OpenManage Integration for VMware vCenter 버전 4.3

웹 클라이언트 설치 가이드

2018 년 10 월
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

이 안내서는 PowerEdge 서버와 함께 사용하기 위해 OpenManage Integration for VMware vCenter(OMIVV)를 설치 및 구성하는 방법에 대한 단계별 지침을 제공합니다. OMIVV 설치가 완료되면 `Dell.com/support/manuals`에서 *OpenManage Integration for VMware vCenter 사용 설명서*를 참조하여 인벤토리 관리, 모니터링 및 경고, 펌웨어 업데이트, 보증 관리를 비롯한 모든 측면의 관리에 대한 정보를 확인하십시오.

주제:

OpenManage Integration for VMware vCenter 라이센싱

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

- 평가판 라이센스 — OMIVV 어플라이언스의 전원을 처음 켜면, 평가판 라이센스가 자동으로 설치됩니다. 평가 버전에는 OpenManage Integration for VMware vCenter에서 관리되는 호스트(서버) 5개에 대한 평가판 라이센스가 포함되어 있습니다. 이 90일 평가 버전은 배송 시 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 **관리 콘솔**을 사용하여 새 라이센스 파일을 업로드합니다.

라이센싱은 다음 정보를 제공합니다.

- 최대 vCenter 연결 라이센스 수 - 등록되어 사용 중인 vCenter 연결은 최대 10개까지 활성화됩니다.
- 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(Dell Digital Locker)에서 .XML 파일(라이센스 키)을 다운로드할 수 있습니다. 라이센스 키가 다운로드되지 않는 경우 주문 지원에서 해당 제품의 지역 Dell 지원 부서 전화 번호를 찾아 Dell 지원 부서에 문의합니다.

호스트 및 vCenter 서버의 라이센스 요구 사항

호스트 및 vCenter에 대한 라이센스 요구 사항은 다음과 같습니다.

- OMIVV로 관리될 Dell EMC 서버의 수량을 지원할 라이센스를 구입할 수 있습니다. 라이센스는 호스트가 연결 프로필에 추가된 후에만 사용됩니다. 라이센스는 특정 서버와 관련이 없습니다.
- OMIVV 인스턴스 하나가 최대 10개의 vCenter 인스턴스를 지원합니다. vCenter 서버의 개수에 해당되는 별도의 라이센스는 없습니다.

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).

라이센스 업로드 후의 옵션

새로 구입한 제품의 라이센스 파일

새 라이센스를 주문할 때 Dell에서는 주문 확인서가 포함된 이메일을 보내 드리며 Dell Digital Locker의 Dell 디지털 로커에서 새 라이센스 파일을 다운로드할 수 있습니다. 라이센스는 .xml 형식이어야 합니다. 라이센스가 zip 형식으로 되어 있으면 zip 파일에서 라이센스 .xml 파일의 압축을 푼 후 업로드하십시오.

라이센스 스태킹

OMIVV 버전 2.1부터는 여러 개의 표준 라이센스를 스태킹하여, 업로드되는 라이센스의 호스트 총합으로 지원되는 호스트의 수를 늘릴 수 있습니다. 단, 평가판 라이센스는 스태킹할 수 없습니다. 스태킹을 통해서는 지원되는 vCenter의 수를 늘릴 수 없으며, 여러 어플라이언스를 사용할 필요가 있습니다.

라이센스를 스태킹하는 기능에는 몇 가지 제한 사항이 있습니다. 기존 표준 라이센스가 만료되기 전에 새 표준 라이센스가 업로드된 경우 라이센스가 스태킹됩니다. 그렇지 않은 경우, 라이센스가 만료되고 새 라이센스가 업로드된 경우 새 라이센스의 호스트 수만 지원됩니다. 여러 개의 라이센스를 이미 업로드한 경우 지원되는 호스트 수는 마지막 라이센스를 업로드한 시점에서 만료되지 않은 라이센스에 있는 호스트의 합계입니다.

만료된 라이센스

일반적으로 구매 날짜로부터 3년 또는 5년으로 정해지는 지원 기간을 경과한 라이센스는 업로드가 차단됩니다. 라이센스가 업로드된 후에 만료된 경우에는 기존 호스트에 대한 기능이 계속 유지되지만 OMIVV의 새 버전으로의 업그레이드가 차단됩니다.

라이센스 교체

주문에 문제가 있어 Dell에서 교체 라이센스를 받을 경우 이 교체 라이센스에는 이전 라이센스와 동일한 권리 ID가 포함됩니다. 교체 라이센스를 업로드하면 이미 동일한 권리 ID로 업로드된 기존 라이센스가 교체됩니다.

적용

어플라이언스 업데이트

모든 라이센스가 만료가 만료되면 어플라이언스가 새 버전으로의 업데이트를 허용하지 않습니다. 새 라이센스를 구입하고 업로드한 후에 어플라이언스 업그레이드를 시도하십시오.

평가판 라이센스

평가판 라이센스가 만료되면 여러 핵심 영역이 작동을 중단하고 오류 메시지가 표시됩니다.

연결 프로필에 호스트 추가

연결 프로필에 호스트를 추가하는 경우 11세대 이상의 라이센스 호스트 수가 라이센스 수를 초과하면 호스트를 더 추가할 수 없습니다.

참조를 위한 중요 참고

- OMIVV 4.0 이상부터 VMware vSphere 웹 클라이언트만 지원되며 vSphere Desktop 클라이언트는 지원되지 않습니다.
- vCenter 6.5 이상의 경우, OMIVV 어플라이언스는 플래시 버전에 대해서만 사용할 수 있습니다. OMIVV 어플라이언스는 HTML 5 버전에는 사용할 수 없습니다.
- DNS 서버를 사용하는 경우 권장 사례는 다음과 같습니다.
  - OMIVV는 IPV4 IP 주소만 지원합니다. 고정 IP 할당과 DHCP 할당이 모두 지원되지만 고정 IP 주소를 할당하는 것이 좋습니다. 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 5.5를 위한 DNS 요구 사항
  - vSphere 6.0을 위한 DNS 요구 사항
  - vSphere 6.5 및 Platform Services Controller 어플라이언스를 위한 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 14을(를) 참조하십시오.

하드웨어 요구 사항

OMIVV는 iDRAC Express 또는 Enterprise가 포함된 서버에 대한 전체 기능과 함께 여러 세대의 Dell EMC 서버 전체를 지원합니다. 플랫폼 요구 사항에 대한 종합적인 정보는 `Dell.com/support/manuals`의 *OpenManage Integration for VMware vCenter 릴리스 정보*에서 확인할 수 있습니다. 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)
- 11세대 이전 서버에 대한 OMSA 지원 및ESXi 버전 지원(배포 및 관리 모두 포함)
- 지원되는 메모리 및 OMIVV 공간

OMIVV를 사용하려면 iDRAC 및 CMC 또는 관리 모듈 시스템 관리 네트워크 및 vCenter 관리 네트워크에 모두 액세스할 수 있는 마더보드/네트워크 도터 카드에 LAN이 필요합니다.

