웹 클라이언트용 OpenManage Integration for VMware vCenter

사용자 가이드 버전 3.2

2017년 4월
개정 A00

DELL EMC

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.**

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

목차

1

소개

VMware vCenter는 IT 관리자가 VMware vSphere ESX/ESXi 호스트를 관리하고 모니터하는 데 사용하는 기본 콘솔입니다. 표준 가상 환경에서 VMware 경고 및 모니터링을 사용하면 별도의 콘솔을 실행하여 하드웨어 문제를 해결하라는 메시지가 표시됩니다. OpenManage Integration for VMware vCenter는 Windows 시스템에 연결하지 않고도 VMware 웹 클라이언트 내에서 VMware vCenter 서버를 관리할 수 있는 제품입니다. OpenManage Integration for VMware vCenter를 사용하면 관리자가 다음과 같이 가상 환경에서 Dell 하드웨어를 관리하고 모니터할 수 있는 기능을 사용할 수 있습니다.

- 경고 및 환경 모니터링: 주요 하드웨어 오류를 감지하고 가상화 인식 작업을 수행합니다(예: 작업부하 마이그레이션 또는 유지 보수 모드에 호스트 배치).
- 단일 서버 모니터링 및 보고: 서버의 모니터링 및 보고 기능입니다.
- 펌웨어 업데이트: Dell 하드웨어를 최신 버전의 BIOS 및 펌웨어로 업데이트합니다.
- 고급 배포 옵션: 하드웨어 프로필과 하이퍼바이저 프로필을 생성하고 운영 체제 미설치 Dell PowerEdge 서버에서 vCenter를 사용하여 PXE 없이 원격으로 두 프로필을 조합하여 배포합니다.

주제:

OpenManage Integration for VMware vCenter 기능

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 장애를 감지하고 가상화 인식 작업을 수행하십시오. 예를 들어, 워크로드를 마이그레이션하거나 호스트를 유지 관리 모드에 배치합니다. 추가 인텔리전스(인벤토리, 이벤트 및 알림)을 제공하여 서버 문제를 진단합니다. 데이터센터 및 클러스터 보기에서 보고하고 CSV 파일로 내보냅니다.
펌웨어 업데이트	Dell 하드웨어를 최신 버전의 BIOS 및 펌웨어로 업데이트합니다.
배포 및 프로비저닝	하드웨어 프로필과 하이퍼바이저 프로필을 생성하고 운영 체제 미설치 Dell PowerEdge 서버에서 VMware vCenter를 사용하여 PXE 없이 두 프로필을 조합하여 원격으로 배포합니다.
서비스 정보	Dell 온라인에서 보증 정보를 가져옵니다.
보안 역할 및 권한	표준 vCenter 인증, 규칙 및 권한과 통합합니다.

이 릴리스의 새로운 기능

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

- Dell OMSA(OpenManage Server Assistant) 버전 8.5 지원
- VMware vCenter 서버 버전 6.0 U3 지원
- VMware ESXi 버전 6.0 U3 지원
- PowerEdge R830 플랫폼 지원
- 불균일 메모리 액세스(NUMA) 결함 복원 메모리(FRM) 지원

노트: 자동 검색 기능은 이 릴리스에서 작동하지 않습니다. 자세한 내용은 다음을 참조하십시오. OMIVV가 자동 검색 프로세스 중에 프로비저닝 서버로 작동할 수 없음 페이지 107

2

OpenManage Integration for VMware vCenter 구성 또는 편집 방법 이해

OMIVV의 기본 설치를 완료한 후에 OMIVV 아이콘을 클릭하면 **초기 구성 마법사**가 표시됩니다. **초기 구성 마법사**를 사용하여 처음 실행 시 **설정**을 구성합니다. 그 다음부터는 **설정** 페이지를 사용하면 됩니다. **초기 구성 마법사**에서 연결 프로필을 생성하고 보증, 인벤토리, 이벤트 및 알람의 설정을 편집할 수 있습니다. **초기 구성 마법사**는 가장 일반적으로 사용되는 방법이지만 어플라이언스의 OMIVV에서 **OpenManage Integration → 관리 → 설정** 페이지를 통해 이 작업을 수행할 수도 있습니다. 초기 구성 마법사에 대한 자세한 내용은 `dell.com/support/manuals`에 제공되는 *OpenManage Integration for VMware vCenter User Guide(OpenManage Integration for VMWare vCenter 사용 설명서)*를 참조하십시오.

구성 마법사를 사용하는 구성 작업

초기 구성 마법사를 사용하여 단일 vCenter 또는 등록된 모든 vCenter에 대해 다음과 같은 설정을 구성할 수 있습니다.

노트: DNS 설정을 변경한 후 OMIVV 관련 작업을 수행하는 동안 vCenter 웹 클라이언트에서 웹 통신 오류를 확인하려면 다음을 수행하십시오.

- 브라우저 캐시를 지웁니다.
- 웹 클라이언트에서 로그아웃했다가 로그인합니다.

1. vCenter 선택
2. 새 연결 프로필 생성
3. 인벤토리 작업 예약
4. 보증 검색 작업 실행
5. 이벤트 및 알람 구성

노트: **시작하기** 페이지에서 **기본 작업** 아래의 **초기 구성 마법사 시작** 링크를 사용하여 초기 구성 마법사를 실행할 수도 있습니다.

주제:

- 구성 마법사 시작 페이지
- vCenter 선택
- 초기 구성 마법사를 사용하여 새 연결 프로필 생성
- 인벤토리 작업 예약 [마법사]
- 보증 검색 작업 실행 [마법사]
- 이벤트 및 알람 구성 [마법사]

구성 마법사 시작 페이지

OMIVV를 설치한 후에 반드시 구성해야 합니다.

1. **vSphere 웹 클라이언트**에서 **홈**을 클릭한 후 **OpenManage Integration** 아이콘을 클릭합니다.
2. **OpenManage Integration** 아이콘을 처음 클릭하면 **구성 마법사**가 열립니다. **OpenManage Integration** > **시작하기** > **초기 구성 마법사 시작** 페이지에서도 이 마법사에 액세스할 수 있습니다.

vCenter 선택

vCenter 선택 페이지를 사용하여 다음을 구성할 수 있습니다.

- 특정 vCenter
- 사용 가능한 모든 vCenter

1. **초기 구성 마법사**의 **시작** 화면에서 **다음**을 클릭합니다.
2. **vCenter** 드롭다운 목록에서 하나 또는 모든 vCenter를 선택합니다.

아직 구성하지 않았거나 사용자 환경에 새 vCenter를 추가한 경우 개별 vCenter를 선택합니다. vCenter 선택 페이지에서 설정을 구성할 하나 이상의 vCenter를 선택할 수 있습니다.

3. **다음**을 클릭하여 **연결 프로필** 설명 페이지를 계속 진행합니다.

   노트: 여러 vCenter 서버가 동일한 SSO에 속해 있는 경우 단일 vCenter 서버를 구성하도록 선택하면 각 vCenter를 구성할 때까지 다음 단계를 반복해야 합니다.

초기 구성 마법사를 사용하여 새 연결 프로필 생성

연결 프로필은 가상 어플라이언스가 Dell 서버와 통신하기 위해 사용하는 iDRAC 및 호스트 자격 증명을 저장합니다. 각 Dell 서버를 연결 프로필과 연결해야만 OMIVV에서 관리할 수 있습니다. 하나의 연결 프로필에 여러 서버를 할당할 수 있습니다. 구성 마법사를 사용하거나 **OpenManage Integration for VMware vCenter** > **설정**에서 연결 프로필을 생성할 수 있습니다.

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

노트: 연결 프로필과 함께 Active Directory 자격 증명을 사용하기 전에 Active Directory 사용자 계정이 Active Directory에 있어야 하며 iDRAC 및 호스트를 Active Directory 기반 인증에 맞게 구성해야 합니다.

노트: Active Directory 자격 증명은 iDRAC와 호스트에서 동일하거나 별도의 Active Directory 자격 증명으로 설정할 수 있습니다. 사용자 자격 증명에는 관리 권한이 있어야 합니다.

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

구성 마법사를 사용하여 새 연결 프로필을 생성하려면 다음을 수행합니다.

1. **연결 프로필 설명** 페이지에서 **다음**을 클릭합니다.
2. **이름 및 자격 증명** 페이지에서 **연결 프로필 이름** 및 선택 사항인 **연결 프로필 설명**을 입력합니다.
3. **이름 및 자격 증명** 페이지의 **iDRAC 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 **Active Directory 사용**을 선택합니다. 그렇지 않으면 iDRAC 자격 증명 구성 단계로 건너뜁니다.
     - **Active Directory 사용자 이름**에 **사용자 이름**을 입력합니다. 사용자 이름은 **도메인/사용자 이름** 또는 **사용자 이름@도메인** 형식 중 하나로 입력합니다. 사용자 이름은 256자로 제한됩니다. 사용자 이름 제한사항에 대해서는 Microsoft Active Directory 설명서를 참조하십시오.
     - **Active Directory 암호**에 암호를 입력합니다. 암호는 127자로 제한됩니다.
     - **암호 확인**에 암호를 다시 입력합니다.
     - 다음 작업 중 하나를 수행합니다.
       - iDRAC 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화**를 선택합니다.
       - iDRAC 인증서를 저장하지 않고 이후의 모든 연결에서 인증서 확인을 수행하지 않으려면 **인증서 확인 활성화**를 선택 취소합니다.
   - Active Directory 없이 iDRAC 자격 증명을 구성하려면 다음을 수행합니다.
     - **사용자 이름**에 사용자 이름을 입력합니다. 사용자 이름은 16자로 제한됩니다. 사용 중인 iDRAC 버전에서의 사용자 이름 제한사항을 보려면 iDRAC 설명서를 참조하십시오.
     - **암호**에 암호를 입력합니다. 암호는 20자로 제한됩니다.
     - **암호 확인**에 암호를 다시 입력합니다.
     - 다음 작업 중 하나를 수행합니다.
       - iDRAC 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화**를 선택합니다.
       - iDRAC 인증서를 저장하지 않고 이후의 모든 연결에서 인증서 확인을 수행하지 않으려면 **인증서 확인 활성화**를 선택 취소합니다.

4. **호스트 루트** 영역에서 다음 중 하나를 수행합니다.
   - Active Directory를 사용할 호스트가 이미 구성되어 있고 Active Directory에 활성화되어 있으면 **Active Directory 사용**을 선택합니다. 그렇지 않으면 **호스트 자격 증명**을 구성합니다.

- **Active Directory 사용자 이름**에 **사용자 이름**을 입력합니다. 사용자 이름은 **도메인/사용자 이름** 또는 **사용자 이름@도메인** 형식 중 하나로 입력합니다. 사용자 이름은 256자로 제한됩니다.

  호스트 사용자 이름과 도메인 제한 사항에 대해서는 다음을 참조하십시오.

  호스트 사용자 이름 요구 사항:

  a. 1자에서 64자 사이

  b. 인쇄할 수 없는 문자를 사용할 수 없습니다.

  c. 잘못된 문자: "/\ []:; | =, +*? < >@

  호스트 도메인 요구 사항:

  a. 1자에서 64자 사이

  b. 첫번째 문자는 반드시 알파벳이어야 합니다.

  c. 공백을 포함할 수 없습니다.

  d. 잘못된 문자: " / \ : | , * ? < > ~ ! @ # $ % ^ & ' ( ) { }

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

- Active Directory 없이 호스트 자격 증명을 구성하려면 다음을 수행합니다.
  - **사용자 이름**에서 **사용자 이름**은 루트입니다. 이 이름은 기본 사용자 이름이며 변경할 수 없습니다. 하지만 Active Directory가 설정되면 루트 이외의 Active Directory 사용자를 선택할 수 있습니다.
  - **암호**에 암호를 입력합니다. 암호는 127자로 제한됩니다.

    노트: OMSA 자격 증명은 ESXi 호스트에 사용된 자격 증명과 동일합니다.
  - **암호 확인**에 암호를 다시 입력합니다.
  - 다음 작업 중 하나를 수행합니다.
    - 호스트 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **인증서 확인 활성화**를 선택합니다.
    - 호스트 인증서를 저장하지 않고 이후의 모든 연결에서 인증서 확인을 수행하지 않으려면 **인증서 확인 활성화**를 선택 취소합니다.

5. **다음**을 클릭합니다.
6. **연결된 호스트** 페이지에서 연결 프로필에 사용할 호스트를 선택하고 **확인**을 클릭합니다.
7. 연결 프로필을 테스트하려면 하나 이상의 호스트를 선택하고 **연결 테스트**을 클릭합니다.

   노트: 이 단계는 선택 사항입니다. 호스트 및 iDRAC 자격 증명이 올바른지 여부를 확인하는 데 사용됩니다.

8. 프로필을 완료하려면 **다음**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.

인벤토리 작업 예약 [마법사]

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

노트: OMIVV에 계속해서 업데이트된 정보가 표시되도록 하려면 주기적인 인벤토리 작업을 예약하는 것이 좋습니다. 인벤토리 작업을 수행하면 최소의 자원이 소비되며 호스트 성능이 저하되지 않습니다.

노트: 모든 호스트에 대해 인벤토리가 실행되고 나면 섀시는 자동으로 검색됩니다. 특정 섀시를 섀시 프로필에 추가하면 그 섀시의 인벤토리가 자동으로 실행됩니다. 여러 개의 vCenter를 갖추고 있는 SSO 환경의 경우, 하나의 vCenter가 예약된 시간에 실행되면 모든 vCenter에 대해 섀시 인벤토리가 자동으로 실행됩니다.

인벤토리 작업을 예약하려면 다음을 수행합니다.

1. **구성 마법사**의 **인벤토리 일정** 창에서 **인벤토리 데이터 검색 활성화**가 활성화되어 있지 않은 경우 활성화합니다.
   인벤토리 데이터 검색 활성화는 기본적으로 활성화되어 있습니다.
2. **인벤토리 데이터 검색 일정**에서 다음을 수행합니다.
   a. 인벤토리를 실행할 각 요일 옆의 확인란을 선택합니다. **모든 요일**이 기본적으로 선택됩니다.
   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 수락하고 계속하려면 **다음**을 클릭하여 보증 일정 설정을 계속 진행합니다.

보증 검색 작업 실행 [마법사]

보증 검색 작업 구성 방법은 OMIVV의 옵션 설정에 있습니다. 또한 보증 검색 작업을 **작업 큐**->**보증**에서 실행 또는 예약할 수 있습니다. 예약된 작업은 작업 큐에 나열됩니다. 여러 개의 vCenter가 있는 SSO 환경에서는, vCenter의 보증이 실행되어 있는 경우 모든 vCenter가 실행될 때마다 섀시 보증이 자동으로 실행됩니다. 섀시 프로필에 보증이 추가된 경우 보증이 자동으로 실행되지 않습니다.

보증 검색 작업을 실행하려면 다음을 수행합니다.

1. **구성 마법사**의 **보증 일정** 창에서 **보증 데이터 검색 활성화**를 선택해 보증을 예약할 수 있습니다.
2. **보증 데이터 검색 일정**에서 다음을 수행합니다.
   a. 보증을 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 수락하고 계속하려면 **다음**을 클릭하여 **이벤트 및 알람** 설정을 계속 진행합니다.

이벤트 및 알람 구성 [마법사]

구성 마법사를 사용하거나 **이벤트 및 알람**에 대한 **설정** 옵션에서 이벤트와 알람을 구성할 수 있습니다. 서버에서 이벤트를 수신하기 위해 OMIVV가 트랩 대상으로 구성됩니다. 12세대 이상 호스트의 경우, iDRAC에서 SNMP 트랩 대상을 설정해야 합니다. 12세대 이전의 호스트는 OMSA에서 트랩 생성을 설정해야 합니다.

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

이벤트 및 알람을 구성하려면 다음을 수행합니다.

1. **초기 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 **Dell 호스트에 알람 활성화** 확인란을 선택합니다.

   노트: 알람이 활성화된 Dell 호스트가 유지 관리 모드로 전환되어 일부 특정 위험 이벤트에 대응합니다.
3. **Dell 알람 경고 활성화** 대화 상자가 표시됩니다. 변경사항을 수락하려면 **계속**을 클릭하고 그렇지 않으면 **취소**를 클릭합니다.

   노트: **Dell 호스트에 알람 활성화**를 선택한 경우에만 이 단계를 완료해야 합니다.

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

4. **적용**을 클릭합니다.

3

VMware vCenter 웹 클라이언트 탐색 정보

VMware vCenter를 쉽게 탐색할 수 있습니다. VMware vCenter에 로그인하여 홈 페이지의 홈 탭으로 이동하면 관리자 그룹 아래의 기본 콘텐츠 영역에 **OpenManage Integration** 아이콘을 볼 수 있습니다. **OpenManage Integration** 아이콘을 사용하여 OpenManage Integration for VMware vCenter 탭으로 이동합니다. 탐색 창 영역에서 Dell 그룹이 표시됩니다.

VMware vCenter 레이아웃에는 다음과 같은 3개의 기본 섹션이 있습니다.

Navigator(탐색 창)	탐색 창 영역은 콘솔에서 여러 가지 보기에 액세스하는 데 사용되는 기본 메뉴입니다. OpenManage Integration for VMware vCenter의 vCenter 메뉴 아래에는 OpenManage Integration for VMware vCenter의 기본 액세스 지점인 특별 그룹이 있습니다.
Main Content(기본 콘텐츠) 영역	Navigator(탐색 창)에서 선택한 보기를 표시합니다. Main Content(기본 콘텐츠) 영역은 대부분의 콘텐츠가 표시되는 영역입니다.
Notifications(알림)	진행 중인 vCenter 알람 및 작업을 표시합니다. OpenManage Integration for VMware vCenter은 vCenter의 알람, 이벤트 및 작업 시스템을 통합하여 Notifications(알림) 영역에 해당 정보를 표시합니다.

주제:

VMware vCenter 내에서 OpenManage Integration for VMware vCenter 탐색

OpenManage Integration for VMware vCenter는 VMware vCenter 내의 특수 Dell 그룹에 있습니다.

1. VMware vCenter에 로그인합니다.
2. VMware vCenter 홈 페이지에서 **OpenManage Integration** 아이콘을 클릭합니다.
   여기에서 OpenManage Integration for VMware vCenter 연결 프로필과 제품 설정을 관리하고, 인벤토리 및 보증 작업을 모니터링하며, 요약 페이지를 확인할 수 있으며 기본 콘텐츠 영역의 탭에서 기타 여러 가지 작업을 수행할 수 있습니다.
3. 호스트, 데이터센터 및 클러스터를 모니터링하려면 왼쪽에 있는 Navigator(탐색 창)의 Inventory Lists(인벤토리 목록) 아래에서 조사할 호스트, 데이터센터 또는 클러스터를 선택한 다음 Object(개체) 탭에서 원하는 개체를 선택합니다.

아이콘 단추 이해

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

표 1. 아이콘 단추가 정의되어 있습니다.

아이콘 단추	정의
	새로 추가하거나 생성하려면 이 더하기 아이콘을 사용합니다.
	연결 프로필, 데이터센터 및 클러스터에 서버를 추가하려면 이 서버 추가 아이콘을 사용합니다.
	작업을 중단하려면 이 아이콘을 사용합니다.

표 1. 아이콘 단추가 정의되어 있습니다. (계속)

아이콘 단추	정의
	목록을 축소하려면 이 아이콘을 사용합니다.
	목록을 확장하려면 이 아이콘을 사용합니다.
	개체를 삭제하려면 이 아이콘을 사용합니다.
	일정을 변경하려면 이 아이콘을 사용합니다.
	편집하려면 이 연필 아이콘을 사용합니다.
	작업을 제거하려면 빗자루 아이콘을 사용합니다.
	파일을 내보내려면 이 아이콘을 사용합니다.

소프트웨어 버전 찾기

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

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

화면 콘텐츠 새로 고치기

VMware vCenter Refresh(VMware vCenter 새로 고침) 아이콘을 사용하여 화면을 언제든지 새로 고칠 수 있습니다.

1. 새로 고칠 페이지를 선택합니다.
2. VMware vCenter 제목 표시줄에서 **Refresh(새로 고침)** 단추를 클릭합니다.
   Refresh(새로 고침) 아이콘은 Search(검색) 영역 왼쪽에 있으며 시계 방향 화살표 모양으로 표시됩니다.

OpenManage Integration for VMware vCenter 라이센싱 탭 보기

OpenManage Integration for VMware vCenter 라이센스를 설치하면, 지원되는 호스트 및 vCenter의 수가 이 탭에 표시됩니다. 페이지 상단에 OpenManage Integration for VMware vCenter의 버전도 표시됩니다.

Licensing(라이센싱) 아래에 다음이 표시됩니다.

- 라이센스 구입

License Management(라이센스 관리) 아래의 이 페이지에는 다음 항목에 대한 링크가 있습니다.

- 제품 라이센스 포털(디지털 락커)
- iDRAC 라이센스 포털
- Administration Console
- 라이센스 구입

OpenManage Integration for VMware vCenter의 Licensing(라이센싱) 탭에서 다음 사항을 확인할 수 있습니다.

호스트 라이센스	• Licenses Available(사용 가능한 라이센스)

	사용 가능한 라이센스 수를 표시합니다. • Licenses In Use(사용 중인 라이센스) 사용 중인 라이센스 수를 표시합니다.
vCenter 라이센스	• Licenses Available(사용 가능한 라이센스) 사용 가능한 라이센스 수를 표시합니다. • Licenses In Use(사용 중인 라이센스) 사용 중인 라이센스 수를 표시합니다.

온라인 도움말 열기

Help and Support(도움말 및 지원) 탭에서 온라인 도움말을 열 수 있습니다. 문서에서 주제의 이해를 돕는 도움말 또는 절차를 검색할 수 있습니다.

1. OpenManage Integration for VMware vCenter에서 다음 중 하나를 수행합니다.
   - Help and Support(도움말 및 지원)의 **Product Help(제품 도움말)**에서 **OpenManage Integration for VMware vCenter Help(OpenManage Integration for VMware vCenter 도움말)**를 클릭합니다.
2. 왼쪽 창의 목차를 사용하거나 검색을 통해 선택할 주제를 찾습니다.
3. 도움말 사용을 마친 후에는 오른쪽 상단에서 해당 창이나 탭을 닫으십시오. 브라우저가 열려 있으면 온라인 도움말 콘텐츠가 브라우저 창에 표시됩니다. 온라인 도움말을 닫으려면 브라우저 창 오른쪽 상단에 있는 **X**를 클릭하십시오.

도움말 및 지원 찾기

OpenManage Integration for VMware vCenter의 Help and Support(도움말 및 지원) 탭은 제품에 대한 정보를 제공합니다. 이 탭에서 다음과 같은 정보를 볼 수 있습니다.

제품 도움말	다음과 같은 링크를 제공합니다. • **OpenManage Integration for VMware vCenter 도움말** 제품 도움말에 대한 링크를 제공하며, 이는 제품 내에 있습니다. 목차 또는 검색을 사용하여 필요한 도움말을 찾습니다. • 정보 이 링크를 클릭하면 Version Information(버전 정보) 대화상자가 표시됩니다. 여기에서 제품 버전을 확인할 수 있습니다.
Dell 매뉴얼	다음에 대한 라이브 링크를 제공합니다. • 서버 매뉴얼 • OpenManage Integration for VMware vCenter 매뉴얼
Administration Console	Administration Console에 대한 링크를 제공합니다.
추가 도움말 및 지원	다음에 대한 라이브 링크를 제공합니다. • 라이프사이클 컨트롤러가 포함된 iDRAC 매뉴얼 • Dell VMware 설명서 • OpenManage Integration for VMware vCenter 제품 페이지 • Dell 도움말 및 지원 홈 • Dell TechCenter
지원 전화 팁	Dell 지원부에 연락하고 통화를 올바르게 연결하는 방법에 대한 팁을 제공합니다.

문제 해결 번들	문제 해결 번들을 생성하고 다운로드할 수 있는 링크를 제공합니다. 기술 지원 센터에 문의할 때 이 번들을 제공하거나 참조하도록 합니다. 자세한 내용은 문제 해결 번들 다운로드를 참조하십시오.
Dell 권장사항	Dell은 Dell Repository Manager를 사용할 것을 권장하며, 여기에서 해당 링크를 찾을 수 있습니다. Dell Repository Manager를 사용하여 시스템에 사용 가능한 모든 펌웨어 업데이트를 찾고 다운로드합니다.
iDRAC 다시 설정	iDRAC가 응답하지 않을 때 사용할 수 있는 Reset iDRAC(iDRAC 다시 설정) 링크를 제공합니다. 이 작업을 수행하면 iDRAC가 정상적으로 재부팅됩니다.

문제 해결 번들 다운로드

이 정보를 사용하여 문제해결을 지원하거나 기술 지원 센터로 보냅니다.

1. OpenManage Integration for VMware vCenter에서 **Help and Support(도움말 및 지원)** 탭을 클릭합니다.
2. **Troubleshooting Bundle(문제 해결 번들)**에서 **Create and Download Troubleshooting Bundle(문제 해결 번들 생성 및 다운로드)**을 클릭합니다.
3. **Create(생성)** 단추를 클릭합니다.
4. 파일을 저장하려면 **Download(다운로드)**를 클릭합니다.
5. File Download(파일 다운로드) 대화 상자에서 **Save(저장)**를 클릭합니다.
6. Save As(다른 이름으로 저장) 대화 상자에서 파일을 저장할 위치를 찾아보고 **Save(저장)**를 클릭합니다.
7. 종료하려면 **Close(닫기)**를 클릭합니다.

iDRAC 다시 설정

iDRAC Reset(iDRAC 재설정) 링크는 Help and Support(도움말 및 지원) 탭에 있습니다. iDRAC를 재설정하면 iDRAC가 정상적으로 다시 부팅됩니다. iDRAC가 다시 부팅될 때 호스트는 다시 부팅되지 않습니다. 재설정을 수행한 후 사용 가능한 상태로 복원되는 데 최대 2분이 소요됩니다. 재설정 작업은 VMware vCenter용 OpenManage Integration에서 iDRAC가 응답하지 않는 경우에만 수행하십시오.

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

iDRAC가 다시 부팅되는 동안에 다음과 같은 상황이 발생할 수 있습니다.

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

  iDRAC에서 DHCP를 IP 주소로 사용할 경우 IP 주소가 변경될 수 있습니다. 이 경우 호스트 인벤토리 작업을 다시 실행하여 인벤토리 데이터에서 새로운 iDRAC IP 주소를 캡처하십시오.

1. OpenManage Integration for VMware vCenter에서 **도움말 및 지원** 탭을 클릭합니다.
2. iDRAC Reset(iDRAC 재설정) 아래에서 **iDRAC 재설정**을 클릭합니다.
3. iDRAC Reset(iDRAC 재설정) 대화 상자의 iDRAC Reset(iDRAC 재설정) 아래에서 IP 주소/이름을 입력합니다.
4. iDRAC 프로세스를 이해한 후 이를 확인하려면 **iDRAC 재설정을 이해했습니다. iDRAC 재설정을 계속합니다.**를 선택합니다.
5. **iDRAC 재설정**을 클릭합니다.

Administration Console 실행

VMware vCenter 웹 클라이언트 내에서 OpenManage Integration for VMware vCenter를 실행하고 Help and Support(도움말 및 지원) 탭에서 Administration Console을 열 수 있습니다.

1. OpenManage Integration for VMware vCenter의 Help and Support(도움말 및 지원) 탭에 있는 Administration Console 아래에서 콘솔에 연결되는 링크를 클릭합니다.
2. Administration Console 로그인에서 관리자 암호를 사용하여 로그인합니다. Administration Console에서 다음 작업을 수행할 수 있습니다.
   a. vCenter를 등록 또는 등록 취소하거나 자격 증명을 수정하거나 인증서를 업데이트합니다.
   b. 라이센스를 업로드합니다.

c. 등록된 vCenter 및 사용 가능한 vCenter의 개수와 사용 중인 호스트 라이센스 및 사용 가능한 최대 호스트 라이센스 개수에 대한 요약을 봅니다.
d. 가상 어플라이언스를 다시 시작합니다.
e. 업데이트(최신 버전으로 업그레이드).
f. 문제 해결 번들 생성.
g. 네트워크 설정을 표시합니다(읽기 전용 모드).
h. HTTP 프록시 설정 구성: 이 설정은 어플라이언스 업그레이드 또는 http://downloads.dell.com/published/Pages/index.html에 연결을 위해 Dell 서버에 연결하는 데 사용됩니다.
i. NTP 설정을 구성합니다. NTP 서버를 사용 또는 사용 안 함으로 설정하고 기본 및 보조 NTP 서버를 구성합니다.
j. 인증서 서명 요청(CSR)을 생성하거나 인증서를 업로드하거나 HTTPS 인증서에 대한 기본 인증서를 복원합니다.
k. 모든 vCenter 인스턴스에서 발생하는 경고가 저장되는 방법에 대해 전역 설정을 구성합니다. 저장되는 경고, 경고 보유 일 수, 중복 경고 시간 제한의 최대값을 구성할 수 있습니다.
l. 백업 또는 복원을 시작합니다.
m. 네트워크 공유의 백업 위치 및 백업된 파일의 암호화 암호를 구성합니다(테스트 네트워크 연결과 함께).
n. 반복 백업을 예약합니다.

4

프로필

Credential Profiles(자격 증명 프로필) 탭을 사용하여 Connection Profiles(연결 프로필) 및 Chassis Profiles(섀시 프로필)를 관리하고 구성할 수 있습니다.

Connection Profiles(연결 프로필)를 사용하면 Dell 서버에 액세스하는 데 필요한 연결 프로필을 관리하고 구성할 수 있습니다. Connection Profiles(연결 프로필) 창에서는 가상 어플라이언스가 Dell 서버와 통신하는 데 사용 되는 자격증명이 포함된 연결 프로필을 관리하고 구성할 수 있습니다. OpenManage Integration for VMware vCenter에서 관리하려면 각 Dell 서버를 하나의 연결 프로필에만 연결하십시오. 연결 프로필 하나에 여러 개의 서버를 지정할 수 있습니다.

Chassis Profiles(섀시 프로필)은 가상 어플라이언스가 Dell 섀시와 통신하는 데 사용하는 자격 증명을 포함하는 연결 프로필을 관리하고 구성할 수 있습니다. VMware vCenter의 OpenManage Integration을 통한 관리를 위해 검색된 각각의 섀시를 하나의 연결 프로필에 할당 하십시오. 하나의 연결 프로필에 여러 개의 섀시를 할당할 수 있습니다.

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

주제:

연결 프로필 보기

연결 프로필이 있거나 생성해야 이 프로필을 볼 수 있습니다.

하나 이상의 연결 프로필을 생성한 후 해당 Connection Profile(연결 프로필) 페이지에서 볼 수 있습니다. OpenManage Integration for VMware vCenter에서는 프로필에 제공된 자격 증명을 사용하여 Dell 호스트와 통신합니다.

OpenManage Integration for VMware vCenter의 **Manage(관리)** > **Profiles(프로필)** > **Credential Profiles(자격 증명 프로필)** > **Connection Profile(연결 프로필)**에서 생성한 연결 프로필을 모두 볼 수 있습니다. 볼 수 있는 정보는 다음과 같습니다.

Profile Name(프로필 이름)	연결 프로필의 이름을 표시합니다.
설명	설명을 표시합니다(제공된 경우).
vCenter	컨텍스트에 따라 vCenter의 FQDN 또는 호스트 이름 또는 IP 주소를 표시합니다.
Associated Hosts(연결된 호스트)	이 연결 프로필과 연결된 호스트를 표시합니다. 둘 이상인 경우 확장 아이콘을 사용하여 모두 표시합니다.
iDRAC Certificate Check(iDRAC 인증서 확인)	iDRAC 인증서 확인이 활성화되어 있는지 또는 비활성화되어 있는지 표시합니다.
Host Root Certificate Check(호스트 루트 인증서 확인)	호스트 루트 인증서 확인이 활성화되어 있는지 또는 비활성화되어 있는지 표시합니다.

Date Created(생성 날짜)	생성 날짜를 표시합니다.
Date Modified(수정 날짜)	수정 날짜를 표시합니다.
Last Modified By(마지막으로 수정한 사람)	사용자의 세부정보를 표시합니다.

연결 프로필 생성

여러 호스트를 하나의 연결 프로필에 연결할 수 있습니다. 다음 단계에 따라 연결 프로필을 생성하십시오.

노트: 이 절차를 수행하는 동안 표시되는 vCenter 호스트는 동일한 SSO(Single Sign On)을 사용하여 인증된 호스트입니다. vCenter 호스트가 표시되지 않으면 다른 SSO를 사용하고 있거나 5.1 이전 버전의 VMware vCenter를 사용하고 있는 것입니다.

1. OpenManage Integration for VMware vCenter의 왼쪽 창에 있는**Manage(관리)** → **Profiles(프로필)** → **Credential Profiles(자격 증명 프로필)** → **Connection Profiles(연결 프로필)** 탭에서 **+**를 클릭합니다.
2. **New Connection Profile(새 연결 프로필)** 페이지에서 다음을 입력합니다.
3. **Profile Name and Description(프로필 이름 및 설명)** 영역에서 다음을 수행합니다.
   a. 프로필 아래에 **Profile Name(프로필 이름)**을 입력하고 원하는 경우 **Description(설명)**을 입력합니다.
   b. Associated Hosts(연결된 호스트) 아래에서 이 연결 프로필과 연결할 하나 이상의 호스트를 선택합니다. 이 옵션을 선택하면 하나 또는 여러 개의 호스트에 대해 하나의 연결 프로필을 생성할 수 있습니다.
   c. **Next(다음)**를 클릭합니다.
   d. **iDRAC Credentials(iDRAC 자격 증명)** 페이지에서 다음을 수행합니다.
      - iDRAC 계정에 관리 권한이 있어야 펌웨어 업데이트, 하드웨어 프로필 적용, 하이퍼바이저 배포를 수행할 수 있습니다.
      - **Active Directory User Name(Active Directory 사용자 이름)** 텍스트 상자에 사용자 이름을 입력합니다. 사용자 이름은 도메인\사용자 이름 또는 사용자 이름@도메인 형식 중 하나로 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.
      - 다음의 작업을 수행하십시오:
        - iDRAC 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **Certificate Check(인증서 확인)** Enabled(활성화됨) 드롭다운 목록을 선택합니다.
        - 확인을 수행하지 않고 인증서를 저장하지 않으려면 **Certificate Check(인증서 확인)**을 선택하지 마십시오.

   e. **Hosts Root(호스트 루트)** 페이지에서 다음을 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 또는 사용자 이름@도메인 형식 중 하나로 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.
      - 다음 작업 중 하나를 수행합니다.
        - 호스트 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 확인란을 선택합니다.
        - 확인을 수행하지 않고 호스트 인증서를 저장하지 않으려면 **Enable Certificate Check(인증서 확인 활성화)** 확인란을 선택하지 마십시오.
      - Active Directory 없이 호스트 자격 증명을 구성하려면 다음을 수행합니다.
      - **User Name(사용자 이름)** 텍스트 상자에서 사용자 이름은 root입니다. 이 이름은 기본 사용자 이름이며 변경할 수 없습니다.
      - Active Directory가 설정되면 루트 이외의 Active Directory 사용자를 선택할 수 있습니다.
      - **Password(암호)** 텍스트 상자에 암호를 입력합니다. 암호는 127자로 제한됩니다.

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

- **Verify Password(암호 확인)** 텍스트 상자에 암호를 다시 입력합니다.
- **Enable Certificate Check(인증서 확인)** 확인란에서 다음 중 하나를 선택합니다:
- 호스트 인증서를 다운로드하여 저장하고 이후의 모든 연결 시에 유효성을 확인하려면 **Enable Certificate Check(인증서 확인 활성화)** 확인란을 선택합니다.
- 확인을 수행하지 않고 호스트 인증서를 저장하지 않으려면 **Enable Certificate Check(인증서 확인 활성화)** 확인란을 선택하지 마십시오.

