데스크탑 클라이언트용 OpenManage Integration for VMware vCenter
사용 설명서 버전 2.2

주, 주의 및 경고

노트: "주"는 컴퓨터를 보다 효율적으로 사용하는 데 도움을 주는 중요 정보를 제공합니다.

주의: "주의"는 하드웨어 손상이나 데이터 손실의 가능성을 설명하며, 이러한 문제를 방지할 수 있는 방법을 알려줍니다.

경고: "경고"는 재산상의 피해나 심각한 부상 또는 사망을 유발할 수 있는 위험이 있음을 알려줍니다.

2014 - 04

Rev. A00

목차

1

개요

OpenManage Integration for VMware vCenter

VMware vCenter는 IT 관리자가 VMware vSphere ESX/ESXi 호스트를 관리하고 모니터하는 데 사용하는 기본 콘솔입니다. 표준 가상 환경에서는 VMware 경고 및 모니터링을 사용하여 관리자에게 별도의 콘솔을 실행하여 하드웨어 문제를 해결한다는 메시지를 표시합니다. 이제 OpenManage Integration for VMware vCenter를 사용하여 관리자가 다음과 같이 가상 환경에서 Dell 하드웨어를 관리하고 모니터할 수 있는 새로운 기능을 사용할 수 있습니다.

- 경고 및 환경 모니터링
- 단일 서버 모니터링 및 보고
- 펌웨어 업데이트
- 향상된 배포 옵션

주요 특징

OpenManage Integration for VMware vCenter를 사용하여 다음을 수행할 수 있습니다.

인벤토리	주요 자산의 재고 목록을 만들고 구성 작업을 수행하고 Dell 플랫폼의 클러스터 및 DataCenter를 제공합니다.
모니터링 및 경고	주요 하드웨어 결함을 감지하고 가상화 인식 작업을 수행합니다(예: 작업부하 마이그레이션 또는 유지 보수 모드에 호스트 배치).
펌웨어 업데이트	Dell 하드웨어를 최신 버전의 BIOS 및 펌웨어로 업데이트합니다.
배포 및 프로비저닝	하드웨어 프로필과 하이퍼바이저 프로필을 생성하고 운영 체제 미설치 Dell PowerEdge 서버에서 vCenter를 사용하여 PXE 없이 원격으로 두 프로필을 조합하여 배포합니다.
서비스 정보	Dell 온라인에서 보증 정보를 가져옵니다.

vCenter 관리에 대한 OpenManage Integration for VMware vCenter의 지원

OpenManage Integration for VMware vCenter에서 현재 vCenter 관리 기능을 보조하는 추가 가상화 기능을 제공합니다.

- 작업을 압축하고 펌웨어 업데이트 및 운영 체제 미설치 배포와 같은 관리 프로세스를 vCenter Server 관리 콘솔에 추가합니다.
- 필요한 PXE(Preboot Execution Environment)가 없이 여러 운영 체제 미설치 서버의 배포를 구성합니다.
- 서버 문제를 진단하기 위해 추가 정보(인벤토리, 이벤트 및 경보)를 제공합니다.

- 표준 vCenter 인증, 규칙 및 권한과 통합합니다.

OpenManage Integration for VMware vCenter 기능

OpenManage Integration for VMware vCenter의 고급 기능은 다음과 같습니다.

- 표준 vCenter 이벤트 및 알람 서브시스템을 사용하여 Dell 플랫폼 모니터링
- 고급 하드웨어 관리 및 구성 수행
- PXE를 사용하지 않고 운영 체제 미설치 시스템에서 VMware ESX / ESXi 하이퍼바이저의 자동 배치 수행
- 하드웨어 및 VMware ESX / ESXi 하이퍼바이저 프로필 빌드
- 펌웨어 업데이트 수행
- 인프라 문제 해결
- Datacenter 및 클러스터 보기에서 보고 - CSV 파일로 내보내기
- 표준 vCenter 역할 및 권한과 OpenManage Integration for VMware vCenter 기능 통합

2
OpenManage Integration for VMware vCenter 구성

다음 섹션에서는 OpenManage Integration for VMware vCenter 초기 구성에 대한 단계별 지침을 제공합니다. 또한 업그레이드, 제거 및 보안 역할 정보도 다음 섹션에 포함되어 있습니다.

보안 역할 및 권한

OpenManage Integration for VMware vCenter는 암호화된 형식으로 사용자 자격 증명을 저장합니다. 이는 문제를 유발할 수 있는 잘못된 요청을 피하기 위해 클라이언트 응용프로그램에 암호를 제공하지 않습니다. 데이터베이스 백업은 사용자 지정 보안 구문을 사용하여 완전히 암호화되므로 데이터가 오용되지 않습니다.

기본적으로 관리자 그룹의 사용자는 모든 권한을 가지고 있습니다. 관리자는 VMware vCenter 클라이언트 또는 웹 클라이언트 내에서 OpenManage Integration for VMware vCenter의 모든 기능을 사용할 수 있습니다. 관리자가 아닌 사용자가 제품을 관리할 수 있도록 하려면 두 가지 Dell 역할이 포함된 역할을 생성한 후 인벤토리의 루트/상위 노드에 권한을 할당하고 필요한 경우 사용자에게 액세스 권한을 부여할 하위 노드에 권한을 전파합니다. 예를 들어, 사용자가 클러스터 A만 관리하도록 하려면 클러스터 A에 대한 권한을 유지하고 다른 클러스터에 대한 권한은 제거합니다.

데이터 무결성

OpenManage Integration for VMware vCenter 가상 어플라이언스, 관리 콘솔 및 vCenter 간의 통신은 SSL/HTTPS를 사용하여 수행됩니다. OpenManage Integration for VMware vCenter은 vCenter와 어플라이언스 간의 신뢰할 수 있는 통신에 사용되는 SSL 인증서를 생성합니다. 또한 통신 및 OpenManage Integration for VMware vCenter 등록 전에 vCenter 서버의 인증서를 확인하고 신뢰합니다. VMware vCenter의 OpenManage Integration for VMware vCenter 콘솔 탭에서는 관리 콘솔과 백 엔드 서버 간에 키가 전송되는 동안 부적절한 요청을 방지하기 위해 보안 절차를 사용합니다. 이 보안 유형을 통해 교차 사이트 요청 위조가 실패합니다.

보안 관리 콘솔 세션에는 5분의 유휴 시간 제한이 있으며 세션이 현재 브라우저 창 및/또는 탭에서만 유효합니다. 사용자가 새 창 또는 탭에서 세션을 열려고 시도하면 유효한 세션을 요청하는 보안 오류가 생성됩니다. 이 작업은 사용자가 관리 콘솔 세션을 공격하도록 시도할 수 있는 악성 URL을 클릭하지 못하도록 방지합니다.

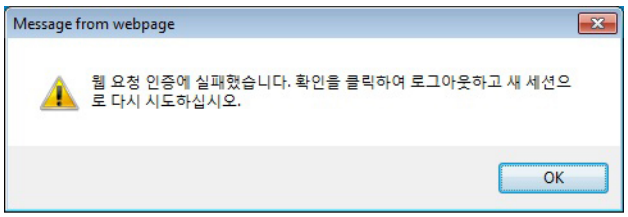

그림 1. 오류 메시지

액세스 제어 인증, 권한 부여 및 역할

OpenManage Integration for VMware vCenter에서는 vSphere 클라이언트의 현재 사용자 세션과 가상 어플라이언스를 위해 저장된 관리 자격 증명을 사용하여 vCenter 작업을 수행합니다. OpenManage Integration for VMware

vCenter에서는 vCenter 서버의 기본 제공 역할 및 권한 모델을 사용하여 가상 어플라이언스와 vCenter 관리 개체(호스트 및 클러스터)에 대한 사용자 작업에 권한을 부여 합니다.

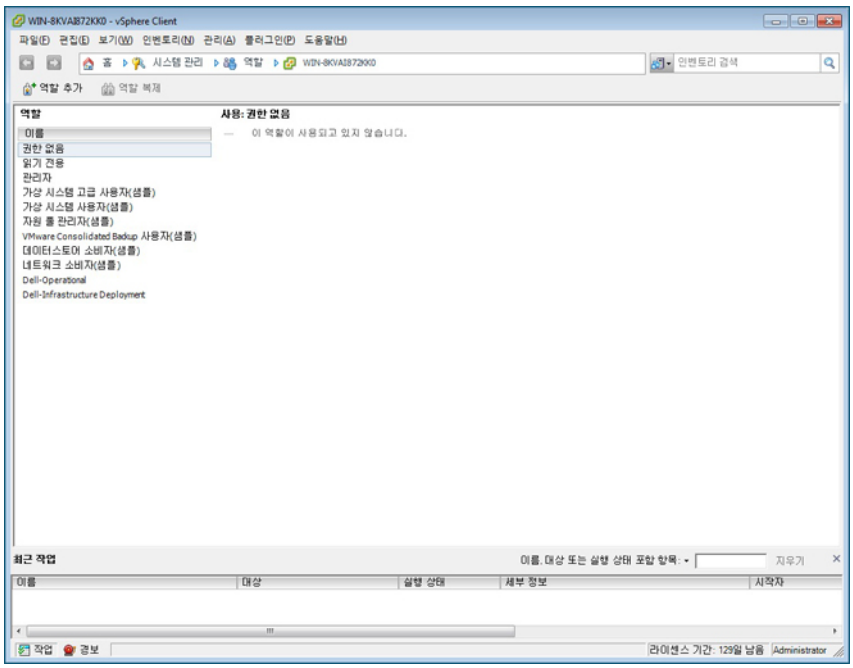

그림 2. vCenter vSphere 클라이언트 역할 및 권한

Dell 작업 역할

펌웨어 업데이트, 하드웨어 인벤토리, 호스트 재시작, 유지 보수 모드에 호스트 배치 또는 vCenter 서버 작업 생성을 비롯하여 어플라이언스 및 vCenter 서버 작업을 수행하기 위한 권한/그룹을 포함합니다.

이 역할에 다음 권한 그룹이 포함됩니다.

권한 그룹 - Dell.Configuration	권한 - 호스트 관련 작업 수행, VCenter 관련 작업 수행, SelLog 구성, 연결 프로필 구성, ClearLed 구성 및 펌웨어 업데이트
권한 그룹 - Dell.Inventory	권한 - 인벤토리 구성, 보증 검색 구성 및 읽기 전용 구성
권한 그룹 - Dell.Monitoring	권한 - 모니터링 구성 및 모니터
권한 그룹 - Dell.Reporting(사용되지 않음)	권한 - 보고서 생성 및 보고서 실행

Dell 인프라 배포 역할

이 역할에는 특히 하이퍼바이저 배포 기능과 관련된 권한이 포함됩니다.

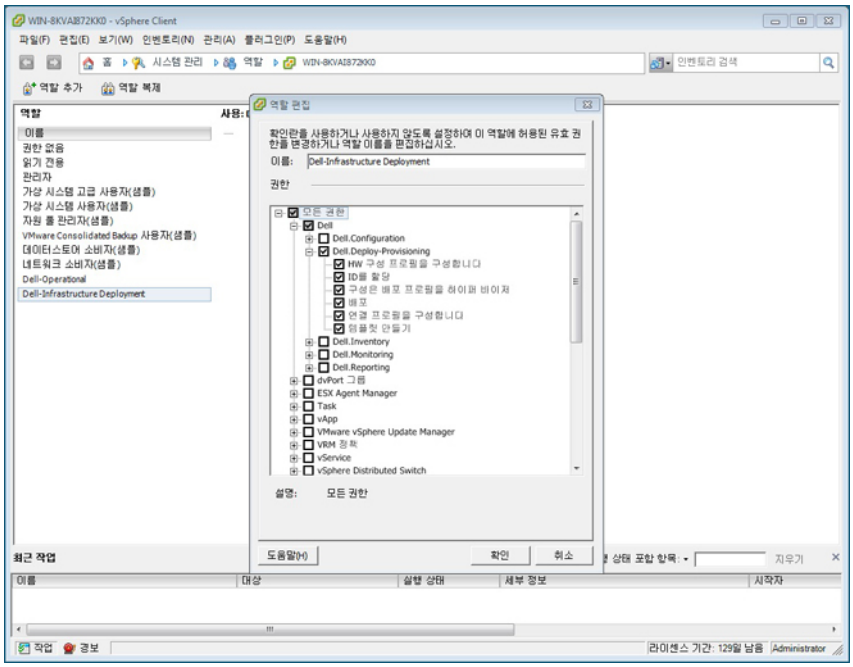

그림 3. Dell 인프라 배포 역할

이 역할에서 제공하는 권한은 템플릿 생성, HW 구성 프로필 구성, 하이퍼바이저 배포 프로필 구성, 연결 프로필 구성, ID 할당 및 배포입니다.

Dell.Deploy - 프로비저닝	템플릿 생성, HW 구성 프로필 구성, 하이퍼바이저 배포 프로필 구성, 연결 프로필 구성, ID 할당 및 배포

권한 이해

OpenManage Integration for VMware vCenter에서 수행되는 모든 작업은 권한과 연결되어 있습니다. 다음 섹션에 사용 가능한 작업 및 연관된 권한이 나열되어 있습니다.

- Dell.Configuration.Perform vCenter-Related Tasks
  - 유지 보수 모드 종료 및 시작
  - 권한을 쿼리하기 위해 vCenter 사용자 그룹 가져오기
  - 경고 구성 및 구성(예: 이벤트 설정 페이지에서 경고 활성화/비활성화)
  - vCenter에 이벤트/경고 게시
  - 이벤트 설정 페이지에 이벤트 설정 구성
  - 이벤트 설정 페이지에서 기본 경고 복원
  - 경고/이벤트 설정을 구성하는 동안 클러스터에 대한 DRS 상태 확인
  - 업데이트 또는 기타 구성 작업을 수행한 후 호스트 재부팅
  - vCenter 작업 상태/진행률 모니터
  - vCenter 작업 생성(예: 펌웨어 업데이트 작업, 호스트 구성 작업 및 인벤토리 작업)
  - vCenter 작업 상태/진행률 업데이트
  - 호스트 프로필 가져오기
  - 데이터 센터에 호스트 추가

- 클러스터에 호스트 추가
- 호스트에 프로필 적용
- CIM 자격 증명 가져오기
- 규정 준수를 위해 호스트 구성
- 규정 준수 작업 상태 가져오기

- Dell.Inventory.Configure ReadOnly
  - 연결 프로필을 구성하는 동안 vCenter 트리를 구성하기 위해 모든 vCenter 호스트 가져오기
  - 탭을 선택할 때 호스트가 Dell 서버인지 확인
  - vCenter의 주소/IP 가져오기
  - 호스트 IP/주소 가져오기
  - vSphere 클라이언트 세션 ID를 기반으로 현재 vCenter 세션 사용자 가져오기
  - 트리 구조에 vCenter 인벤토리를 표시하기 위해 vCenter 인벤토리 트리 가져오기

- Dell.Monitoring.Monitor
  - 이벤트를 게시하기 위한 호스트 이름 가져오기
  - 이벤트 로그 작업 수행(예: 이벤트 개수 가져오기 또는 이벤트 로그 설정 변경)
  - 이벤트/경고 등록, 등록 취소 및 구성 – SNMP 트랩 수신 및 이벤트 게시

- Dell.Configuration.Firmware Update
  - 펌웨어 업데이트 수행
  - 펌웨어 업데이트 마법사 페이지에서 펌웨어 리포지토리 및 DUP 파일 정보 로드
  - 펌웨어 인벤토리 쿼리
  - 펌웨어 리포지토리 설정 구성
  - 준비 폴더 구성 및 준비 기능을 사용하여 업데이트 수행
  - 네트워크 및 리포지토리 연결 테스트

- Dell.Deploy-Provisioning.Create Template
  - 배포 템플릿 생성, 표시, 삭제 및 편집

- Dell.Configuration.Perform Host-Related Tasks
  - LED 점멸, LED 지우기, Dell 서버 관리 탭에서 OMSA URL 구성
  - OMSA 콘솔 시작
  - iDRAC 콘솔 실행
  - SEL 로그 표시 및 지우기

- Dell.Inventory.Configure Inventory
  - Dell 서버 관리 탭에 시스템 인벤토리 표시
  - 저장소 상세정보 가져오기
  - 전원 모니터링 상세정보 가져오기
  - 연결 프로필 페이지에 연결 프로필 생성, 표시, 편집, 삭제 및 테스트
  - 인벤토리 스케줄 예약, 업데이트 및 삭제
  - 호스트에서 인벤토리 실행

3

OpenManage Integration for VMware vCenter 구성 또는 편집 방법 이해

OpenManage Integration for VMware vCenter의 기본 설치를 완료한 후, 다음 섹션에 설명된 방법 중 하나를 사용하여 어플라이언스를 구성할 수 있습니다.

- **구성 마법사를 사용하는 구성 작업**
- **설정 옵션을 사용하는 구성 작업**

구성 마법사를 사용하는 것이 가장 일반적으로 사용되는 방법이지만, Dell Management Center의 어플라이언스 설정 페이지를 통해 완료할 수도 있습니다.

마법사에서는 *저장 후 계속*을 클릭하지만 설정 페이지에서는 *적용*을 클릭하는 점을 제외하고 두 영역에 있는 사용자 인터페이스가 비슷합니다.

구성 마법사를 사용하는 구성 작업

구성 마법사를 사용하여 OpenManage Integration for VMware vCenter를 구성할 때 다음과 같은 작업을 사용합니다.

1. 구성 마법사 시작 페이지
2. 새 연결 프로필 생성
3. 이벤트 및 알람 구성
4. 프록시 서버 설정
5. 인벤토리 작업 예약
6. 보증 검색 작업 실행
7. 배포 자격 증명 구성
8. 기본 펌웨어 업데이트 리포지토리 설정
9. OMSA 링크 사용

설정 옵션을 사용하는 구성 작업

다음과 같은 작업을 통해 OpenManage Integration for VMware vCenter 구성 작업을 설정하거나 편집합니다.

- 새 연결 프로필 생성
- 이벤트 및 알람 구성
- 프록시 서버 설정
- 인벤토리 작업 스케줄 수정
- 보증 검색
- 배포 자격 증명 보기 또는 편집
- 펌웨어 리포지토리 및 자격 증명 설정
- OMSA 링크 사용

OpenManage Integration for VMware vCenter 홈 페이지

OpenManage Integration for VMware vCenter 홈 페이지에 로그인하면 탐색 단추가 왼쪽 창에 있고 오른쪽 창에는 유용한 링크 및 정보가 있습니다. 이 디자인은 사용자가 자주 수행하는 작업에 주요 링크를 제공합니다. 이러한 모든 작업을 왼쪽 창을 탐색하여 확인할 수 있지만 쉽게 사용할 수 있도록 홈 페이지에도 표시됩니다. 이 페이지에 제공된 작업은 다음과 같은 범주에 속합니다.

- 호스트 및 서버 배포
  이 섹션은 호스트 및 서버 배포에 대한 자세한 정보를 제공합니다.
- vSphere 호스트 및 운영 체제 미설치 서버 준수
  이 섹션에서는 비준수 호스트 또는 운영 체제 미설치 서버에 대한 자세한 정보를 보거나 이를 해결하는 마법사를 실행할 수 있습니다.
- 인벤토리 스케줄
  이 섹션에서는 인벤토리 예약 방법을 확인할 수 있습니다.
- 보증 데이터 검색 스케줄
  이 섹션에서 보증 스케줄을 자세히 알아보거나 확인/변경할 수 있습니다.
- 라이센싱
  이 섹션에서는 라이센스에 관해 자세히 알아봅니다. 링크를 사용하여 라이센스 작업으로 갑니다.
- 이벤트 및 알람 설정
  이벤트 및 알람 설정에 대해 자세히 알아 보거나 이 설정을 구성할 수 있는 링크를 사용할 수 있습니다.
- 호스트 연결 라이센스
  실시간으로 호스트 연결 라이센스를 볼 수 있습니다. 또한 지금 구입 링크를 사용하여 여러 개의 호스트를 관리할 수 있는 전체 버전의 라이센스를 구입할 수 있습니다. 지금 구입 링크는 데모 라이센스를 사용하는 경우에만 나타납니다.
- vCenter 연결 라이센스. 여기에서 VMware vCenter 연결 라이센스 관련 정보를 볼 수 있습니다. vCenter 라이센스 연결에 관한 자세한 내용은 OpenManage Integration for VMware vCenter 라이센스 정보를 참조하십시오.

구성 마법사 시작 페이지

OpenManage Integration for VMware vCenter을 설치한 후에는 구성해야 합니다.

1. **Home(홈)** 페이지의 **vSphere Client**에서, **Management(관리)** 탭 아래의 **Dell Management Center** 아이콘을 클릭합니다.
2. **Dell Management Center** 아이콘을 처음 클릭하면 **Configuration Wizard(구성 마법사)**가 열립니다. **Dell Management Center → Settings(설정)** 페이지에서도 이 마법사에 액세스할 수 있습니다.
3. **Welcome(시작)** 탭에서 수행할 단계를 검토하고 **Next(다음)**를 클릭합니다.

새 연결 프로필 생성 [마법사]

연결 프로필은 가상 어플라이언스가 Dell 서버와 통신하는 데 사용하는 자격 증명을 저장합니다. 각 Dell 서버는 하나의 연결 프로필과 연결되어 있어야 Dell Management Plug-in에서 관리할 수 있습니다. 하나의 연결 프로필에 여러 개의 서버를 할당할 수 있습니다. 연결 프로필을 생성하는 방법은 구성 마법사 및 Dell 관리 센터의 설정 옵션을 사용하는 방법과 비슷합니다.

노트: Dell PowerEdge 12세대 이상 서버를 사용하는 호스트에 설치할 경우에는 OMSA 에이전트 설치가 필요하지 않습니다. 11세대 서버에 설치할 경우 배포 프로세스 중에 OMSA 에이전트가 자동으로 설치됩니다.

마법사를 사용하여 새 연결 프로필을 생성하려면 다음을 수행합니다.

1. **Connection Profiles(연결 프로필)** 탭에서 **Create New(새로 생성)**를 클릭합니다.
2. **Profile Name and Description(프로필 이름 및 설명)** 패널에서 사용자 지정 연결 프로필을 관리하는 데 유용한 **Profile Name(프로필 이름)**과 선택 항목인 **Description(설명)**을 입력하고 **Next(다음)**를 클릭합니다.
3. **Associated Hosts (연결된 호스트 패널)**에서 연결 프로필과 연결된 호스트를 선택하고, **Next(다음)**를 클릭합니다.
4. 자격 증명 및 연결 프로토콜에 대한 정보를 확인하고 **Next(다음)**를 클릭합니다.
5. iDRAC 패널에서 **iDRAC credential information(iDRAC 자격 증명 정보)**을 입력합니다.
   a. **User Name(사용자 이름)**, **Password(암호)** 및 **Verify Password(암호 확인)**를 입력합니다. 사용자 이름은 공백을 포함하여 최대 16 문자를 포함할 수 있습니다. 암호는 반드시 일치해야 하며 ASCII-프린트 가능 문자만 사용할 수 있습니다.

      노트: 암호는 최대 20개의 프린트 가능한 ASCII 문자를 포함합니다. 도메인 이름에는 영숫자, - (대시), 및 . (마침표) 만 포함됩니다.

   b. **Certificate Check(인증서 확인)**에서, iDRAC 인증서를 다운로드하여 저장하고 이후의 모든 연결에서 유효성을 검사하려면 **Enable(활성화)**을 선택하고 확인을 수행하지 않고 인증서를 저장하지 않으려면 **Disable(비활성화)**을 선택합니다.

      Active Directory를 사용하는 경우 활성화를 선택해야 합니다.
6. **Next(다음)**를 클릭합니다.
7. **Host Root Credentials(호스트 루트 자격 증명)** 패널에서 다음을 수행합니다.
   a. **User Name(사용자 이름)**, **Password(암호)** 및 **Verify Password(암호 확인)**를 입력합니다. 이 두 암호는 일치해야 합니다.

      노트: 암호는 127자를 넘지 않아야 하며 특수 문자를 사용할 수 없습니다.

      노트: iDRAC Express나 엔터프라이즈 카드가 없는 서버의 경우, iDRAC 테스트 연결이 실행될 시, *Not Applicable for this system(이 시스템에 적용 안 됨)* 메시지가 표시됩니다.

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

   b. **Certificate Check(인증서 확인)**에서, OMSA 인증서를 다운로드하여 저장하고 이후의 모든 연결에서 유효성을 검사하려면 **Enable(활성화)**을 선택하고 확인을 수행하지 않고 인증서를 저장하지 않으려면 **Disable(비활성화)**을 선택합니다.
8. **Next(다음)**을 클릭합니다.
9. **Test Connection(테스트 연결)** 창에서는 입력된 iDRAC 및 호스트 루트 자격 증명을 선택한 서버에서 테스트합니다. 다음 중 하나를 수행합니다.
   - 테스트를 시작하려면 **Test Selected(선택된 항목 테스트)**를 클릭합니다. 다른 옵션은 비활성화됩니다.
   - 테스트를 중지하려면 **모든 테스트 중단**을 클릭합니다.
10. 프로필을 완료하려면 **Save(저장)**를 클릭합니다.
11. 이벤트 및 알람 구성을 계속하려면 **Save and Continue(저장 후 계속)**를 클릭합니다.

이벤트 및 알람 구성 [마법사]

구성 마법사를 사용하거나 Dell Management Center의 설정 옵션을 사용하여 이벤트 및 알람을 구성합니다.

노트: 12세대 이전의 호스트에서 이 기능을 사용하려면 가상 어플라이언스를 OMSA의 트랩 대상으로 구성해야 vCenter에 호스트 이벤트가 표시됩니다.

이벤트 및 알람을 구성하려면 다음을 수행합니다.

1. **구성 마법사**의 **이벤트 게시 수준**에서 다음 중 하나를 선택합니다.
   - 이벤트 게시 안 함 - 하드웨어 이벤트를 차단합니다.

- 모든 이벤트 게시 - 모든 하드웨어 이벤트를 게시합니다.
- 위험 및 경고 이벤트만 게시 - 위험 또는 경고 수준의 하드웨어 이벤트만 게시합니다.
- 가상화 관련 위험 및 경고 이벤트만 게시 - 가상화 관련 위험 및 경고 이벤트만 게시합니다. 기본 이벤트 게시 수준입니다.

2. 모든 하드웨어 알람 및 이벤트를 사용하려면 **Enable Alarms for Dell Hosts(Dell 호스트에 알람 활성화)** 확인란을 선택합니다.

   노트: 알람이 활성화된 Dell 호스트가 유지 보수 모드로 전환되어 위험 이벤트에 대응합니다.

3. 표시되는 대화상자에서 **계속**을 클릭하여 변경을 허용하거나 **취소**를 클릭합니다.

   노트: 이 단계는 **Dell 호스트에 알람 활성화**를 선택한 경우에만 표시됩니다.

4. 관리되는 모든 Dell 서버에서 기본 vCenter 알람 설정을 복원하려면 **Restore Default Alarms(기본 알람 복원)**를 클릭합니다.

   변경이 적용되는 데 1분 정도 걸릴 수 있습니다.

5. 마법사를 계속하려면 **저장 후 계속**을 클릭합니다.

OpenManage Integration for VMware vCenter 어플라이언스 백업 복원은 모든 알람 설정을 복원하지 않습니다. 그러나, OpenManage Integration for VMware GUI의 **알람 및 이벤트** 필드에 복원된 설정을 표시합니다. 이 문제를 해결하려면 OpenManage Integration for VMware GUI의**Manage(관리) → Settings(설정)** 탭에서 이벤트 및 알람 설정을 수동으로 변경합니다.

노트: 어플라이언스를 복원한 후에 그래픽 사용자 인터페이스가 활성화되어 있다해도 이벤트 및 알람 설정은 활성화되지 않습니다. 설정 페이지에서 이벤트 및 알람 설정을 다시 활성화해야 합니다.

프록시 서버 설정 [마법사]

구성 마법사에서 프록시 서버를 설정하거나 Dell Management Center의 **Settings(설정) → Proxy(프록시)** 페이지를 사용하여 나중에 설정합니다.
프록시 서버를 설정하려면 다음을 수행합니다.

1. **HTTP 프록시 구성 창**에서 다음 중 하나를 수행합니다.
   - 프록시 서버를 사용하지 않으려면 **저장 후 계속**을 클릭합니다.
   - 프록시 서버를 사용하려면 **설정** 아래에 **프록시 서버 주소**를 입력합니다.
2. **프록시 포트 번호**를 입력합니다.
3. 필요한 경우 **자격 증명 필요** 확인란을 선택합니다.
4. **자격 증명 필요**를 선택한 경우 다음을 수행합니다.
   a. **프록시 사용자 이름** 텍스트 상자에서 프록시 사용자 이름을 입력합니다.
   b. **프록시 암호** 텍스트 상자에서 프록시 암호를 입력합니다.
   c. **암호 확인** 텍스트 상자에 프록시 암호를 다시 입력합니다.
5. **프록시**에서 **프록시 사용** 확인란을 선택합니다.
6. 옵션을 저장하고 계속하려면 **저장 후 계속**을 클릭합니다.

인벤토리 작업 예약 [마법사]

인벤토리 일정 구성 방법은 연결 마법사에서 수행하는 방법과 **Dell Management Center → Settings(설정)**옵션을 사용하는 방법이 비슷합니다. 마법사에서는 인벤토리를 즉시 실행할 수 있는 옵션을 제공한다는 점이 다릅니다.

노트: OpenManage Integration for VMware vCenter에 업데이트된 정보가 계속해서 표시되도록 하려면 주기적인 인벤토리 작업을 예약하는 것이 좋습니다. 인벤토리 작업을 수행하면 최소한의 리소스가 사용되며 호스트 성능이 저하되지 않습니다.

인벤토리 작업을 예약하려면 다음을 수행합니다.

1. **Configuration Wizard(구성 마법사)**의 **Inventory Schedule(인벤토리 일정)** 창에서 다음 중 하나를 수행합니다.
   - 인벤토리 스케줄을 실행하려면 **선택한 요일**을 클릭합니다.
   - 인벤토리 스케줄을 실행하지 않으려면 **Dell 호스트에서 인벤토리를 실행하지 않음**을 선택합니다.
2. **On Selected Days(선택한 요일)**를 선택한 경우 다음을 수행합니다.
   a. 인벤토리를 실행할 각 요일 옆에 있는 확인란을 선택합니다.
   b. 텍스트 상자에 HH:MM 형식으로 시간을 입력합니다.
      입력하는 시간은 로컬 시간입니다. 따라서 가상 어플라이언스 시간대에 인벤토리를 실행하려면 로컬 시간대와 가상 어플라이언스 시간대와의 시차를 계산하여 적절한 시간을 입력하십시오.
3. 변경사항을 적용하고 계속하려면 **Save and Continue(저장 후 계속)**를 클릭합니다.

보증 검색 작업 실행 [마법사]

보증 검색 작업 구성은 마법사에서 수행하는 방법과 **Dell Management Center → Settings(설정)** 옵션을 사용하는 방법이 비슷합니다. 또한 현재 작업 큐에서 지금 보증 검색 작업을 실행할 수 있습니다.

보증 검색 작업을 실행하려면 다음을 수행합니다.

1. **구성 마법사**의 **보증 스케줄** 창에서 다음 중 하나를 수행합니다.
   - 보증 스케줄을 실행하려면 **선택한 요일**을 클릭합니다.
   - 보증 스케줄을 실행하지 않으려면, **보증 데이터 검색 안 함**을 선택합니다.
2. **선택한 요일**을 선택한 경우 다음을 수행합니다.
   a. 보증 작업을 실행할 각 요일 옆에 있는 텍스트 상자를 선택합니다.
   b. 텍스트 상자에 HH:MM 형식으로 시간을 입력합니다.
      입력하는 시간은 로컬 시간입니다. 따라서 가상 어플라이언스 시간대에 인벤토리를 실행하려면 로컬 시간대와 가상 어플라이언스 시간대와의 시차를 계산하여 적절한 시간을 입력하십시오.
3. 변경사항을 적용하고 계속하려면 **저장 후 계속**을 클릭합니다.

배포 자격 증명 구성 [마법사]

배포 자격 증명은 AutoDiscovery를 사용하여 검색된 운영 체제 미설치 시스템과 안전하게 통신하는 데 사용됩니다. 보안 통신의 경우 초기 검색부터 배포 프로세스가 끝날 때까지 iDRAC를 사용합니다. 배포가 완료되면 자격 증명은 배포 마법사에서 운영 체제 미설치 시스템에 일치하는 연결 프로필에 있는 자격 증명으로 변경됩니다. 배포 자격 증명이 변경되면 해당 시점부터 새로 검색된 모든 시스템이 새 자격 증명으로 프로비저닝됩니다. 하지만 변경 이전에 검색된 서버의 자격 증명은 영향을 받지 않습니다.

노트: OpenManage Integration for VMware vCenter는 프로비저닝 서버 역할을 합니다. 배포 자격 증명은 자동 검색 프로세스에서 프로비저닝 서버로서 플러그인을 사용하는 iDRAC에 설정됩니다.

배포 자격 증명을 구성하려면 다음을 수행합니다.

1. **배포 자격 증명** 창에서 자격 증명을 보거나 변경할 수 있습니다. 운영 체제 미설치 서버가 이러한 자격 증명을 연결 프로필에 지정된 자격 증명으로 변경합니다.
2. 자격 증명을 변경하려면 **운영 체제 미설치 서버 배포용 자격 증명**에서 다음을 수행합니다.
   a. **사용자 이름** 텍스트 상자에서 사용자 이름을 편집합니다.
   b. **암호** 텍스트 상자에서 암호를 편집합니다.
   c. **암호 확인** 텍스트 상자에서 암호를 확인합니다.
3. 지정된 자격 증명을 저장하고 구성 마법사를 계속하려면 **저장 후 계속**을 클릭합니다.

기본 펌웨어 업데이트 리포지토리 설정 [마법사]

펌웨어 리포지토리 설정에는 배포된 서버를 업데이트하는 데 사용되는 펌웨어 카탈로그 위치가 포함되어 있습니다. 처음에 이 마법사에서 펌웨어 리포지토리를 설정하거나 **Dell Management Center → Settings(설정)** 옵션에서 나중에 설정할 수 있습니다. 또한 OpenManage Integration 탭에서 나중에 펌웨어 업데이트를 실행할 수 있습니다.

기본 펌웨어 업데이트 리포지토리를 설정하려면 다음을 수행합니다.

1. **Configuration Wizard(구성 마법사)**의 **Firmware Repository(펌웨어 리포지토리)** 페이지에서 펌웨어 업데이트에 사용되는 기본 리포지토리를 선택하려면 다음 중 하나를 선택합니다.

   - Dell 온라인

     스태이징 폴더가 있는 기본 펌웨어 리포지토리(ftp.dell.com)입니다. OpenManage Integration for VMware vCenter가 선택한 펌웨어 업데이트를 다운로드하고 스태이징 폴더에 저장한 후 필요에 따라 적용합니다.
   - 로컬/공유 리포지토리

     Dell Repository Manager(Dell 리포지토리 관리자) 응용 프로그램을 사용하여 생성됩니다. 로컬 리포지토리는 Windows 기반 파일 공유에 있어야 합니다.
2. **Local/shared repository(로컬/공유 리포지토리)**를 선택한 경우 다음을 수행합니다.
   a. 다음과 같은 형식을 사용하여 **Catalog File Location(카탈로그 파일 위치)**을 입력합니다.

      - xml 파일용 NFS 공유: host:/share/filename.xml
      - gz 파일용 NFS 공유: host:/share/filename.gz
      - xml 파일용 CIFS 공유: \\host\share\filename.xml
      - gz 파일용 CIFS 공유: \\host\share\filename.gz

   b. CIFS 공유를 사용하는 경우 **User Name(사용자 이름)**, **Password(암호)** 및 **Verify Password(암호 확인)**을 입력합니다. 이 두 암호는 일치해야 합니다. 이러한 필드는 CIFS 공유를 입력할 때만 활성화됩니다.

      노트: @ 문자는 공유 네트워크 폴더 사용자 이름/암호에 사용할 수 없습니다.

   c. 항목의 유효성을 검사하려면 **Begin Test(테스트 시작)**를 클릭합니다.
3. 이 선택 항목을 저장하고 **Configuration Wizard(구성 마법사)**를 계속하려면 **Save and Continue(저장 후 계속)**를 클릭합니다.

OMSA 링크 사용 [마법사]

OpenManage Integration for VMware vCenter 가상 어플라이언스에서 OMSA(OpenManage Server Administator)를 실행하려면 OMSA 웹 서버가 설치 및 구성되어 있어야 합니다. 웹 서버 설치 및 구성 방법에 대한 지침을 보려면 *OpenManage Server Administrator 설치 안내서*를 참조하십시오.

노트: OMSA는 Dell PowerEdge 12세대 서버 이전의 Dell 서버에서만 필요합니다.

OMSA를 사용하여 다음을 수행할 수 있습니다.

- vCenter 요소를 관리합니다(자세한 센서/구성요소 수준 상태 정보).
- 명령 로그 및 SEL(시스템 이벤트 로그)을 지웁니다.
- NIC 통계를 가져옵니다.
- OpenManage Integration for VMware vCenter가 선택한 호스트에서 이벤트를 캡처하는지 확인합니다.

1. **Configuration Wizard(구성 마법사)**의 **OpenManage Server Admin** 페이지에서 **OMSA Web Server URL(OMSA 웹 서버 URL)** 텍스트 상자를 사용하여 OMSA URL을 입력합니다. HTTPS와 포트 번호를 포함하는 전체 URL을 입력해야 합니다. 예를 들어,

https:\\ <OMSA_Server_IP_or_hostname>: 1311.

2. 이 URL을 저장하고 구성 마법사를 마치려면 **Finish(완료)**를 클릭합니다.

NFS 공유 구성

백업 및 복원 작업, 펌웨어 업데이트, 스테이징 폴더를 위해 OpenManage Integration for VMware vCenter에서 NFS 공유를 사용하려면 특정 구성 항목을 완료해야 합니다. CIFS 공유에는 추가 구성이 필요하지 않습니다.

NFS 공유를 구성하려면 다음을 수행합니다.

1. NFS 공유를 호스트하는 Linux 또는 Unix OS 시스템에서 **/etc/exports**를 편집하여 **/share/path <appliance IP> (rw) *(ro)**를 추가합니다.

   이렇게 하면 가상 어플라이언스는 공유에 대해 전체 읽기 및 쓰기 액세스 권한이 허용되지만 기타 모든 사용자는 읽기 권한으로만 제한됩니다.

2. nfs 서비스 시작:

   ```
   service portmap start service nfs start service nfslock status
   ```

   노트: 위의 단계는 사용 중인 Linux 배포에 따라 다를 수 있습니다.

3. 이미 실행 중인 서비스가 있는 경우:

   ```
   exportfs -ra
   ```

설정 개요

설정 섹션에서 다음 작업을 수행할 수 있습니다.

