상태는 경고로 표시됩니다.

노트: 전력 모니터링 정보는 케이블로 연결된 PSU가 있는 호스트 또는 모듈식 서버에는 이용할 수 없습니다.

OMIVV 호스트 정보 보기

OMIVV 호스트 정보 페이지에서 모든 OMIVV 관리 호스트에 대한 하드웨어, 스토리지, 펌웨어, 전원 모니터링, 보증 및 시스템 이벤트 로그 정보를 볼 수 있습니다.

1. OMIVV 홈 페이지에서 **메뉴**를 확장한 다음 **호스트 및 클러스터**를 선택합니다.
2. 왼쪽 창에서 호스트를 선택한 후 **모니터** > **OMIVV 호스트 정보**를 클릭합니다.

호스트의 하드웨어 정보 보기

표 14. 단일 호스트에 대한 하드웨어 세부 정보

하드웨어: *구성 요소*	정보
FRU	• **부품 이름** - FRU 부품 이름을 표시합니다. • **부품 번호** - FRU 부품 번호를 표시합니다. • **제조업체** - 제조업체의 이름을 표시합니다. • **일련 번호** - 제조업체의 일련 번호를 표시합니다. • **제조일** - 제조일을 표시합니다.
프로세서	• **소켓** - 슬롯 번호를 표시합니다. • **속도** - 현재 속도를 표시합니다. • **브랜드** - 프로세서 브랜드를 표시합니다. • **버전** - 프로세서 버전을 표시합니다. • **코어** - 이 프로세서의 코어 수를 표시합니다.

전원 공급 장치	• **유형** — 전원 공급 장치의 종류를 표시합니다. 전원 공급 장치 종류는 다음과 같습니다.
	  ○ 알 수 없음
	  ○ 선형
	  ○ 스위칭
	  ○ 배터리
	  ○ UPS
	  ○ 변환기
	  ○ 조절기
	  ○ AC
	  ○ DC
	  ○ VRM
	• **위치** - 전원 공급 장치의 위치를 표시합니다(예: 슬롯 1).
	• **출력(와트)** - 전력을 표시합니다(와트).

표 14. 단일 호스트에 대한 하드웨어 세부 정보 (계속)

하드웨어: *구성 요소*	정보
메모리	• **메모리 슬롯** - 사용된 메모리 개수, 총 메모리 개수 및 사용 가능한 메모리 개수를 표시합니다. • **메모리 용량** - 설치된 메모리, 총 메모리 용량 및 사용 가능한 메모리를 표시합니다. • **슬롯** - DIMM 슬롯을 표시합니다. • **크기** - 메모리 크기를 표시합니다. • **유형** - 메모리 유형을 표시합니다.
NIC	• **총** - 사용 가능한 네트워크 인터페이스 카드의 총 개수를 표시합니다. • **이름** - NIC 이름을 표시합니다. • **제조업체** - 제조업체 이름만 표시합니다. • **MAC 주소** — NIC MAC 주소를 표시합니다.
PCI 슬롯	• **PCI 슬롯** - 사용된 슬롯, 총 슬롯 및 사용 가능한 PCI 슬롯을 표시합니다. • **슬롯** - 슬롯을 표시합니다. • **제조업체** - PCI 슬롯의 제조업체 이름을 표시합니다. • **설명** - PCI 장치에 대한 설명을 표시합니다. • **유형** - PCI 슬롯 유형을 표시합니다. • **폭** - 데이터 버스 폭을 표시합니다(해당되는 경우).
원격 액세스 카드	• **IP 주소** - 원격 액세스 카드의 IP 주소를 표시합니다. 통합 IP 주소를 사용하여 호스트를 관리하는 경우 iDRAC IP가 이 섹션에 표시되지 않습니다. • **MAC 주소** - 원격 액세스 카드의 MAC 주소를 표시합니다. • **RAC 유형** - 원격 액세스 카드의 유형을 표시합니다. • **URL** - 이 호스트와 관련된 iDRAC의 라이브 URL을 표시합니다.

호스트의 스토리지 정보 보기

가상 디스크, 컨트롤러, 엔클로저, 전용 핫 스패어, 그리고 전역 핫 스패어와 관련된 물리적 디스크의 개수를 볼 수 있습니다. 각 스토리지 구성 요소에 대한 자세한 내용을 보려면 **보기** 드롭다운 메뉴에서 특정 구성 요소를 선택합니다.

섀시를 사용하여 관리되는 호스트의 경우 컨트롤러, 엔클로저, 전역 핫 스패어 및 전용 핫 스패어인 전체 스토리지 정보가 표시되지 않습니다.

노트: 섀시 프로필을 사용하여 호스트를 관리하는 경우 **스토리지**를 클릭하고 **보기** 드롭다운 메뉴에서 아래 사항을 선택합니다.

- **엔클로저**- 스토리지 엔클로저의 컨트롤러 ID가 올바른 컨트롤러 ID 대신 0으로 표시됩니다.
- **물리적 디스크** - HDD의 미디어 유형은 **하드 디스크 드라이브** 대신 **마그네틱 드라이브**로 표시됩니다.

표 15. 단일 호스트에 대한 저장소 세부 정보

정보	설명
가상 디스크	• **이름** - 가상 드라이브의 이름을 표시합니다. • **장치 FQDD** - FQDD를 표시합니다. • **물리적 디스크** - 가상 드라이브가 있는 물리적 디스크를 표시합니다. • **용량** - 가상 드라이브의 용량을 표시합니다. • **레이아웃** - 가상 스토리지의 레이아웃 유형, 즉 이 가상 드라이브에 구성된 RAID 유형을 표시합니다. • **미디어 유형** - SSD 또는 HDD로 표시합니다. 스트라이프 크기, 버스 프로토콜 및 캐시 정책 같은 정보를 보려면 가상 디스크를 선택합니다.

표 15. 단일 호스트에 대한 저장소 세부 정보 (계속)

정보	설명
	• **컨트롤러 ID** - 컨트롤러 ID를 표시합니다. • **장치 ID** - 장치 ID를 표시합니다. • **스트라이프 크기** - 단일 디스크에서 각 스트라이프가 사용하는 공간의 크기인 스트라이프 크기를 표시합니다. • **버스 프로토콜** - 가상 드라이브에 포함된 물리적 디스크에서 사용하는 기술을 표시. 값은 다음과 같습니다. ○ SCSI ○ SAS ○ SATA • **기본 읽기 정책** - 컨트롤러에서 지원하는 기본 읽기 정책을 표시. 다음과 같은 옵션을 사용할 수 있습니다. ○ 미리 읽기 ○ 미리 읽기 없음 ○ 적응성 미리 읽기 ○ 읽기 캐시 활성 상태 ○ 읽기 캐시 비활성 상태 • **기본 쓰기 정책** - 컨트롤러에서 지원하는 기본 쓰기 정책을 표시합니다. 다음과 같은 옵션을 사용할 수 있습니다. ○ 나중 쓰기 ○ 강제 나중 쓰기 ○ 나중 쓰기 활성 상태 ○ 연속 쓰기 ○ 쓰기 캐시 활성 상태 보호 ○ 쓰기 캐시 비활성 상태 • **캐시 정책** - 캐시 정책이 활성화되어 있는지 여부를 표시합니다.
물리 디스크 **보기** 드롭다운 메뉴에서 이 옵션을 선택하면 **필터** 드롭다운 목록이 표시됩니다. 이 필터에서 다음 옵션을 사용할 수 있습니다. • **모든 실제 디스크** • **전역 핫 스패어** • **전용 핫 스패어** • 마지막 옵션은 가상 드라이브의 사용자 지정 이름을 표시합니다.	• **이름** - 물리적 디스크의 이름을 표시합니다. • **장치 FQDD** - 장치 FQDD를 표시합니다. • **용량** - 실제 디스크 용량을 표시합니다. • **디스크 상태** - 실제 디스크 상태를 표시합니다. 다음과 같은 옵션을 사용할 수 있습니다. ○ 온라인 ○ 준비 완료 ○ 저하됨 ○ 실패 ○ 오프라인 ○ 재구축 중 ○ 호환되지 않음 ○ 제거됨 ○ 지워짐 ○ 스마트 알림 감지됨 ○ 알 수 없음 ○ 외부 ○ 지원되지 않음 • **구성됨** - 디스크가 구성되어 있는지 여부를 표시합니다. • **핫 스패어 유형**(PCIe에는 적용 안 됨) - 핫 스패어 유형을 표시. 다음과 같은 옵션을 사용할 수 있습니다. ○ 없음 - 핫 스패어가 없습니다. ○ 전역 - 디스크 그룹에 속하는 사용되지 않은 백업 디스크 ○ 전용 - 단일 가상 드라이브에 할당된 사용되지 않은 백업 디스크. 가상 드라이브의 물리적 디스크에 충돌이 발생하면 시스템 중단이나 사용자 개입이 없

표 15. 단일 호스트에 대한 저장소 세부 정보 (계속)

정보	설명
	어도 이 핫 스패어가 활성화되어 장애가 발생한 물리적 디스크를 대체합니다. • **가상 디스크** - 가상 드라이브의 이름을 표시합니다. • **버스 프로토콜** - 버스 프로토콜을 표시합니다. • **컨트롤러 ID** - 컨트롤러 ID를 표시합니다. • **미디어 유형** - SSD 또는 HDD로 표시합니다. • **잔여 정격 쓰기 내구성**- SSD 잔여 쓰기 내구성을 표시합니다. • **커넥터 ID** - 커넥터 ID를 표시합니다. • **엔클로저 ID** - 엔클로저 ID를 표시합니다. • **장치 ID** - 장치 ID를 표시합니다. • **모델** - 물리적 스토리지의 모델 번호를 표시합니다. • **부품 번호** - 스토리지 부품 번호를 표시합니다. • **일련 번호** - 스토리지 일련 번호를 표시합니다. • **공급업체** - 스토리지 공급업체 이름을 표시합니다.
컨트롤러	• **컨트롤러 ID** - 컨트롤러 ID를 표시합니다. • **이름** - 컨트롤러의 이름을 표시합니다. • **장치 FQDD** - 장치의 FQDD를 표시합니다. • **펌웨어 버전** - 펌웨어 버전을 표시합니다. • **최소 필수 펌웨어**- 최소 필수 펌웨어를 표시합니다. 이 열은 펌웨어가 오래되고 최신 버전이 사용 가능할 때 채워집니다. • **드라이버 버전** - 드라이버 버전을 표시합니다. • **패트롤 읽기 상태** - 패트롤 읽기 상태를 표시합니다. • **캐시 크기** - 캐시 크기를 표시합니다. **노트:** 이 섹션은 칩셋 컨트롤러 정보를 표시합니다. 이 정보는 iDRAC UI의 스토리지 컨트롤러 섹션에 표시되지 않지만 iDRAC의 인벤토리 페이지에 대한 정보는 볼 수 있습니다.
엔클로저	• **컨트롤러 ID** - 컨트롤러 ID를 표시합니다. • **커넥터 ID** - 커넥터 ID를 표시합니다. • **엔클로저 ID** - 엔클로저 ID를 표시합니다. • **이름** - 엔클로저의 이름을 표시합니다. • **장치 FQDD** - 장치 FQDD를 표시합니다. • **서비스 태그** - 서비스 태그를 표시합니다.

단일 호스트의 펌웨어 정보 보기

다음과 같은 펌웨어 관련 정보가 표시됩니다.

- **이름** - 이 호스트에 있는 모든 펌웨어 이름을 표시합니다.
- **유형** - 펌웨어의 유형을 표시합니다.
- **버전** - 이 호스트에 있는 모든 펌웨어 버전을 표시합니다.
- **설치일** - 설치일을 표시합니다.

노트: 섀시 자격 증명 프로필을 사용하여 호스트를 관리하는 경우 펌웨어 인벤토리 데이터는 수명 주기 컨트롤러 및 소프트웨어 RAID와 같은 몇 가지 추가 구성 요소를 보여줍니다.

이 페이지에서 펌웨어 업데이트를 실행하고 시스템 잠금 모드 마법사를 구성할 수 있습니다.

단일 호스트의 전원 모니터링 정보 보기

일반 정보, 임계값, 예비 전력 용량 및 에너지 통계와 같은 정보를 볼 수 있습니다.

- **일반 정보** - 전력 예산 및 현재 프로필 이름을 표시합니다.

- **임계값** - 경고 및 오류 임계값을 표시합니다(와트).
- **예비 전력 용량** - 순간 및 최고 예비 전력 용량을 표시합니다(와트).

에너지 통계

- **유형** - 에너지 통계 유형을 표시합니다.
- **측정 시작 시간(호스트 시간)** - 호스트가 전원을 사용하기 시작한 날짜 및 시간을 표시합니다.
- **측정 종료 시간(호스트 시간)** - 호스트가 전원 사용을 중지한 날짜 및 시간을 표시합니다.
- **노트:** 여기에서 사용되는 호스트 시간은 호스트가 있는 로컬 시간을 의미합니다.

  측정값 - 1분 이상 동안의 평균 측정값을 표시합니다.
- **최고 시간(호스트 시간)** - 호스트가 최대 암페어를 사용한 날짜 및 시간을 표시합니다.
- **최고 측정값** - 시스템 최대 전력 통계(즉, 시스템에서 소비한 최대 전력)를 표시합니다(와트).

노트: 전력 모니터링 정보는 케이블로 연결된 PSU가 있는 호스트 또는 모듈식 서버에는 이용할 수 없습니다.

노트: 섀시를 사용하여 관리되는 호스트의 경우 전체 전력 모니터링 정보가 표시되지 않습니다.

단일 호스트의 보증 정보 보기

보증 상태를 보려면 보증 작업을 실행해야 합니다. 보증 검색 작업 예약 페이지 95을(를) 참조하십시오. **보증 상태** 페이지에서 보증 만료일을 모니터링할 수 있습니다. Dell 온라인에서 서버 보증 정보가 검색되는 경우 보증 일정을 사용하거나 사용 안 함으로 설정한 다음 최소 일 수 임계값 알림을 설정하여 보증 설정을 제어합니다.

- **공급자** - 보증 공급자의 이름을 표시합니다.
- **설명** - 설명을 표시합니다.
- **상태** - 호스트의 보증 상태를 표시합니다. 상태 옵션은 다음과 같습니다.
  - 활성 - 호스트에 보증이 적용되며 임계값을 초과하지 않음
  - 경고 - 호스트가 활성 상태이지만 경고 임계값을 초과함
  - 위험 - 경고와 동일하지만 위험 임계값
  - 만료됨 - 이 호스트에 대한 보증이 만료됨
  - 알 수 없음 - 보증 작업이 실행되지 않았거나, 데이터를 가져오는 중에 오류가 발생했거나, 시스템에 보증이 없기 때문에 OMIVV가 보증 상태를 가져오지 못함
- **소유 권한 유형** - 다음 상태를 표시합니다.
  - 초기
  - 확장
  - 만료
- **시작일** - 보증 시작 날짜를 표시합니다.
- **종료일** - 보증 종료 날짜를 표시합니다.
- **만료일 수** - 남은 보증 일 수를 표시합니다.
- **마지막 업데이트** - 마지막으로 보증을 업데이트한 시간입니다.

단일 호스트의 시스템 이벤트 로그 정보 보기

시스템 이벤트 로그(SEL)는 OMIVV에서 검색된 하드웨어의 상태 정보를 제공하고 다음과 같은 정보를 표시합니다.

- **상태** - 정보(파란색 느낌표), 경고(느낌표가 있는 노란색 삼각형), 오류(빨간색 X) 및 알 수 없음(물음표(?)가 있는 상자)과 같은 여러 상태 아이콘이 있습니다.

  심각도 수준은 다음과 같이 정의됩니다.
  - 정보
  - 경고
  - 오류
- **시간(서버 시간)** - 이벤트가 발생한 날짜 및 시간을 나타냅니다.

모든 시스템 이벤트 로그를 지우려면 **로그 지우기**를 클릭합니다. 로그를 지운 후에 로그 데이터를 복구할 수 없다는 메시지가 표시됩니다.

클러스터 및 데이터 센터의 호스트 모니터링

OMIVV에서 데이터 센터 또는 클러스터의 모든 호스트에 대한 세부 정보를 볼 수 있습니다.

OMIVV 데이터 센터 및 클러스터 정보 보기

데이터 센터 및 클러스터 개요 보기

데이터 센터 또는 클러스터 정보, 시스템 잠금 모드, 하드웨어 리소스 및 보증 정보와 같은 정보를 볼 수 있습니다. 이 페이지에 대한 정보를 보려면 인벤토리가 성공적으로 완료되었는지 확인하십시오. OMIVV 데이터 센터 및 클러스터 보기는 iDRAC에서 직접 데이터를 보고합니다.

1. OMIVV 홈 페이지에서 **메뉴**를 확장한 다음 **호스트 및 클러스터**를 선택합니다.
2. 왼쪽 창에서 데이터 센터 또는 클러스터를 선택한 후 **모니터링** > **OMIVV 클러스터 또는 데이터센터 정보**를 클릭합니다.
3. 자세한 내용을 보려면 특정 호스트를 선택하십시오.

   iDRAC IP, 섀시 URL, CPU 및 메모리와 같은 정보가 페이지의 맨 아래쪽 수평 창에 표시됩니다.

표 16. 데이터 센터 및 클러스터 개요

정보	설명
데이터센터/클러스터 정보	다음을 표시합니다. • 데이터센터/클러스터 이름 • 관리되는 호스트의 수 • 총 에너지 소비량
시스템 잠금 모드	iDRAC 잠금 모드의 상태를 표시합니다. 총 호스트 수의 iDRAC 잠금 모드 상태는 다음과 같이 표시됩니다. • 켜짐 • 꺼짐 • 적용되지 않음(iDRAC9 기반 서버에만 적용) iDRAC9 기반 서버 목록은 호환성 매트릭스를 참조하십시오.
하드웨어 리소스	다음을 표시합니다. • 총 프로세서 수 • 메모리 총량 • 가상 디스크 용량
보증 요약	선택한 호스트의 보증 상태를 표시합니다. 상태 옵션은 다음과 같습니다. • 만료된 보증 • 활성 보증 • 경고 임계값 초과 • 중요 임계값 초과 • 알 수 없는 보증 다수의 또는 다양한 보증이 있는 호스트 또는 섀시(예: ND 및 4DP와 같은 서비스 수준 코드)의 경우 OMIVV는 남은 보증 일수가 가장 적은 보증 유형에 의거해 상태를 고려합니다.
호스트	호스트 이름 표시
서비스 태그	호스트 시스템 서비스 태그 표시
모델	PowerEdge 모델 표시
자산 태그	자산 태그 표시(구성된 경우)
섀시 서비스 태그	섀시 서비스 태그 표시(해당되는 경우)

표 16. 데이터 센터 및 클러스터 개요 (계속)

정보	설명
OS 버전	ESXi OS 버전 표시
위치	블레이드의 경우: 슬롯 위치를 표시합니다. 기타의 경우 “적용되지 않음”으로 표시됩니다.
시스템 잠금 모드	iDRAC9 기반 서버에만 적용: 호스트의 iDRAC 잠금 모드를 켜기, 끄기 또는 알 수 없음으로 표시합니다. iDRAC9 기반 이전 모든 PowerEdge 서버의 경우 시스템 잠금 모드는 **적용되지 않음**으로 표시됩니다. iDRAC9 기반 서버 목록은 호환성 매트릭스를 참조하십시오.
iDRAC IP	iDRAC IP 주소 표시
서비스 콘솔 IP	서비스 콘솔 IP 표시
CMC 또는 관리 모듈 URL	모듈형 서버의 섀시 URL, 즉 CMC 또는 관리 모듈 URL을 표시하거나, 그렇지 않으면 "적용되지 않음"으로 표시
CPU	CPU 수 표시
메모리	호스트 메모리 표시
전원 상태	호스트 전원 상태 표시
마지막 인벤토리	마지막 인벤토리 작업의 요일, 날짜 및 시간 표시
호스트 자격 증명 프로필	호스트 자격 증명 프로필 이름 표시
원격 액세스 카드 버전	원격 액세스 카드 버전 표시
BIOS 펌웨어 버전	BIOS 펌웨어 버전 표시

데이터 센터 및 클러스터의 하드웨어 정보 보기

표 17. 데이터 센터 및 클러스터에 대한 하드웨어 정보

하드웨어: *구성 요소*	정보
하드웨어: FRU	• **호스트** - 호스트 이름을 표시합니다. • **서비스 태그** - 호스트의 서비스 태그를 표시합니다. • **부품 이름** - FRU 부품 이름을 표시합니다. • **부품 번호** - FRU 부품 번호를 표시합니다. • **제조업체** - 제조업체의 이름을 표시합니다. • **일련 번호** - 제조업체의 일련 번호를 표시합니다. • **제조일** - 제조일을 표시합니다.
하드웨어: 프로세서	• **호스트** - 호스트 이름을 표시합니다. • **서비스 태그** - 호스트의 서비스 태그를 표시합니다. • **소켓** - 슬롯 번호를 표시합니다. • **속도** - 현재 속도를 표시합니다. • **브랜드** - 프로세서 브랜드를 표시합니다. • **버전** - 프로세서 버전을 표시합니다. • **코어** - 이 프로세서의 코어 수를 표시합니다.
하드웨어: 전원 공급 장치	• **호스트** - 호스트 이름을 표시합니다. • **서비스 태그** - 호스트의 서비스 태그를 표시합니다. • **유형** — 전원 공급 장치의 종류를 표시합니다. 전원 공급 장치 종류는 다음과 같습니다. ○ 알 수 없음

표 17. 데이터 센터 및 클러스터에 대한 하드웨어 정보 (계속)

하드웨어: *구성 요소*	정보
	○ 선형 ○ 스위칭 ○ 배터리 ○ UPS ○ 컨버터 ○ 조절기 ○ AC ○ DC ○ VRM • **위치** - 전원 공급 장치의 위치를 표시합니다(예: 슬롯 1). • **출력(와트)** - 전력을 표시합니다(와트). • **상태** — 전원 공급 장치의 상태를 표시합니다. 상태 옵션은 다음과 같습니다. ○ 기타 ○ 알 수 없음 ○ 확인 ○ 위험 ○ 위험하지 않음 ○ 복구 가능 ○ 복구 불가능 ○ 높음 ○ 낮음
하드웨어: 메모리	• **호스트** - 호스트 이름을 표시합니다. • **서비스 태그** - 호스트의 서비스 태그를 표시합니다. • **슬롯** - DIMM 슬롯을 표시합니다. • **크기** - 메모리 크기를 표시합니다. • **유형** - 메모리 유형을 표시합니다.
하드웨어: NIC	• **호스트** - 호스트 이름을 표시합니다. • **서비스 태그** - 호스트의 서비스 태그를 표시합니다. • **이름** - NIC 이름을 표시합니다. • **제조업체** - 제조업체 이름만 표시합니다. • **MAC 주소** — NIC MAC 주소를 표시합니다.
하드웨어: PCI 슬롯	• **호스트** - 호스트 이름을 표시합니다. • **서비스 태그** - 호스트의 서비스 태그를 표시합니다. • **슬롯** - 슬롯을 표시합니다. • **제조업체** - PCI 슬롯의 제조업체 이름을 표시합니다. • **설명** - PCI 디바이스에 대한 설명을 표시합니다. • **유형** - PCI 슬롯 유형을 표시합니다. • **폭** - 데이터 버스 폭을 표시합니다(해당되는 경우).
하드웨어: 원격 액세스 카드	• **호스트** - 호스트 이름을 표시합니다. • **서비스 태그** - 호스트의 서비스 태그를 표시합니다. • **IP 주소** - 원격 액세스 카드의 IP 주소를 표시합니다. • **MAC 주소** - 원격 액세스 카드의 MAC 주소를 표시합니다. • **RAC 유형** - 원격 액세스 카드의 유형을 표시합니다. • **URL** - 이 호스트와 관련된 iDRAC의 라이브 URL을 표시합니다.

