Microsoft Endpoint Configuration Manager 및 System Center Virtual Machine Manager를 위한 Microsoft System Center용 OpenManage Integration 버전 7.3

통합 사용자 가이드

2021년 6월
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 OMIMSSC

이 문서는 OMIMSSC의 사용, 설치, 모범 사례와 관련된 모든 정보를 제공하는 통합 사용자 가이드입니다.

Microsoft System Center용 OpenManage Integration (OMIMSSC)는 Microsoft System Center 제품군과 통합된 어플라이언스로 제공됩니다. OMIMSSC LC(Lifecycle Controller)가 장착된 iDRAC(Integrated Dell Remote Access Controller)를 통해 Dell EMC PowerEdge 서버의 전체 수명주기를 관리할 수 있습니다.

OMIMSSC 운영 체제 배포, Microsoft Windows server용 Dell EMC HCI 솔루션, 하드웨어 패치, 펌웨어 업데이트, 서버 및 모듈형 시스템의 유지 보수를 제공합니다. OMIMSSC를 이전에 SCCM(System Center Configuration Manager)으로 알려진 Microsoft MECM(Microsoft Endpoint Configuration Manager)과 통합하여 기존 데이터 센터의 Dell PowerEdge 서버를 관리하거나 OMIMSSC를 Microsoft SCVMM(System Center Virtual Machine Manager)과 통합하여 가상 및 클라우드 환경에서 Dell PowerEdge 서버를 관리할 수 있습니다.

MECM, SCVMM 및 SCCM 브랜드 이름 변경에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

주제:

새로운 기능

- MECM(Microsoft Endpoint Configuration Manager) 버전 2103 지원
- MECM(Microsoft Endpoint Configuration Manager) 버전 2010 지원
- MECM(Microsoft Endpoint Configuration Manager) 버전 2006 지원
- SCVMM(System Center Virtual Machine Manager) 2019 UR3 지원
- SCVMM(System Center Virtual Machine Manager) 2019 UR2 지원
- SCVMM(System Center Virtual Machine Manager) 2016 UR10 지원
- 사용자 지정 SSL 인증서 관리 지원
- 이제 HCI 및 페일오버 클러스터용 클러스터 인식 업데이트에는 Windows Server 기반 클러스터용 BIOS 및 펌웨어와 함께 드라이버 업데이트를 수행할 수 있는 기능이 포함되어 있습니다.
- 새로운 인텔 기반 iDRAC 9 기반 PowerEdge 서버 지원
  - R750
  - R750xa
  - R650
  - C6520
  - MX750c
  - XE2420
- Windows Server 기반 HCI 클러스터 생성, AX 노드 및 S2D ready node의 관리 및 클러스터 인식 업데이트 지원
  - AX6515
  - AX740xd
  - AX640
  - R440
- Dell EMC OpenManage 서버 드라이버 팩을 사용한 WinPE 드라이버 삽입 지원

  노트: DTK는 Dell EMC의 EOL(End of Life) 제품입니다. WinPE 드라이버용 Dell EMC OpenManage 서버 드라이버 팩을 사용합니다.
- ESXi 운영 체제 배포 버전 7.0 U2, 7.0 U1 및 6.7 U3 지원
- RHEL 운영 체제 배포 버전 7.9, 8.0, 8.3 및 8.4 지원
- 재구성된 사용자 설명서 (설치 가이드, 사용자 가이드, 문제 해결 정보가 단일 통합 문서로 연결됨).
- .ova 파일을 사용하여 다음 VMware ESXi 버전에서 MECM(Microsoft Endpoint Configuration Manager) 및 SCVMM(System Center Virtual Machine Manager) 버전 7.3에 대한 OpenManage Integration용 Dell EMC OMIMSSC 어플라이언스 배포 지원
  - 버전 6.5
  - 버전 6.7
  - 버전 7.0

또한 .vhd 파일을 사용하여 Hyper-V에서 MECM 및 SCVMM에 대한 Dell EMC OMIMSSC 어플라이언스를 배포하는 기존 지원과 함께 제공됩니다.

2

OMIMSSC 라이선스

OMIMSSC OMIMSSC는 두 가지 유형의 라이선스를 제공합니다.

- 평가 라이선스 - 5개의 서버에 대한 평가 라이선스(호스트 또는 할당되지 않음)가 포함된 평가판 버전 라이선스로, 설치 후 자동으로 가져오기가 완료됩니다. 이는 11세대 이상의 Dell EMC 서버에만 적용됩니다.
- 운영 라이선스 - OMIMSSC에서 관리하는 서버 수에 관계없이 Dell EMC에서 운영 라이선스를 구입할 수 있습니다. 이 라이선스에는 제품 지원 및 OMIMSSC 어플라이언스 업데이트가 포함됩니다.

라이선스를 구입하면 Dell Digital Locker에서 .XML 파일(라이선스 키)을 다운로드할 수 있습니다. 라이선스 키가 다운로드되지 않는 경우 `dell.com/support/softwarecontacts`에서 해당 제품의 지역 Dell 지원 부서 전화번호를 찾아 Dell 지원 부서에 문의합니다.

OMIMSSC에서 단일 라이선스 파일을 사용하여 서버를 검색할 수 있습니다. OMIMSSC에서 서버가 검색되면 라이선스가 사용됩니다. 그리고 서버를 삭제하면 라이선스가 해제됩니다. OMIMSSC의 활동 로그에 다음과 같은 작업에 대한 항목이 생성됩니다.

- 라이선스 파일을 가져왔습니다.
- OMIMSSC에서 서버가 삭제되고 라이선스가 해제되었습니다.
- 서버를 검색한 후 라이선스가 사용됩니다.

평가판 라이선스에서 운영 라이선스로 업그레이드하면 평가판 라이선스가 운영 라이선스로 덮어쓰기 됩니다. **라이선스가 있는 노드** 수는 구입한 운영 라이선스 수와 동일합니다.

주제:

라이선스 기능에 대해 지원되는 옵션

라이선스 기능에 지원되는 옵션은 다음과 같습니다. OMIMSSC

새 라이선스 구매하기

새 라이선스를 주문할 때 Dell에서는 주문 확인서가 포함된 이메일을 보내드리며 Dell 디지털 스토어에서 새 라이선스 파일을 다운로드할 수 있습니다. 라이선스는 .xml 형식이어야 합니다. 라이선스가 zip 형식으로 되어 있으면 zip 파일에서 라이선스 .xml 파일의 압축을 푼 후 업로드하십시오.

여러 라이선스 스태킹하기

여러 개의 생산 라이선스를 스태킹하여 지원되는 서버 수를 늘리고 업로드된 라이선스의 서버 합계를 늘릴 수 있습니다. 단, 평가판 라이선스는 스태킹할 수 없습니다. 스태킹으로는 지원되는 서버의 수를 늘릴 수 없으며, 여러 OMIMSSC 어플라이언스를 사용해야 합니다.

여러 개의 라이선스를 이미 업로드한 경우 지원되는 서버 수는 마지막 라이선스를 업로드한 시점에서 라이선스에 있는 서버의 합계입니다.

라이선스 교체하기

주문에 문제가 있거나 수정되거나 손상된 파일을 업로드하려고 하면 동일한 오류 메시지가 표시됩니다. Dell Digital Locker에서 다른 라이선스 파일을 요청할 수 있습니다. 교체 라이선스를 받은 후에는 교체 라이선스에 이전 라이선스와 동일한 사용 권한 ID가 포함됩니다. 교체 라이선스를 업로드하면 이미 동일한 권리 ID로 업로드된 기존 라이선스가 교체됩니다.

라이선스 다시 가져오기

동일한 라이선스 파일을 가져오려고 하면 오류 메시지가 표시됩니다. 새 라이선스를 구입하고 새 라이선스 파일을 가져옵니다.

여러 라이선스 가져오기

OMIMSSC에서 검색하고 유지 관리할 수 있는 서버 수를 늘리기 위해 사용 권한 ID가 다른 여러 라이선스 파일을 가져올 수 있습니다.

라이선스 업그레이드하기

지원되는 모든 서버 세대에 대해 기존 라이선스 파일을 사용하여 OMIMSSC로 작업을 할 수 있습니다. 라이선스 파일이 최신 서버 세대를 지원하지 않는 경우 새 라이선스를 구매합니다.

평가판 라이선스

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

서버 검색 후 OMIMSSC에서 라이선스 사용하기

호스트를 추가하거나 베어 메탈 서버를 검색하려고 하면 사용 관련 경고가 표시됩니다. 다음과 같은 경우에는 새 라이선스를 구매하는 것이 좋습니다.

- 라이선스가 있는 서버 수가 구매한 라이선스 수를 초과하는 경우
- 구매한 라이선스 수와 동일한 서버를 발견한 경우
- 구매한 라이선스 수를 초과한 경우 유예 라이선스가 제공됨
- 구매한 라이선스 수와 모든 유예 라이선스 수를 초과한 경우

노트: 유예 라이선스는 구매한 총 라이선스 수의 20%에 해당 따라서 OMIMSSC에서 사용할 수 있는 실제 라이선스는 구매한 총 라이선스와 유예 라이선스입니다.

로 라이선스 가져오기 OMIMSSC

라이선스를 구매한 후 다음 단계를 수행하여 OMIMSSC로 가져옵니다.

1. OMIMSSC 관리 포털에서 **라이선스 센터**를 클릭합니다.
2. **라이선스 가져오기**를 클릭하고 Dell 디지털 스토어에서 다운로드한 라이선스 파일을 찾아 선택합니다.

   노트: 유효한 라이선스 파일만 가져올 수 있습니다. 파일이 손상되었거나 변조된 경우 그에 따른 오류 메시지가 표시됩니다. Dell 디지털 스토어에서 파일을 다시 다운로드하거나 Dell 담당자에게 문의하여 유효한 라이선스 파일을 받으십시오.

라이선스 센터 보기

1. 브라우저를 열고 OMIMSSC 어플라이언스 URL을 입력합니다.

   OMIMSSC 관리 포털 로그인 페이지가 표시됩니다.
2. **라이선스 센터**를 클릭합니다.

   페이지에는 다음 정보가 표시됩니다.

   라이선스 요약 - OMIMSSC에 대한 라이선스 세부 정보를 표시합니다.
   - **라이선스가 있는 노드** - 구입한 총 라이선스 수
   - **사용 중인 노드** - 라이선스를 소진했으며 검색되는 서버 수
   - **사용 가능한 노드** - OMIMSSC에서 검색할 수 있는 라이선스가 있는 나머지 노드

   라이선스 관리 - 권한 ID, 제품 설명, 라이선스 파일을 가져온 날짜, 라이선스 파일이 유효한 시작 날짜, 라이선스가 지원하는 모든 서버 세대 목록과 같은 세부 정보와 함께 가져온 각 라이선스 파일을 표시합니다.

3

OMIMSSC 구성 요소

다음은 OMIMSSC 구성 요소의 목록과 이 가이드에서 사용된 구성 요소의 이름입니다.

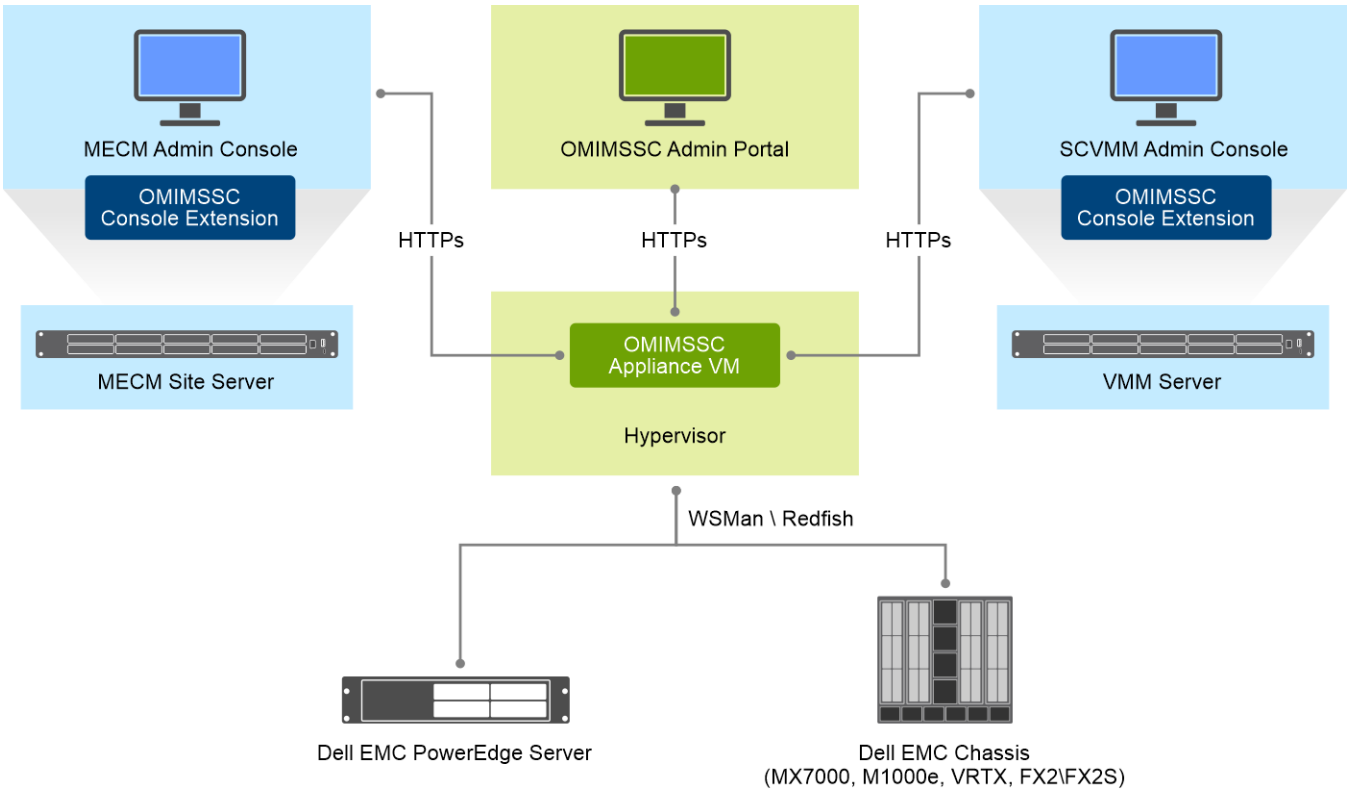
표 1. 구성 요소 OMIMSSC

구성 요소	설명
Microsoft System Center용 OpenManage Integration 어플라이언스 가상 머신(OMIMSSC 어플라이언스라고도 함).	CentOS 기반의 가상 머신으로 Hyper-V에서 OMIMSSC 어플라이언스를 호스팅하고 다음 작업을 수행합니다. • WSMan(Web Services Management) 명령을 사용해 iDRAC를 통하여 Dell EMC 서버와 상호 작용합니다. • REST API 명령을 사용하여 OME-Modular(OpenManage Enterprise Modular)를 통해 Dell EMC PowerEdge MX7000 디바이스와 상호 작용합니다.
관리 포털	관리 포털을 이용하여 관리하는 작업은 다음과 같습니다. • 라이선스 관리 • OMIMSSC에 시스템 센터 등록 • 어플라이언스 관리 • 어플라이언스 업그레이드 및 백업 • 어플라이언스 로그 다운로드
Microsoft System Center용 OpenManage Integration 콘솔은 OMIMSSC 콘솔이라고도 합니다.	MECM 및 SCVMM 콘솔에도 동일한 콘솔 확장 프로그램이 사용되며, 이를 다음과 같이 지칭하기도 합니다. • OMIMSSC MECM용 콘솔 확장 프로그램 • OMIMSSC SCVMM용 콘솔 확장 프로그램

관리 시스템은 OMIMSSC 및 해당 구성 요소가 설치되는 시스템입니다.

관리형 시스템은 OMIMSSC에서 관리하는 서버입니다.

OMIMSSC 아키텍처



4

Support Matrix OMIMSSC

주제:

지원되는 시스템 센터 버전

OMIMSSC에 사용할 수 있는 모든 MECM 및 SCVMM 버전은 다음과 같습니다.

OMIMSSC **지원되는 시스템 센터**

- Microsoft SCCM(System Center Configuration Manager) 2012 R2
- Microsoft SCCM(System Center Configuration Manager) 2012 R2 SP1
- Microsoft SCCM(System Center Configuration Manager) 버전 1809
- Microsoft SCCM(System Center Configuration Manager) 버전 1810
- Microsoft SCCM(System Center Configuration Manager) 버전 1902
- Microsoft SCCM(System Center Configuration Manager) 버전 1906
- MECM(Microsoft Endpoint Configuration Manager) 버전 1910
- MECM(Microsoft Endpoint Configuration Manager) 버전 2002
- MECM(Microsoft Endpoint Configuration Manager) 버전 2103
- MECM(Microsoft Endpoint Configuration Manager) 버전 2010
- MECM(Microsoft Endpoint Configuration Manager) 버전 2006
- Microsoft SCVMM(System Center Virtual Machine Manager) 2012 R2
- Microsoft SCVMM(System Center Virtual Machine Manager) 2016
- Microsoft SCVMM(System Center Virtual Machine Manager) 2016 UR8
- Microsoft SCVMM(System Center Virtual Machine Manager) 2016 UR9
- Microsoft SCVMM(System Center Virtual Machine Manager) 2016 UR3
- Microsoft SCVMM(System Center Virtual Machine Manager) 2019
- Microsoft SCVMM(System Center Virtual Machine Manager) 2019 UR1
- Microsoft SCVMM(System Center Virtual Machine Manager) 2019 UR2
- Microsoft SCVMM(System Center Virtual Machine Manager) 2019 UR10

표 2. 지원되는 디바이스

Dell EMC 시스템	지원되는 버전
iDRAC9 기반 PowerEdge 서버	• 지원 플랫폼용 OS 드라이버 팩: ○ R750, R750xa 및 R650 - 21.03.10 이상 ○ XE2420 - 20.11.04 ○ R6515, R7515, C6525, R6525 - 19.12.08 ○ R7525 - 19.12.07 ○ C6520 - 21.03.10 이상 ○ MX750c - 21.03.10 이상 • AMD 지원 플랫폼용 Lifecycle Controller 버전 및 Integrated Dell EMC Remote Access Controller 버전: ○ R750, R750xa 및 R650 - 4.40.20.00 이상 ○ XE2420 - 4.40.10.00

표 2. 지원되는 디바이스 (계속)

Dell EMC 시스템	지원되는 버전
	○ C6520 - 4.40.20.0 이상 ○ MX750c - 4.40.20.0 이상 ● Dell EMC OpenManage Server 드라이버 팩 버전 10.0.1 ● **MECM** ○ R6515 및 R7515 - 3.40.40.40 이상 ○ C6525 및 R6525 - 3.42.42.42 이상 ○ R7525 - 4.10.10.10 이상 ● **SCVMM** ○ R6515, R7515, C6525, R6525, R7525 - 4.30.30.30 이상 **노트:** vFlash \ stage에서 vFlash 방식으로 부팅하는 운영 체제 배포 및 서버 프로파일 백업 기능은 지원되지 않습니다.
PowerEdge 서버 14세대	● OS 드라이버 팩: 17.05.21 ● Lifecycle Controller 버전 및 Integration Dell EMC Remote Access Controller 버전 - 3.00.00.00 이상 ● Dell EMC OpenManage Server 드라이버 팩 버전 10.0.1
PowerEdge 서버 13세대	● OS 드라이버 팩: 16.08.13 ● Lifecycle Controller 버전 - 2.40.40.40 이상 ● Integration Dell Remote Access Controller 버전 - 2.40.40.40 이상 ● Dell EMC OpenManage Server 드라이버 팩 버전 10.0.1
PowerEdge 서버 12세대	● OS 드라이버 팩: R220 및 FM120 서버용 - 16.08.13 ● 기타 지원 플랫폼 OS 드라이버 팩: 15.07.07 ● Lifecycle Controller 버전 2.40.40.40 이상 ● Integration Dell Remote Access Controller 버전 2.40.40.40 이상 ● Dell EMC OpenManage Server 드라이버 팩 버전 10.0.1
CMC(Chassis Management Console)	● FX2 1.4 이상 ● M1000e 5.2 이상 ● VRTX 2.2 이상
Dell EMC OpenManage Enterprise-Modular	● PowerEdge MX7000 섀시 1.0
Microsoft Windows Server용 Dell EMC HCI 솔루션의 타겟 노드로 지원되는 AX 및/또는 Storage Spaces Direct Ready Node(Windows Server 운영 체제 사용)	AX 노드: AX-640, AX-740xd 및 AX-6515 Storage Spaces Direct Ready Nodes: R440, R640, R740xd 및 R740xd2

노트: PowerEdge 서버 11세대에 대한 지원은 OMIMSSC 버전 7.2.1 릴리스 이후부터 중단됩니다.

표 3. 지원되는 운영 체제(배포):

운영 체제	지원되는 버전
Microsoft Windows	● Windows Server 2019 ● Windows Server 2016 ● Windows Server 2012 R2
비 Windows 운영 체제	● RHEL 8.0, 8.3, 8.4 ● RHEL 7.2, 7.3, 7.4, 7.5 ● RHEL 6.9
VMWare ESXi	● ESXi 7.0 U2 - A00 ● ESXi 7.0 U1 - A05 ● ESXI 6.7 U3 - A10 ● ESXi 6.7 - A06 ● ESXi 6.5 U3

표 3. 지원되는 운영 체제(배포): (계속)

운영 체제	지원되는 버전
	• ESXi 6.5 U1 - A11 • ESXi 6.5 - A03 • ESXi 6.0 U3 - A15 • ESXi 6.0 - A02 **노트:** https://www.dell.com/support/에서 이미지를 다운로드하여, OMIMSSC 지원 버전에 따라 특정 서버 모델의 드라이버 및 다운로드 페이지를 참조하십시오.

OMIMSSC 지원되는 클러스터

- SCVMM 콘솔에서 Windows 2016 및 2019 Windows 서버 HCI 지원 클러스터 생성 및 관리
- SCVMM 콘솔에서 Windows 2012 R2, 2016, 2019 Hyper-V 호스트 클러스터 관리

네트워크 요구 사항

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

표 4. 가상 어플라이언스

포트 번호	프로토콜	포트 유형	최대 암호화 수준	방향	대상	사용	설명
53	DNS	TCP	없음	출력	DNS 서버에 대한 OMIMSSC 어플라이언스	DNS 클라이언트	DNS 서버에 대한 연결 또는 호스트 이름 확인으로 사용
68	DHCP	UDP	없음	입력	OMIMSSC 어플라이언스에 대한 DHCP 서버	동적 네트워크 구성	IP, 게이트웨이, 넷마스크 및 DNS와 같은 네트워크 세부 정보를 가져옵니다.
69	TFTP	UDP	128비트	출력	iDRAC에 대한 OMIMSSC	간이 파일 전송	베어 메탈 서버는 지원되는 최소 펌웨어 버전으로 업데이트하는 데 사용됩니다.
123	NTP	UDP	없음	입력	OMIMSSC 어플라이언스에 대한 NTP	시간 동기화	특정 시간대와 동기화합니다.
80/443	HTTP/HTTPS	TCP	없음	출력	인터넷에 대한 OMIMSSC 어플라이언스	Dell 온라인 데이터 액세스	온라인(인터넷) 보증, 펌웨어 및 최신 RPM 정보에 연결하는 데 사용됩니다.
443	HTTPS	TCP	128비트	입력	OMIMSSC 어플라이언스에 대한 OMIMSSC UI	HTTPS 서버	OMIMSSC에서 제공하는 웹 서비스입니다. 이러한 웹 서비스는 vSphere Client 및 Dell 관리 포털에서 사용합니다.
443	HTTPS	TCP	128비트	입력	OMIMSSC 어플라이언스에 대한 ESXi 서버	HTTPS 서버	OMIMSSC 어플라이언스와 통신하기 위한 사후 설치 스크립트용 운영 체제 구축 흐름에 사용됩니다.
443	HTTPS	TCP	128비트	입력	OMIMSSC 어플라이언스에 대한 iDRAC	자동 검색	관리된 노드 자동 검색에 사용되는 프로비저닝 서버입니다.
443	WSMAN	TCP	128비트	입력/출력	iDRAC에 대한/부터의 OMIMSSC 어플라이언스	iDRAC 통신	관리되는 노드를 관리하고 모니터링하는 데 사용되는 iDRAC, CMC 또는 OME-Modular 통신입니다.

표 4. 가상 어플라이언스 (계속)

포트 번호	프로토콜	포트 유형	최대 암호화 수준	방향	대상	사용	설명
111	HTTPS	TCP	없음	입력	OMIMSSC 어플라이언스에 대한 iDRAC	원격 프로시저 호출	RPC 함수의 주소를 확인하는 데 사용됩니다.
4433	HTTPS	TCP	없음	입력	OMIMSSC 어플라이언스에 대한 iDRAC	자동 검색	자동 검색에 사용됩니다.
445/139	SMB	TCP	128비트	출력	CIFS에 대한 OMIMSSC 어플라이언스	CIFS 통신	Windows 공유와 통신합니다.
2049	NFS	UDP/TCP	없음	입력/출력	NFS에 대한 OMIMSSC 어플라이언스	공개 공유	NFS 공개 공유는 OMIMSSC 어플라이언스에 의해 관리된 노드에 노출되었으며 펌웨어 업데이트 및 운영 체제 구축 흐름에 사용됩니다.
4001~4004	NFS	UDP/TCP	없음	입력/출력	NFS에 대한 OMIMSSC 어플라이언스	공개 공유	NFS 서버의 V2 및 V3 프로토콜에서 statd, quotd, lockd 및 mountd 서비스를 실행하려면 이러한 포트를 열린 상태로 유지해야 합니다.
사용자 정의	모든	UDP/TCP	없음	출력	프록시 서버에 대한 OMIMSSC 어플라이언스	프록시	프록시 서버와 통신합니다.

표 5. 관리된 노드(ESXi)

포트 번호	프로토콜	포트 유형	최대 암호화 수준	방향	대상	사용	설명
443	WSMAN	TCP	128비트	입력	ESXi에 대한 OMIMSSC 어플라이언스	iDRAC 통신	관리 스테이션에 정보를 제공하는 데 사용됩니다. 이 포트는 ESXi에서 열어야 합니다.
443	HTTPS	TCP	128비트	입력	ESXi에 대한 OMIMSSC 어플라이언스	HTTPS 서버	관리 스테이션에 정보를 제공하는 데 사용됩니다. 이 포트는 ESXi에서 열어야 합니다.

iDRAC 및 CMC 포트 정보에 대한 자세한 내용은 **https://www.dell.com/support**에서 제공되는 *Integrated Dell Remote Access Controller 사용자 가이드* 및 *Dell Chassis Management Controller 사용자 가이드*를 참조하십시오.

OME-Modular 포트 정보에 대한 자세한 내용은 **https://www.dell.com/support**에서 제공되는 *Dell EMC OME-Modular 사용자 가이드*를 참조하십시오.

Infrastructure administration using Microsoft System Center Console

Microsoft System Center user account privileges

All the required account privileges to use OMIMSSC are as follows:

User must be member of the following groups in System Center Consoles for Account privileges to use OMIMSSC console extension.

Table 6. User accounts with required privileges

Users	Privileges/Roles
For enrollment	• Account used to enroll the MECM console with OMIMSSC should be a full admin or an administrator in MECM. • Account used to enroll the SCVMM console with OMIMSSC should be a member of administrator role in SCVMM. • Domain user. • Member of Local Administrator group in system center machine.
For logging in to console extensions	• Account used to enroll the MECM console with OMIMSSC should be a full admin or an administrator in MECM. • Account used to enroll the SCVMM console with OMIMSSC should be a delegated admin or an administrator in SCVMM. • Domain user. • Member of Local Administrator group in system center machine.

에 대한 시스템 요구 사항 OMIMSSC

OMIMSSC를 설치하기 전에 나열된 세 가지 OMIMSSC 구성 요소를 기준으로 다음 소프트웨어 사전 요구 사항을 완료해야 합니다.

- OMIMSSC 어플라이언스:
  - Windows Server를 설치하고 Hyper-V 역할을 활성화합니다.
  - OMIMSSC는 멀티 콘솔 등록을 지원하므로 원하는 수의 MECM 또는 SCVMM 콘솔을 하나의 OMIMSSC 어플라이언스와 함께 등록할 수 있습니다. 등록할 콘솔 수에 따른 하드웨어 요구 사항은 다음과 같습니다.

표 7. 하드웨어 요구 사항

구성 요소	MECM 또는 SCVMM 콘솔 1개용	MECM 또는 SCVMM 콘솔 N개용
RAM	8GB	8GB*N
프로세서 개수	4	4*N

- 다음 Windows 운영 체제 버전 중 하나를 설치합니다.
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
- 다음 버전의 ESXi 중 하나 설치:
  - 버전 6.5
  - 버전 6.7
  - 버전 7.0
- OMIMSSC 지원 포털: 지원되는 다음 브라우저 중 하나를 설치해야 합니다.
  - Internet Explorer 10 이상
  - Mozilla Firefox 30 이상
  - Google Chrome 23 이상
  - Microsoft Edge

SCVMM용 OMIMSSC 콘솔 확장 프로그램의 시스템 요구 사항

SCVMM용 OMIMSSC 콘솔 확장 프로그램을 설치하려면 다음을 수행합니다.

- 동일한 버전의 SCVMM 관리 콘솔 및 SCVMM 서버를 설치합니다.
- 페일오버 클러스터링 기능은 SCVMM 서버에서 활성화됩니다.
- 등록된 사용자는 SCVMM 서버에 대한 관리 권한이 있어야 합니다.

- 등록된 사용자는 관리되는 클러스터에 대한 관리 권한이 있어야 합니다.

5

배포 OMIMSSC

주제:

웹에서 OMIMSSC 다운로드

OMIMSSC를 다운로드하려면 https://www.dell.com/support에서 다음을 수행합니다.

1. **모든 제품 탐색** > **소프트웨어** > **엔터프라이즈 시스템 관리** > **Microsoft 시스템용 OpenManage Integration**을 클릭합니다.
2. 필수 OMIMSSC 버전을 선택합니다.
3. **드라이버 및 다운로드** 탭을 클릭합니다.
4. OMIMSSC vhd 파일을 다운로드합니다.
5. vhd 파일의 압축을 푼 다음 OMIMSSC 어플라이언스를 설정합니다.
   vhd 파일 크기는 약 5GB이므로 배포를 완료하는 데 5~10분 정도 소요됩니다.
6. 파일의 압축을 풀 위치를 지정하고 압축 해제 버튼을 클릭하여 파일의 압축을 풉니다.
   - **OMIMSSC_<file version>_for_VMM_and_ConfigMgr**

Hyper-V에서 OMIMSSC 어플라이언스 설정

OMIMSSC 어플라이언스를 설정하는 Hyper-V에서 다음 요구 사항이 충족되었는지 확인합니다.

- 가상 스위치가 구성되었으며 사용할 수 있습니다.
- 등록할 Microsoft 콘솔 수를 기준으로 OMIMSSC 어플라이언스 VM에 메모리를 할당합니다. 자세한 내용은 공통 요구 사항을 참조하십시오.

OMIMSSC 어플라이언스를 설정하려면 다음을 수행합니다.

1. 다음 단계를 수행하여 OMIMSSC 어플라이언스 VM을 배포합니다.
   a. **Windows Server**, **Hyper-V Manager**의 **작업** 메뉴에서 **새로 만들기**를 선택하고 **Virtual Machine Manager**를 클릭합니다.
   새 가상 머신 마법사가 표시됩니다.
   b. **시작하기 전에**에서, **다음**을 클릭합니다.
   c. **이름 및 위치 지정**에 가상 머신의 이름을 입력합니다.
   VM을 다른 위치에 저장하려는 경우 **다른 위치에 가상 머신 저장**을 선택하고 **탐색**을 클릭하여 새 위치로 이동합니다.
   d. **세대 지정**에서 **1세대**를 선택하고 **다음**을 클릭합니다.
   e. **메모리 할당**에 사전 요구 사항의 메모리 용량을 할당합니다.
   f. **네트워킹 구성**의 **연결**에서 사용하고자 하는 네트워크를 선택한 후 **다음**을 클릭합니다.
   g. **가상 하드 디스크 연결**에서 **기존 가상 하드 디스크 사용**을 선택하고 **OMIMSSC_<file version>_for_VMM_and_ConfigMgr** VHD 파일이 있는 위치로 이동하여 파일을 선택합니다.
   vhd 파일 크기는 약 5GB이므로 배포를 완료하는 데 5~10분 정도 소요됩니다.
   h. **요약**에서 입력한 세부 정보를 확인하고 **마침**을 클릭합니다.
   i. **가상 프로세서 개수** 값을 4로 설정합니다. 기본적으로 프로세서 개수는 1로 설정되어 있습니다.
   프로세서 개수를 설정하려면:
      i. OMIMSSC 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 **설정**을 선택합니다.
      ii. **설정**에서 **프로세서**를 선택하고 **가상 프로세서 개수**를 4로 설정합니다.
2. OMIMSSC 어플라이언스가 시작되면 다음 작업을 수행합니다.

노트: 모든 서비스가 시작될 수 있도록 **관리자**로 로그인하기 전에 5분을 기다릴 것을 권장합니다.

a. **로컬호스트 로그인**에 admin을 입력합니다.
b. **새로운 관리자 암호를 입력합니다**에 암호를 입력합니다.

노트: Dell EMC는 어플라이언스 `admin` 사용자 및 콘솔 확장 프로그램을 인증하는 데 강력한 암호를 구성하여 사용하도록 권장합니다.

c. **새로운 관리자 암호를 확인합니다**에서 암호를 재입력하고, **Enter**를 눌러 계속 진행합니다.
d. 나열된 옵션에서 **네트워크 구성**을 선택하고 **Enter** 키를 누른 후 다음의 하위 단계를 수행합니다.
   - **NetworkManagerTUI**에서 **시스템 호스트 이름 설정**을 선택하고 OMIMSSC 어플라이언스 이름을 입력하고 **확인**을 클릭합니다.

     예를 들면, 다음과 같습니다. `Hostname.domain.com`

     노트: 네트워크 구성 옵션을 선택하여 OMIMSSC 어플라이언스의 IP 주소를 변경할 수 있습니다. 이 시점 이후에는 OMIMSSC 어플라이언스의 IP 주소나 호스트 이름을 변경할 수 없습니다.
   - 정적 IP 주소를 입력하는 경우 **연결 편집**을 선택하고 **Ethernet0**를 선택합니다.

     IPv4 구성을 선택하고 **수동**을 선택한 다음 **표시**를 클릭합니다. IP 구성 주소, 게이트웨이 주소, DNS 서버 IP를 입력하고 **확인**을 클릭합니다.

e. OMIMSSC 어플라이언스의 OMIMSSC 관리 포털 URL을 확인합니다.

노트: OMIMSSC 어플라이언스 IP 및 FQDN을 DNS의 정방향 조회 영역 및 역방향 조회 영역에 추가합니다.

노트: 어플라이언스 로그는 관리자가 아닌 사용자가 액세스할 수 있습니다. 단, 이러한 로그에는 기밀 정보가 포함되어 있지 않습니다. 해결 방법으로 어플라이언스 URL을 보호합니다.

ESXi에서 OMIMSSC 어플라이언스 설정

ESXi를 사용하여 OMIMSSC를 배포하기 전에 압축된 ZIP 파일에서 로컬 드라이브로 OVA 파일의 압축을 풀었는지 확인합니다. ESXi에 OMIMSSC를 배포하려면 다음을 수행합니다.

1. IP 주소를 사용하여 ESXi를 시작합니다.

   VMware ESXI 로그인 페이지가 표시됩니다.
2. 사용자 이름과 암호를 입력하고 로그인을 클릭합니다.
3. 왼쪽 창에서 가상 머신을 선택합니다.
4. VM을 생성하려면 VM 생성 또는 등록을 선택합니다.

   새 가상 머신 마법사가 표시됩니다.
   a. 생성 유형 선택 섹션에서 OVF 또는 OVA 파일에서 가상 머신 배포 옵션을 선택합니다.
   b. 다음을 클릭합니다.
   c. OVF 및 VMDK 파일 선택에서 생성하려는 VM의 이름을 입력합니다.
   d. 클릭하여 파일을 선택 또는 끌어서 놓기를 클릭합니다.
   e. OMIMSSC_xx.ova 파일을 두 번 클릭합니다. OVA 관리 팩이 설치 프로세스에 업로드됩니다.
   f. 다음을 클릭합니다.
   g. 스토리지 선택 섹션에서 구성 및 VD 파일을 저장할 스토리지 또는 데이터스토어를 선택합니다.
   h. 다음을 클릭합니다.
   i. 배포 옵션 섹션에서 필요한 네트워크 매핑을 선택합니다.
      - 기본적으로 디스크 프로비저닝 기능은 씬으로 선택됩니다.
      - VM의 전원을 자동으로 켜는 옵션이 활성화됩니다.
   j. 다음을 클릭합니다.
   k. 완료 준비 섹션에서 지정한 설정을 확인한 다음 마침을 클릭합니다.

      VM 생성 프로세스가 시작됩니다. 최근 작업 창에서 상태를 볼 수 있습니다.
5. ESXi에서 호스팅된 VM에서 호스트와 게스트 시간 동기화 옵션을 활성화합니다.
   a. VM을 선택하고 편집 옵션을 클릭합니다.
   b. VM 옵션을 선택합니다.
   c. VMware Tools > 시간 > 호스트와 게스트 시간 동기화를 선택합니다.

여러 Microsoft 콘솔 등록

OMIMSSC에 여러 Microsoft 콘솔이 등록되어 있는 경우 OMIMSSC 어플라이언스 리소스를 관리합니다.

OMIMSSC 어플라이언스에 등록할 Microsoft 콘솔 수에 따라 하드웨어 요구 사항이 충족되도록 해야 합니다. 자세한 내용은 OMIMSSC에 대한 공통 시스템 요구 사항을 참조하십시오.

여러 Microsoft 콘솔에 대한 리소스를 구성하려면 다음을 수행합니다.

1. OMIMSSC 어플라이언스를 실행하고 로그인합니다.
2. **등록 매개변수 구성**으로 이동한 후 **Enter**를 클릭합니다.
3. OMIMSSC 어플라이언스에 등록할 콘솔 수를 입력합니다.
   필요한 리소스가 나열됩니다.

OMIMSSC 관리 포털을 실행하여 OMIMSSC 구성 요소 다운로드

1. OMIMSSC 어플라이언스에 로그인할 때 사용한 것과 동일한 자격 증명을 사용하여 브라우저를 실행하고 OMIMSSC 관리 포털에 로그인합니다.

   형식: `https://<IP address or FQDN>`

   노트: 로컬 인트라넷 사이트에 OMIMSSC 관리 포털 URL을 추가합니다. 자세한 내용은 브라우저에서 OMIMSSC IP 주소 추가를 참조하십시오.
2. **다운로드**와 **설치 프로그램 다운로드**를 클릭하여 필요한 콘솔 확장 프로그램을 다운로드합니다.

MECM용 OMIMSSC 콘솔 확장 프로그램 설치

- MECM 관리 콘솔에서 사용하기 전에 OMIMSSC를 MECM 사이트 서버에 설치했는지 확인합니다.
- MECM용 OMIMSSC 콘솔 확장 프로그램을 설치, 업그레이드 또는 제거하기 전에 Configuration Manager를 닫는 것이 좋습니다.

1. `OMIMSSC_MECM(SCCM)_Console_Extension.exe`를 두 번 클릭합니다.
   시작 화면이 표시됩니다.
2. **다음**을 클릭합니다.
3. **라이선스 계약** 페이지에서 **라이선스 계약의 조건에 동의합니다**를 선택한 후 **다음**을 클릭합니다.
4. **대상 폴더** 페이지에는 기본적으로 설치 폴더가 선택되어 있습니다. 위치를 변경하려면, **변경**을 클릭하고 새 위치로 이동한 후 **다음**을 클릭합니다.
5. **프로그램 설치 준비** 페이지에서 **설치**를 클릭합니다.
   콘솔 확장 프로그램을 설치한 후 다음 폴더가 생성됩니다.
   - Log - 이 폴더는 콘솔 관련 로그 정보로 구성됩니다.
6. **설치가 성공적으로 완료됨**에서 **마침**을 클릭합니다.

권장 사항: MECM 2103이 설치된 설정에서 시작하여 **MECM 계층 설정 속성의 계층 옵션에 대해 승인된 콘솔 확장만 허용**하는 옵션을 비활성화해야. MECM 콘솔에서 OMIMSSC 콘솔 시작 지점을 볼 수 있습니다. 자세한 내용은 Microsoft 설명서의 Configuration Manager 콘솔 섹션을 참조하십시오.

SCVMM용 OMIMSSC 콘솔 확장 프로그램 설치

- SCVMM 관리 서버 및 SCVMM 콘솔에 OMIMSSC 콘솔 확장 프로그램을 설치합니다. OMIMSSC 콘솔을 설치한 후에만 콘솔 확장 프로그램을 SCVMM으로 가져올 수 있습니다.

1. `OMIMSSC_SCVMM_Console_Extension.exe`를 두 번 클릭합니다.
   시작 화면이 표시됩니다.
2. **다음**을 클릭합니다.
3. **라이선스 계약** 페이지에서 **라이선스 계약의 조건에 동의합니다**를 선택한 후 **다음**을 클릭합니다.
4. **대상 폴더** 페이지에는 기본적으로 설치 폴더가 선택되어 있습니다. 위치를 변경하려면, **변경**을 클릭하고 새 위치로 이동한 후 **다음**을 클릭합니다.

5. **프로그램 설치 준비** 페이지에서 **설치**를 클릭합니다.
   콘솔 확장 프로그램을 설치한 후 다음 폴더가 생성됩니다.
   - Log - 이 폴더는 콘솔 관련 로그 정보로 구성됩니다.
   - OMIMSSC_UPDATE - 이 폴더는 CAU(Cluster Aware Update)에 필요한 모든 작업으로 구성됩니다. 이 폴더에는 CAU 작업에 대한 읽기 및 쓰기 권한만 있습니다. Windows Management Instrumentation(WMI) 권한이 이 폴더에 구성되어 있습니다. 자세한 내용은 Microsoft 설명서를 참조하십시오.
6. **InstallShield 마법사 완료** 페이지에서 **마침**을 클릭합니다.
7. SCVMM용 OMIMSSC 콘솔 확장 프로그램을 SCVMM 콘솔로 가져옵니다. 자세한 내용은 SCVMM용 OMIMSSC 콘솔 확장 프로그램 가져오기를 참조하십시오.

6

Microsoft 콘솔 등록 OMIMSSC

다음 사전 요구 사항 및 필요한 계정 권한이 충족되었는지 확인합니다.

- MECM 사용자의 경우 MECM 콘솔용 OMIMSSC 콘솔 확장 프로그램이 설치됩니다.
- SCVMM 사용자의 경우 SCVMM용 OMIMSSC 콘솔 확장 프로그램이 설치됩니다.

다음과 같은 정보를 사용할 수 있는지 확인합니다.

- Microsoft System Center가 설정된 시스템의 사용자 자격 증명은 필요한 계정 권한을 참조하십시오.
- MECM의 FQDN 또는 SCVMM의 FQDN

OMIMSSC에 MECM 또는 SCVMM 콘솔을 등록하려면 다음을 수행합니다.

