

OpenManage Integration for VMware vCenter Web Client 버전 5.0 설치 가이드

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.

장 1: 소개.....	5
OpenManage Integration for VMware vCenter 라이선싱.....	5
소프트웨어 라이선스 구입.....	5
라이선스 업로드 후의 옵션.....	6
적용.....	6
참조를 위한 중요 참고.....	7
하드웨어 요구 사항.....	7
배포 모드 구성.....	7
Lifecycle Controller 버전 포함 BIOS 및 iDRAC.....	8
PowerEdge 서버에서 지원되는 기능.....	10
PowerEdge 새시에서 지원되는 기능.....	11
프로비저닝된 스토리지에 필요한 스토리지 공간.....	11
소프트웨어 요구사항.....	12
OpenManage Integration for VMware vCenter 요구사항.....	12
포트 정보.....	12
필수 조건 점검 사항.....	14
장 2: OMIVV 설치 및 구성.....	16
OpenManage Integration for VMware vCenter 다운로드.....	16
vSphere Client(HTML-5)를 사용하여 OMIVV OVF 배포.....	17
OMIVV 어플라이언스 구성.....	18
Network Time Protocol 서버 설정.....	20
2개의 네트워크 어댑터로 OMIVV 어플라이언스 구성.....	20
인증서 서명 요청(CSR) 생성.....	24
HTTPS 인증서 업로드.....	25
기본 HTTPS 인증서 복원.....	25
OpenManage Integration for VMware vCenter 등록 및 라이선스 파일 가져오기.....	25
관리자가 아닌 사용자를 사용하여 vCenter 서버 등록.....	27
관리자가 아닌 사용자의 필수 권한.....	28
기존 역할에 Dell 권한 할당.....	29
등록된 vCenter 버전을 업그레이드한 후 OMIVV 재구성.....	29
설치 확인.....	30
백업 및 복원 관리.....	30
백업 및 복원 구성.....	30
자동 백업 예약.....	31
즉시 백업 수행.....	31
백업에서 OMIVV 데이터베이스 복원.....	31
백업 및 복원 설정 재설정.....	31
OMIVV 어플라이언스 및 리포지토리 위치 업데이트.....	31
RPM을 사용하여 OMIVV 어플라이언스 업그레이드.....	32
Vmware 툴 업그레이드.....	33
백업 및 복원을 사용하여 OMIVV 어플라이언스 업그레이드.....	33
OpenManage Integration for VMware vCenter 등록 취소.....	34
등록 취소 후 OMIVV 복구.....	34

이전 버전의 OMIVV를 등록 취소한 후 OMIVV 복구.....	34
등록 취소 및 재등록 관리.....	34
장 3: VMware vCenter용 어플라이언스 구성.....	35
초기 구성 마법사를 사용하여 구성 작업.....	35
초기 구성.....	35
호스트 자격 증명 프로필 생성.....	36
인벤토리 작업 예약.....	37
보증 검색 작업 예약.....	38
이벤트 및 알람 구성.....	38
설정 페이지에서 구성 작업.....	39
보증 만료 알람 구성.....	39
최신 어플라이언스 버전 알람 구성.....	39
배포 자격 증명 구성.....	39
상태 업데이트 알람의 심각도 재정의.....	40
장 4: Dell EMC 지원 사이트에서 문서 액세스.....	41
장 5: 관련 설명서.....	42

소개

이 안내서는 PowerEdge 서버와 함께 사용하기 위해 OpenManage Integration for VMware vCenter(OMIVV)를 설치 및 구성하는 방법에 대한 단계별 지침을 제공합니다. OMIVV 설치 후 인벤토리 관리, 모니터링 및 경고, 펌웨어 업데이트, 보증 관리를 비롯한 모든 측면의 관리에 대한 자세한 내용은 Dell.com/support/manuals에서 사용 가능한 *OpenManage Integration for VMware vCenter 사용자 가이드*를 참조하십시오.

주제:

- OpenManage Integration for VMware vCenter 라이선싱
- 참조를 위한 중요 참고
- 하드웨어 요구 사항
- 소프트웨어 요구사항
- 포트 정보
- 필수 조건 점검 사항

OpenManage Integration for VMware vCenter 라이선싱

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

- 평가판 라이선스 — OMIVV 어플라이언스의 전원을 처음 켜면, 평가판 라이선스가 자동으로 설치됩니다. 평가 버전에는 OpenManage Integration for VMware vCenter에서 관리되는 호스트(서버) 5개에 대한 평가판 라이선스가 포함되어 있습니다. 이 90일 평가 버전은 배송 시 제공되는 기본 라이선스입니다.
- 표준 라이선스 - OMIVV에서 관리하는 호스트 라이선스를 원하는 수만큼 구매할 수 있습니다. 이 라이선스에는 제품 지원 및 OMIVV 어플라이언스 업데이트가 포함됩니다.

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

라이선싱은 다음 정보를 제공합니다.

- 최대 vCenter 연결 라이선스 수 - 등록되어 사용 중인 vCenter 연결은 최대 15개까지 활성화됩니다.
- 최대 호스트 연결 라이선스 수 — 구입한 호스트 연결 수입니다.
- 사용 중 — 사용 중인 vCenter 연결 또는 호스트 연결 라이선스 수입니다. 호스트 연결에서 이 숫자는 인벤토리로 작성된 호스트(또는 서버) 수를 나타냅니다.
- 사용 가능 — 나중에 사용할 수 있는 vCenter 연결 또는 호스트 연결 라이선스의 수입니다.

이 노트: 표준 라이선스 기간은 3~5년뿐이며 추가 라이선스는 기존 라이선스에 추가되기만 하고 덮어쓰지는 않습니다.

이 노트: OpenManage Integration for VMware vCenter를 위해 구매한 모든 라이선스는 해당 기간(구매 후 3년 또는 5년) 동안 사용할 수 있습니다(5.x 릴리스). 기존 OMIVV 인스턴스에서 백업한 라이선스를 이전하거나 Digital Locker에서 다시 다운로드한 현재 라이선스를 5.x 인스턴스에 적용할 수 있습니다.

라이선스를 구매하면 Dell 디지털 로커(Dell Digital Locker)에서 .XML 파일(라이선스 키)을 다운로드할 수 있습니다. 라이선스 키가 다운로드되지 않는 경우 **주문 지원**에서 해당 제품의 지역 Dell 지원 부서 전화 번호를 찾아 Dell 지원 부서에 문의합니다.

소프트웨어 라이선스 구입

정식 제품 버전으로 업그레이드할 때까지는 평가판 라이선스를 실행합니다. **라이선스 구입**을 클릭하여 Dell 웹 사이트로 이동하여 라이선스를 구입합니다. 라이선스를 구입한 후 관리 콘솔을 사용하여 업로드합니다.

1. **설정 > 라이선싱 > 라이선스 구입 또는 대시보드 > 라이선스 구입 또는 관리 포털 > vCenter 등록 > 라이선싱 > 지금 구입**으로 이동합니다.
2. 라이선스 파일을 다운로드하여 알려진 위치에 저장합니다. 라이선스 파일이 .zip 파일 내에 압축되어 있을 수 있습니다. zip 파일의 압축을 풀고 라이선스 .xml 파일만 업로드해야 합니다. 라이선스 파일의 이름은 주문 번호를 기준으로 지정될 것입니다(예: 123456789.xml).

관리 포털에 라이선스 업로드

이 옵션을 사용하여 OMIVV 호스트 라이선스를 업로드할 수 있습니다.

1. `https://<ApplianceIP/hostname/>`으로 이동합니다.
2. 로그인 대화 상자에 암호를 입력합니다.
3. 왼쪽 창에서 **VCENTER 등록**을 클릭합니다.
등록된 vCenter 서버가 작업 창에 표시됩니다.
4. **라이선스 업로드**를 클릭합니다.
5. **라이선스 업로드** 대화 상자에서 **찾아보기**를 클릭하여 라이선스 파일로 이동한 후 **업로드**를 클릭합니다.
라이선스 파일이 수정되었거나 편집된 경우 OMIVV 어플라이언스에서는 라이선스 파일이 손상된 것으로 인식하므로 해당 파일이 작동되지 않습니다.

라이선스 업로드 후의 옵션

새로 구입한 제품의 라이선스 파일

새 라이선스를 주문할 때 Dell에서는 주문 확인서가 포함된 이메일을 보내 드리며 **Dell Digital Locker**의 Dell 디지털 로커에서 새 라이선스 파일을 다운로드할 수 있습니다. 라이선스는 .xml 형식이어야 합니다. 라이선스가 zip 형식으로 되어 있으면 zip 파일에서 라이선스 .xml 파일의 압축을 푼 후 업로드하십시오.

라이선스 스택킹

OMIVV에서는 여러 개의 표준 라이선스를 스택킹하여 지원되는 호스트 수를 늘리고 업로드된 라이선스의 호스트 합계를 늘릴 수 있습니다. 단, 평가판 라이선스는 스택킹할 수 없습니다. 기본적으로 OMIVV에서는 최대 15개의 vCenter를 지원합니다. vCenter를 15개 이상 관리하려면 여러 어플라이언스를 사용합니다.

기존 표준 라이선스가 만료되기 전에 새 표준 라이선스가 업로드된 경우 라이선스가 스택킹됩니다. 그렇지 않은 경우, 라이선스가 만료되고 새 라이선스가 업로드된 경우 새 라이선스의 호스트 수만 지원됩니다. 여러 개의 라이선스를 이미 업로드한 경우 지원되는 호스트 수는 마지막 라이선스를 업로드한 시점에서 만료되지 않은 라이선스에 있는 호스트의 합계입니다.

만료된 라이선스

일반적으로 구매 날짜로부터 3년 또는 5년으로 정해지는 지원 기간을 경과한 라이선스는 업로드가 차단됩니다. 라이선스가 업로드된 후에 만료된 경우 일부 기능이 작동하지 않을 수 있습니다. 그러나 OMIVV의 새 버전으로 업그레이드하는 것은 차단됩니다.

라이선스 교체

주문에 문제가 있어 Dell에서 교체 라이선스를 받을 경우 이 교체 라이선스에는 이전 라이선스와 동일한 권리 ID가 포함됩니다. 교체 라이선스를 업로드하면 이미 동일한 권리 ID로 업로드된 기존 라이선스가 교체됩니다.

적용

어플라이언스 업데이트

모든 라이선스가 만료되면 어플라이언스가 새 버전으로의 업데이트를 허용하지 않습니다. 새 라이선스를 구입하고 업로드한 후에 어플라이언스 업그레이드를 시도하십시오.

평가판 라이선스

평가판 라이선스가 만료되면 여러 핵심 영역이 작동을 중단하고 해당하는 오류 메시지가 표시됩니다.

호스트 자격 증명 프로필에 호스트 추가

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

참조를 위한 중요 참고

- OMIVV 5.0 이상부터는 VMware vSphere Client(HTML-5)만 지원되며 vSphere Web Client(FLEX)는 지원되지 않습니다.
 - DNS 서버를 사용하는 경우 권장 사례는 다음과 같습니다.
 - OMIVV는 IPV4 IP 주소만 지원합니다. 고정 IP 할당과 DHCP 할당이 모두 지원되지만 Dell EMC는 고정 IP 주소 할당을 권장합니다. 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.
- vSphere를 위한 DNS 요구 사항에 대한 자세한 내용은 다음 VMware 링크를 참조하십시오.
- [vSphere 6.5 및 Platform Services Controller 어플라이언스를 위한 DNS 요구 사항](#)
 - [Windows의 vSphere 6.7 및 Platform Services Controller에 대한 DNS 요구 사항](#)
- OMIVV 어플라이언스 모드의 경우 가상화 환경에 따라 적절한 모드로 OMIVV를 배포해야 합니다. 자세한 내용은 [배포 모드 구성](#) 페이지 7을(를) 참조하십시오.
 - 포트 요구 사항에 맞게 네트워크를 구성합니다. 자세한 내용은 [포트 정보](#) 페이지 12을(를) 참조하십시오.
 - Dell EMC는 Google Chrome을 사용하여 OMIVV 기능에 액세스하는 것을 권장합니다. OMIVV에서는 Google Chrome 및 Mozilla Firefox를 지원합니다. Microsoft Internet Explorer는 지원되지 않습니다.

하드웨어 요구 사항

OMIVV는 iDRAC Express 또는 Enterprise가 포함된 서버에 대한 전체 기능과 함께 여러 세대의 Dell EMC 서버 전체를 지원합니다. 사용자의 호스트 서버가 이러한 지원을 받을 수 있는지 여부를 확인하려면 다음의 하위 항목을 참조하십시오.

- [지원되는 서버 및 최소 BIOS](#)
- [지원되는 버전의 iDRAC\(배포 및 관리\)](#)
- [OMIVV에 지원되는 메모리, CPU 및 스토리지 공간](#)

OMIVV를 사용하려면 iDRAC 및 CMC 관리 네트워크 또는 OME-Modular 시스템 관리 네트워크 및 vCenter 관리 네트워크에 액세스할 수 있는 마더보드 또는 네트워크 도터 카드에 대한 LAN이 필요합니다. 자세한 내용은 [OMIVV 어플라이언스 구성](#) 페이지 18 및 [2개의 네트워크 어댑터로 OMIVV 어플라이언스 구성](#) 페이지 20을(를) 참조하십시오.

배포 모드 구성

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

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

표 1. 배포 모드의 시스템 요구 사항

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

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

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(예: 작게, 중간, 크게, 아주 크게)이 표시됩니다. 기본적으로 이 모드는 작게로 설정됩니다.

- 환경을 기반으로 배포 모드를 편집하려면 편집을 클릭합니다.
- 편집 모드에서 필수 구성 요소가 충족되었는지 확인하고 필요한 배포 모드를 선택합니다.
- 적용을 클릭합니다.
설정된 배포 모드에 대해, 그리고 다음과 같은 이벤트 중 하나가 발생한 경우 필요한 CPU 및 메모리를 기준으로 할당된 CPU 및 메모리를 확인합니다.
 - 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.
- 배포 모드가 변경되면 변경 사항을 확인한 다음 어플라이언스를 재시작해야 배포 모드를 업데이트할 수 있습니다.

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

배포 모드 다운그레이드

- 관리 콘솔에 로그인합니다.
- 배포 모드를 필요한 수준으로 변경합니다.
- OMIVV 어플라이언스를 종료하고 시스템 리소스를 필요한 수준으로 변경합니다.
- OMIVV 어플라이언스의 전원을 켭니다.

Lifecycle Controller 버전 포함 BIOS 및 iDRAC

OpenManage Integration for VMware vCenter의 기능을 활성화하려면 Lifecycle Controller 버전이 포함된 BIOS 및 iDRAC가 필요합니다.

Dell EMC는 OMIVV를 사용하기 전에 Repository Manager 또는 Lifecycle Controller의 플랫폼을 사용하여 생성된 부팅 가능 ISO를 사용하여 서버를 다음 기본 버전 중 하나로 업데이트할 것을 권장합니다.