배포 모드 구성

원하는 배포 모드에 대해 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	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.

BIOS, iDRAC, Lifecycle Controller 버전

이 섹션에는 OpenManage Integration for VMware vCenter의 기능을 활성화하는 데 필요한 BIOS, iDRAC, Lifecycle Controller 버전이 나열되어 있습니다.

OMIVV를 사용하려면 Repository Manager 또는 Lifecycle Controller의 플랫폼을 사용하여 생성된 부팅 가능 ISO를 사용하여 서버를 다음 기본 버전 중 하나로 업데이트하는 것이 좋습니다.

노트: OMIVV 4.3에서 Dell EMC OpenManage Enterprise-Modular Edition 버전 1.00.01을 사용하는 것이 좋습니다.

표 2. PowerEdge 11세대 서버용 BIOS

서버	최소 버전
PowerEdge R210	1.8.2 이상
PowerEdge R210II	1.3.1 이상
PowerEdge R310	1.8.2 이상
PowerEdge R410	1.9.0 이상
PowerEdge R415	1.8.6 이상
PowerEdge R510	1.9.0 이상

표 2. PowerEdge 11세대 서버용 BIOS

서버	최소 버전
PowerEdge R515	1.8.6 이상
PowerEdge R610	6.1.0 이상
PowerEdge R710	6.1.0 이상
PowerEdge R710	6.1.0 이상
PowerEdge R715	3.0.0 이상
PowerEdge R810	2.5.0 이상
PowerEdge R815	3.0.0 이상
PowerEdge R910	2.5.0 이상
PowerEdge M610	6.1.0 이상
PowerEdge M610x	6.1.0 이상
PowerEdge M710HD	5.0.1 이상
PowerEdge M910	2.5.0 이상
PowerEdge M915	2.6.0 이상
PowerEdge T110 II	1.8.2 이상
PowerEdge T310	1.8.2 이상
PowerEdge T410	1.9.0 이상
PowerEdge T610	6.1.0 이상
PowerEdge T710	6.1.0 이상

표 3. PowerEdge 12세대 서버용 BIOS

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 4. PowerEdge 13세대 서버용 BIOS

표 4. PowerEdge 13세대 서버용 BIOS

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

표 5. PowerEdge 14세대 서버용 BIOS

서버	최소 버전
R940	1.0.0 이상
R740	1.0.0 이상
R740xd	1.0.0 이상
R640	1.0.0 이상
M640	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
R7415	1.0.0 이상
MX740C	1.0.0 이상
MX840C	1.0.0 이상

표 6. 배포용 iDRAC 및 Lifecycle Controller

세대	버전	
	iDRAC	Lifecycle Controller

표 6. 배포용 iDRAC 및 Lifecycle Controller

세대	버전	
PowerEdge 11세대 서버	모듈식의 경우 3.35, 랙 또는 타워형의 경우 1.85	1.5.2 이상
PowerEdge 12세대 서버	2.30.30.30 이상	2.30.30.30 이상
PowerEdge 13세대 서버	2.30.30.30 이상	2.30.30.30 이상
PowerEdge 14세대 서버	3.00.00.00 이상	3.00.00.00 이상

표 7. 클라우드 서버의 BIOS 및 iDRAC 요구 사항

모델	BIOS	LifeCycle Controller가 포함된 iDRAC
C6320	1.0.2	2.30.30.30 이상
C4130	1.0.2	2.30.30.30 이상
C6420	1.0.0 이상	3.00.00.00 이상
C4140	1.0.0 이상	3.00.00.00 이상

PowerEdge 서버에서 지원되는 기능

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

표 8. PowerEdge 서버에서 지원되는 기능

기능	플랫폼		
	11세대	12세대 및 13세대	14세대
하드웨어 인벤토리	예	예	예
이벤트 및 알람	예(SNMP v1에만 해당)	예(SNMP v1 및 v2)	예(SNMP v1 및 v2)
구성 요소 전체에서 상태 모니터링*	예	예	예
BIOS/펌웨어 업데이트#	예	예	예
Proactive HA$	아니요	예	예
보증 정보	예	예	예
호스트 규정 준수	예	예	예
베어 메탈 서버 자동/수동 검색	예	예	예
베어 메탈 호환성	예	예	예
하드웨어 구성	예	예	예
베어 메탈 하이퍼바이저 배포	예	예	예
서버 LED 깜빡임	예	예	예
SEL 로그 보기/지우기	예	예	예
iDRAC 링크 및 실행	예	예	예
iDRAC 재설정	예	예	예
시스템 잠금 모드	아니요	아니요	예
시스템 프로필	아니요	아니요	예
클러스터 프로필	아니요	Y ^	예

표 8. PowerEdge 서버에서 지원되는 기능

기능	플랫폼		
	11세대	12세대 및 13세대	14세대
통합 섀시 IP를 사용하여 호스트 관리	아니요	아니요	Y@
OEM Server 지원	아니요	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.

^ 클러스터 프로필에서 구성 변경 사항은 지원되지 않습니다.

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

~ 13세대 서버에만 지원됩니다.

PowerEdge 섀시에서 지원되는 기능

이 주제에서는 PowerEdge 섀시에서 지원되는 기능에 대한 정보를 제공합니다.

표 9. 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
라이센스 정보	N/A(해당 없음)	예	예	예
보증 정보	예	예	예	예
상태 보고	예	예	예	예
멀티 섀시 관리 그룹 관계 정보	아니요	아니요	아니요	예

프로비저닝된 저장소에 필요한 공간

OMIVV 가상 어플라이언스에서는 프로비저닝 스토리지를 위해 최소 44GB의 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, 포트 액세스 및 수신 포트 요구 사항을 충족하는지 확인합니다.

VMware vSphere 웹 클라이언트 요구 사항

- vCenter 6.0 이상 지원
- vCenter의 웹 클라이언트 서비스 필요(vSphere Desktop 클라이언트는 지원되지 않음)

구체적인 소프트웨어 요구 사항은 Dell.com/support/manuals의 *OpenManage Integration for VMware vCenter Compatibility Matrix(OpenManage Integration for VMware vCenter 호환성 매트릭스)*에서도 찾을 수 있습니다.

OpenManage Integration for VMware vCenter 요구사항

관리되는 호스트에서 지원되는 ESXi 버전

다음 표는 관리되는 호스트에서 지원되는 ESXi 버전에 대한 정보를 제공합니다.