데이터 센터 및 클러스터의 스토리지 정보 보기

표 18. 데이터 센터 및 클러스터의 스토리지 세부 정보

스토리지: 디스크	설명
물리적 디스크	• **호스트** - 호스트 이름을 표시합니다. • **서비스 태그** - 호스트의 서비스 태그를 표시합니다. • **용량** - 물리적 디스크 용량을 표시합니다. • **디스크 상태** - 물리적 디스크 상태를 표시합니다. 다음과 같은 옵션을 사용할 수 있습니다. ○ 온라인 ○ 준비 완료 ○ 저하됨 ○ 실패 ○ 오프라인 ○ 재구축 중 ○ 호환되지 않음 ○ 제거됨 ○ 지워짐 ○ 스마트 알림 감지됨 ○ 알 수 없음 ○ 외부 ○ 지원되지 않음 ⓘ **노트:** 이러한 알림이 나타내는 의미에 대한 자세한 내용은 다음에서 Dell EMC OpenManage Server Administrator 스토리지 관리 사용자 가이드를 참조하십시오. `dell.com/support` • **모델 번호** - 물리적 스토리지 디스크의 모델 번호를 표시합니다. • **마지막 인벤토리** - 마지막으로 인벤토리가 실행된 월, 일, 시간을 표시합니다. • **상태** - 호스트 상태를 표시합니다. • **컨트롤러 ID** - 컨트롤러 ID를 표시합니다. • **커넥터 ID** - 커넥터 ID를 표시합니다. • **인클로저 ID** - 인클로저 ID를 표시합니다. • **디바이스 ID** - 디바이스 ID를 표시합니다. • **버스 프로토콜** - 버스 프로토콜을 표시합니다. • **잔여 정격 쓰기 내구성**- SSD 잔여 쓰기 내구성을 표시합니다. • **핫 스페어 유형**(PCIe에는 적용 안 됨) - 핫 스페어 유형을 표시. 다음과 같은 옵션을 사용할 수 있습니다. ○ 없음 - 핫 스페어가 없습니다. ○ 전역 - 디스크 그룹에 속하는 사용되지 않은 백업 디스크입니다. ○ 전용 - 단일 가상 드라이브에 할당된 사용되지 않은 백업 디스크입니다. 가상 드라이브에서 물리적 디스크에 장애가 발생할 경우, 시스템 중단이나 사용자 개입이 없어도 이 핫 스페어가 활성화되어 장애가 발행한 물리적 디스크를 대체합니다. • **부품 번호** - 스토리지 부품 번호를 표시합니다. • **일련 번호** - 스토리지 일련 번호를 표시합니다. • **공급업체 이름** - 스토리지 공급업체의 이름을 표시합니다.
가상 디스크	• **호스트** - 호스트 이름을 표시합니다. • **서비스 태그** - 호스트의 서비스 태그를 표시합니다. • **이름** - 가상 드라이브의 이름을 표시합니다. • **물리적 디스크** - 가상 드라이브가 있는 물리적 디스크를 표시합니다. • **용량** - 가상 드라이브의 용량을 표시합니다. • **레이아웃** - 가상 스토리지의 레이아웃 유형을 표시합니다. 이 가상 드라이브에 구성된 RAID 유형을 의미합니다. • **마지막 인벤토리** - 인벤토리가 마지막으로 실행된 요일, 날짜 및 시간을 표시합니다. • **컨트롤러 ID** - 컨트롤러 ID를 표시합니다.

표 18. 데이터 센터 및 클러스터의 스토리지 세부 정보 (계속)

스토리지: 디스크	설명

	• **디바이스 ID** - 디바이스 ID를 표시합니다.
	• **미디어 유형** - SSD 또는 HDD로 표시합니다.
	• **버스 프로토콜** - 가상 드라이브에 포함된 물리적 디스크에서 사용하는 기술을 표시. 값은 다음과 같습니다.
	  ○ SCSI
	  ○ SAS
	  ○ SATA
	  ○ PCIe
	• **스트라이프 크기** - 단일 디스크에서 각 스트라이프가 사용하는 공간을 제공하는 스트라이프 크기를 표시합니다.
	• 기본 읽기 정책 - 컨트롤러에서 지원하는 기본 읽기 정책을 표시합니다. 다음과 같은 옵션을 사용할 수 있습니다.
	  ○ 미리 읽기
	  ○ 미리 읽기 없음
	  ○ 적응성 미리 읽기
	  ○ 읽기 캐시 활성 상태
	  ○ 읽기 캐시 비활성 상태
	• **기본 쓰기 정책** - 컨트롤러에서 지원하는 기본 쓰기 정책을 표시합니다. 다음과 같은 옵션을 사용할 수 있습니다.
	  ○ 나중 쓰기
	  ○ 강제 나중 쓰기
	  ○ 나중 쓰기 활성 상태
	  ○ 연속 쓰기
	  ○ 쓰기 캐시 활성 상태 보호
	  ○ 쓰기 캐시 비활성 상태
	• **디스크 캐시 정책** - 컨트롤러에서 지원하는 기본 캐시 정책을 표시. 다음과 같은 옵션을 사용할 수 있습니다.
	  ○ 활성화됨 - 캐시 I/O
	  ○ 비활성화됨 - 직접 I/o

데이터 센터 및 클러스터의 펌웨어 정보 보기

각 펌웨어 구성 요소에 대해 다음과 같은 정보가 표시됩니다.

- **호스트** - 호스트 이름을 표시합니다.
- **서비스 태그** - 호스트의 서비스 태그를 표시합니다.
- **이름** - 이 호스트에 있는 모든 펌웨어 이름을 표시합니다.
- **버전** - 이 호스트에 있는 모든 펌웨어 버전을 표시합니다.

데이터 센터 및 클러스터의 전원 모니터링 정보 보기

- **호스트** - 호스트 이름을 표시합니다.
- **서비스 태그** - 호스트의 서비스 태그를 표시합니다.
- **현재 프로필** - 시스템 성능을 최대화하고 에너지를 절약할 수 있도록 전원 프로필을 표시합니다.
- **에너지 소비량** - 호스트의 에너지 소비량을 표시합니다.
- **최고 예비 용량** - 최고 전력 예비 용량을 표시합니다.
- **전원 예산** - 이 호스트의 전원 용량을 표시합니다.
- **경고 임계값** - 시스템에 구성된 온도 프로브 경고 임계값의 최대값을 표시합니다.
- **실패 임계값** - 시스템에 구성된 온도 프로브 실패 임계값의 최대값을 표시합니다.
- **순간 예비 용량** - 호스트의 순간 헤드룸 용량을 표시합니다.
- **에너지 소비 시작일** - 호스트가 전원을 사용하기 시작한 날짜 및 시간을 표시합니다.
- **에너지 소비 종료일** - 호스트가 전원 사용을 중지한 날짜 및 시간을 표시합니다.

- **시스템 최대 전력** - 호스트 최대 전원을 표시합니다.
- **시스템 최대 전원 시작일** - 호스트가 최대 전원을 사용하기 시작한 날짜 및 시간을 표시합니다.
- **시스템 최대 전원 종료일** - 호스트가 최대 전원 사용을 종료한 날짜 및 시간을 표시합니다.
- **시스템 최대 암페어** - 호스트 최대 암페어를 표시합니다.
- **시스템 최대 암페어 시작일** - 호스트가 최대 암페어를 사용하기 시작한 날짜 및 시간을 표시합니다.
- **시스템 최대 암페어 종료일** - 호스트가 최대 암페어 사용을 종료한 날짜 및 시간을 표시합니다.

데이터 센터 및 클러스터의 보증 정보 보기

보증 상태를 보려면 보증 작업을 실행해야 합니다. 보증 검색 작업 예약 페이지 95을(를) 참조하십시오. **보증 요약** 페이지에서 보증 만료일을 모니터링할 수 있습니다. Dell 온라인에서 서버 보증 정보가 검색되는 경우 보증 일정을 사용하거나 사용 안 함으로 설정한 다음 최소 일 수 임계값 알림을 설정하여 보증 설정을 제어합니다.

- **보증 요약** - 호스트 보증 요약은 각 상태 카테고리에서 호스트 수를 시각적으로 표시하는 아이콘을 사용하여 표시됩니다.
- **호스트** - 호스트 이름을 표시합니다.
- **서비스 태그** - 호스트의 서비스 태그를 표시합니다.
- **설명** - 설명을 표시합니다.
- **보증 상태** - 호스트의 보증 상태를 표시합니다. 상태 옵션은 다음과 같습니다.
  - 활성 - 호스트에 보증이 적용되며 임계값을 초과하지 않음
  - 경고 - 호스트가 활성 상태이지만 경고 임계값을 초과함
  - 위험 - 경고와 동일하지만 위험 임계값
  - 만료됨 - 이 호스트에 대한 보증이 만료됨
  - 알 수 없음 - 보증 작업이 실행되지 않았거나, 데이터를 가져오는 중에 오류가 발생했거나, 시스템에 보증이 없기 때문에 OpenManage Integration for VMware vCenter이 보증 상태를 가져오지 못함
- **남은 일 수** - 남은 보증 일 수를 표시합니다.

펌웨어 업데이트

OMIVV를 사용하면 관리되는 호스트에서 BIOS 및 펌웨어 업데이트 작업을 수행할 수 있습니다. 여러 클러스터 또는 클러스터링되지 않은 호스트에서 동시에 펌웨어 업데이트 작업을 수행할 수 있습니다. 동일한 클러스터의 호스트 2개에서 동시에 펌웨어 업데이트를 수행할 수 없습니다.

노트: 다중 어플라이언스 환경에서 클러스터 또는 호스트에서 펌웨어 업데이트를 수행하려면 대상 vCenter에 등록된 어플라이언스가 로드되었는지 확인하십시오.

다음은 펌웨어 업데이트를 수행하는 두 가지 방법입니다.

- 단일 DUP - DUP 위치(CIFS 또는 NFS)를 직접 가리켜서 iDRAC 및 BIOS에 대한 펌웨어 업데이트를 수행합니다. 단일 DUP 방법은 호스트 수준에서만 사용할 수 있습니다.
- 리포지토리 프로필 - 펌웨어 및 드라이버 업데이트를 수행합니다. 이 방법은 호스트 수준 및 클러스터 수준에서 모두 사용할 수 있습니다.

  다음은 펌웨어 및 드라이버 업데이트에 사용되는 리포지토리 프로필입니다.

  - 펌웨어 리포지토리 - 펌웨어 카탈로그를 사용하여 펌웨어 정보를 가져오는 리포지토리 프로필입니다.

    다음은 펌웨어 리포지토리의 두 가지 유형입니다.

    - 사용자 생성 펌웨어 리포지토리
    - 출하 시 생성된 펌웨어 리포지토리: 다음은 출하 시 생성된 두 가지 카탈로그 유형입니다. 출하 시 생성된 카탈로그는 vSAN 클러스터 펌웨어 업데이트 및 기준선 설정에 적용되지 않습니다.
      - Dell 기본 카탈로그: Dell EMC 온라인 카탈로그를 사용하여 최신 펌웨어 정보를 가져오는 출하 시 생성된 펌웨어 리포지토리 프로필입니다. 어플라이언스에 인터넷 연결이 없는 경우, 이 리포지토리를 수정하여 로컬 CIFS, NFS 또는 HTTP 또는 HTTPS 기반 공유를 지정합니다.
      - 검증된 MX 스택 카탈로그: Dell EMC 온라인 카탈로그를 사용하여 MX 섀시 및 해당 슬레드에 대한 검증된 펌웨어 정보를 가져오는 출하 시 생성된 펌웨어 리포지토리 프로필입니다.

  - 드라이버 리포지토리 - 리포지토리 프로필에는 vSAN 클러스터에 대한 드라이버를 업데이트하는 데 사용할 수 있는 오프라인 번들이 포함되어 있습니다.

  펌웨어 업데이트 마법사는 iDRAC 및 BIOS의 최소 펌웨어 수준을 항상 확인하며 필요한 최소 버전으로 업데이트를 시도합니다. iDRAC 및 BIOS의 최소 펌웨어 수준에 대한 자세한 내용은 *OpenManage Integration for VMware vCenter 호환성 매트릭스*을 참조

하십시오. iDRAC 및 BIOS 펌웨어 버전이 최소 요구사항을 충족하면 펌웨어 업데이트 프로세스를 통해 iDRAC, RAID 컨트롤러, NIC, BIOS 등 모든 펌웨어 버전의 업데이트가 가능합니다.

노트: PowerEdge XR2 서버를 업데이트하기 위해 OMIVV는 Dell 온라인 카탈로그에 있는 R440 펌웨어 구성 요소를 사용합니다. PowerEdge XR2를 지원하기 위해 오프라인 펌웨어 리포지토리에 사용할 맞춤 구성 카탈로그(DRM 사용)를 만들려면 PowerEdge R440 서버에 해당하는 펌웨어 구성 요소를 사용하십시오.

vSAN 호스트에서 펌웨어 및 드라이버 업데이트

vSAN 호스트(vSAN 사용 클러스터의 호스트)에서 펌웨어 업데이트를 예약하기 전에 다음 조건이 환경에서 충족되는지 확인합니다.

- 호스트가 규정을 준수하고(CSIOR이 활성화되었고 호스트가 ESXi 버전을 지원했음) 호스트 자격 증명 프로필과 연결되어 있고 인벤토리되었는지 확인합니다.
- 펌웨어 업데이트를 예약하기 전에 다음 필수 조건을 확인합니다.
  - DRS가 활성화되어 있습니다.
  - 호스트가 유지 보수 모드에 있지 않습니다.
  - vSAN 데이터 개체의 상태가 정상입니다.

  필수 조건을 건너뛰려면 **업데이트 예약** 페이지에서 **필수 조건 점검** 확인란의 선택을 취소하십시오.
- 스토리지 컨트롤러, HDD 및 SSD 구성 요소의 경우 선택한 리포지토리에서 선택한 드라이버 및 펌웨어 버전은 vSAN 버전을 기반으로 하는 VMware vSAN 지침에 따라 규정을 준수합니다.
- 드라이버의 경우 OMIVV는 VMware 하드웨어 호환성 목록에 나열된 오프라인 번들만 지원합니다.
- 클러스터가 선택한 데이터 마이그레이션 옵션에 대한 vSAN 요구 사항을 만족합니다. vSAN 클러스터가 선택한 데이터 마이그레이션 옵션의 요구 사항을 충족하지 않는 경우 업데이트 시간이 초과됩니다.
- Dell EMC는 기준이 설정된 (클러스터 프로필) 펌웨어나 드라이버 리포지토리를 선택하는 것을 권장합니다.
- 업데이트 중인 클러스터에 활성 펌웨어 업데이트 작업이 없는지 확인합니다.
- "유지 보수 모드 진입" 작업에 필요한 시간 초과 값을 지정하는지 확인합니다. 대기 시간이 지정된 시간을 지나면 업데이트 작업이 실패합니다. 하지만 호스트가 재부팅될 때 구성 요소가 자동으로 업데이트될 수도 있습니다.
- vSAN을 활성화한 후에 인벤토리를 다시 실행합니다.

Dell EMC는 펌웨어 업데이트 프로세스 중에 다음 항목을 삭제 또는 이동하지 않는 것을 권장합니다.

- 펌웨어 업데이트 작업이 진행 중인 vCenter의 호스트
- 펌웨어 업데이트 작업이 진행 중인 호스트의 호스트 자격 증명 프로필
- CIFS 또는 NFS에 있는 리포지토리

OMIVV는 호스트 준수 및 동일한 클러스터 내 호스트에서 진행 중인 다른 펌웨어 업데이트 작업 여부를 확인합니다. 확인 후에 펌웨어 업데이트 마법사가 표시됩니다.

1. 펌웨어 업데이트 마법사를 실행하려면 OMIVV 홈 페이지에서 **메뉴**를 확장하고 **호스트 및 클러스터**를 선택한 후 다음 작업 중 하나를 수행합니다.
   - 호스트를 마우스 오른쪽 버튼으로 클릭하고 **OMIVV 호스트 작업** > **펌웨어 업데이트**를 선택합니다.
   - 호스트를 선택하고 오른쪽 창에서 **모니터링** > **OMIVV 호스트 정보** > **펌웨어** > **펌웨어 마법사 실행**을 선택합니다.
   - 호스트를 선택하고 오른쪽 창에서 **요약**을 선택한 후 **OMIVV 호스트 정보** > **호스트 작업** > **펌웨어 마법사 실행**으로 이동합니다.
2. **펌웨어 업데이트 체크리스트** 페이지에서 업데이트를 예약하기 전에 모든 필수 조건을 확인한 후 **시작하기**를 클릭합니다.
3. **업데이트 소스** 페이지에서 다음 중 하나를 선택합니다.
   - **리포지토리 프로필**
   - **단일 DUP**
4. 파일에서 단일 펌웨어 업데이트를 로드하려면 **단일 DUP**를 선택합니다.
   a. 단일 DUP는 OMIVV 어플라이언스에서 액세스할 수 있는 CIFS 또는 NFS 공유에 있을 수 있습니다. 파일 위치를 다음 형식 중 하나로 입력한 후 9단계로 이동합니다.
      - NFS—`<host>:/<share_path/FileName.exe`
      - CIFS—`\\<host accessible share path>\<FileName>.exe`

      노트: 단일 구성 요소 DUP의 파일 이름에 빈 공간이 없는지 확인합니다.

      CIFS 공유의 경우 OMIVV에 공유 드라이브에 액세스할 수 있는 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다.
5. **리포지토리 프로필** 옵션을 선택한 경우 펌웨어 및 드라이버 리포지토리 프로필을 선택합니다.

클러스터 프로필이 호스트가 있는 클러스터에 연결된 경우 기본적으로 연결된 펌웨어 및 드라이버 리포지토리 프로필이 선택됩니다.

펌웨어 또는 드라이버 리포지토리 프로필을 변경하면 선택한 리포지토리 프로필이 기준과 연결되지 않았음을 나타내는 메시지가 표시되고 다른 리포지토리를 사용하면 기준 비교에 영향을 줄 수 있습니다.

노트: 드라이버 및 펌웨어 리포지토리가 모두 클러스터 프로필에 연결된 경우 드라이버 및 펌웨어를 동시에 업데이트하는 것이 좋습니다.

펌웨어 또는 드라이버를 업데이트하지 않거나, 펌웨어 또는 드라이버가 최신 상태라면 드롭다운 메뉴에서 **선택한 리포지토리 없음**을 선택합니다.

기본 펌웨어 카탈로그(Dell EMC 기본 카탈로그 및 검증된 MX 스택 카탈로그)는 리포지토리 프로필 옵션에 표시되지 않습니다. 리포지토리 프로필을 사용하려면 OMIVV에서 맞춤형 리포지토리를 생성합니다.

사용자 지정 리포지토리 프로필을 생성하려면 다음을 수행합니다.

a. DRM(Dell EMC Repository Manager)으로 이동하여 카탈로그를 생성합니다.

   DRM을 사용한 카탈로그 생성에 대한 자세한 내용은 OMIVV를 사용하여 DRM(Dell EMC Repository Manager)에서 카탈로그 생성 페이지 121을(를) 참조하십시오.

b. 카탈로그 및 해당 파일을 다운로드합니다.

c. 다운로드한 카탈로그를 이용하여 OMIVV에 리포지토리 프로필을 생성합니다.

   리포지토리 프로필 생성에 대한 자세한 내용은 리포지토리 프로필 생성 페이지 42을(를) 참조하십시오.

6. 선택한 펌웨어 리포지토리 프로필을 기반으로 적절한 번들을 선택한 후 **다음**을 클릭합니다. 64비트 번들만 지원됩니다.
7. **드라이버 구성 요소 선택** 페이지에서 업데이트가 필요한 드라이버 구성 요소를 선택한 후 **다음**을 클릭합니다. 업데이트를 위한 드라이버 구성 요소를 선택하면 패키지의 모든 구성 요소가 선택됩니다.