4. **Next(다음)**을 클릭합니다.
5. Associated Hosts(연결된 호스트) 페이지에서 연결 프로필에 대한 호스트를 하나 이상 선택하고 **OK(확인)**를 클릭합니다.
6. 연결 프로필을 테스트하려면 하나 이상의 호스트를 선택하고 Test Connection(연결 테스트) 단추를 선택합니다. 이 설정은 선택사항이며, 호스트 및 iDRAC 자격 증명이 올바른지 여부를 확인하는 데 사용됩니다.
7. 프로필을 완료하려면 **Next(다음)**를 클릭합니다. iDRAC 익스프레스 또는 엔터프라이즈 카드가 없는 서버의 경우 iDRAC 테스트 연결 시 이 시스템에 Not Applicable(해당되지 않음) 상태가 표시됩니다.

연결 프로필 편집

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

노트: 이 절차를 수행하는 동안 표시되는 vCenter는 동일한 SSO(Single Sign On)을 사용하여 인증된 호스트입니다. vCenter 호스트가 표시되지 않으면 다른 SSO를 사용하고 있거나 5.1 이전 버전의 VMware vCenter를 사용하고 있는 것입니다.

노트: 라이센스 제한에 관계없이 연결 프로필을 편집할 수 있습니다.

1. OpenManage Integration for VMware vCenter의 **Manage(관리)** > **Profiles(프로필)** > **Credential Profiles(자격 증명 프로필)** > **Connection Profiles(연결 프로필)** 탭에서 연결 프로필을 선택합니다.
2. **Edit(편집)** 아이콘을 클릭합니다.
3. 연결 프로필 창에서 시작 탭의 정보를 읽고 **Next(다음)**를 클릭합니다.
4. Name and Credentials(이름 및 자격 증명) 창에서 다음을 수행합니다.
   a. 프로필 아래에 **Profile Name(프로필 이름)**을 입력하고 원하는 경우 **Description(설명)**을 입력합니다.
   b. vCenter 아래에서 이 연결 프로필에 대해 연결된 호스트를 봅니다. 여기에 호스트가 표시되는 이유에 대해 앞의 노트를 참조하십시오.
   c. iDRAC 자격 증명에서 다음을 수행합니다.
      - 사용자 이름은 root이며 **Active Directory**를 선택하지 않는 경우 이 이름 항목을 수정할 수 없습니다. **Active Directory**가 설정되어 있는 경우 iDRAC 사용자가 root 자격 증명을 사용할 필요는 없으며 관리자 권한이 있는 iDRAC 사용자면 됩니다.
      - 도메인\사용자 이름: 도메인\사용자 이름 또는 도메인@사용자 이름 형식 중 하나로 사용자 이름을 입력합니다.
        - /(슬래시), &, \(백슬래시), .(마침표), "(따옴표), @ 및 %(퍼센트) 문자는 사용자 이름에 사용할 수 없습니다(127자 제한).
        - 도메인에는 영숫자 문자와 -(dash) 및 .(마침표)만 사용할 수 있습니다(254자 한도). 도메인의 첫 번째와 마지막 문자는 영숫자여야 합니다.
      - 암호: 암호를 입력합니다.

        /(슬래시), &, \(백슬래시), .(마침표), "(따옴표) 문자는 암호에 허용되지 않습니다.
      - 암호 확인: 암호를 다시 입력합니다.
      - 인증서 확인 활성화: 기본적으로 이 확인란은 선택 취소되어 있습니다. iDRAC 인증서를 다운로드하여 저장한 다음 이후의 모든 연결에서 유효성을 확인하려면 **Enable Certificate Check(인증서 확인 활성화)**를 선택하고, 인증서 확인을 수행하지 않고 인증서를 저장하지 않으려면 **Enable Certificate Check(인증서 확인 활성화)** 확인란을 선택 취소하십시오.

        노트: Active Directory를 사용하는 경우 **Enable(활성화)**을 선택해야 합니다.
   d. 호스트 루트에서 다음을 수행합니다.
      - Active Directory와 연관된 모든 콘솔에 액세스하려면 **Use Active Directory(Active Directory 사용)** 확인란을 선택합니다.

        사용자 이름: 기본 사용자 이름은 **root**이며 이 이름을 수정할 수 없습니다. Use Active Directory(Active Directory 사용) 옵션이 선택되어 있으면 원하는 Active Directory 사용자 이름을 사용할 수 있습니다.
      - 암호: 암호를 입력합니다.

        /(슬래시), &, \(백슬래시), .(마침표), "(따옴표) 문자는 암호에 허용되지 않습니다.

- 암호 확인: 암호를 다시 입력합니다.
- 인증서 확인 활성화: 기본적으로 이 확인란은 선택 취소되어 있습니다. iDRAC 인증서를 다운로드하여 저장한 다음 이후의 모든 연결에서 유효성을 확인하려면 **Enable Certificate Check(인증서 확인 활성화)**를 선택하고, 인증서 확인을 수행하지 않고 인증서를 저장하지 않으려면 **Enable Certificate Check(인증서 확인 활성화)** 확인란을 선택 취소하십시오.

  노트: Active Directory를 사용하는 경우 **Enable(활성화)**을 선택해야 합니다.

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

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

5. **Next(다음)**을 클릭합니다.
6. 호스트 선택 대화상자에서 이 연결 프로필의 호스트를 선택합니다.
7. **OK(확인)**를 클릭합니다.
8. 연결된 호스트 탭을 사용하면 선택한 서버에서 iDRAC 및 호스트 자격 증명을 테스트할 수 있습니다. 다음 중 하나를 수행합니다.
   - 테스트를 시작하려면 확인할 호스트를 선택하고 **Test Connection(연결 테스트)** 아이콘을 클릭합니다. 다른 옵션은 비활성화됩니다.

     테스트가 완료되면 **Finish(마침)**를 클릭합니다.
   - 테스트를 중지하려면 **Abort All Tests(모든 테스트 중단)**를 클릭합니다. 테스트 중단 대화상자에서 **OK(확인)**을 클릭한 후 **Finish(완료)**를 클릭합니다.

연결 프로필 새로 고치기

OpenManage Integration for VMware vCenter의 **Manage(관리)** > **Profiles(프로필)** > **Credential Profiles(자격 증명 프로필)** > **Connection Profiles(연결 프로필)** 탭에서 VMware vSphere 웹 클라이언트 제목 표시줄에 있는 **Refresh(새로 고침)** 아이콘을 클릭합니다.

노트: vCenter에서 호스트를 제거한 후 연결 프로필 페이지를 탐색하면 연결 프로필에서 호스트를 제거하라는 메시지가 표시됩니다. 확인하면 연결 프로필에서 호스트가 제거됩니다.

연결 프로필 삭제

1. OpenManage Integration for VMware vCenter의 **Manage(관리)** > **Profiles(프로필)** > **Credential Profiles(자격 증명 프로필)** > **Connection Profiles(연결 프로필)** 탭에서 삭제할 프로필을 선택합니다.
2. **Delete(삭제)** 아이콘을 클릭합니다.
3. Delete Confirmation(삭제 확인) 메시지에서 **Yes(예)**를 클릭하여 프로필을 제거하거나, **No(아니오)**를 클릭하여 삭제 조치를 취소합니다.

연결 프로필 테스트

1. OpenManage Integration for VMware vCenter의 **Manage(관리)** > **Profiles(프로필)** > **Credential Profiles(자격 증명 프로필)** > **Connection Profiles(연결 프로필)** 탭에서 테스트할 연결 프로필을 선택합니다. 이 작업을 완료하는 데 몇 분 정도 걸릴 수 있습니다.
2. 테스트 연결 프로필 대화 상자에서 테스트할 호스트를 선택하고 **Test Connection(연결 테스트)** 아이콘을 클릭합니다.
3. 선택한 모든 테스트를 중단하고 테스트를 취소하려면 **Abort All Tests(모든 테스트 중단)**를 클릭합니다. Abort Tests(테스트 중단) 대화 상자에서 **OK(확인)**를 클릭합니다.
4. 종료하려면 **Cancel(취소)**을 클릭합니다.

섀시 프로필 생성

OMIVV는 OMIVV에서 관리되는 Dell 서버와 연결된 모든 Dell 섀시를 모니터링할 수 있습니다. 섀시를 모니터링하려면 섀시 프로필이 필요합니다. 섀시 자격 증명 프로필을 생성해 하나 또는 여러 개의 섀시와 연결할 수 있습니다. 섀시 프로필은 다음 단계에 따라 생성합니다.

1. **OpenManage Integration for VMware vCenter**에서 **Manage(관리)** > **Profiles(프로필)** > **Credential Profiles(자격 증명 프로필)** > **Chassis Profile(섀시 프로필)**을 선택합니다.
2. **Chassis Profiles(섀시 프로필)** 페이지에서 **Plus(더하기)(+)** 아이콘을 클릭하여 **New Chassis Profile(새 섀시 프로필)**을 생성합니다.
3. **Chassis Profile Wizard(섀시 프로필 마법사)** 페이지에서 다음을 수행합니다.
   a. **프로필 이름** 텍스트 상자에서 프로필 이름을 입력합니다.
   b. **Description(설명)** 텍스트 상자에서 선택적 설명을 입력합니다.
4. **Credentials(자격 증명)**에서 다음을 수행합니다.
   a. **User Name(사용자 이름)** 텍스트 상자에 일반적으로 CMC(Chassis Management Controller)에 로그온할 때 사용하는 관리자 권한이 있는 사용자 이름을 입력합니다.
   b. **Password(암호)** 텍스트 상자에 사용자 이름에 해당하는 암호를 입력합니다.
   c. **Verify Password(암호 확인)** 텍스트 상자에서, **Password(암호)** 텍스트 상자에 입력한 것과 동일한 암호를 입력합니다. 이 두 암호는 일치해야 합니다.

   노트: 자격 증명은 로컬 또는 Active Directory 자격 증명일 수 있습니다. 섀시 프로필과 함께 Active Directory 자격 증명을 사용하기 전에 Active Directory에 Active Directory 사용자 계정이 있어야 하며, Active Directory 기반 인증에 맞게 CMC(Chassis Management Controller)를 구성해야 합니다.

5. **Next(다음)**를 클릭합니다.
   사용 가능한 모든 섀시를 보여 주는 **Select Chassis(섀시 선택)** 페이지가 표시됩니다.

   노트: 섀시 아래에 있는 모듈식 호스트의 성공적인 인벤토리 실행 이후에만 해당 섀시가 검색되고 섀시 프로필과 연결할 수 있습니다.

6. 개별 섀시 또는 다중 섀시를 선택하려면 **IP/Host Name(IP/호스트 이름)** 옆의 옆에 있는 해당 확인란을 선택합니다.
   선택한 섀시가 이미 다른 프로필에 속해있으면 선택한 섀시가 다른 프로필과 연결되어 있음을 나타내는 경고 메시지가 표시됩니다.
   예를 들어, 섀시 A와 연결된 **테스트** 프로필이 있습니다. 다른 프로필 **테스트 1**을 생성하고 섀시 A를 **테스트 1**에 연결하도록 시도하면 경고 메시지가 표시됩니다.
7. **OK(확인)**를 클릭합니다.
   Associated Chassis(연결된 섀시) 페이지가 표시됩니다.
8. 섀시를 선택하고 **Test Connection(연결 테스트)** 아이콘을 클릭하면 자격 증명이 확인되어 섀시의 연결성을 테스트합니다. 결과는 **Test Result(테스트 결과)** 열에 **Pass(통과)** 또는 **Fail(실패)**로 표시됩니다.
9. **Finish(마침)**를 클릭하여 프로필을 완료합니다.

   노트: Associated Chassis(연결된 섀시) 페이지의 왼쪽 위에 표시된 더하기 아이콘을 클릭하여 섀시를 추가하거나 삭제할 수도 있습니다.

섀시 프로필 보기

섀시 프로필을 보려면 다음을 수행합니다.

1. **OpenManage Integration for VMware vCenter**에서**Manage(관리)** > **Profiles(프로필)** > **Credential Profiles(자격 증명 프로필)** > **Chassis Profiles(섀시 프로필)**창을 선택합니다. 섀시 프로필이 표시됩니다.
2. 여러 개의 섀시가 섀시 프로필과 연결되어 있는 경우 화살표 아이콘을 클릭하면 연결된 섀시가 모두 표시됩니다.
3. **Chassis View(섀시 보기)** 페이지에서는 프로필 이름, 설명, 섀시 IP, 서비스 태그 및 섀시를 수정한 날짜를 볼 수 있습니다.
4. **Chassis View(섀시 보기)** 페이지에서 다음과 같은 작업을 수행할 수 있습니다.
   a. 추가
   b. 편집
   c. 삭제
   d. 연결 테스트

섀시 프로필 편집

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

1. OpenManage Integration for VMware vCenter의 **Manage(관리)** > **Profiles(프로필)** > **Credential Profiles(자격 증명 프로필)** > **Chassis Profiles(섀시 프로필)** 탭에서 섀시 프로필을 선택합니다.
2. 기본 메뉴에서 `Pencil`(연필) 아이콘으로 표시되는 **Edit(편집)** 아이콘을 클릭합니다.
3. **Edit Chassis Profile(섀시 프로필 편집)** 창이 표시됩니다.
4. **Chassis Profile(섀시 프로필)** 영역에서 **Profile Name(프로필 이름)** 및 선택 사양인 **Description(설명)**을 편집할 수 있습니다.
5. **Credentials(자격 증명)** 영역 아래에서, **User Name(사용자 이름)**, **Password(암호)**, **Verify Password(암호 확인)**를 편집할 수 있습니다. **Verify Password(암호 확인)**에 입력하는 암호는 **Password(암호)** 필드에 입력한 것과 동일해야 합니다. 입력된 자격 증명에는 해당 섀시에 대한 관리자의 권한이 포함되어 있어야 합니다.
6. **Apply(적용)**를 클릭합니다. 변경사항이 저장됩니다.
7. **Associated Chassis(연결된 섀시)** 탭을 사용하면 선택한 섀시에서 섀시 및 자격 증명을 테스트할 수 있습니다. 다음 중 하나를 수행합니다.
   - 테스트를 시작하려면 검색할 섀시를 하나 또는 여러 개 선택한 후 **Test Connection(연결 테스트)** 아이콘을 클릭합니다. **Test Result(테스트 결과)** 열에 연결 테스트가 성공했는지 여부가 표시됩니다.
   - **Plus(더하기)** 아이콘을 클릭하여 섀시 프로필에 하나 또는 여러 개의 섀시를 추가하거나 삭제할 수 있습니다.

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

섀시 프로필 삭제

섀시 프로필을 삭제하려면 다음을 수행합니다.

1. **OpenManage Integration**에서**Manage(관리)** > **Profiles(프로필)** > **Credential Profile(자격 증명 프로필)** > **Chassis Profiles(섀시 프로필)**창을 선택합니다.
2. 삭제할 섀시 프로필을 선택하고 **Cross(엑스)**(X) 아이콘을 클릭합니다. 경고 메시지가 표시됩니다.
3. 삭제를 계속 진행하려면 **Yes(예)**를 클릭하고 삭제를 취소하려면 **No(아니오)**를 클릭합니다.

   노트: 섀시 프로필과 연결된 모든 섀시가 선택되지 않았거나 다른 프로필로 옮기면, 삭제 확인 메시지가 표시되어 섀시 프로필에 연결된 섀시가 하나도 없으며 섀시 프로필이 삭제될 것임을 알려줍니다. OK(확인)를 클릭하여 섀시 프로필을 삭제합니다.

섀시 프로필 테스트

1. OpenManage Integration for VMware vCenter의 **Manage(관리)** > **Profiles(프로필)** > **Credential Profiles(자격 증명 프로필)** > **Chassis Profiles(섀시 프로필)** 탭에서 테스트할 섀시 프로필을 하나 또는 여러 개 선택합니다. 이 작업을 완료하는 데 몇 분 정도 걸릴 수 있습니다.
2. Test Chassis Profile(섀시 프로필 테스트) 대화 상자에서, 테스트할 섀시를 선택하고 **Test Connection(연결 테스트)** 아이콘을 클릭합니다.
3. 선택한 모든 테스트를 중단하고 테스트를 취소하려면 **Abort All Tests(모든 테스트 중단)**를 클릭합니다. Abort Tests(테스트 중단) 대화 상자에서 **OK(확인)**를 클릭합니다.
4. 종료하려면 **Cancel(취소)**을 클릭합니다.

5

작업 큐

OpenManage Integration for VMware vCenter이 구성되면 Monitor(모니터) 탭 아래에서 인벤토리, 보증 작업 및 펌웨어 업데이트를 모니터링할 수 있습니다. 인벤토리 및 보증은 Configuration Wizard(구성 마법사)를 사용하거나 Settings(설정) 탭에서 설정합니다.

- 인벤토리 내역
- 보증 내역

주제:

인벤토리 내역

인벤토리 작업은 Settings(설정) 탭 또는 초기 구성 마법사를 사용하여 설정됩니다. Inventory History(인벤토리 내역) 탭에서 인벤토리 작업을 확인하십시오. 이 탭에서 다음과 같은 작업을 수행할 수 있습니다.

- 호스트 인벤토리 보기
- 인벤토리 작업 일정 변경
- 지금 인벤토리 작업 실행
- 지금 섀시 인벤토리 작업 실행

호스트 인벤토리 보기

인벤토리 작업에 성공하려면 데이터를 수집해야 합니다. 인벤토리가 완료되면 전체 데이터센터 또는 개별 호스트 시스템에 대한 인벤토리 결과를 볼 수 있습니다. 열은 오름차순 및 내림차순으로 정렬할 수 있습니다.

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

- 서버가 연결 프로필과 연관되지 않아 인벤토리 작업을 실행할 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 Dell PowerEdge 서버 12세대 이후 세대에 필요한 올바른 iDRAC 라이센스가 없으므로 올바른 iDRAC 라이센스를 구입해야 합니다.
- 자격 증명 올바르지 않음
- 대상에 연결할 수 없음

호스트 인벤토리 세부정보를 보려면 다음을 수행합니다.

1. OpenManage Integration for VMware vCenter에서 **Monitor(모니터)** 탭을 클릭합니다.
2. **Job Queue(작업 큐)** > **Inventory History(인벤토리 내역)** > **Hosts Inventory(호스트 인벤토리)**를 클릭합니다.
3. 선택한 vCenter에서 서버 정보를 보려면 vCenter를 선택하여 연관된 모든 호스트 세부정보를 표시합니다.
4. 호스트 인벤토리 정보를 검토합니다.

vCenter 세부정보	
vCenter	vCenter 주소를 표시합니다.
Hosts Passed(통과된 호스트)	통과된 호스트를 표시합니다.

Next Inventory(다음 인벤토리)	다음에 실행될 인벤토리 일정을 표시합니다.
Last Inventory(마지막 인벤토리)	마지막으로 실행된 인벤토리 일정을 표시합니다.
호스트	
호스트	호스트 주소를 표시합니다.
Status(상태)	상태를 표시합니다. 다음과 같은 옵션을 사용할 수 있습니다. • Successful(성공) • Failed(실패) • 진행 중 • 예약됨(Scheduled)
Duration (MM:SS)(기간(MM:SS))	작업 기간을 분 및 초 단위로 표시합니다.
Start Date and Time(시작 날짜 및 시간)	인벤토리 일정이 시작된 날짜 및 시간을 표시합니다.
End Date and Time(종료 날짜 및 시간)	인벤토리 일정이 종료된 시간을 표시합니다.

인벤토리 작업 일정 변경

서버 정보를 최신 상태로 유지하기 위해서는 Dell 서버에서 정기적인 인벤토리를 실행해야 합니다. 인벤토리 작업은 일주일에 한 번 실행하는 것이 좋으며, 호스트 성능에는 영향을 주지 않습니다. **모니터** > **작업 큐** > **인벤토리 내역** > **호스트 인벤토리** 페이지 또는 **초기 구성 마법사**페이지에서 인벤토리 작업 일정을 변경할 수 있습니다.

1. OpenManage Integration for VMware vCenter의 **모니터** > **작업 큐** 탭에서 **인벤토리 내역** > **호스트 인벤토리**를 클릭합니다.
2. vCenter를 선택하고 **Change Schedule(일정 변경)** 아이콘을 클릭합니다.
3. Inventory Data Retrieval(인벤토리 데이터 검색) 대화상자에서 다음을 수행합니다.
   a. Inventory Data(인벤토리 데이터)에서 **Enable Inventory Data Retrieval(인벤토리 데이터 검색 활성화)** 확인란을 선택합니다.
   b. Inventory Data Retrieval Schedule(인벤토리 데이터 검색 일정)에서 작업 요일을 선택합니다.
   c. 인벤토리 데이터 검색 시간 텍스트 상자에 작업의 로컬 시간을 입력합니다.
   작업 구성 시간과 작업 구현 시간의 차이를 고려해야 합니다.
4. **적용**을 클릭하여 설정을 저장하거나, **지우기**를 클릭하여 설정을 다시 설정하거나, **취소**를 클릭하여 작업을 중단합니다.

지금 인벤토리 작업 실행

선택된 VCenter에 대한 인벤토리 작업을 즉시 실행합니다.

1. OpenManage Integration for VMware vCenter의 **Monitor(모니터)** > **Job Queue(작업 큐)** 탭에서 **Inventory History(인벤토리 내역)** > **Hosts Inventory(호스트 인벤토리)**를 클릭합니다.
2. **Run Now(지금 실행)** 단추를 클릭합니다.
3. Success(성공) 대화상자에서 **Close(닫기)**를 클릭합니다.

   노트: 모듈식 호스트 인벤토리를 실행하면, 해당 섀시가 자동으로 검색됩니다.

   인벤토리 작업이 큐에 대기됩니다. 단일 호스트에 대해서는 인벤토리 작업을 실행할 수 없습니다. 인벤토리 작업은 모든 호스트에 대해 시작됩니다.

지금 섀시 인벤토리 작업 실행

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

1. OpenManage Integration for VMware vCenter의 **Monitor(모니터)** > **Job Queue(작업 큐)** 탭에서 **Inventory History(인벤토리 내역)** > **Chassis Inventory(섀시 인벤토리)**를 클릭합니다.
2. 섀시 목록과 마지막 인벤토리 실행에서 인벤토리가 실행된 상태가 표시됩니다.

   노트: 예약된 섀시 인벤토리가 예약된 호스트 인벤토리와 동시에 실행됩니다.

3. **Run Now(지금 실행)**를 클릭하면, 각 섀시에 대한 **Success(성공)** 또는 **Failure(실패)** 상태와 함께 업데이트되어 인벤토리화된 섀시 목록이 표시됩니다.

보증 내역

하드웨어 보증 정보는 Dell 온라인에서 검색되어 OpenManage Integration for VMware vCenter에 표시됩니다. 서버의 서비스 태그는 서버에 대한 보증 정보를 수집하는 데 사용됩니다. 보증 데이터 검색 작업은 구성 마법사를 사용하여 설정됩니다. 이 탭에서 보증 작업 내역을 확인하십시오. 이 탭에서 다음과 같은 작업을 수행할 수 있습니다.

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

보증 내역 보기

보증 작업은 모든 시스템의 support.dell.com에서 보증 정보를 얻기 위해 예약된 작업입니다. 열을 오름차순이나 내림차순으로 정렬할 수 있습니다.

1. OpenManage Integration for VMware vCenter에서 **Monitor(모니터)** 탭을 클릭합니다.
2. **Job Queue(작업 큐)** > **Warranty History(보증 내역)**를 클릭합니다.
3. Warranty History(보증 내역)를 확대하여 **Hosts Warranty(호스트 보증)** 및 **Chassis Warranty(섀시 보증)**가 표시되게 합니다.
4. **Hosts Warranty(호스트 보증)** 또는 **Chassis Warranty(섀시 보증)**를 선택하여 해당 보증 작업 내역 정보를 봅니다.

vCenter 내역	
vCenters	vCenter 목록을 표시합니다.
Hosts Passed(통과된 호스트)	통과된 vCenter 호스트 수를 표시합니다.
Last Warranty(마지막 보증)	마지막으로 실행된 보증 작업을 표시합니다.
Next Warranty(다음 보증)	다음에 실행될 보증 작업을 표시합니다.
Modify Schedule(일정 수정) 단추	보증 작업 일정을 편집합니다.
Run Now(지금 실행) 단추	보증 작업을 실행합니다.
Hosts History(호스트 내역)	
호스트	호스트 주소를 표시합니다.
Status(상태)	상태를 표시합니다. 다음과 같은 옵션을 사용할 수 있습니다. • Successful(성공) • Failed(실패) • 진행 중 • 예약됨(Scheduled)
Duration (MM:SS)(기간(MM:SS))	보증 작업 기간을 MM:SS 단위로 표시합니다.
Start Date and Time(시작 날짜 및 시간)	보증 작업이 시작된 날짜 및 시간을 표시합니다.
End Date and Time(종료 날짜 및 시간)	보증 작업이 종료된 날짜 및 시간을 표시합니다.
섀시 내역	
섀시 IP	섀시 IP 주소를 표시합니다.
서비스 태그	섀시 서비스 태그를 표시합니다. 서비스 태그는 지원 및 유지 관리를 위한고유한 식별자로 제조업체에서 제공합니다.
Status(상태)	섀시 상태를 표시합니다.
Duration (MM:SS)(기간(MM:SS))	보증 작업 기간을 MM:SS 단위로 표시합니다.

Start Date and Time(시작 날짜 및 시간)	보증 작업이 시작된 날짜 및 시간을 표시합니다.
End Date and Time(종료 날짜 및 시간)	보증 작업이 종료된 날짜 및 시간을 표시합니다.

보증 작업 일정 수정

보증 작업은 본래 초기 구성 마법사에서 구성됩니다. 나중에 **Monitor Tab(모니터 탭)** > **Job Queue (작업 큐)** > **Warranty History (보증 내역)** > **Hosts Warranty (호스트 보증)** 페이지 또는**Manage Tab(관리 탭)** > **Settings (설정)** 페이지에서 보증 작업 일정을 수정할 수 있습니다.

1. OpenManage Integration for VMware vCenter의 **Monitor(모니터)** > **Job Queue(작업 큐)** 탭에서 **Warranty History(보증 내역)**를 클릭합니다.
2. **Change Schedule(일정 변경)** 아이콘을 클릭합니다.
3. Warranty Data Retrieval(보증 데이터 검색) 대화상자에서 다음을 수행합니다.
   a. Warranty Data(보증 데이터)에서 **Enable Warranty Data Retrieval(보증 데이터 검색 활성화)** 확인란을 선택합니다.
   b. Warranty Data Retrieval Schedule(보증 데이터 검색 일정)에서 작업 요일을 선택합니다.
   c. Warranty Data Retrieval Time(보증 데이터 검색 시간) 텍스트 상자에 작업의 로컬 시간을 입력합니다.
   이 작업이 올바른 시간에 실행되는 데 필요한 시간차를 계산해야 합니다.
4. **Apply(적용)**를 클릭합니다.

지금 보증 작업 실행

최소한 일주일에 한 번 보증 작업을 실행합니다.

1. OpenManage Integration for VMware vCenter의 **Monitor(모니터)** > **Job Queue(작업 큐)** 탭에서,
2. **Warranty History(보증 내역)** 및 **Hosts Warranty(호스트 보증)**를 클릭하여 실행하고자 하는 보증 작업을 선택합니다.
3. **Run Now(지금 실행)** 단추를 클릭합니다.
4. Success(성공) 대화상자에서 **Close(닫기)**를 클릭합니다.

   노트: 특정 호스트 보증이 실행되고 나면 모든 섀시에 대해 섀시 보증이 자동으로 실행됩니다. 여러 개의 vCenter를 갖추고 있는 SSO 환경의 경우, 하나의 vCenter에 대한 보증이 수동으로 실행되면 모든 vCenter에 대해 섀시 보증이 자동으로 실행됩니다.

   이제 보증 작업이 큐에서 대기 상태가 됩니다.

지금 섀시 보증 작업 실행

최소한 일주일에 한 번 보증 작업을 실행합니다.

1. OpenManage Integration for VMware vCenter의 **Monitor(모니터)** > **Job Queue(작업 큐)** 탭에서
2. **Warranty History(보증 내역)** 및 **Chassis Warranty(섀시 보증)**에서 실행하고자 하는 보증 작업을 선택합니다.
3. **Run Now(지금 실행)** 단추를 클릭합니다.
4. Success(성공) 대화상자에서 **Close(닫기)**를 클릭합니다.
   이제 보증 작업이 큐에서 대기 상태가 됩니다.

로그

OpenManage Integration for VMware vCenter의 **Monitor(모니터)** > **Log(로그)** 탭에서 사용자 작업을 볼 수 있습니다.

2개의 드롭다운 목록을 사용하여 이 페이지의 콘텐츠를 정렬할 수 있습니다. 첫 번째 드롭다운 목록을 사용하면 파일 범주를 정렬할 수 있으며 다음과 같은 정보가 포함되어 있습니다.

- 모든 범주
- 정보
- 경고
- 오류

두 번째 드롭다운 목록은 시간 블록을 정렬하는 데 도움이 되며 다음과 같은 정보가 포함되어 있습니다.

- 지난 주
- 지난 달
- 작년
- Custom Range(사용자 지정 범위)

  사용자 지정 범위를 선택하는 경우 시작 및 종료 날짜를 선택하고 Apply(적용)를 클릭합니다.

열 머리글을 클릭하여 데이터 그리드 열을 오름차순 또는 내림차순으로 정렬할 수도 있습니다.

Filter(필터) 텍스트 상자를 사용하여 콘텐츠 내에서 검색합니다.

페이지 그리드 하단에 다음과 같은 정보가 표시됩니다.

Total items(총 항목 수)	모든 로그 항목의 총 개수를 표시합니다.
Items per screen(화면당 항목 수)	현재 페이지에 있는 로그 항목 개수를 표시합니다. 드롭다운 상자를 사용하여 페이지당 항목 수를 설정합니다.
Page(페이지)	현재 페이지를 표시합니다. 텍스트 상자에 페이지 번호를 입력하거나 Previous(이전) 또는 Next(다음) 단추를 사용하여 원하는 페이지로 이동합니다.
Previous(이전) 또는 Next(다음) 단추	이전 또는 다음 페이지로 이동할 수 있는 단추입니다.
Export All(모두 내보내기) 아이콘	이 아이콘을 사용하여 CSV 파일로 콘텐츠를 내보낼 수 있습니다.

로그 보기

1. OpenManage Integration for VMware vCenter에서 **Monitor(모니터)** 탭을 클릭합니다.
2. Log(로그) 탭에서 OpenManage Integration for VMware vCenter의 사용자 조치 로그를 봅니다. Log(로그) 페이지에서 다음과 같은 정보를 볼 수 있습니다.

모든 범주	다음 로그 유형을 기준으로 로그를 필터링하고 볼 수 있게 합니다. • 모든 범주 • 정보 • 경고 • 오류
날짜 필터	다음과 같은 항목으로 로그를 필터링하고 볼 수 있습니다: • 지난 주 • 지난 달 • 작년 • Custom Range(사용자 지정 범위) 특정 일자를 기준으로 필터링하려면 **사용자 지정 범위**를 선택하고 날짜 필터 드롭다운 목록에서 필터링 하려는 날짜에 맞춰 **시작 일자** 및 **종료 일자**를 입력한 다음 **적용**을 클릭합니다.
Search(검색)	로그 설명 또는 로그에 있는 특정 텍스트를 기준으로 필터링할 수 있습니다.

표 2. 그리드 표 세부정보

범주	**범주 유형이 표시됩니다.**
날짜 및 시간	**사용자 조치의 날짜 및 시간이 표시됩니다.**
설명	**사용자 조치에 대한 설명이 표시됩니다.**

3. 그리드에서 데이터를 정렬하려면 열 머리글을 클릭합니다.

4. 범주 또는 시간 블록으로 정렬하려면 그리드 위에 있는 드롭다운 목록을 사용합니다.
5. 로그 항목 페이지 간을 이동하려면 Previous(이전) 및 Next(다음) 단추를 사용합니다.

로그 파일 내보내기

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

1. OpenManage Integration for VMware vCenter에서 **Monitor(모니터)** 탭을 클릭합니다.
2. CSV 형식의 로그 파일을 내보내려면 화면 오른쪽 하단에서 **Export All(모두 내보내기)** 아이콘을 클릭합니다.
3. **Select location for download(다운로드 위치 선택)** 대화상자에서 로그 정보를 저장할 위치를 찾아봅니다.
4. **File name(파일 이름)** 텍스트 상자에서 기본 이름인 ExportList.csv를 수락하거나 확장명이 .CSV인 고유한 파일 이름을 입력합니다.
5. **Save(저장)**를 클릭합니다.

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.

주제:

관리 콘솔 사용

관리 콘솔의 vCenter 등록 창에서 vCenter 서버를 등록하고, 라이센스를 업로드하거나 구입할 수 있습니다. 데모 라이센스를 사용하는 경우 여러 개의 호스트를 관리할 수 있는 정식 버전 라이센스를 구입할 수 있는 소프트웨어 구입 링크가 표시됩니다. 이 섹션에서 서버를 수정, 업데이트 및 등록 취소할 수도 있습니다.

관련 작업:

- 필요한 권한이 있는 비 관리자 사용자를 사용하여 vCenter 서버 등록 페이지 33
- vCenter 서버 등록
  - vCenter 로그인 수정
  - 등록된 vCenter의 SSL 인증서 업데이트
  - vCenter에서 OpenManage Integration for VMware vCenter 제거
- OpenManage Integration for VMware vCenter 라이센스 업로드

필요한 권한이 있는 비 관리자 사용자를 사용하여 vCenter 서버 등록

vCenter 서버의 vCenter 관리자 자격 증명 또는 필요한 권한이 있는 비 관리자 사용자를 사용하여 OMIVV 어플라이언스용 vCenter 서버를 등록할 수 있습니다.

다음 단계를 수행하여 필요한 권한이 있는 사용자를 사용하여 vCenter 서버를 등록합니다.

1. 역할을 추가하고 역할에 대한 필요한 권한을 선택하거나 기존 역할을 수정하여 해당 역할에 대해 선택된 권한을 변경합니다. vSphere 웹 클라이언트에서 역할을 만들거나 수정하고 권한을 선택하는 데 필요한 단계는 VMware vSphere 설명서를 참조하십시오. 역할과 필요한 모든 권한을 선택하려면 권한 정의 페이지 34을(를) 참조하십시오.

   노트: vCenter 관리자는 역할을 추가하거나 수정해야 합니다.
2. 역할을 정의하고 역할에 대한 권한을 선택한 후에 새로 생성한 역할을 할당합니다. vSphere 웹 클라이언트에서 권한 할당에 대한 자세한 내용은 VMware vSphere 설명서를 참조하십시오. 필요한 권한이 있는 vCenter 서버 비 관리자 사용자는 이제 vCenter를 등록 및/또는 등록 해제하거나 자격 증명을 수정하거나 인증서를 업데이트할 수 있습니다.

   노트: vCenter 관리자는 vSphere 클라이언트에서 권한을 할당해야 합니다.
3. 필요한 권한이 있는 비 관리자 사용자를 사용하여 vCenter 서버를 등록합니다. 필요한 권한이 있는 비 관리자 사용자가 vCenter 서버 등록 페이지 34을(를) 참조하십시오.
4. 1단계에서 생성했거나 수정한 역할에 Dell 권한을 할당합니다. vSphere 웹 클라이언트에서 역할에 Dell 권한 할당 페이지 34을(를) 참조하십시오.