- 일반: vCenter의 Dell 호스트 탭에 표시되는 OMSA URL을 설정합니다. 보증 만료 알림을 활성화 또는 비활성화로 설정할 수도 있습니다.
- 이벤트 및 알람: 모든 하드웨어 알람을 활성화 또는 비활성화로 설정합니다(현재 경고 상태는 알람 탭에 표시됨). 수신되는 이벤트 및 경고 필터링을 구성할 수도 있습니다.
- 프록시: 인터넷 사이트와 통신하는 동안 HTTP 프록시 사용량을 활성화 또는 비활성화로 설정합니다.
- 인벤토리 스케줄: vCenter 호스트 인벤토리 스케줄을 설정합니다.
- 보증 스케줄: Dell 온라인에서 Dell 호스트의 보증 정보 검색 스케줄을 설정합니다.
- 배포 자격 증명: 초기 검색 및 운영 체제 미설치 서버를 배포하는 동안 Dell 서버와 통신하는 데 사용되도록 자격 증명을 설정합니다.
- 펌웨어 리포지토리: 펌웨어 업데이트가 저장되는 위치를 편집할 수 있습니다.
- 보안: 배포되는 서버를 제한하는 서버 화이트 리스트(white list)를 제공합니다.

일반 설정 개요

일반 설정은 다음과 같은 작업에 사용됩니다.

- OMSA(OpenManage Server Administrator) URL을 정의합니다.
- 보증 만료 알림을 활성화 또는 비활성화로 설정합니다.

OMSA 소프트웨어를 사용하여 다음과 같은 작업을 수행할 수 있습니다.

- vCenter 요소를 관리합니다(자세한 센서, 구성요소 수준 상태 정보).
- 명령 로그 및 SEL(시스템 이벤트 로그)을 지웁니다.
- NIC 통계를 가져옵니다.
- OpenManage Integration for VMware vCenter가 선택한 호스트에서 이벤트를 캡처하는지 확인합니다.

노트: OMSA 소프트웨어는 Dell PowerEdge 12세대 서버 이전의 Dell 서버에서만 필요합니다.

보증 만료 알림을 사용하여 다음을 수행할 수 있습니다.

- 보증 만료 날짜를 모니터합니다.
- 경고 또는 위험 경고가 생성된 이후에 남아 있는 최소 보증 일 수 임계값을 설정합니다. 경고는 호스트의 OpenManage Integration 탭에 아이콘으로 표시됩니다.

관련 작업:

- OMSA 링크 사용
- 서버 보증 만료 알림 사용 또는 사용 안 함

구성 마법사 외부에서 OMSA 링크 사용

OpenManage Integration for VMware vCenter 가상 어플라이언스에서 OMSA(OpenManage Server Administrator)를 실행하려면 OMSA 웹 서버가 설치 및 구성되어 있어야 합니다. 웹 서버 설치 및 구성 방법에 대한 지침을 보려면 사용 중인 OMSA 버전의 *Dell OpenManage Server Administrator 설치 안내서*를 참조하십시오.

노트: OMSA는 Dell PowerEdge 12세대 서버 이전의 Dell 서버에서만 필요합니다.

OMSA 링크를 사용하려면 다음을 수행합니다.

1. **Dell Management Center**의 OMSA 시작 관리자 아래에서 **Settings(설정)** → **General(일반)**에서 **Edit(편집)**를 클릭합니다.
2. **OMSA Web Server URL(OMSA 웹 서버 URL)** 텍스트 상자에서 OMSA의 URL을 입력합니다. HTTPS와 포트 번호 1311을 포함하는 전체 URL을 입력해야 합니다.
3. 이 URL을 저장하려면 **Apply(적용)**를 클릭합니다.

   OMSA 트랩 대상 설정에 대한 자세한 내용은 OMSA 트랩 대상 설정을 참조하십시오.

서버 보증 만료 알림 사용 또는 사용 안 함

보증 설정은 보증 일정을 사용 또는 사용 안 함으로 설정한 다음 임계값 경고 최소 일 수를 설정함으로써 서버 보증 정보가 Dell 온라인에서 검색되는 시기를 제어합니다. 이 페이지를 사용하여 호스트 및 클러스터의 서버 보증 만료 알림을 사용 또는 사용 안 함으로 설정합니다. Dell 관리 센터의 설정, 일반 페이지에서 이 기능을 설정하거나 편집합니다.

서버 보증 만료 알림을 사용하거나 사용하지 않으려면 다음을 수행합니다.

1. **Dell Management Center**에서 **설정** → **일반**을 클릭합니다.
2. 알림을 사용하려면 **일반** 페이지에서 **보증 상태 알림 활성화** 확인란을 선택합니다.
3. **임계값 경고 최소 일 수**를 설정하려면 다음을 수행합니다.
   a. 경고를 설정하려면 **경고** 드롭다운 목록에서 서버 보증 상태에 대한 경고 일 수를 선택합니다.
   b. 라이센스 위험 상태를 설정하려면 **위험** 드롭다운 목록에서 위험 상태의 서버 보증을 경고하는 일 수를 설정합니다.
4. 변경사항을 적용하려면 **적용**을 클릭합니다.

새 연결 프로필 생성

연결 프로필은 가상 어플라이언스가 Dell 서버와 통신하는 데 사용하는 자격 증명을 저장합니다. 각 Dell 서버는 하나의 연결 프로필과 연결되어 있어야 OpenManage Integration for VMware vCenter에서 관리할 수 있습니다. 하나의 연결 프로필에 여러 개의 서버를 할당할 수 있습니다. 연결 프로필을 생성하는 방법은 구성 마법사 및**Dell Management Center** → **설정**을 사용하는 방법과 비슷합니다. 구성 마법사는 Dell Management Console에 처음 액세스할 때 실행하거나 설정 창에서 나중에 실행할 수 있습니다.

노트: 이 릴리스의 Dell PowerEdge 12세대 이상 서버의 호스트 설치에서는, OMSA 에이전트 설치가 필수가 아닙니다. Dell PowerEdge 11세대 서버 설치의 경우 배포 프로세스 중에 OMSA 에이전트가 자동으로 설치됩니다.

노트: 라이센싱에 대한 자세한 내용은 OpenManage Integration for VMware vCenter 라이센스 정보를 참조하십시오.

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

새 연결 프로필을 생성하려면 다음을 수행합니다.

1. **OpenManage Integration for VMware vCenter**의 왼쪽 창에서 **Connection Profiles(연결 프로필)**를 클릭합니다.
2. **Profile Name and Description(프로필 이름 및 설명)** 페이지에서 사용자 지정 연결 프로필을 관리하는 데 유용한 **Connection Profile Name(연결 프로필 이름)**과 선택사항인 **Connection Profile Description(연결 프로필 설명)**을 입력합니다.
3. **Associated Hosts(연결된 호스트)** 페이지에서 연결 프로필에 사용할 호스트를 선택하고 **Next(다음)**를 클릭합니다.
4. **Credentials(자격 증명)** 페이지의 정보를 읽고 **Next(다음)**를 클릭합니다.
5. iDRAC 페이지의 자격 증명 아래에서 다음 중 하나를 수행합니다.

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

   - Active Directory를 사용할 iDRAC가 이미 구성되어 있고 Active Directory에 활성화되어 있으면 **Use Active Directory(Active Directory 사용)** 확인란을 선택합니다. 그렇지 않으면 iDRAC 자격 증명 구성 단계로 건너뜁니다.
     - **Active Directory User Name(Active Directory 사용자 이름)** 텍스트 상자에 사용자 이름을 입력합니다. 사용자 이름은 도메인\사용자 이름, 도메인/사용자 이름 또는 사용자 이름@도메인 형식 중 하나를 입력합니다. 사용자 이름은 256자로 제한됩니다. 사용자 이름 제한사항에 대해서는 Microsoft Active Directory 설명서를 참조하십시오.
     - **Active Directory Password(Active Directory 암호)** 텍스트 상자에 암호를 입력합니다. 암호는 127자로 제한됩니다.
     - **Verify Password(암호 확인)** 텍스트 상자에 암호를 다시 입력합니다.
     - Certificate Check(인증서 확인) 드롭다운 목록에서 다음 중 하나를 선택합니다.
       * iDRAC 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **Enable(활성화)**을 선택합니다.
       * 인증서 확인을 수행하지 않고 저장하지 않으려면 **Disabled(비활성화)**를 선택합니다.
   - Active Directory 없이 iDRAC 자격 증명을 구성하려면 다음을 수행합니다.
     - **User Name(사용자 이름)** 텍스트 상자에 사용자 이름을 입력합니다. 사용자 이름은 16자로 제한됩니다. 사용 중인 iDRAC 버전에서의 사용자 이름 제한사항을 보려면 iDRAC 설명서를 참조하십시오.

       노트: 로컬 iDRAC 계정에 관리 권한이 있어야 펌웨어 업데이트, 하드웨어 프로필 적용, 하이퍼바이저 배포를 수행할 수 있습니다.
     - **Password(암호)** 텍스트 상자에 암호를 입력합니다. 암호는 20자로 제한됩니다.
     - **Verify Password(암호 확인)** 텍스트 상자에 암호를 다시 입력합니다.
     - Certificate Check(인증서 확인) 드롭다운 목록에서 다음 중 하나를 선택합니다.
       * iDRAC 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **Enable(활성화)**을 선택합니다.

* iDRAC 인증서 확인을 수행하지 않고 저장하지 않으려면 **Disabled(비활성화)**를 선택합니다.

6. **Next(다음)**를 클릭합니다.
7. Host Credentials(호스트 자격 증명) 페이지의 자격 증명 아래에서 다음 중 하나를 수행합니다.

- Active Directory를 사용할 호스트가 이미 구성되어 있고 Active Directory에 활성화되어 있으면 **Use Active Directory(Active Directory 사용)** 확인란을 선택합니다. 그렇지 않으면 호스트 자격 증명 구성 단계로 건너뜁니다.
  - **Active Directory User Name(Active Directory 사용자 이름)** 텍스트 상자에 사용자 이름을 입력합니다. 사용자 이름은 도메인\사용자 이름, 도메인/사용자 이름 또는 사용자 이름@도메인 형식 중 하나를 입력합니다. 사용자 이름은 256자로 제한됩니다. 사용자 이름 제한사항에 대해서는 Microsoft Active Directory 설명서를 참조하십시오.
  - **Active Directory Password(Active Directory 암호)** 텍스트 상자에 암호를 입력합니다. 암호는 127자로 제한됩니다.
  - **Verify Password(암호 확인)** 텍스트 상자에 암호를 다시 입력합니다.
  - Certificate Check(인증서 확인) 드롭다운 목록에서 다음 중 하나를 선택합니다.
    * 호스트 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **Enable(활성화)**을 선택합니다.
    * 호스트 인증서 확인을 수행하지 않고 저장하지 않으려면 **Disabled(비활성화)**를 선택합니다.
- Active Directory 없이 호스트 자격 증명을 구성하려면 다음을 수행합니다.
  - **User Name(사용자 이름)** 텍스트 상자에 사용자 이름을 입력합니다. 읽기 전용 기본 사용자 이름은 root입니다. **Use Active Directory(Active Directory 사용)**을 선택하는 경우 사용자 이름이 root와 다를 수 있습니다.
  - **Password(암호)** 텍스트 상자에 암호를 입력합니다. 암호는 127자로 제한됩니다.

    노트: OMSA 자격 증명은 ESX 및 ESXi 호스트에 사용된 자격 증명과 동일합니다.
  - **Verify Password(암호 확인)** 텍스트 상자에 암호를 다시 입력합니다.
  - Certificate Check(인증서 확인) 드롭다운 목록에서 다음 중 하나를 선택합니다.
    * 호스트 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **Enable(활성화)**을 선택합니다.
    * 호스트 인증서 확인을 수행하지 않고 저장하지 않으려면 **Disabled(비활성화)**를 선택합니다.

8. **Next(다음)**을 클릭합니다.
9. **Test Connection(연결 테스트)** 링크를 사용하여 선택한 서버에 제공된 iDRAC 및 호스트 자격 증명의 유효성을 검증합니다. 다음 중 하나를 수행합니다.
   - 테스트를 시작하려면 **Test Selected(선택된 항목 테스트)**를 클릭합니다. 다른 옵션은 비활성화됩니다.
   - **테스트 중단**을 클릭합니다.

   노트: iDRAC 익스프레스 또는 엔터프라이즈 카드가 없는 서버의 경우 iDRAC 테스트 연결 시 Not Applicable for this system(이 시스템에 해당되지 않음)이라는 메시지가 표시됩니다.
10. 프로필을 완료하려면 **Save(저장)**를 클릭합니다.
    연결 프로필을 관리하려면 연결 프로필 관리를 참조하십시오.

이벤트 및 알람 구성

Dell Management Center 이벤트 및 알람 페이지를 사용하여 모든 하드웨어 알람을 사용 또는 사용 안 함으로 설정할 수 있습니다. 현재 경고 상태는 vCenter 알람 탭에 표시됩니다. 위험 이벤트는 실제 또는 임박한 데이터 손실이

나 시스템 오류를 나타냅니다. 경고 이벤트는 심각한 상태는 아니지만 향후 문제 발생의 가능성을 나타냅니다. VMware 알람 관리자를 사용하여 이벤트 및 알람을 사용으로 설정할 수도 있습니다. 이벤트는 호스트 및 클러스터 보기의 vCenter 작업 및 이벤트 탭에 표시됩니다.

노트: Dell PowerEdge 12세대 서버 이전의 호스트에서 이 기능을 사용하려면 가상 어플라이언스를 OMSA의 트랩 대상으로 구성해야 vCenter에 호스트 이벤트가 표시됩니다. OMSA에 대한 자세한 내용은 OMSA 트랩 대상 설정을 참조하십시오.

Dell Management Center의 설정 옵션을 사용하여 이벤트 및 알람을 구성할 수 있습니다.
이벤트 및 알람을 구성하려면 다음을 수행합니다.

1. **Dell Management Center**의 **Settings(설정)** → **Events and Alarsm(이벤트 및 알람)**에서 **Edit(편집)**을 클릭합니다.
2. **Event Posting Levels(이벤트 게시 수준)**에서 다음 중 하나를 선택합니다.
   - 이벤트 게시 안 함 - 하드웨어 이벤트를 차단합니다.
   - 모든 이벤트 게시 - 모든 하드웨어 이벤트를 게시합니다.
   - 위험 및 경고 이벤트만 게시 - 위험 또는 경고 수준의 하드웨어 이벤트만 게시합니다.
   - 가상화 관련 위험 및 경고 이벤트만 게시 - 가상화 관련 위험 및 경고 이벤트만 게시합니다. 기본 이벤트 게시 수준입니다.
3. 모든 하드웨어 알람 및 이벤트를 사용하려면 **Enable Alarms for Dell Hosts(Dell 호스트에 알람 활성화)** 확인란을 선택합니다.

   노트: 알람이 활성화된 Dell 호스트가 유지 보수 모드로 전환되어 위험 이벤트에 대응합니다.
4. 표시되는 대화상자에서 **Continue(계속)**를 클릭하여 변경을 허용하거나 **Cancel(취소)**을 클릭합니다.
5. 관리되는 모든 Dell 서버에서 기본 vCenter 알람 설정을 복원하려면 **Restore Default Alarms(기본 알람 복원)**를 클릭합니다.

   변경이 적용되는 데 1분 정도 걸릴 수 있습니다.
6. 저장하려면 **Save(저장)**를 클릭합니다.

프록시 구성 정보

프록시 설정은 HTTP 프록시 및 웹(Dell 온라인 포함)에서 정보를 검색하는 데 필요한 모든 자격 증명을 정의합니다. 예를 들면 다음과 같습니다.

- 프록시 서버 사용 또는 사용 안 함
- 필요한 프록시 서버 및 포트 번호 입력
- 모든 필수 자격 증명 정의 - 사용자 이름 및 암호

관련 작업:

- 프록시 서버 설정
- 웹 기반 데이터 검색에 HTTP 프록시 사용
- 관리 콘솔을 사용하여 HTTP 프록시 설정

프록시 서버 설정

구성 마법사에서 프록시 서버를 설정하거나 설정 옵션, 프록시를 사용하여 나중에 설정합니다.

노트: 프록시 암호는 31자를 넘을 수 없습니다.

프록시 서버를 설정하려면 다음을 수행합니다.

1. Dell Management Center에서 **설정** → **HTTP 프록시**를 선택하고 **편집**을 클릭합니다.
2. **HTTP 프록시** 창에서 다음 중 하나를 수행합니다.

- 프록시 서버를 사용하지 않으려면 **저장 후 계속**을 클릭합니다.
- 프록시 서버를 사용하려면 **설정** 아래에 **프록시 서버 주소**를 입력합니다.

3. **프록시 포트 번호**를 입력합니다.
4. 필요한 경우 **자격 증명 필요** 확인란을 선택합니다.
5. **자격 증명 필요**를 선택한 경우 다음을 수행합니다.
   a. **프록시 사용자 이름** 텍스트 상자에서 프록시 사용자 이름을 입력합니다.
   b. **프록시 암호** 텍스트 상자에서 프록시 암호를 입력합니다.
   c. **암호 확인** 텍스트 상자에서 방금 입력한 프록시 암호를 다시 입력합니다.
6. **프록시**에서 **프록시 사용** 확인란을 선택합니다.
7. 이러한 옵션을 저장하려면 **저장**을 클릭합니다.

웹 기반 데이터 검색에 HTTP 프록시 사용

웹 기반 데이터 검색에 HTTP 프록시를 사용하려면 다음을 수행합니다.

1. **Dell Management Center**에서 **설정** → **프록시**를 선택하고 **편집**을 클릭합니다.
2. **프록시 사용** 확인란을 선택합니다.
3. **Apply(적용)**를 클릭합니다.
4. 설정의 유효성을 검사하려면 **테스트 연결**을 클릭합니다.

인벤토리 작업 실행

인벤토리 작업을 실행하려면 다음을 수행합니다.

1. **Configuration Wizard(구성 마법사)**가 완료되면 **Job Queue(작업 큐)** → **Inventory(인벤토리)** → **Run Now(지금 실행)**를 클릭하여 인벤토리 작업을 즉시 실행합니다.
2. 인벤토리 작업 상태를 확인하려면 **Refresh(새로 고침)**를 클릭합니다.
3. **Host and Cluster(호스트 및 클러스터)** 보기로 이동하여 **Dell host(Dell 호스트)**를 클릭한 다음 **OpenManage Integration** 탭을 클릭합니다. 그러면 다음과 같은 정보가 제공됩니다.

   - 개요 페이지
   - 시스템 이벤트 로그
   - 하드웨어 인벤토리
   - 보관 시
   - 펌웨어
   - 전원 모니터링
   - Warranty Status(보증 상태)

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

   다음 호스트 명령은 OpenManage Integration 탭 안에서 작동합니다.

   - 깜빡이는 표시등
   - 펌웨어 업데이트 마법사 실행
   - 원격 액세스 실행
   - OMSA 실행
   - CMC 실행

보증 검색 작업 실행

또한 보증 검색 작업 구성은 마법사와 **Dell Management Center → 설정** 옵션 간에 유사합니다. 마법사를 실행한 후 **Dell Management Center → 설정 → 보증 일정** 페이지에서 언제든지 편집할 수 있습니다. 현재 **작업 대기열 → 보증 내역** 페이지에서 보증 검색 작업을 실행할 수 있습니다.

보증 검색 작업을 예약하려면 다음을 수행합니다.

1. **Dell Management Center**에서 **Settings(설정) → Warranty Schedule(보증 일정)**을 선택합니다.
2. **보증 스케줄** 창에서 **편집**을 클릭합니다.
3. 스케줄을 구성하려면 다음 중 하나를 수행합니다.
   a. 보증 스케줄을 실행하려면 **선택한 요일**을 클릭합니다.
   b. 보증 스케줄을 실행하지 않으려면 **Dell 호스트에서 인벤토리를 실행하지 않음**을 선택합니다.
4. **선택한 요일**을 선택한 경우 다음을 수행합니다.
   a. 보증 작업을 실행할 각 요일 옆에 있는 확인란을 선택합니다.
   b. 텍스트 상자에 HH:MM 형식으로 시간을 입력합니다.
   입력하는 시간은 로컬 시간입니다. 적절한 시간에 보증 작업을 실행해야 하는 시간 차이를 계산하십시오.
5. 보증 작업을 지금 실행하려면 **작업 큐 → 보증 내역**으로 이동하여 **지금 실행**을 클릭합니다.

배포 자격 증명 보기 또는 편집

Dell 관리 센터에서 배포 자격 증명을 편집할 수 있습니다. 배포 자격 증명은 초기 검색부터 배포 프로세스가 끝날 때까지 iDRAC를 사용하여 운영 체제 미설치 시스템과 안전하게 통신하는 데 사용됩니다. 배포가 완료되면 자격 증명은 배포 마법사에서 운영 체제 미설치 시스템에 일치하는 연결 프로필에 있는 자격 증명으로 변경됩니다. 배포 자격 증명이 변경되면 해당 시점부터 새로 검색된 모든 시스템이 새 자격 증명으로 프로비저닝됩니다. 자격 증명이 변경되기 전에 검색된 서버의 자격 증명은 영향을 받지 않습니다. 사용자 이름은 16자 이하여야 하며(ASCII 표시 가능한 문자만), 암호는 20자 이하여야 합니다(ASCII 표시 가능한 문자만).
배포 자격 증명을 보거나 편집하려면 다음을 수행합니다.

1. **Dell Management Center → Settings(설정) → Deployment Credentials(배포 자격 증명)**에서 **Edit(편집)**를 클릭합니다.
2. **Credentials for Bare Metal Server Deployment(운영 체제 미설치 서버 배포용 자격 증명)**의 **Credentials(자격 증명)**에서 다음을 수행합니다.
   - **사용자 이름** 텍스트 상자에서 사용자 이름을 입력합니다.
     사용자 이름은 16자 이하여야 합니다(ASCII 표시 가능한 문자만).
   - **암호** 텍스트 상자에서 암호를 입력합니다.
     암호는 20자 이하여야 합니다(ASCII 표시 가능한 문자만).
   - **Verify Password(암호 확인)** 텍스트 상자에서 암호를 다시 입력합니다.
     두 암호는 일치해야 합니다.
3. **Apply(적용)**를 클릭합니다.

펌웨어 리포지토리 설정

펌웨어 리포지토리 및 자격 증명을 설정하려면 다음을 수행합니다.

1. **OpenManage Integration for VMware vCenter**에서, **Settings(설정) → Firmware Repository(펌웨어 리포지토리)**를 선택하고 **Edit(편집)**을 클릭합니다.
2. **Firmware Repository(펌웨어 리포지토리)** 페이지에서 펌웨어 업데이트에 사용되는 기본 리포지토리를 선택하려면 다음 중 하나를 선택합니다.

- **Dell 온라인**
  필수 스테이징 폴더와 함께 Dell 온라인(ftp.dell.com)의 기본 펌웨어 업데이트 리포지토리를 사용합니다. OpenManage Integration for VMware vCenter는 선택한 펌웨어 업데이트를 다운로드하여 스테이징 폴더에 저장합니다. 그러면 필요에 따라 이 업데이트가 적용됩니다.
- **공유 네트워크 폴더**
  Lifecycle Controller를 사용하는 호스트는 접속 가능한 네트워크 공유 폴더에 있는 사용자 정의 리포지토리에서 업데이트할 수 있습니다. 사용자 리포지토리를 만들려면, Dell은 Dell Repository Manager를 사용하고 호스트와 OpenManage Integration이 액세스할 수 있는 공유 위치에 저장할 것을 권장합니다. 리포지토리 카탈로그 파일의 위치를 아래에 입력하십시오.

3. **Shared Network Folder (공유 네트워크 폴더)**를 선택했을 경우, **Catalog File Location(카탈로그 파일 위치)** 필드에 전체 카탈로그 파일을 입력하십시오.
4. **Begin Test(테스트 시작)**를 클릭합니다.
5. **Apply(적용)**를 클릭합니다.

배포를 위한 서버 보안 설정

화이트 리스트를 사용하여 배포 가능한 서버 수를 제한합니다. 서버가 화이트 리스트에 있는 경우 자동 검색 및 핸드셰이크 프로세스 중에 자격 증명과 함께 제공되며 배포에 사용되는 서버의 목록에 표시됩니다. 화이트 리스트는 서버 서비스 태그 추가, 서비스 태그 삭제 또는 CSV 파일에서 서비스 태그 목록 가져오기 작업을 수동으로 수행함으로써 유지관리됩니다.

노트: CSV 구분 파일을 사용하여 서버를 가져옵니다. 각 행마다 여러 개의 레코드가 있으며 각 레코드에는 쉼표로 구분된 하나 이상의 서비스 태그가 있습니다.

화이트 리스트를 설정하고 관리하려면 다음에서 선택합니다.

- 서버 화이트 리스트 사용
- 화이트 리스트에 서버 추가
- 화이트 리스트에서 서버 삭제

배포 가능한 서버 화이트 리스트 사용

배포 가능한 서버의 보안 설정에 대한 내용은 배포를 위한 서버 보안 설정을 참조하십시오.

서버 화이트 리스트를 사용으로 설정하려면 다음을 수행합니다.

1. **Dell Management Center**의 왼쪽 창에서 **설정**을 선택합니다.
2. 오른쪽 창에서 **보안**을 선택합니다.
3. **보안** 창에서 **편집**을 클릭합니다.
4. 화이트 리스트를 사용하여 서버 배포를 제한하려면 **서버 화이트 리스트 적용** 확인란을 선택합니다.
5. **적용**을 클릭하면 서버 화이트 리스트가 ENABLED(사용)로 변경됩니다.

화이트 리스트에 배포 가능한 서버 추가

배포 가능한 서버의 보안 설정에 대한 내용은 배포를 위한 서버 보안 설정을 참조하십시오. 이 설정이 적용되는 경우 서버 화이트 리스트에 있는 Dell 서버만 OpenManage Integration for VMware vCenter를 사용하여 배포할 수 있습니다. 배포 가능한 서버를 화이트 목록에 수동으로 추가하거나 목록을 사용하여 가져올 수 있습니다.

배포 가능한 서버를 화이트 목록에 추가하려면 다음을 수행합니다.

1. **Dell Management Center**의 왼쪽 창에서 **설정** → **보안**을 선택합니다.
2. **서버 화이트 리스트** 창에서 **편집**을 클릭하고 다음 중 하나를 수행합니다.
   - 화이트 리스트에 서버를 수동으로 추가하려면 **서버 추가**를 클릭합니다.

- **서비스 태그 추가** 대화상자에서 서비스 태그를 입력합니다.
- 태그를 추가하려면 **계속**을 클릭합니다.

• 서비스 태그 목록을 가져오려면 **화이트 리스트 가져오기**를 클릭합니다.

- **업로드할 파일 선택** 대화상자가 표시되면 CSV 파일을 탐색하고 **열기**를 클릭합니다.
  화이트 리스트의 예는 다음과 같습니다.

  ASDFG12

  SDCNRD0

  TESCVD3

  AS243AS, ASWERF3, FGVCSD9

- **파일에서 해당 서비스 태그를 찾았음**이라는 대화상자가 표시되면 **적용**을 클릭합니다.

그러면 서비스 태그가 서비스 태그 목록에 표시됩니다.

화이트 리스트에서 배포 가능한 서버 삭제

배포 가능한 서버의 보안 설정에 대한 내용은 배포를 위한 서버 보안 설정을 참조하십시오.

화이트 리스트에서 배포 가능한 서버를 삭제하려면 다음을 수행합니다.

1. **Dell Management Center**의 왼쪽 창에서 **설정**을 선택합니다.
2. 오른쪽 창에서 **보안**을 선택합니다.
3. **보안** 창에서 **편집**을 클릭합니다.
4. 다음 중 하나를 수행합니다.
   - 개별 서버를 삭제하려면 **서비스 태그** 확인란을 클릭하고 **선택 항목 삭제**를 클릭합니다.
   - 모든 서버를 삭제하려면 **서비스 태그** 확인란을 클릭하고 **선택 항목 삭제**를 클릭합니다.
5. **선택한 서비스 태그를 삭제하시겠습니까?** 대화상자가 표시되면 **적용**을 클릭하여 적용하거나 **취소**를 클릭하여 취소합니다.
6. 변경사항을 완료하려면 **적용**을 클릭합니다.

호스트, 운영 체제 미설치 및 iDRAC 준수 문제 정보

OpenManage Integration for VMware vCenter을 사용하여 호스트, 운영 체제 미설치 서버 및 iDRAC를 관리하려면 각각 특정 최소 조건을 충족해야 합니다. 이 조건을 준수하지 않으면 OpenManage Integration for VMware vCenter에서 올바르게 관리되지 않습니다. 비준수 호스트, 운영 체제 미설치 서버 및 iDRAC 준수 해결 링크를 사용하여 사용자 구성에서 준수되지 않는 호스트/운영 체제 미설치 서버/iDRAC를 확인하고 해결하십시오. 이 마법사는 다음과 같은 호스트/운영 체제 미설치 서버/iDRAC를 표시합니다.

- 호스트가 연결 프로필에 할당되지 않았습니다.
  연결 프로필이 호스트에 할당되지 않은 경우 연결 프로필 화면으로 이동할 수 있는 대화상자가 표시됩니다. 이 구성은 마법사 외부에 있습니다. 나중에 되돌아 와서 이 마법사를 실행합니다.
- CSIOR(Collect System Inventory on Reboot)이 사용되지 않도록 설정되어 있거나 실행되지 않았습니다. 이 경우 수동으로 다시 부팅해야 합니다.
- OMSA 에이전트(호스트 루트 자격 증명)이 설치되지 않았거나, 오래되었거나, 올바르게 구성되지 않았습니다.
- 운영 체제 미설치 서버에 있는 iDRAC(Integrated Dell Remote Access Controller) 펌웨어, LC(Lifecycle Controller) 펌웨어 또는 BIOS 버전이 오래되었습니다.

주의: 잠금 모드의 호스트는 비준수 호스트인 경우에도 준수 확인에 나타나지 않습니다. 해당 준수 상태를 파악할 수 없기 때문에 표시되지 않습니다. 이러한 시스템의 준수 여부는 수동으로 확인해야 합니다. 이 경우 경고가 표시됩니다.

각각의 경우, 다음 중 하나를 실행하여 준수 문제를 해결해야 합니다.

- vSphere 호스트 준수 문제를 해결하려면 비준수 vSphere 호스트 해결 마법사 실행을 참조하십시오.
- 준수 문제가 있는 운영 체제 미설치 서버를 해결하려면 비준수 운영 체제 미설치 서버 해결 마법사 실행을 참조하십시오.
- iDRAC 준수 문제를 해결하려면 iDRAC 라이센스 준수를 참조하십시오.

관련 정보:

- 운영 체제 미설치 서버 준수 재확인
- 수동 펌웨어 업데이트에 사용할 ISO 다운로드

비준수 vSphere 호스트 해결 마법사 실행

비준수 vSphere 호스트 해결 마법사를 실행하여 비준수 호스트를 해결합니다. 준수에 대한 자세한 내용은 호스트 및 운영 체제 미설치 준수 문제 정보를 참조하십시오. 몇몇 비준수 ESXi 호스트의 경우 다시 부팅해야 합니다. OMSA(OpenManage Server Administrator)를 설치하거나 업데이트해야 할 경우 ESXi 호스트를 다시 부팅해야 합니다. CSIOR을 실행하지 않은 모든 호스트에서도 다시 부팅이 필요합니다. ESXi 호스트가 자동으로 다시 부팅되도록 선택하는 경우 다음과 같은 조치가 수행됩니다.

- CSIOR 상태 해결:
  호스트에서 CSIOR이 활성화되어 있지 않은 경우, CSIOR이 *ON(켜짐)*으로 설정되고 호스트가 유지 보수 모드로 설정되어 재부팅됩니다.
- OMSA 상태 해결:
  a. OMSA가 호스트에 설치됩니다.
  b. 호스트가 유지 보수 모드로 설정된 다음 다시 부팅됩니다.
  c. 다시 부팅이 완료된 후 변경사항이 적용되도록 OMSA가 구성됩니다.
  d. 호스트의 유지 보수 모드가 종료됩니다.
  e. 인벤토리가 실행되어 데이터가 새로 고쳐집니다.

비준수 vSphere 호스트 해결 마법사를 실행하려면 다음을 수행합니다.

1. **Dell Management Center**의 왼쪽 창에서 **준수 → vSphere 호스트**를 클릭합니다.
2. **vSphere 호스트 준수** 창에서 비준수 호스트를 확인하고 **비준수 vSphere 호스트 해결**을 클릭합니다.
3. **비준수 vSphere 호스트 해결** 마법사에서 해결할 호스트의 확인란을 선택합니다.
4. **Next(다음)**를 클릭합니다.
5. 연결 프로필이 없는 서버가 있을 경우 마법사를 종료하고 **연결 프로필** 페이지에서 이러한 시스템을 해결하거나 마법사를 계속 진행할 수 있는 옵션이 제공됩니다. 새 연결 프로필 생성을 참조하십시오. 작업을 마치면 이 마법사로 돌아옵니다.
6. **CSIOR 켜짐** 창에서 선택한 호스트에 대해 **CSIOR**을 사용하려면 확인란을 선택합니다.
7. **Next(다음)**를 클릭합니다.
8. **OMSA 해결** 창에서 선택한 호스트에 대해 **OMSA**를 해결하려면 확인란을 선택합니다.
9. **Next(다음)**를 클릭합니다.
10. **호스트 다시 부팅** 창에서, 다시 부팅해야 하는 ESXi 호스트를 확인합니다. OMSA를 설치하거나 업데이트해야 할 경우 ESXi 호스트를 다시 부팅해야 합니다. CSIOR을 실행하지 않은 모든 호스트에서도 다시 부팅이 필요합니다. 다음 중 하나를 수행합니다.
    - 호스트를 유지 보수 모드로 자동 전환하고 필요할 때마다 다시 부팅하려면 **호스트를 유지 보수 모드로 자동 전환하고 필요할 때마다 다시 부팅** 확인란을 선택합니다.
    - 수동으로 다시 부팅하려면 다음을 수행해야 합니다.

1. 호스트에 대한 *OMSA 설치* 작업이 완료되면 호스트를 다시 부팅합니다.
2. 호스트가 시동된 후 OMSA가 구성되어 있지 않으면 OMSA를 수동으로 구성하거나 준수 마법사를 사용하십시오.
3. 인벤토리를 다시 실행합니다. 인벤토리 작업 실행을 참조하십시오.

11. **Next(다음)**를 클릭합니다.
12. **요약** 창에서 비준수 호스트에 수행되는 조치를 검토합니다. 변경사항을 적용하려면 수동으로 다시 부팅해야 합니다.
13. **Finish(마침)**을 클릭합니다.

비준수 운영 체제 미설치 서버 해결 마법사

비준수 운영 체제 미설치 서버 해결 마법사를 실행하여 비준수 운영 체제 미설치 서버를 해결합니다. 준수에 대한 자세한 내용은 호스트 및 운영 체제 미설치 준수 문제 정보를 참조하십시오.

비준수 운영 체제 미설치 서버 해결 마법사를 실행하려면 다음을 수행합니다.

1. **Dell Management Center**의 왼쪽 창에서 **준수 → 운영 체제 미설치 서버**를 클릭합니다.
2. **운영 체제 미설치 서버** 창에서 비준수 호스트를 확인하고 **비준수 운영 체제 미설치 서버 해결**을 클릭합니다.
3. **운영 체제 미설치 서버 해결** 마법사에서 해결할 호스트의 확인란을 선택합니다.
4. **Next(다음)**를 클릭합니다.
5. **요약** 창에서 비준수 운영 체제 미설치 서버에 수행되는 작업을 검토합니다.
6. **Finish(마침)**을 클릭합니다.

운영 체제 미설치 서버 준수 재확인

OpenManage Integration for VMware vCenter 외부에서 해결한 서버의 경우 서버 준수를 수동으로 재확인해야 합니다. Dell Management Center, Compliance(준수), Bare Metal Servers(운영 체제 미설치 서버) 페이지에서 이 작업을 수행할 수 있습니다.

운영 체제 미설치 서버 준수를 재확인하려면 다음을 수행합니다.

1. **Dell Management Center → Compliance(준수) → Bare Metal Servers(운영 체제 미설치 서버)**페이지에서 **Re-check Compliance(준수 재확인)**를 클릭합니다.
2. **비준수 서버** 창에서 목록을 새로 고치려면 **새로 고침**을 클릭합니다.
3. 재확인을 실행하려면 **준수 확인**을 클릭합니다.
4. 재확인을 중단하려면 **모든 테스트 중단**을 클릭합니다.
5. 시스템을 성공적으로 해결하면 목록이 새로 고쳐지고 목록에서 해당 시스템이 제거됩니다. 그렇지 않을 경우 비준수 시스템이 목록에 남아 있습니다.
6. 작업을 마치면 **완료**를 클릭합니다.

수동 펌웨어 업데이트에 사용할 ISO 다운로드

OpenManage Integration for VMware vCenter는 대부분의 준수 문제를 자동으로 해결합니다. 경우에 따라 ISO를 수동으로 설치해야 합니다. 필요한 ISO를 다운로드하여 다음 단계에 따라 수동으로 준수 문제를 해결할 수 있습니다.

1. **Dell Management Center → 준수 → 운영 체제 미설치 서버** 페이지에서 ISO를 다운로드하려면 **ISO 다운로드**를 클릭합니다.
2. **ISO 다운로드** 대화상자에서 ISO 위치를 찾으려면 **다운로드**를 클릭합니다.

   노트: 이 응용프로그램 창 뒤에 외부 브라우저가 열릴 수 있습니다.
3. 운영 체제 미설치 서버가 준수하도록 할 ISO 파일로 이동합니다.
4. ISO를 굽고 ISO를 통해 호스트를 부팅한 후 FW 구성요소를 필요한 레벨로 업데이트합니다.

iDRAC 라이센스 준수

iDRAC 라이센스 준수 페이지를 선택하면 준수 테스트가 실행됩니다. 이 테스트는 몇 분 정도 소요됩니다. 이 페이지에 나열된 vSphere 호스트 및 운영 체제 미설치 서버에는 호환되는 iDRAC 라이센스가 없기 때문에 비준수로 간주됩니다. 표에 iDRAC 라이센스 상태가 표시됩니다. 이 페이지에서 라이센스에 남은 일 수를 확인하고 필요에 따라 업데이트합니다. *인벤토리 작업 실행* 링크가 비활성화된 경우 iDRAC 라이센스로 인한 비준수 vSphere 호스트가 없음을 의미합니다. *운영 체제 미설치 서버 준수 재확인* 링크가 비활성화된 경우 iDRAC 라이센스로 인한 비준수 운영 체제 미설치 서버가 없음을 의미합니다.

