OpenManage Integration for VMware vCenter 버전 4.2

웹 클라이언트 사용자 가이드

2018년 4월
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. OMIVV(OpenManage Integration for VMware vCenter)를 통해 강화된 배포, 관리, 모니터링, 업그레이드 기능을 제공함으로써 VMware 웹 클라이언트에서 Dell 호스트를 더욱 잘 관리할 수 있습니다.

주제:

이 릴리스의 새로운 기능

이 릴리스의 OpenManage Integration for VMware vCenter에서 제공하는 기능은 다음과 같습니다.

- 기존의 Cluster Aware Update가 vSAN 클러스터를 지원하도록 향상되었습니다. 드라이버 및 펌웨어 업데이트를 지원합니다.
- 드라이버, 펌웨어, 하드웨어 구성 및 드리프트 감지에 대한 vSAN 클러스터를 기준으로 설정하는 기능
- 시스템 프로필 특성을 포함/제외하는 기능
- 14세대 플랫폼 지원
- SMB2 CIFS 공유 지원
- OMSA 9.1 지원
- vSphere 6.7 지원

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, RAC, 보증 정보, 서버, 클러스터 및 데이터 센터 레벨 보기와 같은 PowerEdge 서버 세부 정보 • 섀시 관리 컨트롤러 정보, 섀시 전원 공급 장치, KVM 상태, 팬/열 세부 정보, 보증 정보, 비어 있는 스위치/서버 세부 정보와 같은 섀시 세부 정보
경고 모니터링 및 보내기	모니터링 및 경고는 다음 기능을 포함합니다. • 주요 하드웨어 결함을 감지하고 가상화 인식 작업 수행 (예: 워크로드 마이그레이션 또는 호스트를 유지 관리 모드로 전환). • 인벤토리, 이벤트 및 경보와 같이 서버 문제를 진단하기 위한 지능적인 기능 제공. • VMware ProActive HA 기능 지원.
펌웨어 업데이트	펌웨어 업데이트에는 다음이 포함됩니다. • BIOS 및 펌웨어가 최신 버전으로 업데이트된 Dell EMC 하드웨어. • 현재 Cluster Aware Update 기능은 DRS 옵션이 활성화된 경우 vSAN 클러스터를 지원하도록 향상되었습니다. 또한 향상된 기능은 vSAN 클러스터의 드라이버 및 펌웨어 업데이트도 지원합니다.

표 1. OMIVV 기능 (계속)

기능	설명
배포 및 프로비저닝	PXE를 사용하지 않고 VMware vCenter를 사용하여 하드웨어 프로필(11~13세대 PowerEdge 서버), 시스템 프로필(14세대 서버), 하이퍼바이저 프로필을 생성한 후 베어 메탈 PowerEdge 서버에 원격으로 OS를 배포합니다.
서비스 정보	Dell의 보증 데이터베이스에서 Dell EMC 서버 및 관련 섀시에 대한 보증 정보를 검색하고 간편한 온라인 보증 업그레이드 허용.
보안 역할 및 권한	보안 역할 및 권한에는 다음 기능이 포함됩니다. • 표준 vCenter 인증, 규칙 및 권한과 통합합니다. • 14세대 서버에서 iDRAC 잠금 모드를 지원합니다.

노트: OMIVV 4.0 이상부터 VMware vSphere 웹 클라이언트만 지원되며 vSphere Desktop 클라이언트는 지원되지 않습니다.

노트: vCenter 6.5 이상의 경우, OMIVV 어플라이언스는 플래시 버전에 대해서만 사용할 수 있습니다. OMIVV 어플라이언스는 HTML 5 버전에는 사용할 수 없습니다.

2

관리 콘솔 정보

다음 두 관리 포털을 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)

주제:

관리 포털 사용

관리 포털을 사용하여 다음 작업을 수행할 수 있습니다.

- vCenter 서버를 등록합니다. vCenter 서버 등록을 참조하십시오.
- vCenter 로그인 자격 증명을 수정합니다. vCenter 로그인 자격 증명 수정을 참조하십시오.
- SSL 인증서를 업데이트하십시오. 등록된 vCenter 서버의 SSL 인증서 업데이트를 참조하십시오.
- 라이센스를 업로드하거나 구매하십시오. 평가판 라이센스를 사용하는 경우 **소프트웨어 구매** 링크가 표시됩니다. 이 링크를 클릭하면 여러 개의 호스트를 관리하는 전체 버전 라이센스를 구매할 수 있습니다. 관리 포털에 라이센스 업로드를 참조하십시오.
- OMIVV를 업데이트하십시오. 가상 어플라이언스 리포지토리 위치 및 가상 어플라이언스 업데이트 페이지 16을(를) 참조하십시오.
- 문제 해결 번들 생성. 문제해결 번들 다운로드 페이지 27을(를) 참조하십시오.
- OMIVV를 다시 시작합니다. 가상 어플라이언스 다시 시작 페이지 15을(를) 참조하십시오.
- 백업 및 복원을 수행합니다. 백업 및 복원을 통해 어플라이언스 업데이트 페이지 17을(를) 참조하십시오.
- 경고를 구성합니다. 전역 경고 설정 페이지 19을(를) 참조하십시오.
- 배포 모드를 구성합니다. 배포 구성 모드 페이지 18의 내용을 참조하십시오.

관리자가 아닌 사용자를 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 대해 선택한 권한을 변경하려면 역할을 추가하고 역할에 대해 필요한 권한을 선택하거나 기존 역할을 수정합니다.
   역할을 생성 또는 수정하고 vSphere 웹 클라이언트의 권한을 선택하는 데 필요한 단계는 VMware vSphere 설명서를 참조하십시오. 역할의 필수 권한을 모두 선택하려면 관리자가 아닌 사용자의 필수 권한을 참조하십시오.
   노트: vCenter 관리자는 역할을 추가하거나 수정해야 합니다.
2. 역할을 정의하고 역할에 대한 권한을 선택한 후 새로 생성된 역할에 사용자를 할당합니다.
   vSphere 웹 클라이언트의 권한 할당에 대한 자세한 내용은 VMware vSphere 설명서를 참조하십시오.
   노트: vCenter 관리자는 vSphere 클라이언트에서 권한을 할당해야 합니다.

   필요한 권한이 있는 vCenter 서버 관리자가 아닌 사용자가 이제 vCenter를 등록 및/또는 등록 취소하거나, 자격 증명을 수정하거나, 인증서를 업데이트할 수 있습니다.
3. 필요한 권한이 있는 관리자가 아닌 사용자를 사용하여 vCenter 서버를 등록합니다. 필요한 권한이 있는 관리자가 아닌 사용자로 vCenter 서버 등록을 참조하십시오.
4. 1단계에서 생성했거나 수정한 역할에 Dell 권한을 할당합니다. vSphere 웹 클라이언트에서 역할에 Dell 권한 할당을 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 필요합니다.

노트: 다음 권한이 할당되지 않으면 관리자가 아닌 사용자가 vCenter 서버를 OMIVV에 등록하는 동안 오류 메시지가 표시됩니다.

- 알람
  - 알람 생성
  - 알람 수정
  - 알람 제거
- 확장명
  - 확장명 등록
  - 확장명 등록 취소
  - 확장명 업데이트
- 전역
  - 작업 취소
  - 이벤트 로그
  - 설정

    노트: VMware vCenter 6.5를 사용 중이거나 vCenter 6.5 이상으로 업그레이드 중인 경우 다음의 상태 업데이트 권한을 할당합니다.
- 상태 업데이트 공급자
  - 등록
  - 등록 취소
  - 업데이트
- 호스트
  - CIM
    - CIM 상호 작용
  - 구성
    - 고급 설정
    - 연결
    - 유지관리
    - 네트워크 구성
    - 쿼리 패치
    - 보안 프로필 및 방화벽

    노트: VMware vCenter 6.5를 사용 중이거나 vCenter 6.5 이상으로 업그레이드 중인 경우 다음의 권한을 할당합니다.
    - Host.Config
      - 고급 설정
      - 연결
      - 유지관리
      - 네트워크 구성
      - 쿼리 패치
      - 보안 프로필 및 방화벽
  - 인벤토리
    - 클러스터에 호스트 추가
    - 독립 실행형 호스트 추가
    - 클러스터 수정

      노트: vCenter 6.5를 사용 중이거나 vCenter 6.5 이상으로 업그레이드 중인 경우 클러스터 수정 권한을 할당해야 합니다.
- 호스트 프로필
  - 편집
  - 보기
- 권한
  - 권한 수정
  - 역할 수정
- 세션

- 세션 유효성 검사
- 작업
  - 작업 생성
  - 작업 업데이트

노트: 관리자가 아닌 사용자가 vCenter 서버를 등록하려는 경우 기존 역할에 Dell 권한을 추가해야 합니다. Dell 권한 할당에 대한 자세한 내용은 기존 역할에 Dell 권한 할당 페이지 13을(를) 참조하십시오.

필요한 권한이 있는 관리자가 아닌 사용자를 사용하여 vCenter 서버 등록

필요한 권한이 있는 관리자가 아닌 사용자를 사용하여 OMIVV 어플라이언스용 vCenter 서버를 등록할 수 있습니다. 참조하십시오.vCenter 서버 등록 페이지 13 관리자가 아닌 사용자 또는 관리자를 통한 vCenter 서버 등록에 대한 내용을 참조하십시오.

기존 역할에 Dell 권한 할당

기존 역할을 편집하여 Dell 권한을 할당할 수 있습니다.

노트: 관리자 권한이 있는 사용자로 로그인해야 합니다.

1. 관리 권한을 사용하여 vSphere 웹 클라이언트에 로그인합니다.
2. 왼쪽 창의 vSphere 웹 클라이언트에서 **관리** → **역할**을 클릭합니다.
3. **역할 공급자** 드롭다운 목록에서 vCenter 서버 시스템을 선택합니다.
4. **역할** 목록에서 역할을 선택하고 을 클릭합니다.
5. **권한**을 클릭하고 **Dell**을 확장한 다음 선택된 역할에 대해 다음 Dell 권한을 선택하고 **확인**을 클릭합니다.
   - Dell.Configuration
   - Dell.Deploy-Provisioning
   - Dell.Inventory
   - Dell.Monitoring
   - Dell.Reporting

   vCenter 내에서 사용 가능한 OMIVV 역할에 대한 자세한 내용은 `Dell.com/support/manuals`에서 사용할 수 있는 *OpenManage Integration for VMware vCenter User's Guide(OpenManage Integration for VMware vCenter 사용 설명서)*의 Security roles and permissions(보안 역할 및 권한) 을 참조하십시오.

권한 및 역할에 대한 변경 사항은 즉시 적용됩니다. 필요한 권한을 가진 사용자는 이제 OpenManage Integration for VMware vCenter 작업을 수행할 수 있습니다.

노트: 모든 vCenter 작업의 경우, OMIVV는 로그인 사용자의 권한이 아닌 등록된 사용자의 권한을 사용합니다.

노트: 로그인한 사용자에게 할당된 Dell 권한 없이 OMIVV의 특정 페이지에 액세스한 경우 2000000 오류가 표시됩니다.

vCenter 서버 등록

OpenManage Integration for VMware vCenter를 설치한 후 OMIVV 어플라이언스를 등록할 수 있습니다. OpenManage Integration for VMware vCenter에서는 vCenter 운영에 필요한 권한이 있는 관리자 계정 또는 관리자가 아닌 사용자 계정을 사용합니다. 단일 OMIVV 어플라이언스 인스턴스는 총 10대의 vCenter 서버 및 최대 1000대의 ESXi 호스트를 지원할 수 있습니다.

새 vCenter 서버를 등록하려면 다음 단계를 수행합니다.

1. 지원되는 브라우저에서 **관리 포털**을 엽니다.
   관리 포털을 열려면 OpenManage Integration for VMware vCenter의 **도움말 및 지원** 탭에서 **관리 콘솔** 아래에 있는 링크를 클릭하거나 웹 브라우저를 시작하여 `https:\\<어플라이언스 IP|호스트 이름>`을 입력합니다.
2. 왼쪽 창에서 **VCENTER 등록**을 클릭한 다음 **새 vCenter 서버 등록**을 클릭합니다.
3. **새 vCenter 등록** 대화 상자의 **vCenter 이름** 아래에서 다음 단계를 수행합니다.
   a. **vCenter 서버 IP 또는 호스트 이름** 텍스트 상자에 vCenter IP 주소 또는 호스트 이름 또는 FQDN을 입력합니다.

      노트: 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 고정 IP 주소 및 호스트 이름을 할당합니다. 고정 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 항목이 표시되는지 확인합니다.

b. **설명** 텍스트 상자에서 설명(선택 사항)을 입력합니다.

4. **vCenter 사용자 계정** 아래에서 다음 단계를 수행합니다.
   a. **vCenter 사용자 이름** 텍스트 상자에 관리자의 사용자 이름 또는 필요한 권한이 있는 관리자가 아닌 사용자 이름을 입력합니다.
   b. **암호** 텍스트 상자에 암호를 입력합니다.
   c. **암호 확인** 텍스트 상자에서 암호를 다시 입력합니다.
5. **등록**을 클릭합니다.

vCenter 서버를 등록하면 OMIVV가 vCenter 플러그인으로 등록되고 OMIVV 기능에 액세스할 수 있는 vSphere 웹 클라이언트에 "Dell EMC OpenManage Integration" 아이콘이 표시됩니다.

노트: 모든 vCenter 작업의 경우, OMIVV는 로그인 사용자의 권한이 아닌 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 시작할 수 있습니다. 펌웨어 업데이트 작업을 수행하는 동안 OMIVV는 사용자 X의 권한을 사용하여 호스트를 유지 관리 모드로 두거나 호스트를 재부팅합니다.

vCenter 로그인 자격 증명 수정

vCenter 로그인 자격 증명은 관리자 권한이 있는 사용자 또는 필요한 권한이 있는 관리자가 아닌 사용자가 수정할 수 있습니다.

1. 관리 포털을 열려면 OpenManage Integration for VMware vCenter의 **도움말 및 지원** 탭에서 **관리 콘솔** 아래에 있는 링크를 클릭하거나 웹 브라우저를 시작하여 `https:\\<ApplianceIP|hostname>` URL을 입력합니다.
2. **로그인** 대화 상자에 암호를 입력하고 **로그인**을 클릭합니다.
3. 왼쪽 창에서 **VCENTER REGISTRATION(VCENTER 등록)**을 클릭합니다.
   등록된 vCenter 서버는 **vCenter 서버 연결 관리** 창의 오른쪽 메뉴에 표시됩니다. **MODIFY USER ACCT** 창을 열려면 **자격 증명** 아래에서 등록된 vCenter에 대하여 **수정**을 클릭합니다.
4. vCenter **사용자 이름**, **암호** 및 **암호 확인**을 입력합니다. 이 두 암호는 일치해야 합니다.
5. 암호를 변경하려면 **적용**을 클릭하거나 변경을 취소하려면 **취소**를 클릭합니다.

노트: 제공된 사용자 자격 증명에 필요한 권한이 없는 경우 오류 메시지가 표시됩니다.

등록된 vCenter 서버의 SSL 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. OpenManage Integration for VMware vCenter는 보안 통신용 웹 서버에서 SSL을 활성화하기 위해 디지털 인증서를 사용합니다.

vCenter 서버에서 SSL 인증서가 변경된 경우 다음 단계를 사용하여 OpenManage Integration for VMware vCenter를 위한 새 인증서를 가져옵니다.

1. 관리 포털을 열려면 OpenManage Integration for VMware vCenter의 **도움말 및 지원** 탭에서 **관리 콘솔** 아래에 있는 링크를 클릭하거나 웹 브라우저를 시작하여 `https:\\<ApplianceIP|hostname>` URL을 입력합니다.
2. 왼쪽 창에서 **VCENTER 등록**을 클릭합니다.
   등록된 vCenter 서버가 오른쪽 창에 표시됩니다.
3. vCenter 서버 IP 또는 호스트 이름에 대한 인증서를 업데이트하려면 **업데이트**를 클릭합니다.

OpenManage Integration for VMware vCenter 제거

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

노트: 인벤토리, 보증 또는 배포 작업이 실행 중일 때 vCenter 서버에서 OMIVV를 등록 취소하지 마십시오.

1. 관리 포털을 열려면 OpenManage Integration for VMware vCenter의 **도움말 및 지원** 탭에서 **관리 콘솔** 아래에 있는 링크를 클릭하거나 웹 브라우저를 시작하여 `https:\\<ApplianceIP|hostname>` URL을 입력합니다.
2. **VCENTER 등록** 페이지의 **vCenter 서버 IP 또는 호스트 이름** 표에서 **등록 취소**를 클릭합니다.

   노트: 둘 이상의 vCenter가 있을 수 있으므로 올바른 vCenter를 선택해야 합니다.

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

노트: 클러스터에 자동 관리 HA를 활성화한 경우, 자동 관리 HA가 클러스터에서 비활성화되었는지 확인합니다. 자동 관리 HA 비활성화의 경우 **구성** > **서비스** > **vSphere 가용성**을 선택한 다음, **편집**을 클릭하여 클러스터의 **Proactive HA 오류 및 응답** 화면을 이용합니다. 자동 관리 HA를 비활성화하려면:

Proactive HA 오류 및 응답 화면에서 **Dell Inc** 공급자의 확인란을 선택 취소합니다.

관리 포털에 라이센스 업로드

OMIVV 라이센스를 업로드하여 지원되는 동시에 등록된 vCenter 인스턴스 및 관리되는 호스트 수를 변경할 수 있습니다. 호스트를 추가해야 하는 경우 다음 단계를 수행하여 라이센스를 추가할 수도 있습니다.

1. 관리 포털을 열려면 OpenManage Integration for VMware vCenter의 **도움말 및 지원** 탭에서 **관리 콘솔** 아래에 있는 링크를 클릭하거나 웹 브라우저를 시작하여 `https:\\<ApplianceIP|hostname>` URL을 입력합니다.
2. **로그인** 대화 상자에 암호를 입력합니다.
3. 왼쪽 창에서 **VCENTER 등록**을 클릭합니다.
   등록된 vCenter 서버가 오른쪽 창에 표시됩니다.
4. **라이센스 업로드**를 클릭합니다.
5. **라이센스 업로드** 대화 상자에서 **찾아보기**를 클릭하여 라이센스 파일을 찾은 다음 **업로드**를 클릭합니다.

   노트: 라이센스 파일이 수정되었거나 편집된 경우 OMIVV 어플라이언스에서는 라이센스 파일이 손상된 것으로 인식하므로 해당 파일이 작동되지 않습니다.

가상 어플라이언스 관리

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

- 가상 어플라이언스를 다시 시작합니다. 가상 어플라이언스 다시 시작을 참조하십시오.
- 가상 어플라이언스를 업데이트하고 업데이트 리포지토리 위치를 구성합니다. 가상 어플라이언스 리포지토리 위치 및 가상 어플라이언스 업데이트.
- NTP 서버를 설정합니다. 네트워크 시간 프로토콜 서버 설정을 참조하십시오.
- HTTPS 인증서를 업로드합니다. HTTPS 인증서 업로드를 참조합니다.

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

1. 관리 포털을 열려면 OpenManage Integration for VMware vCenter의 **도움말 및 지원** 탭에서 **관리 콘솔** 아래에 있는 링크를 클릭하거나 웹 브라우저를 시작하여 `https:\\<ApplianceIP|hostname>` URL을 입력합니다.
2. **로그인** 대화 상자에 암호를 입력합니다.
3. 어플라이언스 관리 섹션을 구성하려면 왼쪽 창에서 **어플라이언스 관리**를 클릭합니다.

가상 어플라이언스 다시 시작

1. **어플라이언스 관리** 페이지에서 **가상 어플라이언스를 다시 시작**을 클릭합니다.
2. 가상 어플라이언스를 다시 시작하려면 **가상 어플라이언스 다시 시작** 대화 상자에서 **적용**을 클릭하고 취소하려면 **취소**를 클릭합니다.

가상 어플라이언스의 호스트 이름 변경

다음 단계를 수행합니다.

1. **어플라이언스 관리** 페이지에서 **호스트 이름 변경**을 클릭합니다.
2. 업데이트된 호스트 이름을 입력합니다.
   <hostname> 형식으로 도메인 이름을 입력합니다.
3. **호스트 이름 업데이트**를 클릭합니다.
   어플라이언스 호스트 이름이 업데이트되고 기본 메뉴로 돌아갑니다.
4. 어플라이언스를 재부팅하려면 **어플라이언스 재부팅**을 클릭합니다.

노트: 어플라이언스에 vCenter 서버를 등록한 경우 모든 vCenter 인스턴스의 등록을 취소하고 다시 등록하십시오.

노트: iDRAC, DRM의 프로비저닝 서버와 같은 환경에서 가상 어플라이언스에 대한 모든 참조를 수동으로 업데이트해야 합니다.

가상 어플라이언스 리포지토리 위치 및 가상 어플라이언스 업데이트

모든 데이터를 보호하려면 가상 어플라이언스 업데이트 이전에 OMIVV 데이터베이스의 백업을 수행합니다. 백업 및 복원 관리 페이지 20를 참조하십시오.

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

   노트: 사용할 수 있는 업그레이드 메커니즘을 표시하고 RPM 업그레이드를 수행하려면 OMIVV 어플라이언스에 인터넷 연결이 필요합니다. OMIVV 어플라이언스가 인터넷에 연결되었는지 확인합니다. 네트워크 설정에 따라 네트워크에서 프록시가 필요한 경우 프록시를 활성화하고 프록시 설정을 제공합니다. HTTP 프록시 설정을 참조하십시오.

   노트: **업데이트 리포지토리 경로**가 유효한지 확인합니다.

   사용 가능한 가상 어플라이언스 버전의 경우 적용 가능한 RPM 및 OVF 가상 어플라이언스 업그레이드 메커니즘이 틱 기호와 함께 표시됩니다. 다음은 가능한 업그레이드 메커니즘 옵션이며 업그레이드 메커니즘에 대한 작업 중 하나를 수행할 수 있습니다.

   - 틱 기호가 RPM에 대해 표시되는 경우 기존 버전에서 사용 가능한 최신 버전으로 RPM을 업그레이드할 수 있습니다. 기존 버전에서 최신 버전으로의 업그레이드를 참조하십시오.
   - 틱 기호가 OVF에 대해 표시되는 경우 기존 버전에서 OMIVV 데이터베이스를 백업한 다음 사용 가능한 최신 어플라이언스 버전에서 복원할 수 있습니다. 백업 및 복원을 통한 어플라이언스 업데이트를 참조하십시오.
   - 틱 기호가 RPM 및 OVF 모두에 대해 표시되는 경우 언급된 옵션 중 하나를 수행하여 어플라이언스를 업그레이드할 수 있습니다. 이 시나리오에서 권장되는 옵션은 RPM 업그레이드입니다.

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

   노트: 모든 웹 클라이언트 세션에서 등록된 vCenter 서버로 로그아웃해야 합니다.

   노트: 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.

3. **어플라이언스 관리**를 클릭하고 업그레이드 메커니즘을 확인합니다.

기존 버전에서 최신 버전으로 OMIVV 업그레이드

1. **어플라이언스 관리** 페이지에서 네트워크 설정에 따라 프록시를 활성화하고, 네트워크에 프록시가 필요한 경우 프록시 설정을 제공합니다. HTTP 프록시 설정을 참조합니다.
2. OpenManage Integration 플러그인을 기존 버전에서 최신 버전으로 업그레이드하려면 다음 단계 중 하나를 수행합니다.
   - **업데이트 리포지토리 경로**에서 사용할 수 있는 RPM을 사용하여 업그레이드하려면 **업데이트 리포지토리 경로**가 http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/ 경로로 설정되어 있는지 확인합니다. 경로가 다른 경우, **어플라이언스 관리** 창의 **어플라이언스 업데이트** 영역에서 **편집**을 클릭하여 경로를 **업데이트 리포지토리 경로** 텍스트 박스의 http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/(으)로 업데이트합니다. 저장하려면 **적용**을 클릭합니다.
   - 인터넷에 연결되지 않은 경우 최신 다운로드 RPM 폴더 또는 파일을 사용하여 업그레이드하려면 http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/ 경로에서 모든 파일과 폴더를 다운로드하여 HTTP 공유에 복사합니다. **어플라이언스 관리** 창의 **어플라이언스 업데이트** 섹션에서 **편집**을 클릭한 다음 **업데이트 리포지토리 경로** 텍스트 상자에서 오프라인 HTTP 공유에 대한 경로를 포함하고 **적용**을 클릭합니다.
3. 사용 가능한 가상 어플라이언스 버전과 현재 가상 어플라이언스 버전을 비교하여 사용 가능한 가상 어플라이언스 버전이 현재 가상 어플라이언스 버전보다 최신인지 확인합니다.
4. 업데이트를 가상 어플라이언스에 적용하려면 **어플라이언스 설정** 아래에서 **가상 어플라이언스 업데이트**를 클릭합니다.
5. **어플라이언스 업데이트** 대화 상자에서 **업그레이드**를 클릭합니다.
   업그레이드를 클릭하면 **관리 콘솔** 창에서 로그오프됩니다.
6. 웹 브라우저를 닫습니다.

노트: 업그레이드 프로세스 중에 어플라이언스가 한 번 또는 두 번 다시 시작됩니다.

노트: 어플라이언스에서 RPM을 업그레이드하면 다음 작업을 수행해야 합니다.

- Dell 관리자 포털에 로그인하기 전에 브라우저 캐시를 지웁니다.
- VMWare 도구를 다시 설치합니다.

다음은 VMWare 도구를 다시 설치하는 방법입니다.

1. OMIVV 어플라이언스를 마우스 오른쪽 단추로 클릭합니다.
2. **게스트** 위에 마우스를 올려놓은 다음, **VMware 도구 설치/업그레이드**를 클릭합니다.
3. **VMware 도구 설치/업그레이드** 대화 상자에서 **자동 도구 업그레이드**를 클릭한 다음, **확인**을 클릭합니다.

   최근 작업에서 설치 상태를 볼 수 있습니다.

노트: RPM 업그레이드가 완료되면 OMIVV 콘솔에서 로그인 화면을 볼 수 있습니다. 브라우저를 열고 *https:\\<ApplianceIP| hostname>* 링크를 입력하고 **어플라이언스 업데이트** 영역으로 이동합니다. 이용 가능한 어플라이언스 버전과 최신 버전이 동일한지 확인할 수 있습니다. 클러스터에서 Proactive HA를 활성화한 경우 OMIVV는 이 클러스터에 대한 Dell Inc 공급자를 등록 취소하고 업그레이드 후 Dell Inc 공급자를 다시 등록합니다. 따라서 업그레이드가 완료될 때까지 Dell EMC 호스트에 대한 상태 업데이트를 사용할 수 없습니다.

백업 및 복원을 통해 어플라이언스 업데이트

OMIVV 어플라이언스를 이전 버전에서 최신 버전으로 업데이트하려면 다음 단계를 수행합니다.

1. 이전 릴리스에 대한 데이터베이스 백업을 수행합니다.
2. vCenter에서 이전 OMIVV 어플라이언스를 끕니다.

   노트: vCenter에서 플러그인을 등록 취소하면 vCenter에서 플러그인이 등록 취소되면 OMIVV 플러그인으로 vCenter에 등록한 모든 알람이 제거되고 조치 등과 같이 알람 발생 시 수행되는 모든 사용자 지정 항목이 제거됩니다.

3. 새 OpenManage Integration 어플라이언스 OVF를 배포합니다.
4. OpenManage Integration 신규 플라이언스의 전원을 켭니다.
5. 새 어플라이언스의 네트워크, 시간대 등을 설정합니다.

   노트: 새 OpenManage Integration 어플라이언스의 IP 주소는 이전 어플라이언스와 같아야 합니다.

   노트: 새 어플라이언스의 IP 주소가 이전 어플라이언스의 IP 주소와 다를 경우 OMIVV 플러그인이 제대로 작동하지 않을 수 있습니다. 이러한 경우 모든 vCenter 인스턴스를 등록 취소하고 다시 등록해야 합니다.

6. OMIVV 어플라이언스는 기본 인증서와 함께 제공됩니다. 어플라이언스에 대한 사용자 정의 인증서를 사용하려면 동일 항목을 업데이트합니다. 인증서 서명 요청 생성 페이지 19 및 HTTPS 인증서 업로드 페이지 19의 내용을 참조하십시오. 그렇지 않으면 이 단계를 건너뜁니다.
7. 데이터베이스를 새 OMIVV 어플라이언스에 복원합니다. 백업에서 OMIVV 데이터베이스 복원을 참조하십시오.
8. 어플라이언스를 확인합니다. Dell.com/support/manuals에서 사용 가능한 *OpenManage Integration for VMware vCenter Installation Guide(OpenManage Integration for VMware vCenter 설치 설명서)*에서 설치 확인을 참조하십시오.
9. 등록된 모든 vCenter 서버에서 **인벤토리**를 실행합니다.

   노트: Dell EMC에서는 업그레이드 후 해당 플러그인이 관리하는 모든 호스트에서 인벤토리를 다시 실행하는 것을 권장합니다. 요청 시 인벤토리를 실행하려면 인벤토리 작업 예약을 참조하십시오.

   노트: 새 OMIVV 버전 y의 IP 주소가 OMIVV 버전 x에서 변경된 경우 SNMP 트랩의 트랩 대상이 새 어플라이언스를 가리키도록 구성합니다. 12세대 이상 서버의 경우 해당 호스트에서 인벤토리를 실행하면 IP가 변경됩니다. 12세대 호스트에서 인벤토리를 실행하는 동안 SNMP 트랩이 새 IP를 가리키지 못하면 이러한 호스트는 비준수로 나열됩니다. 이전 버전을 준수했던 12세대 이전 호스트의 경우 IP 변경은 비준수로 표시되기 때문에 Dell EMC OpenManage Server Administrator(OMSA)를 구성해야 합니다. vSphere 호스트 준수 문제를 해결하려면 비준수 vSphere 호스트 마법사 실행을 참조하십시오.

문제 해결 번들 다운로드

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

HTTP 프록시 설정

1. **어플라이언스 관리** 페이지에서 **HTTP 프록시 설정**을 아래로 스크롤한 후 **편집**을 클릭합니다.
2. 편집 모드에서 다음 단계를 수행합니다.
   a. HTTP 프록시 설정 사용을 활성화하려면 **활성화됨**을 선택합니다.
   b. **프록시 서버 주소**에 프록시 서버 주소를 입력합니다.
   c. **프록시 서버 포트**에 프록시 서버 포트를 입력합니다.
   d. 프록시 자격 증명을 사용하려면 **예**를 선택합니다.
   e. 프록시 자격 증명을 사용하는 경우 **사용자 이름**에 사용자 이름을 입력합니다.
   f. **암호**에 암호를 입력합니다.
   g. **적용**을 클릭합니다.

Network Time Protocol 서버 설정

NTP(Network Time Protocol)를 사용하여 가상 어플라이언스 시계와 NTP 서버 시계를 동기화할 수 있습니다.

1. **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.

노트: 가상 어플라이언스 시계를 NTP 서버와 동기화하는 데 약 10분 정도 걸릴 수 있습니다.

배포 구성 모드

원하는 배포 모드에 대해 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	44GB
중간	최대 500	4	16	44GB
크게	최대 1000	8	32	44GB

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

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

1. **어플라이언스 관리** 페이지에서 **배포 모드**까지 아래로 스크롤합니다.
   배포 모드의 구성 값(**소규모**, **보통** 또는 **대규모**)이 표시되고 기본적으로 배포 모드는 **소규모**로 설정됩니다.
2. 환경을 기반으로 배포 모드를 업데이트하려면 **편집**을 클릭합니다.
3. **편집** 모드에서 필수 조건이 충족되었는지 확인한 후 원하는 배포 모드를 선택합니다.
4. **적용**을 클릭합니다.
   설정된 배포 모드에 그리고 다음과 같은 상황 중 하나가 발생한 경우 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 사항 확인 후 OMIVV 어플라이언스를 재부팅하면 배포 모드를 업데이트할 수 있습니다.

노트: OMIVV 어플라이언스 부팅 중에 설정된 배포 모드에 대해 할당된 시스템 리소스가 확인됩니다. 할당된 시스템을 리소스가 설정된 배포 모드보다 적은 경우 OMIVV 어플라이언스가 로그인 화면으로 부팅되지 않습니다. OMIVV 어플라이언스를 부팅하려면 OMIVV 어플라이언스를 종료하고 시스템 리소스를 기존에 설정된 배포 모드로 업데이트한 다음 다운그레이드 배포 모드 작업을 따릅니다.

다운그레이드 배포 모드

1. 관리 콘솔에 로그인합니다.

2. 배포 모드를 원하는 수준으로 변경합니다.
3. OMIVV 어플라이언스를 종료하고 시스템 리소스를 원하는 수준으로 변경합니다.
4. OMIVV 어플라이언스를 켭니다.

인증서 서명 요청 생성

vCenter에서 OMIVV를 등록하기 전에 해당 인증서를 업로드해야 합니다.

새 인증서 서명 요청(CSR)을 생성하면 이전에 생성된 CSR로 생성한 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 클릭하고 취소하려면 **취소**를 클릭합니다.
2. 요청을 계속하는 경우 **인증서 서명 요청 생성** 대화 상자에서 요청에 대한 **일반 이름**, **조직 이름**, **조직 구성 단위**, **구/군/시**, **도 이름**, **국가** 및 **이메일**을 입력합니다. **계속**을 클릭합니다.
3. **다운로드**를 클릭하고 결과로 생성되는 인증서 요청을 액세스 가능한 위치에 저장합니다.

HTTPS 인증서 업로드

인증서는 PEM 형식을 사용해야 합니다.

안전한 가상 어플라이언스와 호스트 시스템 간 통신을 위해 HTTPS 인증서를 사용할 수 있습니다. 이 유형의 보안 통신을 설정하려면 CSR을 인증 기관에 보낸 다음 관리 콘솔을 사용하여 결과로 생성되는 인증서를 업로드해야 합니다. 자체 서명된 기본 인증서를 보안 통신에 사용할 수도 있습니다. 이 인증서는 모든 설치에서 고유합니다.

노트: Microsoft Internet Explorer, Firefox 또는 Chrome을 사용하여 인증서를 업로드할 수 있습니다.

1. **어플라이언스 관리** 페이지의 **HTTPS 인증서** 영역에서 **인증서 업로드**를 클릭합니다.
2. **인증서 업로드** 대화 상자에서 **확인**을 클릭합니다.
3. 업로드할 인증서를 선택하려면 **찾아보기**를 클릭하고 **업로드**를 클릭합니다.
4. 업로드를 취소하려면 **취소**를 클릭합니다.

   노트: 어플라이언스에 대한 사용자 정의 인증서를 업로드하려면 vCenter 등록 전에 새로운 인증서를 업로드해야 합니다. vCenter 등록 후에 새로운 사용자 정의 인증서를 업로드하면 웹 클라이언트에 통신 오류가 표시됩니다. 이 문제를 해결하려면 vCenter에서 어플라이언스를 등록 취소한 후 다시 등록합니다.

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.

전역 경고 설정

경고 관리를 통해 관리자가 모든 vCenter 인스턴스에 대해 경고가 저장되는 방법에 대한 전역 설정을 구성할 수 있습니다.

1. 관리 포털을 열려면 OpenManage Integration for VMware vCenter의 **도움말 및 지원** 탭에서 **관리 콘솔** 아래에 있는 링크를 클릭하거나 웹 브라우저를 시작하여 `https:\\<ApplianceIP|hostname>` URL을 입력합니다.
2. **로그인** 대화 상자에 암호를 입력합니다.
3. 왼쪽 창에서 **경고 관리**를 클릭합니다. 새 vCenter 경고 설정을 입력하려면 **편집**을 클릭합니다.
4. 다음 필드에 숫자 값을 입력합니다.
   - **최대 경고 수**
   - **경고 보관 일 수**
   - **중복 경고 시간 제한(초)**
5. 설정을 저장하려면 **적용**을 클릭하고 취소하려면 **취소**를 클릭합니다.

백업 및 복원 관리

백업 및 복원 관리는 관리 콘솔에서 수행됩니다. 이 페이지에 있는 작업은 다음과 같습니다.

- 백업 및 복원 구성
- 자동 백업 예약
- 즉시 백업 수행
- 백업에서 데이터베이스 복원

OpenManage Integration for VMware vCenter에서 관리 콘솔을 통해 **백업 및 복원 설정** 페이지에 액세스하려면 다음 단계를 수행합니다.

1. 관리 포털을 열려면 OpenManage Integration for VMware vCenter의 **도움말 및 지원** 탭에서 **관리 콘솔** 아래에 있는 링크를 클릭하거나 웹 브라우저를 시작하여 `https:\\<ApplianceIP|hostname>` URL을 입력합니다.
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 저장할 수 있는 원격 위치에 백업합니다. 백업에는 프로필, 템플릿 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 다음 단계를 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**의 텍스트 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. 백업을 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 **지금 백업** 확인란을 선택합니다.
3. **백업 위치**, **사용자 이름**, **암호** 및 **암호화 암호** 값을 입력합니다.
   암호화 암호에는 영숫자와 "!, @, #, $, %, *" 등의 특수 문자를 사용할 수 있습니다. 길이 제한은 없습니다.
4. **백업**을 클릭합니다.

백업에서 OMIVV 데이터베이스 복원

복원 작업이 완료되면 가상 어플라이언스가 재부팅됩니다.

1. **백업 및 복원 설정** 페이지를 엽니다. 백업 및 복원 관리를 참조하십시오.
2. **백업 및 복원 설정** 페이지에서 **지금 복원**을 클릭합니다.
3. **지금 복원** 대화 상자에서 백업 .gz 파일(CIFS/NFS 형식)과 함께 **파일 위치**에 대한 경로를 입력합니다.
4. 백업 파일의 **사용자 이름**, **암호** 및 **암호화 암호**를 입력합니다.
   암호화 암호에는 영숫자와 "!, @, #, $, %, *" 등의 특수 문자를 사용할 수 있습니다. 길이에는 제한이 없습니다.
5. 변경사항을 저장하려면 **적용**을 클릭합니다.
   어플라이언스가 다시 부팅됩니다.

노트: 어플라이언스가 공장 설정으로 재설정되면 OMIVV 어플라이언스를 다시 등록한 후 확인합니다.

vSphere 클라이언트 콘솔 정보

vSphere 클라이언트 콘솔은 가상 시스템의 vSphere 클라이언트 내에서 찾을 수 있습니다. 콘솔은 관리 콘솔과 밀접하게 작동합니다. 콘솔을 사용하여 다음 작업을 수행할 수 있습니다.

- 네트워크 설정 구성
- 가상 어플라이언스 암호 변경
- NTP 구성 및 로컬 시간대 설정
- 가상 어플라이언스 재부팅
- 가상 어플라이언스를 공장 설정으로 다시 설정
- 콘솔에서 로그아웃
- 읽기 전용 사용자 역할 사용

OMIVV 가상 시스템 콘솔 열기

1. vSphere 웹 클라이언트 **홈**에서 **vCenter**를 클릭합니다.
2. **인벤토리 목록**에서 **가상 시스템**을 클릭한 다음 OMIVV 가상 어플라이언스를 선택합니다.
3. 다음 단계 중 하나를 수행합니다.
   - **개체** 탭에서 **작업 → 콘솔 열기**를 선택합니다.
   - 선택한 가상 시스템을 마우스 오른쪽 단추로 클릭하고 **콘솔 열기**를 선택합니다.

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

네트워크 설정 구성

vSphere 클라이언트 콘솔에서 네트워크 설정을 변경할 수 있습니다.

1. 가상 시스템 콘솔을 엽니다. vSphere 클라이언트 콘솔 열기를 참조하십시오.
2. **콘솔** 창에서 **네트워크 구성**을 선택한 다음 **ENTER** 키를 누릅니다.
3. **장치 편집** 또는 **DNS 편집** 아래에 원하는 네트워크 설정을 입력한 후 **저장 후 끝내기**를 클릭합니다. 변경사항을 중단하려면 **끝내기**를 클릭합니다.

가상 어플라이언스 암호 변경

콘솔을 사용하여 vSphere 웹 클라이언트에서 가상 어플라이언스 암호를 변경할 수 있습니다.

1. 가상 시스템 콘솔을 엽니다. vSphere 클라이언트 콘솔 열기를 참조하십시오.
2. **콘솔** 창에서 화살표 키를 사용하여 **관리자 암호 변경**을 선택하고 **ENTER** 키를 누릅니다.
3. **현재 관리자 암호**에 값을 입력하고 **Enter** 키를 누릅니다.
   관리자 암호는 8자 이상이어야 하고 특수 문자 1개, 숫자 1개, 대문자 1개 및 소문자 1개를 포함해야 합니다.
4. **새 관리자 암호 입력**에 새 암호를 입력하고 **ENTER** 키를 누릅니다.
5. **관리자 암호 확인**에 새 암호를 다시 입력하고 **Enter** 키를 누릅니다.

NTP 구성 및 로컬 시간대 설정

1. 가상 시스템 콘솔을 엽니다. vSphere 클라이언트 콘솔 열기를 참조하십시오.
2. OMIVV 시간대 정보를 구성하려면 **날짜/시간 속성**을 클릭합니다.
3. **날짜 및 시간** 탭에서 **네트워크에서 날짜 및 시간 동기화**를 선택합니다.
   NTP 서버 창이 표시됩니다.
4. NTP 서버 IP 또는 호스트 이름을 추가하려면 **추가** 단추를 클릭한 다음 **TAB** 키를 누릅니다.
5. **시간대**를 클릭하고 해당 시간대를 선택한 다음 **확인**을 클릭합니다.

가상 어플라이언스 다시 부팅

1. 가상 시스템 콘솔을 엽니다. vSphere 클라이언트 콘솔 열기를 참조하십시오.
2. **어플라이언스 재부팅**을 클릭합니다.
3. 어플라이언스를 재부팅하려면 **예**를 클릭하고 취소하려면 **아니오**를 클릭합니다.

가상 어플라이언스를 공장 설정으로 다시 설정

1. 가상 시스템 콘솔을 엽니다. vSphere 클라이언트 콘솔 열기를 참조하십시오.
2. **재설정 설정**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. 어플라이언스를 재설정하려면 **예**를 클릭하고 취소하려면 **아니오**를 클릭합니다.
   예를 클릭하면 OMIVV 어플라이언스가 원래 공장 설정으로 재설정되고 다른 모든 설정 및 기존 데이터가 유실됩니다.

노트: 가상 어플라이언스를 공장 설정으로 재설정해도 네트워크 구성에서 수행한 모든 업데이트는 보존됩니다. 이러한 설정은 재설정되지 않습니다.

vSphere 콘솔에서 로그아웃

vSphere 콘솔에서 로그아웃하려면 **로그아웃**을 클릭합니다.

읽기 전용 사용자 역할

진단 목적으로 셸 액세스가 포함된 권한이 없는 읽기 전용 사용자 역할이 있습니다. 읽기 전용 사용자의 권한은 마운트 실행으로 제한됩니다. 이 읽기 전용 사용자의 암호는 **readonly**로 설정됩니다. 이 읽기 전용 사용자 역할의 사용자 암호는 이전 OMIVV 버전(OMIVV 버전 1.0에서 버전 2.3.1)에서는 관리 암호와 같았지만 OMIVV 버전 3.0 이후로는 보안을 위해 변경되었습니다.

3

다중 어플라이언스 관리

동일한 플랫폼 서비스 컨트롤러(PSC) 및 다른 PSC에 속하는 vCenter 서버에 등록하는 여러 OMIVV 어플라이언스를 관리 및 모니터링할 수 있습니다. Dell EMC는 유사한 vCenter 버전을 사용할 것을 권장합니다.

Dell EMC는 페이지가 캐시된 경우 전역 새로 고침을 수행할 것을 권장합니다.

1. VMware vCenter 홈 페이지에서 **OpenManage Integration** 아이콘을 클릭합니다.
2. **탐색** 창의 **Dell EMC** 그룹에서 **OMIVV 어플라이언스**를 클릭합니다.
3. **OMIVV 어플라이언스** 탭에서 다음 정보를 보고 어플라이언스를 모니터링합니다.

   노트: Dell 어플라이언스 탭에서 목록에 어플라이언스가 표시되는 우선 순위는 미리 결정되어 있고 강조 표시된 어플라이언스가 활성 어플라이언스입니다.

   - **이름** — 각 OMIVV 어플라이언스에 대한 IP 주소 또는 FQDN을 사용하여 링크를 표시합니다. 어플라이언스 관련 정보를 보고 모니터링하려면 특정 어플라이언스 이름 링크를 클릭합니다. 어플라이언스 이름 링크를 클릭하면 OMIVV 어플라이언스의 기본 콘텐츠 창으로 이동합니다. OMIVV 작업을 관리하고, 특정 어플라이언스에 대한 호스트, 데이터 센터 및 클러스터를 모니터링할 수 있습니다.

     노트: 여러 어플라이언스를 사용할 경우 **이름**을 클릭하면 캐시된 페이지에서 전역 새로 고침을 수행하라는 메시지 상자가 표시됩니다.

     OMIVV 작업을 관리하고 있는 어플라이언스를 확인하려면 다음 작업을 수행하십시오.

     a. OpenManage Integration for VMware vCenter에서 **도움말 및 지원** 탭을 클릭합니다.
     b. 관리 콘솔에서 특정 OMIVV 어플라이언스 IP를 확인하십시오.
   - **버전** — 각 OMIVV 어플라이언스의 버전을 표시합니다.
   - **준수 상태** — 어플라이언스가 로드된 플러그인과 호환되는지 여부를 지정합니다.

     노트: OMIVV 어플라이언스가 플러그인과 호환되지 않고 **이름** 링크가 비활성화된 경우 어플라이언스의 준수 상태가 **비호환**으로 표시됩니다.
   - **가용성 상태** — 플러그인에서 어플라이언스에 연결할 수 있고 필요한 웹 서비스가 OMIVV 어플라이언스에서 실행 중인 경우를 지정하는 상태를 표시합니다.

     노트: 어플라이언스 준수 상태가 **호환**이고 어플라이언스 가용성 상태가 **정상**일 경우 어플라이언스를 선택할 수 있습니다.
   - **등록된 vCenter 서버** — 로그인한 세션에 대해 액세스할 수 있고 사용자가 어플라이언스에 등록되어 있는 모든 vCenter를 표시합니다. 어플라이언스를 여러 vCenter에 등록한 경우 vCenter가 펼치거나 축소할 수 있는 목록으로 표시됩니다. vCenter 링크를 클릭하면 모든 vCenter가 탐색 창에 나열되는 **vCenter 서버** 페이지로 이동합니다.

4

웹 클라이언트에서 OpenManage Integration 액세스

OMIVV를 설치한 후 VMware vCenter에 로그인하여 **홈** 탭으로 이동하면 **관리** 그룹 아래의 기본 콘텐츠 영역에서 **OpenManage Integration** 아이콘을 볼 수 있습니다. **OpenManage Integration** 아이콘을 사용하여 **OpenManage Integration for VMware vCenter** 페이지로 이동할 수 있습니다. **Dell EMC** 그룹이 **탐색** 창에 표시됩니다.

VMware vCenter 레이아웃에는 다음과 같은 3개의 기본 창이 있습니다.

표 3. OpenManage Integration for VMware vCenter 창

창	설명
탐색 창	콘솔에서 다른 뷰에 액세스합니다. OpenManage Integration for VMware vCenter의 vCenter 메뉴 아래에는 OpenManage Integration for VMware vCenter의 기본 액세스 지점 역할을 하는 특별한 그룹이 있습니다.
기본 콘텐츠	탐색 창에서 선택한 보기를 표시합니다. 기본 콘텐츠 창은 대부분의 콘텐츠가 표시되는 영역입니다.
알림	진행 중인 vCenter 알람 및 작업을 표시합니다. OpenManage Integration for VMware vCenter는 vCenter의 알람, 이벤트 및 작업 시스템을 통합하여 알림 창에 해당 정보를 표시합니다.

주제:

VMware vCenter 웹 클라이언트에서 탐색

OpenManage Integration for VMware vCenter는 VMware vCenter 내의 특별한 **Dell EMC** 그룹에 있습니다.

1. VMware vCenter에 로그인합니다.
2. VMware vCenter 홈 페이지에서 **OpenManage Integration** 아이콘을 클릭합니다.

   여기에서 다음을 수행할 수 있습니다.

   - 기본 콘텐츠 창의 탭에서 OpenManage Integration for VMware vCenter 연결 프로필과 제품 설정을 관리하고 요약 페이지는 보는 등의 작업을 수행할 수 있습니다.
   - 탐색 창의 **vCenter 인벤토리가 목록**에서 호스트, 데이터 센터 및 클러스터를 모니터링합니다. 조사할 호스트, 데이터 센터 또는 클러스터를 선택한 다음 **개체** 탭에서 모니터링을 위해 선택한 개체를 클릭합니다.

웹 클라이언트에 있는 아이콘

제품 사용자 인터페이스에서는 수행되는 조치에 여러 가지 아이콘 기반 조치 단추가 사용됩니다.

표 4. 정의된 아이콘 단추

아이콘 단추	정의
	새 항목을 추가 또는 생성
	연결 프로필, 데이터 센터 및 클러스터에 서버 추가
	작업 중단
	목록 축소
	목록 확장
	개체 삭제
	예약 변경
	편집
	작업 제거
	파일 내보내기
	시스템 프로필 보기
	필터
	지금 실행

소프트웨어 버전 찾기

소프트웨어 버전은 OpenManage Integration for VMware vCenter의 **시작하기** 탭에서 확인할 수 있습니다.

1. VMware vCenter 홈 페이지에서 **OpenManage Integration** 아이콘을 클릭합니다.
2. OpenManage Integration for VMware vCenter의 **시작하기** 탭에서 **버전 정보**를 클릭합니다.
3. **버전 정보** 대화 상자에서 버전 정보를 확인합니다.
4. 대화 상자를 닫으려면 **OK(확인)**를 클릭합니다.

화면 콘텐츠 새로 고침

VMware vCenter **새로 고침** 아이콘을 사용하여 화면을 새로 고칠 수 있습니다.

1. 새로 고칠 페이지를 선택합니다.
2. VMware vCenter 제목 표시줄에서 **새로 고침(Ctrl+Alt+R)** 아이콘을 클릭합니다.
   새로 고침 아이콘은 검색 영역 오른쪽에 있으며 시계 방향 화살표 모양으로 표시됩니다.

Dell EMC 호스트 보기

Dell EMC 호스트만 빠르게 보려면 OpenManage Integration for VMware vCenter의 탐색 창에서 **Dell EMC 호스트**를 선택합니다.

1. VMware vCenter 홈 페이지에서 **OpenManage Integration** 아이콘을 클릭합니다.
2. **탐색**의 **OpenManage Integration**에서 **Dell EMC 호스트**를 클릭합니다.
3. **Dell EMC 호스트** 탭에서 다음과 같은 정보를 볼 수 있습니다.
   - **호스트 이름** - 각 Dell 호스트의 IP 주소를 사용하여 링크를 표시합니다. Dell 호스트 정보를 보려면 특정 호스트 링크를 클릭합니다.
   - **vCenter** - 이 Dell EMC 호스트의 vCenter IP 주소를 표시합니다.

- **클러스터** - Dell EMC 호스트가 클러스터에 있는 경우 클러스터 이름을 표시합니다.
- **연결 프로필** - 연결 프로필 이름을 표시합니다.

OpenManage Integration for VMware vCenter 라이센싱 탭 보기

OpenManage Integration for VMware vCenter 라이센스를 설치하면 다수의 지원되는 호스트 및 vCenter 서버가 이 탭에 표시됩니다. 페이지 상단에서도 OpenManage Integration for VMware vCenter의 버전을 확인할 수 있습니다.

라이센싱 중인 페이지에 **라이센스 구입** 링크가 표시됩니다.

라이센스 관리 섹션에 다음과 같은 사항이 표시됩니다.
- **제품 라이센스 포털(디지털 락커)**
- **iDRAC 라이센스 포털**
- **Administration Console**

OpenManage Integration for VMware vCenter의 **라이센싱** 탭에는 다음과 같은 사항이 표시됩니다.

라이센싱 탭 정보	설명
호스트 라이센스	• 사용 가능한 라이센스 사용 가능한 라이센스 수 표시 • 사용 중인 라이센스 사용 중인 라이센스 수 표시
vCenter 라이센스	• 사용 가능한 라이센스 사용 가능한 라이센스 수 표시 • 사용 중인 라이센스 사용 중인 라이센스 수 표시

도움말 및 지원 액세스

OpenManage Integration for VMware vCenter의 **도움말 및 지원** 탭은 제품에 대한 정보를 제공합니다. 이 탭에서 다음과 같은 정보를 볼 수 있습니다.

표 5. 도움말 및 지원 탭에 있는 정보

이름	설명
제품 도움말	다음과 같은 링크를 제공합니다. • **OpenManage Integration for VMware vCenter 도움말** — 제품 내에 있는 제품 도움말에 대한 링크를 제공합니다. 목차를 사용하거나 검색하여 필요한 정보를 찾습니다. • **정보** — 이 링크는 **버전 정보** 대화 상자를 표시합니다. 여기에서 제품 버전을 볼 수 있습니다.
Dell EMC 매뉴얼	다음에 대한 라이브 링크를 제공합니다. • **서버 매뉴얼** • **OpenManage Integration for VMware vCenter 매뉴얼**
Administration Console	Administration Console에 대한 링크를 제공합니다.
추가 도움말 및 지원	다음에 대한 라이브 링크를 제공합니다. • **라이프사이클 컨트롤러가 포함된 iDRAC 매뉴얼** • **Dell VMware 설명서**

표 5. 도움말 및 지원 탭에 있는 정보 (계속)

이름	설명
	• **OpenManage Integration for VMware vCenter 제품 페이지** • **Dell 도움말 및 지원 홈** • **Dell TechCenter**
지원 전화 팁	Dell 지원부에 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 Downloading the troubleshooting bundle(문제 해결 번들 다운로드)을 참조하십시오.
Dell EMC 권장 사항	Dell EMC Repository Manager(DRM)로 연결되는 링크를 제공합니다. DRM을 사용하여 시스템에 사용 가능한 모든 펌웨어 업데이트를 찾아 다운로드합니다.
iDRAC 다시 설정	iDRAC가 응답하지 않을 때 사용할 수 있는 iDRAC를 재설정하기 위한 링크를 제공합니다. 이를 사용하면 iDRAC가 정상적으로 재부팅됩니다.