표 2. PowerEdge 서버를 위해 지원되는 BIOS 버전

서버	최소 버전
T320	1.0.1 이상
T420	1.0.1 이상
T620	1.2.6 이상
M420	1.2.4 이상
M520	1.2.6 이상
M620	1.2.6 이상
M820	1.2.6 이상
R220	1.0.3 이상
R320	1.2.4 이상
R420	1.2.4 이상
R520	1.2.4 이상
R620	1.2.6 이상
R720	1.2.6 이상
R720xd	1.2.6 이상
R820	1.7.2 이상
R920	1.1.0 이상

표 2. PowerEdge 서버를 위해 지원되는 BIOS 버전

서버	최소 버전
R630	1.0.4 이상
R730	1.0.4 이상
R730xd	1.0.4 이상
R430	1.0.4 이상
R530	1.0.2 이상
R830	1.0.2 이상
R930	1.0.2 이상
R230	1.0.2 이상
R330	1.0.2 이상
T630	1.0.2 이상
T130	1.0.2 이상
T330	1.0.2 이상
T430	1.0.2 이상
M630	1.0.0 이상
M830	1.0.0 이상
FC430	1.0.0 이상
FC630	1.0.0 이상
FC830	1.0.0 이상
R240	1.0.0 이상
R340	1.0.0 이상
R940	1.0.0 이상
R940xa	1.0.0 이상
R740	1.0.0 이상
R740xd	1.0.0 이상
R740xd2	1.0.0 이상
R640	1.0.0 이상
R840	1.0.0 이상
R440	1.0.0 이상
M640	1.0.0 이상
T140	1.0.0 이상
T340	1.0.0 이상
T640	1.0.0 이상
T440	1.0.0 이상
R540	1.0.0 이상
FC640	1.0.0 이상
R6415	1.0.0 이상
R7425	1.0.0 이상

표 2. PowerEdge 서버를 위해 지원되는 BIOS 버전

서버	최소 버전
R7415	1.0.0 이상
MX740C	1.0.0 이상
MX840C	1.0.0 이상
R6515	1.0.3 이상
R7515	1.0.3 이상
R6525	1.0.0 이상

표 3. 배포용으로 지원되는 iDRAC 및 Lifecycle Controller

세대	LifeCycle Controller가 포함된 iDRAC
PowerEdge 12세대 서버	2.50.50.50 이상
PowerEdge 13세대 서버	2.50.50.50 이상
PowerEdge 14세대 서버	3.00.00.00 이상

표 4. 클라우드 서버의 BIOS 및 iDRAC 요구 사항

모델	BIOS	LifeCycle Controller가 포함된 iDRAC
C6320	1.0.2	2.50.50.50 이상
C4130	1.0.2	2.50.50.50 이상
C6420	1.0.0 이상	3.00.00.00 이상
C4140	1.0.0 이상	3.00.00.00 이상
C6525	1.0.0 이상	3.42.42.42 이상

PowerEdge 서버에서 지원되는 기능

OpenManage Integration for VMware vCenter에서 관리하는 호스트에서는 다음과 같은 기능이 지원됩니다.

표 5. PowerEdge 서버에서 지원되는 기능

기능	플랫폼	
	12G 및 13G	14G
하드웨어 인벤토리	예	예
이벤트 및 알람	예(SNMP v1 및 v2)	예(SNMP v1 및 v2)
구성 요소 전체에서 상태 모니터링*	예	예
BIOS/펌웨어 업데이트#	예	예
Proactive HA\$	예	예
보증 정보	예	예
관리 준수	예	예
구성 준수	예	예
베어 메탈 서버 자동/수동 검색	예	예
베어 메탈 호환성	예	예
하드웨어 구성	예	예
OS 배포	예	예

표 5. PowerEdge 서버에서 지원되는 기능

기능	플랫폼	
	예	예
서버 LED 깜빡임	예	예
SEL 로그 보기/지우기	예	예
iDRAC 링크 및 실행	예	예
iDRAC 재설정	예	예
시스템 잠금 모드	아니요	예
시스템 프로필	예	예
클러스터 프로필	예	예
통합 새시 IP를 사용하여 호스트 관리	아니요	Y@
OEM Server 지원	Y~	예

* 모델 번호가 C6320인 클라우드에서는 메자닌 카드에 상태 모니터링이 지원되지 않습니다.

모델 번호가 C6320인 클라우드에서는 메자닌 카드에 펌웨어 업데이트가 지원되지 않습니다.

\$ Proactive HA 기능은 ESXi 6.0 이상이 있는 vCenter 6.5 이상에만 적용 가능합니다. 또한, Proactive HA 기능은 내장형 PSU 및 클라우드 서버 모델이 있는 서버에서 지원되지 않습니다.

@ MX 새시 호스트에만 해당됩니다. 인벤토리, 모니터링, 사전 예방적 HA 및 펌웨어 업데이트 기능이 지원됩니다.

~ 랙 서버에만 지원됩니다.

PowerEdge 새시에서 지원되는 기능

이 주제에서는 PowerEdge 새시에서 지원되는 기능에 대한 정보를 제공합니다.

표 6. 모듈형 인프라에서 지원되는 기능

기능	M1000e	VRTX	FX2s	MX
SNMP 경고	예	예	예	예
하드웨어 인벤토리	예	예	예	예
CMC 또는 관리 모듈 링크 및 실행	예	예	예	예
라이선스 정보	N/A(해당 없음)	예	예	예
보증 정보	예	예	예	예
상태 보고	예	예	예	예
멀티 새시 관리 그룹 관계 정보	아니요	아니요	아니요	예
펌웨어 업데이트	아니요	아니요	아니요	예

프로비저닝된 스토리지에 필요한 스토리지 공간

OMIVV 가상 어플라이언스에서는 프로비저닝 스토리지를 위해 최소 95GB의 디스크 공간이 필요합니다.

기본 가상 어플라이언스 구성

OMIVV 가상 어플라이언스는 8GB RAM과 2개의 가상 CPU로 프로비저닝됩니다(소형 배포 모드).

소프트웨어 요구사항

vSphere 환경이 가상 어플라이언스 시스템 요구 사항, 포트 액세스, 클럭 동기화 및 수신 포트 요구 사항을 충족하는지 확인합니다.

VMware vSphere Client(HTML-5) 요구 사항

vCenter 6.5 이상

OpenManage Integration for VMware vCenter 요구사항

관리되는 호스트에서 지원되는 ESXi 버전

다음 표는 관리되는 호스트에서 지원되는 ESXi 버전에 대한 정보를 제공합니다.

표 7. 지원되는 ESXi 버전

ESXi 버전	서버 세대		
	YX2X	YX3X	YX4X
6.0 U3	예	예	아니요
6.5	예	예	아니요
6.5 U1	예	예	예
6.5 U2	예	예	예
6.5 U3	예	예	예
6.7	아니요	예	예
6.7 U1	아니요	예	예
6.7 U2	아니요	예	예
6.7 U3	아니요	예	예

이 노트: PowerEdge MX 호스트는 ESXi 6.5 U2 이상과 함께 사용하는 경우에만 지원됩니다.

OpenManage Integration for VMware vCenter는 다음과 같은 vCenter Server 버전을 지원합니다.

표 8. 지원되는 vCenter Server 버전

vCenter 버전	클라이언트 지원
6.5 U2	예
6.5 U3	예
6.7	예
6.7 U1	예
6.7 U2	예
6.7 U3	예

OpenManage Integration for VMware vCenter 버전 5.0은 VMware vRealize Operations Manager(vROPS) 버전 2.0을 지원합니다.

OMIVV 5.0 어플라이언스는 CentOS 7.6.1810을 지원합니다.

포트 정보

이 섹션에는 가상 어플라이언스 및 관리되는 노드를 구성하기 위한 모든 포트 요구 사항이 나열되어 있습니다.

표 9. 가상 어플라이언스

포트 번호	프로토콜	포트 유형	최대 암호화 수준	방향	대상	사용	설명
53	DNS	TCP	없음	출력	DNS 서버에 대한 OMIVV 어플라이언스	DNS 클라이언트	DNS 서버에 연결하거나 호스트 이름을 확인합니다.
80/443	HTTP/HTTPS	TCP	없음	출력	인터넷에 대한 OMIVV 어플라이언스	Dell 온라인 데이터 액세스	온라인(인터넷) 보증, 펌웨어 및 최신 RPM 정보에 대한 연결을 설정합니다.
80	HTTP	TCP	없음	입력	OMIVV 어플라이언스에 대한 ESXi 서버	HTTP 서버	OMIVV 어플라이언스와 통신하기 위한 사후 설치 스크립트용 운영 체제 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 vSphere Client 및 Dell 관리 포털에서 사용됩니다.
443	WSMAN	TCP	128비트	입력/출력	iDRAC에 대한/로부터의 OMIVV 어플라이언스	iDRAC 통신	관리되는 노드를 관리하고 모니터링하는 데 사용되는 iDRAC 및 CMC 또는 OME-Modular 통신입니다.
445	SMB	TCP	128비트	출력	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 운영 체제 구축 흐름에 사용됩니다.
4001~4004	NFS	UDP/TCP	없음	입력/출력	NFS에 대한 OMIVV 어플라이언스	공개 공유	NFS 서버의 V2 및 V3 프로토콜에서 statd, quotd, lockd 및 mountd 서비스를 실행하려면 이러한 포트를 열린 상태로 유지해야 합니다.
11620	SNMP 에이전트	UDP	없음	입력	OMIVV 어플라이언스에 대한 iDRAC	SNMP 에이전트(서버)	UDP를 사용하여 표준 SNMP 경고를 수신하는 데 사용되는 포트: 162 iDRAC 및 CMC 또는 OME-Modular의 데이터는 관리되는 노드를 관리하고 모니터링하기 위해 수신됩니다.
사용자 정의	모든	UDP/TCP	없음	출력	프록시 서버에 대한 OMIVV 어플라이언스	프록시	프록시 서버와 통신합니다.

표 10. 관리된 노드(ESXi)

표 10. 관리된 노드(ESXi)

포트 번호	프로토콜	포트 유형	최대 암호화 수준	방향	대상	사용	설명
162, 11620	SNMP	UDP	없음	출력	OMIVV 어플라이언스에 대한 ESXi	하드웨어 이벤트	ESXi에서 보낸 비동기 SNMP 트랩입니다. 이 포트는 ESXi에서 열어야 합니다.
443	WSMAN	TCP	128비트	입력	ESXi에 대한 OMIVV 어플라이언스	iDRAC 통신	관리 스테이션에 정보를 제공하는 데 사용됩니다. 이 포트는 ESXi에서 열어야 합니다.
443	HTTPS	TCP	128비트	입력	ESXi에 대한 OMIVV 어플라이언스	HTTPS 서버	관리 스테이션에 정보를 제공하는 데 사용됩니다. 이 포트는 ESXi에서 열어야 합니다.

표 11. 관리되는 노드(iDRAC 또는 CMC 또는 OME-Modular)

포트 번호	프로토콜	포트 유형	최대 암호화 수준	방향	대상	사용	설명
443	WSMAN/HTTPS, REST/HTTPS	TCP	128비트	입력	iDRAC 또는 CMC 또는 OME-Modular에 대한 OMIVV 어플라이언스	iDRAC 통신	관리 스테이션에 정보를 제공하고 REST 또는 HTTPS 프로토콜을 사용하여 MX 새시와 통신하는 데 사용됩니다. 이 포트는 iDRAC 및 CMC 또는 OME-Modular에서 열어야 합니다.
4433	HTTPS	TCP	128비트	출력	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. 운영 체제 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 운영 체제 배포 및 펌웨어 업데이트에 사용됩니다. OMIVV에서 iDRAC 구성에 액세스합니다. 배포 흐름에 사용됩니다.
69	TFTP	UDP	128비트	입력/출력	OMIVV에 대한/로부터의 iDRAC	간이 파일 전송	관리 스테이션에서 iDRAC를 성공적으로 관리하는 데 사용됩니다.

필수 조건 점검 사항

제품 설치를 시작하기 전에 다음 사항을 확인합니다.

- OMIVV에서 vCenter 서버에 액세스할 수 있는 사용자 이름 및 암호가 있습니다. 사용자는 필요한 모든 권한을 가진 관리자 역할 또는 필요한 권한을 가진 비 관리자 사용자 역할을 보유할 수 있습니다. OMIVV에 필요한 권한 목록에 대한 자세한 내용은 [관리자가 아닌 사용자의 필수 권한](#)을 참조하십시오.
- ESXi 호스트 시스템이나 호스트에 대한 관리 권한이 있는 Active Directory 자격 증명에 대한 루트 비밀번호가 있습니다.
- iDRAC에 대한 관리 권한이 있는 iDRAC Express 또는 Enterprise와 연결된 사용자 이름 및 비밀번호가 있습니다.
- vCenter 서버가 실행 중입니다.
- OMIVV 설치 디렉토리의 위치를 확인합니다.

- OMIVV 및 vCenter 서버가 동일한 네트워크 상에 있습니다.
 - vCenter, OMIVV 및 iDRAC가 서로 다른 네트워크에 연결된 경우 vCenter, OMIVV 및 iDRAC 네트워크 사이에 라우트가 있습니다. OMIVV 어플라이언스가 두 네트워크 어댑터로 구성되지 않은 경우에만 해당합니다.
 - VMware vSphere 환경이 가상 어플라이언스 시스템 요구 사항, 포트 액세스, 클럭 동기화 및 수신 포트 요구 사항을 충족합니다.
- i** **노트:** 가상 어플라이언스가 일반 가상 컴퓨터로 작동합니다. 한 번 중단 또는 종료되면 가상 어플라이언스의 전체 기능에 영향을 미칩니다.
- i** **노트:** OMIVV는 ESXi 5.5 이상 버전에 배포되었을 시 VMware Tools를 실행 중(완료됨) 상태로 표시합니다. 필요할 경우 OMIVV 어플라이언스를 성공적으로 배포한 후 또는 이후 언제든지 VMware Tools를 업그레이드 할 수 있습니다.

OMIVV 설치 및 구성

하드웨어 요구 사항을 충족하며, 필수 VMware vCenter를 실행 중인지 확인합니다.

다음의 대략적인 단계에서는 OMIVV에 대한 전반적인 설치 및 구성 절차에 대해 설명합니다.

1. Dell 지원 웹 사이트(Dell.com/support)에서 *DellEMC_OpenManage_Integration_<버전 번호>.<빌드 번호>.zip* 파일을 다운로드합니다. OMIVV 다운로드에 대한 자세한 내용은 [OpenManage Integration for VMware vCenter 다운로드](#) 페이지 16 항목을 참조하십시오.
2. 파일을 다운로드한 위치로 이동하고 해당 콘텐츠를 추출합니다.
3. vSphere Client(HTML-5)를 사용하여 OMIVV 어플라이언스가 포함된 OVF(Open Virtualization Format) 파일을 배포합니다. [OMIVV OVF 배포](#)를 참조하십시오.
4. OVF를 배포한 후 시간대, 현재 날짜 및 시간을 설정합니다.
5. 라이선스 파일을 업로드합니다. 라이선스 부여에 대한 자세한 내용은 [관리 포털에 라이선스 업로드](#) 페이지 6을(를) 참조하십시오.
6. 요구 사항에 따라 배포 모드를 설정합니다. 자세한 내용은 [배포 모드 구성](#) 페이지 7을(를) 참조하십시오.
7. Administration Console을 사용하여 OMIVV 어플라이언스를 vCenter 서버에 등록합니다. [OMIVV 등록 및 라이선스 파일 가져오기](#)를 참조하십시오.
8. 어플라이언스를 구성하려면 [초기 구성 마법사](#)를 완료합니다. [구성 마법사를 통한 구성 작업](#)을 참조하십시오.