표 10. 지원되는 ESXi 버전

ESXi 버전 지원	서버 세대			
	11세대	12세대	13세대	14G
v5.1	예	예	아니요	아니요
v5.1 U1	예	예	아니요	아니요
v5.1 U2	예	예	예	아니요
v5.1 U3	예	예	예(M830, FC830, FC430 제외)	아니요
v5.5	예	예	아니요	아니요
v5.5 U1	예	예	아니요	아니요
v5.5 U2	예	예	예	아니요
v5.5 U3	예	예	예	아니요
v6.0	예	예	예	아니요
v6.0 U1	예	예	예	아니요
v6.0 U2	예	예	예	아니요
v6.0 U3	예	예	예	예
v6.5	아니요	예	예	아니요
v6.5 U1	아니요	예	예	예
v6.5 U2	아니요	예	예	예
v6.7	아니요	예	예	예
v6.7 U1	아니요	예	예	예

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

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

표 11. 지원되는 vCenter 서버 버전

vCenter 버전	웹 클라이언트 지원
v6.0 U2	예
v6.0 U3	예
v6.5	예
v6.5 U1	예
v6.5 U2	예
v6.7	예
v6.7 U1	예

노트: vCenter 서버 등록에 대한 자세한 내용은 `Dell.com/support/manuals`에서 *OpenManage Integration for VMware vCenter Version 4.3 Web Client Install Guide(OpenManage Integration for VMware vCenter 버전 4.3 웹 클라이언트 설치 가이드)*를 참조하십시오.

OpenManage Integration for VMware vCenter 버전 4.3은 VMware vRealize Operations Manager (vROPS) 버전 1.1 및 1.2를 지원합니다.

포트 정보

가상 어플라이언스 및 관리형 노드

OMIVV에서 **비준수 vSphere 호스트 해결** 마법사에서 제공되는 *비준수 호스트 수정* 링크를 사용하여 OMSA 에이전트를 배포하는 경우 OMIVV는 다음 작업을 수행합니다.

- HTTP 클라이언트 서비스 시작
- 포트 8080 활성화
- 포트를 ESXi 5.0 이상에 대해 사용할 수 있도록 지정하고 OMSA VIB를 다운로드하여 설치

OMSA VIB 설치가 완료된 후에는 서비스 자동으로 중지되고 포트가 닫힙니다.

표 12. 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.
69	TFTP	UDP	없음	출력	TFTP 서버에 대한 OMIVV 어플라이언스	TFTP 클라이언트	이전 펌웨어가 있는 11G 서버의 펌웨어 업데이트에 사용됩니다.
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 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 또는 관리 모듈 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.

표 12. 가상 어플라이언스

포트 번호	프로토콜	포트 유형	최대 암호화 수준	방향	대상	사용	설명
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, OMSA 및 CMC 또는 관리 모듈의 데이터는 관리된 노드를 관리하고 모니터링하기 위해 수신됩니다.
사용자 정의	모든	UDP/TCP	없음	출력	프록시 서버에 대한 OMIVV 어플라이언스	프록시	프록시 서버와 통신합니다.

표 13. 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	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	출력	OMIVV 어플라이언스에 대한 ESXi	HTTP 서버 - OMSA VIB를 다운로드하고 비준수 vSphere 호스트를 수정합니다.	ESXi에서 OMSA/ 드라이버 VIB를 다운로드하는 데 도움이 됩니다.

표 14. 관리된 노드(iDRAC, CMC 또는 관리 모듈)

포트 번호	프로토콜	포트 유형	최대 암호화 수준	방향	대상	사용	설명
443	WSMAN /HTTPS, REST/ HTTPS	TCP	128비트	입력	iDRAC, CMC 또는 관리 모듈에 대한 OMIVV 어플라이언스	iDRAC 통신	관리 스테이션에 정보를 제공하고 REST 또는 HTTPS 프로토콜을 사용하여 MX 섀시와 통신하는 데 사용됩니다. 이 포트는 iDRAC 및 CMC 또는 관리 모듈에서 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.

표 14. 관리된 노드(iDRAC, CMC 또는 관리 모듈)

포트 번호	프로토콜	포트 유형	최대 암호화 수준	방향	대상	사용	설명
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 전의 점검 사항:

- OMIVV에서 vCenter 서버에 액세스할 수 있는 사용자 이름 및 암호가 있는지 확인합니다. 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 권한을 참조하십시오.
- 호스트에 대한 관리자 권한이 있는 Active Directory 자격 증명 또는 ESXi 호스트 시스템에 대한 루트 암호가 있는지 확인합니다.
- iDRAC에 관리 권한이 있는 iDRAC Express 또는 Enterprise와 연결된 사용자 이름 및 암호가 있는지 여부를 확인합니다.
- vCenter 서버가 실행 중인지 확인합니다.
- OMIVV 설치 디렉터리의 위치를 확인합니다.
- VMware vSphere 환경이 가상 어플라이언스, 포트 액세스 및 수신 포트 요구 사항을 충족하는지 확인합니다. 또한 필요한 경우 클라이언트 시스템에 Adobe Flash Player를 설치합니다. 지원되는 Flash Player 버전에 대한 자세한 내용은 *OpenManage Integration for VMware vCenter Compatibility Matrix(OpenManage Integration for VMware vCenter 호환성 매트릭스)*를 참조하십시오.

노트: 가상 어플라이언스가 일반 가상 컴퓨터로 작동합니다. 한 번 중단 또는 종료되면 가상 어플라이언스의 전체 기능에 영향을 미칩니다.

노트: OMIVV는 ESXi 5.5 이상 버전에 배포되었을 시 VMware Tools를 실행 중(만료됨) 상태로 표시합니다. 필요할 경우 OMIVV 어플라이언스를 성공적으로 배포한 후 또는 이후 언제든지 VMware Tools를 업그레이드 할 수 있습니다.

노트: OMIVV 및 vCenter 서버가 동일한 네트워크 상에 있는 것이 좋습니다.

노트: OMIVV 어플라이언스 네트워크에서 iDRAC, 호스트 및 vCenter에 액세스할 수 있어야 합니다.

OMIVV 설치, 구성 및 업그레이드

하드웨어 요구 사항을 충족하며, 필수 VMware vCenter 소프트웨어를 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 Dell OpenManage Integration for VMware vCenter 다운로드 페이지 17 항목을 참조하십시오.
2. 파일을 다운로드한 위치로 이동하고 해당 콘텐츠를 추출합니다.
3. vSphere 웹 클라이언트를 사용하여 OMIVV 어플라이언스가 포함된 Open Virtualization Format(OVF) 파일을 배포합니다. OMIVV OVF 배포를 참조하십시오.
4. 라이센스 파일을 업로드합니다. 라이센스에 대한 자세한 내용은 라이센스 업로드를 참조하십시오.
5. Administration Console을 사용하여 OMIVV 어플라이언스를 vCenter 서버에 등록합니다. OMIVV 등록 및 라이센스 파일 가져오기를 참조하십시오.
6. 어플라이언스를 구성하려면 **초기 구성 마법사**를 완료합니다. 구성 마법사를 통한 구성 작업을 참조하십시오.