문제해결 번들 다운로드

노트: 문제해결 번들을 생성하려면 OMIVV에 쓰기 권한이 있는 사용자로 vSphere 웹 클라이언트에 로그인해야 합니다.

문제 해결 번들 정보를 사용하여 문제 해결에 도움을 받거나 기술 지원 팀에 정보를 보낼 수 있습니다. 문제 해결 정보를 얻으려면 다음 단계를 수행합니다.

1. OpenManage Integration for VMware vCenter에서 **도움말 및 지원** 탭을 클릭합니다.
2. **문제 해결 번들**에서 **문제 해결 번들 생성 및 다운로드**를 클릭합니다.
3. **생성** 단추를 클릭합니다.
4. 파일을 저장하려면 **다운로드**를 클릭합니다.
5. **파일 다운로드** 대화 상자에서 **저장**을 클릭합니다.
6. **다른 이름으로 저장** 대화 상자에서 파일을 저장할 위치를 찾아보고 **저장**을 클릭합니다.
7. 종료하려면 **닫기**를 클릭합니다.

iDRAC 다시 설정

iDRAC 재설정 링크에는 **도움말 및 지원** 탭에 있습니다. iDRAC를 재설정하면 iDRAC가 정상적으로 다시 부팅됩니다. iDRAC가 다시 부팅될 때 호스트는 다시 부팅되지 않습니다. 재설정을 수행한 후 사용 가능한 상태로 복원되는 데 최대 2분이 소요됩니다. 재설정 작업은 OpenManage Integration for VMware vCenter에서 iDRAC가 응답하지 않는 경우 수행하십시오.

노트: iDRAC를 재설정하기 전에 호스트를 유지 관리 모드로 전환하는 것이 좋습니다. 한 번 이상 인벤토리 작업이 수행되었고 연결 프로필에 속하는 호스트에 재설정 작업을 적용할 수 있습니다. 재설정 작업을 수행해도 iDRAC가 사용 가능한 상태로 복원되지 않을 수 있습니다. 이러한 경우에는 하드 리셋이 필요합니다. 하드 리셋에 대한 자세한 내용은 iDRAC 설명서를 참조하십시오.

iDRAC를 재부팅하는 동안에 다음과 같은 상황이 발생할 수 있습니다.

- OpenManage Integration for VMware vCenter가 해당 상태를 가져오는 동안 약간의 지연 또는 통신 오류가 발생할 수 있습니다.
- iDRAC와 함께 열려 있는 모든 세션이 닫힙니다.
- iDRAC의 DHCP 주소가 변경될 수 있습니다.

  iDRAC에서 DHCP를 IP 주소로 사용할 경우 IP 주소가 변경됩니다. IP 주소가 변경되면 호스트 인벤토리 작업을 다시 실행하여 인벤토리 데이터에서 새로운 iDRAC IP 주소를 캡처하십시오.

1. OpenManage Integration for VMware vCenter에서 **도움말 및 지원** 탭을 클릭합니다.
2. iDRAC 재설정 아래에서 **iDRAC 재설정**을 클릭합니다.
3. **iDRAC 재설정** 대화 상자의 iDRAC 재설정 아래에 IP 주소/이름을 입력합니다.

4. iDRAC 재설정프로세스를 이해한 후 이를 확인하려면 **iDRAC 재설정을 이해했습니다. iDRAC 재설정을 계속합니다.**를 선택합니다.
5. **iDRAC 재설정**을 클릭합니다.

온라인 도움말 열기

도움말 및 지원 탭에서 온라인 도움말을 열 수 있습니다. 어떤 주제 또는 절차의 이해에 관한 도움말 문서를 검색할 수 있습니다.

1. OpenManage Integration for VMware vCenter의 **도움말 및 지원**에 있는 **제품 도움말**에서 **OpenManage Integration for VMware vCenter 도움말**을 클릭합니다.
   온라인 도움말 콘텐츠가 브라우저 창에 표시됩니다.
2. 왼쪽 창의 목차를 사용하거나 검색을 통해 선택할 주제를 찾습니다.
3. 온라인 도움말을 닫으려면 브라우저 창 오른쪽 위 모서리에 있는 **X**를 클릭합니다.

관리 콘솔 실행

VMware vCenter 웹 클라이언트 내에서 OpenManage Integration for VMware vCenter를 시작한 다음 **도움말 및 지원** 탭에서 관리 콘솔을 열 수 있습니다.

1. OpenManage Integration for VMware vCenter의 **도움말 및 지원** 탭에 있는 **관리 콘솔** 아래에서 콘솔에 연결되는 링크를 클릭합니다.
2. **관리 콘솔** 로그인 대화 상자에서 관리자 암호를 사용하여 로그인합니다.
   관리 콘솔에서 다음과 같은 작업을 수행할 수 있습니다.
   - vCenter를 등록 또는 등록 취소, 자격 증명 수정 또는 인증서 업데이트.
   - 라이센스를 업로드합니다.
   - 등록되어 사용 가능한 vCenter의 개수와 사용 중이고 사용 가능한 최대 호스트 라이센스 개수에 대한 요약 보기.
   - 가상 어플라이언스를 다시 시작합니다.
   - 최신 버전으로 업데이트 또는 업그레이드.
   - 네트워크 설정 표시(읽기 전용 모드).
   - 어플라이언스 업그레이드 또는 `http://downloads.dell.com/published/Pages/index.html`에 연결하기 위해 Dell EMC 서버에 연결하는 HTTP 프록시 설정 구성.
   - NTP 설정을 구성합니다. NTP 서버를 사용 또는 사용 안 함으로 설정하고 기본 및 보조 NTP 서버를 구성합니다.
   - 인증서 서명 요청(CSR)을 생성하거나 인증서를 업로드하거나 HTTPS 인증서에 대한 기본 인증서를 복원합니다.
   - 모든 vCenter 인스턴스 경고를 저장하는 방법에 대한 전역 설정 구성. 저장되는 경고, 경고 보유 일 수, 중복 경고 시간 제한의 최대값을 구성할 수 있습니다.
   - 모든 vCenter 인스턴스 경고를 저장하는 방법에 대한 전역 설정 구성.
   - 백업 또는 복원 시작.
   - 네트워크 공유의 백업 위치 및 백업된 파일의 암호화 암호를 구성합니다(테스트 네트워크 연결과 함께).
   - 반복 백업을 예약합니다.

로그 내역 보기

로그 페이지에서 OMIVV가 생성한 로그를 볼 수 있습니다.

두 개의 드롭다운 목록을 사용하여 이 페이지의 컨텐츠를 필터링 및 정렬할 수 있습니다. 첫 번째 드롭다운 목록을 사용하면 다음 로그 유형을 기준으로 로그 상세정보를 필터링하고 볼 수 있습니다.

- 모든 범주
- 정보
- 경고
- 오류

두 번째 드롭다운 목록을 사용하면 다음 날짜 및 시간 빈도를 기준으로 로그 상세정보를 정렬할 수 있습니다.

- 지난 주
- 지난 달
- 작년
- 사용자 지정 범위
  - **사용자 지정 범위**를 선택할 경우 필터링할 항목을 기반으로 시작 및 종료 날짜를 지정한 다음, **적용**을 클릭할 수 있습니다.

그리드 표에 다음과 같은 정보가 표시됩니다.

- 범주 — 로그 범주 유형 표시
- 날짜 및 시간 — 사용자 조치 날짜 및 시간 표시
- 설명 — 사용자 조치에 대한 설명 표시

데이터 그리드 열은 열 머리글을 클릭하여 오름차순 또는 내림차순으로 정렬할 수 있습니다. **필터** 텍스트 상자를 사용하여 콘텐츠 내에서 검색합니다. 페이지 그리드 하단에 다음과 같은 정보가 표시됩니다.

표 6. 로그 내역

로그 정보	설명
Total items(총 항목 수)	모든 로그 항목의 총 개수 표시.
Items per screen(화면당 항목 수)	현재 페이지에 있는 로그 항목 개수를 표시합니다. 드롭다운 상자를 사용하여 페이지당 항목 수를 설정합니다.
페이지	로그 정보를 확인하는 동안 현재 페이지를 표시합니다. 텍스트 상자에 페이지 번호를 입력하거나 **이전** 및 **다음** 단추를 사용하여 원하는 페이지로 이동합니다.
이전 또는 다음 단추	이전 또는 다음 페이지로 안내.
Export All(모두 내보내기) 아이콘	로그 콘텐츠를 CSV 파일로 내보내기.

로그 보기

1. OpenManage Integration for VMware vCenter에서 **모니터** 탭을 클릭합니다.
2. **로그** 탭에서 OpenManage Integration for VMware vCenter에 대한 사용자 조치를 봅니다. 표시되는 로그에 대한 자세한 내용은 로그 내역을 참조하십시오.
3. 그리드에서 데이터를 정렬하려면 열 머리글을 클릭합니다.
4. 범주 또는 시간 블록으로 정렬하려면 그리드 앞에 있는 드롭다운 목록을 사용합니다.
5. 로그 항목 페이지 간을 이동하려면 **이전** 및 **다음** 단추를 사용합니다.

로그 파일 내보내기

OpenManage Integration for VMware vCenter는 쉼표로 구분된 값(CSV) 파일 형식을 사용하여 데이터 테이블에서 정보를 내보냅니다.

1. OpenManage Integration for VMware vCenter에서 **모니터** 탭을 클릭합니다.
2. 로그 내용을 CSV 파일로 내보내려면 화면 오른쪽 하단에서  아이콘을 클릭합니다.
3. **다운로드 위치 선택** 대화 상자에서 로그 정보를 저장할 위치를 찾아봅니다.
4. **파일 이름** 텍스트 상자에서 기본 이름인 `ExportList.csv`를 수락하거나 확장명이 .CSV인 고유한 파일 이름을 입력합니다.
5. **저장**을 클릭합니다.

5

OpenManage Integration for VMware vCenter 라이센싱

OpenManage Integration for VMware vCenter에는 다음 두 가지 유형의 라이센스가 있습니다.

- 평가판 라이센스 — OMIVV 버전 4.x 어플라이언스의 전원을 처음 켜면, 평가판 라이센스가 자동으로 설치됩니다. 평가 버전에는 OpenManage Integration for VMware vCenter에서 관리되는 호스트(서버) 5개에 대한 평가판 라이센스가 포함되어 있습니다. 이는 11세대 이후의 Dell EMC 서버에만 해당되며, 90일 간의 평가 기간 동안 제공되는 기본 라이센스입니다.
- 표준 라이센스 — 전체 제품 버전에는 vCenter 서버 10개에 대한 표준 라이센스가 포함되어 있으며 OMIVV에서 관리되는 호스트 연결을 원하는 수 만큼 구입할 수 있습니다.

평가판 라이센스를 정식 표준 라이센스로 업그레이드하면, 이메일로 주문 확인서가 전송되며 Dell 디지털 로커에서 라이센스 파일을 다운로드할 수 있습니다. 라이센스 .XML 파일을 로컬 시스템에 저장하고 **Administration Console**을 사용하여 새 라이센스 파일을 업로드합니다.

라이센싱은 다음 정보를 제공합니다.

- 최대 vCenter 연결 라이센스 수 — 등록되어 사용 중인 vCenter 연결은 최대 10개까지 허용됩니다.
- 최대 호스트 연결 라이센스 수 — 구입한 호스트 연결 수입니다.
- 사용 중 — 사용 중인 vCenter 연결 또는 호스트 연결 라이센스 수입니다. 호스트 연결에서 이 숫자는 검색되어 인벤토리 작성된 호스트(또는 서버) 수를 나타냅니다.
- 사용 가능 — 나중에 사용할 수 있는 vCenter 연결 또는 호스트 연결 라이센스의 수입니다.

노트: 표준 라이센스 기간은 3~5년뿐이며 추가 라이센스는 기존 라이센스에 추가되기만 하고 덮어쓰지는 않습니다.

라이센스를 구매하면 Dell 디지털 로커(http://www.dell.com/support/licensing)에서 .XML 파일(라이센스 키)을 다운로드할 수 있습니다. 라이센스 키를 다운로드할 수 없으면 www.dell.com/support/incidentsonline/in/en/indhs1/email/order-support로 이동하여 해당 제품의 지역별 Dell 지원 전화번호를 찾아 Dell 지원 부서에 문의하십시오.

주제:

소프트웨어 라이센스 구입 및 업로드

정식 제품 버전으로 업그레이드할 때까지는 평가판 라이센스를 실행합니다. Dell 웹 사이트를 탐색하고 라이센스를 구입하려면 제품의 **라이센스 구입** 링크를 사용합니다. 라이센스를 구입한 후 **관리 콘솔**을 사용하여 업로드합니다.

노트: **라이센스 구입** 옵션은 평가판 라이센스를 사용하는 경우에만 표시됩니다.

1. OpenManage Integration for VMware vCenter에서 다음 작업 중 하나를 수행합니다.
   - **라이센싱** 탭에서 **소프트웨어 라이센스** 옆에 있는 **라이센스 구입**을 클릭합니다.
   - **시작하기** 탭의 **기본 작업** 아래에서 **라이센스 구입**을 클릭합니다.
2. 라이센스 파일은 Dell 디지털 로커에서 다운로드한 알려진 위치에 저장합니다.
3. 웹 브라우저에 관리 콘솔 URL을 입력합니다.

   `https://<ApplianceIPAddress>` 형식을 사용합니다.
4. **관리 콘솔** 로그인 창에서 암호를 입력하고 **로그인**을 클릭합니다.
5. **라이센스 업로드**를 클릭합니다.
6. **라이센스 업로드** 창에서 **찾아보기**를 클릭하여 라이센스 파일을 탐색합니다.
7. 라이센스 파일을 선택한 다음 **업로드**를 클릭합니다.

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

6

VMware vCenter용 어플라이언스 구성

OMIVV의 기본 설치와 vCenter 등록을 완료한 후에 OMIVV 아이콘을 클릭하면 **초기 구성 마법사**가 표시됩니다. 다음 방법 중 하나를 사용하여 어플라이언스 구성을 진행할 수 있습니다.

- **초기 구성 마법사**를 통해 어플라이언스를 구성합니다.
- OMIVV의 **설정** 탭을 통해 어플라이언스를 구성합니다.

처음 시작할 때 **초기 구성 마법사**를 사용하여 OMIVV 어플라이언스 설정을 구성할 수 있습니다. 이후의 인스턴스에는 **설정** 탭을 사용합니다.

노트: 사용자 인터페이스는 두 방법 모두에서 비슷합니다.

주제:

구성 마법사를 통해 작업 구성

노트: DNS 설정을 변경한 후 OMIVV 관련 작업을 수행하는 동안 웹 통신 오류를 발견하면, 브라우저 캐시를 지우고 웹 클라이언트에서 로그아웃한 다음 다시 로그인 합니다.

구성 마법사를 사용하여 다음과 같은 작업을 보고 수행할 수 있습니다.

- 구성 마법사 시작 페이지를 봅니다.
- vCenter를 선택합니다. vCenter 선택을 참조하십시오.
- 연결 프로필을 생성합니다. 연결 프로필 생성을 참조하십시오.
- 이벤트 및 알람을 구성합니다. 이벤트 및 알람 구성을 참조하십시오.
- 인벤토리 작업을 예약합니다. 인벤토리 작업 예약을 참조하십시오.
- 보증 검색 작업을 실행합니다. 보증 검색 작업 실행을 참조하십시오.

구성 마법사 시작 대화 상자 보기

vCenter 설치 및 등록 후 OMIVV를 구성하려면 다음 단계를 수행하여 **초기 구성 마법사**를 표시합니다.

1. vSphere 웹 클라이언트에서 **홈**을 클릭한 후 **OpenManage Integration** 아이콘을 클릭합니다.
   다음 옵션 중 하나를 수행하여 초기 구성 마법사에 액세스할 수 있습니다.
   - 처음 **OpenManage Integration** 아이콘을 클릭하면 **초기 구성 마법사**가 자동으로 표시됩니다.
   - **OpenManage Integration** > **시작하기**에서 **초기 구성 마법사 시작**을 클릭합니다.
2. **시작** 대화 상자에서 단계를 검토하고 **다음**을 클릭합니다.

vCenter 선택

vCenter 선택 대화 상자에서 다음 vCenter를 구성할 수 있습니다.

- 특정 vCenter
- 등록된 모든 vCenter

vCenter 선택 대화 상자에 액세스하려면 다음을 수행합니다.

1. **초기 구성 마법사**의 **시작** 대화 상자에서 **다음**을 클릭합니다.
2. **vCenter** 드롭다운 목록에서 하나의 vCenter 또는 등록된 모든 vCenter를 선택합니다.
   아직 구성되지 않았거나 환경에 vCenter를 추가한 경우에 vCenter를 선택하십시오. vCenter 선택 페이지를 통해 1개 이상의 vCenter를 선택하여 설정을 구성할 수 있습니다.

3. **연결 프로필 설명** 대화 상자를 계속 진행하려면 **다음**을 클릭합니다.

   노트: 같은 OMIVV 어플라이언스로 등록된 동일한 SSO(Single Sign On)에 속하는 vCenter 서버가 여러 개 있고 단일 vCenter 서버를 선택하여 구성하는 경우 각 vCenter를 구성할 때까지 1~3단계를 반복합니다.

연결 프로필 생성

연결 프로필과 함께 Active Directory 자격 증명을 사용하기 전에 다음을 확인합니다.

- Active Directory에 Active Directory 사용자 계정이 있는지 여부.
- iDRAC 및 호스트가 Active Directory 기반 인증에 맞게 구성되었는지 여부.

연결 프로필은 가상 어플라이언스가 Dell EMC 서버와 통신하기 위해 사용하는 iDRAC 및 호스트 자격 증명을 저장합니다. 각 Dell EMC 서버는 하나의 연결 프로필과 연결되어 있어야 OMIVV Integration for OpenManage vCenter에서 관리할 수 있습니다. 하나의 연결 프로필에 여러 개의 서버를 할당할 수 있습니다. 구성 마법사를 사용하거나 **OpenManage Integration for VMware vCenter** > **설정** 탭에서 연결 프로필을 생성할 수 있습니다. Active Directory 자격 증명을 사용하여 iDRAC 및 호스트에 로그인할 수 있습니다.

노트: iDRAC 및 호스트에 대한 Active Directory 자격 증명이 동일하거나 별개일 수 있습니다.

노트: 추가된 호스트의 수가 연결 프로필 생성을 위한 라이센스 한도를 초과할 경우에는 연결 프로필을 생성할 수 없습니다.

1. **연결 프로필 설명** 대화 상자에서 **다음**을 클릭합니다.
2. **연결 프로필 이름 및 자격 증명** 대화 상자에서 연결 **프로필 이름** 및 선택 사양인 연결 프로필 **설명**을 입력합니다.
3. **연결 프로필 이름 및 자격 증명** 대화 상자의 **iDRAC 자격 증명** 아래에서 Active Directory를 사용하여 또는 사용하지 않고 iDRAC를 구성했는지에 따라 다음 작업 중 하나를 수행합니다.

   노트: iDRAC 계정에 관리 권한이 있어야 펌웨어 업데이트, 하드웨어 프로필 적용, 14세대 서버에 시스템 프로필 적용 및 하이퍼바이저 배포를 수행할 수 있습니다.

   - Active Directory를 사용할 iDRAC IP가 이미 구성되어 있고 Active Directory에 활성화되어 있으면 **Active Directory 사용**을 선택합니다. 그렇지 않으면 iDRAC 자격 증명 구성까지 아래로 스크롤합니다.
     a. **Active Directory 사용자 이름**에 사용자 이름을 입력합니다. 사용자 이름은 도메인/사용자 이름 또는 사용자 이름@도메인 형식 중 하나로 입력합니다. 사용자 이름은 256자로 제한됩니다.
     b. **Active Directory 암호**에 암호를 입력합니다. 암호는 127자로 제한됩니다.
     c. **암호 확인**에 암호를 다시 입력합니다.
     d. 요구 사항에 따라 다음 작업 중 하나를 수행하십시오.
        - iDRAC 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화**를 선택합니다.
        - iDRAC 인증서를 저장하지 않고 이후의 모든 연결에서 인증서 확인을 수행하지 않으려면 **인증서 확인 활성화**를 선택 취소합니다.
   - Active Directory 없이 iDRAC 자격 증명을 구성하려면 다음 작업을 수행합니다.
     a. **사용자 이름**: 사용자 이름을 입력합니다. 사용자 이름은 16자로 제한됩니다. iDRAC를 사용하는 iDRAC의 버전에 대한 사용자 이름 제한사항에 대한 자세한 내용은 해당 설명서를 참조하십시오.
     b. **암호**에 암호를 입력합니다. 암호는 20자로 제한됩니다.
     c. **암호 확인**에 암호를 다시 입력합니다.
     d. 다음 작업 중 하나를 수행합니다.
        - iDRAC 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화**를 선택합니다.
        - iDRAC 인증서를 저장하지 않고 이후의 모든 연결에서 인증서 확인을 수행하지 않으려면 **인증서 확인 활성화**를 선택 취소합니다.
4. **호스트 루트**에서 다음 단계 중 하나를 수행합니다.
   - Active Directory를 사용할 호스트가 이미 구성되어 있고 Active Directory에 활성화되어 있으면 **Active Directory 사용**을 선택하고 다음 단계를 수행합니다. 그렇지 않으면 호스트 자격 증명을 구성합니다.
     a. **Active Directory 사용자 이름**에 사용자 이름을 입력합니다. 사용자 이름은 도메인/사용자 이름 또는 사용자 이름@도메인 형식 중 하나로 입력합니다. 사용자 이름은 256자로 제한됩니다.

        노트: 호스트 사용자 이름과 도메인 제한 사항에 대해서는 다음을 참조하십시오.

        호스트 사용자 이름 요구 사항:

        - 1자에서 64자 사이.
        - 인쇄할 수 없는 문자 사용 불가능.
        - 잘못된 문자 사용 불가능(예: " / \ [ ] : ; | = , + * ?). < > @.

호스트 도메인 요구 사항:

- 1자에서 64자 사이.
- 첫 번째 문자는 반드시 알파벳이어야 합니다.
- 공백을 포함할 수 없습니다.
- 잘못된 문자 사용 불가능(예: " / \ [ ] : ; | = , + * ?). < > @.

b. **Active Directory 암호**에 암호를 입력합니다. 암호는 127자로 제한됩니다.
c. **암호 확인**에 암호를 다시 입력합니다.
d. 다음 작업 중 하나를 수행합니다.
   - 호스트 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화**를 선택합니다.
   - iDRAC 인증서를 저장하지 않고 이후의 모든 연결에서 인증서 확인을 수행하지 않으려면 **인증서 확인 활성화**를 선택 취소합니다.

- Active Directory 없이 호스트 자격 증명을 구성하려면 다음 작업을 수행합니다.
  a. **사용자 이름**에서, 사용자 이름은 **root**로 기본으로 설정되며 변경될 수 없습니다. Active Directory가 설정되면 루트 이외의 Active Directory 사용자를 선택할 수 있습니다.
  b. **암호**에 암호를 입력합니다. 암호는 127자로 제한됩니다.

  노트: OMSA 자격 증명은 ESXi 호스트에 사용된 자격 증명과 동일합니다.

  c. **암호 확인**에 암호를 다시 입력합니다.
  d. 다음 작업 중 하나를 수행합니다.
     - 호스트 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화**를 선택합니다.
     - 호스트 인증서를 저장하지 않고 이후의 모든 연결에서 인증서 확인을 수행하지 않으려면 **인증서 확인 활성화**를 선택 취소합니다.

5. **다음**을 클릭합니다.
6. **연결 프로필 관련 호스트** 대화 상자에서 연결 프로필에 사용할 호스트를 선택하고 **확인**을 클릭합니다.
7. 연결 프로필을 테스트하려면 하나 이상의 호스트를 선택하고 **연결 테스트**를 클릭합니다.

   노트: 이 단계는 선택 사항이며 호스트 및 iDRAC 자격 증명을 확인합니다. 이 단계는 선택 사항이지만 연결 프로필을 테스트하는 것이 좋습니다.

   노트: WBEM 서비스가 비활성화된 ESXi 6.5 이상을 실행하는 모든 호스트에서 테스트 연결에 실패합니다. 이러한 호스트의 경우, 해당 호스트에서 인벤토리를 수행하면 WBEM 서비스가 자동으로 활성화됩니다. 연결 테스트에 실패하더라도, 연결 프로필 마법사 조치를 완료하고 호스트에서 인벤토리를 실행한 뒤 연결 프로필을 다시 테스트합니다.

8. 프로필 생성을 완료하려면 **다음**을 클릭합니다.
   다음을 클릭하면 이 마법사에서 입력한 모든 세부 사항이 저장되고 마법사에서 세부 사항을 수정할 수 없습니다. 구성 마법사에서 구성을 완료한 후에 **관리** > **프로필 연결 프로필** 페이지 이 vCenter 세부 사항에 대한 연결 프로필을 수정하거나 추가로 생성할 수 있습니다. 이 안내서의 **연결 프로필 수정하기** 항목을 참조하십시오..

노트: iDRAC 익스프레스 또는 엔터프라이즈 카드가 없는 서버의 경우 iDRAC 테스트 연결 시 이 시스템에 적용되지 않습니다.

연결 프로필에 호스트를 추가한 후 OMIVV의 IP 주소가 호스트의 iDRAC SNMP 트랩 대상으로 자동 설정되고 OMIVV는 ESXi 6.5 호스트에 대한 웹 기반 엔터프라이즈 관리(WBEM) 서비스를 자동으로 활성화합니다. 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. SNMP 트랩 대상을 재구성 및/또는 WBEM 서비스를 활성화해야 하는 비준수 호스트를 보려면 을 참조하십시오. vSphere 호스트에 대한 준수 보고 및 해결 페이지 116.

인벤토리 작업 예약

OpenManage Integration > **관리** > **설정** 탭에서 구성 마법사 또는 OpenManage Integration을 사용하여 인벤토리 일정을 구성할 수 있습니다.

노트: OMIVV에 계속해서 업데이트된 정보가 표시되도록 하려면 주기적인 인벤토리 작업을 예약하는 것이 좋습니다. 인벤토리 작업은 최소한의 리소스를 사용하며 호스트 성능을 저하시키지 않습니다.

노트: 모든 호스트에 대한 인벤토리가 실행되면 섀시는 자동으로 검색됩니다. 특정 섀시를 섀시 프로필에 추가하면 그 섀시의 인벤토리가 자동으로 실행됩니다. 여러 개의 vCenter가 있는 SSO 환경의 경우 하나의 vCenter에 대한 인벤토리가 예약된 시간에 실행되면 모든 vCenter에서 섀시 인벤토리가 자동으로 실행됩니다.

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. **초기 구성 마법사**의 **인벤토리 일정** 대화 상자에서 **인벤토리 데이터 검색 활성화**가 활성화되어 있지 않으면 활성화합니다. **인벤토리 데이터 검색 활성화**는 기본적으로 활성화되어 있습니다.
2. **인벤토리 데이터 검색 일정**에서 다음 단계를 수행합니다.
   a. 인벤토리를 실행할 각 요일 옆에 있는 확인란을 선택합니다.
   기본적으로 **하루 종일**이 선택되어 있습니다.
   b. **데이터 검색 시간**에 HH:MM 형식으로 시간을 입력합니다.
   입력하는 시간은 로컬 시간입니다. 따라서 가상 어플라이언스 시간대에 인벤토리를 실행하려면 로컬 시간대와 가상 어플라이언스 시간대와의 시차를 계산하여 적절한 시간을 입력하십시오.
   c. 변경 사항을 적용하고 계속하려면 **다음**을 클릭합니다.

   다음을 클릭하면 이 마법사에서 입력한 모든 세부 사항이 저장되며 이 마법사에서 세부 사항을 수정할 수 없습니다. 구성 마법사에서 구성을 완료한 후 **설정** > **관리** 탭에서 호스트의 인벤토리 일정 세부 사항을 수정할 수 있습니다. 자세한 내용은 인벤토리 작업 일정 수정 페이지 52.을 참조하십시오.

보증 검색 작업 실행

OMIVV의 설정 탭에서 보증 검색 작업 구성을 이용할 수 있습니다. 또한 **작업 큐** > **보증**에서 보증 검색 작업을 실행하거나 예약할 수도 있습니다. 예약된 작업은 작업 큐에 나열됩니다. 여러 개의 vCenter 서버가 있는 SSO 환경에서는 vCenter에 대한 보증이 실행되면 모든 vCenter에 대하여 섀시 보증이 자동으로 실행됩니다. 하지만 보증은 섀시 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. **보증 일정** 대화 상자에서 **보증 데이터 검색 활성화**를 선택합니다.
2. **보증 데이터 검색 일정**에서 다음을 수행합니다.
   a. 보증을 실행할 각 요일 옆에 있는 확인란을 선택합니다.
   b. HH:MM 형식으로 시간을 입력합니다.
   입력하는 시간은 로컬 시간입니다. 따라서 가상 어플라이언스 시간대에 인벤토리를 실행하려면 로컬 시간대와 가상 어플라이언스 시간대와의 시차를 계산하여 적절한 시간을 입력하십시오.
3. 변경사항을 수락하고 계속하려면 **다음**을 클릭하여 **이벤트 및 알람** 설정을 계속 진행합니다.
   다음을 클릭하면 이 마법사에서 입력한 모든 세부 사항이 저장되고 마법사에서 세부 사항을 수정할 수 없습니다. 구성 마법사에서 구성을 완료한 후 **설정** 탭에서 보증 작업 일정을 수정할 수 있습니다. 자세한 내용은 보증 작업 일정 수정 페이지 54을 참조하십시오.

이벤트 및 알람 구성

초기 구성 마법사를 사용하거나 이벤트 및 알람의 **설정** 탭에서 이벤트 및 알람을 구성할 수 있습니다. 서버에서 이벤트를 수신하려면 OMIVV를 트랩 대상으로 구성합니다. 12세대 이상의 호스트의 경우 iDRAC에서 SNMP 트랩 대상이 설정되었는지 확인합니다. 12세대 이전 호스트의 경우 OMSA에서 트랩 대상이 설정되었는지 확인합니다.

노트: OMIVV는 12세대 이상의 호스트에 대해 SNMP v1 및 v2 경고를 지원하며 12세대 이전 호스트의 경우 SNMP v1 경고만 지원합니다.

1. **초기 구성 마법사**의 **이벤트 게시 수준**에서 다음 중 하나를 선택합니다.
   - 이벤트 게시 안 함 — 하드웨어 이벤트 차단
   - 모든 이벤트 게시 — 모든 하드웨어 이벤트 게시
   - 위험 및 경고 이벤트만 게시 — 위험 또는 경고 수준의 하드웨어 이벤트만 게시
   - 가상화 관련 위험 및 경고 이벤트만 게시 — 가상화 관련 위험 및 경고 이벤트(즉, 기본 이벤트 게시 수준)만 게시
2. 모든 하드웨어 알람 및 이벤트를 사용하려면 **모든 Dell EMC 호스트에 알람 활성화**를 선택합니다.

   노트: 알람이 활성화된 Dell EMC 호스트가 유지 관리 모드로 전환되어 특정 위험 수준의 이벤트를 알리며 필요한 경우 알람을 수정할 수 있습니다.

   Dell EMC 알람 경고 활성화 대화 상자가 표시됩니다.
3. 변경 사항을 적용하려면 **계속**을 클릭하고 변경 사항을 취소하려면 **취소**를 클릭합니다.

노트: **모든 Dell EMC 호스트에 알람 활성화**를 선택하는 경우에만 이 단계를 완료해야 합니다.

4. 관리되는 모든 Dell EMC 서버에서 기본 vCenter 알람 설정을 복원하려면 **기본 알람 복원**을 클릭합니다.
   변경이 적용되는 데 1분 정도 걸릴 수 있습니다.
   노트: 어플라이언스를 복원한 후에 GUI가 활성화되어 있다 해도 이벤트 및 알람 설정은 활성화되지 않습니다. **설정** 탭에서 **이벤트 및 알람** 설정을 다시 활성화할 수 있습니다.

   노트: BMC 트랩에 메시지 ID가 없어 경고에 OMIVV의 자세한 내용이 포함되지 않습니다.

5. **적용**을 클릭합니다.

설정 탭을 통해 작업 구성

설정 탭을 사용하여 다음과 같은 구성 작업을 보고 수행할 수 있습니다.

- OMSA 링크를 활성화합니다. OMSA 링크 활성화를 참조하십시오.
- 보증 만료 알림 설정을 구성합니다. 보증 만료 알림 설정 구성을 참조하십시오.
- 펌웨어 업데이트 리포지토리를 설정합니다. 펌웨어 업데이트 리포지토리 설정을 참조하십시오.
- 최신 어플라이언스 버전 알림을 구성합니다. 최신 어플라이언스 버전 알림 구성을 참조하십시오.
- 이벤트 및 알람을 구성하고 봅니다. 이벤트 및 알람 구성을 참조하십시오.
- 인벤토리 및 보증 데이터 검색 일정을 봅니다. 인벤토리 및 보증 데이터 검색 일정 보기를 참조하십시오.

어플라이언스 설정

이 섹션에서 OMIVV 어플라이언스에 대해 다음을 구성합니다.

- 보증 만료 알림
- 펌웨어 업데이트 리포지토리
- 최신 어플라이언스 버전 알림
- 배포 자격 증명

보증 만료 알림 설정 구성

1. OpenManage Integration for VMware vCenter의 **관리** > **설정** 탭에 있는 **어플라이언스 설정** 아래에서 **보증 만료 알림**을 클릭합니다.
2. **보증 만료 알림**을 확장하여 다음 사항을 확인합니다.
   - **보증 만료 알림** — 설정이 활성화 또는 비활성화되었는지 여부
   - **경고** — 최초 경고 설정 일 수
   - **위험** — 위험 경고 설정 일 수
3. 보증 만료 경고에 대한 보증 만료 임계값을 구성하려면 **보증 만료 알림**의 오른쪽에 있는 아이콘을 클릭합니다.
4. **보증 만료 알림** 대화 상자에서 다음을 수행합니다.
   a. 이 설정을 활성화하려면 **호스트의 보증 만료 알림 활성화**를 선택합니다.
   확인란을 선택하면 보증 만료 알림이 활성화됩니다.
   b. **최소 일 수 임계값 경고**에서 다음을 수행합니다.
      i. **경고** 드롭다운 목록에서 보증 만료 경고를 수신하기 전의 일 수를 선택합니다.
      ii. **위험** 드롭다운 목록에서 보증 만료 경고를 수신하기 전의 일 수를 선택합니다.
5. **적용**을 클릭합니다.

펌웨어 업데이트 리포지토리 설정

OMIVV **설정** 탭에서 펌웨어 업데이트 리포지토리를 설정할 수 있습니다.

1. OpenManage Integration for VMware vCenter의 **관리** > **설정** 탭에 있는 **어플라이언스 설정**에서 **펌웨어 업데이트 리포지토리** 오른쪽에 있는 아이콘을 클릭합니다.
2. **펌웨어 업데이트 리포지토리** 대화 상자에서 다음 중 하나를 선택합니다.

- **Dell 온라인**—Dell(Ftp.dell.com)의 펌웨어 업데이트 리포지토리를 사용하는 위치에 액세스할 수 있습니다. OpenManage Integration for VMware vCenter는 선택된 펌웨어 업데이트를 Dell 리포지토리에서 다운로드하고 관리되는 호스트를 업데이트합니다.

  노트: 네트워크 설정을 기반으로 프록시 설정을 활성화합니다(네트워크에서 프록시가 필요한 경우).
- **공유 네트워크 폴더**—CIFS 기반 또는 NFS 기반 네트워크 공유에서 펌웨어의 로컬 리포지토리를 사용할 수 있습니다. 이 리포지토리는 Dell에서 주기적으로 배포하는 SUU(Server Update Utility)의 덤프일 수도 있고 DRM을 사용하여 생성된 사용자 지정 리포지토리일 수도 있습니다. 이 네트워크 공유는 OMIVV에서 액세스할 수 있어야 합니다.

  노트: CIFS 공유를 사용하는 경우 리포지토리 암호는 31자를 넘을 수 없습니다.

  노트: 최신 Dell EMC Repository Manager(DRM) 버전 3.0 이상을 사용해야 합니다.

3. **공유 네트워크 폴더**를 선택한 경우 다음과 같은 형식을 사용하여 **카탈로그 파일 위치**를 입력합니다.
   - XML 파일용 NFS 공유 — host:/share/filename.xml
   - gz 파일용 NFS 공유 — host:/share/filename.gz
   - XML 파일용 CIFS 공유 — \\host\share\filename.xml
   - gz 파일용 CIFS 공유 — \\host\share\filename.gz

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

   노트: CIFS 공유를 사용하는 경우 OMIVV가 사용자 이름 및 암호를 입력하라는 메시지를 표시합니다. @, %, 및 , 문자는 공유 네트워크 폴더 사용자 이름 또는 암호에서 사용할 수 없습니다.
4. 다운로드가 완료되면 **적용**을 클릭합니다.

노트: 소스에서 카탈로그를 읽고 OMIVV 데이터베이스를 업데이트하려면 최대 60~90분이 소요될 수 있습니다.

최신 어플라이언스 버전 알림 구성

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

1. OpenManage Integration for VMware vCenter의 **관리 → 설정 탭**에 있는 **어플라이언스 설정**에서 **최신 버전 알림** 오른쪽에 있는 아이콘을 클릭합니다.
   기본적으로 최신 버전 알림은 비활성화되어 있습니다.
2. **최신 버전 알림 및 검색 일정** 대화 상자에서 다음 작업을 수행합니다.
   a. 최신 버전 알림을 활성화하려면 **최신 버전 알림 활성화** 확인란을 선택합니다.
   b. **최신 버전 검색 일정**에서 이 작업 요일을 선택합니다.
   c. **최신 버전 검색 시간**에서 필수 로컬 시간을 지정합니다.
   시간은 현지 시간을 제공합니다. OMIVV 어플라이언스에서 적절한 시간에 이 작업을 실행하기 위한 시간차를 계산해야 합니다.
3. 설정을 저장하려면 **적용**을 클릭하고 설정을 재설정하려면 **지우기**를 클릭합니다. 그리고 작업을 중단하려면 **취소**를 클릭합니다.

배포 자격 증명 구성

배포 자격 증명을 이용하면 OS 배포가 완료될 때까지 자동 검색을 사용하여 검색되는 운영 체제 미설치 시스템과 안전하게 통신하기 위한 자격 증명을 설정할 수 있습니다. iDRAC와의 보안 통신을 위해 OMIVV는 배포 프로세스가 끝날 때까지 초기 검색에서 배포 자격 증명을 사용합니다. OS 배포 프로세스가 완료되면 OMIVV에서 연결 프로필에 제공된 것처럼 iDRAC 자격 증명을 변경합니다. 배포 자격 증명을 변경하면 해당 시점 이후에 검색되는 모든 새 시스템에는 새 자격 증명이 제공됩니다. 하지만 배포 자격 증명을 변경하기 전에 검색된 서버의 자격 증명은 이 변경의 영향을 받지 않습니다.

노트: OMIVV는 프로비저닝 서버 역할을 합니다. 배포 자격 증명을 사용하면 자동 검색 프로세스에서 프로비저닝 서버로 OMIVV 플러그인을 사용하는 iDRAC와 통신할 수 있습니다.

1. OpenManage Integration for VMware vCenter의 **관리** > **설정** 탭에 있는 **어플라이언스 설정**에서 **배포 자격 증명** 오른쪽에 있는 아이콘을 클릭합니다.
2. **운영 체제 미설치 서버 배포용 자격 증명**의 **자격 증명** 아래에서 다음에 대한 값을 입력합니다.
   - **사용자 이름** 텍스트 상자에서 사용자 이름을 입력합니다.

     사용자 이름은 16자 이하여야 합니다(ASCII 표시 가능한 문자만).

- **암호** 텍스트 상자에 암호를 입력합니다.

  암호는 20자 이하여야 합니다(ASCII 표시 가능한 문자만).
- **암호 확인** 텍스트 상자에서 암호를 다시 입력합니다.

  암호가 일치하는지 확인합니다.

3. 지정된 자격 증명을 저장하려면 **적용**을 클릭합니다.

vCenter 설정

이 섹션에서 다음 vCenter 설정을 구성합니다.
- OMSA 링크를 활성화합니다. OMSA 링크 활성화를 참조하십시오.
- 이벤트 및 알람을 구성합니다. 이벤트 및 알람 구성을 참조하십시오.
- 인벤토리 및 보증 데이터 검색 일정을 구성합니다. 인벤토리 및 보증 데이터 검색 일정 보기를 참조하십시오.

OMSA 링크 활성화

OMSA 링크를 활성화하기 전에 OMSA 웹 서버를 설치 및 구성합니다. 사용 중인 OMSA 버전 및 OMSA 웹 서버를 설치하고 구성하는 방법에 대한 지침은 *Dell OpenManage Server Administrator 설치 안내서*를 참조하십시오.

노트: OMSA는 PowerEdge 11세대 이하 서버에서만 필요합니다.

1. OpenManage Integration for VMware vCenter의 **관리** > **설정** 탭에 있는 **vCenter 설정** 아래와 OMSA 웹 서버 URL 오른쪽에 있는 아이콘을 클릭합니다.
2. **OMSA 웹 서버 URL** 대화상자에 URL을 입력합니다.

   HTTPS 및 포트 번호 1311과 함께 전체 URL을 포함해야 합니다.

   https://<OMSA 서버 IP 또는 fqdn>:1311
3. OMSA URL을 모든 vCenter 서버에 적용하려면 **이 설정을 모든 vCenter에 적용**을 선택합니다.

   노트: 이 확인란을 선택하지 않으면 OMSA URL은 하나의 vCenter에만 적용됩니다.
4. 제공한 OMSA URL 링크가 작동하는지 확인하려면 호스트의 **요약** 탭으로 이동하여 **Dell EMC 호스트 정보** 섹션 내에서 OMSA 콘솔 링크가 작동하는지 확인합니다.

이벤트 및 알람 구성

Dell EMC Management Center 이벤트 및 알람 대화 상자에서 모든 하드웨어 알람을 활성화하거나 비활성화합니다. 현재 경고 상태는 vCenter 알람 탭에 표시됩니다. 위험 이벤트는 실제 또는 임박한 데이터 손실이나 시스템 오류를 나타냅니다. 경고 이벤트는 심각한 상태가 아닐 수도 있지만 향후 문제가 가능성이 있음을 나타냅니다. 이벤트 및 알람은 VMware 알람 관리자를 사용하여 활성화할 수도 있습니다. 이벤트는 vCenter 작업과 호스트 및 클러스터 보기의 이벤트 탭에 표시됩니다. 서버에서 이벤트를 수신하기 위해 OMIVV가 트랩 대상으로 구성됩니다. 12세대 이상의 호스트에서는 SNMP 트랩 대상이 iDRAC에서 설정됩니다. 12세대 이전 호스트의 경우 트랩 대상이 OMSA에서 설정됩니다. **관리** > **설정** 탭에서 OpenManage Integration for VMware vCenter를 사용하여 이벤트 및 알람을 구성할 수 있습니다. vCenter **설정** 아래에서 **이벤트 및 알람** 머리글을 확장하여 Dell EMC 호스트의 vCenter 알람(활성화 또는 비활성화) 및 이벤트 게시 수준을 표시합니다.

노트: OMIVV는 12세대 이상의 호스트에 대해 SNMP v1 및 v2 경고를 지원합니다. 12세대 이전의 호스트에 대해서는 OMIVV가 SNMP v1 경고를 지원합니다.

노트: Dell 이벤트를 수신하려면 알람과 이벤트를 모두 활성화합니다.

1. OpenManage Integration for VMware vCenter의 **관리** > **설정** 탭에 있는 **vCenter 설정** 아래에서 **이벤트 및 알람**을 확장합니다. 현재 **Dell EMC 호스트의 vCenter 알람**(활성화 또는 비활성화) 또는 모든 vCenter 알람 및 **이벤트 게시 수준**이 표시됩니다.
2. **이벤트 및 알람** 오른쪽에 있는 아이콘을 클릭합니다.
3. 모든 하드웨어 알람 및 이벤트를 사용하려면 **모든 Dell EMC 호스트에 알람 활성화**를 선택합니다.

   노트: 알람이 활성화된 Dell EMC 호스트가 유지 관리 모드로 전환되어 위험 수준의 이벤트를 알리며 필요에 따라 알람을 수정할 수 있습니다.
4. 관리되는 모든 Dell 서버에서 기본 vCenter 알람 설정을 복원하려면 **기본 알람 복원**을 클릭합니다.

이 단계는 변경 사항이 적용되기까지 1분 정도 걸릴 수 있고 **Dell EMC 호스트에 알람 활성화**를 선택한 경우에만 사용할 수 있습니다.

5. **이벤트 게시 수준**에서 "이벤트 게시 안 함", "모든 이벤트 게시", "위험 및 경고 이벤트만 게시" 또는 "가상화 관련 위험 및 경고 이벤트만 게시" 중 하나를 선택합니다. 자세한 내용은 이벤트, 알람 및 상태 모니터링을 참조하십시오.
6. 설정을 모든 vCenter에 적용하려면 **이 설정을 모든 vCenter에 적용**을 선택합니다.

   노트: 이 옵션을 선택하면 모든 vCenter의 기존 설정을 재정의합니다.

   노트: **설정** 탭의 드롭다운 목록에서 이미 **등록된 모든 vCenter**를 선택한 경우에는 이 옵션을 사용할 수 없습니다.

7. 저장하려면 **적용**을 클릭합니다.

인벤토리 및 보증 데이터 검색 일정 보기

1. OpenManage Integration for VMware vCenter에서 **관리** > **설정** 탭의 **vCenter 설정** 아래에서 **데이터 검색 일정**을 클릭합니다.
   클릭하면 데이터 검색 일정이 확장되어 인벤토리 및 보증에 대한 편집 옵션을 표시합니다.
2. **인벤토리 검색** 또는 **보증 검색**에 대해 아이콘을 클릭합니다.
   인벤토리/보증 데이터 검색 대화 상자에서 인벤토리 또는 보증 검색에 대한 다음 정보를 확인할 수 있습니다.
   - 인벤토리 및/또는 보증 검색 옵션이 활성화되어 있는지 아니면 비활성화되어 있는지 여부
   - 활성화된 요일입니다.
   - 활성화된 시간입니다.
3. 데이터 검색 일정을 편집하려면 인벤토리 작업 일정 수정 또는 보증 작업 일정 수정을 참조하십시오.
4. **데이터 검색 일정**을 다시 클릭하여 인벤토리 및 보증 일정을 축소하고 한 줄을 표시합니다.

SNMP 트랩 커뮤니티 문자열 구성

1. **OpenManage Integration for VMware vCenter**의 **관리** > **설정** 탭에 있는 **어플라이언스 설정**에서 **OMSA SNMP 트랩 커뮤니티 문자열**에 대해 을 클릭합니다.
   OMSA SNMP 트랩 커뮤니티 문자열 설정 대화 상자가 표시됩니다. 기본적으로, SNMP 트랩 커뮤니티 문자열에 **public**이 표시됩니다.
2. 모든 문자열에 대한 **public** 텍스트를 사용자 정의하고 **적용**을 클릭합니다.

   노트: OMIVV를 통해 OMSA를 설치하거나 업그레이드하는 동안 11세대 PowerEdge 서버의 SNMP 트랩 커뮤니티 문자열 구성이 설정됩니다.

7

기준선 탭 사용

기준선 탭을 사용하여 리포지토리 프로필과 클러스터 프로필을 생성할 수 있습니다.

주제:

리포지토리 프로필

리포지토리 프로필에서는 여러 드라이버 또는 펌웨어 리포지토리 프로필을 생성하거나 유지할 수 있습니다. 해당 드라이버 또는 펌웨어 리포지토리 프로필을 다음 목적으로 사용할 수 있습니다.

- vSAN 클러스터의 변경 사항을 식별하는 기준선 프로필.
- vSAN 클러스터 또는 vSAN 클러스터 노드의 드라이버 또는 펌웨어 업데이트.

노트:

- vSAN 환경 전용으로 생성된 사용자 지정 펌웨어 카탈로그를 사용합니다.
- 드라이버 리포지토리 프로필은 최대 10개의 드라이버를 포함할 수 있습니다.

  노트: 오프라인 번들(.zip 파일)이 10개를 초과하지 않도록 하십시오. 더 많은 파일이 있는 경우 드라이버가 임의로 선택됩니다.
- 드라이버 리포지토리 프로필에서는 오프라인 번들의 VIB 형식 비동기 드라이버만 사용합니다(.zip 파일).

  노트: vSAN 요구 사항에 대해 유효성이 검사되는 비동기 VIB 드라이버만 필요합니다. 자세한 내용은 VMware 하드웨어 호환성 매트릭스를 참조하십시오.
- 드라이버 리포지토리 프로필에서 OMIVV에는 CIFS 또는 NFS 공유에 대한 쓰기 액세스 권한이 필요합니다.
- 드라이버 리포지토리 프로필에서 하위 폴더 내 파일 또는 10MB 크기를 초과하는 파일은 무시됩니다.
- 구문 분석 성공 후에만, 리포지토리 프로필을 **기준선 프로필**에서 사용하거나 vSAN 드라이버 또는 펌웨어 업데이트 작업을 실행할 수 있습니다.
- 둘 이상의 펌웨어 버전을 사용할 수 있는 경우, 항상 가장 최근의 펌웨어 버전이 준수 비교에 사용됩니다.

리포지토리 프로필 페이지를 실행하려면 다음 단계를 수행합니다.

1. **OpenManage Integration for VMware vCenter** 페이지에서 **관리** > **기준선** 탭을 클릭하고 **기준선 정보**를 확장한 다음, **리포지토리 프로필**을 클릭합니다.
   a. 생성한 리포지토리 프로필 목록을 **리포지토리 프로필** 페이지에서 확인합니다.

      리포지토리 프로필이 **프로필 이름**, **설명**, **유형**, **공유 경로**, **마지막 업데이트 시간** 및 **마지막 새로 고침 상태**와 함께 나열된 표가 표시됩니다.

   b. 리포지토리 프로필의 자세한 내용을 보려면 원하는 리포지토리 프로필을 선택합니다.

      프로필 이름, **공유 경로**, **생성 날짜**, **수정 날짜** 및 **마지막으로 수정한 사람**과 같은 리포지토리 프로필 정보가 표시됩니다.

   c. 데이터 그리드 안에서 열을 바꾸려면 데이터 그리드 내에서 열을 끌어 놓습니다.
   d. 데이터 그리드의 내용을 필터링하거나 검색하려면 **필터** 필드에 필터 조건을 입력합니다.
   e. 리포지토리 프로필 정보를 .CSV 파일로 내보내려면 리포지토리 프로필을 선택하고 데이터 그리드의 오른쪽 모서리에서  를 클릭합니다.

리포지토리 프로필 생성

1. **OpenManage Integration for VMware vCenter** 페이지에서 **관리** > **기준선**을 클릭하고 **기준선 정보**를 확장한 다음, **리포지토리 프로필**을 클릭합니다.
2. ✚을 클릭합니다.
3. **시작** 페이지에서 지침을 읽고 **다음**을 클릭하여 자세한 내용을 다음과 같이 추가합니다.
   a. **프로필 이름** 상자에서 리포지토리 프로필 이름을 입력합니다.
   b. **프로필 설명** 상자에서 설명을 입력합니다(선택 사항).
   c. **다음**을 클릭합니다.
4. **프로필 설정** 대화 상자에서 다음 리포지토리 유형 중 하나를 선택합니다.
   - 펌웨어(기본적으로 이 옵션은 선택되어 있음)
   - 드라이버
   a. **리포지토리 공유 위치** 필드에서 리포지토리 공유 위치(CIFS 또는 NFS)를 입력합니다.
   b. CIFS 공유의 경우 사용자 이름과 암호를 입력합니다. 암호에 사용할 수 없는 문자는 &, !, @, % 및 <입니다.
      노트: OMIVV에서는 SMB(Server Message Block) 버전 1.0과 SMB 버전 2.0 기반 CIFS 공유만 지원됩니다.
   c. 제공된 리포지토리 경로에 대한 액세스 권한과 펌웨어 및 드라이버 리포지터리용 카탈로그 파일 존재를 확인하려면 **테스트 시작**을 클릭합니다. 계속 진행하려면 이 유효성 검사가 필요합니다.

      : 테스트 연결 성공을 나타냅니다.

      : 테스트 연결 실패를 나타냅니다.
   d. **다음**을 클릭합니다.

   노트: 드라이버 리포지토리의 경우, 오프라인 드라이버 .zip 파일을 다운로드하여 공유 위치에 저장하고 공유 위치의 전체 경로를 제공합니다. OMIVV에서 OMIVV 어플라이언스 내부에 카탈로그를 자동으로 생성합니다. VIB 드라이버 번들은 https://my.vmware.com/web/vmware/downloads에서 확인할 수 있습니다.

5. **다음**을 클릭합니다.
   리포지토리 프로필에 관한 정보를 제공하는 **요약** 페이지가 표시됩니다.
6. **마침**을 클릭합니다.
   카탈로그 생성 후, 카탈로그 다운로드 및 구문 분석이 시작되며 리포지토리 프로필의 홈 페이지에 상태가 표시됩니다.

   성공적으로 구문 분석된 리포지토리 프로필은 클러스터 프로필을 작성하는 중에, 그리고 vSAN 펌웨어를 업데이트하는 중에 사용 가능합니다.