   필터 옵션을 사용하여 특정 열 이름을 기준으로 데이터를 필터링할 수 있습니다.
8. **펌웨어 구성 요소 선택** 페이지에서 업데이트가 필요한 펌웨어 구성 요소를 선택한 후 **다음**을 클릭합니다.

   중요도 상태(예: 긴급, 권장, 옵션 및 다운그레이드)에 따라 구성 요소의 개수가 표시됩니다.

   카탈로그에서 사용 가능한 버전보다 낮은 버전 또는 같은 수준(최신)이거나 업데이트가 예약된 구성 요소는 선택할 수 없습니다. 사용 가능한 버전보다 낮은 버전의 구성 요소를 선택하려면 **펌웨어 다운그레이드 허용** 확인란을 선택합니다.

   모든 페이지에서 모든 펌웨어 구성 요소를 선택하려면 을 클릭합니다.

   모든 페이지에서 모든 펌웨어 구성 요소를 지우려면 을 클릭합니다.
9. **업데이트 예약** 페이지에서 펌웨어 업데이트 작업 이름 및 설명을 입력합니다. 설명은 선택적인 필드입니다.

   펌웨어 업데이트 작업 이름은 필수입니다. 펌웨어 업데이트 작업 이름을 제거한 경우 작업 이름을 재사용할 수 있습니다.
10. **추가 설정** 섹션에서 다음을 수행합니다.

    a. 유지 보수 모드 시간 초과 값을 60~1440분으로 입력합니다. 대기 시간이 지정된 시간을 지나면 업데이트 작업이 실패하고 유지 보수 진입 작업이 취소되거나 시간 초과됩니다. 하지만 호스트가 재시작될 때 구성 요소가 자동으로 업데이트될 수도 있습니다.

    b. **유지 보수 모드 진입 옵션** 드롭다운 메뉴에서 적절한 데이터 마이그레이션 옵션을 선택합니다. 데이터 마이그레이션 옵션에 대한 자세한 내용은 VMware 설명서를 참조하십시오.

       노트: 클러스터 구성이 전체 데이터 마이그레이션을 지원하지 않거나 스토리지 용량이 부족하면 유지 보수 모드 진입 작업에 실패합니다.

       기본적으로 다음 옵션이 선택되어 있습니다.

       - **펌웨어 업데이트 완료 후 유지 보수 모드 종료** - 이 옵션을 비활성화하면 호스트가 유지 보수 모드로 유지됩니다.
       - **전원이 꺼진 가상 시스템과 일시 중지된 가상 시스템을 클러스터의 다른 호스트로 이동** - 이 옵션을 비활성화하면 호스트 장치가 온라인 상태가 될 때까지 VM 연결이 해제됩니다.

    c. 펌웨어를 업데이트하는 동안에 문제가 발생하면 **작업 대기열 삭제 및 iDRAC 재설정** 확인란을 선택합니다. 이로써 업데이트 프로세스가 성공적으로 완료될 수 있습니다. 이렇게 하면 작업 완료에 필요한 전체 업데이트 시간이 증가하고, iDRAC에 예약되어 있는 모든 보류 중인 작업 또는 활동이 취소되고, iDRAC이 재설정됩니다.

       섀시 자격 증명 프로필을 사용하여 관리되는 호스트의 경우 작업 대기열 삭제가 지원되지 않습니다.

       기본적으로 **필수 조건 점검** 옵션이 선택되어 있습니다.
11. **업데이트 일정** 섹션에서 다음 옵션 중 하나를 선택합니다.

    - **지금 업데이트**
    - **업데이트 예약**
    - **다음 재부팅 시에 업데이트 적용**

12. **요약 검토** 페이지에서 펌웨어 업데이트 정보를 검토한 후 **마침**을 클릭합니다.
펌웨어 업데이트 작업은 구성 요소 및 선택한 서버 수에 따라 최대 몇 시간이 소요될 수 있습니다. **작업** 페이지에서 작업 상태를 볼 수 있습니다.

펌웨어 업데이트 작업이 완료되면 **업데이트 예약** 페이지에서 선택한 옵션을 기반으로 인벤토리가 선택한 호스트에서 자동으로 실행되고 호스트의 유지 보수 모드가 자동으로 종료됩니다.

OMIVV를 사용하여 DRM(Dell EMC Repository Manager)에서 카탈로그 생성

이 섹션에서는 DRM 버전 3.0 이상에서 카탈로그를 생성하는 과정을 설명합니다.

1. DRM 다운로드로 이동하여 DRM을 다운로드합니다.
2. DRM 홈 페이지에서 **새 리포지토리 추가**를 클릭합니다.
리포지토리 추가 창이 표시됩니다.
3. **리포지토리 추가** 창에서 다음을 수행합니다.
   a. **리포지토리 이름**과 **설명**을 입력합니다.
   b. **기본 카탈로그** 드롭다운 메뉴에서 카탈로그를 선택합니다.
   c. **통합 유형** 드롭다운 메뉴에서 **OpenManage Integration for VMware vCenter**를 선택합니다.
4. **OpenManage Integration for VMware vCenter** 창에서 **가상 어플라이언스 IP**, **vCenter 서버 IP**, **사용자 이름**, 및 **암호**를 입력하고 **연결**을 클릭합니다.
생성된 카탈로그가 홈 페이지에 표시됩니다.
5. 카탈로그를 내보내려면 카탈로그를 선택하고 **내보내기**를 클릭합니다.

vSAN 클러스터에서 펌웨어 및 드라이버 업데이트

펌웨어 업데이트를 예약하기 전에 다음 조건이 환경에서 충족되는지 확인합니다.

- 호스트가 규정을 준수하고(CSIOR이 활성화되었고 호스트가 ESXi 버전을 지원했음) 호스트 자격 증명 프로필과 연결되어 있고 인벤토리되었는지 확인합니다. 호스트가 나열되지 않으면 OMIVV에서 호스트에 대한 관리 규정 준수 마법사를 실행한 후 펌웨어 업데이트 마법사를 사용합니다.
- 펌웨어 업데이트를 예약하기 전에 다음 필수 조건을 확인합니다.
  - DRS가 활성화되어 있습니다.
  - 호스트가 유지 보수 모드에 있지 않습니다.
  - vSAN 데이터 개체의 상태가 정상입니다.
- 스토리지 컨트롤러, HDD 및 SSD 구성 요소의 경우 선택한 리포지토리에서 선택한 드라이버 및 펌웨어 버전은 vSAN 버전을 기반으로 하는 VMware vSAN 지침에 따라 규정을 준수하는지 확인합니다.
- 드라이버의 경우 OMIVV는 VMware 하드웨어 호환성 목록에 나열된 오프라인 번들만 지원합니다.
- 클러스터가 선택한 데이터 마이그레이션 옵션에 대한 vSAN 요구 사항을 만족합니다. vSAN 클러스터가 선택한 데이터 마이그레이션 옵션의 요구 사항을 충족하지 않는 경우 업데이트 시간이 초과됩니다.
- Dell EMC는 기준이 설정된 (클러스터 프로필) 펌웨어나 드라이버 리포지토리를 선택하는 것을 권장합니다.
- 업데이트 중인 클러스터에 활성 펌웨어 업데이트 작업이 없는지 확인합니다.
- "유지 보수 모드 진입" 작업에 필요한 시간 초과 값을 지정하는지 확인합니다. 대기 시간이 지정된 시간을 지나면 업데이트 작업이 실패합니다. 하지만 호스트가 재부팅될 때 구성 요소가 자동으로 업데이트될 수도 있습니다.
- vSAN을 활성화한 후 인벤토리를 다시 실행해야 합니다.

Dell EMC는 펌웨어 업데이트 프로세스 중에 다음 항목을 삭제 또는 이동하지 않는 것을 권장합니다.

- 펌웨어 업데이트 작업이 진행 중인 vCenter의 클러스터 호스트
- 펌웨어 업데이트 작업이 진행 중인 호스트의 호스트 자격 증명 프로필
- CIFS 또는 NFS에 있는 리포지토리

노트: VMware에서는 클러스터를 동일한 서버 하드웨어에 구성할 것을 권장합니다.

OMIVV는 호스트 준수 및 동일한 클러스터 내 호스트에서 진행 중인 다른 펌웨어 업데이트 작업 여부를 확인합니다. 확인 후에 펌웨어 업데이트 마법사가 표시됩니다.

1. 펌웨어 업데이트 마법사를 실행하려면 OMIVV 홈 페이지에서 **메뉴**를 확장하고 **호스트 및 클러스터**를 선택한 후 다음 작업 중 하나를 수행합니다.
   - 클러스터를 마우스 오른쪽 버튼으로 클릭하고 **OMIVV 클러스터 작업** > **펌웨어 업데이트**를 선택합니다.

- 클러스터를 선택하고 오른쪽 창에서 **모니터링** > **OMIVV 클러스터 정보** > **펌웨어** > **펌웨어 마법사 실행**을 선택합니다.

2. **펌웨어 업데이트 체크리스트** 페이지에서 업데이트를 예약하기 전에 모든 필수 조건을 확인한 후 **시작하기**를 클릭합니다.
3. **업데이트 소스** 페이지에서 펌웨어 및 드라이버 리포지토리 프로필을 선택합니다.

   클러스터 프로필이 호스트가 있는 클러스터에 연결된 경우 기본적으로 연결된 펌웨어 및 드라이버 리포지토리 프로필이 선택됩니다.

   펌웨어 또는 드라이버 리포지토리 프로필을 변경하면 선택한 리포지토리 프로필이 기준과 연결되지 않았음을 나타내는 메시지가 표시되고 다른 리포지토리를 사용하면 기준 비교에 영향을 줄 수 있습니다.

   노트: 드라이버 및 펌웨어 리포지토리가 모두 클러스터 프로필에 연결된 경우 드라이버 및 펌웨어를 동시에 업데이트하는 것이 좋습니다.

   펌웨어 또는 드라이버를 업데이트하지 않거나, 펌웨어 또는 드라이버가 최신 상태라면 드롭다운 메뉴에서 **선택한 리포지토리 없음**을 선택합니다.

   기본 펌웨어 카탈로그(Dell EMC 기본 카탈로그 및 검증된 MX 스택 카탈로그)는 리포지토리 프로필 옵션에 표시되지 않습니다. 리포지토리 프로필을 사용하려면 OMIVV에서 맞춤형 리포지토리를 생성합니다.

   사용자 지정 리포지토리 프로필을 생성하려면 다음을 수행합니다.

   a. DRM(Dell EMC Repository Manager)으로 이동하여 카탈로그를 생성합니다.

      DRM을 사용한 카탈로그 생성에 대한 자세한 내용은 OMIVV를 사용하여 DRM(Dell EMC Repository Manager)에서 카탈로그 생성 페이지 121을(를) 참조하십시오.

   b. 카탈로그 및 해당 파일을 다운로드합니다.

   c. 다운로드한 카탈로그를 이용하여 OMIVV에 리포지토리 프로필을 생성합니다.

      리포지토리 프로필 생성에 대한 자세한 내용은 리포지토리 프로필 생성 페이지 42을(를) 참조하십시오.

4. 선택한 펌웨어 리포지토리 프로필을 기반으로 적절한 번들을 선택한 후 **다음**을 클릭합니다. 64비트 번들만 지원됩니다.

   노트: OEM(디브랜딩된) 서버의 경우 모델이 달라도 하나의 번들만 선택할 수 있습니다. 하나 이상의 OEM 서버에 번들이 적용되지 않는 경우에도 펌웨어 업데이트 마법사의 구성 요소 페이지에는 각 OEM 서버 또는 펌웨어 구성 요소 쌍이 나열됩니다. 지정된 펌웨어 구성 요소 쌍의 펌웨어 업데이트에 실패하는 경우 OEM 서버에 표시된 대체 번들로 다시 시도하십시오.

5. **드라이버 구성 요소 선택** 페이지에서 업데이트가 필요한 드라이버 구성 요소를 선택한 후 **다음**을 클릭합니다. 업데이트를 위한 드라이버 구성 요소를 선택하면 패키지의 모든 구성 요소가 선택됩니다.

   필터 옵션을 사용하여 특정 열 이름을 기준으로 데이터를 필터링할 수 있습니다.
6. **펌웨어 구성 요소 선택** 페이지에서 업데이트가 필요한 펌웨어 구성 요소를 선택한 후 **다음**을 클릭합니다.

   중요도 상태(예: 긴급, 권장, 옵션 및 다운그레이드)에 따라 구성 요소의 개수가 표시됩니다.

   필터 옵션을 사용하여 특정 열 이름을 기준으로 데이터를 필터링할 수 있습니다.

   카탈로그에서 사용 가능한 버전보다 낮은 버전 또는 같은 수준(최신)이거나 업데이트가 예약된 구성 요소는 선택할 수 없습니다. 사용 가능한 버전보다 낮은 버전의 구성 요소를 선택하려면 **펌웨어 다운그레이드 허용** 확인란을 선택합니다.

   모든 페이지에서 모든 펌웨어 구성 요소를 선택하려면 을 클릭합니다.

   모든 페이지에서 모든 펌웨어 구성 요소를 지우려면 을 클릭합니다.
7. **업데이트 예약** 페이지에서 펌웨어 업데이트 작업 이름 및 설명을 입력합니다. 설명은 선택적인 필드입니다.

   펌웨어 업데이트 작업 이름은 필수입니다. 펌웨어 업데이트 작업 이름을 제거한 경우 작업 이름을 재사용할 수 있습니다.
8. **추가 설정** 섹션에서 다음을 수행합니다.

   a. 유지 보수 모드 시간 초과 값을 60~1440분으로 입력합니다. 대기 시간이 지정된 시간을 지나면 업데이트 작업이 실패하고 유지 보수 진입 작업이 취소되거나 시간 초과됩니다. 하지만 호스트가 재시작될 때 구성 요소가 자동으로 업데이트될 수도 있습니다.

   b. **유지 보수 모드 진입 옵션** 드롭다운 메뉴에서 적절한 데이터 마이그레이션 옵션을 선택합니다. 데이터 마이그레이션 옵션에 대한 자세한 내용은 VMware 설명서를 참조하십시오.

      노트: 클러스터 구성이 전체 데이터 마이그레이션을 지원하지 않거나 스토리지 용량이 부족하면 유지 보수 모드 진입 작업에 실패합니다.

      기본적으로 **전원이 꺼진 가상 시스템과 일시 중지된 가상 시스템을 클러스터의 다른 호스트로 이동** 옵션이 선택되어 있습니다. 이 옵션을 비활성화하면 호스트 장치가 온라인 상태가 될 때까지 VM 연결이 끊깁니다.

   c. 펌웨어를 업데이트하는 동안에 문제가 발생하면 **작업 대기열 삭제 및 iDRAC 재설정** 확인란을 선택합니다. 이로써 업데이트 프로세스가 성공적으로 완료될 수 있습니다. 이렇게 하면 작업 완료에 필요한 전체 업데이트 시간이 증가하고, iDRAC에 예약되어 있는 모든 보류 중인 작업 또는 활동이 취소되고, iDRAC이 재설정됩니다.

      섀시 자격 증명 프로필을 사용하여 관리되는 호스트의 경우 작업 대기열 삭제가 지원되지 않습니다.

9. **업데이트 일정** 섹션에서 다음 옵션 중 하나를 선택합니다.
   - **지금 업데이트**
   - **업데이트 예약**
10. **요약 검토** 페이지에서 펌웨어 업데이트 정보를 검토한 후 **마침**을 클릭합니다.
    펌웨어 업데이트 작업은 구성 요소 및 선택한 서버 수에 따라 최대 몇 시간이 소요될 수 있습니다. **작업** 페이지에서 작업 상태를 볼 수 있습니다.

    펌웨어 업데이트 작업이 완료되면 **업데이트 예약** 페이지에서 선택한 옵션을 기반으로 인벤토리가 선택한 호스트에서 자동으로 실행되고 호스트의 유지 보수 모드가 자동으로 종료됩니다.

vSphere 호스트에서 펌웨어 업데이트

vSphere 호스트에서 펌웨어 업데이트를 예약하기 전에(ESXi만 해당) 환경에서 다음 조건이 환경에서 충족되는지 확인합니다.

- 호스트가 규정을 준수하고(CSIOR이 활성화되었고 호스트가 ESXi 버전을 지원했음) 호스트 자격 증명 프로필과 연결되어 있고 인벤토리되었는지 확인합니다.
- DRS가 활성화되었습니다.

  노트: 독립 실행형 호스트의 경우 DRS 점검을 적용할 수 없습니다.

  필수 조건 점검을 건너뛰려면 **업데이트 예약** 페이지에서 **필수 조건 점검** 확인란의 선택을 취소하십시오.

  노트: 드라이버 업데이트는 vSphere 클러스터 및 호스트에서 지원되지 않습니다.

Dell EMC는 펌웨어 업데이트 프로세스 중에 다음 항목을 삭제 또는 이동하지 않는 것을 권장합니다.

- 펌웨어 업데이트 작업이 진행 중인 vCenter의 호스트
- 펌웨어 업데이트 작업이 진행 중인 호스트의 호스트 자격 증명 프로필
- CIFS 또는 NFS에 있는 리포지토리

OMIVV는 호스트 준수 및 동일한 클러스터 내 호스트에서 진행 중인 다른 펌웨어 업데이트 작업 여부를 확인합니다. 확인 후에 펌웨어 업데이트 마법사가 표시됩니다.

1. 펌웨어 업데이트 마법사를 실행하려면 OMIVV 홈 페이지에서 **메뉴**를 확장하고 **호스트 및 클러스터**를 선택한 후 다음 작업 중 하나를 수행합니다.
   - 호스트를 마우스 오른쪽 단추로 클릭하고 **OMIVV 호스트 작업** > **펌웨어 업데이트**를 선택합니다.
   - 호스트를 선택하고 오른쪽 창에서 **모니터링** > **OMIVV 호스트 정보** > **펌웨어** > **펌웨어 마법사 실행**을 선택합니다.
   - 호스트를 선택하고 오른쪽 창에서 **요약**을 선택한 후 **OMIVV 호스트 정보** > **호스트 작업** > **펌웨어 마법사 실행**으로 이동합니다.
2. **펌웨어 업데이트 체크리스트** 페이지에서 업데이트를 예약하기 전에 모든 필수 조건을 확인한 후 **시작하기**를 클릭합니다.
3. **업데이트 소스** 페이지에서 다음 중 하나를 선택합니다.
   - **리포지토리 프로필**
   - **단일 DUP**
4. 파일에서 단일 펌웨어 업데이트를 로드하려면 **단일 DUP**를 선택합니다.
   a. 단일 DUP는 OMIVV 어플라이언스에서 액세스할 수 있는 CIFS 또는 NFS 공유에 있을 수 있습니다. 파일 위치를 다음 형식 중 하나로 입력한 후 8단계로 이동합니다.
      - NFS—`<host>:/<share_path/FileName.exe`
      - CIFS—`\\<host accessible share path>\<FileName>.exe`

      노트: 단일 구성 요소 DUP의 파일 이름에 빈 공간이 없는지 확인합니다.

      CIFS 공유의 경우 OMIVV에 공유 드라이브에 액세스할 수 있는 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다.
5. **리포지토리 프로필** 옵션을 선택한 경우 펌웨어 리포지토리 프로필을 선택합니다.
   클러스터 프로필이 호스트가 있는 클러스터에 연결된 경우 기본적으로 연결된 펌웨어 리포지토리 프로필이 선택됩니다. 그렇지 않으면 **Dell 기본 카탈로그**가 선택됩니다.

   펌웨어 리포지토리 프로필을 변경하면 선택한 리포지토리 프로필이 기준과 연결되지 않았음을 나타내는 메시지가 표시되고 다른 리포지토리를 사용하면 기준 비교에 영향을 줄 수 있습니다.
6. 선택한 펌웨어 리포지토리 프로필을 기반으로 적절한 번들을 선택한 후 **다음**을 클릭합니다. 64비트 번들만 지원됩니다.
7. **펌웨어 구성 요소 선택** 페이지에서 업데이트가 필요한 펌웨어 구성 요소를 선택한 후 **다음**을 클릭합니다.
   중요도 상태(예: 긴급, 권장, 옵션 및 다운그레이드)에 따라 구성 요소의 개수가 표시됩니다.

필터 옵션을 사용하여 특정 열 이름을 기준으로 데이터를 필터링할 수 있습니다.

카탈로그에서 사용 가능한 버전보다 낮은 버전 또는 같은 수준(최신)이거나 업데이트가 예약된 구성 요소는 선택할 수 없습니다. 사용 가능한 버전보다 낮은 버전의 구성 요소를 선택하려면 **펌웨어 다운그레이드 허용** 확인란을 선택합니다.

모든 페이지에서 모든 펌웨어 구성 요소를 선택하려면 을 클릭합니다.

모든 페이지에서 모든 펌웨어 구성 요소를 지우려면 을 클릭합니다.