이제 필요한 권한이 있는 비 관리자 사용자는 Dell 호스트를 사용하여 OMIVV 기능을 사용할 수 있습니다.

권한 정의

vCenter 서버를 등록하는 데 필요한 권한이 있는 비 관리자 사용자를 사용하려면 다음 권한을 선택합니다.

- Alarms(알람)
  - 알람 생성
  - 알람 수정
  - 알람 제거
- 확장명
  - 확장명 등록
  - 확장명 등록 취소
  - 확장명 업데이트
- Global(전역)
  - 작업 취소
  - 이벤트 로그
  - 설정
- 호스트
  - CIM
    - CIM 상호 작용
  - 구성
    - 고급 설정
    - 연결
    - Maintenance(유지관리)
    - 쿼리 패치
    - 보안 프로필 및 방화벽
  - 인벤토리
    - 클러스터에 호스트 추가
    - 독립 실행형 호스트 추가
- 호스트 프로필
  - 편집
  - View(보기)
- 권한
  - 권한 수정
  - 역할 수정
- 세션
  - 세션 유효성 검사
- 작업
  - 작업 생성
  - 작업 업데이트

노트: 필요한 권한이 있는 비 관리자 사용자가 vCenter 서버를 등록하는 동안 언급한 권한이 할당되지 않은 경우 오류 메시지가 표시됩니다.

필요한 권한이 있는 비 관리자 사용자가 vCenter 서버 등록

필요한 권한이 있는 비 관리자 사용자를 사용하여 OMIVV 어플라이언스용 vCenter 서버를 등록할 수 있습니다. .vCenter 서버 등록에 대한 자세한 내용은 vCenter 서버 등록 페이지 35.를 참조하십시오.

vSphere 웹 클라이언트에서 역할에 Dell 권한 할당

기존 역할을 편집하여 Dell 권한을 할당할 수 있습니다.

노트: 관리자 권한이 있는 사용자로 로그인해야 합니다.

기존 역할에 Dell 권한을 할당하려면 다음을 수행합니다.

1. 관리 권한을 사용하여 vSphere 웹 클라이언트에 로그인합니다.

2. vSphere 웹 클라이언트에서 **관리 → 역할 관리자**로 이동합니다.
3. 드롭다운 메뉴에서 vCenter 서버 시스템을 선택합니다.
4. 역할을 선택하고 **역할 편집 작업**을 클릭합니다.
5. 다음 권한을 선택하고 **확인**을 클릭합니다.
   - Dell
     - Dell.Configuration
     - Dell.Deploy-Provisioning
     - Dell.Inventory
     - Dell.Monitoring
     - Dell.Reporting

   *OpenManage Integration for VMware vCenter User's Guide(OpenManage Integration for VMware vCenter 사용 설명서)OpenManage Integration for VMware vCenter User's Guide(OpenManage Integration for VMware vCenter 사용 설명서)*를 참조하십시오.보안 역할 및 권한 페이지 131vCenter 내에서 사용할 수 있는 OMIVV 역할에 대한 자세한 내용은.

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

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

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

vCenter 서버 등록

OpenManage Integration for VMware vCenter가 설치된 후에 OpenManage Integration for VMware vCenter를 등록할 수 있습니다. OpenManage Integration for VMware vCenter는 관리자 계정 또는 vCenter 작업에 필요한 권한이 있는 관리자가 아닌 사용자 계정을 사용합니다. OpenManage Integration for VMware vCenter는 현재 OMIVV 어플라이언스당 10개의 vCenter를 지원하며 나중에 변경할 수 있습니다.

1. 지원되는 브라우저에서 **관리 콘솔**을 엽니다.
2. 새 vCenter 서버를 등록하려면 **VCENTER 등록**을 클릭한 다음 **새 vCenter 서버 등록**을 클릭합니다.
3. **새 vCenter 등록** 대화 상자의 **vCenter 이름** 아래에서 다음을 수행합니다.
   a. **vCenter 서버 IP 또는 호스트 이름** 텍스트 상자에 vCenter IP 주소 또는 호스트 이름 또는 FQDN을 입력합니다.

      노트: 정규화된 도메인 이름(FQDN)을 사용하여 VMware vCenter에서 OMIVV를 등록할 것을 권장합니다. 모든 등록의 경우 vCenter의 호스트 이름은 DNS 서버에서 올바르게 확인됩니다. 다음은 DNS 서버 사용을 위한 권장 사례입니다.
      - 유효한 DNS 등록에서 OMIVV 어플라이언스를 배포할 때는 정적 IP 주소 및 호스트 이름을 할당합니다. 정적 IP 주소를 사용하면 시스템을 다시 시작하는 동안 OMIVV 어플라이언스의 IP 주소를 동일하게 유지할 수 있습니다.
      - 정방향 및 역방향 조회 모두에 OMIVV 호스트 이름 항목이 표시되는지 확인합니다.

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

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

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

OpenManage Integration for VMware vCenter 요구 사항

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.

표 3. 관리되는 호스트에서 지원되는 ESXi 버전

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

표 4. 릴리스 3.2에 지원되는 vCenter 서버 버전

vCenter 버전	데스크톱 클라이언트 지원	웹 클라이언트 지원
v5.1 U2	Y	아니요
v5.1 U3	Y	아니요
v5.5 U1	Y	Y
v5.5 U2	Y	Y
v5.5 U3	Y	Y
v6.0	Y	Y
v6.0 U1	Y	Y
v6.0 U2	Y	Y
v6.0 U3	Y	Y

vCenter 로그인 수정

vCenter 로그인 자격 증명은 관리자 권한이 있는 사용자 또는 관리자 권한은 없지만 필요한 권한이 있는 사용자가 수정할 수 있습니다.

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

노트: vCenter 로그인 자격 증명을 수정하는 관리 권한이 없는 사용자에게 필요한 권한이 할당되지 않은 경우 오류 메시지가 표시됩니다.

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.

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

1. OpenManage Integration for VMware vCenter의 Administration Console에서, 링크를 사용하여 **Help and Support(도움말 및 지원)** 탭에서 Administration Console을 엽니다.
2. Login(로그인) 대화상자에 암호를 입력합니다.
3. 왼쪽 창에서 **VCENTER REGISTRATION(VCENTER 등록)**을 클릭합니다. 등록된 vCenter가 표에 표시됩니다. 라이센스 업로드 대화상자를 표시하려면 **Upload License(라이센스 업로드)**를 클릭합니다.
4. 라이센스 파일을 탐색하려면 **Browse(찾아보기)** 단추를 클릭하여 라이센스 파일을 탐색한 후 **Upload(업로드)**를 클릭합니다.

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

   노트: 호스트를 더 추가해야 할 경우 라이센스를 추가할 수 있습니다. 위에 설명된 과정에 따라 라이센스를 추가하십시오.

   노트: 성공적으로 인벤토리 작업을 수행한 11세대, 12세대 및 13세대 서버의 수가 구입한 라이센스의 수와 동일할 경우 11세대, 12세대 또는 13세대 서버 몇 개를 제거해 기존 연결 프로필을 편집하십시오. 제거된 11세대, 12세대 또는 13세대 생성 서버에 대해 새 연결 프로필을 생성하십시오.

가상 어플라이언스 관리

가상 어플라이언스 관리에 OpenManage Integration for VMware vCenter 네트워크, 버전, NTP 및 HTTPS 정보가 포함되어 있으며, 이를 사용하여 다음을 수행할 수 있습니다.

- 가상 어플라이언스 다시 시작
- 가상 어플라이언스 업데이트 및 업데이트 리포지토리 위치 구성
- 문제 해결 번들 다운로드
- NTP 서버 설정
- HTTPS 인증서 업로드

가상 어플라이언스 다시 시작

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

1. OpenManage Integration for VMware vCenter의 Administration Console에서 링크를 사용하여 Administration Console을 엽니다.
2. Login(로그인) 대화상자에 암호를 입력합니다.
3. 왼쪽 창에서 **APPLIANCE MANAGEMENT(어플라이언스 관리)**를 클릭합니다.
4. OpenManage Integration for VMware vCenter를 다시 시작하려면 **Restart the Virtual Appliance(가상 어플라이언스 다시 시작)**를 클릭합니다.
5. **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. 백업 관리 및 복원을 참조하십시오.

1. OpenManage Integration for VMware vCenter의 Administration Console에서 링크를 사용하여 Administration Console을 엽니다.
2. Login(로그인) 대화상자에 암호를 입력합니다.
3. 왼쪽 창에서 **APPLIANCE MANAGEMENT(어플라이언스 관리)**를 클릭합니다.
4. 어플라이언스 업데이트 옆에 있는 **Edit(편집)**을 클릭합니다.
5. **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 프록시를 입력해야 합니다.

가상 어플라이언스 소프트웨어 업데이트

데이터 손실을 방지하려면 소프트웨어 업데이트를 시작하기 전에 어플라이언스 백업을 수행합니다.

1. 웹 브라우저를 실행하고 https://<ApplianceIPAddress>를 입력합니다.
2. 왼쪽 창에서 **APPLIANCE MANAGEMENT(어플라이언스 관리)**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. 문제 해결 번들 대화상자를 표시하려면 **Generate Troubleshooting Bundle(문제 해결 번들 생성)**을 클릭합니다.
4. **Download Troubleshooting Bundle(문제 해결 번들 다운로드)** 링크를 클릭합니다.
5. 종료하려면 **Close(닫기)**를 클릭합니다.

HTTP 프록시 설정

Administration Console을 사용하여 HTTP 프록시 설정을 설정합니다.

1. OpenManage Integration for VMware vCenter의 Administration Console에서 링크를 사용하여 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 Administration Console에서 링크를 사용하여 Administration Console을 엽니다.
2. Login(로그인) 대화 상자에 암호를 입력합니다.
3. 왼쪽 창에서 **어플라이언스 관리**를 클릭합니다.
4. **NTP Settings(NTP 설정)** 아래에서 **편집**을 클릭합니다.
5. **사용** 확인란을 선택합니다. **기본** 및 **보조 NTP 서버**의 **호스트 이름** 또는 **IP 주소**를 입력하고 **적용**을 클릭합니다.
6. 종료하려면 **취소**를 클릭합니다.

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

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 Administration Console에서 링크를 사용하여 Administration Console을 엽니다.
2. Login(로그인) 대화상자에 암호를 입력합니다.
3. 왼쪽 창에서 **APPLIANCE MANAGEMENT(어플라이언스 관리)**를 클릭합니다.
4. **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 **계속**을 클릭하고 취소하려면 **취소**를 클릭합니다.
5. 요청에 대해 **일반 이름**, **조직 이름**, **부서**, **지역**, **시/도**, **국가** 및 **전자 메일**을 입력합니다. **계속**을 클릭합니다.
6. **Download(다운로드)**를 클릭하고 결과로 생성되는 인증서 요청을 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 Chrome을 사용하여 인증서를 업로드할 수 있습니다.

1. OpenManage Integration for VMware vCenter의 Administration Console에서 링크를 사용하여 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

노트: 사용자 지정 인증서를 업로드할 경우 vCenter 등록 전에 어플라이언스에 대한 새 인증서를 업로드해야 합니다. vCenter 등록 후 새 사용자 지정 인증서를 업로드할 경우 웹 클라이언트에 통신 오류가 표시됩니다. 이 문제를 해결하려면 vCenter에서 어플라이언스 등록을 취소하고 재등록해야 합니다.

1. OpenManage Integration for VMware vCenter의 Administration Console에서 링크를 사용하여 Administration Console을 엽니다.
2. Login(로그인) 대화상자에 암호를 입력합니다.
3. 왼쪽 창에서 **APPLIANCE MANAGEMENT(어플라이언스 관리)**를 클릭합니다.
4. **HTTPS Certificates(HTTPS 인증서)** 아래에서 **Restore Default Certificate(기본 인증서 복원)** 링크를 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 Administration Console에서 링크를 사용하여 Administration Console을 엽니다.
2. Login(로그인) 대화상자에 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.

노트: NTP 설정은 저장 및 복원되지 않습니다.

1. OpenManage Integration for VMware vCenter의 Administration Console에서 링크를 사용하여 Administration Console을 엽니다.

2. Login(로그인) 대화상자에 암호를 입력합니다.
3. 왼쪽 창에서 **BACKUP AND RESTORE(백업 및 복원)**를 클릭합니다.
4. 현재 백업 및 복원 설정을 편집하려면 **Edit(편집)**를 클릭합니다.
5. **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.
6. 설정을 저장하려면 **Apply(적용)**를 클릭합니다.
7. 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. OpenManage Integration for VMware vCenter의 Administration Console에서 링크를 사용하여 Administration Console을 엽니다.
2. Login(로그인) 대화상자에 암호를 입력합니다.
3. 왼쪽 창에서 **BACKUP AND RESTORE(백업 및 복원)**를 클릭합니다.
4. 백업 및 복원 설정을 편집하려면 **Edit Automatic Scheduled Backup(자동 예약된 백업 편집)**을 클릭합니다. 그러면 필드가 활성화됩니다.
5. 백업을 사용하려면 **Enabled(활성화됨)**를 클릭합니다.
6. 백업을 실행할 요일의 확인란을 선택합니다.
7. **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.
8. **Apply(적용)**를 클릭합니다.

즉시 백업 수행

1. OpenManage Integration for VMware vCenter의 Administration Console에서 링크를 사용하여 Administration Console을 엽니다.
2. Login(로그인) 대화상자에 암호를 입력합니다.
3. 왼쪽 창에서 **BACKUP AND RESTORE(백업 및 복원)**를 클릭합니다.
4. **Backup Now(지금 백업)**를 클릭합니다.
5. 백업 설정에서 위치 및 암호화 암호를 사용하려면 **Backup Now(지금 백업)** 대화상자에서 해당 확인란을 선택합니다.
6. **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.

7. **Backup(백업)**을 클릭합니다.

백업에서 데이터베이스 복원

노트: 복원 작업이 완료되면 가상 어플라이언스가 다시 부팅됩니다.

1. OpenManage Integration for VMware vCenter의 Administration Console에서 링크를 사용하여 Administration Console을 엽니다.
2. Login(로그인) 대화상자에 암호를 입력합니다.
3. 왼쪽 창에서 **BACKUP AND RESTORE(백업 및 복원)**를 클릭하면 현재 백업 및 복원 설정이 표시됩니다.
4. **Restore Now(지금 복원)**를 클릭합니다.

5. Restore Now(지금 복원) 대화상자에 **backup .gz** 파일(CIFS/NFS 형식)과 함께 파일 위치를 입력합니다.
6. 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.

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

vSphere 클라이언트 콘솔 이해

vSphere 클라이언트 콘솔은 가상 시스템의 vSphere 클라이언트 내에서 찾을 수 있습니다. 또한 **콘솔**은 관리 콘솔과 함께 작동합니다. 콘솔은 다음과 같은 기능을 제공합니다.

- 네트워크 설정 구성
- 가상 어플라이언스 암호 변경
- 로컬 시간대 설정
- 가상 어플라이언스 다시 부팅
- 가상 어플라이언스를 공장 설정으로 다시 설정
- 콘솔 새로 고침
- 콘솔에서 로그아웃
- 읽기 전용 사용자 역할
- OpenManage Integration Plugin 2.0 버전에서 최신 버전으로 업그레이드
- 2.x에서 현재 버전으로 마이그레이션하는 마이그레이션 경로

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

네트워크 설정 구성

네트워크 설정 변경은 vSphere 클라이언트 콘솔에서 수행합니다.

1. vSphere 웹 클라이언트의 Navigator(탐색 창)에서 **vCenter**를 클릭합니다.
2. Navigator(탐색 창)에서, 관리할 가상 머신을 선택합니다.
3. 다음 중 하나를 수행합니다.
   - Object(개체) 탭에서**Action(조치)** > **Open Console(콘솔 열기)**을 선택합니다.
   - 선택한 가상 머신을 마우스 오른쪽 단추로 클릭하고 **Open Console(콘솔 열기)**을 선택합니다.
4. **콘솔** 창에서 **네트워크 구성**을 선택한 후 **<ENTER>**를 누릅니다.
5. **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 웹 클라이언트에서 콘솔을 사용하여 변경합니다.

1. vSphere 웹 클라이언트의 Navigator(탐색 창)에서 **vCenter**를 클릭합니다.
2. Navigator(탐색 창)에서, 관리할 가상 머신을 선택합니다.
3. 다음 중 하나를 수행합니다.
   - Object(개체) 탭에서**Action(조치)** > **Open Console(콘솔 열기)**을 선택합니다.
   - 선택한 가상 머신을 마우스 오른쪽 단추로 클릭하고 **Open Console(콘솔 열기)**을 선택합니다.
4. 콘솔에서 화살표 키를 사용하여 **Change Admin Password(관리 암호 변경)**를 선택하고 **<ENTER>** 키를 누릅니다.
5. **현재 관리 암호**를 입력하고 **<ENTER>**를 누릅니다.

관리 암호에는 특수 문자, 숫자, 대문자, 소문자를 각각 하나씩 사용하고 최소 8자여야 합니다.

6. **새 관리 암호 입력**에 새 암호를 입력하고 **<ENTER>**를 누릅니다.
7. **Please Confirm Admin Password(관리 암호를 확인하십시오)** 텍스트 상자에 새 암호를 다시 입력한 후 **<ENTER>** 키를 누릅니다.

로컬 시간대 설정

로컬 시간대를 설정하려면 다음을 수행합니다.

1. 기본 VMware vCenter 창에서 Console(콘솔) 탭을 클릭하여 Administration Console을 시작합니다.
2. OMIVV가 부팅을 완료할 때까지 기다린 후 사용자 이름으로 admin을 입력하고 **Enter**를 누릅니다.
3. 새 관리자 암호를 입력합니다. 암호는 표시되는 암호 복잡성 규칙에 따라 설정해야 합니다. **Enter**키를 누릅니다.
   Password confirmation(암호 확인) 대화 상자가 표시됩니다.
4. 암호를 한 번 더 입력하고 **Enter**를 누릅니다.
   Password Set confirmation(암호 설정 확인) 메시지가 표시됩니다.
5. **Enter**를 눌러 OMIVV 어플라이언스에서 네트워크 및 시간대 정보를 구성합니다.
6. OpenManage Integration for VMware vCenter 시간대 정보를 구성하려면 Date/Time Properties(날짜/시간 속성)를 클릭하여 시간대 및 날짜를 설정합니다.
7. **Date and Time(날짜 및 시간)** 탭에서 **Synchronize date and time over the network(네트워크에서 날짜 및 시간 동기화)**를 선택합니다.
   NTP Servers(NTP 서버) 창이 표시됩니다.
8. **Time Zone(시간대)**을 클릭하고 해당 시간대를 선택한 다음 **OK(확인)**를 클릭합니다.

가상 어플라이언스 다시 부팅

가상 어플라이언스를 다시 부팅하려면 다음을 수행합니다.

1. vSphere 웹 클라이언트의 Navigator(탐색 창)에서 **vCenter**를 클릭합니다.
2. Navigator(탐색 창)에서, 관리할 가상 머신을 선택합니다.
3. 다음 중 하나를 수행합니다.
   - Object(개체) 탭에서 **Action(조치)** > **Open Console(콘솔 열기)**을 선택합니다.
   - 선택한 가상 머신을 마우스 오른쪽 단추로 클릭하고 **Open Console(콘솔 열기)**을 선택합니다.
4. 화살표 키를 사용하여 **Reboot this Virtual Appliance(이 가상 어플라이언스 다시 부팅)**를 선택하고 **<ENTER>**를 누릅니다.
5. 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?
```

6. 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 웹 클라이언트의 Navigator(탐색 창)에서 **vCenter**를 클릭합니다.
2. Navigator(탐색 창)에서, 관리할 가상 머신을 선택합니다.
3. 다음 중 하나를 수행합니다.
   - Object(개체) 탭에서**Action(조치)** > **Open Console(콘솔 열기)**을 선택합니다.
   - 선택한 가상 머신을 마우스 오른쪽 단추로 클릭하고 **Open Console(콘솔 열기)**을 선택합니다.
4. 화살표 키를 사용하여 **Reset this Virtual Appliance to Factory Settings(이 가상 어플라이언스를 공장 설정으로 다시 설정)**를 선택하고 **<ENTER>**를 누릅니다.

5. 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?
```

6. 재설정하려면 **y**를 입력하고 취소하려면 **n**을 입력합니다. 어플라이언스가 원래 공장 설정 및 기타 모든 설정으로 다시 설정되며 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.

콘솔에서 로그아웃

콘솔에서 로그아웃하려면 로그인한 계정에서 오른쪽 상단 모서리의 **로그아웃**을 클릭합니다.

읽기 전용 사용자 역할

진단을 위한 셸 액세스 권한이 있는 읽기 전용이라고 하는 권한 없는 사용자 역할이 있습니다. 읽기 전용 사용자의 권한은 탑재 실행으로 제한됩니다. 읽기 전용 사용자의 암호가 **readonly**로 설정됩니다. 읽기 전용 사용자의 암호가 보안을 위해 관리자 암호에서 변경되었습니다(OMIVV 버전 1.0 - 버전 3.2).

기존 버전에서 최신 버전으로 OMIVV 업그레이드

1. 관리 콘솔을 열려면 OpenManage Integration for VMware vCenter의 **도움말 및 지원** 탭에서 **관리 콘솔** 아래에 있는 링크를 클릭하거나 웹 브라우저를 시작하여 `https:\\<ApplianceIP|hostname>` URL을 입력합니다.
2. **로그인** 대화 상자에 암호를 입력합니다.
3. 관리 콘솔의 왼쪽 창에서 **어플라이언스 관리**를 클릭합니다.
4. **어플라이언스 관리** 페이지에서 네트워크 설정에 따라 프록시를 활성화하고, 네트워크에 프록시가 필요한 경우 프록시 설정을 제공합니다.
5. OpenManage Integration 플러그인을 기존 버전에서 최신 버전으로 업그레이드하려면 다음 단계 중 하나를 수행합니다.
   - **업데이트 리포지토리 경로**가 http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/ 경로로 설정되어 있는지 확인합니다. 경로가 서로 다른 경우 **어플라이언스 관리** 창의 **어플라이언스 업데이트** 영역에서 **편집**을 클릭하여 경로를 **업데이트 리포지토리 경로** 텍스트 상자의 `http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest` 경로로 업데이트합니다. 저장하려면 **Apply(적용)**를 클릭합니다.
   - `http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/` 경로에서 모든 파일과 폴더를 다운로드하여 HTTP 공유에 복사합니다. **어플라이언스 관리** 창의 **어플라이언스 업데이트** 섹션에서 **편집**을 클릭한 다음 **업데이트 리포지토리 경로** 텍스트 상자에서 오프라인 HTTP 공유에 대한 경로를 포함하고 **적용**을 클릭합니다.
6. 사용 가능한 가상 어플라이언스 버전과 현재 가상 어플라이언스 버전을 비교하여 사용 가능한 가상 어플라이언스 버전이 현재 가상 어플라이언스 버전보다 최신인지 확인합니다.
7. 업데이트를 가상 어플라이언스에 적용하려면 **어플라이언스 설정** 아래에서 **가상 어플라이언스 업데이트**를 클릭합니다.
8. **어플라이언스 업데이트** 대화 상자에서 **업그레이드**를 클릭합니다.
   업그레이드를 클릭하면 **관리 콘솔** 창에서 로그오프됩니다.
9. 웹 브라우저를 닫습니다.

노트: RPM 업그레이드가 완료되면 OMIVV 콘솔에서 로그인 화면을 볼 수 있습니다. 브라우저를 열고 `https:\\<ApplianceIP/hostname>\DellAdminPortal` 링크를 입력하고 **어플라이언스 업데이트** 영역으로 이동합니다. 사용할 수 있는 버전과 현재 가상 어플라이언스 버전이 같은지 확인할 수 있습니다.

노트:

2.x에서 3.2으로 마이그레이션

버전을 제거한 후 v3.2 OVF로 새로 배포를 시작한 다음 백업 및 복원 경로를 사용하여 이전 버전(2.x)에서 버전 3.2 버전으로 데이터를 마이그레이션할 수 있습니다.

이전 버전에서 OMIVV 3.2 버전으로 마이그레이션하려면 다음 단계를 수행합니다.

1. 이전 릴리스(v2.x)에 대한 데이터베이스 백업을 수행합니다.
   자세한 내용은 `Dell.com/support/manuals`에서 *OpenManage Integration for VMware vCenter 사용 설명서*를 참조하십시오.
2. vCenter에서 이전 어플라이언스의 전원을 끕니다.
   노트: vCenter에서 플러그인을 등록 취소하면 OMIVV 플러그인에 의해 vCenter에 등록된 모든 알람이 제거되고 조치 등과 같이 알람 발생 시 수행되는 모든 사용자 지정 항목이 제거됩니다. 백업한 후에 플러그인을 등록 취소한 경우, 자세한 내용은 *OpenManage Integration for VMware vCenter vSphere 웹 클라이언트 버전 3.2용 빠른 설치 안내서*를 참조하십시오.
3. 새 OpenManage Integration 버전 3.2 OVF를 배포합니다.
   OVF 배포에 대한 자세한 내용은 *OpenManage Integration for VMware vCenter vSphere 웹 클라이언트 버전 3.2용 빠른 설치 안내서*를 참조하십시오.
4. OpenManage Integration 버전 3.2 어플라이언스의 전원을 켭니다.
5. 어플라이언스에서 네트워크 및 표준 시간대를 설정합니다.
   새 OpenManage Integration 버전 3.2 어플라이언스의 IP 주소는 이전 어플라이언스와 같아야 합니다. 네트워크 세부 정보의 경우 *OpenManage Integration for VMware vCenter vSphere 웹 클라이언트 버전 3.2용 빠른 설치 안내서*를 참조하십시오.
   노트: OMIVV 3.2 어플라이언스의 IP 주소가 이전 어플라이언스의 IP 주소와 다를 경우 OMIVV 플러그인이 제대로 작동하지 않을 수 있습니다. 이러한 경우 모든 vCenter 인스턴스를 등록 취소하고 다시 등록해야 합니다.
6. 데이터베이스를 새 OMIVV 어플라이언스에 복원합니다.
   노트: 클러스터에서 Proactive HA를 활성화한 경우 OMIVV는 이 클러스터에 대한 Dell Inc 공급자를 등록 취소하고 복원 후 Dell Inc 공급자를 다시 등록합니다. 따라서 복원이 완료될 때까지 Dell 호스트에 대한 상태 업데이트를 사용할 수 없습니다.
   자세한 내용은 `Dell.com/support/manuals`에서 *OpenManage Integration for VMware vCenter 사용 설명서*의 **백업에서 OMIVV 데이터베이스 복원**을 참조하십시오.
7. 새 라이센스 파일을 업로드합니다.
   자세한 내용은 *OpenManage Integration for VMware vCenter vSphere 웹 클라이언트 버전 3.2용 빠른 설치 안내서*를 참조하십시오.
8. 어플라이언스를 확인합니다.
   자세한 내용은 *OpenManage Integration for VMware vCenter vSphere 웹 클라이언트 버전 3.2용 빠른 설치 안내서*를 통해 데이터베이스 마이그레이션에 성공했는지 확인하십시오.
9. 모든 호스트에서 **인벤토리**를 실행합니다.
   노트:
   업그레이드 후에는 OMIVV가 관리하는 모든 호스트에서 인벤토리를 다시 실행하는 것이 좋습니다. 자세한 내용은 *OpenManage Integration for VMware vCenter 사용 설명서*의 **인벤토리 작업 실행**을 참조하십시오.
   새 OMIVV 버전 3.2 어플라이언스의 IP 주소가 이전 어플라이언스와는 다른 주소로 변경된 경우 SNMP 트랩에 대한 트랩 대상이 새 어플라이언스를 가리키도록 구성합니다. 12세대 이상 서버의 경우 해당 호스트에서 인벤토리를 실행하면 IP 변경이 수정됩니다. 이전 버전을 준수했던 12세대 이전 호스트의 경우 IP 변경은 비준수로 표시되기 때문에 Dell EMC OpenManage Server Administrator(OMSA)를 구성해야 합니다. 호스트 준수 문제의 해결에 관한 자세한 내용은 `Dell.com/support/manuals`에서 OpenManage Integration for VMware vCenter 사용 설명서의 ***vSphere 호스트에 대한 준수 보고 및 해결***을 참조하십시오.

7

설정

Settings(설정) 탭은 다음을 수행하는 데 사용됩니다.

- 보증 만료 알림 설정 보기
- 보증 만료 알림 구성
- 펌웨어 업데이트 리포지토리 설정
- 알람 및 이벤트 설정 보기
- 이벤트 및 알람 구성 및 관리
- 인벤토리 및 보증의 데이터 검색 일정 보기 및 구성

주제:

OMSA 링크 편집

이 절차에서는 OMSA 웹 서버를 이미 설치했으며 초기 구성 마법사를 사용하여 이 링크를 이전에 구성한 것으로 간주합니다. 사용 중인 OMSA 버전 및 웹 서버 설치와 구성 방법에 대한 지침을 보려면 *OpenManage Server Administrator 설치 안내서*를 참조하십시오.

구성 마법사를 실행하는 동안 링크를 제공하지 않은 경우 OpenManage Integration for VMware vCenter의 **Manage(관리)** > **Settings(설정)**탭에서 이 링크를 편집할 수 있습니다. 이 작업은 웹 클라이언트에는 적용되지 않습니다.

노트: OMSA는 Dell PowerEdge 11세대 서버 이전 서버에서만 필요합니다. 웹 클라이언트 초기 구성 마법사에는 OMSA 링크를 제공하는 옵션이 없습니다. OMSA 링크는 .net 클라이언트에만 적용됩니다.

1. OpenManage Integration for VMware vCenter에서 **Manage(관리)** > **Settings(설정)** 탭의 vCenter Settings(vCenter 설정) 아래에서 OMSA Web Server URL(OMSA 웹 서버 URL) 오른쪽에 있는 **Edit(편집)**를 클릭합니다.
2. OMSA Web Server URL(OMSA 웹 서버 URL) 대화상자에 **URL**을 입력합니다.
   HTTPS를 포함하여 전체 URL을 입력해야 합니다.
3. OMSA URL을 모든 vCenter에 적용하려면 **Apply these settings to all vCenters(이 설정을 모든 vCenter에 적용)** 확인란을 선택합니다. 이 확인란을 선택하지 않으면 OMSA URL은 하나의 vCenter에만 적용됩니다.
4. 이 호스트의 호스트 Summary(요약) 탭을 탐색하여 링크가 올바르게 작동되는지 확인합니다. OMSA 콘솔 링크가 Dell 호스트 정보 내에 있는지 확인합니다.

11세대 서버에서 OMSA 사용 이해

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

Dell PowerEdge 11세대 서버에서 OMSA를 구성하려면 다음을 선택하십시오.

- ESXi 시스템에 OMSA 에이전트 배포
- OMSA 트랩 대상 설정

노트: 위 옵션 외에 .Net 클라이언트를 사용하고 Host Compliance를 실행시켜 OMSA 에이전트를 설치하고 구성할 수 있습니다.