리포지토리 프로필 편집

1. **OpenManage Integration for VMware vCenter** 페이지에서 **관리** > **기준선**을 클릭하고 **기준선 정보** 를 확장한 다음, **리포지토리 프로필**을 클릭합니다.
2. 편집하려는 리포지토리 프로필을 선택하고 을 클릭합니다.
3. **리포지토리 프로필** 마법사에서 **프로필 이름**과 **설명**(선택 사항)을 편집하고 **다음**을 클릭합니다.
4. **프로필 설정** 대화 상자에서 다음을 수행합니다.
   a. CIFS 자격 증명을 편집할 수 있습니다.
   b. 제공된 리포지토리 경로에 대한 액세스 권한과 펌웨어 및 드라이버 리포지터리용 카탈로그 파일 존재를 확인하려면 **테스트 시작**을 클릭합니다. 계속 진행하려면 이 유효성 검사가 필요합니다.

      : 테스트 연결 성공을 나타냅니다.

      : 테스트 연결 실패를 나타냅니다.
   c. 지정된 위치에 최근 내용이 있는 리포지토리를 새로 고치려면 **리포지토리 위치와 동기화**를 클릭합니다.

      노트: 기본적으로 ***리포지토리 위치와 동기화*** 옵션이 선택되어 있습니다. 최근 드라이버 또는 펌웨어 카탈로그(공유 위치)에서 카탈로그를 다시 생성하려는 경우 이 옵션이 선택되었는지 확인합니다.

5. **다음**을 클릭합니다.
   리포지토리 프로필에 관한 정보를 제공하는 **요약** 페이지가 표시됩니다.
6. **마침**을 클릭합니다.

리포지토리 프로필 삭제

리포지토리 프로필을 삭제하기 전에 연결된 클러스터 프로필에서 리포지토리 프로필을 연결 해제했는지 확인합니다.

1. **OpenManage Integration for VMware vCenter** 페이지에서 **관리** > **기준선**을 클릭하고 **기준선 정보**를 확장한 다음, **리포지토리 프로필**을 클릭합니다.
2. 삭제하려는 리포지토리 프로필을 선택한 다음, ✖를 클릭합니다.
3. 프로필을 제거하려면 확인 대화 상자에서 **예**를 클릭하고 취소하려면 **아니오**를 클릭합니다.

클러스터 프로필

클러스터 프로필을 사용하면 하드웨어 구성(14세대 서버의 경우에만 해당), 펌웨어 또는 드라이버 버전과 같은 기준 구성을 캡처하고, 기준선에 대한 드리프트를 식별하여 vSAN 클러스터에 대해 원하는 상태를 유지 관리할 수 있습니다.

노트:
- 펌웨어 및 드라이버 리포지토리 프로필은 생성 후 구문 분석을 수행해야만 클러스터 프로필 생성에 사용할 수 있습니다.
- 클러스터 프로필을 생성하면 변경 사항 감지 작업이 트리거됩니다.
- 클러스터가 클러스터 프로필에 연결되면 이전 클러스터 프로필 연관 사항을 덮어씁니다.

클러스터 프로필 페이지를 실행하려면 다음 단계를 수행합니다.

1. **OpenManage Integration for VMware vCenter** 페이지에서 **관리** > **기준선** 탭을 클릭하고 **기준선 정보**를 확장한 다음, **클러스터 프로필**을 클릭합니다.
   a. 생성한 클러스터 프로필 목록을 **클러스터 프로필** 페이지에서 확인합니다.

      클러스터 프로필이 **프로필 이름**, **설명**, **연관된 시스템 프로필**, **연관된 펌웨어 리포지토리 프로필**, **연관된 드라이버 리포지토리 프로필**, **마지막 업데이트 시간**과 함께 나열된 표가 표시됩니다.

      노트: 기존 클러스터 프로필에 대해 사용할 수 있는 최신 버전의 리포지토리 프로필이 있을 경우 연결된 펌웨어 또는 드라이버 프로필에 경고 기호가 표시됩니다.

   b. 클러스터 프로필의 자세한 내용을 보려면 원하는 클러스터 프로필을 선택합니다.

      프로필 이름, **생성 날짜**, **수정 날짜** 및 **마지막으로 수정한 사람**의 자세한 내용이 클러스터 프로필 정보에 표시됩니다.

   c. 데이터 그리드 안에서 열을 바꾸려면 데이터 그리드 내에서 열을 끌어 놓습니다.
   d. 데이터 그리드의 내용을 필터링하거나 검색하려면 **필터**를 사용합니다.
   e. 리포지토리 프로필 정보를 .CSV 파일로 내보내려면 리포지토리 프로필을 선택한 다음, 데이터 그리드의 오른쪽 모서리에서  를 클릭합니다.

클러스터 프로필 생성

1. 시스템 프로필, 펌웨어와 드라이버 모두에 대한 리포지토리 프로필, 클러스터용 동종 서버 모델
2. vSAN 클러스터가 vCenter에 있어야 합니다.
3. vSAN 클러스터에서 1개 이상 호스트의 연결 프로필이 생성되고 인벤토리가 실행되어야 합니다.

노트: 여러 개의 독립 실행형 vCenter가 OMIVV에 등록된 경우 각 vCenter별로 개별 클러스터 프로필을 생성하는 것이 좋습니다.

노트: 클러스터 프로필이 생성될 때 기준선을 위하여 관련된 펌웨어 및 드라이버 리포지토리의 현재 스냅숏이 생성됩니다. 리포지토리가 변경되는 경우에는 변경 사항을 반영하기 위해 클러스터 프로필을 다시 업데이트해야 합니다. 그렇지 않으면 리포지토리에 수행된 업데이트가 원래 클러스터 프로필 스냅숏에 대하여 업데이트되지 않습니다.

1. **OpenManage Integration for VMware vCenter** 페이지에서 **관리** > **기준선**을 클릭하고 **기준선 정보**를 확장한 다음, **클러스터 프로필**을 클릭합니다.

2. ✚을 클릭합니다.
3. **시작** 페이지에서 지침을 읽고 **다음**을 클릭하여 자세한 내용을 다음과 같이 추가합니다.
   a. **프로필 이름** 필드에서 클러스터 프로필 이름을 입력합니다.
   b. **프로필 설명** 필드에서 클러스터 프로필의 설명을 입력합니다. 프로필 설명은 선택 사항입니다.
   c. **다음**을 클릭합니다.
4. **프로필 설정** 대화 상자에서 다음을 수행합니다.
   a. 시스템 프로필이나 리포지토리 프로필(펌웨어 리포지토리 프로필 또는 드라이버 리포지토리 프로필) 또는 해당 프로필의 조합을 선택합니다.

      노트: 시스템 프로필은 14세대 서버에만 적용할 수 있습니다.

      노트: 시스템 프로필, 펌웨어 및 드라이버 리포지토리를 사용해 기준선을 생성하는 것이 좋습니다.

   b. **다음**을 클릭합니다.
5. **프로필 연관** 대화 상자에서 다음을 수행합니다.
   a. 드롭다운 목록에서 등록된 vCenter 서버를 선택합니다.
   b. **찾아보기**를 클릭하여 필요한 vSAN 클러스터를 연결합니다.
   c. **다음**을 클릭합니다.
6. **변경 사항 감지 일정** 대화 상자에서 날짜와 시간을 선택하고 **다음**을 클릭합니다.
   클러스터 프로필에 관한 정보를 제공하는 **요약** 페이지가 표시됩니다.
7. **마침**을 클릭합니다.
   클러스터 프로필이 자동으로 저장되고 **클러스터 프로필** 페이지에 표시됩니다.
   노트: 변경 사항 감지 작업은 클러스터 프로필을 저장한 직후 실행되고 이후에는 예약된 시간 동안 실행됩니다.

클러스터 프로필 편집

노트: 클러스터 프로필을 편집하면 기준선이 변경되며 그에 따라 준수 수준이 재계산될 수 있습니다.

1. **OpenManage Integration for VMware vCenter** 페이지에서 **관리** > **기준선**을 클릭하고 **기준선 정보** 를 확장한 다음, **클러스터 프로필**을 클릭합니다.
2. 편집하려는 클러스터 프로필을 선택하고 ✎을 클릭합니다.
3. **클러스터 프로필** 마법사에서 **설명**(선택 사항)을 편집하고 **다음**을 클릭해도 됩니다.

   노트: 프로필 이름은 편집할 수 없습니다.

4. **프로필 설정** 대화 상자에서 프로필 조합을 변경할 수 있습니다.
5. **프로필 연관** 대화 상자에서 클러스터 프로필에 필요한 연관 사항과 구성을 변경할 수 있습니다.
6. **프로필 구성** 대화 상자에서 **변경 사항 감지 일정**을 편집하고 **다음**을 클릭해도 됩니다.
   클러스터 프로필에 관한 업데이트된 정보를 제공하는 **요약** 페이지가 표시됩니다.
7. **마침**을 클릭합니다.
   업데이트된 클러스터 프로필이 자동으로 저장되고 클러스터 프로필 창에 표시됩니다.

   노트: 변경 사항 감지 작업은 클러스터 프로필을 저장한 직후 실행되고 이후에는 예약된 시간 동안 실행됩니다.

클러스터 프로필 삭제

1. **OpenManage Integration for VMware vCenter** 페이지에서 **관리** > **기준선**을 클릭하고 **기준선 정보**를 확장한 다음, **클러스터 프로필**을 클릭합니다.
2. 삭제하려는 클러스터 프로필을 선택하고 ✖를 클릭합니다.
3. 프로필을 제거하려면 확인 대화 상자에서 **예**를 클릭하고 취소하려면 **아니오**를 클릭합니다.
   클러스터 프로필을 삭제하면 해당 변경 사항 감지 작업도 삭제됩니다.

8

프로필

자격 증명 프로필을 사용하면 연결 프로필과 섀시 프로필을 관리 및 구성할 수 있고 **배포 템플릿**을 사용하면 하드웨어 및 하이퍼바이저 프로필을 관리 및 구성할 수 있습니다.

주제:

연결 프로필 정보

연결 프로필 탭에서 가상 어플라이언스가 Dell 서버와 통신하는 데 사용하는 자격 증명이 포함되어 있는 연결 프로필을 관리하고 구성할 수 있습니다. OpenManage Integration for VMware vCenter에서 관리하려면 각 Dell EMC 서버를 하나의 연결 프로필에만 연결하십시오. 하나의 연결 프로필에 여러 서버를 할당할 수 있습니다. **초기 구성 마법사**를 실행하면 다음 작업을 수행하여 OpenManage Integration for VMware vCenter에서 연결 프로필을 관리할 수 있습니다.

연결 프로필 보기

연결 프로필을 보려면 연결 프로필이 생성되거나 존재하고 있어야 합니다. 하나 이상의 연결 프로필을 생성하면 **연결 프로필** 페이지에서 볼 수 있습니다. OpenManage Integration for VMware vCenter는 프로파일에 제공된 자격 증명을 사용하여 Dell EMC 호스트와 통신합니다.

1. OpenManage Integration for VMware vCenter에서 **관리**를 클릭합니다.
2. **프로필**을 클릭한 다음 **자격 증명 프로필**을 클릭합니다.
3. **자격 증명 프로필**을 확장하여 **연결 프로필** 탭을 클릭합니다.
   생성한 모든 연결 프로필을 볼 수 있습니다.

표 7. 연결 프로필 정보

연결 프로필 필드	설명
프로필 이름	연결 프로필 이름 표시
설명	설명 표시(제공된 경우)
vCenter	컨텍스트에 따라 vCenter의 FQDN 또는 호스트 이름 또는 IP 주소 표시
연결된 호스트	이 연결 프로필과 연결된 호스트를 표시합니다. 둘 이상인 경우 확장 아이콘을 사용하여 모두 표시
iDRAC 인증서 확인	iDRAC 인증서 확인이 활성화되어 있는지 또는 비활성화되어 있는지 표시
호스트 루트 인증서 확인	호스트 루트 인증서 확인이 활성화되어 있는지 또는 비활성화되어 있는지 표시
생성 날짜	연결 프로필이 생성된 날짜 표시
수정 날짜	연결 프로필이 수정된 날짜 표시

표 7. 연결 프로필 정보 (계속)

연결 프로필 필드	설명
마지막으로 수정한 사람	연결 프로필을 수정한 사용자의 상세정보 표시

연결 프로필 생성

하나의 연결 프로필에 여러 개의 호스트를 할당할 수 있습니다. 프로필을 생성하려면 다음 단계를 수행하십시오.

노트: 이 절차를 수행하는 동안 나열되는 vCenter 호스트는 동일한 SSO(Single Sign On)를 사용하여 인증됩니다. vCenter 호스트가 표시되지 않으면 다른 SSO를 사용하고 있거나 5.5 이전 버전의 VMware vCenter를 사용하고 있는 것입니다.

1. OpenManage Integration for VMware vCenter의 **관리** → **프로필** → **자격 증명 프로필** → **연결 프로필** 탭에서 ✚을 클릭합니다.
2. **시작** 페이지에서 지침을 읽고 **다음**을 클릭합니다.
3. **연결 프로필** 페이지에서 다음 세부 정보를 입력합니다.
   a. **프로필** 아래에 **프로필 이름**을 입력하고 원하는 경우 **설명**을 입력합니다.
   b. **vCenter**의 드롭다운 목록에서 프로필을 생성할 vCenter 서버를 선택합니다.
   이 옵션을 사용하면 각 vCenter에 대해 하나의 연결 프로필을 생성할 수 있습니다.
   c. **iDRAC 자격 증명** 영역에서 다음 작업 중 하나를 수행합니다.

      노트: iDRAC 계정에 관리 권한이 있어야 펌웨어 업데이트, 하드웨어 프로필 적용, 하이퍼바이저 배포를 수행할 수 있습니다.

      - Active Directory를 사용할 iDRAC가 이미 구성되어 있고 Active Directory에 대해 활성화되어 있는 경우 **Active Directory 사용**을 선택합니다. 그렇지 않으면 다음 단계로 건너뜁니다.
        - **Active Directory 사용자 이름** 텍스트 상자에 사용자 이름을 입력합니다. 도메인\사용자 이름 또는 사용자 이름@도메인 형식 중 하나로 사용자 이름을 입력합니다. 사용자 이름은 256자로 제한됩니다. 사용자 이름 제한 사항에 대해서는 Microsoft Active Directory 설명서를 참조하십시오.
        - **Active Directory 암호** 텍스트 상자에 암호를 입력합니다. 암호는 127자로 제한됩니다.
        - **암호 확인** 텍스트 상자에 암호를 다시 입력합니다.
        - iDRAC 인증서를 확인하려면 다음 중 하나를 선택합니다.
          - iDRAC 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화**를 선택합니다.
          - 확인을 수행하지 않고 인증서를 저장하지 않으려면 **인증서 확인 활성화**를 선택 취소합니다.
      - Active Directory 없이 iDRAC 자격 증명을 구성하려면 다음 작업을 수행합니다.
        - **사용자 이름** 텍스트 상자에 사용자 이름을 입력합니다. 사용자 이름은 16자로 제한됩니다. 사용 중인 iDRAC 버전에서의 사용자 이름 제한사항을 보려면 iDRAC 설명서를 참조하십시오.

          노트: 로컬 iDRAC 계정에 관리 권한이 있어야 펌웨어 업데이트, 하드웨어 프로필 적용, 하이퍼바이저 배포를 수행할 수 있습니다.
        - **암호** 텍스트 상자에서 암호를 입력합니다. 암호는 20자로 제한됩니다.
        - **암호 확인** 텍스트 상자에 암호를 다시 입력합니다.
        - iDRAC 인증서를 확인하려면 다음 중 하나를 선택합니다.
          - iDRAC 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화**를 선택합니다.
          - 확인을 수행하지 않고 호스트 인증서를 저장하지 않으려면 **인증서 확인 활성화**를 선택하지 마십시오.

   d. **호스트 루트** 영역에서 다음 중 하나를 수행합니다.
      - Active Directory를 사용할 호스트가 이미 구성되어 있고 Active Directory에 활성화되어 있으면 **Active Directory 사용** 확인란을 선택합니다. 그렇지 않으면 호스트 자격 증명 구성 단계로 건너뜁니다.
        - **Active Directory 사용자 이름** 텍스트 상자에 사용자 이름을 입력합니다. 도메인\사용자 이름 또는 사용자 이름@도메인 형식 중 하나로 사용자 이름을 입력합니다. 사용자 이름은 256자로 제한됩니다. 사용자 이름 제한 사항에 대해서는 Microsoft Active Directory 설명서를 참조하십시오.
        - **Active Directory 암호** 텍스트 상자에 암호를 입력합니다. 암호는 127자로 제한됩니다.
        - **암호 확인** 텍스트 상자에 암호를 다시 입력합니다.
        - 인증서를 확인하려면 다음 중 하나를 선택합니다.
          - 호스트 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화**를 선택합니다.
          - 확인을 수행하지 않고 호스트 인증서를 저장하지 않으려면 **인증서 확인 활성화**를 선택하지 마십시오.

- Active Directory 없이 호스트 자격 증명을 구성하려면 다음 작업을 수행합니다.
  - **사용자 이름** 텍스트 상자에서 사용자 이름은 루트입니다.

    루트 사용자 이름은 기본 사용자 이름이며 변경할 수 없습니다.

    노트: Active Directory가 설정된 경우 모든 Active Directory 사용자 이름을 선택할 수 있고 루트가 아닙니다.
  - **암호** 텍스트 상자에 암호를 입력합니다. 암호는 127자로 제한됩니다.
  - **암호 확인** 텍스트 상자에 암호를 다시 입력합니다.
  - 인증서를 확인하려면 다음 중 하나를 선택합니다.
    - 호스트 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화**를 선택합니다.
    - 확인을 수행하지 않고 호스트 인증서를 저장하지 않으려면 **인증서 확인 활성화**를 선택하지 마십시오.

  노트: OMSA 자격 증명은 ESXi 호스트에 사용된 자격 증명과 동일합니다.

4. **다음**을 클릭합니다.
5. **호스트 선택** 대화 상자에서 이 연결 프로필의 호스트를 선택하고 **확인**을 클릭합니다.
6. **연결된 호스트** 페이지에서 필요한 경우 연결 프로필에 대해 하나 이상의 호스트를 추가합니다.

   호스트를 추가하려면 ✚를 클릭하고 호스트를 선택한 다음 **확인**을 클릭합니다.
7. 연결 프로필을 테스트하려면 하나 이상의 호스트를 선택하고 을 클릭합니다.

   노트: 이 단계는 선택 사항이며 호스트 및 iDRAC 자격 증명이 올바른지 여부를 확인하십시오. 이 단계는 선택 사항이지만 연결 프로필을 테스트하는 것이 좋습니다.

   노트: WBEM 서비스가 비활성화된 ESXi 6.5 이상을 실행하는 모든 호스트에서 테스트 연결에 실패합니다. 이러한 호스트의 경우, 해당 호스트에서 인벤토리를 수행하면 WBEM 서비스가 자동으로 활성화됩니다. 연결 테스트에 실패하더라도, 연결 프로필 마법사 조치를 완료하고 호스트에서 인벤토리를 실행한 뒤 연결 프로필을 다시 테스트합니다.
8. 프로필 생성을 완료하려면 **다음**을 클릭합니다.
   iDRAC 익스프레스 또는 엔터프라이즈 카드가 없는 서버의 경우 iDRAC 테스트 연결 시 이 시스템에 **해당되지 않음**이라는 메시지가 표시됩니다.

연결 프로필에 호스트를 추가한 후 OMIVV의 IP 주소가 호스트의 iDRAC SNMP 트랩 대상으로 자동 설정되고 OMIVV는 ESXi 6.5 호스트에 대한 웹 기반 엔터프라이즈 관리(WBEM) 서비스를 자동으로 활성화합니다. 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. SNMP 트랩 대상을 다시 구성하거나 WBEM 서비스를 활성화해야 하는 비준수 호스트를 보려면 비준수 vSphere 호스트 마법사 실행을 참조하십시오.

연결 프로필 수정

연결 프로필을 생성한 후에는 프로필 이름, 설명, 연결된 호스트, iDRAC 및 호스트 자격 증명을 편집할 수 있습니다.

노트: 이 절차를 수행하는 동안 나열되는 **vCenter**는 동일한 SSO(Single Sign On)를 사용하여 인증됩니다. vCenter 호스트를 볼 수 없으면 다른 SSO를 사용하고 있거나 5.5 이전 버전의 VMware vCenter를 사용하고 있는 것입니다.

노트: 인벤토리, 보증 또는 배포 작업이 실행 중일 때 연결 프로필을 업데이트하지 마십시오.

노트: 인벤토리, 보증 또는 배포 작업이 실행 중일 때 연결 프로필과 연결된 호스트를 다른 연결 프로필로 옮기거나 연결 프로필에서 호스트를 제거하지 않도록 하십시오.

1. OpenManage Integration for VMware vCenter에서 **관리**를 클릭합니다.
2. **프로필**을 클릭한 다음 **자격 증명 프로필**을 클릭합니다.
3. **자격 증명 프로필**을 확장한 다음 **연결 프로필**을 클릭합니다.
4. 프로필을 선택하고 을 클릭합니다.
5. **연결 프로필** 창의 **시작** 탭에서 정보를 읽고 **다음**을 클릭합니다.
6. **이름 및 자격 증명** 탭에서 다음 단계를 수행합니다.
   a. **프로필** 아래에 **프로필 이름**을 입력하고 선택 사항인 **설명**을 입력합니다.
   b. **vCenter** 아래에서 이 연결 프로필에 대해 연결된 호스트를 봅니다. 여기에 호스트가 표시되는 이유에 대해 이전 노트를 참조하십시오.
   c. **iDRAC 자격 증명** 아래에서 다음 단계 중 하나를 수행합니다.

- Active Directory를 사용할 iDRAC 계정이 이미 구성되어 있고 Active Directory에 대해 활성화되어 있는 경우 **Active Directory 사용**을 선택합니다.
  - **Active Directory 사용자 이름** 텍스트 상자에 사용자 이름을 입력합니다. 사용자 이름은 `domain\username`, `domain/username` 또는 `username@domain` 형식 중 하나를 입력합니다. 사용자 이름은 256자로 제한됩니다. 사용자 이름 제한 사항에 대해서는 Microsoft Active Directory 설명서를 참조하십시오.
  - **Active Directory 암호** 텍스트 상자에 암호를 입력합니다. 암호는 127자로 제한됩니다.
  - **암호 확인** 텍스트 상자에 암호를 다시 입력합니다.
  - 인증서를 확인하려면 다음 중 하나를 선택합니다.
    - iDRAC 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화**를 선택합니다.
    - 확인을 수행하지 않고 인증서를 저장하지 않으려면 **인증서 확인 활성화**를 선택하지 마십시오.
- Active Directory 없이 iDRAC 자격 증명을 구성하려면 다음을 입력합니다.
  - **사용자 이름** — 도메인\사용자 이름 또는 도메인@사용자 이름 등의 형식 중 하나로 사용자 이름을 입력합니다.

    사용자 이름으로 허용되는 문자는 /(슬래시), &(앰퍼샌드), \(백슬래시), .(마침표), "(따옴표), @(비율에서) 및 %(퍼센트)(127자로 제한)입니다.

    도메인에는 영숫자 문자와 -(대시) 및 .(마침표)를 사용할 수 있습니다(254자 한도). 도메인의 첫 번째와 마지막 문자는 영숫자여야 합니다.
  - **암호** — 암호를 입력합니다.

    암호에는 /(슬래시), &(앰퍼샌드), \(백슬래시), .(마침표) 및 "(따옴표) 등의 문자가 허용되지 않습니다.
  - **암호 확인** — 암호를 재입력합니다.
  - **인증서 확인 활성화**—기본적으로 이 확인란은 선택되어 있지 않습니다. iDRAC 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화**를 선택합니다. 인증서 확인을 수행하지 않고 인증서를 저장하지 않으려면 **인증서 확인 활성화** 확인란을 선택하지 마십시오.

    노트: Active Directory를 사용하는 경우 **인증서 확인 활성화**를 선택합니다.

d. **호스트 루트**에서 다음 작업을 수행합니다.
- Active Directory에 연결된 모든 콘솔에 액세스하려면 **Active Directory 사용** 확인란을 선택합니다.
- **사용자 이름**—기본 사용자 이름은 root이며 수정할 수 없습니다. **Active Directory 사용**이 선택되어 있으면 원하는 Active Directory 사용자 이름을 사용할 수 있습니다.

  노트: 사용자 이름은 root이며 **Active Directory 사용**을 선택하지 않는 경우 이 항목을 수정할 수 없습니다. iDRAC 사용자가 루트 자격 증명을 사용할 필요는 없으며 Active Directory가 설정되어 있는 경우 모두 관리자 권한일 수 있습니다.
- **암호** — 암호를 입력합니다.

  암호에는 /(슬래시), &(앰퍼샌드), \(백슬래시), .(마침표) 및 "(따옴표) 등의 문자가 허용되지 않습니다.
- **암호 확인** — 암호를 재입력합니다.
- **인증서 확인 활성화**—기본적으로 이 확인란은 선택되어 있지 않습니다. iDRAC 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화**를 선택합니다. 인증서 확인을 수행하지 않고 인증서를 저장하지 않으려면 **인증서 확인 활성화** 확인란을 선택하지 마십시오.

  노트: Active Directory를 사용하는 경우 **인증서 확인 활성화**를 선택합니다.

  노트: OMSA 자격 증명은 ESXi 호스트로 사용된 자격 증명과 동일합니다.

  노트: iDRAC 익스프레스 또는 엔터프라이즈 카드가 없는 호스트의 경우 iDRAC 테스트 연결 시 **이 시스템에 해당되지 않음**이라는 메시지가 표시됩니다.

7. **다음**을 클릭합니다.
8. **호스트 선택** 대화 상자에서 이 연결 프로필의 호스트를 선택합니다.
9. **확인**을 클릭합니다.

   연결된 호스트 대화 상자를 사용하면 선택한 서버에서 iDRAC 및 호스트 자격 증명을 테스트할 수 있습니다.
10. 다음 단계 중 하나를 수행합니다.
    - 자격 증명을 테스트하지 않고 연결 프로필을 생성하려면 **마침**을 클릭합니다.
    - 테스트를 시작하려면 확인할 호스트를 선택하고

      

      을 클릭합니다. 다른 옵션은 비활성화됩니다.

노트: WBEM 서비스가 비활성화된 ESXi 6.5 이상을 실행하는 모든 호스트에서 테스트 연결에 실패합니다. 이러한 호스트의 경우, 해당 호스트에서 인벤토리를 수행하면 WBEM 서비스가 자동으로 활성화됩니다. 연결 테스트에 실패하더라도, 연결 프로필 마법사 조치를 완료하고 호스트에서 인벤토리를 실행한 뒤 연결 프로필을 다시 테스트합니다.

테스트가 완료되면 **마침**을 클릭합니다.

- 테스트를 중지하려면 **모든 테스트 중단**를 클릭합니다. **테스트 중단** 대화 상자에서 **확인**을 클릭한 후 **완료**를 클릭합니다.

노트: **수정 날짜** 및 **마지막으로 수정한 사람** 필드에는 웹 클라이언트 인터페이스를 통해 연결 프로필에 대해 수행한 변경사항이 포함되어 있습니다. 해당하는 연결 프로필에서 OMIVV 어플라이언스가 수행하는 모든 변경사항은 이 두 필드 세부 사항에 영향을 미치지 않습니다.

연결 프로필 삭제

노트: 인벤토리, 보증 또는 배포 작업이 실행 중일 때 호스트와 연결된 연결 프로필을 삭제하지 마십시오.

1. OpenManage Integration for VMware vCenter에서 **관리**를 클릭합니다.
2. **프로필**을 클릭한 다음 **자격 증명 프로필**을 클릭합니다.
3. **자격 증명 프로필**을 확장하고 **연결 프로필** 탭을 클릭하여 삭제할 프로필을 선택합니다.
4. ✖를 클릭합니다.
5. 프로필을 제거하려면 삭제 확인 메시지에서 **예**를 클릭하고 삭제 작업을 취소하려면 **아니오**를 클릭합니다.

노트: OMIVV는 삭제한 연결 프로필에 속하는 호스트가 다른 연결 프로필에 추가될 때까지 해당 호스트를 관리하지 않습니다.

노트: 연결 프로필을 삭제하기 전에 예약된 펌웨어 업데이트 작업을 삭제해야 합니다.

연결 프로필 테스트

1. OpenManage Integration for VMware vCenter에서 **관리**를 클릭합니다.
2. **프로필**을 클릭한 다음 **자격 증명 프로필**을 클릭합니다.
3. **자격 증명 프로필**을 확장하고 **연결 프로필** 탭을 클릭하여 연결 프로필을 선택합니다.
4. **연결 프로필 테스트** 대화 상자에서 테스트할 호스트를 선택하고 아이콘을 클릭합니다.
   연결 프로필을 선택하지 않으면 연결 테스트를 실행하는 데 약간의 시간이 소요됩니다.
5. 선택한 모든 테스트를 중지하고 테스트를 취소하려면 **모든 테스트 중단**을 클릭합니다. **테스트 중단** 대화 상자에서 **확인**을 클릭합니다.
6. 종료하려면 **취소**를 클릭합니다.

섀시 프로필 정보

OMIVV는 Dell 서버와 연결된 모든 Dell 섀시를 모니터링할 수 있습니다. 섀시를 모니터링하려면 섀시 프로필이 필요합니다. 다음과 같은 작업을 수행하여 섀시 프로필을 관리할 수 있습니다.

- 섀시 프로필을 봅니다. 섀시 프로필 보기를 참조하십시오.
- 섀시 프로필을 생성합니다. 섀시 프로필 생성을 참조하십시오.
- 섀시 프로필을 편집합니다. 섀시 프로필 편집을 참조하십시오.
- 섀시 프로필을 삭제합니다. 섀시 프로필 삭제를 참조하십시오.
- 섀시 프로필을 테스트합니다. 섀시 프로필 테스트를 참조하십시오.

섀시 프로필 보기

보기 전에 섀시 프로필을 생성하거나 섀시 프로필이 있는지 확인합니다.

1개 이상의 섀시 프로필이 생성되면 섀시 프로필 페이지에서 볼 수 있습니다.

1. OpenManage Integration for VMware vCenter에서 **관리**를 클릭합니다.

2. **프로필**을 클릭한 다음 **자격 증명 프로필**을 클릭합니다.
3. **자격 증명 프로필**을 확장하여 **섀시 프로필** 탭을 클릭합니다.
   섀시 프로필이 표시됩니다.
4. 섀시 프로필에 여러 개의 섀시가 연결되어 있는 경우 연결된 모든 섀시를 표시하려면 아이콘을 클릭합니다.
5. **섀시 프로필** 페이지에서 섀시 정보를 확인합니다.

표 8. 섀시 프로필 정보

섀시 필드	설명
프로필 이름	섀시 프로필 이름 표시
설명	설명 표시(제공된 경우)
섀시 IP/호스트 이름	섀시 또는 호스트 이름의 IP 주소 표시
섀시 서비스 태그	섀시에 할당된 고유 식별자 표시
수정 날짜	섀시 프로필이 수정된 날짜 표시

섀시 프로필 생성

섀시를 모니터링하려면 섀시 프로필이 필요합니다. 섀시 자격 증명 프로필을 생성하여 단일 또는 여러 개의 섀시와 연결할 수 있습니다.

Active Directory 자격 증명을 사용하여 iDRAC 및 호스트에 로그인할 수 있습니다.

1. OpenManage Integration for VMware vCenter에서 **관리**를 클릭합니다.
2. **속성**을 클릭한 다음 **자격 증명 프로필**을 클릭합니다.
3. **자격 증명 프로필**을 확장하여 **섀시 프로필** 탭을 클릭합니다.
4. **섀시 프로필** 페이지에서 아이콘을 클릭하여 **새 섀시 프로필**을 생성합니다.
5. **섀시 프로필 마법사** 페이지에서 다음을 수행합니다.
   이름에 및 자격 증명 섹션의 **섀시 프로필** 아래에서 다음을 수행합니다.
   a. **프로필 이름** 텍스트 상자에서 프로필 이름을 입력합니다.
   b. **설명** 텍스트 상자에 설명(선택 사항)을 입력합니다.
   자격 증명 섹션에서 다음을 수행합니다.
   a. **사용자 이름** 텍스트 상자에 일반적으로 CMC(Chassis Management Controller)에 로그온할 때 사용하는 관리자 권한이 있는 사용자 이름을 입력합니다.
   b. **암호** 텍스트 상자에 사용자 이름에 해당하는 암호를 입력합니다.
   c. **암호 확인** 텍스트 상자에서, **암호** 텍스트 상자에 입력한 것과 동일한 암호를 입력합니다. 이 두 암호는 서로 일치해야 합니다.

   노트: 자격 증명은 로컬 또는 Active Directory 자격 증명일 수 있습니다. 섀시 프로필과 함께 Active Directory 자격 증명을 사용하기 전에 Active Directory에 Active Directory 사용자 계정이 있어야 하며, Active Directory 기반 인증에 맞게 CMC(Chassis Management Controller)를 구성해야 합니다.
6. **다음**을 클릭합니다.
   사용 가능한 모든 섀시를 보여 주는 **섀시 선택** 페이지가 표시됩니다.

   노트: 섀시 아래에 있는 모듈식 호스트의 성공적인 인벤토리 실행 이후에만 해당 섀시가 검색되고 섀시 프로필과 연결할 수 있습니다.
7. 개별 섀시 또는 다중 섀시를 선택하려면 **IP/호스트 이름** 옆의 옆에 있는 해당 확인란을 선택합니다.
   선택한 섀시가 이미 다른 프로필에 속해 있으면 선택한 섀시가 다른 프로필과 연결되어 있음을 나타내는 경고 메시지가 표시됩니다.
   예를 들어, 섀시 A와 연결된 **테스트** 프로필이 있습니다. 다른 프로필 **테스트 1**을 생성하고 섀시 A를 **테스트 1**에 연결하도록 시도하면 경고 메시지가 표시됩니다.
8. **확인**을 클릭합니다.
   연결된 섀시 페이지가 표시됩니다.
9. 섀시의 연결성을 테스트하려면 섀시를 선택하고 아이콘을 클릭하면 자격 증명이 확인되어 섀시의 연결성을 테스트합니다. 결과는 **테스트 결과** 열에 **통과** 또는 **실패**로 표시됩니다.

10. 프로필을 완료하려면 **마침**을 클릭합니다.

섀시 프로필 편집

섀시 프로필을 생성한 후 프로필 이름, 설명, 연결된 섀시 및 자격 증명을 편집할 수 있습니다.

1. OpenManage Integration for VMware vCenter에서 **관리**를 클릭합니다.
2. **프로필**을 클릭한 다음 **자격 증명 프로필**을 클릭합니다.
3. **자격 증명 프로필**을 확장하고 **섀시 프로필** 탭을 클릭하여 섀시 프로필을 선택합니다.
4. 기본 메뉴에서 아이콘을 클릭합니다.
   섀시 프로필 편집 창이 표시됩니다.
5. **섀시 프로필**에서 **프로필 이름** 및 선택 사항인 **설명**을 편집할 수 있습니다.
6. **자격 증명** 영역 아래에서 **사용자 이름**, **암호** 및 **암호 확인**을 편집할 수 있습니다.
   암호 확인에서 입력한 암호는 **암호** 필드에 입력한 암호와 동일해야 합니다. 입력한 자격 증명에는 섀시에 대한 관리자 권한이 있어야 합니다.
7. 변경 사항을 저장하려면 **적용**을 클릭합니다.
   연결된 섀시 탭을 사용하면 선택한 섀시에서 섀시 및 자격 증명을 테스트할 수 있습니다. 다음 단계 중 하나를 수행합니다.
   - 테스트를 시작하려면 검색할 섀시를 하나 또는 여러 개 선택한 후 을 클릭합니다. 옵션을 선택합니다. **테스트 결과** 열에 연결 테스트 성공 여부가 표시됩니다.
   - 섀시 프로필에 하나 또는 여러 개의 섀시를 추가하거나 삭제할 수 있습니다.

   노트: 섀시가 인벤토리화되지 않은 경우 IP/호스트 이름과 서비스 태그만 표시됩니다. 섀시가 인벤토리화되면 **섀시 이름** 및 **모델** 필드가 표시됩니다.

섀시 프로필 삭제

노트: 섀시 프로필을 삭제하기 전에 섀시 인스턴스가 OMIVV가 등록된 다른 vCenter의 일부가 아닌지 확인합니다.

1. OpenManage Integration for VMware vCenter에서 **관리**를 클릭합니다.
2. **프로필**을 클릭한 다음 **자격 증명 프로필**을 클릭합니다.
3. **자격 증명 프로필**을 확장하여 **섀시 프로필** 탭을 클릭합니다.
4. 삭제하려는 섀시 프로필을 선택하고 아이콘을 클릭합니다.
   경고 메시지가 표시됩니다.
5. 삭제를 계속 진행하려면 **예**를 클릭하고 삭제를 취소하려면 **아니오**를 클릭합니다.
   섀시 프로필에 연결된 모든 섀시가 지워졌거나 다른 프로필로 이동한 경우 섀시 프로필에 연결된 섀시가 없으며 삭제되었다는 삭제 확인 메시지가 표시됩니다. 섀시 프로필을 삭제하려면 삭제 확인 메시지에서 **확인**을 클릭합니다.

노트: OMIVV는 삭제한 연결 프로필에 연결된 섀시가 다른 섀시 프로필에 추가될 때까지 해당 섀시를 모니터링하지 않습니다.

노트: 섀시 프로필이 삭제된 경우 연결된 해당 보증 내역 데이터가 보증 내역에서 삭제되지 않습니다.

섀시 프로필 테스트

1. OpenManage Integration for VMware vCenter에서 **관리**를 클릭합니다.
2. **프로필**을 클릭한 다음 **자격 증명 프로필**을 클릭합니다.
3. **자격 증명 프로필**을 확장하여 **섀시 프로필** 탭을 클릭한 다음 테스트할 단일 또는 여러 섀시 프로필을 선택합니다.
   이 작업을 완료하는 데 몇 분 정도 걸립니다.
4. **섀시 프로필 테스트** 대화 상자에서 테스트할 섀시를 선택하고 을 클릭합니다.
5. 선택한 모든 테스트를 중단하고 테스트를 취소하려면 **모든 테스트 중단**을 클릭합니다. **테스트 중단** 대화 상자에서 **확인**을 클릭합니다.
6. 종료하려면 **취소**를 클릭합니다.

9

인벤토리 및 보증 관리

OMIVV를 구성한 후에는 **모니터** 탭에서 인벤토리 및 보증 작업을 모니터링하고, 배포 작업과 펌웨어 업데이트 작업을 관리할 수 있습니다. 인벤토리 및 보증은 **초기 구성 마법사** 또는 **설정** 탭에서 설정합니다.

작업 큐 페이지에서는 다음과 같은 작업을 관리합니다.

- 제출된 서버 배포 또는 펌웨어 업데이트 작업 표시
- 펌웨어 업데이트나 배포 작업 또는 인벤토리/보증 내역 큐 새로 고침
- 인벤토리 또는 보증 작업 예약
- 펌웨어 업데이트 또는 배포 작업 큐 항목 제거

노트: 재고/보증에 최신 정보를 포함하려면 최소한 일주일에 한 번씩 재고/보증 작업을 실행하도록 예약합니다.

이 페이지에서 수행할 수 있는 작업은 다음과 같습니다.

- 배포 작업 관리
- 펌웨어 업데이트 작업 관리
- 인벤토리 작업 관리
- 보증 작업 관리

노트: 언급한 모든 작업에서 어플라이언스 시간이 미래의 날짜로 변경되었고 되돌려진 경우 작업이 모두 다시 예약되었는지 확인하십시오.

노트: 기본 상태 모니터링의 경우에는 OMIVV 어플라이언스를 재부팅해야 합니다. 확장 상태 모니터링의 경우에는 **확장 모니터링**을 비활성화한 다음에 OMIVV 관리 콘솔에서 활성화해야 합니다.

주제:

- 인벤토리 작업
- 보증 작업
- 단일 호스트 모니터링
- 클러스터 및 데이터 센터의 호스트 모니터링
- 실제 서버 깜빡임 표시등 설정
- 시스템 잠금 모드 구성

인벤토리 작업

인벤토리 작업은 **설정** 탭 또는 **초기 구성 마법사**를 사용하여 설정합니다. **인벤토리 내역** 탭을 사용하여 모든 인벤토리 작업을 볼 수 있습니다. 이 탭에서 수행할 수 있는 작업은 다음과 같습니다.

- 호스트 또는 섀시 인벤토리 보기
- 인벤토리 작업 일정 수정
- 지금 섀시 인벤토리 작업 실행

호스트 인벤토리 보기

데이터를 수집하려면 성공적으로 완료된 인벤토리가 필요합니다. 인벤토리가 완료되면 전체 데이터 센터 또는 개별 호스트 시스템에 대한 인벤토리 결과를 볼 수 있습니다. 오름차순 및/또는 내림차순으로 인벤토리 보기 열을 정렬할 수 있습니다.

노트: 다음은 호스트 데이터를 검색 및 표시할 수 없는 몇 가지 가능한 원인입니다.

- 호스트가 연결 프로필과 연관되지 않아 인벤토리 작업을 실행할 수 없습니다.
- 데이터를 수집할 호스트에서 인벤토리 작업이 실행되지 않아 표시할 사항이 없습니다.
- 호스트 라이센스 수가 초과되었으며 인벤토리 작업을 완료하려면 사용 가능한 추가 라이센스가 있어야 합니다.

- 호스트에 PowerEdge 서버 12세대 이후 세대에 필요한 올바른 iDRAC 라이센스가 없으므로 올바른 iDRAC 라이센스를 구입합니다.
- 자격 증명이 올바르지 않을 수 있습니다.
- 호스트에 연결하지 못할 수 있습니다.

호스트 인벤토리 상세정보를 보려면 다음을 수행합니다.

1. OpenManage Integration for VMware vCenter에서 **모니터** 탭을 클릭합니다.
2. **작업 큐**를 클릭하고, **인벤토리 내역**을 확장한 다음 **호스트 인벤토리**를 클릭합니다.
   상단 그리드에 vCenter 정보가 표시됩니다.
3. 선택한 vCenter에서 호스트 정보를 보려면 vCenter를 선택하여 연관된 모든 호스트 세부 정보를 표시합니다.
4. 호스트 인벤토리 정보를 검토합니다.

표 9. vCenter, 호스트 정보

vCenter	
vCenter	vCenter 주소 표시
통과된 호스트	통과된 호스트 표시
마지막 인벤토리	인벤토리 일정을 실행한 날짜 및 시간 표시
다음 인벤토리	다음에 인벤토리 일정을 실행할 날짜 및 시간 표시
호스트	
호스트	호스트 주소를 표시합니다.
상태	상태를 표시합니다. 다음과 같은 옵션을 사용할 수 있습니다. • 성공 • 실패 • 진행 중 • 예약됨
기간(MM:SS)	작업 기간을 분 및 초 단위로 표시
시작 날짜 및 시간	인벤토리 일정이 시작된 날짜 및 시간 표시
종료 날짜 및 시간	인벤토리 일정이 종료된 시간 표시

섀시 인벤토리 보기

데이터를 수집하려면 성공적으로 완료된 인벤토리가 필요합니다. 오름차순 및/또는 내림차순으로 인벤토리 보기 열을 정렬할 수 있습니다.

1. OpenManage Integration for VMware vCenter에서 **모니터** 탭을 클릭합니다.
2. **작업 큐**를 클릭하고, **인벤토리 내역**을 확장한 다음 **섀시 인벤토리**를 클릭합니다.
3. 호스트 인벤토리 정보를 검토합니다.

표 10. 섀시 정보

섀시 인벤토리	
섀시 IP	섀시 IP 주소 표시
서비스 태그	섀시 서비스 태그를 표시합니다. 서비스 태그는 지원 및 유지 관리를 위한 고유한 식별자로 제조업체에서 제공합니다.
상태	섀시 상태 표시
기간(MM:SS)	작업 기간을 분 및 초 단위로 표시
시작 날짜 및 시간	인벤토리 일정이 시작된 날짜 및 시간 표시
종료 날짜 및 시간	인벤토리 일정이 종료된 시간 표시

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

인벤토리 작업 일정 수정

호스트 정보를 최신 상태로 유지하려면 인벤토리 작업이 일주일에 한 번 이상 실행되도록 예약합니다. 인벤토리 작업은 최소한의 리소스를 사용하며 호스트 성능을 저하시키지 않습니다. **초기 구성 마법사** 또는 **모니터** 탭에서 인벤토리 작업 일정을 변경할 수 있습니다.

인벤토리 작업 일정은 인벤토리 작업을 실행할 시간/요일을 설정합니다. 예를 들면 다음과 같습니다.

- 매주 선택한 요일의 지정된 시간
- 설정된 시간 간격

호스트 시스템에서 인벤토리를 수행하려면 통신 및 인증 정보를 제공하는 연결 프로필을 생성합니다.

1. OpenManage Integration for VMware vCenter에서 **모니터** 탭을 클릭합니다.
2. **작업 큐**, **인벤토리 내역**을 클릭한 다음 **호스트 인벤토리**를 클릭합니다.
3. vCenter를 선택한 다음, 을 클릭합니다.
4. **인벤토리 데이터 검색** 대화 상자에서 다음을 수행합니다.
   a. **인벤토리 데이터**에서 **인벤토리 데이터 검색 활성화** 확인란을 선택합니다.
   b. **인벤토리 데이터 검색 일정**에서 작업 요일을 선택합니다.
   c. **인벤토리 데이터 검색 시간** 텍스트 상자에 작업의 로컬 시간을 입력합니다.
   작업 구성 시간과 작업 구현 시간의 차이를 고려해야 합니다.
5. 설정을 저장하려면 **적용**을 클릭하고 설정을 재설정하려면 **지우기**를 클릭합니다. 그리고 작업을 중단하려면 **취소**를 클릭합니다.
6. 지금 작업을 실행하려면 OpenManage Integration for VMware vCenter의 **모니터** > **작업 큐** 탭에서 **인벤토리 내역** > **호스트 인벤토리**를 클릭합니다.
7. 을 클릭하고 **성공** 대화 상자에서 **닫기**를 클릭합니다.

노트: 모듈식 호스트 인벤토리를 실행하면 해당 섀시가 자동으로 검색됩니다. 섀시가 이미 섀시 프로필에 속하는 경우 호스트 인벤토리 후 섀시 인벤토리가 자동으로 실행됩니다.

지금 인벤토리 작업을 예약하면 인벤토리 작업이 큐에 표시됩니다. 단일 호스트에 대해서는 인벤토리를 실행할 수 없습니다. 인벤토리 작업은 모든 호스트에 대해 시작됩니다.

인벤토리 작업 실행

1. **구성 마법사**가 완료되면 연결 프로필에 추가된 모든 호스트에 대해 인벤토리가 자동으로 트리거됩니다. 후속 인벤토리 온디맨드 실행을 하려면 **작업 큐** > **인벤토리** > **지금 실행**을 클릭하여 인벤토리 작업을 실행하십시오.
2. 인벤토리 작업 상태를 확인하려면 **새로 고침**을 클릭합니다.
3. **호스트 및 클러스터** 보기로 이동하여 **Dell EMC 호스트**를 클릭한 다음 **OpenManage Integration** 탭을 클릭합니다. 다음과 같은 정보가 제공됩니다.
   - 개요 페이지
   - 시스템 이벤트 로그
   - 하드웨어 인벤토리
   - 보관 시
   - 펌웨어
   - 전원 모니터링

   노트: 라이센스 한도를 초과하는 호스트의 인벤토리 작업은 건너뛰며 실패로 표시됩니다.

   다음 호스트 명령은 OpenManage Integration 탭 안에서 작동합니다.
   - 깜빡이는 표시등
   - 펌웨어 업데이트 마법사 실행
   - 원격 액세스 실행
   - OMSA 실행
   - CMC 실행
   - 시스템 잠금 모드 구성

지금 섀시 인벤토리 작업 실행

Chassis Inventory(섀시 인벤토리) 탭에서 섀시 인벤토리 작업을 보고 실행할 수 있습니다.

1. OpenManage Integration for VMware vCenter에서 **모니터** 탭을 클릭합니다.
2. **작업 큐**, **인벤토리 내역**을 클릭한 다음 **섀시 인벤토리**를 클릭합니다.
   섀시 목록 및 마지막 인벤토리 작업의 상태가 표시됩니다.
   노트: 예약된 섀시 인벤토리가 예약된 호스트 인벤토리와 동시에 실행됩니다.
3. 을 클릭합니다.
   각 섀시에 대한 **성공** 또는 **실패** 상태와 함께 업데이트되어 인벤토리화된 섀시 목록이 표시됩니다.

보증 작업

하드웨어 보증 정보는 Dell 온라인에서 검색하고 OMIVV에서 표시합니다. 서버의 서비스 태그를 사용하여 서버에 관한 보증 정보를 수집합니다. 보증 데이터 검색 작업은 **초기 구성 마법사**를 사용하여 설정합니다.

이 탭에서 수행할 수 있는 작업은 다음과 같습니다.

- 보증 내역 보기
- 보증 작업 일정 수정
- 지금 호스트 보증 작업 실행
- 지금 섀시 보증 작업 실행

보증 내역 보기

보증 작업은 모든 시스템의 `Support.dell.com`에서 보증 정보를 가져오도록 예약된 작업입니다. 오름차순 및/또는 내림차순으로 인벤토리 보기 열을 정렬할 수 있습니다.

노트: 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. HTTP 프록시 설정 페이지 18을(를) 참조하십시오.

1. OpenManage Integration for VMware vCenter에서 **모니터** 탭을 클릭합니다.
2. **작업 큐**를 클릭한 다음 **보증 내역**을 클릭합니다.
3. **보증 내역**을 확대하여 **호스트 보증** 및 **섀시 보증**을 표시합니다.
4. 해당 보증 작업 내역 정보를 보려면 **호스트 보증**을 선택한 다음, vCenter를 선택하여 연관된 모든 호스트 세부 정보를 표시합니다.

표 11. vCenter, 호스트 내역 정보

vCenter 내역	
vCenters	vCenter 목록 표시
통과된 호스트	통과된 vCenter 호스트 수 표시
마지막 보증	마지막으로 보증 작업을 실행한 날짜 및 시간 표시
다음 보증	실행할 다음 보증 작업의 날짜 및 시간 표시
호스트 내역	
호스트	호스트 주소 표시
상태	상태를 표시합니다. 다음과 같은 옵션을 사용할 수 있습니다. • 성공 • 실패 • 진행 중 • Scheduled
기간(MM:SS)	보증 작업 기간을 MM:SS 단위로 표시
시작 날짜 및 시간	보증 작업이 시작된 날짜 및 시간 표시

표 11. vCenter, 호스트 내역 정보 (계속)

vCenter 내역	
종료 날짜 및 시간	보증 작업이 종료된 날짜 및 시간 표시

섀시 보증 보기

보증 작업은모든 시스템의 `Support.dell.com`에서 보증 정보를 가져오도록 예약된 작업입니다. 오름차순 및/또는 내림차순으로 인벤토리 보기 열을 정렬할 수 있습니다.

1. OpenManage Integration for VMware vCenter에서 **모니터** 탭을 클릭합니다.
2. **작업 큐**를 클릭한 다음 **보증 내역**을 클릭합니다.
3. **보증 내역**을 확대하여 **호스트 보증** 및 **섀시 보증**을 표시합니다.
4. **섀시 보증**을 클릭합니다.
5. 섀시 보증 세부정보를 확인합니다.

표 12. 섀시 정보

섀시 내역	
섀시 IP	섀시 IP 주소 표시
서비스 태그	섀시 서비스 태그를 표시합니다. 서비스 태그는 지원 및 유지 관리를 위한 고유한 식별자로 제조업체에서 제공합니다.
상태	섀시 상태 표시
기간(MM:SS)	보증 작업 기간을 MM:SS 단위로 표시
시작 날짜 및 시간	보증 작업이 시작된 날짜 및 시간 표시
종료 날짜 및 시간	보증 작업이 종료된 날짜 및 시간 표시

보증 작업 일정 수정

보증 작업은 원래 **초기 구성 마법사**에서 구성됩니다. **설정** 탭에서 보증 작업 일정을 수정할 수 있습니다.

1. OpenManage Integration for VMware vCenter에서 **모니터** 탭을 클릭합니다.
2. **작업 큐**를 클릭한 다음 **보증 내역**을 클릭합니다.
3. **보증 내역**을 확대하여 **호스트 보증** 및 **섀시 보증**을 표시합니다.
4. 해당 보증 작업 내역 정보를 보려면 **호스트 보증** 또는 **섀시 보증**을 선택합니다.
5. 을 클릭합니다.
6. **보증 데이터 검색** 대화 상자에서 다음을 수행합니다.
   a. **보증 데이터**에서 **보증 데이터 검색 활성화** 확인란을 선택합니다.
   b. **보증 데이터 검색 일정**에서 보증 작업 요일을 선택합니다.
   c. **보증 데이터 검색 시간** 텍스트 상자에 작업의 로컬 시간을 입력합니다.
   이 작업이 올바른 시간에 실행되는 데 필요한 시간차를 계산해야 합니다.
7. **적용**을 클릭합니다.

지금 호스트 보증 작업 실행

최소한 일주일에 한 번 보증 작업을 실행합니다.

1. OpenManage Integration for VMware vCenter에서 **모니터** 탭을 클릭합니다.
2. **작업 큐**를 클릭한 다음 **보증 내역**을 클릭합니다.
3. **보증 내역**을 확대하여 **호스트 보증** 및 **섀시 보증**을 표시합니다.
4. 해당 보증 작업 내역 정보를 보려면 **호스트 보증** 또는 **섀시 보증**을 선택합니다.

5. 실행하려는 보증 작업을 선택한 다음 ▶을 클릭합니다.
6. **성공** 대화 상자에서 **닫기**를 클릭합니다.
   이제 보증 작업이 큐에서 대기 상태가 됩니다.