주제:

- [OpenManage Integration for VMware vCenter 다운로드](#)
- [vSphere Client\(HTML-5\)를 사용하여 OMIVV OVF 배포](#)
- [OMIVV 어플라이언스 구성](#)
- [Network Time Protocol 서버 설정](#)
- [2개의 네트워크 어댑터로 OMIVV 어플라이언스 구성](#)
- [인증서 서명 요청\(CSR\) 생성](#)
- [HTTPS 인증서 업로드](#)
- [OpenManage Integration for VMware vCenter 등록 및 라이선스 파일 가져오기](#)
- [관리자가 아닌 사용자를 사용하여 vCenter 서버 등록](#)
- [등록된 vCenter 버전을 업그레이드한 후 OMIVV 재구성](#)
- [설치 확인](#)
- [백업 및 복원 관리](#)
- [OMIVV 어플라이언스 및 리포지토리 위치 업데이트](#)
- [RPM을 사용하여 OMIVV 어플라이언스 업그레이드](#)
- [백업 및 복원을 사용하여 OMIVV 어플라이언스 업그레이드](#)
- [OpenManage Integration for VMware vCenter 등록 취소](#)
- [등록 취소 후 OMIVV 복구](#)

OpenManage Integration for VMware vCenter 다운로드

Dell EMC PowerEdge 서버의 서비스 태그를 준비해 두십시오. 서비스 태그를 사용하여 Dell 지원 웹 사이트에서 모든 지원에 액세스하는 것이 좋습니다. 그러면 플랫폼에 적절한 소프트웨어 버전이 다운로드됩니다.

OMIVV를 다운로드하려면 다음을 수행하십시오.

1. <https://www.dell.com/support>로 이동합니다.
2. 다음 작업 중 하나를 수행합니다.
 - Dell EMC PowerEdge 서버의 서비스 태그를 입력한 다음 검색을 선택합니다.
 - **모든 제품 찾아보기 > 서버 > PowerEdge**를 선택합니다.
3. 적절한 PowerEdge 서버 모델을 선택합니다.
4. 서버 지원 페이지에서 **드라이버 및 다운로드**를 선택합니다.

5. 운영 체제 목록에서 적절한 VMware ESXi 버전을 선택합니다.
6. 범주 목록에서 시스템 관리를 선택합니다.
지원되는 OMIVV 버전이 표시됩니다.
7. 다운로드를 클릭하거나 확인란을 선택하여 다운로드 목록에 소프트웨어를 추가합니다.

vSphere Client(HTML-5)를 사용하여 OMIVV OVF 배포

지원 웹사이트에서 제품 .zip 파일(DellEMC_OpenManage_Integration_<version number>.<build number>.zip)을 다운로드하여 압축을 해제했는지 확인합니다.

이 노트: 다음 작업은 vSphere Client(HTML-5)를 사용하는 경우에만 권장됩니다. 웹 클라이언트를 사용하는 경우 단계가 달라질 수 있습니다.

1. OMIVV를 다운로드한 위치로 이동하여 **DellEMC_OpenManage_Integration.exe**를 두 번 클릭하여 파일의 압축을 풉니다.
exe의 압축을 해제하고 실행할 수 있도록 지원되는 클라이언트 운영 체제 버전은 Windows 7 SP1 이상입니다.
exe의 압축을 해제하고 실행할 수 있도록 지원되는 서버 운영 체제 버전은 Windows 2008 R2 이상입니다.

2. EULA에 동의하고 .ovf 파일을 저장합니다.
3. 어플라이언스를 업로드할 VMware vSphere 호스트에 액세스할 수 있는 위치로 .ovf 파일을 복사하거나 이동합니다.
4. VMware vSphere Client(HTML-5)를 시작합니다.
5. VMware vSphere Client, 에서 호스트를 선택하고 기본 메뉴에서 **조치 > OVF 템플릿 배포**를 클릭합니다.
호스트를 마우스 오른쪽 버튼으로 클릭하고 **OVF 템플릿 배포**를 선택할 수도 있습니다.

OVF 템플릿 배포 마법사가 표시됩니다.

6. OVF 템플릿 선택 창에서 다음을 수행합니다.
 - a. 인터넷에서 OVF 패키지를 다운로드하려면 URL을 선택합니다.
 - b. 로컬 시스템에서 OVF 패키지를 선택하려면 로컬 파일을 선택하고 파일 선택을 클릭합니다.
 - c. 다음을 클릭합니다.
이름 및 폴더 선택 창이 표시됩니다.

이 노트: OVF 패키지가 네트워크 공유에 저장되는 경우 설치 프로세스에 10~30분 정도 소요될 수 있습니다. Dell EMC는 빠른 설치를 위해 로컬 드라이브에 OVF를 호스팅하는 것을 권장합니다.

7. 이름 및 폴더 선택 창에서 다음을 수행합니다.
 - a. 가상 시스템 이름 필드에 템플릿 이름을 입력합니다. 이름의 길이는 최대 80자입니다.
 - b. 가상 시스템 위치 선택 목록에서 템플릿을 배포할 위치를 선택합니다.
 - c. 다음을 클릭합니다.
컴퓨팅 리소스 선택 창이 표시됩니다.
8. 컴퓨팅 리소스 선택 목록에서 대상 컴퓨팅 리소스를 선택한 후 다음을 클릭합니다.
다음 정보가 포함된 세부 정보 검토 창이 표시됩니다.
 - 게시자 - 게시자 데이터
 - 다운로드 크기 - OVF 템플릿의 실제 크기(단위: GB)
 - 디스크 크기 - 씹 프로비저닝 및 씹 프로비저닝에 대한 정보

9. 다음을 클릭합니다.
스토리지 선택 창이 표시됩니다.

10. 스토리지 선택 창에서 다음을 수행합니다.
 - a. 가상 디스크 형식 선택 드롭다운 목록에서 다음 형식 중 하나를 선택합니다.
 - 씹 프로비저닝 레이지 제로
 - 씹 프로비저닝 이거드 제로
 - 씹 프로비저닝
 씹 프로비전(이거드 제로)을 선택하는 것이 좋습니다.

- b. VM 스토리지 정책 드롭다운 목록에서 정책을 선택합니다.
- c. 다음을 클릭합니다.
네트워크 선택 창에 소스 및 대상 네트워크에 대한 상세 정보가 표시됩니다.

11. 네트워크 선택 창에서 각 소스 네트워크의 대상 네트워크를 선택하고 다음을 클릭합니다.

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

vSphere 네트워크와 아웃오브밴드 네트워크가 사용자 환경에서 별도의 분리된 네트워크로 유지되는 경우 OMIVV는 두 개의 네트워크에 액세스해야 합니다. 이 경우 OMIVV 어플라이언스는 두 개의 네트워크 어댑터로 구성되어야 합니다. vSphere 네트워크를 사용하여 아웃오브밴드 네트워크에 액세스할 수 있는 경우 OMIVV 어플라이언스에 대해 네트워크 어댑터를 구성하지 마십시오. 두 개의 네트워크 어댑터 구성에 대한 자세한 내용은 [2개의 네트워크 어댑터로 OMIVV 어플라이언스 구성](#) 페이지 20을(를) 참조하십시오.

- 아웃오브밴드 네트워크 – iDRAC, CMC 및 OME-Modular가 연결되어 있는 관리 네트워크.
- vSphere 네트워크 – ESXi 호스트, vCenter 및 PSC가 연결되어 있는 관리 네트워크.

12. **완료 준비** 창에서 OVF 배포 작업에 대해 선택한 옵션을 검토하고 **마침**을 클릭합니다. 배포 작업이 실행되고 작업 완료 상태를 추적할 수 있는 완료 상태가 표시됩니다.

13. VM의 전원을 켭니다.

이 노트: OVF를 배포한 후 OMIVV에 등록하기 전에 현재 날짜 및 시간을 필수적으로 설정해야 합니다.

OMIVV 어플라이언스 구성

1. VM의 전원을 켭니다.

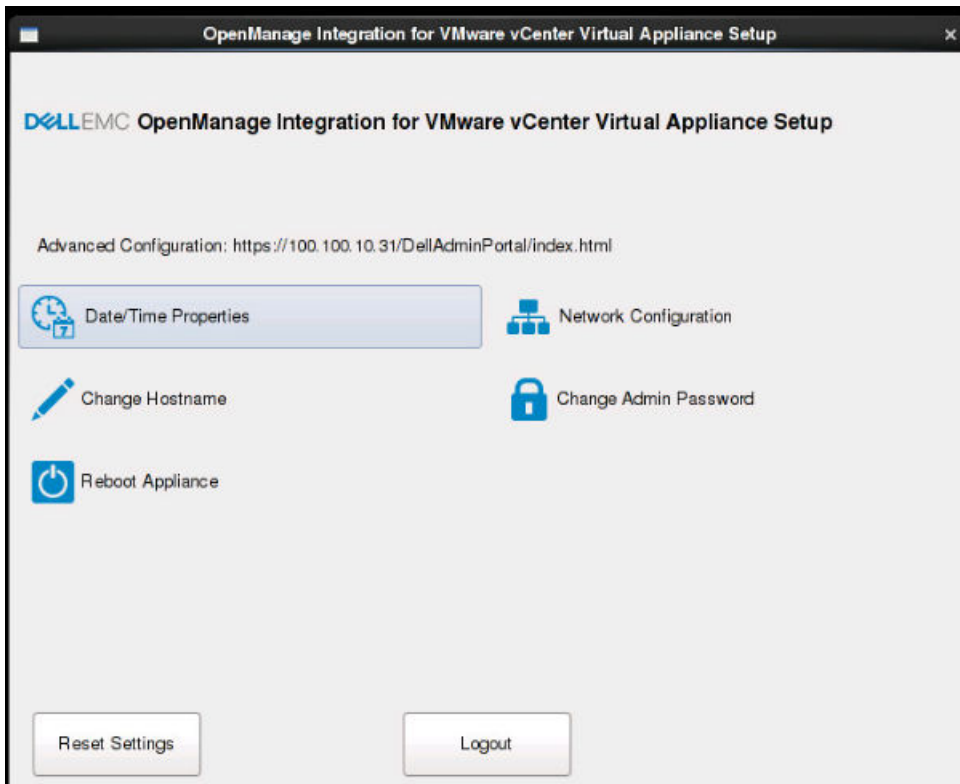
2. 오른쪽 창에서 **웹 콘솔 시작**을 클릭합니다.

3. 관리자로 로그인합니다(기본 사용자 이름은 admin입니다).

4. 처음 로그인하는 경우 화면의 지침에 따라 비밀번호를 설정합니다(Admin 및 ReadOnly 사용자).

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

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



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

a. **날짜 및 시간** 탭에서 **네트워크에서 날짜 및 시간 동기화** 확인란을 선택합니다. **네트워크에서 날짜 및 시간 동기화** 확인란은 관리 포털을 사용하여 NTP를 구성해야 활성화됩니다. NTP 구성에 대한 자세한 내용은 [Network Time Protocol 서버 설정](#) 페이지 20을(를) 참조하십시오.

b. **시간대**를 클릭하고 해당 시간대를 선택한 다음 **확인**을 클릭합니다.


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

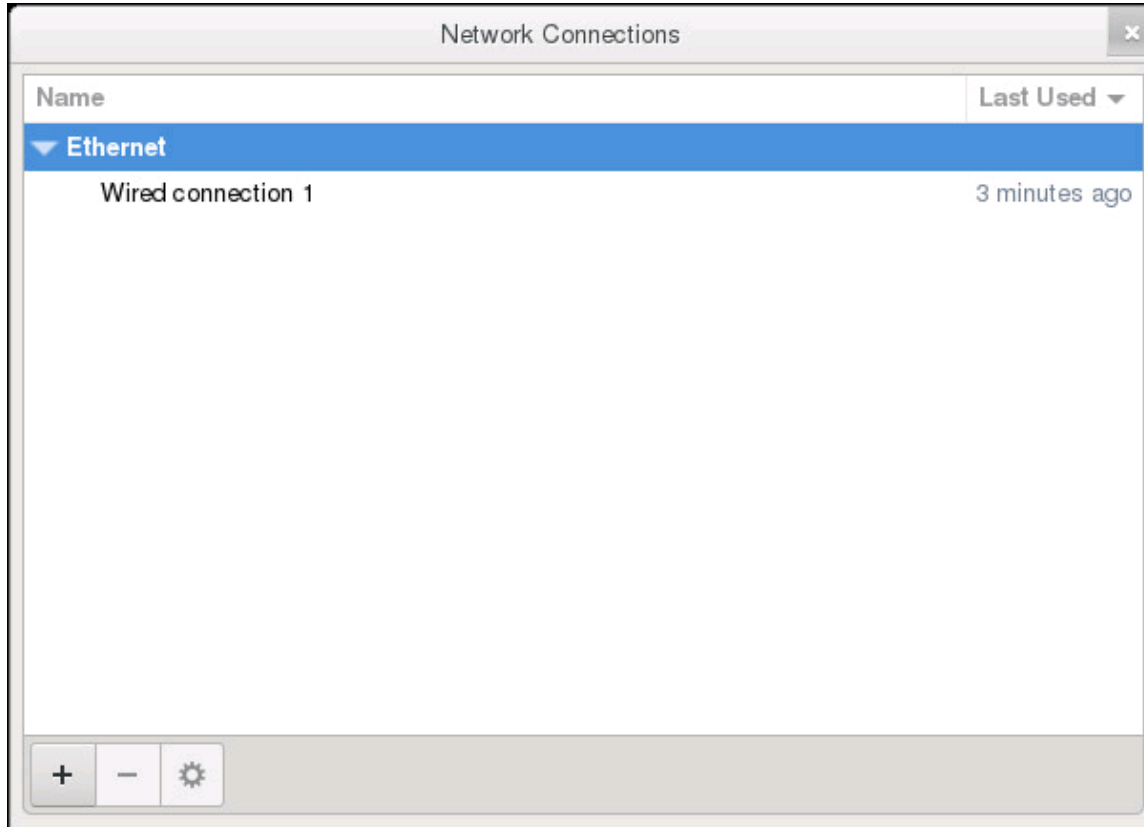
vSphere 환경에서 Dell EMC 서버를 관리하려면 OMIVV에서 vSphere 네트워크(vCenter 및 ESXi 관리 네트워크)와 대역외 네트워크(iDRAC, CMC 및 OME-Modular) 모두에 액세스해야 합니다.

vSphere 네트워크와 대역외 네트워크가 사용자 환경에서 별도의 분리된 네트워크로 유지되는 경우 OMIVV는 두 개의 네트워크에 액세스해야 합니다. 이 경우 OMIVV 어플라이언스는 두 개의 네트워크 어댑터로 구성되어야 합니다. Dell EMC는 초기 구성의 일부로 네트워크를 모두 구성하는 것을 권장합니다.

vSphere 네트워크를 사용하여 대역외 네트워크에 액세스할 수 있는 경우 OMIVV 어플라이언스에 대해 2개의 네트워크 어댑터를 구성하지 마십시오. 두 번째 NIC 구성에 대한 자세한 내용은 **2개의 네트워크 어댑터로 OMIVV 어플라이언스 구성** 페이지 20을 (를) 참조하십시오.



7. **유선 연결 1**을 선택하고  을 클릭합니다.



