



Red Hat Virtualization 4.1

관리 가이드

Red Hat Virtualization에서 관리 작업

Red Hat Virtualization 4.1 관리 가이드

Red Hat Virtualization에서 관리 작업

Red Hat Virtualization Documentation Team
Red Hat Customer Content Services
rhev-docs@redhat.com

법적 공지

Copyright © 2016 Red Hat.

This document is licensed by Red Hat under the [Creative Commons Attribution-ShareAlike 3.0 Unported License](#). If you distribute this document, or a modified version of it, you must provide attribution to Red Hat, Inc. and provide a link to the original. If the document is modified, all Red Hat trademarks must be removed.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

초록

다음 부분에서는 Red Hat Virtualization 관리자와 관련된 절차 및 정보에 대해 설명합니다.

차례

I 부. RED HAT VIRTUALIZATION 환경 관리 및 유지 보수	6
1장. 전체 설정	7
1.1. 역할	7
1.2. 시스템 권한	10
1.3. 스케줄링 정책	15
1.4. 인스턴스 유형	19
1.5. MAC 주소 풀	22
2장. 대시보드	26
2.1. 전제 조건	26
2.2. 전체 인벤토리	26
2.3. 전체 사용량	28
2.4. 클러스터 사용량	29
2.5. 스토리지 사용량	29
II 부. 리소스 관리	31
3장. QOS (QUALITY OF SERVICE)	32
3.1. 스토리지 QOS	32
3.2. 가상 머신 네트워크 QOS	33
3.3. 호스트 네트워크 QOS	35
3.4. CPU QOS (QUALITY OF SERVICE)	36
4장. 데이터 센터	38
4.1. 데이터 센터 소개	38
4.2. SPM (STORAGE POOL MANAGER)	39
4.3. SPM 우선순위	39
4.4. 이벤트 탭을 사용하여 데이터 센터에서 문제가 있는 개체를 식별	39
4.5. 데이터 센터 작업	40
4.6. 데이터 센터 및 스토리지 도메인	43
4.7. 데이터 센터 및 권한	45
5장. 클러스터	48
5.1. 클러스터에 대한 소개	48
5.2. 클러스터 작업	48
5.3. 클러스터 및 권한	68
6장. 논리 네트워크	71
6.1. 논리 네트워크 작업	71
6.2. 가상 네트워크 인터페이스 카드	79
6.3. 외부 공급자 네트워크	85
6.4. 논리 네트워크 및 권한	88
6.5. 호스트 및 네트워킹	90
7장. 호스트	103
7.1. 호스트 소개	103
7.2. RED HAT VIRTUALIZATION HOST	103
7.3. RED HAT ENTERPRISE LINUX 호스트	104
7.4. SATELLITE 호스트 공급자 호스트	104
7.5. 호스트 작업	105
7.6. 호스트 복원	123
7.7. 호스트 및 권한	133

8장. 스토리지	135
8.1. 스토리지 도메인 이해	136
8.2. NFS 스토리지 준비 및 추가	136
8.3. 로컬 스토리지 준비 및 추가	139
8.4. POSIX 호환 파일 시스템 스토리지 추가	141
8.5. 블록 스토리지 추가	143
8.6. 기존 스토리지 도메인 가져오기	150
8.7. 스토리지 작업	157
8.8. 스토리지 및 권한	162
9장. RED HAT GLUSTER STORAGE를 사용하여 작업	165
9.1. RED HAT GLUSTER STORAGE 노트	165
9.2. 스토리지 도메인으로 RED HAT GLUSTER STORAGE 사용	166
9.3. CLUSTERS 및 GLUSTER 후크	175
10장. 풀	180
10.1. 가상 머신 풀 소개	180
10.2. 가상 머신 풀 작업	180
10.3. 풀 및 권한	190
10.4. 신뢰할 수 있는 컴퓨팅 풀	192
11장. 가상 디스크	195
11.1. 가상 머신 스토리지 이해	195
11.2. 가상 디스크 이해	195
11.3. 삭제 후 디스크 장치 초기화 설정	196
11.4. RED HAT VIRTUALIZATION에서 공유 가능한 디스크	197
11.5. RED HAT VIRTUALIZATION에서 읽기 전용 디스크	198
11.6. 가상 디스크 작업	198
11.7. 가상 디스크 및 권한	210
12장. 외부 공급자	213
12.1. RED HAT VIRTUALIZATION에서 외부 공급자 소개	213
12.2. 외부 공급자 추가	214
12.3. 외부 공급자 편집	229
12.4. 외부 공급자 삭제	229
III 부. 환경 관리	230
13장. 백업 및 마이그레이션	231
13.1. RED HAT VIRTUALIZATION MANAGER 백업 및 복구	231
13.2. 백업 및 복구 API를 사용하여 가상 머신 백업 및 복구	238
14장. RED HAT SATELLITE을 사용한 예라타 관리	242
15장. 사용자 및 역할	243
15.1. 사용자에게 대한 소개	243
15.2. 디렉토리 서버 소개	243
15.3. 외부 LDAP 공급자 설정	244
15.4. 단일 사용 승인(SSO)을 위해 LDAP 및 KERBEROS 설정	254
15.5. 사용자 인증	260
15.6. 관리 포털에서 사용자 작업 관리	260
15.7. 명령행에서 사용자 작업 관리	262
15.8. 추가 로컬 도메인 설정	267
16장. 쿼터 및 서비스 수준 계약 정책	268
16.1. 쿼터 소개	268

16.2. 공유된 쿼터 및 개별적으로 정의된 쿼터	269
16.3. 쿼터 계산	269
16.4. 데이터 센터에서 쿼터 모드 활성화 및 변경	270
16.5. 새 쿼터 정책 생성	270
16.6. 쿼터 임계값 설정	271
16.7. 개체에 쿼터 지정	271
16.8. 쿼터를 사용하여 사용자에게 따라 리소스를 제한	272
16.9. 쿼터 편집	273
16.10. 쿼터 삭제	273
16.11. 서비스 수준 계약 정책 적용	274
17장. 이벤트 알림	276
17.1. 관리 포털에서 이벤트 알림 설정	276
17.2. 관리 포털에서 이벤트 공지 취소	278
17.3. OVIRT-ENGINE-NOTIFIER.CONF에서 이벤트 공지 매개 변수	278
17.4. RED HAT VIRTUALIZATION MANAGER를 설정하여 SNMP 트랩 전송	281
18장. 유틸리티	284
18.1. OVIRT ENGINE RENAME 도구	284
18.2. ENGINE 설정 도구	286
18.3. 이미지 업로더 도구	287
18.4. USB 필터 편집기	290
18.5. 로그 수집 도구	297
18.6. ISO 업로더 도구	302
IV 부. 환경 정보	306
19장. 로그 파일	307
19.1. RED HAT VIRTUALIZATION MANAGER 설치 로그 파일	307
19.2. RED HAT VIRTUALIZATION MANAGER 로그 파일	307
19.3. SPICE 로그 파일	308
19.4. RED HAT VIRTUALIZATION HOST 로그 파일	309
19.5. 가상화 호스트 로깅 서버 설정	310
20장. 프록시	312
20.1. SPICE 프록시	312
20.2. SQUID 프록시	314
20.3. WEBSOCKET 프록시	316
부록 A. VDSM 및 후크	318
A.1. VDSM	318
A.2. VDSM 후크	318
A.3. 후크로 VDSM 확장	318
A.4. 지원되는 VDSM 이벤트	318
A.5. VDSM 후크 환경	321
A.6. VDSM 후크 도메인 XML 개체	321
A.7. 사용자 정의 속성 정의	321
A.8. 가상 머신 사용자 정의 속성 설정	323
A.9. VDSM 후크에서 가상 머신 사용자 정의 속성 평가	323
A.10. VDSM 후킹 모듈 사용	323
A.11. VDSM 후크 실행	324
A.12. VDSM 후크 반환 코드	325
A.13. VDSM 후크 예	325
부록 B. 사용자 정의 네트워크 속성	328

B.1. BRIDGE_OPTS 매개 변수	328
B.2. ETHTOOL 사용을 위해 RED HAT VIRTUALIZATION MANAGER 설정	330
B.3. FCOE를 사용하기 위해 RED HAT VIRTUALIZATION MANAGER를 설정하는 방법	331
B.4. 비관리 네트워크를 사용하기 위해 RED HAT VIRTUALIZATION MANAGER를 설정하는 방법	331
부록 C. RED HAT VIRTUALIZATION 사용자 인터페이스 플러그인	333
C.1. RED HAT VIRTUALIZATION 사용자 인터페이스 플러그인	333
C.2. RED HAT VIRTUALIZATION 사용자 인터페이스 플러그인 라이프사이클	333
C.3. 사용자 인터페이스 플러그인 관련 파일 및 위치	335
C.4. 사용자 인터페이스 플러그인 배포 예	335
C.5. RED HAT SUPPORT 플러그인 사용	336
부록 D. RED HAT VIRTUALIZATION 및 SSL	341
D.1. RED HAT VIRTUALIZATION MANAGER SSL 인증서 변경	341
D.2. MANAGER 및 LDAP 서버 간의 SSL 또는 TLS 연결 설정	342
부록 E. 검색, 북마크, 태그 사용	344
E.1. 검색	344
E.2. 북마크	362
E.3. 태그	363
부록 F. 브랜딩	366
F.1. 브랜딩	366
부록 G. 시스템 계정	369
G.1. 시스템 계정	369

I 부. RED HAT VIRTUALIZATION 환경 관리 및 유지 보수

Red Hat Virtualization 환경을 계속 실행하려면 관리자가 필요합니다. 관리자로 실행할 수 있는 작업은 다음과 같습니다:

- 호스트 및 가상 머신과 같은 물리적 및 가상 리소스를 관리합니다. 이에는 호스트 업그레이드 및 추가, 도메인 가져오기, 외부 하이퍼바이저에서 생성된 가상 머신 전환, 가상 머신 풀 관리 등이 포함됩니다.
- 하나의 호스트에서 최대 부하, 메모리 또는 디스크 공간 부족과 같은 잠재적 문제에 대해 전반적인 시스템 리소스를 모니터링하고 필요한 작업 (예: 시스템을 종료하여 리소스를 사용 해제하거나 작업 부하를 줄이기 위해 다른 호스트로 가상 머신을 마이그레이션)을 실행합니다.
- 가상 머신의 새로운 요구 사항에 대응합니다. (예: 운영 체제 업그레이드 또는 더 많은 메모리 할당)
- 태그를 사용하여 사용자 정의 개체 속성을 관리합니다.
- 일반 북마크로 저장된 검색을 관리합니다.
- 사용자 설정 권한 수준을 관리합니다.
- 특정 사용자 또는 전체 시스템 기능에 대한 가상 머신의 문제를 해결합니다.
- 일반 및 특정 보고서를 생성합니다.

1장. 전체 설정

관리 포털에 있는 머리글 표시줄에서 액세스하면 **설정** 창을 통해 사용자, 역할, 시스템 권한, 스케줄링 정책, 인스턴스 유형, 그리고 MAC 주소 풀과 같은 Red Hat Virtualization 환경의 전체 리소스를 설정할 수 있습니다. 이 창에서는 사용자 환경에서 리소스와 상호 작용하는 방식을 사용자 정의할 수 있으며 여러 클러스터에 적용 가능한 옵션을 설정할 수 있습니다.

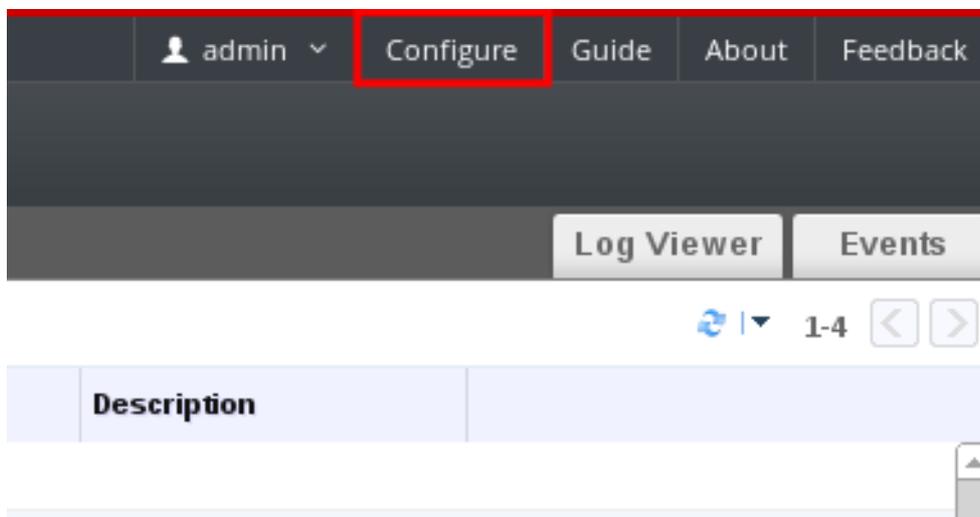


그림 1.1. 설정 창에 액세스하기

1.1. 역할

역할은 Red Hat Virtualization Manager에서 설정할 수 있는 사전 정의된 권한 모음입니다. 역할은 데이터 센터에 있는 다른 리소스 레벨 및 특정 물리/가상 리소스에 대한 액세스 및 관리 권한을 제공합니다.

다단계 관리에서 컨테이너 개체에 적용되는 모든 권한은 컨테이너 내에 있는 개별 개체 모두에 적용됩니다. 예를 들어 호스트 관리자 역할이 특정 호스트에 있는 사용자에게 지정될 때 사용자에게는 지정된 호스트에서만 사용할 수 있는 호스트 작업을 수행할 수 있는 권한이 부여됩니다. 하지만 데이터 센터에 있는 사용자에게 호스트 관리자 역할이 지정되면 사용자는 데이터 센터의 클러스터 내에 있는 모든 호스트에서 호스트 작업을 수행할 수 있는 권한이 부여됩니다.

1.1.1. 새 역할 생성

필요한 역할이 Red Hat Virtualization 기본 역할 목록에 없을 경우 새 역할을 생성하고 필요에 따라 이를 사용자 정의할 수 있습니다.

절차 1.1. 새 역할 생성

1. 머리글 표시줄에서 **설정** 버튼을 클릭하여 **설정** 창을 엽니다. 이 창에는 기본 사용자와 관리자 역할 및 사용자 정의 역할 목록이 표시됩니다.
2. **새로 만들기**를 클릭합니다. **새 역할** 창이 표시됩니다.

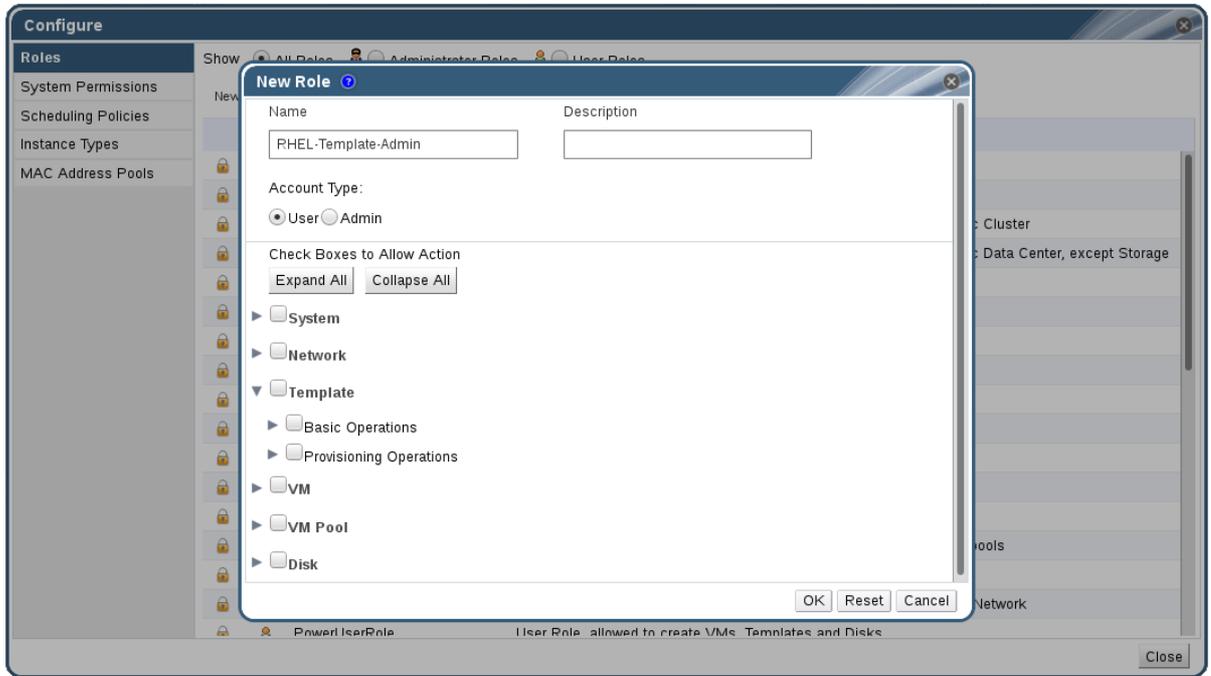


그림 1.2. 새 역할 창

3. 새 역할의 이름 및 설명을 입력합니다.
4. 계정 유형으로 관리자 또는 사용자를 선택합니다.
5. 모두 확장 또는 모두 축소 버튼을 사용하여 작업 허용을 위한 확인란 목록에 있는 개체에 대한 권한을 확장하거나 축소할 수 있습니다. 또한 각 개체에 대한 옵션을 확장하거나 축소할 수 있습니다.
6. 각 개체별로 설정하려는 역할을 허용 또는 거부하고자 하는 작업을 선택 또는 선택 해제합니다.
7. **OK**를 클릭하여 변경 사항을 적용합니다. 역할 목록에 새로운 역할이 표시됩니다.

1.1.2. 역할 편집 또는 역할 복사

생성한 역할 설정을 변경할 수 있지만 기본 역할을 변경할 수 없습니다. 기본 역할을 변경하려면 복제하여 필요에 따라 수정합니다.

절차 1.2. 역할 편집 또는 역할 복사

1. 머릿글 표시줄에서 설정 버튼을 클릭하여 설정 창을 엽니다. 이 창에는 기본 사용자와 관리자 역할 및 사용자 정의 역할 목록이 표시됩니다.
2. 변경하고자 하는 역할을 선택합니다. 편집을 클릭하여 역할 수정 창을 열거나 복사를 클릭하여 역할 복사 창을 엽니다.
3. 필요에 따라 역할의 이름 및 설명을 변경합니다.
4. 모두 확장 또는 모두 축소 버튼을 사용하여 개체에 대한 권한을 확장하거나 축소할 수 있습니다. 또한 각 개체에 대한 옵션을 확장하거나 축소할 수 있습니다.
5. 각 개체별로 편집하려는 역할을 허용 또는 거부하고자 하는 작업을 선택 또는 선택 해제합니다.
6. **OK**를 클릭하여 변경 사항을 적용합니다.

1.1.3. 사용자 역할 및 인증 예

다음 예에서는 이 장에서 설명된 다른 인증 시스템 기능을 사용하여 다양한 시나리오에서 인증 관리를 적용하는 방법에 대해 설명합니다.

예 1.1. 클러스터 권한

Sarah는 회사에서 회계 부서 시스템 관리자입니다. 부서에서 모든 가상 리소스는 **Accounts**라는 Red Hat Virtualization **cluster** 하에 구성되어 있습니다. 계정 클러스터에서 **ClusterAdmin** 역할이 Sarah에게 할당되었습니다. 가상 머신은 클러스터의 자식 개체이기 때문에 이를 통해 클러스터에 있는 모든 가상 머신을 관리할 수 있습니다. 가상 머신 관리에는 디스크와 같은 가상 리소스를 편집, 추가, 삭제하고 스냅샷을 생성하는 것 등이 포함됩니다. 하지만 클러스터 외부 리소스는 관리할 수 없습니다. **ClusterAdmin**은 관리자 역할이기 때문에 관리 포털을 사용하여 이러한 리소스를 관리할 수 있지만 사용자 포털을 통해 액세스할 수 없습니다.

예 1.2. VM PowerUser 권한

John은 회계 부서에서 소프트웨어 개발자로 가상 머신을 사용하여 소프트웨어를 구축 및 테스트합니다. Sarah는 John에 대해 **johndesktop**이라는 가상 데스크탑을 생성했습니다. John에게는 **johndesktop** 가상 머신에 대해 **UserVmManager** 역할이 할당됩니다. 이로 인해 John은 사용자 포털을 사용하여 단일 가상 머신에 액세스할 수 있습니다. John은 **UserVmManager** 권한이 있기 때문에 가상 머신을 수정하거나 새 가상 디스크 등의 리소스를 추가할 수 있습니다. **UserVmManager**는 사용자 역할이기 때문에 관리 포털은 사용할 수 없습니다.

예 1.3. 데이터 센터 Power User Role 권한

Penelope는 사무실 매니저입니다. Penelope는 자신의 업무에 더하여 면접 날짜를 정하고 신원 조회를 하는 것과 같이 인사부 매니저의 인사 관련 업무를 수행했습니다. 회사의 방침에 따라 Penelope는 인사 관련 업무를 실행할 때 특정 애플리케이션을 사용했습니다.

Penelope는 사무실 관리 업무를 위해 자신의 컴퓨터를 사용하지만 인사 관련 애플리케이션을 실행하기 위해 별도의 가상 머신을 생성하고자 합니다. 새 가상 머신이 있는 데이터 센터에 대해 **PowerUserRole** 권한이 Penelope에게 할당되었습니다. 새 가상 머신을 생성하려면 스토리지 도메인에서 가상 디스크 이미지 생성과 같은 데이터 센터 내에 있는 일부 구성 요소를 변경해야 하기 때문입니다.

이는 **DataCenterAdmin** 권한을 Penelope에게 할당하는 것과 동일하지 않음에 유의합니다. 데이터 센터의 **PowerUser**로 Penelope는 사용자 포털에 로그인하여 데이터 센터 내에 있는 가상 머신에 특정 가상 머신 작업을 수행할 수 있습니다. 하지만 데이터 센터에 호스트 또는 스토리지 연결과 같은 데이터 센터 수준의 작업은 수행할 수 없습니다.

예 1.4. 네트워크 관리자 권한

Chris는 IT 부서에서 네트워크 관리자로 일하고 있으며 부서의 Red Hat Virtualization 환경에 있는 네트워크를 생성, 조작, 삭제와 같은 작업을 담당합니다. Chris의 역할을 수행하려면 리소스 및 각 리소스의 네트워크에서 관리자 권한이 필요합니다. 예를 들어 IT 부서의 데이터 센터에서 Chris가 **NetworkAdmin** 권한이 있을 경우 데이터 센터에서 네트워크를 추가 및 삭제할 수 있으며 데이터 센터에 속한 모든 가상 머신의 네트워크를 연결 및 분리할 수 있습니다.

회사의 가상 인프라 네트워크 관리에 더하여 Chris는 하급 네트워크 관리자를 관리합니다. 하급 네트워크 관리자인 Pat는 사내 교육 부서의 소규모 가상 환경을 관리하고 있습니다. Chris는 Pat에게 사내 교육 부서에서 사용하는 가상 머신에 대해 **VnicProfileUser** 권한 및 **UserVmManager** 권한을 할당

했습니다. 이러한 권한을 사용하여 **Pat**는 사용자 포털의 **확장** 탭에서 가상 머신에 네트워크 인터페이스를 추가하는 것과 같은 단순한 관리 작업을 수행할 수 있지만 가상 머신이 실행되는 호스트의 네트워크 또는 가상 머신이 속한 데이터 센터에 있는 네트워크를 변경할 수 있는 권한이 없습니다.

예 1.5. 사용자 정의 역할 권한

Rachel은 IT 부서에서 일하고 있으며 **Red Hat Virtualization**에서 사용자 계정을 관리하는 역할을 담당하고 있습니다. **Rachel**에게는 사용자 계정을 추가하고 적절한 역할 및 권한을 할당하기 위한 권한이 필요합니다. **Rachel** 자신은 가상 머신을 사용하지 않고 호스트, 가상 머신, 클러스터, 데이터의 관리 액세스가 필요하지 않습니다. 이러한 특정 권한을 제공하기 위한 내장된 역할은 없습니다. 사용자 정의 역할을 생성하여 **Rachel**의 담당 부분에 맞는 권한을 설정해야 합니다.

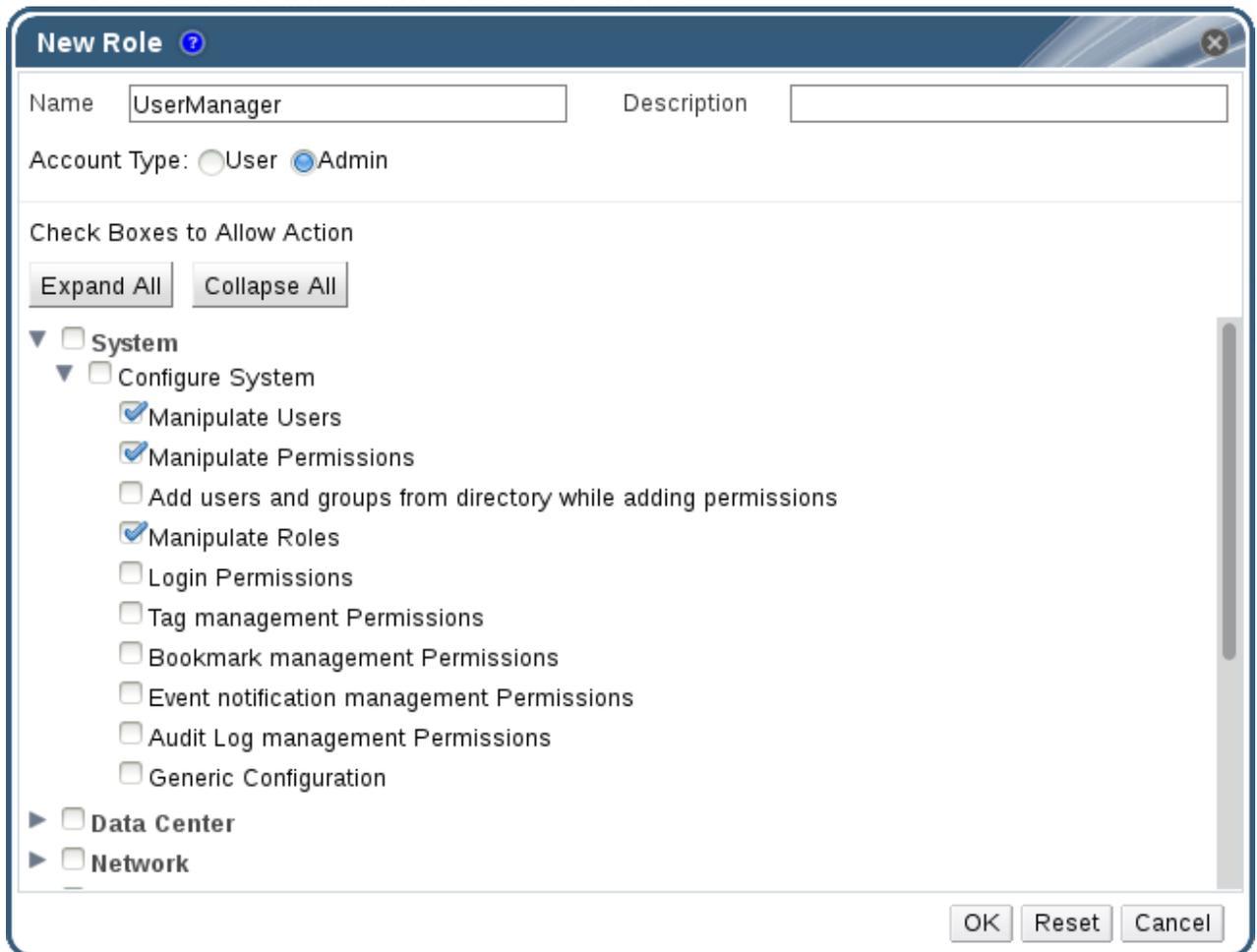


그림 1.3. **UserManager** 사용자 정의 역할

위에서 설명한 **UserManager** 사용자 정의 역할을 통해 사용자, 권한, 역할을 조정할 수 있습니다. 이러한 작업은 그림 1.3. “**UserManager** 사용자 정의 역할”에 있는 계층의 최상위 레벨인 **System** 아래에 구성되어 있으므로 시스템에 있는 모든 다른 개체에 적용할 수 있습니다. 역할은 **관리자의 계정 유형**에 설정되어 있으므로 역할을 할당할 때 **Rachel**은 사용자 포털이 아닌 관리 포털만을 사용할 수 있습니다.

1.2. 시스템 권한

권한은 사용자가 개체 작업을 수행할 수 있게 합니다. 여기서 개체는 개별 개체 또는 컨테이너 개체입니다.

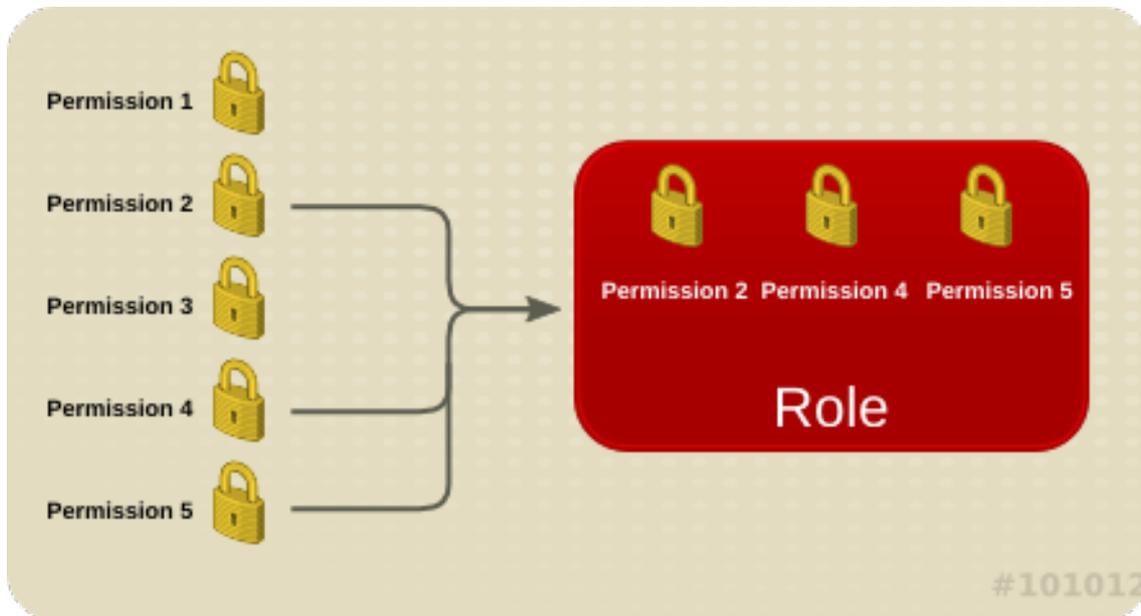


그림 1.4. 권한 & 역할

컨테이너 개체에 적용되는 모든 권한은 해당 컨테이너의 모든 구성원에도 적용됩니다. 다음 그림은 시스템의 개체 계층 구조를 보여줍니다.

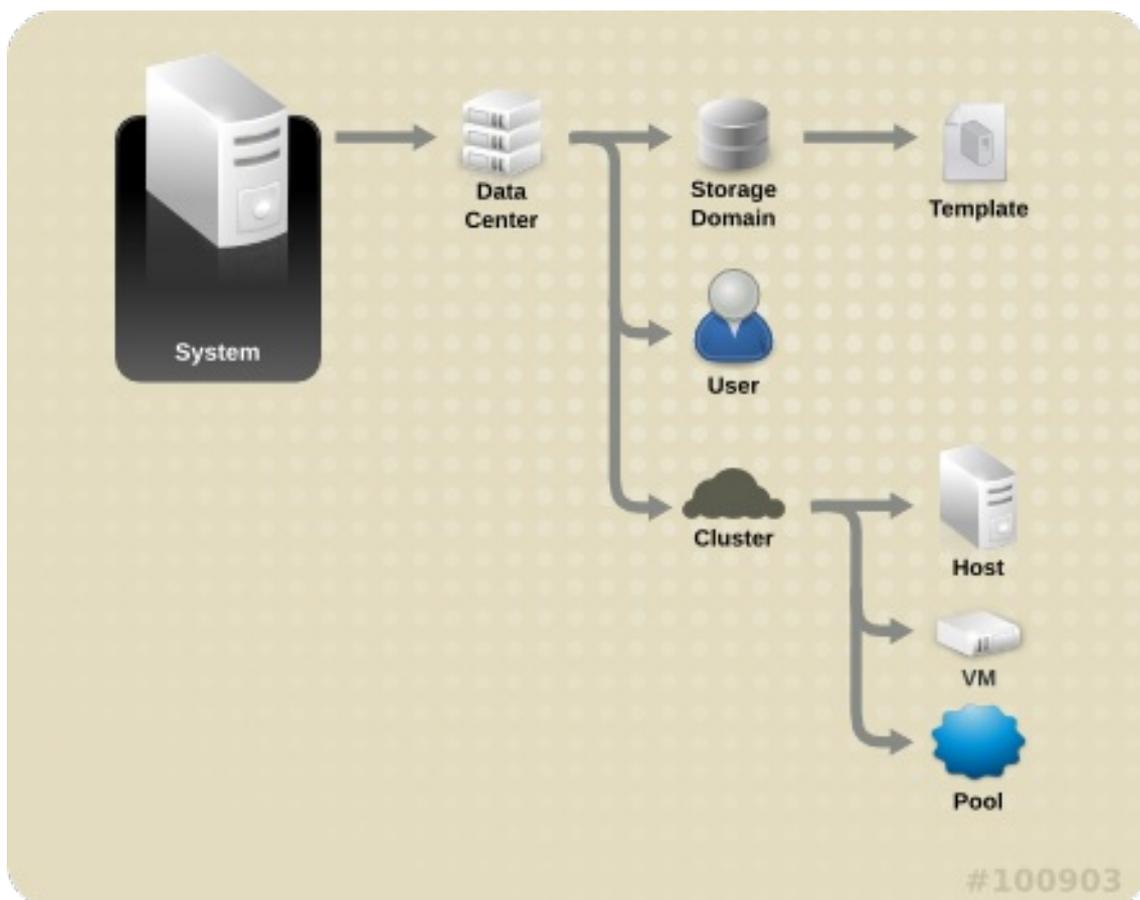


그림 1.5. Red Hat Virtualization 개체 계층 구조

1.2.1. 사용자 속성

역할 및 권한은 사용자의 속성입니다. 역할은 다른 수준의 물리/가상 리소스에 액세스할 수 있도록 허용하는 사전 정의된 권한 모음입니다. 여러 수준의 관리를 통해 정교한 권한 체계를 제공합니다. 예를 들어 데

이더 센터 관리자는 데이터 센터에 있는 모든 개체를 관리할 수 있는 권한이 있지만 호스트 관리자는 하나의 물리적 호스트에 대한 시스템 관리자 권한을 갖습니다. 사용자는 단일 가상 머신을 사용할 수 있는 권한은 있지만 가상 머신 설정을 변경할 수 있는 권한이 없는 반면 다른 사용자는 가상 머신에 시스템 권한을 할당할 수 있습니다.

1.2.2. 사용자 및 관리자 역할

Red Hat Virtualization에서는 시스템 전체의 권한을 갖는 관리자로부터 단일 가상 머신에 액세스할 수 있는 최종 사용자에게 이르기까지 사전 설정된 역할을 제공합니다. 기본 역할을 변경 또는 삭제할 수 없지만 이를 복제 또는 사용자 정의할 수 있으며 요구 사항에 따라 새 역할을 생성할 수 있습니다. 다음과 같은 두 가지 유형의 역할이 있습니다:

- 관리자 역할: 물리/가상 리소스를 관리하기 위해 *관리 포털*에 액세스할 수 있습니다. 관리자 역할에는 사용자 포털에서 실행할 수 있는 작업 권한이 부여되지만 사용자 포털에서 사용자에게 표시되는 항목을 지정할 수 없습니다.
- 사용자 역할: 가상 머신 및 템플릿에 액세스 및 관리하기 위해 *사용자 포털*에 액세스할 수 있습니다. 사용자 역할은 사용자 포털에서 사용자에게 표시되는 항목을 지정할 수 있습니다. 관리자 역할을 갖는 사용자에게 부여된 권한은 사용자 포털에 있는 사용자가 사용할 수 있는 작업에 반영됩니다.

예를 들어 클러스터에서 **administrator** 역할이 있는 경우 *관리 포털*을 사용하여 클러스터에 있는 모든 가상 머신을 관리할 수 있지만 *사용자 포털*에 있는 가상 머신에 액세스할 수 없습니다. 이를 위해 **user** 역할이 필요합니다.

1.2.3. 사용자 역할

다음 표에서는 사용자 포털에 있는 가상 머신에 액세스 및 설정하기 위한 권한을 부여하는 기본 사용자 역할에 대해 설명합니다.

표 1.1. Red Hat Virtualization 사용자 역할 - 기본

역할	권한	알림
UserRole	가상 머신과 풀에 액세스 및 사용할 수 있습니다.	사용자 포털에 로그인하여 지정된 가상 머신 및 풀을 사용하고 가상 머신 상태 및 상세 정보를 확인할 수 있습니다.
PowerUserRole	가상 머신 및 템플릿을 생성 및 관리할 수 있습니다.	설정 창을 사용하여 전체 환경에 대해 사용자에게 이 역할을 적용하거나 특정 데이터 센터 또는 클러스터에 이 역할을 적용할 수 있습니다. 예를 들어 데이터 센터 수준에서 PowerUserRole이 지정되어 있을 경우 PowerUser는 데이터 센터에 가상 머신 및 템플릿을 생성할 수 있습니다.

역할	권한	알림
UserVmManager	가상 머신의 시스템 관리자입니다.	가상 머신을 관리하고 스냅샷을 생성 및 사용할 수 있습니다. 사용자 포털에서 가상 머신을 생성한 사용자에게 자동으로 시스템의 UserVmManager 역할이 할당됩니다.

다음 표에서는 사용자 포털에 있는 리소스에 대한 사용 권한을 보다 정교하게 조정하기 위한 고급 사용자 역할에 대해 설명합니다.

표 1.2. Red Hat Virtualization 사용자 역할 - 고급

역할	권한	알림
UserTemplateBasedVm	템플릿만 사용하도록 권한을 제한합니다.	가상 머신을 생성하기 위한 템플릿을 사용할 수 있습니다.
DiskOperator	가상 디스크 사용자입니다.	가상 디스크를 사용, 보기, 편집할 수 있습니다. 가상 디스크가 연결된 가상 머신을 사용하기 위해 권한을 상속합니다.
VmCreator	사용자 포털에서 가상 머신을 생성할 수 있습니다.	이 역할은 특정 가상 머신에는 적용되지 않습니다. 설정 창을 사용하여 전체 환경에 대해 사용자에게 이 역할을 적용할 수 있습니다. 또는 특정 데이터 센터 또는 클러스터에 이 역할을 적용할 수 있습니다. 클러스터에 이 역할을 지정할 때 전체 데이터 센터나 특정 스토리지 도메인에서 DiskCreator 역할도 적용해야 합니다.
TemplateCreator	지정된 리소스 내에 있는 가상 머신 템플릿을 생성, 편집, 관리, 삭제할 수 있습니다.	이 역할은 특정 템플릿에는 적용되지 않습니다. 설정 창을 사용하여 전체 환경에 대해 사용자에게 이 역할을 적용할 수 있습니다. 또는 특정 데이터 센터, 클러스터, 스토리지 도메인에 이 역할을 적용할 수 있습니다.
DiskCreator	할당된 클러스터 또는 데이터 센터 내에서 가상 디스크를 생성, 편집, 관리, 제거할 수 있습니다.	이 역할은 특정 가상 디스크에는 적용되지 않습니다. 설정 창을 사용하여 전체 환경에 대한 사용자에게 이 역할을 적용할 수 있습니다. 또는 특정 데이터 센터, 스토리지 도메인에 이 역할을 적용할 수 있습니다.

역할	권한	알림
TemplateOwner	템플릿을 편집 및 삭제하고 템플릿의 사용자 권한을 할당 및 관리할 수 있습니다.	이 역할은 템플릿을 생성한 사용자에게 자동으로 할당됩니다. 템플릿에서 TemplateOwner 권한이 없는 다른 사용자는 템플릿을 확인 또는 사용할 수 없습니다.
VnicProfileUser	가상 머신 및 템플릿에 대한 논리 네트워크 및 네트워크 인터페이스 사용자입니다.	특정 논리 네트워크에서 네트워크 인터페이스를 연결 또는 분리할 수 있습니다.

1.2.4. 관리자 역할

다음 표에서는 관리 포털에 있는 리소스에 액세스 및 설정할 수 있는 권한을 부여하는 기본 관리자 역할에 대해 설명합니다.

표 1.3. Red Hat Virtualization 시스템 관리자 역할 - 기본

역할	권한	알림
SuperUser	Red Hat Virtualization 환경의 시스템 관리자입니다.	모든 개체 및 레벨에 걸쳐 완전한 권한을 가지며 모든 데이터 센터에 걸쳐 모든 개체를 관리할 수 있습니다.
ClusterAdmin	클러스터 관리자입니다.	특정 클러스터 하의 모든 개체에 대한 관리 권한을 갖습니다.
DataCenterAdmin	데이터 센터 관리자입니다.	스토리지를 제외한 특정 데이터 센터 하의 모든 개체에 대한 관리 권한을 갖습니다.



중요

Red Hat Virtualization 관리자로 디렉토리 서버의 관리자를 사용하지 않고 Red Hat Virtualization 관리자로 사용할 사용자를 생성합니다.

다음 표에서는 관리 포털에 있는 리소스에 대한 사용 권한을 보다 정교하게 조정하기 위한 고급 관리자 역할에 대해 설명합니다.

표 1.4. Red Hat Virtualization 시스템 관리자 역할 - 고급

역할	권한	알림
TemplateAdmin	가상 머신 템플릿의 관리자입니다.	스토리지 도메인 및 템플릿의 네트워크 정보를 생성, 삭제, 설정하고 도메인 간에 템플릿을 이동할 수 있습니다.

역할	권한	알림
StorageAdmin	스토리지 관리자입니다.	지정된 스토리지 도메인을 생성, 삭제, 설정, 관리할 수 있습니다.
HostAdmin	호스트 관리자입니다.	특정 호스트를 연결, 삭제, 설정, 관리할 수 있습니다.
NetworkAdmin	네트워크 관리자입니다.	특정 데이터 센터 또는 클러스터의 네트워크를 설정 및 관리할 수 있습니다. 데이터 센터 또는 클러스터의 네트워크 관리자는 클러스터 내의 가상 풀에 대한 네트워크 권한을 상속합니다.
VmPoolAdmin	가상 풀의 시스템 관리자입니다.	가상 풀을 생성, 삭제, 관리할 수 있습니다. 가상 풀 사용자를 지정 및 삭제하고 풀에 있는 가상 머신에서 기본 동작을 수행할 수 있습니다.
GlusterAdmin	Gluster 스토리지 관리자입니다.	Gluster 스토리지 볼륨을 생성, 삭제, 설정, 관리할 수 있습니다.
VmImporterExporter	가상 머신의 가져오기 및 내보내기 관리자입니다.	가상 머신을 가져오기 및 내보내기할 수 있습니다. 다른 사용자가 내보내기하는 모든 가상 머신과 템플릿을 볼 수 있습니다.

1.3. 스케줄링 정책

스케줄링 정책은 스케줄링 정책이 적용된 클러스터에 있는 호스트에서 가상 머신이 배포된 논리를 정의하는 규칙 모음입니다. 스케줄링 정책은 필터, 가중치, 로드 밸런싱 정책을 조합하여 이러한 논리를 지정합니다. Red Hat Virtualization Manager는 **Evenly_Distributed**, **InClusterUpgrade**, **None**, **Power_Saving**, **VM_Evenly_Distributed** 이렇게 5개의 기본 스케줄링 정책을 제공합니다. 가상 머신 배포에서 보다 정교하게 제어할 수 있는 새로운 스케줄링 정책을 정의할 수도 있습니다.

1.3.1. 스케줄링 정책 생성

새로운 스케줄링 정책을 생성하여 Red Hat Virtualization 환경에 있는 특정 클러스터에 가상 머신을 분배하는 로직을 제어할 수 있습니다.

절차 1.3. 스케줄링 정책 생성

1. 관리 포털의 머릿글 표시줄에 있는 **설정** 버튼을 클릭하여 **설정** 창을 엽니다.
2. **스케줄링 정책**을 클릭하여 스케줄링 정책 탭을 표시합니다.
3. **새로 만들기**를 클릭하여 새 스케줄링 정책 창을 엽니다.

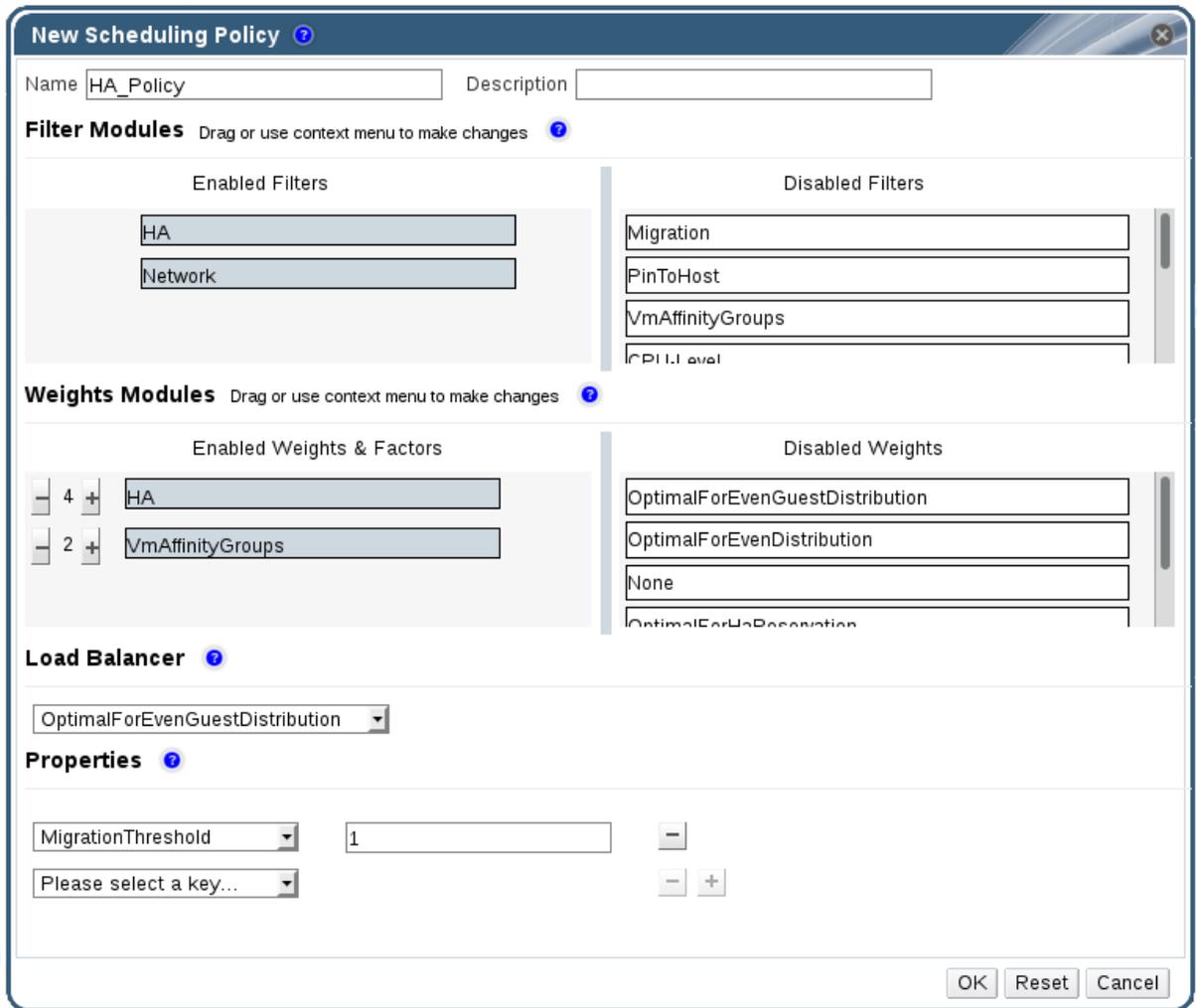


그림 1.6. 새 스케줄링 정책 창

4. 스케줄링 정책의 이름 및 설명을 입력합니다.
5. 필터 모듈을 설정합니다:
 - a. 필터 모듈 섹션의 비활성화된 필터 섹션에서 스케줄링 정책에 적용할 필터 모듈을 드래그하여 활성화된 필터 섹션에 드롭합니다.
 - b. 특정 필터 모듈을 첫 번째로 설정하여 가장 높은 우선순위를 지정하거나 마지막으로 설정하여 가장 낮은 우선 순위로 기본 최적화할 수 있습니다.

우선순위를 설정하려면 필터 모듈을 오른쪽 클릭하여 위치에 가리키면 표시되는 커서에서 첫 번째 또는 마지막으로 선택합니다.
6. 가중치 모듈을 설정합니다:
 - a. 가중치 모듈 섹션의 비활성화된 가중치 섹션에서 스케줄링 정책에 적용할 가중치 모듈을 드래그하여 활성화된 가중치 및 계수 섹션에 드롭합니다.
 - b. 활성화된 가중치 모듈 왼쪽에 있는 + 및 -을 사용하여 해당 모듈의 가중치를 증가 또는 감소시킬 수 있습니다.
7. 로드 밸런싱 정책을 지정합니다:
 - a. 로드 밸런서 부분의 드롭 다운 메뉴에서 스케줄링 정책에 적용할 로드 밸런싱 정책을 선택합니다.

b. 속성 섹션의 드롭 다운 메뉴에서 스케줄링 정책에 적용할 로드 밸런싱 속성을 선택하고 속성 오른쪽에 있는 텍스트 필드에 값을 지정합니다.

c. + 및 - 버튼을 사용하여 속성을 추가하거나 삭제합니다.

8. OK를 클릭합니다.

1.3.2. 새 스케줄링 정책 및 스케줄링 정책 편집 창 설정

다음 표에서는 새 스케줄링 정책 및 스케줄링 정책 편집 창에서 사용할 수 있는 옵션에 대해 설명합니다.

표 1.5. 새 스케줄링 정책 및 스케줄링 정책 편집 설정

필드 이름	설명
이름	스케줄링 정책 이름입니다. Red Hat Virtualization Manager에서 스케줄링 정책을 참조하기 위해 사용되는 이름입니다.
설명	스케줄링 정책을 설명합니다. 이 필드는 권장 입력 사항이며 필수 입력 사항은 아닙니다.

필드 이름	설명
필터 모듈	<p>클러스터에 있는 가상 머신이 실행할 수 있는 호스트를 제어하기 위한 필터 모듈입니다. 필터를 활성화하면 필터에 의해 지정된 다음과 같은 조건에 맞지 않는 호스트는 필터에서 제외됩니다:</p> <ul style="list-style-type: none"> • CpuPinning: CPU 핀 설정 정의를 충족시키지 않는 호스트입니다. • Migration: 동일한 호스트에 마이그레이션되지 않도록 방지합니다. • PinToHost: 가상 머신이 고정된 호스트 이외의 호스트입니다. • CPU-Level: 가상 머신의 CPU 토폴로지에 적합하지 않은 호스트입니다. • CPU: 가상 머신에 할당된 수 보다 적은 CPU가 있는 호스트입니다. • Memory: 가상 머신을 실행하기에 메모리가 충분하지 않은 호스트입니다. • VmAffinityGroups: 선호도 그룹에 속한 가상 머신에 지정된 조건에 맞지 않는 호스트입니다. 예를 들어 선호도 그룹에 있는 가상 머신은 동일한 호스트 또는 다른 호스트에서 실행해야 합니다. • InClusterUpgrade: 현재 가상 머신이 실행 중인 운영 체제 이전의 운영 체제에 실행되는 호스트입니다. • HostDevice: 가상 머신이 필요로 하는 호스트 장치를 지원하지 않는 호스트입니다. • HA: 호스팅 engine 가상 머신이 양의 고가용성 점수를 갖는 호스트에서만 실행되도록 강제합니다. • Emulated-Machine: 제대로 된 에뮬레이션된 시스템 지원이 없는 호스트입니다. • Network: 가상 머신의 네트워크 인터페이스 컨트롤러가 필요한 네트워크가 설치되지 않은 호스트 또는 클러스터의 디스플레이 네트워크가 설치되지 않은 호스트입니다.

필드 이름	설명
가중치 모듈	<p>가상 머신이 실행할 수 있는 클러스터에서 호스트를 지정할 때 고려할 요소의 상대적 우선순위를 제어하기 위한 가중치 모듈입니다.</p> <ul style="list-style-type: none"> • InClusterUpgrade: 호스트의 운영 체제 버전에 따라 호스트에 가중치를 부여합니다. 동일한 운영 체제의 호스트보다 이전 운영 체제의 호스트에 별점을 줘서 더 새로운 운영 체제의 호스트에 우선순위를 줍니다. • OptimalForHaReservation: 고가용성 점수에 따라 호스트에 가중치를 부여합니다. • None: 부하 균등 배분 모듈에 따라 가중치를 부여합니다. • OptimalForEvenGuestDistribution: 호스트에서 실행되는 가상 머신 수에 따라 호스트에 가중치를 부여합니다. • VmAffinityGroups: 가상 머신에 정의된 선호도 그룹에 따라 호스트에 가중치를 부여합니다. 이러한 가중치 모듈은 선호도 그룹에 있는 가상 머신이 선호도 그룹의 매개변수에 따라 동일한 호스트 또는 다른 호스트에서 실행할 지를 결정합니다. • OptimalForPowerSaving: CPU 사용량에 따라 호스트에 가중치를 부여하여 CPU 사용량이 높은 호스트에 우선순위를 줍니다. • OptimalForEvenDistribution: CPU 사용량에 따라 호스트에 가중치를 부여하여 CPU 사용량이 낮은 호스트에 우선순위를 줍니다. • HA: 고가용성 점수에 따라 호스트에 가중치를 부여합니다.
로드 밸런서	<p>이 드롭 다운 메뉴에서는 적용할 로드 밸런싱 모듈을 선택할 수 있습니다. 로드 밸런싱 모듈은 사용률이 높은 호스트에서 사용률이 낮은 호스트로 가상 머신을 마이그레이션하기 위해 사용되는 논리를 결정합니다.</p>
속성	<p>이 드롭 다운 메뉴에서는 로드 밸런싱 모듈의 속성을 추가 또는 삭제할 수 있으며 스케줄링 정책의 로드 밸런싱 모듈을 선택한 경우에만 사용할 수 있습니다. 기본값으로 속성은 지정되어 있지 않으며 사용 가능한 속성은 선택한 로드 밸런싱 모듈에 따라 다릅니다. + 및 - 버튼을 사용하여 로드 밸런싱 모듈에서 속성을 추가 또는 삭제합니다.</p>

1.4. 인스턴스 유형

인스턴스 유형을 사용하여 가상 머신의 하드웨어 설정을 정의할 수 있습니다. 가상 머신을 생성하거나 편집할 때 인스턴스 유형을 선택하면 하드웨어 설정 필드가 자동으로 작성됩니다. 이로 인해 사용자는 수동으로 모든 필드를 작성하지 않고 동일한 하드웨어 설정으로 된 가상 머신을 여러 개 설정할 수 있습니다.

다음 표에서 볼 수 있듯이 사전 정의된 인스턴스 유형을 기본값으로 사용할 수 있습니다:

표 1.6. 사전 정의된 인스턴스 유형

이름	메모리	vCPU
매우 작게 (Tiny)	512 MB	1
작게 (Small)	2 GB	1
중간 (Medium)	4 GB	2
크게 (Large)	8 GB	2
아주 크게 (XLarge)	16 GB	4

관리자는 설정 창의 인스턴스 유형 탭에서 인스턴스 유형을 생성, 편집, 삭제할 수 있습니다.

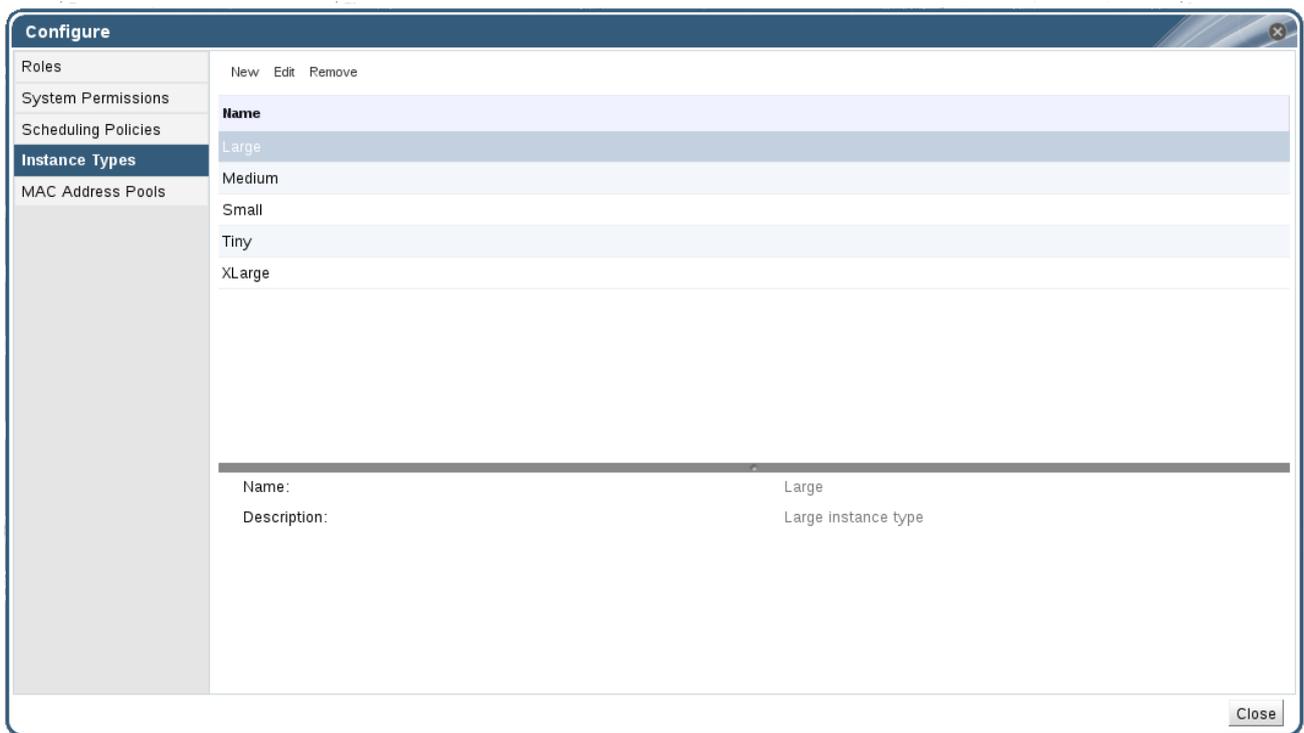


그림 1.7. 인스턴스 유형 탭

인스턴스 유형에 바운딩된 새 가상 머신 및 가상 머신 편집 창에 있는 필드 옆에는 체인 링크 이미지가 있습니다 (). 이 필드의 값을 변경하면 가상 머신은 인스턴스 유형에서 분리되어 사용자 정의로 변경되고 체인 링크가 분리된 이미지가 표시됩니다 (). 하지만 값을 다시 변경할 경우 체인 이미지는 다시 연결되어 인스턴스 유형은 선택한 인스턴스 유형으로 돌아갑니다.