1. OMIMSSC 관리 포털에 로그인합니다.
2. **설정**을 클릭하고 **콘솔 등록**을 클릭한 다음 **등록**을 클릭합니다.
   콘솔 등록 페이지가 표시됩니다.
3. 콘솔의 이름과 설명을 입력합니다.
4. MECM 사이트 서버의 FQDN 또는 SCVMM 서버를 입력하고 자격 증명을 입력합니다.
5. **새로 만들기**를 클릭하여 MECM 또는 SCVMM 콘솔에 액세스하기 위한 Windows 유형 자격 증명 프로파일을 생성합니다.
   - **자격 증명 프로파일 유형**을 **Windows 자격 증명 프로파일**로 선택합니다.
   - 프로파일 이름과 설명을 입력합니다.
   - **자격 증명**에 사용자 이름과 암호를 입력합니다.
   - **도메인**에 도메인 세부 정보를 제공합니다.

   노트: 콘솔 등록을 위한 자격 증명 프로파일을 생성하는 동안 도메인 이름과 TLD(Top Level Domain) 상세 정보를 입력하십시오.

   노트: 도메인 관리자 계정과 로컬 관리자 계정에 대한 자격 증명이 다른 경우에는 도메인 관리자 계정을 사용하여 MECM 또는 SCVMM에 로그인하지 마십시오. 대신 다른 도메인 사용자 계정을 사용하여 MECM 또는 SCVMM에 로그인합니다.

   예를 들어 도메인 이름이 `mydomain`이고 TLD가 `com`인 경우 자격 증명 프로파일에 도메인 이름을 `mydomain.com`으로 입력합니다.
6. OMIMSSC 어플라이언스와 Microsoft 콘솔 간의 연결을 확인하려면 **연결 테스트**를 클릭합니다.
7. 테스트 연결에 성공한 후 콘솔을 등록하려면 **등록**을 클릭합니다.
   등록 후 OMIMSSC는 SCVMM에서 **OMIMSSC SCVMM 콘솔 확장 프로그램 등록 프로파일**이라는 계정을 생성합니다. 이 프로파일이 삭제된 경우 OMIMSSC에서 어떤 작업도 수행할 수 없으므로 이 프로파일이 삭제되지 않도록 하십시오. MECM 관리 콘솔에서 OMIMSSC 콘솔 확장 프로그램을 사용하도록 MECM 사이트 서버를 등록합니다.

주제:

- 등록된 Microsoft 콘솔에서 OMIMSSC에 액세스

등록된 Microsoft 콘솔에서 OMIMSSC에 액세스

등록된 MECM 또는 SCVMM 콘솔에서 OMIMSSC을 실행합니다.

브라우저에서 OMIMSSC FQDN 주소 추가

OMIMSSC를 실행하기 전에 다음 단계를 수행하여 OMIMSSC의 FQDN 주소를 **로컬 인트라넷** 사이트 목록에 사전 요구 사항으로 추가합니다.

1. **IE 설정**을 클릭하고 **인터넷 옵션**을 클릭합니다.
2. **고급**을 클릭하고 **설정** 아래에서 **보안** 섹션을 검색합니다.
3. **암호화된 페이지를 디스크에 저장하지 않음** 옵션을 선택 해제하고 **확인**을 클릭합니다.

MECM용 OMIMSSC 콘솔 확장 프로그램 실행

계정 권한에 나와 있는 사용자 권한 표를 봅니다.

MECM 콘솔에서 **자산 및 규정 준수**를 클릭하고 **개요**를 클릭한 다음 **MECM용 OMIMSSC 콘솔 확장 프로그램**을 클릭합니다.

노트: RDP(Remote Desktop Protocol)를 사용하여 MECM 콘솔에 연결하는 경우 RDP를 닫으면 OMIMSSC 세션이 로그아웃될 수 있습니다. 따라서 RDP 세션을 다시 연 후 로그인하십시오.

SCVMM용 OMIMSSC 콘솔 확장 프로그램 가져오기

SCVMM용 OMIMSSC 콘솔 확장 프로그램을 가져오려면 다음을 수행합니다.

1. 관리자 권한을 사용하거나 위임된 관리자로 SVMM 콘솔을 실행합니다.
2. **설정**을 클릭한 후 **콘솔 애드인 가져오기**를 클릭합니다.
   콘솔 애드인 마법사 가져오기가 표시됩니다.
3. **탐색**을 클릭하고 `C:\Program Files\OMIMSSC\VMM Console Extension`에서 zip 파일을 선택하고 **다음**을 클릭한 후 **마침**을 클릭합니다.
   애드인이 유효한지 확인합니다.

SCVMM용 OMIMSSC 콘솔 확장 프로그램 실행

1. SCVMM 콘솔에서 **패브릭**을 선택한 후 **모든 호스트** 서버 그룹을 선택합니다.

   노트: OMIMSSC를 실행하려면, 액세스할 권한이 있는 호스트 그룹을 임의로 선택할 수 있습니다.

2. **홈** 리본에서 **DELL EMC OMIMSSC**를 선택합니다.

7

OMIMSSC 및 구성 요소 관리

주제:

OMIMSSC 어플라이언스 세부 정보 보기

1. 브라우저에서 OMIMSSC 관리 포털을 실행합니다.
2. OMIMSSC 어플라이언스 VM에 로그인할 때 사용한 것과 동일한 자격 증명을 사용하여 OMIMSSC 관리 포털에 로그인한 후 **어플라이언스 세부 정보**를 클릭합니다. OMIMSSC 어플라이언스의 IP 주소 및 호스트 이름이 표시됩니다.

OMIMSSC 사용자 관리 보기

1. 브라우저에서 OMIMSSC 관리 포털을 실행합니다.
2. OMIMSSC 어플라이언스 VM에 로그인할 때 사용한 것과 동일한 자격 증명을 사용하여 OMIMSSC 관리 포털에 로그인한 후 **OMIMSSC 사용자 관리**를 클릭합니다. 이전에 MECM 또는 SCVMM에 로그인한 사용자의 상태가 표시됩니다.

HTTPS 인증서 관리

OMIMSSC는 보안 HTTP 액세스(HTTPS)용 x.509 PKI 표준 기반 인증서를 사용합니다.

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

보안 강화를 위해 CA(Certificate Authority) 또는 Enterprise CA(내부)에서 서명하거나 맞춤 구성된 인증서 사용이 권장됩니다.

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

다음 유형의 인증서를 OMIMSSC 인증용으로 사용할 수 있습니다.

- 자체 서명된 인증서

  OMIMSSC는 어플라이언스의 호스트 이름이 구성되면 자체 서명된 인증서를 생성합니다.

- 신뢰할 수 있는 CA(Certificate Authority) 공급업체에서 서명하는 인증서입니다.

등록된 OMIMSSC 서버의 인증서 업데이트

OMIMSSC에서는 키 길이가 2,048비트인 RSA 암호화 표준을 이용하여 CSR(인증서 서명 요청)을 생성하기 위해 OpenSSL API를 사용합니다.

OMIMSSC로 생성된 CSR은 신뢰할 수 있는 CA(Certification Authority)에서 디지털 방식으로 서명된 인증서를 받습니다. OMIMSSC는 보안 통신을 위해 웹 서버에서 디지털 인증서를 사용하여 HTTPS를 활성화합니다. 관리 포털을 사용하여 CA에서 서명된 인증서를 업로드할 수 있습니다.

OMIMSSC의 HTTPS 인증서 관리에 대한 자세한 내용은 https://www.dell.com/support에서 *Microsoft Endpoint Configuration Manager용 Microsoft System Center 버전 7.3을 위한 OpenManage Integration 및 System Center Virtual Machine Manager 7.3 사용자 가이드*를 참조하십시오.

CSR(Certificate Signing Request) 생성

새 인증서 CSR를 생성하면 이전에 생성한 CSR로 만든 인증서가 어플라이언스에 업로드되지 않습니다.

노트: CSR을 다운로드하려면 **파일 다운로드** 옵션이 활성화되어 있는지 확인합니다. 이 옵션은 **Internet Explorer** 사용자에게 적용되며 *인터넷 옵션 -> 보안 -> 인터넷 -> 사용자 지정 수준 -> 다운로드*에서 활성화할 수 있습니다.

CSR을 생성하려면 다음을 수행합니다.

1. **포털 관리** 페이지에서 **설정 -> 보안**을 선택하고 **SSL 인증서** 영역에서 **인증서 서명 요청 생성**을 클릭합니다. 새 CSR을 생성하면 이전 CSR을 사용하여 생성한 인증서를 더는 어플라이언스에 업로드할 수 없다는 메시지가 표시됩니다.
2. 요청을 계속할 경우 **인증서 서명 요청 생성** 대화 상자에서 공통 이름, 조직, 지역, 구/군/시, 주, 국가, 기본 SAN(Primary Subject Alternate Name), 보조 SAN(Secondary Subject Alternate Name) 및 이메일 주소 정보를 입력합니다. **Generate(생성)**를 클릭합니다.
3. **다운로드**를 클릭하고 결과로 생성되는 CSR을 액세스 가능한 위치에 저장합니다.

HTTPS 인증서 업로드

인증서는 PEM 형식을 사용해야 합니다.

OMIMSSC 어플라이언스 및 호스트 시스템 또는 OMIMSSC와의 보안 통신을 위해 HTTPS 인증서를 사용할 수 있습니다. 이 유형의 보안 통신을 설정하려면 CSR 인증서를 인증서 서명 기관으로 보낸 다음 관리 콘솔을 사용하여 서명된 인증서를 업로드합니다.

1. **관리 포털** 페이지에서 **설정>보안**을 클릭하고 **SSL 인증서** 영역에서 **인증서 업로드**를 클릭합니다.
2. **인증서 업로드** 대화 상자에서 옵션을 선택합니다.
3. 인증서를 업로드하려면 **탐색**을 클릭한 후 **업로드**를 클릭합니다.
4. 인증서 업로드가 완료되었음을 나타내는 대화 상자가 표시됩니다.

노트: 인증서 업로드 시 서비스가 재시작되는 동안 OMIMSSC 어플라이언스는 몇 분 동안 응답하지 않을 수 있습니다. MECM/SCVMM 콘솔에서 OMIMSSC 관리 포털 및 OMIMSSC 콘솔 플러그인의 기존 브라우저 세션을 모두 닫는 것이 좋습니다. 업로드된 인증서를 보려면 OMIMSSC 관리자 포털에 다시 로그인하십시오.

기본 HTTPS 인증서 복원

1. **관리 포털** 페이지에서 **설정->보안**을 선택하고 **SSL 인증서** 영역에서 기본 인증서 복원을 클릭합니다.
2. **기본 인증서 복원** 대화 상자에서 **예**를 클릭합니다.

노트: 기본 인증서 복원 시 OMIMSSC 어플라이언스는 서비스가 재시작되는 동안 몇 분 동안 응답하지 않을 수 있습니다. MECM/SCVMM 콘솔에서 OMIMSSC 관리 포털 및 OMIMSSC 콘솔 플러그인의 기존 브라우저 세션을 닫고 브라우저 캐시를 지우는 것이 좋습니다. 업데이트된 인증서를 보려면 OMIMSSC 관리 포털에 다시 로그인하십시오.

등록된 콘솔 보기 또는 새로 고침

다음 단계를 수행하여 OMIMSSC에 등록된 모든 Microsoft 콘솔을 볼 수 있습니다.

1. OMIMSSC 관리 포털에서 **설정**을 클릭한 다음 **콘솔 등록**을 클릭합니다.
   등록된 모든 콘솔이 표시됩니다.
2. **설정**을 클릭하고 **콘솔 등록**을 클릭합니다.
   등록된 모든 콘솔이 표시됩니다.
3. 등록된 콘솔의 최신 목록을 보려면 **새로 고침**을 클릭합니다.

OMIMSSC 어플라이언스 암호 변경

OMIMSSC 어플라이언스 VM 콘솔의 암호를 변경하려면 다음을 수행합니다.

1. OMIMSSC 어플라이언스 VM 콘솔을 실행하고 이전 자격 증명을 사용하여 로그인합니다.
2. **관리자 암호 변경**으로 이동하고 **Enter** 키를 누릅니다.
   암호를 변경할 화면이 표시됩니다.
3. 현재 암호를 입력한 다음 나열된 조건과 일치하는 새 암호를 입력합니다. 새 암호를 다시 입력하고 **Enter** 키를 누릅니다.
   암호 변경 후의 상태가 표시됩니다.
4. 홈 페이지로 돌아가려면 **Enter** 키를 누릅니다.

노트: 암호 변경 후 어플라이언스가 재부팅됩니다.

OMIMSSC 어플라이언스 재부팅

OMIMSSC 어플라이언스를 재부팅하려면 다음을 수행합니다.

1. OMIMSSC 어플라이언스 VM을 실행하고 로그인합니다.
2. **이 가상 어플라이언스 재부팅**을 찾은 후 **Enter** 키를 누릅니다.
3. 확인하려면 **예**를 클릭합니다.
   OMIMSSC 어플라이언스가 필요한 모든 서비스와 함께 재시작됩니다.
4. VM이 재시작된 후 OMIMSSC 어플라이언스에 로그인합니다.

OMIMSSC 관리 포털에서 MECM 및 SCVMM 계정 수정

이 옵션을 사용하면 OMIMSSC 콘솔에서 MECM 및 SCVMM 계정의 암호를 변경할 수 있습니다.

OMIMSSC 관리 포털에서 MECM 및 SCVMM 관리자 암호를 수정할 수 있습니다. 이 프로세스는 순차적 작업입니다.

1. Active Directory에서 MECM 또는 SCVMM 관리자 계정의 암호를 수정합니다.
2. OMIMSSC에서 암호를 수정합니다.

OMIMSSC에서 MECM 또는 SCVMM 관리자 계정을 변경하려면 다음을 수행합니다.

1. OMIMSSC 관리 포털에서 **설정**을 클릭한 다음 **콘솔 등록**을 클릭합니다.
   등록된 콘솔이 표시됩니다.
2. **설정**을 클릭한 후 **콘솔 등록**을 클릭합니다.
   등록된 콘솔이 표시됩니다.
3. 편집할 콘솔을 선택하고 **편집**을 클릭합니다.
4. 새로운 암호를 입력하고 **마침**을 클릭하여 변경 사항을 저장합니다.

암호를 업데이트한 후 새 자격 증명을 사용하여 Microsoft 콘솔 및 OMIMSSC 콘솔 확장 프로그램을 다시 실행합니다.

설치 프로그램 복구 또는 수정

설치 프로그램 파일을 복구하려면 다음 항목을 참조하십시오.

- MECM용 OMIMSSC 콘솔 확장 프로그램 복구
- SCVMM용 OMIMSSC 콘솔 확장 프로그램 복구

MECM용 OMIMSSC 콘솔 확장 프로그램 복구

OMIMSSC 파일이 손상된 경우 이를 복구하려면 다음 단계를 수행하십시오.

1. MECM용 OMIMSSC 콘솔 확장 설치 프로그램을 실행합니다.
   시작 화면이 표시됩니다.
2. **다음**을 클릭합니다.
3. **프로그램 유지 보수**에서 **복구**를 선택하고 **다음**을 클릭합니다.

프로그램 복구 준비 화면이 표시됩니다.

4. **설치**를 클릭합니다.
   진행 화면에 설치 진행률이 표시됩니다. 설치가 완료되면 **Installshield 마법사 완료** 창이 표시됩니다.
5. **마침**을 클릭합니다.

SCVMM용 OMIMSSC 콘솔 확장 프로그램 복구

OMIMSSC 파일이 손상된 경우 이를 복구하려면 다음 단계를 수행하십시오.

1. *SCVMM용 OMIMSSC 콘솔 확장* 설치 프로그램을 실행합니다.
2. **프로그램 유지 보수**에서 **복구**를 선택하고 **다음**을 클릭합니다.
3. **프로그램 복구 또는 제거 준비 완료**에서 **복구**를 클릭합니다.
4. 복구 작업이 완료되면 **마침**을 클릭합니다.

8

OMIMSSC 어플라이언스 백업 및 복구

OMIMSSC 어플라이언스의 **백업 어플라이언스 데이터** 옵션을 사용하면 등록된 Microsoft 콘솔, 발견된 디바이스, 프로필, 업데이트 소스, 운영 템플릿, 라이선스 및 OMIMSSC 콘솔 확장 프로그램에서 완료된 작업과 같은 OMIMSSC 정보를 저장할 수 있습니다.

주제:

OMIMSSC 어플라이언스 백업

이 기능을 사용하면 OMIMSSC 어플라이언스 데이터베이스와 중요한 구성을 백업할 수 있습니다. 백업 파일은 사용자가 제공한 암호화된 암호로 CIFS 공유 경로에 저장됩니다. 어플라이언스 데이터를 주기적으로 백업하는 것이 좋습니다.

사전 요구 사항:

- 액세스 자격 증명을 사용하여 CIFS 공유를 생성하고 읽기 및 쓰기 권한을 허용해야 합니다.
- 백업 및 복원 모두에 동일한 암호화 암호가 사용되는지 확인합니다. 암호화 암호는 복구될 수 없습니다.

CIFS 공유에서 OMIMSSC 어플라이언스 데이터를 백업하려면 다음 단계를 수행합니다.

노트: 이 기능은 OMIMSSC 버전 7.2.1 이상에서 사용할 수 있으며 어플라이언스 VM 콘솔에서는 사용할 수 없습니다.

1. OMIMSSC 관리 포털에서 **설정**을 클릭한 다음 **어플라이언스 백업**을 클릭합니다.
2. **백업 설정 및 세부 정보** 페이지에서 백업에 대한 CIFS 공유 경로를 `\\<IP address or FQDN>\<folder name>` 형식으로 제공합니다.
3. 드롭다운 메뉴에서 **CIFS 공유에 대한 자격 증명 프로파일**을 선택합니다.
4. **암호** 및 **암호 재입력** 필드에 암호화 암호를 입력합니다.
5. **연결 테스트**를 클릭하여 OMIMSSC 어플라이언스와 CIFS 공유 간의 연결을 확인합니다.
   언급된 백업 폴더가 존재하며 액세스할 수 있는지 확인합니다.
6. **백업**을 클릭하여 OMIMSSC 어플라이언스 데이터를 백업합니다.

다음 단계

성공적으로 백업되었는지 재확인하려면 백업 폴더로 이동합니다. 백업 폴더에는 다음 형식으로 두 개의 파일이 생성됩니다.

- Dell_OMIMSSC_VM_Backup_<date_and_time>.tar.gz
- Dell_OMIMSSC_VM_Backup_<date_and_time>.tar.gz.sum

노트: 백업 파일에 표시되는 날짜 및 시간은 백업이 수행된 시점을 나타냅니다. 백업 파일의 이름을 변경하지 마십시오.

노트: 어플라이언스 데이터가 성공적으로 백업되었고 백업 파일의 크기가 1KB 이상인지 확인합니다. 파일 크기가 1KB 미만이면 어플라이언스를 재시작합니다. 어플라이언스를 재시작한 후 OMIMSSC 어플라이언스 데이터를 백업합니다.

OMIMSSC 어플라이언스 복원

- 복구 작업은 새로 배포된 어플라이언스에서만 수행해야 합니다. 새 어플라이언스에서 어떠한 작업도 수행되지 않았는지 확인하십시오.
- SCVMM 콘솔에서 이전 콘솔 추가 기능을 제거하고 새 설치 프로그램을 다운로드하여 OMIMSSC 콘솔 추가 기능을 업그레이드하십시오. 자세한 *내용은 OpenManage Integration for Microsoft System Center 통합 사용자 가이드에서 MECM/SCVMM용 OMIMSSC 콘솔 확장 업그레이드 섹션*을 참조하십시오.

OMIMSSC 어플라이언스 데이터를 다음 시나리오 중 하나로 복원합니다.

- 새 버전으로 업그레이드하기 전 OMIMSSC
- 한 OMIMSSC 어플라이언스에서 다른 OMIMSSC 어플라이언스로 마이그레이션하기 전

사전 요구 사항:

새 OMIMSSC 어플라이언스에 대한 작업을 수행하기 전에 데이터를 복원해야 합니다.

새 OMIMSSC 어플라이언스에 이전 OMIMSSC 어플라이언스 데이터를 복원하려면 다음 단계를 수행합니다.

1. OMIMSSC 관리 포털에서 **설정**을 클릭한 다음 **어플라이언스 복원**을 클릭합니다.
2. 어플라이언스 데이터를 복원하는 데 사용할 수 있는 두 가지 옵션이 있습니다.
   - `Option 1: Restore using IP address`

     이 옵션은 OMIMSSC 버전 7.2와 7.2.1에서 데이터를 복원하는 데 사용해야 합니다.

     IP 주소에서 이전 OMIMSSC 어플라이언스의 IP 주소를 입력하고 복원을 클릭합니다.

     노트: 데이터가 새 OMIMSSC 어플라이언스로 복원됩니다.
   - 옵션 2: 맞춤 구성 CIFS 공유를 사용하여 복원

     이 옵션은 7.2.1 릴리스 이후부터 데이터를 복원하는 데 사용해야 합니다

     노트: CIFS 공유 액세스 자격 증명은 데이터베이스에 자격 증명 프로파일로 저장됩니다. 추가 보안 조치용으로, 백업된 파일의 암호를 해독하기 위한 암호화 암호를 제공해야 합니다.

   a. CIFS 공유 위치 경로는 `\\<IP address or FQDN>\<folder name>\<filename>.tar.gz` 형식으로 제공합니다.
   b. 드롭다운 메뉴에서 CIFS 공유에 대한 자격 증명 프로파일을 선택합니다.
   c. 파일 암호화 암호를 입력하고 복원을 클릭합니다.

   복원 페이지가 자동으로 로그아웃됩니다.
3. OMIMSSC 어플라이언스가 재시작된 후 복원 상태를 보려면 다음을 수행합니다.

   모든 서비스가 시작될 수 있도록 로그인하기 전에 몇 분 정도 기다리는 것이 좋습니다.

   a. OMIMSSC 관리 포털에 로그인합니다.
   b. **설정**을 확장한 다음 **로그**를 클릭합니다.
   c. `dlciappliance_main.log` 파일을 다운로드하고 성공적으로 복원되었다는 것을 나타내는 다음 메시지를 찾습니다.

      ```
      Successfully restored OMIMSSC Appliance
      ```
4. SCVMM 콘솔의 경우 OMIMSSC 어플라이언스에서 복원 작업을 성공적으로 수행한 후 새 콘솔 추가 기능을 다시 가져옵니다.

기존 OMIMSSC 어플라이언스를 복원한 후 다음을 수행합니다.

- 기존 OMIMSSC 어플라이언스를 복원한 후 예약된 작업을 재생성하는 것이 좋습니다.
- 이전 버전의 OMIMSSC에서 내보낸 하이퍼바이저 프로파일의 경우 프로파일을 편집하여 ISO 파일 경로 및 Windows 자격 증명 프로파일을 입력해야 합니다.
- 새 CSR 요청을 생성하고 유효한 인증서를 가져옵니다.

9

제거 OMIMSSC

OMIMSSC를 제거하려면 다음을 수행합니다.

1. OMIMSSC 관리 포털에서 OMIMSSC 콘솔을 등록 취소합니다. 자세한 내용은 OMIMSSC 콘솔 등록 취소를 참조하십시오.
2. 등록된 Microsoft 콘솔에서 OMIMSSC 콘솔 확장 프로그램을 제거합니다. 자세한 내용은 MECM용 OMIMSSC 콘솔 확장 프로그램 제거 또는 SCVMM용 OMIMSSC 콘솔 확장 프로그램 제거를 참조하십시오.
3. OMIMSSC 어플라이언스 VM을 제거합니다. 자세한 내용은 OMIMSSC 어플라이언스 VM 제거를 참조하십시오.
4. 어플라이언스별 계정을 제거합니다. 자세한 내용은 기타 제거 작업을 참조하십시오.

주제:

OMIMSSC에서 Microsoft 콘솔 등록 취소 OMIMSSC

하나의 OMIMSSC 어플라이언스에 여러 개의 Microsoft 콘솔을 등록한 경우 단일 콘솔을 등록 취소하고 OMIMSSC로 계속 작업할 수 있습니다. 전체 설치 제거에 대한 자세한 내용은 *OpenManage Integration for Microsoft System Center 사용자 가이드*를 참조하십시오.

Microsoft 콘솔을 등록 취소하려면 다음을 수행합니다.

1. OMIMSSC에서 **콘솔 등록**을 클릭합니다.
   OMIMSSC 어플라이언스에 등록된 모든 콘솔이 표시됩니다.
2. 콘솔을 선택하고 **등록 취소**를 클릭하여 어플라이언스에서 콘솔 등록을 제거합니다.
3. 콘솔 플러그인을 제거합니다.

   노트:
   - 콘솔의 등록을 취소하고 제거하면 콘솔과 연결된 호스트 서버가 OMIMSSC의 할당되지 않은 서버 목록으로 이동합니다.

4. (선택 사항) 콘솔에 연결할 수 없는 경우 콘솔을 강제로 등록 취소하도록 승격 시 **예**를 클릭합니다.
   - 등록 취소를 수행하는 동안 OMIMSSC 콘솔이 이미 열려 있는 경우 Microsoft 콘솔을 닫아 등록 취소를 완료합니다.
   - SCVMM 사용자의 경우에는 다음과 같습니다.
     - SCVMM 서버에 연결할 수 없을 때 OMIMSSC에서 SCVMM 콘솔을 강제로 등록 취소하는 경우 SCVMM에서 **애플리케이션 프로파일**을 수동으로 삭제합니다.

MECM용 OMIMSSC 콘솔 확장 프로그램 제거

`OMIMSSC_MECM(SCCM)_Console_Extension.exe`를 두 번 클릭하고 **제거**를 선택한 다음 화면에 나타나는 지시를 따릅니다.

SCVMM용 OMIMSSC 콘솔 확장 프로그램 제거

SCVMM용 OMIMSSC 콘솔 확장 프로그램을 제거하려면 다음을 수행합니다.

1. **프로그램 제거**를 위한 콘솔 확장 프로그램을 제거합니다.
   - **제어판**에서 **프로그램**을 클릭한 다음 **프로그램 제거**를 클릭합니다.
   - **SCVMM용 콘솔 애드인**을 선택하고 **제거**를 클릭합니다.
2. SCVMM에서 콘솔 확장 프로그램을 제거합니다.
   - SCVMM 콘솔에서 **설정**을 클릭합니다.

- **OMIMSSC**를 마우스 오른쪽 버튼으로 클릭하고 **제거**를 선택합니다.

기타 제거 단계

SCVMM에서 OMIMSSC 콘솔 확장 프로그램을 제거하려면 다음 계정 및 프로파일을 삭제합니다.
- 어플라이언스 특정 RunAsAccounts
- OMIMSSC 애플리케이션 프로파일

어플라이언스 특정 RunAsAccounts 삭제

SCVMM 콘솔에서 어플라이언스 특정 RunAsAccounts를 삭제하려면 다음을 수행하십시오.
1. SCVMM 콘솔에서 **설정**을 클릭합니다.
2. **계정으로 실행**을 클릭합니다.
3. 계정 목록에서 어플라이언스 특정 계정을 삭제합니다.
   어플라이언스 특정 계정은 `Dell_`이 접두어로 붙어 있습니다.

OMIMSSC 애플리케이션 프로파일 삭제

1. SCVMM 콘솔에서 **라이브러리**, **프로파일**을 클릭한 다음, **애플리케이션 프로파일**을 클릭합니다.
   SCVMM에서 사용된 모든 애플리케이션 프로파일이 표시됩니다.
2. **OMIMSSC 등록 프로필**을 선택하고 삭제합니다.

어플라이언스 VM 제거

어플라이언스 VM을 제거하려면 다음을 수행하십시오.
1. **Windows Server**의 **Hyper-V Manager**에서 어플라이언스 VM을 마우스 오른쪽 버튼으로 클릭하고 **종료**를 클릭합니다.
2. 어플라이언스 VM을 마우스 오른쪽 버튼으로 클릭하고 **삭제**를 클릭합니다.

노트: 어플라이언스 VM을 제거하기 전에 백업을 수행합니다. 이는 어플라이언스 VM을 제거하기 전에 백업을 수행할 수 있는 마지막 기회입니다.

10

OMIMSSC 업그레이드

OMIMSSC 어플라이언스 데이터(설정 및 구성 포함)를 백업한 다음 최신 버전의 OMIMSCC 어플라이언스에서 백업 파일을 복원하여 OMIMSSC 어플라이언스를 최신 버전으로 업그레이드할 수 있습니다.

OMIMSSC 어플라이언스의 백업 및 복원에 대한 자세한 내용은 OMIMSSC 어플라이언스 백업 섹션 및 OMIMSSC 어플라이언스 복원 섹션을 참조하십시오.

다음 표는 OMIMSCC 어플라이언스 버전 7.3의 업그레이드 경로를 표시합니다. 일부 버전은 7.3 버전으로 업그레이드하기 전에 중간 업그레이드가 필요합니다.

표 8. OMIMSCC 어플라이언스 버전 7.3의 업그레이드 경로

현재 OMIMCC 어플라이언스 버전	중간 업그레이드 버전	타겟 OMIMSCC 버전
7.2.1	해당 없음(또는 직접 업그레이드)	7.3
7.2	해당 없음(또는 직접 업그레이드)	7.3
7.1.1	7.2.1	7.3
7.1	7.2.1	7.3

11

자격 증명 및 하이퍼바이저 프로파일 관리

프로파일에는 OMIMSSC에서 작업을 수행하는 데 필요한 모든 데이터가 포함되어 있습니다.

주제:

MECM 및 SCVMM의 자격 증명 프로파일

자격 증명 프로파일을 사용하면 사용자의 역할 기반 기능을 인증하여 사용자 자격 증명을 간편하게 사용하고 관리할 수 있습니다. 각 자격 증명 프로파일에는 단일 사용자 계정에 대한 사용자 이름과 암호가 포함되어 있습니다.

OMIMSSC OMIMSSC는 자격 증명 프로파일을 사용하여 관리형 시스템의 iDRAC에 연결합니다.

다음 4가지 유형의 자격 증명 프로파일을 생성할 수 있습니다.

- 디바이스 자격 증명 프로파일 - iDRAC 또는 CMC에 로그인하는 데 사용됩니다. 또한 이 프로파일을 사용하여 서버를 검색하고, 동기화 문제를 해결하고, 운영 체제를 배포할 수 있습니다. 이 프로파일은 콘솔에 한정됩니다. 이 프로파일은 해당 프로파일이 생성된 콘솔에서만 사용하고 관리할 수 있습니다.
- Windows 자격 증명 프로파일 - Windows 운영 체제의 공유 폴더에 액세스하는 데 사용됩니다.
- 프록시 서버 자격 증명 - 업데이트를 위해 FTP 사이트에 액세스할 때 프록시 자격 증명을 제공할 목적으로 사용됩니다.

  노트: 디바이스 프로파일을 제외한 모든 프로파일이 공유 리소스입니다. 등록된 모든 콘솔에서 이러한 프로파일을 사용하고 관리할 수 있습니다.

자격 증명 프로파일 생성

자격 증명 프로파일을 생성할 때 다음 사항을 고려합니다.

- 자동 검색 중에 iDRAC에 대해 사용 가능한 기본 자격 증명 프로파일이 없는 경우 기본 iDRAC 자격 증명이 사용됩니다. 기본 iDRAC 사용자 이름은 `root`이고 암호는 `calvin`입니다.

  노트: 서버를 검색하기 전에 Dell EMC에서는 강력한 암호를 사용하여 기본 iDRAC 자격 증명 프로파일을 생성할 것을 권장합니다. 이 기본 자격 증명 프로파일은 자동 검색에 사용됩니다. 암호 정책 요구 사항에 대한 자세한 내용은 iDRAC 사용자 가이드를 참조하십시오.
- 모듈형 시스템에 대한 정보를 가져오기 위해 기본 CMC 프로파일을 사용하여 모듈형 서버에 액세스합니다. 기본 CMC 프로파일 사용자 이름은`root`이고 암호는 `calvin`입니다.
- (SCVMM 사용자에만 해당) 디바이스 유형 자격 증명 프로파일이 생성될 때 서버 관리를 위해 연결된 **RunAsAccount**가 **SCVMM**에 생성되고, **RunAsAccount**의 이름은 `Dell_CredentialProfileName`입니다.
- SCVMM에서 **RunAsAccount**를 편집하거나 삭제하지 않았는지 확인합니다.

1. OMIMSSC에서 다음 단계를 수행하여 **자격 증명 프로파일**을 생성합니다.
   - OMIMSSC 대시보드에서 **자격 증명 프로파일 생성**을 클릭합니다.
   - 탐색 창에서 **프로파일 및 템플릿** > **자격 증명 프로파일**을 클릭한 후 **생성**을 클릭합니다.
2. **생성**을 클릭합니다.
   자격 증명 프로파일 페이지가 표시됩니다.
3. **자격 증명 유형**에서 사용할 자격 증명 프로파일 유형을 선택합니다.
4. 프로파일 이름과 설명을 입력합니다.

   노트: **기본 프로파일** 옵션은 디바이스 유형 자격 증명 프로파일에만 적용할 수 있습니다.
5. **자격 증명**에 사용자 이름과 암호를 입력합니다.
   - **디바이스 자격 증명 프로파일**을 생성할 경우 **기본 프로파일** 옵션을 선택하여 이 프로파일을 iDRAC 또는 CMC에 로그인하는 데 사용할 기본 프로파일로 지정하려면 선택합니다. 이 프로파일을 기본 프로파일로 설정하지 않으려면 **없음**을 선택합니다.

노트: 기본 자격 증명 프로파일은 콘솔과 관련이 없습니다. 현재 콘솔에서 자격 증명 프로파일을 기본값으로 선택한 경우 다른 콘솔은 선택한 유형에 대해 기본값이 되지 않습니다.

- **Windows 자격 증명 프로파일**을 생성할 경우 **도메인**에 도메인 세부 정보를 제공합니다.

  노트: 콘솔 등록을 위한 자격 증명 프로파일을 생성하는 동안, NETBIOS 이름이 AD(Active Directory)에 구성되어 있는 경우, NETBIOS 이름을 도메인으로 제공합니다. AD에 NETBIOS 이름이 구성되어 있지 않은 경우, 도메인 이름에 TLD(Top Level Domain) 세부 정보를 제공합니다.

  예를 들어 도메인 이름이 `mydomain`이고 TLD가 `com`인 경우 자격 증명 프로파일에 도메인 이름을 다음과 같이 입력합니다. `mydomain.com`

- **프록시 서버 자격 증명**을 생성할 경우 **프록시 서버 URL**에 프록시 서버 URL을 `http://hostname:port` 또는 `http://IPaddress:port` 형식으로 제공합니다.

6. 프로파일을 생성하려면 **마침**을 클릭합니다.

노트: SCVMM에서 디바이스 유형 자격 증명 프로파일을 생성할 때 앞에 **Dell _**이(가) 있는 해당 **RunAsAccount**를 생성합니다. 등록된 사용자가 생성된 디바이스 자격 증명 프로파일을 사용하는 운영 체제 배포와 같은 작업을 위해 해당 **RunAsAccount**에 액세스할 수 있는지 확인합니다.

자격 증명 프로파일 수정

자격 증명 프로파일을 수정하기 전에 다음 사항을 고려합니다.

- 생성한 후에는 자격 증명 프로파일의 유형을 수정할 수 없습니다. 다른 필드는 수정할 수 있습니다.
- 자격 증명 프로파일은 사용 중인 경우 수정할 수 없습니다.

노트: 자격 증명 프로파일 유형을 수정하는 단계는 동일합니다.

1. 수정할 자격 증명 프로파일을 선택한 후 **편집**을 클릭하고 프로파일을 업데이트합니다.
2. 변경사항을 저장하려면 **저장**을 클릭합니다.

변경 사항을 보려면 **자격 증명 프로파일** 페이지를 새로 고칩니다.

자격 증명 프로파일 삭제

자격 증명 프로파일을 삭제할 때 다음 사항을 고려하십시오.

- 디바이스 유형 자격 증명 프로파일이 삭제되면 SCVMM에서 연결된 **실행 계정**도 삭제됩니다.
- SCVMM에서 **실행 계정**이 삭제되면 OMIMSSC에서 해당 자격 증명 프로파일을 사용할 수 없습니다.
- 서버 검색에 사용되는 자격 증명 프로파일을 삭제하려면 검색된 서버를 삭제한 다음에 자격 증명 프로파일을 삭제합니다.
- 배포에 사용되는 디바이스 유형 자격 증명 프로파일을 삭제하려면 우선 SCVMM 환경에서 배포된 서버를 삭제한 다음에 자격 증명 프로파일을 삭제합니다.
- 자격 증명 프로파일이 업데이트 소스에 사용되면 해당 프로파일을 삭제할 수 없습니다.

노트: 자격 증명 프로파일을 삭제하는 단계는 유형에 관계없이 동일합니다.

삭제하려는 자격 증명 프로파일을 선택한 다음에 **삭제**를 클릭합니다.

변경 사항을 보려면 **자격 증명 프로파일** 페이지를 새로 고칩니다.

SCVMM의 하이퍼바이저 프로파일

하이퍼바이저프로파일에는 맞춤 구성된 WinPE ISO(하이퍼바이저배포에 사용되는 WinPE ISO), 호스트 그룹, SCVMM에서 가져온 호스트 프로파일, 삽입을 위한 LC 드라이버가 포함되어 있습니다. SCVMM 사용자를 위한 OMIMSSC 콘솔 확장 프로그램에서만 하이퍼바이저 프로파일을 생성하고 관리할 수 있습니다.

하이퍼바이저 프로파일 생성

하이퍼바이저 프로파일을 만들고 이 프로파일을 사용하여 하이퍼바이저를 배포합니다.

- WinPE ISO 이미지를 업데이트하고 이미지가 저장된 공유 폴더에 액세스합니다. WinPE 이미지 업데이트에 대한 자세한 내용은 WinPE 업데이트를 참조하십시오.

  WinPE ISO 이미지를 업데이트하고 이미지가 저장된 공유 폴더에 액세스합니다. WinPE 이미지 업데이트에 대한 자세한 내용은 *Configuration Manager 및 Virtual Machine Manager를 위한 Microsoft System Center용 OpenManage Integration 통합 사용자 가이드*의 WinPE 업데이트 섹션을 참조하십시오.

- SCVMM에서 호스트 그룹과 호스트 프로파일 또는 물리적 컴퓨터 프로파일을 만듭니다. SCVMM에서 호스트 그룹을 생성하는 방법에 대한 자세한 내용은 Microsoft 문서 자료를 참조하십시오.

1. OMIMSSC에서 다음 작업 중 하나를 수행합니다.
   - OMIMSSC 대시보드에서 **하이퍼바이저 프로파일 생성**을 클릭합니다.
   - 왼쪽 탐색 창에서 **프로파일 및 템플릿**과 **하이퍼바이저 프로파일**을 클릭한 다음에 **생성**을 클릭합니다.

   하이퍼바이저 프로파일 마법사가 표시됩니다.
2. **시작** 페이지에서 **다음**을 클릭합니다.
3. **하이퍼바이저 프로파일**에서 프로파일의 이름과 설명을 입력하고 **다음**을 클릭합니다.
4. **SCVMM 정보** 페이지에서 다음을 수행합니다.
   a. **SCVMM 호스트 그룹 대상**의 경우에는 드롭다운 메뉴에서 SCVMM 호스트 그룹을 선택하여 이 그룹에 호스트를 추가합니다.
   b. **SCVMM 호스트 프로파일/물리적 컴퓨터 프로파일**에서 서버에 적용할 구성 정보가 포함되어 있는 SCVMM에서 호스트 프로파일 또는 물리적 컴퓨터 프로파일을 선택합니다.

      SCVMM의 **물리적 컴퓨터 프로파일**에서 다음 디스크 파티션 방법 중 하나를 선택합니다.
      - UEFI 모드로 부팅할 때는 **GPT(GUID Partition Table)** 옵션을 선택합니다.
      - BIOS 모드로 부팅하는 경우에는 **MBR(Master Board Record)** 옵션을 선택합니다.
5. **WinPE 부팅 이미지 소스**에서 다음과 같은 상세 정보를 입력하고 **다음**을 클릭합니다.
   a. **네트워크 WinPE ISO 이름**에 대해서는 업데이트된 WinPE 파일 이름이 있는 공유 폴더 경로를 입력합니다. WinPE 파일을 업데이트하려면 WinPE 업데이트를 참조하십시오.
   b. **네트워크 WinPE ISO 이름**에 대해서는 업데이트된 WinPE 파일 이름이 있는 공유 폴더 경로를 입력합니다. WinPE 파일 업데이트에 대한 자세한 내용은*Configuration Manager 및 Virtual Machine Manager를 위한 Microsoft System Center용 OpenManage Integration 사용자 가이드*의 WinPE 업데이트를 참조하십시오.
   c. **자격 증명 프로파일**에 대해서는 WinPE 파일이 있는 공유 폴더에 대한 액세스 권한이 있는 자격 증명을 선택합니다.
   d. (선택 사항) Windows 자격 증명 프로파일을 생성하려면 **새로 만들기**를 클릭합니다. 자격 증명 프로파일 생성에 대한 자세한 내용은 자격 증명 프로파일 생성을 참조하십시오.
   e. (선택 사항) Windows 자격 증명 프로파일을 생성하려면 **새로 만들기**를 클릭합니다. 자격 증명 프로파일 생성에 대한 자세한 내용은 *Configuration Manager 및 Virtual Machine Manager를 위한 Microsoft System Center용 OpenManage Integration 사용자 가이드*의 자격 증명 프로파일 생성을 참조하십시오.
6. (선택 사항) LC 드라이버 삽입을 활성화하려면 다음 단계를 수행합니다.

   노트: NIC 카드용 최신 운영 체제 드라이버 팩은 최신 운영 체제 드라이버에서 사용할 수 있기 때문에 **Dell Lifecycle Controller 드라이버 삽입** 확인란을 선택해야 합니다.

   a. **Dell Lifecycle Controller 드라이버 삽입** 확인란을 선택합니다.
   b. 배포하려는 운영 체제를 선택하여 관련 드라이버를 선택합니다.
7. **요약**에서 **완료**를 클릭합니다.

변경 사항을 보려면 **하이퍼바이저 프로파일** 페이지를 새로 고칩니다.

하이퍼바이저 프로파일 수정

하이퍼바이저 프로파일을 수정할 때는 다음 사항을 고려하십시오.

- Lifecycle Controller에서 호스트 프로파일, 호스트 그룹 및 드라이버를 수정할 수 있습니다.
- WinPE ISO 이름을 수정할 수 있습니다. 하지만 ISO 이미지는 수정할 수 없습니다.

1. 수정할 프로파일을 선택하고 **편집**을 클릭합니다.
2. 상세 정보를 입력하고 **완료**를 클릭합니다.

변경 사항을 보려면 **하이퍼바이저 프로파일** 페이지를 새로 고칩니다.

하이퍼바이저 프로파일 삭제

삭제하고자 하는 하이퍼바이저 프로파일을 선택하고 **삭제**를 클릭합니다.
변경 사항을 보려면 **하이퍼바이저 프로파일** 페이지를 새로 고칩니다.

12

OMIMSSC 콘솔을 통한 디바이스 검색 및 서버 동기화

검색은 지원되는 모듈형 시스템 및 PowerEdge 베어 메탈 서버 또는 호스트 서버 또는 노드를 OMIMSSC로 추가하는 프로세스입니다.

MSSC 콘솔과의 동기화는 등록된 Microsoft 콘솔(MECM 또는 SCVMM)에서 호스트 서버를 OMIMSSC로 추가하는 프로세스입니다. 따라서 이러한 프로세스 중의 하나를 사용하여 디바이스를 OMIMSSC에 추가할 수 있습니다. 디바이스를 검색한 후에만 OMIMSSC에서 관리할 수 있습니다.