Dell 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/support로 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 관리**를 선택합니다.
   지원되는 OMIVV 버전이 표시됩니다.
7. **다운로드**를 클릭하거나 확인란을 선택하여 다운로드 목록에 소프트웨어를 추가합니다.

vSphere 웹 클라이언트를 사용하여 OMIVV OVF 배포

Dell 웹 사이트에서 제품 .zip 파일(*Dell_OpenManage_Integration_<버전 번호>.<빌드 번호>.zip*)을 다운로드하여 압축을 해제했는지 확인합니다.

1. 다운로드하여 압축을 푼 OMIVV 가상 디스크를 찾아 **Dell_OpenManage_Integration.exe**를 실행합니다.
   exe의 압축을 해제하고 실행할 수 있도록 지원되는 클라이언트 OS 버전은 Windows 7 SP1 이상입니다.

   exe의 압축을 해제하고 실행할 수 있도록 지원되는 서버 OS 버전은 Windows 2008 R2 이상입니다.

2. **EULA**에 동의하고 .OVF 파일을 저장합니다.
3. 어플라이언스를 업로드할 VMware vSphere 호스트에 액세스할 수 있는 위치로 .OVF 파일을 복사하거나 이동합니다.
4. **VMware vSphere 웹 클라이언트**를 시작합니다.
5. **VMware vSphere 웹 클라이언트**에서 호스트를 선택하고 기본 메뉴에서 **조치** > **OVF 템플릿 배포**를 클릭합니다.
   호스트를 마우스 오른쪽 단추로 클릭하고 **OVF 템플릿 배포**를 선택할 수도 있습니다.

   OVF 템플릿 배포 마법사가 표시됩니다.
6. **소스 선택** 창에서 다음 하위 작업을 수행합니다.
   a. 인터넷에서 OVF 패키지를 다운로드하려면 **URL**을 선택합니다.
   b. 로컬 시스템에서 OVF 패키지를 선택하려면 **로컬 파일**을 선택하고 **찾아보기**를 클릭합니다.

   노트: OVF 패키지가 네트워크 공유에 있는 경우 설치 프로세스는 10~30분 정도 소요될 수 있습니다. 빠른 설치를 위해 로컬 드라이브에 OVF를 호스트하는 것이 좋습니다.

7. **다음**을 클릭합니다.
   다음 정보가 포함된 **세부 정보 검토** 창이 표시됩니다.
   - **제품** - OVF 템플릿 이름이 표시됩니다
   - **버전** - OVF 템플릿의 버전이 표시됩니다.
   - **공급업체** - 공급업체 이름이 표시됩니다.
   - **발행자** - 발행자 세부 정보가 표시됩니다.
   - **다운로드 크기** - OVF 템플릿의 실제 크기(기가바이트 단위)가 표시됩니다.
   - **디스크 크기** - 씩 프로비저닝 및 씬 프로비저닝된 세부 정보가 표시됩니다.
   - **설명** - 설명이 여기에 표시됩니다.
8. **다음**을 클릭합니다.
   이름 및 폴더 선택 창이 표시됩니다.
9. **이름 및 폴더 선택** 창에서 다음 하위 단계를 수행합니다.
   a. **이름**에 템플릿의 이름을 입력합니다. 이름의 길이는 최대 80자입니다.
   b. **폴더 또는 데이터센터 선택** 목록에서 템플릿을 배포할 위치를 선택합니다.
10. **다음**을 클릭합니다.
    스토리지 선택 창이 표시됩니다.

11. **스토리지 선택** 창에서 다음 하위 작업을 수행합니다.
    a. **가상 디스크 형식 선택** 드롭다운 목록에서 다음 형식 중 하나를 선택합니다.
        - **씩 프로비저닝 레이지 제로**
        - **씩 프로비저닝 이거드 제로**
        - **씬 프로비저닝**

        씩 프로비전(이거드 제로)을 선택하는 것이 좋습니다.
    b. **VM 스토리지 정책** 드롭다운 목록에서 정책을 선택합니다.
12. **다음**을 클릭합니다.
    소스 및 대상 네트워크에 대한 세부 정보가 들어 있는 **네트워크 설정** 창이 표시됩니다.
13. **네트워크 설정** 창에서 **다음**을 클릭합니다.

    노트: OMIVV 어플라이언스와 vCenter 서버가 동일한 네트워크에 있는 것이 좋습니다.

14. **완료 준비** 창에서 OVF 배포 작업에 대해 선택한 옵션을 검토하고 **마침**을 클릭합니다.
    배포 작업이 실행되고 작업 진행 상태를 추적할 수 있는 완료 상태 창이 표시됩니다.

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.

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. 역할에 대해 필요한 권한을 모두 선택하려면 관리자가 아닌 사용자를 위해 필요한 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 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. 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 vCenter를 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 20을(를) 참조하십시오.

필수 권한이 있는 비 관리자 사용자에 의한 vCenter 서버 등록하기

필수 권한이 있는 비 관리자 사용자를 통해 OMIVV 어플라이언스를 위한 vCenter 서버를 등록 수 있습니다. 단계 5~9인 **OpenManage Integration for VMware vCenter 등록 및 라이센스 파일 가져오기** 항목을 참조하십시오. 은 관리자가 아닌 사용자 또는 관리자를 통한 vCenter 서버 등록에 대한 정보를 제공합니다.

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.

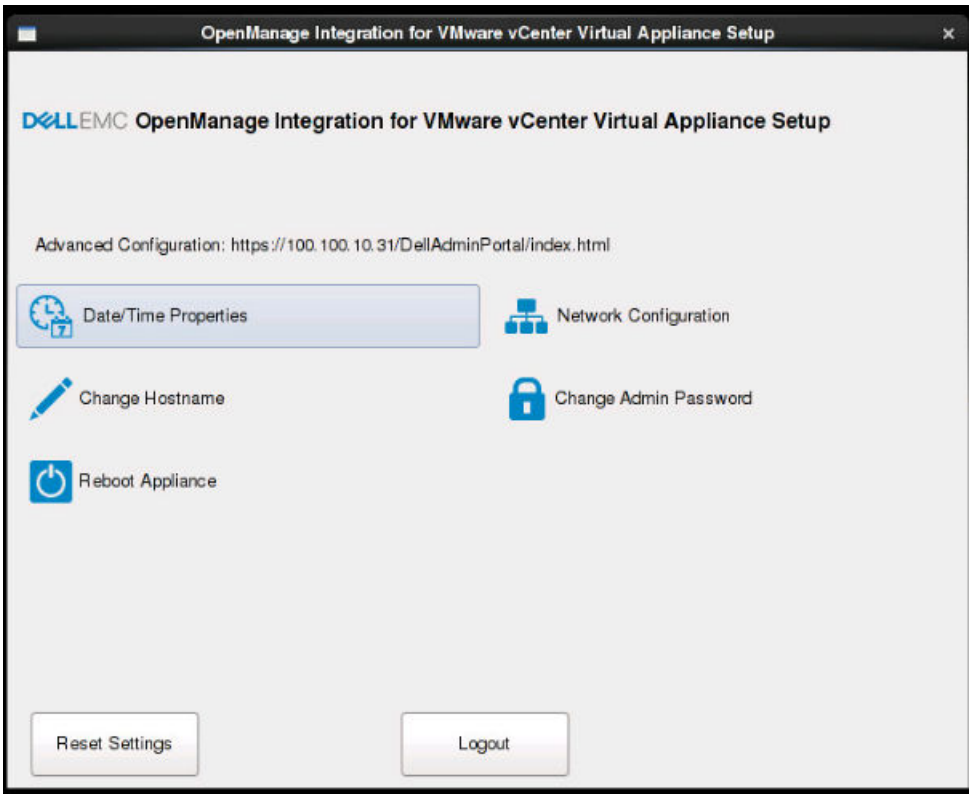
OpenManage Integration for VMware vCenter 등록 및 라이센스 파일 가져오기