8. **업데이트 예약** 페이지에서 펌웨어 업데이트 작업 이름 및 설명을 입력합니다. 설명은 선택적인 필드입니다.
   펌웨어 업데이트 작업 이름은 필수입니다. 펌웨어 업데이트 작업 이름을 제거한 경우 작업 이름을 재사용할 수 있습니다.
9. **추가 설정** 섹션에서 다음을 수행합니다.
   a. 유지 보수 모드 시간 초과 값을 60~1440분으로 입력합니다. 대기 시간이 지정된 시간을 지나면 업데이트 작업이 실패하고 유지 보수 진입 작업이 취소되거나 시간 초과됩니다. 하지만 호스트가 재시작될 때 구성 요소가 자동으로 업데이트될 수도 있습니다.
      기본적으로 다음 옵션이 선택되어 있습니다.
      - **펌웨어 업데이트 완료 후 유지 보수 모드 종료** - 이 옵션을 비활성화하면 호스트가 유지 보수 모드로 유지됩니다.
      - **전원이 꺼진 가상 시스템과 일시 중지된 가상 시스템을 클러스터의 다른 호스트로 이동** - 이 옵션을 비활성화하면 호스트 장치가 온라인 상태가 될 때까지 VM 연결이 해제됩니다.

   b. 펌웨어를 업데이트하는 동안에 문제가 발생하면 **작업 대기열 삭제 및 iDRAC 재설정** 확인란을 선택합니다. 이로써 업데이트 프로세스가 성공적으로 완료될 수 있습니다. 이렇게 하면 작업 완료에 필요한 전체 업데이트 시간이 증가하고, iDRAC에 예약되어 있는 모든 보류 중인 작업 또는 활동이 취소되고, iDRAC이 재설정됩니다.
      섀시 자격 증명 프로필을 사용하여 관리되는 호스트의 경우 작업 대기열 삭제가 지원되지 않습니다.
      기본적으로 **필수 조건 점검** 옵션이 선택되어 있습니다.
10. **업데이트 일정** 섹션에서 다음 옵션 중 하나를 선택합니다.
    - **지금 업데이트**
    - **업데이트 예약**
    - **다음 재부팅 시에 업데이트 적용**
    - **업데이트 적용 및 유지 보수 모드로 진입하지 않고 강제 재부팅**
11. **요약 검토** 페이지에서 펌웨어 업데이트 정보를 검토한 후 **마침**을 클릭합니다.
    펌웨어 업데이트 작업은 구성 요소 및 선택한 서버 수에 따라 최대 몇 시간이 소요될 수 있습니다. **작업** 페이지에서 작업 상태를 볼 수 있습니다.
    펌웨어 업데이트 작업이 완료되면 **업데이트 예약** 페이지에서 선택한 옵션을 기반으로 인벤토리가 선택한 호스트에서 자동으로 실행되고 호스트의 유지 보수 모드가 자동으로 종료됩니다.

vSphere 클러스터에서 펌웨어 업데이트

펌웨어 업데이트를 예약하기 전에 다음 조건이 환경에서 충족되는지 확인합니다.

- 호스트가 규정을 준수하고(CSIOR이 활성화되었고 호스트가 ESXi 버전을 지원했음) 호스트 자격 증명 프로필과 연결되어 있고 인벤토리되었는지 확인합니다. 호스트가 나열되지 않으면 OMIVV에서 호스트에 대한 관리 규정 준수 마법사를 실행한 후 펌웨어 업데이트 마법사를 사용합니다.
- DRS가 활성화되었습니다.
- 업데이트 중인 클러스터에 활성 펌웨어 업데이트 작업이 없는지 확인합니다.
- "유지 보수 모드 진입" 작업에 필요한 시간 초과 값을 지정하는지 확인합니다. 대기 시간이 지정된 시간을 지나면 업데이트 작업이 실패합니다. 하지만 호스트가 재부팅될 때 구성 요소가 자동으로 업데이트될 수도 있습니다.

노트: 드라이버 업데이트는 vSphere 클러스터 및 호스트에서 지원되지 않습니다.

Dell EMC는 펌웨어 업데이트 프로세스 중에 다음 항목을 삭제 또는 이동하지 않는 것을 권장합니다.

- 펌웨어 업데이트 작업이 진행 중인 vCenter의 클러스터 호스트
- 펌웨어 업데이트 작업이 진행 중인 호스트의 호스트 자격 증명 프로필
- CIFS 또는 NFS에 있는 리포지토리

노트: VMware에서는 클러스터를 동일한 서버 하드웨어에 구성할 것을 권장합니다.

OMIVV는 호스트 준수 및 동일한 클러스터 내 호스트에서 진행 중인 다른 펌웨어 업데이트 작업 여부를 확인합니다. 확인 후에 펌웨어 업데이트 마법사가 표시됩니다.

1. 펌웨어 업데이트 마법사를 실행하려면 OMIVV 홈 페이지에서 **메뉴**를 확장하고 **호스트 및 클러스터**를 선택한 후 다음 작업 중 하나를 수행합니다.
   - 클러스터를 마우스 오른쪽 단추로 클릭하고 **OMIVV 클러스터 작업** > **펌웨어 업데이트**를 선택합니다.
   - 클러스터를 선택하고 오른쪽 창에서 **모니터링** > **OMIVV 클러스터 정보** > **펌웨어** > **펌웨어 마법사 실행**을 선택합니다.
2. **펌웨어 업데이트 체크리스트** 페이지에서 업데이트를 예약하기 전에 모든 필수 조건을 확인한 후 **시작하기**를 클릭합니다.
3. **업데이트 소스** 페이지에서 클러스터 프로필이 호스트가 있는 클러스터에 연결된 경우 기본적으로 연결된 펌웨어 리포지토리가 선택됩니다. 그렇지 않으면 **Dell 기본 카탈로그**가 선택됩니다.

   펌웨어 리포지토리 프로필을 변경하면 선택한 리포지토리 프로필이 기준과 연결되지 않았음을 나타내는 메시지가 표시되고 다른 리포지토리를 사용하면 기준 비교에 영향을 줄 수 있습니다.
4. 선택한 펌웨어 리포지토리 프로필을 기반으로 적절한 번들을 선택한 후 **다음**을 클릭합니다. 64비트 번들만 지원됩니다.

   노트: OEM(디브랜딩된) 서버의 경우 모델이 달라도 하나의 번들만 선택할 수 있습니다. 하나 이상의 OEM 서버에 번들이 적용되지 않는 경우에도 펌웨어 업데이트 마법사의 구성 요소 페이지에는 각 OEM 서버 또는 펌웨어 구성 요소 쌍이 나열됩니다. 지정된 펌웨어 구성 요소 쌍의 펌웨어 업데이트에 실패하는 경우 OEM 서버에 표시된 대체 번들로 다시 시도하십시오.
5. **펌웨어 구성 요소 선택** 페이지에서 업데이트가 필요한 펌웨어 구성 요소를 선택한 후 **다음**을 클릭합니다.

   중요도 상태(예: 긴급, 권장, 옵션 및 다운그레이드)에 따라 구성 요소의 개수가 표시됩니다.

   카탈로그에서 사용 가능한 버전보다 낮은 버전 또는 같은 수준(최신)이거나 업데이트가 예약된 구성 요소는 선택할 수 없습니다. 사용 가능한 버전보다 낮은 버전의 구성 요소를 선택하려면 **펌웨어 다운그레이드 허용** 확인란을 선택합니다.

   필터 옵션을 사용하여 특정 열 이름을 기준으로 데이터를 필터링할 수 있습니다.

   모든 페이지에서 모든 펌웨어 구성 요소를 선택하려면  을 클릭합니다.

   모든 페이지에서 모든 펌웨어 구성 요소를 지우려면  을 클릭합니다.
6. **업데이트 예약** 페이지에서 펌웨어 업데이트 작업 이름 및 설명을 입력합니다. 설명은 선택적인 필드입니다.

   펌웨어 업데이트 작업 이름은 필수입니다. 펌웨어 업데이트 작업 이름을 제거한 경우 작업 이름을 재사용할 수 있습니다.
7. **추가 설정** 섹션에서 다음을 수행합니다.
   a. 유지 보수 모드 시간 초과 값을 60~1440분으로 입력합니다. 대기 시간이 지정된 시간을 지나면 업데이트 작업이 실패하고 유지 보수 진입 작업이 취소되거나 시간 초과됩니다. 하지만 호스트가 재시작될 때 구성 요소가 자동으로 업데이트될 수도 있습니다.

      기본적으로 **전원이 꺼진 가상 시스템과 일시 중지된 가상 시스템을 클러스터의 다른 호스트로 이동** 옵션이 선택되어 있습니다. 이 옵션을 비활성화하면 호스트 장치가 온라인 상태가 될 때까지 VM 연결이 끊깁니다.

   b. 펌웨어를 업데이트하는 동안에 문제가 발생하면 **작업 대기열 삭제 및 iDRAC 재설정** 확인란을 선택합니다. 이로써 업데이트 프로세스가 성공적으로 완료될 수 있습니다. 이렇게 하면 작업 완료에 필요한 전체 업데이트 시간이 증가하고, iDRAC에 예약되어 있는 모든 보류 중인 작업 또는 활동이 취소되고, iDRAC이 재설정됩니다.

      섀시 자격 증명 프로필을 사용하여 관리되는 호스트의 경우 작업 대기열 삭제가 지원되지 않습니다.
8. **업데이트 일정** 섹션에서 다음 옵션 중 하나를 선택합니다.
   - **지금 업데이트**
   - **업데이트 예약**
9. **요약 검토** 페이지에서 펌웨어 업데이트 정보를 검토한 후 **마침**을 클릭합니다.
   펌웨어 업데이트 작업은 구성 요소 및 선택한 서버 수에 따라 최대 몇 시간이 소요될 수 있습니다. **작업** 페이지에서 작업 상태를 볼 수 있습니다.

   펌웨어 업데이트 작업이 완료되면 **업데이트 예약** 페이지에서 선택한 옵션을 기반으로 인벤토리가 선택한 호스트에서 자동으로 실행되고 호스트의 유지 보수 모드가 자동으로 종료됩니다.

동일한 펌웨어 구성 요소 유형 업데이트

다음은 동일한 유형의 펌웨어 구성 요소를 업데이트할 때 기억해야 할 핵심 포인트입니다.

- 버전이 같은 동일한 유형의 구성 요소가 서버에 여러 개 있는 경우 구성 요소의 한 가지 버전만 **펌웨어 구성 요소 선택** 페이지에 표시됩니다. 업데이트는 모든 구성 요소에 적용되고 변경 사항 세부 정보는 하나의 구성 요소 버전에만 표시됩니다.

  예를 들면, 다음과 같습니다.

표 19. 서버에 동일한 유형의 구성 요소가 여러 개 있는 예

구성 요소	현재 버전	사용 가능한 버전
HDD1	V1	V3
HDD2	V1	V3
HDD3	V1	V3

이 경우 **펌웨어 구성 요소 선택** 페이지에 다음이 표시됩니다.

표 20. 서버에 동일한 버전의 구성 요소가 여러 개 있는 예

구성 요소	현재 버전	사용 가능한 버전
HDD1	V1	V3

- 버전이 다르지만 동일한 유형의 구성 요소가 서버에 여러 개 있는 경우 각 고유 버전에 대한 단일 구성 요소가 표시됩니다. 이 경우 하나의 구성 요소를 선택하면 현재 펌웨어 버전과 상관없이 모든 구성 요소에 업데이트가 적용됩니다. 변경 사항 세부 정보는 현재 펌웨어 버전과 상관없이 모든 구성 요소에 표시됩니다.

  예를 들면, 다음과 같습니다.

표 21. 서버에 버전이 다른 구성 요소가 여러 개 있는 예

구성 요소	현재 버전	사용 가능한 버전
HDD1	V1	V3
HDD2	V2	V3
HDD3	V2	V3

이 경우 **펌웨어 구성 요소 선택** 페이지에 다음이 표시됩니다.

표 22. 서버에 버전이 다른 구성 요소가 여러 개 있는 예

구성 요소	현재 버전	사용 가능한 버전
HDD1	V1	V3
HDD2	V2	V3

- 카탈로그에 사용 가능한 버전이 여러 개 있는 경우 구성 요소 유형에 사용 가능한 버전 중 하나만 선택하는 것이 좋습니다. 그러면 선택한 펌웨어는 현재 버전과 상관없이 모든 해당 구성 요소에 적용됩니다.

  예를 들면, 다음과 같습니다.

표 23. 카탈로그에 사용 가능한 버전이 여러 개 있는 예

구성 요소	현재 버전	사용 가능한 버전
HDD1	V1	V3
HDD2	V2	V3
HDD3	V2	V3
HDD1	V1	V4
HDD2	V2	V4
HDD3	V2	V4

이 경우 **펌웨어 구성 요소 선택** 페이지에 다음이 표시됩니다.

표 24. 카탈로그에 사용 가능한 버전이 여러 개 있는 예

구성 요소	현재 버전	사용 가능한 버전
HDD1	V1	V3
HDD2	V2	V3

표 24. 카탈로그에 사용 가능한 버전이 여러 개 있는 예 (계속)

구성 요소	현재 버전	사용 가능한 버전
HDD1	V1	V4
HDD2	V2	V4

vSphere Lifecycle Manager 개요

vSphere Lifecycle Manager는 vCenter 서버에서 실행되는 서비스입니다(vCenter 7.0 이상 버전에 해당).

vSphere Lifecycle Manager를 사용하여 ESXi 이미지, 펌웨어 및 드라이버로 구성된 기본 이미지를 생성할 수 있습니다. 이는 클러스터의 모든 호스트가 규정 준수 검사를 수행하여 기본 이미지에 적합하도록 합니다. 규정을 준수하지 않는 경우 클러스터 문제를 해결하는 옵션을 제공합니다.

vSphere Lifecycle Manager에서 OMIVV는 펌웨어 추가 기능 공급자 역할을 합니다. vSphere Lifecycle Manager에 대한 자세한 내용은 VMware 설명서를 참조하십시오.

OMIVV에서 vSphere Lifecycle Manager를 사용하려면 vCenter 등록이 필수입니다. vCenter 등록 및 vSphere Lifecycle Manager에 대한 자세한 내용은 새 vCenter Server 등록 페이지 12을(를) 참조하십시오.

vCenter를 등록하는 동안 Dell EMC 관리 콘솔에서 vCenter 7.0 이상에 해당하는 vSphere Lifecycle Manager를 등록할 수 있습니다. vCenter 등록이 완료되면 Dell EMC 관리 콘솔의 **VCENTER 등록** 페이지에서 vSphere LifeCycle Manager 등록 상태를 수정(등록 또는 등록 취소)할 수 있습니다. 자세한 내용은 Dell EMC 관리 콘솔에서 vSphere Lifecycle Manager 등록 페이지 127 및 Dell EMC 관리 콘솔에서 vSphere Lifecycle Manager 등록 취소 페이지 127을(를) 참조하십시오.

Dell EMC 관리 콘솔에서 vSphere Lifecycle Manager 상태 보기

다음은 **vSphere Lifecycle Manager** 열에서 볼 수 있는 vSphere Lifecycle Manager 상태입니다.

- **등록**(vCenter 7.0 이상에만 해당) - vSphere Lifecycle Manager가 등록되지 않은 경우 표시됩니다.
- **등록 취소**(vCenter 7.0 이상에만 해당) - vSphere Lifecycle Manager가 이미 등록된 경우 표시됩니다.
- **없음** - 등록된 vCenter 버전이 7.0 이전인 경우에만 표시됩니다. vCenter 7.0로 업그레이드된 경우 상태는 **해당 없음**으로 유지됩니다. 상태를 반영하려면 OMIVV 어플라이언스를 재시작합니다.

Dell EMC 관리 콘솔에서 vSphere Lifecycle Manager 등록

vCenter 7.0 이상 버전이어야 합니다.

1. https://<ApplianceIP/hostname/>으로 이동합니다.
2. **VCENTER 등록** 페이지의 **vSphere Lifecycle Manager**에서 **등록**을 클릭합니다.
   VSPHERE LIFECYCLE MANAGER 등록 <vCenter 이름> 대화 상자가 표시됩니다.
3. **vSphere Lifecycle Manager 등록**을 클릭합니다.
   vSphere Lifecycle Manager를 성공적으로 등록했음을 나타내는 메시지가 표시됩니다.

Dell EMC 관리 콘솔에서 vSphere Lifecycle Manager 등록 취소

vCenter 7.0 이상 버전이어야 합니다.

1. https://<ApplianceIP/hostname/>으로 이동합니다.
2. **VCENTER 등록** 페이지의 **vSphere Lifecycle Manager**에서 **등록 취소**를 클릭합니다.
   VSPHERE LIFECYCLE MANAGER 등록 취소 <vCenter 이름> 대화 상자가 표시됩니다.
3. **등록 취소**를 클릭합니다.
   vSphere Lifecycle Manager를 등록 취소했음을 나타내는 메시지가 표시됩니다. **DellEMC OMIVV**는 VSphere Lifecycle Manager의 **하드웨어 지원 관리자** 목록에서 제거됩니다. 이는 OMIVV 기능에는 영향을 미치지 않습니다.

vSphere Lifecycle Manager를 사용하여 클러스터 관리

사전 구성 요소:

vSphere Lifecycle Manager를 사용하여 클러스터를 관리하기 전에 다음을 확인합니다.

- vSphere Lifecycle Manager는 Dell EMC 관리 콘솔에서 활성화됩니다. 자세한 내용은 Dell EMC 관리 콘솔에서 vSphere Lifecycle Manager 등록 페이지 127을(를) 참조하십시오.
- 클러스터의 호스트는 관리 규정을 준수합니다. 자세한 내용은 관리 규정 준수 페이지 63을(를) 참조하십시오.
- 클러스터 프로필은 선택된 클러스터에 대해 생성되었고 클러스터 프로필은 OMIVV의 펌웨어 리포지토리와 연결됩니다. 클러스터 프로필에 대한 자세한 내용은 클러스터 프로필 생성 페이지 46을(를) 참조하십시오.

vSphere Lifecycle Manager의 사용자 인터페이스 또는 vSphere Automation API를 사용하여 클러스터를 관리할 수 있습니다. OMIVV는 사용자 인터페이스와 vSphere Automation API를 모두 사용하여 클러스터 관리를 지원합니다.

노트: VSphere Lifecycle Manager 관리 클러스터에서 시스템 잠금 및 펌웨어 업데이트와 같은 OMIVV 클러스터 작업을 사용할 수 있지만 기준 보고에 영향을 미칠 수 있습니다.

vSphere Lifecycle Manager에서 펌웨어 추가 기능 공급자로 OMIVV 사용 - 사용자 인터페이스

vSphere Lifecycle Manager에서 OMIVV를 펌웨어 추가 기능 공급자로 사용할 수 있습니다.

클러스터 프로필은 vSphere Lifecycle Manager 컨텍스트에서 HSP(Hardware Support Package)라고 합니다. OMIVV에서 생성된 클러스터 프로필은 vSphere Lifecycle Manager에서 **펌웨어 및 드라이버 추가 기능**으로 선택됩니다. 클러스터 프로필에 대한 자세한 내용은 클러스터 프로필 페이지 46을(를) 참조하십시오.

선택된 클러스터에 대한 이미지를 설정하고 OMIVV를 **펌웨어 및 드라이버 추가 기능**으로 연결하려면 다음 작업을 수행합니다.

1. vSphere Client에서 **호스트 및 클러스터**를 클릭한 다음 이미지를 사용하여 관리할 클러스터를 선택합니다.
2. **업데이트** 페이지의 왼쪽 창에서 **호스트**를 확장한 다음 **이미지**를 클릭합니다.
3. 펌웨어 및 드라이버 추가 기능을 선택하려면 선택 아이콘을 클릭합니다.
   펌웨어 및 드라이버 추가 기능 선택 페이지가 표시됩니다.
4. **하드웨어 지원 관리자 선택** 섹션에서 **DellEMC OMIVV**를 선택합니다.

   DELLEMC OMIVV를 선택하면 펌웨어 리포지토리에 연결된 모든 클러스터 프로필과 선택한 vCenter의 클러스터에 연결된 모든 클러스터 프로필이 **펌웨어 및 드라이버 추가 기능 선택** 섹션에 나열됩니다.
5. 선택한 클러스터에 적용할 수 있는 클러스터 프로필을 선택하고 **선택**을 클릭합니다.
   선택한 클러스터에 연결된 클러스터 프로필을 식별하려면 클러스터 프로필에 있는 설명을 참조하십시오.

   노트: OMIVV에서 클러스터 프로필을 생성하지 않은 경우 빈 목록이 표시됩니다. 클러스터 프로필 생성에 대한 자세한 사항은 클러스터 프로필 생성 페이지 46을(를) 참조하십시오.

   - **추가 기능 버전** - 클러스터 프로필의 현재 버전을 나타냅니다. 클러스터 프로필이 수정되거나 OMIVV 버전이 증가하는 경우 vSphere Lifecycle Manager에서 최신 버전의 클러스터 프로필을 사용하는지 확인합니다.

     노트: 경우에 따라 vSphere Lifecycle Manager에 펌웨어 비준수가 표시됩니다. 하지만 비준수 펌웨어는 vSphere Lifecycle Manager에 나열되지 않습니다. 이 문제를 해결하려면 클러스터 문제를 해결합니다. 클러스터 문제를 해결하기 위해 vSphere Lifecycle Manager가 재부팅되지는 않습니다.
   - **지원되는 ESXi 버전** - OMIVV에서 지원되는 ESXi 버전(7.0.0)을 나타냅니다.

   선택한 클러스터 프로필이 **업데이트** 페이지에 펌웨어 추가 기능으로 표시됩니다.
6. **저장**을 클릭합니다.
   vSphere Lifecycle Manager는 클러스터 규정 준수 검사를 수행합니다. 규정 준수 확인 결과는 vSphere Lifecycle Manager의 **이미지 규정 준수** 섹션에 표시됩니다.

   전반적인 규정 준수는 소프트웨어 규정 준수 및 펌웨어 규정 준수로 구성됩니다. OMIVV는 vSphere Lifecycle Manager 작업의 펌웨어 규정 준수 부분을 관리합니다.

클러스터 규정 준수 상태 보기

각 호스트에 대해 가능한 펌웨어 규정 준수 상태는 다음과 같습니다.

- **준수**: 호스트에 설치된 모든 펌웨어 구성 요소의 펌웨어 버전이 OMIVV의 클러스터 프로필에 표시된 펌웨어 버전과 동일한 경우 표시됩니다.
- **비준수**: 호스트에 설치된 하나 이상의 펌웨어 버전이 OMIVV의 클러스터 프로필에 표시된 펌웨어 버전과 일치하지 않은 경우 표시됩니다.

노트: OMIVV 어플라이언스를 업그레이드한 후, 이전 버전의 OMIVV로 생성된 이미지에 대한 vSphere Lifecycle Manager 규정 준수 확인 작업에 오류가 발생합니다. 이 문제를 해결하려면 최신 버전의 HSP(Hardware Support Package)로 이미지를 저장합니다.