1. **Dell Management Center** 왼쪽 창에서 **준수**를 클릭합니다.
2. **준수**를 펼치고 **iDRAC 라이센스**를 클릭합니다.
   이 페이지로 이동하면 준수 테스트가 실행됩니다. 이 테스트는 **새로 고침**을 클릭할 때 실행되는 테스트와 동일합니다.
3. 라이센스가 오래된 경우 **iDRAC 라이센스 구입/갱신**을 클릭합니다.
4. **Dell 라이센스 관리** 페이지에 로그인하여 업데이트하거나 새 iDRAC 라이센스를 구입합니다.
   이 페이지에 있는 정보를 사용하여 iDRAC를 식별하고 업데이트합니다.
5. iDRAC 라이센스를 설치한 후 vSphere 호스트에 대해 인벤토리 작업을 실행하고 인벤토리 작업을 완료한 후 이 페이지로 돌아옵니다. 운영 체제 미설치 서버의 경우, 사용 허가된 운영 체제 미설치 서버의 준수를 재확인합니다.

OpenManage Integration for VMware vCenter 업그레이드

다음은 OpenManage Integration for VMware vCenter에 대한 업그레이드 시나리오입니다.

- 평가판에서 전체 제품 버전으로 업그레이드

노트: 업그레이드를 시작하기 전에 어플라이언스 백업을 수행합니다. 즉시 백업 수행을 참조하십시오.

평가판에서 전체 제품 버전으로 업그레이드

평가판에서 전체 제품 버전으로 업그레이드하려면 다음을 수행합니다.

1. **Dell 웹 사이트**로 이동하여 전체 제품 버전을 구입합니다.
   라이센싱 창의 관리 포털에 있는 링크와 같이 **지금 구입** 링크 중 하나를 사용하여 OpenManage Integration for VMware vCenter에서 Dell 웹 사이트에 액세스할 수도 있습니다. 이는 평가판 라이센스를 사용하는 경우에만 적용됩니다.
2. 다운로드에는 새로운 전체 버전 제품과 새 라이센스 파일이 포함되어 있습니다.
3. 브라우저 창을 실행하고 구성할 가상 시스템에 대해 **vSphere vCenter 콘솔** 탭에 표시된 **관리 콘솔 URL**을 입력하거나 **Dell Management Console → 설정** 페이지에서 링크를 사용합니다. URL 형식은 **https://<ApplianceIPAddress>**이며 대소문자를 구분하지 않습니다.
4. **Administration Console 로그인 창**에서 암호를 입력하고 **로그인**을 클릭합니다.
5. 라이센스 파일을 업로드하려면 **업로드**를 클릭합니다.
6. **라이센스 업로드** 창에서 **찾아보기**를 클릭하여 라이센스 파일을 탐색합니다.
7. 라이센스 파일을 선택하고 **Upload(업로드)**를 클릭합니다.

OpenManage Integration for VMware vCenter 정보

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

평가 라이센스 평가 버전에는 OpenManage Integration for VMware vCenter에서 관리되는 호스트(서버) 5개에 대한 평가 라이센스가 포함되어 있습니다. 이는 11세대 이상에만 해당됩니다. 이 라이센스는 기본 라이센스이며 90일 평가 기간 동안에만 사용할 수 있습니다.

표준 라이센스 전체 제품 버전에는 vCenter 10개에 대한 표준 라이센스가 포함되어 있으며 OpenManage Integration for VMware vCenter에서 관리되는 호스트 연결을 원하는 수 만큼 구입할 수 있습니다.

평가 라이센스에서 전체 표준 라이센스로 업그레이드하면 새 라이센스 XML 파일 및 업로드될 라이센스 파일을 포함한 Zip 파일이 이메일로 사용자에게 전송됩니다. 로컬 시스템에 파일을 저장하고 Administration Console을 사용해 새 라이센스 파일을 업로드합니다. 라이센싱은 다음과 같은 정보를 제공합니다.

- 최대 vCenter 연결 라이센스 수 - 등록되어 사용 중인 vCenter 연결은 최대 3개 허용됩니다.
- 최대 호스트 연결 라이센스 수 - 구입한 호스트 연결 수입니다.
- 사용 중 - 사용 중인 vCenter 연결 또는 호스트 연결 라이센스 수입니다. 호스트 연결에서 이 숫자는 검색되어 인벤토리 작성된 호스트(또는 서버) 수를 나타냅니다.
- 사용 가능 - 나중에 사용할 수 있는 vCenter 연결 또는 호스트 연결 라이센스 수입니다.
- 사용 허가되지 않은 호스트 - 사용이 허가된 양을 초과하는 호스트 연결 수입니다. OpenManage Integration for VMware vCenter은 정상적으로 계속 작동하지만 새 라이센스를 구입하여 설치해야 이 경고가 해결됩니다.

4

엔드-투-엔드 하드웨어 관리

엔드-투-엔드 하드웨어 관리의 목표는 관리자가 Dell Management Center 또는 vCenter를 종료하지 않고도 위험 수준의 하드웨어 이벤트를 처리하는 데 필요한 최신 인프라 정보와 시스템 상태를 제공하는 것입니다. OpenManage Integration for VMware vCenter 내에서 엔드-투-엔드 하드웨어 관리는 다음 4개 부분으로 나뉩니다.

- 모니터링
- 인벤토리
- 고급 호스트 관리
- 보증 검색

데이터센터 및 호스트 시스템 모니터링

데이터센터 및 호스트 시스템 모니터링은 하드웨어(서버 및 스토리지) 및 가상화 관련 이벤트를 vCenter의 작업 및 이벤트 탭에 표시해 관리자가 인프라 상태를 모니터할 수 있도록 합니다. 또한 중요한 하드웨어 경고는 OpenManage Integration for VMware vCenter에서 경보를 유발할 수 있습니다. Dell 가상화 관련 이벤트의 소수의 경보는 관리 호스트 시스템의 유지 관리 모드로 이동할 수 있습니다.

모니터링하려면 다음을 수행합니다.

1. **이벤트 및 알람** 설정을 구성합니다.
2. 필요한 경우 **SNMP OMSA 트랩 대상**을 구성합니다.
3. 이벤트 정보를 검토하려면 vCenter의 **작업 및 이벤트** 탭을 사용합니다.

이벤트 및 알람 이해

OpenManage Integration for VMware vCenter의**Manage(관리) → Settings(설정)**탭에서 이벤트 및 알람을 편집할 수 있습니다. 여기에서 이벤트 게시 수준을 선택하거나, Dell 호스트의 알람을 활성화하거나, 기본 알람을 복원할 수 있습니다. 각 vCenter에 대해 이벤트 및 알람을 구성하거나 등록된 모든 vCenter에 대해 한 번에 구성할 수 있습니다.

이벤트 게시 수준에는 4가지가 있습니다.

표 1. 이벤트 게시 수준 설명

이벤트	설명
Do not post any Events(이벤트 게시하지 않음)	OpenManage Integration for VMware vCenter이 관련 vCenter에 이벤트나 경고를 전달하지 않습니다.
Post all Events(모든 이벤트 게시)	OpenManage Integration for VMware vCenter이 관리되는 Dell 호스트에서 관련 vCenter로 수신하는 비공식 이벤트를 포함하여 모든 이벤트를 게시합니다.
Post only Critical and Warning Events(위험 및 경고 이벤트만 게시)	위험 또는 경고 수준의 이벤트만 관련 vCenter에 게시합니다.

Post only Virtualization-Related Critical and Warning Events(가상화 관련 위험 및 경고 이벤트만 게시)	호스트에서 수신한 가상화 관련 이벤트를 관련 vCenter에 게시합니다. 가상화 관련 이벤트는 가상 시스템을 실행 중인 호스트에 가장 위험한 수준으로 분류된 이벤트입니다.

이벤트 및 알람을 구성할 때 이들을 활성화할 수 있습니다. 활성화할 경우 위험 수준의 하드웨어 알람을 통해 OpenManage Integration for VMware vCenter이 호스트 시스템을 유지 보수 모드로 전환할 수 있으며 가상 시스템을 다른 호스트 시스템으로 마이그레이션하는 경우도 있습니다. OpenManage Integration for VMware vCenter이 관리되는 Dell 호스트에서 수신한 이벤트를 전달하고 해당 이벤트용 알람을 생성합니다. 이러한 알람을 사용하여 다시 부팅, 유지 보수 모드 또는 마이그레이션 등과 같은 작업을 vCenter에서 트리거합니다. 예를 들어, 이중 전원 공급 장치에 오류가 발생하여 알람이 생성되면 해당 시스템의 가상 시스템을 새 시스템으로 마이그레이션할 수 있습니다.

사용자의 요청이 있을 경우에만 호스트의 유지 보수 모드를 시작하거나 끝낼 수 있습니다. 유지 보수 모드로 전환될 때 호스트가 클러스터 내에 있을 경우 전원이 꺼진 가상 시스템을 종료할 수 있는 옵션이 제공됩니다. 클러스터에 가상 시스템에 사용할 수 있는 호환 가능한 호스트가 없는 경우를 제외하고, 이 옵션을 선택하면 전원이 꺼진 각 가상 시스템이 다른 호스트로 마이그레이션됩니다. 유지 보수 모드의 호스트에서는 가상 시스템을 배포하거나 *전원을 켤 수* 없습니다. 유지 보수 모드로 전환되는 호스트에서 실행 중인 가상 시스템은 VMware DRS(Distributed Resource Scheduling)를 통해 수동 또는 자동으로 다른 호스트로 마이그레이션하거나 종료해야 합니다.

클러스터 외부에 있거나 VMware DRS(Distributed Resource Scheduling)가 사용되지 않는 클러스터 내부에 있는 모든 호스트에서는 위험 이벤트로 인해 가상 시스템이 종료될 수 있습니다. DRS는 리소스 풀에서의 사용량을 지속적으로 모니터링하고 업무 필요에 따라 가상 시스템 간에 사용 가능한 리소스를 지능적으로 할당합니다. 위험 수준의 하드웨어 이벤트가 있을 경우 가상 시스템이 자동으로 마이그레이션되도록 하려면 Dell 알람과 함께 DRS가 구성된 클러스터를 사용해야 합니다. 화면 메시지 세부사항에 표시되는 목록은 영향을 받을 수 있는 이 vCenter 인스턴스의 모든 클러스터입니다. 이벤트 및 알람을 활성화하기 전에 클러스터에 영향이 있음을 확인하십시오.

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

노트: Dell 이벤트를 수신하려면 이벤트를 활성화해야 합니다.

노트: OpenManage Integration for VMware vCenter은 호스트에서 가상 시스템을 성공적으로 실행하는 데 필요한 가상화 관련 이벤트를 미리 선택합니다. Dell 호스트 알람이 기본으로 표시되며, Dell 알람이 활성화되어 있는 경우 클러스터에서 VMware Distributed Resource Scheduler를 사용하여 위험 이벤트를 보내는 가상 시스템이 자동으로 마이그레이션되도록 합니다.

Dell PowerEdge 11세대 호스트를 위한 OMSA 이해

Dell PowerEdge 12세대 서버 이전의 서버에서는 OMSA를 설치해야 OpenManage Integration for VMware vCenter을 사용할 수 있습니다. OMSA는 배포 중에 Dell PowerEdge 11세대 호스트에 자동으로 설치되며 수동으로 설치할 수도 있습니다.

노트: OpenManage Integration for VMware vCenter을 사용하여 OMSA 에이전트를 배포하면 OMSA VIB를 다운로드하고 설치할 ESXi 5.0 이후의 릴리스에서 httpClient 서비스가 시작되고 포트 8080이 활성화됩니다. OMSA 설치가 완료되면 서비스가 자동으로 중지되고 포트가 닫힙니다.

Dell PowerEdge 11세대 서버에서 OMSA를 구성하려면 다음 중 하나를 선택하십시오.

- ESXi 시스템에 OMSA 에이전트 배포
- ESX 시스템에 OMSA 에이전트 배포
- OMSA 트랩 대상 설정

ESX 시스템에 OMSA 에이전트 배포

ESX 시스템에 OMSA tar.gz을 설치하여 시스템에서 인벤토리 및 경고 정보를 수집합니다.

노트: OpenManage 에이전트는 Dell PowerEdge 12세대 서버 이전의 Dell 호스트에 필요합니다. OpenManage Integration for VMware vCenter을 사용하여 OMSA를 설치하거나 OpenManage Integration for VMware vCenter을 설치하기 전에 호스트에 수동으로 설치하십시오. 에이전트 수동 설치에 대한 자세한 내용은 **http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.openmanage-server-administrator-omsa.aspx** 에서 볼 수 있습니다.

필수 원격 사용 설정(-c) 옵션을 사용하여 ESX 시스템에 OMSA 에이전트 tar.gz을 배포하려면 다음을 수행합니다.

1. OMSA 에이전트 설치 스크립트 실행:
   ```
   srvadmin-install.sh -x -c
   ```
2. OMSA 서비스 시작:
   ```
   srvadmin-services.sh start
   ```
3. OMSA 에이전트가 이미 설치되어 있는 경우 원격 사용 구성 (-c) 옵션이 있는지 확인하십시오. 그렇지 않으면 OpenManage Integration for VMware vCenter 설치가 성공적으로 완료되지 않습니다. -c 옵션을 사용하여 다시 설치하고 서비스를 다시 시작합니다.
   ```
   srvadmin-install.sh -c srvadmin-services.sh restart
   ```

ESXi 시스템에 OMSA 에이전트 배포

ESXi 시스템에 OMSA VIB를 설치하여 시스템에서 인벤토리 및 경고 정보를 수집합니다.

노트: OpenManage 에이전트는 Dell PowerEdge 12세대 서버 이전의 Dell 호스트에 필요합니다. OpenManage Integration for VMware vCenter을 사용하여 OMSA를 설치하거나 OpenManage Integration for VMware vCenter을 설치하기 전에 호스트에 수동으로 설치하십시오. 에이전트 수동 설치에 대한 자세한 내용은 **http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.openmanage-server-administrator-omsa.aspx** 에서 볼 수 있습니다.

1. 아직 설치되어 있지 않은 경우 **http://www.vmware.com**에서 vSphere 명령줄 도구(vSphere CLI)를 설치합니다.
2. 다음 명령을 입력합니다.
   ```
   Vihostupdate.pl -server <IP Address of ESXi host> -i -b OM-SrvAdmin-Dell-Web-6.3.0-2075.VIB-ESX41i_A00.8.zip
   ```

   노트: OMSA를 설치하는 데 몇 분 정도 걸립니다. 이 명령을 완료한 후에는 호스트를 다시 부팅해야 합니다.

OMSA 트랩 대상 설정

모든 11세대 호스트에 OMSA가 구성되어 있어야 합니다.

노트: OMSA는 Dell PowerEdge 12세대 서버 이전의 Dell 서버에서만 필요합니다.

OMSA 트랩 대상을 설정하려면 다음을 수행합니다.

1. **Settings(설정) → General(일반)**에서 OMSA 사용자 인터페이스로 이동되는 링크를 사용하거나 웹 브라우저(**https://<HostIP>:1311/**)에서 OMSA 에이전트를 탐색합니다.
2. 인터페이스에 로그인하고 **Alert Management(경고 관리)** 탭을 선택합니다.
3. **Alert Actions(경고 조치)**를 선택하고 이벤트가 전송되지 않도록 모니터링되는 모든 이벤트에 **Broadcast Message(브로드캐스트 메시지)** 옵션이 설정되어 있는지 확인합니다.
4. 탭 맨 위에서 **Platform Events(플랫폼 이벤트)** 옵션을 선택합니다.
5. 회색 **Configure Destinations(대상 구성)** 단추를 클릭하고 **Destination(대상)** 링크를 클릭합니다.
6. **Enable Destination(대상 활성화)** 확인란을 선택합니다.
7. **대상 IP 주소** 필드에 OpenManage Integration for VMware vCenter 어플라이언스 IP 주소를 입력합니다.
8. **Apply Changes(변경사항 적용)**를 클릭합니다.

9. 1-8단계를 반복하여 추가 이벤트를 구성합니다.

이벤트 보기

이벤트를 보려면 다음 중 하나를 수행합니다.

- 가상 시스템을 탐색하고 마우스 오른쪽 단추를 클릭하여 **vCenter → 작업 및 이벤트** 탭을 표시한 다음 **이벤트**를 클릭하여 선택한 이벤트 수준이 표시되도록 합니다.
- 호스트의 상위 노드(클러스터 또는 데이터센터) 또는 vCenter의 루트 폴더를 클릭합니다.

vSphere 트리에 있는 해당 노드에만 이벤트가 나타납니다.

vSphere 클라이언트 호스트 개요

이 개요는 개별 구성요소 상태, 식별, 하이퍼바이저 및 펌웨어 정보를 비롯하여 주요 호스트 서버 특성에 대한 정보를 제공합니다.

하드웨어 구성요소 상태

구성요소 상태는 모든 주요 호스트 서버 구성요소(시스템 섀시, 전원 공급 장치, 온도, 팬, 전압, 프로세서, 배터리, 침입, 하드웨어 로그, 전원 관리 및 메모리)의 상태를 그래픽으로 나타낸 것입니다. 사용 가능한 상태는 다음과 같습니다.

- 정상(녹색 확인 표시) - 구성요소가 정상적으로 작동하고 있음
- 경고(느낌표가 있는 노란색 삼각형) - 구성요소에 위험하지 않은 오류가 있음
- 위험(빨간색 X) - 구성요소에 위험한 오류가 있음
- 알 수 없음(물음표) - 구성요소의 상태를 알 수 없음

전체적인 상태는 오른쪽 상단 헤더 표시줄에 표시됩니다.

서버 정보

서버 정보는 다음과 같은 식별, 하이퍼바이저 및 펌웨어 정보를 제공합니다.

- 호스트 이름, 전원 상태, iDRAC IP, 관리 IP, 사용 중인 연결 프로필, 모델, 서비스 태그 및 자산 태그 번호, 남은 보증 일 수 및 마지막으로 인벤토리 스캔이 수행된 시기
- 하이퍼바이저, BIOS 펌웨어 및 iDRAC 펌웨어 버전
- 10개의 최근 시스템 이벤트 로그 항목을 제공합니다. 추가적인 로그 세부사항을 표시하는 시스템 이벤트 로그 창을 실행하려면 상세정보를 클릭합니다.

호스트 정보

호스트 개요 왼쪽 창에서 다음과 같은 유형의 호스트 정보에 연결되는 링크를 찾을 수 있습니다.

- 시스템 이벤트 로그
  하드웨어 시스템 이벤트 로그 정보를 표시합니다. 시스템 이벤트 로그 이해를 참조하십시오.
- 하드웨어 인벤토리
  다음과 같은 하드웨어 장치에 대한 정보를 표시합니다.
  - DIMM, 시스템 플레이너, 전원 공급 장치, 뒤판, 컨트롤러 카드 등과 같은 FRU(현장 교체 장치)
  - 메모리 - 사용 가능/사용 중인 슬롯 수, 사용 중인 메모리의 최대 용량 및 양, 개별 DIMM의 상세정보
  - NIC(네트워크 인터페이스 카드) - 설치된 카드 수 및 개별 NIC의 상세정보
  - PCI 슬롯 - 총 사용 가능/사용 중인 개수 및 개별 슬롯의 상세정보
  - 전원 공급 장치 - 개별 PSU의 수 및 상세정보
  - 프로세서 - 개별 CPU의 수 및 상세정보
  - 원격 액세스 카드 - IP 주소 정보, RAC 유형 및 웹 인터페이스 URL

인벤토리 작업 정보를 참조하십시오.

- 보관 시

  호스트 시스템 저장소는 다음을 비롯하여 호스트 기반 저장소 컨트롤러에 연결된 저장소에 사용되는 실제 및 논리적 저장소의 용량과 유형을 그래픽과 자세한 보기로 보여 줍니다.

  - 호스트 시스템 총 저장소, 구성되지 않은 저장소, 구성된 저장소, 전역 및 전용 핫 스페어 디스크 용량
  - 해당 구성요소에 대한 자세한 정보가 포함된 시스템 구성요소 데이터 테이블에 개별 저장소 구성요소가 몇 개 있는지 보여 주는 목록
- 펌웨어

  펌웨어 업데이트 마법사를 실행하거나 펌웨어 버전을 확인합니다. 펌웨어 업데이트를 참조하십시오.
- 전원 모니터링

  호스트 시스템 전원 모니터링은 다음을 비롯하여 일반 전원 정보, 에너지 통계 및 예비 전원 정보를 제공합니다.

  - 현재 전원 할당량, 프로필, 경고 및 오류 임계값
  - 에너지 소모량, 시스템 최고 전원 및 암페어 통계
  - 예비 전원 및 최고 예비 용량

  노트: 일부 전원 공급 장치에서는 이 기능을 지원하지 않으므로 블레이드 엔클로저 전원 공급 장치가 지원되지 않습니다.
- 보증

  보증 검색을 수행하면 다음과 같은 Dell 서버 정보가 제공됩니다.

  - 업데이트된 서비스 보증 정보(호스트 서비스 태그만 전송)
  - 예약된 간격으로 업데이트된 보증 정보
  - 프록시 서버 및 자격 증명을 사용한 안전한 전송
  - 테스트를 거친 안전한 연결을 통한 정보

  보증 검색을 참조하십시오.

Host Actions(호스트 조치)

호스트 조치는 현재 호스트 서버에 수행한 명령입니다. 예를 들면 다음과 같습니다.

- LCD 전면 표시등이 깜빡이도록 하려면 표시등 깜박임을 사용합니다. 물리 서버 전면 표시등 설정을 참조하십시오.
- 펌웨어 업데이트 마법사를 표시하고 호스트 서버 펌웨어를 업데이트하려면 펌웨어 업데이트 마법사 실행을 사용합니다. 펌웨어 업데이트 마법사 실행을 참조하십시오.
- 어플라이언스를 다시 부팅하지 않고 iDRAC 다시 설정을 사용하여 iDRAC를 다시 설정합니다. iDRAC 다시 설정을 참조하십시오.

Management Consoles(관리 콘솔)

관리 콘솔은 외부 시스템 관리 콘솔을 실행하는 데 사용됩니다. 예를 들면 다음과 같습니다.

- iDRAC(Integrated Dell Remote Access Controller) 웹 사용자 인터페이스를 실행하려면 원격 액세스 콘솔을 클릭합니다.
- OMSA(OpenManage Server Administrator) 사용자 인터페이스를 실행하려면(구성된 경우) OMSA 콘솔을 클릭합니다. OMSA 링크 활성화를 참조하십시오.
- CMC(Chassis Management Controller) 웹 사용자 인터페이스를 실행하려면 블레이드 섀시 콘솔을 클릭합니다.

Dell 온라인 서비스

iDRAC 다시 설정

경우에 따라 iDRAC가 요청에 응답하지 않을 수 있으며 이로 인해 OpenManage Integration for VMware vCenter 내에 예기치 않은 동작이 발생합니다. 이 상태에서 복구하는 유일한 방법은 iDRAC를 재설정하는 것입니다. iDRAC를 재설정하면 iDRAC가 정상적으로 재부팅됩니다. 이러한 재부팅이 수행되어도 호스트는 재부팅되지 않습니다. 재설정을 수행한 후 iDRAC가 사용 가능한 상태로 돌아가는 데 1-2분 정도 걸립니다.

iDRAC가 다시 부팅되는 동안에 다음과 같은 상황이 발생할 수 있습니다.

- OpenManage Integration for VMware vCenter가 해당 상태를 가져오는 동안 일부 지연 또는 통신 오류가 발생할 수 있습니다.
- iDRAC와 함께 열려 있는 모든 세션이 닫힙니다.
- iDRAC의 DHCP 주소가 바뀔 수 있습니다. iDRAC가 해당 IP 주소에 대해 DHCP를 사용할 경우 IP 주소가 바뀔 가능성이 있습니다. 이 문제가 발생하면 호스트 인벤토리 작업을 다시 실행하여 인벤토리 데이터에서 새 iDRAC IP를 획득하십시오.

노트: iDRAC 소프트 재설정을 수행해도 iDRAC를 다시 사용 가능한 상태로 되돌리지 못할 수 있습니다. 하드 리셋을 수행해야 할 수 있습니다. 하드 리셋을 수행하려면 서버에서 서버를 끄고 2분 동안 전원 케이블을 분리한 후 다시 연결합니다. iDRAC 재설정에 대한 자세한 내용은 사용 중인 버전의 iDRAC 사용 설명서를 참조하십시오.

노트: Dell에서는 iDRAC를 다시 설정하기 전에 호스트를 유지 보수 모드로 전환할 것을 권장합니다.

1. **vSphere 클라이언트**에서 **인벤토리** 제목 아래에 있는 **호스트 및 클러스터**를 선택합니다.
2. **호스트 및 클러스터**에 있는 트리 보기에서 호스트 시스템을 선택하고 **OpenManage Integration** 탭을 선택합니다.
3. **호스트 작업** 아래에서 **iDRAC 다시 설정**을 선택합니다.
4. iDRAC 다시 설정 대화상자에서 **iDRAC 다시 설정 계속**을 선택하고 **확인**을 클릭합니다.

인벤토리 스케줄 정보

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

- 매주 선택한 요일의 지정된 시간
- 설정된 시간 간격

대부분의 OpenManage Integration for VMware vCenter기능은 필수 데이터를 수집하기 위해 먼저 인벤토리를 완료해야만 사용할 수 있습니다. 이 정보를 표시하려면 모든 호스트 시스템의 인벤토리를 수집해야 합니다. 호스트 시스템에서 인벤토리를 수행하려면 통신 및 인증 정보를 제공하는 연결 프로필을 생성하십시오. 인벤토리가 완료되면 전체 데이터센터 또는 개별 호스트 시스템에 대한 인벤토리 결과를 볼 수 있습니다.

노트: 인벤토리에 최신 정보가 포함되도록 하려면 인벤토리 작업이 최소 일주일에 한 번 실행되도록 예약하십시오. 인벤토리 작업은 최소한의 리소스를 사용하며 호스트 성능을 저하시키지 않습니다.

관련 작업:

- 인벤토리 작업 실행
- 인벤토리 작업 스케줄 수정
- 단일 호스트 시스템의 인벤토리 표시
- 데이터센터 하드웨어 구성 및 상태 표시

인벤토리 작업 스케줄 수정

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

- 매주 선택한 요일의 지정된 시간
- 설정된 시간 간격에 대부분의 OpenManage Integration for VMware vCenter 기능에 필요한 데이터를 수집하려면 완료된 인벤토리가 필요합니다.

노트: 인벤토리에 최신 정보가 포함되도록 하려면 인벤토리 작업을 최소 1주일에 한 번 실행해야 합니다. 인벤토리 작업은 최소한의 리소스를 사용하며 호스트 성능을 저하시키지 않습니다.

인벤토리 작업 스케줄을 수정하려면 다음을 수행합니다.

1. Dell Management Center에서 **설정 → 인벤토리 스케줄**을 선택합니다.
2. 현재 스케줄을 변경하려면 **편집**을 클릭합니다.
3. **선택한 요일** 옵션 단추를 선택하고 해당 요일의 확인란을 선택한 후 시간을 입력합니다. 항목을 지우려면 **지우기**를 클릭합니다.
4. 인벤토리 스케줄을 변경하려면 **적용**을 클릭하고 취소하려면 **취소**를 클릭합니다.
5. 지금 작업을 실행하려면 관리 센터에서 **작업 큐** 및 **인벤토리 내역** 탭을 선택합니다.
6. **지금 실행**을 클릭합니다.
7. **마지막 인벤토리 작업 상세정보**를 업데이트하려면 **새로 고침**을 클릭합니다.

vCenter에서 단일 호스트 시스템의 인벤토리 표시

단일 호스트 시스템의 인벤토리를 표시하려면 다음을 수행합니다.

1. **vSphere client(vSphere 클라이언트)**에서 **Inventory(인벤토리)** 제목 아래에 있는 **Hosts and Clusters(호스트 및 클러스터)**를 선택합니다.
2. 왼쪽 창의 **Hosts and Clusters(호스트 및 클러스터)**에서 호스트 시스템을 선택하고 **OpenManage Integration** 탭을 선택합니다.
3. 선택한 호스트의 개요가 표시됩니다.

   이 개요는 개별 구성요소 상태, 식별, 하이퍼바이저 및 펌웨어 정보를 비롯하여 주요 호스트 서버 특성에 대한 정보를 제공합니다.

   - 하드웨어 구성요소 상태는 모든 주요 호스트 서버 구성요소(시스템 섀시, 전원 공급 장치, 온도, 팬, 전압, 프로세서, 배터리, 침입, 하드웨어 로그, 전원 관리 및 메모리)의 상태를 그래픽으로 나타낸 것입니다. 사용 가능한 상태는 다음과 같습니다.
     - 정상(녹색 확인 표시) - 구성요소가 정상적으로 작동하고 있음
     - 경고(느낌표가 있는 노란색 삼각형) - 구성요소에 위험하지 않은 오류가 있음
     - 위험(빨간색 X) - 구성요소에 위험한 오류가 있음
     - 알 수 없음(물음표) - 구성요소의 상태를 알 수 없음

     전체적인 상태는 오른쪽 상단 헤더 표시줄에 표시됩니다.
   - 서버 정보는 다음과 같은 식별, 하이퍼바이저 및 펌웨어 정보를 제공합니다.
     - 호스트 이름, 전원 상태, iDRAC IP 주소, 관리 IP 주소, 사용 중인 연결 프로필, 모델, 서비스 태그 및 자산 태그 번호, 남은 보증 일 수 및 마지막으로 인벤토리 스캔이 수행된 시기
     - 하이퍼바이저, BIOS 펌웨어 및 iDRAC 펌웨어 버전
     - FRM(Fault Resilient Memory): BIOS 특성으로, 서버의 초기 설치 중에 BIOS에서 활성화되고 서버의 메모리 작동 모드를 표시합니다. 메모리 작동 모드 값을 변경할 경우 시스템을 다시 시작해야 합니다.

이것은 ESXi 5.5 이후 버전을 포함한 R620, R720, T620, M620 및 13세대 서버에 해당됩니다. 4가지 값은 다음과 같습니다.

* 활성화되고 보호됨: 이 값은 시스템이 지원되고 운영 체제 버전이 ESXi 5.5 이상이며 BIOS의 메모리 작동 모드가 FRM으로 설정되어 있음을 나타냅니다.

* 활성화됨 및 보호되지 않음: 이 값은 BIOS의 메모리 작동 모드가 FRM으로 설정되어 있지만 운영 체제에서 이 기능을 지원하지 않음을 나타냅니다.

* Disabled(비활성화됨): 이 값은 아무 운영 체제 버전으로나 유효한 시스템을 지원함을 나타내며, 여기서 BIOS의 메모리 작동 모드는 FRM으로 설정되지 않습니다.

* Blank(비어 있음): BIOS의 메모리 작동 모드가 지원되지 않으면 FRM 특성이 표시되지 않습니다.

- 최근 시스템 로그 항목은 10개의 최근 시스템 이벤트 로그 항목을 제공합니다. 추가적인 로그 세부사항을 표시하는 **시스템 이벤트 로그** 창을 실행하려면 **상세정보**를 클릭합니다.

4. **Host Information(호스트 정보)** 아래에서 **Hardware Inventory(하드웨어 인벤토리)**를 클릭하여 다음을 비롯한 호스트 시스템에 설치된 모든 구성요소에 대한 목록 및 자세한 내용을 표시합니다.

   - FRU(현장 교체 장치) - DIMMS, 시스템 플레이너, 전원 공급 장치, 뒤판, 컨트롤러 카드 등
   - 메모리 - 사용 가능/사용 중인 슬롯 수, 사용 중인 메모리의 최대 용량 및 양, 개별 DIMM의 상세정보
   - NIC(네트워크 인터페이스 카드) - 설치된 카드 수 및 개별 NIC의 상세정보
   - PCI 슬롯 - 총 사용 가능/사용 중인 개수 및 개별 슬롯의 세부사항
   - 전원 공급 장치 - 개별 PSU의 수 및 상세정보
   - 프로세서 - 개별 CPU의 수 및 상세정보
   - 원격 액세스 카드 - IP 주소 정보, RAC 유형 및 웹 인터페이스 URL

5. **Host Information(호스트 정보)** 아래에서 **Storage(저장소)**를 클릭하여 다음을 비롯한 실제 저장소와 가상 저장소의 용량 및 유형의 그래픽과 자세한 보기를 표시합니다.

   - 호스트 시스템 총 저장소, 구성되지 않은 저장소, 구성된 저장소, 전역 핫 스페어 디스크 용량
   - 시스템에 있는 각 저장소 구성요소 개수 목록
   - 해당 구성요소에 대한 자세한 정보가 있는 구성요소 데이터 테이블

6. **Host Information(호스트 정보)** 아래에서 **Firmware(펌웨어)**를 클릭하여 다음을 비롯한 모든 Dell Lifecycle Controller 펌웨어 정보를 표시합니다.

   - 업데이트 이름 - BIOS, Dell Lifecycle Controller, 전원 공급 장치 등
   - 업데이트 유형 - BIOS, 펌웨어 또는 응용프로그램
   - 개별 업데이트 세부사항 - 버전, 설치 시간, 업데이트가 진행 중인지 여부 또는 업데이트 상태, 업데이트 버전. 업데이트 상태 및 버전에는 업데이트가 예약된 경우에만 데이터가 있으며 업데이트 버전은 시스템이 업데이트되는 펌웨어 버전입니다.

7. **Host Information(호스트 정보)** 아래에서 **Power Monitoring(전원 모니터링)**을 클릭하여 다음을 비롯한 일반 전원 정보, 에너지 통계 및 예비 전원 정보를 표시합니다.

   - 현재 전원 할당량, 프로필, 경고 및 오류 임계값
   - 에너지 소모량, 시스템 최고 전원 및 암페어 통계
   - 예비 전원 및 최고 예비 용량

8. **Host Information(호스트 정보)** 아래에서 **Warranty(보증)**를 클릭하여 다음을 비롯한 시스템 보증 정보를 표시합니다.

   - 보증 제공업체 이름 및 보증에 대한 설명
   - 시작 및 종료 날짜와 남은 보증 일 수
   - 보증 상태(활성, 만료) 및 마지막으로 보증 정보가 업데이트된 시기

인벤토리 및 라이센싱

서버 데이터를 검색하거나 표시할 수 없는 몇 가지 원인은 다음과 같습니다.

- 서버가 연결 프로필에 연결되어 있지 않아 인벤토리 작업을 완료할 수 없습니다.
- 데이터를 수집할 서버에서 인벤토리 작업이 실행되지 않아 표시할 사항이 없습니다.
- 호스트 라이센스 수가 초과되었으며 인벤토리 작업을 완료하려면 사용 가능한 추가 라이센스가 있어야 합니다.
- 서버에 12세대 이후 서버에 필요한 올바른 iDRAC 라이센스가 없으므로 올바른 iDRAC 라이센스를 구입해야 합니다.

지금 구입 링크는 처음으로 제품을 구입할 경우에만 사용할 수 있으며 업그레이드를 위해서는 사용할 수 없습니다. 지금 구입 링크는 평가 라이센스를 사용하는 경우에만 표시됩니다.

관련 작업:

- 기존 연결 프로필 보기 및 편집
- 인벤토리 작업 스케줄 수정

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

- 평가 라이센스: 평가 버전에는 OpenManage Integration for VMware vCenter에서 관리되는 호스트(서버) 5개에 대한 데모 라이센스가 포함되어 있습니다.
- 표준 라이센스: 전체 제품 버전에는 vCenter 10개와 OpenManage Integration for VMware vCenter에서 관리되는 구입한 개수의 호스트 연결을 위한 제품 라이센스가 포함되어 있습니다.

관련 작업:

- OpenManage Integration for VMware vCenter 정보
- Administration Console에 OpenManage Integration for VMware vCenter 라이센스 업로드

저장소 인벤토리 보기

호스트 시스템 저장소는 다음을 비롯하여 호스트 기반 저장소 컨트롤러에 연결된 저장소에 사용되는 실제 및 논리적 저장소의 용량과 유형을 그래픽과 자세한 보기로 보여 줍니다.

- 호스트 시스템 총 저장소, 구성되지 않은 저장소, 구성된 저장소, 전역 핫 스페어 디스크 용량
- 시스템에 있는 각 저장소 구성요소 개수 목록
- 해당 구성요소에 대한 자세한 정보가 있는 구성요소 데이터 테이블

저장소 데이터를 보려면 다음을 수행합니다.

1. **vSphere 클라이언트**에서 호스트를 선택하고 **OpenManage Integration 탭**을 선택합니다.
2. **호스트 개요** 페이지의 왼쪽 창에서 **저장소**를 클릭합니다.
3. **저장소** 페이지에서 그래픽 요약을 보거나 테이블과 **보기** 및 **필터** 드롭다운 목록을 사용하여 인벤토리 정보를 정렬합니다.

호스트 전원 모니터링 보기

호스트 시스템 전원 모니터링은 다음을 비롯하여 일반 전원 정보, 에너지 통계 및 예비 전원 정보를 제공합니다.

- 현재 전원 할당량, 프로필, 경고 및 오류 임계값
- 에너지 소모량, 시스템 최고 전원 및 암페어 통계

- 예비 전원 및 최고 예비 용량

호스트 전원 모니터링을 보려면 다음을 수행합니다.

1. **vSphere 클라이언트**에서 호스트를 선택하고 **OpenManage Integration 탭**을 선택합니다.
2. 왼쪽 창의 **호스트 정보** 아래에서 **전원 모니터링**을 클릭합니다.
3. **전원 모니터링** 페이지에서 이 호스트에 대한 전원을 확인합니다.

전체 데이터센터 하드웨어 구성 및 상태 표시

인벤토리 작업을 완료해야 전체 데이터센터 하드웨어 구성 및 상태를 표시할 수 있습니다. 인벤토리가 실행되면 다음과 같은 사항을 볼 수 있습니다.

- 하드웨어: 현장 교체 장치
- 하드웨어: 프로세서
- 하드웨어: 전원 공급 장치
- 하드웨어: 메모리
- 하드웨어: NIC
- 하드웨어: PCI 슬롯
- 하드웨어: 원격 액세스 카드
- 저장소: 실제 디스크
- 저장소: 가상 디스크
- 펌웨어
- 전원 모니터링
- 보증

전체 데이터센터 하드웨어 구성 및 상태를 표시하려면 다음을 수행합니다.

1. **vSphere 클라이언트**에서 **인벤토리** 제목 아래에 있는 **호스트 및 클러스터**를 선택합니다.
2. **호스트 및 클러스터**에 있는 트리 보기에서 데이터센터를 선택하고 **OpenManage Integration** 탭을 선택합니다.
3. 데이터센터에 있는 모든 호스트의 개요가 표시됩니다. **보기** 드롭다운 목록을 사용하여 인벤토리 카테고리를 봅니다.
4. **필터** 텍스트 상자에서 인벤토리 데이터의 필터를 입력합니다.
5. 표시된 인벤토리를 새로 고치려면 **새로 고침**을 클릭합니다.
6. **다운로드 위치** 창에서 인벤토리를 저장할 위치를 찾고 **저장**을 클릭합니다.