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

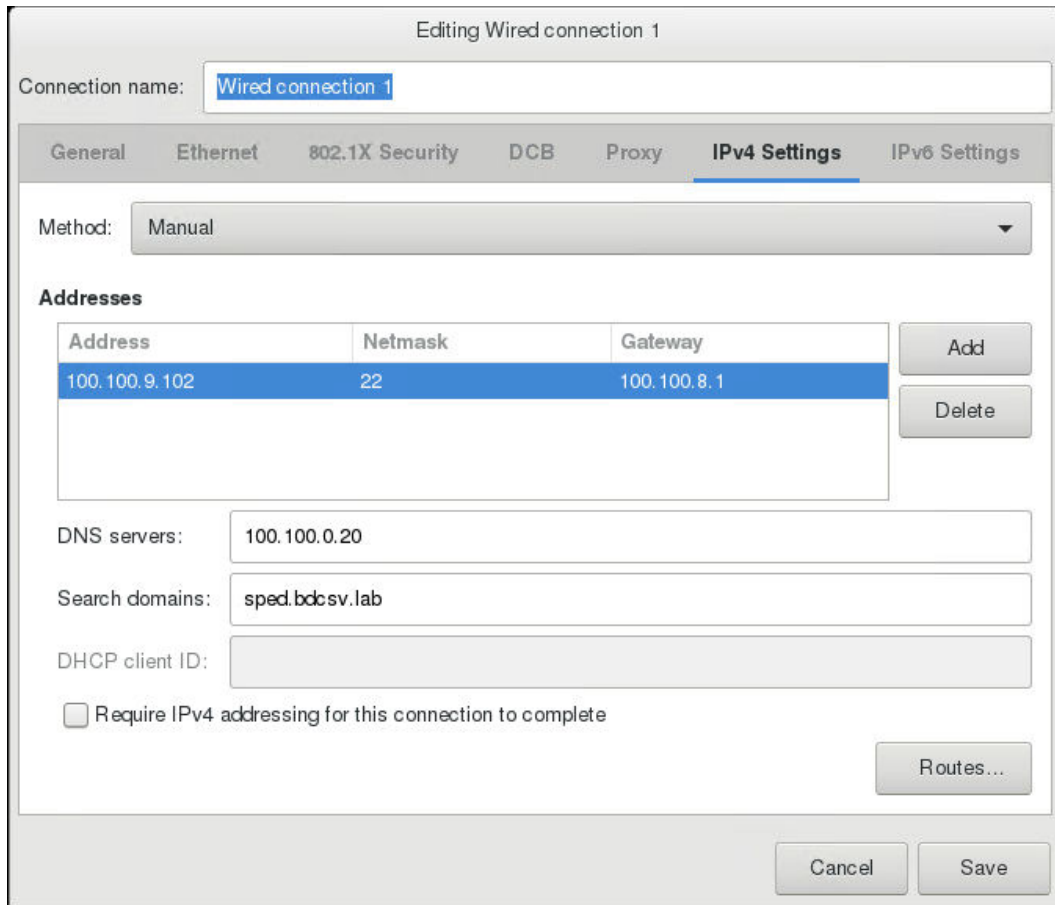
 **노트:** 자동(DHCP)을 선택한 경우, 다음 재시작 중에 OMIVV 어플라이언스가 DHCP 서버로부터 IP를 자동으로 수신하므로 IP 주소를 입력하지 마십시오.

b. 올바른 IP, 넷마스크(CIDR[Classless Inter-Domain Routing] 형식) 및 게이트웨이 정보를 입력합니다.

넷마스크 입력란에 IP 주소를 입력하면 해당하는 CIDR 형식으로 자동 변환됩니다.

c. **DNS 서버** 및 **검색 도메인** 입력란에 검색할 DNS 서버 IP 및 도메인을 각각 입력합니다.

d. 이 연결을 수행하는 데 **IPv4 주소 지정 필요** 확인란을 선택하고 **저장**을 클릭합니다.



이 노트:

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

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

이 노트:

vCenter 서버가 OMIVV 어플라이언스에 이미 등록된 경우 모든 vCenter 인스턴스를 등록 취소하고 다시 등록해야 합니다. 자세한 내용은 **등록 취소 및 재등록 관리** 페이지 34을 참조하십시오.

9. 어플라이언스를 다시 시작합니다.

Network Time Protocol 서버 설정

NTP(Network Time Protocol)를 사용하여 OMIVV 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.
3. NTP를 구성한 후 터미널 콘솔을 시작하고 **네트워크에서 날짜 및 시간 동기화** 확인란을 선택합니다.

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

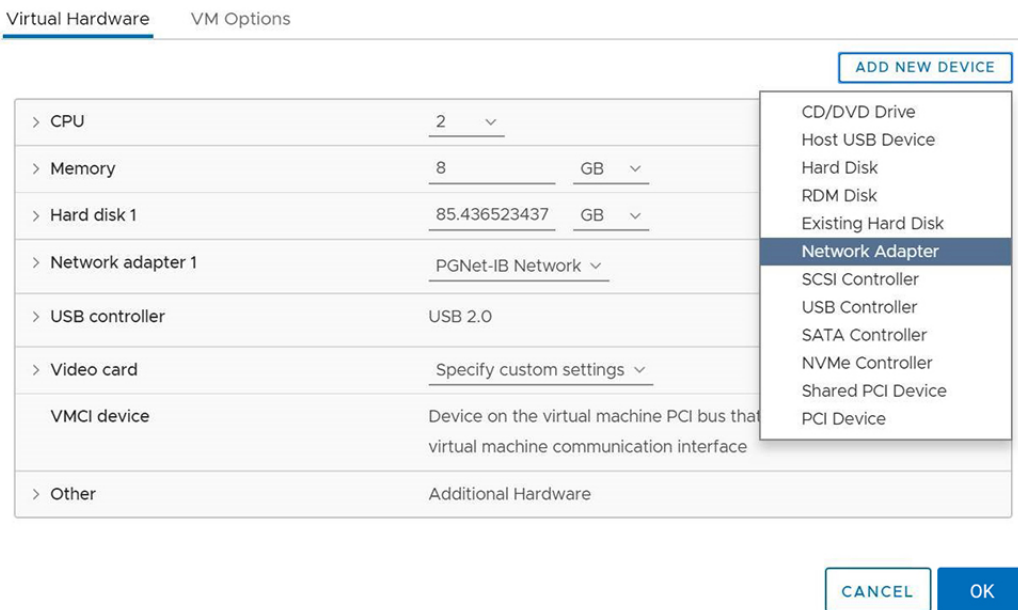
2개의 네트워크 어댑터로 OMIVV 어플라이언스 구성

vSphere 환경에서 Dell EMC 서버를 관리하려면 OMIVV에서 vSphere 네트워크(vCenter 및 ESXi 관리 네트워크)와 대역외 네트워크(iDRAC, CMC 및 OME-Modular) 모두에 액세스해야 합니다. vSphere 네트워크와 대역외 네트워크가 사용자 환경에서 별도의 분리된 네트워크로 유지되는 경우 OMIVV는 두 개의 네트워크에 액세스해야 합니다. 이 경우 OMIVV 어플라이언스는 두 개의 네트워크 어댑

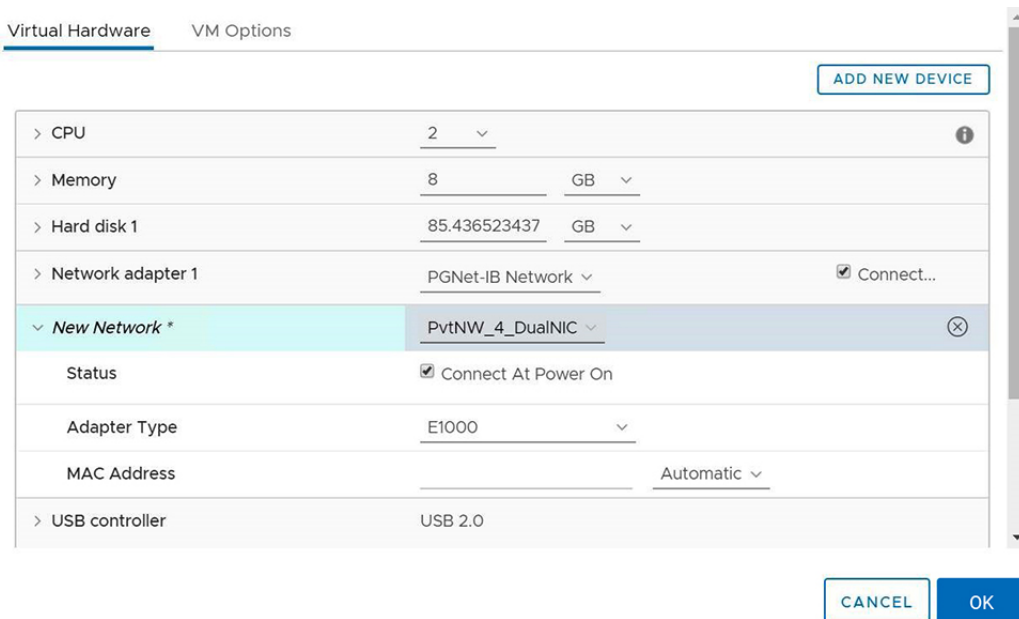
터로 구성되어야 합니다. vSphere 네트워크를 사용하여 대역외 네트워크에 액세스할 수 있는 경우 OMIVV 어플라이언스에 대해 2개의 네트워크 어댑터를 구성하지 마십시오.

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

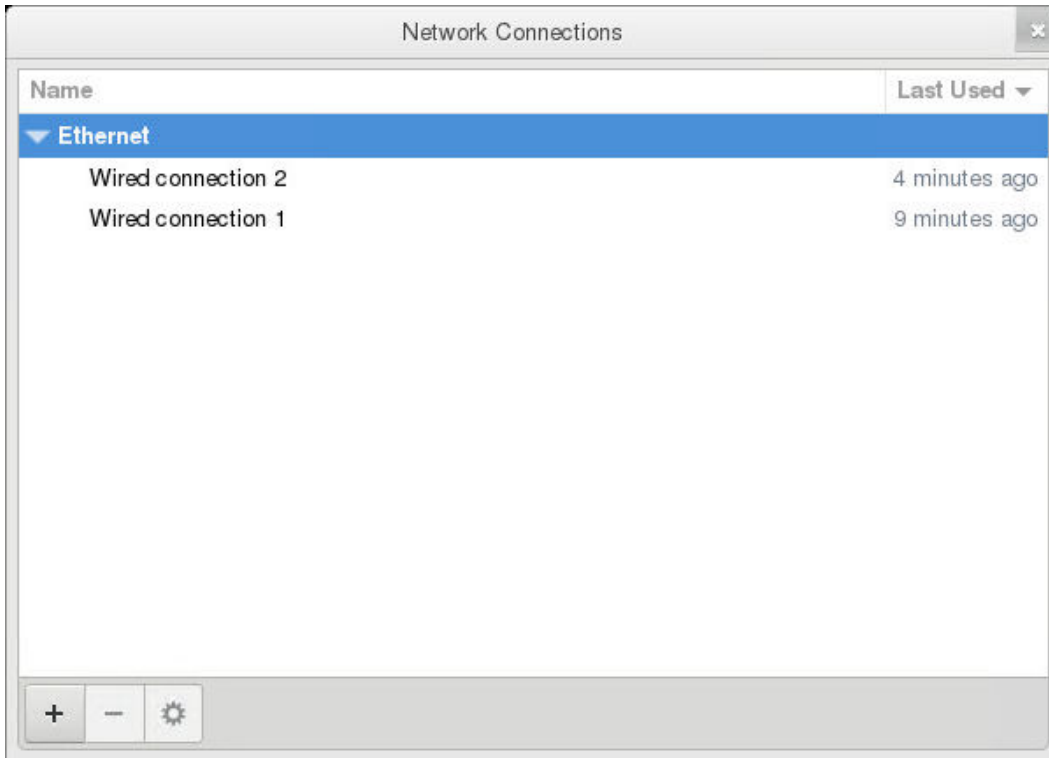
- 어플라이언스의 IP 주소, 넷마스크(CIDR 형식) 및 게이트웨이(고정된 경우)
 - 기본 게이트웨이 - 인터넷에 연결된 하나의 네트워크에 대해서만 기본 게이트웨이를 구성해야 합니다. vSphere 네트워크를 기본 게이트웨이로 사용하는 것이 좋습니다.
 - 라우팅 요구 사항(네트워크 IP, 넷마스크 및 게이트웨이) - 직접 또는 기본 게이트웨이를 통해 연결할 수 없는 다른 외부 네트워크의 경우 고정 경로를 구성합니다.
 - DNS 요구 사항 - OMIVV는 하나의 네트워크에 대해서만 DNS 구성만 지원합니다. DNS 구성에 대한 자세한 내용을 보려면 이 항목의 9단계(b)로 이동하십시오.
1. OMIVV 어플라이언스를 종료합니다.
 2. vSphere Client(HTML-5)를 사용하여 VM 설정을 편집하고 네트워크 어댑터를 추가합니다. VM 설정을 편집하려면 VM을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집** 을 클릭합니다.
 3. **새 장치 추가**를 클릭하고 **네트워크 어댑터**를 선택합니다.



- a. 네트워크 어댑터에 적합한 네트워크를 선택한 후 **전원을 켤 때 연결** 확인란을 선택합니다.
- b. 드롭다운 메뉴에서 **E1000** 어댑터 유형을 선택합니다. OMIVV는 E1000 유형의 네트워크 어댑터만 지원합니다.