주제:

OMIMSSC에서 디바이스 검색 OMIMSSC

OMIMSSC에서 MX7000 모듈형 시스템, 호스트 및 할당되지 않은 서버를 검색합니다. 검색된 디바이스에 대한 정보는 OMIMSSC 어플라이언스에 저장됩니다.

다음과 같은 방법으로 iDRAC IP 주소를 사용하여 Dell EMC 서버를 검색할 수 있습니다.

- 자동 검색을 사용하여 서버 검색
- 수동 검색을 사용하여 서버 검색

노트: OMIMSSC에서 작동하는 데 필요한 지원되는 LC 펌웨어, iDRAC 및 BIOS 버전이 검색된 디바이스에 포함된 경우 해당 디바이스는 하드웨어 호환으로 표시됩니다. 지원되는 버전에 대한 자세한 내용은 Microsoft System Center용 OpenManage Integration 릴리스 노트를 참조하십시오.

수동 검색을 사용하여 모듈형 시스템 검색 방법을 사용하여 디바이스 IP 주소로 모듈형 시스템을 검색합니다.

MECM용 OMIMSSC 콘솔 확장 프로그램에서 디바이스 검색

MECM용 OMIMSSC 콘솔 확장 프로그램에서 디바이스를 검색합니다. 서버를 검색한 후 검색된 서버는 OMIMSSC의 미리 정의된 그룹과 MECM에서 미리 정의된 그룹 또는 컬렉션(**디바이스 컬렉션** 아래의 **모든 Dell Lifecycle Controller 서버 컬렉션** 및 **Dell 서버 가져오기 컬렉션**) 중 하나에 추가됩니다.

검색된 서버가 MECM에 없거나 미리 정의된 그룹 또는 컬렉션이 MECM에 없는 경우 미리 정의된 컬렉션이 생성되고 검색된 서버가 해당 그룹에 추가됩니다.

SCVMM용 OMIMSSC 콘솔 확장 프로그램에서 디바이스 검색

SCVMM용 OMIMSSC 콘솔 확장 프로그램에서 모듈형 시스템, Hyper-V 호스트 및 할당되지 않은 서버를 검색합니다. 검색된 디바이스는 해당되는 미리 정의된 업데이트 그룹에 추가됩니다.

디바이스 검색을 위한 사전 요구 사항

관리형 시스템은 OMIMSSC를 통해 관리되는 디바이스입니다. OMIMSSC 콘솔 확장 프로그램을 사용한 서버 검색에 대한 시스템 요구 사항은 다음과 같습니다.

- OMIMSSC MECM용 콘솔 확장 프로그램은 12세대 이상 서버에서 모듈형, 모놀리식 및 타워 서버 모델을 지원합니다.
- OMIMSSC SCVMM용 콘솔 확장 프로그램은 12세대 이상 서버에서 모듈형 및 모놀리식 서버 모델을 지원합니다.

- 소스 구성 및 대상 구성의 경우 동일한 유형의 디스크, 즉 솔리드 스테이트 드라이브(SSD), SAS 또는 직렬 ATA(SATA) 드라이브만 사용합니다.
- 성공적인 하드웨어 프로파일 RAID 클론 생성을 위해, 대상 시스템 디스크의 경우 소스에 있는 것과 같거나 큰 크기와 개수의 디스크를 사용합니다.
- RAID 슬라이스된 가상 디스크는 지원되지 않습니다.
- 공유 LOM이 있는 iDRAC는 지원되지 않습니다.
- 외장 컨트롤러에 구성된 RAID는 지원되지 않습니다.
- 관리형 시스템에서 Collect System Inventory on Restart(CSIOR)를 설정합니다. 자세한 내용은 iDRAC 설명서를 참조하십시오.

자동 검색을 사용한 서버 검색

서버를 자동으로 검색하려면 서버를 네트워크에 연결하고 서버의 전원을 켭니다. OMIMSSC는 iDRAC의 원격 지원 기능을 사용하여 할당 해제된 서버를 자동으로 검색합니다. OMIMSSC는 프로비저닝 서버로 작동하며 iDRAC 참조를 사용하여 서버를 자동 검색합니다.

1. OMIMSSC에서 iDRAC 자격 증명을 제공하고 서버에 대한 기본값으로 설정하여 디바이스 유형 자격 증명 프로파일을 생성합니다. 자격 증명 프로파일 생성에 대한 자세한 내용은 자격 증명 프로파일 생성을 참조하십시오.
2. 관리형 디바이스의 iDRAC 설정에서 기존 관리자 계정을 비활성화합니다.

   노트: 자동 검색에 실패할 경우 운영자 권한이 있는 게스트 사용자 계정을 사용하여 iDRAC에 로그인하고 강력한 암호를 설정하는 것이 좋습니다.

3. 관리형 디바이스의 iDRAC 설정에서 자동 검색 기능을 활성화합니다. 자세한 내용은 iDRAC 설명서를 참조하십시오.
4. 관리형 디바이스의 iDRAC 설정에서 OMIMSSC 어플라이언스 IP를 **프로비저닝 서버 IP**에 입력한 다음 서버를 재시작합니다.

수동 검색을 사용한 서버 검색

IP 주소 또는 IP 범위를 사용하여 PowerEdge 서버를 수동으로 검색합니다. 서버를 검색하려면 서버의 디바이스 유형 자격 증명과 iDRAC IP 주소를 제공합니다. IP 범위를 사용하여 서버를 검색하는 경우에는 시작 및 끝 범위와 서버의 디바이스 유형 자격 증명을 포함시켜 서브넷 내의 IP(IPv4) 범위를 지정합니다.

기본 자격 증명 프로파일을 사용할 수 있는지 확인합니다.

1. OMIMSSC 콘솔에서 다음 단계 중 하나를 수행합니다.
   - 대시보드에서 **서버 검색**을 클릭합니다.
   - 탐색 창에서 **구성 및 배포**, **서버 보기**, **검색**을 차례로 클릭합니다.
2. **검색**을 클릭합니다.
3. **검색** 페이지에서 필요한 옵션을 선택합니다.
   - **IP 주소 사용 검색** - IP 주소를 사용하여 서버를 검색합니다.
   - **IP 범위 사용 검색** - IP 범위 내의 모든 서버를 검색합니다.
4. 디바이스 유형 자격 증명 프로파일을 생성하려면 디바이스 유형 자격 증명 프로파일을 선택하거나 **새로 생성**을 클릭합니다.

   선택한 프로파일이 모든 서버에 적용됩니다.
5. **iDRAC IP 주소**에 검색할 서버의 IP 주소를 제공합니다.
6. **IP 주소 또는 IP 주소 범위 사용 검색**에서 다음 중 하나를 수행합니다.
   - **IP 주소 시작 범위** 및 **IP 주소 종료 범위**에서 포함하려는 IP 주소 범위를 입력합니다. 여기에는 시작 및 종료 범위가 포함됩니다.
   - IP 주소 범위를 제외하려는 경우 **범위 제외 활성화**를 선택하고 **IP 주소 시작 범위** 및 **IP 주소 종료 범위**에서 제외할 범위를 입력합니다.
7. 고유 작업 이름과 작업에 대한 설명을 입력한 다음 **마침**을 클릭합니다.

   이 작업을 추적하기 위해 기본적으로 **작업 목록으로 이동** 옵션이 선택되어 있습니다.

   작업 및 로그 센터 페이지가 표시됩니다. 검색 작업을 확장하여 **실행 중** 탭에서 작업의 진행 상황을 확인할 수 있습니다.

서버를 검색한 후 **구성 및 배포** 섹션의 **서버 보기** 페이지에 있는 **호스트** 탭 또는 **할당되지 않음** 탭에 서버가 추가됩니다.

- 운영 체제가 배포된 서버가 검색되고 MECM 또는 SCVMM 콘솔에 해당 서버가 이미 있는 경우 이 서버는 **호스트** 탭 아래에 호스트 서버로 나열됩니다.
- MECM 또는 SCVMM에 나열되지 않은 PowerEdge 서버를 검색했을 때 해당 서버가 단일 OMIMSSC 어플라이언스에 등록된 여러 Microsoft 콘솔의 경우 해당 서버는 모든 OMIMSSC 콘솔 확장 프로그램의 **할당되지 않음** 탭 아래에 할당되지 않은 서버로 나열됩니다.

서버를 검색한 후 OMIMSSC에서 작동하도록 지원되는 LC 펌웨어, iDRAC 및 BIOS 버전이 서버에 포함된 경우 서버는 하드웨어 호환으로 표시됩니다. 서버 구성 요소의 펌웨어 버전을 보려면 서버 행에 대한 **하드웨어 호환성** 열 위에 마우스를 올려 놓습니다. 지원되는 버전에 대한 자세한 내용은 Microsoft System Center용 OpenManage Integration 릴리스 노트를 참조하십시오.

검색된 각 서버에 대해 라이선스가 사용됩니다. **라이선스 센터** 페이지의 **라이선스 노드** 수는 검색되는 서버 수에 따라 감소합니다.

노트: 이전 버전의 OMIMSSC 어플라이언스에서 검색된 서버를 사용하려면 해당 서버를 다시 검색합니다.

노트: 위임된 관리자로 OMIMSSC에 로그인한 경우 로그인한 사용자에게 고유하지 않은 모든 호스트 서버와 할당되지 않은 서버를 볼 수 있습니다. 따라서 이러한 서버에서는 어떠한 작업도 수행할 수 없습니다. 이러한 서버에서 작업을 수행하기 전에 필요한 권한이 있는지 확인합니다.

수동 검색을 이용한 모듈형 시스템 MX7000 검색

IP 주소 또는 IP 범위를 사용하여 PowerEdge MX7000 모듈형 시스템을 수동으로 검색하려면 모듈형 시스템의 IP 주소 및 디바이스 유형 자격 증명을 입력합니다. IP 범위를 사용하여 모듈식 시스템을 검색하는 경우 시작 범위와 종료 범위 및 모듈형 시스템의 디바이스 유형 자격 증명을 포함하여 서브넷 내의 IP(IPv4) 범위를 지정합니다.

검색할 모듈형 시스템의 기본 자격 증명 프로파일을 사용할 수 있는지 확인합니다.

모듈형 시스템을 검색하려면 다음을 수행합니다.

1. OMIMSSC에서 **구성 및 배포**, **모듈형 시스템 보기**를 차례로 클릭한 후 **검색**을 클릭합니다.
2. **검색**을 클릭합니다.
3. **검색** 페이지에서 필요한 옵션을 선택합니다.
   - **IP 주소 사용 검색** - IP 주소를 사용하여 모듈형 시스템을 검색합니다.
   - **IP 범위 사용 검색** - IP 범위 내의 모든 모듈형 시스템을 검색합니다.
4. 디바이스 유형 자격 증명 프로파일을 생성하려면 디바이스 유형 자격 증명 프로파일을 선택하거나 **새로 생성**을 클릭합니다.
   선택한 프로파일이 모든 서버에 적용됩니다.
5. **IP 주소**에 검색할 모듈형 시스템의 IP 주소를 입력합니다.
6. **IP 주소 또는 IP 주소 범위 사용 검색**에서 다음 중 하나를 수행합니다.
   - **IP 주소 시작 범위** 및 **IP 주소 종료 범위**에서 포함하려는 IP 주소 범위를 입력합니다. 여기에는 시작 및 종료 범위가 포함됩니다.
   - IP 주소 범위를 제외하려는 경우 **범위 제외 활성화**를 선택하고 **IP 주소 시작 범위** 및 **IP 주소 종료 범위**에서 제외할 범위를 입력합니다.
7. **모듈형 시스템 검색 방법**에서 다음 중 하나를 선택합니다.
   - **단순 검색** - 모듈형 시스템과 모듈형 시스템의 서버 수를 검색합니다.
   - **심층 검색** - I/O 모듈(IOM) 및 스토리지 디바이스와 같은 모듈형 시스템에 있는 디바이스 및 모듈형 시스템을 검색합니다.
     노트: MX7000 및 해당 구성 요소를 심층 검색하려면 PowerEdge MX7000 및 모든 구성 요소에 IPv4 주소가 활성화되어 있어야 합니다.
8. 고유 작업 이름을 입력한 다음 **마침**을 클릭합니다.
   이 작업을 추적하기 위해 기본적으로 **작업 목록으로 이동** 옵션이 선택되어 있습니다.
   실행 중 탭에서 작업의 진행률을 보려면 **작업 및 로그 센터**에서 검색 작업을 확장합니다.

등록된 MECM과 OMIMSSC 콘솔 확장 프로그램의 동기화

등록된 MECM에서 OMIMSSC로 모든 서버(호스트 및 할당 해제된 서버)를 동기화할 수 있습니다. 또한 동기화 후에 서버에 대한 최신 펌웨어 인벤토리 정보를 얻을 수 있습니다.

OMIMSSC와 등록된 MECM 콘솔을 동기화하기 전에 다음 요구 사항이 충족되는지 확인하십시오.

- 서버에 대한 기본 iDRAC 자격 증명 프로파일에 대한 상세 정보가 있습니다.
- MECM과 OMIMSSC를 동기화하기 전에 **Dell 기본 컬렉션**을 업데이트합니다. 그러나 할당 해제된 서버가 MECM에서 검색되는 경우에는 해당 서버는 **가져온 Dell 서버 컬렉션**에 추가됩니다. **Dell 기본 컬렉션**에 이 서버를 추가하려면 **OOB** 페이지에서 서버의 iDRAC IP 주소를 추가합니다.
- MECM에 중복된 디바이스 항목이 없는지 확인합니다.

OMIMSSC를 SCCM과 동기화한 후에 디바이스가 SCCM에 없는 경우에는 **디바이스 컬렉션** 아래에 **모든 Dell Lifecycle Controller 서버** 컬렉션과 **Dell 서버 가져오기** 컬렉션이 생성되고 서버가 각 그룹에 추가됩니다.

등록된 SCVMM과 OMIMSSC 콘솔 확장 프로그램의 동기화

SCVMM 콘솔에서 모든 Hyper-V 호스트, Hyper-V 호스트 클러스터, 모듈형 Hyper-V 호스트 그리고 할당 해제된 서버를 SCVMM용 OMIMSSC 콘솔 확장 프로그램과 동기화할 수 있습니다. 또한 동기화 후에 서버에 대한 최신 펌웨어 인벤토리 정보를 얻을 수 있습니다.

OMIMSSC를 SCVMM과 동기화하기 전에 다음 사항을 고려하십시오.

- 서버에 대한 기본 iDRAC 자격 증명 프로파일에 대한 상세 정보가 있습니다.
- iDRAC IP 주소로 호스트 서버의 BMC(Baseboard Management Controller)를 구성하지 않은 경우에는 호스트 서버를 OMIMSSC와 동기화할 수 없습니다. 따라서 SCVMM에서 BMC를 구성하고(자세한 내용은 `technet.microsoft.com`의 MSDN 기사 참조) OMIMSSC를 SCVMM과 동기화할 수 있습니다.
- SCVMM은 해당 환경에서 여러 호스트를 지원하기 때문에 동기화에 많은 시간이 걸립니다.

등록된 Microsoft 콘솔과 동기화

Microsoft 콘솔에서 관리하는 서버를 OMIMSSC에 추가하려면 다음을 수행합니다.

1. OMIMSSC에서 **구성 및 배포**, **서버 보기**, **OMIMSSC와 동기화**를 차례로 클릭하여 등록된 MSSC에 나열된 모든 호스트를 OMIMSSC 어플라이언스와 동기화합니다.
2. 등록된 MSSC에 나열된 모든 호스트를 어플라이언스와 동기화하려면 **OMIMSSC와 동기화**를 클릭합니다.
   동기화는 시간이 많이 걸리는 작업입니다. **작업 및 로그** 페이지에서 작업 상태를 봅니다.

동기화 오류 해결

OMIMSSC와 동기화되지 않은 서버가 해당 iDRAC IP 주소 및 호스트 이름과 함께 나열됩니다.

노트: 유효하지 않은 자격 증명, iDRAC IP 주소, 연결 또는 기타 문제로 인해 동기화되지 않은 모든 서버는 먼저 문제를 해결한 다음 동기화해야 합니다.

노트: 재동기화 중에는 등록된 MSSC 환경에서 삭제된 호스트 서버가 OMIMSSC 콘솔 확장 프로그램의 **할당 해제된 서버** 탭으로 이동됩니다. 서버가 사용 중지된 경우 할당 해제된 서버 목록에서 해당 서버를 제거합니다.

자격 증명 프로파일 문제가 있는 서버를 재동기화하는 방법:

1. OMIMSSC에서 **구성 및 배포**, **서버 보기**, **동기화 오류 해결**을 차례로 클릭합니다.
2. **동기화 오류 해결**을 클릭합니다.
3. 재동기화할 서버를 선택하고 자격 증명 프로파일을 선택하거나 자격 증명 프로파일을 생성하려면 **새로 만들기**를 클릭합니다.
4. 작업이 제출된 후 자동으로 작업 상태를 보려면 작업 이름을 입력하고 필요하면 **작업 목록으로 이동** 옵션을 선택합니다.
5. 작업을 제출하려면 **완료**를 클릭합니다.

시스템 잠금 모드 보기

시스템 잠금 모드 설정은 14세대 이상의 서버용 iDRAC에서 사용할 수 있습니다. 설정을 켜면 펌웨어 업데이트를 포함하여 시스템 구성이 잠깁니다. 시스템 잠금 모드를 활성화한 후에는 사용자가 구성 설정을 변경할 수 없습니다. 이 설정은 의도하지 않은 변경으로부터 시스템을 보호하기 위해 사용됩니다. 관리형 서버에서 작업을 수행하려면 해당 서버의 iDRAC 콘솔에서 설정을 비활성화해야 합니다. OMIMSSC 콘솔에서 시스템 잠금 모드 상태는 서버의 iDRAC IP 주소 앞에 잠금 이미지로 표시됩니다.

1. 해당 시스템에서 설정을 활성화하면 서버의 iDRAC IP와 함께 잠금 이미지가 표시됩니다.
2. 해당 시스템에서 설정을 비활성화하면 잠금이 해제된 이미지가 서버의 iDRAC IP와 함께 표시됩니다.

노트: OMIMSSC 콘솔 확장 프로그램을 실행하기 전에 관리형 서버에서 iDRAC 시스템 잠금 모드 설정을 확인합니다.

iDRAC 시스템 잠금 모드에 대한 자세한 내용은 `dell.com/support`에서 제공되는 iDRAC 설명서를 참조하십시오.

13

디바이스 제거 OMIMSSC

나열된 서버 중 더 이상 관리할 필요가 없는 서버는 관리 대상 서버 목록에서 제거할 수 있습니다. 시스템 센터에서 서버를 관리에서 제거하면 OMIMSSC 어플라이언스에서 동일한 서버를 제거할 수 있습니다.

서버를 제거하려면 다음을 수행합니다.

서버를 제거하기 전에 다음 사항을 고려합니다.

- 서버를 제거하면 사용된 라이선스는 무시됩니다.
- 다음 기준에 따라 OMIMSSC에 나열된 서버를 제거할 수 있습니다.
  - **할당되지 않은 서버** 탭에 나열된 할당되지 않은 서버.
  - 등록된 MECM 또는 SCVMM에 프로비저닝되어 있고 **호스트** 탭의 OMIMSSC에 있는 호스트 서버를 제거할 경우 먼저 MECM 또는 SCVMM에서 서버를 제거한 다음 OMIMSSC에서 서버를 제거합니다.

1. OMIMSSC 콘솔에서 **구성 및 배포**를 클릭한 다음 **서버 보기**를 클릭합니다.
   - 할당되지 않은 서버를 삭제하려면 **할당되지 않은 서버** 탭에서 서버를 선택하고 **삭제**를 클릭합니다.
   - 호스트 서버를 삭제하려면 **호스트 서버** 탭에서 서버를 선택하고 **삭제**를 클릭합니다.
2. 확인 대화 상자에서 **예**를 클릭합니다.

주제:

- OMIMSSC에서 모듈형 시스템 제거 OMIMSSC

OMIMSSC에서 모듈형 시스템 제거 OMIMSSC

모듈형 시스템을 삭제하려면 다음을 수행합니다.

1. OMIMSSC 콘솔에서 **구성 및 배포**를 클릭한 다음 **모듈형 시스템 보기**를 클릭합니다.
2. 모듈형 시스템을 선택하고 **삭제**를 클릭합니다.

14

OMIMSSC에서 보기

구성 및 배포 페이지의 OMIMSSC에서 검색된 모든 디바이스를 하드웨어 및 펌웨어 인벤토리 정보와 함께 봅니다. 또한 **작업 및 로그 센터** 페이지에서 모든 작업과 상태를 봅니다.

주제:

서버 보기

서버 보기 페이지에는 **할당되지 않은 서버** 및 **호스트** 탭 아래의 OMIMSSC에서 검색되는 모든 호스트 서버와 할당되지 않은 서버가 나열됩니다.

할당되지 않은 서버 탭에서 iDRAC IP 주소, 서비스 태그, 모델, 세대, 프로세서 속도, 서버 메모리, 할당된 작동 템플릿에 대한 템플릿 준수 상태, 모듈형 서버인 경우 모듈형 시스템의 서비스 태그 및 하드웨어 호환성 정보를 봅니다. **하드웨어 호환성** 열 위로 마우스 포인터를 이동하면 해당 디바이스의 BIOS, iDRAC, LC 및 드라이버 팩 버전을 볼 수 있습니다. 하드웨어 호환성에 대한 자세한 내용은 펌웨어 업데이트 정보를 참조하십시오.

호스트 탭에서 호스트 이름, iDRAC IP 주소, 서비스 태그, 모델, 세대, 프로세서 속도, 서버 메모리, 모듈형 시스템의 서비스 태그가 모듈형 서버인 경우, 클러스터의 FQDN(Fully Qualified Domain Name), 서버가 클러스터에 포함된 경우, 할당된 작동 템플릿에 대한 템플릿 준수 상태 및 하드웨어 호환성 정보를 봅니다. **하드웨어 호환성** 열 위로 마우스 포인터를 이동하면 해당 디바이스의 BIOS, iDRAC, LC 및 드라이버 팩 버전을 볼 수 있습니다. 하드웨어 호환성에 대한 자세한 내용은 펌웨어 업데이트 정보를 참조하십시오.

서버 보기 페이지에서 다음 작업을 수행할 수 있습니다.

- 서버 검색
- 페이지를 새로 고쳐 업데이트된 정보를 봅니다.
- OMIMSSC에서 서버를 삭제합니다.
- 등록된 Microsoft 콘솔과 동기화합니다.
- 동기화 오류를 해결합니다.
- 작동 템플릿 할당하고 작동 템플릿 규정 준수를 실행합니다.
- 운영 템플릿을 배포합니다.
- 서버를 클러스터 그룹 및 서버가 속한 모듈형 시스템과 상호 연관합니다.
- iDRAC 콘솔 실행

서버를 보려면 다음을 수행합니다.

1. OMIMSSC 콘솔 확장 프로그램에서 **구성 및 배포**를 클릭한 다음 **서버 보기**를 클릭합니다.
2. **구성 및 배포**를 확장하고 **서버 보기**를 클릭합니다.
3. 베어 메탈 서버를 보려면 **할당되지 않은 서버** 탭을 클릭합니다.
4. 호스트 서버를 보려면 **호스트** 탭을 클릭합니다.
   a. MECM 또는 SCVMM에 그룹화되어 있는 중첩된 형식의 호스트 그룹을 보려면 **콘솔 호스트 선택** 드롭다운 메뉴를 클릭합니다.

   콘솔 호스트 선택 드롭다운 메뉴에는 MECM에 있는 내부 그룹 이름과 모든 호스트 그룹이 나열됩니다. 내부 그룹 이름을 선택하면 MECM과 OMIMSSC에서 검색하고 관리하는 모든 호스트가 표시됩니다.

서버를 검색한 후 다음 사항을 고려합니다.

- 서버를 검색한 후에 **운영 템플릿** 열이 **할당되지 않음**으로 표시됩니다. 펌웨어를 업데이트하고 이러한 서버에 운영 체제를 배포하려면 작동 템플릿을 지정 및 배포합니다. 자세한 내용은 작동 템플릿 관리를 참조하십시오.
- 서버를 검색한 후에 **운영 템플릿** 열이 **할당되지 않음**으로 표시됩니다. 펌웨어를 업데이트하고 이러한 서버에 운영 체제를 배포하려면 작동 템플릿을 지정 및 배포합니다. 자세한 내용은 서버에 대한 작동 템플릿 할당 및 서버에 대한 작동 템플릿 배포를 참조하십시오.

- 검색된 서버는 OMIMSSC의 사전 정의된 그룹에 추가됩니다. 기능 요구 사항에 따라 맞춤 구성 업데이트 그룹을 만들 수 있습니다. 자세한 내용은 업데이트 그룹 정보를 참조하십시오.
- 검색된 서버는 OMIMSSC의 사전 정의된 그룹에 추가됩니다. 기능 요구 사항에 따라 맞춤 구성 업데이트 그룹을 만들 수 있습니다. 자세한 내용은 업데이트 그룹을 참조하십시오.
- 위임된 관리자로 OMIMSSC에 로그인하면 이 사용자와 관련되지 않은 모든 호스트와 할당되지 않은 서버를 볼 수 있습니다. 따라서 서버에 대한 작업을 수행하기 전에 필요한 권한이 있는지 확인하십시오.
- OMIMSSC에 등록된 Microsoft 콘솔이 여러 개 있는 경우 호스트 서버는 관리되는 Microsoft 콘솔에 특화되어 있습니다. 또한 할당되지 않은 서버는 모든 콘솔에 공통됩니다.

iDRAC 콘솔

iDRAC 콘솔을 실행하려면 다음 단계를 수행합니다.

OMIMSSC에서 **구성 및 배포**를 확장하고 다음 중 하나를 선택합니다.**구성 및 배포**를 확장하고 다음 중 하나를 선택합니다.

- **서버 보기**를 클릭합니다. 서버(호스트 또는 할당 해제된 서버인 경우)를 기준으로 **할당 해제된 서버** 또는 **호스트** 탭을 클릭하고 서버의 **iDRAC IP** 주소를 클릭합니다.

  기본적으로 **할당 해제된 서버** 탭이 표시됩니다.

  호스트 탭을 보려면 **호스트**를 클릭합니다.
- **클러스터 보기**를 클릭합니다. 클러스터 유형을 확장하고 클러스터 그룹을 서버 수준으로 확장합니다.

  서버 탭이 표시됩니다.

모듈형 시스템 보기

모듈형 시스템 보기 페이지에는 OMIMSSC에서 검색되는 모든 모듈형 시스템이 나열됩니다.

할당된 작동 템플릿, 서버 수, 입출력(I/O) 모듈, 모듈형 시스템에 있는 스토리지 디바이스 등에 대한 모듈형 시스템의 CMC IP 주소, 서비스 태그, 모델, 펌웨어 버전, 템플릿 준수 상태를 확인합니다. 작동 템플릿을 배포하여 하드웨어를 구성하고 모듈형 시스템 펌웨어를 업데이트합니다.

모듈형 시스템 보기 페이지에서 다음 작업을 수행할 수 있습니다.

- 수동 검색을 사용하여 모듈형 시스템 검색
- 모듈형 시스템 삭제
- 최신 인벤토리 정보를 보려면 페이지를 새로 고칩니다.
- 모듈형 시스템에 대한 작동 템플릿 할당
- 모듈형 시스템에 대한 작동 템플릿 배포
- I/O 모듈 보기
- I/O 모듈 실행

OMIMSSC에서 검색된 모듈형 시스템을 보려면 다음을 수행합니다.

1. OMIMSSC에서 **구성 및 배포**를 클릭한 다음 **모듈형 시스템 보기**를 클릭합니다.
   검색된 모든 모듈형 시스템 모델 이름이 표시됩니다.
2. 특정 모듈형 시스템을 보려면 **모듈형 시스템 보기** 아래에서 모델 이름을 클릭합니다.
   해당 모델의 모든 모듈형 시스템이 서비스 태그와 함께 표시됩니다.
3. 모듈형 시스템에 있는 모든 디바이스를 보려면 서비스 태그를 클릭합니다.
   모든 서버, I/O 모듈 및 스토리지 디바이스가 상세 정보와 함께 표시됩니다.

   노트: 반드시 모듈형 시스템을 세부적으로 검색한 이후에 모듈형 시스템의 모든 디바이스와 해당 정보가 표시됩니다.

   - 기본적으로 **서버** 탭이 표시됩니다.

     이 모듈형 시스템에서 검색되는 모든 서버가 표시됩니다.
   - 모듈형 시스템에 있는 모든 I/O 모듈을 보려면 **I/O 모듈** 탭을 클릭합니다.
   - 모듈형 시스템에 있는 모든 스토리지 디바이스를 보려면 **스토리지 디바이스** 탭을 클릭합니다.

모듈형 시스템을 검색한 후 다음 사항을 고려합니다.

- 모듈형 시스템을 검색한 후에 **운영 템플릿** 열이 **할당되지 않음**으로 표시됩니다. 모듈형 시스템에서 펌웨어를 업데이트하고 운영 체제를 배포하려면 작동 템플릿을 할당 및 배포합니다. 자세한 내용은 작동 템플릿 관리를 참조하십시오.

- 서버를 검색한 후에 **운영 템플릿** 열이 **할당되지 않음**으로 표시됩니다. 모듈형 시스템에서 펌웨어를 업데이트하고 운영 체제를 배포하려면 작동 템플릿을 할당 및 배포합니다. 자세한 내용은 모듈형 시스템에 대한 작동 템플릿 할당 및 모듈형 시스템에 대한 작동 템플릿 배포를 참조하십시오.
- 부분 검색 후 모듈형 시스템에 있는 입/출력, 스토리지 디바이스 및 서버 수를 확인합니다. 심층 검색을 수행하여 모듈형 시스템의 구성 요소에 대한 상세 정보를 확인합니다.

OpenManage Enterprise 모듈형 콘솔

OpenManage Enterprise 모듈형 콘솔을 실행하려면 다음을 수행합니다.

1. OMIMSSC에서 **구성 및 배포**를 확장하고 **모듈형 시스템**을 클릭합니다.
2. 모듈형 시스템의 **디바이스 IP**를 클릭합니다.

입출력(I/O) 모듈

모든 네트워크 입출력(I/O) 모듈이 해당 IP 주소, 서비스 태그, 입출력 유형, 모델, 펌웨어 버전 및 슬롯 정보와 함께 표시됩니다.

입출력(I/O) 모듈 페이지에서 I/O 모듈 콘솔을 실행합니다.

입출력(I/O) 모듈에 대한 정보를 보려면 다음 단계를 수행합니다.

1. OMIMSSC에서 **구성 및 배포**를 클릭한 다음 **모듈식 시스템 보기**를 클릭합니다. **모듈식 시스템 보기**를 확장하고 서비스 태그를 클릭합니다.
   해당 모델의 모든 서비스 태그가 표시됩니다.
2. 모듈식 시스템 모델을 클릭하여 아래에 나열된 디바이스를 확장합니다. 특정 모듈식 시스템을 보려면 서비스 태그를 클릭합니다.
3. 입출력(I/O) 모듈을 보려면 **I/O 모듈** 탭을 클릭합니다.

입출력 모듈 콘솔

입출력(I/O) 모듈 콘솔을 실행하려면 다음 단계를 수행합니다.

1. OMIMSSC에서 **구성 및 배포**를 확장하고 **모듈형 시스템 보기**를 클릭합니다. 모델을 개별 디바이스 수준으로 확장합니다.
   해당 모델 아래의 모든 디바이스가 표시됩니다.
2. **I/O 모듈** 탭을 클릭합니다.
3. 디바이스의 **IP 주소**를 클릭합니다.

클러스터 보기

클러스터 보기 페이지에는 OMIMSSC에서 검색되는 모든 클러스터가 나열됩니다. 클러스터의 정규화된 이름(FQDN), 서비스 태그 및 해당 클러스터에 있는 서버 수를 확인할 수 있습니다. 또한 클러스터에 대한 논리 스위치를 생성한 다음 미리 정의된 작동 템플릿을 사용하여 Windows 서버 HCI 클러스터를 생성합니다.

클러스터 보기 페이지에서 다음 작업을 수행할 수 있습니다.

- 논리 스위치 생성(SCVMM 2016 및 2019 사용자만 해당)
- Windows 서버 HCI 클러스터 생성(SCVMM 2016 및 2019 사용자만 해당)
- iDRAC 콘솔 실행
- 검색된 최신 클러스터를 보려면 페이지를 새로 고치십시오.

OMIMSSC에서 검색된 클러스터 그룹을 보려면 다음을 수행합니다.

1. OMIMSSC에서 **구성 및 배포**를 클릭한 다음 **클러스터 보기**를 클릭합니다.
   다양한 유형의 클러스터가 모두 그룹화되어 나열됩니다.
2. 특정 유형의 클러스터에 대한 정보를 보려면 클러스터 유형을 확장합니다.
   이 유형의 모든 클러스터가 왼쪽 창에 나열됩니다.
3. 클러스터에 있는 서버를 보려면 클러스터 이름을 클릭합니다.

유지 보수 센터 보기

유지 보수 센터 페이지에는 그룹에서 검색된 모든 디바이스와 OMIMSSC에서 디바이스를 유지 보수하는 데 필요한 리소스가 나열되어 있습니다. **유지 보수 센터** 페이지에서 Windows 서버 HCI 클러스터 그룹을 보려면 **업데이트 그룹** 드롭다운 메뉴에서 **모든 업데이트 그룹**을 선택했는지 확인합니다. 디바이스의 펌웨어 인벤토리를 확인하고, 권장 사항에 따라 펌웨어를 최신 상태로 유지하여 디바이스를 관리하고, 오류가 발생한 경우 서버를 이전 상태로 되돌리고, 교체된 구성 요소를 이전 구성 요소와 동일한 구성으로 설정하고, 문제 해결을 위해 서버 로그를 내보냅니다. **업데이트 설정** 페이지에서 모든 업데이트 소스, 기본 업데이트 소스의 최신 업데이트 폴링 및 알림, 유사한 관리가 필요한 디바이스 그룹 업데이트, 서버 구성에 필요한 모든 보호 볼트를 볼 수 있습니다.

노트: 기본적으로 OMIMSSC는 미리 정의된 HTTPS 업데이트 소스에 대한 비교 보고서의 이전 버전을 표시하는 카탈로그 파일과 함께 패키지로 포함되어 있습니다. 따라서 최신 비교 보고서를 표시하려면 최신 카탈로그를 다운로드하십시오. 최신 카탈로그를 다운로드하려면 HTTPS 업데이트 소스를 편집하고 저장합니다.

노트: 선택한 업데이트 소스 카탈로그에 업데이트가 없는 경우 디바이스의 특정 구성 요소의 기준 버전은 사용할 수 없음으로 표시됩니다.

유지 보수 센터 페이지에서 다음 작업을 수행할 수 있습니다.

- 업데이트 소스 생성
- 폴링 주파수 설정
- 미리 정의된 업데이트 그룹을 선택하거나 사용자 지정 업데이트 그룹을 생성합니다.
- 펌웨어 인벤토리 보기 및 새로 고침
- 업데이트 실행 메서드를 사용하여 펌웨어 버전 업그레이드 및 다운그레이드
- 보호 볼트 생성
- 서버 프로파일 내보내기
- 서버 프로파일 가져오기
- 인벤토리 내보내기

유지 보수 센터 페이지를 보려면 다음을 수행합니다.

OMIMSSC에서 **유지 보수 센터**를 클릭합니다.
유지 보수 센터 페이지가 표시됩니다.

작업 및 로그 센터

OMIMSSC에서 시작된 작업과 작업의 진행 상태, 그리고 하위 작업에 대한 정보를 봅니다. 또한 특정 작업 범주의 작업을 필터링하여 볼 수 있습니다.

OMIMSSC 관리 포털 및 OMIMSSC 콘솔 확장 프로그램에서 OMIMSSC에서 시작된 작업을 볼 수 있습니다.

- OMIMSSC 관리 포털 - 모든 OMIMSSC 콘솔 및 사용자가 시작한 작업을 표시합니다.
- OMIMSSC 콘솔 - 사용자 및 콘솔에 대한 작업을 표시합니다.

작업 이름은 시스템에서 생성되거나 사용자가 제공하며 하위 작업의 이름은 관리형 시스템의 IP 주소 또는 호스트 이름에 따라 작성됩니다. 해당 작업의 활동 로그를 보려면 하위 작업을 확장합니다. 작업은 다음 4개 그룹으로 분류됩니다.

- **실행 중** - 현재 실행 중인 모든 작업과 진행 상태를 표시합니다.
- **내역** - 이전에 실행된 모든 작업과 해당 작업의 상태를 표시합니다.
- **예약됨** - 미래 날짜 및 시간에 대해 예약된 모든 작업을 표시합니다. 예약된 작업을 취소할 수도 있습니다.
- **일반 로그** - 작업 및 기타 활동에 고유하지 않은 OMIMSSC 어플라이언스별 공통 로그 메시지를 표시합니다. 모든 작업은 사용자 이름과 작업을 시작한 콘솔 FQDN과 함께 표시됩니다.
  - **어플라이언스 로그 메시지** - OMIMSSC 어플라이언스 재시작과 같은 모든 OMIMSSC 어플라이언스별 로그 메시지를 표시합니다. OMIMSSC 관리 포털에서만 이 메시지 범주를 볼 수 있습니다.
  - **일반 로그 메시지** - **실행 중**, **내역** 및 **예약됨** 탭에 나열된 여러 작업 범주에 공통적인 모든 로그 메시지를 표시합니다. 이러한 로그는 콘솔 및 사용자에 따라 다릅니다.

    예를 들어 서버 그룹에 대하여 펌웨어 업데이트 작업이 진행 중인 경우에는 해당 작업에 대한 SUU(Server Update Utility) 저장소 생성과 관련된 로그 메시지가 탭에 표시됩니다.

OMIMSSC에 정의된 작업의 다양한 상태는 다음과 같습니다.

- **취소됨** - 작업이 수동으로 취소되거나 OMIMSSC 어플라이언스가 재시작된 후에 취소됩니다.
- **성공** - 작업이 성공적으로 완료되었습니다.
- **실패** - 작업이 실패했습니다.

- **진행 중** - 작업이 실행 중입니다.
- **예약됨** - 작업이 미래 날짜 및 시간에 대하여 예약되었습니다.

  노트: 여러 작업을 동시에 같은 디바이스로 제출하면 작업이 실패합니다. 따라서 같은 디바이스에 대하여 다른 시간에 작업을 예약해야 합니다.
- **대기 중** - 작업이 대기열에 있습니다.
- **반복 일정** - 작업이 일정한 간격으로 예약됩니다.

1. OMIMSSC에서 **작업 및 로그 센터**를 클릭합니다.
2. **예약됨**, **내역** 또는 **일반**과 같은 작업의 특정 범주를 보려면 필요한 탭을 클릭합니다.

   작업을 확장하면 작업에 포함된 모든 디바이스를 볼 수 있습니다. 작업을 더 확장하면 해당 작업에 대한 로그 메시지를 볼 수 있습니다.

   노트: 모든 작업 관련 일반 로그 메시지는 **일반** 탭 아래에 나열되며 **실행 중** 또는 **내역** 탭 아래에는 나열되지 않습니다.
3. (선택 사항) 필터를 적용하여 **상태** 열에서 다양한 작업 그룹과 작업 상태를 확인할 수 있습니다.

15

작동 템플릿 관리하기

작동 템플릿은 완전한 디바이스 구성을 포함하며 Microsoft 환경 내에서 PowerEdge 서버 및 모듈형 시스템에 대한 운영 체제 배포 및 펌웨어 업데이트에 사용됩니다.

작동 템플릿은 운영 체제를 프로비저닝하는 동안 참조 서버(Golden Server)의 하드웨어와 펌웨어를 다른 여러 서버에 복제합니다. 여기에는 펌웨어, 하드웨어 및 운영 체제 구성 요소가 포함되어 있으며 해당 특성이 참조 서버의 현재 값으로 설정됩니다. 이러한 값은 디바이스에 이 템플릿을 적용하기 전에 수정할 수 있습니다. 또한 할당된 작동 템플릿에 대하여 규정 준수 상태를 확인하고 요약 페이지에서 규정 준수 보고서를 볼 수 있습니다.

참조 서버에서 사용할 수 있는 이러한 구성 요소만 검색하여 동적으로 작동 템플릿 구성 요소로 표시됩니다. 예를 들어 서버에 FC 구성 요소가 없는 경우 작동 템플릿에 동일한 구성 요소가 표시되지 않습니다.

참조 서버 및 참조 모듈형 시스템에 대한 자세한 내용은 참조 서버 구성 정보 및 참조 모듈형 시스템 구성 정보를 참조하십시오.

다음 표는 작동 템플릿에 나열된 구성 요소와 각 구성 요소의 보기 및 배포 기능에 대해 설명합니다.

표 9. 작동 템플릿의 기능

구성 요소	구성 배포	펌웨어 업데이트	구성 보기	운영 템플릿 규정 준수 상태
BIOS	예	예	예	예
iDRAC	예	예	예	예
NIC/CNA	예	예	예	예
RAID	예	예	예	예
FC	예	예	예	예
Windows	예	—	아니요	—
RHEL	예	—	아니요	—
ESXI	예	—	아니요	—
관리 모듈	예	예	예	예

주제:

- 사전 정의된 작동 템플릿
- 참조 서버 구성 정보
- 참조 모듈식 시스템 구성 정보
- 참조 서버에서 작동 템플릿 생성
- 참조 모듈형 시스템에서 작동 템플릿 생성
- 작동 템플릿을 이용한 클러스터 생성
- 작동 템플릿 보기
- 작동 템플릿 편집
- 여러 서버에서 운영 템플릿을 사용하여 시스템별 값(풀 값) 구성
- 서버에 대한 작동 템플릿 할당 및 운영 템플릿 규정 준수 실행
- 운영 템플릿 배포
- 작동 템플릿 할당 해제
- 작동 템플릿 삭제

사전 정의된 작동 템플릿

사전 정의된 템플릿에는 Windows 서버 HCI 클러스터 또는 Windows Server 소프트웨어 정의(WSSD)를 생성하는 데 필요한 모든 구성이 있습니다. OMIMSSC는 해당 네트워크 어댑터와 함께 AX-6515, AX-740XD, AX-640, RN740XD, RN740XD2, RN640, Windows 서버 HCI Ready Node 모델에서 클러스터 생성을 지원합니다.

표 10. 사전 정의된 작동 템플릿의 목록

작동 템플릿 이름	설명
AX-6515_QLogic	이 운영 템플릿은 Microsoft Windows Server용 Dell EMC HCI 솔루션(AX-6515 모델)을 위한 것입니다.
AX-6515_Mellanox	이 운영 템플릿은 Microsoft Windows Server용 Dell EMC HCI 솔루션(AX-6515 모델)을 위한 것입니다.
AX-740xd_RN740xd_QLogic	이 운영 템플릿은 Microsoft Windows Server용 Dell EMC HCI 솔루션(AX-740xd 및 RN740xd 모델)을 위한 것입니다.
AX-740xd_RN740xd_Mellanox	이 운영 템플릿은 Microsoft Windows Server용 Dell EMC HCI 솔루션(AX-740xd 및 RN740xd 모델)을 위한 것입니다.
AX-640_RN640_Mellanox	이 운영 템플릿은 Microsoft Windows Server용 Dell EMC HCI 솔루션(AX-640 및 RN640 모델)을 위한 것입니다.
AX-640_RN640_QLogic	이 운영 템플릿은 Microsoft Windows Server용 Dell EMC HCI 솔루션(AX-640 및 RN640 모델)을 위한 것입니다.
RN440_QLogic	이 운영 템플릿은 Microsoft Windows Server용 Dell EMC HCI 솔루션(RN440 모델)을 위한 것입니다.
RN740xd2_Mellanox	이 운영 템플릿은 Microsoft Windows Server용 Dell EMC HCI 솔루션(RN740xd2 모델)을 위한 것입니다.
RN740xd2_QLogic	이 운영 템플릿은 Microsoft Windows Server용 Dell EMC HCI 솔루션(RN740xd2 모델)을 위한 것입니다.