Dell Digital Locker에서 라이센스를 다운로드할 준비가 되었는지 확인합니다. 라이센스를 두 개 이상 주문한 경우, 각자 다른 시간에 따로 제공될 수 있습니다. 주문 현황에서 다른 라이센스 항목의 상태를 확인할 수 있습니다. 라이센스 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 웹 클라이언트에 통신 오류가 표시됩니다. 이 문제를 해결하려면 vCenter에서 어플라이언스를 등록 취소한 후 다시 등록합니다.

1. vSphere 웹 클라이언트에서 **홈** > **호스트 및 클러스터**를 클릭하고 왼쪽 패널에서 방금 배포한 OMIVV를 찾아서 **가상 컴퓨터 전원 켜기**을 클릭합니다.
   배포 중에 **배포 후에 전원 켜기**를 선택한 경우 배포 완료 후에 VM 전원이 자동으로 켜집니다.
2. **관리 콘솔**을 실행하려면 기본 **VMware vCenter** 창에서 **콘솔** 탭을 클릭합니다.
3. OMIVV가 부팅을 완료할 때까지 기다린 후 사용자 이름으로 **기본값**을 입력하고 **Enter** 키를 누릅니다.
4. 새로운 관리자 암호를 입력합니다. 관리자 암호가 인터페이스에 표시되는 암호 복잡성 규칙에 부합하는지 확인합니다. **Enter** 키를 누릅니다.
5. 암호를 한 번 더 입력하고 **Enter** 키를 누릅니다.
   OMIVV 어플라이언스에서 네트워크 및 시간대 정보를 구성하려면 **Enter** 키를 누릅니다.
6. OMIVV 시간대 정보를 구성하려면 **날짜/시간 속성**을 클릭합니다.

그림 1. 콘솔 탭



7. **날짜 및 시간** 탭에서 **네트워크에서 날짜 및 시간 동기화**를 선택합니다.
   NTP 서버 상자가 표시됩니다.

8. vCenter가 동기화되는 유효한 NT 서버의 세부정보를 추가합니다.
9. **시간대**를 클릭하고 해당 시간대를 선택한 다음 **확인**을 클릭합니다.
10. OMIVV 어플라이언스에 정적 IP를 구성하려면 **네트워크 구성**을 클릭하거나 17단계로 건너뜁니다.
11. **자동 eth0**을 선택하고 **편집**을 클릭합니다.
12. **IPV4 설정** 탭을 선택하고 **방법** 드롭다운에서 **수동**을 선택합니다.
13. **Add**를 클릭한 후 유효한 IP, 넷마스크 및 게이트웨이 정보를 추가합니다.
14. **DNS 서버** 필드에서 DNS 서버 세부정보를 제공합니다.
15. **적용**을 클릭합니다.
16. OMIVV 어플라이언스의 호스트 이름을 변경하려면 **호스트 이름 변경**을 클릭합니다.
17. 유효한 호스트 이름을 입력하고 **호스트 이름 업데이트**를 클릭합니다.

    노트: 호스트 이름 및 NTP를 변경한 후에는 시스템을 재부팅해야 합니다.

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

    관리 콘솔을 열기 전에 먼저 iDRAC, DRM에서 프로비저닝 서버와 같은 어플라이언스에 대한 모든 참조를 수동으로 업데이트해야 합니다.

18. 지원되는 브라우저에서 **관리 콘솔**을 엽니다.

    관리 콘솔을 열려면 OpenManage Integration for VMware vCenter의 **도움말 및 지원** 탭에서 **관리 콘솔** 아래에 있는 링크를 클릭하거나 웹 브라우저를 시작하여 `https://<ApplianceIP 또는 Appliance hostname>` URL을 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.

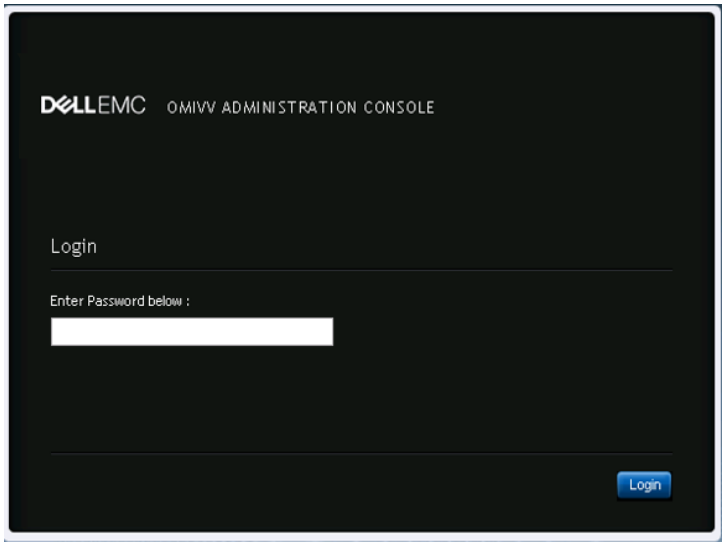


그림 2 . 관리 콘솔

19. **관리 콘솔** 로그인 창에서 암호를 입력하고 **로그인**을 클릭합니다.