- **호환되지 않음**: 다음과 같은 경우 표시됩니다.
  - vCenter에서 선택한 클러스터가 선택한 **펌웨어 및 드라이버 추가 기능**(OMIVV의 클러스터 프로필)에 연결되어 있지 않습니다.
  - 선택한 클러스터의 vSphere Lifecycle Manager 이미지를 저장한 후 클러스터 프로필의 펌웨어 리포지토리가 업데이트된 경우.
- **알 수 없음**: 호스트가 OMIVV에서 인벤토리되지 않은 경우 표시됩니다. 자세한 내용은 호스트 자격 증명 프로필 페이지 35을(를) 참조하십시오.

노트: OMIVV 및 vSphere Lifecycle Manager 변경 사항 보고서 간에 불일치가 발생할 수 있습니다. 이는 vSphere Lifecycle Manager에는 항상 실시간 변경 사항 보고서가 표시되고 OMIVV에는 예약 날짜 및 시간을 기준으로 변경 사항 보고서가 표시되기 때문입니다. 변경 사항 보고서 간에 불일치가 발생하는 경우 필요에 따라 OMIVV의 **변경 사항 감지 작업** 페이지에서 변경 사항 감지 작업을 실행합니다.

클러스터 규정 준수 문제 해결

1. 호스트 상태가 **준수**인 경우 해당 호스트에 대한 추가 조치는 필요하지 않습니다.
2. 호스트 상태가 **비준수**인 경우 문제 해결을 계속 진행합니다. 자세한 내용은 vSphere LifeCycle Manager에서 클러스터 문제 해결 페이지 130을(를) 참조하십시오.
3. 호스트 상태가 **호환되지 않음**인 경우 다음을 수행합니다.
   a. vCenter에서 선택한 클러스터가 클러스터 프로필에 연결되어 있는지 확인합니다. vSphere Lifecycle Manager에서 **펌웨어 및 드라이버 추가 기능**과 동일한 클러스터 프로필을 선택합니다.
   b. vSphere Lifecycle Manager 이미지를 편집하고 업데이트된 클러스터 프로필(펌웨어 및 드라이버 추가 기능)을 다시 선택한 후 이미지를 저장합니다.
4. 호스트 상태가 **알 수 없음**인 경우 OMIVV 및 인벤토리의 호스트 자격 증명 프로필에 추가된 호스트가 실행되고 있는지 확인합니다.

하드웨어 호환성 검사

vSphere Lifecycle Manager는 펌웨어 문제 해결을 수행하기 전에 vSAN 클러스터에 대한 하드웨어 호환성 검사를 수행하는 옵션을 제공합니다. 하드웨어 호환성 검사는 vSAN HCL(Hardware Compatibility List)에 나열된 하드웨어 및 지원되는 드라이버와 이미지에 있는 펌웨어 및 드라이버를 비교합니다. vSphere Lifecycle Manager는 스토리지 컨트롤러(PCIe 디바이스)에 대해서만 하드웨어 호환성 검사를 수행합니다. 지원되는 펌웨어 목록의 경우 vSphere Client에서 **모니터** > **vSAN** > **Skyline 상태**로 이동합니다.

하드웨어 호환성 검사를 수행하려면 **이미지 규정 준수** 섹션에서 **규정 준수 확인**을 클릭합니다.

OMIVV는 하드웨어 호환성 검사를 수행하는 동안 클러스터 프로필에 있는 펌웨어 버전을 반환합니다.

펌웨어 버전이 HCL(Hardware Compatibility List)에 나열된 펌웨어와 호환되는 경우 vSphere Lifecycle Manager가 규정 준수 상태를 **호환**으로 표시합니다. 규정 준수 상태에 대한 자세한 내용은 VMware 설명서를 참조하십시오.

하드웨어 호환성 검사 결과는 **하드웨어 호환성** 페이지에 표시됩니다.

문제 해결 사전 검사 실행

사전 검사 작업은 클러스터의 각 호스트에 대한 다양한 검사를 수행하여 클러스터에서 펌웨어 문제 해결을 준비하도록 합니다.

사전 검사는 호스트 또는 클러스터 수준에서 수행할 수 있는 선택적 작업입니다.

사전 검사 작업은 건너뛸 수 있습니다. vSphere Lifecycle Manager에서 문제 해결 시 사전 검사를 수행합니다.

사전 검사의 일환으로 OMIVV에서 다음 사항에 대해 사전 요구 사항 검사를 수행합니다.

- iDRAC 연결
- iDRAC 잠금 모드
- 선택한 클러스터의 호스트에 대해 OMIVV에서 트리거된 펌웨어 업데이트 작업(있는 경우)의 상태
- CSIOR(Collect System Inventory On Reboot) 활성화
- 펌웨어 리포지토리와 필요한 펌웨어 구성 요소에 대한 연결

펌웨어 문제 해결을 위한 사전 요구 사항을 확인하려면 **사전 검사 실행**을 클릭합니다.

사전 검사 작업 상태 및 결과는 **이미지 규정 준수** 섹션에 표시됩니다.

호스트에 대한 사전 검사에 실패할 경우 문제를 해결한 후 사전 검사를 다시 실행하거나 업데이트 작업을 계속합니다.

vSphere LifeCycle Manager에서 클러스터 문제 해결

이미지 규정 준수 섹션에서 개별 호스트 또는 클러스터에 있는 모든 호스트 문제를 한 번에 해결할 수 있습니다.

a. 개별 호스트에 대해 문제 해결 작업을 수행하려면 **이미지 규정 준수** 섹션에서 호스트 옆에 있는 세로로 된 생략 부호 아이콘을 클릭한 다음 **문제 해결**을 선택합니다.

b. 클러스터에 있는 모든 호스트에 대해 문제 해결 작업을 수행하려면 **이미지 규정 준수** 섹션에서 **모두 문제 해결**을 클릭합니다.

펌웨어 업데이트를 실행하기 전에 iDRAC 재설정을 수행하는 것이 좋습니다. iDRAC 재설정을 수행하면 장애가 발생할 가능성이 줄어듭니다.

각 호스트에서 vSphere Lifecycle Manager를 사용하여 펌웨어 업데이트를 수행하기 전에 iDRAC를 자동으로 재설정하려면 OMIVV에서 **iDRAC 작업 지우기 및 iDRAC 재설정** 확인란을 활성화합니다. 자세한 내용은 펌웨어 업데이트 설정 페이지 81을(를) 참조하십시오.

문제 해결 작업의 상태를 확인하려면 **업데이트** 페이지에서 **자세히 표시**를 클릭합니다.

OMIVV의 **로그** 페이지에서 OMIVV와 관련된 로그를 볼 수 있습니다.

vSphere Lifecycle Manager에서 펌웨어 추가 기능 공급자로 OMIVV 사용 - vSphere Automation API

VSphere Automation API를 사용하여 클러스터를 관리하기 전에 vSphere Lifecycle Manager 사용자 인터페이스를 사용하여 다음 작업을 완료해야 합니다.

- 하드웨어 지원 관리자로 DellEMC OMIVV를 선택합니다.
- 선택한 클러스터에 적용할 수 있는 클러스터 프로필을 선택하고 이미지를 저장합니다.

펌웨어 규정 준수 검사

명령: POST https://{VC IP/FQDN}/api/esx/settings/clusters/{cluster ID}/software?vmw-task=true&action=scan

```
{
    "spec" : {
      "message": "test commit"
    }
}
```

설명: 클러스터에 있는 모든 호스트에 대해 클러스터의 원하는 상태를 검사합니다. 이 작업의 결과는 `cis/tasks/{task-id}`를 호출하여 쿼리할 수 있습니다. 여기서 task-id는 이 작업의 응답입니다.

HTTP 응답 코드: 200 모든 응답 코드의 목록은 응답 코드 페이지 162을(를) 참조하십시오.

예제 응답:

```
{task ID}
```

규정 준수 작업 상태 가져오기

명령: GET https://{VC IP/FQDN}/rest/cis/tasks/{task ID}

설명: 작업에 대한 정보를 반환합니다.

HTTP 응답 코드: 200 모든 응답 코드의 목록은 응답 코드 페이지 162을(를) 참조하십시오.

예제 응답: 다음 예에는 펌웨어 비준수만 포함되어 있습니다.

```
"result":
[
```

```
{
 "value":
[
{
"value":
{
"hardware_modules":
[
{
 "value":
 {
 "current":
 {
 "version": "25.5.6.0009"
 },
 "details":
 {
 "component_class": "PCI_DEVICE",
 "description": "PERC H730 Mini"
 } "notifications":
 {
  "info":
 [
 {
 "id": "Different versions.",
 "time": "2020-02-04T10:47:54.422Z",
 "message":
 {
 "args": [],
 "default_message": "Different versions.",
 "id": "Different versions."
  }
  }
 ]
 },
 "status": "NON_COMPLIANT",
 "target": {
 "version": "25.5.5.0005"
  }
  }
 "key": ""
  }
  ],
 "notifications":
 {
 "info":
 [
 {
 "id": "[vCenter:<vCenter IP/FQDN>][Cluster: <Cluster name>][Host: <host IP/
FQDN>]              The host is non-compliant",
 "time": "2020-02-04T10:47:54.423Z",
 "message":
 {
 "args": [],
 "default_message": "[vCenter:<vCenter IP/FQDN>][Cluster: <Cluster name>][Host: <host IP/
FQDN>] The host is non-compliant",
 "id": "[vCenter:<vCenter IP/FQDN>][Cluster: <Cluster name>][Host: <host IP/FQDN>] The host
is non-compliant"
 }
 }]
 },
"status": "NON_COMPLIANT",
"target": {
"pkg": "<cluster profile name>",
 "version": "0.0.0-0"
 }
 },
 "key": "com.dell.plugin.OpenManager_HWSupportManager"
 }
 ],
```

문제 해결 사전 검사 실행

명령: POST https://{VC IP/FQDN}/api/esx/settings/clusters/{cluster ID}/software?vmw-task=true&action=check

설명: 클러스터에 있는 모든 호스트에 원하는 상태를 적용하기 전에 클러스터에 대한 검사를 실행합니다. 클러스터의 모든 호스트가 원하는 상태로 업데이트될 수 있는 양호한 상태인지 확인합니다.

HTTP 응답 코드: 200 모든 응답 코드의 목록은 응답 코드 페이지 162을(를) 참조하십시오.

예제 응답:

```
{task-id}
```

문제 해결 사전 검사 작업 상태

명령: GET https://{VC IP/FQDN}/rest/cis/tasks/{task ID}

설명: 작업에 대한 정보를 반환합니다.

HTTP 응답 코드: 200 모든 응답 코드의 목록은 응답 코드 페이지 162을(를) 참조하십시오.

예제 응답:

```
{
 "value":
{
"parent": "",
"cancelable": true,
"end_time": "2020-02-12T18:03:59.391Z",
"description":
{
 "args": [],
 "default_message": "Task created by VMware vSphere Lifecycle Manager",
 "id": "com.vmware.vcIntegrity.lifecycle.Task.Description"
  },
 "target":
{
"id": "domain-c8",
 "type": "ClusterComputeResource"
 },
 "result":
{
"start_time": "2020-02-12T17:52:09.264Z",
"commit": "",
"end_time": "2020-02-12T18:03:59.386Z",
 "entity_results":
[
{
"host": "host-47",
"type": "HOST",
"check_statuses": [],
"status": "OK"
 }
 {
"host": "host-41",
"type": "HOST",
"check_statuses": [],
"status": "OK"
 },
 {
 "host": "host-22",
 "type": "HOST",
 "check_statuses": [],
 "status": "OK"
  },
{
  "host": "host-16",
  "type": "HOST",
  "check_statuses": [
{
```

```
  "check":
 {
   "name":
  {
  "args": [],
  "default_message": "Host Hardware support check.",
  "id": "com.vmware.vcIntegrity.lifecycle.ClusterHealthCheckTask.HwSupportCheck.Name"
   },
  "description":
 {
  "args": [],
  "default_message": "Checks if the hardware update can be performed.",
  "id": "com.vmware.vcIntegrity.lifecycle.ClusterHealthCheckTask.HwSupportCheck.Description"
  },
  "check": "com.vmware.vcIntegrity.lifecycle.ClusterHealthCheckTask.HwSupportCheck"
  },
 "issues": [
 {
 "args": [],
 "default_message": "[vCenter: jpvc7dot0d5-2.sped.bdcsv.lab][Cluster:
R6415_vSAN_AllFlash_ESXi7.0RC+][Host: 100.100.10.154][Update PreCheck Task] System Lockdown
Mode is turned On for iDRAC IP, 172.20.5.5; hence Firmware update cannot continue.",
"id": "[vCenter: jpvc7dot0d5-2.sped.bdcsv.lab][Cluster: R6415_vSAN_AllFlash_ESXi7.0RC+][Host:
100.100.10.154][Update PreCheck Task] System Lockdown Mode is turned On for iDRAC IP,
172.20.5.5; hence Firmware update cannot continue."
 }
],
"status": "ERROR"
 }
 ],
"status": "ERROR"
 },
 {
 "host": "host-19",
 "type": "HOST",
 "check_statuses": [],
 "status": "OK"
 },
 {
"host": "host-13",
 "type": "HOST",

 "check_statuses": [],
 "status": "OK"
  },
```


클러스터 문제 해결

명령: POST https://{{VC IP/FQDN}/}}/api/esx/settings/clusters/{cluster ID}/software?vmw-task=true&action=apply

```
{
 "accept_eula" : true
}
```

설명: 지정된 클러스터와 관련된 원하는 상태를 클러스터에 있는 호스트에 적용합니다.

HTTP 응답 코드: 200 모든 응답 코드의 목록은 응답 코드 페이지 162을(를) 참조하십시오.

예제 응답:

```
{task-id}
```

깜박임 표시등 설정

대규모 데이터센터 환경에서 실제 서버를 쉽게 찾기 위해 일정 기간(시간) 동안 전면 표시등이 깜빡이도록 설정할 수 있습니다.

1. **서버 LED 깜박임 표시등** 마법사를 실행하려면 다음 작업 중 하나를 수행하십시오.
   a. OMIVV 홈 페이지에서 **메뉴**를 확장하고 **호스트 및 클러스터**를 선택하고 호스트 또는 클러스터를 마우스 오른쪽 버튼으로 클릭한 후 **요약** > **OMIVV 호스트 정보** > **호스트 작업** > **서버 LED 깜박임 표시등**으로 이동합니다.
   b. 호스트를 마우스 오른쪽 버튼으로 클릭하고 **OMIVV 호스트 작업** > **서버 LED 깜박임 표시등**으로 이동합니다.
2. 오른쪽 창에서 요약을 클릭한 후 **OMIVV 호스트 정보** > **호스트 작업** > **서버 LED 깜박임 표시등**으로 이동합니다.
   서버 LED 깜박임 표시등 대화 상자가 표시됩니다.
3. 다음 중 하나를 선택합니다.
   a. 서버 LED 표시등을 켜고 기간을 설정하려면 **켜기**를 클릭합니다.
   b. 서버 LED 표시등을 끄려면 **끄기**를 클릭합니다.

시스템 잠금 모드 구성

시스템 잠금 모드는 Enterprise 라이선스가 있는 iDRAC9 기반 서버에서만 지원됩니다. 시스템 잠금 모드를 켜는 경우 펌웨어 업데이트를 포함하여 시스템 구성이 잠깁니다. 시스템 잠금 모드 설정은 의도하지 않은 변경으로부터 시스템을 보호하기 위해 사용됩니다. OMIVV 어플라이언스를 사용하거나 iDRAC 콘솔에서 관리되는 호스트에 대한 시스템 잠금 모드를 켜거나 끌 수 있습니다. OMIVV 버전 4.1 이상에서 서버의 iDRAC 잠금 모드를 구성하고 모니터링할 수 있습니다. 또한 iDRAC에 Enterprise 라이선스가 있어야 잠금 모드를 활성화할 수 있습니다.

노트: 섀시 자격 증명 프로필을 사용하여 관리하는 호스트는 시스템 잠금 모드를 변경할 수 없습니다.

호스트나 클러스터 수준에서 호스트 또는 클러스터를 잠그거나 잠금 해제하여 시스템 잠금 모드를 구성할 수 있습니다. 시스템 잠금 모드가 켜져 있으면 다음과 같은 기능이 제한됩니다.

- 모든 구성 작업(예: 펌웨어 업데이트, OS 배포, 시스템 이벤트 로그 지우기, iDRAC 재설정 및 iDRAC 트랩 대상 구성)

1. 시스템 잠금 모드 구성 마법사를 실행하려면 다음과 같은 작업 중 하나를 수행하십시오.
   a. OMIVV 홈 페이지에서 **메뉴**를 확장하고 **호스트 및 클러스터**를 선택하고 호스트 또는 클러스터를 마우스 오른쪽 버튼으로 클릭한 후 **요약** > **OMIVV 호스트 정보** > **호스트 작업** > **시스템 잠금 모드 구성**으로 이동합니다.
   b. 호스트 또는 클러스터를 마우스 오른쪽 버튼으로 클릭하고 **OMIVV Host 작업** > **시스템 잠금 모드 구성**으로 이동합니다.
   c. 호스트 또는 클러스터를 선택하고 **모니터** > **OMIVV 호스트 또는 클러스터 정보** > **펌웨어** > **시스템 잠금 모드 구성**으로 이동합니다.
2. 클러스터 수준에서 시스템 잠금 모드 작업 이름 및 설명을 입력합니다. 설명은 선택적인 필드입니다.
3. 시스템 잠금 모드를 활성화하려면 **켜기**를 클릭합니다. 이 옵션은 시스템의 시스템 구성(펌웨어 및 BIOS 버전 포함) 변경을 제한합니다.
4. 시스템 잠금 모드를 비활성화하려면 **끄기**를 클릭합니다. 이 옵션은 시스템의 시스템 구성(펌웨어 및 BIOS 버전) 변경을 허용합니다.

   13세대 이전 PowerEdge 서버의 시스템 잠금 모드를 구성하려고 할 경우 해당 기능은 이 플랫폼에서 지원되지 않는다는 메시지가 표시됩니다.
5. **확인**을 클릭합니다.
   시스템 잠금 모드 구성을 위한 작업이 생성되었습니다. 작업 상태를 확인하려면 **작업** > **시스템 잠금 모드**로 이동하십시오. 시스템 잠금 모드 작업에 대한 자세한 내용은 시스템 잠금 모드 작업 페이지 70을(를) 참조하십시오.

18

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.

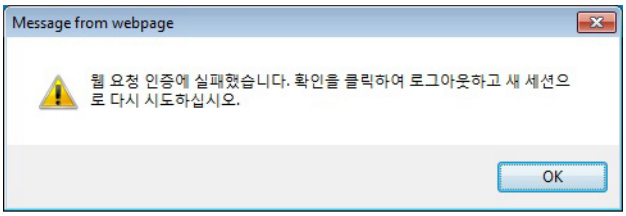


그림 1. 보안 오류 메시지

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 25. 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

표 25. 권한 그룹 (계속)

그룹 이름	설명
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

19

FAQ(자주 묻는 질문)

이 섹션에서는 문제 해결 질문에 대한 답을 확인할 수 있습니다. 이 섹션에 포함된 내용은 다음과 같습니다.

FAQ(자주 묻는 질문)

이 섹션에는 몇 가지 일반적인 질문과 해결 방법이 포함되어 있습니다.

비준수 vSphere 호스트에 대한 iDRAC 라이선스 유형 및 설명이 올바르지 않게 표시됨

CSIOR이 비활성화되어 있거나 실행되지 않았을 때 호스트가 비준수 상태인 경우, 유효한 iDRAC 라이선스를 이용할 수 있더라도 iDRAC 라이선스 정보가 올바르지 않게 표시됩니다. 따라서 vSphere 호스트 목록에서 호스트를 볼 수는 있지만 상세 정보를 보기 위해 호스트를 클릭하면 **iDRAC 라이선스 유형**의 정보가 빈 것으로 표시되고 **iDRAC 라이선스 설명**이 "라이선스를 업그레이드해야 합니다."로 표시됩니다.

해결 방법: 이 문제를 수정하려면 참조 서버에서 CSIOR을 활성화합니다.

적용 버전: 4.0 이상

Dell 공급자가 상태 업데이트 공급자로 표시되지 않음

OMIVV로 vCenter Server를 등록한 다음에 vCenter 6.0에서 vCenter 6.5로 업그레이드하는 것처럼 vCenter Server 버전을 업그레이드하면 Dell 공급자가 **Proactive HA 공급자** 목록에 표시되지 않습니다.

해결 방법: 비관리자 사용자 또는 관리자 사용자를 위해 등록된 vCenter를 업그레이드할 수 있습니다. vCenter Server의 최신 버전으로 업그레이드하려면 VMware 문서를 참조하여 다음과 같은 옵션 중의 하나를 해당하는 대로 수행합니다.

- 관리자가 아닌 사용자의 경우:
  1. 필요한 경우 관리자가 아닌 사용자에게 추가 권한을 할당합니다. 관리자가 아닌 사용자의 필수 권한 페이지 13을(를) 참조하십시오.
  2. 등록된 OMIVV 어플라이언스를 재부팅합니다.
  3. vSphere Client에서 로그아웃한 후 다시 로그인합니다.
- 관리자 사용자의 경우:
  1. 등록된 OMIVV 어플라이언스를 재부팅합니다.
  2. vSphere Client에서 로그아웃한 후 다시 로그인합니다.

이제 Dell 공급자가 **Proactive HA 공급자** 목록에 나열됩니다.

적용 버전: 4.0 이상

유효하지 않거나 알려지지 않은 iDRAC IP 때문에 호스트 인벤토리 또는 테스트 연결이 실패함

유효하지 않거나 알려지지 않은 iDRAC IP 때문에 호스트 인벤토리나 테스트 연결이 실패하여 "네트워크 지연 또는 접근할 수 없는 호스트", "연결 거부", "작업 시간 초과", "WSMAN", "호스트로 라우팅 없음", "IP 주소: null" 등의 메시지를 받았습니다.