1.4.1. 인스턴스 유형 생성

관리자는 가상 머신을 생성 또는 편집시 사용자가 선택할 수 있는 새로운 인스턴스 유형을 생성할 수 있습니다.

절차 1.4. 인스턴스 유형 생성

1. 머릿글 표시줄에서 **설정**을 클릭합니다.
2. **인스턴스 유형** 탭을 클릭합니다.
3. **새로 만들기** 버튼을 클릭하여 **새 인스턴스 유형** 창을 엽니다.

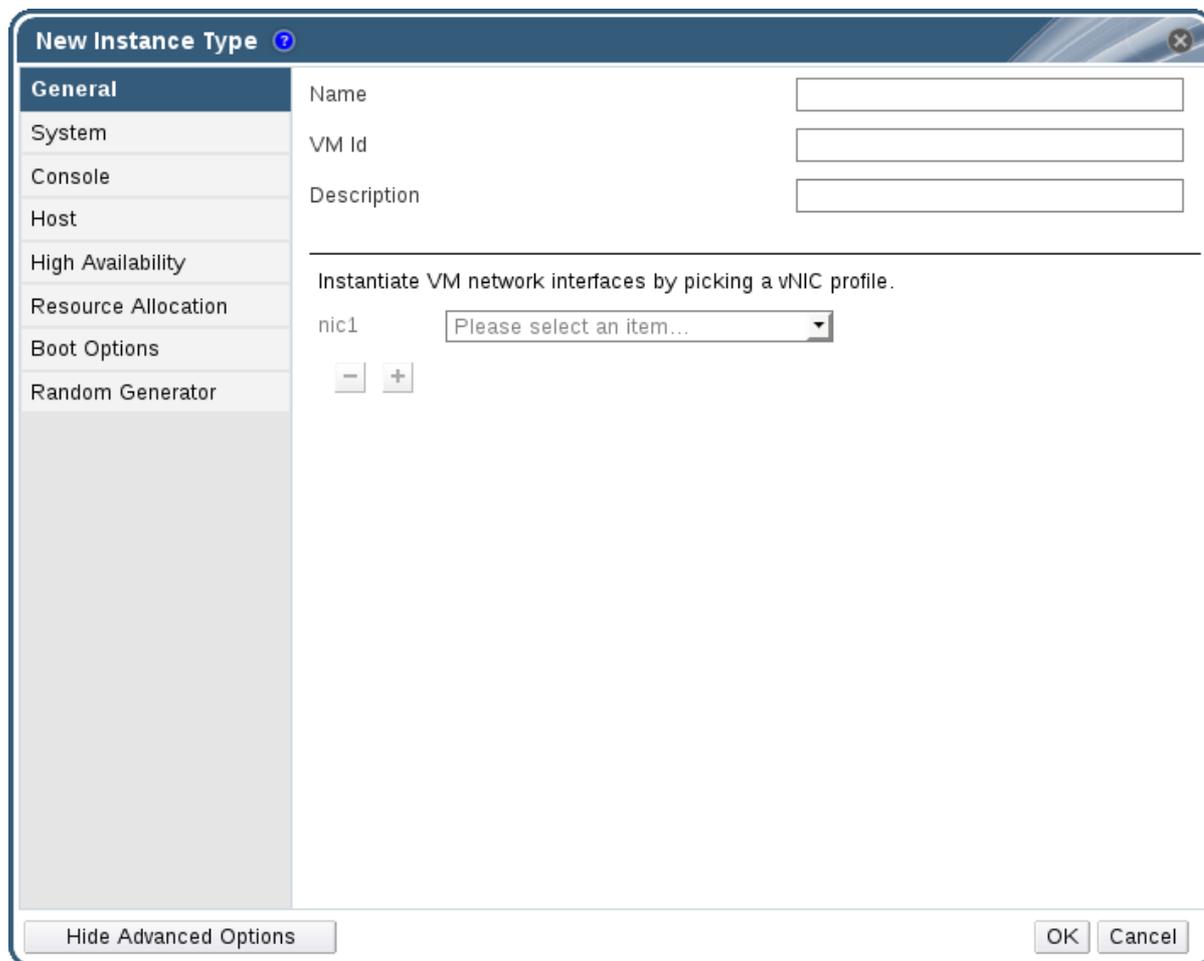


그림 1.8. 새 인스턴스 유형 창

4. 인스턴스 유형의 **이름** 및 **설명**을 입력합니다.
5. **고급 옵션 표시**를 클릭하여 필요에 따라 인스턴스 유형을 설정합니다. **새 인스턴스 유형** 창에 표시되는 설정은 **새 가상 머신** 창에 표시되는 내용과 동일하지만 관련 필드만 표시됩니다. 자세한 내용은 [가상 머신 관리 가이드](#)에 있는 [새 가상 머신 및 가상 머신 편집 창 설정에 대한 설명](#)을 참조하십시오.
6. **OK**를 클릭합니다.

새 인스턴스 유형은 **설정** 창에 있는 **인스턴스 유형** 탭에 나타나며 가상 머신을 생성하거나 편집할 때 **인스턴스 유형** 드롭 다운 목록에서 선택할 수 있습니다.

1.4.2. 인스턴스 유형 편집

관리자는 **설정** 창에서 기존 인스턴스 유형을 편집할 수 있습니다.

절차 1.5. 인스턴스 유형 속성 편집

1. 머릿글 표시줄에서 **설정**을 클릭합니다.
2. **인스턴스 유형** 탭을 클릭합니다.
3. 편집할 인스턴스 유형을 선택합니다.
4. **편집** 버튼을 클릭하여 **인스턴스 유형 편집** 창을 엽니다.
5. 필요에 따라 설정을 변경합니다.
6. **OK**를 클릭합니다.

인스턴스 유형 설정이 업데이트됩니다. 인스턴스 유형에 기반하는 새 가상 머신 및 다시 시작된 기존 가상 머신 모두 새 설정을 사용하게 됩니다.

1.4.3. 인스턴스 유형 삭제

절차 1.6. 인스턴스 유형 삭제

1. 머릿글 표시줄에서 **설정**을 클릭합니다.
2. **인스턴스 유형** 탭을 클릭합니다.
3. 삭제할 인스턴스 유형을 선택합니다.
4. **삭제** 버튼을 클릭하여 **인스턴스 유형 삭제** 창을 엽니다.
5. 가상 머신이 제거할 인스턴스 유형에 기반하는 경우 연결된 가상 머신이 나열된 경고 창이 나타납니다. 인스턴스 유형을 계속 제거하려면 **승인** 체크박스를 클릭합니다. 그렇지 않을 경우 **취소**를 클릭합니다.
6. **OK**를 클릭합니다.

인스턴스 유형은 **인스턴스 유형** 목록에서 삭제되어 새 가상 머신을 생성할 때 더 이상 사용할 수 없게 됩니다. 삭제된 인스턴스 유형에 연결된 모든 가상 머신은 **사용자 정의**(인스턴스 유형 없음)에 연결됩니다.

1.5. MAC 주소 풀

MAC 주소 풀은 각 클러스터에 할당된 MAC 주소의 범위를 정의합니다. 각 클러스터에 MAC 주소 풀이 지정됩니다. Red Hat Virtualization에서는 MAC 주소 풀을 사용하여 새 가상 네트워크 장치에 MAC 주소를 자동으로 생성 및 할당하며 이는 MAC 주소가 중복되지 않도록 하는 데 도움이 됩니다. MAC 주소 풀은 클러스터와 관련된 모든 MAC 주소가 할당된 MAC 주소 풀 범위 내에 있을 때 메모리 효율성이 더 높습니다.

여러 클러스터에서 동일한 MAC 주소 풀을 공유할 수 있지만 각 클러스터에는 단일 MAC 주소 풀만 할당됩니다. 다른 MAC 주소 풀이 할당되지 않은 경우 Red Hat Virtualization에서 기본 MAC 주소 풀을 생성하여 사용합니다. 클러스터에 MAC 주소 풀을 할당하는 방법에 대한 자세한 내용은 [5.2.1절. "새 클러스터 생성"](#)에서 참조하십시오.

MAC 주소 풀은 해당 풀에 마지막으로 반환된 주소 다음으로 사용 가능한 MAC 주소를 지정합니다. 범위에 남은 주소가 없는 경우 해당 범위 처음부터 검색이 다시 시작됩니다. 단일 MAC 주소 풀에 사용 가능한 MAC 주소가 있는 MAC 주소 범위가 여러 개 있는 경우 MAC 주소가 선택되는 방법과 같은 방법으로 해당 범위는 들어오는 요청을 차례대로 수행합니다.

1.5.1. MAC 주소 풀 생성

새로운 Mac 주소 풀을 생성할 수 있습니다.

절차 1.7. MAC 주소 풀 생성

1. 머릿글 표시줄에서 **설정** 버튼을 클릭하여 **설정** 창을 엽니다.
2. **MAC** 주소 풀 탭을 클릭합니다.
3. 추가 버튼을 클릭하여 새 **MAC** 주소 풀 창을 엽니다.

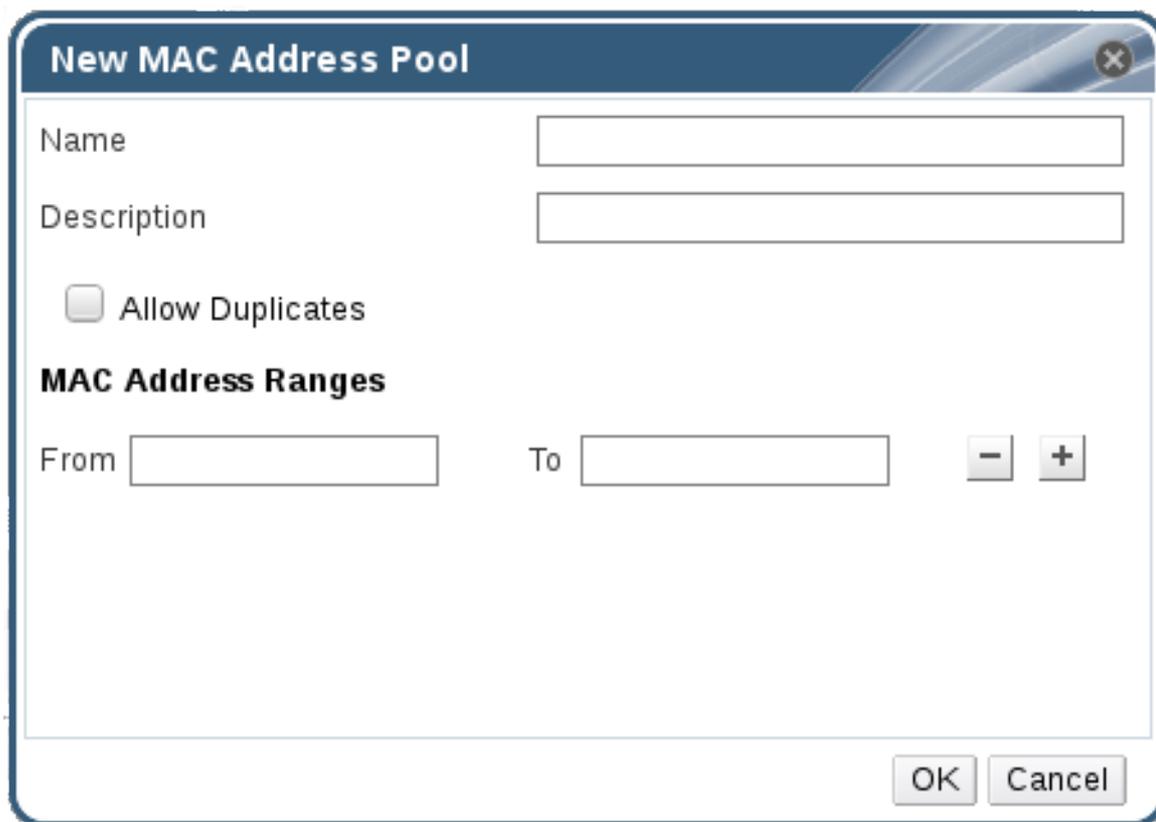


그림 1.9. 새 MAC 주소 풀 창

4. 새 MAC 주소 풀의 이름 및 설명을 입력합니다.
5. 중복 허용 확인란을 선택하면 MAC 주소가 풀에서 여러 번 사용됩니다. MAC 주소 풀이 중복되는 MAC 주소를 자동적으로 사용하지는 않지만 중복 허용 옵션을 활성화하면 사용자가 중복되는 MAC 주소를 수동으로 사용할 수 있습니다.



참고

하나의 MAC 주소 풀이 중복 옵션을 비활성화하고 다른 MAC 주소 풀이 중복 옵션을 활성화하면 각 MAC 주소는 중복이 비활성화된 풀에서는 한 번 사용되지만 중복이 활성화된 풀에서는 여러 번 사용될 수 있습니다.

6. 필요한 MAC 주소 범위를 입력합니다. 범위를 여러 개 입력하려면 범위 시작 및 범위 끝 필드 옆의 플러스 버튼을 클릭합니다.
7. **OK**를 클릭합니다.

1.5.2. MAC 주소 풀 편집

MAC 주소 풀을 편집해서 해당 풀의 사용 가능한 MAC 주소 범위 또는 중복 허용 여부 등을 변경합니다.

절차 1.8. MAC 주소 풀 속성 편집

1. 머리글 표시줄에서 **설정** 버튼을 클릭하여 **설정** 창을 엽니다.
2. **MAC 주소 풀** 탭을 클릭합니다.
3. 편집할 **MAC 주소 풀**을 선택합니다.
4. **편집** 버튼을 클릭하여 **MAC 주소 풀 편집** 창을 엽니다.
5. 필요에 따라 **이름**, **설명**, **중복 허용** 및 **MAC 주소 범위**란을 변경합니다.



참고

MAC 주소 범위가 업데이트되는 경우 기존 NIC의 MAC 주소는 재할당되지 않습니다. 이미 할당되었지만 새 MAC 주소 범위에서 벗어나는 MAC 주소는 사용자 지정 MAC 주소로 추가되며 계속해서 해당 MAC 주소 풀에서 추적됩니다.

6. **OK**를 클릭합니다.

1.5.3. MAC 주소 풀 권한 편집

MAC 주소 풀 생성 후 사용자 권한을 편집할 수 있습니다. 사용자 권한은 어느 데이터 센터가 해당 MAC 주소 풀을 사용할 수 있는지를 제어합니다. 새로운 사용자 권한 추가에 대한 정보는 [1.1절. "역할"](#)을 참조하십시오.

절차 1.9. MAC 주소 풀 권한 편집

1. 머리글 표시줄에서 **설정** 버튼을 클릭하여 **설정** 창을 엽니다.
2. **MAC 주소 풀** 탭을 클릭합니다.
3. 필요한 **MAC 주소 풀**을 선택합니다.
4. 해당 **MAC 주소 풀**의 사용자 권한을 편집합니다.
 - 해당 **MAC 주소 풀**에 사용자 권한을 추가합니다:
 - a. **설정** 창 아래의 사용자 권한 창에 있는 **추가** 버튼을 누릅니다.
 - b. 사용자를 검색 및 선택합니다.
 - c. **할당할 역할** 드롭 다운 목록에서 역할을 선택합니다.
 - d. **OK** 버튼을 클릭해서 사용자 권한을 추가합니다.
 - **MAC 주소 풀**에서 사용자 권한을 제거합니다:
 - a. **설정** 창 아래의 사용자 권한 창에서 제거할 사용자 권한을 선택합니다.
 - b. **제거** 버튼을 클릭해서 사용자 권한을 제거합니다.

1.5.4. MAC 주소 풀 삭제

생성된 MAC 주소 풀이 클러스터와 연결되어 있지 않은 경우 해당 풀을 제거할 수 있지만 기본 MAC 주소 풀은 제거할 수 없습니다.

절차 1.10. MAC 주소 풀 삭제

1. 머리글 표시줄에서 **설정** 버튼을 클릭하여 **설정** 창을 엽니다.
2. **MAC 주소 풀** 탭을 클릭합니다.
3. 삭제할 **MAC 주소 풀**을 선택합니다.
4. **삭제** 버튼을 클릭하여 **MAC 주소 풀 삭제** 창을 엽니다.
5. **OK**를 클릭합니다.

2장. 대시보드

대시보드는 Red Hat Virtualization 리소스 및 활용 상황을 요약 표시해서 Red Hat Virtualization 시스템 상태 개요를 제공합니다. 이 요약 표시 내용을 바탕으로 문제를 발견하고 분석할 수 있습니다.

대시보드 정보는 데이터 웨어하우스에서 기본값으로 15분마다 업데이트되거나, Manager API에 의해서 기본값으로 15초마다 새로고침되거나, 또는 대시보드가 새로고침될 때마다 새로고침됩니다. 대시보드는 사용자가 다른 탭에서 다시 오거나 수동으로 새로고침했을 때 새로고침됩니다. 대시보드는 자동으로 새로고침되지 않습니다. 인벤토리 카드 정보는 Manager API에서 제공되며 사용 정보는 데이터 웨어하우스에서 제공됩니다. 대시보드는 UI 플러그인 구성 요소로 구현되며 자동 설치되어 Manager와 함께 업그레이드됩니다.

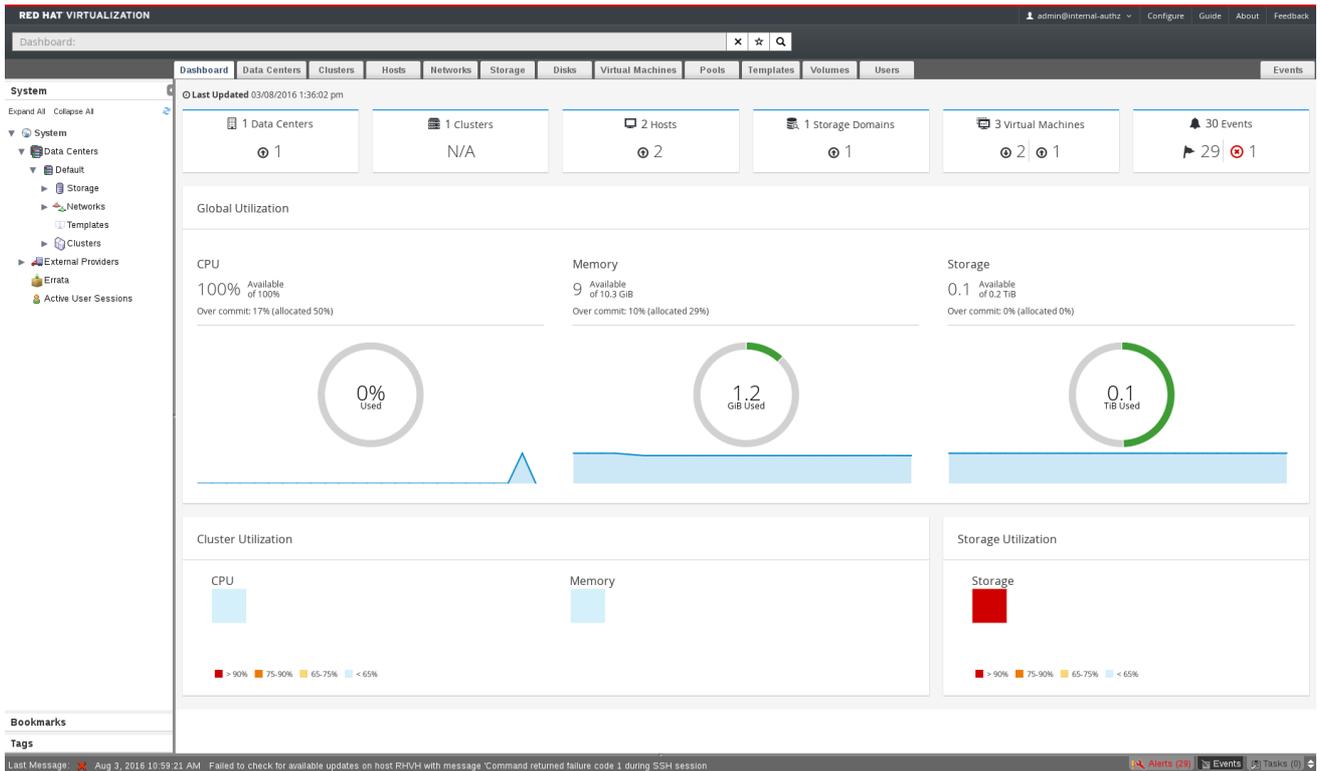


그림 2.1. 대시보드

2.1. 전제 조건

대시보드를 사용하려면 데이터 웨어하우스를 설치 및 설정해야 합니다. 데이터 웨어하우스 설치 및 설정에 대한 자세한 내용은 데이터 웨어하우스 가이드에 있는 데이터 웨어하우스 설치 및 설정을 참조하십시오.

2.2. 전체 인벤토리

대시보드 상단에는 Red Hat Virtualization 리소스의 전체 인벤토리가 제공되며 데이터 센터, 클러스터, 호스트, 스토리지 도메인, 가상 머신, 그리고 이벤트 등의 항목이 있습니다. 아이콘은 각 리소스 상태를 나타내며 숫자는 해당 상태의 리소스 수량을 나타냅니다.



그림 2.2. 전체 인벤토리

제목에는 각 리소스 종류의 수량이 표시되며 리소스 상태가 제목 밑에 표시됩니다. 리소스 제목을 클릭해서 Red Hat Virtualization Manager에 있는 해당 탭으로 갑니다. 클러스터 상태는 항상 해당 없음으로 표시됩니다.

표 2.1. 리소스 상태

아이콘	상태
	해당 리소스가 Red Hat Virtualization에 하나도 추가되지 않음.
	경고 상태의 리소스 수량이 표시됩니다. 아이콘을 클릭해서 해당 탭으로 가며 검색은 경고 상태의 리소스로 제한됩니다. 각 리소스별 검색 제한 방식이 다릅니다: <ul style="list-style-type: none"> • 데이터 센터: 동작이 되지 않거나 반응이 없는 데이터 센터로 검색이 제한됩니다. • 호스트: 미할당, 유지 보수 모드, 설치, 재부팅, 유지 보수 준비, 승인 대기, 또는 연결중인 호스트로 검색이 제한됩니다. • 스토리지 도메인: 초기화되지 않거나, 연결되지 않거나, 비활성, 유지 보수 모드, 유지 보수 준비, 분리, 또는 활성화 중인 스토리지 도메인으로 검색이 제한됩니다. • 가상 머신: 파워 업, 일시정지, 마이그레이션, 대기, 중단, 또는 꺼지고 있는 상태의 가상 머신으로 검색이 제한됩니다. • 이벤트: 그 심각성이 경고 상태인 이벤트로 검색이 제한됩니다.
	실행 중인 상태인 리소스 수량이 표시됩니다. 아이콘을 클릭해서 해당 탭으로 가며 검색은 실행 중인 상태의 리소스로 제한됩니다.
	정지 상태인 리소스 수량이 표시됩니다. 아이콘을 클릭해서 해당 탭으로 가며 검색은 정지 상태의 리소스로 제한됩니다. 각 리소스별 검색 제한 방식이 다릅니다: <ul style="list-style-type: none"> • 데이터 센터: 초기화되지 않거나, 유지 보수 모드, 또는 중지 상태의 데이터 센터로 검색이 제한됩니다. • 호스트: 반응이 없거나, 오류가 났거나, 설치 오류가 났거나, 동작이 되지 않거나, 초기화, 또는 중지 상태의 호스트로 검색이 제한됩니다. • 스토리지 도메인: 분리되거나 비활성화 상태의 스토리지 도메인으로 검색이 제한됩니다. • 가상 머신: 중지되거나, 반응이 없거나, 또는 재부팅 상태의 가상 머신으로 검색이 제한됩니다.
	경고 상태의 이벤트 수량이 표시됩니다. 아이콘을 클릭해서 이벤트 탭으로 가며 그 심각성이 경고 상태인 이벤트로 검색이 제한됩니다.
	오류 상태의 이벤트 수량이 표시됩니다. 아이콘을 클릭해서 이벤트 탭으로 가며 그 심각성이 오류 상태인 이벤트로 검색이 제한됩니다.

2.3. 전체 사용량

전체 사용량 부분에는 CPU, 메모리, 그리고 스토리지의 시스템 사용량이 표시됩니다.

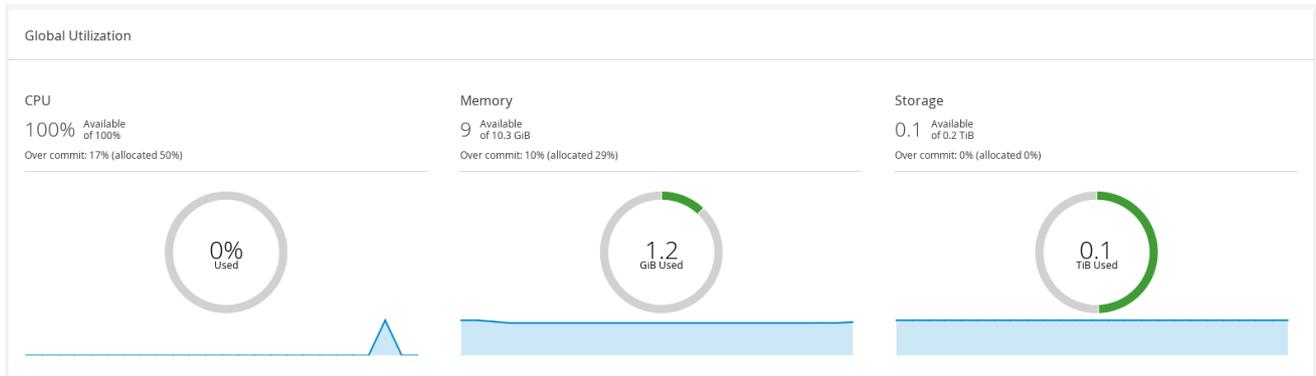


그림 2.3. 전체 사용량

- 윗부분에는 사용 가능 CPU, 메모리, 스토리지 등의 백분율이 표시되며 오버 커밋 비율이 표시됩니다. 예를 들어 CPU의 오버 커밋 비율 계산 시 가상 코어 수량을 데이터 웨어하우스의 최신 데이터를 바탕으로 가상 머신을 실행 가능한 물리 코어 수량으로 나눕니다.
- 도넛 모양에는 CPU, 메모리, 스토리지 등의 사용량이 백분율로 표시되며 최근 5분 동안의 평균 사용량을 바탕으로 모든 호스트의 평균 사용량이 표시됩니다. 도넛 모양의 어느 부분 위에 커서를 올리면 해당 부분의 값이 표시됩니다.
- 아랫부분의 선 그래프는 지난 24시간 동안의 트렌드를 보여줍니다. 각 데이터 포인트는 특정 시간의 평균 사용량을 보여줍니다. 그래프 상의 어느 부분 위에 커서를 올리면 CPU 그래프에 사용된 시간과 백분율이 표시되며 메모리 및 스토리지 그래프 사용량이 표시됩니다.

2.3.1. 가장 많이 사용된 리소스

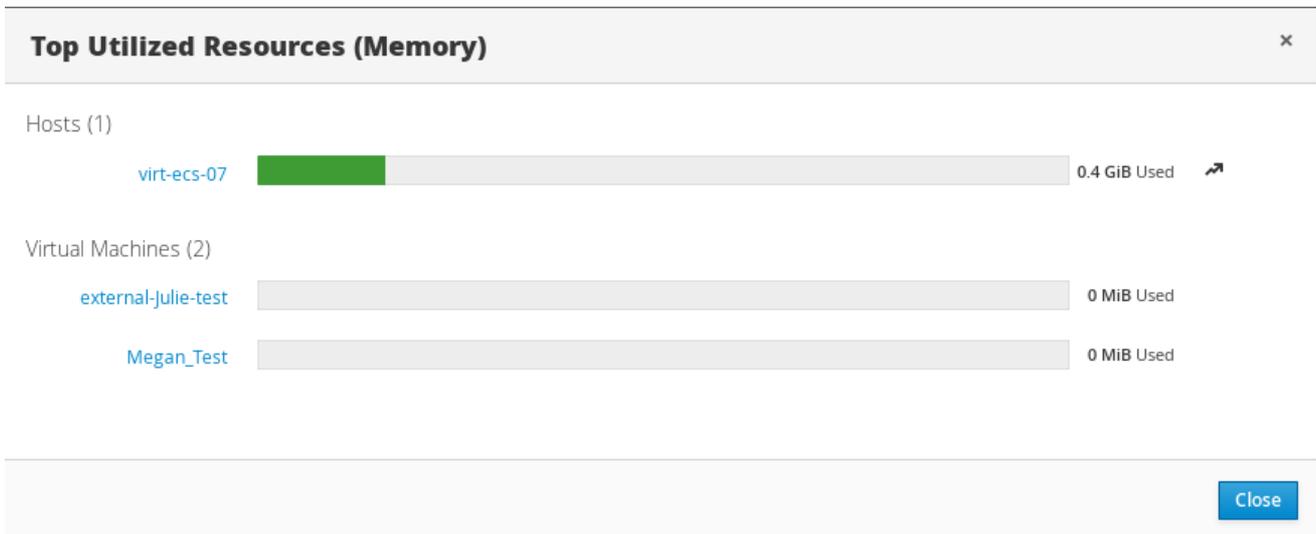


그림 2.4. 가장 많이 사용된 리소스 (메모리)

대시보드의 전체 사용량 부분의 도넛 모양을 클릭하면 CPU, 메모리, 스토리지의 사용량이 가장 높은 리소스 목록이 표시됩니다. CPU와 메모리의 경우 사용량이 가장 높은 상위 열 개의 호스트 및 가상 머신 목록이 팝업 창에 표시됩니다. 스토리지의 경우 사용량이 가장 높은 상위 열 개의 스토리지 및 가상 머신 목록이 팝업 창에 표시됩니다. 사용량 표시 줄 오른쪽의 화살표는 지난 1분 동안 해당 리소스의 사용 트렌드를 표시합니다.

2.4. 클러스터 사용량

클러스터 사용량 부분에는 CPU 및 메모리의 클러스터 사용량이 히트맵으로 표시됩니다.

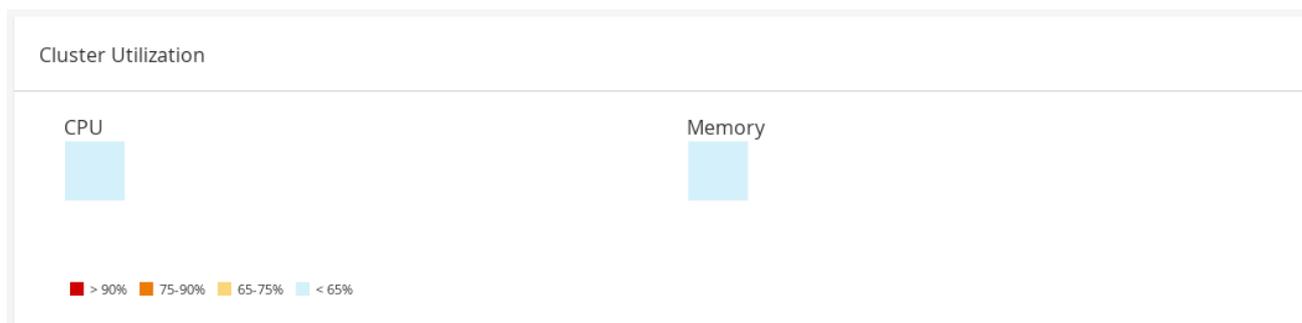


그림 2.5. 클러스터 사용량

2.4.1. CPU

특정 클러스터의 CPU 사용량을 나타내는 히트맵이며 지난 24시간 동안의 CPU 평균 사용량이 표시됩니다. 히트맵 위에 커서를 올리면 클러스터 이름이 표시됩니다. 히트맵을 클릭해서 호스트 탭으로 가며 특정 클러스터에 대해 CPU 사용량 순으로 정렬된 검색 결과가 표시됩니다. 클러스터의 CPU 사용량을 계산하는 공식은 클러스터에서의 평균 호스트 CPU 사용량입니다. 이를 계산하기 위해 지난 24시간 동안 각 호스트의 평균 호스트 CPU 사용량을 사용하여 해당 클러스터의 CPU 전체 평균 사용량을 계산합니다.

2.4.2. 메모리

특정 클러스터의 메모리 사용량을 나타내는 히트맵이며 지난 24시간 동안의 메모리 평균 사용량이 표시됩니다. 히트맵 위에 커서를 올리면 클러스터 이름이 표시됩니다. 히트맵을 클릭해서 호스트 탭으로 가며 특정 클러스터에 대해 메모리 사용량 순으로 정렬된 검색 결과가 표시됩니다. 클러스터의 메모리 사용량을 계산하는 공식은 클러스터에서의 메모리 총 사용량을 GB로 표시합니다. 이를 계산하기 위해 지난 24시간 동안 각 호스트의 평균 호스트 메모리 사용량을 사용하여 해당 클러스터의 메모리 전체 평균 사용량을 계산합니다.

2.5. 스토리지 사용량

스토리지 사용량 부분에는 스토리지 사용량이 히트맵으로 표시됩니다.

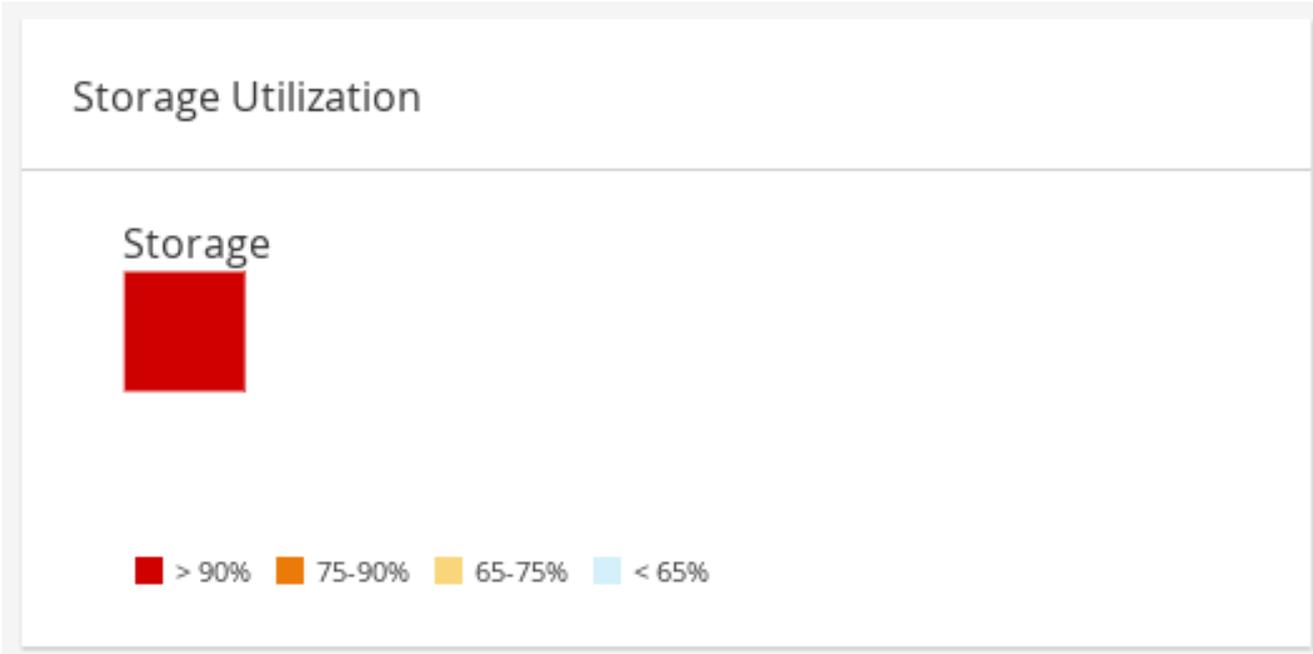


그림 2.6. 스토리지 사용량

지난 24시간 동안의 스토리지 평균 사용량이 표시되는 히트맵입니다. 클러스터의 스토리지 사용량을 계산하는 공식은 클러스터에서의 스토리지 총 사용량을 계산합니다. 이를 계산하기 위해 지난 24시간 동안 각 호스트의 평균 스토리지 사용량을 사용하여 해당 클러스터의 스토리지 전체 평균 사용량을 계산합니다. 히트맵 위에 커서를 올리면 스토리지 도메인 이름이 표시됩니다. 히트맵을 클릭해서 스토리지 탭으로 가며 스토리지 도메인이 사용량 순으로 정렬되어 표시됩니다.

II 부. 리소스 관리

3장. QOS (QUALITY OF SERVICE)

Red Hat Virtualization에서는 사용자 환경에 있는 리소스를 액세스할 수 있는 입출력, 처리, 네트워크 기능 정도에 대한 정교한 제어를 가능하게 하는 QoS (Quality of Service) 항목을 정의할 수 있습니다. QoS 항목은 데이터 센터 수준에서 정의되어 클러스터 및 스토리지 도메인 아래에서 생성된 프로파일에 지정됩니다. 이러한 프로파일은 프로파일이 생성된 클러스터 및 스토리지 도메인에 있는 개별 리소스에 지정됩니다.

3.1. 스토리지 QOS

스토리지 QoS는 스토리지 도메인에 있는 가상 디스크의 최대 입출력 수준 및 처리 가능한 최대 용량을 정의합니다. 스토리지 QoS를 가상 디스크에 지정하려면 스토리지 도메인 성능을 조정하고 가상 디스크와 관련된 스토리지 작업이 동일한 스토리지 도메인에서 호스팅되는 다른 가상 디스크에서 사용 가능한 스토리지 기능에 영향을 받지 않도록 할 수 있습니다.

3.1.1. 스토리지 QoS 항목 생성

스토리지 QoS 항목을 생성합니다.

절차 3.1. 스토리지 QoS 항목 생성

1. 데이터 센터 리소스 탭을 클릭하고 데이터 센터를 선택합니다.
2. 상세 정보 창에서 **QoS**를 클릭합니다.
3. 스토리지를 클릭합니다.
4. 새로 만들기를 클릭합니다.
5. **QoS** 이름 필드에 QoS 항목 이름을 입력합니다.
6. 설명란에 QoS 항목에 대한 설명을 입력합니다.
7. QoS 처리량을 지정합니다:
 - a. 처리량 체크 상자를 선택합니다.
 - b. 합계란에 허용된 최대 처리량 합계를 입력합니다.
 - c. 읽기란에 읽기 작업에 허용되는 최대 처리량을 입력합니다.
 - d. 쓰기란에 쓰기 작업에 허용되는 최대 처리량을 입력합니다.
8. 입력 및 출력 QoS를 지정합니다:
 - a. **IOPS** 체크 상자를 선택합니다.
 - b. 합계 필드에 초당 최대 허용 입출력 작업 수를 입력합니다.
 - c. 읽기 필드에 초당 최대 허용 입력 작업 수를 입력합니다.
 - d. 쓰기 필드에 초당 최대 허용 출력 작업 수를 입력합니다.
9. **OK**를 클릭합니다.

스토리지 QoS 항목을 생성하고 데이터 센터에 속한 데이터 스토리지 도메인에 있는 항목에 기초하여 디스크 프로파일을 생성할 수 있습니다.

3.1.2. 스토리지 QoS 항목 삭제

기존 스토리지 QoS 항목을 삭제합니다.

절차 3.2. 스토리지 QoS 항목 삭제

1. 데이터 센터 리소스 탭을 클릭하고 데이터 센터를 선택합니다.
2. 상세 정보 창에서 **QoS**를 클릭합니다.
3. 스토리지를 클릭합니다.
4. 삭제할 스토리지 QoS 항목을 선택합니다.
5. 삭제를 클릭합니다.
6. 메시지가 나타나면 **OK**를 클릭합니다.

스토리지 QoS 항목이 삭제되어 이 항목은 더 이상 사용할 수 없습니다. 디스크 프로파일이 이 항목에 기반하고 있을 경우 해당 프로파일의 스토리지 QoS 항목은 자동으로 무제한 [**unlimited**]으로 설정됩니다.

3.2. 가상 머신 네트워크 QoS

가상 머신 네트워크 QoS(Quality of Service)는 개별적 가상 네트워크 인터페이스 컨트롤러의 인바운드 및 아웃바운드 트래픽 모두를 제한하기 위해 프로파일을 생성할 수 있게 하는 기능입니다. 이 기능을 사용하여 여러 레이어에서 대역폭을 제한하여 네트워크 리소스 사용을 제어할 수 있습니다.

3.2.1. 가상 머신 네트워크 QoS 항목 생성

가상 머신 네트워크 인터페이스 프로파일로 알려진 가상 네트워크 인터페이스 컨트롤러 (vNIC)에 적용 시 네트워크 트래픽을 조정할 가상 머신 네트워크 QoS 항목을 생성합니다.

절차 3.3. 가상 머신 네트워크 QoS 항목 생성

1. 데이터 센터 리소스 탭을 클릭하고 데이터 센터를 선택합니다.
2. 상세 정보 창에서 **QoS** 탭을 클릭합니다.
3. 가상 머신 네트워크를 클릭합니다.
4. 새로 만들기를 클릭합니다.
5. 이름 필드에 가상 머신 네트워크 QoS 이름을 입력합니다.
6. 인바운드 및 아웃바운드 네트워크 트래픽 제한을 입력합니다.
7. **OK**를 클릭합니다.

가상 네트워크 인터페이스 컨트롤러에서 사용할 수 있는 가상 머신 네트워크 QoS가 생성됩니다.

3.2.2. 새 가상 머신 네트워크 QoS 설정 및 가상 머신 네트워크 QoS 편집

가상 머신 네트워크 QoS 설정을 통해 세 가지 레벨로 인바운드 및 아웃바운드 모두에 대한 대역폭 제한을 설정할 수 있습니다.

표 3.1. 가상 머신 네트워크 QoS 설정

필드 이름	설명
데이터 센터	가상 머신 네트워크 QoS 정책이 추가되는 데이터 센터입니다. 이 필드는 선택된 데이터 센터에 따라 자동으로 설정됩니다.
이름	Manager 내에서 가상 머신 네트워크 QoS 정책을 표시하기 위한 이름입니다.
인바운드	<p>인바운드 트래픽에 적용할 설정입니다. 이러한 설정을 활성화 또는 비활성화하려면 인바운드 확인란을 선택하거나 선택 취소합니다.</p> <ul style="list-style-type: none"> ● 평균: 인바운드 트래픽의 평균 속도입니다. ● 최대 값: 피크 (peak) 시간동안 인바운드 트래픽 속도입니다. ● 버스트: 버스트 동안 인바운드 트래픽 속도입니다.
아웃바운드	<p>아웃바운드 트래픽에 적용할 설정입니다. 이러한 설정을 활성화 또는 비활성화하려면 아웃바운드 확인란을 선택하거나 선택 취소합니다.</p> <ul style="list-style-type: none"> ● 평균: 아웃바운드 트래픽의 평균 속도입니다. ● 최대 값: 피크 (peak) 시간동안 아웃바운드 트래픽 속도입니다. ● 버스트: 버스트 동안 아웃바운드 트래픽 속도입니다.

3.2.3. 가상 머신 네트워크 QoS 항목 삭제

기존 가상 머신 네트워크 QoS 항목을 삭제합니다.

절차 3.4. 가상 머신 네트워크 QoS 항목 삭제

1. **데이터 센터** 리소스 탭을 클릭하고 데이터 센터를 선택합니다.
2. 상세 정보 창에서 **QoS** 탭을 클릭합니다.
3. **가상 머신 네트워크**를 클릭합니다.
4. 삭제할 가상 머신 네트워크 QoS 항목을 선택합니다.
5. **삭제**를 클릭합니다.

6. 메시지가 나타나면 **OK**를 클릭합니다.

가상 머신 네트워크 QoS 항목이 삭제되어 더 이상 이 항목을 사용할 수 없습니다.

3.3. 호스트 네트워크 QoS

호스트 네트워크 QoS는 호스트 네트워크를 설정해서 물리 인터페이스를 통한 네트워크 트래픽을 제어할 수 있게 해줍니다. 호스트 네트워크 QoS는 같은 네트워크 인터페이스 컨트롤러의 네트워크 리소스 사용을 제어해서 네트워크 성능을 정교하게 조정할 수 있게 해줍니다. 이를 통해 트래픽 과다 시 하나의 네트워크로 인해 같은 물리 네트워크 인터페이스의 다른 네트워크가 더 이상 작동을 하지 않는 상황을 막을 수 있습니다. 호스트 네트워크 QoS를 설정하면 해당 네트워크가 혼잡 문제 없이 같은 물리 네트워크 인터페이스에서 작동합니다.

3.3.1. 호스트 네트워크 QoS 항목 생성

호스트 네트워크 QoS 항목을 생성합니다.

절차 3.5. 호스트 네트워크 QoS 항목 생성

1. **데이터 센터** 리소스 탭을 클릭하고 데이터 센터를 선택합니다.
2. 상세 정보 창에서 **QoS**를 클릭합니다.
3. **호스트 네트워크**를 클릭합니다.
4. **새로 만들기**를 클릭합니다.
5. **QoS 이름** 필드에 QoS 항목 이름을 입력합니다.
6. **설명**란에 QoS 항목에 대한 설명을 입력합니다.
7. **가중 공유, 속도 제한 [Mbps], and 커밋 속도 [Mbps]** 항목에 원하는 값을 입력합니다.
8. **OK**를 클릭합니다.

3.3.2. 새 호스트 네트워크 QoS 설정 및 호스트 네트워크 QoS 편집

호스트 네트워크 QoS 설정을 통해 아웃바운드 트래픽에 대한 대역폭 제한을 설정할 수 있습니다.

표 3.2. 호스트 네트워크 QoS 설정

필드 이름	설명
데이터 센터	호스트 네트워크 QoS 정책이 추가되는 데이터 센터입니다. 이 필드는 선택된 데이터 센터에 따라 자동으로 설정됩니다.
QoS 이름	Manager 내에서 호스트 네트워크 QoS 정책을 표시하기 위한 이름입니다.
설명	호스트 네트워크 QoS 정책에 대한 설명입니다.

필드 이름	설명
아웃바운드	<p>아웃바운드 트래픽에 적용할 설정입니다.</p> <ul style="list-style-type: none"> • 가중 공유: 같은 논리 링크에 연결된 다른 네트워크와 비교해서 어떤 특정 네트워크에 해당 논리 링크의 용량이 얼마나 할당되는지를 나타냅니다. 정확한 공유량은 해당 링크의 모든 네트워크의 총 공유량에 따라 다릅니다. 기본으로 이 수치는 1-100 범위에 있습니다. • 속도 제한 [Mbps]: 네트워크가 사용하는 최대 대역폭입니다. • 커밋 속도 [Mbps]: 네트워크가 필요로 하는 최소 대역폭입니다. 사용자가 요청하는 커밋 속도는 보장되지 않으며 네트워크 인프라와 같은 논리 링크에 있는 다른 네트워크에서 요청하는 커밋 속도에 따라 다릅니다.

3.3.3. 호스트 네트워크 QoS 항목 삭제

기존 네트워크 QoS 항목을 삭제합니다.

절차 3.6. 호스트 네트워크 QoS 항목 삭제

1. 데이터 센터 리소스 탭을 클릭하고 데이터 센터를 선택합니다.
2. 상세 정보 창에서 **QoS** 탭을 클릭합니다.
3. **호스트 네트워크**를 클릭합니다.
4. 삭제할 네트워크 QoS 항목을 선택합니다.
5. 삭제를 클릭합니다.
6. 메시지가 나타나면 **OK**를 클릭합니다.

3.4. CPU QOS (QUALITY OF SERVICE)

CPU QoS (Quality of Service)는 가상 머신이 이를 실행하는 호스트에서 액세스할 수 있는 처리 가능한 최대 용량을 정의하고 호스트에서 사용 가능한 총 처리 용량의 백분율로 표시합니다. CPU QoS를 가상 머신에 지정하여 클러스터에 있는 하나의 가상 머신에서의 워크로드가 동일한 클러스터에 있는 다른 가상 머신에서 사용 가능한 처리 리소스에 영향을 미치지 않게 할 수 있습니다.

3.4.1. CPU QoS 항목 생성

CPU QoS 항목을 생성합니다.

절차 3.7. CPU QoS 항목 생성

1. 데이터 센터 리소스 탭을 클릭하고 데이터 센터를 선택합니다.
2. 상세 정보 창에서 **QoS**를 클릭합니다.
3. **CPU**를 클릭합니다.
4. 새로 만들기를 클릭합니다.
5. **QoS** 이름 필드에 QoS 항목 이름을 입력합니다.
6. 설명란에 QoS 항목에 대한 설명을 입력합니다.
7. 제한 필드에서 백분율로 QoS 최대 처리 용량을 입력합니다.% 기호를 입력하지 않습니다.
8. **OK**를 클릭합니다.

CPU QoS 항목이 생성되어 데이터 센터에 속한 클러그터에 있는 항목에 따라 CPU 프로파일을 생성할 수 있습니다.

3.4.2. CPU QoS 항목 삭제

기존 CPU QoS 항목을 삭제합니다.

절차 3.8. CPU QoS 항목 삭제

1. 데이터 센터 리소스 탭을 클릭하고 데이터 센터를 선택합니다.
2. 상세 정보 창에서 **QoS**를 클릭합니다.
3. **CPU**를 클릭합니다.
4. 삭제할 CPU QoS 항목을 선택합니다.
5. 삭제를 클릭합니다.
6. 메시지가 나타나면 **OK**를 클릭합니다.

CPU QoS 항목이 삭제되어 해당 항목을 더 이상 사용할 수 없습니다. CPU 프로파일이 해당 항목에 기반할 경우 해당 프로파일의 CPU QoS 항목은 무제한 **[unlimited]**으로 자동 설정됩니다.

4장. 데이터 센터

4.1. 데이터 센터 소개

데이터 센터는 특정 환경에서 사용되는 리소스를 정의하는 논리적 엔티티입니다. 데이터 센터는 클러스터 및 호스트 형태; 네트워크 리소스 형태, 논리 네트워크 및 물리적 NIC 및 스토리지 리소스 형태, 스토리지 도메인 형태와 같은 논리적 리소스로 구성되어 있다는 점에서 컨테이너 리소스로 간주됩니다.

데이터 센터는 여러 호스트를 포함할 수 있는 여러 클러스터에서 구성할 수 있습니다. 또한 데이터 센터에 여러 스토리지 도메인을 연결할 수 있으며 각 호스트에서 여러 가상 머신을 지원할 수 있습니다. Red Hat Virtualization 환경에는 여러 데이터 센터로 구성할 수 있으며 데이터 센터 인프라는 이러한 센터를 별도로 유지할 수 있습니다.

모든 데이터 센터는 단일 관리 포털에서 관리됩니다.

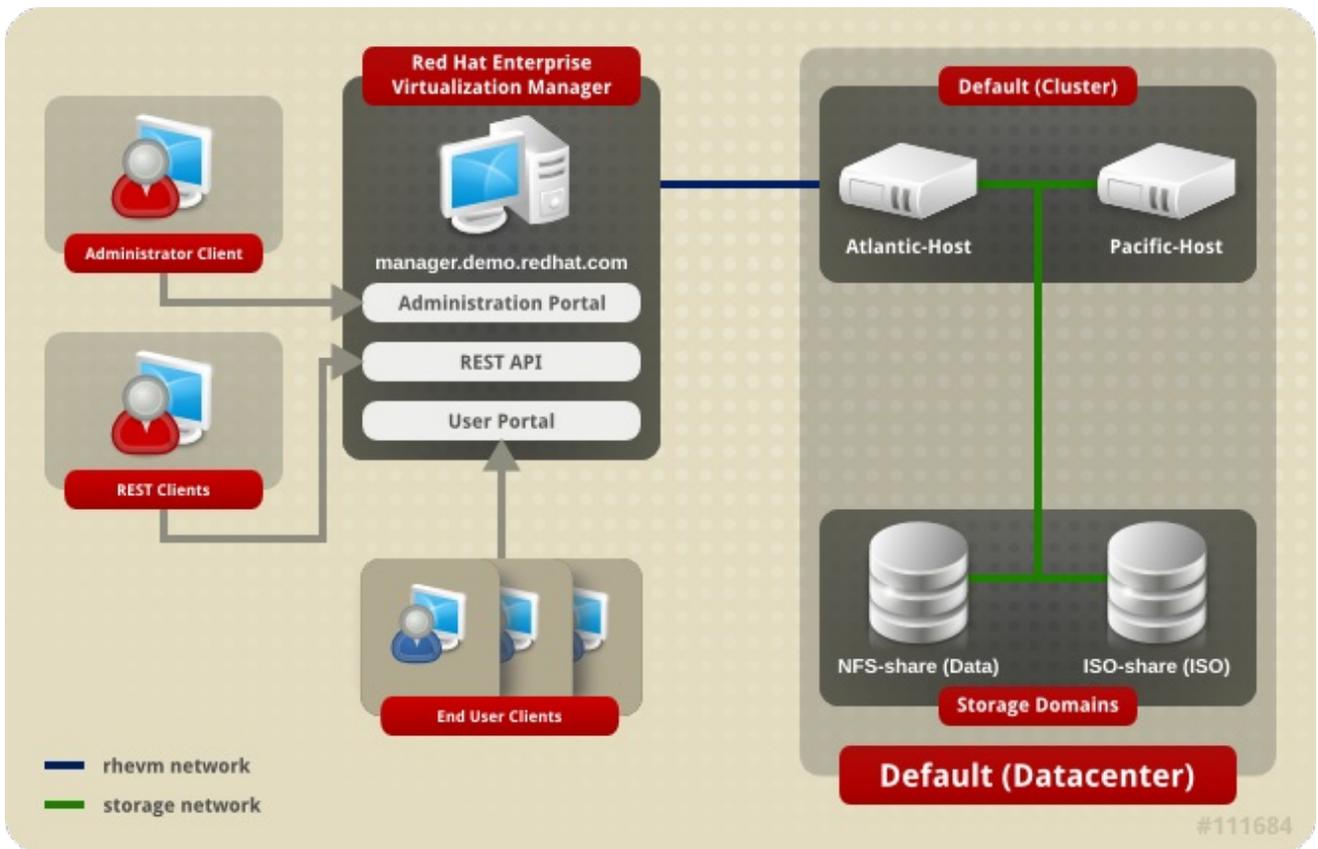


그림 4.1. 데이터 센터

Red Hat Virtualization은 설치 시 기본 데이터 센터를 생성합니다. 기본 데이터 센터를 설정하거나 이름을 지정하여 새로 데이터 센터를 설정할 수 있습니다.

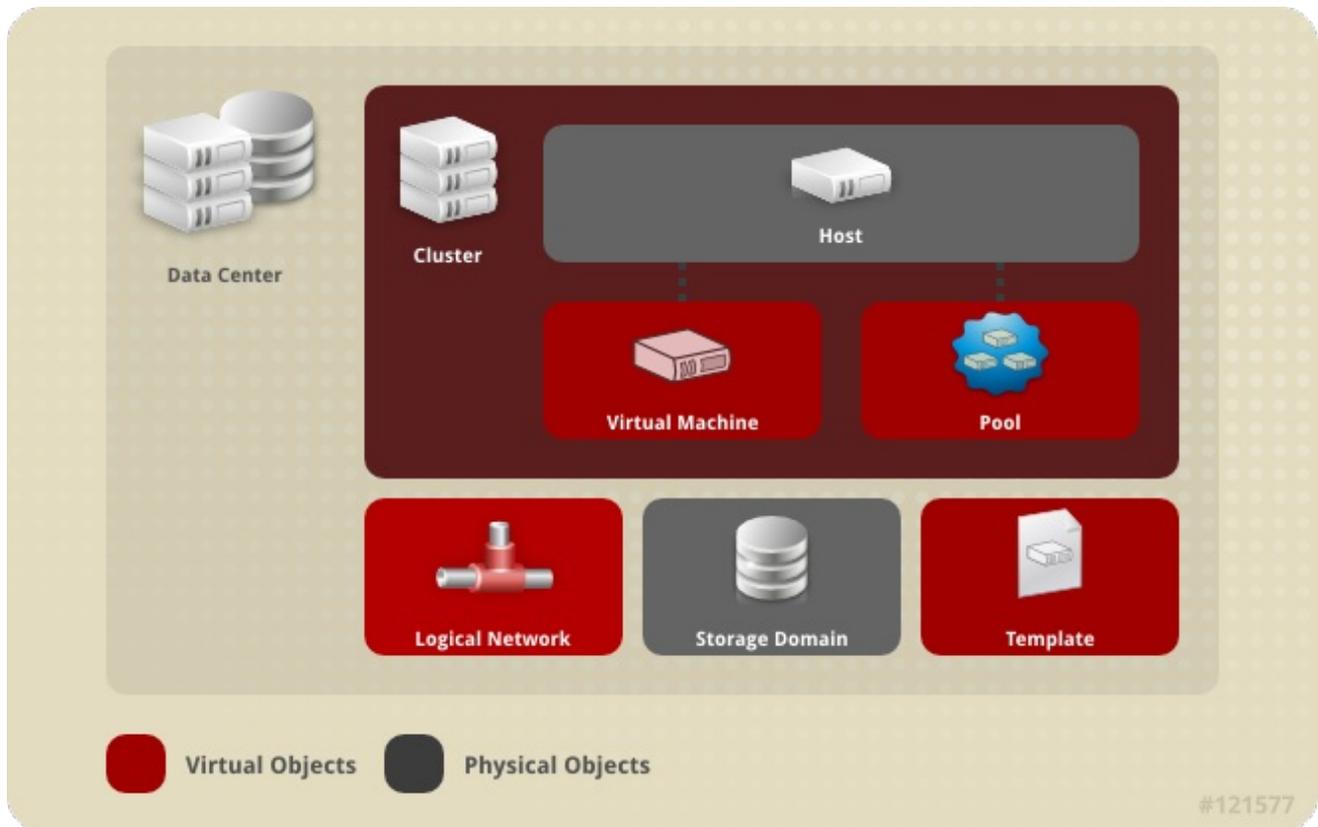


그림 4.2. 데이터 센터 개체

4.2. SPM (STORAGE POOL MANAGER)

SPM (Storage Pool Manager)는 데이터 센터의 스토리지 도메인을 관리하기 위해 데이터 센터에 있는 하나의 호스트에 지정된 역할입니다. SPM 엔티티는 데이터 센터에 있는 모든 호스트에서 실행할 수 있습니다. Red Hat Virtualization Manager는 하나의 호스트에 역할을 부여합니다. SPM에 의해 호스트가 표준 작업을 실행할 수 없는 것은 아니며 SPM으로 실행하는 호스트는 계속 가상 리소스를 호스팅할 수 있습니다.