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 <OMSA version X.X>
```

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

OMSA 트랩 대상 설정

이 작업은 iDRAC6 대신 OMSA를 사용하여 이벤트를 생성하는 호스트 시스템에만 해당됩니다. iDRAC6에서는 추가 구성이 필요하지 않습니다.

노트: OMSA는 Dell PowerEdge 12세대 서버 이전 버전의 Dell 서버에서만 필요합니다.

1. OpenManage Integration for VMware vCenter **Manage(관리)** > **Settings(설정)** 탭에서 OMSA 사용자 인터페이스로 이동되는 링크를 사용하거나, 웹 브라우저(**https://<HostIP>:1311/**)에서 OMSA 에이전트를 탐색합니다.
2. 인터페이스에 로그인하고 **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 상단에서 **Platform Events(플랫폼 이벤트)** 옵션을 선택합니다.
5. 회색 **대상 구성** 단추를 클릭하고 **대상** 링크를 클릭합니다.
6. **대상 활성화** 확인란을 선택합니다.
7. **대상 IP 주소** 필드에 OpenManage Integration for VMware vCenter 어플라이언스 IP 주소를 입력합니다.
8. **변경사항 적용**을 클릭합니다.
9. 1-8단계를 반복하여 추가 이벤트를 구성합니다.

보증 만료 알림 설정 보기

1. OpenManage Integration for VMware vCenter에서 **Manage(관리)** > **Settings(설정)**탭의 Appliance Settings(어플라이언스 설정) 아래에서 **Warranty Expiration Notification(보증 만료 알림)**을 클릭합니다.
2. Warranty Expiration Notification(보증 만료 알림)에서 다음 정보를 확인할 수 있습니다.
   - 설정의 활성화 여부
   - 최초 경고 설정 일 수
   - 위험 경고 설정 일 수
3. 보증 만료 알림을 구성하려면 보증 만료 알림 구성을 참조하십시오.

보증 만료 알림 구성

보증 만료를 경고하는 보증 만료 임계값을 구성할 수 있습니다.

1. OpenManage Integration for VMware vCenter의 **Manage(관리)** > **Settings(설정)** 탭에 있는 Appliance Settings(어플라이언스 설정)에서 **Warranty Expiration Notification(보증 만료 알림)** 오른쪽의 **Edit(편집)** 아이콘을 클릭합니다.
2. Warranty Expiration Notification(보증 만료 알림) 대화상자에서 다음을 수행합니다.
   a. 이 설정을 활성화하려면 **Enable warranty expiration notification for hosts(호스트의 보증 만료 알림 활성화)** 확인란을 선택합니다.
   확인란을 선택하면 보증 만료 알림이 활성화됩니다.

b. Minimum Days Threshold(최소 일 수 임계값) 경고에서 다음을 수행합니다.
   i. Warning(경고) 드롭다운 목록에서, 보증 만료 경고를 수신하기 전의 일 수를 선택합니다.
   ii. Critical(위험) 드롭다운 목록에서, 보증 만료 경고를 수신하기 전의 일 수를 선택합니다.

3. **Apply(적용)**를 클릭합니다.

이벤트 및 알람 구성

Dell Management Center Events and Alarms(이벤트 및 알람) 페이지에서 모든 하드웨어 알람을 활성화하고 비활성화합니다. vCenter Alarms(vCenter 알람) 탭에 현재 알람 상태가 표시됩니다. 위험 이벤트는 실제 또는 임박한 데이터 손실이나 시스템 오작동을 나타냅니다. 경고 이벤트는 심각한 상태는 아니지만 향후 문제 발생의 가능성을 나타냅니다. VMware Alarm Manager를 사용해 이벤트 및 알람을 활성화할 수도 있습니다. 이벤트는 Hosts and Clusters(호스트 및 클러스터) 보기의 vCenter Tasks and Events(vCenter 작업 및 이벤트) 탭에 표시됩니다. 서버에서 이벤트를 수신하기 위해 OMIVV가 SNMP 트랩 대상을 구성됩니다. 12세대 이상의 호스트에서는 SNMP 트랩 대상이 iDRAC에서 설정됩니다. 12세대 이전 호스트의 경우 트랩 대상이 OMSA에서 설정됩니다. **Management(관리) Settings(설정)** 탭에서 OpenManage Integration for VMware vCenter를 사용하여 이벤트와 알람을 구성할 수 있습니다. vCenter Settings(vCenter 설정) 아래에서 Events and Alarms(이벤트 및 알람) 제목을 확장해 모든 Dell 호스트에 대한 현재 vCenter 알람 또는 이벤트 게시 수준(활성화된 또는 비활성화됨)을 표시하십시오.

노트: OMIVV는 12세대 이상의 호스트에 대해 SNMP v1 및 v2 경고를 지원합니다. 12세대 이전 호스트의 경우 OMIVV가 vCenter에서 SNMP v1 경고를 지원합니다. 트랩 대상 설정에 대한 자세한 내용은 OMSA 트랩 대상 설정을 참조하십시오.

노트: Dell 이벤트를 수신하려면 알람과 이벤트를 모두 활성화해야 합니다.

1. Events and Alarms(이벤트 및 알람) 오른쪽의 **Edit(편집)** 아이콘을 클릭합니다.
2. 모든 하드웨어 알람 및 이벤트를 활성화하려면 **Enable Alarms for all Dell Hosts(모든 Dell 호스트에 알람 활성화)** 확인란을 선택합니다.

   노트: 알람이 활성화된 Dell 호스트가 유지 보수 모드로 전환되어 위험 수준의 이벤트를 알리며 필요에 따라 알람을 수정할 수 있습니다.

3. 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.

   노트: 이 단계는 Dell 호스트에 알람 활성화를 선택한 경우에만 표시됩니다.

4. **Event Posting Level(이벤트 게시 수준)**에서 다음 중 하나를 선택합니다.
   - Do not post any events(이벤트 게시하지 않음)

     하드웨어 이벤트를 차단합니다.
   - Post All Events(모든 이벤트 게시)

     모든 하드웨어 이벤트를 게시합니다.
   - Post only Critical and Warning Events(위험 및 경고 이벤트만 게시)

     위험 및 경고 수준의 하드웨어 이벤트만 게시합니다.
   - Post only Virtualization-Related Critical and Warning Events(가상화 관련 위험 및 경고 이벤트만 게시)

     가상화 관련 위험 및 경고 이벤트만 게시합니다. 이벤트 게시 수준의 기본값입니다.

5. 설정을 모든 vCenter에 적용하려면 **Apply these settings to all vCenters(이 설정을 모든 vCenter에 적용)** 확인란을 선택합니다.

   노트: 이 옵션을 선택하면 모든 vCenter의 기존 설정이 재설정됩니다.

   Setting(설정) 페이지에서 All Registered vCenters(등록된 모든 vCenter)가 이미 선택되어 있으면 이 옵션이 회색으로 표시됩니다.
6. 저장하려면 **Apply(적용)**를 클릭합니다.

알람 및 이벤트 설정 보기

알람 및 이벤트가 구성되면 Settings(설정) 탭에서 호스트에 vCenter 알람이 활성화되어 있는지 여부와 선택된 이벤트 게시 수준을 볼 수 있습니다.

1. **OpenManage Integration for VMware vCenter** > **Manage(관리)** > **Settings(설정)** 탭의 vCenter Settings(vCenter 설정) 아래에서 Events and Alarms(이벤트 및 알람)를 확장합니다.
2. Events and Alarms(이벤트 및 알람)에서 다음과 같은 사항을 확인할 수 있습니다.
   - Dell 호스트의 vCenter 알람: Enabled(활성화됨) 또는 Disabled(비활성화됨)로 표시됩니다.
   - 이벤트 게시 수준

     표시할 수 있는 이벤트 게시 수준을 보려면 알람 및 이벤트 이해를 참조하십시오.
3. 알람 및 이벤트를 구성하려면 이벤트 및 알람 구성을 참조하십시오.

이벤트 보기

이벤트를 구성하여 Events(이벤트) 탭에서 볼 수 있습니다. 이벤트 및 알람 구성을 참조하십시오.

Events(이벤트) 탭에서 호스트, 데이터센터 또는 클러스터의 이벤트를 봅니다.

1. OpenManage Integration for VMware vCenter의 Navigator(탐색 창)에서 **Hosts(호스트)**, **Datacenter(데이터센터)** 또는 **Clusters(클러스터)**를 클릭합니다.
2. Objects(개체) 탭에서, 이벤트를 확인할 특정 호스트, 데이터센터 또는 클러스터를 선택합니다.
3. Monitor(모니터) 탭에서 **Events(이벤트)**를 클릭합니다.
4. 추가적인 이벤트 세부정보를 보려면 특정 이벤트를 선택하십시오.

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.

관련 정보:

- 펌웨어 업데이트 리포지토리 설정 페이지 49

펌웨어 업데이트 리포지토리 설정

OpenManage Integration for VMware vCenter의 Settings(설정) 탭에서 펌웨어 업데이트 리포지토리를 설정할 수 있습니다.

1. OpenManage Integration for VMware vCenter의 **관리** > **설정** 탭에 있는 **어플라이언스 설정**에서 펌웨어 업데이트 리포지토리 오른쪽의 **편집** 아이콘을 클릭합니다.
2. Firmware Update Repository(펌웨어 업데이트 리포지토리) 대화 상자에서 다음 중 하나를 선택합니다.
   - Dell 온라인

     스테이징 폴더가 포함된 기본 펌웨어 리포지토리(http://downloads.dell.com/published/Pages/index.html). OpenManage Integration for VMware vCenter는 선택된 펌웨어 업데이트를 다운로드하여 스테이징 폴더에 저장합니다. 사용자가 펌웨어 마법사를 실행하여 펌웨어를 업데이트해야 합니다.
   - 공유 네트워크 폴더

이는 Dell Repository Manager 응용프로그램을 통해 생성됩니다. Windows 기반 파일 공유에서 이러한 로컬 리포지토리를 찾습니다. 라이브 링크를 사용하여 Dell Repository Manager로 이동합니다.

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

   b. **Select Update Source(업데이트 소스 선택)** 화면에 표시되는 선택한 리포지토리 경로에서 파일 다운로드가 진행 중이면, 다운로드가 진행 중이라고 알리는 오류 메시지가 표시됩니다.
4. 파일 다운로드가 완료되면 **Apply(적용)**를 클릭합니다.

단일 호스트에 대해 펌웨어 업데이트 마법사 실행

이 기능은 iDRAC Express 또는 엔터프라이즈 카드가 있는 11, 12 및 13세대의 Dell 서버에만 사용할 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: 펌웨어 마법사에 액세스하려면 다음 중 하나를 수행합니다.

- **호스트** > **모든 OpenManage 통합 작업** > **펌웨어 업데이트**를 마우스 오른쪽 단추로 클릭합니다.
- **호스트** > **작업** > **모든 OpenManage 통합 작업** > **펌웨어 업데이트**를 클릭합니다.
- **호스트** > **요약** > **Dell 호스트 정보** > **펌웨어 업데이트**를 클릭합니다.

펌웨어 업데이트 마법사를 실행하려면 다음을 수행합니다.

1. **vSphere 웹 클라이언트**에서 **호스트**를 클릭합니다. 사용 가능한 호스트 목록이 표시됩니다.
2. 표시된 목록에서 호스트를 선택합니다.
3. 기본 메뉴에서 **모니터**를 클릭하고 **Dell 호스트 정보** 탭을 선택합니다. Dell 호스트의 인벤토리 정보가 표시됩니다.
4. **펌웨어**를 클릭합니다. 세부 정보와 함께 사용 가능한 펌웨어가 표시됩니다.
5. **펌웨어 마법사 실행**을 클릭합니다. **펌웨어 업데이트** 화면이 표시됩니다.
6. **다음**을 클릭합니다. **업데이트 소스 선택** 화면이 표시되면, 지정된 호스트에 대한 펌웨어 업데이트 번들이 표시됩니다. 화면의 **업데이트 번들 선택** 드롭다운 목록에서 펌웨어 업데이트 번들을 선택합니다.

   노트:
   - 64비트 번들은 iDRAC 1.51 이전 버전을 사용하는 12세대 호스트에는 지원되지 않습니다.
   - 64비트 번들은 모든 iDRAC 버전에서 11세대 호스트에는 지원되지 않습니다.

7. **다음**을 클릭합니다. 구성 요소의 펌웨어 세부 정보가 나열된 **구성 요소 선택** 화면이 표시됩니다.
8. 원하는 펌웨어 업데이트를 선택하고 **다음**을 클릭합니다. 다운그레이드 상태이거나 현재 업데이트 예약된 구성 요소는 선택할 수 없습니다. **펌웨어 다운그레이드 허용** 확인란을 선택할 경우 다운그레이드로 나열되는 옵션을 선택합니다. 이 옵션은 펌웨어 다운그레이드에 대해 잘 알고 있는 고급 사용자에게만 권장됩니다.
9. **Next(다음)**를 클릭합니다. **Schedule Firmware Update(펌웨어 업데이트 예약)** 화면이 표시됩니다.
   - **Firmware Update Job Name(펌웨어 업데이트 작업 이름)** 필드에 작업 이름을 입력하고 **Firmware Update Description(펌웨어 업데이트 설명)** 필드에 설명을 입력합니다. 이 필드는 선택사항입니다.
   - **지금 업데이트**를 선택하면 펌웨어 업데이트 작업이 즉시 시작됩니다.
   - 펌웨어 업데이트 작업을 나중에 실행하려면 **업데이트 예약**이라는 무선 단추를 선택하고 **다음**을 클릭합니다. 현재 시간에서 30분 후에 펌웨어 업데이트 작업을 예약할 수 있습니다.
   - Calendar(달력) 상자에서 월 및 일을 선택합니다.
   - Time(시간) 텍스트 상자에 HH:MM 형식으로 시간을 입력하고 Next(다음)를 클릭합니다. 시간은 클라이언트가 실제로 위치해 있는 로컬 시간대입니다. 시간 값이 올바르지 않으면 업데이트가 차단됩니다.
   - **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.

10. **Next(다음)**를 클릭합니다. 펌웨어 업데이트 이후의 모든 구성요소에 대한 세부정보를 보여주는 **Summary(요약)** 페이지가 표시됩니다.
11. **Finish(마침)**를 클릭합니다.
12. 업데이트 성공 여부를 확인하려면 **Monitor(모니터)** 탭에서 **Job Queue(작업 큐)** > **Firmware Updates(펌웨어 업데이트)**를 선택한 다음 **OpenManage Integration Overview(OpenManage Integration 개요)** 페이지에서 새 버전이 있는지 확인합니다.

클러스터에 대해 펌웨어 업데이트 마법사 실행

이 기능은 iDRAC Express 또는 Enterprise 카드가 있는 11세대, 12세대 및 13세대 Dell 서버에서만 사용할 수 있습니다. 2010년 10월 14일 당일 또는 그 이후에 설치된 펌웨어의 경우 펌웨어 업데이트 마법사를 사용하여 펌웨어 버전을 자동으로 업데이트할 수 있습니다. 이 마법사는 연결 프로필에 속하고 펌웨어, CSIOR 상태, 하이퍼바이저, OMSA 상태(11세대 서버에만 해당)와 관련하여 준수하는 호스트만 업데이트합니다. Clusters(클러스터) 보기에 나열된 클러스터를 선택하고 펌웨어 업데이트 마법사를 사용합니다. 각 클러스터의 펌웨어 구성요소를 업데이트하는 데 일반적으로 30분에서 60분 정도 소요됩니다. 펌웨어 업데이트가 진행되는 동안 호스트의 유지 보수 모드가 시작되거나 종료될 때 가상 시스템이 마이그레이션되도록 클러스터에서 DRS를 활성화합니다. 한 번에 하나의 펌웨어 업데이트 작업만 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: VMware에서는 동일한 서버 하드웨어를 사용하여 클러스터를 구축하는 것이 좋습니다. 여러 가지 모델의 Dell 서버로 구성되었거나 VMware에서 클러스터에 권장되는 최대 개수에 근접한 개수의 호스트를 사용하여 클러스터 수준에서 펌웨어 업데이트를 수행하는 경우에는 vSpher 웹 클라이언트를 사용할 것을 권장합니다.

노트: 기본 시간 제한 설정 변경에 대한 자세한 내용은 *사용 설명서*의 문제 해결 절을 참조하십시오.

작업 큐 페이지에서 상태를 보고 펌웨어 업데이트 작업을 관리할 수 있습니다. 데이터센터 및 클러스터에 대한 펌웨어 상세 정보 보기를 참조하십시오.

1. **OpenManage Integration** 아이콘을 클릭하고 왼쪽 창에 표시되는 **클러스터**를 클릭합니다. 그러면 클러스터 목록이 표시됩니다.
2. 표시되는 목록에서 클러스터를 클릭합니다. 여러 가지 옵션이 포함된 기본 메뉴가 표시됩니다.
3. **모니터** -->**Dell 클러스터 정보** -->**펌웨어**를 클릭합니다. **펌웨어 마법사 실행** 화면이 표시됩니다.
4. **펌웨어 마법사 실행** 링크를 클릭합니다. **시작** 페이지가 표시됩니다.
5. **Next(다음)**를 클릭합니다. **Select Update Source(업데이트 소스 선택)** 화면이 표시되고 여기에서 번들을 선택할 수 있습니다. 리포지토리 위치도 표시됩니다.
6. **Select Bundles(번들 선택)** 영역에 표시된 목록에서 호스트를 선택합니다. 펌웨어 업데이트에 사용되는 번들을 하나 이상 선택해야 합니다. 각 호스트의 이름 옆에 드롭다운 목록이 표시되고 여기에서 필요한 번들을 선택할 수 있습니다.

   노트:
   - 64비트 번들은 iDRAC 1.51 이전 버전을 사용하는 12세대 호스트에는 지원되지 않습니다.
   - 64비트 번들은 모든 iDRAC 버전에서 11세대 호스트에는 지원되지 않습니다.

7. **다음**을 클릭합니다. **구성 요소 선택** 화면이 표시됩니다. 이 화면에는 선택한 호스트의 모델 이름, 호스트 이름, 서비스 태그, 구성 요소 등과 같은 구성 요소의 상세 정보가 표시됩니다.
8. 목록에서 하나 이상의 구성 요소를 선택하고 **다음**을 클릭하여 계속 진행합니다. **필터** 필드를 사용하거나 구성 요소 데이터 그리드 내에서 열을 끌어 놓아 구성 요소 데이터 그리드의 내용을 필터링할 수 있습니다. **펌웨어 다운그레이드 허용** 확인란을 선택하면 기존 펌웨어 버전이 이전에 사용 가능한 버전으로 롤백됩니다.
9. **Next(다음)**를 클릭합니다. **Schedule Firmware Update(펌웨어 업데이트 예약)** 화면이 표시됩니다.
   a. **Firmware Update Job Name(펌웨어 업데이트 작업 이름)** 필드에 펌웨어 업데이트 작업 이름을 입력합니다. 이 값은 필수입니다.
   b. **Firmware Update Description(펌웨어 업데이트 설명)** 필드에 펌웨어 업데이트 설명을 입력합니다. 이 값은 필수입니다.
10. 다음 옵션 중 하나를 선택합니다.
    a. 펌웨어 업데이트 작업을 지금 실행하려면 **지금 업데이트** 라디오 단추를 선택하고 **다음**을 클릭합니다.
    b. 펌웨어 업데이트 작업을 나중에 실행하려면 **업데이트 예약**이라는 무선 단추를 선택하고 **다음**을 클릭합니다. 현재 시간에서 30분 후에 펌웨어 업데이트 작업을 예약할 수 있습니다.
    c. **Calendar(달력)** 상자에서 월 및 일을 선택합니다.
    d. **시간** 텍스트 상자에 HH:MM 형식으로 시간을 입력하고 **다음**을 클릭합니다. 시간은 클라이언트가 실제로 위치해 있는 로컬 시간대입니다. 시간 값이 올바르지 않으면 업데이트가 차단됩니다.
11. 모든 펌웨어 업데이트 세부정보를 보여주는 **Summary(요약)** 화면이 표시됩니다.

12. **마침**을 클릭하면 성공적인 펌웨어 업데이트를 위한 **펌웨어 업데이트 작업이 생성되었습니다**라는 메시지가 표시됩니다.

클러스터 및 데이터센터용 펌웨어 업데이트 상태 보기

이 페이지에 표시되는 정보를 보려면 클러스터 또는 호스트의 펌웨어 업데이트를 실행하거나 예약하십시오.

이 페이지에서 펌웨어 업데이트 작업을 새로 고치거나 제거하거나 중단할 수 있습니다.

1. OpenManage Integration에서**Monitor(모니터)** > **Job Queue(작업 큐)** > **Firmware Updates(펌웨어 업데이트)**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.
   - 상태
   - 예약된 시간
   - 이름
   - 설명
   - vCenter
   - 컬렉션 크기

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

     진행률 요약에는 이 펌웨어 업데이트의 진행률 상세정보가 나열됩니다.
4. 특정 작업에 대한 세부정보를 보려면 특정 작업의 데이터 그리드에서 마스터 데이터 그리드의 항목을 클릭합니다. 그러면 세부정보 데이터 그리드에 세부정보가 표시됩니다.

   여기에서 다음과 같은 상세정보를 찾을 수 있습니다.
   - 호스트 이름
   - 상태
   - 시작 시간
   - 종료 시간
5. 실행되고 있지 않은 예약된 펌웨어 업데이트를 중단하려는 경우 **Abort(중단)**를 클릭합니다.
6. 예약된 작업을 수정하려면 **Modify(수정)**를 클릭합니다.
7. 예약된 펌웨어 업데이트를 제거하려면 **작업 큐 제거**를 클릭하십시오.
   성공적으로 완료 또는 실패했거나 취소된 작업만 제거할 수 있습니다.
8. **Older than date and job Status(다음 기간 이후 및 작업 상태)**를 선택하고 **Apply(적용)**를 클릭하십시오. 그러면 선택한 작업이 큐에서 지워집니다.

인벤토리 및 보증의 데이터 검색 일정 보기

1. OpenManage Integration for VMware vCenter에서 **관리** > **설정** 탭의 **vCenter 설정** 아래에서 **데이터 검색 일정**을 클릭합니다.
   데이터 검색 일정을 클릭하면 인벤토리 및 보증의 일정이 표시됩니다.
2. 인벤토리 또는 보증 검색의 다음과 같은 설정을 확인합니다.
   - 옵션의 활성화 여부
   - 활성화된 요일 표시
   - 활성화된 시간 표시
3. **Data Retrieval Schedule(데이터 검색 일정)**을 다시 클릭하면 단일 행으로 정보가 표시되고 해당 옵션의 활성화 여부가 표시됩니다.
4. 데이터 검색 일정을 편집하려면 인벤토리 작업 일정 수정 또는 보증 작업 일정 수정을 참조하십시오.

11세대 서버에서 OMSA 사용 이해

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

Dell PowerEdge 11세대 서버에서 OMSA를 구성하려면 다음을 선택하십시오.

- ESXi 시스템에 OMSA 에이전트 배포
- OMSA 트랩 대상 설정

노트: 위 옵션 외에 .Net 클라이언트를 사용하고 Host Compliance를 실행시켜 OMSA 에이전트를 설치하고 구성할 수 있습니다.

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 <OMSA version X.X>
```

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

OMSA 트랩 대상 설정

이 작업은 iDRAC6 대신 OMSA를 사용하여 이벤트를 생성하는 호스트 시스템에만 해당됩니다. iDRAC6에서는 추가 구성이 필요하지 않습니다.

노트: OMSA는 Dell PowerEdge 12세대 서버 이전 버전의 Dell 서버에서만 필요합니다.

1. OpenManage Integration for VMware vCenter **Manage(관리)** > **Settings(설정)** 탭에서 OMSA 사용자 인터페이스로 이동되는 링크를 사용하거나, 웹 브라우저(**https://<HostIP>:1311/**)에서 OMSA 에이전트를 탐색합니다.
2. 인터페이스에 로그인하고 **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 상단에서 **Platform Events(플랫폼 이벤트)** 옵션을 선택합니다.
5. 회색 **대상 구성** 단추를 클릭하고 **대상** 링크를 클릭합니다.
6. **대상 활성화** 확인란을 선택합니다.
7. **대상 IP 주소** 필드에 OpenManage Integration for VMware vCenter 어플라이언스 IP 주소를 입력합니다.
8. **변경사항 적용**을 클릭합니다.
9. 1-8단계를 반복하여 추가 이벤트를 구성합니다.

8

보증 만료 알림 설정 보기

1. OpenManage Integration for VMware vCenter에서 **Manage(관리)** > **Settings(설정)**탭의 Appliance Settings(어플라이언스 설정) 아래에서 **Warranty Expiration Notification(보증 만료 알림)**을 클릭합니다.
2. Warranty Expiration Notification(보증 만료 알림)에서 다음 정보를 확인할 수 있습니다.
   - 설정의 활성화 여부
   - 최초 경고 설정 일 수
   - 위험 경고 설정 일 수
3. 보증 만료 알림을 구성하려면 보증 만료 알림 구성을 참조하십시오.

주제:

- 보증 만료 알림 구성

보증 만료 알림 구성

보증 만료를 경고하는 보증 만료 임계값을 구성할 수 있습니다.

1. OpenManage Integration for VMware vCenter의 **Manage(관리)** > **Settings(설정)** 탭에 있는 Appliance Settings(어플라이언스 설정)에서 **Warranty Expiration Notification(보증 만료 알림)** 오른쪽의 **Edit(편집)** 아이콘을 클릭합니다.
2. Warranty Expiration Notification(보증 만료 알림) 대화상자에서 다음을 수행합니다.
   a. 이 설정을 활성화하려면 **Enable warranty expiration notification for hosts(호스트의 보증 만료 알림 활성화)** 확인란을 선택합니다.
   확인란을 선택하면 보증 만료 알림이 활성화됩니다.
   b. Minimum Days Threshold(최소 일 수 임계값) 경고에서 다음을 수행합니다.
      i. Warning(경고) 드롭다운 목록에서, 보증 만료 경고를 수신하기 전의 일 수를 선택합니다.
      ii. Critical(위험) 드롭다운 목록에서, 보증 만료 경고를 수신하기 전의 일 수를 선택합니다.
3. **Apply(적용)**를 클릭합니다.

9

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.

관련 정보:

- 펌웨어 업데이트 리포지토리 설정 페이지 49

주제:

펌웨어 업데이트 리포지토리 설정

OpenManage Integration for VMware vCenter의 Settings(설정) 탭에서 펌웨어 업데이트 리포지토리를 설정할 수 있습니다.

1. OpenManage Integration for VMware vCenter의 **관리** > **설정** 탭에 있는 **어플라이언스 설정**에서 펌웨어 업데이트 리포지토리 오른쪽의 **편집** 아이콘을 클릭합니다.
2. Firmware Update Repository(펌웨어 업데이트 리포지토리) 대화 상자에서 다음 중 하나를 선택합니다.
   - Dell 온라인

     스테이징 폴더가 포함된 기본 펌웨어 리포지토리(http://downloads.dell.com/published/Pages/index.html). OpenManage Integration for VMware vCenter는 선택된 펌웨어 업데이트를 다운로드하여 스테이징 폴더에 저장합니다. 사용자가 펌웨어 마법사를 실행하여 펌웨어를 업데이트해야 합니다.
   - 공유 네트워크 폴더

     이는 Dell Repository Manager 응용프로그램을 통해 생성됩니다. Windows 기반 파일 공유에서 이러한 로컬 리포지토리를 찾습니다. 라이브 링크를 사용하여 Dell Repository Manager로 이동합니다.
3. **공유 네트워크 폴더**를 선택한 경우 다음을 수행하십시오.
   a. 다음과 같은 형식을 사용하여 **카탈로그 파일 위치**를 입력합니다.
      - xml 파일용 NFS 공유: host:/share/filename.xml
      - gz 파일용 NFS 공유: host:/share/filename.gz
      - xml 파일용 CIFS 공유: \\host\share\filename.xml
      - gz 파일용 CIFS 공유: \\host\share\filename.gz

   b. **Select Update Source(업데이트 소스 선택)** 화면에 표시되는 선택한 리포지토리 경로에서 파일 다운로드가 진행 중이면, 다운로드가 진행 중이라고 알리는 오류 메시지가 표시됩니다.
4. 파일 다운로드가 완료되면 **Apply(적용)**를 클릭합니다.

단일 호스트에 대해 펌웨어 업데이트 마법사 실행

이 기능은 iDRAC Express 또는 엔터프라이즈 카드가 있는 11, 12 및 13세대의 Dell 서버에만 사용할 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: 펌웨어 마법사에 액세스하려면 다음 중 하나를 수행합니다.

- **호스트** > **모든 OpenManage 통합 작업** > **펌웨어 업데이트**를 마우스 오른쪽 단추로 클릭합니다.
- **호스트** > **작업** > **모든 OpenManage 통합 작업** > **펌웨어 업데이트**를 클릭합니다.
- **호스트** > **요약** > **Dell 호스트 정보** > **펌웨어 업데이트**를 클릭합니다.

펌웨어 업데이트 마법사를 실행하려면 다음을 수행합니다.

1. **vSphere 웹 클라이언트**에서 **호스트**를 클릭합니다. 사용 가능한 호스트 목록이 표시됩니다.
2. 표시된 목록에서 호스트를 선택합니다.
3. 기본 메뉴에서 **모니터**를 클릭하고 **Dell 호스트 정보** 탭을 선택합니다. Dell 호스트의 인벤토리 정보가 표시됩니다.
4. **펌웨어**를 클릭합니다. 세부 정보와 함께 사용 가능한 펌웨어가 표시됩니다.
5. **펌웨어 마법사 실행**을 클릭합니다. **펌웨어 업데이트** 화면이 표시됩니다.
6. **다음**을 클릭합니다. **업데이트 소스 선택** 화면이 표시되면, 지정된 호스트에 대한 펌웨어 업데이트 번들이 표시됩니다. 화면의 **업데이트 번들 선택** 드롭다운 목록에서 펌웨어 업데이트 번들을 선택합니다.

   노트:
   - 64비트 번들은 iDRAC 1.51 이전 버전을 사용하는 12세대 호스트에는 지원되지 않습니다.
   - 64비트 번들은 모든 iDRAC 버전에서 11세대 호스트에는 지원되지 않습니다.

7. **다음**을 클릭합니다. 구성 요소의 펌웨어 세부 정보가 나열된 **구성 요소 선택** 화면이 표시됩니다.
8. 원하는 펌웨어 업데이트를 선택하고 **다음**을 클릭합니다. 다운그레이드 상태이거나 현재 업데이트 예약된 구성 요소는 선택할 수 없습니다. **펌웨어 다운그레이드 허용** 확인란을 선택할 경우 다운그레이드로 나열되는 옵션을 선택합니다. 이 옵션은 펌웨어 다운그레이드에 대해 잘 알고 있는 고급 사용자에게만 권장됩니다.
9. **Next(다음)**를 클릭합니다. **Schedule Firmware Update(펌웨어 업데이트 예약)** 화면이 표시됩니다.
   - **Firmware Update Job Name(펌웨어 업데이트 작업 이름)** 필드에 작업 이름을 입력하고 **Firmware Update Description(펌웨어 업데이트 설명)** 필드에 설명을 입력합니다. 이 필드는 선택사항입니다.
   - **지금 업데이트**를 선택하면 펌웨어 업데이트 작업이 즉시 시작됩니다.
   - 펌웨어 업데이트 작업을 나중에 실행하려면 **업데이트 예약**이라는 무선 단추를 선택하고 **다음**을 클릭합니다. 현재 시간에서 30분 후에 펌웨어 업데이트 작업을 예약할 수 있습니다.
   - Calendar(달력) 상자에서 월 및 일을 선택합니다.
   - Time(시간) 텍스트 상자에 HH:MM 형식으로 시간을 입력하고 Next(다음)를 클릭합니다. 시간은 클라이언트가 실제로 위치해 있는 로컬 시간대입니다. 시간 값이 올바르지 않으면 업데이트가 차단됩니다.
   - **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.
10. **Next(다음)**를 클릭합니다. 펌웨어 업데이트 이후의 모든 구성요소에 대한 세부정보를 보여주는 **Summary(요약)** 페이지가 표시됩니다.
11. **Finish(마침)**를 클릭합니다.
12. 업데이트 성공 여부를 확인하려면 **Monitor(모니터)** 탭에서 **Job Queue(작업 큐)** > **Firmware Updates(펌웨어 업데이트)**를 선택한 다음 **OpenManage Integration Overview(OpenManage Integration 개요)** 페이지에서 새 버전이 있는지 확인합니다.

클러스터에 대해 펌웨어 업데이트 마법사 실행

이 기능은 iDRAC Express 또는 Enterprise 카드가 있는 11세대, 12세대 및 13세대 Dell 서버에서만 사용할 수 있습니다. 2010년 10월 14일 당일 또는 그 이후에 설치된 펌웨어의 경우 펌웨어 업데이트 마법사를 사용하여 펌웨어 버전을 자동으로 업데이트할 수 있습니다. 이 마법사는 연결 프로필에 속하고 펌웨어, CSIOR 상태, 하이퍼바이저, OMSA 상태(11세대 서버에만 해당)와 관련하여 준수하는 호스트

만 업데이트합니다. Clusters(클러스터) 보기에 나열된 클러스터를 선택하고 펌웨어 업데이트 마법사를 사용합니다. 각 클러스터의 펌웨어 구성요소를 업데이트하는 데 일반적으로 30분에서 60분 정도 소요됩니다. 펌웨어 업데이트가 진행되는 동안 호스트의 유지 보수 모드가 시작되거나 종료될 때 가상 시스템이 마이그레이션되도록 클러스터에서 DRS를 활성화합니다. 한 번에 하나의 펌웨어 업데이트 작업만 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: VMware에서는 동일한 서버 하드웨어를 사용하여 클러스터를 구축하는 것이 좋습니다. 여러 가지 모델의 Dell 서버로 구성되었거나 VMware에서 클러스터에 권장되는 최대 개수에 근접한 개수의 호스트를 사용하여 클러스터 수준에서 펌웨어 업데이트를 수행하는 경우에는 vSpher 웹 클라이언트를 사용할 것을 권장합니다.

노트: 기본 시간 제한 설정 변경에 대한 자세한 내용은 *사용 설명서*의 문제 해결 절을 참조하십시오.

작업 큐 페이지에서 상태를 보고 펌웨어 업데이트 작업을 관리할 수 있습니다. 데이터센터 및 클러스터에 대한 펌웨어 상세 정보 보기를 참조하십시오.

1. **OpenManage Integration** 아이콘을 클릭하고 왼쪽 창에 표시되는 **클러스터**를 클릭합니다. 그러면 클러스터 목록이 표시됩니다.
2. 표시되는 목록에서 클러스터를 클릭합니다. 여러 가지 옵션이 포함된 기본 메뉴가 표시됩니다.
3. **모니터** -->**Dell 클러스터 정보** -->**펌웨어**를 클릭합니다. **펌웨어 마법사 실행** 화면이 표시됩니다.
4. **펌웨어 마법사 실행** 링크를 클릭합니다. **시작** 페이지가 표시됩니다.
5. **Next(다음)**를 클릭합니다. **Select Update Source(업데이트 소스 선택)** 화면이 표시되고 여기에서 번들을 선택할 수 있습니다. 리포지토리 위치도 표시됩니다.
6. **Select Bundles(번들 선택)** 영역에 표시된 목록에서 호스트를 선택합니다. 펌웨어 업데이트에 사용되는 번들을 하나 이상 선택해야 합니다. 각 호스트의 이름 옆에 드롭다운 목록이 표시되고 여기에서 필요한 번들을 선택할 수 있습니다.

   노트:
   - 64비트 번들은 iDRAC 1.51 이전 버전을 사용하는 12세대 호스트에는 지원되지 않습니다.
   - 64비트 번들은 모든 iDRAC 버전에서 11세대 호스트에는 지원되지 않습니다.

7. **다음**을 클릭합니다. **구성 요소 선택** 화면이 표시됩니다. 이 화면에는 선택한 호스트의 모델 이름, 호스트 이름, 서비스 태그, 구성 요소 등과 같은 구성 요소의 상세 정보가 표시됩니다.
8. 목록에서 하나 이상의 구성 요소를 선택하고 **다음**을 클릭하여 계속 진행합니다. **필터** 필드를 사용하거나 구성 요소 데이터 그리드 내에서 열을 끌어 놓아 구성 요소 데이터 그리드의 내용을 필터링할 수 있습니다. **펌웨어 다운그레이드 허용** 확인란을 선택하면 기존 펌웨어 버전이 이전에 사용 가능한 버전으로 롤백됩니다.
9. **Next(다음)**를 클릭합니다. **Schedule Firmware Update(펌웨어 업데이트 예약)** 화면이 표시됩니다.
   a. **Firmware Update Job Name(펌웨어 업데이트 작업 이름)** 필드에 펌웨어 업데이트 작업 이름을 입력합니다. 이 값은 필수입니다.
   b. **Firmware Update Description(펌웨어 업데이트 설명)** 필드에 펌웨어 업데이트 설명을 입력합니다. 이 값은 필수입니다.
10. 다음 옵션 중 하나를 선택합니다.
    a. 펌웨어 업데이트 작업을 지금 실행하려면 **지금 업데이트** 라디오 단추를 선택하고 **다음**을 클릭합니다.
    b. 펌웨어 업데이트 작업을 나중에 실행하려면 **업데이트 예약**이라는 무선 단추를 선택하고 **다음**을 클릭합니다. 현재 시간에서 30분 후에 펌웨어 업데이트 작업을 예약할 수 있습니다.
    c. **Calendar(달력)** 상자에서 월 및 일을 선택합니다.
    d. **시간** 텍스트 상자에 HH:MM 형식으로 시간을 입력하고 **다음**을 클릭합니다. 시간은 클라이언트가 실제로 위치해 있는 로컬 시간대입니다. 시간 값이 올바르지 않으면 업데이트가 차단됩니다.
11. 모든 펌웨어 업데이트 세부정보를 보여주는 **Summary(요약)** 화면이 표시됩니다.
12. **마침**을 클릭하면 성공적인 펌웨어 업데이트를 위한 **펌웨어 업데이트 작업이 생성되었습니다**라는 메시지가 표시됩니다.

10

호스트에 관한 이벤트 및 알람에 대한 이해

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

이벤트 게시 수준에는 4가지가 있습니다.

표 5. 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: 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.

주제:

- 섀시에 관한 이벤트 및 알람에 대한 이해
- 이벤트 및 알람 구성
- 인벤토리 및 보증의 데이터 검색 일정 보기

섀시에 관한 이벤트 및 알람에 대한 이해

섀시에 해당되는 이벤트 및 알람은 vCenter 수준에서만 표시됩니다. 모든 vCenter에서 호스트에 대해 수행되는 이벤트 및 알람 설정은 섀시 수준에도 적용됩니다. OpenManage Integration for VMware vCenter의**Manage(관리)** > **Settings(설정)**탭에서 이벤트 및 알람 설정을 편집할 수 있습니다. 여기에서 이벤트 게시 수준을 선택하거나, Dell 호스트 및 섀시에 대한 알람을 활성화하거나, 기본 알람을 복원할 수 있습니다. 이벤트 및 알람을 각 vCenter에 대해 개별 구성하거나 등록된 모든 vCenter에 대해 한 번에 구성할 수 있습니다.

노트: Dell 이벤트를 수신하려면 알람과 이벤트를 모두 활성화해야 합니다.

Viewing Chassis Events

1. 왼쪽 창에서 vCenter를 선택하고, vCenter Servers를 클릭합니다.
2. 특정 vCenter를 클릭합니다.
3. Monitor(모니터) 탭에서 Events(이벤트)를 클릭합니다.
4. 추가적인 이벤트 세부정보를 보려면 특정 이벤트를 선택하십시오.

섀시 알람 보기

1. 왼쪽 창에서 vCenter를 선택하고, vCenter Servers를 클릭합니다.
2. 특정 vCenter를 클릭합니다.
3. 해당 알람이 표시됩니다. 처음 4개의 알람만 표시됩니다. Show All(모두 표시)을 클릭하면 Monitor(모니터) 탭에 All Issues(모든 항목) 세부 목록이 표시됩니다.
4. **Triggered Alarms(작동된 알람)**의 해당 Alarm(알람)을 클릭하면 Alarm Definition(알람 정의)을 볼 수 있습니다.