연결 프로필 관리

연결 프로필은 액세스 및 배포 자격 증명을 일련의 호스트 시스템과 연결하며 일반적으로 다음과 같은 사항이 들어 있습니다.

- 프로필 이름 및 고유한 설명(프로필 관리에 유용)
- 연결 프로필과 연결된 호스트 목록
- iDRAC 자격 증명
- 호스트 자격 증명
- Date Created(생성된 날짜)
- Date Modified(수정된 날짜)
- 마지막 수정 사용자

구성 마법사를 실행한 후 다음을 사용하여 OpenManage Integration for VMware vCenter **관리 탭 → 템플릿 및 프로필**에서 자격 증명 프로필을 관리합니다.

- 연결 프로필 생성
- 기존 연결 프로필 보기 및 편집
- 연결 프로필 삭제
- 연결 프로필 테스트
- 연결 프로필 새로 고치기

기존 연결 프로필 보기 또는 편집

연결 프로필을 구성한 후에는 프로필 이름, 설명, 연결된 호스트, iDRAC 및 OMSA 에이전트 자격 증명을 편집할 수 있습니다.
기존 연결 프로필을 보거나 편집하려면 다음을 수행합니다.

1. OpenManage Integration for VMware vCenter **Connection Profiles(연결 프로필)**를 선택합니다.
2. **Available Profiles(사용 가능한 프로필)**에서 보거나 편집할 프로필을 선택하고 **Edit/View(편집/보기)**를 클릭합니다.
3. **Profile Name and Description(프로필 이름 및 설명)** 페이지에서 사용자 지정 연결 프로필을 관리하는 데 유용한 **Connection Profile Name(연결 프로필 이름)**과 선택사항인 **Connection Profile Description(연결 프로필 설명)**을 입력합니다.
4. **Associated Hosts(연결된 호스트)** 페이지에서 연결 프로필에 사용할 호스트를 선택하고 **Next(다음)**를 클릭합니다.
5. **Credentials(자격 증명)** 페이지의 정보를 읽고 **Next(다음)**를 클릭합니다.
6. iDRAC 페이지의 자격 증명 아래에서 다음 중 하나를 수행합니다.

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

   - Active Directory를 사용할 iDRAC가 이미 구성되어 있고 Active Directory에 활성화되어 있으면 **Use Active Directory(Active Directory 사용)** 확인란을 선택합니다. 그렇지 않으면 iDRAC 자격 증명 구성 단계로 건너뜁니다.
     - **Active Directory User Name(Active Directory 사용자 이름)** 텍스트 상자에 사용자 이름을 입력합니다. 사용자 이름은 도메인\사용자 이름, 도메인/사용자 이름 또는 사용자 이름@도메인 형식 중 하나를 입력합니다. 사용자 이름은 256자로 제한됩니다. 사용자 이름 제한사항에 대해서는 Microsoft Active Directory 설명서를 참조하십시오.
     - **Active Directory Password(Active Directory 암호)** 텍스트 상자에 암호를 입력합니다. 암호는 127자로 제한됩니다.
     - **Verify Password(암호 확인)** 텍스트 상자에 암호를 다시 입력합니다.
     - Certificate Check(인증서 확인) 드롭다운 목록에서 다음 중 하나를 선택합니다.
       * iDRAC 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **Enable(활성화)**을 선택합니다.
       * 인증서 확인을 수행하지 않고 저장하지 않으려면 **Disabled(비활성화)**를 선택합니다.
   - Active Directory 없이 iDRAC 자격 증명을 구성하려면 다음을 수행합니다.
     - **User Name(사용자 이름)** 텍스트 상자에 사용자 이름을 입력합니다. 사용자 이름은 16자로 제한됩니다. 사용 중인 iDRAC 버전에서의 사용자 이름 제한사항을 보려면 iDRAC 설명서를 참조하십시오.

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

- **Password(암호)** 텍스트 상자에 암호를 입력합니다. 암호는 20자로 제한됩니다.
- **Verify Password(암호 확인)** 텍스트 상자에 암호를 다시 입력합니다.
- Certificate Check(인증서 확인) 드롭다운 목록에서 다음 중 하나를 선택합니다.
  - * iDRAC 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **Enable(활성화)**을 선택합니다.
  - * iDRAC 인증서 확인을 수행하지 않고 저장하지 않으려면 **Disabled(비활성화)**를 선택합니다.

7. **Next(다음)**를 클릭합니다.
8. Host Credentials(호스트 자격 증명) 페이지의 자격 증명 아래에서 다음 중 하나를 수행합니다.

- Active Directory를 사용할 호스트가 이미 구성되어 있고 Active Directory에 활성화되어 있으면 **Use Active Directory(Active Directory 사용)** 확인란을 선택합니다. 그렇지 않으면 호스트 자격 증명 구성 단계로 건너뜁니다.
  - **Active Directory User Name(Active Directory 사용자 이름)** 텍스트 상자에 사용자 이름을 입력합니다. 사용자 이름은 도메인\사용자 이름, 도메인/사용자 이름 또는 사용자 이름@도메인 형식 중 하나를 입력합니다. 사용자 이름은 256자로 제한됩니다. 사용자 이름 제한사항에 대해서는 Microsoft Active Directory 설명서를 참조하십시오.
  - **Active Directory Password(Active Directory 암호)** 텍스트 상자에 암호를 입력합니다. 암호는 127자로 제한됩니다.
  - **Verify Password(암호 확인)** 텍스트 상자에 암호를 다시 입력합니다.
  - Certificate Check(인증서 확인) 드롭다운 목록에서 다음 중 하나를 선택합니다.
    - * 호스트 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **Enable(활성화)**을 선택합니다.
    - * 호스트 인증서 확인을 수행하지 않고 저장하지 않으려면 **Disabled(비활성화)**를 선택합니다.
- Active Directory 없이 호스트 자격 증명을 구성하려면 다음을 수행합니다.
  - **User Name(사용자 이름)** 텍스트 상자에 사용자 이름을 입력합니다. 사용자 이름은 루트여야 합니다.
  - **Password(암호)** 텍스트 상자에 암호를 입력합니다. 암호는 127자로 제한됩니다.

    노트: iDRAC 익스프레스 또는 엔터프라이즈 카드가 없는 서버의 경우 iDRAC 테스트 연결 시 Not Applicable for this system(이 시스템에 해당되지 않음)이라는 메시지가 표시됩니다.

    노트: OMSA 자격 증명은 ESX 및 ESXi 호스트에 사용된 자격 증명과 동일합니다.
  - **Verify Password(암호 확인)** 텍스트 상자에 암호를 다시 입력합니다.
  - Certificate Check(인증서 확인) 드롭다운 목록에서 다음 중 하나를 선택합니다.
    - * 호스트 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **Enable(활성화)**을 선택합니다.
    - * 호스트 인증서 확인을 수행하지 않고 저장하지 않으려면 **Disabled(비활성화)**를 선택합니다.

9. **Save(저장)**를 클릭합니다.
10. 창을 닫으려면 오른쪽 상단 구석에 있는 **X**를 클릭합니다.

연결 프로필 삭제

OpenManage Integration for VMware vCenter에서 연결 프로필을 제거할 수 있습니다.

연결 프로필을 삭제하려면 다음을 수행합니다.

1. **OpenManage Integration for VMware vCenter**에서, **Connection Profiles(연결 프로필)**를 클릭합니다.
2. **Available Profiles(사용 가능한 프로필)**에서 삭제할 프로필을 선택하고 **Delete(삭제)**를 클릭합니다.
3. 표시되는 메시지에서 **Delete(삭제)**를 클릭하여 프로필을 제거하거나 **Cancel(취소)**을 클릭하여 삭제 작업을 취소합니다.

연결 프로필 테스트

연결 프로필을 테스트하려면 다음을 수행합니다.

1. **OpenManage Integration for VMware vCenter** 에서, **Connection Profiles(연결 프로필)**를 선택합니다.
2. 선택한 서버에서 입력된 iDRAC 및 호스트 루트 자격 증명을 테스트하려면 **Available Profiles(사용 가능한 프로필)**에서 연결 프로필을 선택하고 **Test Connection(테스트 연결)**을 클릭합니다.
3. 확인란을 사용하여 테스트할 호스트를 선택한 다음 **Test Selected(선택된 항목 테스트)**를 클릭합니다.
4. 선택한 모든 테스트를 중단하고 테스트를 취소하려면 **Abort All Tests(모든 테스트 중단)**를 클릭합니다.
5. 종료하려면 **Done(완료)**을 클릭합니다.

연결 프로필 새로 고치기

연결 프로필을 새로 고치려면 다음을 수행합니다.

새로 고침을 클릭합니다.

노트: 호스트가 vCenter에서 제거되면 연결 프로필에서도 제거됩니다.

vSphere 클라이언트 호스트 보기의 시스템 이벤트 로그 이해

시스템 이벤트 로그는 OpenManage Integration for VMware vCenter에서 검색한 하드웨어에 대한 상태 정보를 제공합니다.

시스템 이벤트 로그는 다음과 같은 기준에 따라 정보를 제공합니다.

상태	정보용(파란색 느낌표), 경고(느낌표가 있는 노란색 삼각형), 오류(빨간색 X) 등 몇 가지 상태 아이콘이 있습니다.
시간(서버 시간)	이벤트가 발생한 날짜 및 시간을 나타냅니다.
이 페이지 검색	특정 메시지, 서버 이름, 구성 설정 등을 표시합니다.

심각도 수준은 다음과 같이 정의됩니다.

정보	OpenManage Integration for VMware vCenter 작업이 성공적으로 완료되었습니다.
경고	OpenManage Integration for VMware vCenter 작업에 일부만 성공하고 일부는 실패했습니다.
오류	OpenManage Integration for VMware vCenter 작업에 실패했습니다.
보안	시스템 보안에 대한 정보가 들어 있습니다.

로그를 외부 CSV 파일로 저장할 수 있습니다.

관련 정보:

- 개별 호스트의 시스템 이벤트 로그 표시

Dell Management Center의 로그 표시

Dell Management Center 로그에는 검색된 하드웨어의 상태 정보와 사용자 조치의 내역이 포함되어 있습니다. Dell Management Center의 로그를 표시하려면 다음을 수행합니다.

1. **Dell Management Center**의 왼쪽 창에서 **로그**를 선택합니다.
2. 최신 데이터로 로그를 업데이트하려면 **새로 고침**을 클릭합니다.
3. 로그 데이터를 필터링할 심각도 카테고리를 선택하려면 **모든 카테고리** 드롭다운 목록에서 모든 카테고리, 정보, 경고, 오류 또는 보안 중 하나를 선택합니다.
4. 로그 데이터를 필터링할 날짜 범위를 선택하려면 **지난 주** 드롭다운 목록을 클릭하고 지난 주, 지난 달, 작년 또는 사용자 지정 범위 중 하나를 선택합니다.

   사용자 지정 범위를 선택하는 경우 **시작 날짜** 및 **중지 날짜** 드롭다운 목록이 표시됩니다.
5. 사용자 지정 범위를 선택한 경우 다음을 수행합니다.
   a. 캘린더를 클릭하여 **시작** 날짜를 채웁니다.
   b. 캘린더를 클릭하여 **종료** 날짜를 채웁니다.
   c. 구성을 저장하려면 **적용**을 클릭합니다.
6. 로그가 표시되는 방법을 제어하려면 표시 제어를 사용하여 **화면 당 레코드 수**를 설정하고, 원하는 **페이지**로 이동한 다음, 앞으로 및 뒤로 페이지 제어를 사용합니다.
7. 로그 컨텐츠를 CSV(쉼표로 구분된 값) 파일로 내보내려면 **내보내기**를 클릭합니다.
8. 다운로드 위치 창에서, 로그를 저장할 위치를 찾고 **저장**을 클릭합니다.

개별 호스트의 이벤트 로그 표시

시스템 하드웨어 이벤트 로그는 다음과 같은 기준에 따라 정보를 제공합니다.

- 상태
  정보용(파란색 느낌표), 경고(느낌표가 있는 노란색 삼각형), 오류(빨간색 X) 등 몇 가지 상태 아이콘이 있습니다.
- 시간(서버 시간)
  이벤트가 발생한 날짜 및 시간을 표시합니다.
- 이 페이지 검색
  특정 메시지, 서버 이름, 구성 설정 등을 표시합니다.

개별 호스트의 시스템 이벤트 로그를 표시하려면 다음을 수행합니다.

1. **vSphere 클라이언트**에서 **인벤토리** 제목 아래에 있는 **호스트 및 클러스터**를 선택합니다.
2. 트리 보기에서 호스트 시스템을 선택합니다.
3. **OpenManage Integration** 탭을 선택합니다.
4. **시스템 이벤트 로그** 창을 실행하려면 **최근 시스템 로그 항목**에서 **상세정보**를 클릭합니다.
5. **시스템 이벤트 로그**를 업데이트하려면 **로그 새로 고침**을 클릭합니다.
6. 이벤트 로그 항목 수를 제한(필터)하려면 다음 중 하나를 선택합니다.
   - 검색 필터 텍스트 상자에서 로그 항목을 동적으로 필터링하는 텍스트 문자열을 입력합니다.
   - 필터 텍스트 상자를 지우려면 **X**를 클릭합니다. 그러면 모든 이벤트 로그 항목이 표시됩니다.
7. 모든 이벤트 로그 항목을 지우려면 **로그 지우기**를 클릭합니다. 모든 로그 항목이 지워진 후에는 삭제된다는 내용의 메시지가 표시됩니다. 다음 중 하나를 선택합니다.
   - 로그 항목을 지우려면 **확인**을 클릭합니다.
   - 취소하려면 **취소**를 클릭합니다.

8. 이벤트 로그를 CSV 파일로 내보내려면 **내보내기**를 클릭합니다.
9. 시스템 이벤트 로그를 저장할 위치를 찾아보고 **저장**을 클릭합니다.

펌웨어 업데이트 정보

서버가 펌웨어 업데이트를 수신하는 위치는 Settings(설정) 탭의 OpenManage Integration for VMware vCenter에서 사용할 수 있는 전역 설정입니다.

펌웨어 리포지토리 설정에는 배포된 서버를 업데이트하는 데 사용되는 펌웨어 카탈로그 위치가 있습니다. 위치 유형에는 두 가지가 있습니다.

Dell(ftp.dell.com)	Dell(**ftp.dell.com**)의 펌웨어 업데이트 리포지토리를 사용합니다. OpenManage Integration for VMware vCenter는 선택된 펌웨어 업데이트를 Dell 리포지토리에서 다운로드합니다.
공유 네트워크 폴더	Dell Repository Manager™를 사용하여 생성됩니다. 이러한 로컬 리포지토리는 CIFS 또는 NFS 파일 공유에 있습니다.

노트: 리포지토리가 생성되면 등록된 호스트가 액세스할 수 있는 위치에 저장해야 합니다. 리포지토리 암호는 31자를 넘을 수 없으며 @, &, %, ', ", ,(쉼표), < >와 같은 특수 문자를 사용할 수 없습니다.

펌웨어 업데이트 마법사는 iDRAC, BIOS 및 수명 주기 컨트롤러의 최소 펌웨어 수준을 항상 확인하며, 필요한 최소 버전으로 업데이트하도록 시도합니다. iDRAC, 수명 주기 컨트롤러 및 BIOS 펌웨어 버전이 최소 요구사항을 충족하면 펌웨어 업데이트 마법사가 iDRAC, 수명 주기 컨트롤러, RAID, NIC/LOM, 전원 공급 장치 및 BIOS 등을 비롯한 모든 펌웨어의 업데이트를 허용합니다.

노트: 9세대 및 10세대 서버의 경우, BIOS/BMC/DRAC 펌웨어 버전은 vCenter의 클러스터 보기 수준 또는 개별 호스트 보기의 Overview(개요) 페이지에서만 볼 수 있습니다. 펌웨어 버전 정보가 펌웨어 아래의 개별 호스트 보기에서 활성화되지 않으며 원격 펌웨어 업데이트를 사용할 수 없습니다.

2010년 10월 14일 이후의 펌웨어 버전

2010년 10월 14일 이후에 업데이트된 펌웨어의 경우 펌웨어 업데이트 마법사가 실행됩니다.

2009년 7월 29일에서 10월 14일 사이의 펌웨어 버전

2009년 7월 29일에서 10월 14일 사이에 업데이트된 펌웨어의 경우, 펌웨어 업데이트 마법사를 사용할 수 없지만 펌웨어를 업데이트할 수 있는 ISO 번들이 제공됩니다. 이 업데이트 후에는 최신 펌웨어를 사용할 수 없습니다. 번들을 실행한 후에는 업데이트를 다시 실행하는 것이 좋습니다.

2009년 7월 29일 이전의 펌웨어 버전

펌웨어가 2009년 7월 29일 이전 버전일 경우 시스템을 업데이트할 수 있는 ISO 파일을 다운로드하여 실행해야 합니다. ISO를 실행한 후에는 펌웨어 업데이트 마법사를 다시 실행하는 것이 좋습니다.

관련 정보:

- 펌웨어 리포지토리 설정

펌웨어 업데이트 마법사 실행

이 기능은 iDRAC Express 또는 Enterprise 카드가 있는 Dell 서버의 11세대 이후 세대에서만 사용할 수 있습니다. 2010년 10월 14일 당일 이후에 펌웨어를 설치한 경우 펌웨어 업데이트 마법사를 사용하여 펌웨어 버전을 자동으로 업데이트할 수 있습니다.

노트: 브라우저 시간 제한으로부터 보호하려면 기본 시간 제한을 30초로 변경하십시오. 기본 시간 제한 설정을 변경하는 방법에 대한 자세한 내용은 *사용 설명서*의 문제 해결 섹션에서 펌웨어 업데이트 링크를 클릭한 후에 오류 메시지가 표시되는 이유를 참조하십시오.

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

펌웨어 업데이트 마법사를 실행하려면 다음을 수행합니다.

1. **vSphere Client(vSphere 클라이언트) → Dell Server Management tab(Dell Server Management 탭) → Host Information(호스트 정보)**에서 **Firmware(펌웨어) → Run Firmware Update Wizard(펌웨어 업데이트 마법사 실행)**를 클릭합니다.
2. **Load a single firmware update from a file(파일에서 단일 펌웨어 업데이트 로드)** 옵션을 사용하려면 다음을 수행합니다.
   a. 다음 형식으로 파일 경로를 입력합니다.
      ```
      CIFS: \\<host accessible share path>\<FileName>.exe or NFS: host:/share/filename.exe
      ```
   b. NFS를 사용하는 경우 7단계로 건너뜁니다. 그렇지 않을 경우 공유 드라이브에 액세스할 수 있는 **User Name(사용자 이름)** 및 **Password(암호)**를 도메인 형식에 입력합니다.
   c. 7단계를 계속 진행합니다.

   또는 **리포지토리에서 업데이트** 옵션을 사용하려면 다음을 수행합니다.
   a. **리포지토리에서 업데이트**를 선택합니다.
   b. **ftp.dell.com**에 대한 네트워크 연결을 확인합니다.
   c. **Next(다음)**를 클릭합니다.
3. 호스트용 번들을 선택하고 **Next(다음)**를 클릭합니다.
4. 원하는 펌웨어 업데이트를 선택하고 **Next(다음)**를 클릭합니다. 다운그레이드, 최신 상태 또는 현재 업데이트 예약된 구성요소는 선택할 수 없습니다. **Allow Components to be Downgraded(다운그레이드되는 구성요소 허용)** 확인란을 선택할 경우 다운그레이드로 나열되는 옵션을 선택합니다. 이 옵션은 펌웨어 다운그레이드에 대해 잘 알고 있는 고급 사용자에게만 권장됩니다.
5. 원하는 다시 시작 옵션을 선택합니다.
   - **유지 보수 모드로 전환하고 업데이트를 적용한 후 다시 시작합니다.**
     호스트가 유지 보수 모드로 전환됩니다. 호스트가 유지 보수 모드로 전환되지 않으면 호스트가 다시 시작되지 않고 다음에 다시 부팅할 때 업데이트가 적용됩니다. 업데이트 후에 유지 보수 모드를 종료하려면 **펌웨어 업데이트 완료 후 유지 보수 모드 종료** 확인란을 선택합니다.
   - **다음에 다시 부팅할 때 업데이트를 적용합니다.**
     서비스가 중단되지 않도록 하려면 다시 부팅하기 전에 호스트를 유지 보수 모드로 전환하는 것이 좋습니다.
   - **업데이트를 적용한 후 유지 보수 모드로 전환하지 않고 강제로 다시 부팅합니다.**
     업데이트가 적용되며, 호스트가 유지 보수 모드가 아니어도 다시 부팅됩니다. 이 방법은 권장되지 않습니다.
6. **Finish(마침)**를 클릭합니다.
7. 업데이트에 성공했는지 확인하려면 Dell Management Center에서 **Job Queue(작업 큐) → Inventory History(인벤토리 내역) → Run Now(지금 실행)**를 선택하고, 새 버전을 보려면**vSphere Client(vSphere 클라이언트) → OpenManage Integration tab(OpenManage Integration 탭)**에서 **Firmware(펌웨어)**를 클릭합니다.

이전 펌웨어 버전 업데이트

펌웨어는 펌웨어 업데이트 마법사를 실행할 수 있는 최소 수준이어야 합니다. 해당 수준이 아닐 경우 펌웨어 업데이트 마법사를 실행하기 전에 펌웨어를 업데이트하는 데 도움이 되는 옵션이 제공됩니다. 일반적으로 2009년 7월 29일 이전에 설치된 펌웨어에서는 ISO 파일을 다운로드하여 실행해야 합니다(펌웨어 업데이트 참조). 2009년 7월 29일과 2010년 10월 14일 사이에 설치된 펌웨어의 경우 OpenManage Integration for VMware vCenter에서 자동으로 설치할 수 있는 ISO 번들이 제공됩니다. 2010년 10월 14일 이후에 업데이트된 펌웨어는 펌웨어 업데이트 마법사를 실행합니다. 펌웨어 업데이트는 호스트 Dell Server Management(Dell 서버 관리) 탭의 vSphere 클라이언트에서 실행됩니다. 리포지토리를 설정하려면 펌웨어 리포지토리 설정을 참조하십시오.

이전 펌웨어 버전을 업데이트하려면 다음을 수행합니다.

1. **vSphere 클라이언트**의 **OpenManage Integration** 탭에서 **호스트 작업** 아래에 있는 **펌웨어 업데이트 마법사 실행**을 클릭합니다.

   호스트가 마법사에서 지원하는 것보다 낮은 수준의 펌웨어에 있을 경우 Update Required(업데이트 필요) 대화상자가 표시됩니다. ISO 파일을 다운로드하여 실행하라는 메시지가 표시되거나 실행할 업데이트 번들이 제공됩니다.
2. **업데이트 필요** 대화상자에서 다음 중 하나를 수행합니다.

   - 펌웨어 업데이트 후에 유지 보수 모드를 자동으로 종료하려면 **펌웨어 업데이트 완료 후 유지 보수 모드를 종료합니다** 확인란을 선택합니다.
   - 시스템을 클러스터에 다시 추가하기 전에 검사하거나 테스트하기 위해 유지 보수 모드로 전환하려면 확인란을 선택하지 마십시오.
3. **업데이트**를 클릭합니다.
4. **성공** 대화 상자에 업데이트가 현재 진행 중이라는 메시지가 표시됩니다.

   펌웨어 업데이트 완료 후 유지 보수 모드를 종료합니다를 선택한 경우 펌웨어 업데이트가 호스트를 유지 보수 모드로 전환한 다음 자동으로 다시 부팅합니다. 그렇지 않으면 유지 보수 모드로 유지됩니다.
5. 업데이트 진행 상태를 보려면 vSphere 클라이언트의 **최근 작업** 영역을 참조하십시오.

   이 절차가 끝난 후 펌웨어 업데이트 마법사를 다시 실행하여 펌웨어가 완전히 업데이트되었는지 확인합니다.

클러스터 및 데이터센터용 펌웨어 업데이트 마법사 실행

이 기능은 iDRAC Express 또는 Enterprise 카드가 있는 11세대 이후 Dell 서버에서만 사용할 수 있습니다. 펌웨어가 2010년 10월 14일 당일 이후에 설치된 경우, 펌웨어 업데이트 마법사를 사용하여 펌웨어 버전을 자동 업데이트할 수 있습니다. 이 마법사는 연결 프로필의 일부이며 펌웨어, CSIOR 상태, 하이퍼바이저 및 OMSA 상태(11세대 서버만)에 대해 준수하는 호스트만 업데이트합니다. 호스트가 나열되지 않으면 OpenManage Integration for VMware vCenter에서 Compliance Wizard for vSphere(vSphere 호스트용 준수 마법사)를 실행하거나 Hosts and Clusters(호스트 및 클러스터) 보기에서 나열되어 있지 않은 호스트를 선택하고 펌웨어 업데이트 마법사를 사용하십시오. 일반적으로 각 호스트에 대한 펌웨어 구성요소를 업데이트하는 데 30분에서 60분 정도 걸립니다. 펌웨어 업데이트 프로세스 중에 호스트가 유지 보수 모드로 전환되거나 유지 보수 모드가 종료될 경우 가상 시스템을 이동할 수 있도록 클러스터에서 DRS를 활성화하십시오. 한 번에 하나의 펌웨어 업데이트만 예약하거나 실행할 수 있습니다.

마법사에서 내보내야 하는 경우 CSV로 내보내기 단추를 사용하십시오. 검색은 적용된 날짜를 제외하고 데이터 격자에서 특정 클러스터, 데이터센터, 호스트 또는 주제 항목을 찾는 데 사용할 수 있습니다.

노트: 펌웨어는 항상 리포지토리 번들(BIOS, iDRAC 및 Lifecycle Controller)의 일부로 함께 업데이트하십시오.

노트: 기본 시간 제한 설정을 변경하는 방법에 대한 자세한 내용은 *사용 설명서*의 문제 해결 섹션에서 펌웨어 업데이트 링크를 클릭한 후에 오류 메시지가 표시되는 이유를 참조하십시오.

작업 큐 페이지에서 상태를 보고 펌웨어 업데이트 작업을 관리할 수 있습니다. 클러스터 및 데이터센터용 펌웨어 업데이트 상태 보기를 참조하십시오.

1. **vSphere 클라이언트**에서 **Inventory(인벤토리)** 제목 아래에 있는 **Hosts and Clusters(호스트 및 클러스터)**를 선택합니다.
2. **Hosts and Clusters(호스트 및 클러스터)**의 트리 보기에서 데이터센터 또는 클러스터를 선택하고 **OpenManage Integration** 탭을 선택합니다.
3. **Update Firmware(펌웨어 업데이트)**를 클릭합니다.

   이 링크가 활성화되어 있지 않거나 이 옵션을 클릭할 때 팝업 메시지가 나타나면 진행 중이거나 예약된 펌웨어 업데이트 작업이 있는 것입니다. 대화상자를 닫고 기다렸다가 나중에 다시 시도하십시오. Job Queues(작업 큐)의 Firmware Update Jobs(펌웨어 업데이트 작업) 탭에서 모든 작업의 상태를 확인하십시오.

4. 마법사를 계속하기 전에 시작 페이지에서 업데이트에 대한 정보를 검토합니다.
5. **Next(다음)**를 클릭합니다.
6. 펌웨어 인벤토리 페이지에서 시스템에 이미 설치되어 있는 구성요소를 검토합니다.
7. **Next(다음)**를 클릭합니다.
8. 업데이트된 번들 선택 페이지에서 확인란을 사용하여 업데이트 번들을 선택합니다.
9. **Next(다음)**를 클릭합니다.
10. 업데이트할 시스템/구성요소 선택 페이지에서 확인란을 사용하여 업그레이드하거나 다운그레이드할 구성요소를 선택합니다. 다운그레이드하려면 **Allow components to be downgraded(다운그레이드되는 구성요소 허용)** 확인란을 선택하십시오.

    노트: 모든 구성요소를 선택한 후에 일부가 선택되지 않은 상태로 남아 있으면 해당 구성요소에 대해 사용할 수 있는 업그레이드가 없다는 뜻입니다. 해당 구성요소는 다운그레이드를 위해 선택할 수 있습니다.
11. **Next(다음)**를 클릭합니다.
12. 펌웨어 업데이트 정보 페이지에서 업그레이드나 다운그레이드를 위해 선택한 구성요소를 검토합니다.
13. **Next(다음)**를 클릭합니다.
14. 펌웨어 업데이트 예약 페이지의 작업 이름 아래에서 다음을 수행합니다.
    a. 펌웨어 업데이트 작업 이름 텍스트 상자에 **firmware update job name(펌웨어 업데이트 작업 이름)**을 입력합니다.

       필수 필드입니다. 이 필드를 입력하지 않으면 이 업그레이드가 예약되지 않습니다. 이미 사용 중인 이름은 사용하지 마십시오. 이 이름을 제거해도 다시 재사용할 수 있습니다.
    b. 펌웨어 업데이트 설명에 **Description(설명)**을 입력합니다.
15. 작업 스케줄 아래에서 다음 중 하나를 수행합니다.

    노트: 반드시 옵션을 선택해야 합니다. 옵션을 선택하지 않으면 업그레이드가 차단됩니다.

    - 지금 업데이트 작업을 실행하려면 **지금 업데이트**를 클릭하고 **완료**를 클릭합니다.
    - 나중에 업데이트 작업을 실행하려면 **업데이트 예약**을 클릭하고 다음을 수행합니다.

      1. 달력 상자에서 **월 및 일**을 선택합니다.
      2. 시간 텍스트 상자에 HH:MM 형식으로 **시간**을 입력하고 **완료**를 클릭합니다.

         노트: 시간은 클라이언트가 실제로 위치한 현지 시간대입니다. 시간 값이 잘못되면 업데이트가 차단됩니다.

클러스터 및 데이터센터용 펌웨어 업데이트 상태 보기

이 페이지에 정보가 표시되도록 하려면 클러스터나 데이터센터를 위한 펌웨어 업데이트를 실행하십시오. 이 페이지에는 클러스터 및 데이터센터의 펌웨어 업데이트에 대한 정보만 표시됩니다. 클러스터 및 데이터센터용 펌웨어 업데이트 마법사 실행을 참조하십시오.
이 페이지에서 펌웨어 업데이트 작업을 새로 고치거나 제거하거나 중단할 수 있습니다.

1. Dell Management Center에서 **Job Queue(작업 큐)** → **Firmware Update Jobs(펌웨어 업데이트 작업)**를 선택합니다.
2. 최신 정보를 표시하려면 **Refresh(새로 고침)**를 클릭합니다.
3. 데이터 격자에서 상태를 봅니다. 이 격자는 펌웨어 업데이트 작업에 대해 다음 정보를 제공합니다.

   - Status(상태)
   - 예약된 시간
   - 이름
   - 설명

- 컬렉션 크기

  컬렉션 크기는 이 펌웨어 인벤토리 작업에 있는 서버의 개수입니다.
- 진행률 요약

  진행률 요약에는 이 펌웨어 업데이트의 진행률 상세정보가 나열됩니다.

4. 특정 작업에 대해 보다 자세한 정보를 보려면 특정 작업의 데이터 격자에서 **Details(상세정보)**를 클릭하십시오.

   여기에서 다음과 같은 상세정보를 찾을 수 있습니다.

   - 서비스 태그
   - iDRAC IP
   - Status(상태)
   - 경고
   - 펌웨어 업데이트 작업 상세정보
   - 시작 시간
   - 종료 시간
5. 실행 중이지 않은 예약된 펌웨어 업데이트를 중단하려면 중단하려는 작업과 같은 줄에서 **Abort(중단)**를 클릭하십시오.
6. 예약된 펌웨어 업데이트를 제거하려면 **Purge Job Queue(작업 큐 제거)**를 클릭하십시오.

   완료되거나 예약된 작업만 제거할 수 있습니다.
7. **Older than date and job Status(다음 기간 이후 및 작업 상태)**를 선택하고 **Apply(적용)**를 클릭하십시오. 그러면 선택한 작업이 큐에서 지워집니다.

vCenter를 사용한 고급 호스트 관리

고급 호스트 관리 작업은 호스트 시스템 기반 작업으로서 관리자가 데이터센터 환경에서 실제 서버를 식별하고, 서버 기반 관리 도구를 실행하며, 서버 보증 정보를 표시할 수 있습니다. 이러한 모든 작업은 vCenter의 OpenManage Integration 탭을 사용하거나 개별 호스트 시스템의 *호스트 및 클러스터* 보기에서 해당 호스트를 마우스 오른쪽 단추로 클릭하여 시작할 수 있습니다.

실제 서버 전면 표시등 설정

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

1. **vSphere 클라이언트**에서 **인벤토리** 제목 아래에 있는 **호스트 및 클러스터**를 선택합니다.
2. **호스트 및 클러스터**에 있는 트리 보기에서 호스트 시스템을 선택하고 **OpenManage Integration** 탭을 선택합니다.
3. **호스트 작업**에서 **표시등 깜빡임**을 선택합니다.
4. 다음 중 하나를 선택합니다.

   - 깜빡임 및 기간을 설정하려면 **표시등** 대화 상자에서 **깜빡임 켜기**를 클릭하고 시간 제한 드롭다운 목록을 사용하여 시간 제한 증가를 선택한 다음 **확인**을 클릭합니다.
   - 깜빡임을 해제하려면 **표시등** 대화 상자에서 **깜빡임 끄기**를 클릭하고 **확인**을 클릭합니다.

서버 기반 관리 도구

서버 기반 관리 도구에는 iDRAC 및 OMSA 두 가지가 있으며 **vSphere 클라이언트 → OpenManage Integration** 탭에서 실행할 수 있습니다. 왼쪽 창에 있는 관리 콘솔 링크에서 다음 옵션에 액세스할 수 있습니다.

- 원격 액세스 실행
  이 옵션을 사용하여 iDRAC 사용자 인터페이스를 실행합니다.
- OMSA 실행
  이 옵션을 사용하여 초기 구성 마법사 또는 **설정 → 일반**을 통해 관리 센터에 입력된 OpenManage Server Administrator 사용자 인터페이스 URL을 실행합니다. Windows 기반 관리 스테이션에서는 서버 관리자 웹 서버의 URL을 설치해야 합니다.
- 블레이드 시스템에서 작업하는 경우 CMC를 실행하여 Chassis Management Controller 사용자 인터페이스를 실행합니다. 블레이드 시스템이 아닐 경우 이 옵션이 표시되지 않습니다.

보증 검색

보증 검색을 수행하면 다음과 같은 Dell 서버 정보가 제공됩니다.

- 업데이트된 서비스 보증 정보(호스트 서비스 태그만 전송)
- 예약된 간격으로 업데이트된 보증 정보
- 프록시 서버 및 자격 증명을 사용한 안전한 전송

노트: Dell은 전송된 서비스 태그 정보를 저장하지 않습니다.

관련 작업:

- 보증 검색 작업 실행
- 단일 호스트의 서버 보증 정보 보기
- 전체 데이터센터의 보증 정보 보기

전체 데이터센터의 서버 보증 정보 보기

보증 작업이 완료되면 vSphere 클라이언트의 데이터센터 보기 페이지에서 서버 보증 정보를 볼 수 있습니다.

전체 데이터센터의 서버 보증 정보를 보려면 다음을 수행합니다.

1. vSphere 클라이언트에서 **인벤토리** 제목 아래에 있는 **호스트 및 클러스터**를 선택합니다.
2. **호스트 및 클러스터**에 있는 트리 보기에서 데이터센터를 선택하고 **OpenManage Integration** 탭을 선택합니다.
3. 데이터센터에 있는 모든 호스트의 개요가 표시됩니다. 보기 드롭다운 상자에서 **보증**을 선택합니다.
4. **필터** 텍스트 상자에 보증 데이터의 필터를 입력합니다.
5. 표시된 인벤토리를 새로 고치려면 **새로 고침**을 클릭합니다.
6. 인벤토리를 CSV 파일로 내보내려면 **내보내기**를 클릭합니다. 다운로드 위치 창에서 인벤토리를 저장할 위치를 찾아보고 **저장**을 클릭합니다.

단일 호스트의 서버 보증 정보 보기

보증 작업이 완료되면 vSphere 클라이언트의 호스트 보기 페이지에서 단일 호스트의 보증 정보를 볼 수 있습니다.

단일 호스트의 서버 보증 정보를 보려면 다음을 수행합니다.

1. vSphere 클라이언트에서 **인벤토리** 제목 아래에 있는 **호스트 및 클러스터**를 선택합니다.
2. **호스트 및 클러스터**에 있는 트리 보기에서 호스트 시스템을 선택하고 **OpenManage Integration** 탭을 선택합니다.

3. 시스템 보증 정보를 표시하려면 **보증**을 선택합니다. 보증 상태 페이지에 다음과 같은 정보가 제공됩니다.

   - 보증 제공업체 이름 및 보증에 대한 설명
   - 시작 및 종료 날짜와 남은 보증 일 수
   - 보증 상태(활성, 비활성) 및 마지막으로 보증 정보가 업데이트된 시기

5

하드웨어 관리

필수 조건:
하드웨어 프로비저닝 및 배포를 성공적으로 수행하기 위해서는 실제 서버가 배포 마법사에 나타나야 합니다. 모든 실제 서버는 다음과 같은 필수 조건을 충족해야 합니다.

- 특정 하드웨어 지원 정보에 대해서는 *OpenManage Integration for VMware vCenter릴리스 노트*를 참조하십시오.
- 서버에는 최소한의 지원되는 버전의 iDRAC 펌웨어, Lifecycle 컨트롤러 및 BIOS가 있어야 합니다. 특정 하드웨어 지원 정보에 대해서는 *OpenManage Integration for VMware vCenter 릴리스 노트*를 참조하십시오.

  노트: 펌웨어 버전이 오래된 경우 2단계 업그레이드 프로세스를 수행해야 합니다. 자세한 업그레이드 지침은 펌웨어 문서를 참조하십시오.
- OpenManage Integration for VMware vCenter에서는 내장형/외장형 LOM만 사용하여 배포를 수행할 수 있습니다. 배포 후에 PCI 슬롯에 NIC를 수동으로 구성할 수 있습니다. 추가 기능 NIC를 사용할 경우 시스템에서 호스트 LOM을 사용할 수 있어야 합니다.
- OpenManage Integration for VMware vCenter는 내부 이중 SD 모듈(하이퍼바이저만) 또는 로컬 하드 드라이브에 배포를 허가합니다. 내부 이중 SD 모듈은 하이퍼바이저를 배포하기 전에 OpenManage Integration for VMware vCenter에서 활성화되어야 합니다. 관리 NIC를 수동으로 변경할 수 있으며 시스템을 vCenter에 추가할 수 있습니다.