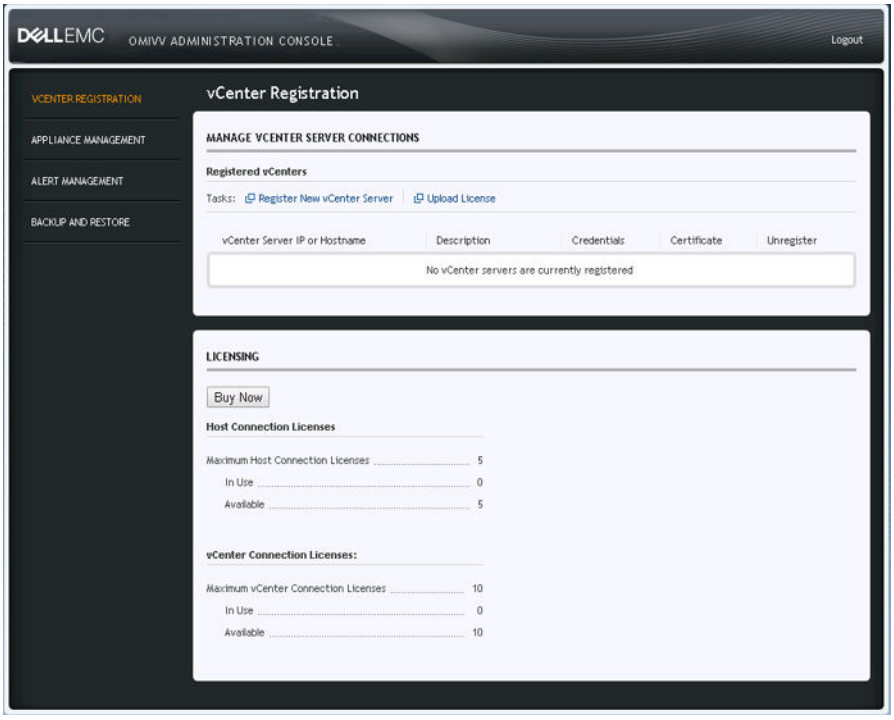


그림 3 . 관리 콘솔의 vCenter 등록 창

20. **vCenter 등록** 창에서 **새 vCenter 서버 등록**을 클릭합니다.
21. **새 vCenter 서버 등록** 창에서 다음 하위 작업을 수행합니다.
    a. **vCenter 이름** 아래의 **vCenter 서버 IP 또는 호스트 이름** 텍스트 상자에 서버 IP 또는 호스트 이름을 입력하고 **설명** 텍스트 상자에 설명을 입력합니다.
    설명은 선택 사항입니다.
    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 이름**에서 관리자 이름 또는 필요한 권한을 가진 사용자 이름을 입력합니다.
    `domain\user` 또는 `domain/user` 또는 `user@domain`으로 **username**을 입력합니다. OMIVV는 관리자 사용자 계정 또는 vCenter 관리에 필요한 권한을 지닌 사용자를 사용합니다.
    c. **암호**에 암호를 입력합니다.
    d. **암호 확인**에 암호를 다시 입력합니다.
22. **등록**을 클릭합니다.
    노트: OpenManage Integration for VMware vCenter는 현재 링크된 모드를 사용하여 단일 vCenter 인스턴스 또는 다중 vCenter 서버를 포함하는 대규모 배포 모드에서 최대 1,000개의 호스트를 지원합니다.
23. 다음 작업 중 하나를 수행합니다.
    - OMIVV 평가판 버전을 사용하는 경우 OMIVV 아이콘을 확인할 수 있습니다.
    - 정식 제품 버전을 사용하는 경우 Dell Digital Locker의 Dell 디지털 로커에서 라이센스 파일을 다운로드할 수 있으며, 이 라이센스를 가상 어플라이언스에 가져올 수 있습니다. 라이센스 파일을 가져오려면 **Upload License**를 클릭합니다.
24. **라이센스 업로드** 창에서 **찾아보기**를 클릭하여 라이센스 파일을 탐색한 후 **업로드**를 클릭하여 라이센스 파일을 가져옵니다.
    노트: 라이센스 파일을 수정하거나 편집하면 해당 라이센스 파일(.XML 파일)이 작동하지 않으며 Dell 디지털 로커에서 .XML 파일(라이센스 키)을 다운로드할 수 있습니다. 라이센스 키가 다운로드되지 않는 경우 기술 지원 팀에 연락에서 해당 제품의 지역 Dell 지원 부서 전화 번호를 찾아 Dell 지원 부서에 문의합니다.

OMIVV가 등록되면 OMIVV 아이콘이 웹 클라이언트 홈 페이지의 **Administration** 범주 아래에 표시됩니다.

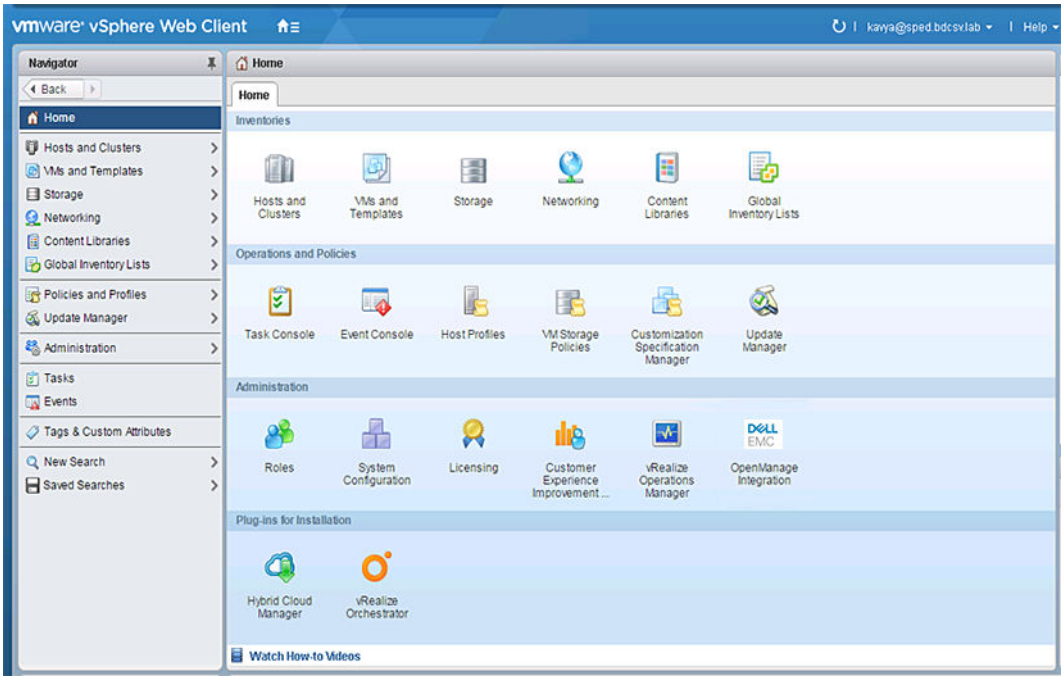


그림 4 . OpenManage Integration for VMware vCenter가 vCenter에 성공적으로 추가됨

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.

등록된 vCenter 업그레이드

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 19을 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 클라이언트 창을 닫고 새 VSphere 웹 클라이언트를 시작합니다.
2. OMIVV 아이콘이 vSphere 웹 클라이언트에 나타나는지 확인합니다.
3. vCenter 서버에서 가상 어플라이언스 IP 주소 또는 호스트 이름으로 ping 명령을 시도하여 vCenter가 OMIVV와 통신할 수 있는지 확인합니다.
4. vSphere 웹 클라이언트에서 **홈** > **관리** > **솔루션**을 클릭한 뒤 **플러그인 관리**(이전 vCenter 버전) 또는 **클라이언트 플러그인**(최신 버전)을 클릭합니다.