작동 템플릿을 배포하기 전에 다음 사항을 고려하십시오.

- 사전 정의된 템플릿은 SCVMM 2016 및 2019를 실행하는 관리 시스템에만 사용할 수 있습니다.
- 사전 정의된 Windows 서버 HCI 템플릿에서는 슬롯 1에 NIC 카드가 표시됩니다. 하지만 작동 템플릿을 배포하는 동안에 NIC 구성이 올바른 슬롯에 적용됩니다. 또한 디바이스에 여러 개의 NIC 카드가 있는 경우에 모든 NIC 카드는 작동 템플릿에 지정된 것과 동일하게 구성됩니다.

참조 서버 구성 정보

기본 부팅 순서, BIOS, RAID 설정, 하드웨어 구성, 펌웨어 업데이트 속성, 조직에 가장 적합한 운영 체제 매개변수를 포함하는 서버 구성을 참조 서버 구성이라고 합니다.

참조 서버를 검색하고 작동 템플릿에서 참조 서버 설정을 캡처하여 동일한 하드웨어 구성으로 여러 서버에 복제합니다.

참조 모듈식 시스템 구성 정보

조직에 이상적으로 맞는 선호 네트워크 구성, 사용자 계정, 보안 및 알림이 있는 모듈식 시스템 구성을 참조 모듈식 시스템 구성 또는 참조 섀시라고 합니다.

참조 모듈식 시스템을 검색하고 작동 템플릿에서 참조 모듈식 시스템 설정을 캡처한 다음에 동일한 모델의 서로 다른 모듈식 시스템에 걸쳐 복제합니다.

참조 서버에서 작동 템플릿 생성

작동 템플릿을 생성하기 전에 다음 작업을 완료해야 합니다.

- 검색 기능을 사용하여 참조 서버를 검색합니다. 서버 검색에 대한 자세한 내용은 수동 검색을 사용하여 서버 검색을 참조하십시오.
- MECM 사용자의 경우에는 다음을 수행합니다.
  - 작업 시퀀스를 생성합니다. 자세한 내용은 작업 시퀀스 생성을 참조하십시오.
  - 작업 시퀀스를 생성합니다. 자세한 내용은 Microsoft System Center용 OpenManage Integration 통합 사용자 가이드를 참조하십시오.
  - Windows 이외의 운영 체제 배포의 경우에는 디바이스 유형 자격 증명 프로파일이 있어야 합니다. 자세한 내용은 자격 증명 프로파일 생성을 참조하십시오.
- SCVMM 사용자의 경우에는 다음과 같습니다.
  - 하이퍼바이저 프로파일을 생성합니다. 하이퍼바이저 프로파일 생성에 대한 자세한 내용은 하이퍼바이저 프로파일 생성을 참조하십시오.
  - Windows 배포의 경우에는 디바이스 유형 자격 증명 프로파일이 있어야 합니다. 자세한 내용은 자격 증명 프로파일 생성을 참조하십시오.
- 기본 업데이트 소스를 사용하지 않는 경우에는 업데이트 소스를 만듭니다. 자세한 내용은 업데이트 소스 생성을 참조하십시오.

참조 서버의 구성을 캡처하여 작동 템플릿을 생성할 수 있습니다. 구성을 캡처한 후에 템플릿을 직접 저장하거나 요구 사항에 따라 업데이트 소스, 하드웨어 구성 및 Windows 구성 요소의 속성을 편집할 수 있습니다. 이제 PowerEdge 동종 서버에서 사용할 수 있는 템플릿을 저장할 수 있습니다.

1. OMIMSSC에서 다음 중 아무 작업이나 수행하여 작동 템플릿을 엽니다.
   - OMIMSSC 대시보드에서, **운영 템플릿 생성**을 클릭합니다.
   - 탐색 창에서 **프로파일** > **운영 템플릿**을 클릭한 다음에 **생성**을 클릭합니다.

   운영 템플릿 마법사가 표시됩니다.
2. **생성**을 클릭합니다.
   운영 템플릿 마법사가 표시됩니다.
3. 템플릿에 대한 이름과 설명을 입력합니다.
4. 디바이스 유형을 선택하고 참조 디바이스의 IP 주소를 입력한 다음에 다음을 클릭합니다.

   노트: iDRAC 2.0 이상을 사용하여 참조 서버의 구성을 캡처할 수 있습니다.

5. 디바이스 구성 요소에서 사용 가능한 속성과 값을 보려는 구성 요소를 클릭합니다.
   구성 요소는 다음과 같습니다.
   - 펌웨어 업데이트
   - 하드웨어 구성 요소(RAID, NIC 및 BIOS)

     노트: iDRAC 내장형 1 구성 요소에서 다음은 **사용자 관리 권한** 속성에 대한 권한 및 값입니다.

값	권한
1	로그인
2	구성
4	사용자 구성
8	로그
16	시스템 제어
32	가상 콘솔 액세스
64	가상 미디어 액세스
128	시스템 작업
256	디버그
499	작업자 권한

   - 운영 체제 - Windows, ESXi 또는 RHEL 중 하나를 선택합니다.
6. 수평 스크롤 바를 사용하여 구성 요소를 찾습니다. 구성 요소를 선택하고 그룹을 확장한 다음에 속성 값을 편집합니다. 수직 스크롤 바를 사용하여 구성 요소의 속성과 그룹을 편집합니다.
7. 운영 템플릿이 적용될 때 선택한 구성 요소의 구성이 관리형 디바이스에 적용되기 때문에 각 구성 요소에 대하여 확인란을 선택합니다. 그러나 참조 디바이스의 모든 구성은 캡처되어 템플릿에 저장됩니다.

노트: 각 구성 요소에 대하여 확인란에서 선택한 항목에 관계없이 모든 구성이 템플릿에서 캡처됩니다.

노트: 운영 템플릿은 참조 서버에서 검색하는 동안 암호를 캡처하지 않습니다. 배포 전에 선택한 속성의 암호 값을 설정해야 합니다.

운영 체제 구성 요소에서 요구 사항에 따라 다음 옵션 중 하나의 단계를 수행합니다.

- MECM에 대한 Windows 운영 체제 배포의 경우에는 MECM용 OMIMSSC 콘솔 확장에 대한 Windows 구성 요소를 참조하십시오.
- SCVMM에 대한 Windows 운영 체제 배포의 경우에는 SCVMM용 OMIMSSC 콘솔 확장에 대한 Windows 구성 요소를 참조하십시오.
- OMIMSSC
- Windows가 아닌 운영 체제의 배포의 경우에는 OMIMSSC 콘솔 확장에 대한 Windows가 아닌 운영 체제의 구성 요소를 참조하십시오.

8. 프로파일을 저장하려면 **완료**를 클릭합니다.

권장 사항: 참조 서버 iDRAC에 엔터프라이즈 라이선스가 있고 텔레메트리/SCEP 속성이 표시되는 경우 이러한 속성은 데이터 센터 라이선스만 지원하므로 선택 취소해야 합니다.

MECM용 OMIMSSC 콘솔 확장 프로그램에 대한 Windows OS 구성 요소

서버에 대한 작동 템플릿을 생성하거나 편집할 때 Windows 구성 요소에 다음 단계를 수행합니다.

1. 작업 시퀀스 및 배포 방법을 선택합니다.

   노트: 컬렉션에 배포된 작업 시퀀스만 드롭다운 메뉴에 나열됩니다.

   작업 시퀀스에 대한 자세한 내용은 작업 시퀀스를 참조하십시오.

   작업 시퀀스에 대한 자세한 내용은 Microsoft System Center용 OpenManage Integration 통합 사용자 가이드를 참조하십시오.

2. **배포 방법**에 대한 다음 옵션 중 하나를 선택합니다.
   - **네트워크 ISO로 부팅** — 지정된 ISO를 재부팅합니다.
   - **vFlash로 ISO 스테이징 및 재부팅** — ISO를 vFlash로 다운로드하고 재부팅합니다.
   - **vFlash로 재부팅** - vFlash로 재부팅합니다. ISO가 vFlash에 존재하는지 확인합니다.

     노트: vFlash로 재부팅 옵션을 사용하려면 vFlash에 생성된 파티션의 레이블 이름이 **ISOIMG**가 되어야 합니다.

3. (선택 사항) 네트워크 공유에 있는 이미지를 사용하려면 **네트워크 ISO를 장애 복구로 사용** 옵션을 선택합니다.
4. LC 부팅 미디어 이미지 파일을 입력합니다.
5. 운영 체제에 필요한 드라이버를 선택합니다.

노트: AMD 플랫폼에서의 Windows Server 2016 운영 체제 배포는 x2apic을 지원하지 않습니다. 운영 체제를 설치하기 전에 BIOS x2apic 및 논리 프로세서 설정을 비활성화해야 합니다.

SCVMM용 OMIMSSC 콘솔 확장 프로그램에 대한 Windows OS 구성 요소

서버에 대한 작동 템플릿을 생성하거나 편집할 때 Windows 구성 요소에 다음 단계를 수행합니다.

하이퍼바이저 프로파일, **자격 증명 프로파일** 및 **서버 IP 출처**를 선택합니다.

노트: 호스트 이름과 **서버 관리 NIC**는 항상 풀 값입니다. 서버 관리 NIC의 경우 운영 체제가 SCVMM과 통신하려는 네트워크 포트의 MAC 주소를 제공합니다.

서버 IP 출처를 **정적**으로 선택한 경우에는 SCVMM에서 논리 네트워크를 구성했고 다음과 같은 필드가 풀 값인지 확인합니다.

- **콘솔 논리 네트워크**
- **IP 서브넷**
- **정적 IP 주소**

노트: AMD 플랫폼에서의 Windows Server 2016 운영 체제 배포는 x2apic을 지원하지 않습니다. 운영 체제를 설치하기 전에 BIOS x2apic 및 논리 프로세서 설정을 비활성화해야 합니다.

OMIMSSC 콘솔 확장 프로그램을 위한 비 Windows 구성 요소

서버에 대한 작동 템플릿을 생성하거나 편집하는 동안 비 Windows 구성 요소에 대해 다음을 수행합니다.

Windows가 아닌 운영 체제, 운영 체제 버전, 공유 폴더 유형, ISO 파일 이름, ISO 파일 위치 그리고 운영 체제의 루트 계정에 대한 암호를 선택합니다.

(선택 사항) CIFS 공유에 액세스하기 위한 Windows 유형 자격 증명 프로파일을 선택합니다.

호스트 이름은 풀 값이며, DHCP 옵션을 비활성화하면 다음과 같은 필드가 풀 값이 됩니다.

- **IP 주소**
- **서브넷 마스크**
- **기본 게이트웨이**
- **기본 DNS**
- **보조 DNS**

노트: Windows가 아닌 운영 체제 배포 환경에 대해 NFS(Network File System) 및 CIFS(Common Internet File System) 공유 유형이 지원됩니다.

참조 모듈형 시스템에서 작동 템플릿 생성

작동 템플릿을 생성하기 전에 다음 작업을 완료해야 합니다.

- **검색** 기능을 사용하여 모듈형 시스템을 검색합니다. 모듈형 시스템 검색에 대한 자세한 내용은 수동 검색을 사용하여 모듈형 시스템 검색을 참조하십시오.
- 기본 업데이트 소스를 사용하지 않는 경우에는 업데이트 소스를 만듭니다. 자세한 내용은 업데이트 소스 생성을 참조하십시오.

참조 모듈형 시스템의 구성을 캡처하여 작동 템플릿을 생성할 수 있습니다. 구성을 캡처한 후에 템플릿을 직접 저장하거나 요구 사항에 따라 업데이트 소스 및 하드웨어 구성에 대한 속성을 편집할 수 있습니다. 이제 같은 모델의 다른 모듈형 시스템을 구성하는 데 사용할 수 있는 템플릿을 저장할 수 있습니다.

노트: 다른 MX7000 디바이스에 AD(Active Directory) 사용자를 구성하려면 모든 AD 사용자가 구성되는 MX7000 모듈형 시스템에서 작동 템플릿을 생성할 수 있어야 합니다.

노트: 보안상의 이유로 사용자 계정의 암호는 참조 모듈형 시스템으로부터 운영 템플릿에 캡처되지 않습니다. 작동 템플릿을 편집하여 새 사용자 계정 및 암호를 추가한 다음에 관리형 모듈형 시스템에 작동 템플릿을 적용합니다. 또는 사용자 계정을 변경하지 않고 작동 템플릿을 적용하고 참조 모듈형 시스템에서 사용되는 것과 같은 암호를 관리형 모듈형 시스템에 적용할 수 있습니다.

1. OMIMSSC에서 다음 중 아무 작업이나 수행하여 작동 템플릿을 엽니다.
   - OMIMSSC 대시보드에서, **운영 템플릿 생성**을 클릭합니다.
   - 탐색 창에서 **프로파일** > **운영 템플릿**을 클릭한 다음에 **생성**을 클릭합니다.

   운영 템플릿 마법사가 표시됩니다.
2. **생성**을 클릭합니다.
   운영 템플릿 마법사가 표시됩니다.
3. 템플릿에 대한 이름과 설명을 입력합니다.
4. **디바이스 구성 요소**에서 사용 가능한 속성과 값을 보려는 구성 요소를 클릭합니다.
   구성 요소는 다음과 같습니다.
   - 펌웨어 업데이트
   - 내장형 관리 모듈

     노트: 웹 서버 속성이 사용 설정되어 있는지 확인합니다. 이 구성 요소가 사용 설정되어 있지 않으면 작동 템플릿을 배포한 후에 OMIMSSC를 통해 MX7000 모듈형 시스템에 액세스할 수 없습니다.

     노트: SNMP 구성 및 **Syslog 구성**의 경우에는 각 속성에서 사용 가능한 네 가지 구성을 모두 선택하여 관리형 디바이스에 적용합니다.
5. 수평 스크롤 바를 사용하여 구성 요소를 찾습니다. 구성 요소를 선택하고 그룹을 확장한 다음에 속성 값을 편집합니다. 수직 스크롤 바를 사용하여 구성 요소의 속성과 그룹을 편집합니다.
6. 작동 템플릿이 적용될 때 선택한 구성 요소의 구성이 관리형 디바이스에 적용되기 때문에 각 구성 요소에 대하여 확인란을 선택합니다. 그러나 참조 디바이스의 모든 구성은 캡처되어 템플릿에 저장됩니다.
7. 프로파일을 저장하려면 **완료**를 클릭합니다.

작동 템플릿을 이용한 클러스터 생성

이 장에서는 Windows 서버 HCI 클러스터 생성에 대한 정보를 다룹니다.

Windows 서버 HCI 클러스터용 논리 스위치 생성

SCVMM의 OMIMSSC에서 논리 스위치를 생성합니다.

노트: 관리 구성 섹션에서 입력한 IP 주소는 Windows 서버 HCI에서 사전 정의한 작동 템플릿의 운영 체제 구성 요소에서 입력한 IP 주소를 재정의합니다.

1. OMIMSSC에서 **구성 및 배포**를 확장하고 **클러스터 보기**를 클릭한 다음 클러스터에 대한 **논리 스위치 생성**을 클릭합니다.
2. **클러스터에 대한 논리 스위치 생성**을 클릭합니다.
3. 논리 스위치 이름을 입력하고 논리 스위치를 연결하기 위해 SCVMM에 있는 호스트 그룹을 선택합니다.
4. 다음과 같은 상세 정보를 입력하고 **생성**을 클릭합니다.
   a. **관리 구성**에서 **서브넷**, **시작 IP**, **종료 IP**, **DNS 서버**, **DNS 접미사** 및 **게이트웨이** 상세 정보를 입력합니다.

      노트: CIDR(Classless InterDomain Routing) 표기법으로 서브넷 정보를 입력합니다.

   b. **스토리지 구성**에서 **VLAN**, **서브넷**, **시작 IP** 및 **종료 IP** 상세 정보를 입력합니다.
5. 고유한 작업 이름과 작업에 대한 설명을 입력하고 **생성**을 클릭합니다.
   이 작업을 추적하기 위해 기본적으로 **작업 목록으로 이동** 옵션이 선택되어 있습니다.

논리 스위치가 제대로 생성되었는지 확인하려면 **클러스터 생성** 페이지에 있는 드롭다운 메뉴에서 논리 스위치 이름을 확인합니다.

논리 스위치의 상세 정보를 보려면 SCVMM에서 다음 단계를 수행합니다.

1. 논리 스위치 이름을 보려면 **패브릭**을 클릭하고 **Networking**에서 **논리 스위치**를 클릭합니다.
2. 논리 스위치의 UPP(Uplink Port Profile)을 보려면 **패브릭**을 클릭하고 **Networking**에서 **논리 스위치**를 클릭합니다.
3. 논리 스위치의 네트워크를 보려면 **패브릭**을 클릭하고 **Networking**에서 **논리 네트워크**를 클릭합니다.

Windows 서버 HCI 클러스터 생성

- 클러스터 기능에 대한 **Create logical switch**를 사용하여 논리 네트워크를 생성하는지 확인합니다.
- SCVMM 2016 또는 2019를 사용 중인지 확인합니다.
- Windows Server 2016 또는 2019 Datacenter 에디션을 사용 중인지 확인합니다.
- 관리되는 서버 구성이 Windows 서버 HCI 솔루션 펌웨어 및 드라이버 버전 요구 사항과 일치하는지 확인합니다. 자세한 내용은 *Dell EMC Windows 서버 HCI Ready Nodes PowerEdge R740XD, R740XD2 및 PowerEdge R640 Support Matrix* 설명서를 참조하십시오.
- Windows 서버 HCI의 인프라 및 관리에 대한 자세한 내용은 *Dell EMC Microsoft Windows 서버 HCI Ready Node 배포 가이드 - RN740xd, RN740XD2, RN640, RN440 및 AX6515 Windows 서버 HCI Ready Node가 있는 확장 가능한 하이퍼 컨버지드 인프라스트럭처 설명서*를 참조하십시오.

Windows 서버 HCI 클러스터를 생성하기 전에 다음 사항을 고려하십시오.

- 정적 IP 주소만 제공하여 OMIMSSC에서 Windows 서버 HCI 클러스터를 생성할 수 있습니다.
- 가상 디스크 크기는 Windows 서버 HCI에 사전 정의된 운영 템플릿에 0으로 표시됩니다. 하지만 Windows 서버 HCI에 사전 정의된 운영 템플릿을 적용한 이후에는 M.2 물리적 스토리지 미디어의 전체 크기와 동일한 크기의 가상 드라이브만 생성됩니다. 가상 드라이브 공간에 대한 자세한 내용은 `dell.com/support`에서 iDRAC 사용자 가이드를 참조하십시오.
- 운영 체제-iDRAC 패스스루 옵션이 활성화된 경우, 운영 템플릿에 IP 주소가 구성되어 있는지 확인해야 합니다.

Windows 서버 HCI 클러스터를 생성하려면 다음을 수행합니다.

1. OMIMSSC에서 **구성 및 배포**를 클릭한 다음 **클러스터 보기**를 클릭합니다.
   클러스터 보기 페이지가 표시됩니다.
2. 클러스터를 생성하려면 **생성**을 클릭합니다.
   클러스터 생성 페이지가 표시됩니다.
3. 클러스터 이름을 제공하고 Windows 서버 HCI 클러스터 생성을 위해 미리 정의된 작동 템플릿을 선택합니다.
   - 특정 서버 모델 및 NIC 카드에만 속하는 할당되지 않은 서버는 **작동 템플릿** 드롭다운 메뉴에서 선택하는 작동 템플릿을 기반으로 표시됩니다.
4. 클러스터에 서버를 추가하려면 확인란을 사용하여 서버를 선택합니다.

5. 시스템 고유 풀 값을 추가하려면 **속성 값 풀 내보내기**를 클릭합니다.
   시스템 고유 풀 값을 제공할 수 있도록 파일을 편집하고 저장합니다. 자세한 내용은 풀 값 CSV 파일 입력을 참조하십시오.
6. (선택 사항) 시스템 고유 값을 설정해야 하는 경우 **속성 값 풀**에서 **탐색**을 클릭하고 편집된 .CSV 파일을 선택합니다.
7. 고유 작업 이름을 입력한 다음 **생성**을 클릭합니다.
   이 작업을 추적하기 위해 기본적으로 **작업 목록으로 이동** 옵션이 선택되어 있습니다.

   노트: 운영 체제 배포가 진행 중일 때 SCVMM(서버 GUID가 추가된 이름)에서 복제 중인 호스트 프로파일/물리적 컴퓨터 프로파일이 표시됩니다. 이러한 프로파일은 개별 서버 OSD에 사용됩니다.

클러스터가 생성되었는지 확인하려면 다음을 수행합니다.
1. 클러스터 작업 생성의 성공 상태를 확인합니다.
2. **클러스터 보기** 페이지에서 클러스터를 확인합니다.
3. SCVMM에서 클러스터를 확인합니다.

자세한 내용은 베어 메탈 컴퓨터에서 Hyper-V 호스트 또는 클러스터 프로비저닝에 대한 Microsoft 설명서의 사전 요구 사항 섹션에서 물리적 컴퓨터 프로파일 만들기 섹션을 참조하십시오.

노트: 두 노드 클러스터에 대해 클러스터 감시를 구성하는 것이 좋습니다. 클러스터 감시 구성은 노드 또는 네트워크 통신이 실패할 때 클러스터 또는 스토리지 쿼럼을 유지하는 데 도움이 됩니다. 자세한 정보는 Windows 서버 HCI 배포 가이드를 참조하십시오.

작동 템플릿 보기

생성된 작동 템플릿을 보려면 다음을 수행합니다.

OMIMSSC 콘솔에서 **프로파일 및 템플릿**을 클릭한 다음 **운영 템플릿**을 클릭합니다. 생성된 모든 템플릿이 여기에 나열됩니다.

작동 템플릿 편집

운영 템플릿의 업데이트 소스, 하드웨어 구성 및 운영 체제를 수정할 수 있습니다.

작동 템플릿을 수정하기 전에 다음 사항을 고려하십시오.

- 일부 속성의 값은 다른 속성의 값에 따라 달라집니다. 속성 값을 수동으로 변경할 때는 상호 종속적인 속성도 변경해야 합니다. 이러한 상호 종속적인 값이 적절하게 변경되지 않으면 하드웨어 구성을 적용하지 못할 수 있습니다.
- 작동 템플릿을 생성하면 시스템별 특성이 포함되어 있을 수 있는 지정된 참조 서버에서 모든 하드웨어 구성을 가져옵니다. 정적 IPv4 주소, 자산 태그 등을 예로 들 수 있습니다. 시스템별 특성을 구성하려면 작동 템플릿을 사용하여 시스템별 값 구성을 참조하십시오.
- 작동 템플릿의 특성이 참조 서버의 현재 값과 함께 할당됩니다. 작동 템플릿 에는 특성에 적용 가능한 다른 값도 나열되어 있습니다.
- 사전 정의된 작동 템플릿 및 사용자 지정 생성된 작동 템플릿을 수정하려면 다음 단계를 수행합니다.

노트: (SCVMM 사용자 및 서버에만 해당) 모든 필수 특성 (운영 템플릿에 캡처된 필수 특성은 Windows 서버 HCI 클러스터에 대한 Dell EMC 권장 특성) Windows 서버 HCI에 필요한 특성으로 사전 정의된 Windows 서버 HCI 템플릿의 읽기 전용 속성입니다. 그러나 템플릿 이름, 운영 체제 구성 요소 및 임의 하드웨어 구성 특성은 편집할 수 있습니다.

1. 수정할 템플릿을 선택하고 **편집**을 클릭합니다.
   작동 템플릿 페이지가 표시됩니다.
2. (선택 사항) 템플릿의 이름과 설명을 편집하고 **다음**을 클릭합니다.
3. **디바이스 구성 요소**에서 사용 가능한 속성 및 해당 값을 보려면 구성 요소를 클릭합니다.
4. 사용 가능한 속성 값을 수정합니다.

   노트: 작동 템플릿이 적용될 때 선택된 구성 요소의 구성만 관리 시스템에 적용되므로 각 구성 요소의 확인란을 선택합니다.

   노트: 작동 템플릿을 편집할 때 읽기 전용인 일부 고급 호스트 컨트롤러 인터페이스(AHCI) 구성 요소 속성은 편집 가능한 것으로 나열됩니다. 그러나 이러한 읽기 전용 속성이 설정되고 작동 템플릿이 배포될 때는 디바이스에 대한 변경 사항이 없습니다.

   - MX7000 모듈형 시스템의 경우:

- 구성은 그룹에 대한 모든 속성을 선택한 경우에만 적용됩니다. 따라서 그룹의 속성 중 하나를 변경하려는 경우에도 그룹의 모든 속성을 선택해야 합니다.
- 작동 템플릿을 통해 새 사용자를 추가하려면 작동 템플릿을 캡처할 때 내보낸 기존 사용자의 모든 속성을 선택하고, 최근에 추가된 사용자 그룹을 선택한 다음 작동 템플릿을 저장합니다.
- 시간대 값을 입력하려면 부록을 참조하십시오.

5. 운영 체제 구성 요소의 경우 요구 사항에 따라 다음 작업 중 하나를 수행합니다.
   - MECM에 대한 Windows 운영 체제 배포의 경우에는 MECM용 OMIMSSC 콘솔 확장에 대한 Windows 구성 요소를 참조하십시오.
   - SCVMM에 대한 Windows 운영 체제 배포의 경우에는 SCVMM용 OMIMSSC 콘솔 확장에 대한 Windows 구성 요소를 참조하십시오.
   - OMIMSSC
   - Windows가 아닌 운영 체제의 배포의 경우에는 OMIMSSC 콘솔 확장에 대한 Windows가 아닌 운영 체제의 구성 요소를 참조하십시오.
6. 프로파일을 저장하려면 **완료**를 클릭합니다.

권장 사항: 운영 템플릿을 편집할 때 읽기 전용인 일부 AHCI(Advanced Host Controller Interface) 구성 요소 속성은 편집 가능한 것으로 나열됩니다. 그러나 이러한 읽기 전용 속성이 설정되고 운영 템플릿이 배포될 때는 디바이스에 대한 변경 사항이 없습니다.

여러 서버에서 운영 템플릿을 사용하여 시스템별 값(풀 값) 구성

OMIMSSC 디바이스의 구성대로 검색합니다. 시스템에 특정한 특성(예: iDRAC에 대한 정적 IPv4 주소)은 운영 템플릿에 풀 값으로 표시됩니다. 종속 특성인 풀 값 특성은 기본적으로 다른 특성과 함께 선택됩니다.

1. 수정할 템플릿을 선택하고 편집을 클릭합니다.
   작동 템플릿 페이지가 표시됩니다.
2. (선택 사항) 템플릿의 이름과 설명을 편집하고 **다음**을 클릭합니다.
3. 디바이스 구성 요소에서 사용 가능한 속성 및 해당 값을 보려면 구성 요소를 클릭합니다.
4. **특성 그룹**을 확장합니다. 특성 값이 **풀 값**인 경우 속성이 시스템별 특성으로 식별됩니다. 모든 시스템 특정 속성의 속성 그룹 및 구성 요소에 대한 자세한 내용은 운영 템플릿의 시스템별 특성 섹션의 표 13을 참조하십시오.
5. 이러한 시스템별 특성을 적용하지 않으려면 해당 특성(4단계에서 언급)을 식별하고 운영 템플릿을 편집하는 동안 선택 취소합니다.
6. 운영 템플릿을 배포하는 동안 **풀 특성 내보내기**를 사용하여 .CSV 파일을 통해 이러한 시스템별 특성에 대한 입력을 제공할 수 있습니다. 자세한 내용은 서버에 운영 템플릿 배포를 참조하십시오.

노트: 풀 값 CSV 파일을 채우는 방법에 대한 자세한 내용은 운영 템플릿에서 풀 값 CSV 파일 및 시스템별 특성 채우기를 참조하십시오.

권장 사항:운영 템플릿을 생성할 때 풀 값이 있는 종속 속성의 확인란을 선택하고 선택 취소하면 운영 템플릿을 저장할 수 없으며 다음 오류 메시지가 표시됩니다. `Select at least one attribute, under the selected components, before creating the Operational Template` 따라서 풀 값 또는 같은 종속 특성을 가진 종속 특성을 선택하고 운영 템플릿을 저장합니다. 그런 다음 새로운 운영 템플릿을 생성합니다.

서버에 대한 작동 템플릿 할당 및 운영 템플릿 규정 준수 실행

서버에 작동 템플릿을 할당하고 작동 템플릿 규정 준수를 실행합니다. 작동 템플릿을 서버에 할당한 후에만 작동 템플릿 규정 준수 상태를 볼 수 있습니다. 템플릿을 서버에 할당하여 서버의 구성을 작동 템플릿과 비교할 수 있습니다. 작동 템플릿을 할당한 다음에는 규정 준수 작업이 실행되고 완료 시에 작동 템플릿 상태가 표시됩니다.

작동 템플릿을 할당하려면 다음 단계를 수행합니다.

1. OMIMSSC에서 **구성 및 배포**를 클릭한 다음에 **서버 보기**를 클릭합니다. 필요한 서버를 선택하고 **운영 템플릿 할당 및 규정 준수 실행**을 클릭합니다.
   작동 템플릿 **할당** 및 규정 준수 실행 페이지가 표시됩니다.
2. 필요한 서버를 선택하고 **운영 템플릿 할당 및 규정 준수 실행**을 클릭합니다.
3. 작동 템플릿 드롭다운 메뉴에서 템플릿을 선택하고 작업 이름을 입력한 다음 **할당**을 클릭합니다.

작동 템플릿 드롭다운에는 이전 단계에서 선택한 디바이스의 유형과 동일한 유형의 템플릿이 나열됩니다.

디바이스가 템플릿에 부합하면 확인 표시가 있는 **녹색** 상자가 표시됩니다.

작동 템플릿이 디바이스에 제대로 적용되지 않거나 작동 템플릿의 하드웨어 구성 요소를 선택하지 않은 경우에는 **정보** 기호 상자가 표시됩니다.

디바이스가 템플릿에 맞지 않는 경우에는 **경고** 기호 상자가 표시됩니다. 디바이스가 할당된 작동 템플릿에 부합하지 않는 경우에만 템플릿 이름 링크를 클릭하여 요약 보고서를 볼 수 있습니다. 작동 템플릿 **규정 준수 - 요약 보고서** 페이지에는 템플릿과 디바이스 간의 차이점에 대한 요약 보고서가 표시됩니다.

보고서 세부 정보를 보려면 다음 단계를 수행합니다.

a. **규정 준수 세부 정보 보기**를 클릭합니다. 여기에 할당된 템플릿의 속성 값과 다른 속성 값을 가진 구성 요소가 표시됩니다. 색상은 작동 템플릿 규정 준수의 여러 가지 상태를 나타냅니다.
   - 노란색 경고 기호 - 비준수. 디바이스의 구성이 템플릿 값과 일치하지 않는다는 것을 나타냅니다.
   - 빨간색 상자 - 디바이스에 구성 요소가 없다는 것을 나타냅니다.

모듈형 시스템에 작동 템플릿 할당

작동 템플릿을 모듈형 시스템에 할당하고 작동 템플릿 규정 준수를 실행합니다. 이 작업에서는 선택한 템플릿을 모듈형 시스템에 할당하여 모듈형 시스템의 구성을 작동 템플릿과 비교합니다. 작동 템플릿을 할당한 후에는 규정 준수 작업이 실행되고 완료 시에 규정 준수 상태가 표시됩니다.

모듈형 시스템에 작동 템플릿을 할당하려면 다음 단계를 수행합니다.

1. OMIMSSC에서 **구성 및 배포**를 클릭하고 **모듈형 시스템 보기**를 클릭합니다. 필요한 모듈형 시스템을 선택하고 **운영 템플릿 할당**을 클릭합니다.
   작동 템플릿 **할당** 페이지가 표시됩니다.
2. 필요한 모듈형 시스템을 선택하고 **운영 템플릿 할당 및 규정 준수 실행**을 클릭합니다.
   작동 템플릿 **할당** 페이지가 표시됩니다.
3. 작동 템플릿 드롭다운 메뉴에서 템플릿을 선택하고 작업 이름을 입력한 다음 **할당**을 클릭합니다.
   디바이스가 템플릿에 부합하면 확인 표시가 있는 **녹색** 상자가 표시됩니다.
   작동 템플릿이 디바이스에 제대로 적용되지 않거나 작동 템플릿의 하드웨어 구성 요소를 선택하지 않은 경우에는 **정보** 기호 상자가 표시됩니다.

   노트: 작동 템플릿 규정 준수 상태에서 사용자 속성에 대한 변경 사항은 제외됩니다.

   디바이스가 템플릿에 맞지 않는 경우에는 **경고** 기호 상자가 표시됩니다. 디바이스가 할당된 작동 템플릿에 부합하지 않는 경우에만 템플릿 이름 링크를 클릭하여 요약 보고서를 볼 수 있습니다. 작동 템플릿 **규정 준수 - 요약 보고서** 페이지에는 템플릿과 디바이스 간의 차이점에 대한 요약 보고서가 표시됩니다.

   보고서 세부 정보를 보려면 다음 단계를 수행합니다.

   a. **규정 준수 세부 정보 보기**를 클릭합니다. 여기에 할당된 템플릿의 속성 값과 다른 속성 값을 가진 구성 요소가 표시됩니다. 색상은 작동 템플릿 규정 준수의 여러 가지 상태를 나타냅니다.
      - 노란색 경고 기호 - 비준수. 디바이스의 구성이 템플릿 값과 일치하지 않는다는 것을 나타냅니다.
      - 빨간색 상자 - 디바이스에 구성 요소가 없다는 것을 나타냅니다.

운영 템플릿 배포

노트: 작동 템플릿을 배포한 후에 디바이스에 로그인하려면 자격 증명을 변경하는 속성을 활성화시키지 말아야 합니다.

1. OMIMSSC에서 **구성 및 배포**를 클릭하고 **서버 보기**를 클릭합니다. 템플릿을 적용한 서버를 선택한 다음에 **작동 템플릿 배포**를 클릭합니다.
   작동 템플릿 배포 페이지가 표시됩니다.
2. OMIMSSC에서 **구성 및 배포**를 클릭하고 **모듈형 시스템 보기**를 클릭합니다. 템플릿을 할당한 모듈형 시스템을 선택한 다음에 **작동 템플릿 배포**를 클릭합니다.
   작동 템플릿 배포 페이지가 표시됩니다.
3. (선택 사항) 선택한 템플릿에서 풀 값으로 표시된 모든 속성을 .CSV 파일로 내보내려면 **풀 속성 내보내기**를 클릭하고, 그렇지 않으면 4단계로 이동합니다.

노트: 풀 값을 내보내기 전에 OMIMSSC 콘솔 확장 프로그램이 설치된 OMIMSSC 어플라이언스의 IP 주소를 로컬 인트라넷 사이트에 추가합니다. IE 브라우저에서 IP 주소를 추가하는 방법에 대한 자세한 내용은 *System Center Configuration Manager 및 System Center Virtual Machine Manager를 위한 Microsoft System Center 버전 7.2.1용 Dell EMC OpenManage Integration 사용자 가이드*의 *브라우저 설정* 섹션을 참조하십시오.

4. 풀 값을 내보낸 경우에는 .CSV 파일에서 풀 값으로 표시된 모든 속성에 대한 값을 입력하고 파일을 저장합니다. **속성 값 풀**에서 이 파일을 선택하여 가져옵니다.

   .CSV 파일의 형식 `attribute-value-pool.csv`

   노트: iDRAC IP 또는 iDRAC 자격 증명이 변경된 후에 OMIMSSC에서 작업을 추적하지 않고 작업이 iDRAC에서 성공했을 수도 있지만 실패로 표시되기 때문에 모든 적절한 속성을 가진 .CSV 파일을 선택하고 템플릿 때문에 iDRAC IP 또는 iDRAC 자격 증명이 변경되지 않게 해야 합니다.

5. 고유한 작업 이름과 작업 설명을 입력한 다음에 **배포**를 클릭합니다.

   이 작업을 추적하기 위해 기본적으로 **작업 목록으로 이동** 옵션이 선택되어 있습니다.

서버에 작동 템플릿 배포

관리되는 서버에 운영 체제를 배포하려면 관리 시스템과 배포에 사용된 운영 체제 이미지에 KB 문서 4093492 이상이 설치되어 있는지 확인합니다.

서버에 할당된 작동 템플릿을 배포하여 Windows 및 비 Windows 운영 체제(ESXi 및 RHEL)를 배포할 수 있습니다.

노트: 12세대 서버에 Windows 2016 또는 Windows 2019 운영 체제를 배포한 후 장치 관리자 아래에 노란색 느낌표가 표시되면 `Dell.com/support`에서 적절한 드라이버를 다운로드하여 설치합니다.

노트: 서버에서 잠금 모드가 활성화된 경우 서버에 운영 템플릿 배포가 차단됩니다.

노트: UEFI 기반 디바이스에 Windows를 배포할 때 GPT(GUID Partition Table) 파일 시스템을 사용하여 Windows 파티션이 포함된 하드 드라이브를 포맷합니다. 자세한 내용은 Microsoft 설명서의 UEFIGPT 기반 하드 드라이브 파티션 섹션을 참조하십시오.

1. OMIMSSC에서 **구성 및 배포**를 클릭하고 **서버 보기**를 클릭합니다. 템플릿을 배포할 서버를 선택한 다음 **작동 템플릿 배포**를 클릭합니다.
   작동 템플릿 배포 페이지가 표시됩니다.

   노트: 작업 순서 미디어로 부팅하는 동안 *Press any key to boot to CD \ DVD .....* 프롬프트가 표시되는 경우, 프롬프트 제거 및 작업 순서 미디어로 자동 부팅에 대한 자세한 내용은 Microsoft 설명서의 EFI 기반 컴퓨터에 Windows 설치 섹션을 참조하십시오.

2. 템플릿을 배포할 서버를 선택한 다음 **작동 템플릿 배포**를 클릭합니다.
   작동 템플릿 배포 페이지가 표시됩니다.
3. 선택한 템플릿에서 풀 값으로 표시된 모든 속성을 .CSV 파일로 내보내려면 **풀 속성 내보내기**를 클릭합니다.

   풀 값을 내보내기 전에 OMIMSSC 콘솔 확장 프로그램이 설치된 OMIMSSC 어플라이언스의 IP 주소를 로컬 인트라넷 사이트에 추가합니다.
4. 풀 값을 내보낸 경우에는 .CSV 파일에서 풀 값으로 표시된 모든 속성에 대한 값을 입력하고 파일을 저장합니다. **속성 값 풀**에서 이 파일을 선택하여 가져옵니다.

   .CSV 파일의 형식 `attribute-value-pool.csv`

   노트: iDRAC IP 또는 iDRAC 자격 증명이 변경된 후에 OMIMSSC에서 작업을 추적하지 않고 작업이 iDRAC에서 성공했을 수도 있지만 실패로 표시되기 때문에 모든 적절한 속성을 가진 .CSV 파일을 선택하고 템플릿 때문에 iDRAC IP 또는 iDRAC 자격 증명이 변경되지 않게 해야 합니다.

5. 고유한 작업 이름과 작업 설명을 입력한 다음에 **배포**를 클릭합니다.

   이 작업을 추적하기 위해 기본적으로 **작업 목록으로 이동** 옵션이 선택되어 있습니다.

모듈형 시스템에 대한 작동 템플릿 배포

모듈형 시스템 구성 요소를 지성하고 할당된 작동 템플릿을 배포하여 모듈형 시스템 펌웨어 버전을 업데이트할 수 있습니다.

노트: 다중 섀시 관리(MCM)에서 **구성원 섀시로 전파**를 사용하여 리드 섀시를 구성하는 경우에 OMIMSSC에서 리드 섀시와 구성원 섀시를 구성 및 업데이트하면 전파를 통해 수행한 변경 사항이 재정의됩니다.

1. OMIMSSC에서 **구성 및 배포**를 클릭하고 **모듈형 시스템 보기**를 클릭합니다. 템플릿을 할당한 모듈형 시스템을 선택한 다음에 **작동 템플릿 배포**를 클릭합니다.
   작동 템플릿 **배포** 페이지가 표시됩니다.
2. (선택 사항) 선택한 템플릿에서 풀 값으로 표시된 모든 속성을 .CSV 파일로 내보내려면 **풀 속성 내보내기**를 클릭하고, 그렇지 않으면 4단계로 이동합니다.
3. 풀 값을 내보낸 경우에는 .CSV 파일에서 풀 값으로 표시된 모든 속성에 대한 값을 입력하고 파일을 저장합니다. **속성 값 풀**에서 이 파일을 선택하여 가져옵니다.

   .CSV 파일의 형식 `attribute-value-pool.csv`

   노트: CMC IP 또는 CMC 자격 증명이 변경된 후에 OMIMSSC에서 해당 작업을 추적하지 않기 때문에 모든 적절한 속성을 가진 .CSV 파일을 선택하고 CMC IP 또는 CMC 자격 증명이 템플릿 때문에 변경되지 않았는지 확인하십시오.

4. 고유한 작업 이름과 작업 설명을 입력한 다음에 **배포**를 클릭합니다.

   노트: 모듈형 시스템에 대해 지원되는 시스템 고유 풀 값 속성은 없습니다. 따라서 내보낼 풀 값이 없습니다.

   이 작업을 추적하기 위해 기본적으로 **작업 목록으로 이동** 옵션이 선택되어 있습니다.

작동 템플릿 할당 해제

1. OMIMSSC에서 다음 작업 중 하나를 수행합니다.
   - **구성 및 배포**를 클릭하고 **서버 보기**를 클릭합니다.
   - **구성 및 배포**를 클릭하고 **모듈형 시스템 보기**를 클릭합니다.

   필요한 디바이스를 선택하고 **운영 템플릿 할당 및 규정 준수 실행**을 클릭합니다.

   작동 템플릿 할당 및 규정 준수 실행 페이지가 표시됩니다.
2. 디바이스를 선택하고 **작동 템플릿 할당 및 규정 준수 실행**을 클릭합니다.
   작동 템플릿 할당 및 규정 준수 실행 페이지가 표시됩니다.
3. **작동 템플릿** 드롭다운 메뉴에서 **할당 해제**를 선택하고 **할당**을 클릭합니다.
   작동 템플릿이 선택한 디바이스에 대하여 할당 해제됩니다.

작동 템플릿 삭제

작동 템플릿을 삭제하려면 다음을 수행합니다.

작동 템플릿을 삭제하기 전에 다음을 확인합니다.

- 선택한 작동 템플릿이 서버 또는 모듈형 시스템과 연결되어 있지 않은지 확인합니다. 디바이스와 연결되어 있는 경우 템플릿을 할당 해제한 다음 템플릿을 삭제합니다.
- 작동 템플릿과 연결된 작업이 실행되고 있지 않은지 확인합니다.
- 미리 정의된 템플릿은 삭제할 수 없으므로 미리 정의된 작동 템플릿을 선택하지 않았는지 확인합니다.
- 모든 유형의 작동 템플릿을 삭제하는 단계는 동일합니다.

삭제할 템플릿을 선택하고 **삭제**를 클릭합니다. 확인하려면 **예**를 클릭합니다.