  노트: 지원되는 듀얼 SD 모듈에 관해서는, 해당 서버 제품 설명서를 참조하십시오.
- iDRAC가 전용 모드일 경우 해당 NIC가 OpenManage Integration for VMware vCenter와 통신할 수 있어야 합니다.
- CSIOR을 사용할 수 있어야 합니다. 또한 자동 검색을 시작하기 전에 최신 상태의 데이터가 검색되도록 하려면 시스템의 전원을 완전히 껐다가 다시 켜야 합니다(하드 재부팅).
- 공장 출하 시 자동 검색 및 핸드셰이크 옵션이 미리 구성된 Dell 서버를 주문할 수 있습니다. 서버에 이러한 옵션이 미리 구성되어 있지 않을 경우 OpenManage Integration for VMware vCenter 주소를 수동으로 입력하거나 로컬 네트워크를 구성하여 이 정보를 제공해야 합니다.
- 하드웨어 구성에 OpenManage Integration for VMware vCenter를 사용하지 않을 경우 하이퍼바이저 배포를 시작하기 전에 다음과 같은 조건이 충족되는지 확인해야 합니다.
  - BIOS에서 VT(Virtualization Technology) 플래그를 활성화
  - 운영 체제 설치를 위한 시스템 부팅 순서를 부팅 가능한 가상 디스크 또는 내부 이중 SD 모듈로 설정
- 하드웨어 구성에 OpenManage Integration for VMware vCenter를 사용할 경우 VT의 BIOS 구성이 하드웨어 프로필에 속하지 않더라도 BIOS 설정이 자동으로 활성화됩니다. 가상 디스크가 대상 시스템에 아직 없는 경우 Express/Clone RAID 구성이 필요합니다.
- 서버가 Dell PowerEdge 12세대 서버 이전 버전일 경우 배포 프로세스에서 OpenManage Server Administrator 패키지가 대상 시스템에 자동으로 설치되고 SNMP 트랩 대상이 OpenManage Integration for VMware vCenter를 가리키도록 자동으로 구성됩니다.
- 배포 작업을 수행하려면 모든Dell 드라이버를 포함하는 사용자 지정 ESXi 이미지가 필요합니다. Dell 드라이버 및 다운로드 페이지로 이동하고 배포 과정 중에 액세스할 수 있는 위치에 사용자 지정 이미지를 저장하여 올바른 이미지를 찾을 수 있습니다. 이 릴리스에 지원되는 ESXi 버전의 최신 목록을 보려면 릴리스 정보를 참조하십시오.
- *OpenManage Integration for VMware vCenter*는 BIOS 모드 만을 지원하여 대상 서버에 있는 하이퍼바이저를 자동 배포합니다. 하이퍼바이저 프로필을 적용하기 전에 참조 하드웨어 프로필에 BIOS 모드가 선택되어 있는지 확인합니다. 하드웨어 프로필이 선택되지 않은 경우에는 수동으로 부팅 모드를 BIOS로 구성하고 하이퍼바이저 프로필을 적용하기 전에 서버를 다시 부팅합니다.

노트: 대상 시스템에서 BOOT 모드가 UEFI로 설정되면 OMIVV(OpenManage Integration for VMware and vCenter)로 부터 운영 체제 배포에 장애가 발생합니다.

프로비저닝 개요

데이터센터의 물리적 인벤토리가 완료되면 자동으로 검색된 모든 운영 체제 미설치 시스템을 OpenManage Integration for VMware vCenter에 사용하여 자동화된 하드웨어 프로비저닝 및 하이퍼바이저 배포를 수행할 수 있습니다. 프로비저닝 및 배포를 준비하려면 다음을 수행해야 합니다.

하드웨어 프로필 생성	새 서버를 배포하는 데 사용되는 참조 서버에서 수집된 하드웨어 설정이 들어 있습니다. 새 하드웨어 프로필 생성을 참조하십시오.
하이퍼바이저 프로필 생성	ESX/ESXi 배포에 필요한 하이퍼바이저 설치 정보가 들어 있습니다. 새 하이퍼바이저 프로필 생성을 참조하십시오.
배포 템플릿 생성	선택 사항으로서 하드웨어 프로필, 하이퍼바이저 프로필 또는 둘 다 들어 있습니다. 이러한 프로필을 저장하여 필요에 따라 사용 가능한 모든 데이터센터 서버에 재사용할 수 있습니다. 배포 템플릿 작성을 참조하십시오.

배포 템플릿이 생성되면 배포 마법사를 사용하여 서버 하드웨어를 프로비저닝하고 vCenter에 새 호스트를 배포하는 예약된 작업을 생성하는 데 필요한 정보를 수집합니다. 배포 마법사 실행에 대한 자세한 내용은 배포 마법사 실행을 참조하십시오. 마지막으로, 작업 큐를 사용하여 작업 상태를 확인하고 보류 중인 배포 작업을 변경합니다.

노트: 연속적으로 실행되도록 예약할 수 있는 배포 작업은 최대 2건입니다. 여러 개의 작업에서 예약 기능을 사용하면 배포 실행이 지연됩니다.

배포 작업 시간 이해

운영 체제 미설치 서버의 프로비저닝 및 배포를 완료하는 데에는 특정 요소에 따라 30분에서 몇 시간 정도 소요될 수 있습니다. 배포 작업을 시작할 때는 제공된 지침에 따라 배포 시간을 계획하는 것이 좋습니다. 프로비저닝 및 배포를 완료하는 데 걸리는 시간은 배포 유형, 복잡한 정도, 동시에 실행되는 배포 작업 수에 따라 다릅니다. 아래 표는 배포 작업에 걸리는 예상 시간에 대한 지침을 제공합니다. 배포 작업은 최대 5개의 동시 서버로 일괄 실행되므로 전체적인 배포 작업의 시간을 개선합니다. 정확한 동시 작업 수는 사용 가능한 리소스에 따라 다릅니다.

표 2. 예상 배포 시간 시나리오

배포 유형	배포 당 예상 소요 시간
하이퍼바이저만	30분 - 130분
하드웨어만	복잡한 정도와 구성할 RAID, BIOS 및 부팅 옵션에 따라 최대 2시간
하이퍼바이저 및 하드웨어 프로필	1 - 4시간

배포 시퀀스 내의 서버 상태

인벤토리 작업이 실행될 때 자동 검색된 운영 체제 미설치(bare-metal) 시스템은 다른 상태로 분류되어 서버가 데이터센터에 새로운 것이거나 일정이 잡힌 보류 배포 작업인지 결정하는데 도움을 줍니다. 관리자는 이 상태를 사용하여 서버가 배포 작업에 포함되는지 결정합니다. 이러한 상태는 다음과 같습니다:

구성되지 않음 서버가 OpenManage Integration for VMware vCenter과 연결된 후 구성을 위해 대기합니다. 배포 작업 시간 이해를 참조하십시오.

구성됨 서버가 성공적인 하이퍼바이저 배포에 필요한 모든 하드웨어 정보로 구성됩니다.

사용자 지정 Dell ISO 이미지 다운로드

배포 작업을 수행하려면 *모든* Dell 드라이버를 포함하는 사용자 지정 ESXi 이미지가 필요합니다. Dell은 사용자 지정 ESX 4.1 이미지를 생성할 수 없습니다. 올바른 배포를 위해서는 ISO VMware 제품에 *모든* 드라이버가 기본적으로 있어야 합니다. 이 릴리스에 지원되는 ESXi 버전의 최신 목록을 보려면 릴리스 정보를 참조하십시오.

노트: OpenManage Integration for VMware vCenter ISO에는 배포에 필요한 ESXi ISO 이미지가 없습니다. 배포 중에 액세스 가능한 위치에 이러한 이미지를 다운로드해야 합니다. 그렇지 않으면 배포에 실패합니다.

1. **support.dell.com**으로 이동합니다.
2. **드라이버 및 다운로드** 페이지를 찾아본 후 다음 중 하나를 수행합니다.
   - 서비스 태그 또는 익스프레스 서비스 코드를 사용하여 드라이버를 선택하려면 **예** 아래의 텍스트 상자에 서비스 태그 또는 익스프레스 서비스 코드를 입력한 다음 **제출**을 클릭합니다.
   - 다른 옵션을 사용하여 드라이버를 선택하려면 **아니오**에서 다음 중 하나를 선택합니다.
     - 내 서비스 태그 자동 인식
     - 내 제품 및 서비스 목록에서 선택
     - 모든 Dell 제품 목록에서 선택

     계속을 클릭하고 선택한 옵션의 지시를 따릅니다.
3. 선택한 서버의 페이지에서, 아래로 스크롤하여 **결과 범위 좁히기**로 이동하고 **운영 체제** 아래의 드롭다운 목록을 사용하여 원하는 ESX 또는 ESXi 시스템을 선택합니다.
4. **엔터프라이즈 솔루션**을 클릭합니다.
5. **엔터프라이즈 솔루션** 목록에서 필요한 ISO 버전을 선택하고 **파일 다운로드**를 클릭합니다.

   노트: 내장형 ISO는 이중 내부 SD 모듈에서의 하이퍼바이저 설치에 사용됩니다. 설치 가능한 ISO는 하드 디스크에서의 설치에 사용됩니다.
6. 대화상자에서 **브라우저를 통한 단일 파일 다운로드용**을 선택하고 **지금 다운로드**를 클릭합니다.
7. 대화상자에서 배포용 ISO 이미지를 저장할 위치를 찾아봅니다.

하드웨어 프로필 구성 방법 이해

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

부팅 순서 부팅 순서는 부팅 장치 시퀀스 및 하드 드라이브 시퀀스로서 부팅 모드가 BIOS로 설정된 경우에만 편집할 수 있습니다.

BIOS 설정 BIOS 설정에는 메모리, 프로세서, SATA, 통합 장치, 직렬 통신, 내장형 서버 관리, 전원 관리, 시스템 보안 및 기타 설정이 포함됩니다.

iDRAC 설정 iDRAC 설정에는 네트워크, 사용자 목록 및 사용자 구성((IPMI/iDRAC 권한)이 포함됩니다.

노트: iDRAC 익스프레스가 포함된 시스템의 경우, iDRAC 구성을 추출할 수 없습니다. 따라서 해당 서버를 참조 서버로 사용할 수 없습니다. 이 시스템을 대상 시스템으로 사용하는 경우 참조 서버의 iDRAC 구성이 적용됩니다.

RAID 구성

RAID 구성에는 하드웨어 프로필이 추출된 시점에서 참조 서버의 현재 RAID 토폴로지가 표시됩니다.

노트: 하드웨어 프로필에 두 개의 RAID 구성 옵션이 구성되어 있습니다. 1. *RAID1 적용 및 전용 핫 스페어 생성(해당되는 경우).* 대상 서버에 기본 RAID 구성 설정을 적용하려면 이 옵션을 선택합니다. RAID 구성 작업은 RAID1 사용 가능한 통합 컨트롤러의 처음 두 개 드라이브에서 RAID1로 기본 설정됩니다. 또한 후보 드라이브가 기존 기준을 충족하는 경우 RAID1 어레이의 전용 핫 스페어가 생성됩니다. 2. *아래에 표시된 대로 참조 서버에서 RAID 구성 클론.* 참조 서버 설정을 클론하려면 이 옵션을 사용합니다. 새 하드웨어 프로필 생성을 참조하십시오.

노트: OpenManage Integration for VMware vCenter은 참조 서버의 설정과 관계없이 배포된 모든 서버의 BIOS에 있는 프로세서 그룹에서 특정 BIOS 설정을 사용할 수 있도록 합니다. 참조 서버를 사용하여 새 하드웨어 프로필을 생성하기 전에 CSIOR(Collect System Inventory On Reboot) 설정을 활성화해야 하며 정확한 인벤토리 및 구성 정보를 제공하도록 다시 부팅해야 합니다.

하드웨어 프로필 생성 작업은 다음과 같습니다.

- 참조 서버에서 CSIOR 사용
- 새 하드웨어 프로필 생성
- 새 하드웨어 프로필 복제
- 하드웨어 프로필 관리 정보

새 하드웨어 프로필 생성

새 하드웨어 프로필을 생성하려면 다음을 수행합니다.

1. Dell Management Center에서 **배포 → 배포 템플릿 → 하드웨어 프로필**을 선택합니다.
2. **새로 생성**을 클릭합니다.
3. **새 하드웨어 프로필** 페이지에서 다음을 수행합니다.
   - **프로필 이름** 텍스트 상자에서 프로필 이름을 입력합니다.
   - **설명** 텍스트 상자에서 선택적 설명을 입력합니다.
4. **Save(저장)**를 클릭합니다.
5. 계속하려면 왼쪽 창에서 **참조 서버**를 클릭합니다.
6. 참조 서버 창에서 **편집**을 클릭합니다.
7. 기준에 맞고 vCenter에서 관리되며 OpenManage Integration for VMware vCenter에서 성공적으로 인벤토리 작성된 참조 서버를 찾으려면 **Browse(찾아보기)**를 클릭합니다.
8. **서버** 대화상자에서 아래로 스크롤하여 목록에서 올바른 참조 서버를 찾은 다음 **선택**을 클릭합니다.
9. 참조 서버 설정을 기본값으로 사용자 지정하려면 **참조 서버의 설정 사용자 지정**을 클릭하고 **저장**을 클릭합니다.
10. 설정을 추출하는 데 몇 분 정도 소요된다는 내용의 대화상자가 표시됩니다. 설정을 채우려면 **계속**을 클릭합니다. 선택한 서버의 이름, iDRAC IP 주소 및 서비스 태그가 **참조 서버 창**에 표시됩니다.
11. 왼쪽 창에서 **부팅 순서**를 선택합니다. 부팅 순서 정보를 프로필에 포함하려면 **이 하드웨어 프로필에 부팅 순서 포함** 확인란을 선택합니다.
12. 부팅 순서 옵션을 표시하려면 **부팅 순서**를 펼치고 **편집**을 클릭하여 업데이트합니다.

노트: Dell 13세대 PowerEdge 서버에서는, 하드웨어 프로필에 현재 부팅 모드 상세내역만이 표시됩니다.

노트: 대상 시스템에서 BOOT 모드가 UEFI로 설정되면 OMIVV(OpenManage Integration for VMware and vCenter)로 부터 운영 체제 배포에 장애가 발생합니다.

a. **부팅 모드** 드롭다운 목록에서 BIOS 또는 UEFI를 선택합니다.
b. 표시된 부팅 장치 시퀀스를 변경하려면 **보기/구성** 드롭다운 목록의 **부팅 장치 시퀀스**에서 **위로 이동** 또는 **아래로 이동**을 클릭합니다.
c. **부팅 재시도 시퀀스** 드롭다운 목록에서, 서버가 자동으로 부팅 시퀀스를 재시도하도록 하려면 **활성화**를 선택하고 시퀀스를 재시도하지 않도록 하려면 **비활성화**를 선택합니다.
d. **저장**을 클릭하여 변경사항을 저장하거나 **취소**를 클릭하여 변경사항을 취소합니다.

13. **BIOS 부팅 모드**를 선택한 경우 **하드 드라이브 시퀀스**를 펼쳐 하드 드라이브 시퀀스 옵션을 표시하고 **편집**을 클릭하여 업데이트할 수 있습니다.

- 표시된 하드 드라이브 시퀀스를 변경하려면 장치를 선택하고 **위로 이동** 또는 **아래로 이동**을 클릭합니다.
- **저장**을 클릭하여 변경사항을 저장하거나 **취소**를 클릭하여 변경사항을 취소합니다.

14. 왼쪽 창에서 **BIOS 설정**을 선택합니다. BIOS 설정 정보를 프로필에 포함하려면 **이 하드웨어 프로필에 BIOS 설정 포함** 확인란을 선택합니다. 카테고리를 펼쳐 설정 옵션을 표시하고 **편집**을 클릭하여 다음 중 하나를 업데이트합니다.

- 메모리 설정
- 프로세서 설정
- SATA 설정
- 내장형 장치
- 직렬 통신
- 내장형 서버 관리
- 전원 관리
- 시스템 보안
- 기타 설정

모든 카테고리 업데이트를 완료한 후 **적용**을 클릭하여 변경사항을 저장하거나 **취소**를 클릭하여 변경사항을 취소합니다.

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

15. 왼쪽 창에서 **iDRAC 설정**을 선택한 다음 **네트워크**를 선택합니다.
16. 네트워크 설정을 프로필에 포함하려면 **이 하드웨어 프로필에 네트워크 설정 포함** 확인란을 선택합니다. 카테고리를 펼쳐 설정 옵션을 표시하고 **편집**을 클릭하여 다음 중 하나를 업데이트합니다.

- 네트워크
- 네트워크 설정
- 가상 매체

모든 카테고리 업데이트를 완료한 후 **적용**을 클릭하여 변경사항을 저장하거나 **취소**를 클릭하여 변경사항을 취소합니다.

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

17. 왼쪽 창에서 **iDRAC 설정 → 사용자 목록**을 선택합니다. 사용자 목록 정보를 프로필에 포함하려면 **이 하드웨어 프로필에 사용자 목록 포함** 확인란을 선택합니다. iDRAC 로컬 사용자 목록에서 다음 중 하나를 수행합니다.

a. **사용자 추가**: iDRAC 사용자 및 필요한 정보를 수동으로 입력합니다. 입력을 마치면 **저장**을 클릭하여 변경사항을 저장하거나 **취소**를 클릭하여 변경사항을 취소합니다.

b. **사용자 삭제**: 선택한 사용자를 삭제합니다. 해당 사용자의 확인란을 선택하고 **삭제**를 클릭하거나 **취소**를 클릭하여 취소합니다.
c. **사용자 편집**: iDRAC 사용자 정보를 수동으로 편집합니다. 편집을 마치면 **저장**을 클릭하여 변경사항을 저장하거나 **취소**를 클릭하여 취소합니다.

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

18. 왼쪽 창에서 **RAID 구성**을 선택합니다. RAID 구성 정보를 프로필에 포함하려면 **이 하드웨어 프로필에 RAID 구성 포함** 확인란을 선택합니다. 다음 중 하나를 선택합니다.

- RAID1 적용 및 전용 핫 스페어 생성(해당되는 경우).
  대상 서버에 기본 RAID 구성 설정을 적용하려면 이 옵션을 선택합니다. RAID 구성 작업은 RAID1 사용 가능한 통합 컨트롤러의 처음 두 개 드라이브에서 RAID1로 기본 설정됩니다. 또한 후보 드라이브가 기존 기준을 충족하는 경우 RAID1 어레이의 전용 핫 스페어가 생성됩니다.
- 참조 서버에서 RAID 구성 클론.
  참조 서버 설정을 클론하려면 이 옵션을 사용합니다.

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

참조 서버에서 CSIOR 사용

참조 서버를 사용하여 하드웨어 프로필을 생성하기 전에 CSIOR(Collect System Inventory On Reboot) 설정이 사용 가능 상태여야 하며 다시 부팅해야 정확한 인벤토리 및 구성 정보를 제공할 수 있습니다. 두 가지 방법으로 CSIOR을 사용할 수 있습니다.

로컬	Dell Lifecycle Controller USC(United Server Configurator) 사용자 인터페이스를 사용하는 개별 호스트를 사용합니다.
원격	WS-Man 스크립트를 사용합니다. 이 기능 스크립에 대한 자세한 내용은 *Dell 기술 센터* 및 *DCIM Lifecycle Controller 관리 프로필*을 참조하십시오.

참조 서버에서 CSIOR을 로컬로 사용하려면 다음을 수행합니다.

1. 시스템의 전원을 켜고 POST 중에 **<F10>** 키를 눌러 USC를 실행합니다.
2. **하드웨어 구성 → 부품 교체 구성**을 선택합니다.
3. **다시 부팅할 때 시스템 인벤토리 수집**을 사용 가능으로 설정하고 USC를 종료합니다.

하드웨어 프로필 복제

새 하드웨어 프로필을 복제하려면 다음을 수행합니다.

1. Dell Management Center에서 **배포 → 배포 템플릿 → 하드웨어 프로필**을 선택합니다.
2. **새로 생성**을 클릭합니다.
3. **새 하드웨어 프로필** 페이지에서 다음을 수행합니다.
   - **프로필 이름** 텍스트 상자에서 프로필 이름을 입력합니다.
   - **Description(설명)** 텍스트 상자에서 선택적 설명을 입력합니다.
4. **Save(저장)**를 클릭합니다.
5. 왼쪽 창에서 **참조 서버**를 클릭합니다.
6. **참조 서버** 창에서 **편집**을 클릭합니다.
7. 참조 서버에서 모든 하드웨어 설정을 추출하려면 **사본 참조 서버 설정** 옵션 단추를 클릭합니다.
8. **저장**을 클릭합니다.
9. 설정을 추출하는 데 몇 분 정도 소요된다는 내용의 대화상자가 표시되면 **계속**을 클릭합니다. 설정이 채워지고 선택한 서버의 이름, iDRAC IP 주소 및 서비스 태그가 참조 서버 창에 표시됩니다.

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

하드웨어 프로필 관리 정보

하드웨어 프로필은 참조 서버를 사용하여 서버의 하드웨어 구성을 정의합니다. 다음과 같은 작업을 비롯하여 Dell Management Center에서 기존 하드웨어에 몇 가지 관리 작업을 수행할 수 있습니다.

- 하드웨어 프로필 보기 또는 편집
- 하드웨어 프로필 복제
- 하드웨어 프로필 이름 바꾸기
- 하드웨어 프로필 삭제
- 하드웨어 프로필 새로 고치기

하드웨어 프로필 보기 또는 편집

하드웨어 프로필을 보거나 편집하려면 다음을 수행합니다.

1. Dell Management Center에서 **배포** → **배포 템플릿** → **하드웨어 프로필**을 선택합니다.
2. 프로필을 선택하고 **보기/편집**을 클릭합니다.
3. **하드웨어 프로필** 창에서 변경을 수행하고 **편집**을 클릭합니다.
4. **저장**을 클릭하여 변경사항을 적용하거나 **취소**를 클릭하여 변경사항을 취소합니다.

하드웨어 프로필 복제

하드웨어 프로필을 복제하려면 다음을 수행합니다.

1. Dell Management Center에서 **배포** → **배포 템플릿** → **하드웨어 프로필**을 선택합니다.
2. **하드웨어 프로필** 페이지에서 프로필을 선택하고 **복제**를 클릭합니다.
3. **복제** 대화상자에서 고유한 하드웨어 프로필 이름을 입력합니다.
4. **적용**을 클릭하여 새 이름으로 프로필 사본을 작성하거나 **취소**를 클릭하여 취소합니다.

하드웨어 프로필 이름 바꾸기

하드웨어 프로필의 이름을 바꾸려면 다음을 수행합니다.

1. Dell Management Center에서 **배포** → **배포 템플릿** → **하드웨어 프로필**을 선택합니다.
2. **하드웨어 프로필** 페이지에서 프로필을 선택하고 **이름 바꾸기**를 클릭합니다.
3. **이름 바꾸기** 대화상자에서 고유한 하드웨어 프로필 이름을 입력합니다.
4. **적용**을 클릭하여 새 이름을 사용하거나 **취소**를 클릭하여 취소합니다.

하드웨어 프로필 삭제

하드웨어 프로필을 삭제하려면 다음을 수행합니다.

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

1. Dell Management Center에서 **배포** → **배포 템플릿** → **하드웨어 프로필**을 선택합니다.
2. 프로필을 선택하고 **삭제**를 클릭합니다.
3. 메시지 대화상자에서 프로필을 제거하려면 **삭제**를 클릭하거나 **취소**를 클릭하여 취소합니다.

업데이트된 하드웨어 프로필 새로 고침

업데이트된 하드웨어 프로필을 새로 고치려면 다음을 수행합니다.

1. Dell Management Center에서 **배포 → 배포 템플릿 → 하드웨어 프로필**을 선택합니다.
2. **새로 고침**을 클릭합니다.
   업데이트된 하드웨어 프로필 정보가 표시됩니다.

새 하이퍼바이저 프로필 생성

ESX/ESXi를 서버에 배포하여 구성하려면 하이퍼바이저 프로필을 생성해야 합니다. 하이퍼바이저 프로필에는 다음과 같은 정보가 필요합니다.

- NFS 또는 CIFS 공유의 스크립트 가능한 참조 ISO 소프트웨어 매체 위치
- 배포된 호스트를 관리하는 vCenter 인스턴스와 선택적 호스트 프로필
- 플러그인이 vCenter의 서버를 배포하는 대상 클러스터 또는 데이터센터

노트: 참조 ISO 파일 이름에 다음 명명 규칙 중 하나를 사용합니다.

```
NFS format: host:/share/hypervisor_image.iso

CIFS format: \\host\share\hypervisor.iso
```

노트: 성공적으로 배포하려면 올바른 드라이버가 있는 ESX ISO가 필요합니다. 최신 Dell 시스템에서 배포하려면 모든 필수 Dell 드라이버가 있는 Dell 사용자 지정 ISO 이미지를 사용해야 합니다. ESX 4.1은 최신 Dell 시스템에서 작동되지 않을 수 있으며 Dell에서 제공하는 사용자 지정 ISO가 없을 수 있습니다.

새 하이퍼바이저 프로필을 생성하려면 다음을 수행합니다.

1. **Dell Management Center**에서 **배포 → 배포 템플릿 → 하이퍼바이저 프로필**을 선택합니다.
2. **하이퍼바이저 프로필** 페이지에서 **새로 생성**을 클릭합니다.
3. **새 하이퍼바이저 프로필** 페이지에서 다음을 수행합니다.
   - **프로필 이름** 텍스트 상자에서 프로필 이름을 입력합니다.
   - **Description(설명)** 텍스트 상자에서 선택적 설명을 입력합니다.
4. 왼쪽 창에서 **참조 ISO**를 클릭한 다음 **편집**을 클릭하고 **하이퍼바이저 설치 소스** 대화상자에서 다음 정보를 입력합니다.
   - **설치 소스 ISO** 텍스트 상자에서 하이퍼바이저 공유 위치의 경로를 입력합니다. 이 하이퍼바이저 이미지의 사본이 수정되어 스크립트된 설치를 허용합니다. 참조 ISO 위치는 다음 형식 중 하나여야 합니다.
     NFS 형식: host:/share/hypervisor_image.iso
     CIFS 형식: ₩₩host₩share₩hypervisor.iso
   - **버전 선택** 드롭다운 목록에서 ESX 또는 ESXi 버전을 선택합니다.

   하이퍼바이저 프로필을 사용하여 배포된 모든 서버에는 이 이미지가 있으며 서버가 12G 이전 버전일 경우 권장되는 최신 버전의 OpenManage Server Administrator가 설치됩니다.
5. CIFS 공유를 사용하는 경우 **사용자 이름**, **암호** 및 **암호 확인**을 입력합니다. 이 두 암호는 서로 일치해야 합니다.
6. 설정을 프로필에 추가하려면 **저장**을 클릭합니다.
7. 왼쪽 창에서, **vCenter 설정**을 클릭하고 필요에 따라 편집합니다.
   - **vCenter 인스턴스**: 배포 후에 호스트를 관리하는 서버 인스턴스를 표시합니다.
   - **vCenter 버전**: 현재 버전을 표시합니다.

- **vCenter 대상 컨테이너**: 새 실제 서버를 호스트하는 데이터센터 또는 클러스터. **찾아보기**를 클릭하여 vCenter 대상을 검색합니다.
- **vCenter 호스트 프로필**: 호스트 구성을 캡슐화하고 호스트 구성을 관리하는 데 유용한 프로필을 선택합니다.

8. 정보를 프로필에 추가하려면 **저장**을 클릭합니다.

하이퍼바이저 프로필 관리에 대한 자세한 내용은 하이퍼바이저 프로필 관리를 참조하십시오.

하이퍼바이저 프로필 관리

기존 하이퍼바이저 프로필에서 다음을 비롯하여 몇 가지 관리 조치를 수행할 수 있습니다.

- VLAN 지원 이해
- 하이퍼바이저 프로필 보기 또는 편집
- 하이퍼바이저 프로필 복제
- 하이퍼바이저 프로필 이름 바꾸기
- 하이퍼바이저 프로필 삭제
- 하이퍼바이저 프로필 새로 고치기

VLAN 지원

OpenManage Integration for VMware vCenter을 사용하면 라우트 가능한 VLAN에 하이퍼바이저를 배포할 수 있습니다. 배포 마법사에서 VLAN 지원을 구성하십시오. 배포 마법사의 이 단계에서는 VLAN 사용 및 VLAN ID를 지정할 수 있는 옵션이 있습니다. VLAN ID가 제공되면 이 ID는 배포 중에 하이퍼바이저의 관리 인터페이스에 적용되며 VLAN ID를 사용하는 모든 트래픽을 태그 지정합니다.

배포 중에 제공된 VLAN이 가상 어플라이언스 및 vCenter 서버와 통신하도록 해야 합니다. 이러한 대상 중 하나 또는 둘 다에 통신할 수 없는 VLAN에 하이퍼바이저를 배포하면 배포에 실패합니다.

단일 배포 작업에서 여러 개의 베어 메탈 서버를 선택하고 동일한 VLAN ID를 모든 서버에 적용하려면, 배포 마법사의 서버 식별 단계에서 기본 설정 아래 있는 *선택된 모든 서버에 설정 적용* 단추를 사용하십시오. 이 옵션을 사용하면 동일한 VLAN ID를 다른 네트워크 설정과 함께 배포 작업의 모든 서버에 적용할 수 있습니다.

노트: OpenManage Integration for VMware vCenter은 멀티홈 구성을 지원하지 않습니다. 보조 네트워크와의 통신을 위해 어플라이언스에 보조 네트워크 인터페이스를 추가하면 하이퍼바이저 배포, 서버 준수 및 펌웨어 업데이트와 관련된 워크플로에 문제가 발생합니다.

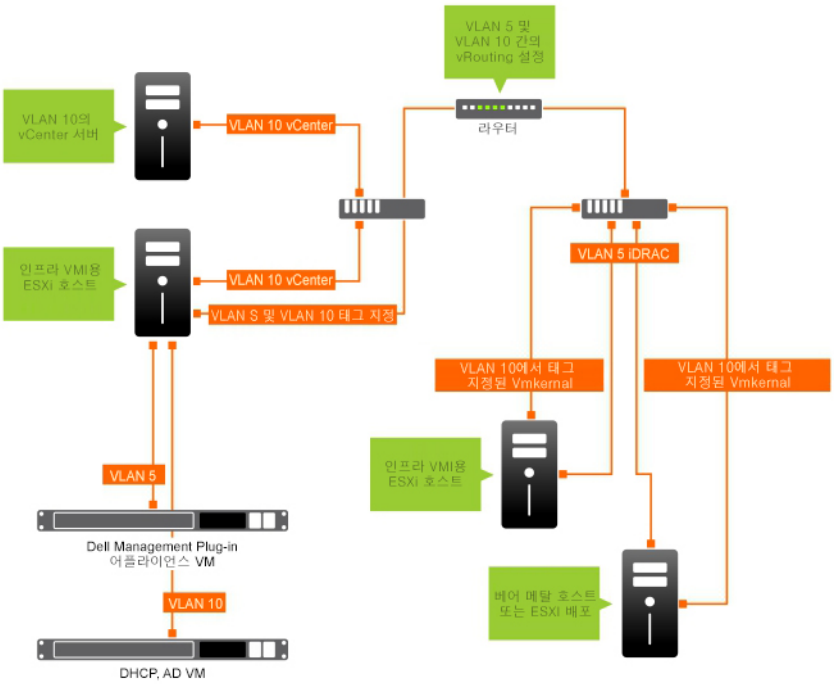

그림 4. VLAN 네트워크 예.

예로 제시된 이 네트워크에서는 OpenManage Integration for VMware vCenter이 VLAN 5에 있고 배포되는 ESXi 호스트의 vCenter 및 VMkernal은 VLAN 10에 있습니다. OpenManage Integration for VMware vCenter은 멀티 VLAN 홈을 지원하지 않으므로, 모든 시스템에 대해 VLAN 5가 VLAN 10에 라우팅해야 상호 올바르게 통신할 수 있습니다. VLAN 간에 라우팅이 활성화되어 있지 않으면 배포에 실패합니다.

하이퍼바이저 프로필 보기 또는 편집

하이퍼바이저 프로필을 보거나 편집하려면 다음을 수행합니다.

1. Dell Management Center에서 **배포 → 배포 템플릿 → 하이퍼바이저 프로필** 창을 선택합니다.
2. 프로필을 선택하고 **보기/편집**을 클릭합니다.
3. **하이퍼바이저 프로필: 프로필 이름** 창에서 표시하거나 변경할 프로필 섹션을 선택하고 필요에 따라 변경합니다.
4. **저장**을 클릭하여 변경사항을 적용하거나 **취소**를 클릭하여 변경사항을 취소합니다.

하이퍼바이저 프로필 복제

하이퍼바이저 프로필을 복제하려면 다음을 수행합니다.

1. Dell Management Center에서 **배포 → 배포 템플릿 → 하이퍼바이저 프로필**을 선택합니다.
2. **하이퍼바이저 프로필** 페이지에서 프로필을 선택하고 **복제**를 클릭합니다.
3. **복제** 대화상자에서 고유한 하이퍼바이저 프로필 이름을 입력합니다.
4. **적용**을 클릭하여 새 이름으로 프로필 사본을 작성하거나 **취소**를 클릭하여 취소합니다.

하이퍼바이저 프로필 이름 바꾸기

하이퍼바이저 프로필의 이름을 바꾸려면 다음을 수행합니다.

1. Dell Management Center에서 **배포 → 배포 템플릿 → 하이퍼바이저 프로필**을 선택합니다.
2. **하이퍼바이저 프로필** 페이지에서 프로필을 선택하고 **이름 바꾸기**를 클릭합니다.
3. **이름 바꾸기** 대화상자에서 고유한 하이퍼바이저 프로필 이름을 입력합니다.
4. **적용**을 클릭하여 새 이름을 사용하거나 **취소**를 클릭하여 취소합니다.

하이퍼바이저 프로필 삭제

하이퍼바이저 프로필을 삭제하려면 다음을 수행합니다.

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

1. Dell Management Center에서 **배포 → 배포 템플릿 → 하이퍼바이저 프로필**을 선택합니다.
2. 프로필을 선택하고 **삭제**를 클릭합니다.
3. 메시지 대화상자에서 **삭제**를 클릭하여 프로필을 제거하거나 **취소**를 클릭하여 취소합니다.

하이퍼바이저 프로필 새로 고치기

업데이트된 하이퍼바이저 프로필을 새로 고치려면 다음을 수행합니다.

1. Dell Management Center에서 **배포 → 배포 템플릿 → 하이퍼바이저 프로필**을 선택합니다.
2. **새로 고침**을 클릭합니다.
   업데이트된 하이퍼바이저 프로필 정보가 표시됩니다.

새 배포 템플릿 작성

배포 템플릿에는 하드웨어 프로필, 하이퍼바이저 프로필 또는 둘 다 들어 있습니다. 배포 마법사에서 이 템플릿을 사용하여 서버 하드웨어를 프로비저닝하고 vCenter 내에 호스트를 배포합니다.

새 배포 템플릿을 작성하려면 다음을 수행합니다.

1. Dell Management Center에서 **배포 → 배포 템플릿**을 선택합니다.
2. **사용 가능한 프로필**에서 **새로 생성**을 클릭합니다.
3. **새로 생성** 창에서 템플릿 이름을 입력하고 **저장**을 클릭합니다.
4. 템플릿을 완료하려면 **편집**을 클릭합니다.
5. 왼쪽 창의 **프로필** 드롭다운 목록에서 프로필을 선택하고 다음 중 하나를 수행합니다.
   - 선택한 프로필에 대한 하드웨어/하이퍼바이저 프로필 설정을 표시하려면 **보기**를 클릭합니다.
   - 새 하드웨어/하이퍼바이저 프로필을 생성하려면 **새로 생성**을 클릭합니다.
6. 템플릿 관리에 도움이 되는 배포 템플릿에 대한 선택적 **설명**을 입력합니다.
7. 프로필 선택 항목을 적용하고 변경사항을 저장하려면 **저장**을 클릭합니다. 취소하려면 **취소**를 클릭합니다.

배포 템플릿 관리

Dell Management Center를 통해 기존 배포 템플릿에서 다음을 비롯한 몇 가지 관리 작업을 수행할 수 있습니다.

- 배포 템플릿 작성

- 배포 템플릿 복제
- 배포 템플릿 이름 바꾸기
- 배포 템플릿 삭제

배포 템플릿 복제
배포 템플릿을 복제하려면 다음을 수행합니다.

1. Dell Management Center에서 **배포** → **배포 템플릿**을 선택합니다.
2. 배포 템플릿 페이지에서 템플릿을 선택하고 **복제**를 클릭합니다.
3. 템플릿의 새 이름을 입력하고 **적용**을 클릭합니다. 템플릿의 이름은 고유해야 합니다.

배포 템플릿 삭제
배포 템플릿을 삭제하려면 다음을 수행합니다.

1. Dell Management Center에서 **배포** → **배포 템플릿**을 선택합니다.
2. **배포 템플릿** 페이지에서 템플릿을 선택하고 **삭제**를 클릭합니다.
3. 메시지 상자에서 **삭제**를 클릭하여 템플릿을 삭제하거나 **취소**를 클릭하여 취소합니다.

배포 템플릿 이름 바꾸기
배포 템플릿의 이름을 바꾸려면 다음을 수행합니다.

1. Dell Management Center에서 **배포** → **배포 템플릿**을 선택합니다.
2. **배포 템플릿** 페이지에서 템플릿을 선택하고 **이름 바꾸기**를 클릭합니다.
3. 템플릿의 새 이름을 입력하고 **적용**을 클릭합니다. 템플릿의 이름은 고유해야 합니다.
4. 업데이트된 모든 배포 템플릿을 표시하려면 **Dell Management Center**에서 **배포** → **배포 템플릿**을 선택하고 **새로 고침**을 클릭합니다.

배포 마법사 실행

배포 마법사는 운영 체제 미설치 서버 배포 프로세스를 단계별로 안내합니다.

- 배포되지 않은 서버 선택.
  하이퍼바이저를 배포할 때 최소 1GB의 저장소로 내부 이중 SD 모듈에 배포할 수 있습니다. 내부 이중 SD 모듈을 BIOS에서 사용 가능으로 설정해야 OpenManage Integration for VMware vCenter을 통해 하이퍼바이저를 배포할 수 있습니다.
- 배포 템플릿 사용(하드웨어 및 하이퍼바이저 프로필 조합).
- 전역 설정. 이 페이지에서 하이퍼바이저를 하드 디스크 또는 내부 이중 SD 모듈에 배포할 수 있습니다.
- 배포된 서버에 식별 할당.
- 원하는 연결 프로필을 각 서버에 일치.
- 서버 배포 작업 실행 예약.
- 배포 작업을 관리할 수 있는 작업 큐 표시.

노트: 하드웨어 프로필만 배포하는 경우 새 전역 설정, 서버 식별 및 연결 프로필 페이지를 건너뛰고 작업 예약 페이지로 이동됩니다.