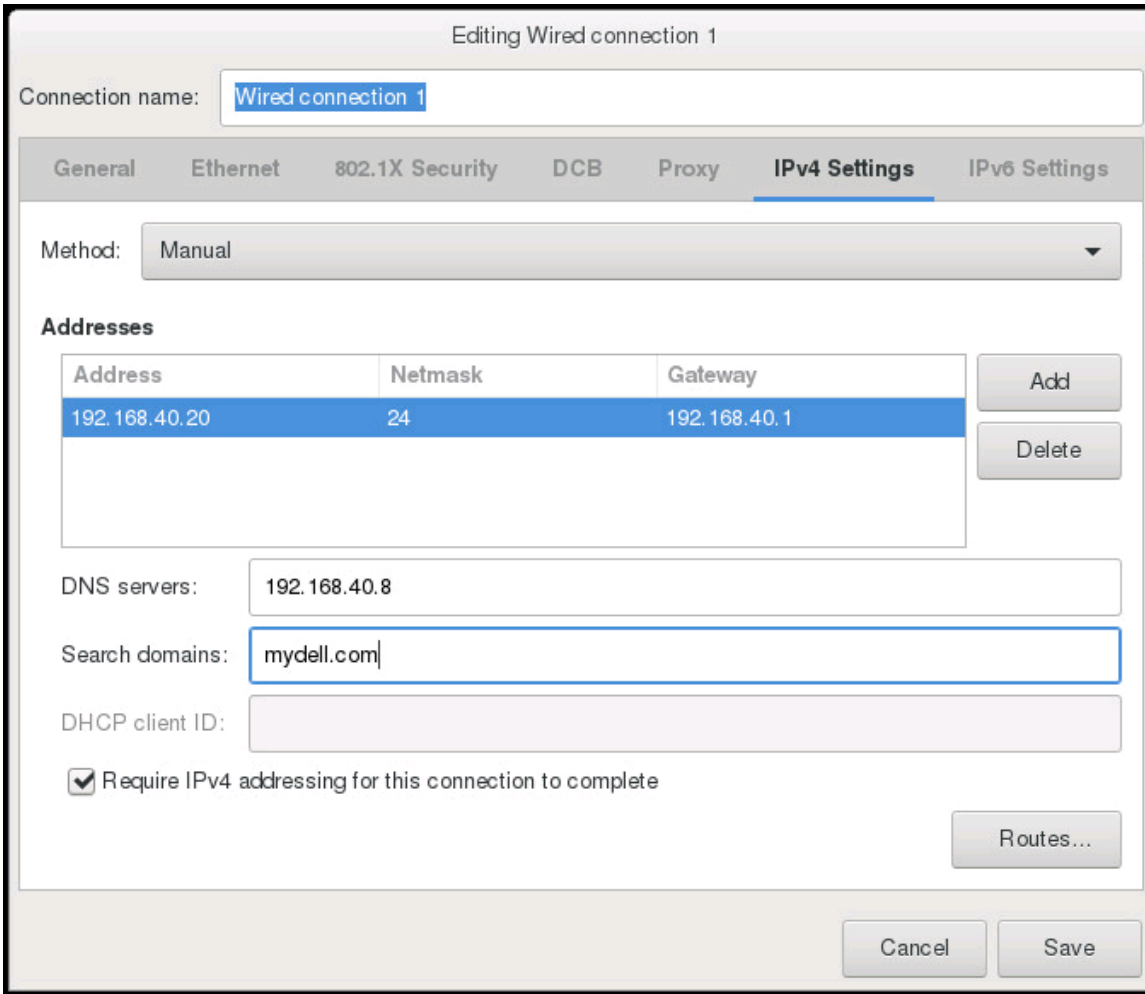
4. VM의 전원을 켭니다. 관리자(기본 사용자 이름: Admin)로 로그인한 후 **Enter** 키를 누릅니다.
5. **OpenManage Integration for VMware vCenter 가상 어플라이언스 설정** 페이지에서 **네트워크 구성**을 선택합니다. **네트워크 연결** 페이지에 NIC 2개가 표시됩니다.



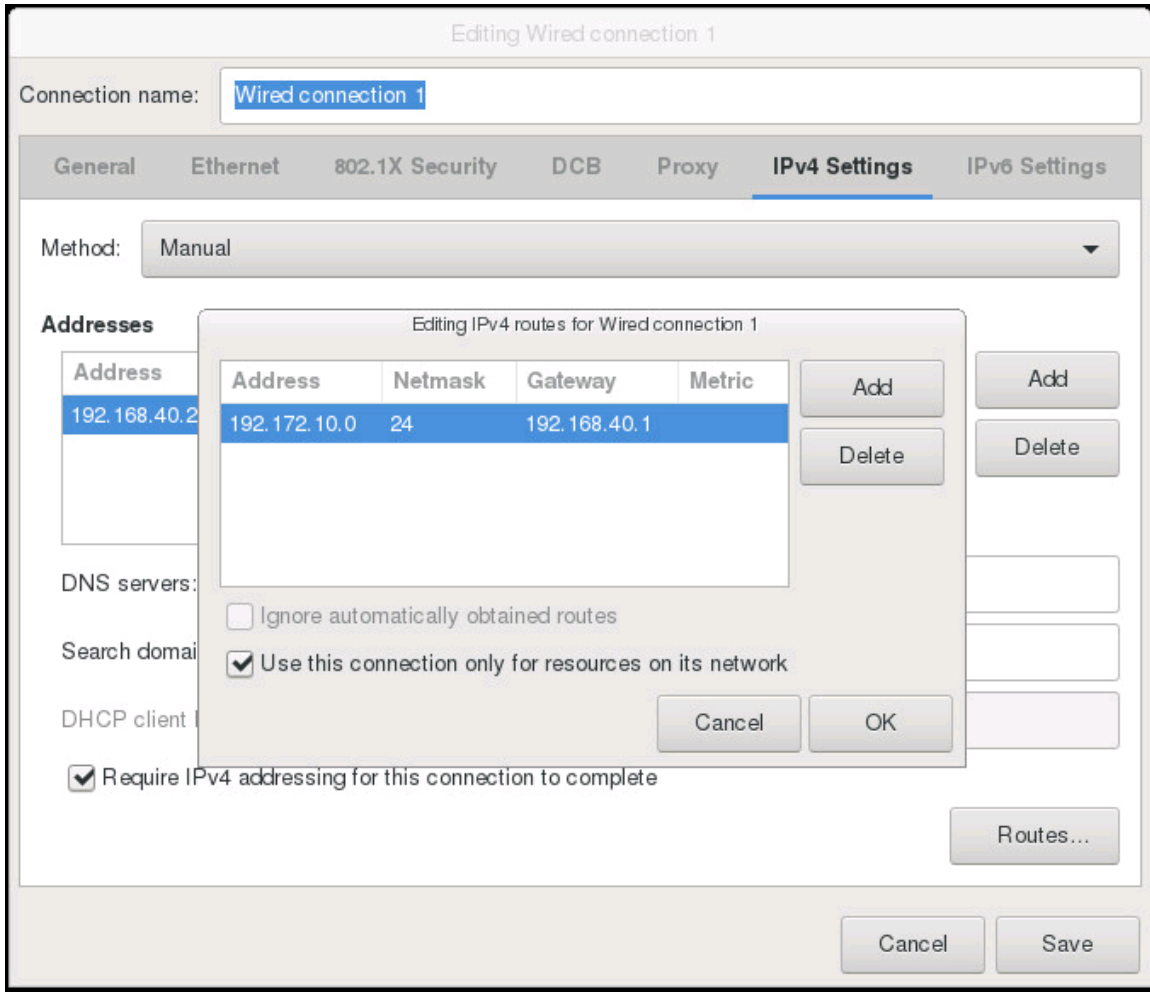
경고: "+"를 사용하여 새 네트워크 인터페이스를 추가하지 마십시오. 네트워크 어댑터를 추가하려면 vSphere 편집 설정을 사용해야 합니다.



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



- a. 방법 드롭다운 목록에서 수동 또는 자동(DHCP)을 선택합니다.
- b. 수동 방법을 선택한 경우 **추가**를 클릭하고 올바른 IP 주소, 넷마스크(CIDR 형식) 및 게이트웨이 세부 정보를 입력합니다. DNS 서버의 우선 순위(기본 및 보조 DNS 항목)를 제어하려면 고정 IP를 사용하는 것이 좋습니다.
일반적으로 vCenter 및 ESXi 호스트와 같은 데이터 센터의 vSphere 요소는 호스트 이름 또는 FQDN을 사용하여 관리됩니다. iDRAC, CMC 및 OME-Modular는 IP 주소를 사용하여 관리됩니다. 이 경우 vSphere 네트워크에 대해서만 DNS 설정을 구성하는 것이 좋습니다.
호스트 이름 또는 FQDN을 사용하여 vSphere 네트워크와 iDRAC 관리 네트워크를 모두 관리하는 경우 DNS 서버가 두 개의 네트워크에 대해 호스트 이름 또는 FQDN을 확인하도록 구성되어야 합니다. 자세한 내용은 CentOS 설명서를 참조하십시오.
❗ 노트: 마지막으로 구성된 DNS 서버는 DNS가 구성된 네트워크와 상관없이 기본 DNS가 됩니다.
- c. **DNS 서버 및 검색 도메인** 상자에 검색할 DNS 서버 IP 및 도메인을 각각 입력합니다.
- d. 이 연결을 수행하는 데 **IPv4 주소 지정 필요** 확인란을 선택하고 **저장**을 클릭합니다.
- e. 이 네트워크를 기본 네트워크(게이트웨이)로 사용하지 않으려면 **루트**를 클릭하고 이 연결을 해당 네트워크의 리소스에 대해 **서만 사용** 확인란을 선택합니다.
❗ 노트: 여러 네트워크를 기본 게이트웨이로 추가하면 네트워크 문제가 발생하고 OMIVV 기능이 영향을 받을 수 있습니다.
- f. 알려진 게이트웨이를 사용하여 외부 네트워크에 연결하려는 경우 동일한 페이지에서 **추가**를 클릭하고 네트워크 IP 주소, 넷마스크(CIDR 형식) 및 게이트웨이 세부 정보를 추가합니다.



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

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

g. 확인을 클릭합니다.

10. 저장을 클릭합니다. 다른 NIC를 구성하려면 6~10번 작업을 반복합니다.

11. **OpenManage Integration for VMware vCenter 가상 어플라이언스 설정** 유틸리티에서 **어플라이언스 재부팅**을 클릭합니다. 네트워크 구성은 OMIVV 어플라이언스를 재시작해야 완료됩니다.

노트:

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

인증서 서명 요청(CSR) 생성

vCenter에 OMIVV를 등록하기 전에 CSR을 업로드해야 합니다.

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

1. **어플라이언스 관리** 페이지의 **HTTPS 인증서** 영역에서 **인증서 서명 요청 생성**을 클릭합니다.

새 요청을 생성하면 이전 CSR을 사용하여 생성한 인증서를 더는 어플라이언스에 업로드할 수 없다는 메시지가 표시됩니다. 요청을 계속하려면 **계속**을 클릭합니다.

- 요청을 계속할 경우 **인증서 서명 요청 생성** 대화 상자에서 공통 이름, 조직, 지역, 구/군/시, 주, 국가 및 이메일 주소 정보를 입력합니다. **계속**을 클릭합니다.
- 다운로드**를 클릭하고 결과로 생성되는 CSR을 액세스 가능한 위치에 저장합니다.

HTTPS 인증서 업로드

인증서는 PEM 형식을 사용해야 합니다.

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

- 어플라이언스 관리 페이지의 **HTTPS 인증서** 영역에서 **인증서 업로드**를 클릭합니다.
- 인증서 업로드** 대화 상자에서 **확인**을 클릭합니다.
- 인증서를 업로드하려면 **찾아보기**를 클릭한 후 **업로드**를 클릭합니다.

노트: 사용자 정의 CSR을 OMIVV로 업로드하려면 vCenter 등록 전에 새로운 인증서를 업로드해야 합니다. vCenter 등록 후에 새로운 사용자 정의 인증서를 업로드하면 vSphere Client(HTML-5)에 통신 오류가 표시됩니다. 이 문제를 해결하려면 vCenter에서 어플라이언스를 등록 취소한 후 다시 등록합니다. 자세한 내용은 **등록 취소 및 재등록 관리** 페이지 34을 참조하십시오.

HTTPS 인증서 업로드 작업이 완료되면 브라우저 세션을 닫고 새 브라우저 세션에서 관리 포털에 액세스합니다.

기본 HTTPS 인증서 복원

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

기본 HTTPS 인증서 복원 작업이 완료된 후 브라우저 세션을 닫고 새 브라우저 세션에서 관리 포털에 액세스합니다.

OpenManage Integration for VMware vCenter 등록 및 라이선스 파일 가져오기

Dell Digital Locker에서 라이선스를 다운로드할 준비가 되었는지 확인합니다. 라이선스를 두 개 이상 주문한 경우, 각자 다른 시간에 따로 제공될 수 있습니다. **주문 현황**에서 다른 라이선스 항목의 상태를 확인할 수 있습니다. 라이선스 파일은 .XML 형식으로 제공됩니다.

노트: 어플라이언스에 대한 사용자 정의 인증서를 업로드하려면 vCenter 등록 전에 새로운 인증서를 업로드해야 합니다. vCenter 등록 후에 새로운 사용자 정의 인증서를 업로드하면 vSphere Client(HTML-5)에 통신 오류가 표시됩니다. 이 문제를 해결하려면 vCenter에서 어플라이언스를 등록 취소한 후 다시 등록합니다. 자세한 내용은 **등록 취소 및 재등록 관리** 페이지 34을(를) 참조하십시오.

- 지원되는 브라우저에서 **관리 콘솔**을 엽니다.

관리 콘솔을 열려면 웹 브라우저를 시작하고 `https://<ApplianceIP>` 또는 `Appliance hostname` 또는 `FQDN`을 입력합니다.

IP 주소는 ESXi 호스트 IP 주소가 아니라 어플라이언스 VM의 IP 주소입니다. 관리 콘솔에는 콘솔 위에 나온 URL을 이용하여 액세스할 수 있습니다.

예: `https://10.210.126.120` 또는 `https://myesxihost`

URL은 대소문자를 구분하지 않습니다.

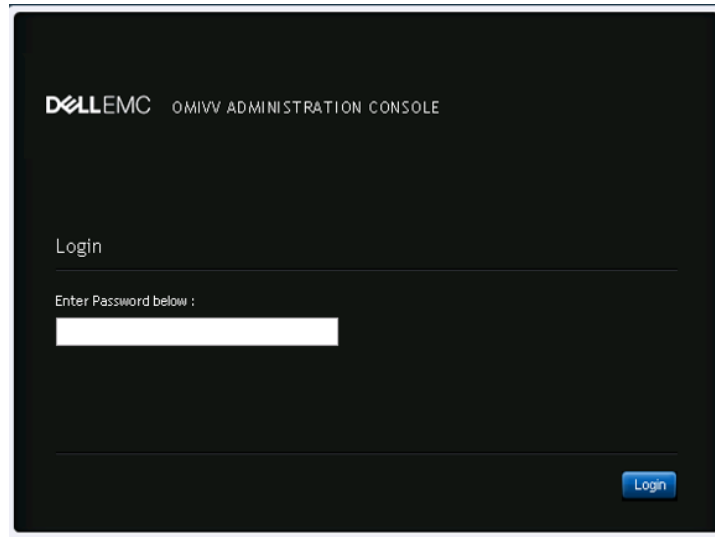


그림 1. 관리 콘솔

2. 관리 콘솔 로그인 창에서 암호를 입력하고 로그인을 클릭합니다.

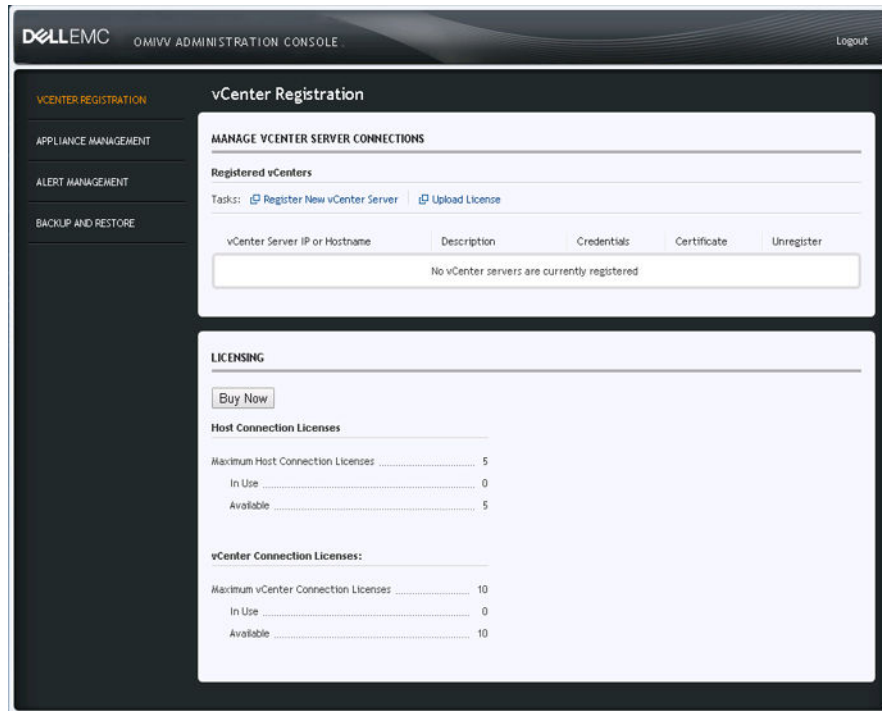


그림 2. 관리 콘솔의 vCenter 등록 창

3. vCenter 등록 창에서 새 vCenter 서버 등록을 클릭합니다.
4. 새 vCenter 서버 등록 창에서 다음 하위 작업을 수행합니다.
 - a. vCenter 이름 아래에 있는 vCenter 서버 IP 또는 호스트 이름 텍스트 상자에 서버 IP 또는 FQDN을 입력한 후 설명 텍스트 상자에 설명을 입력합니다. 설명은 선택 사항입니다.