SPM 엔티티는 스토리지 도메인 간의 메타데이터를 조정하여 스토리지로의 액세스를 제어합니다. 이는 가상 디스크 (이미지), 스냅샷, 템플릿을 생성, 삭제, 조정하고 (SAN 상의) 스파스 블록 장치에 대한 스토리지를 할당합니다. 이 역할은 배타적이며 메타데이터 무결성을 위해 한번에 하나의 호스트만 데이터 센터에서 SPM이 될 수 있습니다.

Red Hat Virtualization Manager는 SPM을 항상 사용할 수 있는지 확인합니다. Manager는 SPM 호스트가 스토리지에 액세스하는데 문제가 발생할 경우 SPM 역할을 다른 호스트로 옮깁니다. SPM을 시작하면 이는 유일한 호스트 역할이 부여되므로 스토리지 중심적이 됩니다. 이러한 절차에는 다소 시간이 소요될 수 있습니다.

4.3. SPM 우선순위

SPM 역할은 호스트의 사용 가능한 리소스 일부를 사용합니다. 호스트의 SPM 우선순위 설정으로 호스트에 SPM 역할이 할당될 가능성이 변경됩니다. 높은 SPM 우선순위를 갖는 호스트에는 낮은 SPM 우선순위의 호스트 보다 먼저 SPM 역할이 할당됩니다. 낮은 SPM 우선순위를 갖는 호스트에 있는 중요한 가상 머신은 호스트의 리소스에 대한 SPM 운영에 있어서 경합할 필요가 없습니다.

호스트를 편집하여 호스트의 SPM 우선순위를 변경할 수 있습니다.

4.4. 이벤트 탭을 사용하여 데이터 센터에서 문제가 있는 개체를 식별

데이터 센터의 **이벤트** 탭에서는 데이터 센터와 관련된 모든 이벤트를 표시합니다. 이벤트에는 감사, 경고, 오류 등이 포함됩니다. 결과 목록에 표시된 정보는 Red Hat Virtualization 환경에서 문제가 있는 개체를 식별하는데 사용할 수 있습니다.

이벤트 결과 목록에는 기본 보기 및 고급 보기의 두 가지 보기가 있습니다. 기본 보기에는 이벤트 아이콘, 이벤트, 시간, 이벤트 설명 등이 표시됩니다. 고급 보기에는 기본 보기에 있는 내용 이외에 이벤트 ID, 연결된 사용자, 호스트, 가상 머신, 템플릿, 데이터 센터, 스토리지, 클러스터, Gluster 볼륨, 상관 관계 ID 등이 표시됩니다.

4.5. 데이터 센터 작업

4.5.1. 새 데이터 센터 생성

다음 절차에서는 가상화 환경에 데이터 센터를 생성하는 방법에 대해 설명합니다. 데이터 센터에는 클러스터, 호스트, 스토리지 도메인 기능이 필요합니다.



참고

스토리지 **유형**은 첫 번째 스토리지 도메인이 데이터 센터에 추가될 때 까지 편집할 수 있습니다. 스토리지 도메인이 추가되면 스토리지 **유형**을 변경할 수 없습니다.

호환 버전을 한번 설정하고 난 후 하위 버전으로 변경하는 것은 허용되지 않습니다.

데이터 센터에 대한 **MAC** 풀 범위를 지정하는 옵션이 비활성화되었으며 이제 클러스터 수준에서 수행됩니다.

절차 4.1. 새 데이터 센터 생성

1. **데이터 센터** 리소스 탭을 선택하여 결과 목록에 모든 데이터 센터를 나열합니다.
2. **새로 만들기**를 클릭하여 **새로운 데이터 센터** 창을 엽니다.
3. 데이터 센터의 **이름** 및 **설명**을 입력합니다.
4. 드롭 다운 메뉴에서 데이터 센터의 **스토리지 유형**, **호환 버전**, **쿼터 모드**를 선택합니다.
5. **OK**를 클릭하여 데이터 센터를 생성하고 **데이터 센터 - 가이드** 창을 엽니다.
6. **가이드** 창에는 데이터 센터 설정에 필요한 엔티티가 나열됩니다. 이러한 엔티티를 설정하거나 **중에 설정** 버튼을 클릭하여 나중에 설정합니다. 설정을 다시 시작하려면 데이터 센터를 선택하고 **가이드** 버튼을 클릭합니다.

새 데이터 센터가 가상화 환경에 추가됩니다. 클러스터, 호스트, 스토리지 도메인이 설정되기 전 까지 **초기화되지 않음** 상태로 남아있게 됩니다. **가이드**를 사용하여 이러한 항목을 설정합니다.

4.5.2. 새 데이터 센터 및 데이터 센터 편집 창 설정

다음 표에서는 **새 데이터 센터** 및 **데이터 센터 편집** 창에 표시된 데이터 센터를 설정하는 방법에 대해 설명합니다. **OK**를 클릭 시 잘못된 항목은 주황색으로 표시되고 변경 사항이 적용되지 않습니다. 또한 필드 프롬프트에는 값의 예상 값 또는 예상 값 범위가 표시됩니다.

표 4.1. 데이터 센터 속성

필드	설명/동작
이름	데이터 센터 이름입니다. 텍스트 필드는 최대 40 자로 제한되어 있으며 알파벳 대문자, 소문자, 숫자, 하이픈, 밑줄로 조합된 고유한 이름이어야 합니다.
설명	데이터 센터 설명입니다. 이는 권장 사항이며 필수 입력 사항은 아닙니다.
유형	스토리지 유형입니다. 다음 중 하나를 선택합니다: <ul style="list-style-type: none"> • 공유 • 로컬 <p>데이터 도메인 유형에 따라 데이터 센터 유형을 지정하고 생성 후 서비스가 중단될 수 있으므로 수정하지 않습니다. 로컬 도메인과 공유 도메인을 혼합할 수 없지만 여러 유형의 스토리지 도메인 (iSCSI, NFS, FC, POSIX, Gluster)을 동일한 데이터 센터에 추가할 수 있습니다.</p>
호환성 버전	Red Hat Virtualization 버전입니다. 다음 중 하나를 선택합니다: <ul style="list-style-type: none"> • 3.6 • 4.0 • 4.1 <p>Red Hat Virtualization Manager로 업그레이드한 후 호스트, 클러스터, 데이터 센터가 이전 버전에 남아 있을 수 있습니다. 데이터 센터의 호환성 수준을 업그레이드하기 전 모든 호스트를 업그레이드한 후 클러스터를 업그레이드합니다.</p>
쿼터 모드	쿼터는 Red Hat Virtualization에 제공되는 리소스 제한 도구입니다. 다음 중 하나를 선택합니다: <ul style="list-style-type: none"> • 비활성화됨: 쿼터를 구현하지 않을 경우 선택합니다. • 감사: 쿼터 설정을 편집하고자 할 경우 선택합니다. • 강제 적용: 쿼터를 구현하고자 할 경우 선택합니다.

4.5.3. 데이터 센터 재초기화: 복구 절차

다음 복구 절차에서는 데이터 센터의 마스터 데이터 도메인을 새 마스터 도메인으로 대체합니다. 이는 마스터 데이터 도메인의 데이터가 손상된 경우에 필요합니다. 데이터 센터를 다시 초기화하여 클러스터, 호스트, 문제 없는 스토리지 도메인을 포함하여 데이터 센터에 연결된 모든 다른 리소스를 복구할 수 있습니다.

백업, 내보내기한 가상 머신 또는 템플릿을 새로운 마스터 데이터 도메인으로 가져올 수 있습니다.

절차 4.2. 데이터 센터 재초기화

1. 데이터 센터 리소스 탭을 클릭하여 재초기화할 데이터 센터를 선택합니다.
2. 데이터 센터에 연결된 스토리지 도메인이 유지 관리 모드인지를 확인합니다.
3. 데이터 센터를 오른쪽 클릭하고 드롭 다운 메뉴에서 **데이터 센터의 재 초기화**를 선택하여 **데이터 센터의 재 초기화** 창을 엽니다.
4. **데이터 센터의 재 초기화** 창에는 모든 사용 가능한 스토리지 도메인 목록이 표시됩니다. 데이터 센터에 추가하려는 스토리지 도메인의 라디오 버튼을 클릭합니다.
5. **작업 승인** 확인란을 선택합니다.
6. **OK**를 클릭하여 창을 닫고 데이터 센터를 다시 초기화합니다.

스토리지 도메인이 마스터 데이터 도메인으로 데이터 센터에 연결되어 활성화됩니다. 백업, 내보내기한 가상 머신, 템플릿을 새 마스터 데이터 도메인으로 가져올 수 있습니다.

4.5.4. 데이터 센터 삭제

데이터 센터를 삭제하려면 활성 호스트가 필요합니다. 데이터 센터를 삭제해도 데이터 센터에 연결된 리소스는 삭제되지 않습니다.

절차 4.3. 데이터 센터 삭제

1. 데이터 센터에 연결된 스토리지 도메인이 유지 관리 모드인지를 확인합니다.
2. **데이터 센터** 리소스 탭을 클릭하여 삭제할 데이터 센터를 선택합니다.
3. **삭제**를 클릭하여 **데이터 센터 삭제** 확인 창을 엽니다.
4. **OK**를 클릭합니다.

4.5.5. 데이터 센터 강제 삭제

연결된 스토리지 도메인이 손상되어 있거나 호스트가 **Non Responsive** 상태일 경우 데이터 센터는 **Non Responsive** 상태가 됩니다. 이러한 상태에서는 데이터 센터를 **삭제**할 수 없습니다.

강제 삭제에는 활성 호스트가 필요하지 않습니다. 이는 연결된 스토리지 도메인도 영구적으로 삭제합니다.

데이터 센터를 **강제 삭제**하기 전 손상된 스토리지 도메인을 **삭제**해야 합니다.

절차 4.4. 데이터 센터 강제 삭제

1. **데이터 센터** 리소스 탭을 클릭하여 삭제할 데이터 센터를 선택합니다.
2. **강제 삭제**를 클릭하여 **데이터 센터 강제 삭제** 확인 창을 엽니다.
3. **작업 승인** 확인란을 선택합니다.
4. **OK**를 클릭합니다.

데이터 센터 및 연결된 스토리지 도메인이 Red Hat Virtualization 환경에서 영구적으로 삭제됩니다.

4.5.6. 데이터 센터 호환 버전 변경

Red Hat Virtualization 데이터 센터에는 호환 버전이 있습니다. 호환 버전은 데이터 센터와 호환되는 Red Hat Virtualization 버전을 나타냅니다. 데이터 센터에 있는 모든 클러스터는 원하는 호환 수준을 지원해야 합니다.



참고

데이터 센터 호환 버전을 변경하려면 먼저 데이터 센터에 있는 모든 클러스터를 원하는 호환 수준을 지원하는 레벨로 업데이트해야 합니다.

절차 4.5. 데이터 센터 호환 버전 변경

1. 관리 포털에서 **데이터 센터** 탭을 클릭합니다.
2. 표시된 목록에서 변경하려는 데이터 센터를 선택합니다.
3. **편집**을 클릭합니다.
4. **호환 버전**을 원하는 값으로 변경합니다.
5. **OK**를 클릭하여 **데이터 센터 호환 버전 변경** 확인 창을 엽니다.
6. **OK**를 클릭하여 확인합니다.

데이터 센터의 호환 버전이 업데이트됩니다.



중요

호환성을 업그레이드하면 데이터 센터에 속한 모든 스토리지 도메인도 업그레이드됩니다.

4.6. 데이터 센터 및 스토리지 도메인

4.6.1. 데이터 센터에 기존 데이터 도메인 연결

연결 해제 데이터 도메인은 데이터 센터에 연결할 수 있습니다. 여러 유형 (iSCSI, NFS, FC, POSIX, Gluster)의 공유 스토리지 도메인은 동일한 데이터 센터에 추가할 수 있습니다.

절차 4.6. 데이터 센터에 기존 데이터 도메인 연결

1. **데이터 센터 리소스** 탭을 클릭하여 적절한 데이터 센터를 선택합니다.
2. 상세 정보 창에서 **스토리지** 탭을 선택하여 데이터 센터에 이미 연결된 스토리지 도메인 목록을 나열합니다.
3. **데이터 연결**을 클릭하여 **스토리지 연결** 창을 엽니다.
4. 데이터 센터에 연결하려는 데이터 도메인의 확인란을 선택합니다. 확인란을 여러 개 선택하여 여러 데이터 도메인을 연결할 수 있습니다.
5. **OK**를 클릭합니다.

데이터 도메인이 데이터 센터에 연결되어 자동으로 활성화됩니다.

4.6.2. 데이터 센터에 기존 ISO 도메인 연결

연결 해제 ISO 도메인이 데이터 센터에 연결될 수 있습니다. ISO 도메인은 데이터 센터와 같은 **스토리지 유형**이어야 합니다.

하나의 ISO 도메인만 데이터 센터에 연결될 수 있습니다.

절차 4.7. 데이터 센터에 기존 ISO 도메인 연결

1. **데이터 센터 리소스** 탭을 클릭하여 해당하는 데이터 센터를 선택합니다.
2. 상세 정보 창에서 **스토리지** 탭을 선택하여 데이터 센터에 이미 연결된 스토리지 도메인 목록을 나열합니다.
3. **ISO 연결**을 클릭하여 **ISO 라이브러리 연결** 창을 엽니다.
4. 해당 ISO 도메인의 라디오 버튼을 클릭합니다.
5. **OK**를 클릭합니다.

ISO 도메인이 데이터 센터에 연결되어 자동으로 활성화됩니다.

4.6.3. 기존 내보내기 도메인을 데이터 센터에 연결



참고

내보내기 스토리지 도메인은 사용되지 않습니다. 스토리지 데이터 도메인을 데이터 센터에서 분리한 후 같은 환경이나 다른 환경의 데이터 센터로 가져오기할 수 있습니다. 그 후에 가상 머신, 플로팅 가상 디스크 이미지, 그리고 템플릿을 가져오기한 스토리지 도메인에서 연결된 데이터 센터로 업로드할 수 있습니다. 스토리지 도메인을 가져오기하는 방법에 대한 자세한 내용은 [8.6절. "기존 스토리지 도메인 가져오기"](#)에서 참조하십시오.

연결 해제 내보내기 도메인은 데이터 센터에 연결할 수 있습니다. 하나의 내보내기 도메인만 데이터 센터에 연결할 수 있습니다.

절차 4.8. 기존 내보내기 도메인을 데이터 센터에 연결

1. **데이터 센터 리소스** 탭을 클릭하여 적절한 데이터 센터를 선택합니다.
2. 상세 정보 창에서 **스토리지** 탭을 선택하여 데이터 센터에 이미 연결된 스토리지 도메인 목록을 나열합니다.
3. **내보내기 연결**을 클릭하면 **내보내기 도메인 연결** 창이 열립니다.
4. 해당 내보내기 도메인의 라디오 버튼을 클릭합니다.
5. **OK**를 클릭합니다.

내보내기 도메인이 데이터 센터에 연결되어 자동으로 활성화됩니다.

4.6.4. 데이터 센터에서 스토리지 도메인 분리

데이터 센터에서 스토리지 도메인을 분리하면 스토리지 도메인에 연결된 데이터 센터가 중지합니다. 스토리지 도메인은 Red Hat Virtualization 환경에서 삭제되지 않고 이는 다른 데이터 센터에 연결할 수 있습니다.

가상 머신 및 템플릿과 같은 데이터는 스토리지 도메인에 연결된 상태로 남아 있습니다.



참고

마지막 사용 가능한 스토리지 도메인이 마스터 스토리지일 경우 이를 삭제할 수 없습니다.

절차 4.9. 데이터 센터에서 스토리지 도메인 분리

1. 데이터 센터 리소스 탭을 클릭하여 해당하는 데이터 센터를 선택합니다.
2. 상세 정보 창에서 스토리지 탭을 선택하여 데이터 센터에 연결된 스토리지 도메인 목록을 나열합니다.
3. 분리할 스토리지 도메인을 선택합니다. 스토리지 도메인이 **Active** 상태일 경우 **유지 관리**를 클릭하여 **스토리지 도메인 유지 관리 확인** 창을 엽니다.
4. **OK**를 클릭하여 유지 관리 모드를 시작합니다.
5. **분리**를 클릭하여 **스토리지 분리 확인** 창을 엽니다.
6. **OK**를 클릭합니다.

데이터 센터에서 스토리지 도메인이 분리되었습니다. 스토리지 도메인이 상세 정보 창에서 몇 분 이내에 사라질 것입니다.

4.7. 데이터 센터 및 권한

4.7.1. 데이터 센터의 시스템 권한 관리

SuperUser로서 시스템 관리자는 관리 포털의 모든 면을 관리합니다. 보다 특정한 관리 역할은 다른 사용자에게 부여될 수 있습니다. 이러한 제한된 관리자 역할은 특정 리소스에 제한하여 사용자 관리 권한을 부여할 경우 유용합니다. 예를 들어 **DataCenterAdmin** 역할은 데이터 센터의 스토리지를 제외한 할당된 데이터 센터에 대해서만 관리자 권한을 갖으며 **ClusterAdmin**은 할당된 클러스터에 대해서만 관리자 권한을 갖습니다.

데이터 센터 관리자는 특정 데이터 센터에 대해서만 시스템 관리자 역할을 수행합니다. 이는 각 데이터 센터에 관리자가 필요한 여러 데이터 센터가 있는 가상화 환경의 경우 유용합니다. **DataCenterAdmin** 역할은 계층적 모델로 데이터 센터에 대해 데이터 센터 관리자 역할이 지정된 사용자가 데이터 센터 스토리지를 제외한 데이터 센터에 있는 모든 개체를 관리할 수 있습니다. 헤더 바에 있는 **설정** 버튼을 사용하여 가상화 환경의 모든 데이터 센터에 대해 데이터 센터 관리자를 지정합니다.

데이터 센터 관리자 역할은 다음과 같은 작업을 허용합니다:

- 데이터 센터와 관련된 클러스터를 생성 및 삭제합니다.
- 데이터 센터와 관련된 호스트, 가상 머신, 풀을 추가 및 삭제합니다.
- 데이터 센터와 관련된 가상 머신의 사용자 권한을 편집합니다.



참고

기존 사용자에게만 역할 및 권한을 할당할 수 있습니다.

기존 시스템 관리자를 삭제하고 새로운 시스템 관리자를 추가하여 데이터 센터의 시스템 관리자를 변경할 수 있습니다.

4.7.2. 데이터 센터 관리자 역할

데이터 센터 권한이 있는 역할

아래 표에서는 데이터 센터 관리에 적용할 수 있는 관리자 역할 및 권한에 대해 설명합니다.

표 4.2. Red Hat Virtualization 시스템 관리자 역할

역할	권한	알림
DataCenterAdmin	데이터 센터 관리자	스토리지를 제외하고 클러스터, 호스트, 템플릿, 가상 머신을 포함하여 특정 데이터 센터에 있는 모든 물리적 및 가상 리소스를 사용, 생성, 삭제, 관리할 수 있습니다.
NetworkAdmin	네트워크 관리자	특정 데이터 센터의 네트워크를 설정 및 관리할 수 있습니다. 데이터 센터의 네트워크 관리자는 데이터 센터 내의 가상 머신에 대한 네트워크 권한을 상속합니다.

4.7.3. 리소스에 관리자 또는 사용자 역할 할당

리소스에 관리자 또는 사용자 역할을 할당하여 사용자가 리소스에 액세스 및 관리할 수 있게 합니다.

절차 4.10. 리소스에 역할 할당

1. 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 리소스를 검색 및 선택합니다.
2. 상세 정보 창에 있는 권한 탭을 클릭하여 할당된 사용자, 사용자 역할, 선택한 리소스에 대해 상속된 권한을 나열합니다.
3. 추가를 클릭합니다.
4. 검색 텍스트 상자에 기존 사용자의 이름 또는 사용자 이름을 입력하고 **검색**을 클릭합니다. 검색 결과 목록에서 일치하는 사용자를 선택합니다.
5. 할당할 역할 드롭 다운 목록에서 역할을 선택합니다.
6. **OK**를 클릭합니다.

사용자에게 역할이 할당되어 이제 사용자는 리소스에 대해 활성화된 역할에 상속된 권한을 갖습니다.

4.7.4. 리소스에서 관리자 또는 사용자 역할 삭제

리소스에서 관리자 또는 사용자 역할을 삭제합니다. 사용자는 리소스에서의 역할과 관련하여 상속된 권한을 손실합니다.

절차 4.11. 리소스에서 역할 삭제

1. 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 리소스를 검색 및 선택합니다.
2. 상세 정보 창에 있는 **권한** 탭을 클릭하여 할당된 사용자 목록, 사용자 역할, 선택한 리소스에서 상속된 권한을 나열합니다.
3. 리소스에서 삭제할 사용자를 선택합니다.
4. **삭제**를 클릭합니다. **권한 삭제** 창이 열리면 권한 삭제를 확인합니다.
5. **OK**를 클릭합니다.

리소스에서 사용자 역할 및 관련된 권한이 삭제됩니다.

5장. 클러스터

5.1. 클러스터에 대한 소개

클러스터는 동일한 스토리지 도메인을 공유하고 동일한 CPU 유형 (Intel 또는 AMD)을 갖는 호스트의 논리적 그룹입니다. 호스트의 CPU 모델 세대가 다른 경우 모든 모델에 있는 기능만 사용합니다.

시스템에 있는 각 클러스터는 하나의 데이터 센터에 속해 있어야 하며 시스템에 있는 각 호스트는 클러스터에 속해 있어야 합니다. 가상 머신은 클러스터 탭이나 런타임 시 설정 도구에 정의된 정책에 따라 클러스터에 있는 호스트에 동적으로 할당되어 이들 사이에서 마이그레이션할 수 있습니다. 클러스터는 최상위에 있으므로 전원 및 부하 공유 정책을 정의할 수 있습니다.

클러스터에 속한 호스트 수 및 가상 머신 수는 호스트 수 및 가상 머신 수 아래의 결과 목록에 표시됩니다.

클러스터는 가상 머신 또는 Red Hat Gluster Storage Servers를 실행합니다. 이러한 두 가지 사용 용도는 상호 배타적이므로 하나의 단일 클러스터에서 가상화 및 스토리지 호스트를 동시에 지원할 수 없습니다.

Red Hat Virtualization은 설치 도중 기본 데이터 센터에 기본 클러스터를 생성합니다.

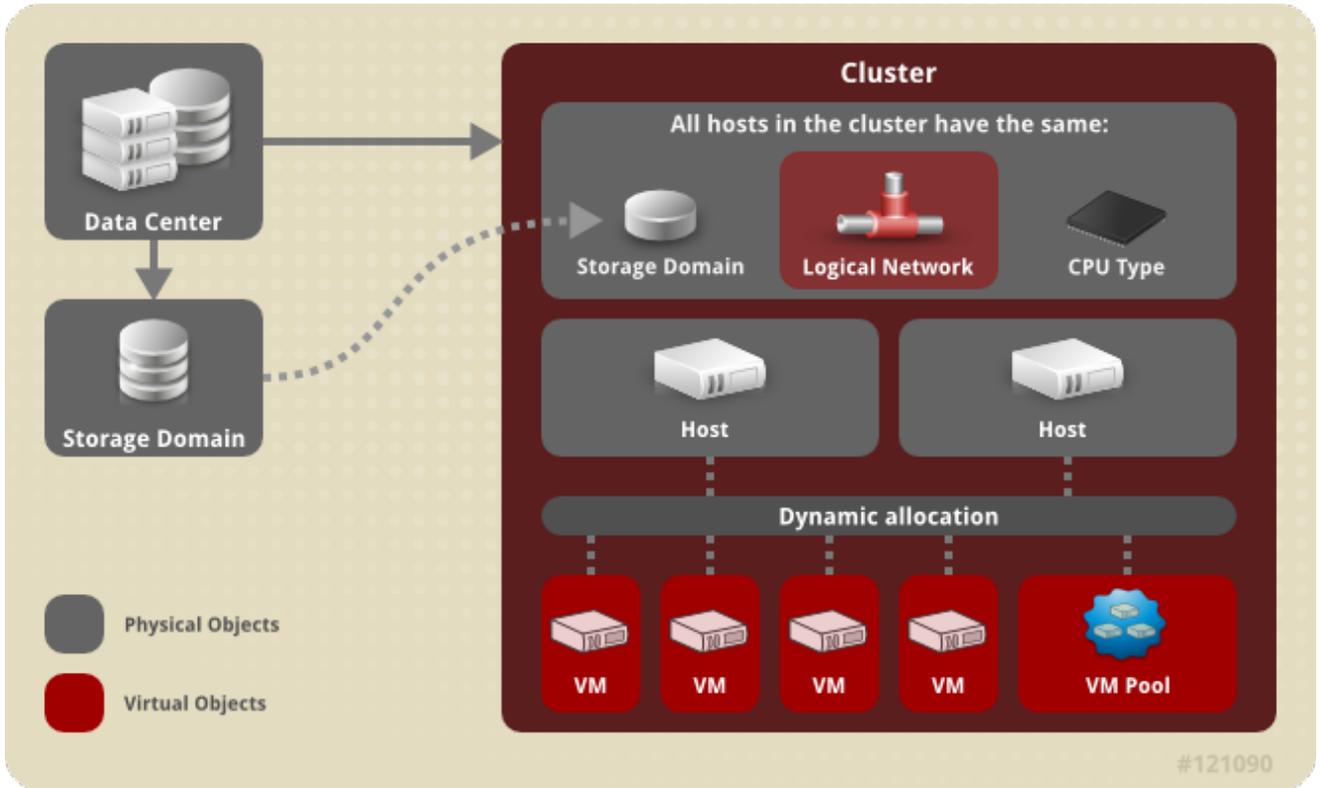


그림 5.1. 클러스터

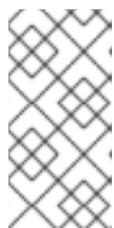
5.2. 클러스터 작업

5.2.1. 새 클러스터 생성

데이터 센터에는 여러 클러스터가 들어 있을 수 있으며 클러스터에는 여러 호스트가 들어 있을 수 있습니다. 클러스터에 있는 모든 호스트는 동일한 CPU 유형 (Intel 또는 AMD)으로 되어 있어야 합니다. CPU 유형을 최적화하기 위해 클러스터를 생성하기 전 호스트를 생성하는 것이 좋습니다. 하지만 가이드 버튼을 사용하여 나중에 호스트를 설정할 수 있습니다.

절차 5.1. 새 클러스터 생성

1. 클러스터 리소스 탭을 선택합니다.
2. 새로 만들기를 클릭합니다.
3. 드롭 다운 목록에서 클러스터가 속할 데이터 센터를 선택합니다.
4. 클러스터의 이름 및 설명을 입력합니다.
5. 관리 네트워크 드롭 다운 목록에서 네트워크를 선택하고 관리 네트워크 역할을 지정합니다.
6. 드롭 다운 목록에서 CPU 아키텍처 및 CPU 유형을 선택합니다. CPU 프로세스 제품군과 클러스터에 연결하고자 하는 호스트의 최소 CPU 프로세서 유형과 일치해야 합니다. 그렇지 않을 경우 호스트는 작동하지 않게 됩니다.



참고

Intel과 AMD CPU 유형 모두의 경우 CPU 모델은 오래된 것 부터 가장 최신의 논리적 순서로 나열됩니다. 클러스터에 다른 CPU 모델이 있는 호스트가 포함되어 있을 경우 오래된 CPU 모델을 선택합니다. 각 CPU 모델에 대한 보다 자세한 내용은 <https://access.redhat.com/solutions/634853>에서 참조하십시오.

7. 드롭 다운 목록에서 클러스터의 호환 버전을 선택합니다.
8. Virt 서비스 활성화 또는 Gluster 서비스 활성화 라디오 버튼을 선택하여 클러스터를 가상 머신 호스트 또는 Gluster 활성 노드로 배포할지 여부를 지정합니다. Red Hat Virtualization Host(RHVH)를 Gluster 활성 클러스터에 추가할 수 없음에 유의합니다.
9. 가상 머신 유지 보수 이유 설정을 활성화 옵션을 선택하여 가상 머신이 Manager에서 종료 시 이유 설정 옵션을 사용하여 관리자가 유지 관리에 대한 설명을 제공할 수 있게 합니다.
10. 호스트 유지 보수 이유 설정을 활성화 옵션을 선택하여 호스트가 Manager에서 유지 관리 모드로 전환 시 이유 설정 옵션을 사용하여 관리자가 유지 관리에 대한 설명을 제공할 수 있게 합니다.
11. 선택적으로 /dev/hwrng 소스(외부 하드웨어 장치) 확인란을 선택하여 클러스터의 모든 호스트에서 사용할 난수 생성기 장치를 지정합니다. /dev/urandom 소스(Linux 제공 장치)는 기본적으로 활성화됩니다.
12. 최적화 탭을 클릭하여 클러스터의 메모리 페이지 공유 임계값을 선택하고 클러스터에 있는 호스트에서 CPU 스레드 처리 및 메모리 부울 옵션을 활성화합니다.
13. 마이그레이션 정책 탭을 클릭하여 클러스터의 가상 머신 마이그레이션 정책을 지정합니다.
14. 스케줄링 정책 탭을 클릭하여 스케줄링 정책 설정, 스케줄러 최적화 설정, 클러스터에 있는 호스트의 신뢰할 수 있는 서비스 활성화, HA 예약 활성화, 사용자 정의 일련 번호 정책 추가와 같은 옵션을 설정합니다.
15. 콘솔 탭을 클릭하여 글로벌 SPICE 프록시를 덮어쓰기하고 클러스터에 있는 호스트의 SPICE 프록시 주소를 지정합니다.
16. 펜싱 정책 탭을 클릭하여 클러스터의 펜싱을 활성화 또는 비활성화하고 펜싱 옵션을 선택합니다.
17. MAC 주소 풀 탭을 클릭하여 클러스터에 대해 기본 풀이 아닌 MAC 주소 풀을 지정합니다. MAC 주소 풀 생성, 편집 또는 제거에 대한 자세한 옵션은 1.5절. "MAC 주소 풀"을 참조하십시오.

18. **OK**를 클릭하여 클러스터를 생성하고 **새 클러스터 - 가이드** 창을 엽니다.

19. 가이드 창에는 클러스터 설정에 필요한 엔티티가 나열됩니다. 이러한 엔티티를 설정하거나 **나중에 설정** 버튼을 클릭하여 나중에 설정합니다. 설정을 다시 시작하려면 클러스터를 선택하고 **가이드** 버튼을 클릭합니다.

새 클러스터가 가상화 환경에 추가됩니다.

5.2.2. 새 클러스터 및 클러스터 편집 창 설정 및 제어

5.2.2.1. 일반 클러스터 설정

다음 표에서는 **새 클러스터** 및 **클러스터 편집** 창에서 **일반** 탭을 설정하는 방법에 대해 설명합니다. **OK**를 클릭 시 잘못된 항목은 주황색으로 표시되고 변경 사항이 적용되지 않습니다. 또한 필드 프롬프트에는 값의 예상 값 또는 예상 값 범위가 표시됩니다.

표 5.1. 일반 클러스터 설정

필드	설명/동작
데이터 센터	데이터 센터에는 클러스터가 포함되어 있습니다. 데이터 센터는 클러스터를 추가하기 전에 생성해야 합니다.
이름	클러스터 이름입니다. 텍스트 필드는 최대 40 자로 제한되어 있으며 알파벳 대문자, 소문자, 숫자, 하이픈, 밑줄로 조합된 고유한 이름이어야 합니다.
설명 / 코멘트	클러스터 설명 또는 추가 알림 내용입니다. 이는 권장 사항이며 필수 입력 사항은 아닙니다.
관리 네트워크	관리 네트워크 역할을 할당할 논리 네트워크입니다. 기본값은 ovirtmgmt 입니다. 기존 클러스터에서 관리 네트워크는 상세 정보 창에서 논리 네트워크 탭에 있는 네트워크 관리 버튼을 통해서만 변경될 수 있습니다.
CPU 아키텍처	클러스터의 CPU 아키텍처입니다. 선택된 CPU 아키텍처에 따라 다른 CPU 유형을 사용할 수 있습니다. <ul style="list-style-type: none"> • 정의되지 않음: 모든 CPU 유형을 사용할 수 있습니다. • x86_64: 모든 Intel 및 AMD CPU 유형을 사용할 수 있습니다. • ppc64: IBM POWER 8 만을 사용할 수 있습니다.

필드	설명/동작
CPU 유형	<p>클러스터의 CPU 유형입니다. 다음 중 하나를 선택합니다:</p> <ul style="list-style-type: none"> • Intel Conroe 제품군 • Intel Penryn 제품군 • Intel Nehalem 제품군 • Intel Westmere 제품군 • Intel SandyBridge 제품군 • Intel Haswell 제품군 • Intel Skylake 제품군 • AMD Opteron G1 • AMD Opteron G2 • AMD Opteron G3 • AMD Opteron G4 • AMD Opteron G5 • IBM POWER 8 <p>클러스터에 있는 모든 호스트는 Intel, AMD, IBM POWER 8 CPU 유형 중 하나로 실행해야 합니다. 생성 후 변경할 경우 서비스가 중단될 수 있습니다. CPU 유형은 클러스터에서 가장 오래된 CPU 모델로 설정해야 합니다. 모든 모델에 있는 기능만 사용할 수 있습니다. Intel 및 AMD CPU 유형의 경우 CPU 모델은 가장 오래된 것 부터 가장 최신의 논리적 순서로 나열됩니다.</p>
호환성 버전	<p>Red Hat Virtualization 버전입니다. 다음 중 하나를 선택합니다:</p> <ul style="list-style-type: none"> • 3.6 • 4.0 <p>데이터 센터에 지정된 버전 보다 이전 버전을 선택할 수 없습니다.</p>
Virt 서비스 활성화	<p>라디오 버튼이 선택되어 있을 경우 클러스터에 있는 호스트는 가상 머신을 실행하는데 사용됩니다.</p>
Gluster 서비스 활성화	<p>라디오 버튼이 선택되어 있을 경우 클러스터에 있는 호스트는 Red Hat Gluster Storage Server 노드로 사용되고 가상 머신을 실행하지 않게 됩니다. Red Hat Virtualization Host를 이러한 옵션이 활성화된 클러스터에 추가할 수 없습니다.</p>

필드	설명/동작
<p>기존 Gluster 설정 가져오기</p>	<p>다음 확인란은 Gluster 서비스 활성화 라디오 버튼이 선택되어 있을 경우에만 사용할 수 있습니다. 이 옵션을 통해 기존 Gluster 활성 클러스터 및 Red Hat Virtualization Manager에 연결된 모든 호스트를 가져올 수 있습니다.</p> <p>다음 옵션은 가져오기할 클러스터에 있는 각 호스트에 필요합니다:</p> <ul style="list-style-type: none"> • 주소: Gluster 호스트 서버의 IP 주소 또는 정규화된 도메인 이름을 입력합니다. • 지문: Red Hat Virtualization Manager는 호스트의 지문을 가져오기하여 올바른 호스트에 연결되어 있는지 확인합니다. • Root 암호: 호스트와 통신하는데 필요한 root 암호를 입력합니다.
<p>가상 머신 유지 관리 이유 설정 활성화</p>	<p>이 확인란이 선택되어 있는 경우 클러스터에 있는 가상 머신을 Manager에서 종료할 때 이유를 입력할 수 있는 필드가 표시됩니다. 이를 통해 유지 관리 이유를 입력하면 가상 머신 전원이 다시 켜졌을 때 로그에 표시됩니다.</p>
<p>호스트 유지 관리 이유 설정 활성화</p>	<p>이 확인란이 선택되어 있는 경우 클러스터에 있는 호스트를 Manager에서 유지 관리 모드로 전환하면 이유를 입력할 수 있는 필드가 표시됩니다. 이를 통해 유지 관리 이유를 입력하면 호스트가 다시 활성화되었을 때 로그에 표시됩니다.</p>
<p>추가 난수 생성기 소스</p>	<p>이 확인란을 선택하면 클러스터에 있는 모든 호스트에서 추가 난수 생성기 장치를 사용할 수 있습니다. 이는 난수 생성기 장치에서 가상 머신으로 엔트로피의 통과를 활성화합니다.</p>

5.2.2.2. 최적화 설정

메모리 페이지 공유로 가상 머신은 다른 가상 머신에 사용하지 않는 메모리를 활용하여 할당된 메모리의 최대 200% 까지 사용할 수 있습니다. 이 절차는 **Red Hat Virtualization** 환경에 있는 가상 머신이 동시에 전체 용량을 사용하지 않고 특정 가상 머신에 할당된 사용하지 않는 메모리를 임시적으로 사용할 수 있다는 것을 전제로 합니다.

CPU 스레드를 처리하여 호스트는 호스트에 있는 코어 수를 초과하는 총 프로세서 코어 수로 가상 머신을 실행할 수 있습니다. 이는 **CPU** 이외의 구성 요소를 많이 사용하는 작업에 유용하며 더 많은 가상 머신을 실행하여 하드웨어 요구 사항을 줄일 수 있습니다. 또한 게스트 코어 수가 호스트 코어 수와 호스트 스레드 수 사이의 값일 경우 이러한 기능이 없으면 불가능한 **CPU** 토폴로지로 가상 머신을 실행할 수 있습니다.

다음 표에서는 새 클러스터 및 클러스터 편집 창에서 **최적화** 탭을 설정하는 방법에 대해 설명합니다.

표 5.2. 최적화 설정

필드	설명/동작
메모리 최적화	<ul style="list-style-type: none"> • 없음 - 메모리 오버커밋을 비활성화: 메모리 페이지 공유를 비활성화합니다. • 서버용 로드 - 실제 메모리의 150%의 스케줄링을 허용: 각 호스트에서 시스템 메모리의 150%로 메모리 페이지 공유 임계값을 설정합니다. • 데스크톱용 로드 - 실제 메모리의 200%의 스케줄링을 허용: 각 호스트에서 시스템 메모리의 200%로 메모리 페이지 공유 임계값을 설정합니다.
CPU 스레드	<p>스레드를 코어로 계산 확인란을 선택하여 호스트가 호스트에 있는 코어 수를 초과하는 총 프로세서 코어 수로 가상 머신을 실행합니다.</p> <p>표시된 호스트 스레드는 코어로 처리되며 가상 머신에서 활용할 수 있습니다. 예를 들어 코어 당 2 개의 스레드가 있는 24 코어 시스템 (총 48 스레드)의 경우 각각 최대 48 코어로 가상 머신을 실행할 수 있으며 호스트 CPU 부하를 산출하는 알고리즘은 2 배의 사용 가능한 코어로 부하를 비교하게 됩니다.</p>
메모리 Balloon	<p>메모리 Balloon 최적화 활성화 확인란을 선택하여 클러스터에 있는 호스트에서 실행되는 가상 머신의 메모리 오버커밋을 활성화합니다. 이 옵션을 설정하면 MoM (Memory Overcommit Manager)은 각 가상 머신에 확보된 메모리 크리를 제한하여 메모리 ballooning을 시작합니다.</p> <p>메모리 ballooning을 시작하려면 가상 머신에 적절한 드라이버와 함께 balloon 장치가 필요합니다. 각 가상 머신에는 삭제하지 않는 한 balloon 장치가 포함되어 있습니다. 이러한 클러스터에 있는 각 호스트는 클러스터가 상태가 Up으로 변경되면 balloon 정책 업데이트를 받을 수 있습니다. 필요한 경우 상태를 변경하지 않고 호스트에 있는 balloon 정책을 수동으로 업데이트할 수 있습니다. 보다 자세한 내용은 5.2.5 절. “클러스터에 있는 호스트에서 MoM 정책 업데이트”에서 참조하십시오.</p> <p>일부 시나리오에서는 메모리 ballooning으로 인해 KSM과 충돌할 수 있음을 이해하고 있어야 합니다. 이러한 경우 MoM은 충돌을 최소화하기 위해 balloon 크기를 조정하게 됩니다. 또한 일부 시나리오에서는 메모리 ballooning으로 인해 가상 머신의 성능이 최적화되지 않을 수 있습니다. 관리자는 신중하게 ballooning 최적화를 사용해야 합니다.</p>
KSM 컨트롤	<p>KSM 활성화 확인란을 선택하여 CPU 비용을 초과하는 메모리 저장에서 높은 혜택을 얻을 경우 MoM이 활성화하여 KSM (Kernel Same-page Merging)을 실행합니다.</p>

5.2.2.3. 마이그레이션 정책 설정

마이그레이션 정책은 호스트 오류 시 가상 머신의 라이브 마이그레이션 조건을 지정합니다. 이러한 조건에는 마이그레이션 중 가상 머신의 다운 타임, 네트워크 대역폭, 그리고 가상 머신 우선순위 결정 방법 등이 있습니다.

표 5.3. 마이그레이션 정책

정책	설명
Legacy	3.6 버전의 레거시 동작입니다. vdsm.conf 의 덮어쓰기는 여전히 적용됩니다. 게스트 에이전트 후크 메커니즘은 비활성화됩니다.
Minimal downtime	일반적인 상황에서 가상 머신 마이그레이션을 할 수 있게 해주는 정책입니다. 가상 머신의 다운 타임은 길지 않습니다. 가상 머신 마이그레이션이 오랫동안 (QEMU 반복에 따라 최대 500 밀리초까지) 수렴되지 않는 경우 마이그레이션이 중단됩니다. 게스트 에이전트 후크 메커니즘은 활성화됩니다.
Post-copy migration	이는 기술 프리뷰 기능입니다. 가상 머신에는 최소 다운타임 정책과 비슷한 중요한 다운타임이 발생해서는 안 됩니다. 오랫동안 가상 머신 마이그레이션이 통합되지 않는 경우 마이그레이션이 복사 후로 전환됩니다. 이 정책의 단점은 복사 후 단계에서 메모리의 누락된 부분이 호스트 간에 전송될 때 가상 머신의 속도가 크게 느려질 수 있다는 것입니다. 복사 후 단계 중에 호스트 간 네트워크 오류와 같은 문제가 발생하는 경우 실행 중인 가상 머신 인스턴스가 손실됩니다. 따라서 복사 후 단계 중에 마이그레이션을 중단할 수 없습니다. 게스트 에이전트 후크 메커니즘은 활성화됩니다.
Suspend workload if needed	대부분의 상황에서 가상 머신 마이그레이션을 할 수 있게 해주는 정책이며, 가상 머신이 많은 작업량을 실행하는 경우를 포함합니다. 가상 머신의 다운 타임이 길 수 있습니다. 최대 부하 시 마이그레이션이 중단될 수도 있습니다. 게스트 에이전트 후크 메커니즘은 활성화됩니다.

대역폭 설정은 각 호스트에서 나가고 들어오는 모든 마이그레이션의 최대 대역폭을 지정합니다.

표 5.4. 대역폭

정책	설명
Auto	데이터 센터 호스트 네트워크 QoS의 속도 제한 [Mbps] 설정에서 대역폭이 복사됩니다. 제한 속도를 설정하지 않은 경우 네트워크 인터페이스의 송수신 최소 연결 속도로 계산됩니다. 제한 속도가 설정되지 않고 사용 가능한 연결 속도가 없는 경우 제한 속도는 보내는 호스트의 로컬 VDSM 설정에 따라 결정됩니다.

정책	설명
Hypervisor default	대역폭은 보내는 호스트의 로컬 VDSM 설정에 따라 결정됩니다.
Custom	사용자가 지정합니다. (단위: Mbps)

복구 정책은 마이그레이션 시 가상 머신의 우선순위 결정 방법을 지정합니다.

표 5.5. 복구 정책 설정

필드	설명/동작
가상 머신을 마이그레이션함	가상 머신을 설정된 우선순위 순서대로 마이그레이션합니다.
고가용성 가상 머신만 마이그레이션	고가용성 가상 머신만 마이그레이션하여 다른 호스트가 오버로딩되지 않게 합니다.
가상 머신은 마이그레이션 하지 않음	가상 머신이 마이그레이션되지 않게 합니다.

추가 속성은 **Legacy** 마이그레이션 정책의 경우에만 적용됩니다.

표 5.6. 추가 속성

속성	설명
마이그레이션 자동 통합	<p>가상 머신의 라이브 마이그레이션 중 자동 컨버전스를 사용할지에 대한 여부를 설정합니다. 워크로드가 큰 대형 가상 머신은 라이브 마이그레이션 중 전송 속도 보다 더 빠르게 더티 메모리 상태가 되어 마이그레이션을 컨버전스하지 못하게 합니다. QEMU의 자동 컨버전스 기능을 통해 가상 머신 마이그레이션 컨버전스를 강제할 수 있습니다. QEMU는 자동으로 컨버전스되지 않음을 감지하고 가상 머신에 있는 vCPU의 스로틀을 감소시킵니다. 자동 컨버전스는 전역에서 기본값으로 비활성화되어 있습니다.</p> <ul style="list-style-type: none"> ● 글로벌 설정에서 가져오기를 선택하여 전역 수준에서 설정되는 자동 컨버전스 설정을 사용합니다. ● 자동 통합을 선택하여 전역 설정을 덮어쓰기하고 가상 머신의 자동 통합을 허용합니다. ● 자동 통합 해제를 선택하여 전역 설정을 덮어쓰기하고 가상 머신이 자동 통합되지 않도록 합니다.

속성	설명
<p>마이그레이션 압축 활성화</p>	<p>이 옵션을 통해 가상 머신의 라이브 마이그레이션 중 마이그레이션 압축을 사용하도록 설정할 수 있습니다. 이 기능은 Xor Binary Zero Run-Length-Encoding을 사용하여 가상 머신 다운 타임 및 집약적 메모리 쓰기 작업을 실행하는 가상 머신이나 스파스 메모리 업데이트 패턴이 있는 애플리케이션의 총 라이브 마이그레이션 시간을 단축할 수 있습니다. 마이그레이션 압축은 전역에서 기본값으로 비활성화되어 있습니다.</p> <ul style="list-style-type: none"> • 글로벌 설정에서 가져오기를 선택하여 전역 수준에서 설정되는 압축 설정을 사용합니다. 이 옵션은 기본값으로 선택되어 있습니다. • 압축을 선택하여 전역 설정을 덮어쓰기하고 가상 머신의 압축을 허용합니다. • 압축 해제를 선택하여 전역 설정을 덮어쓰기하고 가상 머신이 압축되지 않도록 합니다.

5.2.2.4. 스케줄링 정책 설정

스케줄링 정책을 사용하여 사용 가능한 호스트 간의 가상 머신 사용 및 배포를 지정할 수 있습니다. 클러스터에 있는 호스트에서 자동으로 부하 분산을 조정할 수 있도록 스케줄링 정책을 지정합니다.

기존 클러스터에 스케줄링 정책을 추가하기 위해 **클러스터 탭** 클릭 후 **편집** 버튼을 클릭하고 **스케줄링 정책** 탭을 클릭합니다.

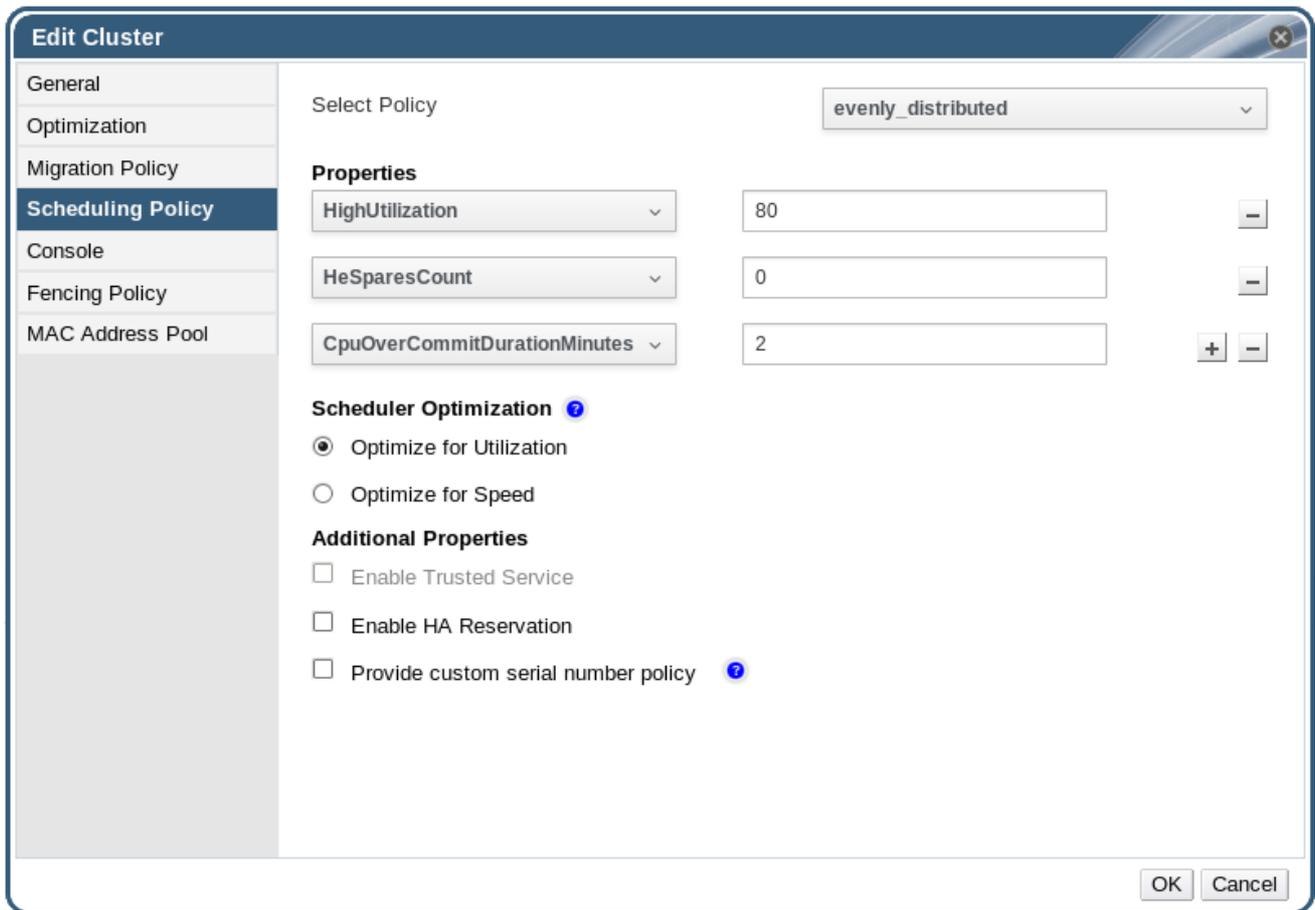


그림 5.2. 스케줄링 정책 설정: **evenly_distributed**

다음 표에서는 스케줄링 정책 탭 설정에 대해 설명합니다.

표 5.7. 스케줄링 정책 탭 속성

필드	설명/동작
----	-------

필드	설명/동작
<p>정책 선택</p>	<p>드롭 다운 목록에서 정책을 선택합니다.</p> <ul style="list-style-type: none"> <p>none: 이미 실행 중인 가상 머신의 호스트 간에 로드 또는 전원 공유를 하지 않으려면 정책 값을 none으로 설정합니다. 이는 기본 모드입니다. 가상 머신이 시작되면 메모리 및 CPU 처리 로드가 클러스터의 모든 호스트에서 균등하게 분산됩니다. 호스트가 정의된 CpuOverCommitDurationMinutes, HighUtilization 또는 MaxFreeMemoryForOverUtilized에 도달한 경우 호스트에 연결된 추가 가상 머신이 시작되지 않습니다.</p> <p>evenly_distributed: 클러스터에 있는 모든 호스트에 메모리 및 CPU 처리 로드를 균등하게 분산합니다. 호스트가 정의된 CpuOverCommitDurationMinutes, HighUtilization 또는 MaxFreeMemoryForOverUtilized에 도달한 경우 호스트에 연결된 추가 가상 머신이 시작되지 않습니다.</p> <p>InClusterUpgrade: 호스트 운영 체제 버전을 바탕으로 가상 머신을 분배합니다. 현재 가상 머신이 실행 중인 운영 체제 버전 이후 버전의 운영 체제를 가진 호스트가 같은 운영 체제를 가진 호스트보다 우선순위가 주어집니다. 더 새로운 운영 체제를 가진 호스트로 마이그레이션한 가상 머신은 이전 버전의 운영 체제로 돌아가지 않습니다. 가상 머신은 클러스터의 모든 호스트에서 재시작 가능합니다. 해당 정책을 통해 클러스터 호스트가 혼합된 운영 체제 버전을 가져도 업그레이드될 수 있습니다. 사전 조건이 충족되어야 해당 정책을 활성화할 수 있습니다. 더 자세한 정보는 Upgrade Guide를 참조하십시오.</p> <p>power_saving: 사용률이 낮은 호스트의 전원 소비를 감소하기 위해 사용가능한 호스트의 서브 세트에서 메모리 및 CPU 처리 부하를 분산합니다. 지정된 시간 간격 보다 길게 사용량의 하한치 이하에 있는 호스트 CPU 부하는 모든 가상 머신을 다른 호스트로 마이그레이션하므로 전원을 끌 수 있습니다. 호스트가 지정된 사용량 상한치에 도달할 경우 호스트에 연결된 추가 가상 머신은 시작되지 않습니다.</p> <p>vm_evenly_distributed: 가상 머신 수에 따라 가상 머신을 균등하게 호스트로 분배합니다. 호스트가 HighVmCount 보다 많은 가상 머신을 실행하고 있고 가상 머신 수에서 최소 하나의 호스트가 MigrationThreshold 범위 밖에 있을 경우 클러스터는 불균형 상태로 간주됩니다.</p>

다음 속성은 선택한 정책에 따라 표시되며 필요에 따라
설명/동작 수 있습니다:

- HighVmCount:** 각 호스트에서 실행할 수 있는 최대 가상 머신 수를 설정합니다. 제한을 초과하면 호스트는 과부하 상태가 됩니다. 기본값은 **10**입니다.
- MigrationThreshold:** 가상 머신이 호스트에서 마이그레이션되기 전 버퍼를 정의합니다. 이는 사용률이 가장 높은 호스트와 사용률이 가장 낮은 호스트 간의 최대 가상 머신 수 차이 값입니다. 클러스터의 모든 호스트에 있는 가상 머신 수가 마이그레이션 임계값 내에 있는 경우 클러스터는 균형 상태가 됩니다. 기본값은 **5**입니다.
- SpmVmGrace:** SPM 호스트에 예약된 가상 머신 용 슬롯 수를 정의합니다. SPM 호스트는 다른 호스트 보다 부하가 낮기 때문에 이러한 변수는 호스트 이외에 얼마나 적은 수의 가상 머신을 실행할 수 있는지를 정의합니다. 기본값은 **5**입니다.
- CpuOverCommitDurationMinutes:** 스케줄링 정책이 적용되기 전 호스트가 정의된 사용 값 밖에서 CPU 부하를 실행할 수 있는 시간 (분 단위)을 설정합니다. 시간 간격을 정의하여 일시적 CPU 부하 스파이크로 인한 스케줄링 정책 활성화 및 불필요한 가상 머신 마이그레이션이 발생하지 않게 합니다. 최대 2 자리 수 까지로 합니다. 기본값은 **2**입니다.
- HighUtilization:** 백분율로 표시합니다. 호스트가 지정된 시간 동안 상한치 이상의 CPU 사용량을 실행할 경우 Red Hat Virtualization Manager는 호스트의 CPU 부하가 최대 상한 임계값 이하로 될 때 까지 클러스터에 있는 다른 호스트로 가상 머신을 마이그레이션합니다. 기본값은 **80**입니다.
- LowUtilization:** 백분율로 표시합니다. 호스트가 지정된 시간 동안 하한치 이하의 CPU 사용량을 실행할 경우 Red Hat Virtualization Manager는 클러스터에 있는 다른 호스트에 가상 머신을 마이그레이션합니다. Manager 는 원래 호스트 머신의 전원을 종료하고 부하 분산이 필요하거나 클러스터에서 여유 호스트가 충분하지 않을 경우 호스트를 다시 시작합니다. 기본값은 **20**입니다.
- ScaleDown:** 호스트 값을 지정된 값으로 나누기하여 HA 예약 가중 함수의 영향을 줄입니다. 이는 none을 포함하여 정책에 추가할 수 있는 옵션 속성입니다.
- HostsInReserve:** 실행 중인 가상 머신이 없어도 계속 실행할 호스트 수를 지정합니다. 이는 power_saving 정책에 추가할 수 있는 옵션 속성입니다.
- EnableAutomaticHostPowerManag**

필드	설명/동작
	<p>ement: 클러스터에 있는 모든 호스트의 자동 전원 관리를 활성화합니다. 이는 power_saving 정책에 추가할 수 있는 옵션 속성입니다. 기본 값은 true입니다.</p> <ul style="list-style-type: none"> MaxFreeMemoryForOverUtilized: 최소 서비스 수준에 필요한 최소 여유 메모리를 MB로 설정합니다. 호스트의 사용 가능한 메모리가 이 값과 같거나 더 낮은 경우 Red Hat Virtualization Manager는 해당 호스트의 사용 가능한 메모리가 최소 서비스 임계값 아래에 있는 동안 클러스터의 다른 호스트로 가상 머신을 마이그레이션합니다. MaxFreeMemoryForOverUtilized 및 MinFreeMemoryForUnderUtilized 값을 모두 OMB로 설정하면 메모리 기반 밸런싱이 비활성화됩니다. 이는 power_saving 및 evenly_distributed 정책에 추가할 수 있는 속성 옵션입니다. MinFreeMemoryForUnderUtilized: 호스트 사용률이 낮은 것으로 간주되는 최소 필수 여유 메모리를 MB로 표시합니다. 호스트의 사용 가능한 메모리가 해당 값을 초과하는 경우 Red Hat Virtualization Manager는 클러스터에 있는 다른 호스트에 가상 머신을 마이그레이션하고 호스트 시스템의 전원을 종료하며, 로드 밸런싱이 필요하거나 클러스터에 여유 호스트가 충분하지 않을 경우 해당 시스템을 다시 시작합니다. MaxFreeMemoryForOverUtilized 및 MinFreeMemoryForUnderUtilized 값을 모두 OMB로 설정하는 경우 메모리 기반 밸런싱이 비활성화됩니다. 이는 power_saving 및 evenly_distributed 정책에 추가할 수 있는 속성 옵션입니다.
스케줄러 최적화	<p>호스트 가중치/순서 스케줄링을 최적화합니다.</p> <ul style="list-style-type: none"> 사용률 최적화: 스케줄링에 가중치 모듈을 포함되어 최적 선택이 가능합니다. 속도 최적화: 10 개 이상의 대기 중인 요청이 있을 경우 호스트의 가중치를 건너뛵니다.
신뢰할 수 있는 서비스 활성화	<p>OpenAttestation 서버와의 통합을 활성화합니다. 이를 활성화하기 전 engine-config 도구를 사용하여 OpenAttestation 서버 정보를 입력합니다. 자세한 정보는 10.4절. "신뢰할 수 있는 컴퓨팅 풀"을 참조하십시오.</p>

필드	설명/동작
HA 예약 활성화	Manager를 활성화하여 고가용성 가상 머신 용 클러스터 용량을 모니터링합니다. Manager는 기존 호스트에서 예기치 않은 오류 발생 시 마이그레이션을 위해 고가용성으로 지정된 가상 머신의 클러스터내에 적절한 용량을 보유하도록 합니다.
사용자 정의 일련 번호 정책 지정	이 확인란에서 클러스터에 있는 가상 머신의 일련 번호 정책을 지정합니다. 다음 옵션 중 하나를 선택합니다: <ul style="list-style-type: none"> • 호스트 ID: 가상 머신의 일련 번호로 호스트의 UUID를 설정합니다. • 가상 머신 ID: 가상 머신의 일련 번호로 가상 머신의 UUID를 설정합니다. • 사용자 정의 일련 번호: 사용자 정의 일련 번호를 지정할 수 있습니다.