노트: 섀시 보증은 호스트 보증이 실행되면 모든 섀시에 대해 자동으로 실행됩니다. 여러 개의 vCenter가 있는 SSO 환경의 경우 하나의 vCenter에 대한 보증을 수동으로 실행하면 모든 vCenter에서 섀시 보증이 자동으로 실행됩니다.

지금 섀시 보증 작업 실행

최소한 일주일에 한 번 보증 작업을 실행합니다.

1. OpenManage Integration for VMware vCenter에서 **모니터** > **작업 큐** 탭으로 이동합니다.
2. 실행하려는 보증 작업을 선택하고 **보증 내역**을 클릭한 다음 **섀시 보증**을 클릭합니다.
3. ▶을 클릭합니다.
4. **성공** 대화 상자에서 **닫기**를 클릭합니다.
   이제 보증 작업이 큐에서 대기 상태가 됩니다.

단일 호스트 모니터링

OpenManage Integration for VMware vCenter를 통해 단일 호스트에 대한 자세한 정보를 볼 수 있습니다. 모든 벤더의 모든 호스트를 표시하는 탐색 창에서 VMware vCenter에 있는 호스트에 액세스할 수 있습니다. 자세한 내용을 보려면 특정 Dell EMC 호스트를 클릭합니다. Dell 호스트 목록을 보려면 OpenManage Integration for VMware vCenter의 탐색 창에서 **Dell EMC 호스트**를 클릭합니다.

호스트 요약 세부 정보 보기

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

- Dell EMC 호스트 상태
- Dell EMC 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. OpenManage Integration for VMware vCenter의 탐색 창에서 **호스트**를 클릭합니다.
2. **개체** 탭에서 보려는 특정 호스트를 선택합니다.
3. **요약** 탭을 클릭합니다.
4. 호스트 요약 세부 정보 보기:

표 13. 호스트 요약 정보

정보	설명
대체 시스템	상태 영역 아래 노란색 상자에 OpenManage Integration for VMware vCenter에 대한 경고가 표시되고 포틀릿을 선행합니다.
알림 영역	오른쪽 창 영역에 Dell 제품 통합 정보가 표시되고, 여기에서 다음에 대한 정보를 확인할 수 있습니다. • 최근 작업 • 진행 중인 작업 • 알람 알림 영역 포틀릿에 Dell 알람 정보가 표시됩니다.

5. 아래로 스크롤하여 Dell EMC 서버 관리 포틀릿을 봅니다.

표 14. Dell EMC 서버 관리 포틀릿

정보	설명
서비스 태그	PowerEdge 서버의 서비스 태그를 표시합니다. 지원 부서에 전화로 문의할 때 이 ID를 사용하십시오.
모델 이름	서버 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 장애 복원 메모리(FRM)를 지원하고 ESXi 5.5 이상 버전을 실행하는 12세대 PowerEdge 서버 이상에 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	14세대 PowerEdge 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 - Dell EMC 호스트 이름 표시 ● 전원 상태 - 전원이 켜져 있는지 아니면 꺼져 있는지 여부 표시 ● iDRAC IP - iDRAC IP 주소 표시 ● 관리 IP - 관리 IP 주소 표시 ● 연결 프로필 - 이 호스트의 연결 프로필 이름 표시 ● 모델 - Dell EMC 서버 모델 표시 ● 서비스 태그 - 장치의 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	관리 콘솔은 외부 시스템 관리 콘솔을 실행하는 데 사용됩니다. 예를 들면 다음과 같습니다. ● 원격 액세스 콘솔(iDRAC) 시작 - Integrated Dell Remote Access Controller(iDRAC) 웹 사용자 인터페이스를 시작합니다. ● OMSA 콘솔 시작 - OMSA 콘솔을 시작하여 OpenManage Server Administrator 사용자 인터페이스에 액세스합니다.

표 14. Dell EMC 서버 관리 포틀릿 (계속)

정보	설명
호스트 조치	다양한 시간 간격으로 깜빡이도록 하려면 실제 서버가 다양한 시간 간격으로 깜빡이도록 설정합니다. 깜박임 표시등을 참조하십시오.

6. Dell EMC 호스트 상태 포틀릿 보기:

표 15. Dell EMC 호스트 상태

정보	설명
Dell EMC 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(주황색 역삼각형과 느낌표)의 두 가지 상태 표시등만이 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: 케이블로 연결된 PSU에 대한 전원 모니터링은 OMIVV에서 사용할 수 없습니다.

단일 호스트에 대한 하드웨어 세부 정보 보기

Dell EMC 호스트 정보 탭에서 단일 호스트에 대한 하드웨어 세부 정보를 볼 수 있습니다. 이 페이지에 정보가 표시되도록 하려면 인벤토리 작업을 실행해야 합니다. 하드웨어 보기는 OMSA 및 iDRAC에서 데이터를 직접 보고합니다. 인벤토리 작업 실행을 참조하십시오.

1. OpenManage Integration for VMware vCenter의 탐색 창에서 **호스트**를 클릭합니다.
2. **호스트** 탭에서 하드웨어의 `<Component Name>` 세부 정보를 확인할 특정 호스트를 선택합니다.
3. **모니터** 탭에서 **Dell EMC 호스트 정보** 탭을 선택합니다.

노트: 14세대 호스트에 대해 시스템 잠금 모드가 켜져 있는 경우, 맨 위에 잠긴 자물쇠 아이콘과 함께 노란색 대역이 표시됩니다.

하드웨어의 `<Component Name>` 하위 탭에서 각 구성 요소에 대해 다음과 같은 정보를 확인합니다.

표 16. 단일 호스트에 대한 하드웨어 세부 정보

하드웨어: *구성 요소*	정보
하드웨어: FRU	• **부품 이름** - FRU 부품 이름 표시 • **부품 번호** - FRU 부품 번호 표시 • **제조업체** - 제조업체 이름 표시 • **일련 번호** - 제조업체의 일련 번호 표시 • **제조일** - 제조일 표시
하드웨어: 프로세서	• **소켓** - 슬롯 번호 표시 • **속도** - 현재 속도 표시 • **브랜드** - 프로세서 브랜드 표시 • **버전** - 프로세서 버전 표시

표 16. 단일 호스트에 대한 하드웨어 세부 정보 (계속)

하드웨어: *구성 요소*	정보
	• **코어** - 이 프로세서의 코어 수 표시
하드웨어: 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 위치 표시(예: 슬롯 1) • **출력(와트)** - 전원 표시(와트)
하드웨어: 메모리	• **메모리 슬롯** - 사용된, 총 및 사용 가능한 메모리 용량 표시 • **메모리 용량** - 설치된 메모리, 총 메모리 용량 및 사용 가능한 메모리 표시 • **슬롯** - DIMM 슬롯 표시 • **크기** - 메모리 크기 표시 • **유형** - 메모리 유형 표시
하드웨어: NIC	• **총** - 사용 가능한 네트워크 인터페이스 카드의 총 개수 표시 • **이름** - NIC 이름 표시 • **제조업체** - 제조업체 이름만 표시 • **MAC 주소** - NIC MAC 주소 표시
하드웨어: PCI 슬롯	• **PCI 슬롯** - 사용된, 총 및 사용 가능한 PCI 슬롯 표시 • **슬롯** - 슬롯 표시 • **제조업체** - PCI 슬롯의 제조업체 이름 표시 • **설명** - PCI 장치에 대한 설명 표시 • **유형** - PCI 슬롯 유형 표시 • **폭** - 데이터 버스 폭 표시(해당되는 경우)
하드웨어: 원격 액세스 카드	• **IP 주소** - 원격 액세스 카드의 IP 주소 표시 • **MAC 주소** - 원격 액세스 카드의 MAC 주소 표시 • **RAC 유형** - 원격 액세스 카드의 유형 표시 • **URL** - 이 호스트와 연관된 iDRAC의 라이브 URL 표시

단일 호스트에 대한 저장소 세부 정보 보기

Dell EMC 호스트 정보 탭에서 단일 호스트에 대한 저장소 세부 정보를 볼 수 있습니다. 이 페이지에 정보가 표시되도록 하려면 인벤토리 작업을 실행해야 합니다. 하드웨어 OMSA 및 iDRAC에서 직접 데이터를 보고합니다. 인벤토리 작업 실행을 참조하십시오. 페이지는 **보기** 드롭다운 목록에서 선택한 사항에 따라 다른 옵션을 표시합니다. **물리 디스크를 선택하는 경우**, 다른 드롭다운 목록이 표시됩니다. 다음 드롭다운 목록을 필터라고 하며 물리 디스크 옵션을 필터링할 수 있습니다. 저장소 세부정보를 보려면 다음을 수행하십시오.

1. OpenManage Integration for VMware vCenter의 탐색 창에서 **호스트**를 클릭합니다.
2. **개체** 탭에서 저장소: 실제 디스크 세부 정보를 확인할 특정 호스트를 선택합니다.
3. **모니터** 탭에서 **Dell EMC 호스트 정보** 탭을 선택합니다.
   저장소 하위 탭에서 다음 사항을 확인합니다.

표 17. 단일 호스트에 대한 저장소 세부 정보

구성 요소	정보
저장소	가상 디스크, 컨트롤러, 엔클로저, 및 전역 핫 스페어 및 전용 핫 스페어 개수와 관련된 물리 디스크의 개수를 표시합니다. 보기 드롭다운 목록에서 선택하면 선택한 옵션이 강조 표시됩니다.
보기	이 호스트에 대해 보려는 옵션을 표시합니다. • 가상 디스크 • 물리 디스크 • 컨트롤러 • 엔클로저

보기 옵션에 대한 저장소 세부 정보 보기

보기 드롭다운 목록에서 선택하는 항목에 따라 **호스트 저장소** 페이지의 저장소 옵션이 달라집니다.

보기 드롭다운 목록에서 언급한 옵션 중 하나를 선택하고 다음 사항을 확인합니다.

표 18. 단일 호스트에 대한 저장소 세부 정보

정보	설명

가상 디스크	• **이름** - 가상 디스크 이름 표시
	• **장치 FQDD** - 장치 FQDD 표시
	• **실제 디스크** - 가상 디스크가 있는 실제 디스크 표시
	• **용량** - 가상 디스크 용량 표시
	• **레이아웃** - 가상 저장소의 레이아웃 유형을 표시합니다. 이 가상 디스크에 구성된 RAID 유형을 의미합니다.
	• **미디어 유형** - SSD 또는 HDD 표시
	• **컨트롤러 ID** - 컨트롤러 ID 표시
	• **장치 ID** - 장치 ID 표시
	• **스트라이프 크기** - 단일 디스크에서 각 스트라이프가 사용하는 공간을 제공하는 스트라이프 크기 표시
	• **버스 프로토콜** - 가상 디스크에 포함된 실제 디스크가 사용하는 기술을 표시합니다. 값은 다음과 같습니다.
	  ○ SCSI
	  ○ SAS
	  ○ SATA
	• **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
	• **캐시 정책** - 캐시 정책이 활성화되어 있는지 여부 표시

물리 디스크 — 이 옵션을 선택하면 **필터** 드롭다운 목록이 표시됩니다.	• **이름** - 실제 디스크 이름 표시 • **장치 FQDD** - 장치 FQDD 표시 • **용량** - 실제 디스크 용량 표시

표 18. 단일 호스트에 대한 저장소 세부 정보 (계속)

정보	설명
다음과 같은 옵션에 따라 물리 디스크를 필터링할 수 있습니다. • 모든 실제 디스크 • 전역 핫 스패어 • 전용 핫 스패어 • 마지막 옵션은 명명된 사용자 지정 가상 디스크를 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 경고 감지됨 ○ 알 수 없음 ○ 외부 ○ 지원되지 않음 • **구성됨** - 디스크가 구성되어 있는지 여부 표시 • **핫 스패어 유형** - 핫 스페어 유형을 표시합니다. 다음과 같은 옵션을 사용할 수 있습니다. ○ 없음 - 핫 스패어가 없음을 의미합니다. ○ 전역 - 디스크 그룹에 속하는 사용되지 않은 백업 디스크 ○ 전용 - 단일 가상 디스크에 할당된 사용되지 않은 백업 디스크입니다. 가상 디스크에서 실제 디스크에 장애가 발생할 경우, 시스템 중단이나 사용자 개입이 없어도 이 핫 스패어가 활성화되어 장애가 발행한 실제 디스크를 대체합니다. • **가상 디스크** - 가상 디스크 이름 표시 • **버스 프로토콜** - 버스 프로토콜 표시 • **컨트롤러 ID** - 컨트롤러 ID 표시 • **커넥터 ID** - 커넥터 ID 표시 • **엔클로저 ID** - 엔클로저 ID 표시 • **장치 ID** - 장치 ID 표시 • **모델** - 실제 저장소 디스크의 모델 번호 표시 • **부품 번호** - 저장소 부품 번호 표시 • **일련 번호** - 저장소 일련 번호 표시 • **공급업체** - 저장소 공급업체 이름 표시
컨트롤러	• **컨트롤러 ID** - 컨트롤러 ID 표시 • **이름** - 컨트롤러 이름 표시 • **장치 FQDD** - 장치 FQDD 표시 • **펌웨어 버전** - 펌웨어 버전 표시 • **최소 필수 펌웨어**- 최소 필수 펌웨어를 표시합니다. 최소 필수 펌웨어를 표시합니다. 이 열은 펌웨어가 오래되고 최신 버전이 사용 가능할 때 채워집니다. • **드라이버 버전** - 드라이버 버전 표시 • **패트롤 읽기 상태** - 패트롤 읽기 상태 표시 • **캐시 크기** - 캐시 크기 표시
엔클로저	• **컨트롤러 ID** - 컨트롤러 ID 표시 • **커넥터 ID** - 커넥터 ID 표시 • **엔클로저 ID** - 엔클로저 ID 표시 • **이름** - 엔클로저 이름 표시 • **장치 FQDD** - 장치 FQDD 표시 • **서비스 태그** - 서비스 태그 표시

웹 클라이언트의 시스템 이벤트 로그 정보

시스템 이벤트 로그(SEL)는 OMIVV에서 검색된 하드웨어의 상태 정보를 제공하고 다음과 같은 기준에 따라 정보를 표시합니다:

상태	여러 상태 아이콘이 있습니다. 정보는 파란색 느낌표, 경고는 느낌표가 있는 노란색 삼각형, 오류는 빨간색 X, 알 수 없음은 물음표(?)가 있는 상자로 표시됩니다.
시간(서버 시간)	이벤트가 발생한 날짜 및 시간을 나타냅니다.
이 페이지 검색	특정 메시지, 서버 이름, 구성 설정 등을 표시합니다.

심각도 수준은 다음과 같이 정의됩니다.

정보	OMIVV 작업이 성공적으로 완료되었습니다.
경고	OMIVV 작업이 일부는 실패하고 일부는 성공했습니다
오류	OMIVV 작업이 실패했습니다.

로그를 외부 CSV 파일로 저장할 수 있습니다. 개별 호스트의 시스템 이벤트 로그 표시를 참조하십시오.

단일 호스트에 대한 이벤트 로그 표시

이벤트를 표시하려면 다음 단계를 수행하십시오.

1. **모니터** 탭에 액세스하고 **시스템 이벤트 로그** 하위 탭을 열려면 다음 단계 중 하나를 수행합니다.

옵션	설명
OMIVV에서	이 옵션의 다음 단계를 수행합니다. a. OpenManage Integration for VMware vCenter의 탐색 창에서 **호스트**를 클릭합니다. b. **개체** 탭에서 SEL 로그를 확인할 특정 호스트를 두 번 클릭합니다.
홈 페이지에서	**홈** 페이지에서 **호스트 및 클러스터**를 클릭합니다.

2. **모니터** 탭에서 **Dell EMC 호스트 정보** > **시스템 이벤트 로그**를 선택합니다.
   최근 시스템 로그 항목에서 10개의 최근 시스템 이벤트 로그 항목을 제공합니다.
3. **시스템 이벤트 로그**를 업데이트하려면 전역 새로 고침을 수행합니다.
4. 이벤트 로그 항목 수를 제한(필터)하려면 다음 옵션 중 하나를 선택합니다.
   - 로그 항목을 동적으로 필터링하려면 검색 필터 텍스트 상자에서 텍스트 문자열을 입력합니다.
   - 필터 텍스트 상자를 지우려면 **X**를 클릭합니다. 그러면 모든 이벤트 로그 항목이 표시됩니다.
5. 모든 이벤트 로그 항목을 지우려면 **로그 지우기**를 클릭합니다.
   모든 로그 항목이 지워진 후 삭제되었음을 알리는 메시지가 표시됩니다. 그러면 다음 옵션 중 하나를 선택할 수 있습니다.
   - 로그 항목 지우기에 동의하려면 **로그 지우기**를 클릭합니다.
   - 취소하려면 **취소**를 클릭합니다.
6. 이벤트 로그를 CSV 파일로 내보내려면  를 클릭합니다.
7. 위치를 찾아서 시스템 이벤트 로그를 저장하려면 **저장**을 클릭합니다.

단일 호스트에 대한 추가 하드웨어 세부 정보 보기

Dell EMC 호스트 정보 탭의 단일 호스트에 대한 펌웨어, 전원 모니터링, 보증 상태 세부 정보를 볼 수 있습니다. 이 페이지에 정보가 표시되도록 하려면 인벤토리 작업을 실행해야 합니다. 하드웨어 보기는 OMSA 및 iDRAC에서 데이터를 직접 보고합니다. 지금 섀시 인벤토리 작업 실행을 참조하십시오.

1. OpenManage Integration for VMware vCenter의 탐색 창에서 **호스트**를 클릭합니다.
2. **개체** 탭에서 `<Component Name>` 세부 정보를 확인할 특정 호스트를 선택합니다.
3. **모니터** 탭에서 **Dell EMC 호스트 정보** 탭을 선택합니다.
   하드웨어의 `<Component Name>` 하위 탭에서 각 구성 요소에 대해 다음과 같은 정보를 확인합니다.

표 19. 단일 호스트 정보

구성 요소	정보
펌웨어 호스트 페이지에서 검색 및 필터를 사용하고 펌웨어 정보의 CSV 파일을 내보낼 수 있음	• **이름** - 이 호스트에 있는 모든 펌웨어 이름 표시 • **유형** - 펌웨어 유형 표시 • **버전** - 이 호스트에 있는 모든 펌웨어 버전 표시 • **설치일** - 설치일 표시
전원 모니터링 **노트:** 여기에서 사용되는 호스트 시간은 호스트가 있는 로컬 시간을 의미합니다.	• **일반 정보** - 전원 예산 및 현재 프로필 이름 표시 • **임계값** - 경고 및 오류 임계값 표시(와트) • **전원 예비 용량** - 순간 및 최고 전원 예비 용량 표시(와트) **에너지 통계** • **유형** - 에너지 통계 유형 표시 • **측정 시작 시간(호스트 시간)** - 호스트가 전원을 사용하기 시작한 날짜 및 시간 표시 • **측정 종료 시간(호스트 시간)** - 호스트가 전원 사용을 중지한 날짜 및 시간 표시 • **측정값** - 1분 이상 동안의 평균 측정값 표시 • **최고 시간(호스트 시간)** - 호스트가 최대 암페어를 사용한 날짜 및 시간 표시 • **최고 측정값** - 시스템 최대 전원 통계(즉, 시스템에서 소비한 최대 전원) 표시(와트)
보증 **노트:** 보증 상태를 보려면 보증 작업을 실행해야 합니다. 보증 검색 작업 실행을 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 경고를 설정하여 보증 설정을 제어합니다.	• **공급자** - 보증 공급자 이름 표시 • **설명** - 설명 표시 • **시작일** - 보증 시작 날짜 표시 • **종료일** - 보증 종료 날짜 표시 • **남은 일 수** - 남은 보증 일 수 표시 • **마지막 업데이트** - 마지막으로 보증을 업데이트한 시간

클러스터 및 데이터 센터의 호스트 모니터링

OpenManage Integration for VMware vCenter에서 데이터 센터 또는 클러스터에 포함된 모든 호스트에 대한 상세 정보를 볼 수 있습니다. 데이터 그리드 행 헤더를 클릭하여 데이터를 정렬할 수 있습니다. 데이터 센터 및 클러스터 페이지에서는 정보를 CSV 파일로 내보낼 수 있으며 데이터 그리드에 대한 필터 또는 검색 기능을 제공합니다.

데이터 센터 및 클러스터 개요 보기

Dell 데이터센터/클러스터 정보 탭에서 데이터센터 또는 클러스터의 호스트 세부 정보를 봅니다. 이 페이지에 정보가 표시되도록 하려면 인벤토리 작업을 실행해야 합니다. 표시되는 데이터는 데이터에 액세스하는 보기에 따라 다를 수 있습니다. 하드웨어 보기는 OMSA 및 iDRAC에서 데이터를 직접 보고합니다. 인벤토리 작업 실행을 참조하십시오.

노트: 데이터 센터 및 클러스터 페이지에서는 정보를 CSV 파일로 내보낼 수 있으며, 데이터 그리드에 필터 또는 검색 기능을 제공합니다.

1. OpenManage Integration for VMware vCenter의 탐색 창에서 **vCenter**를 클릭합니다.
2. **데이터센터** 또는 **클러스터**를 클릭합니다.
3. **개체** 탭에서 호스트 세부 정보를 확인할 특정 데이터센터 또는 클러스터를 선택합니다.
4. **모니터** 탭에서 **Dell EMC 데이터센터/클러스터 정보** > **개요** 탭을 선택하여 세부 정보를 봅니다.

   노트: 전체 세부 정보 목록을 표시하려면 데이터 그리드에서 특정 호스트를 선택하십시오.

표 20. 데이터 센터 및 클러스터 개요

정보	설명
데이터센터/클러스터 정보	다음을 표시합니다.

표 20. 데이터 센터 및 클러스터 개요 (계속)

정보	설명
	• 데이터센터/클러스터 이름 • Dell의 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 • 해당되지 않음(14세대 서버의 경우만 해당)
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 • 알 수 없는 보증
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)
OS 버전	ESXi OS 버전 표시
위치	블레이드의 경우: 슬롯 위치를 표시합니다. 기타의 경우 “적용되지 않음”으로 표시됩니다.
시스템 잠금 모드	14세대 PowerEdge 서버에만 해당: 호스트의 iDRAC 잠금 모드를 켜기, 끄기 또는 알 수 없음으로 표시합니다. 14세대 이전 모든 PowerEdge 서버는 시스템 잠금 모드 표시에 해당되지 않습니다.
iDRAC IP	iDRAC IP 주소 표시
서비스 콘솔 IP	서비스 콘솔 IP 표시
CMC URL	블레이드 서버의 섀시 URL, 즉 CMC URL을 표시하거나, 그렇지 않으면 "적용되지 않음" 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
연결 프로필	연결 프로필 이름 표시
원격 액세스 카드 버전	원격 액세스 카드 버전 표시
BIOS 펌웨어 버전	BIOS 펌웨어 버전 표시

데이터 센터 및 클러스터에 대한 하드웨어 세부 정보 보기

Dell EMC 데이터 센터/클러스터 정보 탭에서 단일 호스트에 대한 하드웨어 세부 정보를 볼 수 있습니다. 이 페이지에 정보가 표시되도록 하려면 인벤토리 작업을 실행해야 합니다. 데이터 센터 및 클러스터 페이지에서는 정보를 CSV 파일로 내보낼 수 있으며 데이터 그리드에 필터/검색 기능을 제공합니다. 표시되는 데이터는 데이터에 액세스하는 보기에 따라 다를 수 있습니다. 하드웨어 보기는 OMSA 및 iDRAC에서 데이터를 직접 보고합니다. 인벤토리 작업 실행을 참조하십시오.

1. OpenManage Integration for VMware vCenter의 탐색 창에서 **vCenter 인벤토리 목록**을 클릭합니다.
2. **데이터센터** 또는 **클러스터**를 클릭합니다.
3. **개체** 탭에서 구성 요소별 세부 정보를 확인할 특정 데이터 센터 또는 클러스터를 선택합니다.
4. **모니터** 탭에서 **Dell EMC 데이터센터/클러스터 정보** 탭을 선택합니다.
   하드웨어의 `<Component Name>` 하위 탭에서 각 구성 요소에 대해 다음과 같은 정보를 확인합니다.

표 21. 데이터 센터 및 클러스터에 대한 하드웨어 정보

하드웨어: *구성 요소*	정보
하드웨어: FRU	• **호스트** - 호스트 이름 표시 • **서비스 태그** - 호스트의 서비스 태그 표시 • **부품 이름** - FRU 부품 이름 표시 • **부품 번호** - FRU 부품 번호 표시 • **제조업체** - 제조업체 이름 표시 • **일련 번호** - 제조업체의 일련 번호 표시 • **제조일** - 제조일 표시
하드웨어: 프로세서	• **호스트** - 호스트 이름 표시 • **서비스 태그** - 호스트의 서비스 태그 표시 • **소켓** - 슬롯 번호 표시 • **속도** - 현재 속도 표시 • **브랜드** - 프로세서 브랜드 표시 • **버전** - 프로세서 버전 표시 • **코어** - 이 프로세서의 코어 수 표시

하드웨어: 전원 공급 장치	• **호스트** - 호스트 이름 표시
	• **서비스 태그** - 호스트의 서비스 태그 표시
	• **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 위치 표시(예: 슬롯 1)
	• **출력(와트)** - 전원 표시(와트)
	• **상태** — 전원 공급 장치의 상태를 표시합니다. 상태 옵션은 다음과 같습니다.
	  ○ 기타
	  ○ 알 수 없음
	  ○ 양호
	  ○ 위험
	  ○ 위험하지 않음
	  ○ 복구 가능
	  ○ 복구 불가능
	  ○ 높음

표 21. 데이터 센터 및 클러스터에 대한 하드웨어 정보 (계속)

하드웨어: *구성 요소*	정보
	○ 낮음
하드웨어: 메모리	• **호스트** - 호스트 이름 표시 • **서비스 태그** - 호스트의 서비스 태그 표시 • **슬롯** - DIMM 슬롯 표시 • **크기** - 메모리 크기 표시 • **유형** - 메모리 유형 표시
하드웨어: NIC	• **호스트** - 호스트 이름 표시 • **서비스 태그** - 호스트의 서비스 태그 표시 • **이름** - NIC 이름 표시 • **제조업체** - 제조업체 이름만 표시 • **MAC 주소** - NIC MAC 주소 표시
하드웨어: PCI 슬롯	• **호스트** - 호스트 이름 표시 • **서비스 태그** - 호스트의 서비스 태그 표시 • **슬롯** - 슬롯 표시 • **제조업체** - PCI 슬롯의 제조업체 이름 표시 • **설명** - PCI 장치에 대한 설명 표시 • **유형** - PCI 슬롯 유형 표시 • **폭** - 데이터 버스 폭 표시(해당되는 경우)
하드웨어: 원격 액세스 카드	• **호스트** - 호스트 이름 표시 • **서비스 태그** - 호스트의 서비스 태그 표시 • **IP 주소** - 원격 액세스 카드의 IP 주소 표시 • **MAC 주소** - 원격 액세스 카드의 MAC 주소 표시 • **RAC 유형** - 원격 액세스 카드의 유형 표시 • **URL** - 이 호스트와 연관된 iDRAC의 라이브 URL 표시

데이터 센터 및 클러스터에 대한 스토리지 세부 정보 보기

데이터센터/클러스터 정보 탭에서 데이터 센터 또는 클러스터에 대한 물리적 스토리지 세부 정보를 볼 수 있습니다. 이 페이지에 정보가 표시되도록 하려면 인벤토리 작업을 실행해야 합니다. 데이터 센터 및 클러스터 페이지에서는 정보를 CSV 파일로 내보낼 수 있으며 데이터 그리드에 필터/검색 기능을 제공합니다. 하드웨어 보기는 OMSA 및 iDRAC에서 데이터를 직접 보고합니다. 인벤토리 작업 실행을 참조하십시오.

1. OpenManage Integration for VMware vCenter의 탐색 창에서 **vCenter 인벤토리 목록**을 클릭합니다.
2. **데이터센터** 또는 **클러스터**를 클릭합니다.
3. **개체** 탭에서 특정 데이터 센터 또는 클러스터를 선택합니다.
4. **모니터** 탭에서 **Dell EMC 데이터 센터/클러스터 정보** 탭을 선택하고 **스토리지** > **실제 디스크/가상 디스크**로 이동합니다.
   전체 세부 정보 목록을 표시하려면 데이터 그리드에서 특정 호스트를 선택하십시오.

표 22. 데이터 센터 및 클러스터의 스토리지 세부 정보

스토리지: 디스크	설명
실제 디스크	• **호스트** - 호스트 이름 표시 • **서비스 태그** - 호스트의 서비스 태그 표시 • **용량** - 실제 디스크 용량 표시 • **디스크 상태** - 실제 디스크 상태를 표시합니다. 다음과 같은 옵션을 사용할 수 있습니다. ○ 온라인 ○ 준비 완료 ○ 저하됨 ○ 실패 ○ 오프라인

표 22. 데이터 센터 및 클러스터의 스토리지 세부 정보 (계속)

스토리지: 디스크	설명
	○ 재구축 중 ○ 호환되지 않음 ○ 제거됨 ○ 지워짐 ○ 스마트 경고 감지됨 ○ 알 수 없음 ○ 외부 ○ 지원되지 않음 **노트:** 이러한 경고가 나타내는 의미에 대한 자세한 내용은 `dell.com/support`에 있는 Dell EMC OpenManage Server Administrator Storage Management 사용 설명서를 참조하십시오. • **모델 번호** - 실제 스토리지 디스크의 모델 번호 표시 • **마지막 인벤토리** - 마지막으로 인벤토리가 실행된 월, 일, 시간 표시 • **상태** - 호스트 상태 표시 • **컨트롤러 ID** - 컨트롤러 ID 표시 • **커넥터 ID** - 커넥터 ID 표시 • **엔클로저 ID** - 엔클로저 ID 표시 • **장치 ID** - 장치 ID 표시 • **버스 프로토콜** - 버스 프로토콜 표시 • **핫 스페어 유형** - 핫 스페어 유형을 표시합니다. 다음과 같은 옵션을 사용할 수 있습니다. ○ 없음 - 핫 스페어가 없음을 의미합니다. ○ 전역 - 디스크 그룹에 속하는 사용되지 않은 백업 디스크. ○ 전용 - 단일 가상 디스크에 할당된 사용되지 않은 백업 디스크입니다. 가상 디스크에서 실제 디스크에 장애가 발생할 경우, 시스템 중단이나 사용자 개입이 없어도 이 핫 스페어가 활성화되어 장애가 발행한 실제 디스크를 대체합니다. • **부품 번호** - 스토리지 부품 번호 표시 • **일련 번호** - 스토리지 일련 번호 표시 • **공급업체 이름** - 스토리지 공급업체 이름 표시
가상 디스크	• **호스트** - 호스트 이름 표시 • **서비스 태그** - 호스트의 서비스 태그 표시 • **이름** - 가상 디스크 이름 표시 • **실제 디스크** - 가상 디스크가 있는 실제 디스크 표시 • **용량** - 가상 디스크 용량 표시 • **레이아웃** - 가상 스토리지의 레이아웃 유형을 표시합니다. 이 가상 디스크에 구성된 RAID 유형을 의미합니다. • **마지막 인벤토리** - 인벤토리가 마지막으로 실행된 요일, 날짜 및 시간 표시 • **컨트롤러 ID** - 컨트롤러 ID 표시 • **장치 ID** - 장치 ID 표시 • **미디어 유형** - SSD 또는 HDD 표시 • **버스 프로토콜** - 가상 디스크에 포함된 실제 디스크가 사용하는 기술을 표시합니다. 값은 다음과 같습니다. ○ SCSI ○ SAS ○ SATA • **스트라이프 크기** - 단일 디스크에서 각 스트라이프가 사용하는 공간을 제공하는 스트라이프 크기 표시 • 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

표 22. 데이터 센터 및 클러스터의 스토리지 세부 정보 (계속)

스토리지: 디스크	설명
	○ 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 표시합니다. 다음과 같은 옵션을 사용할 수 있습니다. ○ 활성화됨 - 캐시 I/O ○ 비활성화됨 - 직접 I/o

데이터 센터 및 클러스터에 대한 추가 하드웨어 세부 정보 보기

Dell EMC 데이터센터/클러스터 정보 탭의 데이터센터 및 클러스터에 대한 펌웨어, 전원 모니터링, 보증 상태 세부 정보를 볼 수 있습니다. 이 페이지에 정보가 표시되도록 하려면 인벤토리 작업을 실행해야 합니다. 데이터 센터 및 클러스터 페이지에서는 정보를 CSV 파일로 내보낼 수 있으며 데이터 그리드에 필터/검색 기능을 제공합니다. 하드웨어 보기는 OMSA 및 iDRAC에서 데이터를 직접 보고합니다. 지금 인벤토리 작업 실행을 참조하십시오.

1. OpenManage Integration for VMware vCenter의 탐색 창에서 **vCenter**를 클릭합니다.
2. **데이터센터** 또는 **클러스터**를 클릭합니다.
3. **개체** 탭에서 호스트 구성 요소 세부 정보를 확인할 특정 데이터 센터 또는 클러스터를 선택합니다.
4. **모니터** 탭에서 **Dell EMC 데이터센터/클러스터 정보** 탭을 선택합니다.

   `<Component Name>` 하위 탭에서 각 구성 요소에 대해 다음과 같은 정보를 확인합니다.

표 23. 단일 호스트 정보

구성 요소	정보
펌웨어	• **호스트** - 호스트 이름 표시 • **서비스 태그** - 호스트의 서비스 태그 표시 • **이름** - 이 호스트에 있는 모든 펌웨어 이름 표시 • **버전** - 이 호스트에 있는 모든 펌웨어 버전 표시
전원 모니터링 **노트:** 전체 세부 정보 목록을 표시하려면 데이터 그리드에서 특정 호스트를 선택하십시오.	• **호스트** - 호스트 이름 표시 • **서비스 태그** - 호스트의 서비스 태그 표시 • **현재 프로필** - 시스템 성능을 최대화하고 에너지를 절약할 수 있도록 전원 프로필 표시 • **에너지 소비량** - 호스트의 에너지 소비량 표시 • **최고 예비 용량** - 최고 전원 예비 용량 표시 • **전원 예산** - 이 호스트의 전원 용량 표시 • **경고 임계값** - 시스템에 구성된 온도 프로브 경고 임계값의 최대값 표시 • **실패 임계값** - 시스템에 구성된 온도 프로브 실패 임계값의 최대값 표시 • **순간 예비 용량** - 호스트의 순간 헤드룸 용량 표시 • **에너지 소모 시작일** - 호스트가 전원을 사용하기 시작한 날짜 및 시간 표시 • **에너지 소모 종료일** - 호스트가 전원 사용을 중지한 날짜 및 시간 표시 • **시스템 최대 전원** - 호스트 최대 전원 표시 • **시스템 최대 전원 시작일** - 호스트가 최대 전원을 사용하기 시작한 날짜 및 시간 표시

표 23. 단일 호스트 정보 (계속)

구성 요소	정보
	• **시스템 최대 전원 종료일** - 호스트가 최대 전원 사용을 종료한 날짜 및 시간 표시 • **시스템 최대 암페어** - 호스트 최대 암페어 표시 • **시스템 최대 암페어 시작일** - 호스트가 최대 암페어를 사용하기 시작한 날짜 및 시간 표시 • **시스템 최대 암페어 종료일** - 호스트가 최대 암페어 사용을 종료한 날짜 및 시간 표시
보증 요약 **노트:** 보증 상태를 보려면 보증 작업을 실행해야 합니다. 보증 검색 작업 실행을 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 경고를 설정하여 보증 설정을 제어합니다.	• **보증 요약** - 호스트 보증 요약은 각 상태 카테고리에서 호스트 수를 시각적으로 표시하는 아이콘을 사용하여 표시됨 • **호스트** - 호스트 이름 표시 • **서비스 태그** - 호스트의 서비스 태그 표시 • **설명** - 설명 표시 • **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 vCenter가 보증 상태를 가져오지 못함 • **남은 일 수** - 남은 보증 일 수 표시

실제 서버 깜빡임 표시등 설정

대규모 데이터센터 환경에서 실제 서버를 쉽게 찾기 위해 일정 기간(시간) 동안 전면 표시등이 깜빡이도록 설정할 수 있습니다.

1. OpenManage Integration for VMware vCenter의 탐색 창 영역에 있는 인벤토리 목록 아래에서 **호스트**를 클릭합니다.
2. **개체** 탭에서 원하는 호스트를 두 번 클릭합니다.
3. **요약** 탭에서 Dell EMC 서버 관리 포틀릿까지 아래로 스크롤합니다.
4. **호스트 작업**에서 **표시등 깜빡임**을 선택합니다.
5. 다음 중 하나를 선택합니다.
   - 깜빡임을 켜고 기간을 설정하려면 **표시등** 대화 상자에서 **깜빡임 켜기**를 클릭하고 시간 제한 드롭다운 목록을 사용하여 시간 제한 증가를 선택한 다음 **확인**을 클릭합니다.
   - 깜빡임을 끄려면 **표시등** 대화 상자에서 **깜빡임 끄기**를 클릭하고 **확인**을 클릭합니다.

시스템 잠금 모드 구성

시스템 잠금 모드 설정은 PowerEdge 서버의 14세대에 대한 iDRAC에서 사용할 수 있습니다. 전원을 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. 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)

호스트나 클러스터 수준에서 호스트 또는 클러스터의 시스템 잠금 모드를 구성하려면 다음 단계를 수행하십시오.

1. 시스템 잠금 모드 구성 마법사를 실행하려면 다음과 같은 하위 단계 중 하나를 수행하십시오.
   a. **탐색** 창에서 **호스트 및 클러스터**를 클릭합니다. 호스트나 클러스터를 선택하고 마우스 오른쪽 단추로 클릭하여 **작업** 드롭다운 목록을 클릭한 다음 **모든 OpenManage Integration 작업** > **시스템 잠금 모드 구성**을 선택합니다.

b. OpenManage Integration에서 **호스트** 또는 **클러스터** 페이지를 클릭합니다, 호스트나 클러스터를 선택하고 마우스 오른쪽 단추로 클릭하거나 호스트 또는 클러스터를 선택하고 **작업** 드롭다운 목록을 클릭한 다음 **모든 OpenManage Integration 작업** > **시스템 잠금 모드 구성**을 선택합니다.
c. **탐색** 창에서 호스트를 선택한 다음 **요약** > **Dell EMC 호스트 정보** > **시스템 잠금 모드 구성**을 클릭합니다.
d. **탐색** 창에서 호스트나 클러스터를 선택한 다음 **모니터링** > **Dell EMC 호스트 정보** > **펌웨어** > **시스템 잠금 모드 구성**을 클릭합니다.

2. 시스템 잠금 모드를 활성화하려면 **켜기** 옵션을 선택합니다. 또한 잠금 모드를 비활성화하려면 **끄기**를 선택합니다.
3. **적용**을 클릭합니다.

11~13세대 PowerEdge 서버의 시스템 잠금 모드를 구성하려고 할 경우 해당 기능은 이 플랫폼에서 지원되지 않는다는 메시지가 표시됩니다.

시스템 잠금 구성이 완료되면 **작업 큐** 페이지에서 잠금 모드의 업데이트된 상태를 볼 수 있습니다. 잠금 모드의 작업 큐 정보는 클러스터 수준에서만 유효합니다. 작업 큐 페이지에 액세스하려면 OpenManage Integration에서 **모니터링** > **작업 큐** > **시스템 잠금 모드 작업**을 선택합니다. 시스템 잠금 모드에 대한 자세한 내용은 iDRAC 설명서를 참조하십시오.

10

이벤트, 알람 및 상태 모니터링

하드웨어의 관리 목표는 관리자가 OMIVV 플러그인 또는 vCenter를 종료하지 않고도 위험 수준의 하드웨어 이벤트에 응답하는 데 필요한 시스템 상태 및 최신 인프라 정보를 제공해야 합니다.

데이터 센터 및 호스트 시스템 모니터링에서는 관리자가 vCenter의 **작업** 및 **이벤트** 탭에 하드웨어(서버 및 저장소) 및 가상화 관련 이벤트를 표시하여 인프라 상태를 모니터링할 수 있습니다. 또한 위험 하드웨어 경고는 OpenManage Integration for VMware vCenter 알람을 유발할 수 있으며 Dell 가상화 관련 이벤트에 대해 정의된 소수의 알람은 관리 호스트 시스템을 유지 관리 모드로 이동할 수 있습니다.

서버에서 이벤트를 수신하기 위해 모니터링되는 모든 장치에서 OMIVV가 트랩 대상으로 구성되며 다양한 대상은 다음과 같습니다.

- 12세대 이상 호스트의 경우 iDRAC에서 SNMP 트랩 대상이 설정됩니다.
- 12세대 이전 호스트의 경우 OMSA에서 트랩 대상이 설정됩니다.
- 섀시의 경우 CMC에서 트랩 대상이 설정됩니다.

노트: OMIVV는 12세대 이상의 호스트에 대해 SNMP v1 및 v2 경고를 지원합니다. 12세대 이전의 호스트에 대해서는 OMIVV가 SNMP v1 경고만 지원합니다.

모니터링하려면 다음을 수행합니다.

- **이벤트 및 알람** 설정을 구성합니다.
- 필요한 경우 SNMP OMSA 트랩 대상을 구성합니다.
- 이벤트 정보를 검토하려면 vCenter의 **작업** 및 **이벤트** 탭을 사용합니다.

주제:

호스트 이벤트 및 알람 정보

관리 > **설정** 탭에서 OpenManage Integration for VMware vCenter를 사용하여 이벤트 및 알람을 편집할 수 있습니다. 여기에서 이벤트 게시 수준을 선택하고 Dell EMC 호스트에 대한 알람을 활성화하며 기본 알람으로 복원할 수 있습니다. 각 vCenter에 대해 이벤트 및 알람을 구성하거나 등록된 모든 vCenter에 대해 한 번에 구성할 수 있습니다.

4개의 이벤트 게시 수준은 다음과 같습니다.

표 24. 이벤트 게시 수준

이벤트	설명
이벤트 게시하지 않음	OpenManage Integration for VMware vCenter에서 관련 vCenter에 이벤트나 경고를 전달하는 것을 허용하지 않습니다.
모든 이벤트 게시	OpenManage Integration for VMware vCenter이 관리되는 Dell EMC 호스트에서 관련 vCenter로 수신하는 비공식 이벤트를 포함하여 모든 이벤트를 게시합니다.
위험 및 경고 이벤트만 게시	위험 또는 경고 수준의 이벤트만 관련 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 이들을 사용 가능으로 설정할 수 있습니다. 사용하도록 설정하면 위험 수준의 하드웨어 알람을 통해 OMIVV 어플라이언스가 호스트 시스템을 유지관리 모드로 전환할 수 있으며 가상 시스템을 다른 호스트 시스템으로 마이그레이션하는 경우도 있습니다. OpenManage Integration for VMware vCenter가 관리되는 Dell 호스트에서 수신한 이벤트를 전달하고 해당 이벤트용 알람을 생성합니다. 이러한 알람은 다시 부팅, 유지관리 모드 또는 마이그레이션 등과 같은 조치를 vCenter로부터 트리거하기 위해 사용됩니다.

예를 들어, 이중 전원 공급 장치에서 오류가 발생하여 알람이 생성되면 후속 조치로 시스템을 유지 관리 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. DRS는 리소스 풀에서의 사용량을 지속적으로 모니터링하고 업무 필요에 따라 가상 시스템 간에 사용 가능한 리소스를 지능적으로 할당합니다. 중요 하드웨어 이벤트에서 가상 시스템이 자동으로 마이그레이션되는지 확인하려면 DRS가 구성된 Dell EMC 알람을 사용하십시오. 화면 메시지 세부 정보는 영향을 받을 수 있는 이 vCenter 인스턴스의 클러스터를 나열합니다. 이벤트 및 알람을 활성화하기 전에 클러스터에 영향이 있는지 확인하십시오.

기본 알람 설정을 복원해야 할 경우 **기본 알람 재설정** 단추를 사용하면 됩니다. 이 단추는 제품을 제거하거나 다시 설치하지 않고도 기본 알람 구성을 복원하는 데 유용한 옵션입니다. 설치 후 Dell EMC 알람 구성이 변경된 경우 이 단추를 사용하면 변경사항이 되돌려집니다.

노트: Dell 이벤트를 수신하려면 이벤트를 활성화해야 합니다.

노트: OpenManage Integration for VMware vCenter는 호스트에서 가상 시스템을 성공적으로 실행하는 데 꼭 필요한 가상화 관련 이벤트를 미리 선택합니다. 기본적으로 Dell 호스트 알람은 비활성화되어 있습니다. Dell 알람이 활성화된 경우 클러스터에서 DRS를 사용하여 중요 이벤트를 보내는 가상 시스템이 자동으로 마이그레이션되도록 해야 합니다.

섀시 이벤트 및 알람 정보

섀시에 해당되는 이벤트 및 알람은 vCenter 수준에서만 표시됩니다. 모든 vCenter에 있는 호스트의 이벤트 및 알람 설정도 섀시 레벨에서 적용됩니다. OpenManage Integration for VMware vCenter의 **관리** > **설정** 탭에서 이벤트 및 알람 설정을 편집할 수 있습니다. 여기에서 이벤트 게시 수준을 선택하거나, Dell 호스트 및 섀시에 대한 알람을 활성화하거나, 기본 알람을 복원할 수 있습니다. 이벤트 및 알람은 각 vCenter에 대해 또는 등록된 모든 vCenter에 대해 한 번에 구성할 수 있습니다.

섀시 이벤트 보기

1. 왼쪽 창에서 vCenter를 선택하고 vCenter 서버를 클릭합니다.
2. 특정 vCenter를 클릭합니다.
3. **모니터** > **이벤트** 탭을 클릭합니다.
4. 추가적인 이벤트 세부정보를 보려면 특정 이벤트를 선택하십시오.

섀시 알람 보기

1. 왼쪽 창에서 vCenter를 선택하고 vCenter 서버를 클릭합니다.
2. 특정 vCenter를 클릭합니다.
   해당 알람이 표시됩니다. 처음 4개의 알람만 표시됩니다.
3. 전체 목록을 보려면 **모두 표시**를 클릭하여 **모니터** 탭에서 **모든 문제**처럼 상세 목록을 봅니다.
4. **트리거된 알람**에서 **알람**을 클릭하여 알람 정의를 봅니다.

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 번호*>, 메시지:<*메시지 설명*>.

섀시 이벤트는 다음 형식으로 표시됩니다.

Dell-Message:<*메시지 설명*>, 섀시 이름:<*섀시의 이름*>, 섀시 서비스 태그:<*섀시 서비스 태그*>, 섀시 위치:<*섀시의 위치*>

표 25. 가상화 이벤트

이벤트 이름	설명	심각도	권장 작업
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 장치 상태 경고	메모리 장치 수정 등급이 적정 값을 초과했습니다.	경고	작업 안 함
Dell-메모리 장치 오류	메모리 장치 수정 등급이 적정 수준을 초과했거나 메모리 스패어 뱅크가 활성화되었거나 멀티 비트 ECC 오류가 발생했습니다.	오류	시스템을 유지 보수 모두에 배치
Dell-팬 엔클로저가 시스템에 삽입됨	정상 값으로 반환된 센서	정보	작업 안 함
Dell-팬 엔클로저가 시스템에서 제거됨	지정된 시스템에서 팬 엔클로저가 제거되었습니다.	경고	작업 안 함
Dell-팬 엔클로저가 연장된 시간 동안 시스템에서 제거됨	사용자 정의 가능한 기간 동안 지정된 시스템에서 팬 엔클로저가 제거되었습니다.	오류	작업 안 함
Dell-팬 엔클로저 센서가 복구할 수 없는 값을 감지함	지정된 시스템의 팬 엔클로저 센서가 복구할 수 없는 오류를 감지했습니다.	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

표 25. 가상화 이벤트 (계속)

이벤트 이름	설명	심각도	권장 작업
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-장치 구성 오류	지정된 시스템의 플러그형 장치에 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-터리 센서가 복구할 수 없는 값을 감지함	지정된 시스템의 배터리 센서가 배터리에 오류가 있음을 감지했습니다.	오류	작업 안 함
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 엔클로저가 제거된 경우 특정 시스템에서 이 이벤트가 시작될 수도 있습니다.	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 후면판 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 후면판 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 후면판 보드, 시스템 보드 또는 드라이브 이동 장치의 온도 센서가 복	오류	작업 안 함

표 25. 가상화 이벤트 (계속)

이벤트 이름	설명	심각도	권장 작업
	구할 수 없는 오류를 감지했습니다.		
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
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 장치에 종속되지 않는 오류 상태를 감지했습니다.	오류	시스템을 유지 보수 모두에 배치
Dell-스토리지: 컨트롤러 경고	실제 디스크의 일부가 손상되었습니다.	경고	작업 안 함
Dell-스토리지: 컨트롤러 오류	실제 디스크의 일부가 손상되었습니다.	오류	시스템을 유지 보수 모두에 배치
Dell-스토리지: 채널 오류	채널 오류	오류	시스템을 유지 보수 모두에 배치
Dell-스토리지: 엔클로저 하드웨어 정보	엔클로저 하드웨어 정보	정보	작업 안 함
Dell-스토리지: 엔클로저 하드웨어 경고	엔클로저 하드웨어 경고	경고	작업 안 함
Dell-스토리지: 엔클로저 하드웨어 오류	엔클로저 하드웨어 오류	오류	시스템을 유지 보수 모두에 배치
Dell-스토리지: 어레이 디스크 오류	어레이 디스크 오류	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 실제 디스크 온도 센서 경고입니다.	경고	작업 안 함

표 25. 가상화 이벤트 (계속)

이벤트 이름	설명	심각도	권장 작업
Dell-스토리지: 온도 센서 오류	너무 차갑거나 너무 뜨거운 실제 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
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 오류	Fluid Cache 디스크 오류	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-섀시 관리 컨트롤러가 경고 감지	섀시 관리 컨트롤러가 경고 감지	경고	작업 안 함
Dell-섀시 관리 컨트롤러가 오류 감지	섀시 관리 컨트롤러가 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-섀시 관리 컨트롤러 감사 경고	섀시 관리 컨트롤러 감사 경고	경고	작업 안 함
Dell-섀시 관리 컨트롤러 감사 실패 또는 위험 이벤트	섀시 관리 컨트롤러 감사 실패 또는 위험 이벤트	오류	시스템을 유지 보수 모두에 배치
Dell-PCI 장치 감사 경고	PCI 장치 감사 경고	경고	작업 안 함

표 25. 가상화 이벤트 (계속)

이벤트 이름	설명	심각도	권장 작업
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
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 전력 사용량을 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 전력 사용량을 검토하십시오.
전원 공급 장치가 중복되지 않습니다.	현재의 전원 공급 장치 구성이 중복성을 보장하기 위한 플랫	정보	이 문제가 의도치 않게 발생한 경우라면 시스템 구성 및 전력

표 25. 가상화 이벤트 (계속)

이벤트 이름	설명	심각도	권장 작업
	폼 요구 사항을 충족하지 못합니다. 전원 공급 장치에 오류가 발생하면 시스템이 종료될 수 있습니다.		사용량을 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 전력 사용량을 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 전력 사용량을 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 전력 사용량을 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 전력 사용량을 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 전력 사용량을 검토하고 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.

표 25. 가상화 이벤트 (계속)

이벤트 이름	설명	심각도	권장 작업
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.

Proactive HA 이벤트

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

노트: 지원되는 구성 요소의 Proactive HA 상태는 정상(녹색), 경고(노란색), 위험(빨간색) 또는 알 수 없음(회색) 상태가 됩니다.

표 26. 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	저장소	IDSDM 중복성 이벤트

Proactive HA가 활성화된 호스트의 경우, OMIVV에서 다음 트랩이 트리거로 사용되어 구성 요소의 중복 상태를 결정합니다. 중복 상태 정보에 따라 Proactive HA 상태 업데이트를 해당 호스트의 vCenter에 보낼 수 있습니다. 이러한 트랩은 Proactive HA 호스트의 vCenter로 직접 전달되지 않습니다.

표 27. Proactive HA 이벤트

이벤트 이름	설명	심각도
Fan Information(팬 정보)	팬 정보	정보
Fan Warning(팬 경고)	팬 경고	경고
Fan Failure(팬 오류)	팬 오류	위험
Power Supply Normal(전원 공급 장치 정상)	전원 공급 장치가 정상으로 돌아옴	정보
Power Supply Warning(전원 공급 장치 경고)	전원 장치에서 경고를 감지함	경고
Power Supply Failure(전원 공급 장치 오류)	전원 공급 장치에서 장애를 감지함	위험
Power Supply Absent(전원 공급 장치 없음)	전원 공급 장치가 없음	위험
Redundancy Information(중복성 정보)	중복성 정보	정보
Redundancy Degraded(중복성 저하)	중복성이 저하됨	경고
Redundancy Lost(중복성 손실)	중복성이 손실됨	위험

표 27. Proactive HA 이벤트 (계속)

이벤트 이름	설명	심각도
Integrated Dual SD Module Information(통합 듀얼 SD 모듈 정보)	통합 듀얼 SD 모듈(IDSDM) 정보	정보
Integrated Dual SD Module Warning(통합 듀얼 SD 모듈 경고)	통합 듀얼 SD 모듈 경고	경고
Integrated Dual SD Module Failure(통합 듀얼 SD 모듈 오류)	통합 듀얼 SD 모듈 오류	위험
Integrated Dual SD Module Absent(통합 듀얼 SD 모듈 없음)	통합 듀얼 SD 모듈이 없음	위험
Integrated Dual SD Module Redundancy Information(통합 듀얼 SD 모듈 중복성 정보)	통합 듀얼 SD 모듈 중복성 정보	정보
Integrated Dual SD Module Redundancy Degraded(통합 듀얼 SD 모듈 중복성 저하)	통합 듀얼 SD 모듈 중복성이 저하됨	경고
Integrated Dual SD Module Redundancy Lost(통합 듀얼 SD 모듈 중복성 손실)	통합 듀얼 SD 모듈 중복성이 손실됨	위험
섀시 이벤트		
Fan Information(팬 정보)	팬 정보	정보
Fan Warning(팬 경고)	팬 경고	경고
Fan Failure(팬 오류)	팬 오류	위험
Power Supply Normal(전원 공급 장치 정상)	전원 공급 장치가 정상으로 돌아옴	정보
Power Supply Warning(전원 공급 장치 경고)	전원 장치에서 경고를 감지함	경고
Power Supply Failure(전원 공급 장치 오류)	전원 공급 장치에서 장애를 감지함	위험
Redundancy Information(중복성 정보)	중복성 정보	정보
Redundancy Degraded(중복성 저하)	중복성이 저하됨	경고
Redundancy Lost(중복성 손실)	중복성이 손실됨	위험

알람 및 이벤트 설정 보기

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

1. OpenManage Integration for VMware vCenter의 **관리** > **설정** 탭에 있는 **vCenter 설정**에서 **이벤트 및 알람**을 확장합니다.
   다음과 같은 세부 사항이 표시됩니다.
   - Dell EMC 호스트의 vCenter 알람 - **활성화됨** 또는 **비활성화됨**으로 표시됩니다.
   - 이벤트 게시 수준
2. 이벤트와 알람을 구성합니다. 이벤트 및 알람 구성을 참조하십시오.