16

OMIMSSC를 이용한 운영 체제 배포

관리되는 서버에서 Windows 운영 체제를 배포하기 전에 WinPE 이미지를 업데이트하고 작업 시퀀스, LC 부팅 미디어 파일 및 작업 시퀀스 미디어 부팅 가능한 ISO 파일을 생성합니다. MECM 콘솔 사용자와 SCVMM 콘솔 사용자를 위한 단계가 서로 다릅니다. 상세 정보는 아래 섹션을 참조하십시오. Windows가 아닌 운영 체제를 배포할 경우 비 Windows OS 배포 준비 섹션에 언급된 사항에 유의하십시오.

주제:

- WinPE 이미지 정보 업데이트
- MECM 콘솔에서 운영 체제 배포 준비
- Windows가 아닌 운영 체제 배포 준비

WinPE 이미지 정보 업데이트

Windows 사전 설치 환경(WinPE) 이미지는 운영 체제 배포에 사용됩니다. MECM 또는 SCVMM에서 사용할 수 있는 WinPE 이미지에 최신 드라이버가 포함되어 있지 않을 수 있으므로 운영 체제를 배포하려면 업데이트된 WinPE 이미지를 사용합니다. 필요한 드라이버가 모두 포함된 WinPE 이미지를 생성하려면 Dell EMC OpenManage 드라이버 팩을 사용하여 이미지를 업데이트합니다. Lifecycle Controller에 관련 운영 체제에 연관된 드라이버 팩이 설치되어 있는지 확인합니다.

1. 필요한 드라이버가 모두 포함된 WinPE 이미지를 생성하려면 Dell EMC OpenManage 드라이버 팩을 사용하여 이미지를 업데이트합니다.
2. Lifecycle Controller에 관련 운영 체제에 연관된 드라이버 팩이 설치되어 있는지 확인합니다.

노트: `boot.wim` 파일 이름을 변경하지 마십시오.

MECM용 WIM 파일 제공

`boot.wim` 파일을 다음 위치 `\\shareip\sms_sitecode\OSD\boot\x64\boot.wim`에서 복사한 다음, OMIMSSC에서 액세스할 수 있는 공유 폴더에 붙여 넣습니다.
예를 들어, 공유 경로의 위치는 다음과 같습니다. `\\shareip\sharefolder\boot.wim`

SCVMM용 WIM 파일 제공

WinPE 기본 이미지는 OpenManage Server 드라이버 팩에서 부팅에 중요한 Dell 드라이버를 삽입하는 데 필요합니다. 이 이미지는 SCVMM에 PXE 서버를 설치하여 생성됩니다. SCVMM에서 PXE 서버를 설치하는 방법에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

1. 서버에 WDS(Windows Deployment Server) 역할을 설치 및 구성하고 PXE 서버를 SCVMM에 추가합니다.
   서버에 WDS 역할을 추가하고 PXE 서버를 SCVMM에 추가하는 방법에 대한 자세한 내용은 Microsoft 설명서의 베어 메탈 컴퓨터에서 Hyper-V 호스트 또는 클러스터 프로비저닝 섹션을 참조하십시오.
2. `boot.wim` 파일을 다음 위치 `C:\RemoteInstall\DCMgr\Boot\Windows\Images`에 존재하는 PXE 서버에서 복사한 다음, OMIMSSC에서 액세스할 수 있는 공유 폴더에 붙여 넣습니다.
   예를 들어, 공유 경로의 위치는 다음과 같습니다. `\\shareip\sharefolder\boot.wim`

WDS 및 PXE 서버는 WinPE 기반 boot.in 이미지를 생성하는 경우에만 필요하며, 배포 시나리오에서 사용할 필요는 없습니다.

OpenManage 서버 드라이버 팩에서 드라이버 추출

Dell EMC OpenManage Server Driver Pack DVD는 모든 플랫폼에 대한 OS 드라이버를 패키징하는 Dell EMC에서 공식적으로 릴리스한 패키지입니다. 현재 버전부터 OMIMSC는 관리자가 OpenManage 드라이버 팩만 사용하여 WinPE 이미지를 만들 수 있도록 도와야 합니다.

To download OpenManage driver pack, launch **https://www.dell.com/support/** -> Search for the keyword **Dell EMC OpenMange server Driver Pack DVD** and download the corresponding openManage server driver pack based on the supported platforms.

1. 로컬 Windows 시스템에서 ISO를 드라이브로 마운트합니다.
   노트: 올바른 WinPE 버전을 사용해야 합니다.
2. 명령 프롬프트를 사용하여 다음 <MountedDrive>:\server_assistant\driver_tool\bin.경로로 이동합니다 .
3. 다음 명령을 실행합니다. make_driver_dir.exe -i <MountedDrive> -d <ExtractedWinPEPath> -o <filter option> --extract

   마운트된 드라이브가 F에 있고 추출된 출력 경로가 다음 C:\om_server_diver_pack 예제를 사용하여 지원되는 모든 플랫폼에 대한 드라이버를 추출한다고 가정합니다.

   a. 지원되는 모든 플랫폼에서 사용할 Windows 2016 및 2019 드라이버를 추출합니다. make_driver_dir.exe -i F:\ -d c:\om_server_driver_pack -o WINPE10 --extract
   b. 지원되는 모든 플랫폼에 대해 Windows 2012 R2 드라이버를 추출하려면 다음을 사용하십시오. make_driver_dir.exe -i F:\ -d c:\om_server_driver_pack -o WINPE5 --extract

노트: 추출이 완료되면 다음 디렉토리에서 드라이버를 제거합니다.
<ExtractedWinPEPath>\WINPE5\chipset\9D99N\SBDrv.

WinPE 이미지 업데이트

각 WinPE 업데이트 작업에 고유한 작업 이름이 할당됩니다.

1. OMIMSSC에서 **WinPE 업데이트**를 선택합니다.
   WinPE 업데이트 페이지가 표시됩니다.
2. **이미지 소스**의 **맞춤 구성 WinPE 이미지 경로**에 이미지가 있는 파일 이름과 함께 WinPE 이미지 경로를 입력합니다.
   예: \\Shareip\sharefolder\WIM\boot.wim.
3. **DTK 드라이버 경로**의 **DTK 드라이버 DVD 경로** 아래에 Dell EMC OpenManage 드라이버 위치를 입력합니다.
   예를 들면, 다음과 같습니다. \\Shareip\sharefolder\<extracted share folder>
4. **출력 파일** 아래에서, **ISO 또는 WIM 파일 이름**에 대해, WinPE 이미지가 생성될 공유 파일 경로와 함께 파일 이름을 입력합니다.

   출력 파일 형식 중 하나를 입력합니다.

   - MECM용 WIM 파일
   - SCVMM용 ISO 파일
5. **자격 증명 프로파일**의 **자격 증명 프로파일** 아래에 WinPE 이미지가 저장된 공유 폴더에 대한 액세스 권한이 있는 자격 증명을 입력합니다.
6. (선택 사항) 작업 목록을 보려면 **작업 목록으로 이동**을 선택합니다.
   - MECM용 WIM 파일
   - SCVMM용 ISO 파일
   - MECM용 WIM 파일
   - SCVMM용 ISO 파일

   각 Windows 사전 설치 환경(WinPE) 업데이트에 대해 고유한 작업 이름이 지정됩니다.
7. **업데이트**를 클릭합니다.
   이전 단계에서 제공한 파일 이름이 있는 WinPE 이미지는 \\Shareip\sharefolder\WIM 아래에 생성됩니다.

MECM 콘솔에서 운영 체제 배포 준비

MECM 콘솔에서 OMIMSSC를 통해 검색되는 관리되는 서버에 운영 체제를 배포하기 전에 Dell EMC 특정 또는 사용자 지정 작업 시퀀스, LC 부팅 미디어 파일 및 작업 시퀀스 미디어 부팅 가능한 ISO 파일을 생성합니다.

작업 시퀀스 - MECM

작업 시퀀스는 MECM을 사용하여 관리하는 시스템에서 운영 체제를 배포하는 데 사용되는 일련의 명령입니다.

Dell EMC는 작동 템플릿을 생성하기 전에 다음 사전 요구 사항을 완료하는 것을 권장합니다.

1. Configuration Manager에서, 시스템이 검색되어 **자산 및 규정 준수** > **디바이스 컬렉션** > **모든 Dell Lifecycle Controller 서버** 아래에 있는지 확인합니다. 자세한 내용은 서버 검색을 참조하십시오.
2. 시스템에 최신 BIOS 버전을 설치합니다.
3. 시스템에 최신 버전의 Lifecycle Controller를 설치합니다.
4. 시스템에 최신 버전의 iDRAC 펌웨어를 설치합니다.

노트: Configuration Manager 콘솔은 항상 관리자 권한으로 실행합니다.

작업 시퀀스 유형

다음과 같은 두 가지 방법으로 작업 시퀀스를 생성할 수 있습니다.

- OMIMSSC 배포 템플릿을 사용하여 Dell 고유 작업 시퀀스를 생성합니다.
- 사용자 지정 작업 시퀀스를 생성합니다.

명령의 성공 또는 실패와 관계 없이 작업 시퀀스가 다음 작업 시퀀스 단계로 계속 진행됩니다.

Dell 고유 작업 시퀀스 생성

MECM의 **OMIMSSC 서버 구축 템플릿** 옵션을 사용하여 Dell 고유 작업 시퀀스를 생성하려면 다음을 수행하십시오.

1. Configuration Manager를 시작합니다.
   Configuration Manager 콘솔 화면이 표시됩니다.
2. 왼쪽 창에서 **소프트웨어 라이브러리** > **개요** > **운영 체제** > **작업 시퀀스**를 선택합니다.
3. **작업 시퀀스**를 마우스 오른쪽 버튼으로 클릭한 후 **OMIMSSC 서버 구축** > **OMIMSSC 서버 구축 템플릿 생성**을 클릭합니다.
   OMIMSSC 서버 구축 작업 시퀀스 마법사가 표시됩니다.
4. **작업 시퀀스 이름** 필드에 작업 시퀀스의 이름을 입력합니다.
5. 드롭다운 목록에서 사용할 부팅 이미지를 선택합니다.

   노트: 생성한 Dell 맞춤 구성 부팅 이미지를 사용하는 것이 좋습니다.

6. **운영 체제 설치**에서 운영 체제 설치 유형을 선택합니다. 옵션은 다음과 같습니다.
   - **OS WIM 이미지 사용**
   - **스크립팅된 OS 설치**
7. **사용할 운영 체제 패키지** 드롭다운 메뉴에서 운영 체제 패키지를 선택합니다.
8. **unattend.xml**을 사용하는 패키지가 있는 경우 **unattend.xml을 사용하는 패키지 정보** 메뉴에서 선택하고 그렇지 않은 경우 **<지금 선택 안 함>**을 선택합니다.
9. **생성**을 클릭합니다.
   생성된 작업 시퀀스의 이름과 함께 **작업 시퀀스 생성됨** 창이 표시됩니다.
10. 표시되는 확인 메시지 상자에서 **닫기**를 클릭합니다.

사용자 지정 작업 시퀀스 생성

1. Configuration Manager를 시작합니다.
   Configuration Manager 콘솔이 표시됩니다.
2. 왼쪽 창에서 **소프트웨어 라이브러리** > **개요** > **운영 체제** > **작업 시퀀스**를 선택합니다.
3. **작업 시퀀스**를 마우스 오른쪽 버튼으로 클릭하고 **작업 시퀀스 생성**을 클릭합니다.
   작업 시퀀스 생성 마법사가 표시됩니다.
4. **새 맞춤 구성 작업 시퀀스 생성**을 선택하고 **다음**을 클릭합니다.
5. **작업 시퀀스 이름** 텍스트 상자에 작업 시퀀스의 이름을 입력합니다.
6. 생성한 Dell 부팅 이미지를 찾아보고 **다음**을 클릭합니다.
   설정 확인 화면이 표시됩니다.
7. 설정을 검토하고 **다음**을 클릭합니다.
8. 표시되는 확인 메시지 상자에서 **닫기**를 클릭합니다.

작업 시퀀스 편집

노트: MECM 2016 및 2019에서 작업 시퀀스를 편집하는 동안 누락된 개체 참조 메시지에 **Windows 및 ConfigMgr 설정** 패키지가 나열되지 않습니다. 패키지를 추가한 다음 작업 순서를 저장합니다.

1. Configuration Manager를 시작합니다.
   구성 관리자 화면이 표시됩니다.
2. 왼쪽 창에서 **소프트웨어 라이브러리** > **운영 체제** > **작업 순서**를 선택합니다.
3. 편집할 작업 시퀀스를 마우스 오른쪽 버튼으로 클릭하고 **편집**을 클릭합니다.
   작업 시퀀스 편집기 창이 표시됩니다.
4. **추가** > **Dell 배포** > **Dell Lifecycle Controller에서 드라이버 적용**을 클릭합니다.
   Dell 서버 구축을 위한 맞춤 지정 작업이 로드됩니다. 이제 작업 순서를 변경할 수 있습니다.

   노트: 작업 순서를 처음 편집할 때 오류 메시지, **Setup Windows and Configuration Manager**이 표시됩니다. 이 오류를 해결하려면 구성 관리자 클라이언트 업그레이드 패키지를 만들고 선택합니다. 패키지 생성에 대한 자세한 내용은 **Technet.microsoft.com**에서 구성 관리자 설명서를 참조하십시오.

   노트: MECM 2016 및 2019에서 작업 순서를 편집할 때 누락된 개체 참조 메시지에 Windows 및 ConfigMgr 설정 패키지가 나열되지 않습니다. 따라서 패키지를 추가한 다음 작업 시퀀스를 저장해야 합니다.

Lifecycle Controller 부팅 미디어에 대한 기본 공유 위치 설정

Lifecycle Controller 부팅 미디어에 대한 기본 공유 위치를 설정하려면 다음을 수행합니다.

1. **Configuration Manager**에서 **관리** > **사이트 구성** > **사이트**를 선택합니다.
2. **<사이트 서버 이름>**을 마우스 오른쪽 버튼으로 클릭하고 **사이트 구성 요소 구성**을 선택한 다음 **대역 외 관리**를 선택합니다.
   대역 외 관리 구성 요소 속성 창이 표시됩니다.
3. **Lifecycle Controller** 탭을 클릭합니다.
4. **사용자 정의 Lifecycle Controller 부팅 미디어용 기본 공유 위치** 아래에서 **수정**을 클릭하여 사용자 정의 Lifecycle Controller 부팅 미디어의 기본 공유 위치를 수정합니다.
5. **공유 정보 수정** 창에 새로운 공유 이름 및 공유 경로를 입력합니다.
6. **확인**을 클릭합니다.

작업 순서 미디어 생성(부팅 가능한 ISO)

1. **소프트웨어 라이브러리**의 Configuration Manager에서 **작업 시퀀스**를 마우스 오른쪽 버튼으로 클릭하고 **작업 시퀀스 미디어 생성**을 선택합니다.

   노트: 이 마법사를 시작하기 전에 모든 배포 지점 전반의 부팅 이미지를 관리하고 업데이트해야 합니다.

   노트: OMIMSSC 작업 순서 미디어를 생성하는 데 독립 실행형 미디어 방법을 지원하지 않습니다.

2. **작업 시퀀스 미디어 마법사**에서 **부팅 미디어**를 선택하고 **무인 운영 체제 배포 허용** 옵션을 선택하고 **다음**을 클릭합니다.
3. **CD/DVD 세트**를 선택하고 **탐색**을 클릭하여 ISO 이미지를 저장할 위치를 선택합니다.
4. **다음**을 클릭합니다.
5. **암호를 사용하여 미디어 보호** 확인란의 선택을 취소하고 **다음**을 클릭합니다.
6. **PowerEdge 서버 구축 부팅 이미지**를 찾아서 선택합니다.

   노트: DTK를 사용하여 생성한 부팅 이미지만 사용하십시오.

7. 드롭다운 메뉴에서 배포 지점을 선택하고 **하위 사이트에서 배포 지점 표시** 확인란을 선택합니다.
8. **다음**을 클릭합니다.
   작업 시퀀스 미디어 정보가 있는 **요약** 화면이 표시됩니다.
9. **다음**을 클릭합니다.
   진행률 표시줄이 표시됩니다.
10. 이미지 생성이 완료되면 마법사를 닫습니다.

Windows가 아닌 운영 체제 배포 준비

관리형 시스템에 Windows가 아닌 운영 체제를 배포하는 경우에 다음 사항을 기억해야 합니다.

- ISO 파일은 읽기 및 쓰기 액세스가 있는 NFS(Network File System) 버전 또는 CIFS(Common Internet File System) 공유에서 사용할 수 있습니다.
- 관리형 시스템에서 가상 드라이브를 사용할 수 있는지 확인합니다.
- ESXi 운영 체제를 배포한 후에 서버는 MECM의 **Managed Lifecycle Controller(ESXi)** 컬렉션으로 이동합니다.
- Windows가 아닌 운영 체제 유형을 배포한 후에 서버는 **Windows가 아닌 기본 호스트 업데이트 그룹**으로 이동합니다.
- 네트워크 어댑터를 운영 체제가 배포 중인 서버의 네트워크 포트에 연결하는 것이 좋습니다.

17

OMIMSSC를 이용한 디바이스 프로비저닝 OMIMSSC

이 장에서는 OMIMSSC를 사용한 검색, 운영 체제 배포, 클러스터 생성 및 Dell EMC 디바이스 유지 보수에 대한 개괄적인 정보를 제공합니다.

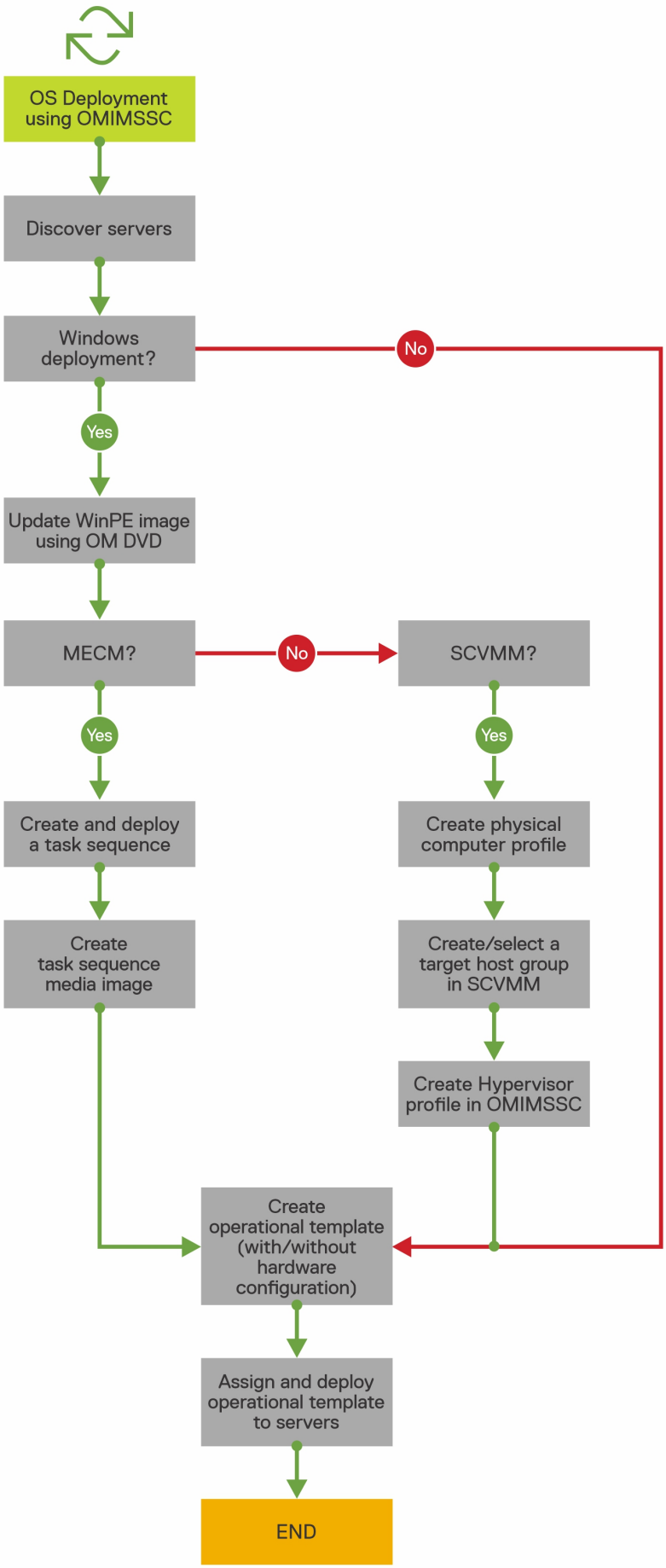
주제:

배포 시나리오에 대한 워크플로

OMIMSSC를 사용하여 작동 템플릿을 사용하는 MECM 또는 SCVMM 환경에 Windows 운영 체제 및 Windows가 아닌 운영 체제를 배포합니다.

노트: 운영 체제를 배포하기 전에 디바이스 펌웨어 버전을 `downloads.dell.com`에 있는 최신 버전으로 업그레이드해야 합니다.

다음은 OMIMSSC의 운영 체제 배포 활용 사례를 그림으로 나타낸 것입니다.


OS Deployment using OMIMSSC
Discover servers
Windows deployment?
No
Yes
Update WinPE image using OM DVD
MECM?
No
SCVMM?
Yes
Yes
Create and deploy a task sequence
Create physical computer profile
Create task sequence media image
Create/select a target host group in SCVMM
Create Hypervisor profile in OMIMSSC
Create operational template (with/without hardware configuration)
Assign and deploy operational template to servers
END

MECM용 OMIMSSC 콘솔 확장 프로그램을 사용한 Windows OS 배포

OMIMSSC를 사용하는 MECM 콘솔을 통해 Windows OS를 배포하려면 다음 단계를 수행합니다.

노트: 호스트 서버에 OS를 배포하기 전에 MECM에서 서버의 **클라이언트** 상태가 **아니요**인지 확인합니다.

1. 최신 Dell EMC OpenManage 서버 드라이버 팩을 다운로드하고 WinPE(Windows Preinstallation Environment) 부팅 WIM 이미지를 생성합니다. 자세한 내용은 WinPE 업데이트를 참조하십시오.
2. 이 .WIN 이미지를 MECM 콘솔로 가져오고 MECM에서 부팅 이미지를 생성합니다. 자세한 내용은 *Microsoft 설명서*를 참조하십시오.
3. MECM에서 작업 시퀀스를 생성합니다. 자세한 내용은 작업 시퀀스 생성을 참조하십시오.
4. MECM에서 작업 시퀀스 미디어 이미지를 생성합니다. 자세한 내용은 *Microsoft 설명서*를 참조하십시오.

   노트: 무인 OS 배포를 활성화하려면 작업 시퀀스 미디어를 생성할 때 **미디어 유형 선택**에서 **무인 운영 체제 배포 허용** 확인란을 선택합니다.

5. **검색** 페이지에서 참조 서버를 검색합니다. 자세한 내용은 수동 검색을 사용하여 서버 검색을 참조하십시오.
6. 검색된 서버의 모든 상세 정보를 캡처하여 작동 템플릿을 생성합니다. 자세한 내용은 참조 서버에서 운영 템플릿 작성을 참조하십시오.
7. 관리형 디바이스에서 작동 템플릿을 할당하고 템플릿 규정 준수를 확인합니다. 자세한 내용은 운영 템플릿 할당 및 운영 템플릿 규정 준수 실행을 참조하십시오.
8. 디바이스 템플릿 규정 준수를 위해 운영 템플릿을 배포합니다. 자세한 내용은 운영 템플릿 배포를 참조하십시오.
9. **작업 및 로그 센터** 페이지에서 운영 체제 배포에 대한 작업 상태를 봅니다. 자세한 내용은 작업 및 로그 센터 실행을 참조하십시오.

SCVMM용 OMIMSSC 콘솔 확장 프로그램을 사용한 하이퍼바이저 배포

하이퍼바이저 배포를 위한 다양한 시나리오는 다음과 같습니다.

표 11. 하이퍼바이저 배포 시나리오

상태	작업
최신 출하 시 드라이버가 필요한 경우.	하이퍼바이저 프로파일을 생성하는 동안 LC(Lifecycle Controller) 드라이버 삽입 기능을 활성화합니다.
기존 하드웨어 구성을 유지하려는 경우.	작동 템플릿을 작성하는 동안 변경이 필요하지 않은 모든 구성 요소에 대한 확인란을 선택 취소합니다.

OMIMSSC를 사용하여 SCVMM 콘솔을 통해 하이퍼바이저를 배포하려면 다음 단계를 수행합니다.

1. 최신 Dell EMC OpenManage 드라이버 팩을 다운로드하고 WinPE(Windows Preinstallation Environment) 부팅 ISO 이미지를 생성합니다. 자세한 내용은 WinPE 업데이트 섹션을 참조하십시오.
2. SCVMM에서 물리적 컴퓨터 프로파일과 호스트 그룹을 생성합니다. 자세한 내용은 SCVMM 설명서를 참조하십시오.
3. SCVMM용 OMIMSSC 콘솔 확장 프로그램에서 하이퍼바이저 프로파일을 생성합니다. 자세한 내용은 하이퍼바이저 프로파일 생성을 참조하십시오.
4. 검색 페이지에서 참조 서버를 검색합니다. 자세한 내용은 수동 검색을 사용하여 서버 검색을 참조하십시오.
5. 검색된 서버의 모든 상세 정보를 캡처하여 운영 템플릿을 생성합니다. 자세한 내용은 참조 서버에서 운영 템플릿 작성을 참조하십시오.
6. 관리형 디바이스에서 운영 템플릿을 할당하고 템플릿 규정 준수를 확인합니다. 자세한 내용은 운영 템플릿 할당 및 운영 템플릿 규정 준수 실행을 참조하십시오.
7. 디바이스 템플릿 규정 준수를 위해 운영 템플릿을 배포합니다. 자세한 내용은 운영 템플릿 배포를 참조하십시오.
8. 작업 및 로그 센터 페이지에서 운영 체제 배포에 대한 작업 상태를 봅니다. 자세한 내용은 작업 및 로그 센터 실행을 참조하십시오.

Windows OS 재배포 OMIMSSC

MECM용 OMIMSSC 콘솔 확장 프로그램이나 SCVMM의 OMIMSSC 콘솔 확장 프로그램을 사용하여 서버에 Windows OS를 재배포하려면 다음 단계를 수행합니다.

1. Microsoft 콘솔에서 서버를 삭제합니다. 자세한 내용은 Microsoft 설명서를 참조하십시오.

2. 서버를 재검색하거나 등록된 Microsoft 콘솔과 OMIMSSC를 동기화합니다. 이 서버는 OMIMSSC에서 할당 취소된 서버로 추가됩니다. 검색에 대한 자세한 내용은 수동 검색을 사용하여 서버 검색을 참조하십시오. 동기화에 대한 자세한 내용은 등록된 Microsoft 콘솔과 동기화를 참조하십시오.
3. 검색된 서버의 모든 상세 정보를 캡처하여 작동 템플릿을 생성합니다. 자세한 내용은 참조 서버에서 운영 템플릿 작성을 참조하십시오.
4. 관리형 디바이스에서 작동 템플릿을 할당하고 템플릿 규정 준수를 확인합니다. 자세한 내용은 운영 템플릿 할당 및 운영 템플릿 규정 준수 실행을 참조하십시오.
5. 디바이스 템플릿 규정 준수를 위해 운영 템플릿을 배포합니다. 자세한 내용은 운영 템플릿 배포를 참조하십시오.
6. **작업 및 로그 센터** 페이지에서 운영 체제 배포에 대한 작업 상태를 봅니다. 자세한 내용은 작업 및 로그 센터 실행을 참조하십시오.

OMIMSSC 콘솔 확장 프로그램을 사용한 Windows가 아닌 OS의 배포

OMIMSSC를 사용하여 Windows가 아닌 OS를 배포하려면 다음 단계를 수행합니다.

노트: OMIMSSC를 통해 Windows가 아닌 운영 체제를 배포하는 단계는 Microsoft 콘솔 모두에서 일반적입니다.

1. **검색** 페이지에서 참조 서버를 검색합니다. 자세한 내용은 수동 검색을 사용하여 서버 검색을 참조하십시오.
2. 검색된 서버의 모든 상세 정보를 캡처하여 작동 템플릿을 생성합니다. 자세한 내용은 참조 서버에서 운영 템플릿 작성을 참조하십시오.
3. 관리형 디바이스에서 작동 템플릿을 할당하고 템플릿 규정 준수를 확인합니다. 자세한 내용은 운영 템플릿 할당 및 운영 템플릿 규정 준수 실행을 참조하십시오.
4. 디바이스 템플릿 규정 준수를 위해 운영 템플릿을 배포합니다. 자세한 내용은 운영 템플릿 배포를 참조하십시오.

   노트: 배포 중에 DHCP 조회가 실패하면 서버가 시간 초과되고 MECM의 **Managed Lifecycle Controller(ESXi)** 컬렉션으로 이동하지 않습니다.

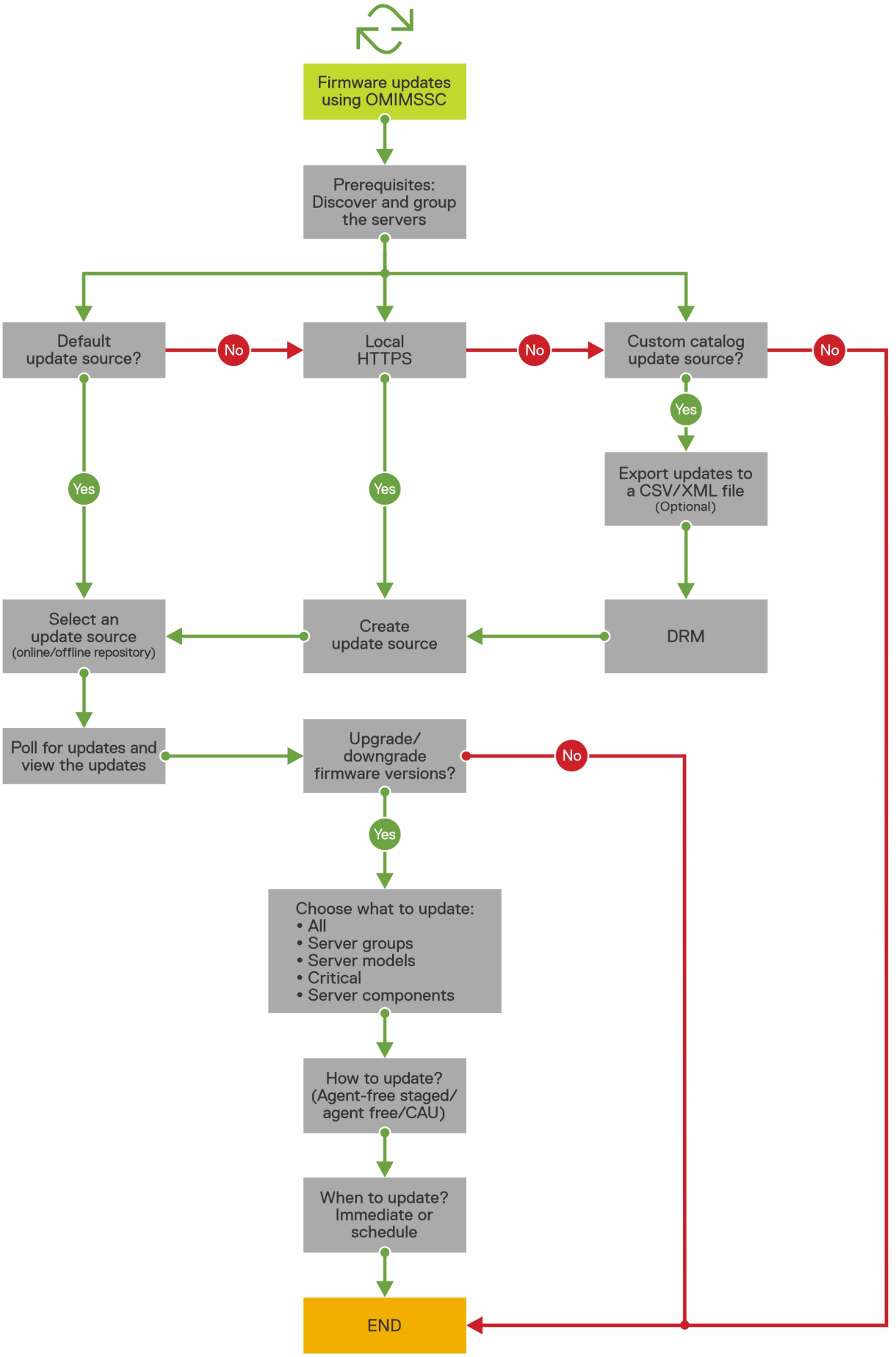
사전 정의된 작동 템플릿을 사용하여 Windows 서버 HCI 클러스터 생성

OMIMSSC를 사용하여 클러스터를 만들려면 다음 단계를 수행합니다.

1. **검색** 페이지에서 참조 서버를 검색합니다. 자세한 내용은 수동 검색을 사용하여 서버 검색을 참조하십시오.
2. 사전 정의된 작동 템플릿을 편집합니다. 자세한 내용은 작동 템플릿 수정을 참조하십시오.
3. 논리 스위치를 생성합니다. 자세한 내용은 논리 스위치 생성을 참조하십시오.
4. Windows 서버 HCI 클러스터를 만듭니다. 자세한 내용은 Windows 서버 HCI 클러스터 만들기를 참조하십시오.

서버 및 MX7000 디바이스의 펌웨어 업데이트

다음은 펌웨어 업데이트 워크플로를 그림으로 나타낸 것입니다.


Firmware updates using OMIMSSC
Prerequisites: Discover and group the servers
Default update source?
No
Local HTTPS
No
Custom catalog update source?
No
Yes
Export updates to a CSV/XML file (Optional)
Yes
Yes
Select an update source (online/offline repository)
Create update source
DRM
Poll for updates and view the updates
Upgrade/ downgrade firmware versions?
No
Yes
Choose what to update:
• All
• Server groups
• Server models
• Critical
• Server components
How to update? (Agent-free staged/ agent free/CAU)
When to update? Immediate or schedule
END

온라인 소스 또는 로컬 소스(DRM/HTTPS)를 사용하여 선택한 디바이스를 업데이트할 수 있습니다.

1. 기본 업데이트 소스를 만들거나 선택합니다. 업데이트 소스에 대한 자세한 내용은 업데이트 소스를 참조하십시오.

   노트: 폴링 및 알림 기능을 사용하여 최신 카탈로그로 업데이트 소스를 업데이트해야 합니다. 폴링 및 알림에 대한 자세한 내용은 폴링 및 알림을 참조하십시오.

   Windows 서버 HCI 클러스터를 업데이트하는 경우에는 Windows 서버 HCI 클러스터에 특정한 사전 정의된 업데이트 소스를 선택합니다. 이러한 업데이트 소스는 **유지 보수 센터** 페이지에만 표시됩니다.

   MX7000 디바이스를 업데이트하는 경우에는 모듈형 시스템 고유 사전 정의된 업데이트 소스를 선택합니다. 이러한 업데이트 소스는 **유지 보수 센터** 페이지에만 표시됩니다.

2. 기본 업데이트 그룹을 만들거나 선택합니다. 업데이트 그룹에 대한 자세한 내용은 업데이트 그룹을 참조하십시오.
3. 디바이스를 검색하거나 등록된 Microsoft 콘솔과 동기화하고 디바이스 인벤토리가 최신 상태인지 확인합니다. 검색 및 동기화에 대한 자세한 내용은 디바이스 검색 및 동기화를 참조하십시오. 서버 인벤토리에 대한 자세한 내용은 서버 보기 실행을 참조하십시오.
4. 다음 옵션 중 하나를 사용하여 디바이스를 업데이트합니다.
   - 필요한 디바이스를 선택하고 **업데이트 실행**을 클릭합니다. 자세한 내용은 업데이트 실행 방법을 이용한 펌웨어 버전 업그레이드 또는 다운그레이드를 참조하십시오.

     노트: 디바이스 구성 요소의 펌웨어를 다운그레이드하려면 **다운그레이드 허용** 확인란을 선택합니다. 이 옵션을 선택하지 않으면 펌웨어 다운그레이드가 필요한 구성 요소에 대한 작업이 없습니다.
   - 작동 템플릿에서 펌웨어 업데이트 구성 요소를 선택하고 이 템플릿을 배포합니다. 작동 템플릿에 대한 자세한 내용은 작동 템플릿을 참조하십시오.

교체된 구성 요소 구성

교체된 구성 요소의 펌웨어 버전 또는 구성 설정을 이전 구성 요소와 일치시키려면 펌웨어 및 구성 설정 적용을 참조하십시오.

서버 프로파일 내보내기 및 가져오기

특정 인스턴스에서 서버 프로파일을 내보낸 다음 프로파일을 가져와서 서버를 복원합니다.

1. 보호 볼트를 생성합니다. 보호 볼트 생성에 대한 자세한 내용은 보호 볼트 생성을 참고하십시오.
2. 서버 프로파일을 내보냅니다. 서버 프로파일 내보내기에 대한 자세한 내용은 서버 프로파일 내보내기를 참조하십시오.
3. 내보낸 서버와 동일한 서버로 서버 프로파일을 가져옵니다. 서버 프로파일 가져오기에 대한 자세한 내용은 서버 프로파일 가져오기를 참조하십시오.

   노트: RAID 구성을 프로파일로 내보낸 경우에만 RAID 구성을 포함하는 서버 프로파일을 가져올 수 있습니다.

서버 프로파일 내보내기 및 가져오기 기능은 다음에서 지원되지 않습니다.

- iDRAC 버전 4.40.00.00 이상이 설치된 서버
- iDRAC 9 기반 PowerEdge 서버

  서버 하드웨어 구성, 펌웨어 및 운영 체제 기준을 백업하려면 운영 템플릿을 사용하십시오.

18

OMIMSSC를 사용한 펌웨어 업데이트 OMIMSSC

OMIMSSC를 사용하여 보안, 문제 수정 및 개선 사항을 사용하려면 최신 펌웨어로 업그레이드하여 Dell EMC 디바이스를 최신 상태로 유지 보수합니다. Dell EMC 업데이트 리포지토리를 사용하여 디바이스의 펌웨어를 업데이트합니다.

펌웨어 업데이트는 하드웨어 호환 디바이스에서만 지원됩니다. 관리형 디바이스에서 OMIMSSC에서 사용할 수 있는 기능을 사용하려면 관리형 디바이스에 최소 필수 펌웨어 버전의 iDRAC, LC(Lifecycle Controller) 및 BIOS가 있어야 합니다. 필요한 펌웨어 버전이 있는 디바이스는 하드웨어와 호환됩니다.

주제:

업데이트 그룹 정보

업데이트 그룹은 비슷한 업데이트 관리가 필요한 디바이스 그룹입니다. OMIMSSC에서 지원되는 업데이트 그룹은 두 가지 유형이 있습니다.

- 사전 정의된 업데이트 그룹 - 사전 정의된 업데이트 그룹은 수동으로 생성, 수정 또는 삭제할 수 없습니다.
- 사용자 지정 업데이트 그룹 - 이러한 그룹에서 디바이스를 생성하고 수정하고 삭제할 수 있습니다.

노트: SCVMM에 있는 모든 서버 그룹은 OMIMSSC에 나열됩니다. 하지만 OMIMSSC에 있는 서버의 목록은 사용자와 관련이 없습니다. 따라서 이러한 디바이스에 대한 작업을 수행할 수 있는 액세스 권한이 있는지 확인해야 합니다.

사전 정의된 업데이트 그룹

디바이스를 검색한 후에 검색된 디바이스는 다음의 사전 정의된 그룹 중 하나에 추가됩니다.

- **기본 호스트 그룹** - 이 그룹은 Windows 운영 체제와 함께 배포되거나 등록된 Microsoft 콘솔과 동기화되는 서버로 구성됩니다.
- **할당 해제된 기본 그룹** - 이 그룹은 검색된 할당 해제 또는 베어 메탈 서버로 구성됩니다.
- **Windows가 아닌 기본 호스트 그룹** - 이 그룹은 Windows가 아닌 운영 체제와 함께 배포된 서버로 구성됩니다.
- **섀시 업데이트 그룹** - 이 그룹은 모듈형 서버 및 섀시 또는 모듈형 시스템으로 구성됩니다. 12세대 이상의 서버는 섀시 정보와 함께 검색됩니다. 기본적으로 그룹은 `Chassis-Service-tag-of-Chassis-Group`과 같은 이름 형식으로 생성됩니다. 예: `Chassis-GJDC4BS-Group`. 모듈형 서버가 클러스터 업데이트 그룹에서 삭제되는 경우에 해당 서버는 CMC 정보와 함께 섀시 업데이트 그룹에 추가됩니다. 섀시의 모든 모듈형 서버가 클러스터 업데이트 그룹에 있어서 해당 섀시 업데이트 그룹에 모듈형 서버가 없는 경우에도 섀시 업데이트 그룹은 계속 존재하지만 CMC 정보만 표시됩니다.
- **클러스터 업데이트 그룹** - 이 그룹은 **Windows Server 페일오버 클러스터**로 구성됩니다. 12세대 이상의 모듈형 서버가 클러스터의 일부인 경우에는 CMC 정보도 **유지 보수 센터** 페이지의 인벤토리에 추가됩니다.

사용자 지정 업데이트 그룹

검색된 디바이스를 비슷한 관리가 필요한 그룹에 추가하여 **일반 업데이트 그룹** 유형의 사용자 지정 업데이트 그룹을 생성합니다. 하지만 **할당 해제된 기본 업데이트 그룹** 및 **기본 호스트 업데이트 그룹**에서만 디바이스를 사용자 지정 업데이트 그룹에 추가할 수 있습니다. 사용자 지정 업데이트 그룹에 서버를 추가하려면 해당 서비스 태그를 사용하여 필요한 디바이스를 검색합니다. 사용자 지정 업데이트 그룹에 디바이스를 추가한 후에 해당 디바이스는 사전 정의된 업데이트 그룹에서 제거되며 사용자 지정 업데이트 그룹에서만 사용할 수 있습니다.

업데이트 그룹 보기

업데이트 그룹을 보려면

1. **OMIMSSC**에서 **유지 보수 센터**를 클릭한 다음에 **유지 보수 설정**을 클릭합니다.
2. **유지 보수 설정**에서, **업데이트 그룹**을 클릭합니다.
   생성된 모든 맞춤 지정 그룹이 그룹의 이름, 그룹 유형 및 서버 수와 함께 표시됩니다.

사용자 지정 업데이트 그룹 만들기

1. OMIMSSC 콘솔에서 **유지 보수 센터**를 클릭한 다음 **유지 보수 설정**을 클릭합니다.
2. **유지 보수 설정**에서 **업데이트 그룹**을 클릭한 다음 **만들기**를 클릭합니다.
   펌웨어 업데이트 그룹 페이지가 표시됩니다.
3. 그룹 이름과 설명을 입력하고 생성할 업데이트 그룹의 유형을 선택합니다.
   사용자 지정 업데이트 그룹은 다음과 같은 업데이트 그룹 유형에서만 서버를 사용할 수 있습니다.
   - 일반 업데이트 그룹 - 할당되지 않은 업데이트 그룹 및 기본 호스트 업데이트 그룹의 서버로 구성되어 있습니다.
   - 호스트 업데이트 그룹 – 기본 호스트 업데이트 그룹의 서버로 구성되어 있습니다.

   또한 두 가지 유형의 서버 그룹에서 서버를 조합하여 사용할 수 있습니다.
4. 업데이트 그룹에 서버를 추가하려면 서비스 태그를 사용하여 서버를 검색하고, **업데이트 그룹 테이블에 포함된 서버** 표에 서버를 추가하려면 오른쪽 화살표를 클릭합니다.
5. 사용자 지정 업데이트 그룹을 생성하려면 **저장**을 클릭합니다.