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

관련 작업:

- 배포 마법사 1단계: 서버 선택
- 배포 마법사 2단계: 배포 템플릿

- 배포 마법사 3단계: 전역 설정
- 배포 마법사 4단계: 서버 식별
- 배포 마법사 5단계: 연결 프로필
- 배포 마법사 6단계: 작업 예약

배포 마법사 - 단계 1: 서버 선택

이 페이지는 서버 배포에 대한 내용을 다룹니다. 내부 이중 SD 모듈에 하이퍼바이저를 배포하는 경우, 이 페이지에는 해당 옵션 사용 가능 여부가 표시됩니다. 내부 이중 SD 모듈에 대한 자세한 내용은 배포 마법사 실행을 참조하십시오. 배포할 서버가 단계 2의 목록에 표시되지 않으면 이 단계의 목록에 표시되도록 수동으로 추가할 수 있습니다. 수동으로 서버 추가를 참조하십시오.
서버를 선택하려면 다음을 수행합니다.

1. **Dell Management Center**에서 **배포** → **배포 마법사**를 선택합니다.
2. 배포되지 않은 서버를 이 배포 작업에 할당하려면 **서버 선택** 창에서 확인란을 사용하여 **서버**를 선택합니다.
3. **다음**을 클릭합니다.

단계 2 작업을 계속 진행하려면 배포 마법사 단계 2를 클릭합니다.

배포 마법사 단계 2: 배포 템플릿

하드웨어 프로필 배포와 하이퍼바이저 배포에는 차이점이 있습니다. 하드웨어 프로필을 배포하는 경우 배포 마법사 단계 6을 클릭합니다.

노트: 성공적으로 배포하려면 올바른 드라이버가 있는 ESX ISO가 필요합니다. 최신 Dell 시스템에서 배포하려면 모든 필수 Dell 드라이버가 있는 Dell 사용자 지정 ISO 이미지를 사용해야 합니다. ESX 4.1은 최신 Dell 시스템에서 작동되지 않을 수 있으며 Dell에서 제공하는 사용자 지정 ISO가 없을 수 있습니다.

배포 템플릿을 선택하려면 다음을 수행합니다.

1. 배포 템플릿은 몇 가지 방법 중 하나로 배포 템플릿을 선택하거나 생성합니다.
   - **사용 가능한 템플릿** 아래에서 기존 배포 템플릿을 선택합니다. 선택한 템플릿의 정보가 오른쪽 창에 채워집니다.
   - 기존 배포 템플릿을 선택하고 **편집**을 클릭하여 연결된 프로필 중 하나 또는 둘 다 변경합니다.
   - **새로 생성**을 클릭하여 새 템플릿을 정의합니다.
2. 다음 중 하나를 선택합니다.
   - 하드웨어 프로필을 배포하는 경우 **다음**을 클릭하여 배포 마법사 단계 6으로 이동합니다.
   - 하이퍼바이저 프로필을 배포하는 경우 **다음**을 클릭하여 배포 마법사 단계 3으로 갑니다.

배포 마법사 3단계: 전역 설정

하이퍼바이저를 하드 드라이브 또는 내부 이중 SD 모듈에 배포할 수 있습니다. 내부 이중 SD 모듈을 최소 하나 이상의 선택된 서버에서 사용할 수 있는 경우 **내부 이중 SD 모듈** 옵션은 기본적으로 활성화되어 있습니다. 그렇지 않은 경우, **하드 디스크** 및 **내부 이중 SD 모듈** 옵션이 모두 선택되지 않습니다.
하이퍼바이저를 배포하려면 다음 단계를 수행하십시오:

1. 글로벌 설정 페이지에서 다음 옵션 중 하나를 선택합니다.
   - **하드 디스크** - 하드 디스크 드라이브에 하이퍼바이저를 배포합니다.
   - **내부 이중 SD 모듈** - 내부 이중 SD 모듈에 하이퍼바이저를 배포합니다.
2. 선택된 서버 중 하나라도 내부 이중 SD 모듈을 지원하지 않거나 배포 중에 내부 이중 SD 모듈이 없는 경우 다음 작업 중 하나를 수행합니다:

- 하이퍼바이저를 서버의 첫 번째 하드 디스크에 배포할 경우 **사용 가능한 내부 이중 SD 모듈이 없는 서버의 첫 번째 하드 디스크에 하이퍼바이저 배포** 확인란을 선택합니다.

  주의: 이 옵션을 선택해 서버의 첫 번째 하드 디스크에 하이퍼바이저를 배포하면, 디스크 드라이브의 모든 데이터가 지워집니다.

- 해당 서버에서의 배포를 건너뛰려면 **사용 가능한 내부 이중 SD 모듈이 없는 서버의 첫 번째 하드 디스크에 하이퍼바이저 배포** 확인란을 선택해 다음 서버에서 하이퍼바이저 배포를 수행할 수 있습니다.

3. **Next(다음)**를 클릭합니다.

   단계 4 작업을 계속 진행하려면 배포 마법사 단계 4: 서버 식별을 클릭합니다.

배포 마법사 단계 4: 서버 식별

서버 식별은 두 가지 방법으로 제공할 수 있습니다.

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

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

이 화면은 VLAN ID를 지정하는 옵션을 제공합니다. VLAN ID가 제공되면 배포 중에 하이퍼바이저의 관리 인터페이스에 적용되며 모든 트래픽이 VLAN ID로 태그 지정됩니다.
서버를 식별하려면 다음을 수행합니다.

1. 서버 식별은 배포된 서버에 새 이름과 네트워크 식별을 할당합니다. 펌웨어 또는 BIOS의 최소 요구사항을 충족하지 않거나 기타 문제가 있는 서버의 목록을 표시하려면 **비준수 서버**를 클릭합니다.
2. 추가 정보를 보려면 **상세정보**를 클릭합니다.
3. 시스템이 업데이트되면 **준수 확인**을 클릭하여 다시 테스트하고 수정 사항을 확인합니다. 목록을 새로 고치려면 **새로 고침**을 클릭하고 테스트를 취소하려면 **모든 테스트 중단**을 클릭합니다.
4. ^를 클릭하여 개별 서버 정보를 펼쳐서 봅니다.
5. **호스트 이름 및 NIC**에서 서버의 **정규화된 호스트 이름**을 입력합니다.
6. **NIC 관리 작업** 드롭다운 목록에서 서버를 관리하는 데 사용할 NIC를 선택합니다.
7. **IP 주소, 서브넷 마스크** 및 기타 네트워크 정보를 입력하거나 **DHCP를 사용하여 가져오기** 확인란을 선택합니다.
8. VLAN ID가 필요한 네트워크에 배포하는 경우, VLAN 확인란을 선택한 다음 VLAN ID를 입력합니다.

   VLAN ID에 1 - 4094 범위의 숫자를 사용합니다. VLAN ID 0은 프레임 우선순위를 태그 지정하도록 예약되어 있습니다.
9. 배포할 모든 서버에 이 단계를 반복하거나 **선택한 모든 서버에 설정 적용** 확인란을 선택합니다.
10. **Next**(다음)를 클릭합니다.

    단계 5 작업을 계속 진행하려면 배포 마법사 단계 5를 클릭합니다.

배포 마법사 단계 5: 연결 프로필

연결 프로필은 호스트의 연결 자격 증명을 iDRAC 또는 호스트 루트 자격 증명과 연결하여 설정하는 데 사용됩니다. 연결 프로필 창에서 다음과 같은 작업을 수행할 수 있습니다.

- 현재 연결 프로필 표시 또는 편집
- 현재 연결 프로필 삭제
- vCenter 호스트 변경사항을 반영하도록 연결 프로필 새로 고침

연결 프로필을 생성하려면 다음을 수행합니다.

1. 연결 프로필은 배포 작업이 완료된 후 연결 프로필에 서버를 자동으로 할당합니다.
   연결 프로필을 선택한 후 **다음**을 클릭합니다.
2. **동일한 연결 프로필에 모든 서버 할당** 옵션 단추를 선택하고 기존의 동일한 프로필에 모든 서버를 할당할 연결 프로필을 드롭다운 목록에서 선택합니다.
3. 새 프로필을 생성하려면 **새로 생성**을 클릭하고 선택한 프로필을 보거나 편집하려면 **보기/편집**을 클릭합니다.
4. 선택한 연결 프로필 설정을 표시하려면 **보기**를 클릭합니다.
5. **각 서버의 연결 프로필 선택** 옵션 단추를 선택한 후 드롭다운 목록에서 각 서버의 개별 연결 프로필을 선택합니다.
6. 연결 프로필을 선택한 후 **다음**을 클릭합니다.
   단계 6 작업을 계속 진행하려면 배포 마법사 단계 6을 클릭합니다.

배포 마법사 단계 6: 작업 예약

예약 작업에서는 배포 작업 일정을 설정합니다. 배포 작업 실행에 사용할 수 있는 옵션에는 즉시, 선택한 날짜 및 시간에 배포 작업이 실행되도록 예약, 배포 작업을 보류하고 수동으로 시작 등이 있습니다.

스케줄을 설정하려면 다음을 수행합니다.

1. 날짜 및 시간을 입력하여 배포 작업을 실행할 시기를 결정합니다.
   a. **서버 배포 예약**을 클릭합니다.
   b. 캘린더 제어를 사용하여 날짜를 선택합니다.
   c. 시간을 입력합니다.
      - 즉시: **지금 서버 배포**를 클릭합니다.
      - 작업 연기: **배포 작업 생성**을 클릭합니다.
      - 보류: 이 옵션을 사용하면 스케줄을 수정할 수만 있고 기타 모든 배포 작업 옵션을 변경할 수 없습니다.
2. **작업 이름** 및 **작업 설명** 을 입력합니다.
3. **마침**을 클릭합니다.
4. 이제 배포 마법사가 완료되고 **작업 큐**를 사용하여 배포 작업을 관리할 수 있습니다.
5. 펌웨어 업데이트가 있어야 마법사를 완료할 수 있는 비준수 서버 목록을 표시하려면 **비준수 서버**를 클릭합니다.

관련 작업:

- 배포 작업 큐를 사용하여 배포 작업 관리

작업 큐 이해

작업 큐는 다음과 같은 서버 배포 및 인벤토리 검색 작업을 관리합니다.

- 제출된 서버 배포 작업 표시
- 배포 작업 또는 인벤토리/보증 내역 큐 새로 고치기
- 현재 vCenter에 있는 Dell 서버 특성을 업데이트할 인벤토리 작업 예약
- 배포 작업 큐 항목 제거

- 클러스터 및 데이터베이스용 펌웨어 업데이트 관리

노트: 인벤토리/보증에 최신 정보가 포함되도록 하려면 인벤토리/보증 작업이 최소 1주일에 한 번 실행되도록 예약하십시오. 인벤토리/보증 작업은 최소한의 리소스를 사용하며 호스트 성능을 저하시키지 않습니다.

이 페이지에 있는 작업은 다음과 같습니다.

- 배포 작업 큐를 사용하여 배포 작업 관리
- 인벤토리 작업 실행
- 인벤토리 작업 스케줄 수정
- 클러스터 및 데이터센터용 펌웨어 업데이트 상태 보기

배포 작업 큐를 사용하여 배포 작업 관리

배포 작업 큐를 사용하여 배포 작업을 관리하려면 다음을 수행합니다.

1. Dell Management Center에서 **작업 큐** → **배포 작업**을 선택합니다.
2. **배포 작업 상세정보**를 업데이트하려면 **새로 고침**을 클릭합니다.
3. 배포 작업에 포함된 서버의 자세한 정보가 있는 배포 작업 상세정보 대화상자를 표시하려면 **상세정보**를 클릭합니다. 이 대화상자에는 다음과 같은 세부사항이 표시됩니다.
   - 서비스 태그
   - iDRAC IP 주소
   - 서버 상태
   - 경고 발생 여부
   - 배포 작업 세부사항
   - 시작 및 종료 시간

   대화상자의 표에 있는 각 항목에 대한 전체 정보를 표시하려면 항목 위에 마우스를 올려 놓습니다. 그러면 추가 텍스트 팝업이 표시됩니다.
4. 선택한 작업을 보류하거나 업데이트된 일정을 입력하려면 **수정**을 클릭합니다.
5. 배포 작업을 중단하려면 **중단**을 클릭합니다.
6. 메시지가 표시되면 **작업 중단**을 클릭하여 중단하거나 **작업 중단하지 않음**을 클릭하여 취소합니다.

   노트: 진행 중인 배포 작업은 중단할 수 없습니다.
7. 배포 작업 큐 제거 창을 표시하려면 **작업 큐 제거**를 클릭합니다. **다음 기간 이후 및 작업 상태**를 선택하고 **적용**을 클릭합니다. 선택한 작업이 큐에서 지워집니다.

수동으로 서버 추가

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

1. Dell Management Center의 **배포**에서 **배포 마법사**를 클릭합니다.
2. **서버 선택** 탭에서 **서버 추가**를 클릭합니다.
3. **서버 추가** 대화상자에서 다음을 수행합니다.
   a. **iDRAC IP 주소** 텍스트 상자에서 iDRAC IP 주소를 입력합니다.
   b. **사용자 이름** 텍스트 상자에서 사용자 이름을 입력합니다.
   c. **암호** 텍스트 상자에 암호를 입력합니다.
4. **서버 추가**를 클릭합니다. 작업이 완료되는 데 몇 분 정도 걸릴 수 있습니다.

운영 체제 미설치 서버 제거

자동으로 검색되거나 수동으로 추가된 서버를 수동으로 제거할 수 있습니다.

1. Dell Management Center의 **Deployment(배포)**에서 **Deployment Wizard(배포 마법사)**를 클릭합니다.
2. **서버 선택** 탭에서 **서버 제거**를 클릭합니다.
3. **서버 제거** 대화상자에서 제거할 서버의 확인란을 선택합니다.
4. **선택한 서버 제거**를 클릭합니다.
5. **서버 선택** 탭에서 표에 나열된 서버를 보고 제거되었는지 확인합니다.

6

콘솔 관리

OpenManage Integration for VMware vCenter 및 가상 환경은 두 개의 추가 관리 포털을 사용하여 관리할 수 있습니다.

- 웹기반 Administration Console
- 개별 서버의 콘솔 보기(어플라이언스 가상 시스템 콘솔)

이 두 포털을 사용하여 vCenter 관리, OpenManage Integration for VMware vCenter 데이터베이스 백업 및 복원, 다시 설정/다시 시작 조치를 위한 전역 설정을 입력하고 모든 vCenter 인스턴스에서 사용할 수 있습니다.

웹기반 Administration Console

웹 기반 Administration Console은 vCenter 서버 등록 및 관리, 가상 어플라이언스 관리, 전역 vCenter 경고 설정 및 백업/복원 설정 등과 같은 몇 가지 주요 기능을 제공합니다.

vCenter 서버 연결 관리

Administration Console의 vCenter Registration(vCenter 등록) 창에서 vCenter 서버를 등록하고, 라이센스를 업로드하거나 구입할 수 있습니다. 데모 라이센스를 사용하는 경우 **Buy Now(지금 구입)** 링크가 표시되므로 여러 개의 호스트를 관리할 수 있는 전체 버전의 라이센스를 구입할 수 있습니다. 이 섹션에서 서버를 수정, 업데이트 및 등록 취소할 수도 있습니다.

관련 작업:

- vCenter 서버 등록
  - 관리자 vCenter 로그인 수정
  - 등록된 vCenter의 SSL 인증서 업데이트
  - vCenter에서 OpenManage Integration for VMware vCenter 제거
- Administration Console을 사용하여 OpenManage Integration for VMware vCenter 라이센스 업로드

vCenter 서버 등록

OpenManage Integration for VMware vCenter가 설치된 후에 OpenManage Integration for VMware vCenter를 등록할 수 있습니다. OpenManage Integration for VMware vCenter는 vCenter 작업에 관리자 계정을 사용합니다. OpenManage Integration for VMware vCenter에서는 어플라이언스당 10개의 vCenter를 지원합니다.

1. OpenManage Integration for VMware vCenter의 Summary(요약) 탭에서 링크를 사용해 Administration Console을 엽니다.
2. Login(로그인) 대화상자에 암호를 입력합니다.
3. 새 서버를 등록하려면 **VCENTER REGISTRATION(VCENTER 등록)**을 클릭한 다음 **Register New vCenter Server(새 vCenter 서버 등록)**를 클릭합니다.
4. **Register a New vCenter(새 vCenter 등록)** 대화상자의 **vCenter Name(vCenter 이름)** 아래에서 다음을 수행합니다.

a. **vCenter Server IP or Hostname(vCenter 서버 IP 또는 호스트 이름)** 텍스트 상자에 vCenter IP 주소 또는 호스트 이름 또는 FQDN을 입력합니다.
b. **Description(설명)** 텍스트 상자에서 선택적 설명을 입력합니다.

5. **Admin User Account(관리자 계정)** 아래에서 다음을 수행합니다.
   a. **Admin User Name(관리자 이름)** 텍스트 상자에서 관리자 이름을 입력합니다.
   b. **Password(암호)** 텍스트 상자에 암호를 입력합니다.
   c. **Verify Password(암호 확인)** 텍스트 상자에서 암호를 다시 입력합니다.
6. **Register(등록)**를 클릭합니다.

OpenManage Integration for VMware vCenter 요구사항

릴리스 2.2에 지원되는 vSphere 버전

OpenManage Integration for VMware vCenter(OMIVV)에는 이전 세대의 서버에 있는 OpenManage의 정보가 필요하며, 최신 플랫폼은 최신 칩셋을 인식하는 vSphere 버전에서만 시작됩니다. 이로 인해 지정된 OMIVV 버전이 작동되는 vSphere 버전이 제한되어 있습니다.

버전 2.2의 경우, 이전 플랫폼에서 지원되는 vSphere 버전은 다음과 같습니다.

ESX/ESXi 버전 지원

v4.1 (ESX/ESXi)

v4.1 U1 (ESX/ESXi)

v4.1 U2 (ESX/ESXi)

v4.1 U3 (ESX/ESXi)

v5.0

v5.0 U1

v5.0 U2

v5.0 U3

v5.1

v5.1 U1

v5.1 U2

v5.5

vSphere v5.5 U1 지원

현재, v5.5 U1 지원은 Lifecycle Controller 지원이 포함된 iDRAC를 통해 12세대 서버에서만 가능합니다. 이전 세대 서버에서 v5.5 U1의 OpenManage 지원은 곧 제공될 계획입니다. vSphere v5.5 U1은 최신 칩셋에서 지원되지 않으므로 13세대 플랫폼에서는 지원되지 않습니다.

vSphere v5.5 U2 지원

Lifecycle Controller가 포함된 iDRAC 지원이 있을 경우, vSphere v5.5 U2가 최신 13세대 플랫폼에서 지원됩니다. 이전 세대 서버에서 v5.5 U2의 OpenManage 지원은 곧 제공될 계획입니다.

릴리스 2.2에 지원되는 vCenter 서버 버전

OpenManage Integration for VMware vCenter는 다음과 같은 버전의 vCenter 서버에서 작동됩니다.

vCenter 버전	데스크탑 클라이언트 지원	웹 클라이언트 지원
v5.0 U3	Y	N
v5.1 U2	Y	N
v5.5	Y	Y

v5.5 U1	Y	Y
v5.5 U2	Y	Y

지정된 vCenter 버전의 경우, 해당 버전이 관리하는 ESX / ESXi 호스트의 버전이 같거나 낮아야 합니다. OMIVV에서 vSphere v4.1 또는 v5.0 환경을 관리하려면 v5.0 U3 vCenter 이상의 버전이 있어야 합니다.

vCenter 관리자 로그인 수정

1. OpenManage Integration for VMware vCenter의 Summary(요약) 탭에서 링크를 사용해 Administration Console을 엽니다.
2. Login(로그인) 대화상자에 암호를 입력합니다.
3. 왼쪽 창에서 **VCENTER REGISTRATION(VCENTER 등록)**을 클릭합니다. 등록된 vCenter가 오른쪽 창에 표시됩니다. **Modify Admin Acct(관리자 계정 수정)** 창을 표시하려면 **Credentials(자격 증명)** 아래에서 **Modify(수정)**를 클릭합니다.
4. vCenter 관리자의 **User Name(사용자 이름)**, **Password(암호)** 및 **Verify Password(암호 확인)**를 입력합니다. 이 두 암호는 일치해야 합니다.
5. 암호를 변경하려면 **Apply(적용)**를 클릭하거나 변경을 취소하려면 **Cancel(취소)**을 클릭합니다.

등록된 vCenter 서버의 SSL 인증서 업데이트

SSL 인증서가 vCenter 서버에서 변경된 경우 다음 단계에 따라 OpenManage Integration for VMware vCenter에 사용할 새 인증서를 가져옵니다. OpenManage Integration for VMware vCenter는 이 인증서를 사용하여 가짜 서버가 아닌 올바른 vCenter 서버와 통신하고 있는지 확인합니다.

OpenManage Integration for VMware vCenter는 2048비트 키 길이의 RSA 암호화 표준을 사용하는 CSR(인증서 서명 요청)을 생성하기 위해 openssl API를 사용합니다. OpenManage Integration for VMware vCenter에서 생성한 CSR은 신뢰할 수 있는 인증 기관에서 디지털 방식으로 서명한 인증서를 가져오는 데 사용됩니다. OpenManage Integration for VMware vCenter는 안전한 통신을 위해 디지털 인증서를 사용해 웹 서버에서 SSL을 활성화합니다.

1. 웹 브라우저를 실행하고 https://<ApplianceIPAdrdress>를 입력합니다.
2. 왼쪽 창에서 **VCENTER REGISTRATION(VCENTER 등록)**을 클릭합니다. 등록된 vCenter가 오른쪽 창에 표시됩니다. 인증서 업데이트하려면 **Update(업데이트)**를 클릭합니다.

VMware vCenter에서 OpenManage Integration for VMware vCenter 제거

OpenManage Integration for VMware vCenter을 제거하려면 Administration Console을 사용하여 vCenter에서 등록을 취소해야 합니다.

1. 웹 브라우저를 실행하고 https://<ApplianceIPAdrdress>를 입력합니다.
2. **vCenter Registration(vCenter 등록)** 페이지의 vCenter 서버 표 아래에서 **Unregister(등록 취소)**를 클릭하여 OpenManage Integration for VMware vCenter의 등록을 취소합니다.

   둘 이상의 vCenter가 있을 수 있으므로 올바른 vCenter를 선택했는지 확인합니다.
3. 이 서버를 등록 취소할지 묻는 **Unregister vCenter(vCenter 등록 취소)** 대화상자에서 **Unregister(등록 취소)**를 클릭합니다.

Administration Console에 OpenManage Integration for VMware vCenter 라이센스 업로드

Administration Portal에 OpenManage Integration for VMware vCenter 라이센스를 업로드하려면 다음을 수행합니다.

1. 웹 브라우저를 실행하고 https://<ApplianceIPAddress>를 입력합니다.
2. 왼쪽 창에서 **VCENTER REGISTRATION(VCENTER 등록)**을 클릭합니다. 등록된 vCenter가 오른쪽 창에 표시됩니다. 라이센스 업로드 대화상자를 표시하려면 **Upload License(라이센스 업로드)**를 클릭합니다.

3. 라이센스 파일로 이동하려면 **찾아보기** 단추를 클릭하고 **업로드**를 클릭합니다.

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

가상 어플라이언스 관리

가상 어플라이언스 관리에는 OpenManage Integration for VMware vCenter 네트워크, 버전, NTP 및 HTTPS 정보가 포함되며, 여기에서 관리자는 다음을 수행할 수 있습니다.

- 가상 어플라이언스 다시 시작
- 가상 어플라이언스 업데이트 및 업데이트 리포지토리 위치 구성
- 어플라이언스 로깅 정보가 있는 문제 해결 번들 생성
- NTP(Network Time Protocol) 설정 입력
- HTTPS 인증서 업로드 및 관리

관련 작업:

- 가상 어플라이언스 다시 시작
- 리포지토리 위치 및 어플라이언스 업데이트
- 문제해결 번들 다운로드
- NTP 서버 설정

가상 어플라이언스 다시 시작

가상 어플라이언스를 다시 시작하려면 다음을 수행합니다.

노트: 가상 어플라이언스를 다시 시작하면 Administration Console에서 로그아웃되며 가상 어플라이언스 및 해당 서비스가 활성화될 때까지 OpenManage Integration for VMware vCenter를 사용할 수 없습니다.

1. 웹 브라우저를 실행하고 https://<ApplianceIPAddress>를 입력합니다.
2. 왼쪽 창에서 **APPLIANCE MANAGEMENT(어플라이언스 관리)**를 클릭합니다.
3. OpenManage Integration for VMware vCenter를 다시 시작하려면 **Restart the Virtual Appliance(가상 어플라이언스 다시 시작)**를 클릭합니다.
4. **Restart the Virtual Appliance(가상 어플라이언스 다시 시작)** 대화상자에서, 가상 어플라이언스를 다시 시작하려면 **Apply(적용)**를 클릭하고 취소하려면 **Cancel(취소)**을 클릭합니다.

리포지토리 위치 및 가상 어플라이언스 업데이트

가상 어플라이언스를 업데이트하기 전에 모든 데이터가 보호되도록 백업을 수행합니다.

1. 웹 브라우저를 실행하고 https://<ApplianceIPAddress>를 입력합니다.
2. 왼쪽 창에서 **APPLIANCE MANAGEMENT(어플라이언스 관리)**를 클릭합니다.
3. 어플라이언스 업데이트 옆에 있는 **Edit(편집)**을 클릭합니다.
4. **Appliance Update(어플라이언스 업데이트)** 창에 **Repository Location URL(리포지토리 위치 URL)**을 입력하고 **Apply(적용)**을 클릭합니다.

   노트: 업데이트 위치가 외부 네트워크에 있는 경우(예: Dell FTP 사이트), HTTP 프록시 영역에 프록시가 입력되어 있어야 합니다.

가상 어플라이언스 소프트웨어 버전 업데이트

데이터 손실을 방지하려면 소프트웨어 업데이트를 시작하기 전에 어플라이언스 백업을 수행합니다.

1. 웹 브라우저를 실행하고 https://<ApplianceIPAddress>를 입력합니다.
2. 왼쪽 창에서 **APPLIANCE MAINTENANCE(어플라이언스 유지 보수)**를 클릭합니다.
3. **Appliance Update(어플라이언스 업데이트)**에 나열된 소프트웨어 버전으로 가상 어플라이언스를 업데이트하려면 **Update Virtual Appliance(가상 어플라이언스 업데이트)**를 클릭합니다.
4. **Update Appliance(어플라이언스 업데이트)** 대화상자에 사용 가능한 현재 버전이 나열됩니다. 업데이트를 시작하려면 **Update(업데이트)**를 클릭합니다.
5. 시스템이 잠기고 유지 보수 모드로 전환됩니다. 업데이트가 완료되면 새로 나열된 버전을 보여 주는 어플라이언스 페이지가 표시됩니다.

문제 해결 번들 다운로드

이 정보를 사용하여 문제해결을 지원하거나 기술 지원 센터로 보냅니다.

1. 웹 브라우저를 실행하고 https://<ApplianceIPAddress>를 입력합니다.
2. 왼쪽 창에서 **APPLIANCE MANAGEMENT(어플라이언스 관리)**를 클릭합니다.
3. 문제해결 번들 대화상자를 표시하려면 **문제해결 번들 생성**을 클릭합니다.
4. 가상 어플라이언스 로깅 정보가 있는 Zip 파일을 열거나 저장하려면 **문제해결 번들 다운로드** 링크를 클릭합니다.
5. 종료하려면 **Close(닫기)**를 클릭합니다.

HTTP 프록시 설정

Administration Console 또는 Dell Administration Console을 사용하여 HTTP 프록시를 설정할 수 있습니다.

1. OpenManage Integration for VMware vCenter의 Summary(요약) 탭에서 링크를 사용해 Administration Console을 엽니다.
2. Login(로그인) 대화상자에 암호를 입력합니다.
3. 왼쪽 창에서 **APPLIANCE MANAGEMENT(어플라이언스 관리)**를 클릭합니다.
4. **Appliance Management(어플라이언스 관리)** 페이지에서 **HTTP Proxy Settings(HTTP 프록시 설정)**를 아래로 스크롤한 후 **Edit(편집)**를 클릭합니다.
5. **Edit(편집)** 페이지에서 다음을 수행합니다.
   a. HTTP 프록시 설정을 사용하려면 **Use HTTP Proxy Settings(HTTP 프록시 설정 사용)** 옆에 있는 **Enable(활성화)**을 선택합니다.
   b. **Proxy Server Address(프록시 서버 주소)** 텍스트 상자에서 프록시 서버 주소를 입력합니다.
   c. **Proxy Server Port(프록시 서버 포트)** 텍스트 상자에서 프록시 서버 포트를 입력합니다.
   d. 프록시 자격 증명을 사용하려면 **Use Proxy Credentials(프록시 자격 증명 사용)** 옆에 있는 **Yes(예)**를 선택합니다.
   e. 자격 증명을 사용하는 경우 **User Name(사용자 이름)** 텍스트 상자에서 사용자 이름을 입력합니다.
   f. **Password(암호)** 텍스트 상자에서 암호를 입력합니다.
6. **Apply(적용)**를 클릭합니다.

NTP 서버 설정

NTP(Network Time Protocol)를 사용하여 가상 어플라이언스 시계와 NTP 서버 시계를 동기화합니다.

1. OpenManage Integration for VMware vCenter의 요약 탭에서 링크를 사용해 Administration Console을 엽니다.
2. 로그인 대화 상자에 암호를 입력합니다.
3. 왼쪽 창에서 **어플라이언스 관리**를 클릭합니다.
4. **NTP 편집**을 클릭합니다.
5. **활성화** 확인란을 선택합니다. **기본** 및 **보조 NTP 서버**의 **호스트 이름** 또는 **IP 주소**를 입력하고 **적용**을 클릭합니다.
6. 종료하려면 **취소**를 클릭합니다.

인증서 서명 요청 생성

노트: vCenter를 포함한 OpenManage Integration for VMware vCenter를 등록하기 전에 해당 인증서를 업로드해야 합니다.

새 인증서 서명 요청을 생성하면 이전에 작성된 CSR로 생성된 인증서가 어플라이언스에 업로드되지 않습니다.

1. OpenManage Integration for VMware vCenter의 Summary(요약) 탭에서 링크를 사용해 Administration Console을 엽니다.
2. Login(로그인) 대화상자에 암호를 입력합니다.
3. 왼쪽 창에서 **APPLIANCE MANAGEMENT(어플라이언스 관리)**를 클릭합니다.
4. **Generate Certificate Signing Request for HTTPS Certificates(HTTPS 인증서의 인증서 서명 요청 생성)**을 클릭합니다. 새 요청이 생성되면 이전 CSR을 사용하여 생성된 인증서를 더 이상 어플라이언스에 업로드할 수 없다는 메시지가 표시됩니다. 요청을 계속하려면 **Continue(계속)**를 클릭하고 취소하려면 **Cancel(취소)**을 클릭합니다.
5. 요청에 대해 **Common Name(일반 이름)**, **Organizational Name(조직 이름)**, **Organizational Unit(부서)**, **Locality(지역)**, **State Name(시/도)**, **Country(국가)** 및 **Email(전자 메일)**을 입력합니다. **Continue(계속)**를 클릭합니다.
6. **Download(다운로드)**를 클릭하고 HTTPS 인증서를 액세스 가능한 위치에 저장합니다.

HTTPS 인증서 업로드

가상 어플라이언스와 호스트 시스템 간에 안전한 통신을 위해 HTTPS 인증서를 사용할 수 있습니다. 이 유형의 보안 통신을 설정하려면 인증서 서명 요청을 인증 기관에 보낸 다음 Administration Console을 사용하여 해당 인증서를 업로드해야 합니다. 자체 서명된 기본 인증서를 보안 통신에 사용할 수도 있습니다. 이 인증서는 모든 설치에서 고유합니다.

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

1. OpenManage Integration for VMware vCenter의 Summary(요약) 탭에서 링크를 사용해 Administration Console을 엽니다.
2. Login(로그인) 대화상자에 암호를 입력합니다.
3. 왼쪽 창에서 **APPLIANCE MANAGEMENT(어플라이언스 관리)**를 클릭합니다.
4. **Upload Certificate for HTTPS Certificates(HTTPS 인증서의 인증서 업로드)**를 클릭합니다.
5. **Upload Certificates(인증서 업로드)** 대화상자에서 **OK(확인)**를 클릭합니다.
6. 업로드할 인증서를 선택하려면 **Browse(찾아보기)**를 클릭하고 **Upload(업로드)**를 클릭합니다.
7. 업로드를 중단하려면 **Cancel(취소)**을 클릭합니다.

노트: 인증서는 PEM 형식이어야 합니다.

기본 HTTPS 인증서 복원

1. OpenManage Integration for VMware vCenter의 요약 탭에서 링크를 사용해 Administration Console을 엽니다.
2. 로그인 대화 상자에 암호를 입력합니다.
3. 왼쪽 창에서 **어플라이언스 관리**를 클릭합니다.
4. **HTTPS 인증서의 기본 인증서 복원**을 클릭합니다.
5. 기본 인증서 복원 대화상자에서 **적용**을 클릭합니다.

전역 경고 설정

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

1. OpenManage Integration for VMware vCenter의 요약 탭에서 링크를 사용해 Administration Console을 엽니다.
2. 로그인 대화 상자에 암호를 입력합니다.
3. 왼쪽 창에서 **경고 관리**를 클릭합니다. 새 vCenter 경고 설정을 입력하려면 **편집**을 클릭합니다.
4. 다음 항목에 숫자 값을 입력합니다.
   - 최대 경고 수
   - 경고 보관 일 수
   - 중복 경고 시간 제한(초)
5. 설정을 저장하려면 **적용**을 클릭하고 취소하려면 **취소**를 클릭합니다.

백업 및 복원 관리

백업 및 복원 관리는 Administrative Console에서 수행합니다. 이 페이지에서 수행할 수 있는 작업은 다음과 같습니다.

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

백업 및 복원 구성

백업 및 복원 기능은 OpenManage Integration for VMware vCenter 데이터베이스를 나중에 복원할 수 있는 원격 위치에 백업합니다. 백업에는 프로필, 템플릿 및 호스트 정보가 포함됩니다. 데이터 유실을 방지하려면 자동 백업을 예약하는 것이 좋습니다. 이 절차를 마친 후에는 백업 스케줄을 구성해야 합니다.

백업 및 복원을 구성하려면 다음을 수행합니다.

1. 웹 브라우저를 실행하고 https://<ApplianceIPAddress>를 입력합니다.
2. 왼쪽 창에서 **BACKUP AND RESTORE(백업 및 복원)**를 클릭합니다.
3. 현재 백업 및 복원 설정을 편집하려면 **Edit(편집)**를 클릭합니다.
4. **Settings and Details(설정 및 세부정보)** 페이지에서 다음을 수행합니다.
   a. **Backup Location(백업 위치)** 텍스트 상자에서 백업 파일의 경로를 입력합니다.
   b. **User Name(사용자 이름)** 텍스트 상자에서 사용자 이름을 입력합니다.
   c. **Password(암호)** 텍스트 상자에서 암호를 입력합니다.
   d. **Enter the password used to encrypt backups(백업 암호화에 사용되는 암호 입력)**에서, 텍스트 상자에 암호화된 암호를 입력합니다.

암호화된 암호는 영숫자 및 다음의 특수 문자를 포함합니다: !@#$%*. 길이 제한은 없습니다.

e. **Verify Password(암호 확인)** 텍스트 상자에서 암호화된 암호를 다시 입력합니다.

5. 설정을 저장하려면 **Apply(적용)**를 클릭합니다.
6. 백업 일정을 구성합니다. 자세한 내용은 자동 백업 예약을 참조하십시오.

자동 백업 예약

백업 및 복원 구성의 두 번째 부분입니다. 백업 위치 및 자격 증명 구성에 대한 자세한 내용은 백업 및 복원 구성을 참조하십시오.
자동 백업을 예약하려면 다음을 수행합니다.

1. 웹 브라우저를 실행하고 https://<ApplianceIPAddress>를 입력합니다.
2. 왼쪽 창에서 **BACKUP AND RESTORE(백업 및 복원)**를 클릭합니다.
3. 백업 및 복원 설정을 편집하려면 **Edit Automatic Scheduled Backup(자동 예약된 백업 편집)**을 클릭합니다. 그러면 필드가 활성화됩니다.
4. 백업을 사용하려면 **Enabled(활성화됨)**를 클릭합니다.
5. 백업을 실행할 요일의 확인란을 선택합니다.
6. **Time for Backup (24 Hour Time Format, HH:mm)(백업 시간(24시간 형식, HH:mm))** 텍스트 상자에서 HH:mm 형식으로 시간을 입력합니다.

   다음에 예약된 백업의 날짜와 시간으로 **다음 백업**이 채워집니다.
7. **Apply(적용)**를 클릭합니다.

즉시 백업 수행

다음과 같이 즉시 백업을 수행합니다.

1. 웹 브라우저를 실행하고 https://<ApplianceIPAddress>를 입력합니다.
2. 왼쪽 창에서 **BACKUP AND RESTORE(백업 및 복원)**를 클릭합니다.
3. **Backup Now(지금 백업)**를 클릭합니다.
4. 백업 설정에서 위치 및 암호화 암호를 사용하려면 **Backup Now(지금 백업)** 대화상자에서 해당 확인란을 선택합니다.
5. **Backup Location(백업 위치)**, **User Name(사용자 이름)**, **Password(암호)** 및 **Encryption Password(암호화 암호)**를 입력합니다.

   암호화된 암호는 영숫자 및 다음의 특수 문자를 포함합니다: !@#$%*. 길이 제한은 없습니다.
6. **Backup(백업)**을 클릭합니다.

백업에서 데이터베이스 복원

노트: 복원 작업이 완료되면 가상 어플라이언스가 다시 부팅됩니다.

백업에서 데이터베이스를 복원하려면 다음을 수행합니다.

1. 웹 브라우저를 실행하고 https://<ApplianceIPAddress>를 입력합니다.
2. 왼쪽 창에서 **BACKUP AND RESTORE(백업 및 복원)**를 클릭하면 현재 백업 및 복원 설정이 표시됩니다.
3. **Restore Now(지금 복원)**를 클릭합니다.
4. Restore Now(지금 복원) 대화상자에서 **File Location (CIFS/NFS Format)(파일 위치(CIFS/NFS 형식))**를 입력합니다.
5. 백업 파일의 **User Name(사용자 이름)**, **Password(암호)** 및 **Encryption Password(암호화 암호)**를 입력합니다.

   암호화된 암호는 영숫자 및 다음의 특수 문자를 포함합니다: !@#$%*. 길이 제한은 없습니다.