이벤트 및 알람 구성

Dell Management Center Events and Alarms(이벤트 및 알람) 페이지에서 모든 하드웨어 알람을 활성화하고 비활성화합니다. vCenter Alarms(vCenter 알람) 탭에 현재 알람 상태가 표시됩니다. 위험 이벤트는 실제 또는 임박한 데이터 손실이나 시스템 오작동을 나타냅니다. 경고 이벤트는 심각한 상태는 아니지만 향후 문제 발생의 가능성을 나타냅니다. VMware Alarm Manager를 사용해 이벤트 및 알람을 활성화할 수도 있습니다. 이벤트는 Hosts and Clusters(호스트 및 클러스터) 보기의 vCenter Tasks and Events(vCenter 작업 및 이벤트) 탭에 표시됩니다. 서버에서 이벤트를 수신하기 위해 OMIVV가 SNMP 트랩 대상을 구성됩니다. 12세대 이상의 호스트에서는 SNMP 트랩 대상이 iDRAC에서 설정됩니다. 12세대 이전 호스트의 경우 트랩 대상이 OMSA에서 설정됩니다. **Management(관리)** **Settings(설정)** 탭에서 OpenManage Integration for VMware vCenter를 사용하여 이벤트와 알람을 구성할 수 있습니다. vCenter Settings(vCenter 설정) 아래에서 Events and Alarms(이벤트 및 알람) 제목을 확장해 모든 Dell 호스트에 대한 현재 vCenter 알람 또는 이벤트 게시 수준(활성화된 또는 비활성화됨)을 표시하십시오.

노트: OMIVV는 12세대 이상의 호스트에 대해 SNMP v1 및 v2 경고를 지원합니다. 12세대 이전 호스트의 경우 OMIVV가 vCenter에서 SNMP v1 경고를 지원합니다. 트랩 대상 설정에 대한 자세한 내용은 OMSA 트랩 대상 설정을 참조하십시오.

노트: Dell 이벤트를 수신하려면 알람과 이벤트를 모두 활성화해야 합니다.

1. Events and Alarms(이벤트 및 알람) 오른쪽의 **Edit(편집)** 아이콘을 클릭합니다.
2. 모든 하드웨어 알람 및 이벤트를 활성화하려면 **Enable Alarms for all Dell Hosts(모든 Dell 호스트에 알람 활성화)** 확인란을 선택합니다.

   노트: 알람이 활성화된 Dell 호스트가 유지 보수 모드로 전환되어 위험 수준의 이벤트를 알리며 필요에 따라 알람을 수정할 수 있습니다.

3. 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.

   노트: 이 단계는 Dell 호스트에 알람 활성화를 선택한 경우에만 표시됩니다.

4. **Event Posting Level(이벤트 게시 수준)**에서 다음 중 하나를 선택합니다.
   - Do not post any events(이벤트 게시하지 않음)

     하드웨어 이벤트를 차단합니다.
   - Post All Events(모든 이벤트 게시)

     모든 하드웨어 이벤트를 게시합니다.

- Post only Critical and Warning Events(위험 및 경고 이벤트만 게시)

  위험 및 경고 수준의 하드웨어 이벤트만 게시합니다.
- Post only Virtualization-Related Critical and Warning Events(가상화 관련 위험 및 경고 이벤트만 게시)

  가상화 관련 위험 및 경고 이벤트만 게시합니다. 이벤트 게시 수준의 기본값입니다.

5. 설정을 모든 vCenter에 적용하려면 **Apply these settings to all vCenters(이 설정을 모든 vCenter에 적용)** 확인란을 선택합니다.

   노트: 이 옵션을 선택하면 모든 vCenter의 기존 설정이 재설정됩니다.

   Setting(설정) 페이지에서 All Registered vCenters(등록된 모든 vCenter)가 이미 선택되어 있으면 이 옵션이 회색으로 표시됩니다.
6. 저장하려면 **Apply(적용)**를 클릭합니다.

이벤트 보기

이벤트를 구성하여 Events(이벤트) 탭에서 볼 수 있습니다. 이벤트 및 알람 구성을 참조하십시오.

Events(이벤트) 탭에서 호스트, 데이터센터 또는 클러스터의 이벤트를 봅니다.

1. OpenManage Integration for VMware vCenter의 Navigator(탐색 창)에서 **Hosts(호스트)**, **Datacenter(데이터센터)** 또는 **Clusters(클러스터)**를 클릭합니다.
2. Objects(개체) 탭에서, 이벤트를 확인할 특정 호스트, 데이터센터 또는 클러스터를 선택합니다.
3. Monitor(모니터) 탭에서 **Events(이벤트)**를 클릭합니다.
4. 추가적인 이벤트 세부정보를 보려면 특정 이벤트를 선택하십시오.

알람 및 이벤트 설정 보기

알람 및 이벤트가 구성되면 Settings(설정) 탭에서 호스트에 vCenter 알람이 활성화되어 있는지 여부와 선택된 이벤트 게시 수준을 볼 수 있습니다.

1. **OpenManage Integration for VMware vCenter** > **Manage(관리)** > **Settings(설정)** 탭의 vCenter Settings(vCenter 설정) 아래에서 Events and Alarms(이벤트 및 알람)를 확장합니다.
2. Events and Alarms(이벤트 및 알람)에서 다음과 같은 사항을 확인할 수 있습니다.
   - Dell 호스트의 vCenter 알람: Enabled(활성화됨) 또는 Disabled(비활성화됨)로 표시됩니다.
   - 이벤트 게시 수준

     표시할 수 있는 이벤트 게시 수준을 보려면 알람 및 이벤트 이해를 참조하십시오.
3. 알람 및 이벤트를 구성하려면 이벤트 및 알람 구성을 참조하십시오.

인벤토리 및 보증의 데이터 검색 일정 보기

1. OpenManage Integration for VMware vCenter에서 **관리** > **설정** 탭의 **vCenter 설정** 아래에서 **데이터 검색 일정**을 클릭합니다. 데이터 검색 일정을 클릭하면 인벤토리 및 보증의 일정이 표시됩니다.
2. 인벤토리 또는 보증 검색의 다음과 같은 설정을 확인합니다.
   - 옵션의 활성화 여부
   - 활성화된 요일 표시
   - 활성화된 시간 표시
3. **Data Retrieval Schedule(데이터 검색 일정)**을 다시 클릭하면 단일 행으로 정보가 표시되고 해당 옵션의 활성화 여부가 표시됩니다.
4. 데이터 검색 일정을 편집하려면 인벤토리 작업 일정 수정 또는 보증 작업 일정 수정을 참조하십시오.

11

섀시에 대한 연결된 호스트 보기

Manage(관리) 페이지에서 선택한 섀시의 연결된 호스트에 대한 정보를 볼 수 있습니다.

연결된 호스트에 대한 정보를 보려면 다음을 수행하십시오.

1. **홈** 페이지에서 **vCenter**를 클릭합니다.
2. 왼쪽 창에 있는 **OpenManage Integration** 아래에서 **Dell Chassis(Dell 섀시)**를 클릭합니다.
3. 왼쪽 창에서 해당 섀시 IP를 선택합니다.
4. **Manage(관리)** 탭을 클릭합니다.
   연결된 호스트에 대해 다음과 같은 정보가 표시됩니다.
   - 호스트 이름(선택한 호스트 IP를 클릭하면 호스트에 대한 상세 정보가 표시됨)
   - 서비스 태그
   - Model(모델)
   - iDRAC IP
   - Slot Location(슬롯 위치)
   - Last Inventory(마지막 인벤토리)

12

섀시 관리

OpenManage Integration for VMware vCenter를 사용하면 선택한 섀시에 대한 추가 정보를 볼 수 있습니다. Chassis Information(섀시 정보) 탭에서 개별 섀시에 대한 섀시 개요 세부 정보와 하드웨어 인벤토리, 펌웨어 및 관리 컨트롤러에 관한 정보를 볼 수 있습니다. 각 섀시마다 다음 세 가지 탭이 표시되며 일부 섀시의 경우 모델에 따라 표시되는 탭이 다릅니다.

Summary(요약) 탭

Monitor(모니터) 탭

Manage(관리) 탭

주제:

섀시 요약 세부정보 보기

섀시 요약 페이지에서 개별 섀시에 대한 섀시 요약 상세 정보를 볼 수 있습니다.

섀시 요약 세부정보를 보려면 다음을 수행하십시오.

1. **홈** 페이지에서 **vCenter**를 클릭합니다.
2. 왼쪽 창에 있는 **OpenManage Integration** 아래에서 **Dell Chassis(Dell 섀시)**를 클릭합니다.
3. 왼쪽 창에서 해당 섀시 IP를 선택합니다.
4. **Summary(요약)** 탭을 클릭합니다.

   선택한 섀시에 대해 다음과 같은 정보가 표시됩니다.

   - 이름
   - Model(모델)
   - Firmware Version(펌웨어 버전)
   - 서비스 태그
   - CMC(**CMC** 링크를 클릭하면 Chassis Management Controller(섀시 관리 컨트롤러) 페이지가 표시됨)

     노트: 섀시를 인벤토리화하지 않는 경우 서비스 태그와 CMC IP 주소만 표시됩니다.

5. 선택한 섀시에 연결된 장치들의 상태를 볼 수 있습니다. 기본 창에는 섀시의 전체적인 상태가 표시됩니다. 표시되는 상태 인디케이터에는 **Healthy(양호)**, **Warning(경고)**, **Critical(치명적 결함)**, **Not Present(표시되지 않음)**가 있습니다. **Chassis Health(섀시 상태)** 그리드 보기에는 각 구성 요소의 상태가 표시됩니다. 이들 섀시 상태 매개변수는 **VRTX 버전 1.0 이상**과 **M1000e 버전 4.4 이상**에 적용됩니다. 4.3 이전 버전의 경우, **Healthy(양호)**와 **Warning(경고) 또는 Critical(치명적 결함)**(주황색 역삼각형과 느낌표)의 두 가지 상태 인디케이터만이 표시됩니다.

   노트: 전체적인 상태에는 상태 매개변수가 가장 낮은 섀시를 기초로 하여 상태가 표시됩니다. 예를 들어, 양호 표시가 5개 있고 경고 표시가 1개 있다면, 전체적인 상태는 경고로 표시됩니다.

6. CMC **Enterprise** 또는 **Express** 등의 라이센스 유형과 섀시의 만료 날짜를 확인할 수 있습니다. 이것은 M1000e 섀시에는 해당되지 않습니다.
7. **Warranty(보증)** 아이콘에는 서버의 남은 일 수와 사용한 일 수가 표시됩니다. 하나 이상의 보증을 보유하고 있는 경우, 보증 잔여 일 수를 계산할 때 마지막 보증의 최종일이 감안됩니다.
8. **Active Errors(활성 오류)** 표에는 **Chassis Health(섀시 상태)** 페이지에 표시된 섀시에 대한 오류들이 표시됩니다. M1000e 4.3 버전 이하의 경우, 활성 오류가 표시되지 않습니다.

하드웨어 인벤토리 보기: 팬

선택한 섀시 내의 팬에 대한 정보를 볼 수 있습니다. 이 페이지에서 정보를 보려면 인벤토리 작업을 실행해야 합니다. 팬 정보의 CSV 파일을 내보낼 수 있습니다.

팬에 대한 정보를 보려면 다음을 수행하십시오.

1. **홈** 페이지에서 **vCenter**를 클릭합니다.
2. 왼쪽 창에 있는 **OpenManage Integration** 아래에서 **Dell 섀시**를 클릭합니다.
3. 왼쪽 창에서 해당 섀시 IP를 선택합니다.
4. **Monitor(모니터)** 탭을 클릭합니다.
5. 팬에 대한 정보를 보려면 다음 중 하나를 수행하십시오.
   a. **Overview(개요)** 탭에서 **Fans(팬)**을 클릭합니다.
   b. **Monitor(모니터)** 탭에서 왼쪽 창을 확장하고 **Hardware Inventory(하드웨어 인벤토리)**를 클릭한 후 **Fans(팬)**를 클릭합니다.

   다음 정보가 표시됩니다.
   - 이름
   - Present(표시)
   - Power State(전원 상태)
   - Reading(판독값)
   - Warning Threshold(경고 임계값)
   - Critical Threshold(중요 임계값)
     - 최소
     - 최대

하드웨어 인벤토리 보기: I/O 모듈

선택한 섀시의 I/O 모듈에 대한 정보를 볼 수 있습니다. 이 페이지에서 정보를 보려면 인벤토리 작업을 실행해야 합니다. I/O 모듈 정보의 CSV 파일을 내보낼 수 있습니다.

I/O 모듈에 대한 정보를 보려면 다음을 수행하십시오.

1. **홈** 페이지에서 **vCenter**를 클릭합니다.
2. 왼쪽 창에 있는 **OpenManage Integration** 아래에서 **Dell Chassis(Dell 섀시)**를 클릭합니다.
3. 왼쪽 창에서 해당 섀시 IP를 선택합니다.
4. **Monitor(모니터)** 탭을 클릭합니다.
5. **I/O Modules(I/O 모듈)**에 대한 정보를 보려면 다음 중 하나를 수행하십시오.
   a. **Overview(개요)** 탭에서 **I/O Modules(I/O 모듈)**를 클릭합니다.
   b. **Monitor(모니터)** 탭에서 왼쪽 창을 확장하고 **Hardware Inventory(하드웨어 인벤토리)**를 클릭한 후 **I/O Modules(I/O 모듈)**를 클릭합니다.

   다음 정보가 표시됩니다.
   - Slot/Location(슬롯/위치)
   - Present(표시)

- 이름
- 패브릭
- 서비스 태그
- Power Status(전원 상태)

추가 정보를 보려면 해당 I/O 모듈을 선택합니다. 다음 정보가 표시됩니다.

- Role(역할)
- Firmware Version(펌웨어 버전)
- Hardware Version(하드웨어 버전)
- IP Address(IP 주소)
- Subnet Mask(서브넷 마스크)
- Gateway(게이트웨이)
- Mac Address(MAC 주소)
- DHCP Enabled(DHCP 활성화)

하드웨어 인벤토리 보기: iKVM

선택한 섀시의 iKVM에 대한 정보를 볼 수 있습니다. 이 페이지에서 정보를 보려면 인벤토리 작업을 실행해야 합니다. iKVM 정보의 CSV 파일을 내보낼 수 있습니다.

노트: PowerEdge M1000e 섀시에 대해서만 iKVM에 대한 정보를 볼 수 있습니다.

iKVM에 대한 정보를 보려면 다음을 수행하십시오.

1. **홈** 페이지에서 **vCenter**를 클릭합니다.
2. 왼쪽 창에 있는 **OpenManage Integration** 아래에서 **Dell Chassis(Dell 섀시)**를 클릭합니다.
3. 왼쪽 창에서 해당 섀시 IP를 선택합니다.
4. **Monitor(모니터)** 탭을 클릭합니다.
5. **iKVM**에 대한 정보를 보려면 다음 중 하나를 수행하십시오.
   a. **Overview(개요)** 탭에서 **iKVM**을 클릭합니다.
   b. **Monitor(모니터)** 탭에서 왼쪽 창을 확장하고 **Hardware Inventory(하드웨어 인벤토리)**를 클릭한 후 **iKVM**을 클릭합니다.

   다음 정보가 표시됩니다.
   - iKVM Name(iKVM 이름)
   - Present(표시)
   - Firmware Version(펌웨어 버전)
   - Front Panel USB/Video Enabled(전면 패널 USB/비디오 활성화)
   - Allow access to CMC CLI(CMC CLI에 대한 액세스 허용)

   노트: iKVM 탭은 섀시에 iKVM 모듈이 포함되어 있는 경우에만 표시됩니다.

하드웨어 인벤토리 보기: PCIe

선택한 섀시의 PCIe에 대한 정보를 볼 수 있습니다. 이 페이지에서 정보를 보려면 인벤토리 작업을 실행해야 합니다. PCIe 정보의 CSV 파일을 내보낼 수 있습니다.

PCIe에 대한 정보를 보려면 다음을 수행하십시오.

1. **홈** 페이지에서 **vCenter**를 클릭합니다.
2. 왼쪽 창에 있는 **OpenManage Integration** 아래에서 **Dell Chassis(Dell 섀시)**를 클릭합니다.

3. 왼쪽 창에서 해당 섀시 IP를 선택합니다.
4. **Monitor(모니터)** 탭을 클릭합니다.
5. PCIe에 대한 정보를 보려면 다음 중 하나를 수행하십시오.

   노트: PCIe 정보는 M1000e 섀시에는 해당되지 않습니다.

   a. **Overview(개요)** 탭에서 **PCIe**를 클릭합니다.

   b. **모니터** 탭에서 왼쪽 창을 확장하고 **하드웨어 인벤토리**를 클릭한 후 **PCIe**를 클릭합니다.

   다음 정보가 표시됩니다.
   - PCIe 슬롯
     - Slot(슬롯)
     - 이름
     - Power Status(전원 상태)
     - 패브릭
   - Server Slot(서버 슬롯)
     - 이름
     - 번호

   추가 정보를 보려면 해당 PCIe를 선택합니다. 다음 정보가 표시됩니다.
   - Slot Type(슬롯 유형)
   - Server Mapping(서버 매핑)
   - Assignment Status(할당 상태)
   - Allocated Slot Power(할당된 슬롯 전원)
   - PCI ID
   - 벤더 ID

하드웨어 인벤토리 보기: 전원 공급 장치

선택한 섀시의 전원 공급 장치에 대한 정보를 볼 수 있습니다. 이 페이지에서 정보를 보려면 인벤토리 작업을 실행해야 합니다. 전원 공급 장치 정보의 CSV 파일을 내보낼 수 있습니다.

전원 공급 장치에 대한 정보를 보려면 다음을 수행하십시오.

1. **홈** 페이지에서 **vCenter**를 클릭합니다.
2. 왼쪽 창에 있는 **OpenManage Integration** 아래에서 **Dell Chassis(Dell 섀시)**를 클릭합니다.
3. 왼쪽 창에서 해당 섀시 IP를 선택합니다.
4. **Monitor(모니터)** 탭을 클릭합니다.
5. 전원 공급 장치에 대한 정보를 보려면 다음 중 하나를 수행하십시오.

   a. **Overview(개요)** 탭에서 **Power Supplies(전원 공급 장치)**를 클릭합니다.

   b. **모니터** 탭에서 왼쪽 창을 확장하고 **하드웨어 인벤토리**를 클릭한 후 **전원 공급 장치**를 클릭합니다.

   다음 정보가 표시됩니다.
   - 이름
   - Capacity(용량)
   - Present(표시)
   - Power State(전원 상태)

하드웨어 인벤토리 보기: 온도 센서

선택한 섀시의 온도 센서에 대한 정보를 볼 수 있습니다. 이 페이지에서 정보를 보려면 인벤토리 작업을 실행해야 합니다. 온도 센서 정보의 CSV 파일을 내보낼 수 있습니다.

온도 센서에 대한 정보를 보려면 다음을 수행하십시오.

1. **홈** 페이지에서 **vCenter**를 클릭합니다.
2. 왼쪽 창에 있는 **OpenManage Integration** 아래에서 **Dell Chassis(Dell 섀시)**를 클릭합니다.
3. 왼쪽 창에서 해당 섀시 IP를 선택합니다.
4. **Monitor(모니터)** 탭을 클릭합니다.
5. 온도 센서에 대한 정보를 보려면 다음 중 하나를 수행하십시오.
   a. **Overview(개요)** 탭에서 **Temperature Sensors(온도 센서)**를 클릭합니다.
   b. **모니터** 탭에서 왼쪽 창을 확장하고 **하드웨어 인벤토리**를 클릭한 후 **온도 센서**를 클릭합니다.

   다음 정보가 표시됩니다.
   - 위치
   - Reading(판독값)
   - Warning Threshold(경고 임계값)
     - 최소
     - 최대
   - Critical Threshold(중요 임계값)
     - 최소
     - 최대

   노트: PowerEdge M1000e 섀시의 경우, 섀시의 온도 센서에 대한 정보만 표시됩니다. 다른 섀시의 경우, 섀시 및 연결된 모듈식 서버의 온도 센서에 대한 정보가 표시됩니다.

보증 세부 정보 보기

보증 창에는 보증 세부 정보가 저장됩니다.

보증에 대한 정보를 보려면,

1. **홈** 페이지에서 **vCenter**를 클릭합니다.
2. 왼쪽 창에 있는 **OpenManage Integration** 아래에서 **Dell Chassis(Dell 섀시)**를 클릭합니다.
3. 왼쪽 창에서 해당 섀시 IP를 선택합니다.
4. **Monitor(모니터)** 탭을 클릭합니다.
5. **Warranty(보증)** 탭에는 다음 정보가 포함되어 있습니다.
   a. **Provider(공급자)**
   b. **설명**
   c. **Status(상태)**
   d. **Start Date(시작 날짜)**
   e. **End Date(종료 날짜)**
   f. **Days Left(남은 일 수)**
   g. **Last Updated(마지막으로 업데이트한 날짜)**

스토리지 보기

스토리지 창에는 섀시에 대한 정보가 저장되어 있습니다.

스토리지에 대한 정보를 보려면,

1. **홈** 페이지에서 **vCenter**를 클릭합니다.
2. 왼쪽 창에 있는 **OpenManage Integration** 아래에서 **Dell Chassis(Dell 섀시)**를 클릭합니다.
3. 왼쪽 창에서 해당 섀시 IP를 선택합니다.
4. **Monitor(모니터)** 탭을 클릭합니다.
5. **Storage(스토리지)** 탭에는 다음 정보가 포함되어 있습니다.
   a. **가상 디스크**
   b. **컨트롤러**
   c. **인클로저**
   d. **물리 디스크**
   e. **핫 스페어**

   스토리지 아래의 강조 표시된 각 링크를 클릭하면, **보기** 표에 강조 표시된 각 항목에 대한 세부 정보가 표시됩니다. 보기 표에서 각 라인 항목을 클릭하면 강조 표시된 각 항목에 대한 세부 정보가 표시됩니다.
6. M1000e 섀시의 경우, 스토리지 모듈이 있다면 다른 추가 정보 없이 다음과 같은 스토리지 세부 사항이 격자 형태로 표시됩니다.
   a. 이름
   b. Model(모델)
   c. 서비스 태그
   d. IP 주소(스토리지로 연결되는 링크)
   e. 패브릭
   f. 그룹 이름
   g. 그룹 IP 주소(스토리지 그룹으로 연결되는 링크)

섀시에 대한 펌웨어 세부정보 보기

선택한 섀시의 펌웨어 세부정보에 대한 정보를 볼 수 있습니다. 펌웨어 정보의 CSV 파일을 내보낼 수 있습니다.

펌웨어에 대한 정보를 보려면 다음을 수행하십시오.

1. **홈** 페이지에서 **vCenter**를 클릭합니다.
2. 왼쪽 창에 있는 **OpenManage Integration** 아래에서 **Dell Chassis(Dell 섀시)**를 클릭합니다.
3. 왼쪽 창에서 해당 섀시 IP를 선택합니다.
4. **Monitor(모니터)** 탭을 클릭합니다.
5. 이중 화살표 표시를 클릭하고 왼쪽 창을 확장한 후 **Firmware(펌웨어)**를 클릭합니다.
   다음 정보가 표시됩니다.
   - Component(구성 요소)
   - Current Version(현재 버전)
6. **Launch CMC(CMC 실행)**를 클릭하면 **Chassis Management Controller(섀시 관리 컨트롤러)** 페이지가 표시됩니다.

섀시에 대한 관리 컨트롤러 세부정보 보기

선택한 섀시의 관리 컨트롤러 세부정보에 대한 정보를 볼 수 있습니다.

관리 컨트롤러에 대한 정보를 보려면 다음을 수행하십시오.

1. **홈** 페이지에서 **vCenter**를 클릭합니다.
2. 왼쪽 창에 있는 **OpenManage Integration** 아래에서 **Dell Chassis(Dell 섀시)**를 클릭합니다.
3. 왼쪽 창에서 해당 섀시 IP를 선택합니다.

4. **Monitor(모니터)** 탭을 클릭합니다.
5. 이중 화살표 표시를 클릭하고 왼쪽 창을 확장한 후 **Management Controller(관리 컨트롤러)**를 클릭합니다.
6. **Management Controller(관리 컨트롤러)** 페이지에서 추가 정보를 보려면 화살표 표시를 클릭하고 왼쪽 열을 확장합니다. 다음 정보가 표시됩니다.
   - 일반
     - 이름
     - Firmware Version(펌웨어 버전)
     - Last Update Time(마지막 업데이트 시간)
     - CMC Location(CMC 위치)
     - Hardware Version(하드웨어 버전)
   - Common Network(공용 네트워크)
     - DNS Domain Name(DNS 도메인 이름)
     - Use DHCP for DNS(DNS의 DHCP 사용)
     - MAC Address(MAC 주소)
     - 중복 모드
   - CMC IPv4 Information(CMC IPv4 정보)
     - IPv4 Enabled(IPv4 활성화)
     - DHCP Enabled(DHCP 활성화)
     - IP Address(IP 주소)
     - Subnet Mask(서브넷 마스크)
     - Gateway(게이트웨이)
     - Preferred DNS Server(기본 DNS 서버)
     - Alternate DNS Server(대체 DNS 서버)

13

단일 호스트 모니터링

OpenManage Integration for VMware vCenter를 통해 단일 호스트에 대한 자세한 정보를 볼 수 있습니다. 왼쪽 Navigator(탐색 창)에서 VMware vCenter에 있는 호스트에 액세스할 수 있습니다. 그러면 모든 벤더의 모든 호스트가 나열됩니다. 자세한 정보를 찾아볼 특정 Dell 호스트를 클릭합니다. Dell 호스트 목록을 빠르게 보려면 OpenManage Integration for VMware vCenter의 왼쪽 Navigator(탐색 창)에서 Dell Hosts(Dell 호스트)를 클릭합니다.

- 호스트 요약 세부정보 보기
- 단일 호스트에 대한 하드웨어: FRU 세부정보 보기
- 단일 호스트에 대한 하드웨어: 프로세서 세부정보 보기
- 단일 호스트에 대한 하드웨어: 전원 공급 장치 세부정보 보기
- 단일 호스트에 대한 하드웨어: 메모리 세부정보 보기
- 단일 호스트에 대한 하드웨어: NIC 세부정보 보기
- 단일 호스트에 대한 하드웨어: PCI 슬롯 세부정보 보기
- 단일 호스트에 대한 하드웨어: 원격 액세스 카드 세부정보 보기
- 단일 호스트에 대한 스토리지 세부정보 보기
  - 단일 호스트에 대한 스토리지: 가상 디스크 세부정보 보기
  - 단일 호스트에 대한 스토리지: 실제 디스크 세부정보 보기
  - 단일 호스트에 대한 스토리지: 컨트롤러 세부정보 보기
  - 단일 호스트에 대한 스토리지: 인클로저 세부정보 보기
- 단일 호스트에 대한 펌웨어 세부정보 보기
- 단일 호스트에 대한 전원 모니터링 보기
- 단일 호스트에 대한 보증 상태 보기
- Dell 호스트만 빠르게 보기

주제:

- 호스트 요약 세부정보 보기
- 관리 콘솔 시작
- 원격 액세스 콘솔(iDRAC) 시작
- 실제 서버 깜빡임 표시등 설정
- 실제 서버 깜빡임 표시등 설정

호스트 요약 세부정보 보기

호스트 요약 페이지에서 개별 호스트에 대한 호스트 요약 세부정보를 봅니다. 이 페이지에 다양한 포틀릿이 표시됩니다. 포틀릿 중 2개를 OpenManage Integration for VMware vCenter에 적용할 수 있습니다.

적용되는 포틀릿은 다음과 같습니다.

- Dell 호스트 상태
- Dell 호스트 정보

2개의 포틀릿을 원하는 위치에 끌어 놓을 수 있으며 다른 포틀릿과 마찬가지로 요구 사항에 따라 이 2개의 포틀릿을 포맷하고 사용자 지정할 수 있습니다.

1. OpenManage Integration for VMware vCenter의 Navigator(탐색 창)에서 **Hosts(호스트)**를 클릭합니다.
2. 개체 탭에서 보려는 특정 호스트를 선택합니다.

3. **요약** 탭을 클릭합니다.
4. 호스트 요약 세부정보 보기:

Alerting system(시스템 경고)	OpenManage Integration for VMware vCenter에 대한 경고가 있을 경우 상태 영역 아래와 포틀릿 위에 노란색 상자로 경고가 표시됩니다.
알림 영역	Dell 제품은 이 오른쪽 측면 패널 영역에 있는 정보를 통합합니다. 다음과 같은 정보를 확인할 수 있습니다. ● 최근 작업 ● 진행 중인 작업 ● 알람 이 알림 영역 포틀릿에 Dell 알람 정보가 표시됩니다.

5. 아래로 스크롤하여 Dell 서버 관리 포틀릿을 봅니다.

서비스 태그	Dell PowerEdge 서버의 서비스 태그입니다. 지원 부서에 전화로 문의할 때 이 ID를 사용하십시오.
모델 이름	서버 모델 이름을 표시합니다.
결함 복원 메모리	이것은 BIOS 특성이며, 서버 초기 설치 중에 BIOS에서 활성화되고 서버의 메모리 작동 모드를 표시합니다. 메모리 작동 모드 값을 변경한 경우 시스템을 다시 시작합니다. 이 기능은 ESXi 5.5 이상 버전이 설치된 R620, R720, T620, M620 서버에 적용됩니다. 이는 장애 복원 메모리를 지원하고 ESXi 5.5 이상 버전을 실행하는 12세대 PowerEdge 서버에 적용됩니다. 4가지 값은 다음과 같습니다. ● Enabled and Protected(활성화되고 보호됨): 이 값은 시스템이 지원되고 운영 체제 버전이 ESXi 5.5 이상이며 BIOS의 메모리 작동 모드가 FRM으로 설정되어 있음을 나타냅니다. ● 활성화되고 보호되지 않음: 이 값은 ESXi 5.5 이하의 운영 체제 버전으로 시스템을 지원함을 나타냅니다. ● Disabled(사용 안 함): 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.
불균일 메모리 액세스(NUMA) 결함 복원 메모리(FRM)	NUMA FRM은 최소 2개 또는 4개의 프로세서가 장착된 Dell의 13세대 PowerEdge 시스템의 BIOS 설정에서 사용할 수 있는 새로운 메모리 작동 모드입니다. 이 모드는 모든 CPU에서 결함 복원 기능을 갖는 메모리 영역을 설정하여, 영향을 줄 수 있는 수정 불가능한 메모리 오류에 대하여 하이퍼바이저에 동일한 보호 기능을 제공하면서 NUMA 메모리 기능 및 성능을 유지합니다. 4가지 값은 다음과 같습니다. ● NUMA 사용되고 보호됨: 이 값은 시스템이 지원되고 운영 체제 버전이 ESXi 5.5 이상이며 BIOS의 메모리 작동 모드가 NUMA FRM으로 설정되어 있음을 나타냅니다. ● NUMA 활성화되고 보호되지 않음: 이 값은 ESXi 5.5 이하의 운영 체제 버전으로 시스템을 지원함을 나타냅니다. ● Disabled(사용 안 함): 이 값은 아무 운영 체제 버전으로나 유효한 시스템을 지원함을 나타내며, 여기서 BIOS의 메모리 작동 모드는 NUMA FRM으로 설정되지 않습니다. ● Blank(비어 있음): BIOS의 메모리 작동 모드가 지원되지 않으면 NUMA FRM 특성이 표시되지 않습니다.
식별	● 호스트 이름 Dell 호스트의 이름입니다. ● 전원 상태 전원이 켜져 있는지 또는 꺼져 있는지 표시합니다. ● iDRAC IP iDRAC IP 주소를 표시합니다. ● Management IP(관리 IP) 관리 IP 주소를 표시합니다. ● 연결 프로필 이 호스트에 대한 연결 프로필 이름을 표시합니다. ● 모델

	Dell 서버 모델을 표시합니다. • 서비스 태그 서버의 서비스 태그를 표시합니다. • Asset Tag 자산 태그를 표시합니다. • Warranty Days Left(남은 보증 기간) 보증의 남은 일 수를 표시합니다. • Last Inventory Scan(마지막 인벤토리 검색) 마지막 인벤토리 검색의 날짜와 시간을 표시합니다.
하이퍼바이저 및 펌웨어	• Hypervisor(하이퍼바이저) 하이퍼바이저 버전을 표시합니다. • BIOS Version BIOS 버전을 표시합니다. • 원격 액세스 카드 버전 원격 액세스 카드 버전을 표시합니다.
관리 콘솔	관리 콘솔은 외부 시스템 관리 콘솔을 실행하는 데 사용됩니다. 예를 들면 다음과 같습니다. • 원격 액세스 콘솔(iDRAC) iDRAC(Integrated Dell Remote Access Controller) 웹 사용자 인터페이스를 시작합니다.
호스트 조치	Blink Indicator Light(깜빡임 표시등)를 통해 다양한 시간 간격으로 표시등이 깜빡이도록 실제 서버를 설정할 수 있습니다.

6. Dell 호스트 상태 포틀릿 보기:

Dell 호스트 상태	구성 요소 상태는 호스트 서버의 모든 주요 구성 요소들의 상태를 그림으로 나타낸 것으로, 서버의 전반적인 상태, 서버, 전원 공급 장치, 온도, 전압, 프로세서, 배터리, 침입, 하드웨어 로그, 전력 관리, 전원 및 메모리 등으로 구성됩니다. 이들 섀시 상태 매개변수는 **VRTX 버전 1.0** 이상과 **M1000e 버전 4.4 이상**에 적용됩니다. 4.3 이전 버전의 경우, **양호** 및 **경고 또는 치명적** 결함(주황색 역삼각형과 느낌표)의 두 가지 상태 표시등만이 표시됩니다. 전체적인 상태에는 상태 매개변수가 가장 낮은 섀시를 기초로 하여 상태가 표시됩니다. 예를 들어, 양호 기호가 5개 있고 경고 기호가 1개 있는 경우 전체적인 상태는 경고로 표시됩니다. 다음과 같은 옵션을 사용할 수 있습니다. • 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

관리 콘솔 시작

Dell 서버 관리 포틀릿에서 실행할 수 있는 두 가지 관리 콘솔은 다음과 같습니다.

- 원격 액세스 콘솔(iDRAC 콘솔)

  iDRAC 사용자 인터페이스에 액세스할 수 있는 원격 액세스 콘솔을 시작합니다.

- OMSA 콘솔

  OMSA 콘솔을 시작하여 OpenManage Server Administrator 사용자 인터페이스에 액세스합니다. OMSA 콘솔을 시작하기 전에 OMSA URL이 Open Management Integration for VMware vCenter에 구성되어 있어야 합니다.

OMSA 콘솔 시작

OMSA 콘솔을 시작하려면 OMSA URL을 설정한 후 OMSA 웹 서버를 설치하고 구성해야 합니다. Settings(설정) 탭에서 OMSA URL을 설정합니다.

노트: OpenManage Integration for VMware vCenter를 사용하여 Dell PowerEdge 11세대 서버를 모니터링하고 관리하려면 OMSA를 설치해야 합니다.

1. OpenManage Integration for VMware vCenter의 Navigator(탐색 창) 영역에 있는 Inventory Lists(인벤토리 목록) 아래에서 **Hosts(호스트)**를 클릭합니다.
2. Object(개체) 탭에서 원하는 호스트를 두 번 클릭합니다.
3. Summary(요약) 탭에서 Dell 서버 관리 포틀릿까지 아래로 스크롤합니다.
4. OMSA 콘솔을 열려면**Management Consoles(관리 콘솔)** > **OMSA Console(OMSA 콘솔)을** 클릭합니다.