1. iDRAC 가상 콘솔을 엽니다.
2. F2 키를 누르고 **문제 해결 옵션**으로 이동합니다.

3. **문제 해결 옵션**에서 **관리 에이전트 다시 시작**으로 이동합니다.
4. 관리 에이전트를 다시 시작하려면 F11을 누릅니다.

이제 유효한 iDRAC IP를 이용할 수 있습니다.

노트: OMIVV가 ESXi 6.5을 실행하는 호스트에서 WBEM 서비스 활성화에 실패하는 경우 호스트 인벤토리도 실패할 수 있습니다. WBEM 서비스에 관한 자세한 내용은 호스트 자격 증명 프로필 생성 페이지 35를 참조하십시오.

비준수 vSphere 호스트 수정 마법사를 실행할 때 특정 호스트의 상태가 "알 수 없음"으로 표시됨

비준수 호스트를 수정하기 위해 비준수 vSphere 호스트 수정 마법사를 실행할 때 특정 호스트의 상태가 "알 수 없음"으로 표시됩니다. 이 알 수 없음 상태는 iDRAC에 연결할 수 없을 때 표시됩니다.

해결 방법: 호스트의 iDRAC 연결을 확인하고 인벤토리가 올바르게 실행되는지 확인합니다.

적용 버전: 4.0

OMIVV 어플라이언스를 등록하는 동안 할당된 Dell 권한은 OMIVV를 등록 취소한 후에 제거되지 않음

OMIVV 어플라이언스로 vCenter를 등록하고 나면 여러 Dell 권한이 vCenter 권한 목록에 추가됩니다. OMIVV 어플라이언스에서 vCenter의 등록을 취소해도 Dell 권한은 제거되지 않습니다.

노트: Dell 권한은 제거되지 않지만 OMIVV 작업에 미치는 영향은 없습니다.

적용 버전: 3.1 이상

VMCA(VMware Certificate Authority)에 의해 발생한 오류 코드 2000000을 해결하는 방법

vSphere 인증서 관리자를 실행하고 vCenter 서버 또는 플랫폼 서비스 컨트롤러(PSC) 인증서를 vCenter 6.0에 대한 새 CA 인증서 및 키로 교체하면 OMIVV에서 오류 코드 2000000을 표시하고 예외를 발생시킵니다.

해결 방법: 이 예외를 해결하려면 서비스에 대한 ssl 기준 위치를 업데이트해야 합니다. ssl 기준 위치는 PSC에서 `ls_update_certs.py` 스크립트를 실행하여 업데이트할 수 있습니다. 이 스크립트는 기존 인증서 엄지손가락 지문을 입력 인수로 받으며 새 인증서가 설치됩니다. 기존 인증서는 교체 전의 인증서이고 새 인증서는 교체 후의 인증서입니다. 자세한 내용은 https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701 및 https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121689를 참조하십시오.

적용 버전: 3.0 이상, vCenter 6.0 이상

vCenter Windows 설치 시 인증서 바꾸기

자세한 내용은 https://kb.vmware.com/s/article/2121689를 참조하십시오.

vCenter 서버 어플라이언스에서 인증서 바꾸기

자세한 내용은 https://kb.vmware.com/s/article/2121689를 참조하십시오.

MOB(Managed Object Browser)에서 기존 인증서 검색

자세한 내용은 https://kb.vmware.com/s/article/2121701을 참조하십시오.

기존 인증서에서 엄지손가락 지문 추출

자세한 내용은 https://kb.vmware.com/s/article/2121701을 참조하십시오.

관리 콘솔에서 어플라이언스를 출하 시 기본 설정으로 재설정한 이후에도 업데이트 리포지토리 경로가 기본 경로로 설정되지 않음

어플라이언스를 재설정한 후에 **관리 콘솔**로 이동한 다음에 왼쪽 창에 있는 **어플라이언스 관리**를 클릭합니다. **어플라이언스 설정** 페이지에서 **업데이트 리포지토리 경로**가 기본 경로로 변경되지 않습니다.

해결 방법: **관리 콘솔**에서 **기본 업데이트 리포지토리** 필드의 경로를 **업데이트 리포지토리 경로** 필드로 수동으로 복사합니다.

OMIVV에서 DNS 설정을 변경한 후 열린 vCenter HTML-5 클라이언트에 웹 통신 오류가 나타나는 경우 수행할 작업

DNS 설정을 변경한 후 OMIVV 관련 작업을 하는 동안 vCenter HTML-5 클라이언트에서 웹 통신 오류가 나타날 경우 다음 중 하나를 수행하십시오.

- 브라우저 캐시를 지웁니다.
- 로그아웃한 다음 vSphere Client에 로그인합니다.

펌웨어 페이지에서 일부 펌웨어의 설치 날짜가 12-31-1969로 표시됨

vSphere Client에서 호스트에 대한 펌웨어 페이지의 일부 펌웨어 항목에 설치 날짜가 12/31/1969로 표시됩니다. 펌웨어 설치 날짜를 사용할 수 없는 경우에 이전 날짜가 표시됩니다.

해결 방법: 펌웨어 구성 요소에 대해 이 이전 날짜가 표시되는 경우 설치 날짜를 사용할 수 없음을 간주하십시오.

적용 버전: 2.2 이상

vCenter에 플러그인을 성공적으로 등록했지만 HTML-5 클라이언트에 OpenManage Integration 아이콘이 표시되지 않음

vCenter 클라이언트 서비스를 다시 시작하지 않으면 vSphere 클라이언트에 OpenManage Integration 아이콘이 표시되지 않습니다. OpenManage Integration for VMware vCenter 어플라이언스를 등록할 때 vSphere 클라이언트를 사용하여 어플라이언스를 등록합니다. 어플라이언스의 등록을 취소한 다음 같은 버전을 다시 등록하거나 새 버전의 어플라이언스를 등록하면 등록은 되지만 OMIVV 아이콘이 vSphere 클라이언트에 나타나지 않을 수도 있습니다. 이는 VMware의 캐싱 문제로 인해 발생합니다. 이 문제를 해결하려면 vCenter 서버에서 Sphere 클라이언트 서비스를 다시 시작해야 합니다. 그 다음에 플러그인이 UI에 표시됩니다.

해결 방법: vCenter 서버에서 vSphere 클라이언트 서비스를 다시 시작하십시오.

적용 버전: 2.2 이상

어플라이언스 IP 및 DNS 설정을 DHCP 값으로 덮어쓰는 경우, 어플라이언스를 재부팅하고 나면 DNS 구성 설정이 원래 설정으로 복원되는 이유

정적으로 할당된 DNS 설정이 DHCP의 값으로 교체되는 알려진 결함이 있습니다. 이 문제는 DHCP를 사용하여 IP 설정을 구하고 DNS 값을 정적으로 할당할 때 발생할 수 있습니다. DHCP 리스를 갱신하거나 어플라이언스를 다시 시작할 때 정적으로 할당된 DNS 설정이 제거됩니다.

해결 방법: DNS 서버 설정이 DHCP와 다른 경우 IP 설정을 정적으로 할당합니다.

적용 버전: 모든 버전

펌웨어 업데이트를 실행하면 오류 메시지가 표시될 수 있음, 펌웨어 리포지토리 파일이 없거나 유효하지 않음

펌웨어 업데이트 마법사를 실행하는 동안 클러스터 수준에서 **펌웨어 리포지토리 파일이 없거나 유효하지 않습니다**라는 오류 메시지가 표시될 수 있습니다. 이는 리포지토리에서 카탈로그 파일을 다운로드하고 캐싱할 수 없는 일일 백그라운드 프로세스 때문일 수 있습니다. 이 문제는 백그라운드 프로세스가 실행될 때 카탈로그 파일에 연결할 수 없는 경우에 발생합니다.

해결 방법: 카탈로그 연결 문제를 해결한 후 펌웨어 리포지토리 위치를 변경한 다음 원래 위치로 다시 설정하여 백그라운드 프로세스를 다시 시작할 수 있습니다. 백그라운드 프로세스가 완료될 때까지 약 5분 정도 기다립니다. CIFS에 제공된 자격 증명에 @ 문자가 없는지 확인합니다. 또한, 공유 위치에 DUP 파일이 있는지 확인합니다.

적용 버전: 모든 버전

펌웨어 버전 13.5.2로 인텔 네트워크 카드를 업데이트하기 위해 OMIVV를 사용하는 것이 지원되지 않음

펌웨어 버전 13.5.2를 사용하는 일부 인텔 네트워크 카드와 Dell EMC PowerEdge 서버에는 알려진 문제가 있습니다. Lifecycle Controller가 있는 iDRAC를 사용하여 펌웨어 업데이트를 적용할 때 이 버전의 펌웨어로 일부 인텔 네트워크 카드 모델의 업데이트가 실패합니다. 이 버전의 펌웨어를 사용하는 고객은 운영 체제를 사용하여 네트워크 드라이버 소프트웨어를 업데이트해야 합니다. 인텔 네트워크 카드에 13.5.2 이외의 펌웨어 버전이 있는 경우에는 OMIVV를 사용하여 업데이트할 수 있습니다. 자세한 내용은 http://en.community.dell.com/techcenter/b/techcenter/archive/2013/03/20/intel-network-controller-card-with-v13-5-2-firmware-cannot-be-upgraded-using-lifecycle-controller-to-v13-5-6.aspx를 참조하십시오.

노트: 일대다 펌웨어 업데이트를 수행할 때 인텔 네트워크 어댑터의 버전이 13.5.2이면 업데이트가 실패하고 업데이트 작업에서 나머지 서버 업데이트가 중단되기 때문에 이 버전의 인텔 네트워크 어댑터는 선택하지 마십시오.

DUP의 스테이징 요구 사항으로 인해 OMIVV를 사용하여 인텔 네트워크 카드를 14.5 또는 15.0에서 16.x로 업데이트하지 못함

이것은 14.5 및 15.0 NIC에서 알려진 문제입니다. 펌웨어를 16.x로 업데이트하기 전에 사용자 지정 카탈로그를 사용하여 펌웨어를 15.5.0으로 업데이트하도록 합니다.

적용 버전: 모든 버전

관리 포털에서 연결할 수 없는 업데이트 리포지토리 위치를 표시하는 이유

연결할 수 없는 업데이트 리포지토리 경로를 제공하는 경우 어플라이언스 업데이트 보기 상단에 "실패: URL에 연결하는 동안 오류가 발생했습니다" 오류 메시지가 표시됩니다. 하지만 업데이트 리포지토리 경로는 업데이트 전의 값으로 변경되지 않습니다.

해결 방법: 이 페이지에서 다른 페이지로 이동하고 페이지를 새로 고치십시오.

적용 버전: 모든 버전

일대다 펌웨어 업데이트를 수행할 때 시스템이 유지 보수 모드로 시작되지 않는 이유

일부 펌웨어 업데이트에서는 호스트를 재부팅할 필요가 없습니다. 이러한 경우에는 호스트를 유지 관리 모드로 시작하지 않고 펌웨어 업데이트가 수행됩니다.

일부 전원 공급 상태가 치명적인 상태로 변경된 이후에도 섀시의 전체 전원 상태가 양호한 것으로 표시됨

전원 공급 장치에 관한 섀시의 전체 상태는 계속 온라인 상태에 있으면서 작동 중인 PSU가 섀시 전원 요구 사항을 만족하는지 여부와 중복 정책을 바탕으로 합니다. 따라서 PSU 일부가 전원이 꺼진 경우에도 섀시의 전체 전원 요구사항은 만족되는 것입니다. 따라서 섀시의 전체 상태는 양호합니다. 전원 공급 장치 및 전원 관리에 대한 자세한 내용은 Dell EMC PowerEdge M1000e 섀시 관리 컨트롤러 펌웨어 문서의 사용자 가이드를 참조하십시오.

시스템 개요 페이지에서 프로세서 보기의 프로세서 버전이 "해당 없음"으로 표시됨

12세대 이상 서버의 경우 프로세서 버전이 브랜드 열에 있습니다. 이보다 낮은 세대 서버의 프로세서 버전은 **버전** 열에 표시됩니다.

링크된 모드에서 OMIVV의 vCenter 지원 여부

예. OMIVV는 링크된 모드에 있는지 여부와 관계없이 최대 10개의 vCenter 서버를 지원합니다.

OMIVV의 필수 포트 설정

OMIVV에 대한 다음과 같은 포트 설정을 사용하십시오.

표 26. 가상 어플라이언스

포트 번호	프로토콜	포트 유형	최대 암호화 수준	방향	대상	사용	설명
53	DNS	TCP	없음	출력	DNS 서버에 대한 OMIVV 어플라이언스	DNS 클라이언트	DNS 서버에 연결하거나 호스트 이름을 확인합니다.
68	DHCP	UDP	없음	입력	OMIVV 어플라이언스에 대한 DHCP 서버	동적 네트워크 구성	IP, 게이트웨이, 넷마스크 및 DNS와 같은 네트워크 세부 정보를 가져옵니다.
69	TFTP	UDP	128비트	출력	iDRAC에 대한 OMIVV	간이 파일 전송	운영 체제 미설치 서버는 지원되는 최소 펌웨어 버전으로 업데이트하는 데 사용됩니다.
123	NTP	UDP	없음	입력	OMIVV 어플라이언스에 대한 NTP	시간 동기화	특정 시간대와 동기화합니다.
162	SNMP 에이전트	UDP	없음	입력	OMIVV 어플라이언스에 대한 iDRAC, CMC 또는 OME-Modular	SNMP 에이전트(서버)	관리된 노드에서 SNMP 트랩을 수신합니다.
80/443	HTTP/HTTPS	TCP	없음	출력	인터넷에 대한 OMIVV 어플라이언스	Dell 온라인 데이터 액세스	온라인(인터넷) 보증, 펌웨어 및 최신 RPM 정보에 대한 연결을 설정합니다.
443	HTTPS	TCP	128비트	입력	OMIVV 어플라이언스에 대한 OMIVV UI	HTTPS 서버	OMIVV에서 제공하는 웹 서비스입니다. 이러한 웹 서비스는 vSphere Client 및 Dell 관리 포털에서 사용합니다.
443	HTTPS	TCP	128비트	입력	OMIVV 어플라이언스에 대한 ESXi 서버	HTTPS 서버	OMIVV 어플라이언스와 통신하기 위한 사후 설치 스크립트용 운영 체제 구축 흐름에 사용됩니다.
443	HTTPS	TCP	128비트	입력	OMIVV 어플라이언스에 대한 iDRAC	자동 검색	관리된 노드 자동 검색에 사용되는 프로비저닝 서버입니다.
443	WSMAN	TCP	128비트	입력/출력	iDRAC에 대한/로부터의 OMIVV 어플라이언스	iDRAC 통신	관리되는 노드를 관리하고 모니터링하는 데 사용되는 iDRAC, CMC 또는 OME-Modular 통신입니다.
445/139	SMB	TCP	128비트	출력	CIFS에 대한 OMIVV 어플라이언스	CIFS 통신	Windows 공유와 통신합니다.
2049/111	NFS	UDP/TCP	없음	입력/출력	NFS에 대한 OMIVV 어플라이언스	공개 공유	NFS 공개 공유는 OMIVV 어플라이언스에 의해 관리된 노드에 노출되었으며 펌웨어 업데이트 및 운영 체제 구축 흐름에 사용됩니다.
4001~4004	NFS	UDP/TCP	없음	입력/출력	NFS에 대한 OMIVV 어플라이언스	공개 공유	NFS 서버의 V2 및 V3 프로토콜에서 statd, quotd, lockd 및 mountd 서비스를 실행하려면 이러한 포트를 열린 상태로 유지해야 합니다.

표 26. 가상 어플라이언스 (계속)

포트 번호	프로토콜	포트 유형	최대 암호화 수준	방향	대상	사용	설명
사용자 정의	모든	UDP/TCP	없음	출력	프록시 서버에 대한 OMIVV 어플라이언스	프록시	프록시 서버와 통신합니다.

표 27. 관리된 노드(ESXi)

포트 번호	프로토콜	포트 유형	최대 암호화 수준	방향	대상	사용	설명
162	SNMP	UDP	없음	출력	OMIVV 어플라이언스에 대한 ESXi	하드웨어 이벤트	ESXi에서 보낸 비동기 SNMP 트랩입니다. 이 포트는 ESXi에서 열어야 합니다.
443	WSMAN	TCP	128비트	입력	ESXi에 대한 OMIVV 어플라이언스	iDRAC 통신	관리 스테이션에 정보를 제공하는 데 사용됩니다. 이 포트는 ESXi에서 열어야 합니다.
443	HTTPS	TCP	128비트	입력	ESXi에 대한 OMIVV 어플라이언스	HTTPS 서버	관리 스테이션에 정보를 제공하는 데 사용됩니다. 이 포트는 ESXi에서 열어야 합니다.

iDRAC 및 CMC 포트 정보에 대한 자세한 내용은 **https://www.dell.com/support**에서 제공되는 *Integrated Dell Remote Access Controller 사용자 가이드* 및 *Dell Chassis Management Controller 사용자 가이드*를 참조하십시오.

OME-Modular 포트 정보에 대한 자세한 내용은 **https://www.dell.com/support**에서 제공되는 *Dell EMC OME-Modular 사용자 가이드*를 참조하십시오.

노트: iDRAC9 기반 서버의 경우 iDRAC는 포트 2049에서 TCP를 통해 NFS를 마운트합니다. iDRAC9 기반 서버 목록은 호환성 매트릭스를 참조하십시오.

iDRAC 사용자 목록에서 새로 변경한 자격 증명을 가진 동일한 사용자가 있는 시스템 프로필을 성공적으로 적용한 후에 운영 체제 미설치 검색에 사용되는 사용자에 대한 암호가 변경되지 않음

시스템 프로필(하드웨어 구성)만 배포하도록 선택한 경우 탐색에 사용되는 사용자 암호는 새 자격 증명으로 변경되지 않습니다. 이는 향후 배포가 필요할 때 사용하기 위해 플러그인이 iDRAC과 통신할 수 있도록 의도적으로 그렇게 수행됩니다.

vCenter 호스트 및 클러스터 페이지에 나열된 새 iDRAC 버전 세부 정보를 볼 수 없음

해결 방법: vSphere 웹 클라이언트에서 펌웨어 업데이트 작업을 완료한 후에 **펌웨어 업데이트** 페이지를 새로 고칩니다. 페이지에 기존 버전이 표시되는 경우에는 OpenManage Integration for VMware vCenter의 **호스트 준수** 페이지로 이동하여 해당 호스트의 CSIOR 상태를 확인합니다. CSIOR이 활성화되어 있지 않으면 CSIOR을 활성화하고 호스트를 재부팅합니다. CSIOR이 이미 활성화되어 있으면 iDRAC 콘솔에 로그인하고 iDRAC를 재설정하고, 몇 분 정도 기다린 후에 **펌웨어 업데이트** 페이지를 새로 고칩니다.

잠금 모드가 활성화된 상태에서 OMIVV의 ESXi 지원 여부

예. ESXi 6.0 이상인 호스트의 이 릴리즈에서 잠금 모드가 지원됩니다.

잠금 모드 사용을 시도하였지만 실패함

잠금 모드에서 호스트 자격 증명 프로필에 호스트를 추가하면 인벤토리가 시작되지만 "원격 액세스 컨트롤러를 찾을 수 없거나 이 호스트에서 인벤토리가 지원되지 않습니다."라는 메시지와 함께 실패합니다.

호스트를 잠금 모드에 배치하거나 잠금 모드에서 호스트를 제거하는 경우 30분을 기다린 후에 OMIVV에서 다음 작업을 수행해야 합니다.

서버에서 ESXi 배포 시도가 실패함

1. **ISO 위치(NFS 경로)** 및 준비 **폴더 경로**가 정확한지 확인합니다.
2. 서버 ID를 할당하는 동안 선택된 **NIC**가 가상 어플라이언스에서 액세스할 수 있는지 확인합니다.
3. OMIVV에 대한 네트워크 연결을 기반으로 관리 NIC를 선택해야 합니다.
4. **고정 IP 주소**를 사용하는 경우, 제공된 네트워크 정보(서브넷 마스크 및 기본 게이트웨이 포함)가 정확한지 확인합니다. 또한, IP 주소가 이미 네트워크에 할당되지 않았는지 확인합니다.
5. 최소 한 개의 가상 디스크, IDSDM 또는 BOSS가 시스템에서 확인되는지 확인합니다.

자동 검색된 시스템이 배포 마법사에 모델 정보 없이 표시됨

이것은 대개 시스템에 설치된 펌웨어 버전이 권장 최소 요구 사항을 만족하지 못한다는 것을 나타냅니다. 펌웨어 업데이트가 시스템에 등록되지 않았을 수도 있습니다.

해결 방법: 시스템을 콜드 부팅하거나 블레이드를 다시 장착하면 문제가 해결됩니다. 모델 정보 및 NIC 정보를 OMIVV로 제공하기 위해서는 iDRAC의 새로 활성화된 계정을 비활성화하고 자동 검색을 다시 시작해야 합니다.

NFS 공유가 ESXi ISO와 함께 설치되었지만 공유 위치 마운트 오류로 인해 배포에 실패함

해결 방법을 찾으려면 다음을 수행하십시오.

1. iDRAC가 어플라이언스에 대한 Ping을 수행할 수 있는지 확인합니다.
2. 네트워크 실행 속도가 너무 느리지 않은지 확인합니다.
3. 2049, 4001-4004 포트가 열려 있고 그에 따라 방화벽이 설정되어 있는지 확인합니다.

vCenter에서 OMIVV 어플라이언스를 강제로 제거하는 방법

1. vSphere Client로 이동하여 모든 Proactive HA 활성화 클러스터의 Dell 공급자에 대한 확인란을 선택 취소합니다.
2. **https://<vcenter_serverIPAddress>/mob**로 이동합니다.
3. VMware vCenter 관리자 자격 증명을 입력합니다.
4. **홈** > **콘텐츠** > **HealthUpdateManager**를 클릭합니다.
5. **Queryproviderlist** > **메서드 호출**을 클릭합니다.
6. 공급자 ID 문자열 값을 복사하고 창을 닫습니다.
7. **UnregisterHealthUpdateProvider**를 클릭하고 복사된 제공자 ID 문자열 값을 입력합니다.
8. **메서드 호출**을 클릭합니다.
9. **홈** > **콘텐츠**로 이동합니다.
10. **ExtensionManager**를 클릭합니다.
11. **UnregisterExtension**을 클릭합니다.
12. 확장 키를 입력하여 com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient의 등록을 취소하고 **메서드 호출**을 클릭합니다.
13. vSphere Client에서 OMIVV의 전원을 끄고 삭제합니다. 등록을 취소하는 키가 vSphere Client용이어야 합니다.
14. vCenter에서 serenity 항목을 지우고 vCenter 서비스를 재시작합니다.