   노트: 사용자 지정 업데이트 그룹은 시스템 센터에 따라 다르며 동일한 시스템 센터의 다른 사용자가 볼 수 있습니다.

사용자 지정 업데이트 그룹 수정

사용자 지정 업데이트 그룹을 수정할 때는 다음 사항을 고려하십시오.

- 업데이트 그룹이 생성된 후 업데이트 그룹의 유형을 변경할 수 없습니다.
- 서버를 한 사용자 지정 업데이트 그룹에서 다른 사용자 지정 업데이트 그룹으로 이동하기 위해 다음을 수행할 수 있습니다.
  1. 기존 사용자 지정 업데이트 그룹에서 서버를 제거합니다. 그러면 미리 정의된 업데이트 그룹에 자동으로 추가됩니다.
  2. 서버를 추가할 사용자 지정 그룹을 편집하고 서비스 태그를 사용하여 서버를 검색합니다.

1. **OMIMSSC**에서 **유지 보수 센터**를 클릭한 다음에 **유지 보수 설정**을 클릭합니다.
2. **유지 보수 설정**에서 **업데이트 그룹**을 클릭하고, 업데이트 그룹을 선택한 다음, **편집**을 클릭하여 업데이트 그룹을 수정합니다.

맞춤 구성 업데이트 그룹 삭제

다음과 같은 상황에서 사용자 지정 업데이트 그룹을 삭제하는 경우에는 다음 사항을 고려하십시오.

- 작업이 예약되어 있거나 진행 또는 대기 중인 경우에는 업데이트 그룹을 삭제할 수 없습니다. 따라서 서버 그룹을 삭제하기 전에 사용자 지정 업데이트 그룹과 연결된 예약 작업을 삭제하십시오.
- 업데이트 그룹에 서버가 있는 경우에도 업데이트 그룹을 삭제할 수 있습니다. 하지만 이러한 업데이트 그룹을 삭제하면 해당 서버가 각 사전 정의된 업데이트 그룹으로 이동합니다.
- 사용자 지정 업데이트 그룹에 있는 디바이스가 MSSC에서 삭제되고 사용자가 OMIMSSC를 등록된 MSSC와 동기화하는 경우에 해당 디바이스는 사용자 지정 업데이트 그룹에서 제거되고 해당하는 사전 정의된 그룹으로 이동됩니다.

1. **OMIMSSC**에서 **유지 보수 센터**를 클릭한 다음에 **유지 보수 설정**을 클릭합니다.
2. **유지 보수 설정**에서, **업데이트 그룹**을 클릭하고 업데이트 그룹을 선택한 다음, **삭제**를 클릭하여 업데이트 그룹을 삭제합니다.

업데이트 소스 정보

업데이트 소스는 Dell EMC 업데이트(BIOS, 관리 구성 요소, 네트워크 카드와 같은 드라이버 팩)가 포함된 카탈로그 파일을 참조하며 DUP(Dell Update Package)라는 자체 포함 실행 파일을 제공합니다.

업데이트 소스 또는 리포지토리를 만들어 비교 보고서를 생성하는 기본 업데이트 소스로 설정하고 리포지토리에서 새 카탈로그 파일을 사용할 수 있을 때 알림을 받을 수 있습니다.

OMIMSSC를 사용하면 온라인 또는 오프라인 업데이트 소스를 사용하여 디바이스 펌웨어를 최신 상태로 유지할 수 있습니다.

온라인 업데이트 소스는 Dell EMC에서 관리하는 리포지토리입니다.

오프라인 업데이트 소스는 로컬 리포지토리이며 인터넷에 연결되어 있지 않을 때 사용됩니다.

OMIMSSC 어플라이언스의 로컬 인트라넷에 사용자 지정 리포지토리를 생성하고 네트워크 공유를 배치하는 것이 좋습니다. 이렇게 하면 인터넷 대역폭이 절약되며 안전한 내부 리포지토리도 제공됩니다.

다음 업데이트 소스 중 하나를 사용하여 펌웨어를 업데이트합니다.

- **DRM 리포지토리** - 오프라인 리포지토리입니다. OMIMSSC 어플라이언스에서 검색된 디바이스의 인벤토리 정보를 내보내 DRM에 리포지토리를 준비합니다. DRM과의 통합 및 DRM을 통한 업데이트 소스 생성에 대한 자세한 내용은 DRM과의 통합을 참조하십시오. OMIMSSC에서 DRM에 리포지토리를 생성한 후 DRM을 통해 생성된 업데이트 소스, 관련 디바이스를 선택하고 디바이스에 대한 업데이트를 시작합니다. DRM에 대한 자세한 내용은 `dell.com\support`에서 제공되는 Dell Repository Manager 문서를 참조하십시오.
- **HTTPS** - 온라인 또는 오프라인 리포지토리일 수 있습니다. HTTPS 사이트에서 제공되는 최신 업데이트와 관련하여 디바이스의 특정 구성 요소를 업데이트합니다. Dell EMC에서는 2개월마다 리포지토리를 준비하고 PDK 카탈로그를 통해 다음 업데이트를 게시합니다.
  - 서버 BIOS 및 펌웨어
  - Dell EMC 인증 운영 체제 드라이버 팩(운영 체제 배포용)

  노트: 작동 템플릿을 배포하는 동안 온라인 업데이트 소스를 선택하면 최신 펌웨어 버전이 다운로드되어 관리되는 디바이스에 적용됩니다. 따라서 참조와 배포된 디바이스 간의 펌웨어 버전이 다를 수 있습니다.
- **참조 펌웨어 인벤토리 및 비교** - DRM을 통해 오프라인 리포지토리로 변환할 수 있습니다. 선택한 디바이스의 펌웨어 인벤토리를 포함하는 참조 인벤토리 파일을 만듭니다. 참조 인벤토리 파일은 유형 또는 모델이 같은 디바이스 또는 유형이나 모델이 서로 다른 여러 디바이스의 인벤토리 정보를 포함할 수 있습니다. OMIMSSC에 존재하는 디바이스의 인벤토리 정보를 저장된 참조 인벤토리 파일과 비교할 수 있습니다. 내보낸 파일을 DRM으로 전달하고 리포지토리를 만들려면 `dell.com\support`에서 제공되는 *Dell Repository Manager* 문서를 참조하십시오.

사전 정의된 업데이트 소스 및 기본 업데이트 소스

OMIMSSC에는 새로 설치하거나 업그레이드한 후 사용할 수 있는 사전 정의된 업데이트 소스가 포함되어 있습니다. **DELL EMC ENTERPRISE CATALOG**는 HTTPS 유형의 사전 정의된 기본 업데이트 소스입니다. 그러나 다른 업데이트 소스를 만들어 기본 업데이트 소스로 표시할 수 있습니다.

노트: 프록시 서버를 사용하는 경우, 리포지토리에 액세스하려면 업데이트 소스를 편집하여 프록시 상세 정보를 추가하고 변경 내용을 저장합니다.

Windows 서버 HCI 클러스터에 대한 사전 정의된 기본 업데이트 소스

OMIMSSC 사전 정의된 특정 업데이트 소스를 통해 Windows 서버 HCI 클러스터 업데이트를 지원합니다. 이러한 업데이트 소스는 Windows 서버 HCI 클러스터에 대한 구성 요소의 권장 최신 펌웨어 버전이 포함된 카탈로그 파일을 참조합니다. 이러한 파일은 **유지 보수 센터** 페이지에만 표시됩니다.

MICROSOFT HCI 솔루션용 카탈로그 업데이트는 사전 정의된 HTTPS 유형의 기본 업데이트 소스이며 **DELL EMC 엔터프라이즈 카탈로그**에 포함되어 있습니다.

모듈형 시스템에 대해 사전 정의된 기본 업데이트 소스

OMIMSSC OMIMSSC는 사전 정의된 특정 업데이트 소스를 통해 모듈형 시스템을 업데이트할 수 있도록 지원합니다. 이러한 업데이트 소스는 모듈형 시스템용 구성 요소의 권장 최신 펌웨어 버전이 포함된 카탈로그 파일을 참조합니다. 이러한 파일은 **유지 보수 센터** 페이지에만 표시됩니다.

DELL EMC MX 솔루션 카탈로그는 사전 정의된 HTTPS 유형의 기본 업데이트 소스이며 **DELL EMC 엔터프라이즈 카탈로그**에 포함되어 있습니다.

테스트 연결을 사용하여 데이터 유효성 검사

업데이트 소스를 생성하는 동안 언급된 자격 증명을 이용하여 업데이트 소스에 연결할 수 있는지 확인하려면 **테스트 연결**을 사용합니다. 연결이 성공한 후에만 업데이트 소스를 만들 수 있습니다.

로컬 HTTPS 설정

로컬 HTTPS를 설정하려면 다음을 수행합니다.

1. `downloads.dell.com`을 똑같이 복제한 폴더 구조를 로컬 HTTPS에 생성합니다.
2. 온라인 HTTPS(`https://downloads.dell.com/catalog/catalog.xml.gz`)에서 `catalog.gz` 파일을 다운로드하고 압축을 풉니다.
3. `catalog.xml` 파일을 압축 해제하고 **baseLocation**을 로컬 HTTPS URL로 변경하고 `.gz` 확장명으로 파일을 압축합니다. 예를 들어 **baseLocation**을 `downloads.dell.com`에서 `hostname.com`과 같은 호스트 이름 또는 IP 주소로 변경합니다.
4. `downloads.dell.com`의 구조를 똑같이 복제한 로컬 HTTPS 폴더에 카탈로그 파일과 수정된 카탈로그 파일 및 DUP 파일을 배치합니다.

업데이트 소스 보기

1. **OMIMSSC**에서 **유지 보수 센터**를 클릭합니다.
2. **유지 보수 센터**에서 **유지 보수 설정**를 클릭한 다음 **업데이트 소스**를 클릭합니다.
   설명, 소스 유형, 위치 및 자격 증명 프로파일 이름과 함께 생성되는 모든 업데이트 소스가 표시됩니다.

업데이트 소스 생성

- 업데이트 소스 유형을 기준으로 Windows 자격 증명 프로파일을 사용할 수 있는지 확인합니다.
- DRM 업데이트 소스를 만드는 경우에는 관리자 역할이 있는 DRM을 설치하고 구성해야 합니다.

1. OMIMSSC 콘솔에서 **유지 보수 센터**를 클릭한 다음 **유지 보수 설정**을 클릭합니다.
2. **업데이트 소스**를 클릭합니다.
3. **업데이트 소스** 페이지에서 **새로 만들기**를 클릭하고 업데이트 소스 이름 및 설명을 제공합니다.
4. **소스 유형** 드롭다운 메뉴에서 업데이트 소스 유형을 선택합니다.
   - HTTPS 소스 - 온라인 HTTPS 업데이트 소스를 생성하려면 선택합니다.
     노트: HTTPS 유형의 업데이트 소스를 생성하려는 경우, 업데이트 소스에 액세스하기 위해 카탈로그 이름을 포함한 카탈로그의 전체 경로와 프록시 자격 증명을 제공합니다.

     DRM 저장소 - 로컬 저장소 업데이트 소스를 생성하려면 선택합니다. DRM을 설치했는지 확인합니다.
     노트: DRM 소스를 생성하는 경우에는 Windows 자격 증명을 입력하고 Windows 공유 위치에 액세스할 수 있는지 확인합니다. 위치 필드에 카탈로그 파일의 전체 경로와 파일 이름을 입력합니다.
   - 인벤토리 출력 파일 - 참조 서버 구성에 대한 펌웨어 인벤토리를 보려면 선택합니다.
     노트: **인벤토리 출력 파일**을 업데이트 소스로 사용하여 비교 보고서를 볼 수 있습니다. 참조 서버의 인벤토리 정보와 OMIMSSC에서 검색된 다른 모든 서버의 정보를 비교합니다.
5. **위치**에 HTTPS 소스의 업데이트 소스 URL과 DRM에 대한 Windows 공유 위치를 입력합니다.
6. 업데이트 소스에 액세스하려면 **자격 증명**에서 필요한 자격 증명 프로파일을 선택합니다.
7. HTTPS 소스에 액세스하기 위해 프록시가 필요한 경우에는 **프록시 자격 증명**에서 적절한 프록시 자격 증명을 선택합니다.
8. (선택 사항) 생성된 업데이트 소스를 기본 업데이트 소스로 설정하려면 **이 소스를 기본 소스로 설정**을 선택합니다.
9. 언급된 자격 증명을 사용하여 업데이트 소스의 위치에 연결할 수 있는지 확인하려면 **연결 테스트**를 클릭한 다음에 **저장**을 클릭합니다.

   노트: 연결 테스트에 성공한 후에만 업데이트 소스를 생성할 수 있습니다.

업데이트 소스 편집

업데이트 소스를 수정하기 전에 다음 사항을 고려하십시오.

- **Microsoft HCI 솔루션용 업데이트 카탈로그**에 대한 업데이트 소스를 편집하려면 미리 정의된 해당 업데이트 소스를 편집하고 변경 내용을 저장합니다. 이 업데이트는 **Microsoft HCI 솔루션용 업데이트 카탈로그**에 대한 업데이트 소스에 반영됩니다.
- 업데이트 소스가 생성된 후 업데이트 소스의 유형과 위치를 변경할 수 없습니다.
- 업데이트 소스를 진행 중이거나 예약된 작업에서 사용하고 있거나 배포 템플릿에서 사용하고 있는 경우에도 업데이트 소스를 수정할 수 있습니다. 사용 중인 업데이트 소스를 수정하는 동안에 경고 메시지가 표시됩니다. 변경 사항을 보려면 **확인**을 클릭합니다.

- 업데이트 소스에서 카탈로그 파일을 업데이트할 때 로컬에서 캐싱된 카탈로그 파일은 자동으로 업데이트되지 않습니다. 캐시에 저장된 카탈로그 파일을 업데이트하려면 업데이트 소스를 편집하거나 업데이트 소스를 삭제한 후에 다시 작성합니다.

수정할 업데이트 소스를 선택하고 **편집**을 클릭하고 필요에 따라 소스를 업데이트합니다.

업데이트 소스 제거

업데이트 소스를 삭제하기 전에 다음 사항을 고려하십시오.

- 사전 정의된 업데이트 소스는 삭제할 수 없습니다.
- 업데이트 소스가 진행 중 또는 예약된 작업에 사용되는 경우에는 삭제할 수 없습니다.
- 업데이트 소스가 기본 업데이트 소스인 경우에는 업데이트 소스를 삭제할 수 없습니다.

삭제하려는 업데이트 소스를 선택하고 **삭제**를 클릭합니다.

DRM(Dell EMC Repository Manager)과 통합

OMIMSSC OMIMSSC에서 맞춤 구성 업데이트 소스를 만들려면 DRM과 통합합니다. 통합은 DRM 버전 2.2 이상에서 지원됩니다. OMIMSSC 어플라이언스에서 검색된 디바이스 정보를 DRM에 제공하고 사용 가능한 인벤토리 정보로 DRM에서 맞춤 구성 리포지토리를 만들고 OMIMSSC에서 업데이트 소스로 설정하여 펌웨어 업데이트를 수행하고 관리형 디바이스에서 클러스터를 만들 수 있습니다. DRM에서 리포지토리 생성에 대한 자세한 내용은 `Dell.com/support/home`에 나와 있는 Dell EMC Repository Manager 설명서를 참조하십시오.

DRM 통합 OMIMSSC

이 섹션에서는 통합하여 리포지토리를 생성하는 과정에 대해 설명합니다.

노트: 필요한 업데이트를 준비하려면 테스트 환경 테스트, 보안 업데이트, 애플리케이션 권장 사항, Dell EMC 권장 사항과 같은 요소를 고려해야 합니다.

노트: 검색된 디바이스에 대한 최신 인벤토리 정보를 보려면 OMIMSSC를 업그레이드한 후에 DRM을 OMIMSSC 어플라이언스와 다시 통합하십시오.

1. 홈 페이지에서 **새 리포지토리 추가**를 클릭합니다. **새 리포지토리 추가** 창이 표시됩니다.
2. **통합** 탭을 선택하고 **리포지토리 이름**과 **설명**을 입력합니다.
3. **맞춤 구성**을 선택하고 **시스템 선택**을 클릭하여 특정 시스템을 선택합니다.
4. **통합 유형** 드롭다운 메뉴에서 통합할 제품을 선택합니다. 선택한 제품에 따라 다음 옵션이 표시됩니다. 사용 가능한 옵션은 다음과 같습니다.
   a. Microsoft System Center용 Dell OpenManage 통합 - 호스트 이름 또는 IP, 사용자 이름, 암호 및 프록시 서버를 제공합니다.

      노트: 암호에 `<, >, ',", &`와 같은 특수 문자가 포함되어 있지 않은지 확인합니다.

   b. Dell Console Integration - URL https://<IP>/genericconsolerepository, Admin을 사용자 이름, 암호 및 프록시 서버로 제공합니다.

      노트: Dell Console Integration은 SCVMM(OpenManage Integration for System Center Virtual Machine Manager)과 같은 웹 서비스를 통합한 콘솔에 적용됩니다.

5. 필요한 옵션을 선택한 후 **연결**을 클릭합니다. 사용 가능한 시스템 및 모델이 **통합 유형** 섹션에 표시됩니다.
6. **생성**을 클릭하여 리포지토리를 생성합니다. 홈 페이지에서 사용할 수 있는 리포지토리 대시보드에 리포지토리가 표시됩니다.

   노트: 번들 유형 또는 DUP 형식을 선택하는 경우 Dell PowerEdge MX7000 섀시가 OMIMSSC의 인벤토리에 속할 경우 Windows 64비트 및 운영 체제 독립성을 선택해야 합니다.

DRM을 OMIMSSC와 통합한 후에 다음에서 *Ready Node 수명주기 관리 및 모니터링을 위한 Dell EMC Microsoft HCI Solutions Microsoft Windows Server Ready Node 운영 가이드*의 *Dell Repository Manager를 이용한 HCI Solutions for Microsoft Windows Server Ready Nodes용 펌웨어 카탈로그 구하기*를 참조하십시오. `dell.com/support`

폴링 주파수 설정

업데이트 소스에 기본적으로 선택되는 새 카탈로그 파일이 있을 때 알림을 수신하도록 폴링 및 알림을 구성합니다. OMIMSSC 어플라이언스는 업데이트 소스의 로컬 캐시를 저장합니다. 업데이트 소스에 사용 가능한 새 카탈로그 파일이 있는 경우 알림 종의 색상이 주황색으로 변경됩니다. OMIMSSC 어플라이언스에서 사용 가능한 로컬에 캐싱된 카탈로그를 교체하려면 종 아이콘을 클릭합니다. 이전 카탈로그 파일을 최신 카탈로그 파일로 바꾸면 종 색상이 녹색으로 바뀝니다.

폴링 빈도를 설정하려면 다음을 수행합니다.

1. OMIMSSC에서 **유지 보수 센터**를 클릭한 다음에 **폴링 및 알림**을 클릭합니다.
2. **폴링 및 알림**을 클릭합니다.
3. 얼마나 자주 폴링할지를 선택합니다.
   - **사용 안 함** - 이 옵션은 기본적으로 선택되어 있습니다. 업데이트를 수신하지 않으려면 선택합니다.
   - **일주일에 한 번** - 업데이트 소스에서 사용 가능한 새 카탈로그에 대한 업데이트를 주 단위로 수신하려면 선택합니다.
   - **2주에 한 번** - 업데이트 소스에서 사용 가능한 새 카탈로그에 대한 업데이트를 2주에 한 번 수신하려면 선택합니다.
   - **한 달에 한 번** - 업데이트 소스에서 사용 가능한 새 카탈로그에 대한 업데이트를 월 단위로 수신하려면 선택합니다.

디바이스 인벤토리 보기 및 새로 고침

유지 보수 센터 페이지에서 디바이스의 업데이트 소스와 디바이스의 비교 보고서를 봅니다. 업데이트 소스를 선택하면 선택한 업데이트 소스에 있는 펌웨어와 기존 펌웨어를 비교하는 보고서가 표시됩니다. 업데이트 소스를 변경하면 보고서가 동적으로 생성됩니다. 서버 인벤토리가 업데이트 소스와 비교되고 추천 조치가 나열됩니다. 이 작업은 디바이스 및 디바이스 구성 요소의 수에 따라 상당한 시간이 소요됩니다. 이 프로세스 중에는 다른 작업을 수행할 수 없습니다. 인벤토리를 새로 고치면 해당 디바이스에서 단일 구성 요소를 선택해도 전체 디바이스의 인벤토리가 새로 고쳐집니다.

가끔 디바이스의 인벤토리가 업데이트되지만 페이지에 최신 인벤토리가 표시되지 않는 경우가 있습니다. 따라서 새로 고침 옵션을 사용하여 검색된 디바이스의 최신 인벤토리 정보를 봐야 합니다.

노트: OMIMSSC의 최신 버전으로 업그레이드한 후 `downloads.dell.com`에 연결할 수 없는 경우 기본 Dell 온라인 DELL EMC ENTERPRISE CATALOG 업데이트 소스가 카탈로그 파일을 다운로드할 수 없습니다. 따라서 비교 보고서를 사용할 수 없습니다. 기본 업데이트 소스에 대한 비교 보고서를 보려면 DELL EMC 엔터프라이즈 카탈로그 업데이트 소스를 편집한 다음(필요한 경우 프록시 자격 증명 입력) **업데이트 소스 선택** 드롭다운 메뉴에서 동일한 옵션을 선택합니다. 업데이트 소스 편집에 대한 자세한 내용은 업데이트 소스 수정을 참조하십시오.

노트: 제품 제공 시 카탈로그 파일의 로컬 사본이 OMIMSSC에 있습니다. 따라서 최신 비교 보고서를 사용할 수 없습니다. 최신 비교 보고서를 보려면 카탈로그 파일을 업데이트합니다. 카탈로그 파일을 업데이트하려면 업데이트 소스를 편집하여 저장하거나 업데이트 소스를 삭제하고 다시 작성합니다.

노트: MECM에서 재고 정보를 새로 고친 후에도 **드라이버 팩 버전** 및 운영 체제에 **사용 가능한 드라이버** 같은 서버 상세 정보는 **Dell OOB(Out of Band) 컨트롤러** 속성 페이지에서 업데이트되지 않습니다. OOB 속성을 업데이트하려면 OMIMSSC를 등록된 MECM과 동기화합니다.

노트: OMIMSSC를 업그레이드하면 이전 버전에서 검색된 서버에 대한 정보가 표시되지 않습니다. 최신 서버 정보 및 올바른 비교 보고서를 보려면 서버를 재검색합니다.

검색된 디바이스의 펌웨어 인벤토리를 새로 고치고 보려면 다음을 수행합니다.

1. **OMIMSSC**에서 **유지 보수 센터**를 클릭합니다.
   유지 보수 센터 페이지는 OMIMSSC에서 발견된 모든 디바이스에 대한 비교 보고서와 함께 선택한 업데이트 소스에 대한 보고서를 표시합니다.
2. (선택 사항) 특정 디바이스 그룹에 대한 비교 보고서만 보려면 필요한 디바이스만 선택합니다.
3. (선택 사항) 다른 업데이트 소스에 대한 비교 보고서를 보려면 **업데이트 소스 선택** 드롭다운 목록에서 업데이트 소스를 선택하여 업데이트 소스를 변경합니다.
4. 현재 버전, 베이스라인 버전 및 Dell EMC에서 권장하는 업데이트 작업에 대한 펌웨어 정보를 보려면 **디바이스 그룹/서버**에서 서버 수준으로 서버 그룹을 확장한 후 구성 요소 수준으로 확장합니다. 또한 디바이스의 추천 업데이트 수를 봅니다. 사용 가능한 업데이트 아이콘 위에 커서를 올려놓으면 중요한 업데이트 수, 권장 업데이트 등 해당 업데이트의 세부 정보가 표시됩니다.

   사용 가능한 업데이트 아이콘 표시 색상은 업데이트의 전체적인 중요도를 기반으로 하며, 중요한 업데이트 범주는 다음과 같습니다.

   - 서버 또는 서버 그룹에 하나의 중요한 업데이트가 있어도 색상은 빨간색입니다.
   - 중요한 업데이트가 없으면 색상은 노란색입니다.

- 펌웨어 버전이 최신이면 색상은 녹색입니다.

비교 보고서를 채운 후 다음과 같은 업데이트 작업이 제안됩니다.

- 다운그레이드 - 이전 버전을 사용할 수 있으며 기존 펌웨어를 이 버전으로 다운그레이드할 수 있습니다.
- 조치 필요 없음 - 기존 펌웨어가 업데이트 소스의 펌웨어와 동일합니다.
- 사용 가능한 업데이트 없음 - 이 구성 요소에 대한 업데이트를 사용할 수 없습니다.

  노트: MX7000 모듈형 시스템 및 온라인 카탈로그의 서버에서 PSU(Power Supply Unit) 구성 요소에 사용할 수 있는 업데이트가 없습니다. MX7000 모듈형 시스템의 PSU 구성 요소를 업데이트하려면 Dell EMC PowerEdge MX7000 디바이스의 전원 공급 장치 구성 요소 업데이트를 참조하십시오. 서버용 PSU 구성 요소를 업데이트하려면 Dell EMC 지원에 문의하십시오.
- 업그레이드 - 선택 사항 - 업데이트는 선택 사항이며, 새 기능 또는 특정 구성 업그레이드로 구성됩니다.
- 업그레이드 - 긴급 - BIOS 등과 같은 구성 요소의 보안, 성능 또는 고장 수리 상황을 해결하는 데 사용되는 중요한 업데이트입니다.
- 업그레이드 - 권장 - 업데이트는 구성 요소에 대한 문제 해결 또는 기능 향상입니다. 또한 다른 펌웨어 업데이트와의 호환성 수정 사항이 포함되어 있습니다.

필터 적용

선택한 정보를 비교 보고서에서 보려면 필터를 적용합니다.

사용 가능한 서버 구성 요소를 기준으로 비교 보고서를 필터링합니다. OMIMSSC는 세 가지 필터 범주를 지원합니다.

- **업데이트 특성** - 선택한 업데이트 유형만 서버에서 필터링하고 보려면 선택합니다.
- **구성 요소 유형** - 선택한 구성 요소만 서버에서 필터링하고 보려면 선택합니다.
- **서버 모델** - 선택한 서버 모델만 필터링하고 보려면 선택합니다.

노트: 필터가 적용되면 서버 프로파일을 내보내고 가져올 수 없습니다.

필터를 적용하려면 다음을 수행합니다.

OMIMSSC에서 **유지 보수 센터**를 클릭하고 필터 드롭다운 메뉴를 클릭한 다음 필터를 선택합니다.

필터 제거

필터를 제거하려면 다음을 수행합니다.

OMIMSSC에서 **유지 보수 센터**를 클릭한 다음 **필터 지우기**를 클릭하거나 선택한 확인란을 선택 해제합니다.

업데이트 실행 메서드를 사용하여 펌웨어 버전 업그레이드 및 다운그레이드

디바이스에 업데이트를 적용하기 전에 다음 조건이 충족되는지 확인합니다.

- 업데이트 소스를 사용할 수 있습니다.

  노트: Microsoft HCI 솔루션 업데이트 소스 또는 Dell EMC MX 솔루션 카탈로그 업데이트 소스를 위한 업데이트 카탈로그를 선택하십시오. 그 이후 Windows 서버 HCI 클러스터 또는 MX7000 모듈형 시스템에 펌웨어 업데이트를 적용합니다. 이러한 업데이트 소스는 Windows 서버 HCI 클러스터 및 모듈형 시스템용 구성 요소의 권장 펌웨어 버전이 포함된 카탈로그에 대한 수정된 참조를 확인합니다.
- iDRAC 또는 관리 모듈(MM) 작업 대기열은 관리형 디바이스에 업데이트를 적용하기 전에 지워집니다.

OMIMSSC와 하드웨어 호환되는 선택된 디바이스 그룹에 업데이트를 적용합니다. 업데이트를 즉시 적용하거나 예약할 수 있습니다. 펌웨어 업데이트를 위해 생성된 작업은 **작업 및 로그 센터** 페이지에 나열됩니다.

펌웨어를 업그레이드하거나 다운그레이드하기 전에 다음 사항을 고려하십시오.

- 이 작업을 시작할 때 존재하는 디바이스 및 디바이스 구성 요소의 수에 따라 작업 상당 시간이 소요됩니다.
- 디바이스의 단일 구성 요소 또는 전체 환경에 펌웨어 업데이트를 적용할 수 있습니다.
- 디바이스에 해당하는 업그레이드 또는 다운그레이드가 없는 경우에는 디바이스에 펌웨어 업데이트를 수행해도 디바이스에 아무 작업도 수행되지 않습니다.

- 섀시 업데이트의 경우에는 Dell PowerEdge M1000e Chassis Management Controller 펌웨어 사용자 가이드의 CMC 펌웨어 업데이트 섹션을 참조하십시오.
  - VRTX의 섀시 펌웨어 업데이트에 대해서는 Dell PowerEdge VRTX용 Dell Chassis Management Controller 사용자 가이드의 펌웨어 업데이트 섹션을 참조하십시오.
  - FX2의 섀시 펌웨어 업데이트에 대해서는 Dell PowerEdge FX2용 Dell Chassis Management Controller 사용자 가이드의 펌웨어 업데이트 섹션을 참조하십시오.

1. OMIMSSC에서 **유지 보수 센터**를 클릭하고 서버 또는 모듈형 시스템 그룹과 업데이트 소스를 선택한 다음에 **업데이트 실행**을 클릭합니다.
2. 서버 또는 모듈형 시스템 그룹과 업데이트 소스를 선택한 다음에 **업데이트 실행**을 클릭합니다.
3. **업데이트 상세 정보**에 펌웨어 업데이트 작업 이름 및 설명을 입력합니다.
4. 펌웨어 버전 다운그레이드를 활성화하려면 **다운그레이드 허용** 확인란을 선택합니다.
   이 옵션을 선택하지 않으면 펌웨어 다운그레이드가 필요한 구성 요소에 대한 작업이 없습니다.
5. **업데이트 예약**에서 다음 중 하나를 선택합니다.
   - **지금 실행** - 업데이트를 즉시 적용하려면 선택합니다.
   - 향후에 펌웨어 업데이트를 예약할 날짜 및 시간을 선택합니다.
6. 다음 방법 중 하나를 선택하고 **완료**를 클릭합니다.
   - **에이전트가 필요 없는 스테이징 업데이트** - 시스템을 재시작하지 않고 적용할 수 있는 업데이트가 즉시 적용되며 재시작이 필요한 업데이트는 시스템이 재시작할 때 적용됩니다. 모든 업데이트가 적용되었는지 확인하려면 인벤토리를 새로 고칩니다. 단 하나의 디바이스에서라도 작업이 실패하면 전체 업데이트 작업이 실패합니다.
   - **에이전트가 필요 없는 업데이트** - 업데이트가 적용되고 시스템이 즉시 재시작됩니다.

     노트: OMIMSSC MX7000 모듈형 시스템에 **에이전트가 필요 없는 업데이트**만 지원합니다.

   노트: **클러스터 인식 업데이트(CAU)** - 서버의 가용성을 유지하면서 Windows CAU 기능을 클러스터 업데이트 그룹에 사용하여 업데이트 프로세스를 자동화합니다. 업데이트는 SCVMM 서버가 설치된 동일한 시스템에 있는 클러스터 업데이트 코디네이터로 전달됩니다. 업데이트 프로세스는 자동화되어 서버 가용성이 유지됩니다. 업데이트 작업은 **업데이트 방법** 드롭다운 메뉴에서 선택한 항목에 관계없이 Microsoft 클러스터 인식 업데이트(CAU) 기능으로 제출됩니다. 자세한 내용은 CAU를 사용한 업데이트를 참조하십시오.

   노트: 펌웨어 업데이트 작업을 iDRAC에 제출한 후에 OMIMSSC는 작업의 상태를 확인하기 위해 iDRAC와 상호 작용하고 상태를 OMIMSSC 관리 포털의 **작업 및 로그** 페이지에 표시합니다. iDRAC에서 오랫동안 작업 상태에 대한 응답이 없는 경우에는 작업 상태가 실패로 표시됩니다.

CAU를 사용한 업데이트

(클러스터의 일부인) 서버에 대한 업데이트는 SCVMM 서버가 설치된 동일한 시스템에 있는 클러스터 업데이트 코디네이터를 통해 수행됩니다. 업데이트는 스테이징되지 않으며 즉시 적용됩니다. 클러스터 인식 업데이트(CAU)를 사용하면 중단이나 서버 다운타임을 최소화하여 워크로드의 무중단 가용성을 실현할 수 있습니다. 따라서 클러스터 그룹에서 제공하는 서비스에는 영향을 미치지 않습니다. CAU에 대한 자세한 내용은 `technet.microsoft.com`에서 클러스터 인식 업데이트 개요를 참조하십시오.

클러스터 업데이트 그룹에 업데이트를 적용하기 전에 다음을 확인하십시오.

- 등록된 사용자에게 CAU 기능을 통해 클러스터를 업데이트할 수 있는 관리자 권한이 있는지 확인합니다.
- 선택한 업데이트 소스에 대한 연결성.
- 페일오버 클러스터 가용성.
- 클러스터 업데이트 준비 상태를 확인하고 CAU 방법을 적용하기 위한 클러스터 준비 보고서에 주요 오류 및 경고가 없다는 것을 확인합니다. CAU에 대한 자세한 내용은 `Technet.microsoft.com`에서 클러스터 인식 업데이트에 대한 요구 사항 및 모범 사례 섹션을 참조하십시오.
- CAU 기능을 지원할 수 있도록 모든 페일오버 클러스터 노드에 Windows Server 2012 R2, Windows 2016 또는 Windows 2019 운영 체제가 설치되어 있는지 확인합니다.
- 페일오버 클러스터 노드에서 업데이트를 자동으로 설치하게 하는 자동 업데이트 구성이 활성화되어 있지 않습니다.
- 페일오버 클러스터의 각 노드에서 원격 종료를 허용하는 방화벽 규칙을 활성화합니다.
- 클러스터 그룹에 최소 두 개의 노드가 있는지 확인합니다.

노트:

- 업데이트 적용에 대한 자세한 내용은 업데이트 실행 방법을 이용한 펌웨어 버전 업그레이드 및 다운그레이드를 참조하십시오. 펌웨어 및 드라이버 업데이트를 다운로드하는 Dell EMC Repository Manager에 대한 자세한 내용은 `dell.com\support`의 Microsoft Azure Stack HCI용 Dell EMC Solutions용 펌웨어 및 드라이버 업데이트 카탈로그 페이지로 이동하여 카탈로그 파일을 다운로드하십시오.

19

OMIMSSC를 이용한 디바이스 관리 OMIMSSC

서버 및 모듈형 시스템 구성 요소의 펌웨어를 업그레이드하기 위한 작업을 예약하여 서버 및 모듈형 시스템을 최신 상태로 유지합니다. 이전 구성을 내보내고, 교체된 구성 요소에 이전 구성 요소의 구성을 적용하고, 문제 해결을 위해 LC 로그를 내보내 서버를 이전 상태로 복구하여 서버를 관리합니다.

주제:

서버 복구

서버의 구성을 프로필로 내보내고 같은 서버에 프로필을 가져와서 서버의 구성을 보호 볼트에 저장하여 이전 상태로 복구합니다.

보호 볼트

보호 볼트는 서버 프로필을 저장할 수 있는 안전한 위치입니다. 서버 또는 서버 그룹에서 서버 프로필을 내보내고 동일한 서버 또는 서버 그룹으로 가져옵니다. 이 서버 프로필을 외부 볼트를 생성하여 네트워크의 공유 위치에 저장할 수도 있고 내부 볼트를 생성하여 vFlash SD(Secure Digital) 카드에 저장할 수도 있습니다. 서버 또는 서버 그룹을 단 하나의 보호 볼트에만 연결할 수 있습니다. 하지만 하나의 보호 볼트를 다수의 서버 또는 서버 그룹에 연결할 수 있습니다. 서버 프로필을 하나의 보호 볼트에만 저장할 수 있습니다. 하지만 단일 보호 볼트에 서버 프로필을 원하는 수만큼 저장할 수 있습니다.

보호 볼트 생성

볼트 위치에 접근할 수 있는지 확인합니다.

1. **OMIMSSC**에서 **유지 보수 센터**를 클릭한 다음에 **유지 보수 설정**을 클릭합니다.
2. **유지 보수 센터**에서 **보호 볼트**를 클릭한 다음 **생성**을 클릭합니다.
3. 사용하려는 보호 볼트 유형을 선택하고 세부 정보를 제공합니다.
   - **네트워크 공유** 유형의 보호 볼트를 생성하는 경우 프로파일을 저장할 위치, 이 위치에 액세스할 수 있는 자격 증명, 프로파일을 보호하기 위한 암호문구를 제공합니다.

     노트: 이러한 유형의 보호 볼트는 CIFS(Common Internet File System) 공유 유형의 파일을 지원합니다.
   - **vFlash** 유형의 보호 볼트를 생성하는 경우, 프로파일 보호를 위해 암호 문구를 제공합니다.

보호 볼트 편집

보호 볼트의 이름, 설명, 유형 및 암호 문구를 수정할 수 없습니다.

1. **OMIMSSC**에서 **유지 보수 센터** > **유지 보수 설정** > **보호 볼트**를 클릭합니다.
2. 볼트를 수정하려면 볼트를 선택하고 **편집**을 클릭합니다.

   노트: 서버 프로파일 내보내기 또는 가져오기 작업이 진행 중일 때 보호 볼트가 수정된 경우 편집된 정보가 작업에서 보류 중인 하위 작업에 대해 고려됩니다.

보호 볼트 삭제

다음과 같은 상황에서는 보호 볼트를 삭제할 수 없습니다.

- 보호 볼트가 서버 또는 서버 그룹과 연결되어 있습니다.

  이러한 보호 볼트를 삭제하려면 서버 또는 서버 그룹을 삭제한 다음 보호 볼트를 삭제합니다.

- 보호 볼트와 관련된 예약된 작업이 있습니다. 그러나 이러한 보호 볼트를 삭제하려면 예약된 작업을 삭제한 다음 보호 볼트를 삭제합니다.

1. **OMIMSSC**에서 **유지 보수 센터** > **유지 보수 설정** > **보호 볼트**를 클릭합니다.
2. 삭제할 볼트를 선택하고 **삭제**를 클릭합니다.

서버 프로파일 내보내기

BIOS, RAID, NIC, iDRAC, Lifecycle Controller 등의 다양한 구성 요소에 설치된 펌웨어 이미지를 포함한 서버 프로파일과 해당 구성 요소의 구성을 내보냅니다. OMIMSSC 어플라이언스는 vFlash SD 카드 또는 네트워크 공유에 저장할 수 있는 모든 구성을 포함하는 파일을 생성합니다. 이 파일을 저장할 보호 볼트를 선택합니다. 서버 또는 서버 그룹의 구성 프로파일을 즉시 내보내거나 나중을 위해 예약할 수 있습니다. 또한 서버 프로파일을 내보낼 빈도와 같은 방법으로 관련 반복 옵션을 선택할 수 있습니다.

BIOS 설정에서 **오류 발생 시 F1/F2 프롬프트** 옵션을 비활성화합니다.

서버 프로파일을 내보내기 전에 다음 사항을 고려합니다.

- 인스턴스에서 서버 그룹에 대해 내보내기 구성 작업을 하나만 예약할 수 있습니다.
- 구성 프로파일을 내보내고 있는 서버 또는 서버 그룹에 대해 다른 작업을 수행할 수 없습니다.
- iDRAC의 **자동 백업** 작업이 같은 시간에 예약되지 않도록 하십시오.
- 필터가 적용되면 서버 프로파일을 내보낼 수 없습니다. 서버 프로파일을 내보내려면 적용된 모든 필터를 선택 취소합니다.
- 서버 프로파일을 내보내려면 iDRAC Enterprise 라이선스가 있어야 합니다.
- 서버 프로파일을 내보내기 전에 서버의 IP 주소가 변경되지 않았는지 확인합니다. 다른 작업으로 인해 서버 IP가 변경된 경우 OMIMSSC에서 이 서버를 다시 검색한 후 서버 프로파일 내보내기 작업을 예약합니다.

1. OMIMSSC에서 **유지 보수 센터**를 클릭합니다. 프로파일을 내보낼 서버를 선택하고 드롭다운 메뉴의 **디바이스 프로파일**에서 **내보내기**를 클릭합니다.
   서버 프로파일 내보내기 페이지가 표시됩니다.
2. 프로파일을 내보낼 서버를 선택하고 드롭다운 메뉴의 **디바이스 프로파일**에서 **내보내기**를 클릭합니다.
   서버 프로파일 내보내기 페이지가 표시됩니다.
3. **서버 프로파일 내보내기** 페이지에서 작업 상세 정보를 제공하고 보호 볼트를 선택합니다.

   보호 볼트에 대한 자세한 내용은 보호 볼트 생성을 참조하십시오.

   서버 프로파일 내보내기 예약에서 다음 중 하나를 선택합니다.
   - **지금 실행** - 선택한 서버 또는 서버 그룹의 서버 구성을 즉시 내보냅니다.
   - 일정 - 선택한 서버 그룹의 서버 구성 내보내기 일정을 제공합니다.
     - **사용 안 함** - 서버 프로파일을 예약된 시간 동안 한 번만 내보내려면 선택합니다.
     - **일주일에 한 번** - 서버 프로파일을 주 단위로 내보내려면 선택합니다.
     - **2주에 한 번** - 서버 프로파일을 2주에 한 번 내보내려면 선택합니다.
     - **4주에 한 번** - 서버 프로파일을 4주에 한 번 내보내려면 선택합니다.

서버 프로파일 가져오기

이전에 동일한 서버 또는 서버 그룹에 대하여 내보낸 서버 프로파일을 가져올 수 있습니다. 서버 프로파일 가져오기는 서버의 구성과 펌웨어를 프로파일에 저장된 상태로 복원하는 데 유용합니다.

다음 두 가지 방법으로 서버 프로파일을 가져올 수 있습니다.

- 빠른 서버 프로파일 가져오기 - 해당 서버에 대하여 최근에 내보낸 서버 프로파일을 자동으로 가져올 수 있습니다. 이 작업을 위해 각 서버에 대하여 개별 서버 프로파일을 선택할 필요가 없습니다.
- 사용자 지정 서버 프로파일 가져오기 - 개별적으로 선택한 각 서버에 대하여 서버 프로파일을 가져올 수 있습니다. 예를 들어, 서버 프로파일 내보내기가 예약되었고 서버 프로파일을 매일 내보내는 경우에 이 기능을 통해 서버 프로파일 목록에서 가져올 특정 서버 프로파일을 선택할 수 있습니다. 이 목록은 해당 서버의 보호 볼트에서 볼 수 있습니다.

서버 프로파일 가져오기 참고 사항:

- 해당 서버에 대해서만 내보낸 서버 프로파일 목록에서 서버 프로파일을 가져올 수 있습니다. 다른 서버 또는 서버 그룹에 대해서는 같은 서버 프로파일을 가져올 수 없습니다. 다른 서버 또는 서버 그룹의 서버 프로파일을 가져오려고 하면 서버 프로파일 가져오기 작업이 실패합니다.
- 특정 서버 또는 서버 그룹에 대한 서버 프로파일 이미지를 사용할 수 없는 상태에서 이 특정 서버 또는 서버 그룹에 대하여 서버 프로파일 가져오기 작업을 시도하면 이 서버 프로파일이 있는 특정 서버에 대하여 서버 프로파일 가져오기 작업이 실패합니다. 활동 로그에 실패 상세 정보와 함께 로그 메시지가 추가됩니다.
- 서버 프로파일을 내보낸 후에 서버에서 구성 요소를 제거하고 나서 프로파일 가져오기 작업이 시작되면 누락된 구성 요소 정보는 제외하고 모든 구성 요소 정보가 복원됩니다. OMIMSSC의 활동 로그에서는 이 정보를 이용할 수 없습니다. 누락된 구성 요소에 대한 자세한 내용은 iDRAC의 **수명주기 로그**를 참조하십시오.
- 필터를 적용한 후에는 서버 프로파일을 가져올 수 없습니다. 서버 프로파일을 가져오려면 적용된 모든 필터를 지웁니다.
- 서버 프로파일을 가져오려면 iDRAC Enterprise 라이선스가 있어야 합니다.