원격 액세스 콘솔(iDRAC) 시작

Dell 서버 관리 포틀릿에서 iDRAC 사용자 인터페이스를 시작할 수 있습니다.

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

실제 서버 깜빡임 표시등 설정

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

1. OpenManage Integration for VMware vCenter의 Navigator(탐색 창) 영역에 있는 Inventory Lists(인벤토리 목록)에서 **Hosts(호스트)**를 클릭합니다.
2. Object(개체) 탭에서 원하는 호스트를 두 번 클릭합니다.
3. Summary(요약) 탭에서 Dell 서버 관리 포틀릿까지 아래로 스크롤합니다.
4. **Host Actions(호스트 조치)**에서 **Blink Indicator Light(깜빡임 표시등)**를 선택합니다.
5. 다음 중 하나를 선택합니다.
   - 깜빡임 및 기간을 설정하려면 **Indicator Light(표시등)** 대화상자에서 **Blink On(깜빡임 켜짐)**을 클릭하고 시간 제한 드롭다운 목록을 사용하여 시간 제한 증가를 선택한 다음 **OK(확인)**를 클릭합니다.
   - 깜빡임을 해제하려면 **Indicator Light(표시등)** 대화상자에서 **Blink On(깜빡임 켜짐)**을 클릭하고 **OK(확인)**을 클릭합니다.

실제 서버 깜빡임 표시등 설정

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

1. OpenManage Integration for VMware vCenter의 Navigator(탐색 창) 영역에 있는 Inventory Lists(인벤토리 목록)에서 **Hosts(호스트)**를 클릭합니다.
2. Object(개체) 탭에서 원하는 호스트를 두 번 클릭합니다.
3. Summary(요약) 탭에서 Dell 서버 관리 포틀릿까지 아래로 스크롤합니다.
4. **Host Actions(호스트 조치)**에서 **Blink Indicator Light(깜빡임 표시등)**를 선택합니다.
5. 다음 중 하나를 선택합니다.
   - 깜빡임 및 기간을 설정하려면 **Indicator Light(표시등)** 대화상자에서 **Blink On(깜빡임 켜짐)**을 클릭하고 시간 제한 드롭다운 목록을 사용하여 시간 제한 증가를 선택한 다음 **OK(확인)**를 클릭합니다.
   - 깜빡임을 해제하려면 **Indicator Light(표시등)** 대화상자에서 **Blink On(깜빡임 켜짐)**을 클릭하고 **OK(확인)**을 클릭합니다.

14

OpenManage Integration for VMware vCenter 라이센싱

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

- 평가판 라이센스 — OMIVV 버전 3.2 어플라이언스의 전원을 처음 켜면, 평가판 라이센스가 자동으로 설치됩니다. 평가 버전에는 OpenManage Integration for VMware vCenter에서 관리되는 호스트(서버) 5개에 대한 평가판 라이센스가 포함되어 있습니다. 이는 11세대 이후의 Dell 서버에만 해당되며, 90일 간의 평가 기간 동안 제공되는 기본 라이센스입니다.
- 표준 라이센스 — 전체 제품 버전에는 vCenter 서버 10개에 대한 표준 라이센스가 포함되어 있으며 OMIVV에서 관리되는 호스트 연결을 원하는 수 만큼 구입할 수 있습니다.

평가판 라이센스를 정식 표준 라이센스로 업그레이드하면, 이메일로 주문 확인서가 전송되며 http://www.dell.com/support/licensing에서 사용 가능한 Dell 디지털 스토어에서 라이센스 파일을 다운로드할 수 있습니다. 라이센스 .XML 파일을 로컬 시스템에 저장하고 **Administration Console**을 사용하여 새 라이센스 파일을 업로드합니다.

라이센싱은 다음 정보를 제공합니다.

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

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

라이센스를 구입하면 http://www.dell.com/support/licensing에서 사용 가능한 Dell 디지털 스토어에서 .XML 파일(라이센스 키)을 다운로드할 수 있습니다. 라이센스 키가 다운로드되지 않는 경우 www.dell.com/support/softwarecontacts에서 해당 제품의 지역 Dell 지원 부서 전화 번호를 찾아 Dell 지원 부서에 문의합니다.

주제:

소프트웨어 라이센스 구입 및 업로드

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

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

1. OpenManage Integration for VMware vCenter에서 다음 작업 중 하나를 수행합니다.
   - **라이센싱** 탭에서 **소프트웨어 라이센스** 옆에 있는 **라이센스 구입**을 클릭합니다.
   - **시작하기** 탭의 **기본 작업** 아래에서 **라이센스 구입**을 클릭합니다.
2. http://www.dell.com/support/licensing에서 사용 가능한 Dell 디지털 스토어에서 다운로드한 알려진 위치에 라이센스 파일을 저장합니다.
3. 웹 브라우저에 관리 콘솔 URL을 입력합니다.

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

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

15

단일 호스트에 대한 하드웨어: FRU 세부정보 보기

Dell Host Information(Dell 호스트 정보) 탭에서 단일 호스트에 대한 현장 교체 가능 부품(FRU) 세부정보를 봅니다. 이 페이지에 정보를 표시하려면 인벤토리 작업을 실행해야 합니다. 하드웨어 보기에서는 OMSA 및 iDRAC의 데이터를 직접 보고합니다. 지금 인벤토리 작업 실행을 참조하십시오.

1. OpenManage Integration for VMware vCenter의 Navigator(탐색 창)에서 **Hosts(호스트)**를 클릭합니다.
2. Host(호스트) 탭에서 하드웨어: FRU 세부정보를 확인할 특정 호스트를 선택합니다.
3. Monitor(모니터) 탭에서 **Dell Host Information(Dell 호스트 정보)** 탭을 선택하고 Hardware: FRU(하드웨어: FRU) 하위 탭에서 다음을 확인합니다.

Part Name(부품명)	FRU 부품명을 표시합니다.
Part Number(부품 번호)	FRU 부품 번호를 표시합니다.
Manufacturer(제조업체)	제조업체 이름을 표시합니다.
Serial Number(일련 번호)	제조업체의 일련 번호를 표시합니다.
Manufacture Date(제조 일자)	제조일자를 표시합니다.

16

단일 호스트에 대한 하드웨어: 프로세서 세부정보 보기

Dell Host Information(Dell 호스트 정보) 탭에서 단일 호스트에 대한 프로세스 세부정보를 봅니다. 이 페이지에 정보를 표시하려면 인벤토리 작업을 실행해야 합니다. 하드웨어 보기에서는 OMSA 및 iDRAC의 데이터를 직접 보고합니다. 지금 인벤토리 작업 실행을 참조하십시오.

1. OpenManage Integration for VMware vCenter의 Navigator(탐색 창)에서 **Hosts(호스트)**를 클릭합니다.
2. Objects(개체) 탭에서 프로세서 세부정보를 확인할 특정 호스트를 선택합니다.
3. Monitor(모니터) 탭에서 **Dell Host Information(Dell 호스트 정보)** 탭을 선택하고 Hardware: Processor(하드웨어: 프로세서) 하위 탭에서 다음을 확인합니다.

Socket(소켓)	슬롯 번호를 표시합니다.
Speed(속도)	현재 속도를 표시합니다.
Brand(브랜드)	프로세서 브랜드를 표시합니다.
Version(버전)	프로세서 버전을 표시합니다.
Cores(코어)	이 프로세서의 코어 수를 표시합니다.

17

단일 호스트에 대한 하드웨어: 전원 공급 장치 세부정보 보기

Dell Host Information(Dell 호스트 정보) 탭에서 단일 호스트에 대한 가상 전원 공급 장치 세부정보를 봅니다. 이 페이지에 정보를 표시하려면 인벤토리 작업을 실행해야 합니다. 하드웨어 보기에서는 OMSA 및 iDRAC의 데이터를 직접 보고합니다. 지금 인벤토리 작업 실행을 참조하십시오.

1. OpenManage Integration for VMware vCenter의 Navigator(탐색 창)에서 **Hosts(호스트)**를 클릭합니다.
2. Objects(개체) 탭에서 하드웨어: 전원 공급 장치 세부정보를 확인할 특정 호스트를 선택합니다.
3. Monitor(모니터) 탭에서 **Dell Host Information(Dell 호스트 정보)** 탭을 선택하고 **Hardware: Power Supply(하드웨어: 전원 공급 장치)** 하위 탭에서 다음을 확인합니다.

Type(종류)	전원 공급 장치의 종류를 표시합니다. 전원 공급 장치 종류는 다음과 같습니다. • UNKNOWN(알 수 없음) • LINEAR(선형) • SWITCHING(스위칭) • BATTERY(배터리) • UPS • CONVERTER(변환기) • REGULATOR(조절기) • AC • DC • VRM
Location(위치)	전원 공급 장치의 위치를 표시합니다(예: 슬롯 1).
Output(출력)(와트)	와트 단위로 전원을 표시합니다.

18

단일 호스트에 대한 하드웨어: 메모리 세부정보 보기

Dell Host Information(Dell 호스트 정보) 탭에서 단일 호스트에 대한 메모리 세부정보를 봅니다. 이 페이지에 정보를 표시하려면 인벤토리 작업을 실행해야 합니다. 하드웨어 보기에서는 OMSA 및 iDRAC의 데이터를 직접 보고합니다. 지금 인벤토리 작업 실행을 참조하십시오.

1. OpenManage Integration for VMware vCenter의 Navigator(탐색 창)에서 **Hosts(호스트)**를 클릭합니다.
2. Objects(개체) 탭에서 하드웨어: 메모리 세부정보를 확인할 특정 호스트를 선택합니다.
3. Monitor(모니터) 탭에서 **Dell Host Information(Dell 호스트 정보)** 탭을 선택하고 **Hardware: Memory(하드웨어: 메모리)** 하위 탭에서 다음을 확인합니다.

Memory Slots(메모리 슬롯)	사용한 메모리 용량, 총 메모리 용량 및 사용 가능한 메모리 용량을 표시합니다.
Memory Capacity(메모리 용량)	설치된 메모리, 총 메모리 용량 및 사용 가능한 메모리를 표시합니다.
Slot(슬롯)	DIMM 슬롯을 표시합니다.
Size(크기)	메모리 크기를 표시합니다.
Type(종류)	메모리의 종류를 표시합니다.

19

단일 호스트에 대한 하드웨어: NIC 세부정보 보기

Dell Host Information(Dell 호스트 정보) 탭에서 단일 호스트에 대한 네트워크 인터페이스 카드(NIC) 세부정보를 봅니다. 이 페이지에 정보를 표시하려면 인벤토리 작업을 실행해야 합니다. 하드웨어 보기에서는 OMSA 및 iDRAC의 데이터를 직접 보고합니다. 지금 인벤토리 작업 실행을 참조하십시오.

1. OpenManage Integration for VMware vCenter의 Navigator(탐색 창)에서 **Hosts(호스트)**를 클릭합니다.
2. Objects(개체) 탭에서 하드웨어: NIC 세부정보를 확인할 특정 호스트를 선택합니다.
3. Monitor(모니터) 탭에서 **Dell Host Information(Dell 호스트 정보)** 탭을 선택하고 **Hardware: NIC(하드웨어: NIC)** 하위 탭에서 다음을 확인합니다.

Total(총계)	총 사용 가능한 네트워크 인터페이스 카드 수를 표시합니다.
Name(이름)	NIC 이름을 표시합니다.
Manufacturer(제조업체)	제조업체의 이름만 표시합니다.
MAC Address(MAC 주소)	NIC MAC 주소를 표시합니다.

20

단일 호스트에 대한 하드웨어: PCI 슬롯 보기

Dell Host Information(Dell 호스트 정보) 탭에서 단일 호스트에 대한 PCI 슬롯 세부정보를 봅니다. 이 페이지에 정보를 표시하려면 인벤토리 작업을 실행해야 합니다. 하드웨어 보기에서는 OMSA 및 iDRAC의 데이터를 직접 보고합니다. 지금 인벤토리 작업 실행을 참조하십시오.

1. OpenManage Integration for VMware vCenter의 Navigator(탐색 창)에서 **Hosts(호스트)**를 클릭합니다.
2. Objects(개체) 탭에서 하드웨어: PCI 슬롯 세부정보를 확인할 특정 호스트를 선택합니다.
3. Monitor(모니터) 탭에서 **Dell Host Information(Dell 호스트 정보)** 탭을 선택하고 **Hardware: PCI Slots(하드웨어: PCI 슬롯)** 하위 탭에서 다음을 확인합니다.

PCI Slots(PCI 슬롯)	사용한 PCI 슬롯 수, 총 PCI 슬롯 수 및 사용 가능한 PCI 슬롯 수를 표시합니다.
Slot(슬롯)	슬롯을 표시합니다.
Manufacturer(제조업체)	PCI 슬롯의 제조업체 이름을 표시합니다.
Description(설명)	PCI 장치에 대한 설명을 표시합니다.
Type(종류)	PCI 슬롯 종류를 표시합니다.
Width(너비)	데이터 버스 너비를 표시합니다(사용 가능한 경우).

21

단일 호스트에 대한 하드웨어: 원격 액세스 카드 세부정보 보기

Dell Host Information(Dell 호스트 정보) 탭에서 단일 호스트에 대한 원격 액세스 카드 세부정보를 봅니다. 이 페이지에 정보를 표시하려면 인벤토리 작업을 실행해야 합니다. 하드웨어 보기에서는 OMSA 및 iDRAC의 데이터를 직접 보고합니다. 지금 인벤토리 작업 실행을 참조하십시오.

1. OpenManage Integration for VMware vCenter의 Navigator(탐색 창)에서 **Hosts(호스트)**를 클릭합니다.
2. Objects(개체) 탭에서 하드웨어: 원격 액세스 카드 세부정보를 확인할 특정 호스트를 선택합니다.
3. Monitor(모니터) 탭에서 **Dell Host Information(Dell 호스트 정보)** 탭을 선택하고 **Hardware: Remote Access Card(하드웨어: 원격 액세스 카드)** 하위 탭에서 다음을 확인합니다.

IP Address(IP 주소)	원격 액세스 카드의 IP 주소를 표시합니다.
MAC Address(MAC 주소)	원격 액세스 카드의 MAC 주소를 표시합니다.
RAC Type(RAC 유형)	원격 액세스 카드의 종류를 표시합니다.
URL	이 호스트와 연관된 iDRAC의 라이브 URL을 표시합니다.

22

단일 호스트에 대한 스토리지 세부정보 보기

Dell Host Information(Dell 호스트 정보) 탭에서 단일 호스트에 대한 스토리지 세부정보를 봅니다. 이 페이지에 정보를 표시하려면 인벤토리 작업을 실행합니다. 지금 인벤토리 작업 실행을 참조하십시오. View(보기) 드롭다운 목록에서 선택한 항목에 따라 이 페이지에 다른 옵션이 표시됩니다. 실제 디스크를 선택하는 경우 다른 드롭다운 목록이 표시됩니다. 이러한 새 드롭다운 목록을 필터라고 하며, 이를 통해 실제 디스크 옵션을 필터링할 수 있습니다.

노트: 하드웨어 보기는 OMSA 및 iDRAC에서 데이터를 직접 보고합니다.

1. OpenManage Integration for VMware vCenter의 Navigator(탐색 창)에서 **Hosts(호스트)**를 클릭합니다.
2. Objects(개체) 탭에서 스토리지: 실제 디스크 세부정보를 확인할 특정 호스트를 선택합니다.
3. Monitor(모니터) 탭에서 **Dell Host Information(Dell 호스트 정보)** 탭을 선택하고 **Storage(스토리지)** 하위 탭에서 다음을 확인합니다.

Storage(스토리지)	전역 핫 스페어 및 전용 핫 스페어 개수와 함께 가상 디스크, 컨트롤러, 인클로저 및 연결된 실제 디스크의 개수를 표시합니다. View(보기) 드롭다운 목록에서 선택한 경우 이 옵션이 여기에서 강조표시됩니다.
View(보기)	이 호스트에 대해 보려는 페이지 옵션을 표시합니다. • 가상 디스크 • 물리 디스크 • 컨트롤러 • 인클로저

주제:

- 단일 호스트에 대한 스토리지: 가상 디스크 세부정보 보기
- 단일 호스트에 대한 스토리지: 실제 디스크 세부정보 보기
- 단일 호스트에 대한 스토리지: 컨트롤러 세부정보 보기
- 단일 호스트에 대한 스토리지: 인클로저 세부정보 보기

단일 호스트에 대한 스토리지: 가상 디스크 세부정보 보기

View(보기) 드롭다운 목록에서 선택하는 항목에 따라 호스트 스토리지 페이지의 스토리지 옵션이 달라집니다.

View(보기) 드롭다운 목록에서 가상 디스크를 선택한 경우 다음 옵션이 표시됩니다.

Name(이름)	가상 디스크의 이름을 표시합니다.
Device FQDD(장치 FQDD)	FQDD를 표시합니다.
Physical Disk(실제 디스크)	가상 디스크가 있는 실제 디스크를 표시합니다.
Capacity(용량)	가상 디스크의 용량을 표시합니다.
Layout(레이아웃)	가상 스토리지의 레이아웃 유형을 표시합니다. 이 가상 디스크에 구성된 RAID 유형을 의미합니다.
Media Type(매체 종류)	SSD 또는 HDD를 표시합니다.
Controller ID(컨트롤러 ID)	컨트롤러 ID를 표시합니다.
Device ID(장치 ID)	장치 ID를 표시합니다.

Stripe Size(스트라이프 크기)	스트라이프 크기는 단일 디스크에서 각 스트라이프가 사용하는 공간의 양을 의미합니다.
Bus Protocol(버스 프로토콜)	가상 디스크에 포함된 실제 디스크가 사용하는 기술을 표시합니다. 값은 다음과 같습니다. • SCSI • SAS • SATA
Default Read Policy(기본 읽기 정책)	컨트롤러에서 지원되는 기본 읽기 정책으로서 다음과 같은 옵션을 사용할 수 있습니다. • Read-Ahead(미리 읽기) • No-Read-Ahead(미리 읽기 없음) • Adaptive Read-Ahead(적응성 미리 읽기) • Read Cache Enabled(읽기 캐시 활성 상태) • Read Cache Disabled(읽기 캐시 비활성 상태)
Default Write Policy(기본 쓰기 정책)	컨트롤러에서 지원되는 기본 쓰기 정책으로서 다음과 같은 옵션을 사용할 수 있습니다. • Write-Back(후기입) • Force Write Back(강제 후기입) • Write Back Enabled(후기입 활성 상태) • Write-Through(연속 기입) • Write Cache Enabled Protected(쓰기 캐시 활성 상태 보호) • Write Cache Disabled(쓰기 캐시 비활성 상태)
Cache Policy(캐시 정책)	캐시 정책이 활성화되어 있는지 표시합니다.

단일 호스트에 대한 스토리지: 실제 디스크 세부정보 보기

View(보기) 드롭다운 목록에서 선택하는 항목에 따라 호스트 스토리지 페이지의 스토리지 옵션이 달라집니다. 이 옵션을 선택하면 필터 드롭다운 목록이 표시됩니다. 다음 옵션에 대해 실제 디스크를 필터링할 수 있습니다.

- 모든 실제 디스크
- 전역 핫스페어
- 전용 핫 스페어
- 마지막 옵션은 명명된 사용자 지정 가상 디스크를 표시합니다.

View(보기) 드롭다운 목록에서 실제 디스크를 선택한 경우 다음 옵션이 표시됩니다.

Name(이름)	실제 디스크의 이름을 표시합니다.
Device FQDD(장치 FQDD)	장치 FQDD를 표시합니다.
Capacity(용량)	실제 디스크의 용량을 표시합니다.
Disk Status(디스크 상태)	실제 디스크의 상태를 표시합니다. 다음과 같은 옵션을 사용할 수 있습니다. • ONLINE(온라인) • READY(준비 완료) • DEGRADED(저하됨) • FAILED(장애) • OFFLINE(오프라인) • REBUILDING(재구축 중)

	• INCOMPATIBLE(호환되지 않음) • REMOVED(제거됨) • CLEARED(지워짐) • SMART ALERT DETECTED(스마트 경고 감지됨) • UNKNOWN(알 수 없음) • FOREIGN(외부) • UNSUPPORTED(지원되지 않음)
Configured(구성됨)	디스크가 구성되어 있는지 여부를 표시합니다.
Hot Spare Type(핫 스페어 종류)	핫 스페어 종류를 표시합니다. 다음과 같은 옵션을 사용할 수 있습니다. • No(없음) 핫 스페어가 없음을 의미합니다. • Global(전역) 전역 핫 스페어는 디스크 그룹에 속하는 사용되지 않은 백업 디스크입니다. • Dedicated(전용) 전용 핫 스페어는 단일 가상 디스크에 할당된 사용되지 않은 백업 디스크입니다. 가상 디스크에서 실제 디스크에 장애가 발생할 경우, 시스템 중단이나 사용자 개입이 없어도 이 핫 스페어가 활성화되어 장애가 발행한 실제 디스크를 대체합니다.
Virtual Disk(가상 디스크)	가상 디스크의 이름을 표시합니다.
Bus Protocol(버스 프로토콜)	버스 프로토콜을 표시합니다.
Controller ID(컨트롤러 ID)	컨트롤러 ID를 표시합니다.
Connector ID(커넥터 ID)	커넥터 ID를 표시합니다.
Enclosure ID(인클로저 ID)	인클로저 ID를 표시합니다.
Device ID(장치 ID)	장치 ID를 표시합니다.
Model(모델)	실제 스토리지 디스크의 모델 번호를 표시합니다.
Part Number(부품 번호)	스토리지 부품 번호를 표시합니다.
Serial Number(일련 번호)	스토리지 일련 번호를 표시합니다.
Vendor(벤더)	스토리지 벤더 이름을 표시합니다.

단일 호스트에 대한 스토리지: 컨트롤러 세부정보 보기

View(보기) 드롭다운 목록에서 선택한 항목에 따라 호스트 스토리지 페이지의 스토리지 옵션이 달라집니다.

View(보기) 드롭다운 목록에서 컨트롤러를 선택한 경우 다음 옵션이 표시됩니다.

Controller ID(컨트롤러 ID)	컨트롤러 ID를 표시합니다.
이름	컨트롤러의 이름을 표시합니다.
Device FQDD(장치 FQDD)	장치의 FQDD를 표시합니다.
펌웨어 버전	펌웨어 버전을 표시합니다.
Minimum Required Firmware(최소 필수 펌웨어)	최소 필수 펌웨어를 표시합니다. 이 열은 펌웨어가 오래되고 최신 버전이 사용 가능할 때 채워집니다.

Driver Version(드라이버 버전)	드라이버 버전을 표시합니다.
Patrol Read State(순회 읽기 상태)	순회 읽기 상태를 표시합니다.
Cache Size(캐시 크기)	캐시 크기를 표시합니다.

단일 호스트에 대한 스토리지: 인클로저 세부정보 보기

View(보기) 드롭다운 목록에서 선택한 항목에 따라 호스트 스토리지 페이지의 스토리지 옵션이 달라집니다.

View(보기) 드롭다운 목록에서 인클로저를 선택한 경우 다음 옵션이 표시됩니다.

Controller ID(컨트롤러 ID)	컨트롤러 ID를 표시합니다.
Connector ID(커넥터 ID)	커넥터 ID를 표시합니다.
Enclosure ID(인클로저 ID)	인클로저 ID를 표시합니다.
Name(이름)	인클로저의 이름을 표시합니다.
Device FQDD(장치 FQDD)	장치 FQDD를 표시합니다.
Service Tag(서비스 태그)	서비스 태그를 표시합니다.

23

단일 호스트에 대한 펌웨어 세부정보 보기

Dell Host Information(Dell 호스트 정보) 탭에서 단일 호스트에 대한 펌웨어 세부정보를 봅니다. 이 페이지에 정보를 표시하려면 인벤토리 작업을 실행해야 합니다. 하드웨어 보기에서는 OMSA 및 iDRAC의 데이터를 직접 보고합니다. 지금 인벤토리 작업 실행을 참조하십시오. 이 호스트 페이지에서는 검색 필터를 사용하고 펌웨어 정보의 CSV 파일을 내보낼 수 있습니다.

1. OpenManage Integration for VMware vCenter의 Navigator(탐색 창)에서 **Hosts(호스트)**를 클릭합니다.
2. Objects(개체) 탭에서 펌웨어 세부정보를 확인할 특정 호스트를 선택합니다.
3. Monitor(모니터) 탭에서 **Dell Host Information(Dell 호스트 정보)** 탭을 선택하고 Firmware(펌웨어) 하위 탭에서 다음을 확인합니다.

Name(이름)	이 호스트에 있는 모든 펌웨어의 이름을 표시합니다.
Type(종류)	펌웨어의 유형을 표시합니다.
Version(버전)	이 호스트에 있는 모든 펌웨어의 버전을 표시합니다.
Installation Date(설치 날짜)	설치 날짜를 표시합니다.

24

단일 호스트에 대한 전원 모니터링 보기

Dell Host Information(Dell 호스트 정보) 탭에서 단일 호스트에 대한 전원 모니터링 세부정보를 봅니다. 이 페이지에 정보를 표시하려면 인벤토리 작업을 실행해야 합니다. 하드웨어 보기에서는 OMSA 및 iDRAC의 데이터를 직접 보고합니다. 지금 인벤토리 작업 실행을 참조하십시오.

노트: 여기에서 사용되는 호스트 시간은 호스트가 있는 로컬 시간을 의미합니다.

1. OpenManage Integration for VMware vCenter의 Navigator(탐색 창)에서 **Hosts(호스트)**를 클릭합니다.
2. Objects(개체) 탭에서 전원 모니터링 세부정보를 확인할 특정 호스트를 선택합니다.
3. Monitor(모니터) 탭에서 **Dell Host Information Host(Dell 호스트 정보 호스트)** 탭을 선택하고 Power Monitoring(전원 모니터링) 하위 탭에서 다음을 확인합니다.

General Information(일반 정보)	전원 할당 및 현재 프로필 이름을 표시합니다.
Threshold(임계값)	경고 및 오류 임계값(와트)을 표시합니다.
Reserve Power Capacity(예비 전력 용량)	인스턴트 및 최대 전력 용량(와트)을 표시합니다.
Energy Statistics(에너지 통계)	
종류:	에너지 통계 유형을 표시합니다.
Measurement Start Time(측정 시작 시간)(호스트 시간)	호스트가 전원 사용을 시작한 날짜 및 시간을 표시합니다.
Measurement Finish Time(측정 종료 시간)(호스트 시간)	호스트가 전원 사용을 중지한 날짜 및 시간을 표시합니다.
Reading(판독값)	이 순간 값은 1분 이상의 평균 판독값입니다.
종류:	에너지 통계 유형을 표시합니다.
Measurement Start Time(측정 시작 시간)(호스트 시간)	호스트의 최고 전원이 시작된 날짜 및 시간을 표시합니다.
Peak Time(최대 시간)(호스트 시간)	호스트 최고 암페어의 날짜 및 시간을 표시합니다.
Peak Reading(최대 판독값)	시스템 최대 전력 통계는 시스템에서 사용한 최대 전력(와트)입니다.

25

단일 호스트에 대한 보증 상태 보기

보증 상태를 보려면 보증 작업을 실행해야 합니다. 지금 보증 작업 실행을 참조하십시오.

Dell Host Information(Dell 호스트 정보) 탭에서 단일 호스트에 대한 보증 상태 세부정보를 봅니다. Warranty Status(보증 상태) 페이지에서 보증 만료 날짜를 모니터할 수 있습니다. 보증 설정은 보증 일정을 활성화하거나 비활성화한 후 최소 일 수 임계값 경고를 설정하여 Dell에서 온라인으로 서버 보증 정보를 가져오는 경우를 제어합니다. 보증 내역을 참조하십시오.

1. OpenManage Integration for VMware vCenter의 Navigator(탐색 창)에서 **Hosts(호스트)**를 클릭합니다.
2. Objects(개체) 탭에서 보증 요약 세부정보를 확인할 특정 호스트를 선택합니다.
3. Monitor(모니터) 탭에서 **Dell Host Information(Dell 호스트 정보)**을 클릭하고 **Warranty(보증)** 하위 탭을 클릭합니다. 그러면 다음과 같은 정보가 표시됩니다.

Provider(공급자)	보증에 대한 공급자 이름을 표시합니다.
설명	설명을 표시합니다.
Start Date(시작 날짜)	보증의 시작 날짜를 표시합니다.
End Date(종료 날짜)	보증의 종료 날짜를 표시합니다.
Days Left(남은 일 수)	보증에 대해 남은 일 수 를 표시합니다.
Last Updated(마지막으로 업데이트한 날짜)	보증이 마지막으로 업데이트된 시간입니다.

26

Dell 호스트만 빠르게 보기

OpenManage Integration for VMware vCenter에서 Dell 호스트만 빠르게 볼 수 있으며 탐색 창에서 Dell 호스트를 선택할 수 있습니다.

1. VMware vCenter 홈 페이지에서 **OpenManage Integration** 아이콘을 클릭합니다.
2. 탐색 창의 OpenManage Integration for VMware vCenter에서 Dell 호스트를 클릭합니다.
3. Dell Host(Dell 호스트) 탭에서 다음과 같은 정보를 볼 수 있습니다.

호스트 이름	각 Dell 호스트의 IP 주소를 사용하여 링크를 표시합니다. Dell 호스트 정보를 보려면 특정 호스트 링크를 클릭합니다.
vCenter	이 Dell 호스트의 vCenter IP 주소를 표시합니다.
Cluster(클러스터)	이 Dell 호스트가 클러스터에 있으면 클러스터 이름이 표시됩니다.
Connection Profile(연결 프로필)	연결 프로필의 이름을 표시합니다.

27

클러스터 및 데이터센터에서 호스트 모니터링

OpenManage Integration for VMware vCenter을 사용하면 데이터센터 또는 클러스터에 포함된 모든 호스트에 대한 세부정보를 볼 수 있습니다. 이러한 페이지에서는 데이터 그리드 행 머리글을 클릭하여 데이터를 정렬할 수 있습니다. 데이터센터 및 클러스터 페이지에서는 정보를 CSV 파일로 내보낼 수 있으며, 데이터 그리드에 필터/검색 기능을 제공합니다. 세부정보는 다음과 같습니다.

- 호스트 개요 세부정보 보기
- 하드웨어: FRU 보기
- 하드웨어: 프로세서 세부정보 보기
- 하드웨어: 전원 공급 장치 세부정보 보기
- 하드웨어: 메모리 세부정보 보기
- 하드웨어: NIC 보기
- 하드웨어: PCI 슬롯 세부정보 보기
- 하드웨어: 원격 액세스 카드 세부정보 보기
- 스토리지: 실제 디스크 세부정보 보기
- 스토리지: 가상 디스크 세부정보 보기
- 펌웨어 세부정보 보기
- 전원 모니터링 보기
- 보증 요약 세부정보 보기

28

데이터센터 및 클러스터에 대한 개요 세부정보 보기

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

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

1. VMware vCenter의 Navigator(탐색 창)에서 **vCenter**를 클릭합니다.
2. **Datacenters(데이터센터)** 또는 **Clusters(클러스터)**를 클릭합니다.
3. Objects(개체) 탭에서, 호스트 세부정보를 확인할 특정 데이터센터 또는 클러스터를 선택합니다.
4. Monitor(모니터) 탭에서 **Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보)** > **Overview(개요)**탭을 선택하고 다음과 같은 세부정보를 봅니다.

   노트: 전체 세부정보 목록을 표시하려면 데이터 그리드에서 특정 호스트를 선택하십시오.

데이터센터/클러스터 정보	다음을 표시합니다. • 데이터센터/클러스터 이름 • Dell 관리 호스트 수 • 총 에너지 소비량 이 링크를 클릭하면 이 데이터센터 또는 클러스터에 대한 Power Monitoring(전력 모니터링) 페이지로 이동됩니다.
하드웨어 리소스	다음을 표시합니다. • 총 프로세서 수 이 링크를 클릭하면 Processor Details(프로세서 세부정보) 페이지로 이동됩니다. • Total Memory(총 메모리) 이 링크를 클릭하면 이 데이터센터 또는 클러스터에 대한 Memory Details(메모리 세부정보) 페이지로 이동됩니다. • 가상 디스크 용량 이 링크를 클릭하면 이 데이터센터 또는 클러스터에 대한 Virtual Disk(가상 디스크) 페이지로 이동됩니다.
Warranty Summary(보증 요약)	선택한 호스트의 보증 상태를 표시합니다. 상태 옵션은 다음과 같습니다. • Expired warranty(만료된 보증) • Active warranty(활성 보증) • Unknown warranty(알 수 없는 보증) 이 링크를 클릭하면 Warranty Summary(보증 요약) 페이지로 이동됩니다.
호스트	호스트 이름을 표시합니다.
Service Tag(서비스 태그)	호스트 서비스 태그를 표시합니다.
Model(모델)	Dell PowerEdge 모델을 표시합니다.
Asset Tag(자산 태그)	구성된 경우 자산 태그를 표시합니다.

Chassis Service Tag(섀시 서비스 태그)	섀시 서비스 태그를 표시합니다(해당되는 경우).
OS Version(OS 버전)	ESXi OS 버전을 표시합니다.
Location(위치)	블레이드에만 해당: 위치에 슬롯 위치가 표시됩니다. 그렇지 않으면 위치에 “Not Applicable(적용할 수 없음)”이 표시됩니다.
iDRAC IP	iDRAC IP 주소를 표시합니다.
Service Console IP(서비스 콘솔 IP)	서비스 콘솔 IP를 표시합니다.
CMC URL	블레이드에만 해당: CMC URL은 섀시 URL입니다. 그렇지 않으면 “Not Applicable(적용할 수 없음)”이 표시됩니다.
CPU	CPU 수를 표시합니다.
메모리	호스트 메모리를 표시합니다.
Power State(전원 상태)	호스트의 전원 상태를 표시합니다.
Last Inventory(마지막 인벤토리)	마지막 인벤토리 작업의 요일, 날짜 및 시간을 표시합니다.
Connection Profile(연결 프로필)	연결 프로필의 이름을 표시합니다.
Remote Access Card Version(원격 액세스 카드 버전)	원격 액세스 카드 버전을 표시합니다.
BIOS Firmware Version(BIOS 펌웨어 버전)	BIOS 펌웨어 버전을 표시합니다.

29

데이터센터 또는 클러스터에 대한 하드웨어: FRU 보기

Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보) 탭에서 데이터센터 또는 클러스터에 대한 현장 교체 가능 부품(FRU) 세부정보를 봅니다. 이 페이지에 정보를 표시하려면 인벤토리 작업을 실행합니다. 데이터센터 및 클러스터 페이지에서는 정보를 CSV 파일로 내보낼 수 있으며, 데이터 그리드에 필터/검색 기능을 제공합니다. 표시되는 데이터는 데이터에 액세스하는 보기에 따라 다를 수 있습니다. 하드웨어 보기에서는 OMSA 및 iDRAC의 데이터를 직접 보고합니다. 지금 인벤토리 작업 실행을 참조하십시오.

1. VMware vCenter의 Navigator(탐색 창)에서 **vCenter**를 클릭합니다.
2. **Datacenters(데이터센터)** 또는 **Clusters(클러스터)**를 클릭합니다.
3. Object(개체) 탭에서 하드웨어: FRU 세부정보를 확인할 특정 데이터센터 또는 클러스터를 선택합니다.
4. Monitor(모니터) 탭에서 **Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보)** 탭을 선택하고 **Hardware: FRU(하드웨어: FRU)** 하위 탭에서 다음을 확인합니다.