지금 백업 화면에 암호를 입력하면 오류 메시지 표시

저해상도 모니터를 사용하는 경우에는 지금 백업 창에 암호화 암호 필드가 표시되지 않습니다. 암호화 암호를 입력하려면 페이지를 아래로 스크롤합니다.

펌웨어 업데이트 실패 시 수행할 작업

OMIVV 어플라이언스 로그에서 작업 시간이 초과되었는지 확인합니다. 그렇다면 콜드 재부팅을 수행하여 iDRAC를 재설정해야 합니다. 시스템이 시작되어 실행된 후에는 인벤토리를 실행하거나 **펌웨어** 탭을 사용하여 업데이트에 성공했는지 확인합니다.

vCenter 등록 실패 시 수행할 작업

통신 문제로 인해 vCenter 등록에 실패할 수 있습니다. 이러한 문제가 발생하면 정적 IP 주소를 사용하여 해결할 수 있습니다. 정적 IP 주소를 사용하려면 OpenManage Integration for VMware vCenter의 콘솔 탭에서 **네트워크 구성** > **디바이스 편집**을 선택하고 올바른 **게이트웨이** 및 **FQDN**(정규화된 도메인 이름)을 입력합니다. DNS 구성 편집 아래에 DNS 서버 이름을 입력합니다.

노트: 가상 어플라이언스에서 입력한 DNS 서버를 확인할 수 있는지 확인하십시오.

호스트 자격 증명 프로필 테스트 자격 증명의 수행 속도가 느리거나 응답하지 않음

서버의 iDRAC에 사용자가 하나만 있거나(예: *루트*) 사용자가 비활성화 상태에 있거나 모든 사용자가 비활성화 상태에 있습니다. 비활성화 상태에 있는 서버에 통신을 하면 지연이 발생합니다. 이 문제를 해결하려면 서버의 비활성화 상태를 수정하거나 서버의 iDRAC를 기본 설정으로 재설정하여 루트 사용자를 다시 활성화하면 됩니다.

비활성 상태의 서버를 수정하려면 다음을 수행하십시오.

1. Chassis Management Controller(섀시 관리 컨트롤러) 콘솔을 열고 비활성화된 서버를 선택합니다.
2. iDRAC 콘솔을 자동으로 열려면 **iDRAC GUI 시작**을 클릭합니다.
3. iDRAC 콘솔에서 사용자 목록을 탐색하고 다음 중 하나를 클릭합니다.
   - iDRAC7: **iDRAC 설정** > **사용자 탭**을 선택합니다.
   - iDRAC8: **iDRAC 설정** > **사용자 탭**을 선택합니다.
   - iDRAC9: **iDRAC 설정** > **사용자 탭**을 선택합니다.

   iDRAC 7 및 8의 경우:

   a. 설정을 편집하려면 사용자 ID 열에서 관리(루트) 사용자에 대한 링크를 클릭합니다.
   b. **사용자 구성**을 클릭하고 **다음**을 클릭합니다.
   c. 선택한 사용자의 **사용자 구성** 페이지에서 사용자 활성화 옆에 있는 확인란을 선택하고 **적용**을 클릭합니다.

   iDRAC 9의 경우:

   a. **루트**를 선택하고 **사용**을 클릭합니다.

OMIVV의 VMware vCenter 서버 어플라이언스 지원 여부

예. OMIVV는 v2.1 이후로 VMware vCenter 서버 어플라이언스를 지원합니다.

서버가 CSIOR 상태 "알 수 없음"과 호환되지 않는 것으로 표시될 수 있음

해결 방법: 알 수 없는 CSIOR 상태는 호스트의 응답하지 않는 iDRAC를 나타냅니다. 호스트의 수동 iDRAC 재설정으로 이 문제가 해결됩니다.

적용 버전: 모든 버전

다음 재부팅 시 적용 옵션을 사용하여 펌웨어 업데이트를 수행했고 시스템을 다시 부팅했지만 펌웨어 레벨이 업데이트되지 않음

펌웨어를 업데이트하려면 재부팅이 완료된 후에 호스트에서 인벤토리를 실행합니다. 경우에 따라 재부팅 이벤트가 어플라이언스에 도달하지 않으면 인벤토리가 자동으로 트리거되지 않습니다. 이러한 상황에서 업데이트된 펌웨어 버전을 구하려면 인벤토리를 수동으로 다시 실행해야 합니다.

VCenter 트리에서 호스트를 제거한 후에도 섀시 아래에 호스트가 여전히 표시됨

섀시 아래의 호스트는 섀시 인벤토리의 일부로 식별됩니다. 섀시 인벤토리에 성공하면 섀시 아래의 호스트 목록이 업데이트됩니다. 호스트가 vCenter 트리에서 제거되는 경우에도 호스트가 다음 섀시 인벤토리가 실행될 때까지는 섀시 아래에 표시됩니다.

OMIVV의 백업 및 복원 후에 알람 설정이 복원되지 않음

OMIVV 어플라이언스 백업을 복원해도 모든 알람 설정이 복원되지는 않습니다. 그러나 OpenManage Integration for VMware GUI에서 **알람 및 이벤트** 필드에는 복원된 설정이 표시됩니다.

해결 방법: OMIVV GUI의 **설정** 탭에서 **이벤트 및 알람** 설정을 수동으로 변경합니다.

NPAR이 대상 노드에서 활성화되고 시스템 프로필에서 비활성화되어 있을 때 OS 배포가 실패함

대상 시스템에 NPAR(NIC Partitioning)이 비활성화된 시스템 프로필이 적용될 때 OS 배포가 실패합니다. 여기에서 대상 노드에서 NPAR이 활성화되고 배포 마법사를 통해 배포 프로세스를 수행하는 동안 관리 작업을 위해 파티션 1을 제외하고 파티셔닝된 NIC 중 하나만 NIC로 선택됩니다.

해결 방법: 배포 중 시스템 프로필을 통해 NPAR 상태를 변경하는 경우 배포 마법사에서 관리 네트워크에 대한 첫 번째 파티션만 선택했는지 확인합니다.

적용 버전: 4.1 이상

사용 가능한 버전이 현재 버전보다 낮을 경우 사용할 수 있는 OMIVV 어플라이언스 버전이 잘못된 정보를 표시함

어플라이언스 관리의 OMIVV 관리 콘솔에서 **사용 가능한 가상 어플라이언스 버전**은 RPM 및 OVF 모드를 표시합니다.

노트: 업데이트 리포지토리 경로를 최신 버전으로 설정하고 가상 어플라이언스 버전 다운그레이드는 지원하지 않는 것이 좋습니다.

12세대 이상 운영 체제 미설치 서버를 추가하는 동안 267027 예외가 발생

베어 메탈 검색 도중 잘못된 자격 증명을 입력하면 사용자 계정이 몇 분 동안 자동으로 잠깁니다. 이 기간 동안 iDRAC는 응답하지 않게 되고 정상적인 상태로 복원되는 데 몇 분이 소요됩니다.

해결 방법: 잠시 기다린 후 사용자 자격 증명을 다시 입력합니다.

배포 도중 iDRAC 오류로 인해 시스템 프로필을 적용하지 못함

배포 도중 OMIVV는 iDRAC에서 구성 업데이트 작업을 생성하려고 시도합니다. 그러나 경우에 따라 작업 생성이 실패하고 구성 작업이 이미 생성되었음을 나타내는 메시지가 표시됩니다.

해결 방법: 상태 항목을 지우고 배포를 다시 시도합니다. 작업을 지우려면 iDRAC에 로그인합니다.

프록시가 도메인 사용자 인증으로 구성될 때 OMIVV RPM 업그레이드가 실패함

OMIVV 어플라이언스가 인터넷 연결을 위해 프록시로 구성되고 프록시는 NTLM 인증을 사용하여 인증된 경우, 기본 yum 도구의 문제로 인해 RPM 업데이트가 실패합니다.

적용 버전: OMIVV 4.0 이상

해결 방법: 백업 후 복원하여 OMIVV를 업데이트합니다.

FX 섀시에서 PCIe 카드가 있는 시스템 프로필을 적용할 수 없음

FX 섀시를 사용할 때 소스 서버에 PCIe 카드 정보가 있으면 대상 서버에 OS를 배포하지 못합니다 소스 서버의 시스템 프로필에는 대상 서버와는 다른 `fc.chassislot ID`가 있습니다. OMIVV가 대상 서버에 동일한 `fc.chassislot ID`를 배포하려고 했지만 실패했습니다. 시스템 프로필은 랙 서버(동일함)에서 성공적으로 작동하지만 모듈 서버에서는 제한사항이 거의 없는 프로필을 적용하는 동안 정확한 인스턴스(FQDD)를 검색합니다. 예를 들어 FC640의 경우, 한 모듈형 서버에서 생성된 시스템 프로필은 NIC 레벨 제한사항으로 인해 동일한 FX 섀시에 있는 다른 모듈 서버에는 적용할 수 없습니다.

적용 버전: 4.1 이상

해결 방법: FX2s 섀시의 슬롯1에 있는 FC640 서버의 시스템 프로필은 다른 FX2s 섀시의 슬롯 1에 상주하는 또 다른 FC640 서버에만 적용할 수 있습니다.

변경 사항 감지 기능은 FX 섀시에서 PCIe 카드가 있는 모듈 서버와 호환되지 않음을 표시함

시스템 프로필은 랙 서버(동일함)에서 성공적으로 작동하지만 모듈 서버에서는 제한사항이 거의 없는 기준선과 비교하는 경우 정확한 인스턴스(FQDD)를 검색합니다. 예를 들어 FC640의 경우 한 모듈 서버에서 생성된 시스템 프로필(기준선)은 FQDD와의 불일치로 인해 동일한 FX 섀시에 있는 다른 모듈 서버와 차이를 보입니다.

적용 버전: 4.1 이상

해결 방법: 시스템 프로필을 만드는 동안 다른 서버와 공용이 아닌 FQDD를 지웁니다.

iDRAC이 선택된 NIC의 MAC 주소를 채우지 못하는 경우 PowerEdge 서버에서 OS를 구축할 수 없음

iDRAC이 선택된 NIC 포트의 MAC 주소를 채우지 못하는 경우 PowerEdge 서버에서 OS를 구축할 수 없습니다.

해결 방법: 각 NIC 펌웨어와 iDRAC 펌웨어를 최신 버전으로 업데이트하고 MAC 주소가 NIC 포트에 채워졌는지 확인합니다.

적용 버전: 4.3 이상

ESXi 6.5U1을 사용하는 호스트에 대한 호스트 자격 증명 프로필을 생성하는 경우 호스트의 서비스 태그가 호스트 선택 페이지에 표시되지 않음

OMIVV가 ESXi의 서비스 태그에 대해 vCenter에 쿼리할 때 vCenter는 서비스 태그 값이 null이므로 서비스 태그를 반환할 수 없습니다.

해결 방법: ESXi 버전을 ESXi 6.5U2 또는 ESXi 6.7 U1로 업데이트합니다.

적용 버전: 4.3 이상

이전 OMIVV 버전에서 나중에 나온 OMIVV 버전으로 백업 및 복원을 수행한 후에 Dell EMC 아이콘이 표시되지 않음

이전 OMIVV 버전에서 나중에 나온 OMIVV 버전으로 백업 및 복원을 수행한 후에 다음과 같은 문제가 관찰됩니다.

- vCenter에서 Dell EMC 로고가 표시되지 않습니다.
- 2000000 오류
- 3001 오류

  해상도:

  - vCenter Server에서 vSphere Client를 재시작합니다.
  - 문제가 지속되면, 다음과 같이 하십시오.
    - VMware vCenter Server 어플라이언스의 경우 `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity`로 이동하고, Windows vCenter의 경우 vCenter 어플라이언스의 `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity` 폴더로 이동해

com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX와 같은 이전 데이터가 존재하는지 확인합니다.

- 이전 OMIVV 버전에 해당하는 폴더를 수동으로 지웁니다.

펌웨어 업데이트에 성공한 경우에도 OMIVV를 사용하여 일부 iDRAC 펌웨어 버전을 업그레이드하거나 다운그레이드하는 경우 OMIVV가 작업에 실패했음을 나타낼 수 있음

펌웨어 업데이트 중에 3.20.20.20, 3.21.21.21 및 3.21.21.22와 같은 iDRAC 버전을 다운그레이드하거나 업그레이드할 때 작업이 성공적으로 실행된 경우에도 작업 상태가 실패로 표시됩니다.

해결 방법: 작업 실패 후 인벤토리를 새로 고치고 다른 구성 요소에 대한 작업을 다시 실행합니다.

적용 버전: 4.3

클러스터 레벨에서 시스템 잠금 모드를 구성하면 "클러스터의 어느 호스트에도 성공한 인벤토리가 없습니다"라는 메시지가 표시됨

클러스터 레벨에서 시스템 잠금 모드를 구성하면 "클러스터의 어느 호스트에도 성공한 인벤토리가 없습니다"라는 메시지가 표시됩니다. 이 메시지는 클러스터의 OMIVV에서 관리되는 iDRAC9 기반 서버를 성공적으로 인벤토리한 경우에도 표시됩니다. iDRAC9 기반 서버 목록은 호환성 매트릭스를 참조하십시오.

해결 방법: vCenter를 재부팅합니다.

vCenter를 재부팅하려면 다음을 수행하십시오.

1. vCenter SSO(Single Sign On) 관리자 계정을 사용하여 vSphere Client에 로그인합니다.
2. **관리** > **배포** > **배포** > **시스템 구성**으로 이동합니다.
3. **노드**를 클릭하고 vCenter Server 어플라이언스 노드를 선택한 다음 **관련 개체** 탭을 클릭합니다.
4. vCenter 노드를 다시 부팅합니다.

OMIVV 어플라이언스의 RPM 업그레이드 후, 로그에 여러 항목이 vCenter 최근 작업으로 표시될 때가 있음

RPM 업그레이드 후, vCenter 최근 작업에서 볼 때 로그에 여러 항목이 표시되는 경우가 있습니다.

해결 방법: vCenter 서비스를 다시 시작합니다.

적용 버전: 4.3

vCenter 등록 후 OMIVV의 Dell EMC 로고가 VMware의 홈 페이지에 표시되지 않음

설명: 등록 완료 직후에 VMware vCenter가 플러그인을 검증하므로 OMIVV의 Dell EMC 로고가 VMware의 **홈** 페이지에 표시되지 않을 수 있습니다.

해결 방법: 다음 단계를 수행합니다.

1. 브라우저를 새로 고치거나, 브라우저 캐시를 지우거나, vSphere Client용 Client Services(HTML-5)를 다시 시작합니다.
2. vSphere Client에서 로그아웃한 후 다시 로그인합니다.

적용 버전: 5.0

비준수 11G PowerEdge 서버가 백업 및 복원 후 OMIVV 인벤토리에 보관됨

OMIVV에서 백업 및 복원 작업을 수행한 후에도 비준수 및 인벤토리 작성되지 않은 11G 호스트가 호스트 자격 증명 프로필에 계속 연결되어 있습니다. 그러나 구성 준수를 수정하고 새 인벤토리를 실행하려고 하면 지원되지 않는 11G 서버에서 작업이 실패합니다.

해결 방법: 11G 서버는 OMIVV 5.0에서 지원되지 않습니다. 호스트 자격 증명 프로필에서 지원되지 않는 11G 호스트를 수동으로 제거합니다.

적용 버전: 5.0

OMIVV 어플라이언스를 업그레이드한 후 Flex 클라이언트에서 vCenter를 시작할 수 없음

해결 방법: VMware 기술 문서(https://kb.vmware.com/s/article/54751)를 참조하십시오.

적용 버전: 5.0

OMIVV에 네트워크 어댑터를 추가하거나 제거하면 OMIVV 콘솔에서 기존 NIC가 사라집니다.

때때로 vSphere Client를 사용하여 OMIVV 어플라이언스에 네트워크 어댑터를 추가하거나 제거하면 OMIVV 콘솔에서 기존 NIC가 사라집니다.

해결 방법: 다음 작업 중 하나를 수행합니다.

1. a. 터미널 콘솔 유틸리티에서 모든 작업 어댑터 분리
   b. 어플라이언스 종료
   c. 어플라이언스에서 네트워크 어댑터 분리
   d. OMIVV 어플라이언스 재부팅
   e. 어플라이언스 종료
   f. 필요한 네트워크 어댑터 추가 및 네트워크 어댑터 구성 완료
   g. 어플라이언스 재부팅
2. a. 관리 포털에서 OMIVV 백업
   b. 새 OMIVV 어플라이언스 생성
   c. 어플라이언스 종료
   d. 필요한 네트워크 어댑터 추가 및 네트워크 어댑터 구성 완료
   e. 어플라이언스 재부팅
   f. 최신 백업 데이터 복원

적용 버전: OMIVV 5.0

두 번째 NIC를 추가 또는 제거하면 네트워크 구성 페이지에 세 개의 NIC가 표시됨

vSphere 클라이언트를 사용하여 OMIVV 어플라이언스에서 NIC를 추가하거나 제거한 후 OMIVV 어플라이언스를 부팅하고 OMIVV 터미널 콘솔에 로그인하면 때때로 **네트워크 구성** 페이지에 일치하지 않는 NIC 수가 표시됩니다.

해결 방법: MAC 주소를 사용하여 올바른 NIC를 비교 및 구성하고 **–** 버튼을 사용하여 추가 NIC를 제거합니다.

적용 버전: 5.0

최신 OMIVV 버전으로 백업 및 복원한 후 이전 버전에서 알 수 없는 상태인 서버가 운영 체제 미설치 서버 페이지에 나열되지 않음

이전 버전에서 백업을 복원한 후 지원되지 않는 서버(11G 이전)가 베어 메탈 인벤토리에서 제거됩니다. 이전 버전에서 백업 전에 세대를 확인하지 않은 서버도 제거됩니다.

해결 방법: 서버를 다시 검색합니다. 누락된 서버가 지원되는 경우 운영 체제 미설치 인벤토리에 표시됩니다.

적용 버전: 5.0

OS 배포 후 OMIVV가 ESXi 호스트를 vCenter에 추가하지 못했거나 호스트 프로필을 추가하지 못했거나 호스트에 대한 유지 관리 모드 시작이 실패함

OS 배포 후 OMIVV는 vCenter에 호스트 작업(호스트 추가, 호스트 프로필 추가 또는 유지 관리 모드 시작)을 수행하도록 쿼리합니다. 쿼리가 2분 내에 응답을 받지 못하면 vCenter에 대한 특정 작업이 시간 초과되고 통신 실패를 나타내는 메시지가 작업 내역에 표시됩니다. 하지만 vCenter 쿼리 작업이 성공할 때도 있습니다.

해결 방법: 작업 내역에서 호스트 IP를 가져와 수동으로 추가합니다.

iDRAC IP에 연결할 수 없는 경우 iDRAC 라이선스 상태가 관리 규정 준수 페이지에 준수로 표시됨

주기적으로 인벤토리를 수행한 후 iDRAC에 연결할 수 없는 경우 iDRAC 라이선스 상태가 관리 규정 준수 페이지에 준수로 표시됩니다.

해결 방법: iDRAC에 연결할 수 있는지 확인하고 인벤토리를 다시 실행하여 올바른 iDRAC 라이선스 상세 정보를 가져옵니다.

OMIVV를 사용하여 OS를 성공적으로 배포한 후 ESXi 호스트의 연결이 끊어지거나 응답이 없음

vCenter의 FQDN을 조회하도록 DNS가 올바르게 구성되지 않아 ESXi 호스트가 vCenter로 하트비트 패킷을 전송하지 못합니다.

해결 방법: 다음 작업을 수행합니다.

1. ESXi 호스트를 vCenter 인벤토리에서 제거합니다.
2. **호스트 추가** 마법사를 사용하여 vCenter에 호스트를 추가합니다.
3. 호스트 자격 증명 프로필을 생성하고 인벤토리를 실행합니다.

OMIVV의 NIC(Network Interface Card)가 ESXi 호스트 네트워크에 연결되지 않은 경우 배포 작업 시간이 초과됨

OS 배포는 NIC 선택에 종속되어 있습니다. 올바른 NIC가 선택되지 않은 경우 OSD 작업 시간이 초과됩니다.

해결 방법: 배포 마법사의 호스트 설정 구성 페이지에서 해당되는 '호스트에 연결된 어플라이언스 NIC'를 선택합니다. 이는 OS 설치 프로세스 중에 OMIVV가 ESXi 네트워크에 연결하는 데 필요합니다.

보증 작업이 특정 호스트에 대해 실행되지 않음

여러 vCenter가 있는 PSC 환경에서 FQDN을 사용하여 하나의 vCenter에 호스트를 추가하고 다른 vCenter에 IP를 추가하면 하나의 호스트 인스턴스에 대해서만 보증 작업이 실행됩니다.

해결 방법: 호스트 자격 증명 프로필에서 연결 해제된 호스트 인스턴스를 제거하고 인벤토리 및 보증 작업을 실행합니다.

적용 버전: 5.0

백업 및 복원 수행 후 Proactive HA 초기화가 수행되지 않음

vSphere 클라이언트를 사용하여 등록한 이전 버전에서 OMIVV를 복원하면 Proactive HA 사용 가능 클러스터의 경우 Dell 제공업체의 연결이 끊어집니다.