이벤트 게시 수준을 보려면 이벤트 및 알람 정보를 참조하십시오.

이벤트 보기

이벤트 탭에서 이벤트를 구성한 후에 이벤트를 볼 수 있습니다. 이벤트 및 알람 구성을 참조하십시오.

이벤트 탭에서 호스트, 클러스터 또는 데이터 센터에 대한 이벤트를 봅니다.

1. OpenManage Integration for VMware vCenter Navigator에서 **호스트**, **데이터 센터** 또는 **클러스터**를 클릭합니다.
2. **개체** 탭에서 이벤트를 확인할 특정 호스트, 데이터센터 또는 클러스터를 선택합니다.
3. **모니터** 탭에서 **이벤트**를 클릭합니다.
4. 이벤트 정보를 보려면 특정 이벤트를 선택합니다.

하드웨어 구성 요소 중복 상태—Proactive HA

노트: 지원되는 구성 요소(전원 공급 장치, 팬 및 IDSDM)에 대한 중복 상태를 지원하는 서버에서만 Proactive HA를 사용할 수 있습니다.

노트: OMIVV을 통해 전역 경고를 구성하면 Proactive HA 클러스터에 구성된 Proactive HA 정책이 영향을 받을 수 있습니다.

노트: Proactive HA는 전원, 팬, IDSDM의 중복성을 지원하는 플랫폼에서만 사용할 수 있습니다.

노트: Proactive HA 기능은 중복성을 구성할 수 없는 PSU에 지원되지 않습니다(예: 케이블로 연결된 PSU).

Proactive HA는 OMIVV에서 작동하는 vCenter(vCenter 6.5 이상) 기능입니다. Proactive HA를 활성화하면 호스트에서 지원되는 구성 요소의 중복 상태 저하를 기준으로 사전 조치를 취해 워크로드를 보호합니다.

노트: 연결 프로파일의 일부이고 성공적으로 인벤토리된 PowerEdge 12 세대 이상 및 ESXi 버전 v6.0 이상의 모든 호스트는 Proactive HA에 적합합니다.

지원되는 호스트 구성 요소의 중복 상태를 평가한 후 OMIVV 어플라이언스는 vCenter 서버에 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.
- 위험(심각하게 저하) - 구성 요소에 위험한 오류가 있습니다.

노트: 보통으로 저하 및 심각하게 저하 상태는 **이벤트** 페이지의 **유형** 열에서 *경고*로 표시됩니다.

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 서버를 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 서버로 보냅니다. 폴링은 한 시간마다 실행되며 트랩 손실 가능성을 대비해 유사시 대기 메커니즘으로 사용할 수 있습니다.

랙 및 타워 서버에 대한 사전 HA 구성

랙 및 타워 서버에 대해 구성하려면 다음 단계를 수행하십시오.

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

1. 연결 프로필을 생성하고 호스트를 연결 프로필에 연결합니다. 연결 프로필 생성을 참조하십시오.
2. 호스트 인벤토리가 성공적으로 완료되었는지 확인합니다. 호스트 인벤토리 보기를 참조하십시오.
3. iDRAC에서 SNMP 트랩 대상이 OMIVV 어플라이언스 IP 주소로 설정되었는지 확인합니다.
   노트: **OpenManage Integration** > **모니터** > **로그** 탭에서 Proactive HA 클러스터에 대한 호스트의 가용성이 사용자 작업 로그에서 확인되는지 확인합니다.
4. 클러스터에서 Proactive HA를 활성화합니다. 클러스터에서 Proactive HA 활성화를 참조하십시오.

모듈식 서버에 대한 사전 HA 구성

모듈식 서버에 대해 구성하려면 다음 단계를 수행하십시오.

모듈식 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 오류가 해당 블레이드 모두에 영향을 미치므로 Proactive HA 클러스터의 모든 모듈식 호스트를 동일한 섀시에 두지 않는 것이 좋습니다.

1. 연결 프로필을 생성하고 호스트를 연결 프로필에 연결합니다. 연결 프로필 생성을 참조하십시오.
2. 호스트 인벤토리가 성공적으로 완료되었는지 확인합니다. 호스트 인벤토리 보기를 참조하십시오.
   노트: **OpenManage Integration** > **모니터** > **로그** 탭에서 Proactive HA 클러스터에 대한 호스트의 가용성이 사용자 작업 로그에서 확인되는지 확인합니다.
3. 연결된 섀시에 대한 섀시 프로필을 생성합니다. 섀시 프로필 생성을 참조하십시오.
4. 섀시 인벤토리가 성공적으로 완료되었는지 확인합니다. 섀시 인벤토리 보기를 참조하십시오.
5. CMC를 실행하고 섀시의 트랩 대상이 OMIVV 어플라이언스 IP 주소로 설정되어 있는지 확인합니다.
6. **Chassis Management Controller**에서 **설정** > **일반**으로 이동합니다.
7. **일반 섀시 설정** 페이지에서 **개선된 섀시 로깅 및 이벤트 활성화**를 선택합니다.
8. 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 연결 프로필의 일부이어야 하고 성공적으로 인벤토리되어야 하며 해당하는 경우 섀시 프로필이 섀시에 있어야 합니다.

1. OpenManage Integration에서 **클러스터**를 클릭합니다.
2. **클러스터**에서 클러스터를 클릭하고 **구성** > **vSphere 가용성**을 선택한 다음, **편집**을 클릭합니다.
   클러스터 설정 편집 마법사가 표시됩니다.
3. **vSphere DRS**를 클릭하고 **vSphere DRS 켜기**를 선택합니다(선택되지 않은 경우).
4. **vSphere 가용성**을 클릭하고 **Proactive HA 켜기**를 선택합니다(선택되지 않은 경우).
5. 왼쪽 창의 **vSphere 가용성**에서 **Proactive HA 오류 및 응답**을 클릭합니다.
   Proactive HA 오류 및 응답 화면이 표시됩니다.
6. **Proactive HA 오류 및 응답** 화면에서 **자동화 레벨**을 확장합니다.
7. **자동화 레벨**의 경우 **수동** 또는 **자동**을 선택합니다.
8. **수정**에 대해 심각도 상태(혼합 모드)에 따라 격리 모드, 유지 보수 모드 또는 격리 모드와 유지 보수 모드를 모두 선택합니다. 자세한 내용은 VMware 설명서를 참조하십시오.
9. **Proactive HA 공급자**에 대해 클러스터에 대한 Dell 공급자를 선택하는 확인란을 사용하십시오.
10. 선택한 Dell 공급자에 대해 **편집**을 클릭합니다.
    Proactive HA 공급자에 대해 **차단 오류 조건 편집** 대화 상자가 표시됩니다.
11. 오류 조건에서 이벤트가 게시되지 않도록 하려면 **오류 조건** 표에서 확인란을 사용하여 이벤트(트랩 또는 폴링을 통해 생성)를 선택합니다.

    필터 필드를 사용하여 오류 조건 데이터 그리드의 내용을 필터링하거나 오류 조건 데이터 그리드 안에서 열을 끌어 놓습니다. 클러스터 수준 또는 호스트 수준에서 오류 조건을 적용할 수 있습니다.
12. 클러스터의 현재 및 미래 호스트 전체에 적용하려면 **클러스터 수준** 확인란을 선택합니다.
13. 변경 사항을 적용하려면 **차단 오류 조건 편집**에서 **확인**을 클릭하거나 취소하려면 **취소**를 클릭합니다.
14. 변경 사항을 저장하려면 **클러스터 설정 편집** 마법사에서 **확인**을 클릭하거나 취소하려면 **취소**를 클릭합니다.

Proactive HA가 클러스터에서 활성화되면 OMIVV는 클러스터 내 모든 호스트를 스캔하고 지원되는 모든 호스트 서버 구성 요소의 Proactive HA 상태를 초기화합니다. 이제 OMIVV는 지원되는 구성 요소의 상태 업데이트 알림을 vCenter 서버로 보낼 수 있습니다. vCenter 서버는 OMIVV의 상태 업데이트 알림에 따라 vCenter 서버는 **수정**에 대해 선택한 수동 또는 자동 작업을 수행합니다.

기존 심각도를 재정의하려면 상태 업데이트 알림의 심각도 재정의 페이지 82를 참조하십시오.

상태 업데이트 알림의 심각도 재정의

사용자 환경에 적합하게 사용자 정의된 심각도로 Dell EMC 호스트 및 구성 요소에 대해 Dell Proactive HA의 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 vCenter의 **관리** 탭에서 **Proactive HA 구성** > **Proactive HA 이벤트**를 클릭합니다.
2. 지원되는 이벤트 목록에 대한 정보를 보려면 클릭합니다.
   데이터 그리드는 지원되는 모든 Proactive HA 이벤트를 표시하고 호스트 및 구성 요소의 심각도를 사용자 정의하기 위한 이벤트 ID, 이벤트 설명, 구성 요소 유형, 기본 심각도, 심각도 재정의 열을 포함합니다.
3. 호스트 또는 구성 요소의 심각도를 변경하려면 **심각도 재정의** 열의 드롭다운 목록에서 원하는 상태를 선택합니다.
   이 정책은 OMIVV에 등록된 모든 vCenter 서버의 모든 Proactive HA 호스트에 적용됩니다.
4. 사용자 정의해야 하는 모든 이벤트에 대해 3단계를 반복합니다.
5. 다음 작업 중 하나를 수행합니다.
   a. 사용자 정의를 저장하려면 **변경사항 적용**을 클릭합니다.
   b. 심각도 수준을 선택한 후 재정의 된 심각도를 되돌리려면 **취소**를 클릭합니다.
   c. 재정의된 심각도에 기본 심각도를 적용하려면, **기본값으로 재설정**을 클릭합니다.

관리 콘솔 시작

Dell EMC 서버 관리 포틀릿에서 시작할 수 있는 세 가지 관리 콘솔은 다음과 같습니다.

- iDRAC 사용자 인터페이스에 액세스하려면 원격 액세스 콘솔을 시작합니다. 원격 액세스 콘솔(iDRAC) 실행을 참조하십시오.
- OMSA Server Administrator 사용자 인터페이스에 액세스하려면 OMSA 콘솔을 시작합니다. OMSA 콘솔을 시작하기 전에 OMSA URL이 Open Management Integration for VMware vCenter에 구성되어 있어야 합니다. OMSA 콘솔 실행을 참조하십시오.
- 섀시 사용자 인터페이스에 액세스하려면 블레이드 섀시 콘솔을 클릭합니다. CMC(Chassis Management Controller) 콘솔 실행을 참조하십시오.

  노트: 블레이드 시스템에서 작업하는 경우 CMC를 시작하여 Chassis Management Controller 사용자 인터페이스를 실행합니다. 블레이드 시스템이 아닐 경우 Chassis Management Controller 사용자 인터페이스가 표시되지 않습니다.

원격 액세스 콘솔 실행

Dell EMC 서버 관리 포틀릿에서 iDRAC 사용자 인터페이스를 시작할 수 있습니다.

1. OpenManage Integration for VMware vCenter의 탐색 창 영역에 있는 인벤토리 목록 아래에서 **호스트**를 클릭합니다.
2. **개체** 탭에서 원하는 호스트를 두 번 클릭합니다.
3. **요약** 탭에서 Dell EMC 서버 관리 포틀릿까지 아래로 스크롤합니다.
4. **관리 콘솔** > **Remote Access Console(iDRAC)**을 클릭합니다.

OMSA 콘솔 실행

OMSA 콘솔을 시작하려면 OMSA URL을 설정한 후 OMSA 웹 서버를 설치하고 구성해야 합니다. **설정** 탭에서 OMSA URL을 설정할 수 있습니다.

노트: OMSA를 설치한 후 OpenManage Integration for VMware vCenter를 사용하여 PowerEdge 11세대 서버를 모니터링하고 관리합니다.

1. OpenManage Integration for VMware vCenter의 탐색 창 영역에 있는 인벤토리 목록 아래에서 **호스트**를 클릭합니다.
2. **개체** 탭에서 원하는 호스트를 두 번 클릭합니다.
3. **요약** 탭에서 **Dell EMC 호스트 정보**까지 아래로 스크롤합니다.
4. **Dell EMC 호스트 정보** 섹션에서 **OMSA 콘솔**을 클릭합니다.

Chassis Management Controller 콘솔 실행

Dell EMC 서버 관리 포틀릿에서 섀시 사용자 인터페이스를 시작할 수 있습니다.

1. OpenManage Integration for VMware vCenter의 탐색 창 영역에 있는 인벤토리 목록 아래에서 **호스트**를 클릭합니다.
2. **개체** 탭에서 원하는 블레이드 서버를 두 번 클릭합니다.
3. **요약** 탭에서 Dell EMC 서버 관리 포틀릿까지 아래로 스크롤합니다.
4. **관리 콘솔** > **CMC(Chassis Management Controller) 콘솔**을 클릭합니다.

11

펌웨어 업데이트 정보

OMIVV 어플라이언스를 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.

다음 표에는 다양한 배포 모드에서 동시에 실행할 수 있는 펌웨어 업데이트 작업 수가 나열되어 있습니다. 하지만 펌웨어 업데이트는 원하는 수만큼 예약할 수 있습니다.

표 28. 다양한 배포 모드의 펌웨어 업데이트 작업

소형 배포 모드	중형 배포 모드	대형 배포 모드
5	10	15

다음은 펌웨어 업데이트를 수행할 수 있는 2가지 방법입니다.

- 단일 DUP — DUP 위치를 직접 가리켜서(CIFS 또는 NFS 공유) iDRAC, BIOS 또는 LC에 대한 펌웨어 업데이트를 수행합니다. 단일 DUP 방법은 호스트 수준에서만 사용할 수 있습니다.

  리포지토리 — BIOS 및 모든 지원되는 펌웨어 업데이트를 수행합니다. 이 방법은 호스트 수준 및 클러스터 수준에서 모두 사용할 수 있습니다. 리포지토리의 2가지 유형은 다음과 같습니다.

  - Dell 온라인—Dell(Ftp.dell.com)의 펌웨어 업데이트 리포지토리를 사용하는 위치입니다. OpenManage Integration for VMware vCenter는 선택된 펌웨어 업데이트를 Dell 리포지토리에서 다운로드하고 관리되는 호스트를 업데이트합니다.

    노트: 네트워크 설정을 기반으로 프록시 설정을 활성화합니다(네트워크에서 프록시가 필요한 경우).
  - 공유 네트워크 폴더—CIFS 기반 또는 NFS 기반 네트워크 공유에서 펌웨어의 로컬 리포지토리를 사용할 수 있습니다. 이 리포지토리는 Dell에서 주기적으로 배포하는 SUU(Server Update Utility)의 덤프일 수도 있고 DRM을 사용하여 생성된 사용자 지정 리포지토리일 수도 있습니다. 이 네트워크 공유는 OMIVV에서 액세스할 수 있어야 합니다.

    노트: CIFS 공유를 사용하는 경우 리포지토리 암호는 31자를 넘을 수 없습니다. 암호에 @, &,%, ', ", ,(콤마), <, > 등의 문자를 사용하지 마십시오.

    노트: 최신 DRM 버전(3.x) 이상을 사용해야 합니다.

펌웨어 업데이트 리포지토리 설정에 대한 자세한 내용은 펌웨어 업데이트 리포지토리 설정 페이지 35을(를) 참조하십시오.

펌웨어 업데이트 마법사는 iDRAC, BIOS 및 Lifecycle Controller의 최소 펌웨어 수준을 항상 확인하며 필요한 최소 버전으로 업데이트를 시도합니다. iDRAC, BIOS 및 Lifecycle Controller의 최소 펌웨어 레벨에 대한 자세한 내용은 *OpenManage Integration for VMware vCenter Compatibility Matrix(OpenManage Integration for VMware vCenter 호환성 매트릭스)*를 참조하십시오. iDRAC, Lifecycle Controller 및 BIOS 펌웨어 버전이 최소 요구사항을 충족하면 펌웨어 업데이트 프로세스가 iDRAC, Lifecycle Controller, RAID, NIC/LOM, 전원 공급 장치, BIOS 등을 비롯한 모든 펌웨어 버전의 업데이트를 허용합니다.

주제:

비 vSAN 호스트에 대해 펌웨어 업데이트 실행

노트: 펌웨어 업데이트 프로세스 도중 다음 항목을 삭제해서는 안 됩니다.

- 펌웨어 업데이트 작업이 진행 중인 vCenter의 호스트
- 펌웨어 업데이트 작업이 진행 중인 호스트의 연결 프로필

비 vSAN 호스트에 대한 펌웨어 업데이트를 수행하려면 다음 단계를 수행합니다.

1. 펌웨어 업데이트 마법사에 액세스하려면 OpenManage Integration에서 **호스트**를 클릭하고 다음 작업 중 하나를 수행합니다.

- 호스트를 마우스 오른쪽 단추로 클릭하고 **모든 OpenManage Integration 작업** > **펌웨어 업데이트**를 선택합니다.
- **호스트** 페이지에서 호스트를 클릭한 다음 **모든 OpenManage Integration 작업** > **펌웨어 업데이트**를 선택합니다.
- **탐색** 창에서 호스트를 선택한 다음 **요약** > **Dell EMC 호스트 정보** > **펌웨어 마법사 실행**을 클릭합니다.
- **탐색** 창에서 호스트를 선택한 다음 **모니터** > **Dell EMC 호스트 정보** > **펌웨어** > **펌웨어 마법사 실행**을 클릭합니다.

OMIVV는 호스트 준수 및 동일한 클러스터 내 호스트에서 진행 중인 다른 펌웨어 업데이트 작업 여부를 확인합니다. 확인 후에 **펌웨어 업데이트** 마법사가 표시됩니다.

노트: 이전 버전의 OMIVV에서 사용할 수 있는 버전으로 업그레이드하는 데 이미 예정된 펌웨어 업데이트 작업이 있는 경우 OMIVV 데이터베이스를 백업하고 사용 가능한 버전으로 복원한 후 동일한 호스트에서 펌웨어 업데이트 마법사를 시작할 수 있습니다.

2. **시작** 페이지에서 지침을 읽고 **다음**을 클릭합니다.
   업데이트 소스 선택 페이지가 표시됩니다.
3. **업데이트 소스 선택** 페이지에서 다음 중 하나를 선택합니다.
   a. **현재 리포지토리 위치**를 선택하고 **업데이트 번들 선택** 드롭다운 목록에서 펌웨어 업데이트 번들을 선택합니다.

   노트: 64비트 번들은 iDRAC 버전 1.51 및 이전 버전의 12세대 호스트에 대해 지원되지 않습니다.

   노트: 64비트 번들은 모든 iDRAC 버전의 11세대 호스트에 대해 지원되지 않습니다.

   노트: OMIVV는 32비트 및 64비트 펌웨어 업데이트 번들을 지원합니다. 언급된 번들 외에도 OMIVV는 카탈로그에서 특정 모델에 대해 동일한 릴리스 ID로 사용할 수 있는 32비트 및 64비트 번들이 있는 경우 하이브리드 번들도 생성합니다.

   b. 파일에서 단일 펌웨어 업데이트를 로드하려면 **단일 DUP**를 선택합니다. **단일 DUP**를 선택하는 경우 6단계로 이동합니다.
   단일 DUP는 가상 어플라이언스에서 액세스할 수 있는 CIFS 또는 NFS 공유에 있을 수 있습니다. 다음 형식 중 하나로 **파일 위치**를 입력합니다.
   - NFS 공유 — `<host>:/<share_path/FileName.exe`
   - CIFS 공유 — `\\<호스트에서 액세스할 수 있는 공유 경로>\<파일 이름>.exe`

     CIFS 공유의 경우 OMIVV에 공유 드라이브에 액세스할 수 있는 도메인 형식으로 사용자 이름 및 암호를 입력하라는 메시지가 표시됩니다.

     노트: @, % 및 , 문자는 공유 네트워크 폴더 사용자 이름 또는 암호에서 사용할 수 없습니다.

     노트: OMIVV에서는 SMB(Server Message Block) 버전 1.0과 SMB 버전 2.0 기반 CIFS 공유만 지원됩니다.
4. **다음**을 클릭합니다.
   구성 요소 선택 페이지가 표시됩니다.
5. 확인란을 사용하여 목록에서 하나 이상의 펌웨어 구성 요소를 선택한 후 **다음**을 클릭합니다.
   다운그레이드 중이거나 현재 업데이트가 예정된 구성 요소는 선택할 수 없습니다. **다운그레이드 허용** 옵션을 선택하여 다운그레이드 목록에 표시할 구성 요소를 선택할 수 있습니다.

   펌웨어 업데이트 예약 페이지가 표시됩니다.

   노트: 이전 버전의 OMIVV에서 사용 가능한 버전으로 업그레이드 하는 경우 펌웨어 업데이트 리포지토리를 새로 고침하지 않는 한 재부팅 필요 필드의 모든 구성 요소에 대해 "아니오"가 표시됩니다.

   데이터 그리드의 다양한 구성 요소 콘텐츠에서 쉼표로 구분된 값을 필터링하려면 **필터** 필드를 사용합니다.

   구성 요소 데이터 그리드 안에 열을 끌어서 놓을 수도 있습니다. 마법사에서 내보내는 경우  를 클릭합니다.

   노트: 재부팅이 필요한 구성 요소를 선택하는 경우 vCenter 환경이 워크로드를 마이그레이션할 수 있는 방식으로 구성되어 있는지 확인합니다.
6. **펌웨어 업데이트 예약** 페이지에서 다음을 수행합니다.
   a. **펌웨어 업데이트 작업 이름** 필드에서 작업 이름을 지정하고 **펌웨어 업데이트 설명** 필드(선택 사항)에 설명을 지정합니다.
   펌웨어 업데이트 작업 이름은 필수이며 이미 사용 중인 이름은 사용하지 말아야 합니다. 펌웨어 업데이트 작업을 제거한 경우 작업 이름을 재사용할 수 있습니다.
   b. 유지 관리 모드 시간 초과 값(분 단위)을 입력합니다. 대기 시간이 지정된 시간을 지나면 업데이트 작업이 실패합니다. 업데이트 작업이 실패하고 유지 관리 진입 작업이 취소되거나 시간이 초과됩니다. 하지만 호스트가 재부팅될 때 구성 요소가 자동으로 업데이트될 수도 있습니다.

   노트: 최소 유지 관리 모드 시간 초과 값은 60분입니다.

   노트: 최대 유지 관리 모드 시간 초과 값은 1일입니다.

c. 다음 옵션 중 하나를 선택합니다.
   - **지금 업데이트**를 선택하면 펌웨어 업데이트 작업이 즉시 시작됩니다.

     기본적으로 *펌웨어 업데이트가 완료되면 유지 관리 모드를 종료합니다* 옵션이 선택되어 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 VM의 연결이 끊깁니다.
   - 펌웨어 업데이트 작업을 나중에 실행하려면 **업데이트 예약**을 선택합니다. 현재 시각에서 30분 후에 펌웨어 업데이트 작업을 예약할 수 있습니다.
     - 달력 상자에서 월 및 일을 선택합니다.
     - 시간 텍스트 상자에 HH:MM으로 시간을 입력합니다. 시간은 OMIVV 어플라이언스 시간입니다.
   - 서비스 중단을 방지하려면 **다음 재부팅할 시 업데이트 적용**을 선택합니다.
   - 호스트가 유지 관리 모드가 아닌 경우에도 업데이트 및 재부팅을 적용하려면 **업데이트를 적용한 후 유지 관리 모드로 전환하지 않고 강제로 재부팅**을 선택합니다. 이 방법은 사용하지 않는 것이 좋습니다.

7. **다음**을 클릭합니다.
   펌웨어 업데이트의 모든 구성요소에 대한 세부 정보를 보여주는 **요약** 페이지가 표시됩니다.
8. **마침**을 클릭합니다.

펌웨어 업데이트 작업은 완료하는 데 몇 분 정도 걸리며 시간은 펌웨어 업데이트 작업을 위해 포함된 구성 요소 수에 따라 다릅니다. **작업 큐** 페이지에서 펌웨어 업데이트 작업의 상태를 볼 수 있습니다. 작업 큐 페이지에 액세스하려면 OpenManage Integration에서 **모니터링** > **작업 큐** > **펌웨어 업데이트**를 선택합니다. 펌웨어 업데이트 작업이 완료되면 **펌웨어 업데이트 예약** 페이지에서 선택한 옵션을 기반으로 인벤토리가 선택한 호스트에서 자동으로 실행되고 호스트의 유지 관리 모드가 자동으로 종료됩니다.

vSAN 호스트에 대해 펌웨어 업데이트 마법사 실행

업데이트를 예약하기 전에 다음 사전 요구 사항을 충족해야 합니다.
- DRS가 활성화되어 있습니다.
- 호스트가 유지 관리 모드에 있지 않습니다.
- vSAN 데이터 개체의 상태가 정상입니다.

  위의 점검을 건너 뛰려면 **펌웨어 업데이트 예약** 페이지의 **사전 요구 사항 점검** 확인란의 선택을 해제하십시오.
- 선택된 드라이버 및 펌웨어 버전이 VMware vSAN 지침을 준수합니다. 펌웨어 업데이트를 하기 전에 선택된 드라이버가 설치되어 있습니다.
- 클러스터가 선택한 데이터 마이그레이션 옵션에 대한 vSAN 요구 사항을 만족합니다.
- vSAN을 활성화한 후에 인벤토리를 다시 실행합니다.

노트: 펌웨어 업데이트 프로세스 중에는 다음 항목을 삭제하지 않는 것이 좋습니다.
- 펌웨어 업데이트 작업이 진행 중인 vCenter의 호스트
- 펌웨어 업데이트 작업이 진행 중인 호스트의 연결 프로필

단일 호스트에 대한 펌웨어 업데이트를 수행하려면 다음 단계를 수행합니다.

1. 펌웨어 업데이트 마법사에 액세스하려면 OpenManage Integration에서 **호스트**를 클릭하고 다음 작업 중 하나를 수행합니다.
   - 호스트를 마우스 오른쪽 단추로 클릭하고 **모든 OpenManage Integration 작업** > **펌웨어 업데이트**를 선택합니다.
   - **호스트** 페이지에서 호스트를 클릭한 다음 **모든 OpenManage Integration 작업** > **펌웨어 업데이트**를 선택합니다.
   - **탐색** 창에서 호스트를 선택한 다음 **요약** > **Dell EMC 호스트 정보** > **펌웨어 마법사 실행**을 클릭합니다.
   - **탐색** 창에서 호스트를 선택한 다음 **모니터** > **Dell EMC 호스트 정보** > **펌웨어** > **펌웨어 마법사 실행**을 클릭합니다.

   OMIVV는 호스트 준수 및 동일한 클러스터 내 호스트에서 진행 중인 다른 펌웨어 업데이트 작업 여부를 확인합니다. 확인 후에 **펌웨어 업데이트** 마법사가 표시됩니다.

   노트: 이전 버전의 OMIVV에서 사용할 수 있는 버전으로 업그레이드하는 데 이미 예정된 펌웨어 업데이트 작업이 있는 경우 OMIVV 데이터베이스를 백업하고 사용 가능한 버전으로 복원한 후 동일한 호스트에서 펌웨어 업데이트 마법사를 시작할 수 있습니다.
2. **시작** 페이지에서 지침을 읽고 **다음**을 클릭합니다.
   업데이트 소스 선택 페이지가 표시됩니다.
3. **업데이트 소스 선택** 페이지에서 다음을 수행합니다.
   a. 드롭다운 목록에서 드라이버 리포지토리 프로필 또는 펌웨어 리포지토리 프로필 또는 이들의 조합을 선택합니다.
      기준선 리포지토리가 클러스터 프로필에 연결된 경우 연결된 펌웨어 및 드라이버 리포지토리가 자동으로 선택됩니다.
   b. **업데이트 번들 선택** 드롭다운 메뉴에서 적당한 번들을 선택합니다.

드라이버 리포지토리가 선택된 경우 **드라이버 선택** 페이지가 표시됩니다. **호스트 이름**, **서비스 태그**, **구성 요소 이름**, **공급업체**, **패키지 이름**, **현재 버전**, **사용 가능한 버전**, **적용되는 업데이트**, **재부팅 필요**와 같은 드라이버 구성 요소의 세부 정보가 페이지에 표시됩니다.

c. **드라이버 선택** 페이지에서 업데이트할 드라이버 구성 요소를 선택한 후 **다음**을 클릭합니다.

업데이트를 위한 드라이버 구성 요소를 선택하면 패키지의 모든 구성 요소가 선택됩니다.

펌웨어 리포지토리가 선택된 경우 **구성 요소 선택** 페이지가 표시됩니다. **호스트 이름**, **서비스 태그**, **모델 이름**, **구성 요소**, **현재 버전**, **사용 가능한 버전**, **임계성**, **재부팅 필요**와 같은 구성 요소의 세부 정보가 페이지에 표시됩니다.

d. 확인란을 사용하여 목록에서 하나 이상의 펌웨어 구성 요소를 선택한 후 **다음**을 클릭합니다.

다운그레이드 중이거나 현재 업데이트가 예정된 구성 요소는 선택할 수 없습니다. **다운그레이드 허용** 옵션을 선택하여 다운그레이드 목록에 표시할 구성 요소를 선택할 수 있습니다.

펌웨어 업데이트 예약 페이지가 표시됩니다.

데이터 그리드의 다양한 구성 요소 콘텐츠에서 쉼표로 구분된 값을 필터링하려면 **필터** 필드를 사용합니다.

구성 요소 데이터 그리드 안에 열을 끌어서 놓을 수도 있습니다. 마법사에서 내보내는 경우  를 클릭합니다.

노트: 재부팅이 필요한 구성 요소를 선택하는 경우 vCenter 환경이 워크로드를 마이그레이션할 수 있는 방식으로 구성되어 있는지 확인합니다.

4. **펌웨어 업데이트 예약** 페이지에서 다음을 수행합니다.

a. **펌웨어 업데이트 작업 이름** 필드에서 작업 이름을 지정하고 **펌웨어 업데이트 설명** 필드(선택 사항)에 설명을 지정합니다.

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

노트: 기본적으로 **사전 요구 사항 점검** 확인란이 선택되어 있습니다. 다음과 같은 경우에는 펌웨어 업데이트 작업이 중단됩니다.

- DRS가 활성화되어 있지 않습니다.
- 클러스터의 일부 호스트에 대하여 유지 관리 모드가 활성화되어 있습니다.
- vSAN 개체 상태가 양호하지 않습니다.

b. 유지 관리 모드 시간 초과 값(분 단위)을 입력합니다. 대기 시간이 지정된 시간을 지나면 업데이트 작업이 실패합니다. 업데이트 작업이 실패하고 유지 관리 진입 작업이 취소되거나 시간이 초과됩니다. 하지만 호스트가 재부팅될 때 구성 요소가 자동으로 업데이트될 수도 있습니다.

노트: 최소 유지 관리 모드 시간 초과 값은 60분입니다.

노트: 최대 유지 관리 모드 시간 초과 값은 1일입니다.

c. 다음 옵션 중 하나를 선택합니다.

- **지금 업데이트**를 선택하면 펌웨어 업데이트 작업이 즉시 시작됩니다.

  기본적으로 *펌웨어 업데이트가 완료되면 유지 관리 모드를 종료합니다* 옵션이 선택되어 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 VM의 연결이 끊깁니다.

- 펌웨어 업데이트 작업을 나중에 실행하려면 **업데이트 예약**을 선택합니다. 현재 시각에서 30분 후에 펌웨어 업데이트 작업을 예약할 수 있습니다.
  - 달력 상자에서 월 및 일을 선택합니다.
  - 시간 텍스트 상자에 HH:MM으로 시간을 입력합니다. 시간은 OMIVV 어플라이언스 시간입니다.
- 서비스 중단을 방지하려면 **다음 재부팅할 시 업데이트 적용**을 선택합니다.
- 호스트가 유지 관리 모드가 아닌 경우에도 업데이트 및 재부팅을 적용하려면 **업데이트를 적용한 후 유지 관리 모드로 전환하지 않고 강제로 재부팅**을 선택합니다. 이 방법은 사용하지 않는 것이 좋습니다.

5. **다음**을 클릭합니다.
펌웨어 업데이트의 모든 구성요소에 대한 세부 정보를 보여주는 **요약** 페이지가 표시됩니다.
6. **마침**을 클릭합니다.

펌웨어 업데이트 작업은 완료하는 데 몇 분 정도 걸리며 시간은 펌웨어 업데이트 작업을 위해 포함된 구성 요소 수에 따라 다릅니다. **작업 큐** 페이지에서 펌웨어 업데이트 작업의 상태를 볼 수 있습니다. 작업 큐 페이지에 액세스하려면 OpenManage Integration에서 **모니터링** > **작업 큐** > **펌웨어 업데이트**를 선택합니다. 펌웨어 업데이트 작업이 완료되면 **펌웨어 업데이트 예약** 페이지에서 선택한 옵션을 기반으로 인벤토리가 선택한 호스트에서 자동으로 실행되고 호스트의 유지 관리 모드가 자동으로 종료됩니다.

비 vSAN 클러스터에 대해 펌웨어 업데이트 마법사 실행

OMIVV를 사용하면 클러스터의 모든 호스트에서 BIOS 및 펌웨어 업데이트를 수행할 수 있습니다. 마법사는 연결 프로필의 일부이고 펌웨어, CSIOR 상태, 하이퍼바이저 및 OMSA 상태(11세대 서버만 해당)의 약관을 준수하는 호스트만 업데이트합니다. OMIVV는 클러스터에 DRS(distributed Resource Scheduling)가 활성화되어 있을 경우 호스트가 유지 관리 모드로 전환되거나 유지 관리 모드가 종료될 때 워크로드를 마이그레이션하여 클러스터 인식 펌웨어 업데이트를 수행합니다.

펌웨어 업데이트 마법사를 실행하기 전에 다음의 조건들이 충족되었는지 확인합니다.

- 펌웨어 업데이트 리포지토리가 이미 설정되어 있습니다. 펌웨어 업데이트 리포지토리 설정에 대한 자세한 내용은 펌웨어 업데이트 리포지토리 설정을 참조하십시오.
- 업데이트 중인 클러스터에는 진행 중인 호스트 펌웨어 업데이트 작업이 없습니다.
- 클러스터의 호스트가 연결 프로필에 추가되고 인벤토리가 성공적으로 실행됩니다.
- DRS가 활성화되어 있습니다.

노트: VMware에서는 클러스터를 동일한 서버 하드웨어에 구성할 것을 권장합니다.

노트: 펌웨어 업데이트 프로세스 중에는 다음 항목을 삭제하지 않는 것이 좋습니다.

- 펌웨어 업데이트 작업이 진행 중인 vCenter의 클러스터 호스트.
- 펌웨어 업데이트 작업이 진행 중인 클러스터의 호스트의 연결 프로필.

1. 펌웨어 업데이트 마법사를 시작하려면 OpenManage Integration에서 **클러스터**를 클릭하고 다음 하위 단계 중 하나를 수행합니다.
   - 클러스터를 클릭하고 **작업** > **모든 OpenManage Integration 작업** > **펌웨어 업데이트**를 선택합니다.
   - **개체** 탭에서 **작업** > **모든 OpenManage Integration 작업** > **펌웨어 업데이트**를 선택합니다.
   - 클러스터를 클릭하고 **모니터** > **Dell EMC 클러스터 정보** > **펌웨어**를 선택합니다. **펌웨어** 화면에서 **펌웨어 마법사 실행** 링크를 클릭합니다.
   - 클러스터를 마우스 오른쪽 단추로 클릭하고 **작업** > **모든 OpenManage Integration 작업** > **펌웨어 업데이트**를 선택합니다.

   OMIVV는 호스트 준수 및 동일한 클러스터 내 호스트에서 진행 중인 다른 펌웨어 업데이트 작업 여부를 확인합니다. 확인 후에 **펌웨어 업데이트** 페이지가 표시됩니다.
2. **시작** 페이지에서 지침을 읽고 **다음**을 클릭합니다.
   서버 선택 페이지가 표시됩니다.
3. **서버 선택** 페이지의 **이름** 트리 보기에서 확인란을 사용하여 호스트를 선택합니다.
4. **다음**을 클릭합니다.

   업데이트 소스 선택 페이지가 표시되고 여기에서 번들을 선택할 수 있습니다. 리포지토리 위치도 표시됩니다.
5. **업데이트 소스 선택** 페이지에서 선택된 호스트의 각 모델에는 모델 이름 옆에 필요한 번들을 선택할 수 있는 드롭다운 목록이 있습니다. 펌웨어 업데이트를 원하는 번들을 선택합니다.

   노트: OMIVV는 32비트 및 64비트 펌웨어 업데이트 번들을 지원합니다. 이러한 번들 외에도 OMIVV는 카탈로그에서 동일한 릴리스 ID로 사용할 수 있는 32비트 및 6비트 번들이 여러 개 있는 경우 하이브리드 번들도 생성합니다.

   노트: 64비트 번들은 iDRAC 버전 1.51 및 이전 버전의 12세대 호스트에 대해 지원되지 않습니다.

   노트: 64비트 번들은 모든 iDRAC 버전의 11세대 호스트에 대해 지원되지 않습니다.
6. **다음**을 클릭합니다.
   구성 요소 선택 페이지가 표시됩니다. **호스트 이름**, **서비스 태그**, **모델 이름**, **구성 요소**, **현재 버전**, **사용 가능한 버전**, **중요성**, **재부팅 필요**와 같은 구성 요소의 세부 정보가 페이지에 표시됩니다.
7. **구성 요소 선택** 페이지에서 확인란을 사용하여 목록에서 하나 이상의 구성 요소를 선택한 후 계속 진행하려면 **다음**을 클릭합니다.

   다운그레이드 중이거나 현재 업데이트가 예정된 구성 요소는 선택할 수 없습니다. **다운그레이드 허용** 옵션을 선택하여 다운그레이드 목록에 표시할 구성 요소를 선택할 수 있습니다.

   데이터 그리드의 다양한 구성 요소 콘텐츠에서 쉼표로 구분된 값을 필터링하려면 **필터** 필드를 사용합니다.

   구성 요소 데이터 그리드 안에 열을 끌어서 놓을 수도 있습니다. 마법사에서 내보내는 경우  를 클릭합니다.
8. **FW 업데이트 정보** 페이지에서 모든 펌웨어 업데이트 세부 정보를 봅니다.
9. **다음**을 클릭합니다.

   펌웨어 업데이트 예약 페이지가 표시됩니다.
   a. **펌웨어 업데이트 작업 이름** 필드에 펌웨어 업데이트 작업 이름을 입력합니다.

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

b. **펌웨어 업데이트 설명** 필드에 펌웨어 업데이트 설명을 입력합니다. 이 필드는 선택 사항입니다.

c. 유지 관리 모드 시간 초과 값(분 단위)을 입력합니다. 대기 시간이 지정된 시간을 지나면 업데이트 작업이 실패합니다. 업데이트 작업이 실패하고 유지 관리 진입 작업이 취소되거나 시간이 초과됩니다. 하지만 호스트가 재부팅될 때 구성 요소가 자동으로 업데이트될 수도 있습니다.

노트: 최소 유지 관리 모드 시간 초과 값은 60분입니다.

노트: 최대 유지 관리 모드 시간 초과 값은 1일입니다.

d. **펌웨어 업데이트 예약** 아래에서 다음 옵션을 선택합니다.

- 지금 업데이트 작업을 실행하려면 **지금 업데이트**를 클릭합니다.
- 나중에 업데이트 작업을 실행하려면 **업데이트 예약**을 클릭하고 다음 하위 작업을 수행합니다.
  i. **달력** 상자에서 월 및 일을 선택합니다.
  ii. **시간** 상자에 HH:MM으로 시간을 입력합니다.

10. **다음**을 클릭합니다.
요약 페이지가 표시됩니다.
11. **요약** 페이지에서 **마침**을 클릭하면 **펌웨어 업데이트 작업이 생성**되었다는 메시지가 표시됩니다.

펌웨어 업데이트 작업 완료하는 데 몇 분 정도 걸리며 시간은 선택한 호스트 수와 각 호스트에 있는 구성 요소 수에 따라 다릅니다. **작업 큐** 페이지에서 펌웨어 업데이트 작업의 상태를 볼 수 있습니다. 작업 큐 페이지에 액세스하려면 OpenManage Integration에서 **모니터링** > **작업 큐** > **펌웨어 업데이트**를 선택합니다. 펌웨어 업데이트 작업이 완료되면 선택한 호스트에서 자동으로 인벤토리가 실행되고 호스트의 유지 관리 모드가 자동으로 종료됩니다.

vSAN 클러스터에 대해 펌웨어 업데이트 마법사 실행

펌웨어 업데이트 마법사를 실행하려면 다음 조건을 충족해야 합니다.

- DRS가 활성화되어 있습니다.
- 호스트가 유지 관리 모드가 아닙니다.
- vSAN 데이터 개체의 상태가 정상입니다. 첫 번째 호스트의 vSAN 개체 상태가 양호하지 않은 경우 펌웨어 업데이트 작업이 실패합니다. 다른 호스트의 경우 vSAN 개체 상태가 다시 양호해질 때까지 60분간 기다립니다.
- 선택된 드라이버 및 펌웨어가 VMware vSAN 지침을 준수합니다. 펌웨어 업데이트를 하기 전에 선택된 드라이버가 설치되어 있습니다.
- 클러스터가 선택한 데이터 마이그레이션 옵션에 대한 vSAN 요구 사항을 만족합니다. 기준(클러스터 프로필) 펌웨어나 드라이버 리포지토리를 선택하는 것이 가장 좋습니다.
- 펌웨어 업데이트를 시작하기 전에 드라이버 리포지토리 프로필과 펌웨어 리포지토리 프로필을 생성해야 합니다. 드라이버 리포지토리 및 펌웨어 리포지토리 생성에 대한 자세한 내용은 리포지토리 프로필 생성 페이지 40를 참조하십시오.
- 업데이트 중인 클러스터에는 진행 중인 호스트 펌웨어 업데이트 작업이 없습니다.
- 클러스터의 호스트가 연결 프로필에 추가되고 인벤토리가 성공적으로 실행됩니다.
- vSAN을 활성화한 후에 인벤토리를 다시 실행합니다.

노트: VMware에서는 클러스터를 동일한 서버 하드웨어에 구성할 것을 권장합니다.

노트: 펌웨어 업데이트 프로세스 중에는 다음 항목을 삭제하지 않는 것이 좋습니다.

- 펌웨어 업데이트 작업이 진행 중인 vCenter의 클러스터 호스트.
- 펌웨어 업데이트 작업이 진행 중인 클러스터의 호스트의 연결 프로필.
- CIFS 또는 NFS에 있는 리포지토리

1. 펌웨어 업데이트 마법사를 시작하려면 **OpenManage Integration**에서 **클러스터**를 클릭하고 다음 하위 단계 중 하나를 수행합니다.
   - 클러스터를 클릭하고 **작업** > **모든 OpenManage Integration 작업** > **펌웨어 업데이트**를 선택합니다.
   - **개체** 탭에서 **작업** > **모든 OpenManage Integration 작업** > **펌웨어 업데이트**를 선택합니다.
   - 클러스터를 클릭하고 **모니터** > **Dell EMC 클러스터 정보** > **펌웨어**를 선택합니다. **펌웨어** 화면에서 **펌웨어 마법사 실행** 링크를 클릭합니다.
   - 클러스터를 마우스 오른쪽 단추로 클릭하고 **작업** > **모든 OpenManage Integration 작업** > **펌웨어 업데이트**를 선택합니다.

   OMIVV는 호스트 준수 및 동일한 클러스터 내 호스트에서 진행 중인 다른 펌웨어 업데이트 작업 여부를 확인합니다. 확인 후에 **펌웨어 업데이트** 페이지가 표시됩니다.
2. **시작** 페이지에서 지침을 읽고 **다음**을 클릭합니다.

서버 선택 페이지가 표시됩니다.

3. **서버 선택** 페이지의 **이름** 트리 보기에서 확인란을 사용하여 호스트를 선택합니다.
4. **다음**을 클릭합니다.

   업데이트 소스 선택 페이지가 표시됩니다.
5. **업데이트 소스 선택** 페이지에서 다음을 수행합니다.
   a. 드롭다운 목록에서 드라이버 리포지토리 프로필 또는 펌웨어 리포지토리 프로필 또는 이들의 조합을 선택합니다.

      기준선 리포지토리가 클러스터 프로필에 연결된 경우 연결된 펌웨어 및 드라이버 리포지토리가 자동으로 선택됩니다.

      기본적으로 호스트의 모델 이름이 **번들 선택** 영역에서 선택됩니다.
   b. 펌웨어 리포지토리가 선택된 경우 선택한 호스트의 각 모델에는 모델 이름 옆에 펌웨어 업데이트에 필요한 번들을 선택할 수 있는 드롭다운 목록이 있습니다. 드롭다운 목록에서 원하는 번들을 선택하고 **다음**을 클릭합니다.

      드라이버 리포지토리가 선택된 경우 **드라이버 선택** 페이지가 표시됩니다. **호스트 이름**, **서비스 태그**, **구성 요소 이름**, **공급업체**, **패키지 이름**, **현재 버전**, **사용 가능한 버전**, **적용되는 업데이트**, **재부팅 필요**와 같은 드라이버 구성 요소의 세부 정보가 페이지에 표시됩니다.

   노트: OMIVV는 32비트 및 64비트 펌웨어 업데이트 번들을 지원합니다. 이러한 번들 외에도 OMIVV는 카탈로그에서 동일한 릴리스 ID로 사용할 수 있는 번들이 여러 개 있는 경우 하이브리드 번들도 생성합니다.

   노트: 64비트 번들은 iDRAC 버전 1.51 및 이전 버전의 12세대 호스트에 대해 지원되지 않습니다.

6. **드라이버 선택** 페이지에서 업데이트할 드라이버 구성 요소를 선택한 후 **다음**을 클릭합니다.
   펌웨어 리포지토리가 선택된 경우 **구성 요소 선택** 페이지가 표시됩니다. **호스트 이름**, **서비스 태그**, **모델 이름**, **구성 요소**, **현재 버전**, **사용 가능한 버전**, **중요성**, **재부팅 필요**와 같은 구성 요소의 세부 정보가 페이지에 표시됩니다.
7. **구성 요소 선택** 페이지에서 펌웨어를 업데이트할 구성 요소를 선택한 후 **다음**을 클릭합니다.
   다운그레이드 중이거나 현재 업데이트가 예정된 구성 요소는 선택할 수 없습니다. **다운그레이드 허용** 옵션을 선택하여 다운그레이드 목록에 표시할 구성 요소를 선택할 수 있습니다.

   데이터 그리드의 다양한 구성 요소 콘텐츠에서 쉼표로 구분된 값을 필터링하려면 **필터** 필드를 사용합니다.

   구성 요소 데이터 그리드 안에 열을 끌어서 놓을 수도 있습니다. 마법사에서 내보내는 경우  를 클릭합니다.
8. **FW 업데이트 정보** 페이지에서 모든 펌웨어 업데이트 세부 정보를 본 후 **다음**을 클릭합니다.
   펌웨어 업데이트 예약 페이지가 표시됩니다.
9. **펌웨어 업데이트 예약** 페이지에서 다음을 수행합니다.
   a. **펌웨어 업데이트 작업 이름** 필드에 펌웨어 업데이트 작업 이름을 입력합니다.

      노트: 펌웨어 업데이트 작업 이름은 필수이며 이미 사용 중인 이름은 사용하지 않습니다. 펌웨어 업데이트 작업 이름을 제거한 경우 해당 이름을 재사용할 수 있습니다.

   b. **펌웨어 업데이트 설명** 필드에 펌웨어 업데이트 설명을 입력합니다. 이 필드는 선택 사항입니다.
   c. 유지 관리 모드 시간 초과 값(분 단위)을 입력합니다. 대기 시간이 지정된 시간을 지나면 업데이트 작업이 실패합니다. 업데이트 작업이 실패하고 유지 관리 진입 작업이 취소되거나 시간이 초과됩니다. 하지만 호스트가 재부팅될 때 구성 요소가 자동으로 업데이트될 수도 있습니다.

      노트: 최소 유지 관리 모드 시간 초과 값은 60분입니다.

      노트: 최대 유지 관리 모드 시간 초과 값은 1일입니다.

   d. 지금 업데이트 작업을 실행하려면 **지금 업데이트**를 클릭합니다.
   e. **Virtual vSAN 데이터 마이그레이션** 드롭다운 목록에서 적절한 옵션을 선택합니다. 기본적으로 **액세스 가능성 확인**이 선택되어 있습니다.

      노트: 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 VM의 연결이 끊깁니다.

   f. 나중에 업데이트 작업을 실행하려면 **업데이트 예약**을 클릭하고 다음 작업을 수행합니다.
      i. **달력** 상자에서 월 및 일을 선택합니다.
      ii. **시간** 상자에 HH:MM으로 시간을 입력합니다.
      iii. **Virtual vSAN 데이터 마이그레이션** 드롭다운 목록에서 적절한 옵션을 선택합니다. 기본적으로 **액세스 가능성 확인**이 선택되어 있습니다.

      노트: 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 VM의 연결이 끊깁니다.

10. **다음**을 클릭합니다.
    요약 페이지가 표시됩니다.
11. **요약** 페이지에서 **마침**을 클릭하면 **펌웨어 업데이트 작업이 생성**되었다는 메시지가 표시됩니다.

펌웨어 업데이트 작업 완료하는 데 몇 분 정도 걸리며 시간은 선택한 호스트 수와 각 호스트에 있는 구성 요소 수에 따라 다릅니다. **작업 큐** 페이지에서 펌웨어 업데이트 작업의 상태를 볼 수 있습니다. 작업 큐 페이지에 액세스하려면 OpenManage Integration에서 **모니터링** > **작업 큐** > **펌웨어 업데이트**를 선택합니다. 펌웨어 업데이트 작업이 완료되면 선택한 호스트에서 자동으로 인벤토리가 실행되고 호스트의 유지 관리 모드가 자동으로 종료됩니다.

12

섀시 관리

OMIVV를 사용하면 모듈러 서버와 관련된 섀시의 추가 정보를 볼 수 있습니다. 섀시 정보 탭에서 개별 섀시에 대한 섀시 개요 상세 정보, 하드웨어 인벤토리, 펌웨어 및 관리 컨트롤러에 관한 정보, 개별 섀시 구성 요소의 상태 및 섀시 보증 정보를 볼 수 있습니다. 섀시마다 다음과 같은 3개의 탭이 표시되며 모델에 따라 일부 섀시에서는 다르게 표시됩니다.

- 요약 탭
- 모니터 탭
- 관리 탭

노트: 모든 정보를 보려면, 섀시가 섀시 프로필과 연결되어 있고 섀시 인벤토리가 성공적으로 완료되었는지 확인합니다. 자세한 내용은 섀시 프로필 정보를 참조하십시오.

주제:

섀시 요약 세부 정보 보기

섀시 요약 페이지에서 개별 섀시에 대한 섀시 요약 세부정보를 볼 수 있습니다.

1. **홈** 페이지에서 **vCenter**를 클릭합니다.
2. 왼쪽 창의 **OpenManage Integration**에서 **Dell EMC 섀시**를 클릭합니다.
3. 왼쪽 창에서 해당 섀시 IP를 선택합니다.
4. **요약** 탭을 클릭합니다.
   선택한 섀시에 대해 다음과 같은 정보가 표시됩니다.
   - 이름
   - 모델
   - 펌웨어 버전
   - 서비스 태그
   - CMC

   노트: CMC 링크를 클릭하면 **섀시 관리 컨트롤러** 페이지가 표시됩니다.

   노트: 섀시에 대해 인벤토리 작업을 실행하지 않은 경우 서비스 태그와 CMC IP 주소만 표시됩니다.

5. 선택한 섀시와 연결된 장치의 상태를 봅니다.
   기본 창에는 섀시의 전반적 상태가 표시됩니다. 유효한 상태 표시등은 **정상**, **경고**, **심각**, **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 이전 버전에서는 정상과 경고 또는 위험(주황색 느낌표가 포함된 삼각형을 뒤집은 모양)의 두 가지 상태 표시등만 표시됩니다.
   노트: 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.
6. **CMC Enterprise** 또는 **Express**와 섀시의 라이센스 유형 및 만료 날짜를 함께 확인합니다.
   위의 정보는 M1000e 섀시에 해당하지 않습니다.
7. 호스트의 남은 일수와 사용된 일수를 보려면 **보증** 아이콘을 클릭합니다.
   보증이 둘 이상인 경우 보증의 남은 일수를 계산하는 데 마지막 보증의 마지막 날을 포함합니다.
8. 섀시에 대한 **활성 오류** 표 목록에서 오류를 확인합니다. 이 표는 **섀시 상태** 페이지에 표시됩니다.