6. 변경사항을 저장하려면 **적용** 을 클릭합니다.
   Apply(적용)를 클릭하면 어플라이언스가 다시 부팅되거나 다시 시작됩니다.

vSphere 클라이언트 콘솔 이해

이 **콘솔**은 가상 머신의 vSphere 클라이언트 내에서 볼 수 있습니다. 또한 이 **콘솔**은 Administration Console과 함께 작동됩니다. 이 콘솔을 통해 다음과 같은 작업을 수행합니다:

- 네트워크 설정 구성
- 가상 어플라이언스 암호 변경
- 로컬 시간대 설정
- 가상 어플라이언스 다시 부팅
- 가상 어플라이언스를 공장 설정으로 다시 설정
- 콘솔 새로 고침
- 로그아웃 옵션

화살표 키를 사용하여 위 또는 아래로 이동합니다. 원하는 옵션을 선택한 후 **<ENTER>**를 누릅니다. **콘솔** 화면에 액세스하면 VMware vSphere 클라이언트가 커서를 자동으로 제어합니다. 자동 제어를 해제하려면 **<CTRL> + <ALT>** 키를 누릅니다.

네트워크 설정 구성

네트워크 설정 변경은 vSphere 클라이언트의 **Console(콘솔)** 탭에서 수행합니다.
네트워크 설정을 구성하려면 다음을 수행합니다.

1. **vSphere 클라이언트**에서 OpenManage Integration for VMware vCenter를 선택하고 **Console(콘솔)** 탭을 클릭합니다.
2. **콘솔** 창에서 **네트워크 구성**을 선택한 후 **<ENTER>**를 누릅니다.
3. **장치 편집** 또는 **DNS 편집** 구성 아래에 원하는 네트워크 설정을 입력한 후 **저장 후 끝내기**를 클릭합니다. 변경사항을 중단하려면 **끝내기**를 클릭합니다.

가상 어플라이언스 암호 변경

가상 어플라이언스 암호는 vSphere 클라이언트의 **Console(콘솔)** 탭을 사용하여 변경합니다.
가상 어플라이언스 암호를 변경하려면 다음을 수행합니다.

1. vSphere 클라이언트에서 OpenManage Integration for VMware vCenter를 선택하고 **Console(콘솔)** 탭을 클릭합니다.
2. **Console(콘솔)** 탭에서 화살표 키를 사용하여 **Change Admin Password(관리자 암호 변경)**를 선택하고 **<ENTER>**를 누릅니다.
3. **현재 관리 암호**를 입력하고 **<ENTER>**를 누릅니다.
   관리 암호에는 특수 문자, 숫자, 대문자, 소문자를 각각 하나씩 사용하고 최소 8자여야 합니다.
4. **새 관리 암호 입력**에 새 암호를 입력하고 **<ENTER>**를 누릅니다.
5. **관리 암호를 확인하십시오** 텍스트 상자에 새 암호를 다시 입력하고 **<ENTER>**를 누릅니다. 관리 암호가 변경됩니다.

로컬 시간대 설정

로컬 시간대를 설정하려면 다음을 수행합니다.

노트: 시간대만 편집할 수 있으며 현재 시간과 날짜는 편집할 수 없습니다.

1. **vSphere 클라이언트**에서 OpenManage Integration for VMware vCenter 가상 시스템을 선택하고 **콘솔** 탭을 클릭합니다.
2. **시간대 설정**을 선택하고 **<ENTER>**를 누릅니다.
3. **시간대 선택** 창에서 원하는 시간대를 선택하고 **확인**을 클릭합니다. 변경사항을 취소하려면 **취소**를 클릭합니다. 시간대가 업데이트됩니다.

가상 어플라이언스 다시 부팅

가상 어플라이언스를 다시 부팅하려면 다음을 수행합니다.

1. **vSphere 클라이언트**에서 OpenManage Integration for VMware vCenter 가상 시스템을 선택하고 **콘솔** 탭을 클릭합니다.
2. **이 가상 어플라이언스 다시 부팅**을 선택하고 **<ENTER>**를 누릅니다.
3. 다음과 같은 메시지가 표시됩니다.

   ```
   If there are any processes running on this appliance they will be
   terminated by this action. Are you sure you wish to do this?
   ```
4. 다시 부팅하려면 **y**를 입력하고 취소하려면 **n**을 입력합니다. 어플라이언스가 다시 부팅됩니다.

가상 어플라이언스를 공장 설정으로 다시 설정

가상 어플라이언스를 공장 설정으로 다시 설정하려면 다음을 수행합니다.

1. **vSphere 클라이언트**에서 OpenManage Integration for VMware vCenter를 선택하고 **Console(콘솔)** 탭을 클릭합니다.
2. **이 가상 어플라이언스를 공장 설정으로 다시 설정**을 선택하고 **<ENTER>**를 누릅니다.
3. 다음과 같은 알림이 표시됩니다.

   ```
   This operation is completely Irreversible if you continue you will
   completely reset *this* appliance to its original settings. All changes you
   have made to this appliance will be Lost. Are you sure you wish to Reset
   this Appliance to Factory Settings?
   ```
4. 재설정하려면 **y**를 입력하고 취소하려면 **n**을 입력합니다.

   어플라이언스가 원래 공장 설정으로 재설정되고 기타 모든 설정 및 저장된 데이터는 유실됩니다.

   노트: 가상 어플라이언스가 공장 설정으로 다시 설정되면 네트워크 구성의 모든 업데이트는 보존됩니다. 이러한 설정은 다시 설정되지 않습니다.

콘솔 보기 새로 고치기

콘솔 보기를 새로 고치려면 **Refresh(새로 고침)**를 선택하고 **<ENTER>**를 누릅니다.

읽기 전용 사용자 역할

진단을 위한 셸 액세스 권한이 포함된 읽기 전용이라고 하는 권한 없는 사용자 역할이 있습니다. 읽기 전용 사용자의 권한은 마운트 실행으로 제한됩니다. 읽기 전용 사용자의 암호는 관리자와 동일하게 설정됩니다.

1.6/1.7에서 2.2로의 마이그레이션 경로

버전 1.7 이하의 버전에서 이 버전을 지원할 RPM 업데이트가 없습니다. 백업 및 복원 경로를 사용하여 이전 버전(1.6 또는 1.7)에서 버전 2.2 릴리스로 마이그레이션할 수 있습니다. 또한, 마이그레이션 경로는 버전 1.6 및 1.7에서

만 지원됩니다. 1.6 미만 버전에서는 OpenManage Integration for VMware vCenter 버전 2.2로 마이그레이션을 실행하기 전에 지원되는 버전으로 어플라이언스를 업그레이드해야 합니다.

이전 버전에서 OpenManage Integration for VMware vCenter 2.2 버전으로 마이그레이션하려면 다음과 같이 합니다.

1. 이전 릴리스에 대한 데이터베이스 백업을 수행합니다. 자세한 내용은 이 설명서에서 **Managing Backup and Restore** (백업 및 복원 관리) 섹션을 참조하십시오.
2. vCenter에서 이전 어플라이언스의 전원을 끕니다.

   노트: vCenter에서 플러그인을 등록 취소하지 마십시오. vCenter에서 플러그인을 등록 취소하면 플러그인을 통해 vCenter에 등록된 모든 알람이 제거되며 vCenter에서의 조치 등과 같은 알람에서 수행된 모든 사용자 지정이 제거됩니다. 백업 후에 플러그인을 등록 취소한 경우에는 이 안내서에 있는 **백업 후에 이전 플러그인을 등록 취소한 경우 복원하는 방법**을 참조하십시오.
3. 새 OpenManage Integration 버전 2.2 OVF를 배포합니다. 자세한 내용은 이 안내서의 **vSphere 클라이언트를 사용하여 OpenManage Integration for VMware vCenter OVF 배포** 절을 참조하여 OVF를 배포하십시오.
4. OpenManage Integration 버전 2.2 어플라이언스의 전원을 켭니다.
5. 어플라이언스의 네트워크, 시간대 등을 설정합니다. 새 OpenManage Integration 버전 2.2 어플라이언스의 IP 주소를 이전 어플라이언스의 IP 주소와 동일하게 설정하는 것이 좋습니다. 네트워크 세부사항을 설정하려면 이 안내서의 **Registering OpenManage Integration for VMware vCenter And Importing The License File(OpenManage Integration for VMware vCenter 등록 및 라이센스 파일 가져오기)** 절을 참조하십시오.
6. 데이터베이스를 새 어플라이언스로 복원합니다. 자세한 내용은 이 설명서에서 **백업에서 데이터베이스 복원** 섹션을 참조하십시오.
7. 새 라이센스 파일을 업로드합니다. 자세한 내용은 **OpenManage Integration Version 2.2 Quick Install Guide**(OpenManage Integration 버전 2.2 빠른 설치 안내서)의 **OpenManage Integration for VMware vCenter 등록 및 라이센스 파일 가져오기** 절을 참조하십시오.
8. 어플라이언스를 확인합니다. 자세한 내용은 이 안내서의 **설치 확인** 절을 통해 데이터베이스 마이그레이션에 성공했는지 확인하십시오.
9. 등록된 모든 vCenter에서 인벤토리를 실행합니다.

   노트:

   업그레이드 후에는 플러그인에서 관리되는 모든 호스트에서 인벤토리를 실행하는 것이 좋습니다. 자세한 내용은 **인벤토리 작업 실행** 절에서 필요에 따른 인벤토리 실행 단계를 참조하십시오.

   새 OpenManage Integration 버전 2.2 어플라이언스의 IP 주소가 이전 어플라이언스 IP 주소에서 변경된 경우, SNMP 트랩의 트랩 대상이 새 어플라이언스를 가리키도록 구성해야 합니다. 12세대 이상 서버의 경우 이들 호스트에서 인벤토리를 실행하면 이 문제가 수정됩니다. 이전에 호환되었던 모든 11세대 이하 호스트에서는 이 IP 주소가 비호환으로 표시되므로 OMSA를 구성해야 합니다. 자세한 내용은 이 설명서에서 호스트 호환성 수정을 위한 **비호환 VSphere 호스트 수정 마법사 실행** 절을 참조하십시오.

7

문제 해결

이 섹션에서는 문제 해결 질문에 대한 답을 확인할 수 있습니다. 이 섹션에 포함된 내용은 다음과 같습니다.

FAQ(자주 묻는 질문)

이 섹션에는 몇 가지 일반적인 질문과 해결 방법이 포함되어 있습니다.

펌웨어 버전 13.5.2로 Intel 네트워크 카드를 업데이트하기 위해 OpenManage Integration for VMware vCenter을 사용하는 것은 지원되지 않습니다.

Dell PowerEdge 12세대 서버 및 펌웨어 버전이 13.5.2인 일부 Intel 네트워크 카드에 대해 알려진 문제가 있습니다. Lifecycle Controller를 사용하여 펌웨어 업데이트를 적용할 때 이 펌웨어 버전에서 일부 Intel 네트워크 카드 모델의 업데이트가 실패합니다. 이 버전의 펌웨어를 사용하는 고객은 운영 체제를 사용하여 네트워크 드라이버 소프트웨어를 업데이트해야 합니다. Intel 네트워크 카드에 13.5.2 이외의 펌웨어 버전이 있는 경우 OpenManage Integration for VMware vCenter을 사용하여 업데이트할 수 있습니다. 자세한 내용은 http://en.community.dell.com/techcenter/b/techcenter/archive/2013/03/20/intel-network-controller-card-with-v13-5-2-firmware-cannot-be-upgraded-using-lifecycle-controller-to-v13-5-6.aspx를 참조하십시오.

노트: 참고: 일대다 펌웨어 업데이트를 사용할 때 업데이트가 실패하고 업데이트 작업에서 나머지 서버의 업데이트가 중지되므로 버전 13.5.2에 있는 Intel 네트워크 어댑터를 선택하지 마십시오.

LC의 작업 상태가 '실패'인 경우에도 잘못된 DUP를 사용하여 펌웨어 업데이트를 시도하면 vCenter 콘솔의 하드웨어 업데이트 작업 상태가 실패 또는 시간 초과로 표시됩니다. 이러한 문제가 발생하는 이유는 무엇입니까?

펌웨어 업데이트에 대해 잘못된 DUP를 선택하면 vCenter 콘솔 창의 작업 상태가 '진행 중'으로 남아 있게 되지만 메시지가 실패 이유로 변경됩니다. 이는 알려진 VMWare 오류이며, 이후 VMWare vCenter 릴리스에서 해결될 예정입니다.

해결 방법: 작업을 수동으로 취소해야 합니다.

적용 버전: 모든 버전

관리 포털이 계속해서 연결할 수 없는 업데이트 리포지토리 위치로 표시됩니다.

사용자가 연결할 수 없는 업데이트 리포지토리 경로를 제공한 경우 어플라이언스 업데이트 보기의 맨 위에 "실패: URL …에 연결하는 중에 오류가 발생했습니다."라는 오류 메시지가 표시되지만 업데이트하기 전에는 업데이트 리포지토리 경로의 값이 지워지지 않습니다.

해결 방법: 이 페이지에서 다른 페이지로 이동하고 페이지를 새로 고치십시오.

적용 버전: 모든 버전

덮어 쓴 DNS 설정 및 어플라이언스 IP에 대해 DHCP를 사용하는 경우 어플라이언스를 재부팅한 후 DNS 구성 설정이 원래 설정으로 복원되는 이유는 무엇입니까?

이는 알려진 결함이며, 정적으로 할당된 DNS 설정이 DHCP의 값으로 대체됩니다. DHCP를 사용하여 IP 설정을 가져오고 DNS 값이 정적으로 할당되면 이러한 오류가 발생할 수 있습니다. DHCP 임대가 갱신되거나 어플라이언스가 다시 시작되면 정적으로 할당된 DNS 설정이 제거됩니다. 해결 방법으로, DNS 서버 설정이 DHCP와 다른 경우 IP 설정을 정적으로 할당하십시오.

적용 버전: 모든 버전

일대다 펌웨어 업데이트를 수행할 때 시스템이 유지 보수 모드로 시작되지 않는 이유는 무엇입니까

일부 펌웨어 업데이트에서는 호스트를 재부팅할 필요가 없습니다. 이러한 경우 호스트가 유지 보수 모드로 시작하지 않고 펌웨어 업데이트가 수행됩니다.

내 리포지토리에 선택한 11G 시스템에 대한 번들이 있는 경우에도 펌웨어 업데이트에서 펌웨어 업데이트에 대한 번들이 없는 상태로 표시되는 이유는 무엇입니까?

잠금 모드에서 연결 프로필에 호스트를 추가하면 인벤토리가 시작되지만 "원격 액세스 컨트롤러를 찾을 수 없거나 이 호스트에서 인벤토리가 지원되지 않습니다."라는 메시지와 함께 실패합니다. 정상적으로는 인벤토리가 잠금 모드에서 호스트에 대해 작동해야 하는 것 아닙니까?

호스트를 잠금 모드에 배치하거나 잠금 모드에서 호스트를 제거하는 경우 30분을 기다린 후 다음 작업을 수행해야 합니다. 펌웨어 업데이트에 대해 11G 호스트를 선택하는 경우 제공된 지오메트리에 해당 시스템에 대한 번들이 있어도 펌웨어 업데이트 마법사가 번들을 표시되지 않습니다. 이는 OMSA에 대한 11G 호스트가 OpenManage Integration에 트랩을 보내도록 구성되어 있지 않을 수 있기 때문에 발생합니다.

해결 방법: OpenManage Integration Desktop 클라이언트의 호스트 호환성 화면을 사용하여 호스트가 호환되는지 확인하십시오. 호환되지 않는 경우 호스트 호환성 수정을 사용하여 호환되도록 하십시오.

적용 버전: 2.1 및 2.2

PERC S300 Boot Controller가 있는 서버에서 ESX / ESXi 배포가 실패하는 이유는 무엇입니까?

PERC S300 Boot Controller가 있는 Dell PowerEdge 서버에서 다른 ESX/ESXi 버전을 사용하여 OpenManage Integration for VMware vCenter을 배포하면 오류가 발생합니다. Dell 사용자 지정 ESX/ESXi 운영 체제에서는 PERC S300 Boot Controller에 대한 드라이버를 제공하지 않습니다. 이로 인해 운영 체제를 설치하는 동안 부팅 컨트롤러/HDD가 인식되지 않습니다. PERC S300 Boot Controller가 있는 서버에서는 OpenManage Integration for VMware vCenter 배포가 지원되지 않습니다.

펌웨어 링크를 클릭하면 오류 메시지가 표시되는 이유는 무엇입니까?

네트워크 속도가 저하된 경우(9600BPS) 통신 오류 메시지가 표시될 수 있습니다. vSphere 클라이언트에서 OpenManage Integration for VMware vCenter에 대한 펌웨어 링크를 클릭하면 이 오류 메시지가 표시될 수 있습니다. 이는 소프트웨어 인벤토리 목록을 가져오도록 시도하는 중에 연결 시간이 초과되면 발생합니다. Microsoft Internet Explorer에서 이 시간 초과가 초기화됩니다. Microsoft Internet Explorer 버전 9/10의 경우 기본 "수신 시간 제한" 값이 10초로 설정되어 있습니다. 다음 단계를 사용하여 이 문제를 해결하십시오.

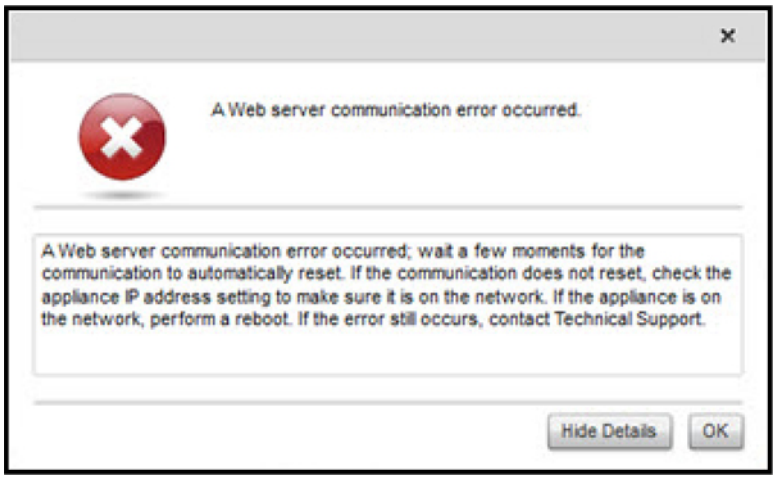

그림 5. 펌웨어 링크 통신 오류

1. Microsoft 레지스트리 편집기(Regedit)를 엽니다.
2. 다음 위치로 이동합니다.
   KHEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
3. 수신 시간 제한에 대한 DWORD 값을 추가합니다.
4. 값을 30초(30000)로 설정합니다 [이 값은 사용자 환경에 따라 더 높은 값이어야 할 수 있음].
5. Regedit를 종료합니다.
6. Internet Explorer를 다시 시작합니다.

노트: 새 Internet Explorer 창을 새로 열기만 하는 것이 아니라 Internet Explorer 브라우저를 다시 시작해야 합니다.

어떤 세대의 Dell 서버에서 OpenManage Integration for VMware vCenter가 SNMP 트랩을 구성하고 지원합니까?

OpenManage Integration for VMware vCenter가 12세대 이전의 서버에서 OMSA SNMP 트랩을 지원하고 12세대 서버에서 iDRAC 트랩을 지원합니다.

OpenManage Integration for VMware vCenter가 링크된 모드에서 4개 이상의 vCenter를 어떻게 지원합니까?

각 가상 어플라이언스가 링크된 모드에서 최대 3개의 vCenter를 지원합니다. vCenter가 11개 이상 있는 경우 연결된 라이센스와 함께 10개의 vCenter마다 하나의 새 어플라이언스 인스턴스가 필요합니다.

OpenManage Integration for VMware vCenter가 링크된 모드에서 vCenter를 지원합니까?

예, OpenManage Integration for VMware vCenter가 링크된 모드에서 최대 10개의 vCenter를 지원합니다. OpenManage Integration for VMware vCenter가 링크된 모드에서 작동하는 방법에 대한 자세한 내용은 www.Dell.com에서 *Dell Management Plug-in for VMware vCenter: 링크된 모드에서 작동* 백서를 참조하십시오.

OpenManage Integration for VMware vCenter에 대한 필수 포트 설정은 무엇입니까?

노트: Dell Management Center의 준수 창에 있는 *비준수 vSphere 호스트 수정* 링크를 사용하여 OMSA 에이전트를 배포할 때 OpenManage Integration for VMware vCenter이 httpClient 서비스를 시작하고 ESXI 5.0 이후의 릴리스에 포트 8080을 활성화하여 OMSA VIB를 다운로드하고 설치합니다. OMSA 설치가 완료되면 서비스가 자동으로 중지되고 포트가 닫힙니다.

OpenManage Integration for VMware vCenter에 다음 포트 설정을 사용하십시오.

표 3. 가상 어플라이언스 포트

포트 번호	프로토콜	포트 유형	최고 암호화 수준	방향	사용	구성 가능
21	FTP	TCP	없음	Out	FTP 명령 클라이언트	No(없음)
53	DNS	TCP	없음	Out	DNS 자동	No(없음)
80	HTTP	TCP	없음	Out	Dell 온라인 데이터 액세스	No(없음)
80	HTTP	TCP	없음	In	Administration Console	No(없음)
162	SNMP 에이전트	UDP	없음	In	SNMP 에이전트(서버)	No(없음)
11620	SNMP 에이전트	UDP	없음	In	SNMP 에이전트(서버)	No(없음)
443	HTTPS	TCP	128비트	In	HTTPS 서버	No(없음)
443	WSMAN	TCP	128비트	In/Out	iDRAC/OMSA 통신	No(없음)
4433	HTTPS	TCP	128비트	In	자동 검색	No(없음)
2049	NFS	UDP	없음	모두	공개 공유	No(없음)
4001–4004	NFS	UDP	없음	모두	공개 공유	No(없음)
11620	SNMP 에이전트	UDP	없음	Om	SNMP 에이전트(서버)	No(없음)

표 4. 관리된 노드

포트 번호	프로토콜	포트 유형	최고 암호화 수준	방향	사용	구성 가능
162, 11620	SNMP	UDP	없음	Out	하드웨어 이벤트	No(없음)
443	WSMAN	TCP	128비트	In	iDRAC/OMSA 통신	No(없음)
4433	HTTPS	TCP	128비트	Out	자동 검색	No(없음)
2049	NFS	UDP	없음	모두	공개 공유	No(없음)
4001–4004	NFS	UDP	없음	모두	공개 공유	No(없음)
443	HTTPS	TCP	128비트	In	HTTPS 서버	No(없음)
8080	HTTP	TCP		In	HTTP 서버; OMSA VIB를	No(없음)

포트 번호	프로토콜	포트 유형	최고 암호화 수준	방향	사용	구성 가능
					다운로드하고 비준수 vSphere 호스트를 수정합니다.	
50	RMCP	UDP/TCP	128비트	Out	원격 메일 확인 프로토콜	No(없음)
51	IMP	UDP/TCP	N/A(해당 없음)	N/A(해당 없음)	IMP 논리적 주소 유지 보수	No(없음)
5353	mDNS	UDP/TCP		모두	Multicast DNS	No(없음)
631	IPP	UDP/TCP	없음	Out	IPP(Internet Printing Protocol)	No(없음)
69	TFTP	UDP	128비트	모두	Trivial File Transfer	No(없음)
111	NFS	UDP/TCP	128비트	In	SUN Remote Procedure Call (Portmap)	No(없음)
68	BOOTP	UDP	없음	Out	Bootstrap Protocol Client	No(없음)

가상 어플라이언스의 성공적인 설치와 작동을 위한 최소 요구 사항은 무엇입니까?

다음 설정은 최소 어플라이언스 요구 사항의 개요를 제공합니다.

- 실제 RAM: 3GB
- 예약된 메모리: 1GB

  노트: 최적의 성능을 위해 Dell은(는) 3GB를 권장합니다.
- 디스크: 32.5GB
- CPU: 2개의 가상 CPU

iDRAC 사용자 목록에서 새로 변경한 자격 증명을 가진 동일한 사용자가 있는 하드웨어 프로필을 성공적으로 적용한 후에 베어 메탈 검색을 위해 사용되는 사용자에 대한 암호가 변경되지 않은 이유는 무엇입니까?

하드웨어 프로필 템플릿 만이 배포를 위해 선택되면 검색에서 사용된 사용자 암호는 새로운 자격 증명에서 변경되지 않습니다. 이는 의도적으로 이루어진 작업으로 플러그 인이 향후 배포 필요 시 iDRAC와 통신할 수 있습니다.

시스템 개요 페이지에서 프로세서 뷰의 프로세서 버전이 "해당 없음"으로 표시되는 이유는 무엇입니까?

PowerEdge 12세대 Dell 서버 이상 세대인 경우 프로세서 버전이 브랜드 열입니다. 하위 세대 서버의 경우 프로세서 버전이 버전 열에 표시됩니다.

덮어 쓴 DNS 설정 및 어플라이언스 IP에 대해 DHCP를 사용하는 경우 어플라이언스를 재부팅한 후 DNS 구성 설정이 원래 설정으로 복원되는 이유는 무엇입니까?

이는 알려진 결함이며, 정적으로 할당된 DNS 설정이 DHCP의 값으로 대체됩니다. DHCP를 사용하여 IP 설정을 가져오고 DNS 값이 정적으로 할당되면 이러한 오류가 발생할 수 있습니다. DHCP 임대가 갱신되거나 어플라이언스가 다시 시작되면 정적으로 할당된 DNS 설정이 제거됩니다. 해결 방법으로, DNS 서버 설정이 DHCP와 다른 경우 IP 설정을 정적으로 할당하십시오.

적용 버전: 모든 버전

vCenter 호스트 및 클러스터 페이지에 나열된 새 iDRAC 상세정보가 나타나지 않는 이유는?

vShpere 데스크탑 클라이어트의 최근 작업 창에서 펌웨어 업데이트 작업을 성공적으로 완료한 후에 Firmware Update(펌웨어 업데이트) 페이지를 새로 고치고 펌웨어 버전을 확인하십시오. 페이지에 이전 버전이 표시되면 OpenManage Integration for VMware vCenter의 Host Compliance(호스트 호환성) 페이지로 이동한 후 해당 호스트의 CISOR 상태를 확인하십시오. CISOR이 활성화되어 있지 않으면 CISOR을 활성화하고 호스트를 재부팅하십시오. CISOR이 이미 활성화되어 있으면 iDRAC 콘솔에 로그인하고 iDRAC를 다시 설정한 후 몇 분 정도 기다렸다가 vSphere 데스크탑 클라이언트에서 Firmware Update(펌웨어 업데이트) 페이지를 새로 고치십시오.

온도 하드웨어 결함을 시뮬레이션하기 위해 OMSA를 사용하여 이벤트 설정을 테스트하는 방법은 무엇입니까?

이벤트가 올바르게 작동하는지 확인하려면 다음을 수행하십시오.

1. OMSA 사용자 인터페이스에서 **경고 관리 → 플랫폼 이벤트**로 이동합니다.
2. **플랫폼 이벤트 필터 경고 활성화** 확인란을 선택합니다.
3. 아래쪽으로 스크롤하고 **변경사항 적용**을 클릭합니다.
4. 온도 경고와 같은 특정 이벤트가 활성화되도록 하려면 왼쪽에 있는 트리에서 **기본 시스템 섀시**를 선택합니다.
5. **기본 시스템 섀시** 아래에서 **온도**를 선택합니다.
6. **경고 관리** 탭을 선택하고 **온도 감지기 경고**를 선택합니다.
7. **메시지 브로드캐스트** 확인란을 선택하고 **변경사항 적용**을 선택합니다.
8. 온도 경고 이벤트를 생성하려면 왼쪽에 있는 트리 보기에서 **기본 시스템 섀시**를 선택합니다.
9. **기본 시스템 섀시** 아래에서 **온도**를 선택합니다.
10. **시스템 보드 주변 온도** 링크를 선택하고 **값으로 설정** 옵션 단추를 선택합니다.
11. **최대 경고 임계값**을 현재 나열된 수치 미만으로 설정합니다. 예를 들어, 현재 수치가 **27**인 경우 임계값을 **25**로 설정합니다.
12. **변경사항 적용**을 선택하면 온도 경고 이벤트가 생성됩니다. 다른 이벤트를 생성하려면 동일한 **값으로 설정** 옵션을 사용하여 원래 설정을 복원합니다. 이벤트가 경고로 생성되고 정상 상태로 지정됩니다. 모든 항목이 제대로 작동하면 **vCenter 작업 및 이벤트** 보기를 탐색하면 온도 센서 경고 이벤트가 표시됩니다.

노트: 중복 이벤트에 대한 필터가 있습니다. 한 행에서 동일한 이벤트를 너무 많이 트리거하도록 시도하면 하나의 이벤트만 수신됩니다. 모든 이벤트를 보려면 이벤트 간에 **30**초 이상 기다리십시오.

Dell 호스트 시스템에 OMSA 에이전트를 설치했지만 OMSA가 설치되지 않았다는 오류 메시지가 계속해서 표시됩니다. 어떻게 해야 합니까?

이 문제를 해결하려면 11세대 서버에서 다음을 수행하십시오.

1. 호스트 시스템에 **원격 활성화** 구성 요소와 함께 **OMSA**를 설치합니다.
2. 명령줄을 사용하여 OMSA를 설치하는 경우 **-c option**을 지정해야 합니다. OMSA가 이미 설치되어 있는 경우 -c option을 사용하여 다시 설치하고 서버를 다시 시작합니다.

   ```
   srvadmin-install.sh -c srvadmin-services.sh restart
   ```

   ESXi 호스트의 경우 **VMware 원격 CLI 도구**를 사용하여 **OMSA VIB**를 설치하고 시스템을 다시 부팅해야 합니다.

OpenManage Integration for VMware vCenter에서 잠금 모드가 활성화된 상태로 ESX/ESXI를 지원할 수 있습니까?

예. 호스트 ESXi 4.1 이상의 이 릴리스에서 잠금 모드가 지원됩니다.

재부팅한 후 잠금 모드의 호스트 ESXi 4.0 업데이트 2 및 ESXi 업데이트 3에서 인벤토리가 실패합니다.

잠금 모드에는 ESXi 4.1 이상이 필요합니다. 이전 버전의 ESXi를 사용하는 경우 잠금 모드 중에 어떠한 이유로든 호스트를 재부팅하면 재부팅한 후 호스트에서 다음 단계를 수행할 때까지 인벤토리가 계속해서 실패합니다.

ESXi 4.0 업데이트 2 및 업데이트 3에 대한 문제 해결 단계는 다음과 같습니다.

1. **vSphere Client**에서 **호스트 및 클러스터**를 선택하고 왼쪽 창에서 **호스트**를 선택한 후 **구성** 탭을 클릭합니다.
2. 왼쪽 창의 **소프트웨어** 아래에서 **보안 프로필**을 클릭합니다.
3. **잠김 모드**를 아래로 스크롤하고 **편집**을 클릭합니다.
4. **잠김 모드** 대화 상자에서 잠금 모드를 비활성화하려면 **활성화** 확인란을 지우고 **확인**을 클릭합니다.
5. 호스트 콘솔에 로그인하고 **관리 에이전트 다시 시작**을 선택한 후 **<ENTER>** 키를 눌러 확인하고 **<F11>** 키를 누릅니다.
6. 잠금 모드를 활성화하려면 여기에서 **활성화** 확인란을 선택한 경우를 제외하고 1에서 4단계를 반복하고 **확인**을 클릭합니다.

잠금 모드를 사용하도록 시도했지만 실패했습니다.

잠금 모드에서 연결 프로필에 호스트를 추가하면 인벤토리가 시작되지만 "원격 액세스 컨트롤러를 찾을 수 없거나 이 호스트에서 인벤토리가 지원되지 않습니다."라는 메시지와 함께 실패합니다. 정상적으로는 인벤토리가 잠금 모드에서 호스트에 대해 작동해야 하는 것 아닙니까?

호스트를 잠금 모드에 배치하거나 잠금 모드에서 호스트를 제거하는 경우 30분을 기다린 후 OpenManage Integration for VMware vCenter에서 다음 작업을 수행해야 합니다.

LC의 작업 상태가 '실패'인 경우에도 잘못된 DUP를 사용하여 펌웨어 업데이트를 시도하면 vCenter 콘솔의 하드웨어 업데이트 작업 상태가 실패 또는 시간 초과로 표시됩니다. 이러한 문제가 발생하는 이유는 무엇입니까?

펌웨어 업데이트에 대해 잘못된 DUP를 선택하면 vCenter 콘솔 창의 작업 상태가 '진행 중'으로 남아 있게 되지만 메시지가 실패 이유로 변경됩니다. 이는 알려진 VMWare 오류이며, 이후 VMWare vCenter 릴리스에서 해결될 예정입니다.

해결 방법: 작업을 수동으로 취소해야 합니다.

적용 버전: 모든 버전

ESXi 4.1 U1에서 UserVars.CIMoeMProviderEnable를 어떻게 설정해야 합니까?

UserVars.CIMoemProviderEnabled를 1로 설정하십시오.

참조 서버를 사용하여 하드웨어 프로필을 생성했지만 실패했습니다. 어떻게 해야 합니까?

iDRAC 펌웨어, 수명 주기 컨트롤러 펌웨어 및 BIOS의 최소 권장 버전이 설치되어 있는지 확인하십시오.

참조 서버에서 검색한 데이터가 최신 상태인지 확인하려면 **CSIOR(Collect System Inventory On Restart)**을 활성화하고 데이터를 추출하기 전에 참조 서버를 다시 시작하십시오. 참조 서버에서 CSIOR 설정을 참조하십시오.

블레이드 서버에서 ESX/ESXi를 배포하도록 시도했지만 실패했습니다. 어떻게 해야 합니까?

이 문제를 해결하려면 다음을 수행하십시오.

1. **ISO 위치(NFS 경로)** 및 준비 **폴더 경로**가 정확한지 확인합니다.
2. 서버 ID를 할당하는 동안 선택된 **NIC**가 가상 어플라이언스와 동일한 네트워크에 있는지 확인합니다.
3. **고정 IP 주소**를 사용하는 경우 제공된 네트워크 정보(서브넷 마스크 및 기본 게이트웨이 포함)가 정확한지 확인합니다. 또한 네트워크에 IP 주소가 할당되어 있지 않은지 확인하십시오.
4. 시스템에 **가상 디스크**가 하나 이상 표시되는지 확인합니다. 또한 내부 RIPS SD 카드에도 ESXi가 설치됩니다.

내 하이퍼바이저 배포가 R210 II 시스템에서 실패하는 이유는 무엇입니까?

연결된 ISO로 부터 부팅하려는 BIOS의 오류로 인해 R210 II 시스템의 타임아웃 문제가 하이퍼바이저 배포 실패 오류의 원인이 됩니다. 이 문제를 해결하려면, 시스템에 수동으로 하이퍼바이저를 설치하십시오.

배포 마법사에 자동 검색 시스템이 모델 정보 없이 표시되는 이유는 무엇입니까?

일반적으로 이는 시스템에 설치된 펌웨어 버전이 권장되는 최소 요구 사항과 일치하지 않음을 나타냅니다. 경우에 따라 시스템에 펌웨어 업데이트가 등록되어 있지 않을 수 있습니다. 시스템을 콜드 부팅하거나 블레이드를 다시 장착하면 이 문제가 해결됩니다. OpenManage Integration for VMware vCenter에 모델 정보와 NIC 정보를 제공하려면 iDRAC에 새로 활성화된 계정을 비활성화하고 자동 검색을 다시 시작해야 합니다.

NFS 공유가 ESX/ESXI ISO와 함께 설치되었지만 공유 위치 탑재 오류로 인해 배포가 실패했습니다.

해결 방법을 찾으려면 다음을 수행하십시오.

1. iDRAC가 어플라이언스를 ping할 수 있는지 확인합니다.
2. 네트워크 실행 속도가 너무 느리지 않은지 확인합니다.

가상 어플라이언스를 강제로 제거하는 방법은 무엇입니까?

1. **https://<vcenter_serverIPAddress>/mob**로 이동합니다.
2. VMware vCenter 관리자 자격 증명을 입력합니다.
3. **Content(콘텐츠)** 를 클릭합니다.

4. **ExtensionManager**를 클릭합니다.
5. **UnregisterExtension**을 클릭합니다.
6. `com.dell.plugin.openManage_integration_for_VMware_vCenter` 확장 키를 입력하고 **Invoke method(방법 호출)**를 클릭합니다.
7. OpenManage Integration for VMware vCenter 가상 어플라이언스를 끄고 삭제합니다.

지금 백업 화면에 암호를 입력하면 오류 메시지 표시

저해상도 모니터를 사용하는 경우 지금 백업 창에 암호화 암호 필드가 표시되지 않습니다. 암호화 암호를 입력하려면 페이지를 아래로 스크롤해야 합니다.

펌웨어 업데이트에 실패했습니다. 어떻게 해야 합니까?

작업 시간이 초과되었는지 확인하기 위해 가상 어플라이언스 로그를 확인합니다. 시간이 초과된 경우 콜드 재부팅을 수행하여 iDRAC를 다시 설정해야 합니다. 시스템이 설치되고 실행되면 펌웨어 탭을 사용하거나 인벤토리를 실행하여 업데이트에 성공했는지 확인합니다.

내 vCenter 업데이트에 실패했습니다. 어떻게 해야 합니까?

통신 문제로 인해 vCenter 등록에 실패할 수 있으므로 이러한 문제가 발생하는 경우 해결할 수 있는 하나의 방법은 정적 IP 주소를 사용하는 것입니다. 정적 IP 주소를 사용하려면 OpenManage Integration for VMware vCenter의 Console(콘솔) 탭에서 **Configure Network(네트워크 구성) → Edit Devices(장치 편집)**를 선택하고 올바른 **게이트웨이**와 **FQDN**(정규화된 도메인 이름)을 입력합니다. Edit DNS Config(DNS 구성 편집) 아래에 DNS 서버 이름을 입력합니다.

노트: 가상 어플라이언스에서 입력한 DNS 서버를 확인할 수 있는지 확인하십시오.

연결 프로필 테스트 자격 증명의 수행 속도가 매우 느리거나 응답하지 않습니다.

서버의 iDRAC에 하나의 사용자(예: 루트)만 있고 사용자가 비활성 상태이거나 모든 사용자가 비활성 상태입니다. 비활성 상태의 서버와 통신하면 지연이 발생합니다. 이 문제를 해결하려면 서버의 비활성 상태를 수정하거나 서버에서 iDRAC를 다시 설정하여 루트 사용자를 기본 설정으로 다시 활성화합니다.

비활성 상태의 서버를 수정하려면 다음을 수행하십시오.

1. Chassis Management Controller(섀시 관리 컨트롤러) 콘솔을 열고 비활성화된 서버를 선택합니다.
2. iDRAC 콘솔을 자동으로 열려면 **Launch iDRAC GUI(iDRAC GUI 시작)**를 클릭합니다.
3. iDRAC 콘솔에서 사용자 목록을 탐색하고 다음 중 하나를 선택합니다.
   - iDRAC 6: **iDRAC settings(iDRAC 설정) → Network/Security tab(네트워크/보안 탭) → Users tab(사용자 탭)**을 선택합니다.
   - iDRAC 7: **iDRAC settings(iDRAC 설정) → Users tab(사용자 탭)**을 선택합니다.
   - iDRAC 8: **iDRAC settings(iDRAC 설정) → Users tab(사용자 탭)**을 선택합니다.
4. 설정을 편집하려면 User ID(사용자 ID) 열에서 관리(루트) 사용자에 대한 링크를 클릭합니다.
5. **Configure User(사용자 구성)**를 클릭하고 **Next(다음)**를 클릭합니다.
6. 선택한 사용자의 User Configuration(사용자 구성) 페이지에서 Enable user(사용자 활성화) 옆에 있는 확인란을 선택하고 **Apply(적용)**를 클릭합니다.