Host(호스트)	호스트 이름을 표시합니다.
Service Tag(서비스 태그)	서비스 태그를 표시합니다.
Part Name(부품명)	FRU 부품명을 표시합니다.
Part Number(부품 번호)	FRU 부품 번호를 표시합니다.
Manufacturer(제조업체)	제조업체 이름을 표시합니다.
Serial Number(일련 번호)	제조업체의 일련 번호를 표시합니다.
Manufacture Date(제조일자)	제조일자를 표시합니다.

30

데이터센터 및 클러스터에 대한 하드웨어: 프로세스 세부정보 보기

Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보) 탭에서 데이터센터 또는 클러스터에 대한 프로세서 세부정보를 봅니다. 이 페이지에 정보를 표시하려면 인벤토리 작업을 실행해야 합니다. 데이터센터 및 클러스터 페이지에서는 정보를 CSV 파일로 내보낼 수 있으며, 데이터 그리드에 필터/검색 기능을 제공합니다. 하드웨어 보기에서는 OMSA 및 iDRAC의 데이터를 직접 보고합니다. 지금 인벤토리 작업 실행을 참조하십시오.

1. VMware vCenter의 Navigator(탐색 창)에서 **vCenter**를 클릭합니다.
2. **Datacenters(데이터센터)** 또는 **Clusters(클러스터)**를 클릭합니다.
3. Datacenter(데이터센터) 또는 Cluster(클러스터) 탭에서 프로세서 세부정보를 확인할 특정 데이터센터 또는 클러스터를 선택합니다.
4. Monitor(모니터) 탭에서, **Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보)** 탭을 선택하고 Hardware: Processor(하드웨어: 프로세서) 하위 탭에서 다음을 확인합니다.

호스트	호스트 이름을 표시합니다.
서비스 태그	서비스 태그를 표시합니다.
Socket(소켓)	슬롯 번호를 표시합니다.
Speed(속도)	현재 속도를 표시합니다.
Brand(브랜드)	프로세서 브랜드를 표시합니다.
Version(버전)	프로세서 버전을 표시합니다.
Cores(코어)	이 프로세서의 코어 수를 표시합니다.

31

데이터센터 및 클러스터에 대한 하드웨어: 전원 공급 장치 세부정보 보기

Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보) 탭에서 데이터센터 또는 클러스터에 대한 가상 전원 공급 장치 세부정보를 봅니다. 이 페이지에 정보를 표시하려면 인벤토리 작업을 실행해야 합니다. 데이터센터 및 클러스터 페이지에서는 정보를 CSV 파일로 내보낼 수 있으며, 데이터 그리드에 필터/검색 기능을 제공합니다. 하드웨어 보기에서는 OMSA 및 iDRAC의 데이터를 직접 보고합니다. 지금 인벤토리 작업 실행을 참조하십시오.

1. VMware vCenter의 Navigator(탐색 창)에서 **vCenter**를 클릭합니다.
2. **Datacenters(데이터센터)** 또는 **Clusters(클러스터)**를 클릭합니다.
3. Objects(개체) 탭에서 하드웨어: 전원 공급 장치 세부정보를 확인할 특정 데이터센터 또는 클러스터를 선택합니다.
4. Monitor(모니터) 탭에서 **Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보)** 탭을 선택하고 **Hardware: Power Supply(하드웨어: 전원 공급 장치)** 하위 탭에서 다음을 확인합니다.

Host(호스트)	호스트의 이름을 표시합니다.
Service Tag(서비스 태그)	서비스 태그를 표시합니다.
Type(종류)	전원 공급 장치의 종류를 표시합니다. 전원 공급 장치 종류는 다음과 같습니다. • UNKNOWN(알 수 없음) • LINEAR(선형) • SWITCHING(스위칭) • BATTERY(배터리) • UPS • CONVERTER(변환기) • REGULATOR(조절기) • AC • DC • VRM
Location(위치)	전원 공급 장치의 위치를 표시합니다(예: 슬롯 1).
Output(출력)(와트)	와트 단위로 전원을 표시합니다.
Status(상태)	전원 공급 장치의 상태를 표시합니다. 상태 옵션은 다음과 같습니다. • OTHER(기타) • UNKNOWN(알 수 없음) • OK(양호) • CRITICAL(위험) • NOT CRITICAL(위험하지 않음) • RECOVERABLE(복구 가능) • NOT RECOVERABLE(복구 불가능) • HIGH(높음) • LOW(낮음)

32

데이터센터 및 클러스터에 대한 하드웨어: 메모리 세부정보 보기

Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보) 탭에서 데이터센터 또는 클러스터에 대한 메모리 세부정보를 봅니다. 이 페이지에 정보를 표시하려면 인벤토리 작업을 실행해야 합니다. 데이터센터 및 클러스터 페이지에서는 정보를 CSV 파일로 내보낼 수 있으며, 데이터 그리드에 필터/검색 기능을 제공합니다. 하드웨어 보기에서는 OMSA 및 iDRAC의 데이터를 직접 보고합니다. 지금 인벤토리 작업 실행을 참조하십시오.

1. VMware vSphere 웹 클라이언트의 Navigator(탐색 창) 영역에서 **vCenter Inventory Lists(vCenter 인벤토리 목록)**를 클릭합니다.
2. **Datacenters(데이터센터)** 또는 **Clusters(클러스터)**를 클릭합니다.
3. **Objects(개체)** 탭에서 하드웨어: 메모리 세부정보를 확인할 특정 데이터센터 또는 클러스터를 선택합니다.
4. **Monitor(모니터)** 탭에서 **Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보)** 탭을 선택하고 **Hardware(하드웨어)** > **Memory(메모리)** 하위 탭에서 다음과 같은 정보를 확인합니다.

호스트	호스트 이름을 표시합니다.
서비스 태그	서비스 태그를 표시합니다.
Slot(슬롯)	DIMM 슬롯을 표시합니다.
Size(크기)	메모리 크기를 표시합니다.
Type(유형)	메모리의 종류를 표시합니다.

33

데이터센터 및 클러스터에 대한 하드웨어: NIC 세부정보 보기

Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보) 탭에서 데이터센터 또는 클러스터에 대한 네트워크 인터페이스 카드(NIC) 세부정보를 봅니다. 이 페이지에 정보를 표시하려면 인벤토리 작업을 실행해야 합니다. 데이터센터 및 클러스터 페이지에서는 정보를 CSV 파일로 내보낼 수 있으며, 데이터 그리드에 필터/검색 기능을 제공합니다. 하드웨어 보기에서는 OMSA 및 iDRAC의 데이터를 직접 보고합니다. 지금 인벤토리 작업 실행을 참조하십시오.

1. VMware vSphere 웹 클라이언트의 Navigator(탐색 창) 영역에서 **vCenter Inventory Lists(vCenter 인벤토리 목록)**를 클릭합니다.
2. **Datacenters(데이터센터)** 또는 **Clusters(클러스터)**를 클릭합니다.
3. **Objects(개체)** 탭에서, 하드웨어 관련 NIC 세부정보를 확인할 특정 데이터센터 또는 클러스터를 클릭합니다.
4. **Monitor(모니터)** 탭에서 **Dell Datacenter/Clusters Information(Dell 데이터센터/클러스터 정보)**을 클릭하고**Hardware(하드웨어)** > **NIC**를 클릭하여 다음과 같은 정보를 확인합니다.

호스트	호스트 이름을 표시합니다.
서비스 태그	서비스 태그를 표시합니다.
이름	제품 이름을 표시합니다.
Manufacturer(제조업체)	제조업체의 이름만 표시합니다.
MAC Address(MAC 주소)	NIC MAC 주소를 표시합니다.

34

데이터센터 및 클러스터에 대한 하드웨어: PCI 슬롯 세부정보 보기

Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보) 탭에서 데이터센터 또는 클러스터에 대한 PCI 슬롯 세부정보를 봅니다. 이 페이지에 정보를 표시하려면 인벤토리 작업을 실행해야 합니다. 데이터센터 및 클러스터 페이지에서는 정보를 CSV 파일로 내보낼 수 있으며, 데이터 그리드에 필터/검색 기능을 제공합니다. 하드웨어 보기에서는 OMSA 및 iDRAC의 데이터를 직접 보고합니다. 지금 인벤토리 작업 실행을 참조하십시오.

1. VMware vSphere 웹 클라이언트의 Navigator(탐색 창) 영역에서 **vCenter Inventory Lists(vCenter 인벤토리 목록)**를 클릭합니다.
2. **Datacenters(데이터센터)** 또는 **Clusters(클러스터)**를 클릭합니다.
3. **Objects(개체)** 탭에서 특정 데이터센터 또는 클러스터를 클릭합니다.
4. **Monitor(모니터)** 탭에서 **Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보)** 탭을 선택하고**Hardware(하드웨어)** > **PCI Slots(PCI 슬롯):** 를 클릭하여 다음과 같은 정보를 확인합니다.

호스트	호스트 이름을 표시합니다.
서비스 태그	서비스 태그를 표시합니다.
Slot(슬롯)	슬롯을 표시합니다.
Manufacturer(제조업체)	PCI 슬롯의 제조업체 이름을 표시합니다.
설명	PCI 장치에 대한 설명을 표시합니다.
Type(유형)	PCI 슬롯 종류를 표시합니다.
폭	데이터 버스 너비를 표시합니다(사용 가능한 경우).

35

하드웨어: 원격 액세스 카드 세부정보 보기

Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보) 탭에서 데이터센터 또는 클러스터에 대한 원격 액세스 카드 세부 정보를 봅니다. 이 페이지에 정보를 표시하려면 인벤토리 작업을 실행해야 합니다. 데이터센터 및 클러스터 페이지에서는 정보를 CSV 파일로 내보낼 수 있으며, 데이터 그리드에 필터/검색 기능을 제공합니다. 하드웨어 보기에서는 OMSA 및 iDRAC의 데이터를 직접 보고합니다. 지금 인벤토리 작업 실행을 참조하십시오.

1. VMware vSphere 웹 클라이언트의 Navigator(탐색 창) 영역에서 **vCenter Inventory Lists(vCenter 인벤토리 목록)**를 클릭합니다.
2. **Datacenters(데이터센터)** 또는 **Clusters(클러스터)**를 클릭합니다.
3. **Objects(개체)** 탭에서 특정 데이터센터 또는 클러스터를 클릭합니다.
4. **Monitor(모니터)** 탭에서 **Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보)** 탭을 클릭하고 **Hardware(하드웨어)** > **Remote Access Card(원격 액세스 카드)**를 클릭하여 다음과 같은 정보를 확인합니다.

호스트	호스트 이름을 표시합니다.
서비스 태그	서비스 태그를 표시합니다.
IP Address(IP 주소)	원격 액세스 카드의 IP 주소를 표시합니다.
Mac Address(MAC 주소)	원격 액세스 카드의 MAC 주소를 표시합니다.
RAC Type(RAC 유형)	원격 액세스 카드의 종류를 표시합니다.
URL	이 호스트와 연관된 iDRAC의 라이브 URL을 표시합니다.

36

데이터센터 및 클러스터에 대한 스토리지: 실제 디스크 보기

Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보) 탭에서 데이터센터 또는 클러스터에 대한 실제 스토리지 세부정보를 봅니다. 이 페이지에 정보를 표시하려면 인벤토리 작업을 실행해야 합니다. 데이터센터 및 클러스터 페이지에서는 정보를 CSV 파일로 내보낼 수 있으며, 데이터 그리드에 필터/검색 기능을 제공합니다. 지금 인벤토리 작업 실행을 참조하십시오.

노트: 하드웨어 보기는 OMSA 및 iDRAC에서 데이터를 직접 보고합니다.

1. VMware vSphere 웹 클라이언트의 Navigator(탐색 창)에서 **vCenter Inventory Lists(vCenter 인벤토리 목록)**를 클릭합니다.
2. **Datacenters(데이터센터)** 또는 **Clusters(클러스터)**를 클릭합니다.
3. **Objects(개체)** 탭에서 특정 데이터센터 또는 클러스터를 선택합니다.
4. **Monitor(모니터)** 탭에서 **Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보)** 탭을 클릭하고 **Storage(스토리지)** > **Physical Disk(실제 디스크)**를 클릭하여 다음과 같은 정보를 확인합니다.

   노트: 전체 세부정보 목록을 표시하려면 데이터 그리드에서 특정 호스트를 선택하십시오.

호스트	호스트의 이름을 표시합니다.
서비스 태그	서비스 태그를 표시합니다.
Capacity(용량)	실제 디스크의 용량을 표시합니다.
Disk Status(디스크 상태)	실제 디스크의 상태를 표시합니다. 다음과 같은 옵션을 사용할 수 있습니다. • ONLINE(온라인) • READY(준비 완료) • DEGRADED(저하됨) • FAILED(장애) • OFFLINE(오프라인) • REBUILDING(재구축 중) • INCOMPATIBLE(호환되지 않음) • REMOVED(제거됨) • CLEARED(지워짐) • SMART ALERT DETECTED(스마트 경고 감지됨) • UNKNOWN(알 수 없음) • FOREIGN(외부) • UNSUPPORTED(지원되지 않음) **노트:** 이러한 경고가 나타내는 의미에 대해서는 *OpenManage™ Server Administrator 스토리지 관리 사용 설명서*(http://support.dell.com/support/edocs/software/svradmin/5.1/en/omss_ug/html/adprin.html)를 참조하십시오.
Model Number(모델 번호)	실제 스토리지 디스크의 모델 번호를 표시합니다.
호스트	호스트 이름을 표시합니다.
Last Inventory(마지막 인벤토리)	마지막으로 인벤토리가 실행된 월, 일, 시간을 표시합니다.
Status(상태)	호스트 상태를 표시합니다.

Controller ID(컨트롤러 ID)	컨트롤러 ID를 표시합니다.
Connector ID(커넥터 ID)	커넥터 ID를 표시합니다.
Enclosure ID(인클로저 ID)	인클로저 ID를 표시합니다.
Device ID(장치 ID)	장치 ID를 표시합니다.
Bus Protocol(버스 프로토콜)	버스 프로토콜을 표시합니다.
Hot Spare Type(핫 스페어 종류)	핫 스페어 종류를 표시합니다. 다음과 같은 옵션을 사용할 수 있습니다. ● 아니오 핫 스페어가 없음을 의미합니다. ● Global(전역) 전역 핫 스페어는 디스크 그룹에 속하는 사용되지 않은 백업 디스크입니다. ● Dedicated(전용) 전용 핫 스페어는 단일 가상 디스크에 할당된 사용되지 않은 백업 디스크입니다. 가상 디스크에서 실제 디스크에 장애가 발생할 경우, 시스템 중단이나 사용자 개입이 없어도 이 핫 스페어가 활성화되어 장애가 발행한 실제 디스크를 대체합니다.
부품 번호	스토리지 부품 번호를 표시합니다.
Serial Number(일련번호)	스토리지 일련 번호를 표시합니다.
Vendor Name(벤더 이름)	스토리지 벤더 이름을 표시합니다.

37

데이터센터 및 클러스터에 대한 스토리지: 가상 디스크 세부정보 보기

Dell Datacenter/Cluster(Dell 데이터센터/클러스터) 탭에서 데이터센터 또는 클러스터에 대한 가상 스토리지 세부정보를 봅니다. 이 페이지에 정보를 표시하려면 인벤토리 작업을 실행해야 합니다. 표시되는 데이터는 데이터에 액세스하는 보기에 따라 다릅니다. 하드웨어 보기에서는 OMSA 및 iDRAC의 데이터를 직접 보고합니다. 지금 인벤토리 작업 실행을 참조하십시오. 데이터센터 및 클러스터 페이지에서는 정보를 CSV 파일로 내보낼 수 있으며, 데이터 그리드에 필터/검색 기능을 제공합니다.

1. VMware vSphere 웹 클라이언트의 Navigator(탐색 창) 영역에서 **vCenter Inventory Lists(vCenter 인벤토리 목록)**를 클릭합니다.
2. **Datacenters(데이터센터)** 또는 **Clusters(클러스터)**를 클릭합니다.
3. **Objects(개체)** 탭에서 특정 데이터센터 또는 클러스터를 선택합니다.
4. **Monitor(모니터)** 탭에서 **Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보)** 탭을 클릭하고 **Storage(스토리지)** > **Virtual Disk(가상 디스크)**를 클릭하여 다음과 같은 정보를 확인합니다.

   노트: 전체 세부정보 목록을 표시하려면 데이터 그리드에서 특정 호스트를 선택하십시오.

호스트	호스트의 이름을 표시합니다.
서비스 태그	서비스 태그를 표시합니다.
이름	가상 디스크의 이름을 표시합니다.
Physical Disk(실제 디스크)	가상 디스크가 있는 실제 디스크를 표시합니다.
Capacity(용량)	가상 디스크의 용량을 표시합니다.
Layout(레이아웃)	가상 스토리지의 레이아웃 유형을 표시합니다. 이 가상 디스크에 구성된 RAID 유형을 의미합니다.
호스트	호스트 이름을 표시합니다.
이름	가상 디스크의 이름을 표시합니다.
Last Inventory(마지막 인벤토리)	인벤토리가 마지막으로 실행된 요일, 날짜 및 시간을 표시합니다.
Controller ID(컨트롤러 ID)	컨트롤러 ID를 표시합니다.
Device ID(장치 ID)	장치 ID를 표시합니다.
Media Type(매체 종류)	SSD 또는 HDD를 표시합니다.
Bus Protocol(버스 프로토콜)	가상 디스크에 포함된 실제 디스크가 사용하는 기술을 표시합니다. 값은 다음과 같습니다. • SCSI • SAS • SATA
Stripe Size(스트라이프 크기)	스트라이프 크기는 단일 디스크에서 각 스트라이프가 사용하는 공간의 양을 의미합니다.
Default Read Policy(기본 읽기 정책)	컨트롤러에서 지원되는 기본 읽기 정책으로서 다음과 같은 옵션을 사용할 수 있습니다. • Read-Ahead(미리 읽기) • No-Read-Ahead(미리 읽기 없음) • Adaptive Read-Ahead(적응성 미리 읽기) • Read Cache Enabled(읽기 캐시 활성 상태)

	• Read Cache Disabled(읽기 캐시 비활성 상태)
Default Write Policy(기본 쓰기 정책)	컨트롤러에서 지원되는 기본 쓰기 정책으로서 다음과 같은 옵션을 사용할 수 있습니다. • Write-Back(후기입) • Force Write Back(강제 후기입) • Write Back Enabled(후기입 활성 상태) • Write-Through(연속 기입) • Write Cache Enabled Protected(쓰기 캐시 활성 상태 보호) • Write Cache Disabled(쓰기 캐시 비활성 상태)
Disk Cache Policy(디스크 캐시 정책)	컨트롤러에서 지원되는 기본 캐시 정책으로서 다음과 같은 옵션을 사용할 수 있습니다. • 활성화 캐시 I/O를 의미합니다. • 비활성 상태 직접 I/O를 의미합니다.

38

데이터센터 및 클러스터에 대한 펌웨어 세부정보 보기

Dell Host(Dell 호스트) 탭에서 데이터센터 또는 클러스터에 대한 펌웨어 세부정보를 봅니다. 이 페이지에 정보를 표시하려면 인벤토리 작업을 실행해야 합니다. 데이터센터 및 클러스터 페이지에서는 정보를 CSV 파일로 내보낼 수 있으며, 데이터 그리드에 필터/검색 기능을 제공합니다. 하드웨어 보기에서는 OMSA 및 iDRAC의 데이터를 직접 보고합니다. 지금 인벤토리 작업 실행을 참조하십시오.

1. VMware vSphere 웹 클라이언트의 Navigator(탐색 창)에서 **vCenter**를 클릭합니다.
2. **Datacenters(데이터센터)** 또는 **Clusters(클러스터)**를 클릭합니다.
3. Objects(개체) 탭에서 펌웨어 세부정보를 확인할 특정 데이터센터 또는 클러스터를 선택합니다.
4. Monitor(모니터) 탭에서 **Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보)** 탭을 선택하고 Firmware(펌웨어) 하위 탭에서 다음을 확인합니다.

호스트	호스트의 이름을 표시합니다.
서비스 태그	서비스 태그를 표시합니다.
이름	이 호스트에 있는 모든 펌웨어의 이름을 표시합니다.
Version(버전)	이 호스트에 있는 모든 펌웨어의 버전을 표시합니다.

39

데이터센터 및 클러스터에 대한 보증 요약 세부정보 보기

보증 요약을 보려면 보증 작업을 실행해야 합니다. 지금 보증 작업 실행을 참조하십시오.

Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보) 탭에서 데이터센터 또는 클러스터에 대한 보증 요약 세부정보를 봅니다. 데이터센터 및 클러스터 페이지에서는 정보를 파일로 내보낼 수 있으며, 데이터 그리드에 필터/검색 기능을 제공합니다. 보증 요약 페이지에서는 보증 만료 날짜를 모니터링할 수 있습니다. 보증 설정은 보증 일정을 활성화하거나 비활성화한 후 최소 일 수 임계값 경고를 설정하여 Dell에서 온라인으로 서버 보증 정보를 가져오는 경우를 제어합니다. 보증 내역을 참조하십시오.

1. VMware vSphere 웹 클라이언트의 Navigator(탐색 창)에서 **vCenter**를 클릭합니다.
2. **Datacenters(데이터센터)** 또는 **Clusters(클러스터)**를 클릭합니다.
3. Objects(개체) 탭에서 보증 요약 세부정보를 확인할 특정 데이터센터 또는 클러스터를 선택합니다.
4. Monitor(모니터) 탭에서 **Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보)** 탭을 선택하고 Warranty Summary(보증 요약) 하위 탭에서 다음을 확인합니다.

Warranty Summary(보증 요약)	호스트 보증 요약은 각 상태 카테고리에서 호스트 수를 시각적으로 표시하는 아이콘을 사용하여 표시됩니다.
호스트	호스트의 이름을 표시합니다.
서비스 태그	호스트의 서비스 태그를 표시합니다.
설명	설명을 표시합니다.
Warranty Status(보증 상태)	호스트의 보증 상태를 표시합니다. 상태 옵션은 다음과 같습니다. • Active(활성) 호스트에 보증이 적용되며 임계값을 초과하지 않았습니다. • 경고 호스트가 활성 상태이지만 경고 임계값을 초과했습니다. • Critical(위험) 경고와 동일하지만 위험 임계값입니다. • Expired(만료됨) 이 호스트의 보증이 만료되었습니다. • Unknown(알 수 없음) 보증 작업이 실행되지 않았거나, 데이터를 가져오는 중에 오류가 발생했거나, 시스템에 보증이 없기 때문에 OpenManage Integration for VMware vCenter가 보증 상태를 가져올 수 없습니다.
Days Left(남은 일 수)	보증의 남은 일 수를 표시합니다.

40

데이터센터 및 클러스터에 대한 전원 모니터링 보기

Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보) 탭에서 데이터센터 또는 클러스터에 대한 전원 모니터링 세부정보를 봅니다. 이 페이지에 정보를 표시하려면 인벤토리 작업을 실행해야 합니다. 데이터센터 및 클러스터 페이지에서는 정보를 CSV 파일로 내보낼 수 있으며, 데이터 그리드에 필터/검색 기능을 제공합니다. 하드웨어 보기에서는 OMSA 및 iDRAC의 데이터를 직접 보고합니다. 지금 인벤토리 작업 실행을 참조하십시오.

1. VMware vSphere 웹 클라이언트의 Navigator(탐색 창)에서 **vCenter**를 클릭합니다.
2. **Datacenters(데이터센터)** 또는 **Clusters(클러스터)**를 클릭합니다.
3. Objects(개체) 탭에서 전원 모니터링 세부정보를 확인할 특정 데이터센터 또는 클러스터를 선택합니다.
4. Monitor(모니터) 탭에서 **Dell Datacenter/Cluster Information(Dell 데이터센터/클러스터 정보)** 탭을 선택하고 Power Monitoring(전원 모니터링) 하위 탭에서 다음을 확인합니다.

   노트: 전체 세부정보 목록을 표시하려면 데이터 그리드에서 특정 호스트를 선택하십시오.

호스트	호스트의 이름을 표시합니다.
서비스 태그	서비스 태그를 표시합니다.
Current Profile(현재 프로필)	시스템 성능을 최대화하고 에너지를 절약할 수 있도록 전원 프로필을 표시합니다.
Energy Consumption(에너지 사용)	호스트의 에너지 사용을 표시합니다.
Peak Reserve Capacity(최고 예비 용량)	최고 전원 예비 용량을 표시합니다.
Power Budget(전원 할당량)	이 호스트의 전원 용량을 표시합니다.
Warning Threshold(경고 임계값)	시스템에 구성된 온도 프로브 경고 임계값의 최대값을 표시합니다.
Failure Threshold(장애 임계값)	시스템에 구성된 온도 프로브 장애 임계값의 최대값을 표시합니다.
Instant Reserve Capacity(순간 예비 용량)	호스트의 순간 헤드룸 용량을 표시합니다.
Energy Consumption Start Date(에너지 사용 시작 날짜)	호스트가 전원 사용을 시작한 날짜 및 시간을 표시합니다.
Energy Consumption End Date(에너지 사용 종료 날짜)	호스트가 전원 사용을 중지한 날짜 및 시간을 표시합니다.
System Peak Power(시스템 최고 전원)	호스트의 최고 전원을 표시합니다.
System Peak Power Start Date(시스템 최고 전원 시작 날짜)	호스트의 최고 전원이 시작된 날짜 및 시간을 표시합니다.
System Peak Power End Date(시스템 최고 전원 종료 날짜)	호스트의 최고 전원이 종료된 날짜 및 시간을 표시합니다.

System Peak Amps(시스템 최고 암페어)	호스트의 최고 암페어를 표시합니다.
System Peak Amps Start Date(시스템 최고 암페어 시작 날짜)	호스트의 최고 암페어 시작 날짜 및 시간을 표시합니다.
System Peak Amps End Date(시스템 최고 암페어 종료 날짜)	호스트의 최고 암페어 종료 날짜 및 시간을 표시합니다.

41

문제 해결

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

- FAQ(자주 묻는 질문)
- Dell에 문의하기 페이지 122
- 관련 제품 정보

주제:

FAQ(자주 묻는 질문)

이 섹션에는 몇 가지 일반적인 질문과 해결 방법이 포함되어 있습니다.

OMIVV가 자동 검색 프로세스 중에 프로비저닝 서버로 작동할 수 없음

새로 추가된 Dell 서버의 iDRAC 설정에서 OMIVV IP 주소가 프로비저닝 서버로 사용되면 이 Dell 서버는 자동으로 검색되지 않습니다. OMIVV 3.2는 MD5로 암호화된 SSL 인증서 서명을 지원하지 않기 때문에 보다 안전한 암호화를 위해 자동 검색 프로세스가 실패합니다.

해결 방법: 없음

OSD 이후 처음에 간헐적인 인벤토리 오류 발생

간헐적인 인벤토리 실패 이후 첫 배포의 경우, 사용자에게 "No inventory record found for the host <IP / Host name>(호스트 <IP/호스트 이름>에 대한 인벤토리 레코드가 없습니다.)"라는 오류가 표시될 수 있습니다.

해결 방법: 인벤토리를 수동으로 실행하여 간헐적인 인벤토리 실패 이후 첫 OSD를 해결할 수 있습니다.

OSD가 성공하면 연결 프로필 페이지의 iDRAC용 테스트 연결이 DNC에서 실패합니다.

OS 배포 후 iDRAC에 대한 즉각적인 테스트 연결이 실패하고 연결 프로필 페이지에 "Fail - Unable to connect to iDRAC(실패 - iDRAC에 연결할 수 없습니다)"라는 오류가 표시됩니다.

해결 방법: BMC가 IP 주소를 확보할 수 없으므로 이 오류가 발생합니다. 이 문제를 해결하려면 관리 네트워크를 다시 시작해야 합니다. 문제가 지속되는 경우 사용자가 ESXi 호스트를 다시 시작해야 합니다.

OMIVV 어플라이언스를 등록하는 동안 할당된 Dell 권한은 OMIVV를 등록 취소한 후에 제거되지 않습니다.

OMIVV 어플라이언스로 vCenter를 등록하고 나면 여러 Dell 권한이 vCenter 권한 목록에 추가됩니다. OMIVV 어플라이언스에서 vCenter의 등록을 취소해도 Dell 권한은 제거되지 않습니다.

노트: Dell 권한은 제거되지 않지만 OMIVV 작업에 미치는 영향은 없습니다.

적용 버전: 3.1

Dell Management Center에서 심각도 범주를 필터링하려고 할 때 모든 관련 로그가 표시되지 않습니다. 어떻게 하면 모든 로그를 볼 수 있습니까?

드롭다운에서 **모든 범주**를 선택하여 로그 데이터를 필터링하기 위해 심각도 범주를 선택할 때 특정 범주에 속하는 모든 로그가 정확하게 표시되지 않습니다. 하지만 드롭다운에서 **정보**를 선택하여 필터링하는 경우에는 펌웨어 업데이트 로그가 표시되지 않고 작업 시작 로그만 표시됩니다.

해결 방법: Dell Management Center에서 모든 로그를 보려면 필터 드롭다운에서 **모든 범주**를 선택합니다.

적용 버전: 3.1

VMCA(VMware Certificate Authority)에서 발생시킨 오류 코드 2000000을 어떻게 해결합니까?

vSphere 인증서 관리자를 실행하고 vCenter Server 또는 플랫폼 서비스 컨트롤러(PSC) 인증서를 vCenter 6.0에 대한 새 CA 인증서 및 키로 교체하면 OMIVV에서 오류 코드 2000000을 표시하고 예외를 발생시킵니다.

해결 방법: 이 예외를 해결하려면 서비스에 대한 ssl 기준 위치를 업데이트해야 합니다. ssl 기준 위치는 PSC에서 `ls_update_certs.py` 스크립트를 실행하여 업데이트할 수 있습니다. 이 스크립트는 기존 인증서 엄지손가락 지문을 입력 인수로 받으며 새 인증서가 설치됩니다. 기존 인증서는 교체 전의 인증서이고 새 인증서는 교체 후의 인증서입니다. 자세한 내용은 http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701 및 http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121689을(를) 참조하십시오.

Windows vSphere 6.0에서 ssl 기준 위치 업데이트

1. http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701에서 lstoolutil.py.zip 파일을 다운로드합니다.
2. lstoolutil.py 파일을 `%VMWARE_CIS_HOME%"\VMware Identity Services\lstool\scripts\` 폴더에 복사합니다.

   노트: vSphere 6.0 업데이트 1을 사용하는 경우에는 lstoolutil.py 파일을 교체하지 마십시오.

다음과 같은 관련 절차를 사용하여 ssl 기준 위치를 업데이트할 수 있습니다.

- Windows 운영 체제에 설치된 vCenter에 대한 ssl 기준 위치를 업데이트하는 경우: vSphere 인증서 관리자 유틸리티를 사용하여 vCenter Windows 설치의 인증서를 교체합니다. vCenter Windows 설치 시 인증서 바꾸기 페이지 108을(를) 참조하십시오.
- vCenter Server 어플라이언스에 대한 ssl 기준 위치를 업데이트하는 경우: vSphere 인증서 관리자 유틸리티를 사용하여 vCenter 서버 어플라이언스의 인증서를 교체합니다. vCenter 서버 어플라이언스에서 인증서 바꾸기 페이지 109을(를) 참조하십시오.

언급한 절차에서 나온 출력에 각각 `Updated 24 service (s)` 및 `Updated 26 service (s)`가 표시되어야 합니다. 표시된 출력이 `Updated 0 service (s)`이면 기존 인증서 엄지손가락 지문이 잘못된 것입니다. 다음과 같은 단계를 수행하여 기존 인증서 엄지손가락 지문을 검색할 수 있습니다. 또한 **vCenter 인증서 관리자**를 사용하여 인증서를 교체하지 않는 경우에는 다음과 같은 절차를 사용하여 기존 인증서를 검색할 수 있습니다.

노트: 획득한 기존 엄지손가락 지문을 사용하여 `ls_update_certs.py`를 실행합니다.

1. MOB(Managed Object Browser)에서 기존 인증서를 검색합니다. 관리되는 개체 브라우저(MOB)에서 기존 인증서 검색 페이지 110을(를) 참조하십시오.
2. 기존 인증서에서 엄지손가락 지문을 추출합니다. 기존 인증서에서 엄지손가락 지문 추출 페이지 111을(를) 참조하십시오.

적용 버전: 3.0 이상, vCenter 6.0 이상

vCenter Windows 설치 시 인증서 바꾸기

vCenter Windows 설치 시 vSphere Certificate Manager 유틸리티를 사용하여 인증서를 바꾸는 경우 다음 단계를 수행합니다.

1. 원격 데스크탑 연결을 통해 External Platform Services Controller에 연결합니다.
2. 관리자 모드로 명령 프롬프트를 엽니다.
3. `mkdir c:\certificates` 명령을 사용하여 `c:\certificates` 폴더를 만듭니다.
4. `"%VMWARE_CIS_HOME%"\vmafdd\vecs-cli entry getcert --store BACKUP_STORE --alias bkp___MACHINE_CERT --output c:\certificates\old_machine.crt` 명령을 사용하여 기존 인증서를 검색합니다.

5. "%VMWARE_OPENSSL_BIN%" x509 -in C:\certificates\old_machine.crt -noout -sha1 -fingerprint 명령을 사용하여 기존 인증서 엄지손가락 지문을 검색합니다.

   노트: 검색된 인증서 엄지손가락 지문은 SHA1 Fingerprint=13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 형식입니다.

   엄지손가락 지문은 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88처럼 나타나는 일련의 숫자와 알파벳입니다.

6. "%VMWARE_CIS_HOME%"\vmafdd\vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT --output c:\certificates\new_machine.crt 명령을 사용하여 새 인증서를 검색합니다.
7. 다음 단계를 수행합니다.
   a. 다음 명령을 사용하여 ls_update_certs.py를 실행합니다. "%VMWARE _PYTHON_BIN%" ls_update_certs.py --url
   b. https://psc.vmware.com/lookupservice/sdk --fingerprint 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 --certfile c:\certificates\new_machine.crt --user Administrator@vsphere.local --password Password 명령을 사용하여 psc.vmware.com을 Lookup_Service_FQDN_of_Platform_Services_Controller로 바꾸고 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 엄지손가락 지문을 5단계에서 구한 엄지손가락 지문으로 바꿉니다.

      노트: 반드시 유효한 자격 증명을 입력합니다.

8. 모든 서비스가 성공적으로 업데이트되면 vCenter 웹 클라이언트에서 로그아웃했다 다시 로그인합니다.

이제 OMIVV가 성공적으로 시작됩니다.

vCenter 서버 어플라이언스에서 인증서 바꾸기

vSphere Certificate Manager 유틸리티를 사용하여 vCenter 서버 어플라이언스의 인증서를 바꾸는 경우 다음 단계를 수행합니다.

1. 콘솔 또는 SSH(보안 셸) 세션을 통해 External Platform Services Controller 어플라이언스에 로그인합니다.
2. Bash 셸에 액세스하려면 shell.set --enabled true 명령을 실행합니다.
3. **shell**을 입력한 다음 **Enter** 키를 누릅니다.
4. mkdir /certificates 명령을 사용하여 폴더 또는 인증서를 만듭니다.
5. /usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store BACKUP_STORE --alias bkp___MACHINE_CERT --output /certificates/old_machine.crt 명령을 사용하여 기존 인증서를 검색합니다.
6. openssl x509 -in /certificates/old_machine.crt -noout -sha1 -fingerprint 명령을 사용하여 기존 인증서 엄지손가락 지문을 검색합니다.

   노트: 검색된 인증서 엄지손가락 지문은 SHA1 Fingerprint=13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 형식입니다.

   엄지손가락 지문은 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88처럼 나타나는 일련의 숫자와 알파벳입니다.