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

섀시의 하드웨어 인벤토리 정보 보기

선택된 섀시 내에서 하드웨어 인벤토리에 대한 정보를 볼 수 있습니다. 이 페이지에서 정보를 보려면 인벤토리 작업을 실행하고 구성 요소 정보가 포함된 CSV 파일을 내보내십시오.

1. **홈** 페이지에서 **vCenter**를 클릭합니다.
2. 왼쪽 창의 **OpenManage Integration**에서 **Dell EMC 섀시**를 클릭합니다.
3. 왼쪽 창에서 해당 섀시 IP를 선택합니다.
4. **모니터** 탭을 클릭합니다.
   관련 구성 요소 정보를 보려면 OMIVV를 탐색합니다.

표 29. 하드웨어 인벤토리 정보

하드웨어 인벤토리: 구성 요소	OMIVV 탐색	정보

팬	다음 방법 중 하나를 사용합니다.
	• **개요** 탭에서 **팬**을 클릭합니다.
	• **모니터** 탭에서 왼쪽 창을 확장하고 **하드웨어 인벤토리**를 클릭한 다음 **팬**을 클릭합니다.
		팬 정보:
		• 이름
		• 표시
		• 전원 상태
		• 판독값
		• 경고 임계값
		• 중요 임계값
		  ○ 최소
		  ○ 최대

전원 공급 장치	다음 방법 중 하나를 사용합니다. • **개요** 탭에서 **전원 공급 장치**를 클릭합니다. • **모니터** 탭에서 왼쪽 창을 확장하고 **하드웨어 인벤토리**를 클릭한 다음 **전원 공급 장치**를 클릭합니다.	전원 공급 장치 정보: • 이름 • 용량 • 표시 • 전원 상태

온도 센서	다음 방법 중 하나를 사용합니다.
	• **개요** 탭에서 **온도 센서**를 클릭합니다.
	• **모니터** 탭에서 왼쪽 창을 확장하고 **하드웨어 인벤토리**를 클릭한 다음 **템플릿 센서**를 클릭합니다.
		온도 센서 정보:
		• 위치
		• 판독값
		• 경고 임계값
		  ○ 최대
		  ○ 최소
		• 중요 임계값
		  ○ 최대
		  ○ 최소
		노트: PowerEdge M1000e 섀시의 경우 섀시의 온도 센서에 대한 정보만 표시됩니다. 다른 섀시는 섀시 및 연결된 모듈식 서버의 온도 센서에 대한 정보가 표시됩니다.

I/O 모듈	다음 방법 중 하나를 사용합니다. • **개요** 탭에서 **I/O 모듈**을 클릭합니다. • **모니터** 탭에서 왼쪽 창을 확장하고 **하드웨어 인벤토리**를 클릭한 다음 **I/O 모듈**을 클릭합니다.	I/O 모듈 정보: • 슬롯/위치 • 표시 • 이름 • 패브릭 • 서비스 태그 • 전원 상태 추가 정보를 보려면 해당 I/O 모듈을 선택합니다. 다음 정보가 표시됩니다. • 역할

표 29. 하드웨어 인벤토리 정보 (계속)

하드웨어 인벤토리: 구성 요소	OMIVV 탐색	정보
		• 펌웨어 버전 • 하드웨어 버전 • IP 주소 • 서브넷 마스크 • 게이트웨이 • MAC 주소 • DHCP 활성화

PCIe	다음 방법 중 하나를 사용합니다.
	• **개요** 탭에서 **PCIe**를 클릭합니다.
	• **모니터** 탭에서 왼쪽 창을 확장하고 **하드웨어 인벤토리**를 클릭한 다음 **PCIe**를 클릭합니다.
		PCIe 정보:
		• PCIe 슬롯
		  ○ 슬롯
		  ○ 이름
		  ○ 전원 상태
		  ○ 패브릭
		• 서버 슬롯
		  ○ 이름
		  ○ 번호
		추가 정보를 보려면 해당 PCIe를 선택합니다. 다음 정보가 표시됩니다.
		• 슬롯 유형
		• 서버 매핑
		• 할당 상태
		• 할당된 슬롯 전원
		• PCI ID
		• 벤더 ID
		노트: PCIe 정보는 M1000e 섀시에는 해당되지 않습니다.

iKVM	다음 방법 중 하나를 사용합니다. • **개요** 탭에서 **iKVM**을 클릭합니다. • **모니터** 탭에서 왼쪽 창을 확장하고 **하드웨어 인벤토리**를 클릭한 다음 **iKVM**을 클릭합니다.	iKVM 정보: • iKVM 이름 • 표시 • 펌웨어 버전 • 전면 패널 USB/비디오 활성화 • CMC CLI에 대한 액세스 허용 **노트:** PowerEdge M1000e 섀시에 대해서만 iKVM에 대한 정보를 볼 수 있습니다. **노트:** iKVM 탭은 섀시에 iKVM 모듈이 포함되어 있는 경우에만 표시됩니다.

섀시의 추가 하드웨어 구성 보기

선택한 섀시 내의 보증, 저장소, 펌웨어, 관리 컨트롤러에 대한 정보를 볼 수 있습니다. 이 페이지에서 정보를 보려면 인벤토리 작업을 실행하고 구성 요소 정보가 포함된 CSV 파일을 내보내십시오.

섀시에 대한 보증, 저장소, 펌웨어, 관리 컨트롤러 세부 사항을 보려면 다음 단계를 수행합니다.

1. **홈** 페이지에서 **vCenter**를 클릭합니다.
2. 왼쪽 창의 **OpenManage Integration**에서 **Dell EMC 섀시**를 클릭합니다.
3. 왼쪽 창에서 해당 섀시 IP를 선택합니다.
4. **모니터** 탭을 클릭합니다.
   보증, 저장소, 펌웨어, 관리 컨트롤러에 대한 정보를 보려면 OMIVV를 탐색합니다.

표 30. 펌웨어 세부정보

하드웨어 구성	OMIVV 탐색	정보
펌웨어	a. **모니터** 탭에서 이중 화살표 표시를 클릭하고 왼쪽 창을 확장한 다음 **펌웨어**를 클릭합니다. b. **모니터** 탭에서 **CMC 시작**을 클릭하면 **섀시 관리 컨트롤러** 페이지가 표시됩니다.	펌웨어 정보: • 구성 요소 • 현재 버전

표 31. 관리 컨트롤러 세부 사항

하드웨어 구성	OMIVV 탐색	정보
관리 컨트롤러	a. **모니터** 탭에서 이중 화살표 표시를 클릭하고 왼쪽 창을 확장한 다음 **관리 컨트롤러**를 클릭합니다. b. **관리 컨트롤러** 페이지에서 추가 정보를 보려면 화살표 표시를 클릭하고 왼쪽 열을 확장합니다.	관리 컨트롤러 정보: • 일반 ○ 이름 ○ 펌웨어 버전 ○ 마지막 업데이트 시간 ○ CMC 위치 ○ 하드웨어 버전 • 공용 네트워크 ○ DNS 도메인 이름 ○ DNS의 DHCP 사용 ○ MAC 주소 ○ 중복 모드 • CMC IPv4 정보 ○ IPv4 활성화 ○ DHCP 활성화 ○ IP 주소 ○ 서브넷 마스크 ○ 게이트웨이 ○ 기본 DNS 서버 ○ 대체 DNS 서버

표 32. 저장소 정보

하드웨어 구성	OMIVV 탐색	정보
저장소	**모니터** 탭에서 **저장소**를 클릭합니다.	저장소 정보: • 가상 디스크 • 컨트롤러 • 엔클로저 • 물리 디스크 • 핫 스패어 **노트:** 저장소 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. M1000e 섀시의 경우, 저장소 모듈이 있다면 다른 추가 정보 없이 다음과 같은 저장소 세부 사항이 격자 형태로 표시됩니다. • 이름 • 모델 • 서비스 태그 • IP 주소(저장소로 연결되는 링크) • 패브릭 • 그룹 이름 • 그룹 IP 주소(저장소 그룹으로 연결되는 링크)

표 33. 보증 정보

하드웨어 구성	OMIVV 탐색	정보
보증	**모니터** 탭에서 **보증**을 클릭합니다.	보증 정보: • 공급자 • 설명 • 상태 • 시작 날짜 • 종료 날짜 • 남은 일 수 • 마지막으로 업데이트한 날짜 **노트:** 보증 상태를 보려면 보증 작업을 실행해야 합니다. 보증 검색 작업 실행을 참조하십시오.

섀시 관련 호스트 보기

관리 탭에서 선택한 섀시의 연결된 호스트에 대한 정보를 볼 수 있습니다.

1. **홈** 페이지에서 **vCenter**를 클릭합니다.
2. 왼쪽 창의 **OpenManage Integration**에서 **Dell EMC 섀시**를 클릭합니다.
3. 왼쪽 창에서 해당 섀시 IP를 선택합니다.
4. **관리** 탭을 클릭합니다.

   연결된 호스트에 대해 다음과 같은 정보가 표시됩니다.
   - 호스트 이름(선택한 호스트 IP를 클릭하면 호스트에 대한 세부 정보가 표시됨)
   - 서비스 태그
   - 모델
   - iDRAC IP
   - 슬롯 위치
   - 마지막 인벤토리

13

하이퍼바이저 배포

OMIVV에서는 지원되는 베어 메탈 서버에 아래 구성 요소를 구성하면서 하이퍼바이저를 배포하고 vCenter의 지정된 데이터 센터 및 클러스터에 추가할 수 있습니다.

- 부팅 순서 설정
- RAID 구성
- BIOS 구성
- iDRAC 구성

PXE를 사용하지 않고 VMware vCenter를 사용하여 베어 메탈 PowerEdge 서버에 하드웨어 프로필, 시스템 프로필과 하이퍼바이저 프로필을 만들 수 있습니다.

노트: 하이퍼바이저를 배포할 때는 14세대 이상 서버에 대해 시스템 프로필을 사용하는 것이 좋습니다.

하드웨어를 프로비저닝하고 배포를 수행하려면 배포 마법사에 실제 서버가 표시되는지 확인하십시오. 모든 실제 서버가 다음과 같은 요구 사항에 따르는지 확인하십시오.

- *OpenManage Integration for VMware vCenter 호환성 매트릭스*에 나와 있는 자세한 하드웨어 지원 정보를 확인하십시오.
- 지원되는 최소 버전의 iDRAC 펌웨어, Lifecycle Controller 및 BIOS를 확인하십시오. 특정 펌웨어 지원 정보에 대해서는 *OpenManage Integration for VMware vCenter Compatibility Matrix(OpenManage Integration for VMware vCenter 호환성 매트릭스)*를 참조하십시오.
- 배포 후에 PCI 슬롯에 NIC를 수동으로 구성합니다. 애드온 NIC를 사용할 경우 시스템에서 호스트 LOM(LAN on Motherboard) 또는 네트워크 도터 카드(NDC)를 활성화하고 네트워크에 연결해야 합니다. OMIVV는 내장 또는 통합 LOM만 사용하여 배포를 지원합니다.
- IDSDM의 스토리지 사양을 충족합니다. IDSDM의 스토리지 사양을 알아보려면 VMware 설명서를 참조하십시오. OMIVV로 하이퍼바이저를 배포하기 전에 BIOS에서 IDSDM이 활성화되어 있는지 확인합니다. OMIVV는 IDSDM 또는 로컬 하드 드라이브에서의 배포를 허용합니다.
- vCenter 및 iDRAC가 다른 네트워크에 연결된 경우 두 네트워크 간 라우트가 있는지 확인하십시오.
- CSIOR(Collect System Inventory on Reboot)이 활성화되어 있어야 합니다. 또한 자동/수동 검색을 시작하기 전에 시스템 전원을 완전히 껐다 다시 켜서(예: 하드 재부팅) 검색된 데이터가 최신인지 확인합니다.
- 공장에서 미리 구성된 자동 검색 및 핸드셰이크 옵션이 있는 Dell EMC 서버를 주문하도록 클릭합니다. 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 하이퍼바이저 배포를 시작하기 전에 다음과 같은 조건이 충족되는지 확인해야 합니다.
  - BIOS에서 VT(가상화 기술) 플래그를 활성화합니다.
  - 운영 체제 설치를 위한 시스템 부팅 순서를 부팅 가능한 가상 디스크 또는 IDSDM으로 설정합니다.
- 하드웨어 구성에 OMIVV가 사용되는 경우 BIOS 구성이 하드웨어 프로필에 속하지 않아도 VT에 대한 BIOS 설정이 자동으로 활성화되어 있는지 확인합니다. 가상 디스크가 대상 시스템에 아직 없는 경우 Express/Clone RAID 구성이 필요합니다.
- 배포에 사용할 수 있는 모든 Dell 드라이버가 사용자 지정 ESXi 이미지에 포함되어 있는지 확인합니다. **Dell 드라이버 및 다운로드** 페이지로 이동하고 배포 프로세스 중에 OMIVV가 액세스할 수 있는 CIFS 또는 NFS 공유 위치로 사용자 지정 이미지를 저장하여 `Support.dell.com`에서 올바른 사용자 지정 이미지를 찾을 수 있습니다. 이 릴리스에서 지원되는 ESXi 버전의 최신 목록은 *OpenManage Integration for VMware vCenter Compatibility Matrix(OpenManage Integration for VMware vCenter 호환성 매트릭스)*를 참조하십시오. 올바른 이미지를 사용하려면 사용자 지정 Dell ISO 이미지 다운로드를 참조하십시오.
- 대상 서버에서 OMIVV가 하이퍼바이저를 자동 배포하기 위해 BIOS 모드만 지원하므로 하이퍼바이저 프로필을 적용하기 전에 참조 하드웨어 프로필에서 BIOS 모드가 선택되었는지 확인합니다. 하드웨어 프로필이 선택되지 않은 경우, 부팅 모드를 BIOS로 수동 구성하고 하이퍼바이저 프로필을 적용하기 전에 서버를 다시 부팅하십시오.

서버가 PowerEdge 12세대 서버보다 이전 버전인 경우 배포 프로세스는 다음과 같습니다.

- 대상 시스템에 OMSA 패키지를 설치합니다
- OMSA에 SNMP 트랩 대상을 자동으로 구성하여 OMIVV를 가리킵니다

주제:

- 하이퍼바이저 프로필 생성
- 배포 템플릿 생성
- 배포 마법사 정보
- 배포 작업 타이밍
- 사용자 지정 Dell EMC ISO 이미지 다운로드

장치 검색

검색은 지원되는 PowerEdge 운영 체제 미설치 서버를 추가하는 과정입니다. 서버를 검색한 후 하이퍼바이저와 하드웨어 배포에 사용할 수 있습니다. 배포에 필요한 PowerEdge 서버 목록은 *OpenManage Integration for VMware vCenter Compatibility Matrix*(*OpenManage Integration for VMware vCenter 호환성 매트릭스*)를 참조하십시오. Dell 운영 체제 미설치 서버의 iDRAC에서 OMIVV 가상 시스템에 대한 네트워크 연결이 필요합니다.

노트: 기존 하이퍼바이저가 있는 호스트가 OMIVV에 검색되지 않아야 하며, 대신 이러한 vCenter에 추가할 수 있어야 합니다. 해당 호스트를 연결 프로필에 추가한 다음 호스트 준수 마법사를 사용하여 OpenManage Integration for VMware vCenter와 조정하십시오.

노트: 운영 체제 미설치 서버가 OMIVV 4.0 이전에 발견된 경우 운영 체제 미설치 서버 목록에서 시스템을 제거하고 재발견했는지 확인하십시오.

노트: 12세대 운영 체제 미설치 PowerEdge 서버용 SD 카드에 OS 배포를 수행하려면 iDRAC 2.30.30.30 이상이 설치되어 있어야 합니다.

수동 검색

검색 프로세스에서 추가되지 않은 베어 메탈 서버를 수동으로 추가할 수 있습니다. 서버가 추가되면 배포 마법사의 서버 목록에 표시됩니다.

1. OpenManage Integration for VMware vCenter의 **관리** > **배포** 탭에서 ✚ 아이콘을 클릭합니다.
   서버 추가 대화 상자가 표시됩니다.
2. **서버 추가** 대화 상자에서 다음을 수행합니다.
   a. **iDRAC IP 주소** 텍스트 상자에서 iDRAC IP 주소를 입력합니다.
   b. **사용자 이름** 텍스트 상자에서 사용자 이름을 입력합니다.
   c. **암호** 텍스트 상자에 암호를 입력합니다.
3. **서버 추가**를 클릭합니다.
   서버를 추가하는 작업은 완료되는 데 몇 분이 소요될 수 있습니다.

OpenManage Integration for VMware vCenter에서 자동 검색

자동 검색은 PowerEdge 운영 체제 미설치 서버를 추가하는 과정입니다. 서버가 검색된 후에는 하이퍼바이저 및 하드웨어 배포에 사용합니다. 자동 검색은 OMIVV에서 운영 체제 미설치 서버를 수동으로 검색해야 하는 필요성을 제거해주는 iDRAC 기능입니다.

자동 검색 필수 조건

Dell 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 운영 체제 미설치 서버의 iDRAC에서 OMIVV 어플라이언스로 네트워크 연결이 가능한지 확인하십시오.

노트: 기존 하이퍼바이저가 있는 호스트는 OMIVV에서 검색되지 않으므로 대신 연결 프로필에 하이퍼바이저를 추가한 후 호스트 준수 마법사를 사용하여 OMIVV와 조정합니다.

자동 검색을 수행하려면 다음 조건을 충족해야 합니다.

- 전원 — 서버를 콘센트에 연결하십시오. 서버의 전원을 켤 필요는 없습니다.
- 네트워크 연결성 — 서버의 iDRAC에 네트워크가 연결되어 있고 포트 4433을 통해 프로비전이 서버와 통신하는지 확인합니다. DHCP 서버를 사용하여 IP 주소를 가져오거나 iDRAC 구성 유틸리티에서 수동으로 지정할 수 있습니다.
- 추가 네트워크 설정 - DHCP를 사용하는 경우 DNS 이름을 확인할 수 있도록 DHCP 설정에서 DNS 서버 주소 가져오기 설정을 활성화합니다.

- 프로비저닝 서비스 위치 — iDRAC가 프로비저닝 서비스 서버의 IP 주소 또는 호스트 이름을 아는지 확인합니다. 프로비저닝 서비스 위치를 참조하십시오.
- 계정 액세스 비활성화 — iDRAC에 대한 관리 계정 액세스를 활성화하고 관리자 권한이 있는 iDRAC 계정이 있는 경우 먼저 iDRAC 웹 콘솔 내에서 비활성화합니다. 자동 검색이 완료되면 관리 iDRAC 계정이 다시 활성화됩니다.
- 자동 검색 활성화 - 자동 검색 프로세스가 시작될 수 있도록 서버의 iDRAC에 자동 검색이 활성화되어 있는지 확인합니다.

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 콘솔에서 수동으로 지정하지 않으면 iDRAC가 DHCP 범위 옵션 값을 사용하려고 합니다. DHCP 범위 옵션이 없으면 iDRAC가 DNS에서 서비스 레코드 값을 사용하려고 합니다.

DHCP 범위 옵션 및 DNS 서비스 레코드를 구성하는 방법은 http://en.community.dell.com/techcenter/extras/m/white_papers/20178466의 Dell 자동 검색 네트워크 설정 사양을 참조하십시오.

iDRAC에서 관리 계정 활성화 또는 비활성화

자동 검색을 설정하기 전에 루트 이외의 모든 관리 계정을 비활성화합니다. 루트 계정은 자동 검색 절차를 수행하는 동안에 비활성화되어야 합니다. 자동 검색을 설정한 다음에는 iDRAC GUI로 돌아가서 루트는 제외하고 꺼져 있는 관리 계정을 다시 활성화합니다.

노트: 자동 검색 실패에 대비하기 위해 iDRAC에서 비관리 계정을 활성화할 수 있습니다. 비관리 계정을 이용하면 자동 검색이 실패했을 때 원격으로 액세스할 수 있습니다.

1. 브라우저에 **iDRAC IP 주소**를 입력합니다.
2. **Integrated Dell Remote Access Controller GUI**에 로그인합니다.
3. 다음 중 하나를 실행하십시오.
   - iDRAC6의 경우: 왼쪽 창에서 **iDRAC 설정** > **네트워크/보안** > **사용자** 탭을 선택합니다.
   - iDRAC7의 경우: 왼쪽 창에서 **iDRAC 설정** > **사용자 인증** > **사용자** 탭을 선택합니다.
   - iDRAC8의 경우: 왼쪽 창에서 **iDRAC 설정** > **사용자 인증** > **사용자** 탭을 선택합니다.
4. **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 성공적으로 설정한 후 1-8단계를 반복합니다. 단, 지금 **사용자 활성화** 확인란을 선택하고 **적용**을 클릭합니다.

수동으로 PowerEdge 11세대 서버의 자동 검색 구성

iDRAC 및 호스트 IP 주소를 확인해 둡니다.

출고 시 자동 검색을 사용하기 위한 베어 메탈 어플라이언스를 주문하지 않은 경우 수동으로 설정할 수 있습니다.

베어 메탈 서버의 자동 검색이 성공하면 핸드셰이크 서비스에서 반환한 자격 증명을 사용하여 기존 계정이 활성화되거나 새 관리자 계정이 생성됩니다. 자동 검색 전에 비활성화된 다른 모든 관리 계정은 활성화되지 않습니다. 자동 검색에 성공하고 나면 관리자 계정을 다시 활성화하십시오. iDRAC에서 관리 계정 활성화 또는 비활성화를 참조하십시오.

노트: 어떤 이유로 자동 검색이 성공적으로 완료되지 않는 경우에는 원격으로 iDRAC에 연결할 수 있는 방법이 없습니다. 원격 연결을 하려면 iDRAC에서 비관리 계정을 활성화할 수 있어야 합니다. iDRAC에 활성화된 비관리 계정이 없는 경우에는 로컬에서 시스템에 로그인하여 iDRAC에서 계정을 활성화하는 것이 유일한 방법입니다.

1. 브라우저에 **iDRAC IP** 주소를 입력합니다.
2. **iDRAC Enterprise GUI**에 로그인합니다.
3. 가상 콘솔 미리 보기의 **Integrated Dell Remote Access Controller 6 — Enterprise** > **시스템 요약** 탭에서 **시작**을 클릭합니다.

4. **경고 - 보안** 대화 상자에서 **예**를 클릭합니다.
5. iDRAC Utility 콘솔에서 **F12** 키를 한 번 또는 두 번 누릅니다.
   인증 필요 대화 상자가 표시됩니다.
6. **인증 필요** 대화 상자에서 표시된 이름을 확인한 다음 **Enter** 키를 누릅니다.
7. **암호**를 입력합니다.
8. **Enter** 키를 누릅니다.
9. **종료/다시 시작** 대화 상자가 표시되면 **F11** 키를 누릅니다.
10. 호스트가 다시 시작되고 화면에 메모리 로드에 대한 정보와 RAID가 차례로 표시된 다음 iDRAC가 표시되고 Ctrl+E 키를 누르라는 메시지가 표시되면 즉시 **Ctrl+E** 키를 누릅니다.
    다음과 같은 대화 상자가 표시되면 작업이 성공적으로 수행된 것입니다. 그렇지 않을 경우 전원 메뉴로 가서 전원을 껐다 다시 켠 다음 이 단계를 반복합니다.

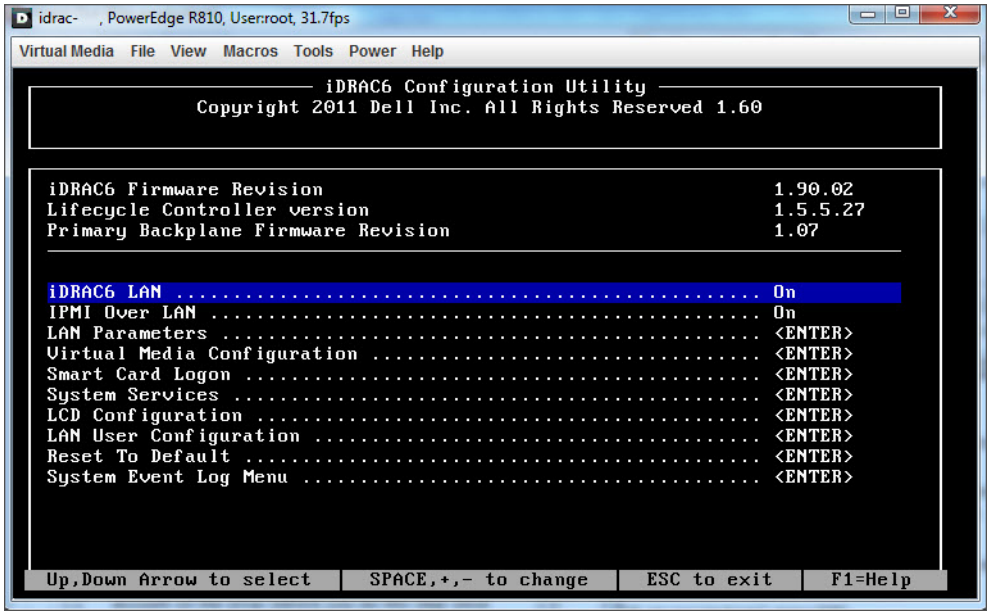

그림 1 . iDRAC 구성 유틸리티

11. iDRAC6 구성 유틸리티에서 화살표 키를 사용하여 **LAN 매개변수**를 선택합니다.
12. **Enter** 키를 누릅니다.
13. 이 호스트가 블레이드인 경우 NIC를 구성하려면 스페이스바를 사용하여 옵션을 **활성화됨**으로 전환합니다.
14. DHCP를 사용하는 경우 화살표 키를 사용하여 **DHCP의 도메인 이름**을 선택합니다.
15. 스페이스바를 사용하여 옵션을 **켜짐**으로 전환합니다.
16. DHCP를 사용하는 경우 화살표 키를 사용하여 IPv4 설정을 탐색하고 **DHCP의 DNS 서버**를 선택합니다.
17. 스페이스바를 사용하여 옵션을 **켜짐**으로 전환합니다.
18. 종료하려면 키보드에서 **ESC** 키를 누릅니다.
19. 화살표 키를 사용하여 **LAN 사용자 구성**을 선택합니다.
20. 화살표 키를 사용하여 **프로비저닝 서버**를 선택합니다.
21. **Enter** 키를 누릅니다.
22. 호스트의 IP 주소를 입력합니다.
23. **Esc** 키를 누릅니다.
24. 화살표 키를 사용하여 **계정 액세스**를 선택합니다.
25. 스페이스바를 사용하여 옵션을 **비활성**으로 전환합니다.
26. 스페이스바를 사용하여 **자동 검색**을 선택합니다.
27. 스페이스바를 사용하여 옵션을 **활성화됨**으로 전환합니다.
28. 키보드에서 **Esc** 키를 누릅니다.
29. **Esc** 키를 다시 누릅니다.

수동으로 PowerEdge 12세대 이후 서버의 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. 이러한 시나리오에서는 Dell EMC로부터 서버를 받은 후에 iDRAC 케이블을 마운트 및 연결한 후 서버의 전원을 켜면 서버가 자동으로 검색되고 배포 마법사의 첫 번째 페이지에 나열됩니다.

노트: 자동으로 검색된 서버의 경우 **관리** > **설정** > **배포 자격 증명**에 제공된 자격 증명이 관리자 자격 증명으로 설정되며 OS 배포가 완료될 때까지 서버와의 추가 통신에 사용됩니다. OS가 성공적으로 배포된 후에는 연결된 연결 프로필에 제공된 iDRAC 자격 증명이 설정됩니다.

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

1. 시스템 설정으로 이동하려면 대상 시스템을 부팅/재부팅하고 초기 부팅 중 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.
   다음 서버 부팅 시 서버가 자동으로 검색됩니다. 성공적인 자동 검색 후에 루트 사용자가 활성화되고 **자동 검색 활성화** 플래그가 자동으로 비활성화됩니다.

운영 체제 미설치 서버 제거

자동으로 검색되거나 수동으로 추가된 서버를 수동으로 제거할 수 있습니다.

1. OpenManage Integration for VMware vCenter에서 **관리** > **배포** 탭을 클릭합니다.
2. **운영 체제 미설치 서버** 페이지에서 서버를 선택하고 ✖를 클릭합니다.

프로비저닝

자동/수동 검색된 운영 체제 미설치 시스템은 OMIVV에서 하드웨어 프로비저닝 및 하이퍼바이저 배포에 사용할 수 있습니다. 프로비저닝 및 배포를 준비하려면 다음을 수행하십시오.

표 34. 배포 준비

단계	설명
시스템 프로필 생성	새 서버를 구성하는 데 사용되는 14세대 참조 서버에서 수집된 시스템 구성 설정이 들어 있습니다.
하드웨어 프로필 생성	새 서버를 배포하는 데 사용되는 참조 서버에서 수집된 하드웨어 설정이 들어 있습니다. 하드웨어 프로필 생성 또는 사용자 지정 페이지 105을 참조하십시오. **노트:** 13세대 이전 서버에 대해 하드웨어 프로필을 사용하는 것이 좋습니다.
하이퍼바이저 프로필 생성	ESXi 배포에 필요한 하이퍼바이저 설치 정보가 들어 있습니다. 하이퍼바이저 프로필 생성 페이지 107을 참조하십시오.
배포 템플릿 생성	배포 템플릿에는 시스템 프로필, 하드웨어 프로필, 하이퍼바이저 프로필 또는 시스템 프로필과 하드웨어 조합 또는 하드웨어 프로필과 하이퍼바이저 프로필 조합이 포함되어 있습니다. 이러한 프로필을 저장한 다음 필요에 따라 사용 가능한 모든 데이터 센터 서버에 다시 사용할 수 있습니다.

배포 템플릿이 생성되면 배포 마법사를 사용하여 서버 하드웨어를 프로비저닝하고 vCenter의 새 호스트를 배포하는 예약된 작업을 생성하는 데 필요한 정보를 수집합니다. 배포 마법사 실행에 대한 자세한 내용은 배포 마법사 실행 페이지 110을 참조하십시오. 마지막으로 작업 대기열을 통해 작업 상태를 보고 보류 중인 배포 작업을 변경합니다.

시스템 프로필

부팅 순서, RAID, BIOS 및 iDRAC를 지원하는 구성을 포함하여 CNA, FCoE 구성에 대한 지원을 제공하는 PowerEdge 서버에 대한 iDRAC에서 시스템 프로필 기능을 사용할 수 있습니다. OMIVV는 iDRAC 14세대의시스템 프로필을 "시스템 프로필"로 지원합니다. 서버 구성 프로필을 지원함으로써 OMIVV는 14세대 Dell EMC 서버의 전체 구성을 내보내고 대상 서버로 가져올 수 있습니다.

FX2 섀시에 설치된 모듈 서버의 시스템 프로필을 다른 FX2 섀시에 설치된 또 다른 유사한 서버에 적용하는 경우 두 서버의 슬롯 수는 동일해야 합니다.

예를 들어, FX2s 섀시의 슬롯1에 있는 FC640 서버의 시스템 프로필은 다른 FX2s 섀시의 슬롯 1에 상주하는 또 다른 FC640 서버에만 적용할 수 있습니다.

노트: 시스템 프로필은 다음과 같은 구성을 지원하지 않습니다.

- 부팅 옵션의 활성화 및 비활성화
- BOSS-related 구성

노트: 시스템 프로필을 사용하는 동안, Enterprise 라이센스를 사용하여 시스템 프로필을 내보내고 Express 라이센스를 사용하여 동일한 시스템 프로필을 서버로 가져오는 것이 실패하며 반대의 작업도 실패합니다.

노트: iDRAC9 펌웨어 3.00.00.00의 Express 라이센스를 사용하여 시스템 프로필을 가져올 수 없습니다. Enterprise 라이센스가 있어야 합니다.

노트: 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 모듈 서버에서 생성된 시스템 프로필은 NIC 레벨 제한사항으로 인해 동일한 FX 섀시에 있는 다른 모듈 서버에는 적용할 수 없습니다. 이 경우 섀시의 각 슬롯에서 참조 시스템 프로필을 가져와 이러한 시스템 프로필을 섀시에서 해당하는 슬롯에만 적용할 것을 권장합니다.

시스템 프로필을 사용하기 위한 일반적인 작업은 다음과 같습니다.

- 참조 서버에서 시스템 프로필 정보를 생성하거나 캡처합니다. 시스템 프로필 생성 페이지 102을 참조하십시오.
- 배포 템플릿을 사용하여 선택한 서버에 프로필을 적용합니다. 배포 템플릿 생성 페이지 108을 참조하십시오.

노트: 14세대 이상의 서버의 경우 시스템 프로필을 사용하는 것이 좋습니다.

시스템 프로필 페이지를 실행하려면 다음 단계를 수행하십시오.

1. OpenManage Integration for VMware vCenter의 **관리** > **배포** 탭에서 **배포 템플릿** > **시스템 프로필**을 선택합니다.
   a. **시스템 프로필** 페이지에서 생성된 시스템 프로필 목록을 확인합니다.

      프로필 이름, 설명, 서버 모델 및 참조 서버 정보와 함께 시스템 프로필이 나열된 표가 표시됩니다.

   b. 시스템 프로필 호스트에 대한 정보를 자세히 보려면 시스템 프로필을 선택합니다.

      프로필 이름, iDRAC IP, iDRAC 유형, 서비스 태그, 호스트 이름, 서버 모델, 생성 날짜, 수정 날짜 및 수정한 사람과 같은 세부 정보가 표시되어 있는 시스템 프로필 정보를 검토하십시오.

   c. 데이터 그리드 안에서 열을 바꾸려면 데이터 그리드 내에서 열을 끌어 놓습니다.
   d. 데이터 그리드의 내용을 필터링하거나 검색하려면 **필터** 필드를 클릭합니다.
   e. 시스템 프로필 정보를 .CSV 파일로 내보내려면 시스템 프로필을 선택하고 데이터 그리드의 오른쪽 모서리에서  아이콘을 클릭합니다.

시스템 프로필 생성

시스템 프로필을 생성하기 전에 다음과 같은 조건이 충족되었는지 확인합니다.

- 참조 서버는 요구 사항에 따라 OMIVV의 외부에 구성됩니다. iDRAC 사용자 암호를 제외하고 현재 버전에서는 특성 값을 수정하는 것을 지원하지 않습니다.
- iDRAC에서 반환된 데이터가 최신 상태가 되도록 CSIOR(Collect System Inventory On Restart)이 참조 서버에서 활성화되어 있고, 참조 서버가 재부팅되었습니다.
- OpenManage Integration에서 각 vCenter 관리 호스트에 대한 인벤토리 작업을 성공적으로 수행했습니다.
- 베어 메탈 서버에는 최소 BIOS 및 펌웨어 버전이 이미 설치되어 있습니다. iDRAC, BIOS 및 Lifecycle Controller의 최소 펌웨어 레벨에 대한 자세한 내용은 *OpenManage Integration for VMware vCenter Compatibility Matrix(OpenManage Integration for VMware vCenter 호환성 매트릭스)*를 참조하십시오.

14세대 참조 서버만 사용하여 시스템 프로필을 생성할 수 있습니다.

1. OpenManage Integration for VMware vCenter의 **관리** > **배포** 탭에서 **배포 템플릿** > **시스템 프로필**을 선택합니다.

2. ✚을 클릭합니다.
3. **시작** 페이지에서 지침을 읽고 **다음**을 클릭합니다.
   - **프로필 이름** 텍스트 상자에서 프로필 이름을 입력합니다.
   - **프로필 설명** 텍스트 상자에 설명을 입력합니다. 설명 값은 선택 사항입니다.
4. **다음**을 클릭합니다.
   참조 서버 대화 상자가 표시됩니다. 대화 상자에서 14세대 참조 서버를 직접 선택하거나 프로필 소스 페이지에서 찾아보기 단추를 사용할 수 있습니다.
5. 다음 하위 단계 중 하나를 실행하여 14세대 참조 서버를 선택합니다.

   노트: 11세대부터 14세대까지의 모든 호스트가 대화 상자에 표시되고 14세대 호환 가능 베어 메탈 서버와 호스트에 대해서만 선택 링크가 활성화됩니다. 14세대 베어 메탈 서버만 표시되고 호환되는 베어 메탈 서버에 대해서만 선택 링크가 활성화됩니다.

   a. **참조 서버** 대화 상자에서 14세대 참조 서버를 클릭하고 참조 서버에 대한 **선택** 링크를 클릭합니다.

      노트: 호환되는 서버에 대해서만 **선택** 링크가 활성화됩니다.

   b. **참조 서버** 페이지에서 **찾아보기**를 클릭하여 OMIVV에서 관리하고 인벤토리를 성공적으로 작성하며 호환되는 14세대 호스트 참조 서버 또는 호환되는 14세대 베어 메탈 서버를 선택합니다.

   설정이 추출되었음을 나타내는 **추출 확인** 대화 상자가 표시됩니다. 참조 서버에서 하드웨어 구성을 추출하려면 **추출 확인** 대화 상자에서 **예**를 클릭합니다. 몇 분 후에 추출 작업이 완료됩니다.

   프로필 소스 페이지에 선택한 서버 이름, 참조 서버 유형, iDRAC IP 주소, 모델, 서비스 태그가 표시됩니다.

   노트: **참조 서버 유형**이 베어 메탈 서버인 경우 iDRAC IP만 표시되는 반면 **참조 서버 유형**이 호스트인 경우 iDRAC IP 및 호스트 IP/FQDN이 모두 표시됩니다.
6. **다음**을 클릭합니다.
7. **프로필 설정** 페이지에서 iDRAC를 확장하여 시스템 프로필 특성을 봅니다. 오름차순 또는 내림차순으로 데이터 그리드 열을 정렬할 수 있습니다. 데이터 필터 아이콘을 클릭하여 데이터를 필터링합니다.
   a. **값** 열에서 암호 설정 링크를 빠르게 확인하려면 ▼을 클릭하고 **포함하는 값**에 'password'를 입력한 후 활성 사용자의 암호를 입력합니다.

      노트: Dell EMC는 베어 메탈 서버를 추가하는 동안 사용되는 자격 증명과 동일한 자격 증명을 제공할 것을 권장합니다. 배포 템플릿에서 암호를 변경하는 경우, 이 변경사항이 루트 사용자에 표시되지 않습니다. OS를 배포하는 동안 하이퍼바이저 프로필이 배포 템플릿과 연관된 경우, 배포에 연결 프로필(iDRAC 및 ESXi) 암호를 사용합니다.

      노트: **암호 설정** 옵션은 유효한 사용자 이름이 있는 iDRAC 사용 가능 사용자에 대해서만 사용할 수 있습니다.

      또한 iDRAC, BIOS, RAID, NIC, CNA, FCoE 및 EvenFilters와 같은 Dell 참조 서버의 구성을 기반으로 구성 요소의 프로필 설정을 볼 수 있습니다.
   b. 각 구성 요소를 확장하여 **인스턴스**, **특성 이름**, **값**, **파괴적**, **종속성** 및 **그룹** 등 설정 옵션을 표시합니다.
      속성 위에 마우스를 올려 놓으면 속성에 관한 자세한 내용이 표시됩니다.
      기본적으로 **읽기 전용**, **시스템 특정** 및 **파괴적** 특성 등 일부 특성은 선택할 수 없습니다.
      종속성 텍스트를 사용할 수 없으면 종속성 텍스트가 비어 있습니다.

   노트: RPM 업그레이드 또는 백업 및 복원 시 다음 항목이 마이그레이션한 모든 프로필에 적용됩니다.
   - 속성 위에 마우스를 올려놓으면 속성 이름이 표시됩니다.
   - 시스템 특정 특성이 아닌 특성만 선택됩니다.
   - 종속성 텍스트는 표시되지 않습니다.
   - 활성화된 특성에는 선택한 총 특성 수가 표시됩니다.
8. **다음**을 클릭합니다.
   프로필 세부 정보 및 시스템 구성의 특성 통계에 관한 정보를 제공하는 **요약** 페이지가 표시됩니다.
   총 특성 수, 활성화된 총 특성 수, 플랫폼별 총 특성 수 및 총 파괴적 특성 수가 특성 통계에 표시됩니다.
9. **요약** 페이지에서 **마침**을 클릭합니다.
   프로필이 자동으로 저장되고 **시스템 프로필** 창에 표시됩니다.

모든 시스템 특정 설정은 현재 릴리스에서 지원되지 않습니다. 시스템별 특성에 대한 자세한 내용은 시스템 특정 특성 페이지 144을 참조하십시오.

OMIVV가 작동하기 위해 일부 시스템 프로필 특성은 무시됩니다. 사용자 정의 특성에 대한 자세한 내용은 사용자 지정 특성 페이지 148을 참조하십시오. 시스템 프로필 구성 템플릿, 특성 및 워크플로에 대한 자세한 내용은 추가 정보 페이지 149를 참조하십시오.

시스템 프로필 관리

시스템 프로필은 참조 서버를 사용하여 서버의 시스템 구성을 정의합니다. OpenManage Integration for VMware vCenter에서 다음을 비롯하여 기존 시스템 프로필의 몇 가지 관리 조치를 수행할 수 있습니다.

- 시스템 프로필 보기
- 시스템 프로필 삭제

노트: 현재 릴리스에서는 OMIVV에서 시스템 프로필을 수정하는 기능이 지원되지 않습니다. OMIVV 외부에 시스템을 구성한 다음 시스템 프로필에 대한 참조 서버로 사용해야 합니다.

하드웨어 프로필 구성

서버 하드웨어 설정을 구성하려면 하드웨어 프로필을 생성해야 합니다. 하드웨어 프로필은 새로 검색된 인프라스트럭처 구성요소에 적용할 수 있는 구성 템플릿으로서 다음과 같은 정보가 필요합니다.

표 35. 하드웨어 프로필 생성 요구 사항

요구 사항	설명
부팅 순서	부팅 순서는 부팅 장치 시퀀스 및 하드 드라이브 시퀀스로서 부팅 모드가 BIOS로 설정된 경우에만 편집할 수 있습니다.
BIOS 설정	BIOS 설정에는 메모리, 프로세서, SATA, 통합 장치, 직렬 통신, 내장형 서버 관리, 전원 관리, 시스템 보안 및 기타 설정이 포함됩니다. **노트:** OpenManage Integration for VMware vCenter를 사용하면 참조 서버의 설정과 관계없이 배포된 모든 서버의 BIOS에 있는 프로세서 그룹에서 특정 BIOS 설정이 가능합니다. 참조 서버를 사용하여 하드웨어 프로필을 생성하기 전에 참조 서버에서 CSIOR 설정을 활성화하고 재부팅해야 정확한 인벤토리 및 구성 정보를 제공할 수 있습니다.
iDRAC 설정	iDRAC 설정에는 네트워크, 사용자 목록, 사용자 구성이 있습니다.
RAID 구성	RAID 구성에는 하드웨어 프로필이 추출된 시점에서 참조 서버의 현재 RAID 토폴로지가 표시됩니다. **노트:** 하드웨어 프로필에는 두 개의 RAID 구성 옵션이 있습니다. 1. RAID1 적용 및 해당되는 전용 핫스페어 생성 — 대상 서버에 기본 RAID 구성 설정을 적용하려면 이 옵션을 사용합니다. 2. 참조 서버에서 RAID 구성 클론 — 참조 서버 설정을 클론하려면 이 옵션을 사용합니다. 하드웨어 프로필 생성을 위한 참조 서버 사용자 지정을 참조하십시오.

하드웨어 프로필 생성 작업은 다음과 같습니다.

- 참조 서버에서 CSIOR 활성화
- 하드웨어 프로필 생성을 위한 참조 서버 사용자 지정
- 하드웨어 프로필 클론

참조 서버에서 CSIOR 활성화

참조 서버를 사용하여 하드웨어 프로필을 생성하기 전에 CSIOR(Collect System Inventory On Reboot) 설정을 활성화하고 다시 부팅한 다음 정확한 인벤토리 및 구성 정보를 입력합니다.

두 가지 방법으로 CSIOR을 사용할 수 있습니다.

표 36. CSIOR 활성화 방법

방법	설명
로컬	Dell Lifecycle Controller USC(United Server Configurator) 사용자 인터페이스를 사용하여 개별 호스트를 사용합니다.

표 36. CSIOR 활성화 방법 (계속)

방법	설명
원격	WS-Man 스크립트를 사용합니다. 이 기능 스크립팅에 대한 자세한 내용은 *Dell TechCenter* 및 *DCIM Lifecycle Controller 관리 프로필*을 참조하십시오.

참조 서버에서 CSIOR을 로컬로 사용하려면 다음을 수행합니다.

1. 시스템 전원을 켜고 POST 중에 **F2** 키를 눌러 USC를 시작합니다.
2. **하드웨어 구성** > **부품 교체 구성**을 선택합니다.
3. **다시 부팅할 때 시스템 인벤토리 수집** 설정을 활성화하고 USC를 종료합니다.

하드웨어 프로필 생성 또는 사용자 지정

1. OpenManage Integration for VMware vCenter의 **관리** > **배포** 탭에서 **배포 템플릿** > **하드웨어 프로필**을 선택합니다.
2. ➕ 아이콘을 클릭합니다.
3. **하드웨어 프로필 마법사**의 **시작** 페이지에서 **다음**을 클릭하고 다음을 수행합니다.
   - **프로필 이름** 텍스트 상자에서 프로필 이름을 입력합니다.
   - **설명** 텍스트 상자에 설명을 입력합니다. 설명은 선택 사항입니다.
4. **다음**을 클릭합니다.
   참조 서버 대화 상자가 표시됩니다. 대화 상자에서 직접 참조 서버를 선택하거나 참조 서버 창에서 찾아보기 단추를 사용할 수 있습니다.
5. 다음 하위 단계 중 하나를 실행하여 참조 서버를 선택합니다.
   - **참조 서버** 대화 상자에서 올바른 참조 서버를 선택하고 참조 서버에 대한 **선택** 링크를 클릭합니다.

     설정이 추출되었음을 나타내는 **추출 확인** 대화 상자가 표시됩니다. 참조 서버에서 하드웨어 구성을 추출하려면 **추출 확인** 대화 상자에서 **예**를 클릭합니다. 몇 분 후에 추출 작업이 완료됩니다.
   - **참조 서버** 페이지에서 **찾아보기**를 클릭하여 OMIVV에서 관리하고 인벤토리를 성공적으로 작성하며 호환되는 참조 서버 또는 호환되는 운영 체제 미설치 서버를 선택합니다.

     참조 서버에서 하드웨어 구성을 추출하려면 **추출 확인** 대화 상자에서 **예**를 클릭합니다.

   참조 서버 페이지에 선택한 서버 이름, iDRAC IP 주소, 모델, 서비스 태그가 표시됩니다.
6. 참조 서버 설정을 사용자 지정하려면 **참조 서버** 페이지에서 **참조 서버 설정 사용자 지정**을 클릭하고 다음 설정을 선택합니다(선택적으로 포함 및 사용자 지정 가능).
   - **RAID 설정**
   - **BIOS 설정**
   - **부팅 순서**
   - **iDRAC 설정**
     - **네트워크 설정**
     - **사용자 목록**
7. **RAID 구성** 창에서 다음 중 하나를 선택하고 **다음**을 클릭합니다.
   - **RAID1 적용 및 해당되는 전용 핫스패어 생성** — 대상 서버에 기본 RAID 구성 설정을 적용하려면 이 옵션을 사용합니다. RAID1 사용이 가능한 통합 컨트롤러의 처음 두 드라이브에서 RAID 구성 작업의 기본값은 RAID1입니다. 또한 후보 드라이브가 RAID 조건을 충족하면 RAID1 어레이의 전용 핫 스패어가 생성됩니다.
   - **아래 보여진 대로 참조 서버로부터 RAID 구성 복제** — 참조 서버 설정을 클론하려면 이 옵션을 사용합니다.
8. 프로필에 **BIOS 설정** 정보를 포함하려면 BIOS 설정 페이지에서 범주를 확장하여 설정 옵션을 표시한 다음 **편집**을 클릭하고 다음 중 하나를 업데이트합니다.
   - **시스템 정보**
   - **메모리 설정**
   - **프로세서 설정**
   - **SATA 설정**
   - **부팅 설정**
   - **일회성 부팅**
   - **내장형 장치**
   - **슬롯 비활성화**

- **직렬 통신**
- **시스템 프로필 설정**
- **시스템 보안**
- **기타 설정**

범주에 대한 모든 업데이트가 완료된 후 변경 사항을 저장하려면 **다음**을 클릭하고 변경 사항을 취소하려면 **취소**를 클릭합니다.

노트: 설정 옵션 및 설명을 비롯한 자세한 BIOS 정보를 보려면 선택한 서버의 *하드웨어 소유자 매뉴얼*을 참조하십시오.

9. **부팅 순서** 페이지에서 다음을 수행하고 **다음**을 클릭합니다.
   a. 부팅 순서 옵션을 표시하려면 **부팅 순서**를 확장한 다음 **편집**을 클릭하고 다음과 같이 업데이트합니다.
      i. **부팅 모드** 목록에서 **BIOS** 또는 **UEFI**를 선택합니다.
      ii. **보기** 목록의 **부팅 장치 순서**에 표시된 부팅 장치 순서를 변경하려면 장치를 선택한 다음 **위로 이동** 또는 **아래로 이동**을 클릭합니다.
      iii. 서버가 부팅 순서를 자동으로 다시 시도하도록 **부팅 순서 재시도 활성화**를 선택합니다.
      iv. 변경 사항을 적용하려면 **확인**을 클릭하고 변경 사항을 취소하려면 **취소**를 클릭합니다.
   b. **하드 드라이브 순서** 옵션을 표시하려면 하드 드라이브 순서를 확장한 다음 **편집**을 클릭합니다. 다음과 같이 업데이트합니다.
      i. 표시된 하드 드라이브 순서를 변경하려면 장치를 선택하고 **위로 이동** 또는 **아래로 이동**을 클릭합니다.
      ii. 변경 사항을 적용하려면 **확인**을 클릭하고 변경 사항을 취소하려면 **취소**를 클릭합니다.

노트: 13세대 이전의 서버의 경우 UEFI 및 BIOS 모드가 모두 표시됩니다. 13번째 또는 그 이후 세대 서버의 경우 BIOS 또는 UEFI 모드가 표시됩니다.

10. **iDRAC 설정** 페이지에서 다음을 수행합니다.
    a. 범주를 확장하여 설정 옵션을 표시하고 **편집**을 클릭합니다.
       다음 중 하나를 업데이트합니다.
       - **네트워크 설정**
       - **네트워크**
       - **가상 매체**
    b. iDRAC 로컬 **사용자 목록**에서 다음 중 하나를 수행합니다.
       - **사용자 추가** — iDRAC 사용자 및 필요한 정보를 수동으로 입력합니다. 완료 후 변경 사항을 적용하려면 **적용**을 클릭하고 취소하려면 **취소**를 클릭합니다.
       - **사용자 삭제** — 선택한 사용자를 삭제합니다. 사용자를 선택하려면 마우스를 사용해 **삭제**를 클릭합니다. 삭제를 확인하려면 **예**를 클릭합니다.
       - **사용자 편집** — iDRAC 사용자 정보를 수동으로 편집합니다. 완료 후 설정을 적용하려면 **적용**을 클릭하고 취소하려면 **취소**를 클릭합니다.

    범주에 대한 모든 업데이트가 완료된 후 변경 사항을 저장하려면 **다음**을 클릭하고 변경 사항을 취소하려면 **취소**를 클릭합니다.

    노트: 설정 옵션 및 설명을 비롯한 자세한 iDRAC 정보를 보려면 선택한 서버의 *iDRAC 사용 설명서*를 참조하십시오.

11. **다음**을 클릭합니다.
12. **요약** 페이지에서 **마침**을 클릭합니다.

프로필이 자동으로 저장되고 **하드웨어 프로필** 창에 표시됩니다.

하드웨어 프로필 생성 또는 복제

1. OpenManage Integration for VMware vCenter의 **관리** > **배포** 탭에서 **배포 템플릿** > **하드웨어 프로필**을 선택합니다.
2. ✚을 클릭합니다.
3. **하드웨어 프로필 마법사**의 **시작** 페이지에서 **다음**을 클릭하고 다음 작업을 수행합니다.
   - **프로필 이름** 텍스트 상자에서 프로필 이름을 입력합니다.
   - **설명** 텍스트 상자에서 **설명**을 입력합니다. 설명은 선택 사항입니다.
4. **다음**을 클릭합니다.
5. 기준에 맞고 vCenter에서 관리되며 Dell EMC OpenManage 플러그인에서 성공적으로 인벤토리 작성된 참조 서버를 선택하려면 **참조 서버** 페이지에서 **찾아보기**를 클릭합니다.
6. 참조 서버에서 모든 하드웨어 설정을 추출하려면 **참조 서버 설정 클론** 옵션을 클릭합니다.

7. **다음**을 클릭합니다.
   설정의 압축 해제를 완료하는 데 몇 분 정도 걸립니다.
8. **다음**을 클릭합니다.
   설정이 채워지고 참조 서버 창에 선택된 서버 이름, iDRAC IP 주소, 서비스 태그가 표시됩니다.

프로필이 저장되고 **하드웨어 프로필** 창의 **사용 가능한 프로필** 아래에 표시됩니다.

하드웨어 프로필 관리

하드웨어 프로필은 참조 서버를 사용하여 서버의 하드웨어 구성을 정의합니다. OpenManage Integration for VMware vCenter에서 다음을 비롯하여 기존 하드웨어 프로필의 몇 가지 관리 조치를 수행할 수 있습니다.