이 노트: FQDN(Fully Qualified Domain Name)을 사용하여 OpenManage Integration for VMware vCenter를 VMware vCenter에 등록할 것을 권장합니다. DNS 서버가 FQDN 기반 등록을 위해 vCenter의 호스트 이름을 적절히 확인할 수 있는지 확인합니다.
 - b. vCenter 사용자 계정 아래 vCenter 사용자 이름에서 관리자 이름 또는 필요한 권한을 가진 사용자 이름을 입력합니다.

domain\user 또는 domain/user 또는 user@domain으로 **username**을 입력합니다. OMIVV는 관리자 사용자 계정 또는 vCenter 관리에 필요한 권한을 지닌 사용자를 사용합니다. 자세한 내용은 [관리자가 아닌 사용자를 사용하여 vCenter 서버 등록 페이지 27](#)을(를) 참조하십시오.

- c. 암호에 암호를 입력합니다.
- d. 암호 확인에 암호를 다시 입력합니다.

5. 등록을 클릭합니다.

노트: OpenManagement Integration for VMware vCenter는 현재 링크된 모드를 사용하여 단일 vCenter 인스턴스 또는 다중 vCenter 서버를 포함하는 추가 대규모 배포 모드에서 최대 2000개의 호스트를 지원합니다.

6. 다음 작업 중 하나를 수행합니다.

- OMIVV 평가판 버전을 사용하는 경우 OMIVV 아이콘을 확인할 수 있습니다.
- 정식 제품 버전을 사용하는 경우 [Dell Digital Locker](#)의 Dell 디지털 로커에서 라이선스 파일을 다운로드할 수 있으며, 이 라이선스를 가상 어플라이언스에 가져올 수 있습니다. 라이선스 파일을 가져오려면 **Upload License**를 클릭합니다.

7. 라이선스 업로드 창에서 **찾아보기**를 클릭하여 라이선스 파일로 이동한 후 **업로드**를 클릭하여 라이선스 파일을 가져옵니다.

노트: 라이선스 파일을 수정하거나 편집하면 해당 라이선스 파일(.XML 파일)이 작동하지 않으며 Dell 디지털 로커에서 .XML 파일(라이선스 키)을 다운로드할 수 있습니다. 라이선스 키가 다운로드되지 않는 경우 [기술 지원 팀에 연락](#)에서 해당 제품의 지역 Dell 지원 부서 전화 번호를 찾아 Dell 지원 부서에 문의합니다.

OMIVV가 등록되면 OMIVV 아이콘이 vSphere Client(HTML-5) 홈 페이지에 표시됩니다.

설치를 확인하려면 [설치 확인](#) 페이지 30을(를) 참조하십시오.

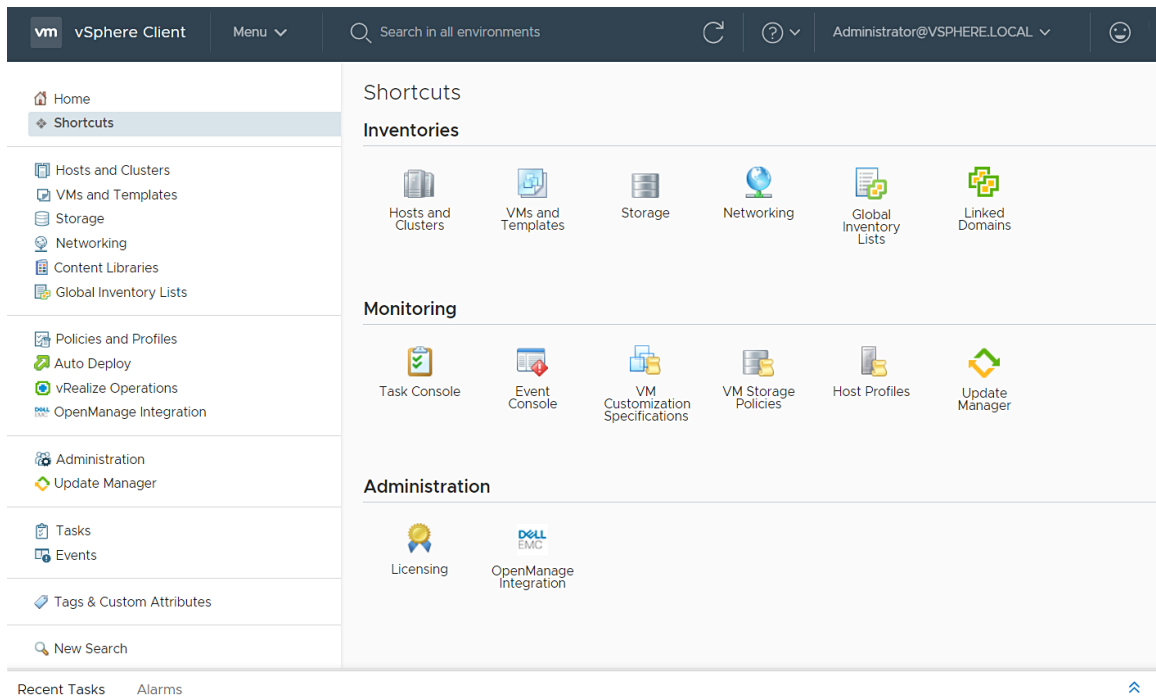


그림 3 . OpenManagement Integration for VMware vCenter가 vCenter에 성공적으로 추가됨

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

예를 들면, 필요한 권한이 있는 사용자 X가 vCenter에 OMIVV를 등록하고 사용자 Y는 Dell 권한만 가지고 있습니다. 사용자 Y는 이제 vCenter에 로그인하여 OMIVV로부터 펌웨어 업데이트 작업을 트리거할 수 있습니다. 펌웨어 업데이트 작업을 수행하는 동안 OMIVV는 사용자 X의 권한을 사용하여 장치를 유지 관리 모드로 두거나 호스트를 재부팅합니다.

관리자가 아닌 사용자를 사용하여 vCenter 서버 등록

다음 작업을 수행하려면 vCenter 관리자 권한이 있어야 합니다.

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

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

1. 역할에 필요한 권한으로 역할을 생성하거나 기존 역할을 수정합니다.
역할에 필요한 권한 목록에 대한 자세한 내용은 **관리자가 아닌 사용자의 필수 권한**을 참조하십시오.
역할을 생성하거나 수정하고 vSphere Client(HTML-5)에서 권한을 선택하는 데 필요한 단계는 VMware vSphere 설명서를 참조하십시오.
2. 역할을 정의하고 역할에 대한 권한을 선택한 후 새로 생성된 역할에 사용자를 할당합니다.
권한에 역할을 할당하기에 대한 자세한 내용은 VMware vSphere 설명서를 참조하십시오.
필요한 권한을 가진 vCenter Server 관리자가 아닌 사용자가 이제 vCenter를 등록 또는 등록 해제하거나, 자격 증명을 수정하거나, 인증서를 업데이트할 수 있습니다.
3. 필요한 권한이 있는 관리자가 아닌 사용자를 사용하여 vCenter 서버를 등록합니다.
4. 등록이 완료된 후에 1단계에서 생성했거나 수정한 역할에 Dell 권한을 할당합니다. **기존 역할에 Dell 권한 할당** 페이지 29을(를) 참조하십시오.

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

관리자가 아닌 사용자의 필수 권한

OMIVV를 vCenter에 등록하려면 관리자가 아닌 사용자에게 다음 권한이 있어야 합니다.

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

- 알람
 - 알람 생성
 - 알람 수정
 - 알람 제거
- 확장명
 - 확장명 등록
 - 확장명 등록 취소
 - 확장명 업데이트
- 전역
 - 작업 취소
 - 이벤트 로그
 - 설정
- **i** **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
 - 설정 변경
 - 연결
 - 유지관리
 - 네트워크 구성
 - 쿼리 패치
 - 보안 프로필 및 방화벽
- **i** **노트:** vCenter 6.5를 사용하거나 vCenter 6.5 이상으로 업그레이드하는 경우 클러스터 수정 권한을 할당해야 합니다.
 - Host.Config
 - 고급 설정
 - 연결

- 유지관리
- 네트워크 구성
- 쿼리 패치
- 보안 프로필 및 방화벽

○ 인벤토리

- 클러스터에 호스트 추가
- 독립 실행형 호스트 추가
- 클러스터 수정

이 노트: vCenter 6.5를 사용하거나 vCenter 6.5 이상으로 업그레이드하는 경우 클러스터 수정 권한을 할당해야 합니다.

● 호스트 프로필

- 편집
- 보기

● 권한

- 권한 수정
- 역할 수정

● 세션

- 세션 유효성 검사

● 작업


- 작업 생성
- 작업 업데이트

이 노트: 관리자가 아닌 사용자를 사용하여 OMIVV 기능에 액세스하기 위해 vCenter 서버를 등록한 경우 관리자가 아닌 사용자는 Dell 권한이 있어야 합니다. Dell 권한 할당에 대한 자세한 내용은 [기본 역할에 Dell 권한 할당](#) 페이지 29을(를) 참조하십시오.

기본 역할에 Dell 권한 할당

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

기본 역할을 편집하여 Dell 권한을 할당할 수 있습니다.

1. 관리 권한을 사용하여 vSphere Client(HTML-5)에 로그인합니다.
2. vSphere Client(HTML-5)에서 **메뉴**를 확장하고 **관리** → **역할**을 클릭합니다.
3. **역할 공급자** 드롭다운 목록에서 vCenter 서버를 선택합니다.
4. **역할** 목록에서 **Dell-Operational**을 선택한 후 **권한**을 클릭합니다.
5. Dell 권한을 할당하려면 편집 아이콘 []을 클릭합니다. **역할 편집** 페이지가 표시됩니다.
6. 왼쪽 창에서 **Dell**을 클릭하고 선택한 역할에 대해 다음 Dell 권한을 선택한 후 **다음**을 클릭합니다.
 - Dell.Configuration
 - Dell.Deploy-Provisioning
 - Dell.Inventory
 - Dell.Monitoring
 - Dell.Reporting

vCenter 내에서 사용 가능한 OMIVV 역할에 대한 자세한 내용은 (사용자 가이드의 보안 역할 및 사용 권한 항목)을 참조하십시오.

7. 필요한 경우 역할 이름을 편집하고 선택한 역할에 대한 설명을 입력합니다.
8. **마침**을 클릭합니다. 로그아웃한 다음 vCenter에서 로그인합니다. 이제 필요한 권한이 있는 사용자가 OMIVV 작업을 수행할 수 있습니다.

등록된 vCenter 버전을 업그레이드한 후 OMIVV 재구성

등록된 vCenter를 업그레이드한 후 다음 작업을 수행합니다.

- 관리자가 아닌 사용자의 경우:
 1. 필요한 경우 관리자가 아닌 사용자에게 추가 권한을 할당합니다. [관리자가 아닌 사용자의 필수 권한](#) 페이지 28을 참조하십시오.

예를 들어, vCenter 6.0에서 vCenter 6.5로 업그레이드하는 경우, 추가 권한을 할당합니다.

- 2. 등록된 OMIVV 어플라이언스를 재부팅합니다.
- 관리자 사용자의 경우:
 1. 등록된 OMIVV 어플라이언스를 재부팅합니다.

설치 확인

다음은 OMIVV 설치가 성공했는지 확인하는 단계입니다.

1. vSphere Client 창을 닫고 새 vSphere Client(HTML-5)를 시작합니다.
2. vCenter 서버에서 가상 어플라이언스 IP 주소 또는 호스트 이름으로 PING 명령을 시도하여 vCenter가 OMIVV와 통신할 수 있는지 확인합니다.
3. vSphere Client에서 **메뉴**를 확장하고 **관리 > 솔루션 > 클라이언트 플러그인**을 클릭합니다.
플러그인 관리 또는 **클라이언트 플러그인** 페이지의 액세스 제한에 대한 자세한 내용은 VMware 설명서를 참조하십시오.
4. **클라이언트 플러그인** 페이지에서 버전을 확인하고 OMIVV가 설치 및 활성화되어 있는지 확인합니다.
OMIVV가 활성화되지 않은 경우 잠시 기다린 후 로그아웃하고 vCenter에서 로그인합니다.
5. vSphere Client(HTML-5) 내에 OMIVV 아이콘이 표시되는지 확인하려면 vSphere Client에서 **메뉴**를 확장합니다.
OpenManage Integration 아이콘이 표시됩니다.

백업 및 복원 관리

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

- 백업 및 복원 구성
- 자동 백업 예약
- 즉시 백업 수행
- 백업에서 데이터베이스 복원
- 백업 및 복원 설정 재설정 페이지 31

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

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

백업 및 복원 구성

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

이 노트: NTP 설정은 저장 및 복원되지 않습니다.

1. **백업 및 복원 설정** 페이지에서 **편집**을 클릭합니다.
2. 강조 표시된 **설정 및 세부 정보** 영역에서 다음을 수행합니다.
 - a. **백업 위치**에 백업 파일 경로를 입력합니다.
 - b. **사용자 이름**에 사용자 이름을 입력합니다.
 - c. **암호**에 암호를 입력합니다. 비밀번호 끝에는 % 부호를 지원하지 않습니다.
 - d. **백업 암호화에 사용되는 암호 입력** 상자에 암호화된 암호를 입력합니다.
암호화 암호에는 영숫자와 "!, @, #, \$, %, *" 등의 특수 문자를 사용할 수 있습니다.
 - e. **암호 확인**에 암호화된 암호를 다시 입력합니다.
3. 설정을 저장하려면 **적용**을 클릭합니다.
4. 백업 일정을 구성합니다. **자동 백업 예약**을 참조하십시오.

이 절차를 마친 후에는 백업 일정을 구성합니다.

자동 백업 예약

백업 위치 및 자격 증명 구성에 대한 자세한 내용은 [백업 및 복원 구성](#)을 참조하십시오.

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

즉시 백업 수행

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

백업에서 OMIVV 데이터베이스 복원

이전 버전에서 OMIVV를 복원한 후 다음을 수행합니다.

- 11G 운영 체제 미설치 서버는 지원되지 않습니다. 12G 이상 세대 서버만 복원 후 유지됩니다.
- 하드웨어 프로필 및 배포 템플릿은 지원되지 않습니다. Dell EMC는 배포에 시스템 프로필을 사용할 것을 권장합니다.
- 11G 서버에서 예약되거나 하드웨어 프로필 기반 배포 템플릿을 사용하는 배포 작업은 취소됩니다.
- 모든 11G 서버는 자격 증명 프로필에서 제거되며 소비된 라이선스는 해제됩니다.
- 리포지토리 프로필은 64비트 번들만 사용합니다.