1. OMIMSSC의 **유지 보수 센터**에서 프로파일을 가져오려는 서버를 선택하고 **디바이스 프로파일** 드롭다운 메뉴에서 **가져오기**를 클릭합니다.
   서버 프로파일 가져오기 페이지가 표시됩니다.
2. 프로파일을 가져오려는 서버를 선택하고 **디바이스 프로파일** 드롭다운 메뉴에서 **가져오기**를 클릭합니다.
   서버 프로파일 가져오기 페이지가 표시됩니다.
3. 상세 정보를 입력하고 원하는 **서버 프로파일 가져오기 유형**을 선택합니다.

   노트: 기존 RAID 구성과 함께 서버 프로파일을 내보냅니다. 하지만 서버 또는 서버 그룹에서 RAID 구성을 포함하거나 제외하고 서버 프로파일을 가져올 수 있습니다. **데이터 보존**이 기본적으로 선택되어 있으며 서버의 기존 RAID 구성을 유지합니다. 서버 프로파일에 저장된 RAID 설정을 적용하려면 이 확인란의 선택을 취소합니다.

4. 프로파일을 가져오려면 **완료**를 클릭합니다.

교체된 구성 요소에 펌웨어 및 구성 설정 적용

부품 교체 기능은 교체된 서버 구성 요소를 이전 구성 요소의 필수 펌웨어 버전 또는 구성으로 자동으로 업데이트합니다. 구성 요소를 교체한 후 서버를 재부팅하면 업데이트가 자동으로 수행됩니다.

부품 교체에 대한 구성을 설정하려면 다음을 수행합니다.

1. OMIMSSC에서 **유지 보수 센터**를 클릭하고 서버 또는 서버 그룹을 선택한 다음에 **부품 교체**를 클릭합니다.

   노트: 부품 교체로 마우스를 가져가면 옵션 이름이 **부품 교체 구성**으로 확장됩니다.

   부품 교체 구성 창이 표시됩니다.
2. 구성 요소를 구성하려는 서버를 선택한 다음에 **부품 교체**를 클릭합니다.

   노트: 부품 교체로 마우스를 가져가면 옵션 이름이 **부품 교체 구성**으로 확장됩니다.

   부품 교체 구성 창이 표시됩니다.
3. **CSIOR**, **부품 펌웨어 업데이트** 및 **부품 구성 업데이트**를 다음 옵션으로 설정한 후 **마침**을 클릭할 수 있습니다.
   - Collect System Inventory on Restart(CSIOR) - 시스템을 재시작할 때마다 모든 구성 요소 정보를 수집합니다.
     - **활성화**- 시스템을 재시작할 때마다 서버 구성 요소의 소프트웨어 및 하드웨어 인벤토리 정보를 자동으로 업데이트합니다.
     - **비활성화**- 서버 구성 요소의 소프트웨어 및 하드웨어 인벤토리 정보를 업데이트하지 않습니다.
     - **서버의 값을 변경하지 않음**- 기존 서버 구성을 보존합니다.
   - 부품 펌웨어 업데이트 - 선택 항목을 기반으로 구성 요소 펌웨어 버전을 복원하거나 업그레이드하거나 다운그레이드합니다.
     - **비활성화**- 부품 펌웨어 업데이트가 비활성화되고 동일한 내용이 교체된 구성 요소에 적용됩니다.
     - **버전 업그레이드만 허용**- 새 구성 요소의 펌웨어 버전이 기존 버전보다 낮은 경우 업그레이드된 펌웨어 버전이 교체된 구성 요소에 적용됩니다.
     - **교체된 부품의 펌웨어 일치**- 새 구성 요소의 펌웨어 버전을 원래 구성 요소의 펌웨어 버전에 일치시킵니다.
     - **서버의 값을 변경하지 않음**- 구성 요소의 기존 구성을 보존합니다.
   - 부품 구성 업데이트 - 선택 항목을 기반으로 구성 요소 구성을 복원하거나 업그레이드합니다.
     - **비활성** - 부품 구성 업데이트가 비활성화되고 이전 구성 요소의 저장된 구성이 교체된 구성 요소에 적용되지 않습니다.
     - **항상 적용** - 부품 구성 업데이트가 활성화되고 이전 구성 요소의 저장된 구성이 교체된 구성 요소에 적용됩니다.
     - **펌웨어가 일치하는 경우에만 적용**- 해당 펌웨어 버전과 일치하는 경우에만 기존의 구성 요소의 저장된 구성이 교체된 구성 요소에 적용됩니다.
     - **서버의 값을 변경하지 않음**- 기존 구성을 보존합니다.

서버에 대한 LC 로그 수집

LC 로그는 관리되는 시스템의 과거 활동에 대한 기록을 제공합니다. 이 로그 파일은 권장되는 조치에 대한 상세 정보와 문제 해결에 유용한 기타 기술 정보를 제공하므로 서버 관리자에게 유용합니다. LC 로그에서 사용할 수 있는 다양한 유형의 정보는 알림 관련, 시스템 하드웨어 구성 요소에 대한 구성 변경, 업그레이드 또는 다운그레이드로 인한 펌웨어 변경, 교체된 부품, 온도 경고, 활동이 시작되었을 때의 상세한 타임스탬프, 활동 심각도 등입니다. 내보낸 LC 로그 파일은 폴더에 저장되며 서버의 서비스 태그 뒤에 폴더 이름이 지정됩니다. LC 로그는 `<YYYYMMDDHHMMSSSSS>.<file format>` 형식으로 저장됩니다. 예를 들어, `20160720103001O597.xml.gz`는 파일이 생성된 날짜와 시간으로 구성된 LC 파일 이름입니다. 두 가지 옵션으로 LC 로그를 수집할 수 있습니다.

- 전체 LC 로그 - 활성 및 아카이빙된 LC 로그 파일을 내보냅니다. 이러한 파일은 크기가 크기 때문에 `.gz` 형식으로 압축하여 CIFS 네트워크 공유의 지정된 위치로 내보냅니다.
- 활성 LC 로그 - 최근 LC 로그 파일을 즉시 내보내거나 로그 파일을 정기적으로 내보내도록 작업을 예약합니다. 이러한 로그 파일을 확인 및 검색하고 OMIMSSC 어플라이언스로 내보냅니다. 또한 로그 파일의 백업을 네트워크 공유에 저장할 수 있습니다.

LC 로그를 수집하려면 다음을 수행합니다.

1. OMIMSSC에서 **유지 보수 센터**를 클릭합니다. 서버 또는 서버 그룹을 선택하고 **LC 로그** 드롭다운 메뉴를 클릭한 다음에 **LC 로그 수집**을 클릭합니다.
2. 로그를 내보내려는 서버를 선택하고 **LC 로그** 드롭다운 메뉴를 클릭한 다음에 **LC 로그 수집**을 클릭합니다.
3. **LC 로그 수집**에서 다음 옵션 중 하나를 선택하고 **마침**을 클릭합니다.
   - **전체 LC 로그 내보내기(.gz)** - Windows 자격 증명을 제공하여 전체 LC 로그를 CIFS 네트워크 공유에 내보내려면 선택합니다.
   - **활성 로그 내보내기(지금 실행)** - 활성 로그를 OMIMSSC 어플라이언스에 즉시 내보내려면 선택합니다.
     - (선택 사항) Windows 자격 증명을 제공하여 CIFS 네트워크 공유에 LC 로그의 백업을 저장하려면 **네트워크 공유에 LC 로그 백업** 확인란을 선택합니다.
   - **LC 로그 수집 예약** - 활성 로그를 주기적으로 내보내려면 선택합니다.

     LC 로그 수집 예약에서 로그 파일을 내보낼 날짜와 시간을 선택합니다.

     파일을 내보낼 빈도에 따라 라디오 버튼을 선택합니다. LC 로그를 얼마나 자주 수집할지 결정할 빈도를 예약할 수 있는 옵션은 다음과 같습니다.

     - **사용 안 함** - 이 옵션은 기본적으로 선택되어 있습니다. LC 로그를 예약된 시간 동안 한 번만 내보내려면 선택합니다.
     - **1일 한 번씩** - LC 로그를 예약된 시간 동안 1일 한 번만 내보내려면 선택합니다.
     - **1주 한 번씩** - LC 로그를 매주 예약된 시간에 내보내려면 선택합니다.
     - **4주마다 한 번씩** - LC 로그를 예약된 시간 동안 4주마다 한 번씩 내보내려면 선택합니다.
     - (선택 사항) Windows 자격 증명을 제공하여 CIFS 네트워크 공유에 LC 로그의 백업을 저장하려면 **네트워크 공유에 LC 로그 백업** 확인란을 선택합니다.

   노트: 내보낸 파일의 크기가 크기 때문에 스토리지 공간이 충분한 공유 폴더를 제공하십시오.

   이 작업을 추적하기 위해 기본적으로 **작업 목록으로 이동** 옵션이 선택되어 있습니다.

LC 로그 보기

모든 활성 LC 로그를 보고 자세한 설명을 검색하고 로그를 CSV 형식으로 다운로드할 수 있습니다.

로컬 인트라넷 사이트에 OMIMSSC 어플라이언스를 추가합니다.

1. OMIMSSC에서 **유지 보수 센터**를 클릭합니다. 서버 또는 서버 그룹을 선택하고 **LC 로그** 드롭다운 메뉴를 클릭하고 **LC 로그 보기**를 클릭합니다.
2. 로그를 보려는 서버를 선택하고 **LC 로그** 드롭다운 메뉴를 클릭한 다음에 **LC 로그 보기**를 클릭합니다.
3. 선택한 그룹에 있는 모든 서버와 LC 로그가 수집되는 서버가 해당 LC 로그 파일에 나열됩니다. 해당 서버에 고유한 LC 로그 파일의 모든 로그 항목을 보려면 파일 이름을 클릭합니다. 자세한 내용은 파일 설명을 참조하십시오.
4. (선택 사항) 검색 상자를 사용하여 모든 로그 파일에서 설명을 검색하고 CSV 형식으로 파일을 내보냅니다.

   다음과 같은 두 가지 방법으로 LC 파일에서 메시지 설명을 검색할 수 있습니다.
   - 파일 이름을 클릭하여 LC 로그 파일을 열고 검색 상자에서 설명을 검색합니다.
   - 검색 상자에 설명을 입력하고 이러한 텍스트의 인스턴스가 있는 모든 LC 파일을 봅니다.

   노트: LC 로그 메시지 설명이 긴 경우, 메시지가 80자로 잘립니다.

   노트: LC 로그 메시지에 표시되는 시간은 iDRAC 시간대를 따릅니다.

파일 설명

이 페이지에서는 권장 작업에 대한 상세 정보와 특정 서버에 대한 추적 또는 알림 용도로 유용한 기타 기술 정보를 볼 수 있습니다.

파일의 내용을 보려면 파일 이름을 클릭합니다.

- 특정 메시지 설명을 검색할 수 있습니다.
- 창에서 로그 파일을 보거나 파일을 다운로드하여 추가 로그 메시지를 확인할 수 있습니다.
- 활동에 대해 사용자가 제공한 모든 설명을 볼 수 있습니다.

노트: 검색 옵션을 사용할 경우 검색 결과만 CSV 파일로 내보냅니다.

노트: 메시지가 긴 경우 메시지가 80자로 잘립니다.

노트: 메시지에 대한 자세한 정보를 보려면 **메시지 ID**를 클릭합니다.

인벤토리 내보내기

선택한 서버 또는 서버 그룹의 인벤토리를 XML 또는 CSV 형식 파일로 내보냅니다. 이 정보를 Windows 공유 디렉토리 또는 관리 시스템에 저장할 수 있습니다. 이 인벤토리 정보를 사용하여 업데이트 소스에서 참조 인벤토리 파일을 생성합니다.

노트: XML 파일을 DRM으로 가져오고 인벤토리 파일을 기반으로 리포지토리를 생성할 수 있다.

노트: 서버의 구성 요소 정보만 선택하고 내보내면, 서버의 전체 인벤토리 정보가 내보내기됩니다.

1. **OMIMSSC**에서 **유지 보수 센터**를 클릭합니다.
2. 인벤토리를 내보낼 서버를 선택하고, **인벤토리 내보내기** 드롭다운 메뉴에서 형식을 선택합니다.
   선택 항목을 기반으로 파일을 CSV 또는 XML 형식으로 내보냅니다. 파일은 서버 그룹, 서버의 서비스 태그, 호스트 이름 또는 IP 주소, 디바이스 모델, 구성 요소 이름, 해당 구성 요소의 현재 펌웨어 버전, 업데이트 소스의 펌웨어 버전, 해당 구성 요소에 대한 업데이트 작업 등과 같은 상세 정보로 구성됩니다.

작업 관리

작업이 **예약됨** 상태인지 확인합니다.

1. OMIMSSC에서 다음 중 하나를 수행합니다.
   - 탐색 창에서 **유지 보수 센터**를 클릭한 다음, **작업 관리**를 클릭합니다.
   - 탐색 창에서 **작업 및 로그 센터**를 클릭한 다음, **예약됨** 탭을 클릭합니다.
2. 취소하려는 작업을 선택하고 **취소**를 클릭한 다음에 **예**를 클릭하여 확인합니다.

20

Azure Stack HCI 클러스터 배포

다음은 Azure Stack HCI 클러스터를 배포하는 단계입니다.

1. 필수 Windows 및 디바이스 자격 증명 프로파일을 생성합니다.
2. WinPE 이미지 생성
   a. SCVMM에 WDS 기능을 설치한 다음 구성합니다.
   b. 리소스 추가를 사용하여 SCVMM 서버에 PXE 서버를 추가하고 동일한 서버 이름(SCVVM 호스트 이름) PXE 서버를 지정합니다.
   c. SCVMM 서버 내에서 공유 폴더를 생성한 다음 *C:\RemoteInstall\DCMgr\Boot\Windows\Images*에서 Boot.wim을 공유 폴더로 복사합니다.
   d. Dell EMC OpenManage 드라이버 팩에서 드라이버를 추출합니다.
   e. WinPE 이미지를 만듭니다.
   f. WinPE 이미지가 SCVMM의 공유 폴더에 있는지 확인합니다.
3. SCVMM 라이브러리에 Windows Server 2016 및 2019 VM 템플릿을 추가합니다. 자세한 내용은 Microsoft 설명서를 참조하십시오.
   a. 다음 속성을 변경합니다.
   - 운영 체제: Windows Server 2016 및 2019 데이터센터
   - 가상화 플랫폼: Microsoft Hyper-V

   노트: OS 배포용 .iso 파일을 사용하여 Windows Server 2019 가상 디스크(.vhdx)를 만들려면 https://gallery.technet.microsoft.com/scriptcenter/Convert-WindowsImageps1-0fe23a8f를 참조하십시오.https://gallery.technet.microsoft.com/scriptcenter/Convert-WindowsImageps1-0fe23a8f
4. SCVMM에서 PCP(Physical Computer Profile)를 생성합니다. 하드웨어 구성 > 디스크 및 파티션에서, 파티션 체계를 **GUID 파티션 테이블**로 선택합니다. 자세한 내용은 베어 메탈 컴퓨터에서 Hyper-V 호스트 또는 클러스터 프로비저닝에 대한 Microsoft 설명서의 필수 구성 요소 섹션에서 물리적 컴퓨터 프로파일 만들기 섹션을 참조하십시오.
5. SCVMM에서 호스트 그룹을 생성하여 Azure Stack HCI 클러스터를 호스팅합니다. SCVMM에서 호스트 그룹을 생성하는 방법에 대한 자세한 내용은 Microsoft 문서 자료를 참조하십시오.
6. 하이퍼바이저 프로파일을 생성합니다.
7. Dell EMC OpenManage 확장에서 서버를 검색합니다.
8. 사전 정의된 작업 템플릿을 사용하여 구성합니다.
9. (선택 사항) 규정 준수(구성 및 배포 > 서버 보기 > 서버 선택 및 작업 템플릿 할당)를 확인합니다.
10. 논리 스위치를 생성합니다.
11. Azure Stack HCI 클러스터를 배포합니다.
    클러스터 배포가 성공했는지 확인하려면 **클러스터 보기**로 이동하여 클러스터가 해당 범주에 나열되어 있는지 확인합니다.

21

문제 해결

주제:

관리에 필요한 리소스 OMIMSSC

이 가이드를 사용하여 OMIMSSC에 필요한 권한을 확인하고 발생한 문제를 해결할 수 있습니다.

OMIMSSC에서 발생하는 문제를 해결하려면 다음 리소스를 보유하고 있는지 확인하십시오.

- OMIMSSC 어플라이언스 로그인하여 다양한 작업을 수행하기 위한 읽기 전용 사용자 계정 상세 정보.

  OMIMSSC 어플라이언스 VM에서 읽기 전용 사용자로 로그인하려면 사용자 이름 `readonly`와 OMIMSSC 어플라이언스 VM에 로그인하는 데 사용되는 동일한 암호를 입력합니다.

- 오류에 대한 전체 상세 정보가 포함된 로그 파일:
  - 활동 로그 – OMIMSSC에서 시작된 작업과 OMIMSSC에서 실행되는 작업의 상태에 대한 사용자별 및 고수준 정보를 포함합니다. 활동 로그를 보려면 OMIMSSC 콘솔 확장 프로그램의 **작업 및 로그** 페이지로 이동합니다.
  - 전체 로그 – OMIMSSC의 관리자 관련 로그 및 시나리오와 관련된 여러 상세 로그를 포함합니다. 전체 로그를 보려면 **OMIMSSC 관리 포털**의 **작업 및 로그** 페이지, **설정**, **로그**로 차례로 이동합니다.
  - LC 로그 – OMIMSSC에서 수행되는 작업에 대한 서버 수준 정보, 자세한 오류 메시지를 포함합니다. LC 로그를 다운로드하고 보려면 *System Center Configuration Manager 및 System Center Virtual Machine Manager를 위한 Microsoft System Center용 Dell EMC OpenManage Integration 사용자 가이드*를 참조하십시오.

    노트: iDRAC 또는 OME-Modular(OpenManage Enterprise Modular) 페이지에서 개별 디바이스의 문제를 해결하려면 OMIMSSC를 시작하고, **구성 및 배포** 페이지를 클릭한 다음, 해당 보기를 시작하고, 디바이스 IP URL을 클릭합니다.

노트: SCVMM Server Administrator 사용자는 SCVMM 서비스 계정이 아니어야 합니다.

노트: SC2012 VMM SP1에서 SC2012 VMM R2로 업그레이드하는 경우에는 Windows PowerShell 4.0으로 업그레이드해야 합니다.

MECM용 OMIMSSC 콘솔 확장 프로그램을 사용하기 위한 권한 확인

OMIMSSC를 설치한 후 등록된 사용자에게 다음 권한이 있는지 확인합니다.

1. OMIMSSC가 설치된 시스템에서 PowerShell 명령을 사용하여 *<Configuration Manager Admin Console Install Dir>\XmlStorage\Extensions\DLCPlugin* 폴더에 대한 **쓰기** 권한을 제공합니다.

   OMIMSSC 구성 요소를 설치하기 전에 사이트 서버 및 SMS 공급자 서버에 대한 다음 사전 요구 사항을 완료합니다.

   a. PowerShell에서 `PSRemoting` 명령을 실행합니다.

   `PSRemoting`명령이 비활성화된 경우, 다음 명령을 사용하여 `PSRemoting` 명령을 활성화합니다.

i. `Enable-PSRemoting` 명령을 실행합니다.
ii. 확인 메시지에 `Y`를 입력합니다.

b. PowerShell에서 `Get-ExecutionPolicy` 명령을 실행합니다.
정책이 `RemoteSigned`로 설정되지 않은 경우 다음 명령을 사용하여 `RemoteSigned`로 설정합니다.
i. `Set-ExecutionPolicy RemoteSigned` 명령을 실행합니다.
ii. 확인 메시지에 `Y`를 입력합니다.

2. WMI(Windows Management Instrumentation)에 대한 사용자 액세스를 구성합니다. 자세한 내용은 WMI에 대한 사용자 액세스 구성을 참조하십시오.
3. 받은 편지함 폴더에 파일을 쓰기 위한 공유 및 폴더 권한을 부여합니다.
DDR 받은 편지함에 파일을 쓰기 위한 공유 및 폴더 권한을 부여하려면 다음 단계를 따르십시오.
a. Configuration Manager 콘솔에서 **관리** 아래에서 **SMS_<sitecode>** 공유에 사용자 쓰기 권한을 부여합니다.
b. **파일 탐색기**를 사용하여, 공유 위치 **SMS_<sitecode>** 공유, 이어서 `ddm.box` 폴더로 이동합니다. 다음 폴더에 대해 도메인 사용자에게 전체 권한을 부여합니다.
- **SMS_<sitecode>**
- 받은 편지함
- `ddm.box`

WMI에 대한 사용자 액세스 구성

원격으로 WMI에 대한 사용자 액세스를 구성하려면 다음 단계를 따르십시오.

노트: 시스템의 방화벽이 WMI 연결을 차단하지 않는지 확인합니다.

1. DCOM(Distributed Component Object Model)을 원격으로 액세스하려면 등록된 MECM 사용자에게 권한을 제공해야 합니다.
DCOM에 대한 사용자 권한을 부여하려면 다음 단계를 따르십시오.
a. `dcomcnfg.exe`를 실행합니다.
b. **구성 요소 서비스** 콘솔의 왼쪽 창에서 **컴퓨터**를 확장하고 **내 컴퓨터**를 마우스 오른쪽 버튼으로 클릭한 다음 **속성**을 선택합니다.
c. **COM 보안**에서 다음을 수행합니다.
- **액세스 권한**에서 **제한 편집**을 클릭하고 **원격 액세스**를 선택합니다.
- **실행 및 활성화 권한**에서 **제한 편집**을 클릭하고 **로컬 시작**, **원격 시작** 및 **원격 활성화**를 선택합니다.

2. DCOM Config WMI(Windows Management and Instrumentation) 구성 요소에 액세스하려면 등록된 사용자에게 사용자 권한을 제공하십시오.
DCOM Config WMI에 대한 사용자 권한을 부여하려면 다음 단계를 따르십시오.
a. `dcomcnfg.exe`를 실행합니다.
b. **내 컴퓨터** > **DCOM 구성**을 확장합니다.
c. **Windows Management and Instrumentation**을 마우스 오른쪽 버튼으로 클릭하고 **속성**을 선택합니다.
d. **보안**의 **실행 및 활성화 권한**에서 **편집**을 클릭하고 **원격 실행** 및 **원격 활성화** 권한을 선택합니다.
3. 네임스페이스 보안 설정 및 권한 부여
네임스페이스 보안을 설정하고 권한을 부여하려면 다음 단계를 따르십시오.
a. 실행 `wmimgmt.msc`
b. **WMI 컨트롤** 창에서 **WMI 컨트롤**을 마우스 오른쪽 버튼으로 클릭하고 **속성**을 선택한 다음 **보안**를 선택합니다.
c. `ROOT\SMS Namespace`로 이동합니다.
d. **실행 방법**, **쓰기 제공**, **계정 활성화** 및 **원격 활성화 권한**을 선택합니다.
e. `Root\cimv2\OMIMSSC`로 이동합니다.
f. **실행 방법**, **쓰기 제공**, **계정 활성화** 및 **원격 활성화 권한**을 선택합니다.
또는 Configuration Manager 사용자가 **SMS_Admin** 그룹의 구성원이 되고 해당 그룹의 기존 권한에 **원격 활성화**를 부여할 수 있습니다.

SCVMM용 OMIMSSC 콘솔 확장 프로그램을 사용하기 위한 PowerShell 권한 확인

PSRemoting 상태가 활성화되고 **ExecutionPolicy**가 **RemoteSigned**로 설정되었는지 확인합니다. 상태가 다른 경우 PowerShell에서 다음 단계를 수행합니다.

a. PowerShell에서 `PSRemoting` 명령을 실행합니다.

   `PSRemoting`명령이 비활성화된 경우, 다음 명령을 사용하여 `PSRemoting` 명령을 활성화합니다.

   i. `Enable-PSRemoting` 명령을 실행합니다.
   ii. 확인 메시지에 `Y`를 입력합니다.

b. PowerShell에서 `Get-ExecutionPolicy` 명령을 실행합니다.

   정책이 `RemoteSigned`로 설정되지 않은 경우 다음 명령을 사용하여 `RemoteSigned`로 설정합니다.

   i. `Set-ExecutionPolicy RemoteSigned` 명령을 실행합니다.
   ii. 확인 메시지에 `Y`를 입력합니다.

설치 및 업그레이드 시나리오 OMIMSSC

이 섹션에서는 OMIMSSC 설치 및 업그레이드와 관련된 모든 문제 해결 정보를 다룹니다.

OMIMSSC 어플라이언스 VM 구성 확인

OMIMSSC 어플라이언스 VM이 적절하게 구성되었는지 확인하려면 OMIMSSC 어플라이언스 VM을 선택하고 마우스 오른쪽 버튼으로 클릭한 후 **설정**을 클릭하고 다음 작업을 수행합니다.

1. OMIMSSC에 대한 공통 시스템 요구 사항에 명시된 요구 사항에 따라 OMIMSSC 어플라이언스에 메모리가 할당되는지 확인합니다. 그렇지 않으면 **시작 RAM**에서 메모리를 지정하고 **적용**을 클릭합니다.
2. 프로세서 수가 OMIMSSC에 대한 시스템 요구 사항 섹션에 명시된 요구 사항과 일치하는지 확인합니다. 그렇지 않으면 **프로세서** 아래의 **가상 프로세서 개수**에서 프로세서 개수를 지정합니다.
3. IDE 컨트롤러: **IDE 컨트롤러 0** > **하드 드라이브** 아래의 **가상 하드 디스크** 필드에서 **가상 하드 디스크**가 **OMIMSSC—v7** 파일을 참조하는지 확인하고, 그렇지 않은 경우 **탐색**을 클릭한 후 VHD 파일의 압축을 해제한 위치로 이동한 다음 **OMIMSSC—v7** 파일을 선택하고 **적용**을 클릭합니다.
4. **네트워크 어댑터** > **가상 스위치**가 물리적 NIC 카드와 연결되어 있는지 확인하고, 그렇지 않은 경우 NIC 카드를 구성한 후 **가상 스위치** 드롭다운 메뉴에서 해당 NIC 카드를 선택한 다음 **적용**을 클릭합니다.

OMIMSSC 어플라이언스에 대해 선택된 가상 하드 디스크를 포함한 새로 작성된 가상 머신이 어떠한 커널 패닉 예외로 부팅에 실패하는 경우, 가상 머신 설정을 편집하고, 이 가상 머신 설정의 동적 메모리 옵션을 활성화합니다. 가상 머신의 동적 메모리 옵션을 활성화하려면 다음 작업을 수행합니다.

1. OMIMSSC 어플라이언스 VM을 마우스 오른쪽 버튼으로 클릭하고 **설정**을 클릭한 후 **메모리**를 클릭합니다.
2. **동적 메모리** 아래에서 **동적 메모리 활성화** 확인란을 활성화하고 상세 정보를 입력합니다.

등록 실패

연결 테스트 또는 등록이 실패하면 오류 메시지가 표시됩니다.

이 문제를 해결하려면 다음 단계를 수행합니다.

- 읽기 전용 사용자로 OMIMSSC 어플라이언스 VM에 로그인하여 OMIMSSC 어플라이언스에서 등록된 MECM 또는 SCVMM 서버 FQDN으로 Ping을 수행합니다. 응답이 있는 경우 잠시 기다린 후 등록을 계속합니다.

  읽기 전용 사용자로 OMIMSSC 어플라이언스 VM을 시작하려면 사용자 이름을 `readonly`로 입력하고 OMIMSSC 어플라이언스 VM에 로그인하는 데 사용한 것과 동일한 암호를 입력합니다.

- MECM 또는 SCVMM가 정상적으로 실행되고 있는지 확인합니다.
- 콘솔 등록에 사용되는 Microsoft 계정은 System Center의 위임된 관리자 또는 관리자와 System Center 서버의 로컬 관리자여야 합니다.
- SCVMM 사용자 전용:
  - SCVMM 서버가 다른 OMIMSSC 어플라이언스에 등록되지 않았는지 확인합니다. 동일한 SCVMM 서버를 OMIMSSC 어플라이언스에 등록하려면 SCVMM 서버에서 **OMIMSSC 등록 프로파일** 애플리케이션 프로파일을 삭제합니다.

- SCVMM 롤업 업데이트를 적용한 경우, 레지스트리 (`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager AdministratorConsole\Settings`)에서 SCVMM 콘솔의 Indigo TCP 포트 번호를 확인합니다. SCVMM 콘솔을 등록할 때 사용한 것과 동일한 포트 번호를 사용합니다. 기본값은 8100입니다.

연결 테스트 실패

도메인 사용자 계정과 로컬 사용자 계정의 사용자 이름이 동일하고 비밀번호가 다른 경우 Microsoft 콘솔과 OMIMSSC 어플라이언스 간의 연결 테스트가 실패합니다.

예를 들어 도메인 사용자 계정이 `domain\user1`이고 비밀번호가 `pwd1`입니다. 로컬 사용자 계정은 `user1`이고 비밀번호는 `Pwd2`입니다. 위의 도메인 사용자 계정으로 등록하려고 하면 연결 테스트가 실패합니다.

이 문제를 해결하려면 도메인 사용자 및 로컬 사용자 계정에 다른 사용자 이름을 사용하거나 OMIMSSC 어플라이언스에서 Microsoft 콘솔을 등록하는 동안 단일 사용자 계정을 로컬 사용자로 사용합니다.

MECM 콘솔 확장 설치 후 OMIMSSC 시작 실패

MECM 2103이 설치된 설정부터 OMIMSSC 콘솔 시작 지점은 기본적으로 MECM 콘솔에서 사용할 수 없습니다.

이 문제를 해결하려면 **계층 설정** 속성에서 **계층에 대해 승인된 콘솔 확장만 허용**하는 옵션을 해제합니다. *자세한 내용은 Microsoft 설명서의 Configuration Manager 콘솔 섹션을 참조하십시오.*

SCVMM용 OMIMSSC 콘솔 확장 프로그램에 연결 실패

SCVMM 환경에서 OMIMSSC 콘솔 확장 프로그램을 등록 및 설치한 후 OMIMSSC를 시작하려고 하면 다음 오류가 표시됩니다. `Connection to server failed.`

이 문제를 해결하려면 다음 단계를 수행합니다.

1. OMIMSSC를 시작할 때 OMIMSSC 어플라이언스 IP 및 FQDN을 SCVMM 콘솔의 로컬 인트라넷에 추가합니다.
2. OMIMSSC 어플라이언스 IP 및 FQDN을 DNS의 **정방향 조회 영역** 및 **역방향 조회 영역**에 추가합니다.
3. 더 자세한 내용을 보려면 `C:\ProgramData\VMMLogs\AdminConsole` 파일에 오류 메시지가 있는지 확인합니다.

SCVMM R2 업데이트 후 콘솔 확장 액세스 오류

SC2012 R2 VMM에 대한 업데이트 롤업을 적용한 후, 이미 설치된 OMIMSSC 콘솔을 열려고 하면 보안상의 이유로 SCVMM에서 오류 메시지가 표시되고 OMIMSSC 콘솔에 액세스할 수 없습니다.

이 문제를 해결하려면 다음을 수행합니다.

1. 기본 경로에서 폴더를 삭제합니다. `C:\Program Files\Microsoft System Center 2012 R2\Virtual Machine Manager\Bin\AddInPipeline\AddIns\<username>`
2. SCVMM을 재시작합니다.
3. 콘솔 확장 프로그램을 제거한 후 *System Center Configuration Manager 및 System Center Virtual Machine Manager를 위한 Microsoft System Center용 Dell EMC OpenManage Integration 설치 가이드*의 *SCVMM용 OMIMSSC 콘솔 확장 프로그램 가져오기* 섹션을 참조하여 콘솔 확장 프로그램을 가져옵니다.

IP 주소가 OMIMSSC 어플라이언스에 할당되지 않음

OMIMSSC 어플라이언스 VM을 생성한 후 시작할 때 OMIMSSC 어플라이언스 IP 주소가 할당 또는 표시되지 않습니다.

이 문제를 해결하려면 가상 스위치가 실제 스위치에 매핑되어 있고, 올바르게 구성되어 있는지 확인한 후 OMIMSSC 어플라이언스에 연결합니다.

OMIMSSC 콘솔 확장을 가져올 때 SCVMM 충돌

OMIMSSC 콘솔 확장을 가져올 때 SC2016 VMM RTM 빌드 4.0.1662.0 관리자 콘솔이 충돌할 수 있습니다.

이 문제를 해결하려면 KB 문서 4094925(`support.microsoft.com/kb/4094925`)를 참조하여 SCVMM을 업그레이드한 후 OMIMSSC 콘솔 확장을 가져옵니다.

OMIMSSC 콘솔 확장에 로그인 실패

OMIMSSC 콘솔 확장 로그인이 다음 오류 메시지와 함께 실패합니다. `Failed to login. Ensure to use correct credentials or check if account is locked in Active Directory.`

이 문제를 해결하려면 올바른 자격 증명을 사용하고 Active Directory에서 계정이 잠겨 있지 않은지 확인하십시오. Active Directory에서 계정이 잠긴 경우 Active Directory 계정 잠금 정책에 따라 몇 분 후에 다시 로그인하십시오. Active Directory 계정 잠금 정책에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

업데이트 중 SC2012 VMM SP1 충돌

SC2012 VMM SP1로 업그레이드한 후 OMIMSSC 콘솔 확장을 SC2012 VMM UR5 이상으로 가져올 때 SCVMM 콘솔이 충돌할 수 있습니다.

이 문제에 대한 자세한 내용과 문제 해결 방법은 기술 자료 URL `support.microsoft.com/kb/2785682`의 문제 5를 참조하십시오.

이 문제를 해결하려면 설치된 업데이트 롤업의 버전과 관계없이 SCVMM을 업데이트합니다.

OMIMSSC 관리 포털 시나리오

이 섹션에서는 OMIMSSC의 관리 포털과 관련된 모든 문제 해결 정보를 다룹니다.

Mozilla Firefox 브라우저를 통해 OMIMSSC 관리 포털에 액세스하는 동안 오류 메시지

Mozilla Firefox 브라우저를 사용하여 OMIMSSC 관리 포털에 액세스할 때 다음과 같은 경고 메시지가 표시됩니다. "`Secure Connection Failed`"

이 문제를 해결하려면 브라우저의 관리 포털의 이전 항목에서 생성된 인증서를 삭제합니다. Mozilla Firefox 브라우저에서 인증서를 삭제하는 방법에 대한 자세한 내용은 `support.mozilla.org`를 참조하십시오.

OMIMSSC 관리 포털에서 Dell EMC 로고 표시 실패

Windows 2016 기본 IE 브라우저에서 OMIMSSC 관리 포털을 실행하면 관리 포털에 Dell EMC 로고가 표시되지 않습니다.

이 문제를 해결하려면 다음 중 하나를 수행합니다.

- IE 브라우저를 최신 버전으로 업그레이드합니다.
- 검색 기록을 삭제하고 OMIMSSC 관리 포털 URL을 브라우저의 즐겨찾기 목록에 추가합니다.

검색, 동기화, 인벤토리 시나리오 OMIMSSC

이 섹션에서는 OMIMSSC를 사용할 때 자격 증명 문제, 서버 검색, 서버 그룹화, 등록된 Microsoft 콘솔을 OMIMSSC와 동기화할 때의 모든 문제 해결 정보를 다룹니다.

서버 검색 실패

여러 Microsoft 콘솔이 OMIMSSC 어플라이언스에 등록되어 있을 때, 서버를 검색하려고 하면 MECM 콘솔 중 하나에 연결할 수 없더라도 서버 검색 작업이 실패합니다.

이 문제를 해결하려면 연결할 수 없는 MECM 콘솔의 등록을 취소하거나 문제를 해결하고 OMIMSSC 어플라이언스에서 해당 MECM 콘솔에 연결할 수 있는지 확인합니다.

iDRAC 서버 자동 검색 실패

기본 디바이스 자격 증명 프로파일에 설정된 암호가 충분히 강력하지 않은 경우 iDRAC 서버의 자동 검색이 실패합니다.

이 문제를 해결하려면 강력한 암호를 설정해야 합니다. 암호 정책 요구 사항에 대한 자세한 내용은 iDRAC 사용자 가이드를 참조하십시오.

검색된 서버가 모든 Dell Lifecycle Controller 서버 컬렉션에 추가되지 않음

MECM용 OMIMSSC 콘솔 확장 프로그램에서 서버를 검색한 후 서버가 **모든 Dell Lifecycle Controller 서버** 컬렉션에 추가되지 않을 수 있습니다.

이 문제를 해결하려면 **모든 Dell Lifecycle Controller 서버** 컬렉션을 삭제한 후 서버를 검색합니다. MECM에서 컬렉션이 자동으로 생성되며 서버가 이 그룹에 추가됩니다.

잘못된 자격 증명으로 인해 서버 검색 실패

검색 중 잘못된 자격 증명 상세 정보를 제공한 경우, iDRAC 버전을 기준으로 다음 해결 방법을 사용할 수 있습니다.

- 2.10.10.10 이상의 iDRAC 버전이 설치된 12세대 PowerEdge 서버를 검색하는 중에, 자격 증명 프로파일에 잘못된 상세 정보를 입력하면 다음과 같은 동작이 발생하면서 서버 검색이 실패합니다.
  - 최초 시도에서는 서버 IP 주소가 차단되지 않습니다.
  - 두 번째 시도에서는 서버 IP 주소가 30초 동안 차단됩니다.
  - 세 번째 및 이후의 시도에서는 서버 IP 주소가 60초 동안 차단됩니다.

  IP 주소 차단이 해제된 후 올바른 자격 증명 프로파일 상세 정보로 서버 검색을 다시 시도할 수 있습니다.
- 어플라이언스에서 서버를 검색하고 추가한 후 기본 iDRAC 자격 증명 프로파일을 변경하면, 서버에서 작업을 수행할 수 없습니다. 서버를 사용하려면 새로운 자격 증명 프로파일을 사용하여 서버를 재검색합니다.

서버 검색 후 잘못된 VRTX 섀시 그룹 생성

이전에 다른 섀시에 있었던 모듈형 서버를 VRTX 섀시에 추가하고 OMIMSSC에서 검색하면 모듈형 서버가 이전의 섀시 서비스 태그 정보를 전달합니다. 따라서 최신 섀시 정보가 아닌 이전 섀시 정보를 가진 VRTX 섀시 그룹이 어플라이언스에 생성됩니다.

이 문제를 해결하려면 다음을 수행합니다.

1. CSIOR을 활성화하고 새로 추가된 모듈형 서버에서 iDRAC를 리셋합니다.
2. VRTX 섀시 그룹의 모든 서버를 수동으로 삭제한 다음, 서버를 다시 검색합니다.

등록된 MECM과 호스트 서버를 동기화할 수 없음

OMIMSSC 콘솔 확장 프로그램을 등록된 MECM과 동기화하는 동안 서버는 동기화 작업에 하위 작업으로 나열되지 않으므로 동기화되지 않습니다.

이 문제를 해결하려면 "관리자 권한으로 실행"으로 MECM 콘솔을 실행하고 서버에 대한 아웃오브밴드 구성을 업데이트합니다. 그런 다음 OMIMSSC 콘솔 확장 프로그램을 등록된 MECM과 동기화합니다.

자세한 내용은 *Microsoft Configuration Manager 및 System Center Virtual Machine Manager를 위한 Microsoft System Center용 OpenManage Integration 버전 7.3 사용자 가이드의* 등록된 Microsoft 콘솔로 동기화 항목을 참조하십시오.

빈 클러스터 업데이트 그룹이 자동 검색 또는 동기화 중에 삭제되지 않음

OMIMSSC에서 클러스터가 검색되면 **유지 관리 센터**에 클러스터 업데이트 그룹이 생성되고 여기에 모든 서버가 나열됩니다. 나중에 SCVMM을 통해 이 클러스터에서 모든 서버를 제거하고 SCVMM 작업으로 자동 검색 또는 동기화를 수행하는 경우 **유지 관리 센터**에서 빈 클러스터 업데이트 그룹이 삭제되지 않습니다.

이 문제를 해결하기 위해 빈 서버 그룹을 삭제하려면 서버를 다시 검색합니다.

클러스터 기능 적용 시 클러스터 생성 실패

클러스터 기능을 적용하는 동안 노드에서 클러스터 생성이 실패하고 운영 체제 배포가 성공한 경우입니다. 클러스터 생성 시 `Failed to install the features on hosts that are required for creating clusters` 오류 메시지가 표시되고 로그에 `Failed to run Pre Cluster Creation Scripts on Host Create Cluster`가 표시됩니다.

이 문제를 해결하려면 클러스터 생성에 사용되는 **물리적 컴퓨터 프로파일**에서 선택한 **컴퓨터 액세스 자격 증명**이 등록된 사용자와 동일한지 확인하십시오. 등록된 사용자는 도메인 관리자 또는 도메인에 시스템을 추가할 수 있는 권한을 가진 도메인 사용자여야 합니다.

클러스터 인식 업데이트 작업 상태를 검색할 수 없음

클러스터 인식 업데이트 작업 상태가 업데이트 작업 완료 후에 표시됩니다.

이 문제를 해결하려면 Microsoft 페일오버 클러스터 관리자 툴을 사용하여 작업 상태를 확인하고 작업 완료 후 SCVMM 서버에서 OMIMSSC 생성 파일을 삭제해야 합니다.

재검색된 서버에 대한 유지 관리 관련 작업 수행 실패

OMIMSSC에서 업데이트 그룹에 속한 서버 또는 모든 서버를 삭제하고 재검색하면 서버에 대해 펌웨어 업데이트, LC 로그 내보내기 및 가져오기, 서버 프로필 내보내기 및 가져오기와 같은 작업을 수행할 수 없습니다.

이 문제를 해결하려면 삭제된 서버 또는 서버를 재검색한 후 **서버 보기**의 **운영 템플릿 배포** 기능을 사용하여 펌웨어 업데이트를 수행하고 기타 유지 보수 시나리오에는 iDRAC를 사용합니다.

일반 시나리오 OMIMSSC

이 섹션에서는 OMIMSSC의 워크플로와는 관계없는 문제 해결 정보를 다룹니다.

호스트 이름을 사용하여 CIFS 공유에 액세스하지 못함

모듈식 서버는 OMIMSSC에서 호스트 이름을 사용하여 CIFS 공유에 액세스하고 작업을 수행할 수 없습니다.

이 문제를 해결하려면 호스트 이름 대신 CIFS 공유가 있는 서버의 IP 주소를 지정합니다.

콘솔 확장에서 작업 및 로그 페이지 표시 실패

OMIMSSC 콘솔 확장에 **작업 및 로그 센터** 페이지가 표시되지 않습니다.

이 문제를 해결하려면 콘솔을 다시 등록한 다음 **작업 및 로그** 페이지를 엽니다.