   플러그인 관리 또는 **클라이언트 플러그인** 페이지의 액세스 제한에 대한 자세한 내용은 VMware 설명서를 참조하십시오.
5. **플러그인 관리** 또는 **클라이언트 플러그인** 창에서 OMIVV가 설치 및 활성화되어 있는지 확인합니다.

가상 어플라이언스 리포지토리 위치 및 가상 어플라이언스 업데이트

모든 데이터를 보호하려면 가상 어플라이언스 업데이트 이전에 OMIVV 데이터베이스의 백업을 수행합니다. 사용자 가이드 에서 **백업 및 복원 관리** 항목을 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. *사용자 가이드* 에서 **HTTP 프록시 설정** 항목을 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. *사용자 가이드*의 **HTTP 프록시 설정** 항목을 참조하십시오.
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 https://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 상자의 https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/(으)로 업데이트하고 **적용**을 클릭합니다.
   - 인터넷에 연결되지 않은 경우 최신 다운로드 RPM 폴더 또는 파일을 사용하여 업그레이드하려면 https://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 18 및 HTTPS 인증서 업로드 페이지 18의 내용을 참조하십시오. 그렇지 않으면 이 단계를 건너뜁니다.
7. 데이터베이스를 새 OMIVV 어플라이언스에 복원합니다. *사용자 가이드의* **백업에서 OMIVV 데이터베이스 복원** 항목을 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 *사용자 가이드의* **비준수 vSphere 호스트 해결 마법사 실행** 항목 을 참조하십시오.

   노트: 이전 OMIVV 버전에서 이후 OMIVV 버전으로 백업 및 복구한 후 2 Million 오류가 발생하거나 Dell EMC 로고가 vCenter에 표시되지 않는 경우 다음을 수행하십시오.

   - vCenter 서버에서 vSphere 웹 클라이언트를 다시 시작합니다.
   - 문제가 지속되면, 다음과 같이 하십시오.
     - vCenter 서버 어플라이언스의 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 com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX와 같은 이전 데이터가 존재하는지 확인합니다.

- 이전 OMIVV 버전에 해당하는 폴더를 수동으로 지웁니다.

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.

노트: 플러그인을 등록 취소할 경우 등록된 알람에서 플러그인으로 적용된 모든 사용자 정의가 제거됩니다. 다음 단계를 통해 사용자 정의가 복원되지 않습니다. 그러나, 기본 상태로 알람이 다시 등록됩니다.

1. 백업 및 복원을 통해 어플라이언스 업데이트 페이지 26에서 3~5단계를 수행합니다.
2. 이전 플러그 인에서 앞서 등록했던 vCenter에 플러그 인을 등록합니다.
3. 마이그레이션을 완료하려면 백업 및 복원을 통해 어플라이언스 업데이트 페이지 26의 6~9단계를 수행합니다.

2

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.
- 섀시 프로필을 생성합니다. iDRAC IPv4를 비활성화한 MX 섀시에 있는 호스트는 섀시 프로필을 사용하여 관리해야 합니다. 섀시 프로필 생성 페이지 36을 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.

노트: 단일의 통합 섀시 관리 IP를 사용하여 MX 섀시를 관리할 수 있습니다. 섀시 프로필을 사용하여 MX 섀시를 관리하려면 섀시 프로필 생성을 참조하십시오. Dell EMC는 전체 OMIVV 기능을 사용할 경우 iDRAC IP를 사용하여 MX 섀시 호스트를 관리하는 것을 권장합니다.

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**에 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.

호스트 도메인 요구 사항:

- 1자에서 64자 사이.
- 첫 번째 문자는 반드시 알파벳이어야 합니다.
- 공백을 포함할 수 없습니다.

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.

노트: OEM 호스트가 호스트 선택 창에 표시되지 않는 경우 OEM 호스트 추가 마법사를 사용하여 OEM 호스트를 추가합니다. 자세한 내용은 *사용자 가이드*에서 **OEM 호스트 추가** 항목을 참조하십시오.

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 Dell EMC는 연결 프로필을 테스트하는 것을 권장합니다.

노트: ESXi 6.5 이상을 실행 중인 모든 호스트에 대해 WBEM 서비스를 비활성화한 경우 이러한 호스트에서 테스트 연결 및 인벤토리를 실행하면 WBEM이 자동으로 활성화됩니다.

노트: 연결 프로필을 생성하는 동안 **등록된 모든 vCenter**를 선택한 경우 WBEM 서비스가 비활성화된 ESXi 6.5 이상을 실행하는 모든 호스트에서 테스트 연결에 실패합니다. 이 경우 연결 프로필 마법사 조치를 완료하고 호스트에서 인벤토리를 실행한 뒤 연결 프로필을 다시 테스트하는 것이 좋습니다.

노트: 올바른 자격 증명을 입력한 이후에도 호스트에 대한 테스트 연결이 실패하고 잘못된 자격 증명을 입력했다는 메시지가 표시될 수 있습니다. 이 문제는 ESXi가 액세스를 차단하기 때문에 발생할 수 있습니다. 15분 정도 기다렸다가 테스트 연결을 다시 시도하십시오.

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 가이드의 **연결 프로필 수정하기**는 `Dell.com/support/manuals`의 *OpenManage Integration for VMware vCenter 사용자 가이드*에서 확인할 수 있습니다. .

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 이상을 실행 중인 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 `Dell.com/support/manuals`에서 *OpenManage Integration for VMware vCenter User's Guide(OpenManage Integration for VMware vCenter 사용 설명서)*의 **vSphere 호스트에 대한 준수 보고 및 해결**을 참조하십시오. .

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 `Dell.com/support/manuals`의 *OpenManage Integration for VMware vCenter User's Guide(OpenManage Integration for VMware vCenter 사용 설명서)*에서 **Modifying inventory job schedules(인벤토리 작업 일정 수정)**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 `Dell.com/support/manuals`의 *OpenManage Integration for VMware vCenter User's Guide(OpenManage Integration for VMware vCenter 사용 설명서)*에 있는 **Modifying warranty job schedules(보증 작업 일정 수정)**을 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.

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.

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.

노트: 이 리포지토리를 사용하는 비 vSAN 호스트 및 클러스터에 대해서만 펌웨어를 업데이트할 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 Online** - 펌웨어 업데이트 기본 리포지토리는 Dell Online(`https://downloads.dell.com`)으로 설정되어 있습니다. OMIVV는 선택된 펌웨어 업데이트를 Dell 리포지토리에서 다운로드하고 관리되는 호스트를 업데이트합니다.
   - **Dell Custom Online** - OMIVV는 선택한 펌웨어 업데이트를 Dell Custom Online에서 다운로드하고 필요에 따라 관리되는 호스트에 적용합니다.