호스트의 여유 메모리가 20% 미만으로 감소하면 **mom.Controllers.Balloon - INFO Ballooning guest:half1 from 1096400 to 1991580**과 같은 부울 명령이 **/var/log/vdsm/mom.log**에 기록됩니다. **/var/log/vdsm/mom.log**는 Memory Overcommit Manager 로그 파일입니다.

5.2.2.5. 클러스터 콘솔 설정

다음 표에서는 새 클러스터 및 클러스터 편집 창에서 콘솔 탭을 설정하는 방법에 대해 설명합니다.

표 5.8. 콘솔 설정

필드	설명/동작
클러스터의 SPICE 프록시 정의	이 옵션을 선택하여 전체 설정에 지정된 SPICE 프록시 덮어쓰기를 활성화할 수 있습니다. 이 기능은 하이퍼바이저가 있는 네트워크 외부에 사용자 (예를 들어 사용자 포털을 통해 연결된 사용자)가 연결되어 있을 경우에 유용합니다.
SPICE 프록시 주소 덮어쓰기	SPICE 클라이언트는 가상 머신에 연결된 프록시입니다. 주소는 다음과 같은 형식으로 지정해야 합니다: <pre>protocol://[host]:[port]</pre>

5.2.2.6. 펜싱 정책 설정

다음 표에서는 새 클러스터 및 클러스터 편집 창에서 펜싱 정책 탭을 설정하는 방법에 대해 설명합니다.

표 5.9. 펜싱 정책 설정

필드	설명/동작
펜싱 활성화	클러스터에서 펜싱을 활성화합니다. 펜싱은 기본적으로 활성화되어 있지만 필요에 따라 비활성화할 수 있습니다. 예를 들어 일시적 네트워크 오류가 발생하거나 발생될 것으로 예상되는 경우 관리자는 진단 또는 유지 보수 작업이 완료될 때까지 펜싱을 비활성화할 수 있습니다. 펜싱이 비활성화되어 있을 경우 Non-Responsive 상태에 있는 호스트에서 실행 중인 고가용성 가상 머신은 다른 호스트에서 다시 시작되지 않음에 유의합니다.
호스트가 스토리지에서 유효한 임대를 가지고 있을 경우 펜싱 건너뛰기	이 확인란이 선택되어 있을 경우 클러스터에 있는 Non Responsive 상태의 모든 호스트 및 아직 스토리지에 연결되어 있는 호스트는 펜싱되지 않습니다.
클러스터 연결 문제가 있는 경우 펜싱 건너뛰기	이 확인란이 선택되어 있을 경우 클러스터에서 연결 문제가 있는 호스트 비율이 지정된 임계값 과 동일하거나 그 이상일 경우 펜싱은 일시적으로 비활성화됩니다. 임계값 은 드롭 다운 목록에서 선택하며 사용 가능한 값은 25, 50, 75, 100 입니다.

5.2.3. 리소스 편집

요약

리소스 속성을 편집합니다.

절차 5.2. 리소스 편집

1. 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 리소스를 검색 및 선택합니다.
2. **편집**을 클릭하여 **편집** 창을 엽니다.
3. 필요한 속성을 변경하고 **OK**를 클릭합니다.

결과

새로운 속성이 리소스에 저장됩니다. 속성 필드가 잘못되어 있을 경우 **편집** 창은 닫히지 않습니다.

5.2.4. 클러스터에 있는 호스트의 전원 관리 정책 및 부하 설정

evenly_distributed 및 **power_saving** 스케줄링 정책을 통해 허용 가능한 메모리 및 CPU 사용률 값과 호스트에서 가상 머신을 마이그레이션해야 할 시점을 지정할 수 있습니다.

vm_evenly_distributed 스케줄링 정책은 가상 머신 수에 따라 호스트에 가상 머신을 균등하게 분배합니다. 클러스터에 있는 호스트에서 자동 부하 균형 분산을 활성화하기 위한 스케줄링 정책을 정의합니다. 각 스케줄링 정책에 대한 자세한 내용은 [5.2.2.4절. "스케줄링 정책 설정"](#)에서 확인하십시오.

절차 5.3. 호스트의 전원 관리 정책 및 부하 설정

1. 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 클러스터를 검색 및 선택합니다.

2. 편집을 클릭하여 클러스터 창을 엽니다.

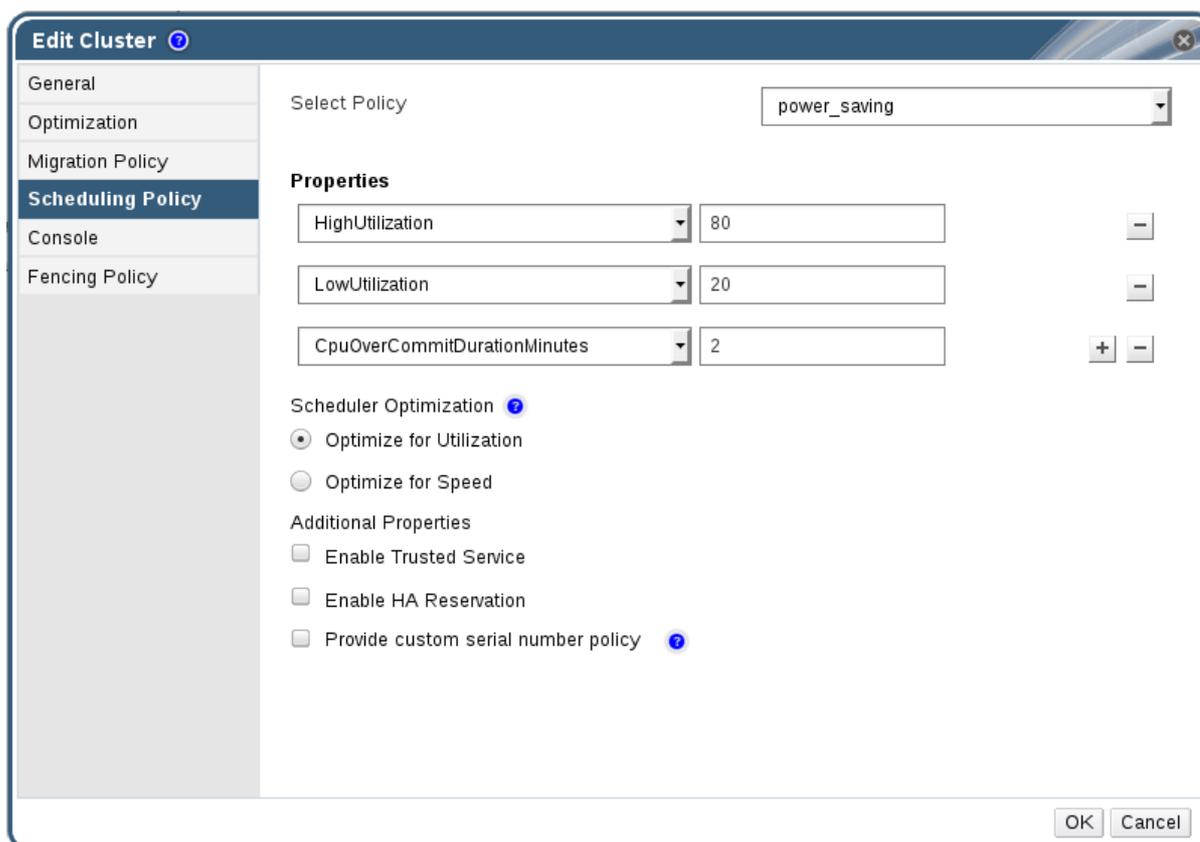


그림 5.3. 스케줄링 정책 편집

3. 다음 정책 중 하나를 선택합니다:

- o **none**
- o **vm_evenly_distributed**
 - a. 각 호스트에서 실행할 수 있는 최대 가상 머신 수를 **HighVmCount** 필드에 설정합니다.
 - b. 가장 많이 사용되는 호스트의 가상 머신 수와 가장 적게 사용되는 호스트의 가상 머신 수 사이에서 허용 가능한 최대 차이를 **MigrationThreshold** 필드에 정의합니다.
 - c. **SpmVmGrace** 필드에 SPM 호스트에 저장된 가상 머신 용 슬롯 수를 지정합니다.
- o **evenly_distributed**
 - a. **CpuOverCommitDurationMinutes** 필드에서 스케줄링 정책이 작동하기 전 호스트가 지정된 사용량 밖에서 CPU 부하를 실행할 수 있는 시간 (분 단위)을 설정합니다.
 - b. CPU 사용량(백분율)이 얼마가 되면 가상 머신이 다른 호스트로 마이그레이션을 시작하는지 해당 백분율을 **HighUtilization** 필드에 입력합니다.
 - c. 가상 머신에서 다른 호스트로 마이그레이션을 시작하는 최소 필수 여유 메모리를 MB 단위로 **MinFreeMemoryForUnderUtilized**에 입력합니다.
 - d. 가상 머신이 다른 호스트로 마이그레이션을 시작하는 최대 필수 여유 메모리를 MB 단위로 **MaxFreeMemoryForOverUtilized**에 입력합니다.
- o **power_saving**

- a. **CpuOverCommitDurationMinutes** 필드에서 스케줄링 정책이 작동하기 전 호스트가 지정된 사용량 밖에서 CPU 부하를 실행할 수 있는 시간 (분 단위)을 설정합니다.
 - b. CPU 사용량(백분율)이 얼마 이하로 내려가면 호스트가 충분히 사용되고 있지 않은 것으로 간주되는지 해당 하한값을 백분율로 **LowUtilization** 필드에 입력합니다.
 - c. CPU 사용량(백분율)이 얼마가 되면 가상 머신이 다른 호스트로 마이그레이션을 시작하는지 해당 백분율을 **HighUtilization** 필드에 입력합니다.
 - d. 가상 머신에서 다른 호스트로 마이그레이션을 시작하는 최소 필수 여유 메모리를 MB 단위로 **MinFreeMemoryForUnderUtilized**에 입력합니다.
 - e. 가상 머신이 다른 호스트로 마이그레이션을 시작하는 최대 필수 여유 메모리를 MB 단위로 **MaxFreeMemoryForOverUtilized**에 입력합니다.
4. 클러스터의 스케줄러 최적화로 다음 중 하나를 선택합니다:
- **사용 최적화**를 선택하면 스케줄링에 가중치 모듈을 포함되어 최상의 선택이 가능합니다.
 - **속도 최적화**를 선택하면 10 개 이상의 대기 중인 요청이 있을 경우 호스트의 가중치를 건너뛴다.
5. OpenAttestation 서버를 사용하여 호스트를 검사하고 **engine-config** 도구를 사용하여 서버 상세 정보를 설정하려면 신뢰할 수 있는 서비스 사용란을 선택합니다.
6. 옵션으로 **HA 예약을 활성화**란을 선택하여 Manager가 고가용성 가상 머신 용 클러스터 용량을 모니터링할 수 있게 합니다.
7. 옵션으로 **사용자 정의 일련 번호 정책 지정**란을 선택하여 클러스터에 있는 가상 머신의 일련 번호 정책을 지정하고 다음 옵션 중 하나를 선택합니다:
- 가상 머신의 일련 번호로 호스트의 **UUID**를 설정하기 위해 **호스트 ID**를 선택합니다.
 - 가상 머신의 일련 번호로 가상 머신의 **UUID**를 설정하기 위해 **가상 머신 ID**를 선택합니다.
 - **사용자 정의 일련 번호**를 선택하고 텍스트 필드에 사용자 정의 일련 번호를 지정합니다.
8. **OK**를 클릭합니다.

5.2.5. 클러스터에 있는 호스트에서 MoM 정책 업데이트

MoM (Memory Overcommit Manager)는 호스트에서 메모리 balloon 및 KSM 기능을 처리합니다. 클러스터 수준에서 이러한 기능을 변경하면 호스트를 재부팅하거나 유지 보수 모드에서 **Up** 상태로 전환한 때에만 호스트에 전달됩니다. 하지만 필요에 따라 호스트가 **Up** 상태일 때 **MoM** 정책을 동기화하여 주요 변경 사항을 호스트에 바로 적용할 수 있습니다. 다음 절차는 각 호스트에서 개별적으로 실행해야 합니다.

절차 5.4. 호스트에서 MoM 정책 동기화

1. 클러스터 탭을 클릭하고 호스트가 속해 있는 클러스터를 선택합니다.
2. 상세 정보 창에서 호스트 탭을 클릭하고 MoM 정책을 업데이트해야 하는 호스트를 선택합니다.
3. **MoM 정책 동기화** 버튼을 클릭합니다.

호스트에서 MoM 정책은 호스트를 유지 보수 모드로 전환하거나 **Up** 상태로 되돌릴 필요 없이 업데이트됩니다.

5.2.6. CPU 프로파일

CPU 프로파일은 클러스터의 가상 머신이 이를 실행하는 호스트에서 액세스할 수 있는 처리 가능한 최대 용량을 정의하며 호스트에서 사용 가능한 총 용량의 백분율로 표시합니다. CPU 프로파일은 데이터 센터 아래에 정의된 CPU 프로파일에 기반하여 생성되며 클러스터에 있는 모든 가상 머신에 자동으로 적용되지 않습니다. 따라서 적용하려면 프로파일에 대한 각각의 가상 머신에 수동으로 지정해야 합니다.

5.2.6.1. CPU 프로파일 생성

CPU 프로파일을 생성합니다. 다음 부분에서는 클러스터가 속한 데이터 센터 아래에 하나 이상의 CPU QoS 항목이 이미 정의되어 있음을 전제로 합니다.

절차 5.5. CPU 프로파일 생성

1. 클러스터 리소스 탭을 클릭하고 클러스터를 선택합니다.
2. 상세 정보 창에서 **CPU 프로파일** 하위 탭을 클릭합니다.
3. **새로 만들기**를 클릭합니다.
4. 이름란에 CPU 프로파일 이름을 입력합니다.
5. 설명란에 CPU 프로파일 설명을 입력합니다.
6. **QoS** 목록에서 CPU 프로파일에 적용할 QoS를 선택합니다.
7. **OK**를 클릭합니다.

CPU 프로파일이 생성되었습니다. CPU 프로파일은 클러스터에 있는 가상 머신에 적용할 수 있습니다.

5.2.6.2. CPU 프로파일 삭제

Red Hat Virtualization 환경에서 기존 CPU 프로파일을 삭제합니다.

절차 5.6. CPU 프로파일 삭제

1. 클러스터 리소스 탭을 클릭하고 클러스터를 선택합니다.
2. 상세 정보 창에서 **CPU 프로파일** 하위 탭을 클릭합니다.
3. 삭제하고자 하는 CPU 프로파일을 선택합니다.
4. **삭제**를 클릭합니다.
5. **OK**를 클릭합니다.

CPU 프로파일이 삭제되어 CPU 프로파일을 더 이상 사용할 수 없습니다. CPU 프로파일이 가상 머신에 지정되어 있을 경우 이러한 가상 머신에는 자동으로 **default** CPU 프로파일이 지정됩니다.

5.2.7. 기존의 Red Hat Gluster Storage 클러스터 가져오기

Red Hat Gluster Storage 클러스터와 클러스터에 속한 모든 호스트를 Red Hat Virtualization Manager에 가져오기할 수 있습니다.

클러스터에 있는 IP 주소 또는 호스트 이름, 호스트 암호와 같은 정보를 제공할 때 SSH를 통해 **gluster peer status** 명령을 호스트에서 실행하면 클러스터의 일부인 호스트 목록이 표시됩니다. 수동으로 각

호스트의 지문을 확인하고 암호를 제공해야 합니다. 클러스터에 있는 호스트 중 하나가 중지되어 있거나 연결할 수 없는 경우 클러스터를 가져올 수 없습니다. 새로 가져온 호스트에는 VDSM이 설치되어 있지 않지만 가져오기한 후 부트스트랩 스크립트는 호스트에 필요한 모든 VDSM 패키지를 설치한 후 이를 재부팅합니다.

절차 5.7. 기존 Red Hat Gluster Storage Cluster를 Red Hat Virtualization Manager에 가져오기

1. 클러스터 리소스 탭을 선택하여 결과 목록에 모든 클러스터를 나열합니다.
2. 새로 만들기 버튼을 클릭하여 새 클러스터 창을 엽니다.
3. 드롭 다운 메뉴에서 클러스터가 속한 데이터 센터를 선택합니다.
4. 클러스터의 이름 및 설명을 입력합니다.
5. 클러스터 서비스 활성화 라디오 버튼 및 기존 클러스터 설정 가져오기 체크 상자를 선택합니다.

기존 Gluster 설정 가져오기 필드는 Gluster 서비스 활성화 라디오 버튼을 선택한 경우에만 표시됩니다.

6. 주소 필드에 클러스터에 있는 서버의 IP 주소 또는 호스트 이름을 입력합니다.

호스트 지문이 표시되어 올바른 호스트와 연결되어 있는지 확인합니다. 호스트가 도달할 수 없거나 네트워크 오류가 있을 경우 지문 검색 중 오류 발생 메시지가 지문 필드에 표시됩니다.

7. 서버의 Root 암호를 입력하고 OK를 클릭합니다.
8. 호스트 추가 창이 열리면 클러스터의 일부분인 호스트 목록이 표시됩니다.
9. 각 호스트에 대해 이름 및 Root 암호를 입력합니다.
10. 모든 호스트에 대해 동일한 암호를 사용하고자 할 경우 일반 암호 사용 확인란을 선택하여 지정된 텍스트 필드에 암호를 입력합니다.

적용 버튼을 클릭하여 입력된 암호를 모든 호스트에 설정합니다.

OK를 클릭하여 지문이 유효한지 확인하고 변경 사항을 제출합니다.

호스트를 가져오기한 후 부트스트랩 스크립트는 호스트에 필요한 모든 VDSM 패키지를 설치하고 재부팅됩니다. 기존 Red Hat Gluster Storage 클러스터를 Red Hat Virtualization Manager에 성공적으로 가져왔습니다.

5.2.8. 호스트 추가 창 설정

호스트 추가 창을 통해 Gluster-활성 클러스터의 일부분으로 가져오기할 호스트의 상세 정보를 지정할 수 있습니다. 이 창은 새 클러스터 창에 있는 Gluster 서비스 활성화 확인란을 선택한 후 필요한 호스트 정보를 입력한 후에 나타납니다.

표 5.10. Gluster 호스트 설정 추가

필드	설명
----	----

필드	설명
공통 암호 사용	클러스터에 속한 모든 호스트에 대해 동일한 암호를 사용하려면 이 체크 박스를 선택합니다. 암호 란에 암호를 입력한 후 적용 버튼을 클릭하면 모든 호스트에 암호가 설정됩니다.
성명	호스트 이름을 입력합니다.
호스트 이름/IP	이 필드는 새 클러스터 창에 지정한 호스트의 정규화된 도메인 이름 또는 IP로 자동 입력됩니다.
Root 암호	각 호스트에 다른 root 암호를 사용하려면 이 필드에 암호를 입력합니다. 이 필드는 클러스터에 있는 모든 호스트에 지정된 공통 암호를 덮어쓰기합니다.
지문	올바른 호스트와 연결되어 있는지 확인하기 위해 호스트 지문이 표시됩니다. 이 필드는 새 클러스터 창에 지정된 호스트의 지문으로 자동 입력됩니다.

5.2.9. 클러스터 삭제

요약

클러스터를 삭제하기 전 클러스터에서 모든 호스트를 이동합니다.



참고

Default 클러스터에 **Blank** 템플릿이 있기 때문에 이를 삭제할 수 없습니다. **Default** 클러스터의 이름을 변경하고 새로운 데이터 센터에 추가할 수 있습니다.

절차 5.8. 클러스터 삭제

1. 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 클러스터를 검색 및 선택합니다.
2. 클러스터에 호스트가 없는지 확인합니다.
3. **삭제**를 클릭하면 **클러스터 삭제** 확인 창이 열립니다.
4. **OK**를 클릭합니다.

결과

클러스터가 삭제됩니다.

5.2.10. 클러스터 호환 버전 변경

Red Hat Virtualization 클러스터에는 호환 버전이 있습니다. 클러스터 호환 버전은 클러스터에 있는 모든 호스트에 의해 지원되는 Red Hat Virtualization 기능을 표시합니다. 클러스터 호환성은 클러스터에서 최소 사용 가능한 호스트 운영 체제 버전에 따라 설정됩니다.



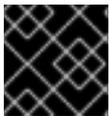
참고

클러스터 호환 버전을 변경하려면 먼저 클러스터에 있는 모든 호스트를 원하는 호환 수준을 지원하는 레벨로 업데이트해야 합니다.

절차 5.9. 클러스터 호환 버전 변경

1. 관리 포털에서 **클러스터** 탭을 클릭합니다.
2. 목록에서 변경할 클러스터를 선택합니다.
3. **편집**을 클릭합니다.
4. **호환 버전**을 원하는 값으로 변경합니다.
5. **OK**를 클릭하여 **클러스터 호환 버전 변경 확인** 창을 엽니다.
6. **OK**를 클릭하여 확인합니다.

클러스터의 호환 버전이 업데이트됩니다. 데이터 센터에 있는 모든 클러스터의 호환 버전을 업데이트한 후 데이터 센터 자체의 호환 버전을 변경할 수 있습니다.



중요

호환성을 업그레이드하면 데이터 센터에 속한 모든 스토리지 도메인도 업그레이드됩니다.

5.3. 클러스터 및 권한

5.3.1. 클러스터의 시스템 권한 관리

SuperUser로서 시스템 관리자는 관리 포털의 모든 면을 관리합니다. 보다 특정한 관리 역할은 다른 사용자에게 부여될 수 있습니다. 이러한 제한된 관리자 역할은 특정 리소스에 제한하여 사용자 관리 권한을 부여할 경우 유용합니다. 예를 들어 **DataCenterAdmin** 역할은 데이터 센터의 스토리지를 제외한 할당된 데이터 센터에 대해서만 관리자 권한을 갖으며 **ClusterAdmin**은 할당된 클러스터에 대해서만 관리자 권한을 갖습니다.

클러스터 관리자는 특정 데이터 센터에 대해서만 시스템 관리자 역할을 수행합니다. 이는 각 클러스터에 시스템 관리자가 필요한 여러 클러스터가 있는 데이터 센터의 경우 유용합니다. **ClusterAdmin** 역할은 계층적 모델로 클러스터에 대해 클러스터 관리자 역할이 지정된 사용자가 클러스터에 있는 모든 개체를 관리할 수 있습니다. 헤더 바에 있는 **설정** 버튼을 사용하여 환경의 모든 클러스터에 대해 클러스터 관리자를 지정합니다.

클러스터 관리자 역할을 사용하여 다음과 같은 작업을 실행할 수 있습니다:

- 관련된 클러스터를 생성 및 삭제합니다.
- 클러스터와 관련된 호스트, 가상 머신, 풀을 추가 및 삭제합니다.
- 클러스터와 관련된 가상 머신의 사용자 권한을 편집합니다.



참고

기존 사용자에게만 역할 및 권한을 할당할 수 있습니다.

기존 시스템 관리자를 삭제하고 새로운 시스템 관리자를 추가하여 클러스터의 시스템 관리자를 변경할 수 있습니다.

5.3.2. 클러스터 관리자 역할

클러스터 권한이 있는 역할

아래 표에서는 클러스터 관리에 적용할 수 있는 관리자 역할 및 권한에 대해 설명합니다.

표 5.11. Red Hat Virtualization 시스템 관리자 역할

역할	권한	알림
ClusterAdmin	클러스터 관리자	호스트, 템플릿, 가상 머신을 포함하여 특정 클러스터에 있는 모든 물리 및 가상 리소스를 사용, 생성, 삭제, 관리할 수 있습니다. 디스플레이 네트워크를 지정하거나 필요 또는 불필요에 따라 네트워크를 표시하는 등 클러스터 내의 네트워크 속성을 설정할 수 있습니다. 하지만 ClusterAdmin 은 클러스터에서 네트워크를 연결 또는 분리할 수 있는 권한이 없습니다. 이러한 작업을 실행하려면 NetworkAdmin 권한이 있어야 합니다.
NetworkAdmin	네트워크 관리자	특정 클러스터의 네트워크를 설정 및 관리할 수 있습니다. 클러스터의 네트워크 관리자는 클러스터 내의 가상 머신에 대한 네트워크 권한을 상속합니다.

5.3.3. 리소스에 관리자 또는 사용자 역할 할당

리소스에 관리자 또는 사용자 역할을 할당하여 사용자가 리소스에 액세스 및 관리할 수 있게 합니다.

절차 5.10. 리소스에 역할 할당

1. 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 리소스를 검색 및 선택합니다.
2. 상세 정보 창에 있는 **권한** 탭을 클릭하여 할당된 사용자, 사용자 역할, 선택한 리소스에 대해 상속된 권한을 나열합니다.
3. **추가**를 클릭합니다.
4. **검색** 텍스트 상자에 기존 사용자의 이름 또는 사용자 이름을 입력하고 **검색**을 클릭합니다. 검색 결과 목록에서 일치하는 사용자를 선택합니다.
5. **할당할 역할** 드롭 다운 목록에서 역할을 선택합니다.
6. **OK**를 클릭합니다.

사용자에게 역할이 할당되어 이제 사용자는 리소스에 대해 활성화된 역할에 상속된 권한을 갖습니다.

5.3.4. 리소스에서 관리자 또는 사용자 역할 삭제

리소스에서 관리자 또는 사용자 역할을 삭제합니다. 사용자는 리소스에서의 역할과 관련하여 상속된 권한을 손실합니다.

절차 5.11. 리소스에서 역할 삭제

1. 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 리소스를 검색 및 선택합니다.
2. 상세 정보 창에 있는 권한 탭을 클릭하여 할당된 사용자 목록, 사용자 역할, 선택한 리소스에서 상속된 권한을 나열합니다.
3. 리소스에서 삭제할 사용자를 선택합니다.
4. 삭제를 클릭합니다. 권한 삭제 창이 열리면 권한 삭제를 확인합니다.
5. **OK**를 클릭합니다.

리소스에서 사용자 역할 및 관련된 권한이 삭제됩니다.

6장. 논리 네트워크

6.1. 논리 네트워크 작업

6.1.1. 네트워크 탭 사용

네트워크 리소스 탭은 각 네트워크의 속성이나 다른 리소스와의 연결에 기반하여 논리 네트워크 관련 작업 및 검색을 수행하기 위한 중앙 지점입니다.

Red Hat Virtualization 환경의 모든 논리 네트워크는 **네트워크 탭**의 결과 목록에 표시됩니다. **새로 만들기, 편집, 삭제** 버튼을 사용하여 데이터 센터 내의 논리 네트워크 생성, 속성 변경, 삭제 등과 같은 작업을 수행할 수 있습니다.

각각의 네트워크 이름을 클릭하고 상세 정보 창에 있는 **클러스터, 호스트, 가상 머신, 템플릿, 권한** 탭을 사용하여 다음과 같은 기능을 수행합니다:

- 클러스터 및 호스트에 네트워크를 연결 또는 분리
- 가상 머신 및 템플릿에서 네트워크 인터페이스 삭제
- 네트워크 액세스 및 관리를 위해 사용자 권한 추가 및 삭제

이러한 기능은 각각의 개별 리소스 탭을 통해 액세스할 수 있습니다.



주의

호스트가 실행 중일 때 데이터 센터 또는 클러스터에 있는 네트워크를 변경할 경우 호스트에 연결되지 않을 수 있으므로 네트워크를 변경하지 않습니다.

중요

Red Hat Virtualization 노드를 사용하여 서비스를 제공하고자 할 경우 Red Hat Virtualization 환경을 실행 중지할 경우 서비스도 중지됨에 유의합니다.

이는 모든 서비스에 적용되지만 Red Hat Virtualization에서 다음과 같은 서비스를 실행하는 경우 위험한 요소가 수반될 수 있습니다:

- 디렉토리 서비스
- DNS
- 스토리지

6.1.2. 데이터 센터 또는 클러스터에 새 논리 네트워크 생성

데이터 센터 또는 데이터 센터에 있는 클러스터에 논리 네트워크를 생성하고 사용 용도를 정의합니다.

절차 6.1. 데이터 센터 또는 클러스터에 새 논리 네트워크 생성

1. **데이터 센터** 또는 **클러스터 리소스** 탭을 클릭하고 검색 결과 목록에서 데이터 센터 또는 클러스터를 선택합니다.
2. 상세 정보 창의 **논리 네트워크** 탭을 클릭하여 기존 논리 네트워크를 나열합니다.
3.
 - **데이터 센터** 상세 정보 창에서 **새로 만들기** 버튼을 클릭하여 **새 논리 네트워크** 창을 엽니다.
 - **클러스터** 상세 정보 창에서 **네트워크 추가**를 클릭하여 **새 논리 네트워크** 창을 엽니다.
4. 논리 네트워크의 **이름, 설명, 코멘트**를 입력합니다.
5. 옵션으로 **외부 공급자에 생성** 확인란을 선택합니다. 드롭 다운 목록에서 **외부 공급자**를 선택하고 **물리 네트워크**의 IP 주소를 지정합니다. **외부 공급자** 드롭 다운 목록에는 읽기 전용 모드의 외부 공급자가 표시되지 않습니다.

외부 공급자에 생성이 선택되어 있을 경우 **네트워크 레이블, 가상 머신 네트워크, MTU** 옵션은 비활성화됩니다.
6. **네트워크 레이블** 텍스트 필드에서 논리 네트워크에 새로운 레이블을 입력하거나 기존 레이블을 선택합니다.
7. 옵션으로 **VLAN 태그 활성화**를 활성화합니다.
8. 옵션으로 **가상 머신 네트워크**를 비활성화합니다.
9. **MTU** 값을 기본 (**1500**) 또는 **사용자 정의**로 설정합니다.
10. **클러스터** 탭에서 네트워크를 지정할 클러스터를 선택합니다. 논리 네트워크를 필수 네트워크로 할 지에 대한 여부를 지정할 수 있습니다.
11. **외부 공급자에 생성**을 선택한 경우 **서브넷** 탭이 표시됩니다. **서브넷** 탭에서 **서브넷 생성**을 선택하고 논리 네트워크가 제공하는 서브넷의 **이름, CIDR, 게이트웨이** 주소를 입력하고 **IP 버전**을 선택합니다. 필요에 따라 **DNS** 서버를 추가할 수 있습니다.
12. **vNIC 프로파일** 탭에서 필요에 따라 논리 네트워크에 **vNIC 프로파일**을 추가합니다.
13. **OK**를 클릭합니다.

데이터 센터에 클러스터에 필요한 리소스로 논리 네트워크가 정의됩니다. 논리 네트워크에 레이블을 지정한 경우 해당 레이블이 붙은 모든 호스트 네트워크 인터페이스에 레이블이 자동으로 추가됩니다.



참고

새 논리 네트워크를 생성하거나 디스플레이 네트워크로 사용되는 기존 논리 네트워크를 변경할 경우 네트워크가 사용 가능하게 되기 전이나 변경 사항을 적용하기 전 해당 네트워크를 사용하는 실행 중인 가상 머신을 재부팅해야 합니다.

6.1.3. 논리 네트워크 편집

논리 네트워크 설정을 편집합니다.

절차 6.2. 논리 네트워크 편집



중요

논리 네트워크가 호스트 상의 네트워크 설정과 동기화되어 있지 않은 경우 논리 네트워크는 편집하거나 다른 인터페이스로 이동할 수 없습니다. 네트워크 동기화 방법은 [6.5.2절](#), “호스트 네트워크 인터페이스 편집 및 호스트에 논리 네트워크 할당”에서 참조하십시오.

1. **데이터 센터** 리소스 탭을 클릭하고 검색 결과 목록에서 논리 네트워크의 데이터 센터를 선택합니다.
2. 상세 정보 창에서 **논리 네트워크** 탭을 클릭하여 데이터 센터에 논리 네트워크 목록을 나열합니다.
3. 논리 네트워크를 선택하고 **편집**을 클릭하여 **논리 네트워크 편집** 창을 엽니다.
4. 필요한 설정을 편집합니다.
5. **OK**를 클릭하여 변경 사항을 저장합니다.



참고

멀티 호스트 네트워크 설정은 네트워크가 할당된 데이터 센터 내에 있는 모든 호스트에 업데이트된 네트워크 설정을 자동으로 적용합니다. 네트워크를 사용하는 가상 머신이 정지 상태일 경우에만 변경 사항을 적용할 수 있습니다. 이미 호스트에 설정된 논리 네트워크 이름을 변경할 수 없습니다. 네트워크를 사용하는 가상 머신이나 템플릿이 실행되는 동안 **가상 머신 네트워크** 옵션을 비활성화할 수 없습니다.

6.1.4. 논리 네트워크 삭제

네트워크 리소스 탭 또는 **데이터 센터** 리소스 탭에서 논리 네트워크를 삭제할 수 있습니다. 다음 절차에서는 데이터 센터와 관련된 논리 네트워크를 삭제하는 방법에 대해 설명합니다. Red Hat Virtualization 환경의 경우 **ovirtmgmt** 관리 네트워크로 사용되는 최소 하나의 논리 네트워크가 있어야 합니다.

절차 6.3. 논리 네트워크 삭제

1. **데이터 센터** 리소스 탭을 클릭하고 검색 결과 목록에서 논리 네트워크의 데이터 센터를 선택합니다.
2. 상세 정보 창에서 **논리 네트워크** 탭을 클릭하여 데이터 센터에 논리 네트워크 목록을 나열합니다.
3. 논리 네트워크를 선택하고 **삭제** 버튼을 클릭하여 **논리 네트워크 삭제** 창을 엽니다.
4. 네트워크가 외부 공급자에 의해 제공되는 경우 옵션으로 **공급자에서 외부 네트워크 삭제** 확인란을 선택하여 **Manager** 및 외부 공급자 모두에서 논리 네트워크를 삭제합니다. 외부 공급자가 읽기 전용 모드인 경우 확인란이 회색으로 표시되어 사용할 수 없습니다.
5. **OK**를 클릭합니다.

논리 네트워크가 **Manager**에서 삭제되어 더 이상 사용할 수 없습니다.

6.1.5. 논리 네트워크의 게이트웨이 표시 또는 편집

사용자는 논리 네트워크의 IP 주소 및 서브넷 마스크와 함께 게이트웨이를 정의할 수 있습니다. 이는 호스트에 여러 네트워크가 존재할 때 기본 게이트웨이 대신 지정된 네트워크를 통해 트래픽을 라우팅해야 할 경우 필요합니다.

호스트에 여러 네트워크가 존재하여 게이트웨이가 정의되어 있지 않을 경우 반환 트래픽은 게이트웨이를 통해 라우팅되어 원하는 대상에 도달하지 않을 수 있습니다. 이로 인해 사용자는 호스트를 ping할 수 없습니다.

Red Hat Virtualization은 인터페이스 상태가 up 또는 down으로 될 때 마다 여러 게이트웨이를 자동으로 처리합니다.

절차 6.4. 논리 네트워크의 게이트웨이 표시 또는 편집

1. 호스트 리소스 탭을 클릭하여 원하는 호스트를 선택합니다.
2. 상세 정보 창에서 **네트워크 인터페이스** 탭을 클릭하여 호스트 및 호스트 설정에 연결된 네트워크 인터페이스를 나열합니다.
3. **호스트 네트워크 설정** 버튼을 클릭하여 **호스트 네트워크 설정** 창을 엽니다.
4. 할당된 논리 네트워크 위에 커서를 이동하고 연필 모양의 아이콘을 클릭하여 **관리 네트워크 편집** 창을 엽니다.

관리 네트워크 편집 창에 네트워크 이름, 부팅 프로토콜, IP, 서브넷 마스크, 게이트웨이 주소가 표시됩니다. 정적 부팅 프로토콜을 선택하여 주소 정보를 수동으로 편집할 수 있습니다.

6.1.6. 새 논리 네트워크 및 논리 네트워크 편집 창 설정 및 제어

6.1.6.1. 논리 네트워크의 일반 설정에 대한 설명

다음 표에서는 새 논리 네트워크 및 논리 네트워크 편집 창의 일반 탭 설정에 대해 설명합니다.

표 6.1. 새 논리 네트워크 및 논리 네트워크 편집

필드 이름	설명
이름	논리 네트워크의 이름입니다. 텍스트 필드는 최대 15자로 제한되어 있으며 알파벳 대문자, 소문자, 숫자, 하이픈, 밑줄로 조합된 고유한 이름이어야 합니다.
설명	논리 네트워크의 설명입니다. 이 텍스트 필드는 최대 40자로 제한되어 있습니다.
코멘트	논리 네트워크 관련 일반 텍스트 형식의 사용자가 읽을 수 있는 코멘트를 추가하기 위한 필드입니다.
외부 공급자에 생성	외부 공급자로 Manager에 추가된 OpenStack Networking 인스턴스에 논리적 네트워크를 생성할 수 있습니다. 외부 공급자 - 논리 볼륨이 생성될 외부 공급자를 선택할 수 있습니다.

필드 이름	설명
VLAN 태그 활성화	VLAN 태그는 논리 네트워크에서 모든 네트워크 트래픽에 특정 특성을 지정하는 보안 기능입니다. VLAN 태그가 붙은 트래픽은 동일한 특성을 가지는 인터페이스에서 읽을 수 없습니다. 논리 네트워크에서 VLAN을 사용하면 하나의 네트워크 인터페이스를 VLAN 태그가 붙은 여러 다른 논리 네트워크에 연결할 수 있습니다. VLAN 태그를 사용하려면 텍스트 입력 필드에 숫자를 입력합니다.
가상 머신 네트워크	가상 머신만 네트워크를 사용하는 경우 이 옵션을 선택합니다. 네트워크가 가상 머신에 관련 없이 스토리지 용 통신과 같은 트래픽에 사용되는 경우 이를 선택하지 마십시오.
MTU	기본을 선택하여 논리 네트워크의 최대 전송 단위 (MTU: Maximum Transmission Unit)를 괄호 안의 값으로 설정하거나 사용자 지정을 선택하여 사용자 지정 MTU를 설정합니다. 이를 사용하여 새 논리 네트워크가 지원하는 MTU 값과 인터페이스 연결하는 하드웨어가 지원하는 MTU 값을 적용할 수 있습니다. 사용자 지정을 선택한 경우 텍스트 입력 필드에 숫자를 입력합니다.
네트워크 레이블	네트워크의 새 레이블을 지정하거나 호스트 네트워크 인터페이스에 이미 연결된 기존 레이블에서 선택하여 지정할 수 있습니다. 기존 레이블을 선택한 경우 논리 네트워크는 레이블된 전체 호스트 네트워크 인터페이스에 자동으로 할당됩니다.

6.1.6.2. 논리 네트워크 클러스터 설정

다음 표에서는 새 논리 네트워크 창의 클러스터 탭 설정에 대해 설명합니다.

표 6.2. 새 논리 네트워크 설정

필드 이름	설명
-------	----

필드 이름	설명
클러스터에서 네트워크를 연결/분리	<p>데이터 센터에 있는 클러스터에서 논리 네트워크를 연결 또는 분리할 수 있으며 개별 클러스터의 네트워크에 논리 네트워크가 필요한지에 대한 여부를 지정할 수 있습니다.</p> <p>이름 - 설정을 적용할 클러스터 이름입니다. 이 값은 편집할 수 없습니다.</p> <p>모두 연결 - 데이터 센터에 있는 모든 클러스터에서 논리 네트워크를 연결 또는 분리할 수 있습니다. 다른 방법으로 각각의 클러스터 이름 옆에 있는 연결 확인란을 선택 또는 선택 해제하여 지정된 클러스터에서 논리 네트워크를 연결 또는 분리할 수 있습니다.</p> <p>모두 필수 - 모든 클러스터에서 논리 네트워크가 필수 네트워크인지의 여부를 지정할 수 있습니다. 다른 방법으로 각각의 클러스터 이름 옆에 있는 필수 확인란을 선택 또는 선택 해제하여 지정된 클러스터에서 논리 네트워크가 필수 항목인지의 여부를 지정할 수 있습니다.</p>

6.1.6.3. 논리 네트워크의 vNIC 프로파일 설정

다음 표에서는 새 논리 네트워크 창의 vNIC 프로파일 탭 설정에 대해 설명합니다.

표 6.3. 새 논리 네트워크 설정

필드 이름	설명
vNIC 프로파일	<p>논리 네트워크에 하나 이상의 vNIC 프로파일을 지정할 수 있습니다. vNIC 프로파일 옆의 플러스 또는 마이너스 버튼을 클릭하여 논리 네트워크에 vNIC 프로파일을 추가하거나 삭제할 수 있습니다.</p> <p>공개 - 프로파일을 모든 사용자가 사용할 수 있는지에 대한 여부를 지정할 수 있습니다.</p> <p>QoS - vNIC 프로파일에 네트워크 QoS (quality of service) 프로파일을 지정할 수 있습니다.</p>

6.1.7. 네트워크 관리 창에서 논리 네트워크에 특정 트래픽 유형을 지정

네트워크 트래픽 흐름을 최적화하기 위해 논리 네트워크의 트래픽 유형을 지정합니다.

절차 6.5. 논리 네트워크의 트래픽 유형 지정

1. 클러스터 리소스 탭을 클릭하고 결과 목록에서 클러스터를 선택합니다.
2. 상세 정보 창에서 논리 네트워크 탭을 선택하여 클러스터에 할당된 논리 네트워크를 나열합니다.
3. 네트워크 관리를 클릭하여 네트워크 관리 창을 엽니다.

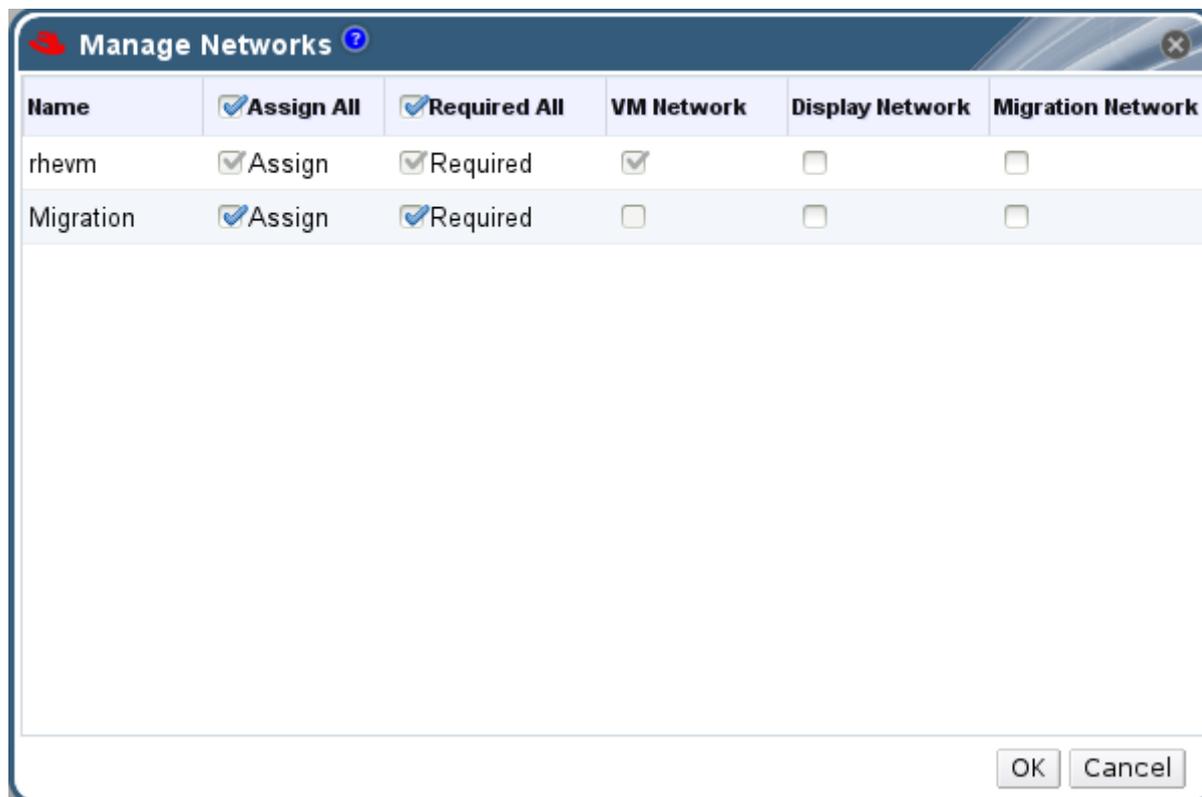


그림 6.1. 네트워크 관리

- 해당 확인란을 선택합니다.
- OK**를 클릭하여 변경 사항을 저장하고 창을 닫습니다.

특정 논리 네트워크에 전송할 특정 트래픽 유형을 지정하여 네트워크 트래픽 흐름이 최적화됩니다.



참고

외부 공급자가 제공하는 논리 네트워크는 가상 머신 네트워크로 사용해야 하며 디스플레이 또는 마이그레이션과 같은 특정 클러스터 역할을 할당할 수 없습니다.

6.1.8. 네트워크 관리 창 설정

다음 표에서는 네트워크 관리 창 설정에 대해 설명합니다.

표 6.4. 네트워크 관리 설정

필드	설명/동작
할당	클러스터에 있는 모든 호스트에 논리 네트워크를 할당합니다.
필수	네트워크에 연결된 호스트가 제대로 작동하려면 "필수"로 표시된 네트워크를 작동하는 상태로 두어야 합니다. 필수 네트워크가 작동을 중단하는 경우 네트워크에 연결된 모든 호스트는 비 작동 상태가 됩니다.

필드	설명/동작
가상 머신 네트워크	"가상 머신 네트워크"로 표시된 논리 네트워크는 가상 머신 네트워크와 관련된 네트워크 트래픽을 전송합니다.
디스플레이 네트워크	"디스플레이 네트워크"로 표시된 논리 네트워크는 SPICE 및 가상 네트워크 컨트롤러와 관련된 네트워크 트래픽을 전송합니다.
마이그레이션 네트워크	"마이그레이션 네트워크"로 표시된 논리 네트워크는 가상 머신 및 스토리지 마이그레이션 트래픽을 전송합니다.

6.1.9. NIC에서 가상 함수 (Virtual Function) 설정 편집

SR-IOV(Single Root I/O Virtualization)를 통해 단일 PCIe 끝점이 여러 개별 장치로 사용될 수 있습니다. 두 개의 PCIe 함수인 물리 함수(PF)과 가상 함수(VF)를 도입하면 이것이 가능합니다. PCIe 카드는 1개에서 8개 사이의 PF를 가질 수 있지만 각 PF은 장치에 따라 더 많은 VF를 지원합니다.

Red Hat Virtualization Manager를 사용해서 각 네트워크 인터페이스 컨트롤러(NIC)에 있는 VF의 수와 해당 VF에 액세스가 허용된 가상 네트워크 지정 등 SR-IOV가 가능한 NIC 설정을 편집합니다.

VF 생성 후 각 VF은 독립형 NIC로 취급됩니다. 하나 이상의 논리 네트워크가 할당될 수 있으며, 해당 네트워크와 결합 인터페이스 생성이 가능하며, 직접 장치 통과를 위해 네트워크에 직접적으로 vNIC를 지정할 수 있습니다.

vNIC는 통과 속성이 활성화되어 있어야 VF에 직접 연결할 수 있습니다. [6.2.4절. "vNIC 프로파일에서 통과\(passthrough\) 활성화"](#)를 참조하시기 바랍니다.

절차 6.6. NIC에서 가상 함수 (Virtual Function) 설정 편집

1. SR-IOV가 가능한 호스트를 선택하고 상세 정보 창에서 **네트워크 인터페이스** 탭을 클릭합니다.
2. **호스트 네트워크 설정**을 클릭하여 **호스트 네트워크 설정** 창을 엽니다.
3.  로 표시된 SR-IOV가 가능한 NIC를 선택하고 연필 모양의 아이콘을 클릭하여 **NICVF (SR-IOV) 설정 편집** 창을 엽니다.
4. **VF 설정** 수 드롭 다운 버튼을 클릭하고 **VF 수** 필드를 수정해서 가상 함수의 수를 편집합니다.



중요

VF 수량 변경 시 네트워크에 있는 기존 VF가 모두 삭제된 후 새 VF가 생성됩니다. 여기에는 가상 머신이 직접 연결된 VF도 모두 포함됩니다.

5. **전체 네트워크** 체크 상자가 기본으로 선택되어 모든 네트워크에서 가상 함수에 액세스할 수 있습니다. 가상 함수 액세스가 허용된 가상 네트워크를 지정하려면 **특정 네트워크** 라디오 버튼을 선택해서 모든 네트워크를 나열합니다. 원하는 네트워크의 체크 상자를 선택하거나 **레이블** 텍스트 영역을 사용해서 하나 이상의 네트워크 레이블을 바탕으로 자동으로 네트워크를 선택합니다.

6. **OK** 버튼을 클릭하여 창을 닫습니다. **호스트 네트워크 설정** 창의 **OK** 버튼을 클릭해야 변경 사항이 저장됩니다.

6.2. 가상 네트워크 인터페이스 카드

6.2.1. vNIC 프로파일 개요

vNIC (Virtual Network Interface Card) 프로파일은 Manager에 있는 개별 가상 네트워크 인터페이스 카드에 적용할 수 있는 설정 모음입니다. vNIC 프로파일을 통해 vNIC에 네트워크 QoS 프로파일을 적용하여 포트 미러링을 활성화 또는 비활성화하거나 사용자 정의 속성을 추가 또는 삭제할 수 있습니다. 또한 vNIC 프로파일을 통해 이러한 프로파일을 사용 (소비)할 수 있는 권한을 특정 사용자에게 부여하는 것과 같이 관리적 유연성을 증가시킬 수 있습니다. 이로 인해 지정된 네트워크에서 다른 사용자에게 제공되는 서비스의 품질을 제어할 수 있습니다.

6.2.2. vNIC 프로파일 생성 또는 편집

사용자 및 그룹의 네트워크 대역폭을 조정하려면 vNIC (Virtual Network Interface Controller) 프로파일을 생성 또는 편집합니다.



참고

포트 미러링이 활성화 또는 비활성화되어 있을 경우 연결된 프로파일을 사용하는 모든 가상 머신은 편집 전 중지 (down) 상태가 되어야 합니다.

절차 6.7. vNIC 프로파일 생성 또는 편집

1. **네트워크 리소스** 탭을 클릭하여 결과 창에 있는 논리 네트워크를 선택합니다.
2. 상세 정보 창에서 **vNIC 프로파일** 탭을 선택합니다. 트리 모드에서 논리 네트워크를 선택한 경우 결과 목록에서 **vNIC 프로파일** 탭을 선택할 수 있습니다.
3. **새로 만들기** 또는 **편집**을 클릭하여 가상 머신 인터페이스 프로파일 창을 엽니다.

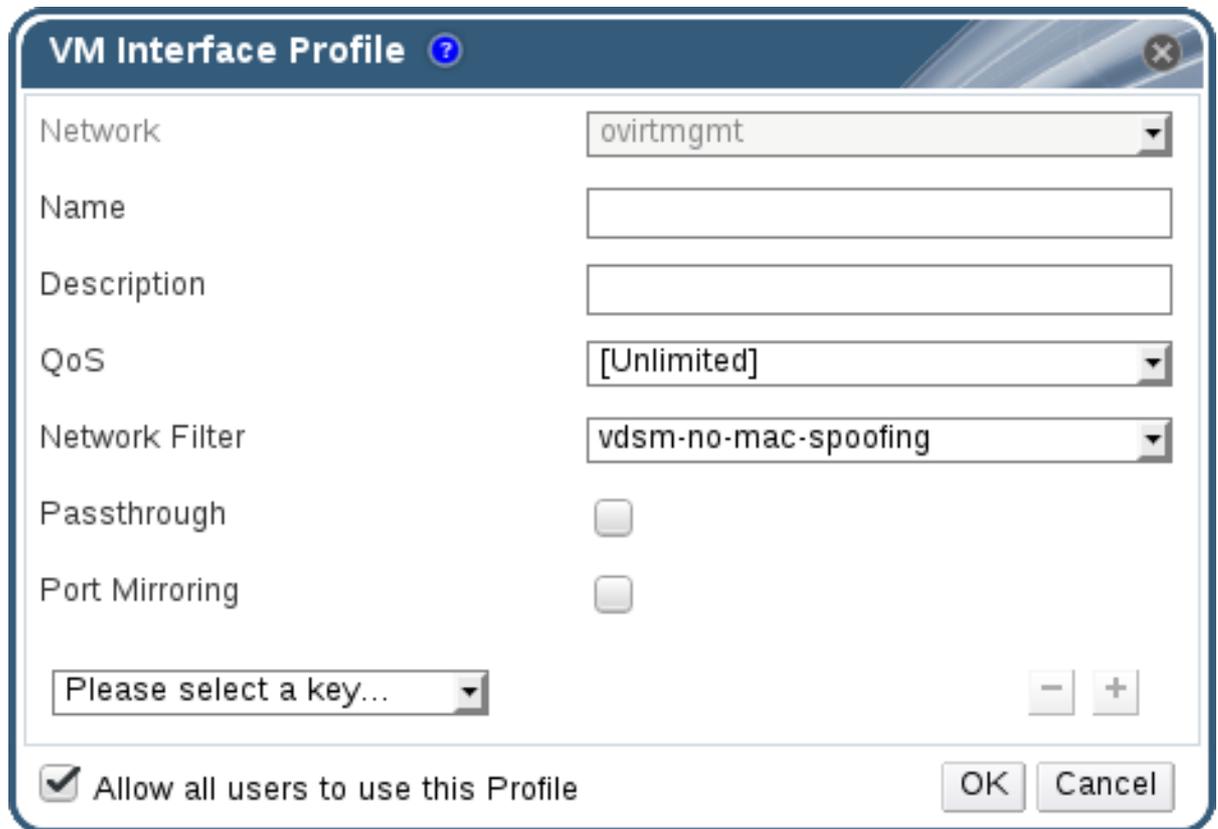
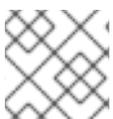


그림 6.2. 가상 머신 인터페이스 프로파일 창

4. 프로파일의 이름 및 설명을 입력합니다.
5. QoS 목록에서 적절한 QoS 정책을 선택합니다.
6. 드롭 다운 목록에서 네트워크 필터를 선택하여 가상 머신과의 네트워크 패킷 트래픽을 관리합니다. 네트워크 필터에 대한 자세한 내용은 *Red Hat Enterprise Linux Virtualization 배포 및 관리 가이드*에 있는 [네트워크 필터링 적용](#)을 참조하십시오.
7. 통과 확인란을 선택하여 vNIC 통과를 활성화하고 가상 장치를 직접 할당할 수 있도록 허용합니다. 통과 속성을 활성화하면 호환되지 않는 QoS, 네트워크 필터링 및 포트 미러링이 비활성화됩니다. 통과에 대한 자세한 내용은 [6.2.4절. "vNIC 프로파일에서 통과\(passthrough\) 활성화"](#)를 참조하십시오.
8. 포트 미러링 및 모든 사용자가 이 프로파일을 사용하도록 허용 확인란에서 이러한 옵션을 변환합니다.
9. 기본적으로 키를 선택하십시오...가 표시되는 사용자 정의 속성 목록에서 사용자 정의 속성을 선택합니다. + 및 - 버튼을 사용하여 사용자 정의 속성을 추가 또는 삭제합니다.
10. OK를 클릭합니다.

vNIC 프로파일이 생성되었습니다. 이 프로파일을 사용자 및 그룹에 적용하여 네트워크 대역폭을 조정합니다. vNIC 프로파일을 편집한 경우 가상 머신을 다시 시작하거나 핫 플러그를 해제한 후 vNIC를 핫플러그합니다.