관리 시스템상의 작업 실패

TLS(Transport Layer Security) 버전 때문에 관리 시스템에서 OMIMSSC의 모든 기능이 예상대로 작동하지 않습니다.

iDRAC 펌웨어 버전 2.40.40.40 이상을 사용하는 경우, 전송 계층 보안(TLS) 버전 1.1 이상은 기본값으로 활성화되어 있습니다. 콘솔 확장을 설치하기 전에 KB 문서 `Support.microsoft.com/en-us/kb/3140245`를 참조하여 TLS 1.1 이상으로 업데이트 및 활성화합니다. OMIMSSC가 예상대로 작동하게 하려면 SCVMM 서버 및 SCVMM 콘솔에서 TLS 1.1 이상에 대한 지원을 활성화하는 것이 좋습니다. iDRAC에 대한 자세한 내용은 Dell.com/idracmanuals에서 확인하십시오.

OMIMSSC의 온라인 도움말 실행 실패

Windows 2012 R2 운영 체제를 사용할 때 상황에 맞는 온라인 도움말 컨텐츠가 실행되어 오류 메시지를 표시합니다.

이 문제를 해결하려면 최신 KB 문서를 참조하여 운영 체제를 업데이트한 후 온라인 도움말 컨텐츠를 봅니다.

OMIMSSC 지원되지 않는 네트워크 공유 암호로 인한 작업 실패

일부 OMIMSSC 작업은 iDRAC에서 지원되지 않는 네트워크 공유 암호의 일부 특수 문자 때문에 실패합니다.

다음은 각 작업 실패와 관련된 작업 실패 및 오류 메시지 목록입니다.

- LC 로그 내보내기 실패 - `Failed to Export Complete LC Logs from iDRAC IP <IP address> Cannot access network share`
- RHEL 및 ESXi 운영 체제 배포 실패 - `Inaccessible network share`
- DRM을 사용한 펌웨어 업데이트 실패 - `Firmware update failed on server with iDRAC IP <IP address> for <Component>`
- Windows 운영 체제 배포 실패 - `Inaccessible network share for iDRAC <IP address>`
- 서버 프로파일 내보내기 및 가져오기 실패 - `Failed to invoke Export Server Profile on iDRAC IP: <iDRAC_IP> with error Cannot Access Network Share`

이 문제를 해결하려면 네트워크 공유에 iDRAC 권장 암호를 사용해야 합니다. 자세한 내용은 iDRAC 설명서를 참조하십시오.

펌웨어 업데이트 시나리오 OMIMSSC

이 섹션에서는 업데이트 원본, 업데이트 그룹, 리포지토리 및 업데이트 후 인벤토리와 관련된 모든 문제 해결 정보를 다룹니다.

로컬 업데이트 소스에 대한 연결 테스트 실패

로컬 업데이트 소스에 대한 상세 정보를 지정한 후, 필수 파일에 액세스하지 못해 연결 테스트가 실패할 수 있습니다.

이 문제를 해결하려면 다음 폴더 구조에 `catalog.gz` 파일이 있는지 확인합니다.

- 로컬 DRM 업데이트 소스: `\\IP address\\catalog\<catalogfile>.gz`

DRM 업데이트 원본 생성 실패

Windows 10 OS(Operating System)에서 실행 중인 관리 서버에서 DRM 업데이트 소스를 생성하지 못해 다음 오류 메시지가 표시될 수 있습니다. `Failed to reach location of update source. Please try again with correct location and/or credentials.`

다음 오류 메시지가 표시되면 OMIMSSC 관리 포털의 **omimsscappliance_main** 로그를 참조하십시오. *`Unix command failed SmbException: com.dell.pg.tetris.business.samba.smbclient.SmbException: session setup failed: NT_STATUS_IO_TIMEOUTwhere EnableSMB1Protocol = false.`*

해결 방법은 다음 KB 문서를 참조하십시오. *support.microsoft.com/en-us/help/4034314*

펌웨어 업데이트 중 리포지토리 생성 실패

업데이트 원본을 생성할 때 잘못된 자격 증명을 제공하여 펌웨어 업데이트 중 리포지토리를 생성할 수 없거나 OMIMSSC 어플라이언스가 업데이트 원본에 연결할 수 없습니다.

이 문제를 해결하려면 OMIMSSC 어플라이언스를 호스팅하는 위치에서 업데이트 원본에 연결할 수 있는지 확인하고 업데이트 원본을 생성할 때 올바른 자격 증명을 제공합니다.

클러스터의 펌웨어 업데이트 실패

OMIMSSC에서 클러스터의 펌웨어 업데이트 작업을 제출하면 특정 오류 때문에 **활동 로그**에 다음 오류 메시지가 표시되며 클러스터가 업데이트되지 않습니다.

```
Cluster Aware Update failed for cluster group <cluster group name>.
```

```
Failed to perform Cluster Aware Update for cluster group <cluster group name>.
```

노트: 클러스터 인식 업데이트 작업은 클러스터 인식 업데이트 보고서가 저장되는 \\<SCVMM CIFS share>\OMIMSSC_UPDATE\reports 폴더에 기록됩니다. \\SCVMM CIFS share\OMIMSSC_UPDATE\reports\log 폴더에는 각 노드에 대한 DSU(Dell EMC System Update) 플러그인 로그가 추가로 포함됩니다. 확장된 스크립트 로그는 Windows 서버 HCI 클러스터의 각 클러스터 노드에 있는 preau.log 및 postcau.log 파일로 구성된 C:\Window\Temp location 위치에서 사용할 수 있습니다.

클러스터의 펌웨어 업데이트가 실패하는 이유와 해결 방법은 다음과 같습니다.

- 선택한 로컬 업데이트 소스에 필요한 DUP 및 카탈로그 파일이 없는 경우.

  이 문제를 해결하려면 필요한 모든 DUP 및 카탈로그 파일이 리포지토리에 있는지 확인한 다음 클러스터의 펌웨어를 업데이트합니다.

- 진행 중인 작업 때문에 클러스터 그룹이 응답하지 않거나 CAU에서 펌웨어 업데이트 작업이 취소된 경우, 클러스터 그룹에 속한 각 서버 클러스터 노드로 DUP가 다운로드 및 배치됩니다.

  이 문제를 해결하려면 Dell 폴더의 파일을 모두 삭제한 다음 클러스터의 펌웨어를 업데이트합니다.

- LC(Lifecycle Controller)가 다른 작업을 수행하고 있는 경우, 클러스터 노드의 펌웨어 업데이트 작업이 실패합니다. LC가 사용 중이어서 업데이트가 실패했는지 확인하려면 다음 경로에서 클러스터 각 노드의 오류 메시지를 확인합니다.
  `C:\dell\suu\invcolError.log`

  ```
  Inventory Failure: IPMI driver is disabled. Please enable or load the driver and then
  reboot the system.
  ```

  이 문제를 해결하려면 서버를 종료하고 전원 케이블을 분리한 다음 서버를 재시작합니다. 재부팅 후 클러스터의 펌웨어를 업데이트합니다.

노트: CAU 오류에 대한 자세한 내용은 Microsoft 장애 조치 클러스터 관리자 툴의 CAU 작업 상태를 확인하고 Microsoft 설명서의 클러스터 인식 업데이트 모범 사례 섹션을 참조하십시오.

작업 큐가 가득 찼기 때문에 펌웨어 업데이트 실패

OMIMSSC에서 iDRAC로 제출한 펌웨어 업데이트 작업이 실패하고 OMIMSSC 메인 로그에 다음 오류가 표시됩니다. `JobQueue Exceeds the size limit. Delete unwanted JobID(s).`

이 문제를 해결하려면 iDRAC에서 완료된 작업을 수동으로 삭제하고 펌웨어 업데이트 작업을 다시 시도합니다. IDRAC의 작업을 삭제하는 방법에 대한 자세한 내용은 **dell.com/support/home**에서 iDRAC 설명서를 참조하십시오.

DRM 업데이트 소스를 사용할 때 펌웨어 업데이트 오류

DRM 업데이트 소스를 사용할 때 공유 폴더에 대한 액세스 권한이 부족하면 펌웨어 업데이트 작업이 실패할 수 있습니다. DRM 업데이트 소스를 생성할 때 제공된 Windows 자격 증명 프로파일이 도메인 관리자 그룹 또는 로컬 관리자 그룹에 포함되지 않은 경우 다음 오류 메시지가 표시됩니다. `Local cache creation failure.`

이 문제를 해결하려면 다음을 수행합니다.

1. DRM에서 리포지토리를 생성한 후 폴더를 마우스 오른쪽 버튼으로 클릭하고 **보안** 탭을 클릭한 다음, **고급**을 클릭합니다.
2. **상속 활성화**를 클릭하고 **이 개체에서 모든 하위 개체 권한 항목을 상속 가능한 권한 항목으로 대체** 옵션을 선택한 다음, 읽기-쓰기 권한이 있는 **전체**과 폴더를 공유합니다.

선택과 상관없는 구성 요소의 펌웨어 업데이트

이러한 개별 서버에서 선택한 구성 요소에 관계없이 펌웨어 업데이트 중에 동일한 서버의 동일한 구성 요소가 업데이트됩니다. 이 현상은 iDRAC 엔터프라이즈 라이선스가 있는 12세대 및 13세대 PowerEdge 서버에서 발견됩니다.

이 문제를 해결하려면 다음 중 하나를 수행합니다.

- 먼저 동일한 서버의 공통 구성 요소에 업데이트를 적용한 다음, 개별 서버의 특정 구성 요소에 업데이트를 적용합니다.
- 운영 중단 시간이 계획되어 있는 단계별 업데이트를 수행하여 펌웨어 업데이트를 적용합니다.

사용자 지정 업데이트 그룹 삭제 오류

사용자 지정 업데이트 그룹에 속한 서버의 작업을 예약한 후 Microsoft 콘솔에서 서버를 삭제하고 등록된 Microsoft 콘솔을 OMIMSSC와 동기화하면, 해당 서버가 사용자 지정 업데이트 그룹에서 제거되고 사전 정의된 업데이트 그룹으로 이동합니다. 이러한 사용자 지정 업데이트 그룹은 예약된 작업과 연결되어 있으므로 삭제할 수 없습니다.

이 문제를 해결하려면 **작업 및 로그** 페이지에서 예약된 작업을 삭제한 다음, 사용자 지정 업데이트 그룹을 삭제합니다.

WinPE 이미지 업데이트 실패

WinPE 이미지를 업데이트하려고 하면 다음 오류 메시지와 함께 업데이트 작업이 실패할 수 있습니다. `Remote connection to console failed.`.

이 문제를 해결하려면 **DISM** 명령을 실행하여 이전에 마운트한 모든 이미지를 Microsoft 콘솔에서 정리하고 WinPE 이미지를 다시 업데이트합니다.

빈도 업데이트 후 폴링 및 알림 벨 색상 변경

OMIMSSC에서 관리 서버를 검색하지 않고 폴링 및 알림 옵션의 빈도를 변경하는 경우, 카탈로그에 변경 사항이 없더라도 잠시 후 벨 색상이 노란색으로 변경됩니다.

이 문제를 해결하려면 관리 대상 서버를 검색한 다음 폴링 및 알림 빈도 옵션을 변경합니다.

OMIMSSC의 운영 체제 배포 시나리오

이 섹션에는 OMIMSSC의 운영 템플릿을 사용한 운영 체제 또는 하이퍼바이저(SCVMM용) 배포와 관련된 모든 문제 해결 정보를 다룹니다.

운영 체제 배포 일반 시나리오

이 섹션에서는 운영 체제 배포와 관련된 모든 일반적인 문제 해결 정보를 다룹니다.

운영 템플릿 배포 실패

선택된 서버에서 운영 템플릿을 배포하면 특성 값이 선택된 .CSV 파일에 적합하지 않거나 템플릿의 구성 때문에 iDRAC IP 또는 iDRAC 자격 증명이 변경됩니다. iDRAC에서 작업이 정상적으로 수행되었지만, 잘못된 .CSV 파일 때문에 OMIMSSC에서 이 작업의 상태가 비정상 또는 실패로 표시되거나, 대상 서버에서 iDRAC가 변경되어 작업을 추적할 수 없습니다.

이 문제를 해결하려면 선택한 .CSV 파일에 적절한 특성 값이 모두 있는지 확인하고, 템플릿의 구성 때문에 iDRAC IP 또는 자격 증명이 변경되지 않도록 합니다.

운영 템플릿 저장 실패

운영 템플릿을 생성할 때 풀 값이 있는 의존 특성의 확인란을 선택 및 해제하면 다음과 같은 오류 메시지가 표시되고 운영 템플릿을 저장할 수 없습니다.

```
Select atleast one attribte, under the selected components, before creating the Operational Template.
```

이 문제를 해결하려면 다음 중 하나를 수행합니다.

- 풀 값이 있는 의존 특성 또는 동일한 의존 특성을 선택하고 운영 템플릿을 저장합니다.
- 새로운 운영 템플릿을 생성합니다.

AMD 서버에 Windows Server 2016 운영 체제 배포 실패

AMD 플랫폼에서의 Windows Server 2016 운영 체제 배포는 x2apic을 지원하지 않습니다. 따라서 운영 체제 배포가 실패합니다.

이 문제를 해결하려면 배포에 사용된 운영 템플릿을 편집하고 BIOS 구성 요소를 선택한 다음 BIOS x2apic 및 논리 프로세서 설정을 비활성화합니다. 그런 다음 이 템플릿을 사용하여 배포를 다시 시도하십시오. 자세한 내용은 Dell EMC AMD 서버가 Windows Server 2016을 설치하는 동안 Windows 로고에서 중단됨 KB 문서를 참조하십시오.

MECM 사용자를 위한 운영 체제 배포 시나리오

이 섹션에서는 MECM 콘솔에서 OMIMSSC를 사용한 운영 체제 배포와 관련된 모든 문제 해결 정보를 다룹니다.

작업 순서에 배포 옵션이 보이지 않음

MECM용 OMIMSSC 콘솔 확장 프로그램을 제거하고 재설치한 후 기존 작업 순서에 **배포** 옵션이 표시되지 않습니다.

이 문제를 해결하려면 편집을 위해 작업 순서를 열고 **적용** 옵션을 다시 활성화한 후 **확인**을 클릭합니다. **배포** 옵션이 다시 표시됩니다.

적용 옵션을 다시 활성화하려면 다음을 수행합니다.

1. 작업 순서를 마우스 오른쪽 버튼으로 클릭하고 **편집**을 선택합니다.
2. **Windows PE에서 재시작**을 선택합니다. **설명** 섹션에 아무 문자나 입력하고 변경 사항이 저장되지 않도록 삭제합니다.
3. **확인**을 클릭합니다.

   이렇게 하면 **적용** 옵션이 다시 활성화됩니다.

서버를 MECM의 Managed Lifecycle Controller ESXi 컬렉션에 추가하지 못함

운영 체제 배포 중에 DHCP 조회가 실패하면, 서버가 시간 초과되고 MECM의 Managed Lifecycle Controller(ESXi) 컬렉션으로 이동하지 않습니다.

이 문제를 해결하려면 MECM 클라이언트 서버를 설치한 후 동기화를 수행하여 서버를 Managed Lifecycle Controller(ESXi) 컬렉션으로 추가합니다.

iDRAC 9 기반 PowerEdge 서버에서 Windows 운영 체제 배포 실패

UEFI 부팅 모드에 있는 iDRAC 9 기반 PowerEdge 서버에서 Windows 운영 체제 배포가 실패합니다.

이 문제를 해결하려면 C:\Program Files\Microsoft Configuration Manager\OSD\bin\x64"에서 찾을 수 있는 Winpeshl.ini 파일에 지연을 추가하십시오. 자세한 내용은 다음에 포함된 Microsoft 포럼 링크 *OS 배포 - 작업 시퀀스를 읽을 수 없음, Wpelnit.exe 자동으로 시작되지 않음*을 참조하십시오.

SCVMM 사용자를 위한 운영 체제 배포 시나리오

이 섹션에서는 SCVMM 콘솔에서 OMIMSSC를 사용한 하이퍼바이저 배포와 관련된 모든 문제 해결 정보를 다룹니다.

LC 또는 방화벽 보호로 인한 하이퍼바이저 배포 실패

하이퍼바이저 배포가 실패하고 활동 로그에 다음 오류 메시지가 표시됩니다. `Error New-SCVMHost failed with following error : An out of band operation (SMASH) for the BMC <IP ADDRESS> failed on IDRAC IP : <IP ADDRESS>..`

다음 이유 중 하나로 인해 이 오류가 발생할 수 있습니다.

- Dell LC(Lifecycle controller) 상태가 잘못되었습니다.

  해결책으로 iDRAC 사용자 인터페이스에 로그인한 후 LC(Lifecycle controller)를 재시작합니다.

  Lifecycle Controller를 재시작한 후 문제가 계속해서 나타난다면 다음의 대안을 사용해 보십시오.
- 안티바이러스 프로그램 또는 방화벽이 `WINRM` 명령의 정상적인 실행을 제한할 수 있습니다.

  다음 KB 문서의 해결방법을 참조하십시오. `support.microsoft.com/kb/961804`

라이브러리 공유에 보존된 드라이버 파일로 인한 하이퍼바이저 배포 실패

하이퍼바이저 배포가 실패하고 활동 로그에 다음 오류 메시지가 표시됩니다.

- **Error**: `Error while applying Hypervisor Profile to host <IP Address>. Failed with error : For input string: ""`
- **Information**: `Successfully deleted drivers from library share sttig.<MicrosoftConsoleName>.com for <server uuid>`
- **Error**: `Deleting staging share (drivers) for <server uuid> failed.`

이러한 오류는 VMM cmdlet `GET-SCJOB status`의 예외 출력으로 인해 발생할 수 있으며, 드라이버 파일이 라이브러리 공유에 남습니다. 재시도하거나 다른 하이퍼바이저 배포를 시도하기 전에 이러한 파일을 라이브러리 공유에서 제거해야 합니다.

라이브러리 공유에서 파일을 제거하려면 다음을 수행합니다.그런 다음 하이퍼바이저를 배포할 수 있습니다.

1. SCVMM 콘솔에서 **라이브러리** > **라이브러리 서버**를 선택한 후 라이브러리 서버로 추가된 IG 서버를 선택합니다.
2. 라이브러리 서버에서 라이브러리 공유를 선택하고 삭제합니다.
3. 라이브러리 공유가 삭제된 후 `\\<Integration Gateway server>\LCDriver\`.를 사용하여 IG 공유에 연결합니다.
4. 드라이버 파일이 들어 있는 폴더를 삭제합니다.

Active Directory에 서버를 추가하는 동안 SCVMM 오류 21119

Active Directory에 서버를 추가하는 동안 SCVMM 오류 21119가 표시됩니다. `Error 21119: The physical computer with <SMBIOS GUID> did not join Active Directory in time. The comptuer was expected to join Active Directory using the computer name <host.domain>.`.

이 문제를 해결하려면 다음을 수행합니다.

1. 얼마 간의 시간동안 기다리며 서버가 Active Directory에 추가되는지 지켜봅니다.
2. 서버가 액티브 디렉토리에 추가되지 않으면 수동으로 Active Directory에 서버를 추가합니다.
3. SCVMM에 서버를 추가합니다.
4. 일단 서버를 SCVMM에 추가한 후 OMIMSSC에서 서버를 재검색합니다.

   서버가 이제 **호스트** 탭 아래에 나열됩니다.

SCVMM 사용자를 위한 Windows 서버 HCI 클러스터 생성 시나리오

이 섹션에는 SCVMM 콘솔에서 OMIMSSC를 사용하여 Windows 서버 HCI를 생성하는 작업과 관련된 모든 문제 해결 정보를 다룹니다.

Windows 서버 HCI 클러스터의 상태를 알 수 없음

기존 클러스터에 속한 노드에 Windows 서버 HCI 클러스터를 생성하면, 스토리지 풀과 디스크 구성에 기존 클러스터의 구성이 포함됩니다. 따라서 클러스터 스토리지 풀이 생성되지 않을 수 있으며 클러스터 스토리지 풀이 생성될 경우 상태가 알 수 없음으로 표시될 수 있습니다.

이 문제를 해결하려면 기존 클러스터 세부 정보가 있는 스토리지 풀 및 디스크 구성을 삭제하고 Windows 서버 HCI 클러스터를 생성합니다. 스토리지 풀 삭제에 대한 자세한 내용은 Microsoft 설명서의 Windows 서버 HCI *상태 및 작동 상태 문제 해결* 섹션을 참조하십시오.

OMIMSSC의 서버 프로필 시나리오

이 섹션에서는 OMIMSSC에서 서버 프로필 내보내기 및 가져오기와 관련된 모든 문제 해결 정보를 다룹니다.

서버 프로파일 내보내기 오류

서버 프로파일 내보내기 작업을 예약했으나 서버 프로파일이 내보내지지 않고 다음 오류 메시지가 표시됩니다. `The selectors for the resource are not valid.`

이 문제를 해결하려면 iDRAC를 리셋한 후 서버 프로파일 내보내기 작업을 예약합니다. 자세한 내용은 `dell.com/support`에서 iDRAC 설명서를 참조하십시오.

서버 프로파일 가져오기 작업이 2시간 후에 시간 초과됨

OMIMSSC에 서버 프로파일 가져오기 작업을 제출하고 2시간이 지나면 작업이 시간 초과됩니다.

이 문제를 해결하려면 다음 단계를 수행합니다.

1. 서버를 시작하고 F2 키를 눌러 **BIOS 설정**으로 들어갑니다.
2. **시스템 설정**을 클릭하고 **기타 설정**을 선택합니다.
3. **오류 시 F1/F2 프롬프트**를 비활성화합니다.

다음 단계를 수행한 후, 서버 프로파일을 다시 내보내고, 동일한 서버 프로파일을 사용하여 해당 서버에서 가져옵니다.

OMIMSSC의 LC 로그 시나리오

이 섹션에서는 LC 로그 내보내기 및 보기와 관련된 모든 문제 해결 정보를 다룹니다.

.CSV 형식으로 LC 로그 내보내기 실패

LC 로그 파일을 .CSV 형식으로 다운로드하려고 할 때 다운로드 작업이 실패합니다.

이 문제를 해결하려면 브라우저에서 로컬 인트라넷 사이트 아래에 OMIMSSC 어플라이언스 FQDN을 추가합니다. 로컬 인트라넷에 OMIMSSC 어플라이언스를 추가하는 방법에 대한 자세한 내용은 Microsoft Endpoint Configuration Manager *및 System Center Virtual Machine Manager를 위한 Microsoft System Center용 Dell EMC OpenManage Integration 버전 7.3 통합 사용자 가이드*의 *LC 로그 보기* 섹션을 참조하십시오.

LC 로그 파일 열기 실패

LC 로그를 수집한 후 서버의 LC 로그 파일을 보려고 하면 다음 오류 메시지가 표시됩니다. "`Failed to perform the requested action. For more information see the activity log`".

이 문제를 해결하려면 iDRAC를 리셋한 후 LC 로그를 수집하여 확인합니다. iDRAC를 리셋하는 방법에 대한 자세한 내용은 `dell.com/support`에서 iDRAC 설명서를 참조하십시오.

연결 테스트 실패

도메인 사용자 계정과 로컬 사용자 계정의 사용자 이름이 동일하고 비밀번호가 다른 경우 Microsoft 콘솔과 OMIMSSC 어플라이언스 간의 연결 테스트가 실패합니다.

예를 들어 도메인 사용자 계정이 `domain\user1`이고 비밀번호가 `pwd1`입니다. 로컬 사용자 계정은 `user1`이고 비밀번호는 `Pwd2`입니다. 위의 도메인 사용자 계정으로 등록하려고 하면 연결 테스트가 실패합니다.

이 문제를 해결하려면 도메인 사용자 및 로컬 사용자 계정에 다른 사용자 이름을 사용하거나 OMIMSSC 어플라이언스에서 Microsoft 콘솔을 등록하는 동안 단일 사용자 계정을 로컬 사용자로 사용합니다.

22

부록 I: 시간대 속성 값

아래 표를 참조하여 MX7000 디바이스에서 시간대 속성 값을 수동으로 입력합니다.

표 12. 시간대 상세 정보

시간대 ID	시간대 차이
TZ_ID_1	(GMT-12:00) 날짜 변경선 서쪽
TZ_ID_2	(GMT+14:00) 사모아
TZ_ID_3	(GMT-10:00) 하와이
TZ_ID_4	(GMT-09:00) 알래스카
TZ_ID_5	(GMT-08:00) 태평양 표준시(미국 및 캐나다)
TZ_ID_6	(GMT-08:00) 바하 캘리포니아
TZ_ID_7	(GMT-07:00) 애리조나
TZ_ID_8	(GMT-07:00) 치와와, 라파스, 마사틀란
TZ_ID_9	(GMT-07:00) 산지 표준시(미국 및 캐나다)
TZ_ID_10	(GMT-06:00) 중앙 아메리카
TZ_ID_11	(GMT-06:00) 중부 표준시(미국 및 캐나다)
TZ_ID_12	(GMT-06:00) 과달라하라, 멕시코시티, 몬테레이
TZ_ID_13	(GMT-06:00) 서스캐처원
TZ_ID_14	(GMT-05:00) 보고타, 리마, 키토
TZ_ID_15	(GMT-05:00) 동부 표준시(미국과 캐나다)
TZ_ID_16	(GMT-05:00) 인디애나(동부)
TZ_ID_17	(GMT-04:30) 카라카스
TZ_ID_18	(GMT-04:00) 아순시온
TZ_ID_19	(GMT-04:00) 대서양 표준시(캐나다)
TZ_ID_20	(GMT-04:00) 쿠이아바
TZ_ID_21	(GMT-04:00) 조지타운, 라파스, 마나우스, 산 후안
TZ_ID_22	(GMT-04:00) 산티아고
TZ_ID_23	(GMT-03:30) 뉴펀들랜드
TZ_ID_24	(GMT-03:00) 브라질리아
TZ_ID_25	(GMT-03:00) 부에노스아이레스
TZ_ID_26	(GMT-03:00) 카옌, 포르탈레자
TZ_ID_27	(GMT-03:00) 그린란드
TZ_ID_28	(GMT-03:00) 몬테비데오
TZ_ID_29	(GMT-02:00) 중부-대서양
TZ_ID_30	(GMT-01:00) 아조레스
TZ_ID_31	(GMT-01:00) 카보베르데 제도

표 12. 시간대 상세 정보 (계속)

시간대 ID	시간대 차이
TZ_ID_32	(GMT+00:00) 카사블랑카
TZ_ID_33	(GMT+00:00) 협정 세계시
TZ_ID_34	(GMT+00:00) 더블린, 에든버러, 리스본, 런던
TZ_ID_35	(GMT+00:00) 몬로비아, 레이캬비크
TZ_ID_36	(GMT+01:00) 암스테르담, 베를린, 베른, 로마, 스톡홀름, 비엔나
TZ_ID_37	(GMT+01:00) 베오그라드, 브라티슬라바, 부다페스트, 류블랴나, 프라하
TZ_ID_38	(GMT+01:00) 브뤼셀, 코펜하겐, 마드리드, 파리
TZ_ID_39	(GMT+01:00) 사라예보, 스코페, 바르샤바, 자그레브
TZ_ID_40	(GMT+01:00) 서중앙 아프리카
TZ_ID_41	(GMT+02:00) 빈트후크
TZ_ID_42	(GMT+02:00) 암만
TZ_ID_43	(GMT+03:00) 이스탄불
TZ_ID_44	(GMT+02:00) 베이루트
TZ_ID_45	(GMT+02:00) 카이로
TZ_ID_46	(GMT+02:00) 다마스쿠스
TZ_ID_47	(GMT+02:00) 하라레, 프리토리아
TZ_ID_48	(GMT+02:00) 헬싱키, 키예프, 리가, 소피아, 탈린, 빌뉴스
TZ_ID_49	(GMT+02:00) 예루살렘
TZ_ID_50	(GMT+02:00) 민스크
TZ_ID_51	(GMT+03:00) 바그다드
TZ_ID_52	(GMT+03:00) 쿠웨이트, 리야드
TZ_ID_53	(GMT+03:00) 모스크바, 상트 페테르부르크, 볼고그라드
TZ_ID_54	(GMT+03:00) 나이로비
TZ_ID_55	(GMT+03:30) 테헤란
TZ_ID_56	(GMT+04:00) 아부다비, 무스카트
TZ_ID_57	(GMT+04:00) 바쿠
TZ_ID_58	(GMT+04:00) 포트루이스
TZ_ID_59	(GMT+04:00) 트빌리시
TZ_ID_60	(GMT+04:00) 예레반
TZ_ID_61	(GMT+04:30) 카불
TZ_ID_62	(GMT+05:00) 예카테린부르크
TZ_ID_63	(GMT+05:00) 이슬라마바드, 카라치
TZ_ID_64	(GMT+05:00) 타슈켄트
TZ_ID_65	(GMT+05:30) 첸나이, 콜카타, 뭄바이, 뉴델리
TZ_ID_66	(GMT+05:30) 스리자야와르데네푸라
TZ_ID_67	(GMT+05:45) 카트만두
TZ_ID_68	(GMT+06:00) 아스타나

표 12. 시간대 상세 정보 (계속)

시간대 ID	시간대 차이
TZ_ID_69	(GMT+06:00) 다카
TZ_ID_70	(GMT+06:00) 노보시비르스크
TZ_ID_71	(GMT+06:30) 양곤(랑군)
TZ_ID_72	(GMT+07:00) 방콕, 하노이, 자카르타
TZ_ID_73	(GMT+07:00) 크라스노야르스크
TZ_ID_74	(GMT+08:00) 베이징, 충칭, 홍콩, 우루무치
TZ_ID_75	(GMT+08:00) 이르쿠츠크
TZ_ID_76	(GMT+08:00) 쿠알라룸푸르, 싱가포르
TZ_ID_77	(GMT+08:00) 퍼스
TZ_ID_78	(GMT+08:00) 타이베이
TZ_ID_79	(GMT+08:00) 울란바토르
TZ_ID_80	(GMT+08:30) 평양
TZ_ID_81	(GMT+09:00) 오사카, 삿포로, 도쿄
TZ_ID_82	(GMT+09:00) 서울
TZ_ID_83	(GMT+09:00) 야쿠츠크
TZ_ID_84	(GMT+09:30) 애들레이드
TZ_ID_85	(GMT+09:30) 다윈
TZ_ID_86	(GMT+10:00) 브리즈번
TZ_ID_87	(GMT+10:00) 캔버라, 멜버른, 시드니
TZ_ID_88	(GMT+10:00) 괌, 포트모르즈비
TZ_ID_89	(GMT+10:00) 호바트
TZ_ID_90	(GMT+10:00) 블라디보스토크
TZ_ID_91	(GMT+11:00) 마가단, 솔로몬 제도 뉴칼레도니아
TZ_ID_92	(GMT+12:00) 오클랜드, 웰링턴
TZ_ID_93	(GMT+12:00) 피지
TZ_ID_94	(GMT+13:00) 누크알로파
TZ_ID_95	(GMT+14:00) 키리티마티
TZ_ID_96	(GMT+02:00) 아테네, 부카레스트

23

부록 II: 풀 값 입력

풀 값 CSV 파일을 입력합니다.

표 13. 풀 값 파일 형식

서비스 태그(자동 입력)	FQDD(자동 입력)	풀 속성 이름	풀 속성 값
시스템별 속성이 내보내진 디바이스의 서비스 태그	시스템별 속성에 연관된 구성 요소를 식별	구성될 시스템별 속성을 식별	지정된 시스템별 속성의 값을 설정

표 14. 하드웨어 구성 요소에 대한 시스템별 값

구성 요소	그룹 이름	특성 이름
BIOS	기타 설정	자산 태그
BIOS	연결 1 설정	초기자 게이트웨이
BIOS	연결 1 설정	이니시에이터 IP 주소
BIOS	연결 1 설정	이니시에이터 서브넷 마스크
BIOS	연결 1 설정	타겟 IP 주소
BIOS	연결 1 설정	타겟 이름
BIOS	연결 2 설정	초기자 게이트웨이
BIOS	연결 2 설정	이니시에이터 IP 주소
BIOS	연결 2 설정	이니시에이터 서브넷 마스크
BIOS	연결 2 설정	타겟 IP 주소
BIOS	연결 2 설정	타겟 이름
BIOS	네트워크 설정	ISCSI 이니시에이터 이름
BIOS	내장형 장치	내장형 네트워크 카드 1 PCIe Link1
BIOS	내장형 장치	내장형 네트워크 카드 1 PCIe Link2
BIOS	내장형 장치	내장형 네트워크 카드 1 PCIe Link3
iDRAC	NIC 정보	DNS RAC 이름
iDRAC	NIC 정보	VLAN 활성화
iDRAC	NIC 정보	VLAN ID
iDRAC	IPv4 정보	IPv4 활성화
iDRAC	IPv4 정보	IPv4 DHCP 활성화
iDRAC	IPv6 정보	IPV6 활성화
iDRAC	IPv6 정보	IPv6 자동 구성
iDRAC	서버 토폴로지	데이터 센터 이름
iDRAC	서버 토폴로지	통로 이름
iDRAC	서버 토폴로지	랙 이름
iDRAC	서버 토폴로지	랙 슬롯

표 14. 하드웨어 구성 요소에 대한 시스템별 값 (계속)

구성 요소	그룹 이름	특성 이름
iDRAC	Active Directory	Active Directory RAC 이름
iDRAC	NIC 정적 정보	DNS 도메인 이름
iDRAC	IPv4 정적 정보	IPv4 주소
iDRAC	IPv4 정적 정보	넷마스크
iDRAC	IPv4 정적 정보	게이트웨이
iDRAC	IPv4 정적 정보	DNS Server 1
iDRAC	IPv4 정적 정보	DNS Server 2
iDRAC	IPv6 정적 정보	IPv6 주소 1
iDRAC	IPv6 정적 정보	IPv6 게이트웨이
iDRAC	IPv6 정적 정보	IPv6 링크 로컬 접두사 길이
iDRAC	IPv6 정적 정보	IPV6 DNS 서버 1
iDRAC	IPv6 정적 정보	IPv6 DNS 서버 2
iDRAC	서버 운영 체제	서버 호스트 이름
iDRAC	서버 토폴로지	방 이름
iDRAC	NIC 정보	DNS RAC 이름
iDRAC	NIC 정보	DNS RAC 이름
iDRAC	IPv4 정보	IPv4 DHCP 활성화
iDRAC	IPv4 정적 정보	IPv4 주소
iDRAC	IPv4 정적 정보	넷마스크
iDRAC	IPv4 정적 정보	게이트웨이
iDRAC	IPv4 정적 정보	DNS Server 1
iDRAC	IPv4 정적 정보	DNS Server 2
iDRAC	IPv6 정적 정보	IPv6 게이트웨이
iDRAC	IPv6 정적 정보	IPv6 링크 로컬 접두사 길이
iDRAC	IPv6 정적 정보	DNS Server 1
iDRAC	IPv6 정적 정보	DNS Server 2
네트워크	iSCSI 일반 매개변수	CHAP 상호 인증 수행
네트워크	iSCSI 첫 번째 타겟 매개변수	연결
네트워크	iSCSI 두 번째 타겟 매개변수	연결
네트워크	iSCSI 첫 번째 타겟 매개변수	부팅 LUN
네트워크	iSCSI 첫 번째 타겟 매개변수	CHAP ID
네트워크	iSCSI 첫 번째 타겟 매개변수	CHAP 암호
네트워크	iSCSI 첫 번째 타겟 매개변수	IP 주소
네트워크	iSCSI 첫 번째 타겟 매개변수	iSCSI 이름
네트워크	iSCSI 첫 번째 타겟 매개변수	TCP 포트
네트워크	iSCSI 이니시에이터 매개변수	CHAP ID
네트워크	iSCSI 이니시에이터 매개변수	CHAP 암호

표 14. 하드웨어 구성 요소에 대한 시스템별 값 (계속)

구성 요소	그룹 이름	특성 이름
네트워크	iSCSI 이니시에이터 매개변수	기본 게이트웨이
네트워크	iSCSI 이니시에이터 매개변수	IP 주소
네트워크	iSCSI 이니시에이터 매개변수	IPv4 주소
네트워크	iSCSI 이니시에이터 매개변수	IPv4 기본 게이트웨이
네트워크	iSCSI 이니시에이터 매개변수	IPv4 기본 DNS
네트워크	iSCSI 이니시에이터 매개변수	IPv4 보조 DNS
네트워크	iSCSI 이니시에이터 매개변수	IPv6 주소
네트워크	iSCSI 이니시에이터 매개변수	IPv6 기본 게이트웨이
네트워크	iSCSI 이니시에이터 매개변수	IPv6 기본 DNS
네트워크	iSCSI 이니시에이터 매개변수	IPv6 보조 DNS
네트워크	iSCSI 이니시에이터 매개변수	iSCSI 이름
네트워크	iSCSI 이니시에이터 매개변수	기본 DNS
네트워크	iSCSI 이니시에이터 매개변수	보조 DNS
네트워크	iSCSI 이니시에이터 매개변수	서브넷 마스크
네트워크	iSCSI 이니시에이터 매개변수	서브넷 마스크 접두사
네트워크	iSCSI 보조 디바이스 매개변수	보조 디바이스 MAC 주소
네트워크	iSCSI 두 번째 타겟 매개변수	부팅 LUN
네트워크	iSCSI 두 번째 타겟 매개변수	CHAP 암호
네트워크	iSCSI 두 번째 타겟 매개변수	CHAP ID
네트워크	iSCSI 두 번째 타겟 매개변수	IP 주소
네트워크	iSCSI 두 번째 타겟 매개변수	iSCSI 이름
네트워크	iSCSI 두 번째 타겟 매개변수	TCP 포트
네트워크	iSCSI 보조 디바이스 매개변수	독립 타겟 이름 사용
네트워크	iSCSI 보조 디바이스 매개변수	독립 타겟 포털 사용
네트워크	기본 구성 페이지	가상 FIP MAC 주소
네트워크	기본 구성 페이지	가상 iSCSI 오프로드 MAC 주소
네트워크	기본 구성 페이지	가상 MAC 주소
네트워크	파티션 n 구성	가상 MAC 주소
네트워크	기본 구성 페이지	가상 포트 GUID
네트워크	기본 구성 페이지	가상 World Wide 노드 이름
네트워크	파티션 n 구성	가상 World Wide 노드 이름
네트워크	기본 구성 페이지	가상 World Wide 포트 이름
네트워크	파티션 n 구성	가상 World Wide 포트 이름
네트워크	기본 구성 페이지	World Wide 노드 이름
네트워크	파티션 n 구성	World Wide 노드 이름
FC	Fibre Channel 타겟 구성	부팅 검사 선택
FC	Fibre Channel 타겟 구성	첫 번째 FC 타겟 LUN

표 14. 하드웨어 구성 요소에 대한 시스템별 값 (계속)

구성 요소	그룹 이름	특성 이름
FC	Fibre Channel 타겟 구성	첫 번째 FC 타겟 World Wide 포트 이름
FC	Fibre Channel 타겟 구성	두 번째 FC 타겟 LUN
FC	Fibre Channel 타겟 구성	두 번째 FC 타겟 World Wide 포트 이름
FC	포트 구성 페이지	가상 World Wide 노드 이름
FC	포트 구성 페이지	가상 World Wide 포트 이름
MX 섀시 관리 모듈	섀시 위치	데이터 센터
MX 섀시 관리 모듈	섀시 위치	공간
MX 섀시 관리 모듈	섀시 위치	통로
MX 섀시 관리 모듈	섀시 위치	랙
MX 섀시 관리 모듈	섀시 위치	랙 슬롯
MX 섀시 관리 모듈	섀시 위치	위치

표 15. Windows 구성 요소에 대한 시스템별 값

서비스 태그 (자동 입력)	FQDD(자동 입력)	풀 속성 이름	풀 속성 값	속성 및 입력 방법에 대한 자세한 내용
xxxxxxx	WINDOWS	호스트 이름	WIN19SRVDTA	설명: 배포/프로비저닝된 서버에서 설정될 호스트 이름입니다.
xxxxxxx	WINDOWS	ServerMngNIC	<MAC 주소>	설명: 시스템 센터 및 OMMISSC 어플라이언스와 통신할 수 있는 네트워크 포트의 MAC 주소입니다. 방법: 특정 포트로 이동하여 iDRAC에서 MAC 주소를 검색합니다.
xxxxxxx	WINDOWS	논리적 네트워크	정적 IP를 사용하는 OSD	설명: MN에 적용될 정적 IP 풀, 서브넷 및 기타 네트워크 세부 정보를 전달하는 SCVMM에서 생성된 네트워크 프로파일입니다 방법: SCVMM에서 논리 네트워크 프로파일을 생성하고 생성된 템플릿 이름을 제공합니다. 자세한 내용은 Microsoft 설명서의 VMM 네트워킹 패브릭 계획 섹션을 참조하십시오.
xxxxxxx	WINDOWS	IP 서브넷	100.100.28.0/22	설명: 상기 논리적 네트워크 프로파일의 정적 IP 풀 입력에 대한 서브넷 마스크입니다.
xxxxxxx	WINDOWS	IP 주소	100.100.31.145	설명: 배포/프로비저닝된 관리형 노드에 적용될 정적 IP입니다.

표 16. Windows가 아닌 구성 요소에 대한 시스템별 값

서비스 태그 (자동 입력)	FQDD(자동 입력)	풀 속성 이름	풀 속성 값	속성 및 입력 방법에 대한 자세한 내용
xxxxxxx	LINUX	호스트 이름	<호스트 이름>	설명: 배포/프로비저닝된 서버에서 설정될 호스트 이름입니다.
xxxxxxx	LINUX	IP 주소	<정적 IP 주소>	설명: 배포/프로비저닝된 관리형 노드에 적용될 정적 IP입니다.
xxxxxxx	LINUX	SUBNETMASK	<서브넷 마스크>	설명: 정적 IP 풀에 대한 서브넷 마스크입니다.
xxxxxxx	LINUX	DEFAULTGATEWAY	<기본 게이트웨이>	내용: 기본 게이트웨이입니다.
xxxxxxx	LINUX	PRIMARYDNSSERVER	<주 DNS 서버>	설명: 주 DNS 서버입니다.
xxxxxxx	LINUX	SECONDARYDNSSERVER	<보조 DNS 서버>	설명: 보조 DNS 서버입니다.

24

Dell EMC 지원 사이트에서 지원 콘텐츠 액세스

직접 링크를 사용하거나 Dell EMC 지원 사이트로 이동하거나 검색 엔진을 사용하여 시스템 관리 툴 어레이와 관련된 지원 콘텐츠에 액세스합니다.

- 직접 링크:
  - Dell EMC 엔터프라이즈 시스템 관리 및 Dell EMC 원격 엔터프라이즈 시스템 관리 -https://www.dell.com/esmmanuals
  - Dell EMC 가상화 솔루션 -https://www.dell.com/SoftwareManuals
  - Dell EMC OpenManage -https://www.dell.com/openmanagemanuals
  - iDRAC -https://www.dell.com/idracmanuals
  - Dell EMC OpenManage Connections Enterprise 시스템 관리 -https://www.dell.com/OMConnectionsEnterpriseSystemsManagement
  - Dell EMC 서비스 가능 툴 -https://www.dell.com/serviceabilitytools
- Dell EMC 지원 사이트:
  1. https://www.dell.com/support로 이동합니다.
  2. **모든 제품 찾아보기**를 클릭합니다.
  3. **모든 제품** 페이지에서 **소프트웨어**를 클릭한 후 필요한 링크를 클릭합니다.
  4. 필요한 제품을 클릭한 다음 필요한 버전을 클릭합니다.

검색 엔진을 사용하여 검색 상자에 문서 이름 및 버전을 입력합니다.