     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.

   a. **Dell Custom Online**을 선택하는 경우에는 다음과 같은 형식으로 **온라인 카탈로그 경로**를 입력합니다.
      - `http://share/filename.xml.gz`
      - `http://share/filename.gz`
      - `https://share/filename.xml.gz`
      - `https://share/filename.gz`

   b. **공유 네트워크 폴더**를 선택하는 경우에는 다음과 같은 형식으로 여 **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. Dell EMC에서는 SMB 버전 2.0 기반의 CIFS 공유를 사용하는 것을 권장합니다.

노트: CIFS 공유를 사용하는 경우 OMIVV가 사용자 이름 및 암호를 입력하라는 메시지를 표시합니다.

c. 지정된 카탈로그 파일 위치의 유효성을 확인하려면 **테스트 시작**을 클릭합니다. 계속 진행하려면 이 유효성 검사가 필요합니다.

— 테스트 연결 성공을 나타냅니다.

— 테스트 연결 실패를 나타냅니다.

3. **적용**을 클릭합니다.

노트: 소스에서 카탈로그를 읽고 OMIVV 데이터베이스를 업데이트하려면 최대 10분이 소요될 수 있습니다.

OMIVV을 사용하여 DRM에서 카탈로그 생성

이 섹션에서는 DRM 버전 3.0 이상에서 카탈로그를 생성하는 과정을 설명합니다.

1. 홈 페이지에서 **새 리포지토리 추가**를 클릭합니다.
   리포지토리 추가 창이 표시됩니다.
2. **리포지토리 추가** 창에서 다음을 수행합니다.
   a. **리포지토리 이름**과 **설명**을 입력합니다.
   b. **기본 카탈로그** 드롭다운 메뉴에서 카탈로그를 선택합니다.
   c. **통합 유형** 드롭다운 메뉴에서 **OpenManage Integration for VMware vCenter**를 선택합니다.
3. **OpenManage Integration for VMware vCenter** 창에서 **가상 어플라이언스 IP**, **vCenter 서버 IP**, **사용자 이름**, 및 **암호**를 입력하고 **연결**을 클릭합니다.
   생성된 카탈로그가 홈 페이지에 표시됩니다.
4. 카탈로그를 내보내려면 카탈로그를 선택하고 **내보내기**를 클릭합니다.

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 *OpenManage Server Administrator Installation Guide(Dell OpenManage Server Administrator 설치 안내서)*를 참조하십시오.

노트: OMSA는 PowerEdge 11세대 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 **OMIVV 호스트 정보** 섹션 내에서 OMSA 콘솔 링크가 작동하는지 확인합니다.

이벤트 및 알람 구성

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 *OpenManage Integration for VMware vCenter*의 **이벤트, 알람 및 상태 모니터링** 섹션을 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 다음 단계를 수행하십시오.
   a. **인벤토리/보증 데이터**에서 **인벤토리/보증 데이터 검색 활성화** 확인란을 선택합니다.
   b. **인벤토리/보증 데이터 검색 일정**에서 작업 요일을 선택합니다.
   c. **인벤토리/보증 데이터 검색 시간** 텍스트 상자에 작업의 로컬 시간을 입력합니다.
      작업 구성 시간과 작업 구현 시간의 차이를 고려해야 합니다.
   d. 설정을 저장하려면 **적용**을 클릭하고 설정을 재설정하려면 **지우기**를 클릭합니다. 그리고 작업을 중단하려면 **취소**를 클릭합니다.
4. **데이터 검색 일정**을 다시 클릭하여 인벤토리 및 보증 일정을 축소하고 한 줄을 표시합니다.

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. **프로필**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. ✚을 클릭합니다. 섀시를 섀시 프로필과 연결합니다.

노트: **MX 섀시 추가**를 사용하여 검색되고, 사용 가능하며, 수동으로 추가되는 섀시는 섀시 아래에 있는 모듈식 호스트의 성공적인 인벤토리 실행 이후에만 섀시 프로필과 연결됩니다.

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. 연결 테스트는 필수 사항이며 선택한 섀시에 대해 자동으로 실행됩니다.

다음과 같은 경우 테스트 연결은 자동으로 실행됩니다.

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

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

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

노트: 추가된 MX 섀시에 연결되는 등록된 vCenters에 호스트가 없는 경우 해당 섀시 연결 테스트에 실패합니다.

노트: 성공적으로 유효성을 검사한 섀시만 섀시 프로필과 연결됩니다.

10. 프로필을 완료하려면 **마침**을 클릭합니다.

노트: 마법사를 완료하려면 하나 이상의 섀시가 성공적으로 검증되어야 합니다.

MX 섀시 관리 모듈 IP를 추가하려면 *사용자 가이드* 에서 **MX 섀시 IP 또는 FQDN 추가** 항목을 참조하십시오.

3

Dell EMC 지원 사이트에서 문서 액세스

다음 링크 중 하나를 통해 필요한 문서에 액세스할 수 있습니다.

- Dell EMC 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 및 Dell EMC Lifecycle Controller 문서의 경우 — www.dell.com/idracmanuals
- Dell EMC OpenManage Connections 엔터프라이즈 시스템 관리 문서의 경우 — www.dell.com/OMConnectionsEnterpriseSystemsManagement
- Dell EMC 서비스 가능 툴 문서의 경우 — www.dell.com/ServiceabilityTools
- 1. www.dell.com/Support/Home으로 이동합니다.
  2. **모든 제품 중에서 선택**을 클릭합니다.
  3. **모든 제품** 섹션에서 **소프트웨어 및 보안**을 클릭한 후 다음 중에서 필요한 링크를 클릭합니다.
     - **엔터프라이즈 시스템 관리**
     - **원격 엔터프라이즈 시스템 관리**
     - **서비스 가능 툴**
     - **Dell Client Command Suite**
     - **Connections 클라이언트 시스템 관리**
  4. 문서를 보려면 필요한 제품 버전을 클릭합니다.
- 검색 엔진 사용:
  - 검색 상자에 문서 이름 및 버전을 입력합니다.

4

관련 설명서

본 가이드 더불어 다른 가이드를 `Dell.com/support`에서 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 4.3**을 클릭합니다.

- *OpenManage Integration for VMware vCenter Version 4.3 Web Client User's Guide(OpenManage Integration for VMware vCenter Web Client 버전 4.3 사용자 가이드)*
- *OpenManage Integration for VMware vCenter Version 4.3 Release Notes(OpenManage Integration for VMware vCenter 버전 4.3 릴리스 정보)*
- *OpenManage Integration for VMware vCenter Version 4.3 Compatibility Matrix(OpenManage Integration for VMware vCenter 버전 4.3 호환성 매트릭스)*

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