OpenManage Integration for VMware vCenter에서 VMware vCenter 서버 어플라이언스를 지원합니까?

예, OpenManage Integration for VMware vCenter에서 VMware vCenter 서버 어플라이언스를 지원합니다.

OpenManage Integration for VMware vCenter에서 vSphere 웹 클라이언트를 지원합니까?

예, OpenManage Integration for VMware vCenter에서 VMware vSphere 웹 클라이언트를 지원합니다.

Administration Console에서, 어플라이언스를 공장 설정으로 재설정한 이후에도 왜 업데이트 리포지토리 경로가 기본 경로로 설정되지 않습니까?

어플라이언스를 재설정한 후, Administration Console로 가서 왼쪽 창의 **APPLIANCE MANAGEMENT(어플라이언스 관리)**를 클릭합니다. **기기 설정** 페이지의 **업데이트 리포지토리 경로**가 기본 경로로 변경되지 않았습니다.

해결 방법: Administration Console에서 **기본 업데이트 리포지토리** 필드의 경로를 수동으로 복사하여 **업데이트 리포지토리 경로** 필드에 입력합니다.

OpenManage Integration for VMware vCenter의 백업 및 복원 후 왜 알람 설정이 복원되지 않습니까?

OpenManage Integration for VMware vCenter 어플라이언스 백업 복원은 모든 알람 설정을 복원하지 않습니다. 그러나, OpenManage Integration for VMware GUI의 **알람 및 이벤트** 필드에 복원된 설정을 표시합니다.

해결 방법: OpenManage Integration for VMware GUI의 **Manage(관리) → Settings(설정)** 탭에서 **이벤트 및 알람** 설정을 수동으로 변경합니다.

운영 체제 미설치(Bare Metal) 배포 문제

이 섹션에서는 배포 프로세스 중에 발견된 문제에 대해 다룹니다.

자동 검색 및 핸드쉐이크 필수 구성 요소

- 자동 검색 및 핸드쉐이크를 실행하기 전에 iDRAC 및 Lifecycle Controller 펌웨어와 BIOS 버전이 최소 권장 사항에 일치하는지 확인합니다.
- CSIOR이 시스템 또는 iDRAC에서 한 번 이상 실행되어야 합니다.

하드웨어 구성 오류

- 배포 작업을 시작하기 전에 시스템에서 CSIOR을 완료하고 재부팅이 진행 중이 아닌지 확인합니다.
- 참조 서버가 동일한 시스템이 되도록 BIOS 구성을 클론 모드에서 실행하는 것이 좋습니다.
- 일부 컨트롤러에서는 하나의 드라이브에 RAID 0 어레이를 생성하는 것을 허용하지 않습니다. 이 기능은 하이엔드 컨트롤러에서만 지원되고 이러한 하드웨어 프로필을 적용하면 오류가 발생할 수 있습니다.

새로 구입한 시스템에서 자동 검색 활성화

기본적으로 호스트 시스템의 자동 검색 기능은 활성화되지 않습니다. 대신 구입할 때 활성화를 요청해야 합니다. 구입할 때 자동 검색 활성화를 요청하면 iDRAC에서 DHCP가 활성화되고 관리 계정이 비활성화됩니다. iDRAC에 대해 고정 IP 주소를 구성할 필요는 없습니다. 이러한 주소는 네트워크의 DHCP 서버에서 가져옵니다. 자동 검색 기능을 사용하려면 DHCP 서버, DNS 서버 또는 둘 모두에서 검색 프로세스를 지원하도록 구성해야 합니다. CSIOR은 공장 프로세스에서 이미 실행되었습니다. 자동 검색을 지원하도록 네트워크를 설정하는 방법에 대한 자세한 내용은 Dell 자동 검색 네트워크 설치 사양(**http://attachments.wetpaintserv.us/xBUlrs4t%2B2TzbrwqYkblvQ%3D%3D2 62254**)을 참조하십시오.

구입할 때 자동 검색을 요청하지 않은 경우 다음과 같이 활성화할 수 있습니다.

1. 부팅 프로세스를 수행하는 동안 **<Ctrl-E>**를 누릅니다.
2. iDRAC setup(iDRAC 설정) 창에서 NIC(블레이드 서버만)를 활성화합니다.
3. Auto-Discovery(자동 검색)를 활성화합니다.
4. DHCP를 활성화합니다.
5. 관리 계정을 비활성화합니다.
6. **DHCP에서 DNS 서버 주소 가져오기**를 활성화합니다.
7. **DHCP에서 DNS 도메인 이름 가져오기**를 활성화합니다.
8. **프로비저닝 서버** 필드에 다음을 입력합니다.

   `<OpenManage Integration virtual appliance IPaddress>:4433`

Dell사에 문의하기

노트: 인터넷 연결을 사용할 수 없는 경우에는 제품 구매서, 포장 명세서, 청구서 또는 Dell 제품 카탈로그에서 연락처 정보를 찾을 수 있습니다.

Dell은 다양한 온라인/전화 기반의 지원 및 서비스 옵션을 제공합니다. 제공 여부는 국가/지역 및 제품에 따라 다르며 일부 서비스는 소재 지역에 제공되지 않을 수 있습니다. 판매, 기술 지원 또는 고객 서비스 문제에 대해 Dell에 문의하려면

1. **dell.com/support**를 방문하십시오.
2. 지원 카테고리를 선택합니다.
3. 페이지 상단의 Choose a Country/Region(국가/지역 선택) 드롭다운 메뉴에서 소재 국가 또는 지역이 있는지 확인합니다.
4. 필요한 서비스 또는 지원 링크를 선택하십시오.

OpenManage Integration for VMware vCenter 관련 정보

- PowerEdge™ 서버의 Dell 서버 문서 보기 또는 다운로드
  http://www.dell.com/poweredgemanuals
- Dell OpenManage System Administrator 문서
  http:// www.delltechcenter.com/omsa
- Dell Lifecycle Controller 문서
  http://www.dell.com/enterprisemanagement

8

Dell PowerEdge 서버의 가상화 관련 이벤트

다음 표는 11세대, 12세대 및 13세대 PowerEdge 서버의 이벤트 이름, 설명 및 심각도를 포함한 가상화 관련 위험 및 경고 이벤트를 포함합니다.

표 5. 11세대, 12세대 및 13세대 PowerEdge 서버의 가상화 관련 이벤트

이벤트 이름	설명	심각도	권장 작업
Dell-Current sensor detected a warning value	지정된 시스템의 전류 센서가 경고 임계값을 초과했습니다.	경고	작업 안 함
Dell-Current sensor detected a failure value	지정된 시스템의 전류 센서가 오류 임계값을 초과했습니다.	오류	시스템을 유지 보수 모두에 배치
Dell-Current sensor detected a non-recoverable value	지정된 시스템의 전류 센서가 복구할 수 없는 오류를 감지함	오류	작업 안 함
Dell-Redundancy regained	정상 값으로 반환된 센서	정보	작업 안 함
Dell-Redundancy degraded	지정된 시스템의 중복성 센서가 중복 단위의 구성 요소 중 하나가 실패하지만 장치가 계속해서 중복됨을 감지했습니다.	경고	작업 안 함
Dell - Redundancy lost	지정된 시스템의 중복성 센서가 중복 단위의 구성 요소 중 하나의 연결이 해제되고 오류가 발생했거나 현재 없음을 감지했습니다.	오류	시스템을 유지 보수 모두에 배치
Dell - Power supply returned to normal	정상 값으로 반환된 센서	정보	작업 안 함
Dell - Power supply detected a warning	지정된 시스템에서 전원 공급 장치 센서 수치가 사용자 정의 가능한 경고 임계값을 초과했습니다.	경고	작업 안 함
Dell - Power supply detected a failure	전원 공급 장치의 연결이 해제되었거나 오류가 발생했습니다.	오류	시스템을 유지 보수 모두에 배치

Dell - Power supply sensor detected a non-recoverable value	지정된 시스템의 전원 공급 장치가 복구할 수 없는 오류를 감지했습니다.	오류	작업 안 함
Dell - Memory Device Status warning	메모리 장치 수정 등급이 적정 값을 초과했습니다.	경고	작업 안 함
Dell - Memory Device error	메모리 장치 수정 등급이 적정 수준을 초과했거나 메모리 스페어 뱅크가 활성화되었거나 멀티 비트 ECC 오류가 발생했습니다.	오류	시스템을 유지 보수 모두에 배치
Dell - Fan enclosure inserted into system	정상 값으로 반환된 센서	정보	작업 안 함
Dell - Fan enclosure removed from system	지정된 시스템에서 팬 인클로저가 제거되었습니다.	경고	작업 안 함
Dell - Fan enclosure removed from system for an extended amount of time	사용자 정의 가능한 기간 동안 지정된 시스템에서 팬 인클로저가 제거되었습니다.	오류	작업 안 함
Dell - Fan enclosure sensor detected a non-recoverable value	지정된 시스템의 팬 인클로저 센서가 복구할 수 없는 오류를 감지했습니다.	오류	작업 안 함
Dell - AC power has been restored	정상 값으로 반환된 센서	정보	작업 안 함
Dell - AC power has been lost warning	AC 전원 코드에서 전원이 손실되었지만 경고로 분류될 만큼 중복됩니다.	경고	작업 안 함
Dell - An AC power cord has lost its power	AC 전원 코드에서 전원이 손실되고 오류로 분리되기에는 중복성이 부족합니다.	오류	작업 안 함
Dell - Processor sensor returned to a normal value	정상 값으로 반환된 센서	정보	작업 안 함
Dell - Processor sensor detected a warning value	지정된 시스템의 프로세서 센서가 정체 상태입니다.	경고	작업 안 함
Dell - Processor sensor detected a failure value	지정된 시스템의 프로세서 센서가 비활성화되고 구성 오류가 발생했거나 가열 트립이 발생했습니다.	오류	작업 안 함

Dell - Processor sensor detected a non-recoverable value	지정된 시스템의 프로세서 센서에 오류가 발생했습니다.	오류	작업 안 함
Dell - Device configuration error	지정된 시스템의 플러그형 장치에 대한 구성 오류가 감지되었습니다.	오류	작업 안 함
Dell - Battery sensor returned to a normal value	정상 값으로 반환된 센서	정보	작업 안 함
Dell - Battery sensor detected a warning value	지정된 시스템의 배터리 센서가 배터리의 예상 오류 상태에 있음을 감지했습니다.	경고	작업 안 함
Dell - Battery sensor detected a failure value	지정된 시스템의 배터리 센서가 배터리에 오류가 있음을 감지했습니다.	오류	작업 안 함
Dell - Battery sensor detected a nonrecoverable value	지정된 시스템의 배터리 센서가 배터리에 오류가 있음을 감지했습니다.	오류	작업 안 함
Dell - Thermal shutdown protection has been initiated	오류 이벤트로 인해 시스템에 가열 종료가 구성된 경우 이 메시지가 생성됩니다. 온도 센서 수치가 시스템에 구성된 오류 임계값을 초과하는 경우 운영 체제가 종료되고 시스템의 전원이 꺼집니다. 연장된 기간 동안 시스템에서 팬 인클로저가 제거된 경우 특정 시스템에서 이 이벤트가 시작될 수도 있습니다.	오류	작업 안 함
Dell - Temperature sensor returned to a normal value	정상 값으로 반환된 센서	정보	작업 안 함
Dell - Temperature sensor detected a warning value	지정된 시스템에 있는 후면판 보드, 시스템 보드, CPU 또는 드라이브 이동 장치의 온도 센서가 경고 임계값을 초과했습니다.	경고	작업 안 함
Dell - Temperature sensor detected a failure value	지정된 시스템에 있는 후면판 보드, 시스템 보드, 또는 드라이브 이동 장치의 온도 센서가 오류 임계값을 초과했습니다.	오류	시스템을 유지 보수 모두에 배치

Dell - Temperature sensor detected a non-recoverable value	지정된 시스템에 있는 후면판 보드, 시스템 보드 또는 드라이브 이동 장치의 온도 센서가 복구할 수 없는 오류를 감지했습니다.	오류	작업 안 함
Dell - Fan sensor returned to a normal value	정상 값으로 반환된 센서	정보	작업 안 함
Dell - Fan sensor detected a warning value	호스트 <x>의 팬 센서 수치가 경고 임계값을 초과했습니다.	경고	작업 안 함
Dell - Fan sensor detected a failure value	지정된 시스템의 팬 센서가 하나 이상의 팬에서 오류를 감지했습니다.	오류	시스템을 유지 보수 모두에 배치
Dell - Fan sensor detected a nonrecoverable value	팬 센서가 복구할 수 없는 오류를 감지했습니다.	오류	작업 안 함
Dell - Voltage sensor returned to a normal value	정상 값으로 반환된 센서	정보	작업 안 함
Dell - Voltage sensor detected a warning value	지정된 시스템의 전압 센서가 경고 임계값을 초과했습니다.	경고	작업 안 함
Dell - Voltage sensor detected a failure value	지정된 시스템의 전압 센서가 오류 임계값을 초과했습니다.	오류	시스템을 유지 보수 모두에 배치
Dell - Voltage sensor detected a nonrecoverable value	지정된 시스템의 전압 센서가 복구할 수 없는 오류를 감지했습니다.	오류	작업 안 함
Dell - Current sensor returned to a normal value	정상 값으로 반환된 센서	정보	작업 안 함
Dell - Storage: storage management error	저장소 관리에서 장치에 종속되지 않는 오류 상태를 감지했습니다.	오류	시스템을 유지 보수 모두에 배치
Dell - Storage: Controller warning	컨트롤러 경고입니다. 자세한 내용은 vSphere 클라이언트에서 작업 및 이벤트 탭을 참조하십시오.	경고	작업 안 함
Dell - Storage: Controller failure	컨트롤러 오류입니다. 자세한 내용은 vSphere 클라이언트에서 작업 및 이벤트 탭을 참조하십시오.	오류	시스템을 유지 보수 모두에 배치
Dell - Storage: Channel Failure	채널 오류가 발생했습니다.	오류	시스템을 유지 보수 모두에 배치
Dell - Storage: Enclosure hardware information	인클로저 하드웨어 정보입니다.	정보	작업 안 함

Dell - Storage: Enclosure hardware warning	인클로저 하드웨어 경고입니다.	경고	작업 안 함
Dell - Storage: Enclosure hardware failure	인클로저 하드웨어 오류입니다.	오류	시스템을 유지 보수 모두에 배치
Dell - Storage: Array disk failure	어레이 디스크 오류입니다.	오류	시스템을 유지 보수 모두에 배치
Dell - Storage: EMM failure	EMM 오류입니다.	오류	시스템을 유지 보수 모두에 배치
Dell - Storage: power supply failure	전원 공급 장치 오류입니다.	오류	시스템을 유지 보수 모두에 배치
Dell - Storage: temperature probe warning	너무 차갑거나 너무 뜨거운 실제 디스크 온도 센서 경고입니다.	경고	작업 안 함
Dell - Storage: temperature probe failure	너무 차갑거나 너무 뜨거운 실제 디스크 온도 센서 오류입니다.	오류	시스템을 유지 보수 모두에 배치
Dell - Storage: Fan failure	팬 오류입니다.	오류	시스템을 유지 보수 모두에 배치
Dell - Storage: Battery warning	배터리 경고입니다.	경고	작업 안 함
Dell - Storage: Virtual disk degraded warning	가상 디스크 성능이 저하됨 경고	경고	작업 안 함
Dell - Storage: Virtual disk degraded failure	가상 디스크 성능 저하 오류	오류	시스템을 유지 보수 모두에 배치
Dell - Storage: Temperature probe information	온도 센서 정보	정보	작업 안 함
Dell - Storage: Array disk warning	어레이 디스크 경고입니다.	경고	작업 안 함
Dell - Storage: Array disk information	어레이 디스크 정보입니다.	정보	작업 안 함
Dell - Storage: Power supply warning	전원 공급 장치 경고입니다.	경고	작업 안 함
Dell - Chassis Intrusion - Physical Security Violation	섀시 침입 - 물리적 보안 위반	오류	작업 안 함
Dell - Chassis Intrusion(Physical Security Violation) Event Cleared	섀시 침입(물리적 보안 위반) 이벤트가 지워짐	정보	작업 안 함
Dell - CPU Presence (Processor Presence detected)	CPU 있음(프로세서가 감지됨)	정보	작업 안 함

Dell - System Event Log (SEL) Full (Logging Disabled)	시스템 이벤트 로그(SEL) 전체(로깅이 비활성화됨)	오류	작업 안 함
Dell - System Event Log (SEL) Cleared	시스템 이벤트 로그(SEL)가 지워짐	정보	작업 안 함
Dell - SD Card redundancy Has Returned to Normal	SD 카드 중복성이 정상으로 반환됨	정보	작업 안 함
Dell - SD Card Redundancy has been Lost	SD 카드 중복성이 손실됨	오류	작업 안 함
Dell - SD Card Redundancy Degraded	SD 카드 중복성이 저하됨	경고	작업 안 함
Dell - Module SD Card Present (SD Card Presence Detected)	모듈 SD 카드가 있음(SD 카드가 감지됨)	정보	작업 안 함
Dell - Module SD Card Failed (Error)	모듈 SD 카드 실패(오류)	오류	작업 안 함
Dell - Module SD Card Write Protect(Warning)	모듈 SD 카드 쓰기 금지(경고)	경고	작업 안 함
Dell - Module SD Card not Present	모듈 SD 카드 없음	정보	작업 안 함
Dell - Watchdog Timer Expired	감시 장치 타이머가 만료됨	오류	작업 안 함
Dell - Watchdog Reset	감시 장치가 재설정됨	오류	작업 안 함
Dell - Watchdog Power Down	감시 장치의 전원이 꺼짐	오류	작업 안 함
Dell - Watchdog Power cycle	감시 장치 전원 주기	오류	작업 안 함
Dell - System Power Exceeds PSU Wattage	시스템 전원이 PSU 와트를 초과함	오류	작업 안 함
Dell - System Power Exceeds Error Cleared	시스템 전원이 소거된 오류를 초과함	정보	작업 안 함
Dell - Power Supply Inserted	전원 공급 장치가 삽입됨	정보	작업 안 함
Dell - Internal Dual SD Module is present	내부 듀얼 SD 모듈이 있음	정보	작업 안 함
Dell - Internal Dual SD Module is online	내부 듀얼 SD 모듈이 온라인 상태임	정보	작업 안 함
Dell - Internal Dual SD Module is operating normally	내부 듀얼 SD 모듈이 정상적으로 작동함	정보	작업 안 함

Dell - Internal Dual SD Module is write protected	내부 듀얼 SD 모듈의 쓰기가 금지됨	경고	작업 안 함
Dell - Internal Dual SD Module is writable	내부 듀얼 SD 모듈이 쓰기 가능함	정보	작업 안 함
Dell - Integrated Dual SD Module is absent	통합 듀얼 SD 모듈이 없음	오류	작업 안 함
Dell - Integrated Dual SD Module redundancy is lost	통합 듀얼 SD 모듈 중복성이 손실됨	오류	작업 안 함
Dell - Internal Dual SD Module is redundant	내부 듀얼 SD 모듈이 중복됨	정보	작업 안 함
Dell - Internal Dual SD Module is not redundant	내부 듀얼 SD 모듈이 중복되지 않음	정보	작업 안 함
Dell - Integrated Dual SD Module failure	통합 듀얼 SD 모듈 오류	오류	작업 안 함
Dell - Internal Dual SD Module is offline	내부 듀얼 SD 모듈이 오프라인 상태임	경고	작업 안 함
Dell - Integrated Dual SD Module redundancy is degraded	통합 듀얼 SD 모듈 중복성이 저하됨	경고	작업 안 함
Dell - SD card device has detected a warning	SD 카드 장치가 경고를 감지함	경고	작업 안 함
Dell - SD card device has detected a failure	SD 카드 장치가 오류를 감지함	오류	작업 안 함
Dell - Integrated Dual SD Module warning	통합 듀얼 SD 모듈 경고	경고	작업 안 함
Dell - Integrated Dual SD Module information	통합 듀얼 SD 모듈 정보	정보	작업 안 함
Dell - Integrated Dual SD Module redundancy information	통합 듀얼 SD 모듈 중복성 정보	정보	작업 안 함
Dell - Network failure or critical event	네트워크 오류 또는 중요 이벤트	오류	작업 안 함
Dell - Network warning	네트워크 경고	경고	작업 안 함
Dell - Network information	네트워크 정보	정보	작업 안 함
Dell - Physical disk failure	실제 디스크 오류	오류	작업 안 함
Dell - Physical disk warning	실제 디스크 경고	경고	작업 안 함
Dell - Physical disk information	실제 디스크 정보	정보	작업 안 함
Dell - An error was detected for a PCI device	PCI 장치에 대한 오류가 감지됨	오류	작업 안 함

Dell - A warning event was detected for a PCI device	PCI 장치에 대한 경고 이벤트가 감지됨	경고	작업 안 함
Dell - An informational event was detected for a PCI device	PCI 장치에 대한 정보 이벤트가 감지됨	정보	작업 안 함

A

자동 검색 이해

자동 검색은 OpenManage Integration for VMware vCenter에서 사용할 수 있도록 사용 가능한 서버의 풀에 Dell PowerEdge 11세대, 12세대, 또는 13세대 운영 체제 미설치 서버를 추가하는 프로세스입니다. 서버가 검색되면 하이퍼바이저 및 하드웨어 배포에 해당 서버를 사용합니다. 이 부록에서는 시스템 구성에 도움이 되도록 자동 검색에 대한 충분한 정보를 제공합니다. 자동 검색은 새 서버를 설정하고 콘솔을 사용하여 해당 서버를 등록하는 Lifecycle Controller 기능입니다. 이 기능을 사용하면 번거롭게 새 서버의 수동 로컬 구성을 수행할 필요가 없으며, 콘솔에 대해 자동화된 방법으로 네트워크와 전원에 연결된 새 서버를 검색할 수 있습니다.

경우에 따라 프로세스에서 자동 검색을 수행한 후 이를 *검색 및 핸드쉐이크*라고 합니다. 자동 검색 기능이 활성화되어 있는 새 서버가 AC 전원과 네트워크에 연결되면 Dell 서버의 Lifecycle Controller가 Dell 프로비저닝 서버와 통합된 배포 콘솔을 *검색*하도록 시도합니다. 그런 다음 자동 검색이 프로비저닝 서버와 Lifecycle Controller 간에 *핸드쉐이크*를 시작합니다.

OpenManage Integration for VMware vCenter는 통합 프로비저닝 서버가 있는 배포 콘솔입니다. 프로비저닝 서버의 위치는 다른 방법을 통해 iDRAC에 제공됩니다. 프로비저닝 서버 위치의 IP 주소 또는 호스트 이름은 OpenManage Integration for VMware vCenter 어플라이언스 가상 시스템의 IP 주소 또는 호스트 이름으로 설정됩니다.

노트: 자동 검색을 수동으로 다시 시작한 후 자동 검색을 위해 구성된 새 서버에서 24시간 동안 90초마다 프로비저닝 서버의 위치를 확인합니다.

OpenManage Integration for VMware vCenter에서 자동 검색 요청을 받으면 SSL 인증서의 유효성을 검사한 후 선택적으로 구성된 보안 절차를 시작합니다(예: 클라이언트 쪽 보안 인증서 및 화이트 리스트에 대한 유효성 검사). 새 서버의 두 번째 유효성 검사 요청이 iDRAC에서 구성할 임시 사용자 이름/암호 자격 증명을 반환합니다. OpenManage Integration for VMware vCenter에서 후속 호출이 시작되며, 이를 통해 서버에 대한 정보를 수집하고, 임시 자격 증명을 제거하고, 관리 액세스를 위해 추가 영구 사용자 정의 자격 증명을 구성할 수 있습니다.

자동 검색에 성공하면 **Settings(설정) → Deployment(배포)**페이지에 제공되는 배포 자격 증명이 대상 iDRAC에 생성됩니다. 그런 다음 자동 검색 기능이 꺼집니다. 그러면 OpenManage Integration for VMware vCenter의 Deployment(배포) 아래에 있는 사용 가능한 운영 체제 미설치 서버의 풀에 서버가 표시됩니다.

현재 vSphere Desktop 클라이언트를 통해 자동 검색을 수행할 수 있습니다.

자동 검색 필수 조건

Dell PowerEdge 11세대나 12세대 이후 세대 운영 체제 미설치 서버를 검색하기 전에 OpenManage Integration for VMware vCenter를 설치합니다. iDRAC Express 또는 iDRAC Enterprise를 포함한 Dell PowerEdge 11세대 이후의 서버만 OpenManage Integration for VMware vCenter의 운영 체제 미설치 풀에서 검색될 수 있습니다. Dell의 운영 체제 미설치 서버의 iDRAC과 OpenManage Integration for VMware vCenter의 가상 머신의 연결이 필요합니다.

노트: 기존 하이퍼바이저가 있는 호스트가 OpenManage Integration for VMware vCenter에서 검색되지 않으므로 대신 연결 프로필에 하이퍼바이저를 추가한 후 호스트 준수 마법사를 사용하여 OpenManage Integration for VMware vCenter와 조정합니다.

자동 검색을 수행하려면 다음 조건을 충족해야 합니다.

- **전원:** 서버를 전원 콘센트에 연결합니다. 서버의 전원을 켤 필요가 없습니다.
- **네트워크 연결:** 서버의 iDRAC에 네트워크가 연결되고 포트 4433을 통해 프로비저닝 서버와 통신해야 합니다. DHCP 서버를 사용하여 IP 주소를 가져오거나 iDRAC 구성 유틸리티에서 수동으로 지정할 수 있습니다.

- **추가 네트워크 설정:** DHCP를 사용하는 경우 DNS 이름이 해석되도록 *Get DNS server address from DHCP(DHCP 에서 DNS 서버 주소 가져오기)* 설정을 활성화합니다.
- **프로비저닝 서비스 위치:** iDRAC에서 프로비저닝 서비스 서버의 IP 주소 또는 호스트 이름을 알고 있어야 합니다.
- **계정 액세스가 비활성화됨:** iDRAC에 대한 관리 계정 액세스를 활성화하고 관리자 권한이 있는 iDRAC 계정이 있는 경우 먼저 iDRAC 웹 콘솔 내에서 비활성화합니다. 자동 검색이 완료되면 관리 iDRAC 계정이 다시 활성화됩니다.
- **자동 검색이 활성화됨:** 자동 검색 프로세스를 시작할 수 있도록 서버의 iDRAC에 자동 검색이 활성화되어 있어야 합니다.

iDRAC 서버에서 관리 계정 활성화 또는 비활성화

자동 검색을 설정하기 전에 루트 이외의 모든 관리 계정을 비활성화합니다. 자동 검색 절차를 수행하는 동안 루트 계정이 비활성화됩니다. 자동 검색이 성공적으로 설정되면 통합 Dell Remote Access Controller 6 GUI로 돌아가 꺼져 있는 계정을 다시 활성화합니다. 이 절차는 Dell PowerEdge 11세대, 12세대 및 13세대 서버에 적용됩니다.

노트: 자동 검색이 실패하지 않도록 보호하기 위해 iDRAC에서 비관리 계정을 활성화할 수 있습니다. 이렇게 하면 자동 검색이 실패할 경우 원격 액세스를 수행할 수 있습니다.

1. 브라우저에 **iDRAC IP address(iDRAC IP 주소)**를 입력합니다.
2. **Integrated Dell Remote Access Controller GUI(통합 Dell Remote Access Controller GUI)**에 로그인합니다.
3. 다음 중 하나를 수행합니다.
   - iDRAC6의 경우: 왼쪽 창에서 **iDRAC Settings(iDRAC 설정) → Network/Security(네트워크/보안) → Users(사용자)** 탭을 선택합니다.
   - iDRAC7의 경우: 왼쪽 창에서 **iDRAC Settings(iDRAC 설정) → Authentication(인증) → Users(사용자)** 탭을 선택합니다.
4. Users(사용자) 탭에서 루트 이외의 관리 계정을 찾습니다.
5. 계정을 비활성화하려면 User ID(사용자 ID) 아래에서 **ID**를 선택합니다.
6. **Next(다음)**을 클릭합니다.
7. User Configuration(사용자 구성) 페이지의 General(일반) 아래에서 **Enable User(사용자 활성화)** 확인란을 선택 취소합니다.
8. **Apply(적용)**를 클릭합니다.
9. 자동 검색을 성공적으로 설정한 후 계정을 각각 다시 활성화하려면 1단계 - 8단계를 반복합니다. 그러나 이 경우에는 **Enable User(사용자 활성화)** 확인란을 선택하고 **Apply(적용)**를 클릭합니다.

서버 자동 검색을 위한 수동 구성(11세대 PowerEdge 서버)

iDRAC와 호스트 IP 주소가 있어야 합니다.
출하 시 자동 검색을 사용하도록 운영 체제 미설치 어플라이언스를 주문하지 않은 경우 수동으로 설치할 수 있습니다. iDRAC에는 두 개의 사용자 인터페이스가 있으며, 둘 모두 설정할 iDRAC의 IP 주소를 통해 연결됩니다.

운영 체제 미설치 서버의 자동 검색이 완료되면 새 관리자 계정이 생성되거나 기존 계정이 핸드쉐이크 서비스에 의해 반환된 자격 증명을 통해 활성화됩니다. 자동 검색 이전에 비활성 상태였던 기타 모든 관리 계정은 활성화되지 않습니다. 자동 검색이 완료된 후 이러한 관리자 계정을 다시 활성화해야 합니다. iDRAC에서 관리 계정 활성화 또는 비활성화를 참조하십시오.

노트: 어떠한 이유로 자동 검색이 성공적으로 완료되지 않은 경우 iDRAC에 원격으로 연결할 수 없습니다. 원격 연결을 수행하려면 iDRAC에 비관리 계정이 활성화되어 있어야 합니다. iDRAC에 활성화된 계정이 없으면 로컬에서 상자에 로그인하여 iDRAC에서 계정을 활성화해야 iDRAC에 액세스할 수 있습니다.

1. 브라우저에 **iDRAC IP** 주소를 입력합니다.
2. **iDRAC Enterprise GUI**에 로그인합니다.
3. 가상 콘솔 미리 보기의 **Integrated Dell Remote Access Controller 6 — Enterprise → Summary(요약)**탭에서 **Launch(실행)**를 클릭합니다.
4. Warning — Security(경고 - 보안) 대화 상자에서 **Yes(예)**를 클릭합니다.
5. iDRAC 유틸리티 콘솔에서 **F12** 키를 한 번 또는 두 번 눌러 Authentication Required(인증 필요) 대화 상자를 표시합니다.
6. Authentication Required(인증 필요) 대화 상자에 이름이 표시되면 **Enter(확인)** 키를 누릅니다.
7. **Password(암호)**를 입력합니다.
8. **Enter(확인)** 키를 누릅니다.
9. Shutdown/Restart(종료/다시 시작) 대화 상자가 표시되면 **F11** 키를 누릅니다.
10. 호스트가 다시 시작되고 화면에 메모리 로드, RAID 및 iDRAC가 표시되는 경우에 대한 정보가 표시되고 Ctrl +E를 누르라는 메시지가 표시됩니다. 이제 즉시 **Ctrl+E**를 누릅니다.

    이 대화 상자가 표시되면 작업이 작동됩니다. 그렇지 않은 경우 전원 메뉴로 이동하여 전원을 끄고 다시 켠 후 이 단계를 반복합니다.

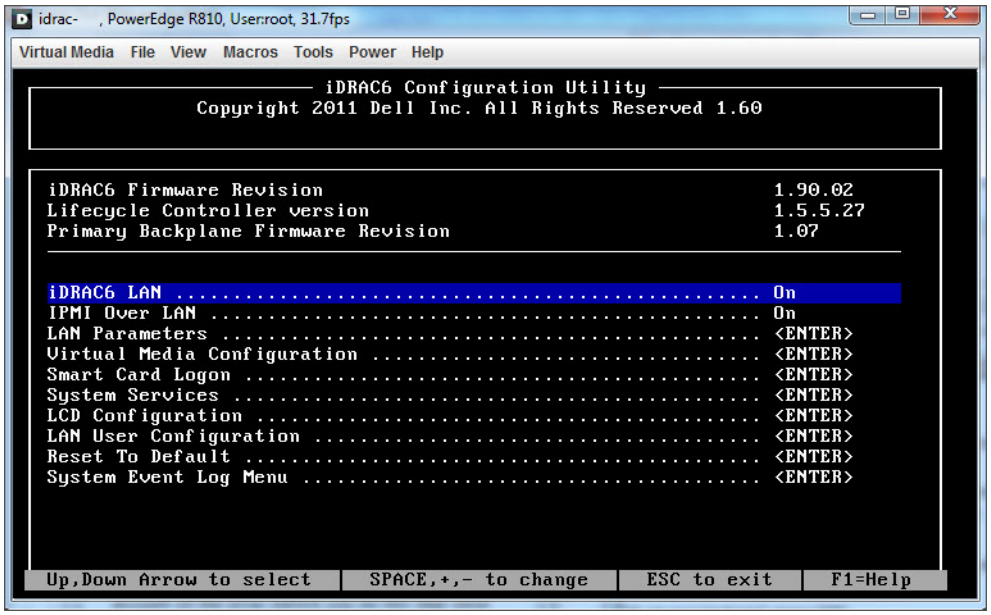

그림 6 . Ctrl+E를 눌러 이 화면을 활성화합니다.

11. iDRAC6 구성 유틸리티에서 화살표 키를 사용하여 **LAN Parameters(LAN 매개변수)**를 선택합니다.
12. **Enter(확인)** 키를 누릅니다.
13. 이 호스트가 블레이드인 경우 NIC를 구성하려면 스페이스바를 사용하여 옵션을 **Enabled(활성화됨)**로 전환합니다.
14. DHCP를 사용하는 경우 화살표 키를 사용하여 **Domain Name from DHCP(DHCP의 도메인 이름)**를 선택합니다.
15. 스페이스바를 사용하여 옵션을 **On(켜짐)**으로 전환합니다.
16. DHCP를 사용하는 경우 화살표 키를 사용하여 IPv4 설정을 탐색하고 **DNS Servers from DHCP(DHCP의 DNS 서버)**를 선택합니다.

17. 스페이스바를 사용하여 옵션을 **On(켜짐)**으로 전환합니다.
18. 종료하려면 키보드에서 **ESC** 키를 누릅니다.
19. 화살표 키를 사용하여 **LAN User Configuration(LAN 사용자 구성)**을 선택합니다.
20. 화살표 키를 사용하여 **Provisioning Server(프로비저닝 서버)**를 선택합니다.
21. **Enter(확인)** 키를 누릅니다.
22. 호스트의 IP 주소를 입력합니다.
23. **Esc** 키를 누릅니다.
24. 화살표 키를 사용하여 **Account Access(계정 액세스)**를 선택합니다.
25. 스페이스바를 사용하여 옵션을 **Disable(비활성)**로 전환합니다.
26. 스페이스바를 사용하여 **Auto-Discovery(자동 검색)**를 선택합니다.
27. 스페이스바를 사용하여 옵션을 **Enabled(활성화됨)**로 전환합니다.
28. 키보드에서 **Esc** 키를 누릅니다.
29. **Esc** 키를 다시 누릅니다.

자동 검색을 위한 서버 수동 구성(12세대 PowerEdge 서버)

iDRAC와 호스트 IP 주소가 있어야 합니다.
출하 시 자동 검색을 사용하도록 운영 체제 미설치 어플라이언스를 주문하지 않은 경우 수동으로 설치할 수 있습니다. iDRAC에는 두 개의 사용자 인터페이스가 있으며, 둘 모두 설정할 iDRAC의 IP 주소를 통해 연결됩니다.

운영 체제 미설치 서버의 자동 검색이 완료되면 새 관리자 계정이 생성되거나 기존 계정이 핸드쉐이크 서비스에 의해 반환된 자격 증명을 통해 활성화됩니다. 자동 검색 이전에 비활성 상태였던 기타 모든 관리 계정은 활성화되지 않습니다. 자동 검색이 완료된 후 이러한 관리자 계정을 다시 활성화합니다. iDRAC에서 관리 계정 활성화 또는 비활성화를 참조하십시오.

노트: 어떠한 이유로 자동 검색이 성공적으로 완료되지 않은 경우 iDRAC에 원격으로 연결할 수 없습니다. 원격 연결을 수행하려면 iDRAC에 비관리 계정이 활성화되어 있어야 합니다. iDRAC에 활성화된 계정이 없으면 로컬에서 상자에 로그인하여 iDRAC에서 계정을 활성화해야 iDRAC에 액세스할 수 있습니다.

1. 브라우저에 **iDRAC IP address(iDRAC IP 주소)**를 입력합니다.
2. **iDRAC Enterprise GUI**에 로그인합니다.
3. 가상 콘솔 미리 보기의 **Integrated Dell Remote Access Controller 7— Enterprise → Summary(요약)**탭에서 **Launch(실행)**를 클릭합니다.
4. Warning — Security(경고 - 보안) 대화 상자에서 **Yes(예)**를 클릭합니다.
5. iDRAC 유틸리티 콘솔에서 **F12** 키를 한 번 또는 두 번 눌러 Authentication Required(인증 필요) 대화 상자를 표시합니다.
6. Authentication Required(인증 필요) 대화 상자에 이름이 표시되면 **Enter** 키를 누릅니다.
7. **Password(암호)**를 입력합니다.
8. **Enter(확인)** 키를 누릅니다.
9. Shutdown/Restart(종료/다시 시작) 대화 상자가 표시되면 **F11** 키를 누릅니다.
10. 호스트가 다시 시작되고 화면에 메모리 로드, RAID 및 Dell 화면에 F2 키를 누르라는 메시지가 표시되는 경우에 대한 정보가 표시됩니다. 이 경우 즉시 **F2** 키를 누릅니다.

    Dell System Setup(Dell 시스템 설정) 화면이 표시될 때까지 기다립니다. Dell System Setup(Dell 시스템 설정)이 표시되는 데 시간이 다소 걸릴 수 있습니다.
11. Dell System Setup(Dell 시스템 설정) 화면에서 화살표 키를 사용하여 **iDRAC Settings(iDRAC 설정)**을 선택합니다.
12. 화살표 키를 사용하여 **Remote Enablement(원격 활성화)**를 선택합니다.
13. 자동 검색을 활성화하려면 **Enable(활성화)**을 클릭합니다.
14. **Esc** 키를 누릅니다.

15. **Esc** 키를 누릅니다.
16. Warning(경고) 화면에서 종료를 확인하려면 **Yes(예)**를 클릭합니다.