이 노트: 4.x에서 5.x로 백업 및 복원을 수행하는 경우 OMIVV에서 5.x의 32비트 펌웨어 번들을 지원하지 않기 때문에 클러스터 프로필 이름에 경고 기호가 표시됩니다. 클러스터 프로필에 대한 최신 변경 사항을 사용하려면 클러스터 프로필을 편집합니다.

- 11G 서버에서 예약된 펌웨어 업데이트 작업은 취소됩니다.

복원 작업이 완료되면 OMIVV 어플라이언스가 재부팅됩니다.

1. **백업 및 복원 설정** 페이지에서 **지금 복원**을 클릭합니다.
2. **지금 복원** 대화 상자의 **파일 위치**에 CIFS 또는 NFS 형식의 백업 .gz 파일에 대한 경로를 입력합니다.
3. 백업 파일의 **사용자 이름, 암호 및 암호화 암호**를 입력합니다.
암호화 암호에는 영숫자와 "!, @, #, \$, %, *" 등의 특수 문자를 사용할 수 있습니다.
4. 변경사항을 저장하려면 **적용**을 클릭합니다.
어플라이언스가 재시작됩니다. 설치를 확인하려면 **설치 확인** 페이지 30을(를) 참조하십시오. .

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

백업 및 복원 설정 재설정

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


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

OMIVV 어플라이언스 및 리포지토리 위치 업데이트

- 모든 데이터를 보호하려면 OMIVV 어플라이언스 업데이트 이전에 OMIVV 데이터베이스의 백업을 수행합니다. [백업 및 복원 관리](#) 페이지 30을(를) 참조하십시오.

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

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

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

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


옵션	설명
1	RPM에 틱 기호가 있는 경우, 기존 버전에서 사용 가능한 최신 버전으로 RPM을 업그레이드할 수 있습니다. RPM을 사용하여 OMIVV 어플라이언스 업그레이드 페이지 32을(를) 참조하십시오.
2	OVF에 틱 기호가 있는 경우, 기존 버전에서 OMIVV 데이터베이스를 백업한 다음 사용 가능한 최신 어플라이언스 버전에서 복원할 수 있습니다. 백업 및 복원을 사용하여 OMIVV 어플라이언스 업그레이드 페이지 33을(를) 참조하십시오.
3	RPM 및 OVF 모두에 틱 기호가 있는 경우, 언급된 옵션 중 하나를 수행하여 어플라이언스를 업그레이드할 수 있습니다. 이 시나리오에서 권장되는 옵션은 RPM 업그레이드입니다.

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

RPM을 사용하여 OMIVV 어플라이언스 업그레이드

현재 버전보다 높은 버전의 어플라이언스로 업그레이드하고 있는지 확인합니다.

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

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

2. OMIVV 플러그인을 기존 버전에서 사용 가능한 버전으로 업그레이드하려면 다음 단계 중 하나를 수행합니다.

- **업데이트 리포지토리 경로**에서 사용할 수 있는 RPM을 사용하여 업그레이드하려면 **업데이트 리포지토리 경로**가 다음 경로로 설정되어 있는지 확인합니다. <https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/>

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

3. 사용 가능한 OMIVV 어플라이언스 버전과 현재 OMIVV 어플라이언스 버전을 비교합니다.


4. 업데이트를 OMIVV 어플라이언스에 적용하려면 **어플라이언스 설정** 아래에서 **가상 어플라이언스 업데이트**를 클릭합니다.


5. **어플라이언스 업데이트** 대화 상자에서 **업그레이드**를 클릭합니다.

업데이트를 클릭하면 **관리 콘솔** 창에서 로그아웃됩니다.

6. 웹 브라우저를 닫습니다.

어플라이언스가 RPM으로 업그레이드되면 Dell 관리 포털에 로그인하기 전에 브라우저 캐시를 지워야 합니다.

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

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

Vmware 툴 업그레이드

1. OMIVV 어플라이언스를 마우스 오른쪽 버튼으로 클릭합니다.
2. 게스트 OS 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 작업** 섹션에서 설치 상태를 볼 수 있습니다.

백업 및 복원을 사용하여 OMIVV 어플라이언스 업그레이드

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

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

OMIVV 어플라이언스를 이전 버전에서 최신 버전으로 업데이트하려면 다음 단계를 수행합니다.

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

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

이 노트: 새 어플라이언스의 IP 주소가 이전 어플라이언스의 IP 주소와 다를 경우 Proactive HA 기능이 제대로 작동하지 않을 수 있습니다. 이러한 시나리오에서는 Dell EMC 호스트가 있는 각 클러스터에 대해 Proactive HA를 비활성화하고 활성화합니다.

6. OMIVV 어플라이언스는 기본 인증서와 함께 제공됩니다. 어플라이언스에 대한 사용자 정의 인증서를 사용하려면 동일 항목을 업데이트합니다. **인증서 서명 요청(CSR) 생성** 페이지 24 및 **HTTPS 인증서 업로드** 페이지 25의 내용을 참조하십시오. 그렇지 않으면 이 단계를 건너뜁니다.
7. 데이터베이스를 새 OMIVV 어플라이언스에 복원합니다. **백업에서 OMIVV 데이터베이스 복원**을 참조하십시오.
8. 어플라이언스를 확인합니다. 자세한 내용은 **설치 확인** 페이지 30을(를) 참조하십시오.
9. Dell EMC는 업그레이드 후 OMIVV 플러그인이 관리하는 모든 호스트에서 인벤토리를 다시 실행할 것을 권장합니다.

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

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

이 노트: 새 OMIVV 버전 Y의 ID(IP 또는 FQDN)가 OMIVV 버전 X에서 변경된 경우 SNMP 트랩의 트랩 대상이 새 어플라이언스를 가리키도록 구성합니다. 12G 이상 서버의 경우 해당 호스트에서 인벤토리를 실행하면 ID 변경이 고정됩니다. 12G 호스트에서 인벤토리를 실행하는 동안 SNMP 트랩이 새 IP를 가리키지 못하면 이러한 호스트는 비준수로 나열됩니다. 호스트 규정 준수 문제를 해결하려면 사용자 가이드의 관리 규정 준수 섹션을 참조하십시오.

이전 버전의 OMIVV에서 업데이트된 버전으로 백업 및 복원한 후 200000 메시지가 표시되거나 Dell EMC 로고가 표시되지 않거나 OMIVV UI가 vCenter UI에서 응답하지 않는 경우 다음을 수행합니다.

- vCenter 서버에서 vSphere Client(HTML-5) 및 vSphere Web Client(FLEX) 모두에 대한 vSphere Client 서비스를 다시 시작합니다.
- 문제가 지속되면, 다음과 같이 하십시오.
 - VMware vCenter 서버 어플라이언스의 경우 `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity`로 이동합니다. Windows vCenter의 경우 vCenter 어플라이언스의 `C:\ProgramData\VMware\VMwareServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity` 폴더로 이동하고 기존 버전에 해당하는 이전 데이터가 있는지 확인합니다.
이전 데이터의 예: `com.dell.plugin.OpenManage—com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX`.
 - 이전 OMIVV 버전에 해당하는 폴더를 수동으로 삭제하고 vSphere Client(HTML-5) 및 Web Client(FLEX) 모두에 대한 vSphere Client 서비스를 다시 시작합니다.

OpenManage Integration for VMware vCenter 등록 취소

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

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

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

1. <https://<ApplianceIP/hostname/>>으로 이동합니다.
2. VCENTER 등록 페이지의 vCenter 서버 IP 또는 호스트 이름 표에서 등록 취소를 클릭합니다.
이 노트: OMIVV는 둘 이상의 vCenter와 연결될 수 있으므로 올바른 vCenter를 선택해야 합니다.
3. 선택한 vCenter 서버의 등록 취소를 확인하려면 VCENTER 등록 취소 대화 상자에서 등록 취소를 클릭합니다.
이 노트: OMIVV를 등록 취소한 후 vSphere Client(HTML-5)에서 로그아웃하고 로그인합니다. OMIVV 아이콘이 계속 표시되면 vSphere Client(HTML-5)와 Web Client(FLEX) 모두에 대한 클라이언트 서비스를 다시 시작합니다.

등록 취소 후 OMIVV 복구

이전 버전의 OMIVV를 등록 취소한 후 OMIVV 복구

이전 버전의 데이터베이스를 백업한 후에 OMIVV 플러그 인을 등록 취소한 경우 다음 단계를 수행한 후에 마이그레이션을 계속 진행하십시오.

- 이 노트:** 플러그인을 등록 취소하면 등록된 알람과 PHA 클러스터에 대한 Dell 상태 업데이트 공급자에서 구현된 모든 사용자 정의가 제거됩니다. 다음 단계를 통해 사용자 정의가 복원되지 않습니다. 그러나, 기본 상태로 알람이 다시 등록됩니다.
- 이 노트:** 새 OMIVV 어플라이언스에 대한 이전 OMIVV 어플라이언스의 ID(IP 또는 FQDN)를 유지하는 것이 좋습니다.
- 이 노트:** 새 어플라이언스의 IP 주소가 이전 어플라이언스의 IP 주소와 다를 경우 Proactive HA 기능이 제대로 작동하지 않을 수 있습니다. 이러한 시나리오에서는 Dell 호스트가 있는 각 클러스터에 대해 PHA를 비활성화하고 활성화합니다.

백업 및 복원을 사용하여 OMIVV 어플라이언스 업그레이드 페이지 33에 나열된 3-9의 작업을 수행합니다.

등록 취소 및 재등록 관리

Dell EMC는 등록 취소를 수행하기 전에 백업을 수행하는 것을 권장합니다.

- 이 노트:** 플러그인을 등록 취소하면 등록된 알람과 PHA 클러스터에 대한 Dell 상태 업데이트 공급자에서 구현된 모든 사용자 정의가 제거됩니다. 다음 단계를 통해 사용자 정의가 복원되지 않습니다. 그러나, 기본 상태로 알람이 다시 등록됩니다.
1. OMIVV 백업을 수행합니다.
2. OMIVV에서 vCenter의 등록을 취소합니다.
3. 계획된 구성 변경을 수행합니다. 예를 들어, 호스트 이름 변경, 새 구성 변경 등이 있습니다.
4. OMIVV 어플라이언스를 다시 시작합니다.
5. 백업 파일을 복원합니다. 자세한 내용은 백업 및 복원을 사용하여 OMIVV 어플라이언스 업그레이드 페이지 33을(를) 참조하십시오.

VMware vCenter용 어플라이언스 구성

다음 방법 중 하나를 사용하여 OMIVV 어플라이언스를 구성할 수 있습니다.

- 초기 구성 마법사를 사용합니다.

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

나중에 초기 구성 마법사를 실행하려면 다음으로 이동하십시오.

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

- 설정 탭을 사용합니다.

이 노트: 사용자 인터페이스는 두 방법 모두에서 비슷합니다.

주제:

- 초기 구성 마법사를 사용하여 구성 작업
- 설정 페이지에서 구성 작업

초기 구성 마법사를 사용하여 구성 작업

이 노트: DNS 설정을 변경한 후 OMIVV 관련 작업을 수행하는 동안 웹 통신 오류가 발견되는 경우 브라우저 캐시를 지우고 vSphere Client(HTML-5)에서 로그아웃한 다음 다시 로그인 합니다.

초기 구성 마법사를 사용하여 다음 작업을 보고 수행할 수 있습니다.

- vCenter를 선택합니다.
- 호스트 자격 증명 프로필을 생성합니다. 자세한 내용은 [호스트 자격 증명 프로필 생성](#) 페이지 36을(를) 참조하십시오.
- 이벤트 및 알람을 구성합니다. 자세한 내용은 [이벤트 및 알람 구성](#) 페이지 38을(를) 참조하십시오.
- 인벤토리 작업을 예약합니다. 자세한 내용은 [인벤토리 작업 예약](#) 페이지 37을(를) 참조하십시오.
- 보증 검색 작업을 예약합니다. 자세한 내용은 [보증 검색 작업 예약](#) 페이지 38을(를) 참조하십시오.

초기 구성

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

나중에 초기 구성 마법사를 실행하려면 다음으로 이동하십시오.

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

1. 시작 페이지에서 지침을 읽은 후 **시작하기**를 클릭합니다.

2. **vCenter 선택** 페이지의 **vCenters** 드롭다운 메뉴에서 특정 vCenter 또는 **등록된 모든 vCenter**를 선택한 후 **다음**을 클릭합니다.

이 노트: 같은 OMIVV 어플라이언스로 등록된 동일한 PSC에 속하는 vCenter 서버가 여러 개 있고 단일 vCenter 서버를 선택하여 구성하는 경우 각 vCenter를 구성할 때까지 2단계를 반복합니다.

3. **호스트 자격 증명 프로필 생성** 페이지에서 **호스트 자격 증명 프로필 생성**을 클릭합니다.

호스트 자격 증명 프로필 생성에 대한 자세한 내용은 [호스트 자격 증명 프로필 생성](#) 페이지 36을(를) 참조하십시오.

호스트 자격 증명 프로필에 호스트를 추가하면 OMIVV의 IP 주소가 호스트의 iDRAC에 대한 SNMP 트랩 대상으로 자동 설정됩니다. OMIVV가 ESXi 6.5 이상을 실행하는 호스트에서 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. 비준수 항목을 보고 해결하려면 사용자 가이드의 관리 규정 준수 섹션을 참조하십시오.

4. **추가 설정 구성** 페이지에서 다음을 수행합니다.

- a. 인벤토리 작업을 예약합니다. 인벤토리 작업 예약에 대한 자세한 내용은 [인벤토리 작업 예약](#) 페이지 37을(를) 참조하십시오.
- b. 보증 검색 작업을 예약합니다. 보증 검색 작업 예약에 대한 자세한 내용은 [보증 검색 작업 예약](#) 페이지 38을(를) 참조하십시오.
인벤토리 작업 일정을 수정하려면 **설정 > vCenter 설정 > 데이터 검색 일정 > 인벤토리 검색 또는 작업 > 인벤토리**로 이동합니다.
보증 검색 작업 예약을 수정하려면 **설정 > 보증 검색 > 작업 > 보증**으로 이동합니다.
- c. 이벤트 및 알람을 구성합니다. 이벤트 및 알람 구성에 대한 자세한 내용은 [이벤트 및 알람 구성](#) 페이지 38을(를) 참조하십시오.
- d. 개별 설정을 적용하려면 **적용** 버튼을 따로 클릭한 후 **다음**을 클릭합니다.
모든 추가 설정을 활성화하는 것이 좋습니다. 추가 설정 중 하나라도 적용되지 않으면 모든 추가 설정이 필수임을 나타내는 메시지가 표시됩니다.