해결 방법: 클러스터에 대해 Proactive HA를 비활성화하고 활성화합니다.

적용 버전: 5.0

OMIVV 페이지에 유효하지 않은 세션, 시간 초과 예외 또는 Firefox 브라우저에 2백만 개의 오류가 표시됨

OMIVV 페이지가 일정 시간(5~10분) 동안 유휴 상태이거나, 유효하지 않은 세션 또는 시간 초과 예외 또는 2백만 개의 오류가 표시되는 경우

해결 방법: 브라우저를 새로 고칩니다. 문제가 지속되면 `vCenter`에서 로그아웃한 다음 로그인하십시오.

OMIVV에서 올바른 데이터를 보려면 해결 방법에 나열된 작업을 완료했는지 확인합니다.

적용 버전: 5.0

vCenter에서 최근 작업 창에 일부 OMIVV 작업 알림에 대한 세부 정보 열이 표시되지 않음

해결 방법: 작업 알림을 보려면 vCenter에서 vCenter의 **작업 콘솔**로 이동합니다.

적용 버전: 5.0

vCenter 6.5 U2를 사용하는 경우 모든 OMIVV 페이지에 2000002 오류가 표시될 수 있음

해결 방법: 6.5 U2의 경우 VMware의 최신 패치를 사용하거나 6.5 U3 이상 버전으로 마이그레이션합니다.

적용 버전: 5.1

RPM 업그레이드 또는 백업을 수행하고 이전 OMIVV 버전에서 최신 OMIVV 버전으로 복원하면 모든 OMIVV 페이지에 2000002 오류가 표시됨

현재 버전을 등록하기 전에 vCenter 서버에 이전 버전의 OMIVV가 있는 경우 SSL 핸드셰이크 예외로 인해 vCenter에서 새 플러그인 데이터를 새로 고침할 때까지 OMIVV가 새 버전으로 업그레이드되지 않습니다. vCenter에는 SSL 트래픽을 다르게 처리하는 이전 버전의 OMIVV의 데이터가 포함되어 있기 때문입니다.

해상도:

- vCenter 서버에서 vSphere Client를 재시작합니다.
- 문제가 지속되면, 다음과 같이 하십시오.
  - VMware vCenter 서버 어플라이언스의 경우 `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity`로 이동하고, Windows vCenter의 경우 vCenter 어플라이언스의 `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity` 폴더로 이동해 com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX와 같은 이전 데이터가 존재하는지 확인합니다.
  - 이전 OMIVV 버전에 해당하는 폴더를 수동으로 지웁니다.
  - vSphere Client용 vSphere Client 서비스 재시작(HTML5)

적용 버전: 5.0 이상

OMIVV에서 vCenter 등록 취소를 완료하는 데 시간이 오래 걸리는 경우가 있음

호스트 수가 많은(300개 이상) vCenter의 등록을 취소하면 OMIVV가 오랫동안 로드 상태로 유지됩니다.

해결 방법: 브라우저를 새로 고칩니다.

vCenter 등록 취소에 실패한 경우 vCenter를 다시 등록 취소합니다.

적용 버전: 5.1

OMIVV 인증서를 업데이트한 후 "OMIVV 어플라이언스를 연결하지 못했습니다. SSL 인증서가 유효하지 않습니다." 오류 메시지가 표시됨

해결 방법: vCenter 클라이언트 서비스를 재시작합니다.

적용 버전: 모든 버전

OMIVV의 배포 작업 실패

Lifecycle Controller가 보류 중이거나 다른 작업을 실행 중이기 때문에 배포 작업이 실패합니다.

해결 방법: 다음 단계를 수행합니다.

1. iDRAC에서 iDRAC 작업 대기열 지우기[선택 사항]
2. iDRAC 재설정
3. 배포 작업 다시 실행

적용 버전: 모든 버전

vCenter 암호를 변경한 후 OMIVV에서 연결 테스트 및 인벤토리가 작동하지 않음

ESXi 버전 6.7 이상의 경우 OMIVV는 IPMI(Intelligent Platform Management Interface) 프로토콜을 사용하여 ESXi 호스트의 iDRAC IP를 검색하며 이 작업은 WBEM에 종속되지 않습니다.

OMIVV가 어떤 이유로든 iDRAC IP를 검색하지 못할 경우 OMIVV는 WBEM 상태에 따라 달라지는 CIM(Common Information Model) 프로토콜(폴백)을 시도합니다. 등록에 사용되는 vCenter 사용자의 암호가 변경된 경우, 테스트 연결 및 인벤토리를 실행하는 동안 WBEM 관련 이슈가 발생할 수 있습니다.

해결 방법: vCenter 암호를 변경한 후 vCenter에서 작업을 수행하기 전에 OMIVV 관리 콘솔에서 vCenter 자격 증명을 수정합니다. 자격 증명 수정에 대한 자세한 내용은 vCenter 로그인 자격 증명 수정 페이지 15을(를) 참조하십시오.

적용 버전: 모든 버전

OMIVV 어플라이언스를 출고 시 설정으로 재설정한 후 OMIVV 인스턴스가 vCenter에서 제거되지 않음

이 문제는 어플라이언스를 출고 시 설정으로 재설정할 때 발생합니다. OMIVV 어플라이언스 항목은 vCenter의 `vsphere-client-serenity` 폴더에 남아 있어 출고 시 설정으로 재설정한 후 vCenter 등록을 방지합니다.

해결 방법: vCenter에서 OMIVV 항목을 제거합니다. 자세한 내용은 vCenter에서 OMIVV 어플라이언스를 강제로 제거하는 방법 페이지 144을(를) 참조하십시오.

적용 버전: 모든 버전

OMIVV가 시스템 프로필의 프로필 설정 페이지에 BIOS 및 iDRAC 특성만 표시

해결 방법: Google Chrome을 최신 버전으로 업그레이드합니다.

적용 버전: 5.2

알 수 없는 오류로 OS 배포가 완료됨

이 이슈는 서버를 검색했던 사용자 이외의 다른 사용자로 OS 배포를 수행할 때 발생합니다. OMIVV **로그** 페이지의 오류 메시지에 클래스를 찾을 수 없음 오류가 표시됩니다.

해결 방법: 해당 없음, 이 이슈는 OMIVV 기능에 영향을 미치지 않습니다.

적용 버전: 5.2

FX2 섀시에서 CMC(Chassis Management Controller) 펌웨어 업데이트 오류

OMIVV를 사용하면 서버 iDRAC을 통해 FX2 섀시 CMC 펌웨어를 업데이트할 수 있습니다. **OS 및 Lifecycle Controller를 통한 CMC 업데이트 허용** 옵션이 iDRAC에서 비활성화되어 있는 경우 CMC 펌웨어 업데이트에 오류가 발생합니다.

해결 방법: iDRAC에서 다음을 수행합니다.

1. **설정** > **업데이트 및 롤백**으로 이동합니다.
2. **OS 및 Lifecycle Controller를 통한 CMC 업데이트 허용**을 **활성화됨**으로 설정합니다.

적용 버전: 5.2

OMIVV에서 ISO 프로필 배포 오류

이전 버전의 OMIVV로 예약된 ISO 프로필 배포 작업이 최신 버전의 OMIVV에서 유효하지 않습니다.

해결 방법: 예약된 작업을 취소하고 필요에 따라 배포 작업을 만듭니다.

예약된 작업이 취소되지 않으면 배포 작업에 오류가 발생합니다. 이러한 경우 서버를 운영 체제 미설치로 검색하고 ISO 프로필 배포 작업을 만듭니다.

적용 버전: 5.2

베어 메탈 배포 문제

이 섹션에서는 배포 프로세스 중에 발견된 문제에 대해 다룹니다.

자동 검색 및 핸드쉐이크 사전 요구 사항

- 자동 검색 및 핸드셰이크를 실행하기 전에 iDRAC 및 Lifecycle Controller 펌웨어와 BIOS 버전이 최소 권장 사항에 일치하는지 확인합니다.
- CSIOR이 시스템 또는 iDRAC에서 한 번 이상 실행되어야 합니다.

하드웨어 구성 오류

- 배포 작업을 시작하기 전에 시스템에서 CSIOR을 완료하고 재부팅이 진행 중이 아닌지 확인합니다.
- 참조 서버가 동일한 시스템이 되도록 클론 모드에서 BIOS 구성을 실행해야 합니다.
- 일부 컨트롤러에서는 하나의 드라이브로 RAID 0 어레이를 생성할 수 없습니다. 이 기능은 최신 컨트롤러에서만 지원되며, 그러한 하드웨어 프로필의 애플리케이션은 오류를 야기할 수 있습니다.

새로 구입한 시스템에서 자동 검색 활성화

호스트 시스템의 자동 검색 기능은 기본적으로 활성화되어 있지 않습니다. 대신 구매 시에 활성화를 요청해야 합니다. 구매 시에 자동 검색 활성화를 요청하면 DHCP가 iDRAC에서 활성화되고 관리 계정이 비활성화됩니다. iDRAC에 정적 IP 주소를 구성할 필요는 없습

니다. 네트워크의 DHCP 서버에서 IP 주소를 가져옵니다. 자동 검색 기능을 사용하려면, 검색 프로세스를 지원하도록 DHCP 서버 또는 DNS 서버 또는 양쪽 모두를 구성해야 합니다. CSIOR이 출하 프로세스 중에 이미 실행되어 있어야 합니다.

구입 시 자동 검색을 요청하지 않은 경우 다음과 같이 활성화할 수 있습니다.

1. 부팅 루틴이 진행되는 동안 **Ctrl + E** 키를 누릅니다.
2. iDRAC 설정 창에서 NIC(블레이드 서버만)를 활성화합니다.
3. 자동 검색을 활성화합니다.
4. DHCP를 활성화합니다.
5. 관리 계정을 비활성화합니다.
6. **DHCP에서 DNS 서버 주소 가져오기**를 활성화합니다.
7. **DHCP에서 DNS 도메인 이름 가져오기**를 활성화합니다.
8. **프로비저닝 서버** 필드에 다음을 입력합니다.

```
<OpenManage Integration virtual appliance IPaddress>:4433
```

A

시스템별 특성

iDRAC

표 28. 시스템 특정 특성 iDRAC

특성 이름	표시 특성 이름	그룹 표시 이름
DNS RAC 이름	DNS RAC 이름	NIC 정보
DataCenterName	데이터 센터 이름	서버 토폴로지
통로 이름	통로 이름	서버 토폴로지
랙 이름	랙 이름	서버 토폴로지
랙 슬롯	랙 슬롯	서버 토폴로지
RacName	Active Directory RAC 이름	Active Directory
주소	IPv4 주소	IPv4 정적 정보
넷마스크	넷마스크	IPv4 정적 정보
게이트웨이	게이트웨이	IPv4 정적 정보
DNS2	DNS Server 2	IPv4 정적 정보
주소 1	IPv6 주소 1	IPv6 정적 정보
게이트웨이	IPv6 게이트웨이	IPv6 정적 정보
접두어 길이	IPv6 링크 로컬 접두사 길이	IPv6 정적 정보
DNS1	IPV6 DNS 서버 1	IPv6 정적 정보
DNS2	IPv6 DNS 서버 2	IPv6 정적 정보
DNSFromDHCP6	DHCP6에서 DNS 서버	IPv6 정적 정보
HostName	서버 호스트 이름	서버 운영 체제
RoomName	RoomName	서버 토폴로지
NodeID	시스템 노드 ID	서버 정보

BIOS

표 29. BIOS에 대한 시스템 특정 특성

특성 이름	표시 특성 이름	그룹 표시 이름
AssetTag	Asset Tag	기타 설정
IscsiDev1Con1Gateway	초기자 게이트웨이	연결 1 설정
IscsiDev1Con1Ip	Initiator IP Address	연결 1 설정
IscsiDev1Con1Mask	Initiator Subnet Mask	연결 1 설정
IscsiDev1Con1TargetIp	Target IP Address	연결 1 설정

표 29. BIOS에 대한 시스템 특정 특성 (계속)

특성 이름	표시 특성 이름	그룹 표시 이름
IscsiDev1Con1TargetName	Target Name	연결 1 설정
IscsiDev1Con2Gateway	초기자 게이트웨이	연결 1 설정
IscsiDev1Con2Ip	Initiator IP Address	연결 1 설정
IscsiDev1Con2Mask	Initiator Subnet Mask	연결 1 설정
IscsiDev1Con2TargetIp	Target IP Address	연결 1 설정
IscsiDev1Con2TargetName	Target Name	연결 1 설정
IscsiInitiatorName	ISCSI 초기자 이름	네트워크 설정
Ndc1PcieLink1	내장형 네트워크 카드 1 PCIe Link1	내장형 장치
Ndc1PcieLink2	내장형 네트워크 카드 1 PCIe Link2	내장형 장치
Ndc1PcieLink3	내장형 네트워크 카드 1 PCIe Link3	내장형 장치
UefiBootSeq	UEFI 부팅 순서	UEFI 부팅 설정

RAID

표 30. RAID에 대한 시스템 특정 특성

특성 이름	표시 특성 이름	그룹 표시 이름
엔클로저 요청 구성 모드	해당 없음	해당 없음
엔클로저 현재 구성 모드	해당 없음	해당 없음

CNA

표 31. CNA에 대한 시스템 특정 특성

특성 이름	표시 특성 이름	그룹 표시 이름
ChapMutualAuth	CHAP 상호 인증 수행	iSCSI 일반 매개 변수
ConnectFirstTgt	Connect	iSCSI 첫 번째 대상 매개변수
ConnectSecondTgt	Connect	iSCSI 두 번째 대상 매개변수
FirstFCoEBootTargetLUN	Boot LUN	FCoE 구성
FirstFCoEWWPNTarget	WPN(World Wide Port Name) 대상	FCoE 구성
FirstTgtBootLun	Boot LUN	iSCSI 첫 번째 대상 매개변수
FirstTgtChapId	CHAP ID	iSCSI 첫 번째 대상 매개변수
FirstTgtChapPwd	CHAP 암호	iSCSI 첫 번째 대상 매개변수
FirstTgtIpAddress	IP 주소	iSCSI 첫 번째 대상 매개변수
FirstTgtIscsiName	iSCSI 이름	iSCSI 첫 번째 대상 매개변수
FirstTgtTcpPort	TCP Port	iSCSI 첫 번째 대상 매개변수
IP 자동 구성	IpAutoConfig	iSCSI 일반 매개 변수
IscsiInitiatorChapId	CHAP ID	iSCSI 초기자 매개 변수
IscsiInitiatorChapPwd	CHAP 암호	iSCSI 초기자 매개 변수
IscsiInitiatorGateway	기본 게이트웨이	iSCSI 초기자 매개 변수

표 31. CNA에 대한 시스템 특정 특성 (계속)

특성 이름	표시 특성 이름	그룹 표시 이름
IscsiInitiatorIpAddr	IP 주소	iSCSI 초기자 매개 변수
IscsiInitiatorIpv4Addr	IPv4 주소	iSCSI 초기자 매개 변수
IscsiInitiatorIpv4Gateway	IPv4 기본 게이트웨이	iSCSI 초기자 매개 변수
IscsiInitiatorIpv4PrimDns	IPv4 기본 DNS	iSCSI 초기자 매개 변수
IscsiInitiatorIpv4SecDns	IPv4 보조 DNS	iSCSI 초기자 매개 변수
IscsiInitiatorIpv6Addr	IPv6 주소	iSCSI 초기자 매개 변수
IscsiInitiatorIpv6Gateway	IPv6 기본 게이트웨이	iSCSI 초기자 매개 변수
IscsiInitiatorIpv6PrimDns	IPv6 기본 DNS	iSCSI 초기자 매개 변수
IscsiInitiatorIpv6SecDns	IPv6 보조 DNS	iSCSI 초기자 매개 변수
IscsiInitiatorName	iSCSI 이름	iSCSI 초기자 매개 변수
IscsiInitiatorPrimDns	기본 DNS	iSCSI 초기자 매개 변수
IscsiInitiatorSecDns	보조 DNS	iSCSI 초기자 매개 변수
IscsiInitiatorSubnet	서브넷 마스크	iSCSI 초기자 매개 변수
IscsiInitiatorSubnetPrefix	서브넷 마스크 접두사	iSCSI 초기자 매개 변수
SecondaryDeviceMacAddr	보조 장치 MAC 주소	iSCSI 보조 장치 매개 변수
SecondTgtBootLun	Boot LUN	iSCSI 두 번째 대상 매개변수
SecondTgtChapPwd	CHAP 암호	iSCSI 두 번째 대상 매개변수
SecondTgtIpAddress	IP 주소	iSCSI 두 번째 대상 매개변수
SecondTgtIscsiName	iSCSI 이름	iSCSI 두 번째 대상 매개변수
SecondTgtTcpPort	TCP Port	iSCSI 두 번째 대상 매개변수
UseIndTgtName	독립 대상 이름 사용	iSCSI 보조 장치 매개 변수
UseIndTgtPortal	독립 대상 포털 사용	iSCSI 보조 장치 매개 변수
VirtFIPMacAddr	가상 FIP MAC 주소	기본 구성 페이지
VirtIscsiMacAddr	가상 iSCSI 오프로드 MAC 주소	기본 구성 페이지
VirtMacAddr	가상 MAC 주소	기본 구성 페이지
VirtMacAddr[Partition:n]	가상 MAC 주소	파티션 n 구성
VirtWWN	가상 World Wide 노드 이름	기본 구성 페이지
VirtWWN[Partition:n]	가상 World Wide 노드 이름	파티션 n 구성
VirtWWPN	가상 World Wide 포트 이름	기본 구성 페이지
VirtWWPN[Partition:n]	가상 World Wide 포트 이름	파티션 n 구성
World Wide 노드 이름	WWN	기본 구성 페이지
World Wide 노드 이름	WWN[Partition:n]	파티션 n 구성

FC

표 32. FC에 대한 시스템 특정 시스템

특성 이름	표시 특성 이름	그룹 표시 이름
VirtualWWN	가상 World Wide 노드 이름	포트 구성 페이지
VirtualWWPN	가상 World Wide 포트 이름	포트 구성 페이지

B

추가 정보

delltechcenter.com에서 사용할 수 있는 다음 Dell 기술 백서는 시스템 프로필 구성 템플릿, 특성 및 작업 흐름에 대한 추가 정보를 제공합니다.

- *서버 구성 프로필을 사용하여 서버 복제*
- *서버 구성 XML 파일*
- *구성 XML 워크플로*
- *구성 XML 워크플로 스크립트 133*
- *XML 구성 파일 예*

C

사용자 지정 특성

표 33. 사용자 지정 특성

FQDD	속성	OMIVV 사용자 지정
BIOS	가상화 기술	항상 활성화
iDRAC	요청 시 시스템 재고 수집	항상 활성화
RAID	IncludedPhysicalDiskID	IncludedPhysicalDiskID 값이 자동 선택인 경우 해당 값 제거
RAID	RAIDPDState	제거됨
iDRAC	사용자 관리자 암호 암호	iDRAC를 활성화한 사용자만 암호를 입력하는 "암호" 링크가 있습니다.
PCIeSSD	PCIeSSDSecureErase	항상 비활성화됨

D

구성 요소와 기준선 버전 비교 매트릭스

표 34. 구성 요소와 기준선 버전 비교 매트릭스

변경 사항 유형				
하드웨어	**연결된 기준선**	**대상 구성 요소**	**시나리오**	**준수 상태**
	사용 가능	사용 가능	하드웨어 구성 요소가 연결된 기준선과 일치합니다.	준수
	사용 가능	사용 가능	하드웨어 구성 요소 속성이 연결된 기준선과 일치하지 않습니다.	비준수
	사용할 수 없음	사용 가능	비교 상태가 계산되지 않고 무시됩니다.	준수
	사용 가능	사용할 수 없음	하드웨어 구성 요소를 연결된 기준선에서 사용할 수 있지만 구성 요소 또는 속성을 호스트에서 사용할 수 없습니다.	비준수
	사용할 수 없음	사용할 수 없음	비교 상태가 계산되지 않고 무시됩니다.	준수
펌웨어	**연결된 기준선**	**대상 구성 요소**	**시나리오**	**준수 상태**
	사용 가능	사용 가능	펌웨어 구성 요소 버전이 연결된 기준선과 일치합니다.	준수
	사용 가능	사용 가능	펌웨어 구성 요소 버전이 연결된 기준선과 일치하지 않습니다.	비준수
	사용할 수 없음	사용 가능	펌웨어 구성 요소 버전을 연결된 기준선에서 사용할 수 없지만 구성 요소를 호스트에서 사용할 수 있습니다. 비교 상태가 계산되지 않고 무시됩니다.	준수
	사용 가능	사용할 수 없음	비교 상태가 계산되지 않고 무시됩니다.	준수
	사용할 수 없음	사용할 수 없음	비교 상태가 계산되지 않고 무시됩니다.	준수
드라이버	**연결된 기준선**	**대상 구성 요소**	**시나리오**	**준수 상태**
	사용 가능	사용 가능	드라이버 구성 요소 버전이 연결된 기준선과 일치합니다.	준수
	사용 가능	사용 가능	드라이버 구성 요소 버전이 연결된 기준선과 일치하지 않습니다.	비준수
	사용할 수 없음	사용 가능	비교 상태가 계산되지 않고 무시됩니다.	준수
	사용 가능	사용할 수 없음	드라이버 구성 요소 버전을 연결된 기준선에서 사용할 수 있지만 구성 요소를 호스트에서 사용할 수 있습니다.	비준수
	사용할 수 없음	사용할 수 없음	비교 상태가 계산되지 않고 무시됩니다.	준수

E

응답 코드

표 35. 응답 코드

응답 코드	설명
200	작업 정보 또는 작업 목록의 성공적인 생성/반환
202	모든 작업이 성공적으로 시작됨
400	잘못된 요청
401	무단 요청
404	찾을 수 없음
409	충돌
500	내부 서버 오류
503	서비스를 사용할 수 없음