- 하드웨어 프로필 보기 또는 편집
- 하드웨어 프로필 삭제

하드웨어 프로필 보기 또는 편집

1. OpenManage Integration for VMware vCenter의 **관리** > **배포** 탭에서 **배포 템플릿** > **하드웨어 프로필**을 선택합니다.
   하드웨어 프로필이 표시됩니다.
2. 프로필을 편집하려면 프로필을 선택하고 을 클릭합니다.
3. **하드웨어 프로필** 마법사에서 다른 값을 구성하려면 **편집**을 클릭합니다.
4. 변경 사항을 적용하려면 **저장**을 클릭하고 변경 사항을 취소하려면 **취소**를 클릭합니다.

하드웨어 프로필 삭제

노트: 실행 중인 배포 작업의 일부인 하드웨어 프로필을 삭제하면 삭제 작업에 오류가 발생할 수 있습니다.

1. OpenManage Integration for VMware vCenter의 **관리** > **배포** 탭에서 **배포 템플릿 하드웨어 프로필**을 선택합니다.
2. 프로필을 선택하고 를 클릭합니다.
3. 프로필을 제거하려면 확인 대화 상자에서 **예**를 클릭하고 취소하려면 **아니오**를 클릭합니다.

하이퍼바이저 프로필 생성

ESXi를 서버에 배포하여 구성하려면 하이퍼바이저 프로필을 생성합니다. 하이퍼바이저 프로필에는 다음과 같은 정보가 필요합니다.

- NFS 또는 CIFS 공유의 Dell 사용자 지정 ISO 소프트웨어 매체 위치
- 배포된 호스트를 관리하는 vCenter 인스턴스 및 선택적 호스트 프로필
- 플러그인이 vCenter에 서버를 배포하는 대상 클러스터 또는 데이터센터

1. OpenManage Integration for VMware vCenter의 **관리** > **배포** 탭에서 **배포 템플릿** > **하이퍼바이저 프로필**을 선택합니다.
2. **하이퍼바이저 프로필** 페이지에서 를 클릭합니다.
3. **하이퍼바이저 프로필** 대화 상자에서 다음 하위 작업을 수행합니다.
   - **프로필 이름** 텍스트 상자에서 프로필 이름을 입력합니다.
   - **설명** 텍스트 상자에서 설명(선택 사항)을 입력합니다.
4. **참조 ISO 경로 및 버전 선택**의 **설치 소스(ISO)** 텍스트 상자에 하이퍼바이저 공유 위치에 대한 경로를 입력합니다.
   스크립트된 설치를 허용하기 위해 하이퍼바이저 이미지 복사본이 수정됩니다. 참조 ISO 위치는 다음 중 한 가지 형식이 가능합니다.
   - `NFS 형식: host:/share/hypervisor.iso`
   - `CIFS 형식: //host/share/hypervisor.iso`

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

   CIFS 공유를 사용하는 경우 **사용자 이름**, **암호** 및 **암호 확인**을 입력합니다. 암호가 일치하는지 확인합니다.
5. **버전 선택** 목록에서 ESXi 버전을 선택합니다.
   이 하이퍼바이저 프로필을 사용하여 배포된 모든 서버에는 이 이미지가 있으며 서버가 12세대 이전 버전인 경우 권장되는 최신 버전의 OMSA도 설치됩니다.

6. 경로와 인증을 확인하려면 **테스트 설정**에서 **테스트 시작**을 클릭합니다.
7. **적용**을 클릭합니다.

하이퍼바이저 프로필 관리

기존 하이퍼바이저 프로필에서 다음을 비롯하여 몇 가지 관리 조치를 수행할 수 있습니다.
- 하이퍼바이저 프로필 보기 또는 편집
- 하이퍼바이저 프로필 삭제

하이퍼바이저 프로필 보기 또는 편집

1. OpenManage Integration for VMware vCenter의 **관리** > **배포** 탭에서 **배포 템플릿** > **하이퍼바이저 프로필**을 선택합니다.
   하이퍼바이저 프로필이 표시됩니다.
2. 프로필을 선택하고 을 클릭합니다.
3. **하이퍼바이저 프로필** 대화 상자에서 업데이트된 값을 제공합니다.
4. 변경 사항을 적용하려면 **저장**을 클릭하고 변경 사항을 취소하려면 **취소**를 클릭합니다.

하이퍼바이저 프로필 삭제

노트: 실행 중인 배포 작업의 일부인 하이퍼바이저 프로필을 삭제하면 작업에 오류가 발생할 수 있습니다.

1. OpenManage Integration for VMware vCenter의 **관리** > **배포** 탭에서 **배포 템플릿** > **하이퍼바이저 프로필**을 선택합니다.
2. 프로필을 선택하고 를 클릭합니다.
3. 프로필을 제거하려면 확인 대화 상자에서 **삭제**를 클릭하고 취소하려면 **취소**를 클릭합니다.

배포 템플릿 생성

배포 템플릿에는 시스템 프로필, 하드웨어 프로필, 하이퍼바이저 프로필 또는 시스템 프로필과 하드웨어 조합 또는 하드웨어 프로필과 하이퍼바이저 프로필 조합이 포함되어 있습니다. **배포 마법사**에서 이 템플릿을 사용하여 서버 하드웨어를 프로비저닝하고 vCenter 내에 호스트를 배포합니다.

1. OpenManage Integration for VMware vCenter의 **관리** > **배포** 탭에서 **배포 템플릿**을 선택합니다.
2. 을 클릭합니다.
3. **배포 템플릿** 대화 상자에서 템플릿의 이름을 입력합니다.
4. 배포 템플릿에 대한 **설명**(선택 사항)을 입력합니다.
5. **시스템 프로필** 또는 **하드웨어 프로필**을 클릭하고 드롭다운 메뉴에서 적절한 프로필을 선택합니다.

   노트: 14세대 서버는 시스템 프로필을 사용하고 13세대 이전 서버는 하드웨어 프로필을 사용하는 것이 좋습니다.

6. 드롭다운 메뉴에서 **하이퍼바이저 프로필**을 선택합니다.
7. 프로필 선택 항목을 적용하고 변경사항을 저장하려면 **저장**을 클릭합니다. 취소하려면 **취소**를 클릭합니다.

배포 템플릿 관리

OpenManage Integration를 통해 기존 배포 템플릿에서 다음을 비롯한 몇 가지 관리 작업을 수행할 수 있습니다.
- 배포 템플릿 보기 또는 편집
- 배포 템플릿 삭제

배포 템플릿 보기 또는 편집

1. OpenManage Integration for VMware vCenter의 **관리** > **배포** 탭에서 **배포 템플릿**을 선택합니다.
   배포 템플릿 프로필이 표시됩니다.

2. **배포 템플릿** 대화 상자에서 새 템플릿의 이름 및 설명을 입력합니다.
   템플릿에 고유한 이름을 지정해야 합니다.
3. 드롭다운 메뉴에서 **하드웨어 프로필** 또는 **시스템 프로필**을 변경합니다.
4. 드롭다운 메뉴에서 **하이퍼바이저 프로필**을 변경한 다음 **저장**을 클릭합니다.

배포 템플릿 삭제

1. OpenManage Integration for VMware vCenter의 **관리** > **배포** 탭에서 **배포 템플릿**을 선택합니다.
2. **배포 템플릿** 페이지에서 템플릿을 선택하고 ✖를 클릭합니다.
3. 템플릿 삭제를 확인하려면 메시지 상자에서 **삭제**를 클릭하고 취소하려면 **취소**를 클릭합니다.

배포 마법사 정보

배포 마법사는 다음과 같은 배포 프로세스에 대해 설명합니다.

- 호환되는 운영 체제 미설치 서버를 선택합니다.

  노트: 14세대 서버 배포를 선택하는 경우 배포 템플릿 목록은 하드웨어 프로필이나 시스템 프로필 또는 하이퍼바이저 프로필이나 하드웨어와 하이퍼바이저의 조합 또는 시스템과 하이퍼바이저 프로필의 조합을 포함합니다.

  노트: 비 14세대 서버 또는 14세대와 비 14세대 서버의 조합을 선택하는 경우 배포 템플릿 목록은 하드웨어 프로필이나 하이퍼바이저 프로필 또는 하드웨어 프로필과 하이퍼바이저 프로필의 조합을 포함합니다.
- 하드웨어 및 하이퍼바이저 프로필로 구성된 배포 템플릿 선택.
- 설치 대상(하드 디스크 또는 IDSDM) 선택.

  하이퍼바이저를 배포할 때 내장 이중 SD 모듈에 배포할 수 있습니다. OMIVV가 포함된 하이퍼바이저를 배포하기 전에 BIOS에서 내장 이중 SD 모듈을 활성화해야 합니다.
- 호스트에 연결할 연결 프로필 선택.
- 각 호스트에 대한 네트워크 세부 사항 할당.
- vCenter, 대상 데이터 센터 또는 클러스터, 호스트 프로필(선택 사항) 선택.
- 서버 배포 작업 실행 예약.

노트: 하드웨어 프로필만 배포할 경우 배포 마법사의 서버 ID, 연결 프로필, 네트워크 세부사항 옵션은 건너뛰고 바로 **일정 배포** 페이지로 이동합니다.

노트: 평가 라이센스의 경우 라이센스가 만료되지 않은 이상 배포 마법사를 사용할 수 있습니다.

VLAN 지원

OMIVV에서는 라우팅 가능 VLAN에 대한 하이퍼바이저 배포를 지원하기 때문에 배포 마법사에서 VLAN 지원을 구성할 수 있습니다. 배포 마법사의 이 부분에는 VLAN의 용도를 지정하고 VLAN ID를 지정할 수 있는 옵션이 있습니다. VLAN ID를 입력하면 배포 중에 하이퍼바이저의 관리 인터페이스에 적용되고 모든 트래픽에 VLAN ID를 태깅합니다.

배포 중에 제공된 VLAN이 가상 어플라이언스 및 vCenter Server와 양쪽 모두 통신하는지 확인합니다. 이러한 대상 중 하나 또는 양쪽 모두에 통신할 수 없는 VLAN에 하이퍼바이저를 배포하면 배포가 실패합니다.

단일 배포 작업에서 복수의 베어 메탈 서버를 선택하고 같은 VLAN ID를 모든 서버에 적용하고 싶으면 배포 마법사의 서버 식별 부분에서 **선택된 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: OMIVV는 멀티홈 구성을 지원하지 않습니다. 보조 네트워크와의 통신을 위해 어플라이언스에 보조 네트워크 인터페이스를 추가하면 하이퍼바이저 배포, 서버 준수 및 펌웨어 업데이트와 관련된 워크플로에 문제가 발생합니다.

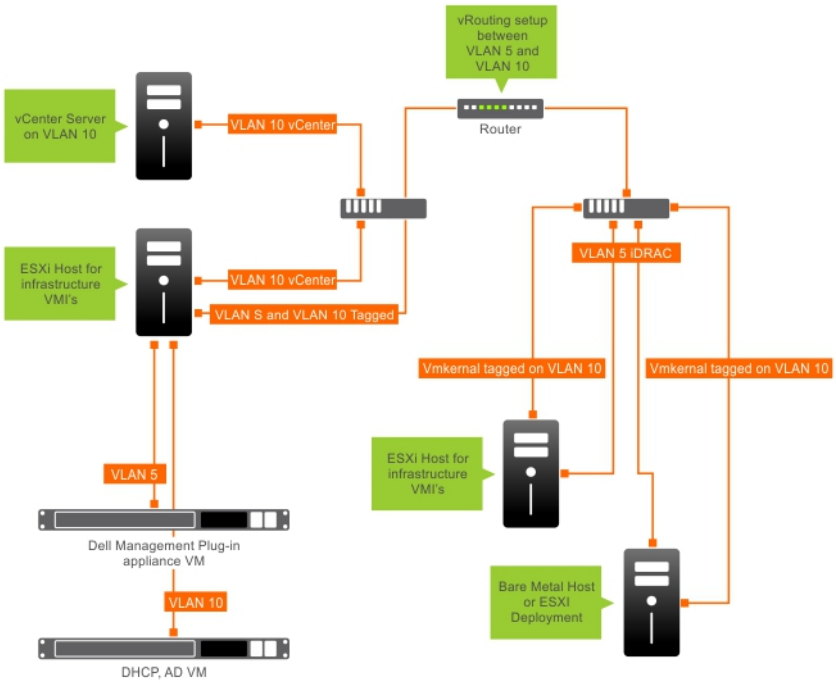

그림 2 . VLAN 네트워크.

이 네트워크 예에서 OMIVV 어플라이언스는 VLAN 5에 있고 배포되고 있는 ESXi 호스트의 VMkernal과 vCenter는 VLAN 10에 있습니다. OMIVV가 멀티 VLAN 홈을 지원하지 않기 때문에 모든 시스템이 서로 올바르게 통신하게 하려면 VLAN 5를 VLAN 10에 라우팅해야 합니다. 이러한 VLAN 간에 라우팅이 활성화되지 않으면 배포가 실패합니다.

배포 마법사 실행

배포 마법사를 실행하기 전에 하드웨어 프로필, 시스템 프로필 및 하이퍼바이저 프로필과 vCenter에 대한 연결 프로필을 사용하여 배포 템플릿을 만드십시오.

배포 마법사를 실행하려면 다음과 같이 하십시오.

1. OpenManage Integration for VMware vCenter에서 **관리** > **배포** 탭을 선택합니다.
2. **운영 체제 미설치 서버** 창에서 **배포 마법사 실행** 링크를 클릭합니다.
   배포 마법사 **시작** 페이지가 표시됩니다.
3. **시작** 페이지에서 정보를 읽고 **다음**을 클릭합니다.
4. 호환되는 운영 체제 미설치 서버를 배포 작업에 할당하려면 **배포용 서버 선택** 페이지에서 서버 목록 옆의 확인란을 클릭합니다.
5. **다음**을 클릭합니다.
6. **템플릿/프로필 선택** 페이지에서 다음 하위 단계를 수행합니다.
   a. **배포 템플릿**의 **배포 템플릿 선택**에서 기존 배포 템플릿을 선택하여 선택된 서버에 배포 템플릿을 할당합니다.

      노트: 시스템 프로필 기반 템플릿은 **배포용 서버를 선택하십시오.** 페이지에서 14세대 서버를 선택하는 경우에만 표시됩니다.

      드롭다운 목록에서 다음 배포 템플릿 중 하나를 선택할 수 있습니다.
      - 서버 하드웨어만 구성하는 하드웨어 프로필 전용 또는 시스템 프로필 전용 배포 템플릿을 선택할 경우 10단계로 이동합니다.
      - 하이퍼바이저 프로필을 배포하는 하이퍼바이저 프로필 배포 템플릿을 선택할 경우 6 (b) 이후부터 계속합니다.

        노트: 하드웨어 프로필 또는 시스템 프로필 전용 배포를 선택할 경우 **일정 배포** 페이지에 대한 정보를 포함하라는 메시지가 자동으로 표시됩니다.

   b. **하이퍼바이저 설치**에서 다음 중 한 가지 옵션을 선택합니다.
      - **첫 번째 부팅 디스크**- 하드 디스크(HDD), 솔리드 스테이트 드라이브(SSD), RAID 컨트롤러에 의해 생성된 가상 디스크에 하이퍼바이저를 배포합니다.
      - **내장 이중 SD 모듈** — IDSDM에 하이퍼바이저를 배포합니다.

노트: 선택된 서버 중 하나 이상에서 IDSDM을 사용할 수 있는 경우 **내장 이중 SD 모듈** 옵션이 활성화됩니다. 그렇지 않을 경우에는 **하드 디스크** 옵션만 사용할 수 있습니다.

선택된 서버 중 하나라도 IDSDM을 지원하지 않거나 배포 중에 IDSDM이 없는 경우 다음 작업 중 하나를 수행합니다:

노트: OS 배포 중에 **HardDiskFailOver**가 활성화되어 있는지 확인합니다.

- 하이퍼바이저를 서버의 첫 번째 부팅 디스크에 배포할 경우 **사용 가능한 내부 이중 SD 모듈이 없는 서버의 첫 번째 부팅 디스크에 하이퍼바이저 배포** 확인란을 선택합니다.
  주의: 이 옵션을 선택해 서버의 첫 번째 부팅 디스크에 하이퍼바이저를 배포하면 디스크 드라이브의 모든 데이터가 지워집니다.
- 선택한 서버에서 배포를 건너뛰고 다음 서버에서 하이퍼바이저 배포를 계속하려면 **사용 가능한 내부 이중 SD 모듈이 없는 서버의 첫 번째 부팅 디스크에 하이퍼바이저 배포**를 선택 취소합니다.

c. **자격 증명 프로필**에서 다음 작업 중 하나를 수행합니다.
   - **모든 서버에 이 자격 증명 프로필 사용** 옵션 단추를 선택하고 동일한 기존 프로필에 모든 서버를 할당하려면 드롭다운 목록에서 연결 프로필을 선택합니다.
   - **각 서버의 연결 프로필 선택** 옵션 단추를 클릭한 후 드롭다운 목록에서 각 서버의 개별 연결 프로필을 선택합니다.

7. **다음**을 클릭합니다.
   서버 식별 페이지가 표시됩니다.

   서버 식별은 두 가지 방법으로 제공할 수 있습니다.
   - 네트워킹 정보(IP 주소, 서브넷 마스크 및 게이트웨이)를 입력합니다. 호스트 이름의 정규화된 도메인 이름은 필수 항목입니다. FQDN에 *localhost*를 사용할 수 없습니다. FQDN은 호스트를 vCenter에 추가할 때 사용됩니다.
   - DHCP(Dynamic Host Configuration Protocol)를 사용하여 IP 주소, 서브넷 마스크, 게이트웨이 IP, 호스트 이름 및 기본/대체 DNS 서버를 구성합니다. DHCP 할당 IP 주소는 호스트를 vCenter에 추가할 때 사용됩니다. DHCP를 사용할 때는 선택된 NIC MAC 주소에 IP 예약을 사용하는 것이 좋습니다.

   노트: 호스트 이름에 localhost 대신 FQDN(Fully Qualified Domain Name)을 사용합니다. ESXi 5.1부터는 localhost 값을 사용하면 호스트에서 보낸 이벤트를 OMIVV 플러그인이 처리하지 못합니다. FQDN에 대한 IP 주소를 확인하는 DNS 레코드를 생성합니다. ESXi 5.1의 SNMP 경고가 올바르게 식별되도록 역방향 조회 요청을 지원하는 DNS 서버를 구성합니다. 배포 작업 실행을 예약하려면 DHCP 예약 및 DNS 호스트 이름이 있고 확인되어야 합니다.

8. **서버 식별** 페이지에서 다음을 수행합니다.
   이 페이지에는 VLAN ID를 지정하는 옵션이 있습니다. VLAN ID를 입력하면 배포 중 하이퍼바이저의 관리 인터페이스에 적용되고 모든 트래픽에 VLAN ID를 태깅합니다. 서버 식별은 배포된 서버에 새 이름과 네트워크 식별을 할당합니다. VLAN 지원을 참조하십시오.

   a. 개별 서버 정보를 확장 및 표시하려면 **선택된 서버**에서 을 클릭합니다.
   b. **호스트 이름 및 NIC**에서 서버의 **정규화된 호스트 이름**을 입력합니다.
   c. **NIC 관리 작업** 드롭다운 목록에서 서버 관리에 사용할 NIC를 선택합니다.
   d. IP 주소, 서브넷 마스크, 기본 게이트웨이, DNS 정보를 입력하거나 **DHCP를 사용하여 가져오기** 확인란을 선택합니다.
   e. VLAN ID가 필요한 네트워크에 배포하는 경우 **VLAN** 확인란을 선택한 다음 **VLAN ID**를 입력합니다.
      VLAN ID에 1 - 4094 범위의 숫자를 사용합니다. VLAN ID 0은 프레임 우선순위를 태그 지정하도록 예약되어 있습니다.
   f. 배포할 모든 서버에 대해 a - h 단계를 반복하거나 **선택된 모든 서버에 설정 적용** 확인란을 선택합니다.
      선택된 모든 서버에 설정 적용을 선택한 경우 기타 서버에 대해 FQDN 이름과 IP 주소를 입력합니다.
      노트: 서버에 대해 FQDN 이름을 지정할 경우 각 서버에 대해 고유한 호스트 이름을 지정하십시오.

9. **다음**을 클릭합니다.
10. **배포 예약** 페이지에서 다음 작업을 수행합니다.
    a. **작업 이름** 및 **작업 설명**을 입력합니다.
    b. **vCenter 설정**에 대해 다음을 입력합니다.
       i. **vCenter 인스턴스**에서 배포 후에 호스트를 관리하는 서버 인스턴스를 선택합니다.
       ii. **vCenter 대상 컨테이너**에 대해 **찾아보기**를 클릭하여 vCenter 대상을 검색합니다.
       iii. **vCenter 호스트 프로필**에서 호스트 구성을 캡슐화하고 호스트 구성을 관리하는 데 유용한 프로필을 선택합니다(선택 사항).
    c. 작업 일정을 선택하여 배포 작업을 실행할 시기를 결정합니다.
       i. **배포 작업 예약**을 선택합니다.
          - 캘린더 제어를 사용하여 날짜를 선택합니다.
          - 시간을 입력합니다.

ii. 작업을 즉시 시작하려면 **지금 배포 작업 실행**을 선택합니다.

배포 작업이 시작된 후 작업 대기열로 이동하려면 **작업 제출 후 작업 대기열로 이동합니다**를 선택합니다.

11. **마침**을 클릭합니다.

배포 마법사 작업이 완료되면 **작업 큐**를 사용하여 배포 작업을 관리할 수 있습니다.

작업 큐를 사용하여 배포 관리

1. OpenManage Integration for VMware vCenter의 **모니터** > **작업 큐** 탭에서 **배포 작업**을 클릭합니다.
   배포 작업에 대한 다음 세부 정보가 상단 그리드에 표시됩니다.
   - 이름
   - 설명
   - 예약된 시간
   - 상태
   - 컬렉션 크기
   - 진행률 요약
2. **배포 작업 세부 정보**를 업데이트하려면 **새로 고침**을 클릭합니다.
3. 배포 작업에 포함된 서버에 대한 세부 정보가 포함되어 있는 배포 작업 세부 정보를 표시하려면 상단 그리드에서 배포 작업을 선택합니다.
   다음과 같은 세부 정보가 하단 그리드에 표시됩니다.
   - 서비스 태그
   - iDRAC IP 주소
   - 작업 상태
   - 경고
   - 배포 작업 세부 정보(마우스를 올려 놓으면 추가 정보가 제공됨)
   - 시작 및 종료 시간
   - 추가 세부 정보

   작업을 선택하고 배포 작업의 **세부 정보** 열 위에 커서를 올려 놓으면 배포 작업에 대한 전체 정보를 팝업 텍스트로 볼 수 있습니다.

   시스템 프로필 기반 작업 실패에 대한 자세한 내용을 보려면 **자세히 보기**를 클릭하십시오. **자세히 보기** 페이지에는 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 이름**과 같지 않습니다.

   세부 정보를 .CSV 파일로 내보내려면 데이터 그리드의 오른쪽 모서리에 있는  를 클릭합니다.
4. 배포 작업을 중단하려면  아이콘을 클릭합니다.
5. 메시지가 표시되는 경우 중단하려면 **작업 중단**을 클릭하고 취소하려면 **작업을 중단하지 않음**을 클릭합니다.
6. **배포 작업 큐 제거** 창을 표시하려면  를 클릭합니다. **이전 날짜 및 작업 상태**를 선택하고 **적용**을 클릭합니다.
   그러면 선택한 작업이 큐에서 지워집니다.

시스템 잠금 모드 작업

1. **OpenManage Integration for VMware vCenter** 페이지에서 **모니터링** > **작업 큐** 탭을 클릭한 다음 **시스템 잠금 모드 작업**을 클릭합니다.
   시스템 잠금 모드 작업에 대한 다음 정보가 상단 그리드에 표시됩니다.
   - 이름
   - 설명
   - 예약된 시간

- vCenter
- 상태
- 컬렉션 크기
- 진행률 요약

2. **시스템 잠금 모드 작업 세부 정보**를 업데이트하려면 **새로 고침** 아이콘을 클릭합니다.
3. 시스템 잠금 모드 작업에 포함된 서버의 세부 정보가 있는 시스템 잠금 모드 작업 세부 정보를 표시하려면 상단 그리드에서 시스템 잠금 모드 작업을 선택합니다.
   다음과 같은 세부 정보가 하단 그리드에 표시됩니다.
   - 서비스 태그
   - iDRAC IP
   - 호스트 이름
   - 상태
   - 세부 정보

     노트: **상태** 열에 **성공**이 표시되면 **세부 정보** 열이 비어 있습니다.

     상태 열에 **실패**가 표시되면 실패에 관한 이유가 **세부 정보** 열에 표시됩니다.
   - 시작 날짜 및 시간
   - 종료 날짜 및 시간

   작업을 선택하고 시스템 잠금 모드 작업의 **세부 정보** 열 위에 커서를 올려 놓으면 시스템 잠금 모드 작업에 대한 전체 정보를 팝업 텍스트로 볼 수 있습니다.
4. 시스템 잠금 모드 작업을 제거하려면, 를 클릭합니다. **이전 날짜 및 작업 상태**를 선택하고 **적용**을 클릭합니다.
   그러면 선택한 작업이 작업 큐에서 지워집니다.

변경 사항 감지 작업

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

1. **OpenManage Integration for VMware vCenter** 페이지에서 **모니터링** > **작업 큐** 탭을 클릭한 다음, **변경 사항 감지 작업**을 클릭합니다.

   변경 사항 감지 작업에 대한 다음 정보가 상단 그리드에 표시됩니다.
   - 이름
   - 마지막 실행
   - 다음 실행
   - 상태
   - 컬렉션 크기
   - 진행률 요약
2. 업데이트된 **변경 사항 감지 작업 세부 사항**을 보려면 **새로 고침**을 클릭합니다.
3. 변경 사항 감지 작업에 포함된 서버에 대한 자세한 내용이 들어 있는 변경 사항 감지 작업 세부 사항을 표시하려면 상단 그리드에서 변경 사항 감지 작업을 선택합니다.

   다음과 같은 세부 정보가 하단 그리드에 표시됩니다.
   - 서비스 태그
   - iDRAC IP
   - 호스트 이름
   - 클러스터
   - vCenter
   - 상태
   - 시작 날짜 및 시간
   - 종료 날짜 및 시간
4. **변경 사항 감지 작업**을 실행하려면 단추를 클릭합니다.

노트: 기준선 클러스터에서 연결 프로필에 호스트 장치를 추가하고 나면 새로 추가된 호스트 장치에 대해 변경 사항 감지 작업이 자동으로 실행됩니다.

펌웨어 업데이트 작업 관리

이 페이지에 있는 정보를 보려면 클러스터에 대해 펌웨어 업데이트 작업을 실행합니다. 클러스터에 대해 펌웨어 업데이트 마법사 실행을 참조하십시오.

페이지에 모든 펌웨어 업데이트 작업이 표시됩니다. 이 페이지에서 펌웨어 업데이트 작업을 보거나 새로 고치거나 제거하거나 중단할 수 있습니다.

1. OpenManage Integration에서 **모니터** > **작업 큐** > **펌웨어 업데이트**를 선택합니다.
2. 최신 정보를 표시하려면 **새로 고침** 아이콘을 클릭합니다.
3. 데이터 격자에서 상태를 봅니다.
   그리드는 펌웨어 업데이트 작업에 대한 다음과 같은 정보를 제공합니다.
   - 상태
   - 예약된 시간
   - 이름
   - 설명
   - vCenter
   - 컬렉션 크기(펌웨어 인벤토리 작업의 서버 수)
   - 진행률 요약(펌웨어 업데이트 진행률 세부 정보)
4. 특정 작업에 대해 보다 자세한 정보를 보려면 특정 작업의 데이터 격자에서 작업을 클릭하십시오.
   여기에서 다음과 같은 상세 정보를 찾을 수 있습니다.
   - 호스트 이름
   - 상태
   - 시작 시간
   - 종료 시간
5. 실행 중이지 않은 예약된 펌웨어 업데이트를 중단하려면 중단하려는 작업을 선택하고  을 클릭합니다.
   노트: 이미 iDRAC에 제출된 펌웨어 업데이트 작업을 중단할 경우 호스트에서는 펌웨어가 업데이트될 수 있지만 OMIVV에서 작업이 취소된 것으로 보고합니다.
6. 이전 펌웨어 업데이트 작업 또는 예약된 펌웨어 업데이트를 제거하려면  를 클릭합니다.
   펌웨어 업데이트 작업 제거 대화 상자가 표시됩니다. 취소, 성공 또는 실패한 작업만 제거할 수 있으며 예약된 또는 활성 작업은 제거할 수 없습니다.
7. **펌웨어 업데이트 작업 제거** 대화 상자에서 **이전**을 선택하고 **적용**을 클릭합니다.
   그러면 선택한 작업이 큐에서 지워집니다.

배포 작업 타이밍

몇 가지 요인에 따라 운영 체제 미설치 서버의 프로비저닝 및 배포를 완료하는 데 30분에서 몇 시간이 소요될 수 있습니다. 배포 작업을 시작할 때는 제공된 지침에 따라 배포 시간을 계획하는 것이 좋습니다. 프로비저닝 및 배포를 완료하는 데 걸리는 시간은 배포 유형, 복잡성, 동시에 실행되는 배포 작업 수에 따라 다릅니다. 다음 표는 배포 작업에 걸릴 수 있는 대략적인 시간을 제공합니다. 배포 작업은 전체 배포 작업에 걸리는 시간을 개선하기 위해 최대 5대의 연속 서버에서 배치로 실행됩니다. 정확한 동시 작업 수는 사용 가능한 리소스에 따라 다릅니다.

표 37. 대략적인 배포 시간

배포 유형	배포 당 예상 소요 시간
하이퍼바이저만	30분 - 130분
하이퍼바이저 및 하드웨어 프로필	1 - 4시간
시스템 프로필만	5 - 6분

표 37. 대략적인 배포 시간 (계속)

배포 유형	배포 당 예상 소요 시간
시스템 프로필 및 하이퍼바이저 프로필	30 - 40분

배포 시퀀스 내의 서버 상태

인벤토리 작업을 실행하면 자동/수동으로 검색된 운영 체제 미설치 시스템이 다른 상태로 분류되므로 데이터센터에 새로운 서버인지 또는 예약된 배포 작업이 보류 중인지를 확인할 수 있습니다. 관리자는 다음 상태를 사용하여 서버를 배포 작업에 포함할지 여부를 결정합니다. 상태는 다음과 같습니다.

표 38. 배포 시퀀스의 서버 상태

서버 상태	설명
구성되지 않음	서버가 OMIVV에 접속했으며 구성을 대기하는 중입니다.
구성됨	서버에 성공적인 하이퍼바이저 배포에 필요한 모든 하드웨어 정보가 구성되어 있습니다.

사용자 지정 Dell EMC ISO 이미지 다운로드

배포를 위해서는 모든 Dell 드라이버가 포함되어 있는 사용자 지정 ESXi 이미지가 필요합니다.

1. `support.dell.com`으로 이동합니다.
2. **모든 제품 중에서 선택** > **서버, 스토리지 및 네트워킹**을 클릭합니다.
3. **제품 선택**에서 **PowerEdge**를 클릭합니다.
4. PowerEdge 서버 모델을 클릭합니다.
5. 서버 모델의 **드라이버 및 다운로드** 페이지를 클릭합니다.
6. **OS 변경** 링크를 클릭한 다음 원하는 ESXi 시스템을 선택합니다.
7. **엔터프라이즈 솔루션**을 클릭합니다.
8. **엔터프라이즈 솔루션** 목록에서 필요한 ISO 버전을 선택하고 **다운로드**를 클릭합니다.

14

호스트, 베어 메탈 및 iDRAC 준수 정보

OMIVV로 호스트 및 베어 메탈 서버를 관리하려면 각각 특정한 최소 조건을 충족해야 합니다. 준수하지 않는 경우에는 OMIVV로 올바르게 관리되지 않습니다. OMIVV는 베어 메탈 또는 호스트에서 비준수에 대한 세부 정보를 표시하고 해당하는 경우 비준수를 수정할 수 있도록 합니다.

각각의 경우 다음 중 하나를 실행하여 준수 문제를 보고 해결할 수 있습니다.

- vSphere 호스트 준수 문제를 보고 해결하려면 비준수 vSphere 호스트 마법사 실행을 참조하십시오.
- 준수 문제가 있는 베어 메탈 서버를 보고 해결하려면 비준수 베어 메탈 서버 마법사 실행을 참조하십시오.

주제:

vSphere 호스트에 대한 준수 보고 및 해결

다음과 같은 경우에는 호스트가 준수되지 않습니다.

- 호스트가 연결 프로필에 할당되지 않은 경우.
- CSIOR(Collect System Inventory on Reboot)이 사용되지 않도록 설정되어 있거나 실행되지 않은 경우. 이 경우에는 수동으로 다시 부팅해야 합니다.
- OMSA 에이전트가 설치되지 않았거나 오래되었거나 올바르게 구성되지 않은 경우. 11세대 서버에서 MSA가 설치 또는 업데이트된 경우 ESXi 호스트 재부팅이 필요합니다.
- 호스트의 SNMP 트랩 대상이 OMIVV 어플라이언스 IP 주소에 구성되어 있지 않습니다. 14세대 호스트에서만 연결 프로필에 제공한 iDRAC 또는 호스트 자격 증명이 올바르지 않거나, iDRAC에 여유 슬롯이 없거나, iDRAC 잠금 모델이 켜져 있는 경우 SNMP 트랩 대상 설정 실패가 발생할 수 있습니다.
- OMIVV가 ESXi 6.5를 실행하는 호스트에서 WBEM 서비스 활성화에 실패했습니다.

주의: 잠금 모드의 호스트는 비준수 호스트인 경우에도 준수 확인에 나타나지 않습니다. 해당 준수 상태를 파악할 수 없기 때문에 표시되지 않습니다. 이러한 시스템의 준수 여부는 수동으로 확인해야 합니다. 이러한 시나리오에서는 경고 메시지가 표시됩니다.

정보비준수 vSphere 호스트 마법사를 실행하여 준수하지 않는 호스트를 해결할 수 있습니다. OMSA를 설치 또는 업데이트해야 할 경우 일부 비준수 ESXi 호스트는 재부팅이 필요합니다. 또한 CSIOR을 실행한 적이 없는 호스트에서도 재부팅이 필요합니다. 또한 CSIOR을 실행한 적이 없는 호스트에도 재부팅이 필요합니다. ESXi 호스트가 자동으로 다시 부팅되도록 선택하는 경우 다음과 같은 조치가 수행됩니다.

- CSIOR 상태 해결:

  CSIOR을 호스트에서 실행하지 않은 경우 호스트에서 CSIOR이 **켜짐**으로 설정되고 호스트가 유지 관리 모드로 설정된 다음 다시 부팅됩니다.

- OMSA가 설치되지 않거나 지원되지 않는 버전의 OMSA를 실행하는 호스트의 경우:
  - OMSA가 호스트에 설치됩니다.
  - 호스트가 유지 관리 모드로 설정된 다음 다시 부팅됩니다.
  - 다시 부팅이 완료된 후 변경사항이 적용되도록 OMSA가 구성됩니다.
  - 호스트의 유지 관리 모드가 종료됩니다.
  - 인벤토리가 실행되어 데이터가 새로 고쳐집니다.
- 지원되는 버전의 OMSA가 설치되어 있지만 구성해야 하는 OMSA 상태 해결:
  - OMSA가 호스트에 구성됩니다.
  - 인벤토리가 실행되어 데이터가 새로 고쳐집니다.

비준수 호스트를 확인하고 해결하려면 다음과 같이 하십시오.

1. OpenManage Integration for VMware vCenter의 **관리** 탭에서 **준수** > **vSphere 호스트**를 클릭합니다.
   a. **vSphere 호스트** 페이지에서 비준수 호스트 목록을 봅니다.

비준수 호스트와 함께 호스트 IP 또는 호스트 이름, 모델, 연결 프로필, CSIOR 상태, OMSA 상태, WBEM 상태, SNMP 트랩 상태, 하이퍼바이저, iDRAC 라이센스 상태가 나열된 표가 표시됩니다.

b. 비준수 호스트에 대한 정보를 자세히 보려면 비준수 호스트를 선택합니다.

c. 표 안에서 열을 바꾸려면 데이터 그리드 내에서 열을 끌어 놓습니다.

2. 비준수 호스트를 해결하려면 **비준수 vSphere 호스트 해결**을 클릭합니다.

   비준수 vSphere 호스트 해결 마법사가 실행됩니다. 이는 동적 마법사이고 선택된 비준수 호스트와 관련된 페이지만 표시됩니다.

   선택한 모든 비준수 호스트가 CSIOR와 호환될 경우 마법사에서 **CSIOR 켜기** 페이지를 볼 수 있습니다.

3. **비준수 vSphere 호스트 해결** 마법사의 **시작** 페이지에서 **다음**을 클릭합니다.
4. **비준수를 해결할 vSphere 호스트 선택 마법사** 페이지에서 해결하려는 호스트의 확인란을 선택합니다.
5. **다음**을 클릭합니다.
   선택된 호스트 중 연결 프로필에 할당되지 않은 호스트가 있을 경우 경고 메시지가 표시되고 준수 마법사를 계속 실행할 것인지 아니면 준수 해결 마법사를 취소할 것인지 묻는 메시지가 표시됩니다. 연결 프로필 비준수를 해결하려면 다음 중 하나를 수행하십시오.
   - 준수 마법사에서 연결 프로필이 할당되지 않은 호스트를 제외하려면 **준수 계속 마법사**를 클릭합니다.
   - 마법사를 종료하고 **연결 프로필** 페이지에서 시스템을 해결하려면 **취소**를 클릭합니다. 연결 프로필 생성 페이지 32을 참조하십시오. 연결 프로필이 생성되면 마법사로 돌아올 수 있습니다.
6. 경고 메시지에서 **준수 계속 마법사**를 클릭한 경우 **CSIOR 켜기** 창에서 확인란을 선택하여 선택된 호스트의 **CSIOR**을 켭니다.
7. **다음**을 클릭합니다.
8. **OMSA 해결** 창에서, 선택한 호스트에 대해 **OMSA**를 해결하려면 확인란을 선택합니다.
9. **다음**을 클릭합니다.
10. **호스트 재부팅** 창에서 재부팅해야 하는 ESXi 호스트를 확인합니다.

    OMSA가 설치 또는 업데이트된 경우 ESXi 호스트 재부팅이 필요합니다. 또한 CSIOR을 실행한 적이 없는 호스트에도 재부팅이 필요합니다. 다음 중 하나를 실행하십시오.
    - 호스트를 유지 관리 모드로 자동 전환하고 필요할 때마다 다시 부팅하려면 **호스트를 유지 관리 모드로 자동 전환하고 필요할 때마다 다시 부팅** 확인란을 선택합니다.
    - 수동으로 재부팅하려는 경우 OMSA를 설치한 후 호스트를 재부팅하고 호스트가 실행되면 OMSA를 수동으로 또는 준수 마법사를 통해 구성합니다. OMSA가 구성되지 않은 경우에는 인벤토리를 다시 실행합니다. 인벤토리 작업 실행을 참조하십시오.
11. **다음**을 클릭합니다.
12. **요약** 창에서 비준수 호스트에서 실행되는 작업을 검토합니다.
    요약 페이지의 작업이 실행되려면 수동 재부팅이 필요합니다.
13. **마침**을 클릭합니다.

연결 프로필에 유효한 정보를 제공하여 iDRAC 또는 호스트 자격 증명을 수정하거나, 처음 4개의 슬롯 중 하나를 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 14세대 서버에만 적용할 수 있습니다.

WBEM 비준수 호스트가 존재하는 경우 WBEM 서비스 활성화 실패로 이어지는 해당 호스트의 조건을 수동으로 수정할 수 있는지 확인합니다. 사용자 로그에서 확인하고 OMIVV에서 인벤토리 작업 중 해당 호스트에 대한 WBEM 서비스를 활성화해 오류 조건을 수정할 수 있습니다.

vSphere 호스트에 대한 iDRAC 라이센스 준수 해결

vSphere 호스트 준수 페이지에 나열된 vSphere 호스트는 준수하는 iDRAC 라이센스가 없으므로 호환되지 않습니다. 표에 iDRAC 라이센스 상태가 표시되어 있습니다. 비준수 호스트를 클릭하여 iDRAC 라이센스의 남은 일수 같은 추가 세부 정보를 보고, 필요한 경우 업데이트할 수 있습니다. 연결 프로필과 관련된 호스트 중 하나의 iDRAC 준수 상태가 "비준수" 또는 "알 수 없음"인 경우 **인벤토리 작업 실행** 링크가 활성화됩니다.

1. OpenManage Integration for VMware vCenter의 **관리** 탭에서 **준수** > **vSphere 호스트**를 클릭합니다.
2. **iDRAC 라이센스 상태**가 **비준수**인 호스트를 선택합니다.
3. 라이센스가 오래된 경우 **iDRAC 라이센스 구입/갱신** 링크를 클릭합니다.
4. **Dell 라이센스 관리** 페이지에 로그인하여 업데이트하거나 새 iDRAC 라이센스를 구입합니다.
   이 페이지에 있는 정보를 사용하여 iDRAC를 식별하고 업데이트합니다.
5. iDRAC 라이센스를 설치한 후 vSphere 호스트에 대해 인벤토리 작업을 실행하고 인벤토리 작업을 완료한 후 이 페이지로 돌아옵니다.

기준선 준수 보기

기준선 준수 페이지는 클러스터 프로필과 연결된 모든 OMIVV 관리 vSAN 호스트를 위해 변경 사항 감지를 토대로 기준선 준수 상태를 표시합니다.

- 구성 준수—클러스터 프로필에 사용된 시스템 프로필과 관련 vSAN 호스트 간의 특성에서 변경 사항을 표시합니다.
- 펌웨어 및 드라이버 준수—클러스터 프로필에 사용된 펌웨어 및/또는 드라이버 리포지토리 프로필과 관련 vSAN 호스트 간의 펌웨어와 드라이버 버전 변경 사항을 표시합니다.

1. **VMware vCenter에 대한 OpenManage 통합** 페이지에서 **관리** > **준수** > **기준선 준수**를 클릭합니다.
   기준선과 연결된 비준수 호스트와 함께 호스트 IP 또는 FQDN, vCenter IP 또는 FQDN, 클러스터 이름, 클러스터 프로필 이름, 구성 준수 상태, 펌웨어 준수 상태 및 드라이버 준수 상태를 나열하는 표가 표시됩니다.

   노트: 기준선 준수 페이지에는 비준수 호스트만 표시됩니다.

   준수 범주는 다음과 같습니다.
   - **준수**—호스트의 구성 요소가 기준선에서 연결된 프로필을 준수함을 나타냅니다.
   - **비준수**—호스트의 구성 요소가 기준선에서 연결된 프로필을 준수하지 않음을 나타냅니다.
   - **적용되지 않음**—펌웨어 또는 드라이버 또는 시스템 프로필이 클러스터 프로필과 연결되지 않음을 나타냅니다.

   a. 호스트에 대한 정보를 자세히 보려면 원하는 호스트를 선택합니다.

      맨 아래 창에서 **호스트 이름** 및 **마지막 변경 사항 감지 시간**을 볼 수 있습니다.

   b. 표 안에서 열을 바꾸려면 데이터 그리드 내에서 열을 끌어 놓습니다.
   c. 데이터 그리드의 내용을 필터링하려면 **필터**를 사용합니다.

   노트: 기준선 준수 페이지에 대한 다음 정보를 확인할 수 있습니다.
   - 총 비준수 호스트 수
   - 총 비준수 클러스터 수
   - 기준선과 연결된 총 호스트 및 클러스터 수
   - 변경 사항 유형의 총 비준수 호스트 배포 수

2. 변경 사항 감지 작업이 성공적으로 완료되면 기준선과 연결된 호스트가 표에 나열됩니다. 변경 사항 세부 사항을 보려면 원하는 호스트를 선택하고 **변경 사항 세부 사항 표시**를 클릭합니다.
   변경 사항 세부 사항 대화 상자가 표시됩니다.
3. **변경 사항 세부 사항** 대화 상자에서는 다음을 확인할 수 있습니다.
   - 준수 변경 사항 감지 작업이 실패하면 실패 이유와 함께 준수 상태가 "비준수"로 표시됩니다. 나타나는 이유를 사용하여 문제를 해결하십시오.
   - 변경 사항 감지 작업이 성공하면 준수 상태가 "비준수"로 표시되고 다음 세부 정보가 **변경 사항 세부 정보** 페이지에 표시됩니다.

     하드웨어의 경우
     - 인스턴스—하드웨어 구성 요소 이름을 나타냅니다.
     - 그룹—특성의 그룹 이름을 나타냅니다.
     - 특성 이름—특성 이름을 나타냅니다.
     - 현재 값—호스트 값을 나타냅니다.
     - 기준선 값—기준선 값을 나타냅니다.
     - 변경 사항 유형—비준수 이유를 나타냅니다. 변경 사항 유형에 대한 자세한 내용은 구성 요소와 기준선 버전 비교 매트릭스 페이지 150을(를) 참조하십시오.

     펌웨어 및 드라이버의 경우
     - 구성 요소 이름—구성 요소의 이름을 나타냅니다.
     - 현재 값—호스트 값을 나타냅니다.
     - 기준선 값—기준선 값을 나타냅니다.
     - 변경 사항 유형—비준수 이유를 나타냅니다. 변경 사항 유형에 대한 자세한 내용은 구성 요소와 기준선 버전 비교 매트릭스 페이지 150을(를) 참조하십시오.
     - 임계성(펌웨어에 해당)—식별된 구성 요소 버전의 업데이트에 대한 중요도 수준을 나타냅니다.
     - 권장 사항(드라이버에 해당)—식별된 구성 요소 버전의 업데이트에 대한 중요도 수준을 나타냅니다.
     - 재부팅 필요—어플라이언스 재부팅이 필요한지 여부를 나타냅니다.

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

4. **마침**을 클릭합니다.

11세대 서버에서 OMSA 사용

PowerEdge 11세대 서버를 관리하려면 OMIVV에서 OMSA가 실행되고 있어야 합니다. OMIVV를 통해 배포된 11세대 호스트의 경우 OMSA가 자동으로 설치됩니다. 수동으로 배포하는 11세대 호스트의 경우 다음 중 하나를 선택할 수 있습니다.

- OMIVV를 사용하여 OMSA를 설치 및 구성합니다. OMSA 트랩 대상 설정 페이지 119을 참조하십시오.
- OMSA를 수동으로 설치 및 구성합니다. ESXi 시스템에 OMSA 에이전트 배포 페이지 119를 참조하십시오.

노트: OMIVV를 사용하여 OMSA 에이전트를 배포하면 OMIVV에서 HttpClient 서비스를 시작하고 OMSA VIB를 다운로드하고 설치할 ESXi 5.0 이후의 릴리스에서 포트 8080을 활성화합니다. OMSA 설치가 완료되면 서비스가 자동으로 중지되고 포트가 닫힙니다.

노트: 위의 옵션 이외에 OMSA 에이전트를 설치 및 구성하는 웹 클라이언트 호스트 준수를 사용할 수 있습니다.

ESXi 시스템에 OMSA 에이전트 배포

ESXi 시스템에 OMSA VIB를 설치하여 시스템에서 인벤토리 및 경고 정보를 수집합니다.

노트: Dell PowerEdge 12세대 서버 이전의 Dell 호스트에서는 OpenManage 에이전트가 필요합니다. OpenManage Integration for VMware vCenter를 설치하기 전에 호스트에 수동으로 OMSA를 설치하거나 OpenManage Integration for VMware vCenter를 사용하여 OMSA를 설치합니다. 다음에 OMSA 에이전트를 수동으로 설치하는 방법에 대한 자세한 내용이 나와 있습니다. http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.openmanage-server-administrator-omsa.aspx

1. OMSA가 설치되어 있지 않은 경우 **www.vmware.com**에서 vSphere 명령줄 도구(vSphere CLI)를 설치합니다.
2. 다음 명령을 입력합니다.

```
Vihostupdate.pl -server <IP Address of ESXi host> -i -b <OMSA version X.X>
```

노트: OMSA를 설치하는 데 몇 분 정도 걸립니다. 이 명령을 완료한 후에는 호스트를 다시 부팅해야 합니다.

노트: SNMP 커뮤니티 문자열은 **관리** > **설정** > **어플라이언스 설정** > **OMSA SNMP 트랩 커뮤니티 문자열**에서 구성할 수 있습니다. SNMP 트랩 커뮤니티 문자열에 대한 자세한 내용은 SNMP 트랩 커뮤니티 문자열 구성을 참조하십시오.

OMSA 트랩 대상 설정

모든 11세대 호스트에 OMSA가 구성되어 있어야 합니다.

노트: OMSA는 PowerEdge 12세대 이전의 Dell EMC 서버에서만 필요합니다.

OMSA 트랩 대상을 설정하려면 다음을 수행합니다.

1. 웹 브라우저에서 `https://<HostIP>:1311/` url을 입력하여 OMSA 에이전트로 이동합니다.
2. 인터페이스에 로그인하고 **경고 관리** 탭을 선택합니다.
3. **경고 조치**를 선택하고 이벤트가 게시되도록 모니터링되는 모든 이벤트에 **브로드캐스트 메시지** 옵션이 설정되어 있는지 확인합니다.
4. 탭 맨 위에서 **플랫폼 이벤트** 옵션을 선택합니다.
5. 회색 **대상 구성** 단추를 클릭하고 **대상** 링크를 클릭합니다.
6. **대상 활성화** 확인란을 선택합니다.
7. **대상 IP 주소** 필드에 OMIVV 어플라이언스 IP 주소를 입력합니다.
8. **변경사항 적용**을 클릭합니다.
9. 1-8단계를 반복하여 추가 이벤트를 구성합니다.

노트: SNMP 커뮤니티 문자열은 **관리** > **설정** > **어플라이언스 설정** > **OMSA SNMP 트랩 커뮤니티 문자열**에서 구성할 수 있습니다. SNMP 트랩 커뮤니티 문자열에 대한 자세한 내용은 SNMP 트랩 커뮤니티 문자열 구성을 참조하십시오.

운영 체제 미설치 서버의 준수 보고 및 해결

다음과 같은 경우에는 운영 체제 미설치 서버가 준수되지 않습니다.

- 지원되는 서버가 아닌 경우.
- 지원되는 iDRAC 라이센스가 없는 경우(iDRAC Express가 최소 요구 사항).
- 지원되는 버전의 iDRAC, BIOS 또는 LC가 없는 경우.
- LOM 또는 rNDC가 없는 경우.
- 시스템 잠금 모드가 설정되었습니다.

준수하지 않는 운영 체제 미설치 서버 목록을 확인하고 해결하려면 다음과 같이 하십시오.

1. OpenManage Integration for VMware vCenter에서 **관리** > **배포** 탭을 선택합니다.
   a. **운영 체제 미설치 서버** 페이지에서 비준수 서버 목록을 봅니다.
      비준수 서버와 함께 서비스 태그, 모델, iDRAC IP, 서버 상태, 시스템 잠금 모드, 준수 상태, iDRAC 라이센스 상태가 나열된 표가 표시됩니다.
   b. 서버에 대한 정보를 보려면 비준수 서버를 선택합니다.
   c. 서버의 비준수 정보를 CSV 파일로 내보내려면 표 오른쪽 모서리에 있는  를 클릭합니다.
   d. 데이터 그리드의 내용을 필터링하려면 **필터** 필드를 클릭합니다.
   e. 표 안에서 열을 바꾸려면 데이터 그리드 내에서 열을 끌어 놓습니다.
2. 비준수 서버를 해결하려면 **비준수 서버 해결**을 클릭합니다.

   노트: **비준수 서버 수정** 링크는 11세대 비준수 서버에 대해서만 활성화됩니다.

3. **운영 체제 미설치 준수 해결** 마법사의 **시작** 페이지에서 **다음**을 클릭합니다.
4. **준수 해결** 페이지에서 해결하려는 서버의 확인란을 선택합니다.
   비준수 서버가 나열되고 해당하는 비준수 펌웨어 구성 요소가 표시됩니다. 나열된 비준수 서버는 다음 펌웨어 구성 요소 중 하나 이상을 업데이트해야 합니다.
   - **iDRAC IP**

     노트: OMIVV에서는 iDRAC 라이센스가 준수하지 않는 운영 체제 미설치 서버를 해결할 수 없습니다. 지원되는 iDRAC 라이센스를 OMIVV 밖의 서버로 업로드한 다음 **운영 체제 미설치 서버 새로 고침**을 클릭합니다. 베어 메탈 서버 새로 고침 페이지 121을 참조하십시오.
   - **BIOS**
   - **LC**
   - **시스템 잠금 모드**

     노트: 해당 iDRAC에서 비준수 운영 체제 미설치 서버의 최신 세부 정보를 보려면 **운영 체제 미설치 세부 정보 새로 고침**을 클릭합니다. 시스템 잠금 모드가 켜져 있는 경우 서버는 비준수이며 반대의 경우도 마찬가지입니다.
5. 준수 문제 세부 정보를 보려면 **준수 문제**를 클릭합니다.

   노트: 시스템 잠금 모드가 켜져 있어 운영 체제 미설치 서버가 비준수인 경우 iDRAC 콘솔에서 서버의 시스템 잠금 모드를 수동으로 구성할지 확인합니다.

6. **다음**을 클릭합니다.
7. **요약** 창에서 비준수 운영 체제 미설치 서버의 펌웨어 구성 요소에 대해 수행되는 작업을 검토합니다.
8. **마침**을 클릭합니다.

운영 체제 미설치 서버의 iDRAC 라이센스 준수 해결

운영 체제 미설치 서버 페이지에 나열된 운영 체제 미설치 서버는 준수하는 iDRAC 라이센스가 없으므로 호환되지 않습니다. 표에 iDRAC 라이센스 상태가 표시되어 있습니다. 비준수 운영 체제 미설치 서버를 클릭하여 iDRAC 라이센스의 남은 일수 같은 추가 세부 정보를 보고, 필요한 경우 업데이트할 수 있습니다. **운영 체제 미설치 서버** 페이지에서 **운영 체제 미설치 서버 새로 고침** 링크가 활성화된 경우 iDRAC 라이센스로 인한 비준수 운영 체제 미설치 서버가 있습니다.