참고

게스트 운영 체제가 vNIC 핫플러그와 핫 언플러그를 지원해야 합니다.

6.2.3. 가상 머신 인터페이스 프로파일 창 설정

표 6.5. 가상 머신 인터페이스 프로파일 창

필드 이름	설명
네트워크	vNIC 프로파일을 적용할 사용 가능한 네트워크의 드롭 다운 목록입니다.
이름	vNIC 프로파일 이름입니다. 1에서 50 자 사이의 알파벳 대소문자, 숫자, 하이픈, 밑줄로 조합된 고유한 이름이어야 합니다.
설명	vNIC 프로파일 설명입니다. 이는 권장 사항이며 필수 입력 사항은 아닙니다.
QoS	vNIC 프로파일에 적용할 사용 가능한 네트워크 QoS(Quality of Service) 정책의 드롭 다운 목록입니다. QoS 정책은 vNIC의 인바운드 및 아웃바운드 네트워크 트래픽을 조절합니다.
네트워크 필터	vNIC 프로파일 적용할 사용 가능한 네트워크 필터의 드롭 다운 목록입니다. 네트워크 필터는 가상 머신과의 전송이 가능한 패킷 유형을 필터링하여 네트워크 보안을 향상합니다. 기본 필터는 vds-m-no-mac-spoofing 으로 no-mac-spoofing 과 no-arp-mac-spoofing 의 조합입니다. libvirt에서 제공하는 네트워크 필터에 대한 자세한 내용은 <i>Red Hat Enterprise Linux Virtualization 배포 및 관리 가이드</i> 의 기존 네트워크 필터 섹션을 참조하십시오. 가상 머신 VLAN 및 본드에는 <네트워크 필터 없음>을 사용해야 합니다. 신뢰할 수 있는 가상 머신에서 네트워크 필터를 사용하지 않도록 선택하면 성능을 향상할 수 있습니다.
통과	통과(passthrough) 속성을 토글하는 체크 상자입니다. 통과는 vNIC가 호스트 NIC의 가상 함수에 직접 연결이 가능하게 합니다. vNIC 프로파일이 가상 머신에 연결되어 있는 경우 통과 속성이 편집될 수 없습니다. QoS, 네트워크 필터 및 포트 미러링은 통과(passthrough)가 활성화된 경우 vNIC 프로파일에서 비활성화됩니다.
포트 미러링	포트 미러링을 전환하는 확인란입니다. 포트 미러링은 논리 네트워크에 있는 계층 3 네트워크 트래픽을 가상 머신의 가상 인터페이스에 복사합니다. 이는 기본값으로 선택되어 있지 않습니다. 자세한 내용은 기술 참조 에 있는 포트 미러링 을 참조하십시오.
장치 사용자 정의 속성	vNIC 프로파일에 적용할 사용 가능한 사용자 정의 속성을 선택하기 위한 드롭 다운 메뉴입니다. + 및 - 버튼을 사용하여 속성을 추가 또는 삭제합니다.

필드 이름	설명
모든 사용자가 이 프로파일을 사용하도록 허용	환경에 있는 모든 사용자에게 프로파일의 사용 가능 여부를 전환하기 위한 확인란입니다. 이는 기본적으로 선택 설정되어 있습니다.

6.2.4. vNIC 프로파일에서 통과(passthrough) 활성화

vNIC 프로파일의 통과 속성을 이용하여 SR-IOV가 가능한 NIC의 가상 함수에 vNIC가 직접 연결될 수 있습니다. vNIC가 소프트웨어 네트워크 가상화를 우회해서 VF에 직접 연결해서 직접 장치 할당을 합니다.

vNIC 프로파일이 이미 vNIC에 연결된 경우 통과 속성이 활성화될 수 없습니다. 이를 방지하기 위해 해당 절차를 통해 새 프로파일이 생성됩니다. vNIC 프로파일에 통과가 활성화된 경우 해당 프로파일의 QoS 및 포트 미러링이 비활성화됩니다.

SR-IOV, 직접 장치 할당, 그리고 이를 Red Hat Virtualization에 구현하기 위한 하드웨어 고려 사항에 대한 자세한 내용은 [SR-IOV 구현을 위한 하드웨어 고려 사항](#)을 참조하십시오.

절차 6.8. 통과 활성화

1. **네트워크 결과 목록**에서 논리 네트워크 선택 후 상세 정보 창에서 **vNIC 프로파일** 탭을 클릭해서 해당 논리 네트워크의 모든 vNIC 프로파일을 나열합니다.
2. **새로 만들기**를 클릭하여 **가상 머신 인터페이스 프로파일** 창을 엽니다.
3. 프로파일의 **이름** 및 **설명**을 입력합니다.
4. **통과** 체크 상자를 선택합니다. **QoS** 및 **포트 미러링**이 비활성화됩니다.
5. 필요한 경우 기본적으로 **키를 선택하십시오...**가 표시되는 사용자 정의 속성 목록에서 사용자 정의 속성을 선택합니다. **+** 및 **-** 버튼을 사용하여 사용자 정의 속성을 추가 또는 삭제합니다.
6. **OK**를 클릭하여 프로파일을 저장하고 창을 닫습니다.

이제 vNIC 프로파일이 통과 가능합니다. 이 프로파일을 사용하여 가상 머신을 NIC 또는 PCI VF에 직접 연결하려면 논리 네트워크를 NIC에 연결하고 통과 vNIC 프로파일을 사용하는 원하는 가상 머신에 새로운 vNIC를 생성합니다. 이러한 각 절차에 대한 자세한 내용은 [가상 머신 관리 가이드](#)에 있는 [6.5.2절. "호스트 네트워크 인터페이스 편집 및 호스트에 논리 네트워크 할당"](#) 및 [새로운 네트워크 인터페이스 추가](#)를 참조하십시오.

6.2.5. vNIC 프로파일 삭제

가상화 환경에서 vNIC 프로파일을 삭제합니다.

절차 6.9. vNIC 프로파일 삭제

1. **네트워크 리소스** 탭을 클릭하여 결과 창에 있는 논리 네트워크를 선택합니다.
2. 상세 정보 창에서 **프로파일** 탭을 선택하여 사용 가능한 vNIC 프로파일을 표시합니다. 트리 모드에서 논리 네트워크를 선택한 경우 결과 목록에서 **vNIC 프로파일** 탭을 선택할 수 있습니다.
3. 하나 이상의 프로파일을 선택하고 **제거**를 클릭하여 **가상 머신 인터페이스 프로파일 삭제** 창을

입니다.

4. **OK**를 클릭하여 프로파일을 삭제하고 창을 닫습니다.

6.2.6. vNIC 프로파일에 보안 그룹 할당



참고

이 기능은 OpenStack Neutron과 통합된 사용자만 사용할 수 있습니다. 보안 그룹은 Red Hat Virtualization Manager로 생성할 수 없습니다. OpenStack 내에 보안 그룹을 생성해야 합니다. 보다 자세한 내용은 *Red Hat OpenStack Platform Users and Identity Management Guide*에 있는 <https://access.redhat.com/documentation/en/red-hat-openstack-platform/9/single/users-and-identity-management-guide#project-security>에서 참조하십시오.

OpenStack Networking 인스턴스에서 가져오기한 Open vSwitch 플러그인을 사용하는 네트워크의 vNIC 프로파일에 보안 그룹을 지정할 수 있습니다. 보안 그룹은 네트워크 인터페이스를 통해 인바운드 및 아웃바운드 트래픽을 필터링할 수 있도록 엄격하게 실행되는 규칙 모음입니다. 다음 절차에서는 vNIC 프로파일에 보안 그룹을 연결하는 방법에 대해 설명합니다.



참고

보안 그룹은 OpenStack Networking 인스턴스에 등록된 보안 그룹의 ID를 사용하여 식별됩니다. OpenStack Networking이 설치된 시스템에서 다음 명령을 실행하여 특정 테넌트의 보안 그룹 ID를 확인할 수 있습니다:

```
# neutron security-group-list
```

절차 6.10. vNIC 프로파일에 보안 그룹 할당

1. **네트워크** 탭을 클릭하여 결과 창에 있는 논리 네트워크를 선택합니다.
2. 상세 정보 창에서 **vNIC 프로파일** 탭을 클릭합니다.
3. **새로 만들기**를 클릭하거나 또는 기존 vNIC 프로파일을 선택하고 **편집**을 클릭하여 **가상 머신 인터페이스 프로파일** 창을 엽니다.
4. 사용자 정의 속성 드롭 다운 목록에서 **보안 그룹**을 선택합니다. 사용자 정의 속성 드롭 다운 목록이 비워 있을 경우 기본 보안 그룹이 적용되어 모든 아웃바운드 트래픽 및 내부 통신을 허용하지만 기본 보안 그룹 외부에서 들어오는 모든 인바운드 트래픽은 거부합니다. **보안 그룹** 속성을 나중에 삭제해도 이미 적용된 보안 그룹에는 영향을 주지 않음에 유의합니다.
5. 텍스트 필드에 vNIC 프로파일에 연결할 보안 그룹 ID를 입력합니다.
6. **OK**를 클릭합니다.

보안 그룹이 vNIC 프로파일에 연결되었습니다. 프로파일이 연결된 논리 네트워크를 통한 모든 트래픽은 보안 그룹에서 정의된 규칙에 따라 필터링됩니다.

6.2.7. vNIC 프로파일 사용자 권한

사용자를 특정 vNIC 프로파일에 지정하기 위한 사용자 권한을 설정합니다. 사용자가 프로파일을 사용할 수 있도록 사용자에게 **VnicProfileUser** 역할을 할당합니다. 해당 프로파일의 권한을 삭제하여 특정 프

로파일을 사용할 수 없도록 사용자를 제한할 수 있습니다.

절차 6.11. vNIC 프로파일 사용자 권한

1. 네트워크 탭을 클릭하여 결과 창에 있는 논리 네트워크를 선택합니다.
2. vNIC 프로파일 리소스 탭을 선택하여 vNIC 프로파일을 표시합니다.
3. 상세 정보 창에서 권한 탭을 선택하여 프로파일의 현재 사용자 권한을 표시합니다.
4. 추가 버튼을 사용하여 사용자에게 권한 추가 창을 열고 삭제 버튼을 사용하여 권한 삭제 창을 열어 vNIC 프로파일의 사용자 권한을 설정합니다.

vNIC 프로파일의 사용자 권한이 설정됩니다.

6.2.8. UCS 통합을 위한 vNIC 프로파일 설정

Cisco의 통합 컴퓨팅 시스템(UCS)은 컴퓨팅, 네트워킹, 스토리지 리소스 등의 데이터 센터 관련 사항을 관리하는 데 사용됩니다.

vds-hook-vmfex-dev 후크를 사용하여 가상 머신이 vNIC 설정 후 Cisco의 UCS 정의 포트 프로파일에 연결될 수 있습니다. UCS 정의 포트 프로파일에는 UCS의 가상 인터페이스 설정에 사용되는 속성과 설정이 포함되어 있습니다. 기본적으로 **vds-hook-vmfex-dev** 후크가 VDSM에 설치됩니다. 더 자세한 정보는 [부록 A. VDSM 및 후크](#)를 참조하십시오.

vNIC 프로파일을 사용하는 가상 머신 생성 시 Cisco vNIC를 사용합니다.

UCS 통합을 위한 vNIC 프로파일 설정 절차의 첫 단계는 사용자 정의 장치 속성을 설정하는 것입니다. 사용자 정의 장치 속성을 설정할 때 기존 값은 덮어쓰기 되므로 이에 유의합니다. 기존 및 새로운 사용자 정의 속성 통합 시 키 값 설정에 사용되는 명령에 있는 모든 사용자 정의 속성을 입력해야 합니다. 각 사용자 정의 속성은 세미콜론으로 구분합니다.



참고

vNIC 프로파일 설정 전에 Cisco UCS에 UCS 포트 프로파일이 먼저 설정되어야 합니다.

절차 6.12. 사용자 정의 장치 속성 설정

1. Red Hat Virtualization Manager에서 **--cver**를 사용해서 **vmfex** 사용자 정의 속성 및 클러스터 호환 수준을 설정합니다.

```
# engine-config -s CustomDeviceProperties='{type=interface;prop={vmfex=[a-zA-Z0-9_.-]{2,32}}}' --cver=3.6
```

2. **vmfex** 사용자 정의 장치 속성의 추가 여부를 확인합니다.

```
# engine-config -g CustomDeviceProperties
```

3. engine을 다시 시작합니다.

```
# systemctl restart ovirt-engine.service
```

설정 대상 vNIC 프로파일은 기존 또는 새로운 논리 네트워크에 속해 있습니다. 새로운 논리 네트워크 설정 방법은 [6.1.2절. "데이터 센터 또는 클러스터에 새 논리 네트워크 생성"](#)을 참조하시기 바랍니다.

절차 6.13. UCS 통합을 위한 vNIC 프로파일 설정

1. **네트워크** 리소스 탭을 클릭하여 결과 창에 있는 논리 네트워크를 선택합니다.
2. 상세 정보 창에서 **vNIC 프로파일** 탭을 선택합니다. 트리 모드에서 논리 네트워크를 선택한 경우 결과 목록에서 **vNIC 프로파일** 탭을 선택할 수 있습니다.
3. **새로 만들기** 또는 **편집**을 클릭하여 **가상 머신 인터페이스 프로파일** 창을 엽니다.
4. 프로파일의 **이름** 및 **설명**을 입력합니다.
5. 사용자 정의 속성 목록에서 **vmfex** 사용자 정의 속성을 선택하고 **UCS 포트 프로파일 이름**을 입력합니다.
6. **OK**를 클릭합니다.

6.3. 외부 공급자 네트워크

6.3.1. 외부 공급자에서 네트워크 가져오기

외부 공급자(OpenStack Networking 또는 OpenStack Neutron REST API를 구현하는 타사 공급자)의 네트워크를 사용하려면 해당 공급자를 Manager에 등록합니다. 자세한 정보는 [12.2.3절. “네트워크 프로비저닝을 위해 OpenStack Networking \(Neutron\) 인스턴스 추가”](#) 또는 [12.2.6절. “외부 네트워크 공급자 추가”](#)를 참조하십시오. 다음의 절차를 이용해서 해당 공급자가 제공하는 네트워크를 Manager로 가져오면 가상 머신에서 해당 네트워크를 사용할 수 있습니다.

절차 6.14. 외부 공급자에서 네트워크 가져오기

1. **네트워크** 탭을 클릭합니다.
2. **가져오기** 버튼을 클릭하여 **네트워크 가져오기** 창을 엽니다.

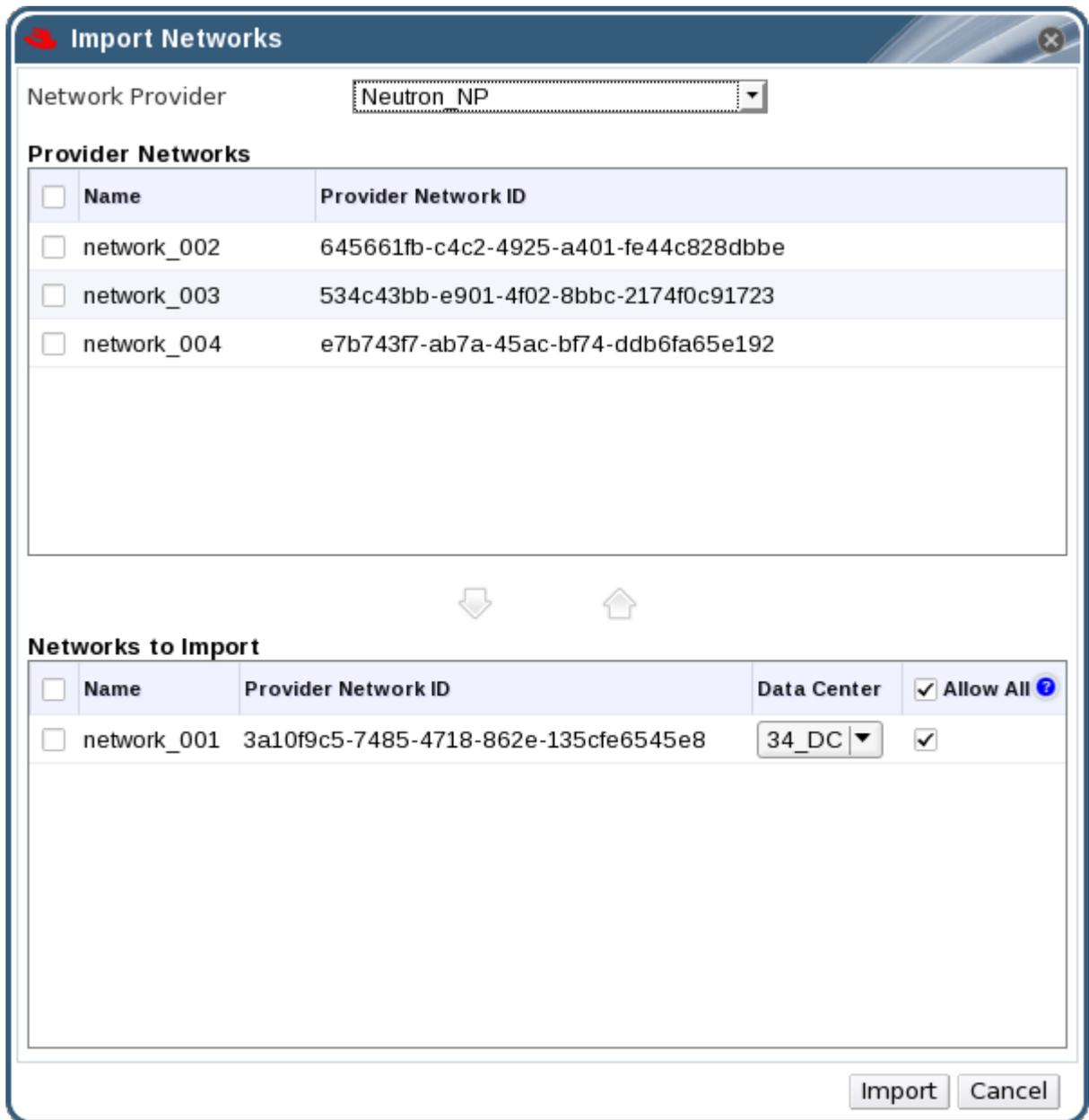


그림 6.3. 네트워크 가져오기 창

3. **네트워크 공급자** 드롭 다운 메뉴에서 외부 공급자를 선택합니다. 공급자가 제공하는 네트워크가 자동으로 감지되어 **공급자 네트워크** 목록에 나열됩니다.
4. 체크 상자를 사용하여 **공급자 네트워크** 목록에서 가져오기할 네트워크를 선택하고 아래로 이동 화살표를 클릭하여 이 네트워크를 **가져오기할 네트워크** 목록으로 이동합니다.
5. 가져오기 할 네트워크 이름을 사용자가 지정할 수 있습니다. 이름을 사용자 지정하려면 **이름** 란에 있는 네트워크 이름을 클릭하고 텍스트를 변경합니다.
6. **데이터 센터** 드롭 다운 목록에서 네트워크를 가져오기할 데이터 센터를 선택합니다.
7. 옵션으로 **가져오기할 네트워크** 목록에 있는 네트워크의 모두 **허용** 체크 상자를 선택해제하여 모든 사용자에게 네트워크 사용을 허용하지 않습니다.
8. **가져오기** 버튼을 클릭합니다.

선택한 네트워크를 대상 데이터 센터로 가져온 후 가상 머신에 연결할 수 있습니다. 자세한 내용은 **가상 머신 관리 가이드**에 있는 **새 네트워크 인터페이스 추가**를 참조하십시오.

6.3.2. 외부 공급자 네트워크 사용 제한

Red Hat Virtualization 환경의 외부 공급자에서 가져온 논리 네트워크를 사용하려면 다음과 같은 제한 사항이 적용됩니다.

- 외부 공급자가 제공하는 논리 네트워크는 가상 머신 네트워크로 사용해야 하며 디스플레이 네트워크로 사용할 수 없습니다.
- 동일한 논리 네트워크를 다른 데이터 센터에만 한 번 이상 가져오기할 수 있습니다.
- **Manager**에서 외부 공급자가 제공하는 논리 네트워크를 편집할 수 없습니다. 외부 공급자가 제공하는 논리 네트워크의 상세 정보를 편집하려면 논리 네트워크를 제공하는 외부 공급자에서 논리 네트워크를 직접 편집해야 합니다.
- 외부 공급자에서 제공하는 논리 네트워크에 연결된 가상 네트워크 인터페이스 카드의 경우 포트 미러링을 사용할 수 없습니다.
- 외부 공급자가 제공하는 논리 네트워크를 가상 머신이 사용할 경우 논리 네트워크가 가상 머신에 의해 사용되고 있는 동안 **Manager**에서 공급자를 삭제할 수 없습니다.
- 외부 공급자가 제공하는 네트워크는 필수가 아닙니다. 따라서 이러한 논리 네트워크를 가져오기 한 클러스터 스케줄링 시 호스트 선택에서 이러한 논리 네트워크를 고려하지 않습니다. 이에 더하여 사용자는 이러한 논리 네트워크를 가져오기한 클러스터에 있는 호스트 상의 논리 네트워크를 사용할 수 있게 해야 합니다.



중요

외부 공급자에서 가져오기한 논리 네트워크는 Red Hat Enterprise Linux 호스트와만 호환 가능하며 RHVH에서 실행되고 있는 가상 머신에 지정할 수 없습니다.

6.3.3. 외부 공급자 논리 네트워크에서 서브넷 설정

6.3.3.1. 외부 공급자 논리 네트워크에서 서브넷 설정

하나 이상의 서브넷이 논리 네트워크에 정의되어 있을 경우 외부 공급자에 의해 지정된 논리 네트워크는 가상 머신에 IP 주소를 할당할 수 있습니다. 서브넷이 지정되어 있지 않을 경우 가상 머신은 IP 주소를 할당하지 않게 됩니다. 하나의 서브넷이 있을 경우 가상 머신은 서브넷에서 IP 주소를 할당하고 여러 서브넷이 있을 경우 가상 머신은 사용 가능한 모든 서브넷에서 IP 주소를 할당하게 됩니다. 논리 네트워크가 호스트되는 외부 네트워크 공급자에 의해 지정된 DHCP 서비스는 이러한 IP 주소를 할당하는 역할을 합니다.

Red Hat Virtualization Manager는 가져오기한 논리 네트워크에서 사전 정의된 서브넷을 자동으로 감지하지만 Manager 내 논리 네트워크에서 서브넷을 추가 또는 삭제할 수 있습니다.

6.3.3.2. 외부 공급자 논리 네트워크에 서브넷 추가

외부 공급자가 지정한 논리 네트워크에 서브넷을 생성합니다.

절차 6.15. 외부 공급자 논리 네트워크에 서브넷 추가

1. 네트워크 탭을 클릭합니다.
2. 외부 공급자에 의해 지정된 논리 네트워크에서 서브넷을 추가할 논리 네트워크를 클릭합니다.
3. 상세 정보 창에서 서브넷 탭을 클릭합니다.

4. 새로 만들기 버튼을 클릭하여 새 외부 서브넷 창을 엽니다.

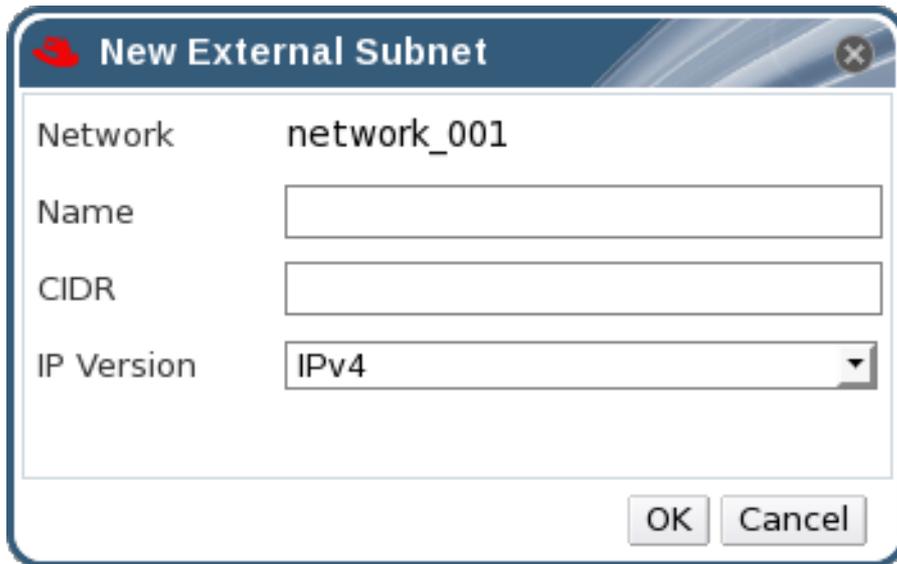


그림 6.4. 새 외부 서브넷 창

5. 새 서브넷의 이름 및 CIDR을 입력합니다.
6. IP 버전 드롭 다운 메뉴에서 IPv4 또는 IPv6를 선택합니다.
7. OK를 클릭합니다.

6.3.3.3. 외부 공급자 논리 네트워크에서 서브넷 삭제

외부 공급자가 지정한 논리 네트워크에서 서브넷을 삭제합니다.

절차 6.16. 외부 공급자 논리 네트워크에서 서브넷 삭제

1. 네트워크 탭을 클릭합니다.
2. 외부 공급자에 의해 지정된 논리 네트워크에서 서브넷을 삭제할 논리 네트워크를 클릭합니다.
3. 상세 정보 창에서 서브넷 탭을 클릭합니다.
4. 삭제하고자 하는 서브넷을 클릭합니다.
5. 삭제 버튼을 클릭하고 메시지가 나타나면 OK를 클릭합니다.

6.4. 논리 네트워크 및 권한

6.4.1. 네트워크의 시스템 권한 관리

SuperUser로서 시스템 관리자는 관리 포털의 모든 면을 관리합니다. 보다 특정한 관리 역할은 다른 사용자에게 부여될 수 있습니다. 이러한 제한된 관리자 역할은 특정 리소스에 제한하여 사용자 관리 권한을 부여할 경우 유용합니다. 예를 들어 **DataCenterAdmin** 역할은 데이터 센터의 스토리지를 제외한 할당된 데이터 센터에 대해서만 관리자 권한을 갖으며 **ClusterAdmin**은 할당된 클러스터에 대해서만 관리자 권한을 갖습니다.

네트워크 관리자는 특정 네트워크 또는 데이터 센터, 클러스터, 호스트 가상 머신, 템플릿의 모든 네트워크에 할당할 수 있는 시스템 관리 역할입니다. 네트워크 사용자는 특정 가상 머신 또는 템플릿에 네트워크

를 연결 및 확인과 같은 제한된 관리 역할을 수행할 수 있습니다. 머리글 표시줄에 있는 **설정** 버튼을 사용하여 환경의 모든 네트워크에 네트워크 관리자를 할당할 수 있습니다.

네트워크 관리자 역할을 사용하여 다음과 같은 작업을 실행할 수 있습니다:

- 네트워크를 생성, 편집, 삭제합니다.
- 포트 미러링 설정을 포함하여 네트워크 설정을 편집합니다.
- 클러스터 및 가상 머신을 포함하여 리소스에서 네트워크를 연결 및 분리합니다.

네트워크를 생성한 사용자에게는 생성한 네트워크에 **NetworkAdmin** 권한이 자동으로 할당됩니다. 기존 관리자를 삭제하거나 새 관리자를 추가하여 네트워크 관리자를 변경할 수도 있습니다.

6.4.2. 네트워크 관리자 및 사용자 역할

네트워크 권한이 있는 역할

아래 표에서는 네트워크 관리에 적용할 수 있는 관리자와 사용자 역할 및 권한에 대해 설명합니다.

표 6.6. Red Hat Virtualization 네트워크 관리자 및 사용자 역할

역할	권한	알림
NetworkAdmin	데이터 센터, 클러스터, 호스트, 가상 머신, 템플릿에 대한 네트워크 관리자입니다. 네트워크를 생성한 사용자에게는 생성된 네트워크에 대한 NetworkAdmin 권한이 자동으로 부여됩니다.	특정 데이터 센터, 클러스터, 호스트, 가상 머신, 템플릿의 네트워크를 설정 및 관리할 수 있습니다. 데이터 센터 또는 클러스터의 네트워크 관리자는 클러스터 내의 가상 풀에 대한 네트워크 권한을 상속합니다. 가상 머신 네트워크에서 포트 미러링을 설정하려면 네트워크에서 NetworkAdmin 역할 및 가상 머신에서 UserVmManager 역할을 적용합니다.
VnicProfileUser	가상 머신 및 템플릿에 대한 논리 네트워크 및 네트워크 인터페이스 사용자입니다.	특정 논리 네트워크에서 네트워크 인터페이스를 연결 또는 분리할 수 있습니다.

6.4.3. 리소스에 관리자 또는 사용자 역할 할당

리소스에 관리자 또는 사용자 역할을 할당하여 사용자가 리소스에 액세스 및 관리할 수 있게 합니다.

절차 6.17. 리소스에 역할 할당

1. 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 리소스를 검색 및 선택합니다.
2. 상세 정보 창에 있는 **권한** 탭을 클릭하여 할당된 사용자, 사용자 역할, 선택한 리소스에 대해 상속된 권한을 나열합니다.
3. **추가**를 클릭합니다.

4. **검색** 텍스트 상자에 기존 사용자의 이름 또는 사용자 이름을 입력하고 **검색**을 클릭합니다. 검색 결과 목록에서 일치하는 사용자를 선택합니다.
5. **할당할 역할** 드롭 다운 목록에서 역할을 선택합니다.
6. **OK**를 클릭합니다.

사용자에게 역할이 할당되어 이제 사용자는 리소스에 대해 활성화된 역할에 상속된 권한을 갖습니다.

6.4.4. 리소스에서 관리자 또는 사용자 역할 삭제

리소스에서 관리자 또는 사용자 역할을 삭제합니다. 사용자는 리소스에서의 역할과 관련하여 상속된 권한을 손실합니다.

절차 6.18. 리소스에서 역할 삭제

1. 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 리소스를 검색 및 선택합니다.
2. 상세 정보 창에 있는 **권한** 탭을 클릭하여 할당된 사용자 목록, 사용자 역할, 선택한 리소스에서 상속된 권한을 나열합니다.
3. 리소스에서 삭제할 사용자를 선택합니다.
4. **삭제**를 클릭합니다. **권한 삭제** 창이 열리면 권한 삭제를 확인합니다.
5. **OK**를 클릭합니다.

리소스에서 사용자 역할 및 관련된 권한이 삭제됩니다.

6.5. 호스트 및 네트워킹

6.5.1. 호스트 기능 새로 고침

네트워크 인터페이스 카드를 호스트에 추가한 경우 호스트 기능을 새로 고침하여 **Manager**에 네트워크 인터페이스 카드를 표시합니다.

절차 6.19. 호스트 기능 새로 고침 방법

1. 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 호스트를 검색 및 선택합니다.
2. **기능을 새로 고침** 버튼을 클릭합니다.

선택한 호스트의 상세 정보 창에 있는 **네트워크 인터페이스** 탭의 네트워크 인터페이스 카드 목록이 업데이트됩니다. 새로운 네트워크 인터페이스 카드를 **Manager**에서 사용할 수 있습니다.

6.5.2. 호스트 네트워크 인터페이스 편집 및 호스트에 논리 네트워크 할당

물리적 호스트의 네트워크 인터페이스의 설정을 변경, 하나의 물리적 호스트의 네트워크 인터페이스에서 다른 인터페이스로 관리 네트워크를 이전, 물리적 호스트의 네트워크 인터페이스에 논리 네트워크를 할당할 수 있습니다. 브릿지 및 **ethtool** 사용자 지정 속성도 지원됩니다.



주의

Red Hat Virtualization에서 호스트의 IP 주소를 변경하는 유일한 방법은 호스트를 제거한 다음 다시 추가하는 것입니다.

호스트의 VLAN 설정을 변경하려면 Manager에서 호스트를 제거하고 다시 설정한 다음 Manager에 다시 추가해야 합니다.

네트워킹의 동기화를 유지하려면 다음을 수행합니다. 호스트를 유지관리 모드로 전환하고 수동으로 관리 네트워크를 호스트에서 제거합니다. 이렇게 하면 새로운 VLAN에서 호스트에 연결할 수 있습니다. 호스트를 클러스터에 추가합니다. 관리 네트워크에 직접 연결되지 않은 가상 머신은 호스트 간에 안전하게 마이그레이션할 수 있습니다.

관리 네트워크의 VLAN ID가 변경되면 다음 경고 메시지가 나타납니다.

관리 네트워크의 특정 속성 (예: VLAN, MTU)을 변경하면 기본 네트워크 인프라가 이러한 변경 사항에 대응하도록 설정되어 있지 않을 경우 데이터 센터에서 호스트에 연결이 끊어질 수 있습니다. 작업을 계속 진행하시겠습니까?

계속 진행하면 데이터 센터에 있는 모든 호스트의 Manager에 대한 연결이 손실되며 호스트가 새 관리 네트워크로 마이그레이션되지 않습니다. 관리 네트워크는 "비동기화"로 보고됩니다.



중요

외부 공급자에 의해 제공되는 논리 네트워크를 물리적 호스트의 네트워크 인터페이스에 할당할 수 없습니다. 이러한 네트워크는 가상 머신의 요청에 따라 호스트에 동적으로 할당됩니다.

절차 6.20. 호스트 네트워크 인터페이스 편집 및 호스트에 논리 네트워크 할당

1. 호스트 리소스 탭을 클릭하여 원하는 호스트를 선택합니다.
2. 상세 정보 창에서 **네트워크 인터페이스** 탭을 클릭합니다.
3. **호스트 네트워크 설정** 버튼을 클릭하여 **호스트 네트워크 설정** 창을 엽니다.
4. 물리적 호스트의 네트워크 인터페이스 옆에 있는 **할당된 논리 네트워크** 영역으로 선택 및 드래그하여 논리 네트워크를 물리적 호스트 네트워크 인터페이스에 연결합니다.

다른 방법으로 논리 네트워크를 오른쪽 클릭하여 드롭 다운 메뉴에서 네트워크 인터페이스를 선택합니다.

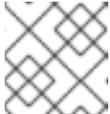
5. 논리 네트워크 설정:
 - a. 할당된 논리 네트워크 위에 커서를 이동하고 연필 모양의 아이콘을 클릭하여 **관리 네트워크 편집** 창을 엽니다.

- b. **IPv4** 탭에서 **부트 프로토콜**을 **None, DHCP, Static** 중에서 선택합니다. **Static**을 선택한 경우 **IP, 넷마스크 / 라우팅 접두사 및 게이트웨이**를 입력합니다.



참고

각 논리 네트워크는 관리 네트워크 게이트웨이에서 정의된 다른 게이트웨이를 가질 수 있습니다. 이렇게 하면 논리 네트워크에 도착하는 트래픽이 관리 네트워크에서 사용되는 기본 게이트웨이가 아닌 논리 네트워크 게이트웨이를 사용하도록 전달됩니다.



참고

IPv6 탭은 현재 지원되지 않으므로 사용할 수 없습니다.

- c. **QoS** 탭을 사용하여 기본 호스트 네트워크의 **QoS**를 덮어쓰기합니다. **QoS 덮어쓰기**를 선택하고 다음 필드에 원하는 값을 입력합니다.
- **가중 공유**: 같은 논리 링크에 연결된 다른 네트워크와 비교해서 어떤 특정 네트워크에 해당 논리 링크의 용량이 얼마나 할당되는지를 나타냅니다. 정확한 공유량은 해당 링크의 모든 네트워크의 총 공유량에 따라 다릅니다. 기본으로 이 수치는 **1-100** 범위에 있습니다.
 - **속도 제한 [Mbps]**: 네트워크가 사용하는 최대 대역폭입니다.
 - **커밋 속도 [Mbps]**: 네트워크가 필요로 하는 최소 대역폭입니다. 사용자가 요청하는 커밋 속도는 보장되지 않으며 네트워크 인프라와 같은 논리 링크에 있는 다른 네트워크에서 요청하는 커밋 속도에 따라 다릅니다.

호스트 네트워크 QoS 설정에 대한 자세한 정보는 [3.3절](#). "[호스트 네트워크 QoS](#)"를 참조하십시오.

- d. 네트워크 브릿지를 설정하려면 **사용자 정의 속성** 탭을 클릭하고 드롭다운 목록에서 **bridge_opts**를 선택합니다. **key=value** 구문을 사용하여 유효한 키와 값을 입력합니다. 여러 항목이 있을 경우 공백으로 구분합니다. 다음과 같은 키가 유효합니다(값은 예로 제공됩니다). 이러한 매개 변수에 대한 자세한 정보는 [B.1절](#). "[bridge_opts 매개 변수](#)"을 참조하십시오.

```
forward_delay=1500
gc_timer=3765
group_addr=1:80:c2:0:0:0
group_fwd_mask=0x0
hash_elasticity=4
hash_max=512
hello_time=200
hello_timer=70
max_age=2000
multicast_last_member_count=2
multicast_last_member_interval=100
multicast_membership_interval=26000
multicast_querier=0
multicast_querier_interval=25500
multicast_query_interval=13000
multicast_query_response_interval=1000
multicast_query_use_ifaddr=0
multicast_router=1
```

```
multicast_snooping=1
multicast_startup_query_count=2
multicast_startup_query_interval=3125
```

- e. 이더넷 속성을 설정하려면 **사용자 정의 속성** 탭을 클릭하고 드롭다운 목록에서 **ethtool_opts**를 선택합니다. ethtool의 명령행 인수 형식을 사용하여 유효한 값을 입력합니다. 예를 들면 다음과 같습니다.

```
--coalesce em1 rx-usecs 14 sample-interval 3 --offload em2 rx on
lro on tso off --change em1 speed 1000 duplex half
```

이 필드에는 와일드카드를 사용할 수 있습니다. 예를 들어 동일한 옵션을 이 네트워크의 모든 인터페이스에 적용하려면 다음을 사용합니다.

```
--coalesce * rx-usecs 14 sample-interval 3
```

ethtool_opts 옵션은 기본적으로 사용할 수 없습니다. 엔진 설정 도구를 사용하여 추가해야 합니다. 자세한 내용은 [B.2절. “Ethtool 사용을 위해 Red Hat Virtualization Manager 설정”](#)을 참조하십시오. ethtool 속성에 대한 자세한 내용은 명령행에 **man ethtool**을 입력하여 **man** 페이지를 참조하십시오.

- f. FCoE(Fibre Channel over Ethernet)를 설정하려면 **사용자 정의 속성** 탭을 클릭하고 드롭다운 목록에서 **fcoe**를 선택합니다. **key=value** 구문을 사용하여 유효한 키와 값을 입력합니다. 최소한 **enable=yes**가 필요합니다. **dcbe=[yes|no]** 및 **auto_vlan=[yes|no]**를 추가할 수도 있습니다. 여러 항목이 있을 경우 공백으로 구분합니다. **fcoe** 옵션은 기본적으로 사용할 수 없습니다. 엔진 설정 도구를 사용하여 추가해야 합니다. 자세한 내용은 [B.3절. “FCoE를 사용하기 위해 Red Hat Virtualization Manager를 설정하는 방법”](#)을 참조하십시오.



참고

FCoE에는 별도의 전용 논리 네트워크를 사용하는 것이 좋습니다.

- g. 관리 네트워크(ovirtmgmt)에서 비관리 네트워크로 호스트에서 사용하는 기본 네트워크를 변경하려면 **사용자 정의 속성** 탭에서 **default_route** 속성을 설정합니다.

i. 관리 네트워크의 경우 **default_route** 사용자 정의 속성을 **false**로 설정합니다.

ii. 비관리 네트워크의 경우 **default_route**를 **true**로 설정합니다.

데이터 센터의 각 호스트에서 이 설정을 반복합니다. **default_route** 옵션은 기본적으로 사용할 수 없습니다. 엔진 설정 도구를 사용하여 추가해야 합니다. 자세한 내용은 [B.4절. “비관리 네트워크를 사용하기 위해 Red Hat Virtualization Manager를 설정하는 방법”](#)을 참조하십시오.

- h. 논리 네트워크 정의가 호스트 상의 네트워크 설정과 동기화되어 있지 않을 경우 **네트워크 동기화** 확인란을 선택합니다. 논리 네트워크는 동기화되기 전 까지 다른 인터페이스로 이동하거나 편집할 수 없습니다.



참고

네트워크가 다음 중 하나의 상태일 경우 동기화된 것으로 간주되지 않습니다:

- 가상 머신 네트워크는 물리적 호스트 네트워크와 다른 경우.
- VLAN ID는 물리적 호스트 네트워크와 다른 경우.
- 사용자 정의 MTU는 논리 네트워크 상에 설정되어 물리적 호스트 네트워크와 다른 경우.

6. 호스트와 Engine간의 연결을 확인 확인란을 선택하여 네트워크 연결 상태를 확인합니다. 이러한 동작은 호스트가 유지 관리 모드일 경우에만 작동합니다.
7. 네트워크 설정 저장 확인란을 선택하여 시스템을 재부팅했을 경우 변경 사항을 영구적으로 저장합니다.
8. OK를 클릭합니다.



참고

호스트의 모든 네트워크 인터페이스 카드가 표시되지 않을 경우 기능을 새로 고침 버튼을 클릭하여 호스트에서 사용 가능한 네트워크 인터페이스 카드 목록을 업데이트합니다.

6.5.3. 논리 네트워크를 사용하여 단일 네트워크 인터페이스에 여러 VLAN 추가

여러 VLAN을 단일 네트워크 인터페이스에 추가하여 하나의 호스트에 있는 트래픽을 분리합니다.



중요

새 논리 네트워크 또는 논리 네트워크 편집 창에서 VLAN 태깅 활성화 확인란을 선택하여 여러 논리 네트워크를 생성해야 합니다.

절차 6.21. 논리 네트워크를 사용하여 네트워크 인터페이스에 여러 VLAN 추가

1. 호스트 리소스 탭을 클릭하고 결과 목록에서 VLAN 태그 논리 네트워크가 할당된 클러스터에 연결된 호스트를 선택합니다.
2. 상세 정보 창에서 네트워크 인터페이스 탭을 클릭하여 데이터 센터에 연결된 실제 네트워크 인터페이스를 나열합니다.
3. 호스트 네트워크 설정을 클릭하여 호스트 네트워크 설정 창을 엽니다.
4. VLAN 태그 논리 네트워크를 물리 네트워크 인터페이스 옆에 있는 할당된 논리 네트워크 영역으로 드래그합니다. VLAN 태그로 물리 네트워크 인터페이스에 여러 논리 네트워크를 할당할 수 있습니다.
5. 할당된 논리 네트워크 위에 커서를 이동하고 연필 모양의 아이콘을 클릭하여 네트워크 편집 창을 열고 논리 네트워크를 편집합니다.

논리 네트워크 정의가 호스트 상의 네트워크 설정과 동기화되어 있지 않을 경우 네트워크 동기화 확인란을 선택합니다.

다음에서 부팅 프로토콜을 선택합니다:

- o None

- **None,**
- **DHCP,**
- **Static,**

IP와 서브넷 마스크를 입력합니다.

OK를 클릭합니다.

6. **호스트와 Engine간의 연결을 확인** 확인란을 선택하여 네트워크를 확인합니다. 이러한 동작은 호스트가 유지 관리 모드일 경우에만 작동합니다.
7. **네트워크 설정 저장** 확인란을 선택합니다.
8. **OK**를 클릭합니다.

클러스터에 있는 각 호스트의 NIC를 편집하여 클러스터에 있는 각 호스트에 논리 네트워크를 추가합니다. 이 작업을 완료한 후 네트워크가 작동됩니다.

하나의 인터페이스에 여러 VLAN 태그된 논리 네트워크를 추가했습니다. 단일 네트워크 인터페이스에 다른 VLAN 태그로 논리 네트워크를 추가하기 위해 각 호스트 마다 동일한 네트워크 인터페이스를 선택 및 편집하는 절차를 여러 번 반복할 수 있습니다.

6.5.4. 호스트 네트워크에 추가 IPv4 주소 할당

ovirtmgmt 관리 네트워크 등의 호스트 네트워크는 초기 설정 시 하나의 IP 주소만 사용하여 생성됩니다. 따라서 NIC의 설정 파일(예: **/etc/sysconfig/network-scripts/ifcfg-eth01**)이 여러 IP 주소로 설정된 경우 첫 번째 나열된 IP 주소만 호스트 네트워크에 할당됩니다. 스토리지에 연결하는 경우 또는 동일한 NIC를 사용하여 별도의 개별 하위 넷에서 서버에 연결하는 경우 추가 IP 주소가 필요할 수 있습니다.

vdsm-hook-extra-ipv4-addrs 후크를 사용하면 호스트 네트워크의 추가 IPv4 주소를 설정할 수 있습니다. 후크에 대한 자세한 내용은 [부록 A. VDSM 및 후크](#)를 참조하십시오.

다음 절차에서는 추가 IP 주소를 설정하려는 각 호스트에 호스트 특정 작업을 수행해야 합니다.

절차 6.22. 호스트 네트워크에 추가 IPv4 주소 할당

1. 추가 IPv4 주소를 설정하려는 호스트에서 **VDSM** 후크 패키지를 설치합니다. Red Hat Virtualization 호스트에서는 해당 패키지가 기본적으로 사용 가능하지만 Red Hat Enterprise Linux 호스트에서는 설치해야 합니다.

```
# yum install vsdm-hook-extra-ipv4-addr
```

2. Manager에서 키를 추가하기 위해 다음의 명령을 실행합니다:

```
# engine-config -s
'UserDefinedNetworkCustomProperties=ipv4_addr=.*'
```

3. **ovirt-engine** 서비스를 다시 시작합니다.

```
# systemctl restart ovirt-engine.service
```

4. 관리 포털에서 **호스트 리소스** 탭을 클릭한 다음 **추가 IP** 주소를 설정해야 하는 호스트를 선택합니다.
5. 세부 정보 창에서 **네트워크 인터페이스** 탭을 클릭하고 **호스트 네트워크 설정** 버튼을 클릭하여 **호스트 네트워크 설정** 창을 엽니다.
6. 할당된 논리 네트워크 위에 커서를 이동하고 연필 모양의 아이콘을 클릭하여 **관리 네트워크 편집** 창을 열고 호스트 네트워크 인터페이스를 편집합니다.
7. 사용자 정의 속성 드롭 다운 목록에서 **ipv4_addr**을 선택하고 추가 IP 주소 및 접두사(예: 5.5.5.5/24)를 추가합니다. 여러 IP 주소는 쉼표로 구분해야 합니다.
8. **OK**를 클릭합니다.
9. **네트워크 설정 저장** 확인란을 선택합니다.
10. **OK**를 클릭합니다.

추가 IP 주소는 Manager에 표시되지 않지만 호스트에서 **ip addr show** 명령을 실행하여 추가되었는지 확인할 수 있습니다.

6.5.5. 네트워크 레이블을 호스트 네트워크 인터페이스에 추가

네트워크 레이블을 사용하여 호스트 네트워크 인터페이스에 논리 네트워크 할당에 관련된 관리 작업을 간소화할 수 있습니다.

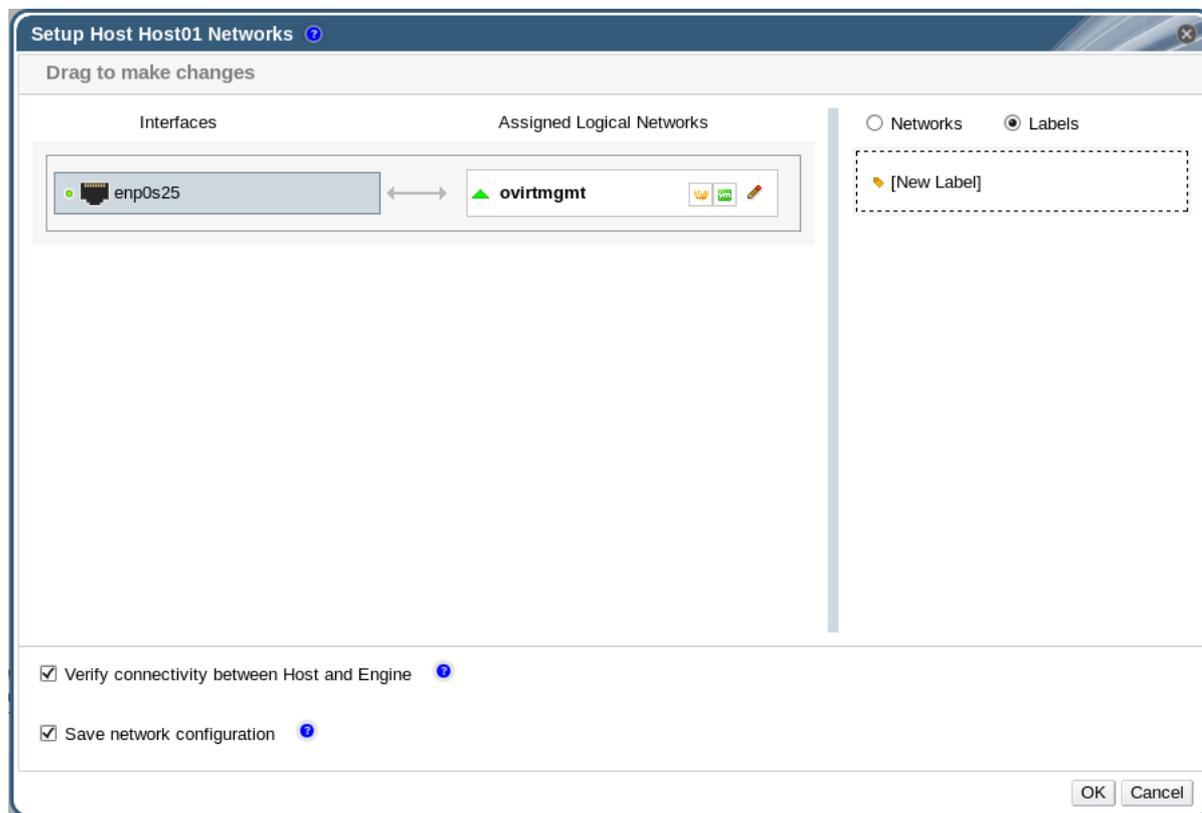


참고

역할 네트워크(예: 마이그레이션 네트워크 또는 디스플레이 네트워크)에서 레이블을 설정하면 모든 호스트에서 해당 네트워크가 대량으로 배포됩니다. 네트워크의 이러한 대량 추가는 DHCP를 사용하여 수행됩니다. 많은 고정 IP 주소를 입력하는 작업 시 확장이 불가능하므로 고정 IP 주소를 입력하는 방식에 이러한 방식의 대량 배포가 선택되었습니다.

절차 6.23. 네트워크 레이블을 호스트 네트워크 인터페이스에 추가

1. **호스트 리소스** 탭을 클릭하고 결과 목록에서 **VLAN** 태그 논리 네트워크가 할당된 클러스터에 연결된 호스트를 선택합니다.
2. 상세 정보 창에서 **네트워크 인터페이스** 탭을 클릭하여 데이터 센터에 연결된 실제 네트워크 인터페이스를 나열합니다.
3. **호스트 네트워크 설정**을 클릭하여 **호스트 네트워크 설정** 창을 엽니다.
4. **레이블**을 클릭하고 **[새 레이블]**을 오른쪽 클릭합니다. 레이블할 실제 네트워크 인터페이스를 선택합니다.



5. 레이블 텍스트 필드에서 네트워크 레이블 이름을 입력합니다.

6. **OK**를 클릭합니다.

호스트 네트워크 인터페이스에 네트워크 레이블이 추가되었습니다. 동일한 레이블이 붙은 새로 생성된 논리 네트워크는 자동으로 해당 레이블의 모든 호스트 네트워크 인터페이스에 자동으로 할당됩니다. 또한 논리 네트워크에서 레이블을 삭제하면 해당 레이블이 붙은 모든 호스트 네트워크 인터페이스에서 논리 네트워크가 자동으로 삭제됩니다.

6.5.6. 본딩

6.5.6.1. Red Hat Virtualization에서 본딩 로직

Red Hat Virtualization Manager 관리 포털에서는 그래픽 인터페이스를 사용하여 본딩 장치를 생성할 수 있습니다. 몇 가지 본딩 생성 시나리오가 있으며 각 시나리오에는 고유한 논리가 적용됩니다.

본딩 로직에 영향을 미치는 두 가지 요소는 다음과 같습니다:

- 장치 중 하나가 이미 논리 네트워크를 전송하고 있습니까?
- 장치가 호환 가능한 논리 네트워크를 전송하고 있습니까?

표 6.7. 본딩 시나리오 및 결과

본딩 시나리오	결과
---------	----

본딩 시나리오	결과
NIC + NIC	<p>새로운 본딩 생성 창이 나타나면 새로운 본딩 장치를 설정할 수 있습니다.</p> <p>네트워크 인터페이스가 호환되지 않는 논리 네트워크를 전송하는 경우 새로운 본딩을 구성한 장치에서 호환되지 않는 논리 네트워크를 분리할 때까지 본딩 작업은 실패합니다.</p>
NIC + Bond	<p>NIC가 본딩 장치에 추가됩니다. NIC 및 본딩에 의해 전송된 논리 네트워크는 호환 가능한 경우 모두 본딩 장치에 추가됩니다.</p> <p>네트워크 인터페이스가 호환되지 않는 논리 네트워크를 전송하는 경우 새 본딩을 구성한 장치에서 호환되지 않는 논리 네트워크를 분리할 때 까지 본딩 작업은 실패합니다.</p>
Bond + Bond	<p>본딩 장치가 논리 네트워크에 연결되어 있지 않거나 호환 가능한 논리 네트워크에 연결되어 있을 경우 새 본딩 장치가 생성됩니다. 이에 모든 네트워크 인터페이스가 포함되며 본딩 구성 장치의 모든 논리 네트워크를 전송합니다. 새로운 본딩 생성 창이 표시되어 새 본딩을 설정할 수 있습니다.</p> <p>네트워크 인터페이스가 호환되지 않는 논리 네트워크를 전송하는 경우 새 본딩을 구성한 장치에서 호환되지 않는 논리 네트워크를 분리할 때 까지 본딩 작업은 실패합니다.</p>

6.5.6.2. 본딩

본딩은 여러 네트워크 인터페이스 카드를 단일 소프트웨어 장치로 정의하는 것입니다. 본딩된 네트워크 인터페이스는 본딩에 포함된 네트워크 인터페이스 카드의 전송 기능을 결합하여 단일 네트워크 인터페이스로 동작하기 때문에 단일 네트워크 인터페이스 카드 보다 더 신속한 전송 속도 기능을 제공합니다. 본딩에 있는 모든 네트워크 인터페이스 카드에 오류가 발생하지 않으면 본딩 자체에 오류가 발생하지 않기 때문에 본딩의 내결함성을 증가시킬 수 있습니다. 하지만 본딩된 네트워크 인터페이스를 구성하는 네트워크 인터페이스 카드는 본딩에서 동일한 옵션 및 모드를 지원하도록 동일한 제조업체 및 모델이어야 한다는 제한이 있습니다.

본딩의 패킷 분산 알고리즘은 사용하는 본딩 모드에 의해 결정됩니다.



중요

모드 1, 2, 3, 4는 가상 머신 (브릿지됨) 및 비 가상 머신 (브릿지되지 않음) 네트워크 유형 모두를 지원합니다. 모드 0, 5, 6은 비 가상 머신 (브릿지되지 않음) 네트워크만 지원합니다.

본딩 모드

Red Hat Virtualization은 기본적으로 모드 4를 사용하지만 다음과 같은 일반적인 본딩 모드를 지원합니다:

모드 0 (round-robin 정책)

네트워크 인터페이스 카드를 통해 순차적으로 패킷을 전송합니다. 패킷은 본딩에서 처음 사용 가능한 네트워크 인터페이스 카드로 시작하여 마지막으로 사용 가능한 네트워크 인터페이스 카드로 종료하는

루프에 전송됩니다. 이후의 모든 루프는 처음 사용 가능한 네트워크 인터페이스 카드에서 시작됩니다. 모드 0는 내결함성을 제공하고 본딩의 모든 네트워크 인터페이스 카드에서 부하 균형을 조정합니다. 하지만 모드 0는 브릿지와 함께 사용할 수 없으므로 가상 머신 논리 네트워크와 호환되지 않습니다.

모드 1 (active-backup 정책)

하나의 네트워크 인터페이스 카드는 활성 상태로 두고 다른 모든 네트워크 인터페이스 카드를 백업 상태로 설정합니다. 활성 네트워크 인터페이스 카드에 오류가 발생하는 경우 백업 네트워크 인터페이스 카드 중 하나가 본딩에서 활성 네트워크 인터페이스 카드로 네트워크 인터페이스 카드를 대체합니다. 모드 1에서 본딩의 MAC 주소가 활성 네트워크 인터페이스 카드를 반영하도록 변경될 경우 발생할 수 있는 혼란을 방지하기 위해 MAC 주소는 하나의 포트에만 표시됩니다. 모드 1은 내결함성을 제공하고 Red Hat Virtualization에서 지원됩니다.