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

- Dell EMC는 OMIVV 호스트를 사용하면 호스트 및 연결된 클러스터에서 발생하는 구성 변경 사항을 면밀히 모니터링할 수 있기 때문에 OMIVV 호스트를 구성 기준선과 연결하는 것을 권장합니다. OMIVV에서 호스트를 성공적으로 관리하면 모든 클러스터에 대해 구성 기준선을 생성할 수 있습니다. 구성 기준선을 만들려면 다음을 수행합니다.
- 펌웨어 및 드라이버용 리포지토리 프로필을 생성하면 기본 펌웨어 및 드라이버 버전을 정의할 수 있습니다.
 - 시스템 프로필을 생성하면 호스트의 기본 하드웨어 구성을 정의할 수 있습니다.
 - 클러스터 프로필 생성 - 기본값을 생성하려면 클러스터를 선택하여 펌웨어, 드라이버 및 하드웨어 구성에 연결하십시오.
 - iDRAC IPv4를 비활성화한 PowerEdge MX 새시에 있는 호스트는 새시 자격 증명 프로필을 사용하여 관리해야 합니다.

호스트 자격 증명 프로필 생성

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

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

- AD에 사용자 계정이 있습니다.
 - iDRAC 또는 호스트가 AD 기반 인증에 맞게 구성되었습니다.
1. OMIVV 홈 페이지에서 **준수 및 배포 > 호스트 자격 증명 프로필**을 클릭합니다.
 2. **호스트 자격 증명 프로필 생성** 페이지에서 **새 프로필 생성**을 클릭합니다.
 3. 마법사의 **호스트 자격 증명 프로필** 페이지에서 지침을 읽고 **시작하기**를 클릭합니다.
 4. **이름 및 자격 증명** 페이지에서 다음을 수행합니다.
 - a. 프로필 이름과 설명을 입력합니다. 설명 필드는 선택 사항입니다.
 - b. **vCenter 이름** 목록에서 호스트 자격 증명 프로필을 생성할 vCenter의 인스턴스를 선택합니다.

이 노트: 호스트 자격 증명 프로필을 생성하는 동안에 **모든 등록된 vCenter**를 선택하면 WBEM 서비스가 비활성화된 ESXi 6.5 이상을 실행하는 모든 호스트에 대한 연결 테스트가 실패합니다. 이러한 경우 호스트 자격 증명 프로필 마법사 작업을 완료하고 호스트에서 인벤토리를 실행한 후 호스트 자격 증명 프로필을 다시 테스트하는 것이 좋습니다.
 - c. **iDRAC 자격 증명** 영역에서 iDRAC 로컬 자격 증명 또는 AD 자격 증명을 입력합니다.
 - iDRAC의 로컬 자격 증명을 입력하려면 다음 작업을 수행합니다.
 - **사용자 이름** 상자에 사용자 이름을 입력합니다. 사용자 이름은 16자로 제한됩니다. 사용자 이름 정의에 대한 자세한 내용은 [dell.com/support](#)에서 *iDRAC 사용자 가이드*를 참조하십시오.
 - 암호를 입력합니다. 사용자 이름 및 비밀번호에 권장되는 문자에 대한 자세한 내용은 [dell.com/support](#)에 있는 *iDRAC 사용자 가이드*를 참조하십시오.
 - iDRAC 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화** 확인란을 선택합니다.
 - AD용으로 이미 구성 및 활성화된 iDRAC에 대한 자격 증명을 입력하려면 **Active Directory 사용** 확인란을 선택합니다.

이 노트: iDRAC 계정에 관리 권한이 있어야 펌웨어 업데이트, OS 배포를 수행할 수 있습니다.

 - **Active Directory 사용자 이름** 상자에 사용자 이름을 입력합니다. domain\username 또는 username@domain 형식 중 하나로 사용자 이름을 입력합니다. 사용자 이름은 256자로 제한됩니다. 사용자 이름 제한 사항에 대해서는 *Microsoft Active Directory 설명서*를 참조하십시오.
 - 암호를 입력합니다.
- iDRAC 및 호스트에 대한 AD 자격 증명은 동일하거나 별개일 수 있습니다.

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

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

- ESXi 호스트의 로컬 자격 증명을 입력하려면 다음 작업을 수행합니다.
 - 기본 사용자 이름은 **root**입니다. 편집할 수 없습니다.
 - 암호를 입력합니다.
 - 호스트 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화** 확인란을 선택합니다.
- AD용으로 이미 구성 및 활성화된 호스트에 대한 자격 증명을 입력하려면 **Active Directory 사용** 확인란을 선택합니다.
 - **Active Directory 사용자 이름** 상자에 사용자 이름을 입력합니다. domain\username 또는 username@domain 형식 중 하나로 사용자 이름을 입력합니다. 사용자 이름은 256자로 제한됩니다. 사용자 이름 제한 사항에 대해서는 *Microsoft Active Directory 설명서*를 참조하십시오.
 - 암호를 입력합니다.
 - 호스트 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화** 확인란을 선택합니다.

이 노트: ESXi 6.5 U2 이상 버전을 실행하는 호스트의 경우, 잘못된 호스트 자격 증명을 입력하더라도 OMIVV에서 iDRAC 정보를 얻을 수 있습니다.

5. 다음을 클릭합니다.

호스트 선택 페이지가 표시됩니다.

이 노트: 단일 호스트 자격 증명 프로필에서 모든 OMIVV 관리 호스트를 관리하려고 하면 vCenter에 Dell 인벤토리 알림을 표시하는 데 몇 분 정도 걸릴 수 있습니다. 이 지연 현상은 호스트 자격 증명 프로필에 많은 수의 호스트를 처음 추가할 때 나타날 수 있습니다. 후속 인벤토리가 정상적으로 실행됩니다.

6. **호스트 선택** 페이지에서 트리 보기를 확장하고 호스트를 선택한 다음 **확인**을 클릭합니다.

- **호스트 추가**를 클릭하여 **연결된 호스트** 페이지에서 호스트를 추가 또는 제거합니다.

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

선택한 호스트가 **연결된 호스트** 페이지에 표시됩니다.

7. 연결을 테스트하려면 하나 이상의 호스트를 선택하고 **테스트 시작**을 클릭합니다. 구성된 모든 호스트에 대해 연결을 테스트하는 것이 좋습니다.

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

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

테스트 결과 섹션에서 연결 테스트 결과를 볼 수 있습니다.

이 노트: ESXi 6.5 이상을 실행하는 모든 호스트에 대한 WBEM 서비스가 비활성화되어 있는 경우, 사용자가 이러한 호스트에 대해 연결 테스트를 수행하거나 인벤토리 실행 중에 WBEM이 자동으로 활성화됩니다.

이 노트: 잘못된 암호를 사용하여 호스트 자격 증명 프로필에서 iDRAC 연결을 테스트하면 iDRAC에서 구성된 페널티 시간이 될 때까지 어플라이언스에 대한 iDRAC 액세스가 잠깁니다. iDRAC의 IP 필터링 및 차단 설정에 지정된 페널티 시간 후에 올바른 암호로 다시 시도하십시오.

8. **마침**을 클릭합니다.

인벤토리 작업 예약

OMIVV에서 최신 인벤토리 데이터를 보려면 정기적으로 실행되도록 인벤토리 작업을 예약하여 호스트 또는 새시의 인벤토리 정보를 최신 상태로 유지해야 합니다. Dell EMC는 인벤토리 작업을 매주 실행할 것을 권장합니다.

이 노트: 새시는 OMIVV 컨텍스트로 관리됩니다. 새시 관리에는 vCenter의 컨텍스트가 없습니다. 예약된 호스트 인벤토리가 완료되면 OMIVV를 사용하여 관리되는 모든 새시에 대해 새시 인벤토리가 트리거됩니다.

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

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

vCenter 서버가 여러 개인 PSC 환경에서 개별 vCenter의 일정이 다르며 인벤토리 일정을 업데이트하기 위해 **모든 등록된 vCenter** 옵션을 선택하는 경우 인벤토리 일정 설정 페이지에 기본 일정이 표시됩니다.

3. 인벤토리 데이터 검색 날짜와 시간을 선택하고 **적용**을 클릭합니다.

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

보증 검색 작업 예약

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

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

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

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

1. OMIVV 홈페이지에서 **설정 > vCenter 설정 > 데이터 검색 일정 > 보증 검색**을 클릭합니다.

2. **보증 데이터 검색 활성화(권장)** 확인란을 선택합니다.

vCenter 서버가 여러 개인 PSC 환경에서 개별 vCenter의 일정이 다르며 보증 일정을 업데이트하기 위해 **모든 등록된 vCenter** 옵션을 선택하는 경우 보증 일정 설정 페이지에 기본 일정이 표시됩니다.

3. 보증 데이터 검색 날짜와 시간을 선택하고 **적용**을 클릭합니다.

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

이벤트 및 알람 구성

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

1. OMIVV 홈 페이지에서 **설정 > vCenter 설정 > 이벤트 및 알람**을 클릭합니다.

2. 모든 호스트 및 새시에 대한 알람을 활성화하려면 **모든 호스트 및 새시 알람 활성화**를 클릭합니다.

Dell EMC 알람 경고 활성화 페이지에는 Dell EMC 알람을 활성화한 후 영향을 받을 수 있는 클러스터와 클러스터링되지 않은 호스트가 표시됩니다.

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

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

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

3. 변경을 수락하려면 **계속**을 클릭합니다.
모든 호스트 및 새시에 대한 알람이 활성화됩니다.

4. 다음 이벤트 게시 수준 중 하나를 선택합니다.

- **이벤트 게시하지 않음** – 이벤트나 알람을 연결된 vCenter에 전달하지 않습니다.
- **모든 이벤트 게시** – 정보 제공 이벤트를 포함한 모든 이벤트와 관리되는 호스트 및 새시에서 수신되는 이벤트를 관련 vCenter에 게시합니다. Dell EMC는 모든 이벤트 게시 옵션을 이벤트 게시 수준으로 선택할 것을 권장합니다.
- **위험 및 경고 이벤트만 게시** – 위험 및 경고 수준 이벤트만 연결된 vCenter에 게시합니다.
- **가상화 관련 이벤트만 게시** – 호스트에서 수신한 가상화 관련 이벤트를 연결된 vCenter에 게시합니다. 가상화 관련 이벤트는 VM을 실행하는 호스트에 가장 중요한 이벤트입니다.

5. 변경 사항을 저장하려면 **적용**을 클릭합니다.

관리되는 모든 호스트 및 새시에서 기본 vCenter 알람 설정을 복원하려면 **알람 복원**을 클릭합니다. 변경이 적용되는 데 1분 정도 걸릴 수 있습니다.

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

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

설정 페이지에서 구성 작업

설정 페이지에서 다음 작업을 수행할 수 있습니다.

- 보증 만료 알람 구성
- 최신 어플라이언스 버전 알람 구성
- 배포 자격 증명 구성
- 상태 업데이트 알람의 심각도 재정의
- 초기 구성

보증 만료 알람 구성

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

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

최신 어플라이언스 버전 알람 구성

새 OMIVV 버전의 가용성에 대한 알람을 받으려면 **최신 버전 알람 활성화(권장)** 확인란을 선택합니다. Dell EMC는 매주 확인할 것을 권장합니다. OMIVV의 최신 어플라이언스 버전 알람 기능을 사용하려면 인터넷에 연결되어 있어야 합니다. 인터넷 연결에 프록시가 필요한 환경에서는 관리 포털에서 프록시 설정을 구성해야 합니다.

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

1. OMIVV 홈 페이지에서 **설정 > 어플라이언스 설정 > 알람 > 최신 버전 알람**을 클릭합니다.
2. **최신 버전 알람 활성화(권장)** 확인란을 선택합니다.
3. 최신 어플라이언스 버전 알람을 수신하려면 날짜 및 시간을 선택합니다.
4. **적용**을 클릭합니다.

배포 자격 증명 구성

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

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

1. OMIVV 홈페이지에서 **설정 > 어플라이언스 설정 > 배포 자격 증명**을 클릭합니다.
2. 사용자 이름 및 암호를 입력합니다. 기본 사용자 이름은 **root**이고 암호는 **calvin**입니다. iDRAC 지원 문자 및 iDRAC 로컬 자격 증명만 제공해야 합니다.
3. **적용**을 클릭합니다.

상태 업데이트 알림의 심각도 재정의

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

각 Proactive HA 이벤트에 해당하는 심각도 수준은 다음과 같습니다.

- 정보
- 보통으로 저하
- 심각하게 저하

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

1. OpenManage Integration for VMware vCenter에서 **설정 > 애플리케이션 설정 > Proactive HA의 심각도 재정의**를 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.
2. 호스트 또는 구성 요소의 심각도를 변경하려면 **심각도 재정의** 열의 드롭다운 목록에서 필요한 상태를 선택합니다. 이 정책은 OMIVV에 등록된 모든 vCenter 서버의 모든 Proactive HA 호스트에 적용됩니다.
3. 사용자 정의해야 하는 모든 이벤트에 대해 2단계를 반복합니다.
4. 다음 작업 중 하나를 수행합니다.
 - a. 사용자 지정 사항을 저장하려면 **적용**을 클릭합니다.
 - b. 심각도 설정 재정의의 취소를 클릭하려면 **취소**를 클릭합니다.심각도 설정 재정의의 기본값으로 재설정하려면 **기본값으로 재설정**을 클릭합니다.

Dell EMC 지원 사이트에서 문서 액세스

다음 링크 중 하나를 통해 필요한 문서에 액세스할 수 있습니다.

- Dell MEC 엔터프라이즈 시스템 관리 문서의 경우 — Dell.com/SoftwareSecurityManuals
- Dell EMC OpenManage 문서의 경우 — www.dell.com/OpenManageManuals
- Dell EMC 원격 엔터프라이즈 시스템 관리 문서의 경우 — www.dell.com/esmmanuals
- iDRAC 문서의 경우 www.dell.com/idracmanuals를 참조하십시오.
- Dell EMC OpenManage Connections Enterprise Systems 관리 문서의 경우 www.dell.com/OMConnectionsEnterpriseSystemsManagement를 참조하십시오.
- Dell EMC 서비스 가능 도구 문서의 경우 — www.dell.com/ServiceabilityTools
- 1. www.support.dell.com으로 이동합니다.
- 2. 모든 제품 찾아보기를 클릭합니다.
- 3. 모든 제품 페이지에서 소프트웨어를 클릭한 후 다음 중에서 필요한 링크를 클릭합니다.
 - 분석
 - 클라이언트 시스템 관리
 - 엔터프라이즈 애플리케이션
 - 엔터프라이즈 시스템 관리
 - 공공 부문 솔루션
 - 유틸리티
 - 메인프레임
 - 서비스 가능 도구
 - 가상화 솔루션
 - 운영 체제
 - 지원
- 4. 문서를 보려면 필요한 제품을 클릭한 다음 필요한 버전을 클릭합니다.
- 검색 엔진 사용:
 - 검색 상자에 문서 이름 및 버전을 입력합니다.

관련 설명서

본 가이드 더불어 다른 가이드를 www.dell.com/support/에서 확인할 수 있습니다. 모든 제품 찾아보기를 클릭한 다음 소프트웨어 > 가상화 솔루션을 클릭합니다. 다음 문서에 액세스하려면 **OpenManage Integration for VMware vCenter 5.0**을 클릭합니다.

- *OpenManage Integration for VMware vCenter 버전 5.0 사용자 가이드*
- *OpenManage Integration for VMware vCenter 버전 5.0 릴리즈 노트*
- *OpenManage Integration for VMware vCenter 버전 5.0 호환성 매트릭스*

<https://www.dell.com/support>에서 백서를 포함한 기술 아티팩트를 찾을 수 있습니다.