1. OpenManage Integration for VMware vCenter에서 **관리** > **배포** 탭을 선택합니다.
   운영 체제 미설치 서버 페이지에서 표에 표시된 비준수 서버 목록을 확인합니다.
2. **iDRAC 라이센스 상태** 가 **비준수** 또는 **알 수 없음**인 운영 체제 미설치 서버를 선택합니다.
3. 라이센스가 오래된 경우 **iDRAC 라이센스 구입/갱신** 링크를 클릭합니다.
4. **Dell 라이센스 관리** 페이지에 로그인하여 업데이트하거나 새 iDRAC 라이센스를 구입합니다.

이 페이지에 있는 정보를 사용하여 iDRAC를 식별하고 업데이트합니다.

5. iDRAC 라이센스를 설치한 후 **운영 체제 미설치 서버 새로 고침**을 클릭합니다.

베어 메탈 서버 새로 고침

1. **OpenManage Integration for VMware vCenter** 페이지에서 **관리** > **배포** > **베어 메탈 서버**를 클릭한 다음에 **베어 메탈 서버 새로 고침**을 클릭합니다.
2. **베어 메탈 서버 새로 고침** 창에서 데이터를 새로 고칠 서버를 선택한 다음 **선택한 서버 새로 고침**을 클릭합니다.

베어 메탈 서버의 데이터 새로 고침은 몇 분 정도 걸릴 수 있습니다.

선택한 베어 메탈 서버의 모든 데이터는 **베어 메탈 서버** 페이지에서 새로 고침됩니다.

15

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 사용자 지정 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 서버를 등록합니다
3. Dell 역할, Dell 운영 역할, Dell 인프라 배포 역할을 포함합니다.

주제:

데이터 무결성

OpenManage Integration for VMware vCenter, 관리 콘솔 및 vCenter 사이의 통신은 SSL/HTTPS를 사용하여 수행합니다. OpenManage Integration for VMware vCenter는 vCenter와 어플라이언스 간 신뢰할 수 있는 통신에 사용되는 SSL 인증서를 만듭니다. 또한 통신 및 OpenManage Integration for VMware vCenter 등록 전에 vCenter Server의 인증서를 확인하고 신뢰합니다. OpenManage Integration for VMware vCenter의 콘솔 탭에서는 관리 콘솔과 백엔드 서비스 사이에 키가 오가는 동안 부적절한 요청을 피하기 위해 보안 절차를 사용합니다. 이러한 유형의 보안을 사용하면 교차 사이트 요청 위조가 실패하게 됩니다.

보안 관리 콘솔 세션은 5분의 유휴 타임아웃이 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.

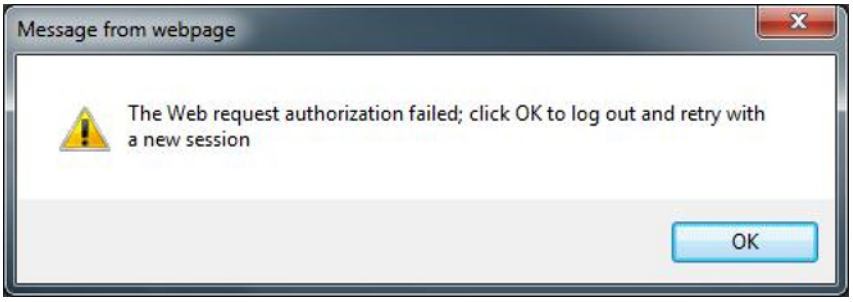

그림 3 . 보안 오류 메시지

액세스 제어 인증, 권한 부여 및 역할

OpenManage Integration for VMware vCenter에서는 vCenter 작업을 수행하기 위해 웹 클라이언트의 현재 사용자 세션과 OpenManage Integration에 대하여 저장된 관리 자격 증명을 사용합니다. OpenManage Integration for VMware vCenter에서는 vCenter 서버의 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 서버 작업 생성을 비롯하여 어플라이언스 및 vCenter 서버 작업을 수행하기 위한 권한/그룹이 포함됩니다.

이 역할에 다음 권한 그룹이 포함됩니다.

표 39. 권한 그룹

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

Dell 인프라 배포 역할

이 역할에는 하이퍼바이저 배포 기능과 관련된 권한이 포함되어 있습니다.

이 역할에서 제공하는 권한은 템플릿 생성, HW 구성 프로필 구성, 하이퍼바이저 배포 프로필 구성, 연결 프로필 구성, ID 할당 및 배포입니다.

권한 그룹 — Dell.Deploy-Provisioning

템플릿 생성, HW 구성 프로필 구성, 하이퍼바이저 배포 프로필 구성, 연결 프로필 구성, ID 할당 및 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
  - 경고 구성 및 구성(예: 이벤트 설정 페이지에서 경고 활성화/비활성화)
  - vCenter에 이벤트/경고 게시
  - 이벤트 설정 페이지에 이벤트 설정 구성
  - 이벤트 설정 페이지에서 기본 경고 복원
  - 경고/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 클라이언트 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/경고 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
  - LED 점멸, LED 지우기, Dell 서버 관리 탭에서 OMSA URL 구성
  - OMSA 콘솔 시작
  - 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

16

FAQ(자주 묻는 질문)

이 섹션에서는 문제 해결 질문에 대한 답을 확인할 수 있습니다. 이 섹션에 포함된 내용은 다음과 같습니다.

- FAQ(자주 묻는 질문)
- 베어 메탈 배포 문제 페이지 141

주제:

FAQ(자주 묻는 질문)

이 섹션에는 몇 가지 일반적인 질문과 해결 방법이 포함되어 있습니다.

Google Chrome에서 모두 내보내기 단추를 사용하여 .CSV 파일로 내보내지 못함

vCenter 서버를 등록한 후에 호스트를 추가하고 연결 프로필을 생성한 다음 호스트의 인벤토리 상세 정보를 볼 때 **모두 내보내기** 단추에서 오류가 발생합니다. **모두 내보내기** 단추는 정보를 .CSV 파일로 내보내지 않습니다.

노트:

Google Chrome 브라우저의 모든 버전에서 **모두 내보내기** 단추는 **Incognito 모드**에서 정보를 .CSV 파일로 내보내지 않습니다.

해결 방법: Google Chrome에서 **모두 내보내기** 단추를 사용하여 .CSV 파일로 정보를 내보내려면 Chrome 브라우저에서 **Incognito 모드**를 비활성화합니다.

적용 버전: 4.0

비준수 vSphere 호스트에 대한 iDRAC 라이센스 유형 및 설명이 올바르지 않게 표시됩니다.

CSIOR이 비활성화되어 있거나 실행되지 않았을 때 호스트가 비준수 상태인 경우, 유효한 iDRAC 라이센스를 이용할 수 있더라도 iDRAC 라이센스 정보가 올바르지 않게 표시됩니다. 따라서 vSphere 호스트 목록에서 호스트를 볼 수는 있지만 상세 정보를 보기 위해 호스트를 클릭하면 **iDRAC 라이센스 유형**의 정보가 빈 것으로 표시되고 **iDRAC 라이센스 설명**이 "라이센스를 업그레이드해야 합니다."로 표시됩니다.

해결 방법: 이 문제를 수정하려면 참조 서버에서 CSIOR을 활성화합니다.

적용 버전: 4.0

이전 OMIVV 버전에서 vCenter 등록 해제 후 Dell EMC 아이콘이 표시되지 않고 최신 OMIVV 버전으로 동일한 vCenter가 등록됩니다.

vCenter 서버가 포함된 이전 OMIVV 버전의 등록을 취소하고 동일한 vCenter 서버가 포함된 이후의 OMIVV 버전을 등록하는 경우, vsphere-client-serenity 폴더의 항목이 있으며, 이는 이전 OMIVV 버전의 오래된 데이터입니다. 그런 이유로, vCenter 어플라이언스의 vsphere-client-serenity 폴더에 존재하는 이전 OMIVV 버전에 특정한 오래된 데이터로 이전 OMIVV 버전을 등록한 후에는 Dell 아이콘이 표시되지 않습니다.

해결 방법: 다음 단계를 수행합니다.

1. vCenter의 경우 `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity`로 이동하고 Windows vCenter의 경우 vCenter 어플라이언스에서 `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity` 폴더로 이동해 다음과 같이 이전 데이터가 존재하는지 확인합니다.
   - com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-3.0.0.197 등의 오래된 데이터가 있는지 확인합니다.
2. 이전 OMIVV 버전에 해당하는 폴더를 수동으로 지웁니다.
3. vCenter 서버의 vSphere 웹 클라이언트 서비스를 다시 시작합니다.

적용 버전: 모든 버전

Dell 공급자가 상태 업데이트 공급자로 표시되지 않습니다.

OMIVV로 vCenter Server를 등록한 다음에 vCenter 6.0에서 vCenter 6.5로 업그레이드하는 것처럼 vCenter Server를 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 12을(를) 참조하십시오.
  2. 등록된 OMIVV 어플라이언스를 재부팅합니다.
  3. 웹 클라이언트에서 로그아웃한 다음에 다시 로그인합니다.
- 관리자 사용자의 경우:
  1. 등록된 OMIVV 어플라이언스를 재부팅합니다.
  2. 웹 클라이언트에서 로그아웃한 다음에 다시 로그인합니다.

이제 Dell 공급자가 **Proactive HA 공급자** 목록에 나열됩니다.

적용 버전: 4.0

ESXi 5.x 호스트에서 펌웨어 업데이트 작업을 수행할 때 인벤토리가 실패함

vCenter 서버를 등록한 후 ESXi 5.x 호스트에서 펌웨어 업데이트 작업을 수행하고 **구성 요소 선택** 화면에서 iDRAC를 구성 요소로 선택하면 호스트의 ESXi가 새 iDRAC IP와 동기화되지 않아서 유효하지 않은 iDRAC IP가 OMIVV로 제공될 수도 있습니다. 따라서 해당 호스트에서 인벤토리를 실행할 수 없게 됩니다.

해결 방법: 이 문제를 해결하려면 ESXi 호스트에서 sfcdb 데몬을 다시 시작하십시오. 자세한 내용은 https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2077693을(를) 참조하십시오.

적용 버전: 4.0

유효하지 않거나 알려지지 않은 iDRAC IP 때문에 호스트 인벤토리 또는 테스트 연결이 실패하였습니다.

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 연결 프로필 생성 페이지 44를 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 않습니다.

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

심각도 카테고리를 필터링하려고 할 때 OMIVV에 모든 관련 로그가 표시되지 않음

드롭다운에서 **모든 범주**를 선택하여 로그 데이터를 필터링하기 위해 심각도 범주를 선택할 때 특정 범주에 속하는 모든 로그가 정확하게 표시되지 않습니다. 하지만 드롭다운에서 **정보**를 선택하여 필터링하는 경우에는 펌웨어 업데이트 로그가 표시되지 않고 작업 시작 로그만 표시됩니다.

해결 방법: OMIVV에서 모든 로그를 보려면 필터 드롭다운에서 **모든 범주**를 선택합니다.

적용 버전: 3.1

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 http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701 및 http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121689을(를) 참조하십시오.

Windows vSphere 6.0에서 ssl 기준 위치 업데이트

1. http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701에서 lstoolutil.py.zip 파일을 다운로드합니다.
2. lstoolutil.py 파일을 `%VMWARE_CIS_HOME%"\VMware Identity Services\lstool\scripts\` 폴더에 복사합니다.

   노트: vSphere 6.0 업데이트 1을 사용하는 경우에는 lstoolutil.py 파일을 교체하지 마십시오.

다음과 같은 관련 절차를 사용하여 ssl 기준 위치를 업데이트할 수 있습니다.

- Windows 운영 체제에 설치된 vCenter에 대한 ssl 기준 위치를 업데이트하는 경우: vSphere 인증서 관리자 유틸리티를 사용하여 vCenter Windows 설치의 인증서를 교체합니다. vCenter Windows 설치 시 인증서 바꾸기 페이지 128을(를) 참조하십시오.
- vCenter 서버 어플라이언스에 대한 ssl 기준 위치를 업데이트하는 경우: vSphere 인증서 관리자 유틸리티를 사용하여 vCenter 서버 어플라이언스의 인증서를 교체합니다. vCenter 서버 어플라이언스에서 인증서 바꾸기 페이지 128을(를) 참조하십시오.

언급한 절차에서 나온 출력에 각각 `Updated 24 service (s)` 및 `Updated 26 service (s)`가 표시되어야 합니다. 표시된 출력이 `Updated 0 service (s)`이면 기존 인증서 엄지손가락 지문이 잘못된 것입니다. 다음과 같은 단계를 수행하여 기존 인증서 엄지손가락 지문을 검색할 수 있습니다. 또한 **vCenter 인증서 관리자**를 사용하여 인증서를 교체하지 않는 경우에는 다음과 같은 절차를 사용하여 기존 인증서를 검색할 수 있습니다.

노트: 획득한 기존 엄지손가락 지문을 사용하여 `ls_update_certs.py`를 실행합니다.

1. MOB(Managed Object Browser)에서 기존 인증서를 검색합니다. MOB(Managed Object Browser)에서 기존 인증서 검색 페이지 129을(를) 참조하십시오.
2. 기존 인증서에서 엄지손가락 지문을 추출합니다. 기존 인증서에서 엄지손가락 지문 추출 페이지 130을(를) 참조하십시오.

적용 버전: 3.0 이상, vCenter 6.0 이상

vCenter Windows 설치 시 인증서 바꾸기

vCenter Windows 설치 시 vSphere Certificate Manager 유틸리티를 사용하여 인증서를 바꾸는 경우 다음 단계를 수행합니다.

1. 원격 데스크탑 연결을 통해 External Platform Services Controller에 연결합니다.
2. 관리자 모드로 명령 프롬프트를 엽니다.
3. `mkdir c:\certificates` 명령을 사용하여 `c:\certificates` 폴더를 만듭니다.
4. `"%VMWARE_CIS_HOME%"\vmafdd\vecs-cli entry getcert --store BACKUP_STORE --alias bkp___MACHINE_CERT --output c:\certificates\old_machine.crt` 명령을 사용하여 기존 인증서를 검색합니다.
5. `"%VMWARE_OPENSSL_BIN%" x509 -in C:\certificates\old_machine.crt -noout -sha1 -fingerprint` 명령을 사용하여 기존 인증서 엄지손가락 지문을 검색합니다.

   노트: 검색된 인증서 엄지손가락 지문은 `SHA1 Fingerprint=13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88` 형식입니다.

   엄지손가락 지문은 `13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88`처럼 나타나는 일련의 숫자와 알파벳입니다.

6. `"%VMWARE_CIS_HOME%"\vmafdd\vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT --output c:\certificates\new_machine.crt` 명령을 사용하여 새 인증서를 검색합니다.
7. 다음 단계를 수행합니다.
   a. 다음 명령을 사용하여 `ls_update_certs.py`를 실행합니다. `"%VMWARE _PYTHON_BIN%" ls_update_certs.py --url`
   b. `https://psc.vmware.com/lookupservice/sdk --fingerprint 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 --certfile c:\certificates\new_machine.crt --user Administrator@vsphere.local --password Password` 명령을 사용하여 psc.vmware.com을 Lookup_Service_FQDN_of_Platform_Services_Controller로 바꾸고 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 엄지손가락 지문을 5단계에서 구한 엄지손가락 지문으로 바꿉니다.

      노트: 반드시 유효한 자격 증명을 입력합니다.

8. 모든 서비스가 성공적으로 업데이트되면 vCenter 웹 클라이언트에서 로그아웃했다 다시 로그인합니다.

이제 OMIVV가 성공적으로 시작됩니다.

vCenter 서버 어플라이언스에서 인증서 바꾸기

vSphere Certificate Manager 유틸리티를 사용하여 vCenter 서버 어플라이언스의 인증서를 바꾸는 경우 다음 단계를 수행합니다.

1. 콘솔 또는 SSH(보안 셸) 세션을 통해 External Platform Services Controller 어플라이언스에 로그인합니다.
2. Bash 셸에 액세스하려면 `shell.set --enabled true` 명령을 실행합니다.
3. **`shell`**을 입력한 다음 **Enter** 키를 누릅니다.
4. `mkdir /certificates` 명령을 사용하여 폴더 또는 인증서를 만듭니다.
5. `/usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store BACKUP_STORE --alias bkp___MACHINE_CERT --output /certificates/old_machine.crt` 명령을 사용하여 기존 인증서를 검색합니다.
6. `openssl x509 -in /certificates/old_machine.crt -noout -sha1 -fingerprint` 명령을 사용하여 기존 인증서 엄지손가락 지문을 검색합니다.

노트: 검색된 인증서 엄지손가락 지문은 `SHA1 Fingerprint=13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88` 형식입니다.

엄지손가락 지문은 `13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88`처럼 나타나는 일련의 숫자와 알파벳입니다.

7. `/usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT --output /certificates/new_machine.crt` 명령을 사용하여 새 인증서를 검색합니다.
8. `cd /usr/lib/vmidentity/tools/scripts/` 명령을 실행하여 디렉터리를 변경합니다.
9. 다음 단계를 수행합니다.
   a. 다음 명령을 사용하여 `ls_update_certs.py`를 실행합니다. `python ls_update_certs.py --url`
   b. `https://psc.vmware.com/lookupservice/sdk --fingerprint 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 --certfile /certificates/new_machine.crt --user Administrator@vsphere.local --password "Password"` 명령을 사용하여 psc.vmware.com을 Lookup_Service_FQDN_of_Platform_Services_Controller로 바꾸고 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 엄지손가락 지문을 6단계에서 구한 엄지손가락 지문으로 바꿉니다.

   노트: 반드시 유효한 자격 증명을 입력합니다.

10. 모든 서비스가 성공적으로 업데이트되면 vCenter 웹 클라이언트에서 로그아웃했다 다시 로그인합니다.

이제 OMIVV가 성공적으로 시작됩니다.

MOB(Managed Object Browser)에서 기존 인증서 검색

MOB(Managed Object Browser)를 사용하여 플랫폼 서비스 컨트롤러(PSC)에 연결하면 vCenter 서버 시스템에 대한 기존 인증서를 검색할 수 있습니다.

기존 인증서를 검색하려면 다음 단계를 수행하여 ArrayOfLookupServiceRegistrationInfo 관리 개체의 sslTrust 필드를 찾아야 합니다.

노트: 이 설명서에서는 `C:\certificates\` 폴더 위치를 사용하여 모든 인증서를 저장합니다.

1. `mkdir C:\certificates\` 명령을 사용하여 PSC에 `C:\certificates\` 폴더를 만듭니다.
2. 브라우저에서 `https://<vCenter FQDN|IP address>/lookupservice/mob?moid=ServiceRegistration&method=List` 링크를 엽니다.
3. `administrator@vsphere.local` 사용자 이름으로 로그인하고 메시지가 나타나면 암호를 입력합니다.

   노트: vCenter SSO(Single Sign-On) 도메인에 사용자 지정 이름을 사용하는 경우에는 해당하는 사용자 이름과 암호를 사용합니다.

4. **filterCriteria**에서 **<filtercriteria></filtercriteria>** 태그만 표시되도록 값 필드를 수정하고 **메서드 호출**을 클릭합니다.
5. 교체할 인증서에 따라 다음과 같은 호스트 이름을 검색합니다.

표 40. 검색 조건 정보

트러스트 앵커	검색 조건
vCenter 서버	Ctrl+F 키를 사용하여 페이지에서 vc_hostname_or_IP.example.com을 검색합니다.
플랫폼 서비스 컨트롤러	Ctrl+F 키를 사용하여 페이지에서 psc_hostname_or_IP.example.com을 검색합니다.

6. 해당하는 sslTrust 필드의 값을 찾습니다. sslTrust 필드의 값은 기존 인증서의 Base64로 인코딩된 문자열입니다.
7. 플랫폼 서비스 컨트롤러 또는 vCenter 서버 트러스트 앵커를 업데이트할 때 다음과 같은 예를 사용하십시오.

   노트: 가독성을 개선하기 위해 실제 문자열을 대폭 줄였습니다.

   - vCenter 서버의 경우

표 41. vCenter 서버의 예

이름	유형	값
url	anyURI	https://vcenter.vmware.local:443/sdk

- 플랫폼 서비스 컨트롤러의 경우

표 42. 플랫폼 서비스 컨트롤러의 예

이름	유형	값
url	anyURI	https://psc.vmware.local/sts/STSService/vsphere.local

8. sslTrust 필드의 콘텐츠를 텍스트 문서에 복사하고 이 문서를 `old_machine.txt`로 저장합니다.
9. 텍스트 편집기에서 `old_machine.txt`를 엽니다.
10. `old_machine.txt` 파일의 시작과 끝에 각각 다음을 추가합니다.

    ```
    -----BEGIN CERTIFICATE-----
    -----END CERTIFICATE-----
    ```

11. 이제 `old_machine.txt`를 `old_machine.crt`로 저장합니다.

이제 이 인증서에서 엄지손가락 지문을 추출할 수 있습니다.

기존 인증서에서 엄지손가락 지문 추출

다음과 같은 옵션을 사용하여 기존 인증서에서 엄지손가락 지문을 추출하고 플랫폼 서비스에 업로드할 수 있습니다.

- 인증서 뷰어 도구를 사용하여 엄지손가락 지문을 추출합니다. 인증서 뷰어 도구를 사용하여 인증서 엄지손가락 지문 추출 페이지 130을(를) 참조하십시오.
- 어플라이언스의 명령줄을 사용하여 엄지손가락 지문을 추출합니다. 명령줄을 사용하여 Thumbprint 추출 페이지 130을(를) 참조하십시오.

인증서 뷰어 도구를 사용하여 인증서 엄지손가락 지문 추출

다음 단계를 수행하여 인증서 엄지손가락 지문을 추출합니다.

1. Windows에서 `old_machine.txt` 파일을 두 번 클릭하여 Windows 인증서 뷰어에서 엽니다.
2. Windows 인증서 뷰어에서 **SHA1 엄지손가락 지문** 필드를 선택합니다.
3. 엄지손가락 지문 문자열을 일반 텍스트 편집기로 복사하고 공백을 콜론으로 바꾸거나 공백을 문자열에서 제거합니다.
   예를 들어 엄지손가락 지문 문자열은 다음 중의 하나로 나타날 수 있습니다.
   - ea87e150bb96fbbe1fa95a3c1d75b48c30db7971
   - ea:87:e1:50:bb:96:fb:be:1f:a9:5a:3c:1d:75:b4:8c:30:db:79:71

명령줄을 사용하여 Thumbprint 추출

어플라이언스와 Windows 설치 시 명령줄을 사용하여 thumbprint를 추출하는 방법은 다음 섹션을 참조하십시오.

vCenter 서버 어플라이언스에서 명령줄을 사용하여 thumbprint 추출

다음 단계를 수행합니다.

1. 기존 인증서 검색 절차의 1단계에서 만들어지는 `C:\certificates\old_machine.crt` 위치의 PSC로 old_machine.crt 인증서를 이동하거나 업로드합니다. WinSCP(Windows Secure Copy) 또는 다른 SCP 클라이언트를 사용하여 인증서를 이동하거나 업로드할 수 있습니다.
2. SSH(보안 셸)를 통해 External Platform Services Controller 어플라이언스에 로그인합니다.
3. `shell.set --enabled true` 명령을 실행하여 Bash 셸에 대한 액세스를 활성화합니다.
4. `shell`을 입력한 다음 **Enter** 키를 누릅니다.
5. `openssl x509 -in /certificates/old_machine.crt -noout -sha1 -fingerprint` 명령을 실행하여 엄지손가락 지문을 추출합니다.

노트: 엄지손가락 지문은 `SHA1 Fingerprint=ea:87:e1:50:bb:96:fb:be:1f:a9:5a:3c:1d:75:b4:8c:30:db:79:71`처럼 등호 부호 다음에 일련의 숫자와 문자로 표시됩니다.

Windows 설치 시 명령줄을 사용하여 thumbprint 추출

다음 단계를 수행합니다.

1. 기존 인증서 검색 절차의 1단계에서 만들어지는 `C:\certificates\old_machine.crt` 위치의 PSC로 old_machine.crt 인증서를 이동하거나 업로드합니다. WinSCP(Windows Secure Copy) 또는 다른 SCP 클라이언트를 사용하여 인증서를 이동하거나 업로드할 수 있습니다.
2. 원격 데스크탑 연결을 통해 External Platform Services Controller에 연결합니다.
3. 관리자 모드로 명령 프롬프트를 엽니다.
4. `"%VMWARE_OPENSSL_BIN%" x509 -in c:\certificates\old_machine.crt -noout -sha1 -fingerprint` 명령을 실행하여 엄지손가락 지문을 추출합니다.

노트: 엄지손가락 지문은 `SHA1 Fingerprint=09:0A:B7:53:7C:D9:D2:35:1B:4D:6D:B8:37:77:E8:2E:48:CD:12:1B`처럼 등호 부호 다음에 일련의 숫자와 문자로 표시됩니다.

기존 엄지손가락 지문으로 ls_update_certs.py를 실행합니다. 서비스가 성공적으로 업데이트되면 vCenter 웹 클라이언트에서 로그아웃했다 다시 로그인합니다. Dell 플러그인이 성공적으로 시작됩니다.

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 콘솔에서 **기본 업데이트 리포지토리** 필드의 경로를 **업데이트 리포지토리 경로** 필드로 수동으로 복사합니다.

작업 큐 페이지에서 보증 및 인벤토리 일정을 선택하면 전체 vCenter에 대한 보증 및 인벤토리 일정이 적용되지 않음

Dell 홈 > **모니터** > **작업 큐** > **보증/인벤토리 내역** > **일정**으로 이동합니다. vCenter를 선택하고 일정 수정 단추를 선택합니다. 대화 상자가 표시되면 **등록된 모든 vCenter에 적용** 메시지가 있는 확인란을 볼 수 있습니다. 확인란을 선택하고 **적용**을 누르면 이 설정은 처음에 선택한 특정 vCenter에 적용되고 모든 vCenter에 적용되지는 않습니다. **작업 큐** 페이지에서 보증 또는 인벤토리 일정을 수정하면 **등록된 모든 vCenter에 적용**을 적용할 수 없습니다.

해결 방법: 선택한 vCenter만 수정하려면 작업 큐에서 보증 또는 인벤토리 일정을 사용하십시오.

적용 버전: 2.2 이상

OMIVV에서 DNS 설정을 변경한 후 vCenter 웹 클라이언트에 웹 통신 오류가 나타나는 경우 수행할 작업

DNS 설정을 변경한 후 OMIVV 관련 작업을 하는 동안 vCenter 웹 클라이언트에서 웹 통신 오류가 나타날 경우 다음 중 하나를 수행하십시오.

- 브라우저 캐시를 지웁니다.
- 로그아웃한 다음 웹 클라이언트에 로그인합니다.

다른 페이지로 이동했다 다시 설정 페이지로 돌아온 경우 설정 페이지가 로드되지 않음

vSphere v5.5의 경우 웹 클라이언트에서 다른 페이지로 이동했다 다시 **설정** 페이지로 돌아오면 페이지가 로드되지 않고 시간 회전자가 계속 회전할 수 있습니다. 로드되지 않는 것은 새로 고침 문제이며 페이지가 올바르게 새로 고침되지 않는 것입니다.

해결 방법: 전역 새로 고침을 클릭하면 화면이 올바르게 새로 고쳐집니다.

적용 버전: 2.2 및 3.0

초기 구성 마법사의 인벤토리 일정/보증 일정 페이지에 "작업을 이전 시간으로 예약할 수 없음" 오류가 표시됨

다음과 같은 경우에 웹 클라이언트에서 "작업을 이전 시간으로 예약할 수 없음" 오류가 표시됩니다.

- 초기 구성 마법사에서 '등록된 모든 vCenter'를 선택하고 호스트가 없는 일부 vCenter가 있는 경우.
- 일부 인벤토리 또는 보증 작업이 있는 vCenter가 이미 예약된 경우.
- 인벤토리 또는 보증 일정이 없는 vCenter가 아직 설정되지 않은 경우.

해결 방법: vCenter의 **설정** 페이지에서 인벤토리 및 보증 예약 설정을 별도로 다시 실행합니다.

적용 버전: 2.2 이상

펌웨어 페이지에서 일부 펌웨어의 설치 날짜가 12-31-1969로 표시됨

웹 클라이언트에서 호스트에 대한 펌웨어 페이지의 일부 펌웨어 항목에 설치 날짜가 12/31/1969로 나타납니다. 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

최근 작업 창에서 연속적인 전역 새로 고침으로 인해 예외가 발생합니다.

새로 고침 단추를 반복적으로 누르면 VMware UI에서 예외를 throw할 수 있습니다.

해결 방법: 이 오류를 무시하고 계속할 수 있습니다.

적용 버전: 2.2 이상

IE 10에서 Dell 화면 중 일부에 대해 웹 클라이언트 UI가 왜곡되는 이유

팝업 대화 상자가 표시될 때 배경의 데이터가 흰색이 되고 왜곡되는 경우가 있습니다.

해결 방법: 대화 상자를 닫으면 화면이 다시 정상 상태가 됩니다.

적용 버전: 2.2 이상

vCenter에 플러그인을 성공적으로 등록했지만 웹 클라이언트에 OpenManage Integration 아이콘이 표시되지 않음

vCenter 웹 클라이언트 서비스를 다시 시작하지 않으면 웹 클라이언트에 OpenManage Integration 아이콘이 표시되지 않습니다. OpenManage Integration for VMware vCenter 어플라이언스를 등록할 때 웹 클라이언트를 사용하여 어플라이언스를 등록합니다. 어플라이언스의 등록을 취소한 다음 같은 버전을 다시 등록하거나 새 버전의 어플라이언스를 등록하면 등록은 되지만 OMIVV 아이콘이 웹 클라이언트에 나타나지 않을 수도 있습니다. 이는 VMware의 캐싱 문제로 인해 발생합니다. 이 문제를 해결하려면 vCenter 서버에서 웹 클라이언트 서비스를 다시 시작해야 합니다. 그 다음에 플러그인이 UI에 표시됩니다.

해결 방법: vCenter 서버에서 웹 클라이언트 서비스를 다시 시작하십시오.

적용 버전: 2.2 이상

리포지토리에 선택한 11G 시스템에 대한 번들이 있는 경우에도 펌웨어 업데이트에서 펌웨어 업데이트에 대한 번들이 없다고 표시됨

잠금 모드에서 연결 프로필에 호스트를 추가하면 인벤토리가 시작되지만 "원격 액세스 컨트롤러를 찾을 수 없거나 이 호스트에서 인벤토리가 지원되지 않습니다."라는 메시지와 함께 실패합니다. 인벤토리는 잠금 모드에서 호스트에 대해 작동해야 합니다.

호스트를 잠금 모드에 배치하거나 잠금 모드에서 호스트를 제거하는 경우 30분을 기다린 후에 다음 작업을 수행해야 합니다. 펌웨어 업데이트에 11G 호스트를 사용하는 경우에 리포지토리에 해당 시스템에 대한 번들이 있더라도 펌웨어 업데이트 마법사에는 번들이 표시되지 않습니다. OMSA에서 OpenManage Integration으로 트랩을 보내도록 11G 호스트가 구성되지 않은 것이 원인일 수 있습니다.

해결 방법: 호스트가 OpenManage Integration 웹 클라이언트의 호스트 규정 준수 마법사를 사용하여 준수하고 있는지 확인합니다. 준수하지 않는 경우에는 호스트 규정 준수 수정을 사용하여 준수하게 합니다.

적용 버전: 2.2 이상

어플라이언스 IP 및 DNS 설정을 DHCP 값으로 덮어쓰는 경우, 어플라이언스를 재부팅하고 나면 DNS 구성 설정이 원래 설정으로 복원되는 이유는 무엇입니까?

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 버전 13.5.2로 인텔 네트워크 카드를 업데이트하기 위해 OMIVV를 사용하는 것이 지원되지 않습니다.

펌웨어 버전 13.5.2를 사용하는 일부 인텔 네트워크 카드와 Dell PowerEdge 12세대 서버에 알려진 문제가 있습니다. Lifecycle Controller를 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: 참고: 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

유효하지 않은 DUP로 펌웨어 업데이트를 시도할 때 LC의 작업 상태가 '실패'로 표시되는 경우에도 vCenter 콘솔의 하드웨어 업데이트 작업 상태가 몇 시간 동안 실패하지도 않고 시간 초과가 발생하지도 않음

펌웨어 업데이트에 대해 잘못된 DUP를 선택하면 vCenter 콘솔 창의 작업 상태가 '진행 중'으로 남아 있게 되지만 메시지가 실패 이유로 변경됩니다. 이것은 알려진 VMWare 결함이며 이후의 VMWare vCenter 릴리즈에서 해결될 예정입니다.

해결 방법: 작업을 수동으로 취소해야 합니다.

적용 버전: 모든 버전

관리 포털에서 연결할 수 없는 업데이트 리포지토리 위치를 표시하는 이유

연결할 수 없는 업데이트 리포지토리 경로를 제공할 경우, "오류: ...URL에 연결하는 동안에 오류 발생" 오류 메시지가 어플라이언스 업데이트 보기의 상단에 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 PowerEdge M1000e 섀시 관리 컨트롤러 펌웨어 문서의 사용자 가이드를 참조하십시오.

시스템 개요 페이지에서 프로세서 보기의 프로세서 버전이 "해당 없음"으로 표시됨

PowerEdge 12세대 및 이후 세대에서 프로세서 버전은 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. OMIVV가 링크된 모드에서 작동하는 방식에 대한 자세한 내용은 www.dell.com의 *OpenManage Integration for VMware vCenter: 링크된 모드에서 작업* 백서를 참조하십시오.

OMIVV의 필수 포트 설정

노트: OMIVV의 **Compliance** 창에 나와 있는 **비준수 vSphere 호스트 수정** 링크를 이용하여 OMSA 에이전트를 배포하는 경우, OMIVV는 http 클라이언트 서비스를 시작하고 ESXI 5.5 이후의 릴리즈에서 포트 8080을 활성화하여 OMSA VIB을 다운로드하여 설치합니다. OMSA VIB 설치가 완료된 후에는 서비스 자동으로 중지되고 포트가 닫힙니다.

OMIVV에 대한 다음과 같은 포트 설정을 사용하십시오.

표 43. 가상 어플라이언스

포트 번호	프로토콜	포트 유형	최대 암호화 수준	방향	대상	사용량	설명
53	DNS	TCP	없음	Out	DNS 서버에 대한 OMIVV 어플라이언스	DNS 클라이언트	DNS 서버에 연결하거나 호스트 이름을 확인합니다.
69	TFTP	UDP	없음	Out	TFTP 서버에 대한 OMIVV 어플라이언스	TFTP 클라이언트	이전 펌웨어가 있는 11G 서버의 펌웨어 업데이트에 사용됩니다.
80	HTTP	TCP	없음	Out	인터넷에 대한 OMIVV 어플라이언스	Dell 온라인 데이터 액세스	온라인(인터넷) 보증, 펌웨어 및 최신 RPM 정보에 대한 연결을 설정합니다.

표 43. 가상 어플라이언스 (계속)

포트 번호	프로토콜	포트 유형	최대 암호화 수준	방향	대상	사용량	설명
80	HTTP	TCP	없음	입력	OMIVV 어플라이언스에 대한 ESXi 서버	HTTP 서버	OMIVV 어플라이언스와 통신하기 위한 사후 설치 스크립트용 OS 구축 흐름에 사용됩니다.
162	SNMP 에이전트	UDP	없음	입력	OMIVV 어플라이언스에 대한 iDRAC/ESXi	SNMP 에이전트(서버)	관리된 노드에서 SNMP 트랩을 수신합니다.
443	HTTPS	TCP	128비트	입력	OMIVV 어플라이언스에 대한 OMIVV UI	HTTPS 서버	OMIVV에서 제공하는 웹 서비스입니다. 이러한 웹 서비스는 vCenter 웹 클라이언트 및 Dell 관리 포털에서 사용합니다.
443	WSMAN	TCP	128비트	입력/출력	iDRAC/OMSA에 대한/로부터의 OMIVV 어플라이언스	iDRAC/OMSA 통신	관리된 노드를 관리하고 모니터링하는 데 사용되는 iDRAC, OMSA 및 CMC 통신입니다.
445	SMB	TCP	128비트	Out	CIFS에 대한 OMIVV 어플라이언스	CIFS 통신	Windows 공유와 통신합니다.
4433	HTTPS	TCP	128비트	입력	OMIVV 어플라이언스에 대한 iDRAC	자동 검색	관리된 노드 자동 검색에 사용되는 프로비저닝 서버입니다.
2049	NFS	UDP/TCP	없음	입력/출력	NFS에 대한 OMIVV 어플라이언스	공개 공유	NFS 공개 공유는 OMIVV 어플라이언스에 의해 관리된 노드에 노출되었으며 펌웨어 업데이트 및 OS 구축 흐름에 사용됩니다.
4001~4004	NFS	UDP/TCP	없음	입력/출력	NFS에 대한 OMIVV 어플라이언스	공개 공유	NFS 공개 공유는 OMIVV 어플라이언스에 의해 관리된 노드에 노출되었으며 펌웨어 업데이트 및 OS 구축 흐름에 사용됩니다.
11620	SNMP 에이전트	UDP	없음	입력	OMIVV 어플라이언스에 대한 iDRAC	SNMP 에이전트(서버)	관리된 노드를 관리하고 모니터링하는 데 사용되는 iDRAC, OMSA 및 CMC 통신입니다.
사용자 정의됨	모든	UDP/TCP	없음	Out	프록시 서버에 대한 OMIVV 어플라이언스	프록시	프록시 서버와 통신하기

표 44. 관리된 노드(ESXi)

포트 번호	프로토콜	포트 유형	최대 암호화 수준	방향	대상	사용량	설명
162, 11620	SNMP	UDP	없음	Out	OMIVV 어플라이언스에 대한 ESXi	하드웨어 이벤트	이 포트는 ESXi에서 보낸 비동기 SNMP 트랩으로 ESXi에서 열어야 합니다.
443	WSMAN	TCP	128비트	입력	ESXi(OMSA)에 대한 OMIVV 어플라이언스	iDRAC/OMSA 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.
8080	HTTP	TCP	128비트	Out	OMIVV 어플라이언스에 대한 ESXi	HTTP 서버 - OMSA VIB를 다운로드하고 비준수 vSphere	ESXi에서 OMSA/ 드라이버 VIB를 다운로드하는 데 도움이 됩니다.

표 44. 관리된 노드(ESXi) (계속)

포트 번호	프로토콜	포트 유형	최대 암호화 수준	방향	대상	사용량	설명
						호스트를 수정합니다.	

표 45. 관리된 노드(iDRAC/CMC)

포트 번호	프로토콜	포트 유형	최대 암호화 수준	방향	대상	사용량	설명
443	WSMAN /HTTPS	TCP	128비트	입력	iDRAC/CMC에 대한 OMIVV 어플라이언스	iDRAC 통신	관리 스테이션에 정보를 제공하는 데 사용됩니다. 이 포트는 iDRAC 및 CMC에서 열어야 합니다.
4433	HTTPS	TCP	128비트	Out	OMIVV 어플라이언스에 대한 iDRAC	자동 검색	관리 스테이션에서 iDRAC(관리된 노드)를 자동 검색합니다.
2049	NFS	UDP	없음	입력/출력	OMIVV에 대한/로부터의 iDRAC	공개 공유	iDRAC가 OMIVV 어플라이언스에 의해 노출되는 NFS 공개 공유에 액세스합니다. OS 배포 및 펌웨어 업데이트에 사용됩니다. OMIVV에서 iDRAC 구성에 액세스합니다. 배포 흐름에 사용됩니다.
4001~ 4004	NFS	UDP	없음	입력/출력	OMIVV에 대한/로부터의 iDRAC	공개 공유	iDRAC가 OMIVV 어플라이언스에 의해 노출되는 NFS 공개 공유에 액세스합니다. 이는 OS 배포 및 펌웨어 업데이트에 사용됩니다. OMIVV에서 iDRAC 구성에 액세스합니다. 배포 흐름에 사용됩니다.
69	TFTP	UDP	128비트	입력/출력	OMIVV에 대한/로부터의 iDRAC	Trivial File Transfer	관리 스테이션에서 iDRAC를 성공적으로 관리하는 데 사용됩니다.

iDRAC 사용자 목록에서 새로 변경한 자격 증명을 가진 동일한 사용자가 있는 하드웨어 또는 시스템 프로필을 성공적으로 적용한 후에 베어 메탈 검색에 사용되는 사용자에 대한 암호가 변경되지 않음

하드웨어 프로필 또는 시스템 프로필 템플릿만 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.

OMSA로 온도 하드웨어 결함을 시뮬레이션하여 이벤트 설정을 테스트하는 방법

이벤트가 올바르게 작동하는지 확인하려면 다음 단계를 수행하십시오.

1. OMSA 사용자 인터페이스에서 **경고 관리** > **플랫폼 이벤트**로 이동합니다.
2. **플랫폼 이벤트 필터 경고 활성화** 확인란을 선택합니다.
3. 아래쪽으로 스크롤하고 **변경사항 적용**을 클릭합니다.
4. 온도 경고와 같은 특정 이벤트가 활성화되어 있는지 확인하려면 왼쪽에 있는 트리에서 **기본 시스템 섀시**를 선택합니다.
5. **기본 시스템 섀시** 아래에서 **온도**를 선택합니다.
6. **경고 관리** 탭을 선택하고 **온도 감지기 경고**를 선택합니다.
7. **메시지 브로드캐스트** 확인란을 선택하고 **변경사항 적용**을 선택합니다.
8. 온도 경고 이벤트를 생성하려면 왼쪽에 있는 트리 보기에서 **기본 시스템 섀시**를 선택합니다.
9. **기본 시스템 섀시** 아래에서 **온도**를 선택합니다.
10. **시스템 보드 주변 온도** 링크를 선택하고 **값으로 설정** 옵션 단추를 선택합니다.
11. **최대 경고 임계값**을 현재 나열된 판독값에 앞서는 값으로 설정합니다.
    예를 들어 현재 판독값이 27이면 임계값을 **25**로 설정합니다.
12. **변경 사항 적용**을 선택하면 온도 경고 이벤트가 만들어집니다.
    다른 이벤트를 생성하려면 동일한 **값으로 설정** 옵션을 사용하여 원래 설정을 복원합니다. 이벤트는 경고로 생성된 다음에 정상 상태로 지정됩니다. 모든 것이 올바르게 작동하면 **vCenter 작업 및 이벤트** 보기로 이동합니다. 온도 Probe 경고 이벤트가 표시되어야 합니다.

    노트: 중복 이벤트에 대한 필터가 있습니다. 한 행에서 동일한 이벤트를 너무 많이 트리거하도록 시도하면 하나의 이벤트만 수신됩니다. 모든 이벤트를 보려면 이벤트 간에 30초 이상을 허용하십시오.

OMSA 에이전트가 OMIVV 호스트 시스템에 설치된 경우에도 계속해서 OMSA가 설치되지 않았다는 오류 메시지가 발생합니다.

이 문제를 해결하려면 11세대 서버에서 다음을 수행하십시오.

1. 호스트 시스템에 **원격 활성화** 구성 요소와 함께 **OMSA**를 설치합니다.
2. 명령줄을 사용하여 OMSA를 설치하는 경우에는 **-c 옵션**을 지정해야 합니다. OMSA가 이미 설치된 경우에는 -c 옵션을 사용하여 다시 설치하고 서비스를 다시 시작합니다.

```
srvadmin-install.sh -c
srvadmin-services.sh restart
```

ESXi 호스트의 경우 **VMware 원격 CLI 도구**를 사용하여 **OMSA VIB**를 설치하고 시스템을 다시 부팅해야 합니다.

잠금 모드가 활성화된 상태에서 OMIVV의 ESXi 지원 여부

예. ESXi 5.0 이상인 호스트의 이 릴리즈에서 잠금 모드가 지원됩니다.

잠금 모드 사용을 시도하였지만 실패했습니다.

잠금 모드에서 연결 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.

참조 서버를 사용하고 있는 경우에 하드웨어 프로필 생성에 실패함

iDRAC 펌웨어, 수명 주기 컨트롤러 펌웨어 및 BIOS의 최소 권장 버전이 설치되어 있는지 확인하십시오.

참조 서버에서 검색한 데이터가 최신 상태인지 확인하려면 **CSIOR(Collect System Inventory On Restart)**을 활성화하고 데이터를 추출하기 전에 참조 서버를 다시 시작하십시오.

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 어플라이언스와 동일한 네트워크에 있는지 확인합니다.
3. **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.
4. 최소 한 개의 **가상 디스크**가 시스템에서 확인되는지 확인합니다.

   ESXi도 내부 SD 카드에 설치됩니다.

Dell PowerEdge R210 II 시스템에서 하이퍼바이저 배포가 실패함

연결된 ISO로부터 부팅하려는 BIOS의 오류로 인해 Dell PowerEdge R210 II 시스템의 시간 초과 문제가 하이퍼바이저 배포 실패 오류의 원인이 됩니다.

해결 방법: 시스템에 수동으로 하이퍼바이저를 설치합니다.

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 실패했습니다.

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 가상 어플라이언스를 강제로 제거하는 방법

1. **Https://<vcenter_serverIPAddress>/mob**로 이동합니다.
2. VMware vCenter 관리자 자격 증명을 입력합니다.
3. **콘텐츠**를 클릭합니다.
4. **ExtensionManager**를 클릭합니다.
5. **UnregisterExtension**을 클릭합니다.
6. 확장 키를 입력하여 com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient의 등록을 취소하고 **메서드 호출**을 클릭합니다.
7. vSphere 웹 클라이언트에서 OMIVV의 전원을 끄고 삭제합니다. 등록을 취소하는 키가 웹 클라이언트용이어야 합니다.

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 스크롤해야 합니다.

vSphere 웹 클라이언트에서 Dell 서버 관리 포틀릿 또는 Dell 아이콘을 클릭하면 404 오류가 나타납니다.

OMIVV 어플라이언스가 실행되고 있는지 확인합니다. 그렇지 않은 경우에는 vSphere 웹 클라이언트에서 재시작합니다. 가상 어플라이언스 웹 서비스가 시작될 때까지 몇 분 정도 기다린 후에 페이지를 새로 고칩니다. 오류가 계속되면 명령줄에서 IP 주소 또는 정규화된 도메인 이름을 사용하여 어플라이언스에 대한 Ping을 시도해 보십시오. Ping으로도 문제가 해결되지 않으면 네트워크 설정을 검토하여 올바른지 확인합니다.

펌웨어 업데이트 실패 시 수행할 작업

가상 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. 따라서 이러한 문제가 발생하면 정적 IP 주소를 사용하여 해결할 수 있습니다. 정적 IP 주소를 사용하려면 OpenManage Integration for VMware vCenter의 콘솔 탭에서 **네트워크 구성** > **장치 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.

연결 프로필 테스트 자격 증명의 수행 속도가 느리거나 응답하지 않습니다.

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.
   - iDRAC6: **iDRAC 설정** > **네트워크/보안 탭** > **사용자 탭**을 선택합니다.
   - iDRAC7: **iDRAC 설정** > **사용자 탭**을 선택합니다.
   - iDRAC8: **iDRAC 설정** > **사용자 탭**을 선택합니다.
4. 설정을 편집하려면 사용자 ID 열에서 관리(루트) 사용자에 대한 링크를 클릭합니다.
5. **사용자 구성**을 클릭하고 **다음**을 클릭합니다.
6. 선택한 사용자의 **사용자 구성** 페이지에서 사용자 활성화 옆에 있는 확인란을 선택하고 **적용**을 클릭합니다.

OMIVV의 VMware vCenter 서버 어플라이언스 지원 여부

예. OMIVV는 v2.1 이후로 VMware vCenter 서버 어플라이언스를 지원합니다.

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. 따라서 호스트가 vCenter 트리에서 제거되는 경우에도 호스트가 다음 섀시 인벤토리가 실행될 때까지는 섀시 아래에 표시됩니다.

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 콘솔에서 **기본 업데이트 리포지토리** 필드의 경로를 **업데이트 리포지토리 경로** 필드로 수동으로 복사합니다.

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: OpenManage Integration for VMware GUI의 **관리** > **설정** 탭에서 **이벤트 및 알람** 설정을 수동으로 변경합니다.

NPAR이 대상 노드에서 활성화되고 시스템 프로필에서 비활성화되어 있을 때 하이퍼바이저 배포가 실패함

대상 시스템에 NIC 파티셔닝(NPAR)이 비활성화된 시스템 프로필이 적용될 때 하이퍼바이저 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

사용 가능한 버전이 현재 버전보다 낮을 경우 사용할 수 있는 가상 어플라이언스 버전이 잘못된 정보를 표시합니다.

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.

Express 라이센스로 12G 베어 메탈 서버를 추가하는 동안 267027 예외가 throw되었습니다.

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.

14G에서 OS 배포 도중 iDRAC 하드웨어 오류로 인해 하드웨어 프로필을 적용하지 못함

14G 서버에서 OS 배포를 진행하는 도중, 하드웨어 프로필이 적용되면 iDRAC에서 구성 업데이트 작업이 생성됩니다. 그러나 경우에 따라 작업이 실패하고 구성 작업이 이미 생성되었음을 나타내는 메시지가 표시됩니다.

해결 방법: 상태 항목을 지우고 OS 배포를 다시 시도하려면 `racadm jobqueue delete -i JID_CLEARALL_FORCE` 명령을 실행합니다.

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` 이 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 모듈 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.

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 없습니다. 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
```

17

관련 설명서

본 안내서와 더불어 다른 안내서를 Dell.com/support에서 확인할 수 있습니다. **모든 제품 중에서 선택**을 클릭한 뒤 **소프트웨어 및 보안** > **가상화 솔루션**을 클릭합니다. 다음 문서에 액세스하려면 **OpenManage Integration for VMware vCenter 4.2**을 클릭합니다.

- *OpenManage Integration for VMware vCenter Web Client 버전 4.2 사용자 가이드*
- *OpenManage Integration for VMware vCenter 버전 4.2 릴리스 정보*
- *OpenManage Integration for VMware vCenter 버전 4.2 호환성 매트릭스*

Delltechcenter.com에서 백서를 포함한 기술 아티팩트를 찾을 수 있습니다. Dell TechCenter Wiki 홈 페이지에서 **시스템 관리** > **OpenManage Integration for VMware vCenter**를 클릭하여 문서를 확인합니다.

주제:

Dell EMC 지원 사이트에서 문서 액세스

다음 방법 중 하나를 통해 필요한 문서에 액세스할 수 있습니다.

- 다음 링크를 사용하십시오.
  - Dell EMC Enterprise 시스템 관리, Dell EMC Remote Enterprise 시스템 관리 및 Dell EMC 가상화 솔루션 문서 — www.dell.com/esmmanuals
  - Dell EMC OpenManage 문서 — www.dell.com/openmanagemanuals
  - iDRAC 문서 — www.dell.com/idracmanuals
  - Dell EMC OpenManage Connections Enterprise 시스템 관리 문서 — www.dell.com/OMConnectionsEnterpriseSystemsManagement
  - Dell EMC 서비스 가능 도구 문서의 경우 — https://www.dell.com/serviceabilitytools
- Dell EMC 지원 사이트에서
  1. https://www.dell.com/support로 갑니다.
  2. **모든 제품 찾아보기**를 클릭합니다.
  3. **모든 제품** 페이지에서 **소프트웨어**를 클릭한 후 다음 중에서 필요한 링크를 클릭합니다.
     - **분석**
     - **클라이언트 시스템 관리**
     - **엔터프라이즈 애플리케이션**
     - **엔터프라이즈 시스템 관리**
     - **메인프레임**
     - **운영 체제**
     - **공공 부문 솔루션**
     - **서비스 가능 도구**
     - **지원**
     - **유틸리티**
     - **가상화 솔루션**
  4. 문서를 보려면 필요한 제품을 클릭한 다음 필요한 버전을 클릭합니다.
- 검색 엔진 사용:
  - 검색 상자에 문서 이름 및 버전을 입력합니다.

A

시스템 특정 특성

iDRAC

표 46. 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
DNSDomainName	DNS 도메인 이름	NIC 정적 정보
주소	IPv4 주소	IPv4 정적 정보
넷마스크	넷마스크	IPv4 정적 정보
게이트웨이	게이트웨이	IPv4 정적 정보
DNS1	DNS Server 1	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 47. 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

표 47. BIOS에 대한 시스템 특정 특성 (계속)

특성 이름	표시 특성 이름	그룹 표시 이름
IscsiDev1Con1TargetIp	Target IP Address	연결 1 설정
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 48. 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 49. 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

표 49. CNA에 대한 시스템 특정 특성 (계속)

특성 이름	표시 특성 이름	그룹 표시 이름
IscsiInitiatorGateway	기본 게이트웨이	iSCSI 초기자 매개 변수
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 50. 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

사용자 지정 특성

표 51. 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.

C

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*

D

구성 요소와 기준선 버전 비교 매트릭스

표 52. 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 요소가 연결된 기준선과 일치하지 않습니다.	비준수
	사용할 수 없음	사용 가능	비교 상태가 계산되지 않고 무시됩니다.	준수
	사용 가능	사용할 수 없음	하드웨어 구성 요소 버전을 연결된 기준선에서 사용할 수 있지만 구성 요소 또는 속성을 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 요소가 연결된 기준선과 일치합니다.	준수
	사용 가능	사용 가능	펌웨어 구성 요소가 연결된 기준선과 일치하지 않습니다.	비준수
	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 요소가 연결된 기준선과 일치합니다.	준수
	사용 가능	사용 가능	드라이버 구성 요소가 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 요소 또는 속성을 사용할 수 없거나 새 구성 요소를 사용할 수 있습니다.	비준수
	사용할 수 없음	사용할 수 없음	비교 상태가 계산되지 않고 무시됩니다.	준수