모드 2 (XOR 정책)

소스에서 XOR 연산 결과 및 대상 MAC 주소 모듈 네트워크 인터페이스 카드 슬레이브 수에 따라 패킷을 전송할 네트워크 인터페이스 카드를 선택합니다. 이러한 계산을 통해 각각의 대상 MAC 주소에 동일한 네트워크 인터페이스 카드가 선택됩니다. 모드 2는 내결함성 및 부하 분산을 제공하고 Red Hat Virtualization에서 지원됩니다.

모드 3 (broadcast 정책)

모든 네트워크 인터페이스 카드에 모든 패킷을 전송합니다. 모드 3은 내결함성을 제공하고 Red Hat Virtualization에서 지원됩니다.

모드 4 (IEEE 802.3ad 정책)

인터페이스가 동일한 속도 및 이중 설정을 공유하는 집계 그룹을 생성합니다. 모드 4는 IEEE 802.3ad 사양에 따라 활성 집계 그룹에 있는 모든 네트워크 인터페이스 카드를 사용하며 Red Hat Virtualization에서 지원됩니다.

모드 5 (adaptive transmit load balancing 정책)

본딩의 각 네트워크 인터페이스 카드에서 부하에 따라 발신 트래픽 계정이 분산되어 현재 네트워크 인터페이스 카드가 모든 들어오는 트래픽을 수신할 수 있게 합니다. 수신 트래픽에 할당된 네트워크 인터페이스 카드에 오류가 발생할 경우 다른 네트워크 인터페이스 카드가 수신 트래픽의 역할을 하도록 지정됩니다. 모드 5는 브리지와 함께 사용할 수 없으므로 가상 머신 논리 네트워크와 호환되지 않습니다.

모드 6 (adaptive load balancing 정책)

특별한 전환 요구 사항없이 모드 5 (adaptive transmit load balancing 정책)는 IPv4 트래픽의 수신 부하 분산과 결합되어 있습니다. ARP 협상은 수신 부하 분산에 사용됩니다. 모드 6은 브리지와 함께 사용할 수 없으므로 가상 머신 논리 네트워크와 호환되지 않습니다.

6.5.6.3. 관리 포털에서 본딩 장치 생성

여러 호환 가능한 네트워크 장치를 결합하여 구성할 수 있습니다. 이러한 설정 유형을 통해 대역폭과 안정성을 증가시킬 수 있습니다. 여러 네트워크 인터페이스, 기존의 본딩 장치 또는 이 둘을 조합하여 구성할 수 있습니다. 본딩은 VLAN 태그 및 비 VLAN 트래픽을 모두 전송할 수 있습니다.

절차 6.24. 관리 포털에서 본딩 장치 생성

1. 호스트 리소스 탭을 클릭하여 결과 목록에서 호스트를 선택합니다.
2. 상세 정보 창에서 **네트워크 인터페이스** 탭을 클릭하여 호스트에 연결된 실제 네트워크 인터페이스를 나열합니다.

3. **호스트 네트워크 설정**을 클릭하여 **호스트 네트워크 설정** 창을 엽니다.
4. 한 장치를 선택하고 다른 장치에 드래그하여 드롭하면 **새로운 본딩 생성** 창이 열립니다. 다른 방법으로 장치 위에 마우스를 두고 오른쪽을 클릭한 후 드롭 다운 메뉴에서 다른 장치를 선택합니다.

장치가 호환되지 않는 경우 본딩 작업이 실패하며 호환 문제를 해결하는 방법을 알려주는 메시지가 나타납니다.
5. 드롭 다운 메뉴에서 **본딩 이름** 및 **본딩 모드**를 선택합니다.

본딩 모드 1, 2, 4, 5를 선택할 수 있습니다. 기타 다른 모드는 **사용자 정의** 옵션을 사용하여 설정할 수 있습니다.
6. **OK**를 클릭하여 본딩을 생성하고 **새로운 본딩 생성** 창을 닫습니다.
7. 새로 생성된 본딩 장치에 논리 네트워크를 지정합니다.
8. 옵션으로 **호스트와 Engine 간의 연결을 확인**을 선택하고 **네트워크 설정 저장**을 선택합니다.
9. **OK**를 클릭하여 변경 사항을 저장하고 **호스트 네트워크 설정** 창을 닫습니다.

네트워크 장치는 본딩 장치에 연결되어 단일 인터페이스로 편집할 수 있습니다. 본딩 장치는 선택한 호스트의 상세 정보 창에 있는 **네트워크 인터페이스** 탭에 나열됩니다.

호스트가 사용하는 스위치 포트에 본딩을 활성화해야 합니다. 본딩을 활성화하는 프로세스는 스위치마다 조금씩 다릅니다. 본딩을 활성화하는 방법에 대한 상세 정보는 스위치 벤더에서 제공하는 설명서에서 참조하십시오.



참고

모드 4 본딩의 경우 모든 슬레이브를 스위치에서 적절히 설정해야 합니다. 스위치에 적절히 설정되지 않은 경우 **ad_partner_mac**이 00:00:00:00:00:00으로 보고됩니다. **Manager**는 **네트워크 인터페이스** 탭에서 본딩에 느낌표 표시 아이콘 형태로 경고를 표시합니다. 슬레이브가 실행 중인 경우 경고가 제공되지 않습니다.

6.5.6.4. 호스트 인터페이스의 사용자 정의 본딩 옵션 사용 예

새로운 본딩 생성 창의 **본딩 모드**에서 **사용자 정의**를 선택하여 사용자 정의 본딩 장치를 생성할 수 있습니다. 필요에 따라 다음의 예를 선별하여 사용합니다. 본딩 옵션 및 전체 설명 목록은 Kernel.org에 있는 [Linux Ethernet Bonding Driver HOWTO](#)에서 참조하십시오.

예 6.1. xmit_hash_policy

이 옵션은 본딩 모드 2와 4의 로드 밸런싱 전송 정책을 정의합니다. 예를 들어 대부분의 트래픽이 여러 다른 IP 주소 사이에 있을 경우 IP 주소 별로 로드 밸런싱 정책을 설정할 수 있습니다. **사용자 정의** 본딩 모드를 선택하고 텍스트 필드에 다음과 같은 값을 입력하여 로드 밸런싱 정책을 설정할 수 있습니다.

```
mode=4 xmit_hash_policy=layer2+3
```

예 6.2. ARP 모니터링

ARP 모니터는 `ethtool`을 통해 적절히 연결 상태를 보고할 수 없는 시스템에 유용합니다. 사용자 정의 본딩 모드를 선택하고 텍스트 필드에 다음과 같은 값을 입력하여 호스트의 본딩 장치에 `arp_interval`을 설정합니다:

```
mode=1 arp_interval=1 arp_ip_target=192.168.0.2
```

예 6.3. 기본

본딩 장치에서 기본 인터페이스로 높은 처리량을 갖는 NIC를 지정하고자 할 수 있습니다. 사용자 정의 본딩 모드를 선택하고 텍스트 필드에 다음과 같은 값을 입력하여 기본 NIC를 지정합니다:

```
mode=1 primary=eth0
```

6.5.7. 호스트의 FQDN 변경

다음 절차에 따라 호스트의 FQDN을 변경합니다.

절차 6.25. 호스트의 FQDN 업데이트

1. 가상 머신이 다른 호스트로 라이브 마이그레이션되도록 호스트를 유지관리 모드로 전환합니다. 자세한 내용은 [7.5.7절. “호스트를 유지 관리 모드로 변경”](#)을 참조하십시오. 또는 모든 가상 머신을 수동으로 종료하거나 다른 호스트로 마이그레이션합니다. 자세한 내용은 [가상 머신 관리 가이드](#)에 있는 [수동으로 가상 머신 마이그레이션](#)을 참조하십시오.
2. 삭제를 클릭하고 **OK**를 클릭하여 관리 포털에서 호스트를 삭제합니다.
3. `hostnamectl` 도구를 사용하여 호스트 이름을 업데이트합니다. 보다 자세한 옵션은 *Red Hat Enterprise Linux 7 네트워킹 가이드*의 [호스트 이름 설정](#)에서 참조하십시오.

```
# hostnamectl set-hostname NEW_FQDN
```

4. 호스트를 재부팅합니다.
5. Manager로 호스트를 다시 등록합니다. 보다 자세한 내용은 [7.5.1절. “Red Hat Virtualization Manager에 대한 Host 추가”](#)에서 참조하십시오.

6.5.8. 호스트의 IP 주소 변경

절차 6.26.

1. 가상 머신이 다른 호스트로 라이브 마이그레이션되도록 호스트를 유지관리 모드로 전환합니다. 자세한 내용은 [7.5.7절. “호스트를 유지 관리 모드로 변경”](#)을 참조하십시오. 또는 모든 가상 머신을 수동으로 종료하거나 다른 호스트로 마이그레이션합니다. 자세한 내용은 [가상 머신 관리 가이드](#)에 있는 [수동으로 가상 머신 마이그레이션](#)을 참조하십시오.
2. 삭제를 클릭하고 **OK**를 클릭하여 관리 포털에서 호스트를 삭제합니다.
3. `admin` 사용자로 호스트에 로그인합니다.
4. **F2**를 누르고 **OK**를 선택한 후 **Enter**를 눌러 복구 셸로 들어갑니다.

5. `/etc/sysconfig/network-scripts/ifcfg-ovirtmgmt` 파일을 편집하여 IP 주소를 수정합니다. 예:

```
# vi /etc/sysconfig/network-scripts/ifcfg-ovirtmgmt
...
BOOTPROTO=none
IPADDR=10.x.x.x
PREFIX=24
...
```

6. 네트워크 서비스를 다시 시작하고 IP 주소가 업데이트되었는지 확인합니다.

```
# systemctl restart network.service
```

```
# ip addr show ovirtmgmt
```

7. **exit**을 입력하여 복구 셸에서 나간 후 텍스트 사용자 인터페이스로 전환합니다.
8. Manager로 호스트를 다시 등록합니다. 보다 자세한 내용은 [7.5.1절. “Red Hat Virtualization Manager에 대한 Host 추가”](#)에서 참조하십시오.

7장. 호스트

7.1. 호스트 소개

하이퍼바이저로 알려진 호스트는 가상 머신을 실행하는 물리적 서버입니다. KVM(Kernel-based Virtual Machine)이라는 로딩 가능한 Linux 커널 모듈을 사용하여 완전 가상화가 제공됩니다.

KVM은 Windows 또는 Linux 운영 체제에서 실행되는 여러 가상 머신을 동시에 호스팅할 수 있습니다. 가상 머신은 호스트 시스템에서 개별 Linux 프로세스 및 스레드로 실행되며 Red Hat Virtualization Manager에 의해 원격으로 관리됩니다. Red Hat Virtualization 환경에는 하나 이상의 여러 호스트를 연결할 수 있습니다.

Red Hat Virtualization은 호스트 설치에 있어서 두 가지 방식을 지원합니다. Red Hat Virtualization Host (RHVH) 설치 미디어를 사용하거나 표준 Red Hat Enterprise Linux 설치에 하이퍼바이저 패키지를 설치합니다.



참고

Red Hat Virtualization Manager 내 개별 호스트의 유형을 확인하려면 해당 호스트를 선택하고 상세 정보 창의 일반 탭에서 소프트웨어를 클릭해서 OS 정보를 확인합니다.

호스트는 **tuned** 프로파일을 사용하여 가상화를 최적화합니다. **tuned**에 대한 보다 자세한 내용은 [Red Hat Enterprise Linux 7 성능 조정 가이드](#)에서 참조하십시오.

Red Hat Virtualization Host에는 보안 기능이 활성화되어 있습니다. SELinux (Security Enhanced Linux) 및 iptables 방화벽은 기본값으로 완전 설정되어 활성화되어 있습니다. 선택한 호스트에서 SELinux 상태는 상태 정보 창의 일반 탭에 있는 **SELinux** 모드에 표시됩니다. Manager는 Red Hat Enterprise Linux 호스트를 환경에 추가할 때 이러한 호스트에서 필요한 포트를 열 수 있습니다.

호스트는 Red Hat Enterprise Linux 7 AMD64/Intel 64 버전을 실행하는 Intel VT 또는 AMD-V 확장 기능을 갖는 64 비트 물리적 서버입니다.

Red Hat Virtualization 플랫폼에서 물리적 호스트의 요구 사항은 다음과 같습니다:

- 시스템에 있는 하나의 클러스터에만 속해 있어야 합니다.
- AMD-V 또는 Intel VT 하드웨어 가상화 확장 기능을 지원하는 CPU가 있어야 합니다.
- 클러스터 생성 시 선택한 가상 CPU 유형으로 공개된 모든 기능을 지원하는 CPU가 있어야 합니다.
- 최소 2 GB RAM이 있어야 합니다.
- 시스템 권한이 있는 시스템 관리자를 지정해야 합니다.

관리자는 Red Hat Virtualization 위치 리스트에서 최신 보안 권고를 받을 수 있습니다. Red Hat Virtualization 제품에 대한 새로운 보안 권고를 이메일로 수신하려면 다음의 양식을 작성하여 Red Hat Virtualization 위치 리스트에 등록해야 합니다:

<http://www.redhat.com/mailman/listinfo/rhev-watch-list/>

7.2. RED HAT VIRTUALIZATION HOST

Red Hat Virtualization Host(RHVH)는 호스트 가상 머신에 필요한 패키지만 포함된 Red Hat

Enterprise Linux의 특수 빌드를 사용하여 설치됩니다. Red Hat Enterprise Linux 호스트에서 사용하는 항목을 기반으로 **Anaconda** 설치 인터페이스를 사용하며 Red Hat Virtualization Manager 또는 **yum**을 통해 업데이트할 수 있습니다. 추가 패키지를 설치하고 업그레이드 후에도 유지되도록 하려면 **yum** 명령을 사용해야 합니다.

RHVH에는 호스트 리소스 모니터링 및 관리 작업을 위한 **Cockpit** 사용자 인터페이스가 있습니다. SSH 또는 콘솔을 통해 RHVH에 직접 연결하는 것은 지원되지 않기 때문에 **Cockpit** 사용자 인터페이스는 네트워킹 설정과 셸프 호스트 엔진 배포 등 호스트가 Red Hat Virtualization Manager에 추가되기 전에 수행되는 작업을 위한 그래픽 사용자 인터페이스를 제공하며 **도구 > 터미널** 하위 탭을 사용해서 터미널 명령을 실행하는 데 사용될 수도 있습니다.

웹 브라우저의 <https://HostFQDNorIP:9090> 에서 **Cockpit** 사용자 인터페이스에 액세스합니다. RHVH의 **Cockpit**에는 호스트의 상태, SSH 호스트 키, 셸프 호스트 엔진 상태, 가상 머신, 그리고 가상 머신 통계를 보여주는 사용자 설정 **Virtualization** 대시보드가 있습니다.



참고

grubby 도구를 사용하여 사용자 설정 커널 인수를 Red Hat Virtualization Host에 추가할 수 있습니다. **grubby** 도구는 **grub.cfg** 파일의 변경 사항을 영구적으로 적용합니다. 호스트의 **Cockpit** 사용자 인터페이스의 **도구 > 터미널** 하위 탭으로 가서 **grubby** 명령을 사용합니다. 보다 자세한 내용은 [Red Hat Enterprise Linux 시스템 관리자 가이드](#)에서 참조하십시오.



주의

로컬 보안 취약점을 악용할 수 있으므로 RHVH에 신뢰할 수 없는 사용자를 만들지 않는 것이 좋습니다.

7.3. RED HAT ENTERPRISE LINUX 호스트

사용 가능한 하드웨어에 Red Hat Enterprise Linux 7을 설치하여 호스트로 사용할 수 있습니다. Red Hat Virtualization은 Intel VT 또는 AMD-V 확장 기능이 있는 Red Hat Enterprise Linux 7 Server AMD64/Intel 64 버전을 실행하는 호스트를 지원합니다. 호스트로 Red Hat Enterprise Linux 시스템을 사용하려면 **Red Hat Enterprise Linux Server** 인타이틀먼트 및 **Red Hat Virtualization** 인타이틀먼트에 연결해야 합니다.

호스트를 추가하는데 플랫폼에서 가상화 확인, 패키지 설치, 브릿지 생성, 호스트 재부팅과 같은 작업을 완료해야 하므로 시간이 소요될 수 있습니다. 상세 정보 창에서 호스트 및 관리 시스템을 연결하기 위한 프로세스를 모니터링할 수 있습니다.



중요

타사 감시 장치는 VDSM의 감시 장치 데몬과 충돌할 수도 있으므로 Red Hat Enterprise Linux 호스트에 타사 감시 장치가 설치되어 있지 않아야 합니다.

7.4. SATELLITE 호스트 공급자 호스트

Satellite 호스트 공급자가 제공하는 호스트는 Red Hat Virtualization Manager에 의해 가상 호스트로 사용될 수 있습니다. Satellite 호스트 공급자가 외부 공급자로 Manager에 추가된 후 호스트 공급자가

제공하는 모든 호스트는 Red Hat Virtualization에 추가하여 Red Hat Virtualization Host (RHVH) 및 Red Hat Enterprise Linux 호스트와 동일한 방식으로 사용할 수 있습니다.

7.5. 호스트 작업

7.5.1. Red Hat Virtualization Manager에 대한 Host 추가

사용자의 Red Hat Virtualization 환경에 호스트를 추가하려면 플랫폼을 통해 가상화 확인, 패키지 설치, 브리지 생성, 그리고 호스트 재부팅 등의 단계를 거쳐야 하므로 시간이 소요될 수 있습니다. 상세 정보 창을 사용해서 호스트와 Manager의 연결 과정을 모니터링합니다.

절차 7.1. Red Hat Virtualization Manager에 대한 Host 추가

1. 관리 포털에서 호스트 리소스 탭을 클릭합니다.
2. 새로 만들기를 클릭합니다.
3. 드롭 다운 목록을 사용하여 새 호스트의 데이터 센터 및 호스트 클러스터를 선택합니다.
4. 새 호스트의 이름과 주소를 입력합니다. SSH 포트란에 표준 SSH 포트인 포트 22가 자동으로 채워집니다.
5. Manager가 호스트에 액세스 시 인증방법을 선택합니다.
 - 인증 암호를 사용하기 위해 root 사용자 암호를 입력합니다.
 - 또는, SSH 공개키 필드에 표시된 키를 호스트에 있는 `/root/.ssh/authorized_keys`에 복사하여 공개키 인증에 사용합니다.
6. 고급 매개 변수 버튼을 클릭해서 고급 호스트 설정을 표시합니다.
 - a. 옵션으로 자동 방화벽 설정을 비활성화합니다.
 - b. 옵션으로 보안을 강화하기 위해 호스트 SSH 지문을 추가합니다. 이를 수동으로 추가하거나 자동으로 가져오기할 수 있습니다.
7. 옵션에서 전원 관리, SPM, 콘솔, 네트워크 공급자 및 커널을 설정합니다. 자세한 내용은 [7.5.4 절. "새 호스트 및 호스트 편집 창 설정 및 제어"](#)을 참조하십시오. 셀프 호스트 엔진 배포를 위해 호스트를 배포하거나 배포 취소하는 경우 호스트 엔진이 사용됩니다.
8. OK를 클릭합니다.

새 호스트는 **Installing** 상태로 호스트 목록에 표시되고 상세 정보 창에서 설치 진행 상태를 확인할 수 있습니다. 잠시 후 호스트 상태가 **Up**으로 변경됩니다.

7.5.2. Satellite 호스트 공급자 호스트 추가

Satellite 호스트 공급자 호스트를 추가하는 절차는 Manager에서 호스트를 구별하는 방법을 제외하고 Red Hat Enterprise Linux 호스트를 추가하는 방법과 거의 동일합니다. 다음 부분에서는 Satellite 호스트 공급자가 제공하는 호스트를 추가하는 방법에 대해 설명합니다.

절차 7.2. Satellite 호스트 공급자 호스트 추가

1. 호스트 리소스 탭을 클릭하여 결과 목록에 호스트를 나열합니다.

2. 새로 만들기를 클릭하여 새 호스트 창을 엽니다.
3. 드롭 다운 메뉴를 사용하여 새 호스트의 호스트 클러스터를 선택합니다.
4. **Foreman/Satellite** 확인란을 선택하여 **Satellite** 호스트 공급자 호스트를 추가하기 위한 옵션을 표시하고 호스트를 추가할 공급자를 선택합니다.
5. 검색된 호스트 또는 프로비저닝된 호스트를 선택합니다.
 - 검색된 호스트 (기본 옵션): 드롭 다운 메뉴에서 호스트, 호스트 그룹, 컴퓨터 리소스를 선택합니다.
 - 프로비저닝된 호스트: 공급자 호스트 드롭 다운 메뉴에서 호스트를 선택합니다.

외부 공급자에서 검색할 수 있는 호스트에 관한 모든 세부 사항은 자동으로 설정되어 원하는 대로 편집할 수 있습니다.
6. 새 호스트의 이름, 주소, **SSH** 포트 (프로비저닝된 호스트만)를 입력합니다.
7. 호스트에 사용할 인증 방식을 선택합니다.
 - 인증 암호를 사용하기 위해 **root** 사용자 암호를 입력합니다.
 - **SSH** 공개키 필드에 표시된 키를 호스트에 있는 **/root/.ssh/authorized_hosts**에 복사하여 공개키 인증에 사용합니다 (프로비저닝된 호스트만 해당).
8. **Red Hat Enterprise Linux** 호스트를 추가하기 위한 필수 단계를 완료했습니다. **고급 매개 변수** 드롭 다운 메뉴 버튼을 클릭하여 고급 호스트 설정을 표시합니다.
 - a. 옵션으로 자동 방화벽 설정을 비활성화합니다.
 - b. 옵션으로 보안을 강화하기 위해 호스트 **SSH** 지문을 추가합니다. 이를 수동으로 추가하거나 자동으로 가져오기할 수 있습니다.
9. 해당 탭을 통해 전원 관리, **SPM**, 콘솔, 네트워크 공급자를 설정할 수 있습니다. 하지만 이러한 설정은 **Red Hat Enterprise Linux** 호스트를 추가하는데 필요하지 않기 때문에 이 부분에서는 설명하지 않습니다.
10. **OK**를 클릭하여 호스트를 추가하고 창을 닫습니다.

새 호스트는 **Installing** 상태로 호스트 목록에 표시되고 상세 정보 창에서 설치 진행 상태를 확인할 수 있습니다. 설치 완료 후 상태는 **Reboot**가 됩니다. 상태를 **Up**으로 변경하기 위해 호스트를 활성화해야 합니다.

7.5.3. 호스트에 대한 **Satellite** 에라타 관리 설정

Red Hat Virtualization 설정 시 **Red Hat Satellite**에서 에라타를 표시하도록 설정할 수 있습니다. 이를 통해 호스트 관리자는 호스트 설정 관리에 사용하는 것과 동일한 대시보드에서 사용 가능한 에라타 업데이트와 그 중요성에 대한 정보를 받을 수 있습니다. **Red Hat Satellite**에 대한 보다 자세한 내용은 [Red Hat Satellite 사용자 가이드](#)에서 참조하십시오.

Red Hat Virtualization 4.1은 **Red Hat Satellite 6.1**을 사용한 에라타 관리를 지원합니다.

 **중요**

Satellite 서버에서 호스트를 FQDN로 식별합니다. IP 주소를 사용해서 추가된 호스트는 에라타 보고를 할 수 없습니다. 이를 통해 외부 컨텐츠 호스트 ID가 Red Hat Virtualization에서 유지되지 않아도 됩니다.

호스트 관리에 사용되는 Satellite 계정은 관리자 권한이 있고 기본 조직이 설정되어야 합니다.

절차 7.3. 호스트에 대한 Satellite 에라타 관리 설정

1. Satellite 서버를 외부 공급자로 추가합니다. 보다 자세한 내용은 [12.2.1절. “호스트 프로비저닝을 위한 Red Hat Satellite 인스턴스 추가”](#)에서 참조하십시오.
2. 필요한 호스트를 Satellite 서버에 연결합니다.

 **참고**

호스트는 해당 Satellite 서버에 등록되어 있고 katello-agent 패키지가 설치되어 있어야 합니다.

호스트 등록 설정 방법에 대한 보다 자세한 내용은 *Red Hat Satellite User Guide*에 있는 [Configuring a Host for Registration](#)에서 참조하고 호스트 등록 및 katello-agent 패키지 설치에 대한 보다 자세한 내용은 *Red Hat Satellite User Guide*에 있는 [Registration](#)에서 참조하시기 바랍니다.

- a. 호스트 탭에서 결과 목록에 있는 호스트를 선택합니다.
- b. 편집을 클릭하여 호스트 편집 창을 엽니다.
- c. Check the **Foreman/Satellite** 사용 체크 상자를 선택합니다.
- d. 드롭 다운 목록에서 원하는 Satellite 서버를 선택합니다.
- e. **OK**를 클릭합니다.

사용 가능한 에라타와 그 중요성에 대한 정보가 호스트 설정을 관리하는 대시보드에서 표시되도록 호스트가 설정되었습니다.

7.5.4. 새 호스트 및 호스트 편집 창 설정 및 제어**7.5.4.1. 호스트 일반 설정**

호스트 상세 정보를 수정하거나 새 Red Hat Enterprise Linux 호스트 및 Satellite 호스트 공급자 호스트를 추가할 때 다음 설정을 적용합니다.

일반 설정 탭에는 새 호스트 또는 호스트 편집 창의 일반 탭에 필요한 정보가 있습니다.

표 7.1. 일반 설정

필드 이름	설명
-------	----

필드 이름	설명
데이터 센터	호스트가 속한 데이터 센터입니다. Red Hat Virtualization Host(RHVH)는 Gluster-활성 클러스터에 추가할 수 없습니다.
호스트 클러스터	호스트가 속한 클러스터입니다.
Foreman/Satellite 사용	<p>이 확인란을 선택 또는 선택 해제하여 Satellite 호스트 공급자가 제공하는 호스트를 추가하기 위한 옵션을 표시 또는 숨기기합니다. 다음과 같은 옵션도 사용 가능합니다:</p> <p>검색된 호스트</p> <ul style="list-style-type: none"> • 검색된 호스트 - engine에 의해 검색된 Satellite 호스트의 이름으로 표시된 그룹 다운 목록입니다. • 호스트 그룹 -사용 가능한 호스트 그룹이 있는 그룹 다운 목록입니다. • 컴퓨터 리소스 - 컴퓨터 리소스를 제공하기 위한 하이퍼바이저의 그룹다운 목록입니다. <p>프로비저닝된 호스트</p> <ul style="list-style-type: none"> • 공급자 호스트 - 선택한 외부 공급자에 의해 제공되는 호스트의 이름으로된 그룹 다운 목록입니다. 이 목록에 있는 항목은 공급자 검색 필터에 입력된 검색 쿼리에 따라 필터링됩니다. • 공급자 검색 필터 - 선택한 외부 공급자가 제공하는 호스트를 검색할 수 있는 텍스트 필드입니다. 이 옵션은 공급자 별로 되어 있습니다. 특정 공급자에 대한 검색 쿼리 작성에 대한 자세한 내용은 공급자 설명서를 참조하십시오. 사용 가능한 모든 호스트를 보려면 이 필드를 비워 둡니다.
이름	클러스터 이름입니다. 텍스트 필드는 최대 40 자로 제한되어 있으며 알파벳 대문자, 소문자, 숫자, 하이픈, 밑줄로 조합된 고유한 이름이어야 합니다.
코멘트	호스트 관련 일반 텍스트 형식의 사용자가 읽을 수 있는 코멘트를 추가하기 위한 필드입니다.
주소	IP 주소 또는 확인 가능한 호스트의 호스트 이름입니다.
암호	호스트의 root 사용자 암호입니다. 호스트 추가 시에만 지정할 수 있으며 그 이후에는 편집할 수 없습니다.

필드 이름	설명
SSH 공개키	호스트 인증을 위해 암호를 사용하는 대신 Manager의 SSH 키를 사용하는 경우 호스트에 있는 <code>/root/.known_hosts</code> 파일에 텍스트 상자의 내용을 복사합니다.
호스트 방화벽 자동 설정	새 호스트를 추가 할 때 Manager는 호스트의 방화벽에 필요한 포트를 열 수 있습니다. 이 옵션은 기본적으로 활성화되어 있습니다. 이는 고급 매개 변수 입니다.
SSH 지문	호스트의 SSH 지문을 가져오기 하여 호스트가 반환할 것으로 예상하는 지문과 일치하는지 비교할 수 있습니다. 이는 고급 매개 변수 입니다.

7.5.4.2. 호스트 전원 관리 설정

전원 관리 설정 표에는 새 호스트 또는 호스트 편집 창의 전원 관리 탭에 필요한 정보가 나와 있습니다. 호스트에 지원되는 전원 관리 카드가 있는 경우 전원 관리를 설정할 수 있습니다.

표 7.2. 전원 관리 설정

필드 이름	설명
전원 관리 활성화	호스트에서 전원 관리를 활성화합니다. 이 확인란을 선택하여 전원 관리 탭에 있는 나머지 필드를 활성화합니다.
Kdump 통합	커널 크래시 덤프를 수행하는 동안 호스트가 펜싱되지 않도록 하여 크래시 덤프가 중단되지 않도록 합니다. Red Hat Enterprise Linux 7.1 이상에서 kdump는 기본값으로 사용 가능합니다. 호스트에서 Kdump를 사용할 수 있지만 설정이 유효하지 않은 (kdump 서비스를 시작할 수 없는) 경우 Kdump 통합 을 사용하면 호스트 설치에 실패하게 됩니다. 이러한 경우 7.6.4절. " fence_kdump 고급 설정 "에서 참조하십시오.
전원 관리 정책 제어를 비활성화	전원 관리는 호스트 클러스터의 스케줄링 정책에 의해 제어됩니다. 전원 관리를 활성화하고 지정된 사용량 하한치에 도달한 경우 Manager는 호스트 머신의 전원을 종료하고 부하 분산이 필요하거나 클러스터에 여유 호스트가 충분하지 않을 경우 호스트를 다시 시작합니다. 이 확인란을 선택하여 정책 제어를 비활성화합니다.

필드 이름	설명
순서대로 정렬된 에이전트	<p>호스트의 펜스 에이전트를 나열합니다. 펜스 에이전트는 순차적으로나 동시에 또는 이 두가지를 혼합하여 사용할 수 있습니다.</p> <ul style="list-style-type: none"> • 펜스 에이전트가 순차적으로 사용되는 경우 첫 번째 에이전트를 사용하여 호스트를 정지 또는 시작하며 실패할 경우 두 번째 에이전트가 사용됩니다. • 펜스 에이전트가 동시에 사용되는 경우 두 펜스 에이전트가 중지하려는 호스트의 중지 명령에 응답해야 합니다. 하나의 에이전트가 시작 명령에 응답하면 호스트가 시작됩니다. <p>기본값으로 펜스 에이전트는 순차적으로 사용됩니다. 위, 아래 버튼을 사용하여 사용할 펜스 에이전트 순서를 변경합니다.</p> <p>두 개의 펜스 에이전트를 동시에 사용하려면 다른 펜스 에이전트 옆에 있는 동시 사용 에이전트 드롭 다운 목록에서 하나의 펜스 에이전트를 선택합니다. 추가 펜스 에이전트 옆에 있는 동시 사용 에이전트 드롭 다운 목록에서 그룹을 선택하여 동시에 사용할 펜스 에이전트 그룹에 추가 펜스 에이전트를 추가할 수 있습니다.</p>
펜스 에이전트 추가	<p>플러스 (+) 버튼을 클릭하여 새 펜싱 에이전트를 추가합니다. 펜스 에이전트 편집 창이 열립니다. 다음 표에는 이 창에 있는 필드에 대한 자세한 설명이 있습니다.</p>
전원 관리 프록시 설정	<p>기본값으로 Manager는 호스트와 동일한 cluster 내에 있는 펜싱 프록시를 검색하도록 지정되며 펜싱 프록시가 검색되지 않을 경우 Manager는 동일한 dc (데이터 센터)에서 검색합니다. 위, 아래 버튼을 사용하여 이러한 리소스의 사용 순서를 변경합니다. 이 필드는 고급 매개 변수 아래에 있습니다.</p>

다음 표에는 **펜스 에이전트 편집** 창에 필요한 정보가 있습니다.

표 7.3. 펜스 에이전트 편집 설정

필드 이름	설명
주소	호스트의 전원 관리 장치에 액세스하기 위한 주소입니다. 확인 가능한 호스트 이름 또는 IP 주소입니다.
사용자 이름	전원 관리 장치에 액세스하기 위한 사용자 계정입니다. 장치에 사용자를 설정하거나 기본 사용자를 사용할 수 있습니다.
암호	전원 관리 장치에 액세스하기 위한 사용자 암호입니다.

필드 이름	설명
유형	<p>호스트의 전원 관리 장치 유형입니다.</p> <p>다음 중 하나를 선택합니다:</p> <ul style="list-style-type: none"> • apc - APC MasterSwitch 네트워크 전원 스위치. APC 5.x 전원 스위치 장치에 사용할 수 없습니다. • apc_snmp - APC 5.x 전원 스위치 장치에 사용합니다. • bladecenter - IBM Bladecenter Remote Supervisor Adapter. • cisco_ucs - Cisco Unified Computing System. • drac5 - Dell 컴퓨터 용 Dell Remote Access Controller. • drac7 - Dell 컴퓨터 용 Dell Remote Access Controller. • eps - ePowerSwitch 8M+ 네트워크 전원 스위치. • hpblade - HP BladeSystem. • ilo, ilo2, ilo3, ilo4 - HP Integrated Lights-Out. • ipmilan - Intelligent Platform Management Interface 및 Sun Integrated Lights Out Management 장치. • rsa - IBM Remote Supervisor Adapter. • rsb - Fujitsu-Siemens RSB 관리 인터페이스. • wti - WTI Network Power Switch.
포트	<p>전원 관리 장치가 호스트와의 통신에 사용하는 포트 번호입니다.</p>
슬롯	<p>전원 관리 장치의 블레이드를 구별하기 위해 사용하는 번호입니다.</p>
서비스 프로파일	<p>전원 관리 장치의 블레이드를 구별하기 위해 사용하는 서비스 프로파일 이름입니다. 이 필드는 장치 유형이 cisco_ucs일 때 슬롯 대신 나타납니다.</p>

필드 이름	설명
옵션	전원 관리 장치 관련 옵션입니다. 'key=value'로 입력합니다. 사용 가능한 옵션은 호스트의 전원 관리 장치 관련 문서에서 참조하십시오. Red Hat Enterprise Linux 7 호스트의 경우 전원 관리 장치로 cisco_ucs를 사용하고 있을 경우 옵션 필드에 ssl_insecure=1 을 추가해야 합니다.
보안	이 확인란을 선택하여 전원 관리 장치를 호스트에 안전하게 연결합니다. 이는 전원 관리 에이전트에 따라 ssh, ssl, 기타 다른 인증 프로토콜을 통해 실행될 수 있습니다.

7.5.4.3. SPM 우선순위 설정

SPM 설정 탭에는 새 호스트 또는 호스트 편집 창의 SPM 탭에 필요한 정보에 대해 설명하고 있습니다.

표 7.4. SPM 설정

필드 이름	설명
SPM 우선순위	SPM (Storage Pool Manager) 역할이 지정된 호스트의 우선순위를 정의합니다. 우선순위 옵션에는 낮음, 보통, 높음 이 있습니다. 낮은 우선순위는 해당 호스트에 SPM 역할이 할당될 수 있는 가능성이 낮아지고 높은 우선순위는 가능성이 높아짐을 의미합니다. 기본 설정은 보통입니다.

7.5.4.4. 호스트 콘솔 설정

콘솔 설정 표에서는 새로운 호스트 또는 호스트 편집 창의 콘솔 탭에 필요한 정보를 설명하고 있습니다.

표 7.5. 콘솔 설정

필드 이름	설명
출력 주소 덮어쓰기	이 체크 상자를 선택하여 호스트의 디스플레이 주소를 덮어쓰기합니다. 이 기능은 호스트가 내부 IP로 정의되어 있고 NAT 방화벽을 사용하고 있을 경우 유용합니다. 사용자가 내부 네트워크의 외부에서 가상 머신에 연결할 때 가상 머신을 실행하고 있는 호스트의 비공개 주소를 반환하지 않고 공용 IP 또는 FQDN을 (공용 IP의 외부 네트워크에서 확인됨) 반환합니다.
주소 출력	여기에 지정된 디스플레이 주소는 이 호스트에서 실행되는 모든 가상 머신에 사용됩니다. 주소는 완전 정규화된 도메인 이름이나 IP 주소 형식이어야 합니다.

7.5.4.5. 네트워크 공급자 설정

네트워크 공급자 설정 표에는 새 호스트 또는 호스트 편집 창의 네트워크 공급자 탭에 필요한 정보가 자세히 나와 있습니다.

표 7.6. 네트워크 공급자 설정

필드 이름	설명
외부 네트워크 공급자	외부 네트워크 공급자를 추가했고 호스트의 네트워크를 외부 네트워크 공급자에서 프로비전하도록 하려면 목록에서 하나를 선택합니다.

7.5.4.6. 커널 설정

커널 설정 표에는 새 호스트 또는 호스트 편집 창의 커널 탭에 필요한 상세 정보가 나와 있습니다. 일반적인 커널 부트 매개 변수 옵션은 체크 박스로 표시되어 있으므로 쉽게 선택할 수 있습니다. 보다 복잡한 변경 사항의 경우 커널 명령행 옆에 있는 자유 텍스트 항목 필드를 사용하여 필요한 추가 매개 변수를 추가하십시오.



중요

호스트가 이미 Manager에 연결되어 있는 경우 변경 사항을 적용하기 전에 호스트를 유지 관리 모드로 전환하십시오. 다시 설치를 클릭하여 호스트를 다시 설치하고, 설치가 완료된 후 변경 사항이 적용되도록 호스트를 재부팅해야 합니다.

표 7.7. 커널 설정

필드 이름	설명
호스트 장치 통과 & SR-IOV	호스트 장치가 가상 머신 자체에 직접 연결된 장치인 것처럼 가상 머신에서 호스트 장치를 사용할 수 있도록 커널에서 IOMMU 플래그를 활성화합니다. 호스트 하드웨어 및 펌웨어도 IOMMU를 지원해야 합니다. 가상화 확장 파일 및 IOMMU 확장 파일은 하드웨어에서 활성화해야 합니다. 자세한 내용은 설치 가이드 에 있는 PCI 통과(Passthrough)를 위한 호스트 설정 을 참조하십시오. IBM POWER8에는 IOMMU가 기본적으로 활성화되어 있습니다.
중첩된 가상화	가상 머신 내에서 가상 머신을 실행할 수 있도록 vmx 또는 svm 플래그를 활성화합니다. 이 옵션은 프로덕션 목적으로는 지원되지 않으며 평가 목적으로만 사용됩니다. <code>vdsm-hook-nestedvt</code> 후크는 호스트에 설치해야 합니다.
안전하지 않은 인터럽트	IOMMU가 활성화되어 있지만 하드웨어가 인터럽트 리매핑을 지원하지 않아 통과에 실패하는 경우 이 옵션을 활성화할 수 있습니다. 호스트에 있는 가상 머신을 신뢰할 수 있는 경우에만 이 옵션을 활성화해야 합니다. 이 옵션을 활성화하면 호스트가 가상 머신으로부터 MSI 공격에 잠재적으로 노출됩니다. 이 옵션은 평가를 위해 인증되지 않은 하드웨어를 사용할 때 문제 해결을 위해서만 사용합니다.

필드 이름	설명
PCI 재할당	SR-IOV NIC에서 메모리 문제로 인해 가상 기능을 할당할 수 없는 경우 이 옵션을 활성화할 수 있습니다. 호스트 하드웨어 및 펌웨어도 PCI 재할당을 지원해야 합니다. 이 옵션은 평가를 위해 인증되지 않은 하드웨어를 사용할 때 문제 해결을 위해서만 사용합니다.
커널 명령행	이 필드를 사용하면 추가 커널 매개 변수를 기본 매개 변수로 추가할 수 있습니다.



참고

커널 부트 매개 변수가 회색으로 표시되는 경우 **재설정** 버튼을 클릭하면 옵션을 사용할 수 있게 됩니다.

7.5.4.7. 호스트 엔진 설정

호스트 엔진 설정 표에는 새 호스트 또는 호스트 편집 창의 호스트 엔진 탭에 필요한 정보가 자세히 나와 있습니다.

표 7.8. 호스트 엔진 설정

필드 이름	설명
호스트 엔진 배치 작업 선택	세 가지 옵션을 사용할 수 있습니다. <ul style="list-style-type: none"> • 없음 - 필요한 작업이 없습니다. • 배포 - 호스트를 셀프 호스트 엔진 호스트로 배포하려면 이 옵션을 선택합니다. • 배포 취소 - 셀프 호스트 엔진 호스트에 대해 이 옵션을 선택하여 호스트를 배포 취소하고 셀프 호스트 엔진 관련 설정을 제거할 수 있습니다.

7.5.5. 호스트 전원 관리 기능 설정

관리 포털에서 호스트 라이프 사이클 동작 (정지, 시작, 다시 시작)을 수행하려면 호스트 전원 관리 장치 기능을 설정합니다.

호스트 고가용성 및 가상 머신 고가용성을 활용하려면 호스트 전원을 관리 설정해야 합니다.



중요

전원 관리 설정을 구성하기 전 호스트가 **maintenance mode**인지 확인합니다. 호스트가 이 모드에 있지 않을 경우 해당 호스트에서 실행되는 모든 가상 머신은 호스트를 다시 시작할 때 중단되어 제품 환경에 장애가 발생할 수 있습니다. 호스트가 **maintenance mode**로 올바르게 설정되어 있지 않은 경우 경고 메시지가 표시됩니다.

절차 7.4. 전원 관리 설정

1. 호스트 탭에서 결과 목록에 있는 호스트를 선택합니다.
2. 편집을 클릭하여 호스트 편집 창을 엽니다.
3. 전원 관리 탭을 클릭하여 전원 관리 설정을 표시합니다.
4. 필드를 활성화하려면 전원 관리 활성화 확인란을 선택합니다.
5. **Kdump** 통합 확인란을 선택하여 커널 크래시 덤프 실행 시 호스트가 차단되지 않게 합니다.



중요

기존 호스트에서 **Kdump** 통합을 활성화할 때 **kdump**를 설정하기 위해 호스트를 다시 설치해야 합니다. [7.5.11절. "호스트 다시 설치"](#)에서 참조하십시오.

6. 옵션으로 호스트의 전원 관리가 호스트 클러스터의 스케줄링 정책에 의해 제어되지 않게 하려면 전원 관리 정책 제어를 비활성화 확인란을 선택합니다.
7. 플러스 (+) 버튼을 클릭하여 새 전원 관리 장치를 추가합니다. 펜스 에이전트 편집 창이 열립니다.
8. 해당 란에 전원 관리 장치의 주소, 사용자 이름, 암호를 입력합니다.
9. 드롭 다운 목록에서 전원 관리 장치 유형을 선택합니다.
10. 전원 관리 장치가 사용하는 SSH 포트 번호를 입력하여 호스트와 통신합니다.
11. 전원 관리 장치의 블레이드를 구별하기 위해 사용하는 슬롯 번호를 입력합니다.
12. 전원 관리 장치의 옵션을 입력합니다. 콤마로 구분된 'key=value' 항목을 사용합니다.
13. 보안 확인란을 선택하여 호스트에 안전하게 연결하는 전원 관리 장치를 활성화합니다.
14. 테스트를 클릭하여 설정이 올바른지 확인합니다. 작업 완료 후 *Test Succeeded, Host Status is: on*이 표시됩니다.
15. **OK**를 클릭하여 펜스 에이전트 편집 창을 닫습니다.
16. 전원 관리 탭에서 옵션으로 고급 매개변수를 확장하고 위, 아래 버튼을 사용하여 Manager가 펜싱 프록시 용으로 호스트의 클러스터 및 **dc** (datacenter)를 검색할 순서를 지정합니다.
17. **OK**를 클릭합니다.

관리 포털에서 전원 관리 드롭 다운 메뉴가 활성화됩니다.

7.5.6. 호스트의 Storage Pool Manager 설정

SPM (Storage Pool Manager)는 데이터 센터에 있는 호스트에 할당된 관리 역할로 스토리지 도메인을 통해 액세스 제어를 유지관리합니다. SPM은 항상 사용 가능해야 하고 SPM 호스트가 사용 불가능하게 될 경우 SPM 역할은 다른 호스트에 할당됩니다. SPM 역할은 일부 호스트의 사용 가능한 리소스를 사용하므로 리소스에 여유가 있는 호스트의 우선순위를 높게 설정하는 것이 중요합니다.

호스트의 SPM (Storage Pool Manager) 우선순위 설정에 따라 SPM 역할에 할당될 가능성을 변경할 수 있습니다. 높은 SPM 우선순위를 갖는 호스트는 낮은 SPM 우선순위를 갖는 호스트 보다 먼저 SPM 역할이 할당됩니다.

절차 7.5. SPM 항목 설정

1. 호스트 리소스 탭을 클릭하여 결과 목록에서 호스트를 선택합니다.
2. 편집을 클릭하여 호스트 편집 창을 엽니다.
3. SPM 탭을 클릭하여 SPM 우선순위 설정을 표시합니다.
4. 라디오 버튼을 사용하여 호스트에 대해 알맞는 SPM 우선순위를 선택합니다.
5. OK를 클릭하여 설정을 저장하고 창을 닫습니다.

호스트의 SPM 우선순위가 설정됩니다.

7.5.7. 호스트를 유지 관리 모드로 변경

네트워크 설정 및 소프트웨어 업데이트 배포를 포함하여 일반적인 유지 보수 작업을 하려면 호스트를 유지 보수 모드로 전환해야 합니다. 재부팅이나 네트워크 또는 스토리지 관련 문제로 인해 VDSM이 올바르게 작동하지 않을 수 있으므로 이러한 문제가 발생하기 전 호스트를 유지 보수 모드로 전환해야 합니다.

호스트를 유지 관리 모드로 전환할 때 Red Hat Virtualization Manager는 실행 중인 모든 가상 머신을 다른 호스트에 마이그레이션하려 합니다. 라이브 마이그레이션의 경우 표준 전제 조건이 적용되며 특히 클러스터에 마이그레이션된 가상 머신을 실행할 용량이 있는 활성 호스트가 최소 1대 있어야 합니다.

절차 7.6. 호스트를 유지 관리 모드로 전환

1. 호스트 리소스 탭을 클릭하여 원하는 호스트를 선택합니다.
2. 유지보수를 클릭하면 호스트 유지관리 모드 확인 창이 열립니다.
3. 옵션으로 호스트 유지관리 모드 확인 창에서 호스트를 유지 관리 모드로 전환하려는 이유를 입력합니다. 이를 통해 유지 관리에 대한 설명을 제공할 수 있으며 이는 로그에 호스트가 다시 활성화될 때에 표시됩니다.



참고

호스트 유지 관리 이유 필드는 클러스터 설정에서 활성화되어 있는 경우에만 표시됩니다. 보다 자세한 내용은 [5.2.2.1절. "일반 클러스터 설정"](#)에서 참조하십시오.

4. OK를 클릭하여 유지 관리 모드를 시작합니다.

실행 중인 모든 가상 머신은 다른 호스트에 마이그레이션됩니다. 호스트가 SPM (Storage Pool Manager)일 경우 SPM 역할은 다른 호스트에 마이그레이션됩니다. 호스트의 상태 필드는 **Preparing for Maintenance**로 변경되고 작업이 성공적으로 완료되면 **Maintenance**로 됩니다. VDSM은 호스트가 유지 관리 모드일 경우 중지되지 않습니다.



참고

가상 머신에서 마이그레이션을 실패할 경우 호스트에 있는 **활성화**를 클릭하여 유지 관리 모드로의 전환 작업을 중지한 후 가상 머신에 있는 **마이그레이션 취소**를 클릭하여 마이그레이션을 중지합니다.

7.5.8. 유지 관리 모드에서 호스트 활성화

유지 관리 모드에 있는 호스트나 최근 환경에 추가된 호스트는 사용하기 전 활성화해야 합니다. 호스트가 준비되어 있지 않은 경우 활성화되지 않을 수 있습니다. 호스트를 활성화하기 전 모든 작업이 완료되었는지 확인합니다.

절차 7.7. 유지 관리 모드에서 호스트 활성화

1. 호스트 리소스 탭을 클릭하여 호스트를 선택합니다.
2. 활성화 버튼을 클릭합니다.

호스트의 상태를 **Unassigned**로 변경하고 작업 완료되면 **Up** 상태가 됩니다. 이제 가상 머신을 호스트에서 실행할 수 있습니다. 호스트가 유지 보수 모드로 되어 있을 때 다른 호스트로 마이그레이션된 가상 머신은 활성화 시 호스트에 자동으로 마이그레이션 반환되지 않지만 수동으로 마이그레이션할 수 있습니다. 호스트를 유지 관리 모드로 변경하기 전 호스트가 **SPM (Storage Pool Manager)**인 경우 호스트 활성화 시 **SPM** 역할은 자동으로 반환되지 않습니다.

7.5.9. 호스트 삭제

가상 환경에서 호스트를 삭제합니다.

절차 7.8. 호스트 삭제

1. 관리 포털에서 호스트 리소스 탭을 클릭하고 결과 목록에서 호스트를 선택합니다.
2. 호스트를 유지 관리 모드로 변경합니다.
3. 삭제를 클릭하면 호스트 삭제 확인 창이 열립니다.
4. 호스트가 Red Hat Gluster Storage 클러스터의 부분으로 볼륨 브릭이 있거나 호스트가 응답하지 않는 경우 강제 삭제 확인란을 선택합니다.
5. **OK**를 클릭합니다.

호스트가 환경에서 삭제되어 더 이상 호스트 탭에서 볼 수 없습니다.

7.5.10. 마이너 릴리스 간 호스트 업데이트

마이너 릴리스 간에 호스트를 최신 상태로 유지하기 위한 지침은 업그레이드 가이드의 다음 섹션을 참조하십시오. https://access.redhat.com/documentation/en/red-hat-virtualization/4.1/single/upgrade-guide/#chap-Updates_between_Minor_Releases.

7.5.11. 호스트 다시 설치

관리 포털에서 Red Hat Virtualization Host (RHVH) 및 Red Hat Enterprise Linux 호스트를 다시 설치합니다. 다음 절차에 따라 현재 설치된 RHVH ISO 이미지와 동일한 버전의 RHVH를 다시 설치합니다. 이 절차에서는 Red Hat Enterprise Linux 호스트에 VDSM가 다시 설치되며 이에는 호스트 중지 및 재시작이 포함됩니다. 클러스터 레벨에서 마이그레이션이 활성화되어 있을 경우 가상 머신은 클러스터에 있는 다른 호스트로 자동으로 마이그레이션되므로 호스트 사용량이 비교적 적을 때 호스트 재설치 작업을 수행하는 것이 좋습니다.

호스트가 속한 클러스터에는 호스트가 유지 관리를 수행하기에 충분한 메모리를 보유하고 있어야 합니다. 메모리가 불충분한 클러스터에서 실행되는 가상 머신이 유지 관리 모드로 전환하면 가상 머신 마이그레이션 작업이 중단되고 작업 실패하게 됩니다. 호스트를 유지 관리 모드로 전환하기 전 일부 또는 모든 가상

머신을 종료하여 작업의 메모리 사용량을 감소시킬 수 있습니다.



중요

다시 설치를 수행하기 전 클러스터에 하나 이상의 호스트가 포함되어 있는지 확인합니다. 모든 호스트를 동시에 다시 설치하지 않도록 합니다. 하나의 호스트는 **SPM (Storage Pool Manager)** 작업을 수행할 수 있도록 사용 가능한 상태로 남아 있어야 합니다.

절차 7.9. Red Hat Virtualization Host 또는 Red Hat Enterprise Linux 호스트 다시 설치

1. **호스트 리소스 탭**, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 호스트를 검색 및 선택합니다.
2. **유지 관리**를 클릭합니다. 클러스터 레벨에서 마이그레이션이 활성화되어 있을 경우 호스트에서 실행되고 있는 가상 머신은 다른 호스트로 마이그레이션됩니다. 호스트가 **SPM**일 경우 이 기능은 다른 호스트로 이동합니다. 호스트가 유지 관리 모드가 되면 호스트 상태가 변경됩니다.
3. **다시 설치**를 클릭하여 **호스트 설치** 창을 엽니다.
4. **OK**를 클릭하여 호스트를 다시 설치합니다.

다시 설치를 완료하면 호스트는 **Up** 상태로 표시됩니다. 이 시점에서 호스트에서 마이그레이션된 가상 머신을 원래 호스트로 되돌릴 수 있습니다.



중요

Red Hat Virtualization Host를 Red Hat Virtualization Manager에 등록 완료하고 다시 설치한 후 관리 포털에 **설치 실패** 상태로 표시되는 경우가 있습니다. **활성화**를 클릭하면 **Host**는 **Up** 상태로 변경되어 사용 가능한 상태가 됩니다.

7.5.12. 태그로 호스트를 사용자 정의하기

태그를 사용하여 호스트에 관한 정보를 저장할 수 있습니다. 그 후 태그에 따라 호스트를 검색할 수 있습니다.

절차 7.10. 태그로 호스트를 사용자 정의하기

1. **호스트 리소스 탭**, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 호스트를 검색 및 선택합니다.
2. **태그 지정**을 클릭하여 **태그 지정** 창을 엽니다.



그림 7.1. 태그 지정 창

3. 태그 지정 창에 사용가능한 모든 태그가 나열됩니다. 해당 태그의 체크 상자를 선택합니다.
4. **OK**를 클릭하여 태그를 지정하고 창을 닫습니다.

호스트에 대한 검색 가능한 정보가 태그로 추가됩니다.

7.5.13. 호스트 에라타 표시

호스트가 Red Hat Satellite 서버에서 에라타 정보를 받도록 설정된 후 각 호스트의 에라타가 표시됩니다. 에라타 정보를 받도록 호스트를 설정하는 방법에 대한 보다 자세한 내용은 [7.5.3절. “호스트에 대한 Satellite 에라타 관리 설정”](#)에서 참조하십시오.

절차 7.11. 호스트 에라타 표시

1. 호스트 리소스 탭을 클릭하여 결과 목록에서 호스트를 선택합니다.
2. 상세 정보 창의 **일반** 탭을 클릭합니다.
3. **일반** 탭에서 **에라타** 하위 탭을 클릭합니다.

7.5.14. 호스트 상태 표시

호스트는 일반적인 **상태** 외에 외부 상태가 있습니다. 외부 상태는 플러그인 또는 외부 시스템에 의해 보고되거나 관리자가 설정하며 호스트 이름 왼쪽에 다음의 아이콘 중에서 하나가 표시됩니다:

- **OK:** 아이콘 없음
- **Info:** 
- **Warning:** 
- **Error:** 
- **Failure:** 

호스트 상태에 대한 상세 정보를 표시하기 위해 해당 호스트를 선택하고 **이벤트** 하위 탭을 클릭합니다.

호스트 상태는 REST API로 표시될 수도 있습니다. 호스트에 대한 **GET** 요청에는 호스트 상태가 들어 있는 **external_status** 요소가 포함됩니다.

events 컬렉션을 통해 REST API에서 호스트 상태를 설정할 수 있습니다. 자세한 내용은 [REST API 가이드](#)에 있는 **이벤트 추가**를 참조하십시오.

7.5.15. 호스트 장치 표시

상세 정보 창에서 각 호스트의 호스트 장치를 표시할 수 있습니다. 호스트에 직접 장치 할당이 설정된 경우 해당 장치는 성능 향상을 위해 가상 머신에 직접 연결될 수 있습니다.

직접 장치 할당에 필요한 하드웨어 요구 사항에 대한 자세한 내용은 [SR-IOV 구현을 위한 Red Hat Virtualization 하드웨어 고려 사항](#)에 있는 [장치 할당 사용을 위한 추가 하드웨어 고려 사항](#)을 참조하십시오.

직접 장치 할당을 위한 호스트 설정에 대한 자세한 내용은 [설치 가이드](#)에 있는 [PCI 통과\(Passthrough\)를 위한 호스트 설정](#)을 참조하십시오.

가상 머신에 호스트 장치를 연결하는 방법에 대한 자세한 내용은 [가상 머신 관리 가이드](#)에 있는 [호스트 장치](#)를 참조하십시오.

절차 7.12. 호스트 장치 표시

1. 호스트 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 호스트를 검색 및 선택합니다.
2. 상세 정보 창에서 **호스트 장치** 탭을 클릭합니다.

상세 정보 창에는 호스트 장치가 가상 머신에 연결되어 있는지 여부, 현재 그 가상 머신에 의해 사용중인 지 여부 등 호스트 장치에 대한 상세 정보가 표시됩니다.

7.5.16. GPU 통과(Passthrough)에 필요한 호스트 및 게스트 시스템 준비

호스트의 GPU(그래픽 처리 장치) 장치를 가상 머신에 직접 할당할 수 있습니다. 이를 수행하려면 호스트 및 가상 머신 모두에서 **grub** 설정 파일을 수정해야 합니다. 관리 포털에서 **커널 명령행** 자유 텍스트 항목 필드를 통해 호스트 **grub** 설정 파일을 편집할 수 있습니다. 변경 사항을 적용하려면 호스트 머신과 가상 머신 모두를 재부팅해야 합니다.

이 절차는 x86_64 또는 ppc64le 아키텍처의 호스트에 해당됩니다.

장치를 직접 할당하기 위한 하드웨어 요구 사항에 대한 자세한 정보는 [설치 가이드](#)에 있는 [PCI 장치 요구 사항](#)을 참조하십시오.



중요

호스트가 이미 Manager에 연결되어 있는 경우 변경 사항을 적용하기 전에 호스트를 유지 관리 모드로 전환합니다.