7. /usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT --output /certificates/new_machine.crt 명령을 사용하여 새 인증서를 검색합니다.
8. cd /usr/lib/vmidentity/tools/scripts/ 명령을 실행하여 디렉터리를 변경합니다.
9. 다음 단계를 수행합니다.
   a. 다음 명령을 사용하여 ls_update_certs.py를 실행합니다. python ls_update_certs.py --url
   b. https://psc.vmware.com/lookupservice/sdk --fingerprint 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 --certfile /certificates/new_machine.crt --user Administrator@vsphere.local --password "Password" 명령을 사용하여 psc.vmware.com을 Lookup_Service_FQDN_of_Platform_Services_Controller로 바꾸고 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 엄지손가락 지문을 6단계에서 구한 엄지손가락 지문으로 바꿉니다.

      노트: 반드시 유효한 자격 증명을 입력합니다.

10. 모든 서비스가 성공적으로 업데이트되면 vCenter 웹 클라이언트에서 로그아웃했다 다시 로그인합니다.

이제 OMIVV가 성공적으로 시작됩니다.

관리되는 개체 브라우저(MOB)에서 기존 인증서 검색

관리되는 개체 브라우저(MOB)를 사용하여 Platform Service Controller(PSC)에 연결하여 vCenter 서버 시스템을 위한 기존 인증서를 검색할 수 있습니다.

기존 인증서를 검색하려면 다음 단계를 수행하여 ArrayOfLookupServiceRegistrationInfo 관리되는 개체의 sslTrust 필드를 찾아야 합니다.

노트: 이 설명서에서는 `C:\certificates\` 폴더 위치가 모든 인증서를 저장하는 데 사용됩니다.

1. 다음 명령을 사용하여 PSC에 `C:\certificates\` 폴더를 생성합니다. `mkdir C:\certificates\`.
2. 브라우저에서 다음 링크를 엽니다. `https://<vCenter FQDN/IP address>/lookupservice/mob?moid=ServiceRegistration&method=List`
3. `administrator@vsphere.local` 사용자 이름을 사용하여 로그인하고 암호를 입력하라는 메시지가 나타나면 암호를 제공합니다.

   노트: vCenter SSO(Single Sign-On) 도메인의 사용자 지정 이름을 사용하는 경우 해당 사용자 이름과 암호를 사용합니다.

4. **filterCriteria**에서 값 필드를 수정하여 **<filtercriteria></filtercriteria>** 태그만 표시하고 **호출 방법**을 클릭합니다.
5. 대체하려는 인증서에 따라 다음 호스트 이름을 검색합니다.

표 6. 검색 기준 정보

신뢰하는 앵커	검색 기준
vCenter 서버	Ctrl+F 키를 사용하여 페이지에서 vc_hostname_or_IP.example.com 검색
플랫폼 서비스 컨트롤러	Ctrl+F 키를 사용하여 페이지에서 psc_hostname_or_IP.example.com 검색

6. 해당 sslTrust 필드의 값을 찾습니다. sslTrust 필드의 값은 기존 인증서의 Base64 인코딩된 문자열입니다.
7. Platform Services Controller 또는 vCenter 서버 신뢰하는 앵커를 업데이트할 때 다음 예제를 사용합니다.

   노트: 실제 문자열은 가독성을 개선하기 위해 많이 짧아집니다.

   - vCenter 서버의 경우

표 7. vCenter 서버 예

이름	Type(유형)	값
URL	anyURI	https://vcenter.vmware.local:443/sdk

   - Platform Services Controller의 경우

표 8. Platform Services Controller 예

이름	Type(유형)	값
URL	anyURI	https://psc.vmware.local/sts/STSService/vsphere.local

8. sslTrust 필드의 내용을 텍스트 문서에 복사하고 문서를 `old_machine.txt`로 저장합니다.
9. 텍스트 편집기에서 `old_machine.txt`를 엽니다.
10. `old_machine.txt` 파일 시작과 끝 부분에 각각 다음을 추가합니다.

    ```
    -----BEGIN CERTIFICATE-----
    -----END CERTIFICATE-----
    ```

11. 이제 `old_machine.txt`를 `old_machine.crt`로 저장합니다.

이제 이 인증서에서 지문을 추출할 수 있습니다.

기존 인증서에서 엄지손가락 지문 추출

다음과 같은 옵션을 사용하여 기존 인증서에서 엄지손가락 지문을 추출하고 플랫폼 서비스에 업로드할 수 있습니다.

- 인증서 뷰어 도구를 사용하여 엄지손가락 지문을 추출합니다. 인증서 뷰어 도구를 사용하여 인증서 엄지손가락 지문 추출 페이지 111을(를) 참조하십시오.
- 어플라이언스의 명령줄을 사용하여 엄지손가락 지문을 추출합니다. 명령줄을 사용하여 Thumbprint 추출 페이지 111을(를) 참조하십시오.

인증서 뷰어 도구를 사용하여 인증서 엄지손가락 지문 추출

다음 단계를 수행하여 인증서 엄지손가락 지문을 추출합니다.

1. Windows에서 `old_machine.txt` 파일을 두 번 클릭하여 Windows 인증서 뷰어에서 엽니다.
2. Windows 인증서 뷰어에서 **SHA1 엄지손가락 지문** 필드를 선택합니다.
3. 엄지손가락 지문 문자열을 일반 텍스트 편집기로 복사하고 공백을 콜론으로 바꾸거나 공백을 문자열에서 제거합니다.
   예를 들어 엄지손가락 지문 문자열은 다음 중의 하나로 나타날 수 있습니다.
   - ea87e150bb96fbbe1fa95a3c1d75b48c30db7971
   - ea:87:e1:50:bb:96:fb:be:1f:a9:5a:3c:1d:75:b4:8c:30:db:79:71

명령줄을 사용하여 Thumbprint 추출

어플라이언스와 Windows 설치 시 명령줄을 사용하여 thumbprint를 추출하는 방법은 다음 섹션을 참조하십시오.

vCenter 서버 어플라이언스에서 명령줄을 사용하여 thumbprint 추출

다음 단계를 수행합니다.

1. 기존 인증서 검색 절차의 1단계에서 만들어지는 `C:\certificates\old_machine.crt` 위치의 PSC로 old_machine.crt 인증서를 이동하거나 업로드합니다. WinSCP(Windows Secure Copy) 또는 다른 SCP 클라이언트를 사용하여 인증서를 이동하거나 업로드할 수 있습니다.
2. SSH(보안 셸)를 통해 External Platform Services Controller 어플라이언스에 로그인합니다.
3. `shell.set --enabled true` 명령을 실행하여 Bash 셸에 대한 액세스를 활성화합니다.
4. `shell`을 입력한 다음 **Enter** 키를 누릅니다.
5. `openssl x509 -in /certificates/old_machine.crt -noout -sha1 -fingerprint` 명령을 실행하여 엄지손가락 지문을 추출합니다.

노트: 엄지손가락 지문은 `SHA1 Fingerprint=ea:87:e1:50:bb:96:fb:be:1f:a9:5a:3c:1d:75:b4:8c:30:db:79:71`처럼 등호 부호 다음에 일련의 숫자와 문자로 표시됩니다.

Windows 설치 시 명령줄을 사용하여 thumbprint 추출

다음 단계를 수행합니다.

1. 기존 인증서 검색 절차의 1단계에서 만들어지는 `C:\certificates\old_machine.crt` 위치의 PSC로 old_machine.crt 인증서를 이동하거나 업로드합니다. WinSCP(Windows Secure Copy) 또는 다른 SCP 클라이언트를 사용하여 인증서를 이동하거나 업로드할 수 있습니다.
2. 원격 데스크탑 연결을 통해 External Platform Services Controller에 연결합니다.
3. 관리자 모드로 명령 프롬프트를 엽니다.
4. `"%VMWARE_OPENSSL_BIN%" x509 -in c:\certificates\old_machine.crt -noout -sha1 -fingerprint` 명령을 실행하여 엄지손가락 지문을 추출합니다.

노트: 엄지손가락 지문은 `SHA1 Fingerprint=09:0A:B7:53:7C:D9:D2:35:1B:4D:6D:B8:37:77:E8:2E:48:CD:12:1B`처럼 등호 부호 다음에 일련의 숫자와 문자로 표시됩니다.

기존 엄지손가락 지문으로 ls_update_certs.py를 실행합니다. 서비스가 성공적으로 업데이트되면 vCenter 웹 클라이언트에서 로그아웃했다 다시 로그인합니다. Dell 플러그인이 성공적으로 시작됩니다.

펌웨어 업데이트 마법사는 펌웨어 리포지토리에서 번들을 검색하지 않았다는 메시지를 표시합니다. 펌웨어 업데이트를 계속하려면 어떻게 합니까?

웹 클라이언트에서 단일 호스트에 대해 펌웨어 업데이트 마법사를 실행하면 **구성 요소 선택** 화면에 구성 요소에 대한 펌웨어 정보가 표시됩니다. 원하는 펌웨어 업데이트를 선택하고 **뒤로**를 두 번 클릭하여 **시작** 페이지를 표시한 후에 **다음**을 클릭하면 **업데이트 소스 선택** 화면에서 펌웨어 리포지토리에서 번들을 검색하지 않았다는 메시지가 표시됩니다.

해결 방법: 원하는 펌웨어 업데이트를 선택하고 **다음**을 클릭하여 펌웨어 업데이트를 계속할 수 있습니다.

적용 버전: 3.0 이상

클러스터 수준에서 30개 호스트의 펌웨어 업데이트 실패

VMware에서는 동일한 서버 하드웨어를 사용하여 클러스터를 구축하는 것이 좋습니다. 여러 가지 모델의 Dell 서버로 구성되었거나 VMware에서 클러스터에 권장되는 최대 개수에 근접한 개수의 호스트를 사용하여 클러스터 수준에서 펌웨어 업데이트를 수행하는 경우에는 vSpher 웹 클라이언트를 사용할 것을 권장합니다.

일부 vCenter에 대한 보증 및 인벤토리 일정을 "Dell 홈 > 모니터 > 작업 큐 > 보증/인벤토리 내역 > 일정" 아래에서 선택해도 표시되지 않습니다.

고객이 작업 대기열 페이지를 탐색하고 vCenter를 선택한 후 일정 수정 단추를 선택합니다. 대화 상자가 표시될 때 이 새 설정을 모든 등록된 vCenter에 적용하는 확인란이 표시됩니다. 이를 선택하고 적용을 누르면 모든 vCenter가 아닌 초기에 선택한 특정 vCenter에만 설정이 적용됩니다. 작업 대기열 페이지에서 보증 또는 인벤토리 일정이 수정되면 '모든 등록된 vCenter에 적용'을 적용할 수 없습니다.

해결 방법: 선택한 vCenter만 수정하려면 작업 대기열에서 보증 또는 인벤토리 일정을 사용하십시오.

적용 버전: 2.2 이상

OpenManage Integration for VMware vCenter에서 DNS 설정을 변경한 후 vCenter 웹 클라이언트에서 웹 통신 오류가 발생합니다.

DNS 설정을 변경한 후 OMIVV 관련 작업을 수행할 때 vCenter 웹 클라이언트에서 웹 통신 오류가 발생하는 경우에는, 브라우저 캐시를 지우거나 웹 클라이언트에서 로그아웃했다가 다시 로그인하십시오.

다른 페이지로 이동한 후 '설정' 페이지로 다시 이동하면 '설정' 페이지가 로드되지 않습니다.

vSphere v5.5의 경우, 웹 클라이언트에서는 다른 페이지로 이동한 후 '설정' 페이지로 다시 이동하면 페이지가 로드되지 않고 회전자가 계속해서 표시되는 경우가 있습니다. 이는 새로 고침 문제이며 페이지가 올바르게 새로 고쳐지지 않습니다.

해결 방법: 전역 새로 고침을 클릭하면 화면이 올바르게 새로 고쳐집니다.

적용 버전: 2.2 및 3.0

초기 구성 마법사의 인벤토리 일정/보증 일정 페이지에 "작업을 이전 시간으로 예약할 수 없음" 오류가 표시되는 이유는 무엇입니까?

웹 클라이언트에서는 사용자가 초기 구성 마법사에서 '모든 등록된 vCenter'를 선택하는 경우 및 일부 vCenter에 호스트가 없거나 일부에 인벤토리 또는 보증 작업이 이미 예약되어 있고 일부에 인벤토리 또는 보증 일정이 설정되어 있지 않은 vCenter가 있는 경우 사용자에게 "작업을 이전 시간으로 예약할 수 없음" 오류가 표시될 수도 있습니다.

해결 방법: 일부 vCenter에 호스트가 없거나 일부에 인벤토리 또는 보증 작업이 이미 예약되어 있고 일부에 인벤토리 또는 보증 일정이 설정되어 있지 않은 vCenter가 있는 경우 이러한 vCenter에 대한 설정 페이지에서 인벤토리 및 보증 일정의 설정을 각각 다시 실행하십시오.

적용 버전: 2.2 이상

펌웨어 페이지에서 일부 펌웨어에 대해 설치 날짜가 12/31/1969로 표시되는 이유는 무엇입니까?

웹 클라이언트에서는 호스트의 펌웨어 페이지에 일부 펌웨어에 대한 설치 날짜가 12/31/1969로 표시됩니다. 펌웨어 설치 날짜를 사용할 수 없는 경우 이러한 매우 오래된 날짜가 표시됩니다.

해결 방법: 펌웨어 구성 요소에 대해 이 이전 날짜가 표시되는 경우 설치 날짜를 사용할 수 없음을 간주하십시오.

적용 버전: 2.2 이상

최근 작업 창에서 연속적인 전역 새로 고침으로 인해 예외가 발생하는 이유는 무엇입니까?

고객이 새로 고침 단추를 반복적으로 누르려고 시도하는 경우 의 경우 VMware UI에 예외가 발생할 수 있습니다.

해결 방법: 사용자가 이 오류를 해결하면 계속해서 수행할 수 있습니다.

적용 버전: 2.2 이상

IE 10에서 Dell 화면 중 일부에 대해 웹 클라이언트 UI가 왜곡되는 이유는 무엇입니까?

경우에 따라 팝업 대화 상자가 나타날 때 배경의 데이터가 완전히 흰색으로 표시되고 왜곡될 수 있습니다.

해결 방법: 대화 상자를 닫으면 화면이 다시 정상 상태가 됩니다.

적용 버전: 2.2 이상

vCenter에 플러그인의 등록에 성공한 경우에도 웹 클라이언트에 OpenManage Integration 아이콘이 표시되지 않는 이유는 무엇입니까?

vCenter 웹 클라이언트 서비스를 다시 시작하지 않거나 상자를 재부팅하지 않으면 웹 클라이언트에 OpenManage Integration 아이콘이 표시되지 않습니다. 사용자가 OpenManage Integration for VMware vCenter 어플라이언스를 등록하면 Desktop 클라이언트와 웹 클라이언트에 모두 등록됩니다. 사용자가 어플라이언스의 등록을 취소한 후 동일한 버전을 다시 등록하거나 새 버전의 어플라이언스를 등록하면 두 클라이언트에 모두 성공적으로 등록되지만 웹 클라이언트에 Dell 아이콘이 나타나지 않을 수도 있습니다. 이는 VMware의 캐싱 문제 때문입니다. 문제를 해결하려면 사용자가 vCenter 서버에서 웹 클라이언트 서비스를 다시 시작해야 합니다. 이를 수행해야 UI에 플러그인이 나타납니다.

해결 방법: vCenter 서버에서 웹 클라이언트 서비스를 다시 시작하십시오.

적용 버전: 2.2 이상

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 모드로 전환하거나 호스트를 잠금 모드에서 해제할 경우 30분을 기다린 후 다음 작업을 수행해야 합니다. 펌웨어 업데이트에 11G 호스트를 사용하는 경우 제공된 리포지토리에 해당 시스템에 대한 번들이 있어도 펌웨어 업데이트 마법사에 번들이 표시되지 않습니다. 이는 OMSA에 사용되는 11G 호스트가 OpenManage Integration에 트랩을 보내도록 구성되지 않았기 때문일 수 있습니다.

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

적용 버전: 2.2 이상

보증 검색 작업을 실행하면 보증 작업 상태가 보증 작업 큐 페이지에 나열되지 않습니다.

인터넷에 연결하려면 네트워크에 프록시 상세 정보가 필요한 데 OMIVV 어플라이언스에서 프록시가 설정되지 않은 경우 보증 검색 작업이 실패하고 작업이 보증 작업 큐에 나열되지 않습니다.

해결 방법: 프록시 상세 정보를 설정하고 보증 작업을 다시 시작합니다.

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

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.

DUP의 스테이징 요구 사항으로 인해 OpenManage Integration for VMware vCenter를 사용하여 Intel Network 카드를 14.5 또는 15.0 또는 16.x에서 업데이트하지 못함

이는 NIC 14.5 및 15.0에서 알려진 문제입니다. 펌웨어를 16.x로 업데이트하기 전에 사용자 지정 카탈로그를 사용하여 펌웨어를 15.5.0로 업데이트해야 합니다.

적용 버전: 모든 버전

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

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.

전원 공급 장치 중 몇몇이 치명적인 상태로 변경된 이후에도 왜 섀시의 전체 전원 상태가 양호하다고 표시됩니까?

전원 공급 장치에 따른 섀시의 전체 전원 공급 상태는 중복성 정책 및 섀시의 전원 요구 상태가 온라인 상태이며 기능하고 있는 PSU에 의해 충족되었는지 여부를 기준으로 합니다. 따라서 몇몇 PSU의 전원이 나가더라도 섀시의 전체 전원 요구 사항은 충족됩니다. 그에 따라 전체 전원 상태는 양호로 표시됩니다. 전원 공급 장치 및 전원 관리에 대한 자세한 내용은 Dell PowerEdge M1000e Chassis Management Controller Firmware 문서의 사용 설명서를 참조하십시오.

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.

웹 클라이언트를 통해 연결 프로필을 편집한 후 마침을 클릭할 때마다 예외가 나타납니다. 이유는 무엇입니까?

이는 vCenter 서버가 FQDN 대신 IP를 통해 어플라이언스에 등록된 경우 발생합니다. 연결 프로필은 Desktop 클라이언트를 통해 편집할 수 있습니다. vCenter 서버를 동일한 어플라이언스에 다시 등록해도 이 문제가 해결되지 않습니다. FQDN으로 등록된 새 설정이 필요합니다.

웹 GUI에서 연결 프로필을 생성/편집할 때 호스트가 속하는 연결 프로필을 볼 수 없습니다. 이유는 무엇입니까?

이는 vCenter 서버가 FQDN 대신 IP를 통해 어플라이언스에 등록된 경우 발생합니다. vCenter 서버를 동일한 어플라이언스에 다시 등록해도 이 문제가 해결되지 않습니다. FQDN으로 등록된 새 설정이 필요합니다.

연결 프로필 편집 시 웹 UI의 호스트 선택 창이 비어 있습니다. 이유는 무엇입니까?

이는 vCenter 서버가 FQDN 대신 IP를 통해 어플라이언스에 등록된 경우 발생합니다. vCenter 서버를 동일한 어플라이언스에 다시 등록해도 이 문제가 해결되지 않습니다. FQDN으로 등록된 새 설정이 필요합니다.

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.

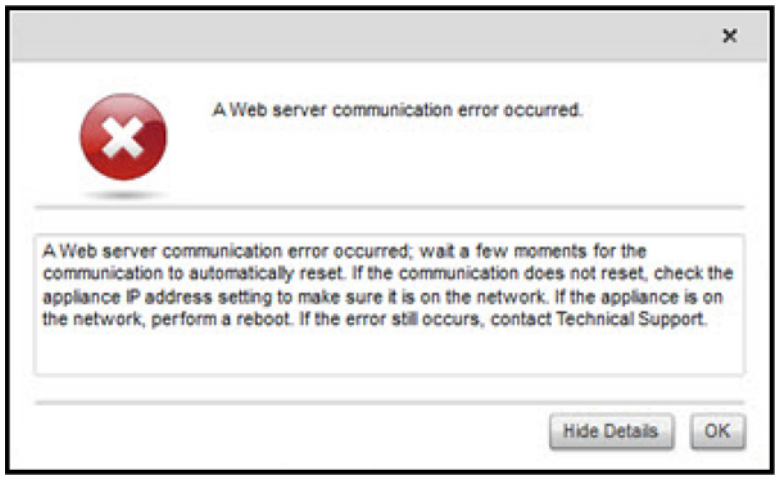

그림 1. 펌웨어 링크 통신 오류

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 vCenter에서 관리되는 vCenter는 무엇입니까?

OpenManage Integration for VMware vCenter는 링크된 모드 또는 링크되지 않은 모드의 등록된 vCenter만 관리합니다.

OpenManage Integration for VMware vCenter가 링크된 모드에서 vCenter를 지원합니까?

예, OpenManage Integration for VMware vCenter는 링크된 모드 또는 링크된 모드가 아닌 모드에서 최대 10개의 vCenter를 지원합니다. OpenManage Integration for VMware vCenter가 링크된 모드에서 작동되는 방식에 대해서는 www.Dell.com에서 *OpenManage Integration for VMware vCenter: 링크된 모드에서 작동* 백서를 참조하십시오.

OpenManage Integration for VMware vCenter의 필수 포트 설정은 무엇입니까?

노트: OpenManage Integration for VMware vCenter의 Compliance(준수) 창에 있는 *Fix non-complient vSphere hosts(비준수 vSphere 호스트 수정)* 링크를 사용하여 OMSA 에이전트를 배포하면, OpenManage Integration for VMware vCenter는 http Client 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 다음과 같은 포트 설정을 사용하십시오.

표 9. 가상 어플라이언스 포트

Port Number(포트 번호)	프로토콜	포트 유형	최고 암호화 수준	방향	Usage(사용량)	구성 가능
21	FTP	TCP	없음	Out	FTP 명령 클라이언트	아니오
53	DNS	TCP	없음	Out	DNS 자동	아니오
80	HTTP	TCP	없음	Out	Dell온라인 데이터 액세스	아니오
80	HTTP	TCP	없음	In	Administration Console	아니오
162	SNMP 에이전트	UDP	없음	In	SNMP 에이전트(서버)	아니오
11620	SNMP 에이전트	UDP	없음	In	SNMP 에이전트(서버)	아니오
443	HTTPS	TCP	128비트	In	HTTPS 서버	아니오
443	WSMAN	TCP	128비트	In/Out	iDRAC/OMSA 통신	아니오
4433	HTTPS	TCP	128비트	In	자동 검색	아니오
2049	NFS	UDP	없음	In/Out	공개 공유	아니오
4001–4004	NFS	UDP	없음	In/Out	공개 공유	아니오
11620	SNMP 에이전트	UDP	없음	In	SNMP 에이전트(서버)	아니오

표 10. 관리된 노드

Port Number(포트 번호)	프로토콜	포트 유형	최고 암호화 수준	방향	Usage(사용량)	구성 가능
162, 11620	SNMP	UDP	없음	Out	하드웨어 이벤트	아니오

표 10. 관리된 노드 (계속)

Port Number(포트 번호)	프로토콜	포트 유형	최고 암호화 수준	방향	Usage(사용량)	구성 가능
443	WSMAN	TCP	128비트	In	iDRAC/OMSA 통신	아니오
4433	HTTPS	TCP	128비트	Out	자동 검색	아니오
2049	NFS	UDP	없음	In/Out	공개 공유	아니오
4001–4004	NFS	UDP	없음	In/Out	공개 공유	아니오
443	HTTPS	TCP	128비트	In	HTTPS 서버	아니오
8080	HTTP	TCP		In	HTTP 서버; OMSA VIB를 다운로드하고 비준수 vSphere 호스트를 수정합니다.	아니오
50	RMCP	UDP/TCP	128비트	Out	원격 메일 확인 프로토콜	아니오
51	IMP	UDP/TCP	N/A(해당 없음)	N/A(해당 없음)	IMP 논리적 주소 유지 보수	아니오
5353	mDNS	UDP/TCP		In/Out	Multicast DNS	아니오
631	IPP	UDP/TCP	없음	Out	IPP(Internet Printing Protocol)	아니오
69	TFTP	UDP	128비트	In/Out	Trivial File Transfer	아니오
111	NFS	UDP/TCP	128비트	In	SUN Remote Procedure Call (Portmap)	아니오
68	BOOTP	UDP	없음	Out	Bootstrap Protocol Client	아니오

가상 어플라이언스의 성공적인 설치와 작동을 위한 최소 요구 사항은 무엇입니까?

다음 설정은 최소 어플라이언스 요구 사항의 개요를 제공합니다.

- Google Chrome, 버전 28 이상

  .
- Microsoft Internet Explorer, 버전 9 및 10
- Mozilla Firefox, 버전 22 이상
- 예약된 메모리: 2GB

  노트: 최적의 성능을 위해 Dell에서는 3GB를 권장합니다.
- 디스크: 43.5GB
- CPU: 2개의 가상 CPU

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 vCenter

의 Host Compliance(호스트 호환성) 페이지로 이동한 후 해당 호스트의 CSIOR 상태를 확인하십시오. CSIOR이 활성화되어 있지 않으면 CSIOR을 활성화하고 호스트를 재부팅하십시오. CSIOR이 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 27인 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 30초 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 ESXi가 지원됩니까?

예. 호스트 ESXi 5.0 이상의 이 릴리스에서 잠금 모드가 지원됩니다.

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.

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.

블레이드 서버에서 ESXi를 배포하도록 시도했지만 실패했습니다. 어떻게 해야 합니까?

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 내 Dell PowerEdge R210 II 시스템에서 실패하는 이유는 무엇입니까?

연결된 ISO로부터 부팅하려는 BIOS의 오류로 인해 Dell PowerEdge R210 II 시스템의 시간 초과 문제가 하이퍼바이저 배포 실패 오류의 원인이 됩니다. 이 문제를 해결하려면 시스템에 수동으로 하이퍼바이저를 설치하십시오.

NFS 공유가 ESXi ISO와 함께 설치되었지만 공유 위치 탑재 오류로 인해 배포에 실패했습니다.

해결 방법을 찾으려면 다음을 수행하십시오.

1. iDRAC가 어플라이언스를 ping할 수 있는지 확인합니다.
2. 네트워크 실행 속도가 너무 느리지 않은지 확인합니다.
3. 2049, 4001 - 4004 포트가 열려 있고 그에 따라 방화벽이 설정되어 있는지 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. 확장 키를 입력하여 com.dell.plugin.openManage_integration_for_VMware_vCenter의 등록을 취소하고 **Invoke method(메서드 호출)**를 클릭합니다.
7. 확장 키를 입력하여 com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient의 등록을 취소하고 **Invoke method(메서드 호출)**를 클릭합니다.
8. vSphere 웹 클라이언트에서 OpenManage Integration for VMware vCenter를 끄고 삭제합니다. 등록 취소할 키는 웹 클라이언트용이어야 합니다.

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.

vSphere 웹 클라이언트에서 Dell Server Management 포틀릿 또는 Dell 아이콘을 클릭하면 404 오류가 나타납니다.

어플라이언스가 실행 중인지 확인합니다. 실행되지 않는 경우 vSphere 웹 클라이언트에서 해당 어플라이언스가 다시 시작됩니다. 가상 어플라이언스 웹 서버가 시작될 때까지 잠시 기다린 후 페이지를 새로 고칩니다. 계속해서 오류가 발생하는 경우 명령줄에서 정규화된 도메인 이름 또는 IP 주소를 사용하여 어플라이언스를 시도하고 ping하십시오. ping을 통해 오류가 해결되지 않는 경우 네트워크 설정이 올바른지 확인하십시오.

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 **Gateway(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 vCenter는 v2.1부터 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.

다음 재부팅 시 적용 옵션을 사용하여 펌웨어 업데이트를 수행했고 시스템을 다시 부팅했는데 펌웨어 레벨이 아직 업데이트되지 않은 이유는 무엇입니까?

펌웨어를 업데이트하려면 재부팅이 완료된 후에 호스트에서 인벤토리를 실행하십시오. 재부팅이 어플라이언스에 적용되지 않는 경우도 있기 때문에 인벤토리가 자동으로 트리거되지 않습니다. 이 경우, 인벤토리를 수동으로 다시 실행해야 펌웨어 버전이 업데이트됩니다.

VCenter 트리에서 호스트를 제거한 후에도 섀시 아래에 호스트가 여전히 표시되는 이유는 무엇입니까?

섀시 아래의 호스트는 섀시 인벤토리의 일부로 식별됩니다. 섀시 인벤토리에 성공하면 섀시 아래의 호스트 목록이 업데이트됩니다. 따라서 VCenter 트리에서 호스트가 제거되어도 다음 섀시 인벤토리가 실행될 때까지 섀시 아래에 호스트가 계속 표시됩니다.

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.

Dell에 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/support로 이동합니다.
2. 지원 카테고리를 선택합니다.
3. 페이지 맨 아래에 있는 **Choose a Country/Region(국가/지역 선택)** 드롭다운 메뉴에서 국가 또는 지역을 확인합니다.
4. 필요한 서비스 또는 지원 링크를 선택하십시오.

OpenManage Integration for VMware vCenter 관련 정보

- PowerEdge™ 서버에 대한 Dell 서버 문서 보기 및 다운로드: Dell PoweEdge 설명서
- Dell OpenManage 시스템 관리자 문서: Dell OMSA 문서
- Dell Lifecycle Controller 문서: DLCI 문서

42

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 11. 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

표 11. 11세대, 12세대 및 13세대 PowerEdge 서버의 가상화 관련 이벤트 (계속)

이벤트 이름	설명	심각도	권장 작업
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

표 11. 11세대, 12세대 및 13세대 PowerEdge 서버의 가상화 관련 이벤트 (계속)

이벤트 이름	설명	심각도	권장 작업
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

표 11. 11세대, 12세대 및 13세대 PowerEdge 서버의 가상화 관련 이벤트 (계속)

이벤트 이름	설명	심각도	권장 작업
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

표 11. 11세대, 12세대 및 13세대 PowerEdge 서버의 가상화 관련 이벤트 (계속)

이벤트 이름	설명	심각도	권장 작업
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

표 11. 11세대, 12세대 및 13세대 PowerEdge 서버의 가상화 관련 이벤트 (계속)

이벤트 이름	설명	심각도	권장 작업
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
Dell - Virtual Disk Partition failure.	가상 디스크 파티션 실패.	오류	작업 안 함
Dell - Virtual Disk Partition warning.	가상 디스크 파티션 경고.	경고	작업 안 함
Dell - Cable failure or critical event	케이블 연결 실패 또는 위험 이벤트	오류	작업 안 함
Dell - Chassis Management Controller detected an error.	섀시 관리 컨트롤러가 오류 감지.	오류	작업 안 함
Dell - IO Virtualization failure or critical event.	IO 가상화 실패 또는 위험 이벤트.	오류	작업 안 함
Dell - Link status failure or critical event.	링크 상태 실패 또는 위험 이벤트.	오류	작업 안 함
Dell - System: Software configuration failure.	시스템: 소프트웨어 구성 오류.	오류	작업 안 함
Dell - Storage Security failure or critical event.	스토리지 보안 실패 또는 위험 이벤트.	오류	작업 안 함
Dell - Chassis Management Controller audit failure or critical event.	섀시 관리 컨트롤러 감사 실패 또는 위험 이벤트.	오류	작업 안 함
Dell - Power Supply audit failure or critical event.	전원 공급 장치 감사 실패 또는 위험 이벤트.	오류	작업 안 함
Dell - Power usage audit failure or critical event.	전원 사용 감사 실패 또는 위험 이벤트.	오류	작업 안 함

표 11. 11세대, 12세대 및 13세대 PowerEdge 서버의 가상화 관련 이벤트 (계속)

이벤트 이름	설명	심각도	권장 작업
Dell - Configuration: Software configuration failure.	구성: 소프트웨어 구성 오류.	오류	작업 안 함
Dell - Chassis Management Controller detected a warning.	섀시 관리 컨트롤러가 경고 감지.	경고	작업 안 함
Dell - Link status warning.	링크 상태 경고.	경고	작업 안 함
Dell - Security warning.	보안 경고.	경고	작업 안 함
Dell - System: Software configuration warning.	시스템: 소프트웨어 구성 경고.	경고	작업 안 함
Dell - Storage Security warning.	스토리지 보안 경고.	경고	작업 안 함
Dell - Software change update warning	소프트웨어 변경사항 업데이트 경고	경고	작업 안 함
Dell - Chassis Management Controller audit warning.	섀시 관리 컨트롤러 감사 경고.	경고	작업 안 함
Dell - PCI device audit warning.	PCI 장치 감사 경고.	경고	시스템을 유지 보수 모두에 배치
Dell - Power Supply audit warning.	전원 공급 장치 감사 경고.	경고	작업 안 함
Dell - Power usage audit warning.	전원 사용 감사 경고.	경고	작업 안 함
Dell - Security configuration warning.	보안 구성 경고.	경고	작업 안 함
Dell - Configuration: Software configuration warning.	구성: 소프트웨어 구성 경고.	경고	작업 안 함

A

주제:

- 보안 역할 및 권한

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 그룹에는 모든 권한이 있습니다. 관리자는 VMware vSphere 클라이언트 또는 웹 클라이언트 내에서 OpenManage Integration for VMware vCenter의 모든 기능을 사용할 수 있습니다. 사용자가 제품을 관리하는 데 필요한 권한을 갖도록 하려면 필요한 권한이 있는 역할을 생성하고 사용자에게 역할을 할당하고 사용자를 사용하여 vCenter 서버를 등록하고 두 Dell 역할을 모두 포함합니다.

데이터 무결성

OpenManage Integration for VMware vCenter, 관리 콘솔 및 vCenter 간의 통신은 SSL/HTTPS를 사용하여 수행됩니다. OpenManage Integration for VMware vCenter가 vCenter와 어플라이언스 간에 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 탭에서 관리 콘솔과 백엔드 서비스 간에 키를 전송하는 중에 잘못된 요청이 발생하지 않도록 보안 절차를 사용합니다. 이러한 유형의 보안을 사용하면 교차 사이트 요청 위조가 실패하게 됩니다.

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. 이를 통해 사용자가 Administration Console 세션을 공격할 수 있는 악성 URL을 클릭하지 않도록 합니다.

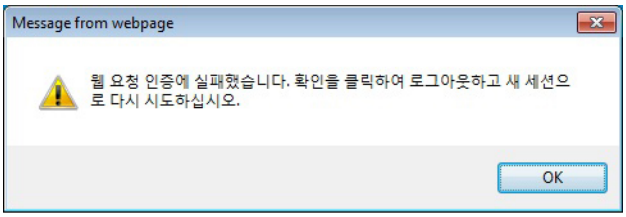

그림 2 . 오류 메시지

액세스 제어 인증, 권한 부여 및 역할

OpenManage Integration for VMware vCenter는 웹 클라이언트의 현재 사용자 세션 및 OpenManage Integration의 저장된 관리 자격 증명을 사용하여 vCenter 작업을 수행합니다. 또한 OpenManage Integration for VMware vCenter는 서버의 기본 제공 역할 및 권한 모델을 사용하여 OpenManage Integration 및 vCenter 관리되는 개체(호스트 및 클러스터)의 사용자 작업에 권한을 부여합니다. VMware vCenter 홈 페이지에서 역할에 액세스합니다.

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.

표 12. 권한 그룹

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

Dell 인프라 배포 역할

이 역할에는 특히 하이퍼바이저 배포 기능과 관련된 권한이 포함됩니다.

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

권한 그룹 — Dell.Deploy — Provisioning	템플릿 생성, HW 구성 프로필 구성, 하이퍼바이저 배포 프로필 구성, 연결 프로필 구성, ID 할당 및 배포

권한 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
  - HW 구성 프로필 구성
  - 하이퍼바이저 배포 프로필 구성
  - 연결 프로필 구성
  - ID 할당
  - 배포
- 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

B