절차 7.13. GPU 통과(Passthrough)에 필요한 호스트 준비

1. 관리 포털에서 호스트를 선택합니다.
2. 상세 정보 창에서 **일반** 탭을 클릭하고 **하드웨어**를 클릭합니다. GPU 장치 **벤더 ID: 제품 ID**를 찾습니다. 이 예에서 ID는 **10de:13ba** 및 **10de:0fbc**입니다.
3. 호스트를 오른쪽 클릭하고 **편집**을 선택합니다. **커널** 탭을 클릭합니다.
4. 커널 명령행 자유 텍스트 항목 필드에 이전 단계에서 찾은 ID를 입력합니다.

```
pci-stub.ids=10de:13ba,10de:0fbc
```

5. 호스트에서 해당하는 드라이버를 블랙리스트에 추가합니다. 예를 들어 `pci-stub.ids=xxxx:xxxx` 옆에 있는 nVidia의 nouveau 드라이버를 블랙리스트에 추가하려면 `rdblacklist=nouveau`를 입력합니다.

```
pci-stub.ids=10de:13ba,10de:0fbc rdblacklist=nouveau
```

6. **OK**를 클릭하여 변경 사항을 저장합니다.
7. **다시 설치**를 클릭하여 변경 사항을 호스트에 적용합니다.
8. 재설치가 완료되면 호스트를 재부팅합니다.



참고

장치가 **pci-stub** 드라이버에 연결되어 있는지 확인하려면 `lspci` 명령을 실행합니다.

```
# lspci -nnk
...
01:00.0 VGA compatible controller [0300]: NVIDIA Corporation
GM107GL [Quadro K2200] [10de:13ba] (rev a2)
    Subsystem: NVIDIA Corporation Device [10de:1097]
    Kernel driver in use: pci-stub
01:00.1 Audio device [0403]: NVIDIA Corporation Device
[10de:0fbc] (rev a1)
    Subsystem: NVIDIA Corporation Device [10de:1097]
    Kernel driver in use: pci-stub
...
```

grub 설정 파일을 수동으로 편집하여 위의 사항을 변경하는 방법에 대한 지침은 [3.6 관리 가이드](#)에 있는 **GPU 통과(Passthrough)에 필요한 호스트 및 게스트 시스템 준비**를 참조하십시오.

게스트 시스템에서 GPU 통과(Passthrough) 설정을 위해 다음 절차를 진행합니다.

절차 7.14. GPU 통과(Passthrough)에 필요한 게스트 가상 머신 준비

- ◦ Linux의 경우
 - a. 독점 GPU 드라이버만 지원됩니다. 해당되는 오픈소스 드라이버를 **grub** 설정 파일의 블랙리스트에 추가합니다. 예:

```
$ vi /etc/default/grub
...
GRUB_CMDLINE_LINUX="nofb splash=quiet console=tty0 ...
rdblacklist=nouveau"
...
```

- b. GPU BusID를 찾습니다. 다음의 예시에서 BusID는 **00:09.0**입니다.

```
# lspci | grep VGA
00:09.0 VGA compatible controller: NVIDIA Corporation GK106GL
[Quadro K4000] (rev a1)
```

- c. **/etc/X11/xorg.conf** 파일을 편집하여 다음 내용을 추가합니다:

```
Section "Device"
Identifier "Device0"
Driver "nvidia"
VendorName "NVIDIA Corporation"
BusID "PCI:0:9:0"
EndSection
```

- d. 가상 머신을 다시 시작합니다.

- Windows의 경우

- a. 장치에 해당되는 드라이버를 다운로드하여 설치합니다. 예를 들어 Nvidia 드라이버의 경우 [NVIDIA Driver Downloads](#)로 갑니다.
- b. 가상 머신을 다시 시작합니다.

이제 호스트 GPU를 준비된 가상 머신에 직접 할당할 수 있습니다. 가상 머신에 호스트 장치를 할당하는 방법에 대한 자세한 정보는 [가상 머신 관리 가이드](#)에 있는 [호스트 장치](#)를 참조하십시오.

7.5.17. 관리 포털에서 Cockpit 액세스

Cockpit UI 플러그인은 Red Hat Virtualization 환경에 설치할 수 있는 옵션 기능입니다. 이러한 플러그인을 사용하여 관리 포털에서 호스트 리소스를 모니터링 및 관리하는 Cockpit 사용자 인터페이스에 액세스할 수 있습니다. Cockpit이 설치된 호스트를 선택하면 관리 포털의 상세 정보 창에서 **Cockpit** 하위 탭에 직접 Cockpit 사용자 인터페이스가 표시됩니다. 또는 메인 **호스트** 메뉴에 있는 **Cockpit** 버튼을 누르면 새 브라우저 탭에서 Cockpit 사용자 인터페이스가 열립니다.

Cockpit 사용자 인터페이스는 기본적으로 Red Hat Virtualization Host (RHVH)에서 사용 가능합니다. 현재 Red Hat Enterprise Linux 호스트에서는 지원되지 않습니다.

절차 7.15. 관리 포털에서 Cockpit 액세스

1. Manager 시스템에 Cockpit UI 플러그인을 설치합니다.

```
# yum install cockpit-ovirt-uiplugin
```

2. **ovirt-engine** 서비스를 다시 시작합니다.

```
# systemctl restart ovirt-engine.service
```

3. 관리 포털에서 **호스트** 탭을 클릭하고 호스트를 선택합니다.

4. 새 탭에서 **Cockpit** 사용자 인터페이스를 열거나 관리 포털에서 바로 표시합니다:

- 호스트를 오른쪽 클릭하고 **Cockpit**을 선택하면 새 브라우저 탭에서 **Cockpit** 사용자 인터페이스가 열립니다.
- **Cockpit** 하위 탭을 클릭하여 **Hosts** 탭의 상세 정보 창에 **Cockpit** 사용자 인터페이스를 표시합니다.



참고

선택한 호스트에서 **Cockpit**을 사용할 수 없는 경우 **Cockpit** 하위 탭에 기본적인 문제 해결 방법이 설명되어 있습니다.

7.6. 호스트 복원

7.6.1. 호스트 고가용성

Red Hat Virtualization Manager는 펜싱을 사용하여 클러스터에 있는 호스트를 응답 가능한 상태로 둡니다. **응답하지 않음** 호스트는 **작동하지 않음** 호스트와 다릅니다. **Manager**는 **작동하지 않음** 호스트와 통신할 수 있지만 논리 네트워크의 누락과 같은 잘못된 설정이 있을 수 있습니다. **Manager**는 **응답하지 않음** 호스트와 통신할 수 없습니다.

전원 관리 장치를 사용하는 호스트가 **Manager**와 통신할 수 없을 경우 관리 포털에서 펜싱 (재부팅)할 수 있습니다. 호스트에서 실행되는 모든 가상 머신이 중지되고 고가용성 가상 머신이 다른 호스트에서 시작됩니다.

모든 전원 관리 작업은 Red Hat Virtualization Manager에 의해 직접 실행되는 것이 아닌 프록시 호스트를 사용하여 실행됩니다. 전원 관리 작업에는 최소 2 개의 호스트가 필요합니다.

펜싱을 통해 클러스터는 예기치 않은 호스트 오류, 절전, 부하 분산, 가상 머신 가용성 정책에 대응할 수 있습니다. 호스트의 전원 관리 장치에 따라 펜싱 매개 변수를 설정하고 수시로 설정이 올바른지 테스트합니다.

전원 관리 매개 변수를 사용하여 호스트를 자동으로 펜싱하거나 호스트를 오른쪽 클릭하여 나타나는 메뉴의 옵션을 사용하여 수동으로 펜싱합니다. 펜싱 작업에서 응답 없음 상태의 호스트가 재부팅되고 지정된 시간 내에 호스트가 활성 상태로 반환되지 않을 경우 수동으로 문제해결을 하지 않는 한 응답 없음 상태가 유지됩니다.

호스트가 고가용성 가상 머신을 실행해야 할 경우 전원 관리를 활성화 및 설정해야 합니다.

7.6.2. Red Hat Virtualization에서 프록시를 통해 전원 관리

Red Hat Virtualization Manager는 펜스 에이전트와 직접 통신하지 않습니다. 대신 **Manager**는 프록시를 사용하여 호스트 전원 관리 장치에 전원 관리 명령을 전송합니다. **Manager**는 **VDSM**을 사용하여 전원 관리 장치 작업을 실행하고 환경에 있는 다른 호스트는 펜싱 프록시로 사용됩니다.

다음 중 하나를 선택할 수 있습니다:

- 펜싱이 필요한 호스트와 동일한 클러스터에 있는 호스트입니다.
- 펜싱이 필요한 호스트와 동일한 데이터 센터에 있는 호스트입니다.

사용 가능한 펜싱 프록시 호스트는 **UP** 또는 **유지 관리** 상태입니다.

7.6.3. 호스트에서 펜싱 매개 변수 설정

호스트 펜싱용 매개 변수는 새 **호스트** 또는 **호스트 편집** 창의 **전원 관리** 필드에서 설정합니다. 전원 관리에서 시스템은 RAC (Remote Access Card)와 같은 추가 인터페이스를 사용하여 호스트 문제를 펜싱합니다.

모든 전원 관리 작업은 Red Hat Virtualization Manager에 의해 직접 실행되는 것이 아닌 프록시 호스트를 사용하여 실행됩니다. 전원 관리 작업에는 최소 2 개의 호스트가 필요합니다.

절차 7.16. 호스트에서 펜싱 매개 변수 설정

1. **호스트 리소스 탭**, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 호스트를 검색 및 선택합니다.
2. **편집**을 클릭하여 **호스트 편집** 창을 엽니다.
3. **전원 관리** 탭을 클릭합니다.

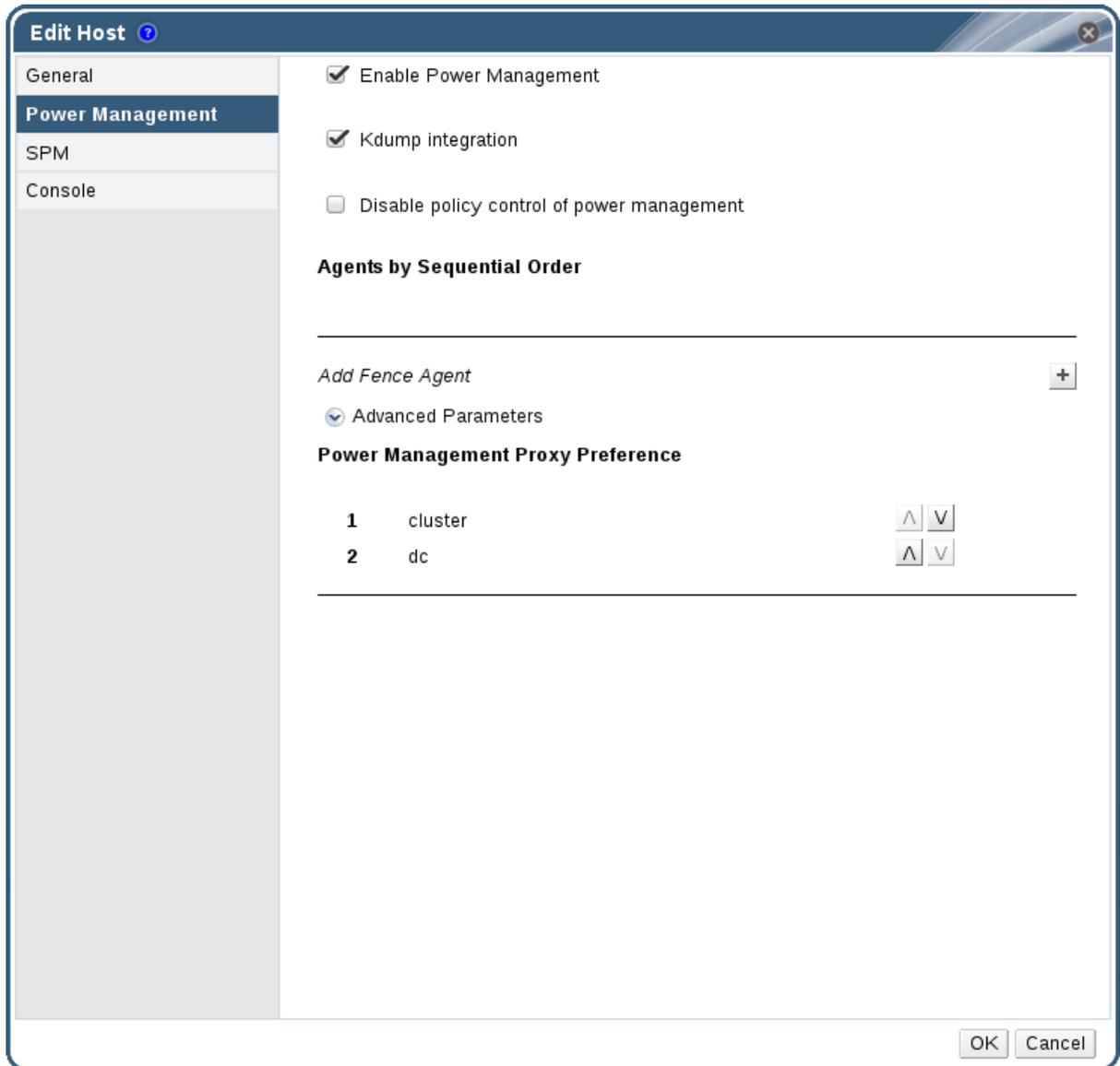


그림 7.2. 전원 관리 설정

4. 필드를 활성화하려면 **전원 관리 활성화** 확인란을 선택합니다.
5. **Kdump** 통합 확인란을 선택하여 커널 크래시 덤프 실행 시 호스트가 차단되지 않게 합니다.



중요

기존 호스트에서 **Kdump** 통합을 활성화할 때 **kdump**를 설정하기 위해 호스트를 다시 설치해야 합니다. [7.5.11절. "호스트 다시 설치"](#)에서 참조하십시오.

6. 옵션으로 호스트의 전원 관리가 호스트 클러스터의 스케줄링 정책에 의해 제어되지 않게 하려면 **전원 관리 정책 제어를 비활성화** 확인란을 선택합니다.
7. 플러스 (+) 버튼을 클릭하여 새 전원 관리 장치를 추가합니다. **펜스 에이전트 편집** 창이 열립니다.

그림 7.3. 펜스 에이전트 편집

8. 전원 관리 장치의 주소, 사용자 이름, 암호를 입력합니다.
9. 드롭 다운 목록에서 전원 관리 장치 유형을 선택합니다.



참고

사용자 정의 전원 관리 장치 설정 방법에 대한 자세한 내용은 <https://access.redhat.com/articles/1238743>에서 참조하십시오.

10. 전원 관리 장치가 사용하는 **SSH** 포트 번호를 입력하여 호스트와 통신합니다.
11. 전원 관리 장치의 블레이드를 구별하기 위해 사용하는 슬롯 번호를 입력합니다.
12. 전원 관리 장치의 옵션을 입력합니다. 콤마로 구분된 'key=value' 항목을 사용합니다.
13. 보안 확인란을 선택하여 호스트에 안전하게 연결하는 전원 관리 장치를 활성화합니다.
14. 테스트 버튼을 클릭하여 설정이 올바른지 확인합니다. 작업 완료 후 *Test Succeeded, Host Status is: on*이 표시됩니다.



주의

전원 관리 매개 변수 (사용자 ID, 암호, 옵션 등)는 설정 시 Red Hat Virtualization Manager에 의해 테스트되며 그 후에는 수동으로 실행합니다. 잘못된 매개 변수에 대한 경고를 무시하거나 매개 변수가 전원 관리 하드웨어에서 변경되었지만 Red Hat Virtualization Manager에서는 변경되지 않은 경우 펜싱 실행을 실패할 수 있습니다.

15. **OK**를 클릭하여 펜스 에이전트 편집 창을 닫습니다.
16. 전원 관리 탭에서 옵션으로 고급 매개변수를 확장하고 위, 아래 버튼을 사용하여 Manager가 펜싱 프록시 용으로 호스트의 클러스터 및 **dc** (datacenter)를 검색할 순서를 지정합니다.
17. **OK**를 클릭합니다.

호스트 목록으로 돌아갑니다. 전원관리가 올바르게 설정 완료되었음을 나타내는 호스트 이름 옆의 느낌표는 더이상 표시되지 않음에 유의합니다.

7.6.4. fence_kdump 고급 설정

kdump

상세 정보 창의 일반 탭에서 kdump 서비스 상태를 확인하기 위해 호스트를 선택합니다.

- **활성화됨:** kdump가 올바르게 설정되어 kdump 서비스가 실행되고 있습니다.
- **비활성화됨:** kdump 서비스가 실행되고 있지 않습니다 (이 경우 kdump 통합이 올바르게 작동하지 않게 됩니다).
- **알 수 없음:** kdump 상태를 보고하지 않는 이전 VDSM 버전을 사용하는 호스트의 경우에만 발생합니다.

kdump 설치 및 사용에 대한 보다 자세한 내용은 [Red Hat Enterprise Linux 7 Kernel Crash Dump Guide](#)에서 참조하십시오.

fence_kdump

새 호스트 또는 호스트 수정 창의 전원 관리 탭에서 **Kdump** 통합을 활성화하여 표준 fence_kdump 설정을 구성합니다. 환경의 네트워크 설정이 간단하고 Manager의 FQDN이 모든 호스트에서 확인 가능한 경우 기본 fence_kdump 설정이면 충분합니다.

하지만 일부 경우 fence_kdump 고급 설정이 필요할 수 있습니다. 보다 복잡한 네트워크로 구성된 환경의 경우 Manager, fence_kdump 수신기 또는 두 가지 모두를 설정하기 위해 수동으로 구성을 변경해야 할 수도 있습니다. 예를 들어 Manager의 FQDN을 **Kdump** 통합이 활성화된 모든 호스트에서 사용 불가능할 경우 **engine-config**를 사용하여 적절한 호스트 이름이나 IP 주소를 설정할 수 있습니다:

```
engine-config -s FenceKdumpDestinationAddress=A.B.C.D
```

다음 예에서는 설정 사항을 변경해야 할 수 있습니다:

- Manager에는 두 개의 NIC가 있습니다. 여기서 하나는 public-facing에 용이고 다른 하나는 fence_kdump 메시지의 지정 대상이 됩니다.

- 다른 IP 또는 포트에서 `fence_kdump` 수신기를 실행해야 합니다.
- `fence_kdump` 통지 메시지에 대해 사용자 정의 간격을 설정하여 가능한 패킷 손실을 방지합니다.

사용자 정의된 `fence_kdump` 검색 설정은 고급 사용자의 경우에만 권장됩니다. 이는 기본 설정으로의 변경이 보다 복잡한 네트워킹 설정에만 필요하기 때문입니다. `fence_kdump` 수신기의 설정 옵션은 [7.6.4.1절. “fence_kdump 수신기 설정”](#)에서 참조하십시오. Manager에서 `kdump` 설정에 대한 내용은 [7.6.4.2절. “Manager에서 fence_kdump 설정”](#)에서 참조하십시오.

7.6.4.1. fence_kdump 수신기 설정

`fence_kdump` 수신기 설정을 편집합니다. 이는 기본 설정으로 충분하지 않은 경우에만 편집합니다.

절차 7.17. 수동으로 fence_kdump 수신기 설정

1. `/etc/ovirt-engine/ovirt-fence-kdump-listener.conf.d/`에 새로운 파일을 (예: `my-fence-kdump.conf`) 생성합니다.
2. `OPTION=value` 구문으로 사용자 설정 항목을 입력하고 파일을 저장합니다.



중요

편집된 값은 [7.6.4.2절. “Manager에서 fence_kdump 설정”](#)에 있는 `fence_kdump` 수신기 설정 옵션 표에서 설명되어 있듯이 `engine-config`도 변경해야 합니다.

3. `fence_kdump` 수신기를 다시 시작합니다:

```
# systemctl restart ovirt-fence-kdump-listener.service
```

필요한 경우 다음과 같은 옵션을 사용자 설정합니다:

표 7.9. fence_kdump 수신기 설정 옵션

변수	설명	기본값	알림
<code>LISTENER_ADDRESS</code>	<code>fence_kdump</code> 메시지를 수신하기 위해 IP 주소를 정의합니다.	0.0.0.0	이 매개 변수 값을 변경할 경우 <code>engine-config</code> 에 있는 <code>FenceKdumpDestinationAddress</code> 값과 일치해야 합니다.
<code>LISTENER_PORT</code>	<code>fence_kdump</code> 메시지를 수신하기 위해 포트를 정의합니다.	7410	이 매개 변수 값을 변경할 경우 <code>engine-config</code> 에 있는 <code>FenceKdumpDestinationPort</code> 값과 일치해야 합니다.
<code>HEARTBEAT_INTERVAL</code>	수신기의 하트비트 업데이트 간격을 초 단위로 정의합니다.	30	매개 변수 값을 변경할 경우 <code>engine-config</code> 에 있는 <code>FenceKdumpListenerTimeout</code> 값 보다 작은 절반 이하의 크기여야 합니다.

변수	설명	기본값	알림
SESSION_SYNC_INTERVAL	수신기의 호스트 메모리에서 <code>kdumping</code> 세션을 데이터베이스로 동기화하는 간격을 초 단위로 정의합니다.	5	매개 변수 값을 변경할 경우 engine-config 에 있는 KdumpStartedTimeout 값 보다 작은 절반 이하의 크기여야 합니다.
REOPEN_DB_CONNECTION_INTERVAL	이전에 사용 불가능했던 데이터 베이스 연결을 다시 열기 위한 간격을 초 단위로 정의합니다.	30	-
KDUMP_FINISHED_TIMEOUT	호스트의 <code>kdump</code> 흐름이 <code>FINISHED</code> 로 표시된 후 <code>kdump</code> 실행 호스트에서 마지막으로 메시지를 수신할 때 까지 최대 시간 제한을 초 단위로 정의합니다.	60	매개 변수 값을 변경할 경우 engine-config 에 있는 FenceKdumpMessageInterval 값 보다 2 배 이상으로 큰 크기여야 합니다.

7.6.4.2. Manager에서 fence_kdump 설정

Manager의 `kdump` 설정을 편집합니다. 이는 기본 설정으로 충분하지 않을 경우에만 필요합니다. 현재 설정 값은 다음을 사용하여 확인할 수 있습니다:

```
# engine-config -g OPTION
```

절차 7.18. engine-config를 사용하여 수동으로 Kdump 설정

1. **engine-config** 명령을 사용하여 `kdump` 설정을 편집합니다:

```
# engine-config -s OPTION=value
```



중요

편집된 값은 **Kdump** 설정 옵션 표에 설명되어 있듯이 **fence_kdump** 수신기 설정 파일에도 변경해야 합니다. 자세한 내용은 [7.6.4.1절. "fence_kdump 수신기 설정"](#)에서 참조하십시오.

2. **ovirt-engine** 서비스를 다시 시작합니다:

```
# systemctl restart ovirt-engine.service
```

3. 필요한 경우 **Kdump** 통합 활성화로 모든 호스트를 다시 설치합니다 (아래 표 참조).

다음 옵션은 **engine-config** 명령을 사용하여 설정할 수 있습니다:

표 7.10. Kdump 설정 옵션

변수	설명	기본값	알림
FenceKdumpDestinationAddress	fence_kdump 메시지를 전송할 호스트 이름 또는 IP 주소를 정의합니다. 값이 비어 있을 경우 Manager의 FQDN이 사용됩니다.	빈 문자열 (Manager의 FQDN이 사용됨)	이 매개 변수 값을 변경할 경우 fence_kdump 수신기 설정 파일에 있는 LISTENER_ADDRESS 값과 일치해야 하며 Kdump 통합 활성화된 모든 호스트를 다시 설치해야 합니다.
FenceKdumpDestinationPort	fence_kdump 메시지를 전송하기 위한 포트를 정의합니다.	7410	이 매개 변수 값을 변경할 경우 fence_kdump 수신기 설정 파일에 있는 LISTENER_PORT 값과 일치해야 하며 Kdump 통합 활성화된 모든 호스트를 다시 설치해야 합니다.
FenceKdumpMessageInterval	fence_kdump에서의 메시지 전송 간격을 초 단위로 정의합니다.	5	이 매개 변수 값을 변경할 경우 fence_kdump 수신기 설정 파일에 있는 KDUMP_FINISHED_TIMEOUT 값보다 작거나 절반 이하로 해야 하며 Kdump 통합 활성화된 모든 호스트를 다시 설치해야 합니다.
FenceKdumpListenerTimeout	마지막 하트비트 후 fence_kdump 수신기가 실행될 것으로 예상되는 최대 시간 제한을 초 단위로 정의합니다.	90	이 매개 변수 값을 변경할 경우 fence_kdump 수신기 설정 파일에 있는 HEARTBEAT_INTERVAL 값보다 두 배 이상으로 커야 합니다.
KdumpStartedTimeout	kdump를 실행하는 호스트에서 첫 번째 메시지를 수신할 때 까지 (호스트 kdump 흐름을 감지할 때 까지) 최대 대기 시간 시간 제한을 초 단위로 정의합니다.	30	이 매개 변수 값을 변경할 경우 fence_kdump 수신기 설정 파일에 있는 SESSION_SYNC_INTERVAL 및 FenceKdumpMessageInterval 값보다 두 배 이상으로 커야 합니다.

7.6.5. 호스트 소프트웨어 펜싱

경우에 따라 호스트는 예상치 못한 문제가 발생하여 응답 없음 (non-responsive) 상태가 될 수 있으며 VDSM은 요청에 응답할 수 없지만 VDSM에 의존하는 가상 머신은 가동 및 액세스 가능한 상태가 됩니다. 이러한 경우 VDSM을 다시 시작하면 VDSM은 응답 가능한 상태가 되어 이러한 문제가 해결됩니다.

"SSH 소프트웨어 펜싱"은 Manager가 응답 없음 상태의 호스트에서 SSH를 통해 VDSM을 다시 시작하는 절차입니다. Manager가 SSH를 통해 VDSM을 다시 시작할 수 없는 경우 외부 펜싱 에이전트가 설정되어 있을 때 펜싱은 외부 펜싱 에이전트의 책임이 됩니다.

SSH를 통한 소프트웨어 펜싱은 다음과 같은 경우에 작동합니다. 호스트에서 펜싱이 설정되어 활성화되어 있어야 하며 유효한 프록시 호스트 (데이터 센터에서 UP 상태의 두 번째 호스트)가 존재해야 합니다.

Manager와 호스트 간의 연결 시간 초과 시 다음과 같은 상태가 발생합니다:

1. 첫 번째 네트워크 장애 발생 시 호스트 상태는 "connecting"으로 변경됩니다.
2. Manager는 VDSM에게 상태를 3번 확인하거나 호스트에서의 로딩에 의해 결정되는 대기 시간 동안 기다립니다. 이러한 대기 시간을 결정하는 수식은 $\text{TimeoutToResetVdsInSeconds}$ (기본값 60 초) + $[\text{DelayResetPerVmInSeconds}$ (기본값 0.5 초)]*(호스트에서 실행 중인 가상 머신 수) + $[\text{DelayResetForSpmlnSeconds}$ (기본값 20 초)] * 1 (호스트가 SPM으로 실행 중인 경우) 또는 0 (호스트가 SPM으로 실행하지 않는 경우)의 설정 값에 의해 지정됩니다. VDSM에 최대 응답 시간을 부여하려면 Manager는 위의 옵션 (VDSM의 상태를 3번 확인하거나 위의 수식에 의해 지정되는 대기 시간 동안 대기) 중 두 개의 긴 옵션을 선택합니다.
3. 시간이 경과해도 호스트가 응답하지 않을 경우 SSH를 통해 **vdsml restart**가 실행됩니다.
4. **vdsml restart**가 호스트와 Manager 간의 연결을 다시 설정하지 않을 경우 호스트 상태는 **Non Responsive**로 변경되며 전원 관리가 설정되어 있을 경우 펜싱은 외부 펜싱 에이전트로 전달됩니다.



참고

SSH를 통한 소프트웨어 펜싱은 전원 관리가 설정되어 있지 않은 호스트에서 실행될 수 있습니다. 이는 "펜싱 (fencing)"과는 다릅니다. 펜싱은 전원 관리가 설정되어 있는 호스트에서만 수행할 수 있습니다.

7.6.6. 호스트 전원 관리 기능 사용

요약

호스트에 전원 관리가 설정된 경우 관리 포털 인터페이스에서 여러 옵션에 액세스할 수 있습니다. 각각의 전원 관리 장치에는 사용자 정의 옵션이 있지만 모든 장치에서는 호스트를 시작, 중지, 다시 시작하기 위해 기본 옵션을 지원합니다.

절차 7.19. 호스트 전원 관리 기능 사용

1. 호스트 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 호스트를 검색 및 선택합니다.
2. 전원 관리 드롭 다운 메뉴를 클릭합니다.
3. 다음 중 한가지 옵션을 선택합니다:
 - **다시 시작**: 이 옵션은 호스트를 중지하고 호스트의 상태가 **Down**으로 변경될 때 까지 기다립니다. 에이전트가 호스트가 **Down**된 것을 확인하면 고가용성 가상 머신이 클러스터에 있는 다른 호스트에서 다시 시작됩니다. 그 후 에이전트는 호스트를 다시 시작합니다. 호스트가 사용 가능하게 되면 **Up** 상태로 표시됩니다.

- **시작:** 이 옵션은 호스트를 시작하고 클러스터에 추가합니다. 사용 가능하게 될 경우 **Up** 상태로 표시됩니다.
- **중지:** 이 옵션은 호스트 전원을 끕니다. 이 옵션을 사용하기 전 호스트에서 실행되고 있는 가상 머신이 클러스터에 있는 다른 호스트로 마이그레이션되었는지 확인합니다. 그렇지 않을 경우 가상 머신이 중단되고 고가용성 가상 머신만 다른 호스트에서 다시 시작됩니다. 호스트가 중지하면 **Non-Operational** 상태로 표시됩니다.



중요

두 펜싱 에이전트가 호스트에서 정의될 때 동시에 또는 순차적으로 사용될 수 있습니다. 동시에 에이전트가 사용될 경우 두 에이전트 모두 중지할 호스트에 대해 **Stop** 명령에 응답해야 합니다. 하나의 에이전트가 **Start** 명령에 응답하면 호스트가 실행됩니다. 순차적으로 에이전트가 사용될 경우 호스트를 시작 또는 중지하기 위해 주요 에이전트가 먼저 사용되며 실패할 경우 2차 에이전트가 사용됩니다.

4. 위의 옵션 중 하나를 선택하여 확인 창을 엽니다. **OK**를 클릭하여 확인하고 계속 진행합니다.

결과

선택된 동작이 수행됩니다.

7.6.7. 응답 없음 (Non Responsive) 상태의 호스트를 수동으로 펜싱 또는 분리

요약

하드웨어 오류 등과 같은 문제로 인해 호스트가 응답 없음 (non-responsive) 상태로 될 경우 이는 환경의 성능에 크게 영향을 미칠 수 있습니다. 전원 관리 장치가 없거나 잘못 설정되어 있을 경우 수동으로 호스트를 재부팅할 수 있습니다.



주의

수동으로 호스트를 재부팅하는 경우를 제외하고 호스트가 재부팅되었는지 확인 옵션을 사용하지 않습니다. 호스트가 실행되는 동안 이러한 옵션을 사용할 경우 가상 머신 이미지가 손상될 수 있습니다.

절차 7.20. 응답 없음 (Non Responsive) 상태의 호스트를 수동으로 펜싱 또는 분리

1. 호스트 탭에서 호스트를 선택합니다. 상태는 **non-responsive**로 표시해야 합니다.
2. 수동으로 호스트를 재부팅합니다. 이는 물리적으로 시스템에 들어가 호스트를 재부팅하는 것을 의미합니다.
3. 관리 포털에서 호스트 항목을 오른쪽 클릭하여 호스트가 재부팅되었는지 확인 버튼을 선택합니다.
4. 호스트가 종료되었거나 재부팅되었는지를 확인하라는 메시지가 표시됩니다. **작업 승인** 확인란을 선택하고 **OK**를 클릭합니다.

결과

수동으로 호스트를 재부팅하여 활성 호스트에서 고가용성 가상 머신을 시작할 수 있게 합니다. 관리 포털

에서 수동 펜싱 작업을 확인하면 호스트가 다시 온라인 상태로 됩니다.

7.7. 호스트 및 권한

7.7.1. 호스트의 시스템 권한 관리

SuperUser로서 시스템 관리자는 관리 포털의 모든 면을 관리합니다. 보다 특정한 관리 역할은 다른 사용자에게 부여될 수 있습니다. 이러한 제한된 관리자 역할은 특정 리소스에 제한하여 사용자 관리 권한을 부여할 경우 유용합니다. 예를 들어 **DataCenterAdmin** 역할은 데이터 센터의 스토리지를 제외한 할당된 데이터 센터에 대해서만 관리자 권한을 갖으며 **ClusterAdmin**은 할당된 클러스터에 대해서만 관리자 권한을 갖습니다.

호스트 관리자는 특정 호스트에 대한 시스템 관리자 역할입니다. 이는 각 호스트에 시스템 관리자가 필요한 여러 호스트로 구성된 클러스터에서 유용합니다. 머릿글 표시줄에 있는 **설정** 버튼을 사용하여 환경의 모든 호스트에 호스트 관리자를 지정할 수 있습니다.

호스트 관리자 역할을 다음과 같은 작업을 허용합니다:

- 호스트 설정을 편집합니다.
- 논리 네트워크를 설정합니다.
- 호스트를 삭제합니다.

기존 시스템 관리자를 삭제하고 새로운 시스템 관리자를 추가하여 호스트의 시스템 관리자를 변경할 수 있습니다.

7.7.2. 호스트 관리자 역할

호스트 권한 역할

아래 표에서는 호스트 관리에 적용할 수 있는 관리자 역할 및 권한에 대해 설명합니다.

표 7.11. Red Hat Virtualization 시스템 관리자 역할

역할	권한	알림
HostAdmin	호스트 관리자	특정 호스트를 설정, 관리, 삭제할 수 있습니다. 또한 특정 호스트에서 네트워크 관련 작업을 수행할 수 있습니다.

7.7.3. 리소스에 관리자 또는 사용자 역할 할당

리소스에 관리자 또는 사용자 역할을 할당하여 사용자가 리소스에 액세스 및 관리할 수 있게 합니다.

절차 7.21. 리소스에 역할 할당

1. 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 리소스를 검색 및 선택합니다.
2. 상세 정보 창에 있는 **권한** 탭을 클릭하여 할당된 사용자, 사용자 역할, 선택한 리소스에 대해 상속된 권한을 나열합니다.

3. **추가**를 클릭합니다.
4. **검색** 텍스트 상자에 기존 사용자의 이름 또는 사용자 이름을 입력하고 **검색**을 클릭합니다. 검색 결과 목록에서 일치하는 사용자를 선택합니다.
5. **할당할 역할** 드롭 다운 목록에서 역할을 선택합니다.
6. **OK**를 클릭합니다.

사용자에게 역할이 할당되어 이제 사용자는 리소스에 대해 활성화된 역할에 상속된 권한을 갖습니다.

7.7.4. 리소스에서 관리자 또는 사용자 역할 삭제

리소스에서 관리자 또는 사용자 역할을 삭제합니다. 사용자는 리소스에서의 역할과 관련하여 상속된 권한을 손실합니다.

절차 7.22. 리소스에서 역할 삭제

1. 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 리소스를 검색 및 선택합니다.
2. 상세 정보 창에 있는 **권한** 탭을 클릭하여 할당된 사용자 목록, 사용자 역할, 선택한 리소스에서 상속된 권한을 나열합니다.
3. 리소스에서 삭제할 사용자를 선택합니다.
4. **삭제**를 클릭합니다. **권한 삭제** 창이 열리면 권한 삭제를 확인합니다.
5. **OK**를 클릭합니다.

리소스에서 사용자 역할 및 관련된 권한이 삭제됩니다.

8장. 스토리지

Red Hat Virtualization은 가상 디스크 이미지, ISO 파일 및 스냅샷에 대해 중앙 집중화된 스토리지 시스템을 사용합니다. 스토리지 네트워킹은 다음을 사용하여 구현할 수 있습니다.

- 네트워크 파일 시스템 (NFS)
- GlusterFS 내보내기
- 기타 다른 POSIX 호환 파일 시스템
- iSCSI (Internet Small Computer System Interface)
- 가상 호스트에 직접 연결된 로컬 스토리지
- FCP (Fibre Channel Protocol)
- pNFS (Parallel NFS)

스토리지 설정은 새로운 데이터 센터의 필수 구성 요소입니다. 이는 스토리지 도메인이 연결되지 않아 활성화되지 않으면 데이터 센터를 초기화할 수 없기 때문입니다.

Red Hat Virtualization 시스템 관리자로 가상화된 엔터프라이즈에 대한 스토리지를 생성, 설정, 연결, 유지관리해야 합니다. 시스템 관리자는 스토리지 유형 및 사용에 익숙해야 합니다. 스토리지 배열 공급 업체의 가이드를 읽어 보시기 바랍니다. 스토리지에 대한 개념, 프로토콜, 요구 사항, 일반 사용 방법에 대한 보다 자세한 내용은 [Red Hat Enterprise Linux 스토리지 관리 가이드](#)에서 참조하십시오.

Red Hat Virtualization에서는 관리 포털의 스토리지 탭을 사용하여 스토리지를 할당 및 관리할 수 있습니다. 스토리지 결과 목록에 모든 스토리지 도메인을 표시하고 상세 정보 창에는 도메인에 대한 일반 정보가 표시됩니다.

스토리지 도메인을 추가하려면 관리 포털에 성공적으로 액세스하여 **Up** 상태인 최소 하나의 호스트에 연결되어 있어야 합니다.

Red Hat Virtualization에는 세 가지 유형의 스토리지 도메인이 있습니다:

- **데이터 도메인:** 데이터 도메인에는 데이터 센터에 있는 모든 가상 머신의 가상 하드 디스크 및 OVF 파일과 템플릿이 저장되어 있습니다. 또한 가상 머신의 스냅샷도 데이터 도메인에 저장되어 있습니다.

데이터 도메인은 데이터 센터에서 공유될 수 없습니다. 여러 유형의 데이터 도메인 (iSCSI, NFS, FC, POSIX, Gluster)을 동일한 데이터 센터에 추가하여 로컬 도메인이 아닌 모든 호스트에서 공유하게 할 수 있습니다.

다른 유형의 도메인을 연결하기 전 데이터 센터에 데이터 도메인을 연결해야 합니다.

- **ISO 도메인:** ISO 도메인에는 가상 머신의 운영 체제 및 애플리케이션을 설치 및 시작하는데 사용하는 ISO 파일 (또는 논리 CD)이 저장되어 있습니다. ISO 도메인에서의 데이터 센터에서는 물리적 미디어가 필요하지 않습니다. ISO 도메인은 다른 데이터 센터에서 공유될 수 있습니다. ISO 도메인은 NFS만을 기반으로 할 수 있습니다. 하나의 ISO 도메인만 데이터 센터에 추가할 수 있습니다.
- **내보내기 도메인:** 내보내기 도메인은 데이터 센터와 Red Hat Virtualization 환경 간의 이미지를 복사 및 이동하는 데 사용되는 임시 스토리지 리포지터리입니다. 내보내기 도메인은 가상 머신을 백업하는 데 사용할 수 있습니다. 내보내기 도메인은 데이터 센터 간에 이동할 수 있지만 한 번에 하나의 데이터 센터에서만 활성화할 수 있습니다. 내보내기 도메인은 NFS만을 기반으로 할 수 있습니다. 하나의 내보내기 도메인만 데이터 센터에 추가할 수 있습니다.



참고

내보내기 스토리지 도메인은 사용되지 않습니다. 스토리지 데이터 도메인을 데이터 센터에서 분리한 후 같은 환경이나 다른 환경의 데이터 센터로 가져오기할 수 있습니다. 그 후에 가상 머신, 플로팅 가상 디스크 이미지, 그리고 템플릿을 가져오기한 스토리지 도메인에서 연결된 데이터 센터로 업로드할 수 있습니다. 스토리지 도메인을 가져오기하는 방법에 대한 자세한 내용은 [8.6절. “기존 스토리지 도메인 가져오기”](#)에서 참조하십시오.



중요

데이터 센터에 필요한 스토리지를 지정한 후 Red Hat Virtualization 환경의 스토리지를 설정 및 연결할 수 있습니다.

8.1. 스토리지 도메인 이해

스토리지 도메인은 일반적인 스토리지 인터페이스가 있는 이미지 모음입니다. 스토리지 도메인에는 템플릿 이미지와 가상 머신 (스냅샷 포함)의 전체 이미지 또는 ISO 파일이 들어 있습니다. 스토리지 도메인은 블록 장치 (SAN - iSCSI 또는 FCP) 또는 파일 시스템 (NAS - NFS, GlusterFS, 또는 기타 다른 POSIX 호환 파일 시스템)이 될 수 있습니다.

NFS에서는 가상 디스크, 템플릿, 스냅샷은 모두 파일입니다.

SAN (iSCSI/FCP)에서는 각 가상 디스크, 템플릿, 스냅샷은 논리 볼륨입니다. 블록 장치는 볼륨 그룹이라는 논리 엔티티로 통합된 후 가상 하드디스크로 사용하기 위해 LVM (Logical Volume Manager)에 의해 논리 볼륨으로 나뉘어 집니다. LVM에 대한 자세한 내용은 *Red Hat Enterprise Linux 논리 볼륨 관리자 관리 가이드*에서 참조하십시오.

가상 디스크는 QCOW2 또는 RAW의 두가지 형식 중 하나를 사용할 수 있습니다. 스토리지 유형은 스파스 또는 사전할당될 수 있습니다. 스냅샷은 항상 스파스 지원을 사용하지만 RAW 또는 스파스에서 생성한 디스크를 사용할 수 있습니다.

동일한 스토리지 도메인을 공유하는 가상 머신은 동일한 클러스터에 속한 호스트 간에 마이그레이션할 수 있습니다.

8.2. NFS 스토리지 준비 및 추가

8.2.1. NFS 스토리지 준비

Red Hat Enterprise Linux 서버에서 데이터 도메인으로 사용할 NFS 공유를 설정합니다. Red Hat Enterprise Virtualization Manager 설치 절차에서 ISO 도메인을 생성한 경우 이를 생성할 필요가 없습니다.



참고

내보내기 스토리지 도메인은 사용되지 않습니다. 스토리지 데이터 도메인을 데이터 센터에서 분리한 후 같은 환경이나 다른 환경의 데이터 센터로 가져오기할 수 있습니다. 그 후에 가상 머신, 플로팅 가상 디스크 이미지, 그리고 템플릿을 가져오기한 스토리지 도메인에서 연결된 데이터 센터로 업로드할 수 있습니다. 스토리지 도메인을 가져오기하는 방법에 대한 자세한 내용은 [8.6절. “기존 스토리지 도메인 가져오기”](#)에서 참조하십시오.

Red Hat Enterprise Linux에서의 NFS 설정에 대한 내용은 *Red Hat Enterprise Linux 6 스토리지 관리 가이드*에 있는 **NFS(네트워크 파일 시스템)** 또는 *Red Hat Enterprise Linux 7 스토리지 관리 가이드*에 있는 **NFS(네트워크 파일 시스템)**를 참조하십시오.

Manager가 내보낸 디렉토리에 의해 표시되는 스토리지 도메인에 데이터를 저장할 수 있도록 특정 시스템 사용자 계정 및 시스템 사용자 그룹이 Red Hat Virtualization에서 필요합니다.

절차 8.1. 필수 시스템 사용자 계정 및 시스템 사용자 그룹 설정

1. 그룹 **kvm**을 생성합니다:

```
# groupadd kvm -g 36
```

2. **kvm** 그룹에 사용자 **vds**를 생성합니다:

```
# useradd vds -u 36 -g 36
```

3. 내보내기된 디렉토리의 소유권을 36:36으로 설정하여 vds:kvm 소유권을 제공합니다.

```
# chown -R 36:36 /exports/data
# chown -R 36:36 /exports/export
```

4. 디렉토리 모드를 변경하여 소유자에게 읽기 및 쓰기 액세스를 허용하고 그룹 및 기타 사용자에게 읽기 및 실행 액세스를 허용합니다:

```
# chmod 0755 /exports/data
# chmod 0755 /exports/export
```

필수 시스템 사용자 및 그룹에 대한 자세한 내용은 [부록 G. 시스템 계정](#)에서 참조하십시오.

8.2.2. NFS 스토리지 연결

NFS 스토리지 도메인을 Red Hat Virtualization 환경에 있는 데이터 센터에 연결합니다. 이러한 스토리지 도메인은 가상 게스트 이미지 및 ISO 부팅 미디어에 대한 스토리지를 제공합니다. 다음 절차에서는 이미 공유가 내보내기되어 있다고 가정합니다. 내보내기 도메인을 생성하기 전 데이터 도메인을 생성해야 합니다. 동일한 절차를 사용하여 내보내기 도메인을 생성하고 **도메인 기능 / 스토리지 유형** 목록에서 **Export / NFS**를 선택합니다.

1. Red Hat Virtualization Manager 관리 포털에서 스토리지 리소스 탭을 클릭합니다.
2. 새로운 도메인을 클릭합니다.

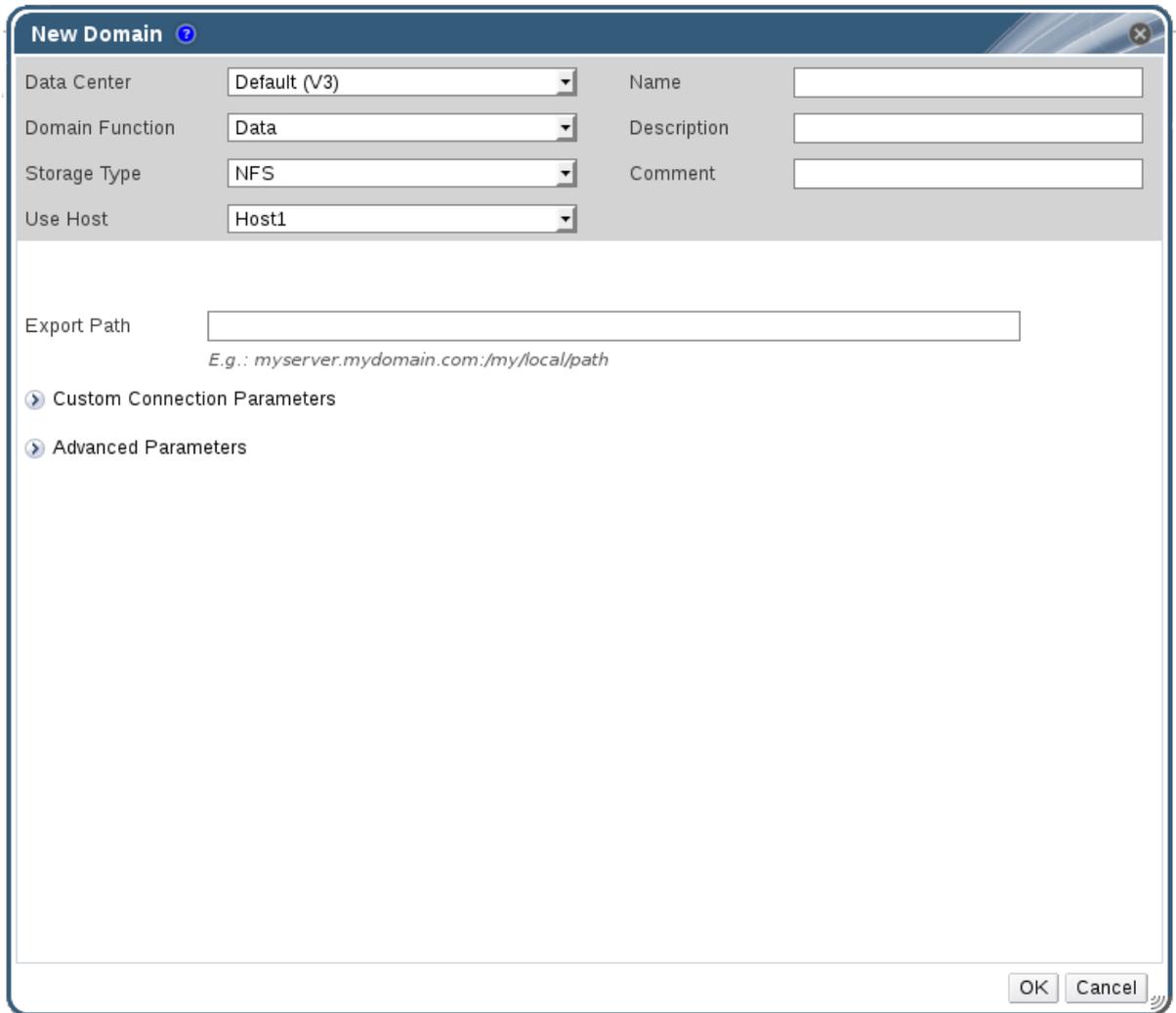


그림 8.1. 새로운 도메인 창

3. 스토리지 도메인의 이름을 입력합니다.
4. 데이터 센터, 도메인 기능, 스토리지 유형, 포맷, 및 사용 호스트 목록의 기본 값을 허용합니다.
5. 스토리지 도메인에 사용할 내보내기 경로를 입력합니다.

내보내기 경로는 `192.168.0.10:/data` 또는 `domain.example.com:/data` 형식이어야 합니다.

6. 옵션으로 고급 매개 변수를 설정할 수 있습니다.
 - a. 고급 매개 변수를 클릭합니다.
 - b. 디스크 공간 부족 경고 표시 필드에 백분율 값을 입력합니다. 스토리지 도메인에서 사용 가능한 여유 공간이 이러한 백분율 값 아래로 내려가면 사용자에게 경고 메시지가 표시되고 기록됩니다.
 - c. 심각히 부족한 디스크 공간에서 동작 차단 필드에 GB 단위로 값을 입력합니다. 스토리지 도메인에서 사용 가능한 여유 공간이 이 값 아래로 내려가면 사용자에게 오류 메시지가 표시되고 기록되며 공간을 소비하는 모든 새로운 동작은 일시적이라도 모두 차단됩니다.
 - d. 삭제 후 초기화 확인란을 선택하여 삭제 후 초기화 옵션을 활성화합니다. 이 옵션은 도메인 생성 후 편집할 수 있지만 이러한 경우 이미 존재하는 디스크의 삭제 후 초기화 속성은 변경되지 않습니다.

7. OK를 클릭합니다.

새로운 NFS 데이터 도메인은 스토리지 탭에 표시되며 디스크가 준비되기 전 까지 **Locked** 상태로 있습니다. 그 후 데이터 도메인은 데이터 센터에 자동으로 연결됩니다.

8.2.3. NFS 스토리지 확장

NFS 스토리지 양을 확장하려면 새 스토리지 도메인을 생성하거나 기존 데이터 센터에 이를 추가하거나 NFS 서버에서 사용 가능한 여유 공간을 늘립니다. 첫 번째 옵션의 경우 8.2.2절. “NFS 스토리지 연결”에서 참조하십시오. 다음 절차에서는 기존 NFS 서버에서 사용 가능한 여유 공간을 늘리는 방법에 대해 설명합니다.

절차 8.2. 기존 NFS 스토리지 도메인 확장

1. 스토리지 리소스 탭을 클릭하고 NFS 스토리지 도메인을 선택합니다.
2. 상세 정보 창에서 데이터 센터 탭을 클릭하고 유지 관리 버튼을 클릭하여 스토리지 도메인을 유지 관리 모드로 변경합니다. 이는 기존 공유를 마운트 해제하고 스토리지 도메인 크기를 변경할 수 있게 합니다.
3. NFS 서버에서 스토리지 크기를 변경합니다. Red Hat Enterprise Linux 6 시스템의 경우 Red Hat Enterprise Linux 6 스토리지 관리 가이드에서 참조하십시오. Red Hat Enterprise Linux 7 시스템의 경우 Red Hat Enterprise Linux 7 스토리지 관리 가이드에서 참조하십시오.
4. 상세 정보 창에서 데이터 센터 탭을 클릭하고 활성화 버튼을 클릭하여 스토리지 도메인을 마운트합니다.

8.3. 로컬 스토리지 준비 및 추가

8.3.1. 로컬 스토리지 준비

로컬 스토리지 도메인을 호스트에 설정할 수 있습니다. 로컬 스토리지를 사용하기 위해 호스트 설정 시 호스트는 다른 호스트를 추가할 수 없는 새로운 데이터 센터 및 클러스터에 자동으로 추가됩니다. 여러 호스트 클러스터에서는 모든 호스트가 모든 스토리지 도메인으로 액세스할 수 있어야 하며 이는 로컬 스토리지는 불가능합니다. 단일 호스트 클러스터에 생성된 가상 머신은 마이그레이션, 펜싱, 스케줄링할 수 없습니다. 필요한 시스템 사용자와 그룹에 대한 보다 자세한 내용은 부록 G. 시스템 계정에서 참조하십시오.



참고

Red Hat Virtualization Host(RHVM)를 다시 설치할 때 로컬 스토리지 도메인을 보존하는 방법에 대한 자세한 내용은 <https://access.redhat.com/solutions/2804081>을 참조하십시오.



중요

Red Hat Virtualization Host(RHVM)에서 로컬 스토리지에 사용되는 경로는 /var 디렉토리에 있어야 합니다. 다음의 절차에 따라 /var 내에서 스토리지 디렉토리를 생성합니다.

절차 8.3. 로컬 스토리지 준비

1. 호스트에서 로컬 스토리지에 사용할 디렉토리를 생성합니다.

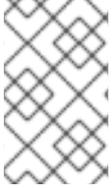
```
# mkdir -p /data/images
```

2. 디렉토리에서 **vdsm** 사용자 (UID 36) 및 **kvm** 그룹 (GID 36)에 대한 읽기/쓰기 액세스를 허용하는 권한을 설정합니다.

```
# chown 36:36 /data /data/images
```

```
# chmod 0755 /data /data/images
```

로컬 스토리지를 Red Hat Virtualization 환경에 추가할 준비가 되어 있습니다.



참고

로컬 스토리지 도메인으로 사용하기 위해서 호스트 머신에 외부 스토리지를 마운트할 수도 있습니다. 스토리지 마운트에 대한 보다 자세한 내용은 [Red Hat Enterprise Linux Storage Administration Guide](#)에서 참조하십시오.

8.3.2. 로컬 스토리지 추가

호스트의 로컬 스토리지가 준비되었습니다. 이제 **Manager**를 사용하여 스토리지를 호스트에 추가합니다.

호스트에 로컬 스토리지를 추가하면 호스트는 새로운 데이터 센터 및 클러스터에 배치됩니다. 로컬 스토리지 설정 창에서는 데이터 센터, 클러스터, 스토리지 생성을 단일 프로세스로 통합합니다.

절차 8.4. 로컬 스토리지 추가

1. **호스트 리소스 탭**을 클릭하여 결과 목록에서 호스트를 선택합니다.
2. **유지 관리**를 클릭하면 **호스트 유지 관리 확인** 창이 열립니다.
3. **OK**를 클릭하여 유지 관리 모드를 시작합니다.
4. **로컬 스토리지 설정** 버튼을 클릭하여 **로컬 스토리지 설정** 창을 엽니다.

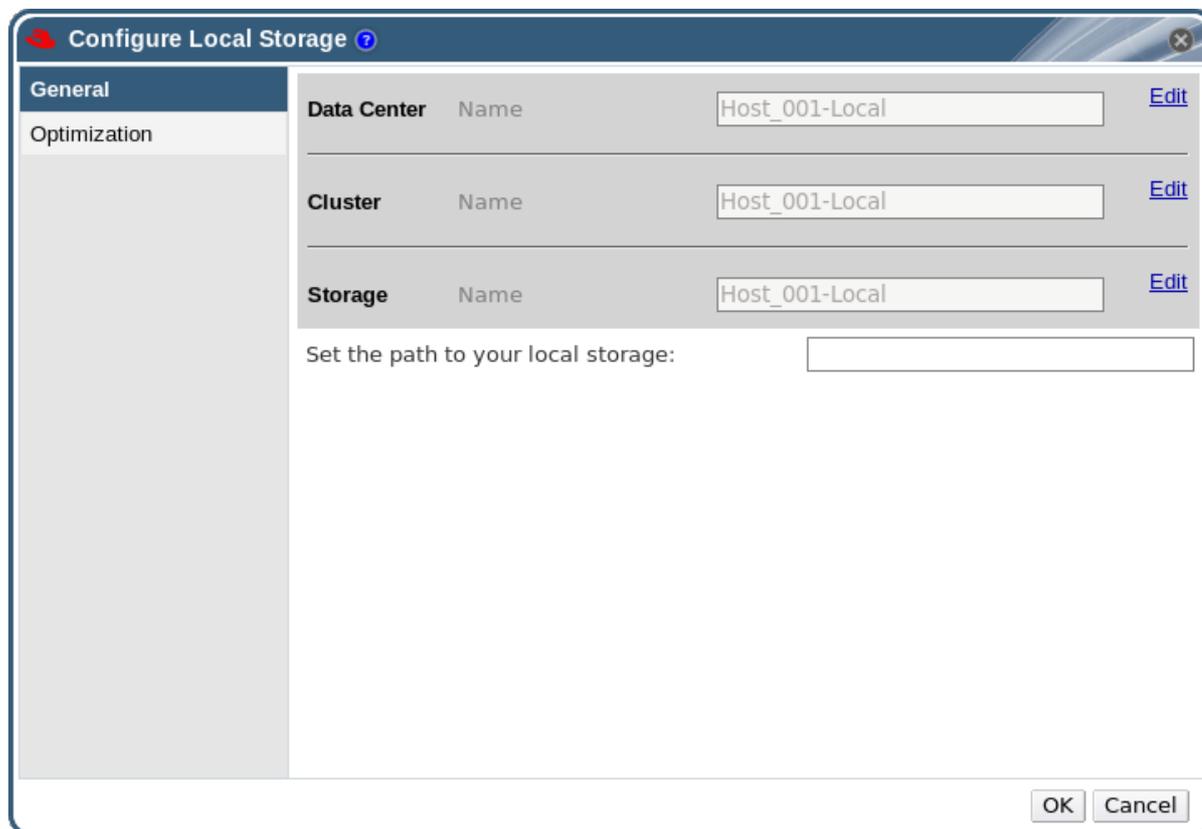


그림 8.2. 로컬 스토리지 설정 창

5. 데이터 센터, 클러스터, 스토리지 옆에 있는 편집 버튼을 클릭하여 로컬 스토리지 도메인을 설정하고 이름을 지정합니다.
6. 텍스트 입력 필드에 로컬 스토리지 경로를 설정합니다.
7. 최적화 탭을 선택하여 새 로컬 스토리지 클러스터에 대한 메모리 최적화 정책을 설정합니다.
8. **OK**를 클릭하여 설정을 저장하고 창을 닫습니다.

호스트는 자체 데이터 센터에서 온라인 상태로 표시됩니다.

8.4. POSIX 호환 파일 시스템 스토리지 추가

POSIX 파일 시스템 지원에서는 명령행에서 수동으로 마운트할 때 사용하는 것과 동일한 마운트 옵션을 사용하여 파일 시스템을 마운트할 수 있습니다. 이 기능은 NFS, iSCSI, FCP를 사용하여 마운트되지 않는 스토리지에 액세스할 수 있도록 하려는 것입니다.

Red Hat Virtualization에서 스토리지 도메인으로 사용하는 POSIX 호환 파일 시스템은 스파스 파일 및 직접 I/O를 지원해야 합니다. 예를 들어 CIFS (Common Internet File System)은 직접 I/O를 지원하지 않기 때문에 Red Hat Virtualization과 호환성이 없습니다.



중요

POSIX 호환 파일 시스템 스토리지 도메인을 생성하여 NFS 스토리지를 마운트하지 않습니다. 대신 NFS 스토리지 도메인을 생성합니다.

8.4.1. POSIX 호환 파일 시스템 스토리지 연결

NFS, iSCSI, FCP를 사용하여 표시되지 않은 POSIX 호환 파일 시스템을 스토리지 도메인으로 사용합니다.

절차 8.5. POSIX 호환 파일 시스템 스토리지 연결

1. 스토리지 리소스 탭을 클릭하면 결과 목록에 기존 스토리지 도메인 목록이 표시됩니다.
2. 새로운 도메인을 클릭하면 새로운 도메인 창이 열립니다.

그림 8.3. POSIX 스토리지

3. 스토리지 도메인의 이름을 입력합니다.
4. 스토리지 도메인과 관련된 데이터 센터를 선택합니다. 선택한 데이터 센터의 유형은 **POSIX (POSIX compliant FS)** 이어야 합니다. 또는 **(none)** 을 선택합니다.
5. 도메인 기능 / 스토리지 유형 드롭 다운 메뉴에서 **Data / POSIX compliant FS**를 선택합니다.

해당하는 경우 드롭 다운 메뉴에서 포맷을 선택합니다.

6. 사용하는 호스트 드롭 다운 메뉴에서 호스트를 선택합니다. 선택한 데이터 내에 호스트만 표시됩니다. 선택한 호스트를 사용하여 스토리지 도메인에 연결합니다.
7. **mount** 명령에 지정하는 것 처럼 POSIX 파일 시스템에 경로를 입력합니다.

8. **-t** 인수를 사용하여 **mount** 명령에 지정하는 것 처럼 **VFS 유형**을 입력합니다. 유효한 **VFS** 유형 목록은 **man mount**에서 확인하십시오.
9. **-o** 인수를 사용하여 **mount** 명령에 지정하는 것 처럼 **추가마운트 옵션**을 입력합니다. 마운트 옵션은 콤마로 구분합니다. 유효한 마운트 옵션 목록은 **man mount**에서 확인하십시오.
10. 옵션으로 고급 매개 변수를 설정할 수 있습니다.
 - a. **고급 매개 변수**를 클릭합니다.
 - b. **디스크 공간 부족 경고 표시 필드**에 백분율 값을 입력합니다. 스토리지 도메인에서 사용 가능한 여유 공간이 이러한 백분율 값 아래로 내려가면 사용자에게 경고 메시지가 표시되고 기록됩니다.
 - c. **심각히 부족한 디스크 공간에서 동작 차단 필드**에 **GB** 단위로 값을 입력합니다. 스토리지 도메인에서 사용 가능한 여유 공간이 이 값 아래로 내려가면 사용자에게 오류 메시지가 표시되고 기록되며 공간을 소비하는 모든 새로운 동작은 일시적이라도 모두 차단됩니다.
 - d. **삭제 후 초기화 확인란**을 선택하여 삭제 후 초기화 옵션을 활성화합니다. 이 옵션은 도메인 생성 후 편집할 수 있지만 이러한 경우 이미 존재하는 디스크의 삭제 후 초기화 속성은 변경되지 않습니다.
11. **OK**를 클릭하여 새 스토리지 도메인을 연결한 후 창을 닫습니다.

8.5. 블록 스토리지 추가

8.5.1. iSCSI 스토리지 추가

Red Hat Virtualization은 기존의 LUN으로 구성된 볼륨 그룹에서 스토리지 도메인을 생성하여 iSCSI 스토리지를 지원합니다. 볼륨 그룹 및 LUN은 모두 한 번에 여러 스토리지 도메인에 연결할 수 없습니다.

Red Hat Enterprise Linux에서 iSCSI를 설정하는 방법에 대한 자세한 내용은 *Red Hat Enterprise Linux 6 스토리지 관리 가이드*에 있는 [iSCSI 대상 생성](#) 또는 *Red Hat Enterprise Linux 7 스토리지 관리 가이드*에 있는 [온라인 스토리지 관리](#)를 참조하십시오.

절차 8.6. iSCSI 스토리지 추가

1. 스토리지 리소스 탭을 클릭하면 결과 목록에 기존 스토리지 도메인 목록이 표시됩니다.
2. **새로운 도메인** 버튼을 클릭하면 **새로운 도메인** 창이 열립니다.
3. 새 스토리지 도메인의 **이름**을 입력합니다.

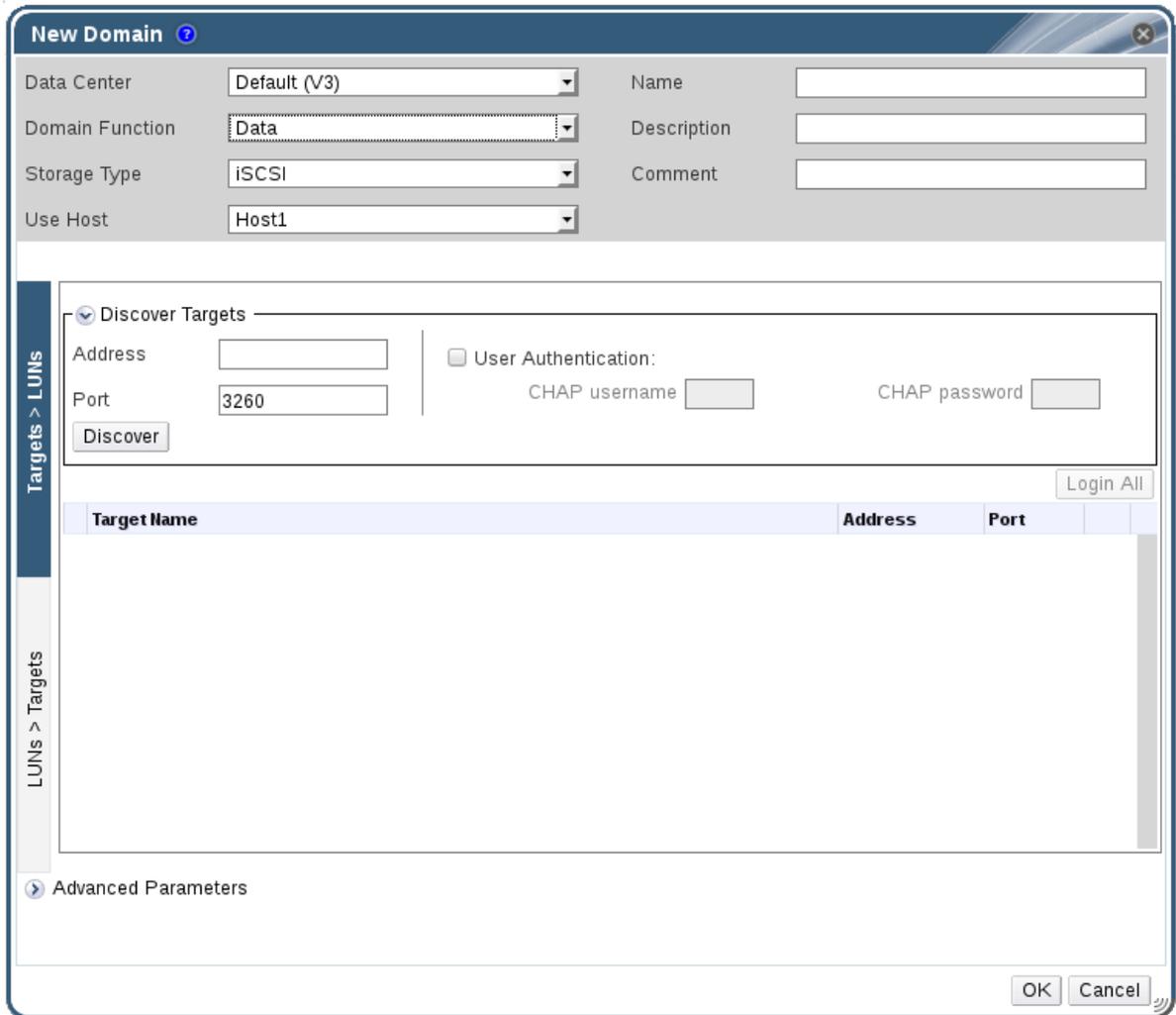


그림 8.4. 새 iSCSI 도메인

4. 데이터 센터 드롭 다운 메뉴에서 데이터 센터를 선택합니다.
5. 드롭 다운 메뉴를 사용하여 도메인 기능 및 스토리지 유형을 선택합니다. 선택한 도메인 기능과 호환되지 않는 스토리지 도메인 유형은 사용할 수 없습니다.
6. 사용 호스트란에 활성 호스트를 선택합니다. 데이터 센터에 있는 첫 번째 데이터 도메인이 아닐 경우 데이터 센터의 SPM 호스트를 선택해야 합니다.



중요

스토리지 도메인에서의 모든 통신은 Red Hat Virtualization Manager에서 직접 이루어지는 것이 아니라 선택한 호스트를 통해 이루어집니다. 시스템에 최소한 하나의 활성 호스트가 존재해야 하며 선택한 데이터 센터에 연결되어 있어야 합니다. 모든 호스트는 스토리지 도메인을 설정하기 전 스토리지 장치에 액세스할 수 있어야 합니다.

7. Red Hat Virtualization Manager는 iSCSI 대상을 LUN으로 또는 LUN을 iSCSI 대상으로 매핑할 수 있습니다. 스토리지 유형으로 iSCSI가 선택되어 있을 경우 새로운 도메인 창에는 사용하지 않는 LUN이 있는 알려진 대상이 자동으로 표시됩니다. 스토리지를 추가하려는 대상이 목록에 없을 경우 대상 검색을 사용하여 검색할 수 있습니다. 대상이 목록에 있을 경우 다음 단계를 진행합니다.

iSCSI 대상 검색

1. **대상 검색**을 클릭하여 대상 검색 옵션을 활성화합니다. 대상이 검색되어 로그인하면**새로운 도메인** 창에 환경에서 사용하지 않는**LUN**이 있는 대상이 자동으로 표시됩니다.



참고

환경 외부에서 사용되는 **LUN**도 표시됩니다.

대상 검색 옵션을 사용하여 여러 대상에 **LUN**을 추가하거나 동일한 **UN**에 여러 경로를 추가할 수 있습니다.

2. 주소란에 **iSCSI** 호스트의 **IP** 주소 또는 정규화된 도메인 이름을 입력합니다.
3. 포트란에서 대상을 검색할 때 호스트에 연결할 포트를 입력합니다. 기본값은**3260**입니다.
4. 스토리지 보안을 위해 **CHAP (Challenge Handshake Authentication Protocol)**을 사용할 경우 **사용자 인증** 확인란을 선택합니다. **CHAP 사용자 이름** 및 **CHAP 암호**를 입력합니다.



참고

이제 **REST API**를 사용하여 호스트별로 각 **iSCSI** 대상에 특정 인증 정보를 정의할 수 있습니다. 자세한 내용은 **REST API 가이드**에 있는 **iSCSI 대상에 인증 정보 정의**를 참조하십시오.

5. 검색 버튼을 클릭합니다.
6. 검색 결과에서 사용할 대상을 선택하고 **로그인** 버튼을 클릭합니다.

다른 방법으로 **전체 로그인**을 선택하여 검색된 대상 모두에 로그인합니다.



중요

하나 이상의 경로 액세스가 필요한 경우 모든 필요한 경로를 통해 대상을 찾아서 로그인합니다. 스토리지 도메인을 수정해서 경로를 추가하는 것은 현재 지원되지 않습니다.

8. 원하는 대상 옆에 있는 **+** 버튼을 클릭합니다. 이는 항목을 펼치기하여 대상에 연결된 사용되지 않는 모든 **LUN**을 표시합니다.
9. 스토리지 도메인을 생성하기 위해 사용하려는 각 **LUN**의 확인란을 선택합니다.
10. 옵션으로 고급 매개 변수를 설정할 수 있습니다.
 - a. **고급 매개 변수**를 클릭합니다.
 - b. **디스크 공간 부족 경고 표시** 필드에 백분율 값을 입력합니다. 스토리지 도메인에서 사용 가능한 여유 공간이 이러한 백분율 값 아래로 내려가면 사용자에게 경고 메시지가 표시되고 기록됩니다.
 - c. **심각히 부족한 디스크 공간에서 동작 차단** 필드에 **GB** 단위로 값을 입력합니다. 스토리지 도메인에서 사용 가능한 여유 공간이 이 값 아래로 내려가면 사용자에게 오류 메시지가 표시되고 기록되며 공간을 소비하는 모든 새로운 동작은 일시적이라도 모두 차단됩니다.

- d. **삭제 후 초기화** 확인란을 선택하여 삭제 후 초기화 옵션을 활성화합니다. 이 옵션은 도메인 생성 후 편집할 수 있지만 이러한 경우 이미 존재하는 디스크의 삭제 후 초기화 속성은 변경되지 않습니다.
- e. **삭제 후 폐기** 확인란을 선택하여 삭제 후 폐기 옵션을 활성화합니다. 이 옵션은 도메인 생성 후 편집할 수 있으며 스토리지 도메인을 차단하는 데에만 사용할 수 있습니다.

11. **OK**를 클릭하여 스토리지 도메인을 생성하고 창을 닫습니다.

같은 대상에 여러 개의 스토리지 연결을 설정한 경우 [8.5.2절. “iSCSI 멀티패스 설정”](#)에 있는 절차를 사용하여 iSCSI 본딩을 완료합니다.

8.5.2. iSCSI 멀티패스 설정

iSCSI 멀티패스를 사용하여 논리 네트워크 그룹과 iSCSI 스토리지 연결을 생성 및 관리합니다. 네트워크 경로에 장애 발생 시 호스트 가동 중지 상태가 되지 않도록 하기 위해 호스트와 iSCSI 스토리지 간에 여러 개의 네트워크 경로를 설정합니다. 설정 후 **Manager**는 같은 iSCSI 본딩의 논리 네트워크 관련 **NIC/VLAN**을 통해 데이터 센터의 각 호스트를 본딩이 된 각각의 대상에 연결합니다. 호스트가 기본 네트워크를 통해 트래픽을 라우팅하도록 허용하지 않고 사용자가 스토리지 트래픽에 사용될 네트워크를 지정할 수도 있습니다. 이 옵션은 최소한 하나의 iSCSI 스토리지 도메인이 데이터 센터에 연결된 후 관리 포털에서만 사용 가능합니다.

전제 조건

- iSCSI 스토리지 도메인이 생성되었으며 모든 iSCSI 대상 경로에 로그인했는지 확인합니다.
- iSCSI 스토리지 연결과 본딩할 **필수가 아닌** 논리 네트워크가 생성되었는지 확인합니다. 여러 개의 논리 네트워크 또는 본드 네트워크가 네트워크 장애 조치를 허용하도록 설정할 수 있습니다.

절차 8.7. iSCSI 멀티패스 설정

1. **데이터 센터** 탭을 클릭하여 검색 결과 목록에서 데이터 센터를 선택합니다.
2. 상세 정보 창에서 **iSCSI 멀티패스** 탭을 클릭합니다.
3. **추가**를 클릭합니다.
4. **iSCSI 본딩 추가** 창에서 본딩의 **이름** 및 **설명**을 입력합니다.
5. **논리 네트워크** 목록에서 본딩에 사용할 네트워크를 선택합니다. 해당 네트워크는 **필수가 아닌** 네트워크여야 합니다.



참고

네트워크의 **필수** 대상을 변경하려면 관리 포털에서 네트워크 선택 후 **클러스터** 탭을 클릭하고 **네트워크 관리** 버튼을 클릭합니다.

6. **스토리지 대상** 목록에서 선택한 네트워크를 통해 액세스할 스토리지 도메인을 선택합니다. 같은 대상의 모든 경로를 선택합니다.
7. **OK**를 클릭합니다.

데이터 센터에 있는 모든 호스트는 선택한 논리 네트워크를 통해 선택한 iSCSI 대상에 연결됩니다.

8.5.3. FCP 스토리지 추가

Red Hat Virtualization 플랫폼은 기존의 LUN에서 만들어진 볼륨 그룹에서 스토리지 도메인을 생성하여 SAN 스토리지를 지원합니다. 볼륨 그룹이나 LUN 모두 동시에 여러 스토리지 도메인에 연결할 수 없습니다.

Red Hat Virtualization 시스템 관리자는 SAN (Storage Area Networks) 개념에 대한 작업 지식이 필요합니다. 일반적으로 SAN은 호스트와 외부 공유 스토리지 간의 트래픽에 대해 FCP(Fibre Channel Protocol)를 사용합니다. 이러한 이유로 SAN은 FCP 스토리지라고도 합니다.

Red Hat Enterprise Linux에서 FCP 또는 멀티패스 설정에 대한 보다 자세한 내용은 [Storage Administration Guide](#) 및 [DM Multipath 가이드](#)에서 참조하십시오.

다음 절차에서는 데이터 도메인으로 Red Hat Virtualization 환경에 기존 FCP 스토리지를 연결하는 방법에 대해 설명합니다. 기타 다른 지원 스토리지 유형에 대한 보다 자세한 내용은 [8장. 스토리지](#)에서 참조하십시오.

절차 8.8. FCP 스토리지 추가

1. 스토리지 리소스 탭을 클릭하면 모든 스토리지 도메인 목록이 표시됩니다.
2. 새로운 도메인을 클릭하면 새로운 도메인 창이 열립니다.
3. 스토리지 도메인의 이름을 입력합니다.

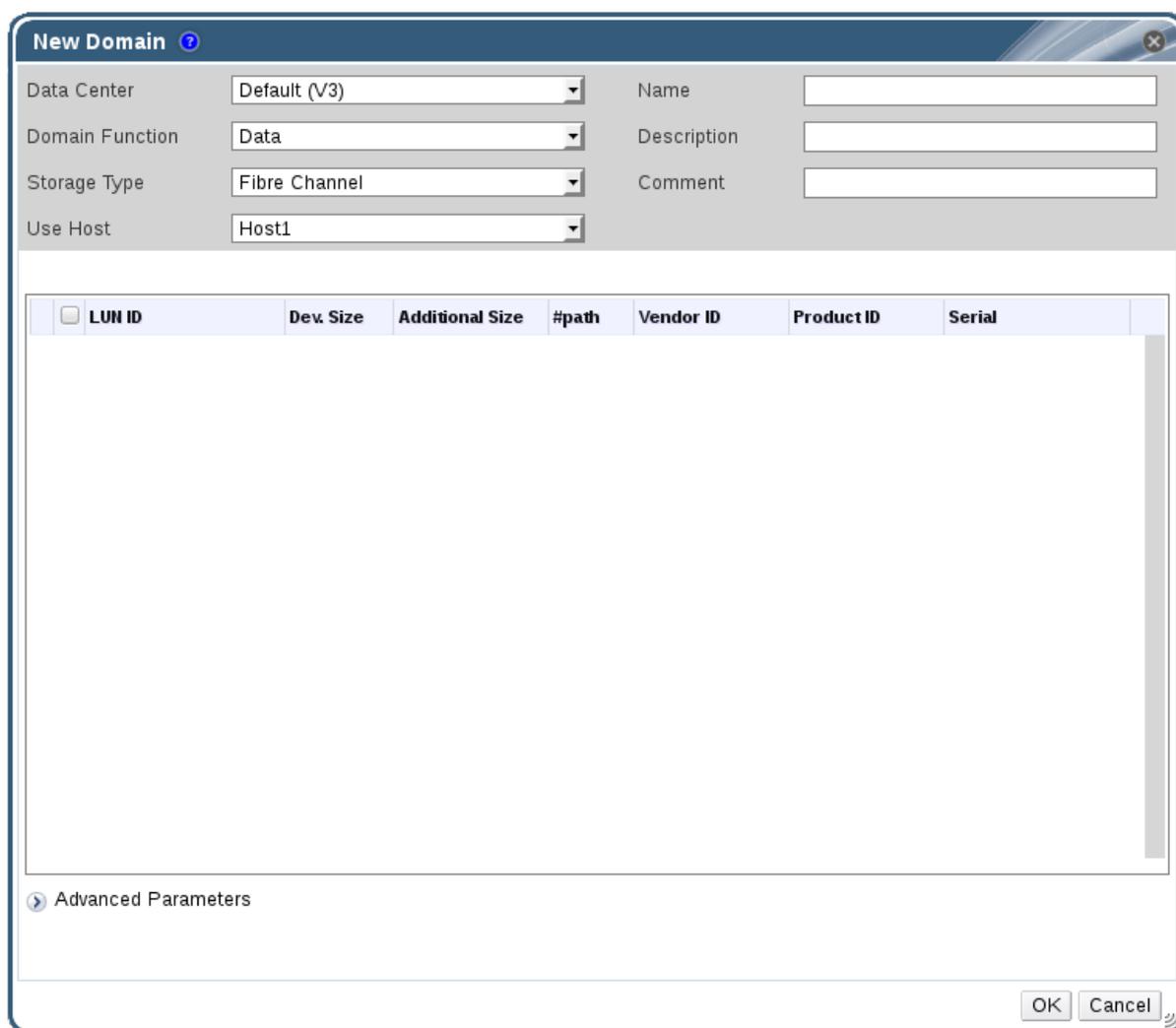


그림 8.5. FCP 스토리지 추가

4. 데이터 센터 드롭 다운 메뉴에서 FCP 데이터 센터를 선택합니다.

적절한 FCP 데이터 센터가 없을 경우 (**없음**)을 선택합니다.

5. 드롭 다운 메뉴를 사용하여 **도메인 기능 및 스토리지 유형**을 선택합니다. 선택한 데이터 센터와 호환되지 않는 스토리지 도메인 유형은 사용할 수 없습니다.
6. **사용 호스트**란에 활성 호스트를 선택합니다. 데이터 센터에 있는 첫 번째 데이터 도메인이 아닐 경우 데이터 센터의 **SPM** 호스트를 선택해야 합니다.



중요

스토리지 도메인에서의 모든 통신은 **Red Hat Virtualization Manager**에서 직접 이루어지는 것이 아니라 선택한 호스트를 통해 이루어집니다. 시스템에 최소한 하나의 활성 호스트가 존재해야 하며 선택한 데이터 센터에 연결되어 있어야 합니다. 모든 호스트는 스토리지 도메인을 설정하기 전 스토리지 장치에 액세스할 수 있어야 합니다.

7. 스토리지 유형으로 **Data / Fibre Channel**이 선택되어 있을 때 **새로운 도메인** 창에는 사용하지 않는 LUN과 함께 알려진 대상이 자동으로 표시됩니다. **LUN ID** 확인란을 선택하여 사용 가능한 모든 LUN을 선택합니다.
8. 옵션으로 고급 매개 변수를 설정할 수 있습니다.
 - a. **고급 매개 변수**를 클릭합니다.
 - b. **디스크 공간 부족 경고 표시** 필드에 백분율 값을 입력합니다. 스토리지 도메인에서 사용 가능한 여유 공간이 이러한 백분율 값 아래로 내려가면 사용자에게 경고 메시지가 표시되고 기록됩니다.
 - c. **심각히 부족한 디스크 공간의 동작 차단** 필드에 **GB** 단위로 값을 입력합니다. 스토리지 도메인에서 사용 가능한 여유 공간이 이 값 아래로 내려가면 사용자에게 오류 메시지가 표시되고 기록되며 공간을 소비하는 모든 새로운 동작은 일시적이라도 모두 차단됩니다.
 - d. **삭제 후 초기화** 확인란을 선택하여 삭제 후 초기화 옵션을 활성화합니다. 이 옵션은 도메인 생성 후 편집할 수 있지만 이러한 경우 이미 존재하는 디스크의 삭제 후 초기화 속성은 변경되지 않습니다.
 - e. **삭제 후 폐기** 확인란을 선택하여 삭제 후 폐기 옵션을 활성화합니다. 이 옵션은 도메인 생성 후 편집할 수 있으며 스토리지 도메인을 차단하는 데에만 사용할 수 있습니다.
9. **OK**를 클릭하여 스토리지 도메인을 생성하고 창을 닫습니다.

새로운 FCP 데이터 도메인이 **스토리지** 탭에 표시됩니다. 이는 사용 준비될 때 까지 **Locked** 상태로 되어 있습니다. 사용 준비되면 이는 자동으로 데이터 센터에 연결됩니다.

8.5.4. iSCSI 또는 FCP 스토리지 확장

iSCSI 또는 FCP 스토리지를 확장하는 방법은 여러 가지 있습니다:

- 새 LUN으로 새로운 스토리지 도메인을 생성하고 이를 기존 데이터 센터에 추가합니다. **8.5.1절. "iSCSI 스토리지 추가"**를 참조하시기 바랍니다.
- 새로운 LUN을 생성하고 이를 기존 데이터 센터에 추가합니다.
- 기본 LUN 크기를 변경하여 스토리지 도메인을 확장합니다.

Red Hat Enterprise Linux 6 시스템에서 iSCSI 스토리지 생성, 설정, 또는 크기 변경하는 방법에 대한

자세한 내용은 [Red Hat Enterprise Linux 6 스토리지 관리 가이드](#)에서 참조하십시오. Red Hat Enterprise Linux 7 시스템의 경우 [Red Hat Enterprise Linux 7 스토리지 관리 가이드](#)에서 참조하십시오.

다음 절차에서는 새 LUN을 기존 스토리지 도메인에 추가하여 SAN (storage area network) 스토리지를 확장하는 방법에 대해 설명합니다.

절차 8.9. 기존 iSCSI 또는 FCP 스토리지 도메인 확장

1. SAN에 새로운 LUN을 생성합니다.
2. 스토리지 리소스 탭을 클릭하고 iSCSI 또는 FCP 스토리지 도메인을 선택합니다.
3. 도메인 관리 버튼을 클릭합니다.
4. 대상 > LUN을 클릭하고 대상 검색 확장 버튼을 클릭합니다.
5. 스토리지 서버의 연결 정보를 입력하고 검색 버튼을 클릭하여 연결을 시작합니다.
6. LUN > 대상을 클릭하고 새로 사용 가능한 LUN 체크 상자를 선택합니다.
7. OK를 클릭하여 LUN을 선택한 스토리지 도메인에 추가합니다.

추가된 LUN 크기에 따라 스토리지 도메인이 확장됩니다.

기본 LUN 크기를 변경하여 스토리지 도메인을 확장하는 경우 해당 LUN이 Red Hat Virtualization 관리 포털에서도 새로고침되어야 합니다.

절차 8.10. LUN 크기 새로고침

1. 스토리지 리소스 탭을 클릭하고 iSCSI 또는 FCP 스토리지 도메인을 선택합니다.
2. 도메인 관리 버튼을 클릭합니다.
3. LUN > 대상을 클릭합니다.
4. 추가 크기 열에서 해당 LUN의 추가 **Additional_Storage_Size** 버튼을 눌러서 새로고침합니다.
5. OK를 클릭하여 LUN을 새로고침해서 변경된 스토리지 크기를 표시합니다.

8.5.5. Red Hat Virtualization에서 사용할 수 없는 LUN

경우에 따라서 Red Hat Virtualization Manager는 스토리지 도메인이나 가상 머신 하드 디스크를 생성하는데 LUN을 사용하는 것을 허용하지 않습니다.

- 현재 Red Hat Virtualization 환경의 부분인 LUN은 사용되지 않도록 자동 설정되어 있습니다.

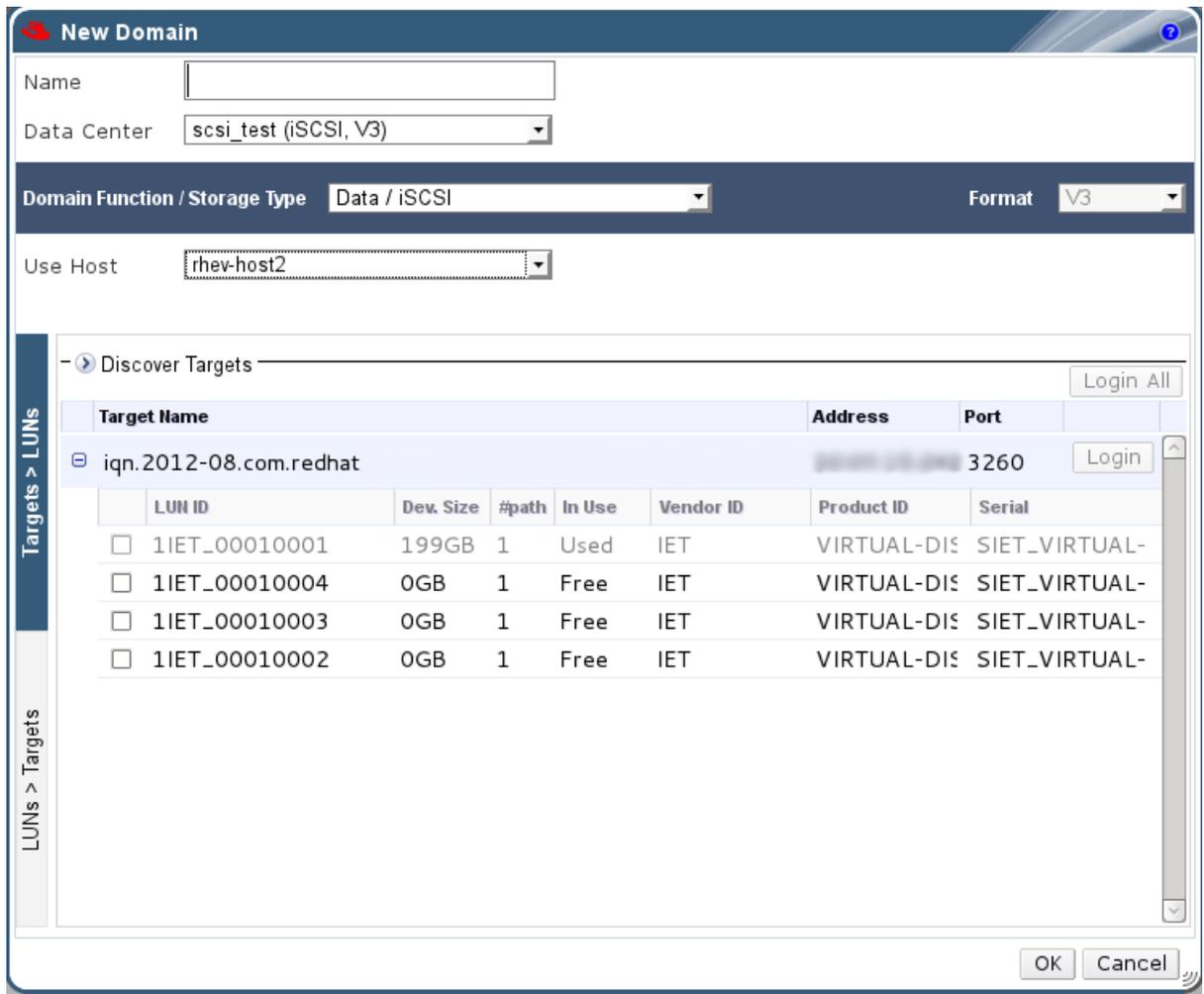


그림 8.6. Red Hat Virtualization 관리 포털에서 사용할 수 없는 LUN

- SPM 호스트에 의해 사용되고 있는 LUN은 사용 중인 상태로 표시됩니다. 이러한 LUN의 콘텐츠를 강제로 덮어쓰기하도록 선택할 수 있지만 작업이 성공적으로 동작할지는 확실하지 않습니다.

8.6. 기존 스토리지 도메인 가져오기

8.6.1. 기존 스토리지 도메인 가져오기에 대한 개요

데이터가 들어 있지 않은 새로운 스토리지 도메인을 추가할 수 있음은 물론 기존 스토리지 도메인을 가져오기하여 그 안에 저장된 데이터에 액세스할 수 있습니다. 스토리지 도메인 가져오기 기능을 통해 **Manager** 데이터베이스에 오류 발생 시 데이터를 복구하여 데이터 센터 또는 환경 간에 데이터를 마이그레이션할 수 있습니다.

각 스토리지 도메인 유형 가져오기에 대한 개요는 다음과 같습니다:

데이터

기존 데이터 스토리지 도메인 가져오기를 통해 데이터 스토리지 도메인이 들어있는 모든 가상 머신 및 템플릿에 액세스할 수 있습니다. 스토리지 도메인을 가져오기한 후 가상 머신, 플로팅 디스크 이미지, 그리고 템플릿을 대상 데이터 센터에 수동으로 가져오기해야 합니다. 데이터 스토리지 도메인에 저장된 가상 머신 및 템플릿을 가져오기위한 절차는 스토리지 도메인 내보내기 절차와 유사합니다. 하지만 데이터 스토리지 도메인에는 지정된 데이터 센터에 모든 가상 머신 및 템플릿이 들어 있기 때문에 데이터 복구 또는 데이터 센터나 환경 사이의 대규모 가상 머신 마이그레이션의 경우 데이터 스토리지 도메인을 가져오기하는 것이 좋습니다.



중요

호환성 수준 3.5 이상의 데이터 센터에 연결된 기존 데이터 스토리지 도메인만 가져올 수 있습니다.

ISO

기존 ISO 스토리지 도메인 가져오기를 통해 ISO 스토리지 도메인이 포함된 모든 ISO 파일 및 가상 디스크에 액세스할 수 있습니다. 스토리지 도메인을 가져온 후 리소스에 액세스하기 위한 추가 작업이 필요하지 않으므로 필요에 따라 가상 머신에 연결할 수 있습니다.

내보내기

기존 내보내기 스토리지 도메인을 가져오면 내보내기 스토리지 도메인에 포함된 모든 가상 머신 이미지와 템플릿에 액세스할 수 있습니다. 내보내기 도메인은 가상 머신 이미지 및 템플릿의 내보내기 및 가져오기를 위해 설계되어 있으므로 환경 내에서 또는 환경 간에 적은 수의 가상 머신 및 템플릿을 마이그레이션하는 데에는 내보내기 스토리지 도메인을 가져오는 방식을 사용하는 것이 좋습니다. 내보내기 스토리지 도메인에서 가상 머신 및 템플릿을 내보내고 가져오는 방법에 대한 자세한 내용은 [가상 머신 관리 가이드](#)에 있는 [가상 머신 및 템플릿 내보내기 및 가져오기](#)를 참조하십시오.



참고

내보내기 스토리지 도메인은 사용되지 않습니다. 스토리지 데이터 도메인을 데이터 센터에서 분리한 후 같은 환경이나 다른 환경의 데이터 센터로 가져오기할 수 있습니다. 그 후에 가상 머신, 플로팅 가상 디스크 이미지, 그리고 템플릿을 가져오기한 스토리지 도메인에서 연결된 데이터 센터로 업로드할 수 있습니다.

8.6.2. 스토리지 도메인 가져오기

동일한 환경 또는 다른 환경에 있는 데이터 센터에 이전에 연결된 스토리지 도메인을 가져옵니다. 다음 절차에서는 데이터 손상을 막기 위해 스토리지 도메인이 더 이상 환경에 있는 데이터 센터에 연결되어 있지 않다고 간주합니다. 데이터 센터에 기존 데이터 스토리지를 가져오기 및 연결하려면 가져오기 대상 데이터 센터를 초기화해야 합니다.

절차 8.11. 스토리지 도메인 가져오기

1. 스토리지 리소스 탭을 클릭합니다.
2. 도메인 가져오기를 클릭합니다.

그림 8.7. 사전 설정된 도메인 가져오기 창

3. 데이터 센터 드롭 다운 목록에서 스토리지 도메인을 연결하는 데이터 센터를 선택합니다.
4. 스토리지 도메인의 이름을 입력합니다.
5. 도메인 기능 및 스토리지 유형 드롭 다운 목록에서 적절한 항목을 선택합니다.
6. 사용 호스트 드롭 다운 목록에서 호스트를 선택합니다.



중요

스토리지 도메인에서의 모든 통신은 Red Hat Virtualization Manager에서 직접 이루어지는 것이 아니라 선택한 호스트를 통해 이루어집니다. 시스템에 최소한 하나의 활성 호스트가 존재해야 하며 선택한 데이터 센터에 연결되어 있어야 합니다. 모든 호스트는 스토리지 도메인을 설정하기 전 스토리지 장치에 액세스할 수 있어야 합니다.

7. 스토리지 도메인의 상세 정보를 입력합니다.



참고

도메인 기능 / 스토리지 유형 목록에서 선택한 값에 따라 변경되는 스토리지 도메인 상세 정보를 지정하기 위한 필드입니다. 이러한 옵션은 새로운 스토리지 도메인 추가를 위해 사용 가능한 옵션과 동일합니다. 이러한 옵션에 대한 보다 자세한 내용은 **8.1절. “스토리지 도메인 이해”**에서 참조하십시오.

8. **데이터 센터에서 도메인을 활성화** 확인란을 선택하여 선택한 데이터 센터에 스토리지 도메인을 연결한 후 이를 활성화합니다.
9. **OK**를 클릭합니다.

스토리지 도메인이 가져오기되어 **스토리지** 탭에 표시됩니다. 스토리지 도메인에서 데이터 센터로 가상 머신과 템플릿을 가져올 수 있습니다.

8.6.3. 동일한 환경에서 데이터 센터 간 스토리지 도메인 마이그레이션

동일한 Red Hat Virtualization 환경에서 스토리지 도메인을 하나의 데이터 센터에서 다른 데이터 센터로 마이그레이션하여 대상 데이터 센터에서 스토리지 도메인에 있는 데이터에 액세스할 수 있습니다. 다음의 절차를 통해 하나의 데이터 센터에서 스토리지 도메인을 분리하여 다른 데이터 센터에 연결합니다.

절차 8.12. 동일한 환경에서 데이터 센터 간 스토리지 도메인 마이그레이션

1. 필요한 스토리지 도메인에서 실행 중인 모든 가상 머신을 종료합니다.
2. **스토리지 리소스** 탭을 클릭하고 검색 결과 목록에서 스토리지 도메인을 선택합니다.
3. 상세 정보 창에서 **데이터 센터** 탭을 클릭합니다.
4. **유지보수**를 클릭하고 **OK**를 클릭하여 스토리지 도메인을 유지 관리 모드로 전환합니다.
5. **분리**를 클릭하고 **OK**를 클릭하여 스토리지 도메인을 데이터 센터에서 분리합니다.
6. **연결**을 클릭합니다.
7. 대상 데이터 센터를 선택하고 **OK**를 클릭합니다.

스토리지 도메인이 대상 데이터 센터에 연결되어 자동으로 활성화됩니다. 스토리지 도메인에서 대상 데이터 센터로 가상 머신과 템플릿을 가져올 수 있습니다.

8.6.4. 다른 환경에서 데이터 센터 간 스토리지 도메인 마이그레이션

하나의 Red Hat Virtualization 환경에서 다른 환경으로 스토리지 도메인을 마이그레이션하여 대상 환경에서 스토리지 도메인에 있는 데이터에 액세스할 수 있습니다. 다음의 절차를 통해 하나의 Red Hat Virtualization 환경에서 스토리지 도메인을 삭제하여 다른 환경으로 가져오기합니다. 기존 스토리지 도메인을 Red Hat Virtualization 데이터 센터에 가져오기해서 연결하기 위해 해당 스토리지 도메인의 소스 데이터 센터의 호환성 수준이 3.5 이상이어야 합니다.

절차 8.13. 다른 환경에서 데이터 센터 간 스토리지 도메인 마이그레이션

1. 소스 환경의 관리 포털에 로그인합니다.
2. 필요한 스토리지 도메인에서 실행 중인 모든 가상 머신을 종료합니다.
3. **스토리지 리소스** 탭을 클릭하고 검색 결과 목록에서 스토리지 도메인을 선택합니다.

4. 상세 정보 창에서 **데이터 센터** 탭을 클릭합니다.
5. **유지보수**를 클릭하고 **OK**를 클릭하여 스토리지 도메인을 유지 관리 모드로 전환합니다.
6. **분리**를 클릭하고 **OK**를 클릭하여 스토리지 도메인을 데이터 센터에서 분리합니다.
7. **삭제**를 클릭합니다.
8. 스토리지 **삭제** 창에서 **도메인을 포맷합니다. 스토리지 콘텐츠가 손실됩니다!** 확인란이 선택 해제되었는지 확인합니다. 이 단계를 통해 나중에 위해 스토리지 도메인의 데이터를 보관합니다.
9. **OK**를 클릭하여 소스 환경에서 스토리지 도메인을 삭제합니다.
10. 대상 환경의 관리 포털에 로그인합니다.
11. 스토리지 리소스 탭을 클릭합니다.
12. **도메인 가져오기**를 클릭합니다.

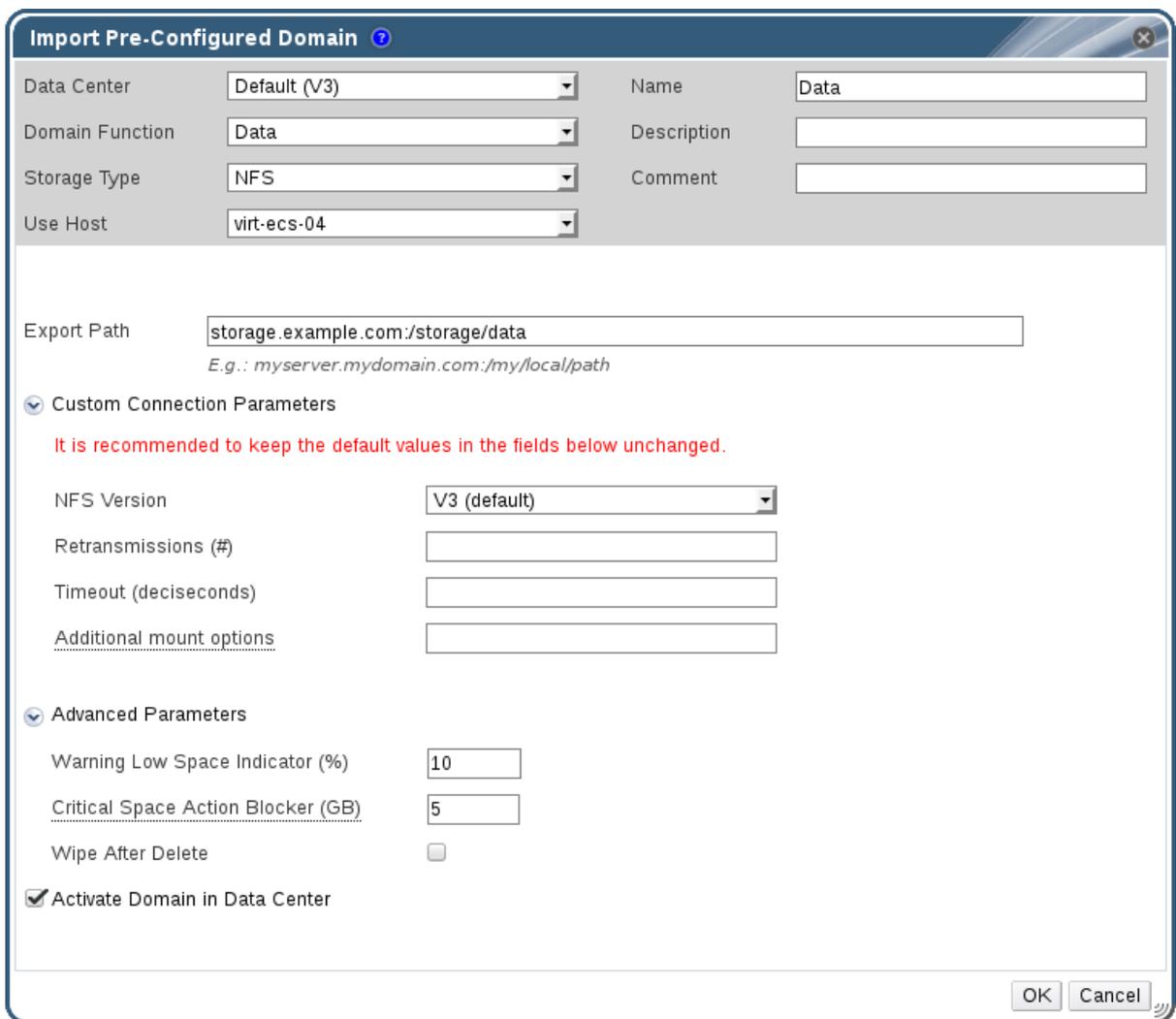


그림 8.8. 사전 설정된 도메인 가져오기 창

13. **데이터 센터** 드롭 다운 목록에서 대상 데이터 센터를 선택합니다.
14. 스토리지 도메인의 이름을 입력합니다.
15. **도메인 기능 및 스토리지 유형** 드롭 다운 목록에서 적절한 항목을 선택합니다.

16. **사용 호스트** 드롭 다운 목록에서 호스트를 선택합니다.

17. 스토리지 도메인의 상세 정보를 입력합니다.



참고

스토리지 유형 드롭 다운 목록에서 선택한 값에 따라 변경되는 스토리지 도메인 상세 정보를 지정하기 위한 필드입니다. 이러한 옵션은 새로운 스토리지 도메인 추가를 위해 사용 가능한 옵션과 동일합니다. 이러한 옵션에 대한 보다 자세한 내용은 [8.1절. “스토리지 도메인 이해”](#)에서 참조하십시오.

18. **데이터 센터에서 도메인을 활성화** 확인란을 선택하여 스토리지 도메인을 연결 시 자동으로 활성화합니다.

19. **OK**를 클릭합니다.

스토리지 도메인이 새로운 **Red Hat Virtualization** 환경의 대상 데이터 센터에 연결되어 자동으로 활성화됩니다. 가져온 스토리지 도메인에서 대상 데이터 센터로 가상 머신과 템플릿을 가져올 수 있습니다.

8.6.5. 가져온 데이터 스토리지 도메인에서 가상 머신 가져오기

Red Hat Virtualization 환경으로 가져온 데이터 스토리지 도메인에서 하나 이상의 클러스터로 가상 머신을 가져옵니다. 이러한 절차에서는 가져온 데이터 스토리지 도메인이 데이터 센터에 연결되어 활성화되어 있다고 간주합니다.

절차 8.14. 가져온 데이터 스토리지 도메인에서 가상 머신 가져오기

1. 스토리지 리소스 탭을 클릭합니다.
2. 가져온 데이터 스토리지 도메인을 클릭합니다.
3. 상세 정보 창에서 **가상 머신 가져오기** 탭을 클릭합니다.
4. 가져오기할 가상 머신을 하나 이상 선택합니다.
5. **가져오기** 버튼을 클릭합니다.
6. **가상 머신 가져오기** 창에 있는 각 가상 머신에 대해 **클러스터** 목록에서 올바른 대상 클러스터가 선택되어 있는지 확인합니다.
7. 대상 클러스터에 있는 프로파일로 외부 가상 머신 **vNIC** 프로파일을 매핑합니다.
 - a. **vNic 프로파일 매핑**을 클릭합니다.
 - b. **대상 vNic 프로파일** 드롭 다운 목록에서 사용할 **vNIC** 프로파일을 선택합니다.
 - c. 여러 대상 클러스터가 **가상 머신 가져오기** 창에 선택되어 있는 경우 **대상 클러스터** 드롭 다운 목록에서 각 대상 클러스터를 선택하고 매핑이 올바른지 확인합니다.
 - d. **OK**를 클릭합니다.
8. **MAC** 주소 충돌이 감지되면 느낌표가 가상 머신의 이름 옆에 나타납니다. 아이콘 위로 마우스를 가져가서 발생한 오류 유형을 표시하는 도구 팁을 확인합니다.

잘못된 MAC 재할당 확인란을 선택하여 새 **MAC** 주소를 문제가 있는 모든 가상 머신에 재할당합니다. 또는 가상 머신별로 **재할당** 확인란을 선택할 수 있습니다.



참고

할당할 수 있는 주소가 없는 경우 가져오기 작업이 실패합니다. 하지만 클러스터의 MAC 주소 풀 범위 외에 있는 MAC 주소의 경우 새 MAC 주소를 다시 할당하지 않고도 가상 머신을 가져올 수 있습니다.

9. OK를 클릭합니다.

하나 이상의 가상 머신을 환경에 가져왔습니다. 가져온 가상 머신은 더이상 **가상 머신 가져오기** 탭 목록에 나타나지 않습니다.

8.6.6. 가져온 데이터 스토리지 도메인에서 템플릿 가져오기

Red Hat Virtualization 환경으로 가져온 데이터 스토리지 도메인에서 템플릿을 가져옵니다. 이러한 절차에서는 가져온 데이터 스토리지 도메인이 데이터 센터에 연결되어 활성화되어 있다고 간주합니다.

절차 8.15. 가져온 데이터 스토리지 도메인에서 템플릿 가져오기

1. 스토리지 리소스 탭을 클릭합니다.
2. 가져온 데이터 스토리지 도메인을 클릭합니다.
3. 상세 정보 창에서 **템플릿 가져오기** 탭을 클릭합니다.
4. 가져오기할 템플릿을 하나 이상 선택합니다.
5. **가져오기** 버튼을 클릭합니다.
6. 클러스터 목록에서 템플릿을 가져오기한 클러스터를 선택합니다.
7. **OK**를 클릭합니다.

하나 이상의 템플릿을 환경에 가져왔습니다. 가져온 템플릿은 더이상 **템플릿 가져오기** 탭 목록에 나타나지 않습니다.

8.6.7. 가져온 스토리지 도메인에서 디스크 이미지 가져오기

가져온 스토리지 도메인에서 플로팅 가상 디스크를 가져오기 위해 상세 정보 창의 **디스크 불러오기** 탭을 사용합니다.



참고

QEMU와 호환되는 디스크만 **Manager**로 불러올 수 있습니다.

절차 8.16. 디스크 이미지 가져오기

1. 데이터 센터로 가져온 스토리지 도메인을 선택합니다.
2. 상세 정보 창에서 **디스크 불러오기**를 클릭합니다.
3. 하나 이상의 디스크 이미지를 선택 후 **가져오기**를 클릭하여 **디스크 불러오기** 창을 엽니다.
4. 각 디스크의 적절한 **디스크 프로파일**을 선택합니다.
5. **OK**를 클릭하여 선택된 디스크를 가져옵니다.

8.6.8. 가져온 스토리지 도메인에서 미등록된 디스크 이미지 가져오기

스토리지 도메인에서 플로팅 가상 디스크를 가져오기 위해 상세 정보 창의 **디스크 불러오기** 탭을 사용합니다. Red Hat Virtualization 환경 외부(outside)에서 생성된 플로팅 디스크는 Manager에 등록되어 있지 않습니다. 미등록된 플로팅 디스크를 찾아서 가져오기 위하여 스토리지 도메인을 검색합니다.



참고

QEMU와 호환되는 디스크만 Manager로 가져올 수 있습니다.

절차 8.17. 디스크 이미지 불러오기

1. 데이터 센터로 가져온 스토리지 도메인을 선택합니다.
2. 스토리지 도메인을 오른쪽 클릭하고 **디스크 검사**를 선택하여 Manager가 미등록된 디스크를 찾습니다.
3. 상세 정보 창에서 **디스크 불러오기**를 클릭합니다.
4. 하나 이상의 디스크 이미지를 선택 후 **가져오기**를 클릭하여 **디스크 불러오기** 창을 엽니다.
5. 각 디스크의 적절한 **디스크 프로파일**을 선택합니다.
6. **OK**를 클릭하여 선택된 디스크를 가져옵니다.

8.7. 스토리지 작업

8.7.1. ISO 스토리지 도메인 표시

ISO 스토리지 도메인은 데이터 센터에 연결되어 있습니다. ISO 이미지를 업로드해야 합니다. Red Hat Virtualization은 ISO 업로더 도구를 제공하여 올바른 사용자 권한을 갖는 올바른 디렉토리 경로로 이미지를 업로드합니다.

물리적 미디어에서 ISO 이미지를 생성하는 방법은 이 문서에서 설명하고 있지 않습니다. 환경에 필요한 이미지에 액세스하고 있음을 전제로 합니다.

절차 8.18. ISO 스토리지 도메인 표시

1. Red Hat Virtualization Manager를 실행하고 있는 시스템의 임시 디렉토리에 필요한 ISO 이미지를 복사합니다.
2. **root** 사용자로 Red Hat Virtualization Manager를 실행하고 있는 시스템에 로그인합니다.
3. **engine-iso-uploader** 명령을 사용하여 ISO 이미지를 업로드합니다. 작업을 완료하는데 시간이 소요될 수 있습니다. 업로드할 이미지 크기와 사용 가능한 네트워크 대역폭에 따라 작업 시간이 달라질 수 있습니다.

예 8.1. ISO 업로더 사용

예에서 ISO 이미지 **RHEL6.iso**는 NFS를 사용하는 **ISODomain**이라는 ISO 도메인에 업로드되어 있습니다. 명령을 통해 관리자의 사용자 이름과 암호를 입력합니다. 사용자 이름은 **user name@domain** 형식으로 입력해야 합니다.

```
# engine-iso-uploader --iso-domain=ISODomain upload RHEL6.iso
```

ISO 이미지가 업로드되어 지정된 ISO 스토리지 도메인에 표시됩니다. 이는 스토리지 도메인이 연결된 데이터 센터에서 가상 머신을 생성할 때 사용 가능한 부팅 미디어 목록에도 표시됩니다.

8.7.2. 스토리지 도메인을 유지 관리 모드로 전환

스토리지 도메인을 분리하고 제거하려면 유지관리 모드여야 합니다. 이는 다른 데이터 도메인을 마스터 데이터 도메인으로 재지정하기 위해 필요합니다.



중요

가상 머신의 스토리지 도메인에 임대가 있는 경우 스토리지 도메인을 유지관리 모드로 전환할 수 없습니다. 가상 머신을 종료하거나 임대를 제거하거나 다른 스토리지 도메인으로 먼저 이동해야 합니다. 가상 머신 임대에 대한 자세한 내용은 [가상 머신 관리 가이드](#)를 참조하십시오.

도메인이 활성화되어 있을 때에만 LUN을 추가하여 iSCSI 도메인을 확장할 수 있습니다.

절차 8.19. 스토리지 도메인을 유지 관리 모드로 전환

1. 스토리지 도메인에서 실행 중인 모든 가상 머신을 종료합니다.
2. 스토리지 리소스 탭을 클릭하고 스토리지 도메인을 선택합니다.
3. 상세 정보 창에서 **데이터 센터** 탭을 클릭합니다.
4. **유지보수**를 클릭하여 **스토리지 도메인 관리 확인** 창을 엽니다.
5. **OK**를 클릭하여 유지 관리 모드를 시작합니다. 스토리지 도메인이 비활성화되고 결과 목록에서 **Inactive** 상태가 됩니다.

데이터 센터에서 비활성 스토리지 도메인을 편집, 분리, 삭제, 다시 활성화할 수 있습니다.



참고

도메인이 연결된 데이터 센터의 상세 정보 창에 있는 스토리지 탭을 사용하여 도메인을 유지 관리 모드로 활성화, 분리, 전환할 수 있습니다.

8.7.3. 스토리지 도메인 편집

관리 포털을 통해 스토리지 도메인의 매개 변수를 편집할 수 있습니다. 스토리지 도메인 상태 (활성 또는 비활성 상태)에 따라 편집할 수 있는 필드가 다릅니다. **데이터 센터, 도메인 기능, 스토리지 유형, 포맷**과 같은 필드는 변경할 수 없습니다.

- **활성:** 스토리지 도메인이 활성 상태일 때 **이름, 설명, 코멘트, 디스크 공간 부족 경고 표시(%), 심각히 부족한 디스크 공간의 동작 차단(GB), 삭제 후 초기화 및 삭제 후 폐기** 필드를 편집할 수 있습니다. **이름** 필드는 스토리지 도메인이 활성 상태일 때에만 편집할 수 있습니다. 다른 모든 필드는 스토리지 도메인이 비활성 상태일 때에도 편집할 수 있습니다.
- **비활성 (Inactive):** 스토리지 도메인이 유지 관리 모드이거나 연결되어 있지 않아 비활성상태일 경우 **이름, 데이터 센터, 도메인 기능, 스토리지 유형, 및 포맷**을 제외한 모든 필드를 편집할 수 있습니다. 스토리지 연결, 마운트 옵션, 기타 다른 고급 매개 변수를 편집하려면 스토리지 도메인은 비활성 상태이어야 합니다. 이는 **NFS, POSIX, 로컬** 스토리지 유형에서만 지원됩니다.



참고

iSCSI 스토리지 연결은 관리 포털을 통해 편집할 수 없지만 REST API를 통해 편집할 수 있습니다. *REST API 가이드*에 있는 [iSCSI 스토리지 연결 업데이트](#)를 참조하십시오.

절차 8.20. 활성화된 스토리지 도메인 편집

1. 스토리지 리소스 탭을 클릭하고 스토리지 도메인을 선택합니다.
2. 도메인 관리를 클릭합니다.
3. 필요에 따라 사용 가능한 필드를 편집합니다.
4. **OK**를 클릭합니다.

절차 8.21. 비활성화된 스토리지 도메인 편집

1. 스토리지 리소스 탭을 클릭하고 스토리지 도메인을 선택합니다.
2. 스토리지 도메인이 활성화되어 있을 경우 상세 정보 창에서 **데이터 센터** 탭을 클릭하고 **유지 보수**를 클릭합니다.
3. 도메인 관리를 클릭합니다.
4. 필요에 따라 스토리지 경로 및 기타 상세 정보를 편집합니다. 새로운 연결 상세 정보는 기존 연결과 동일한 스토리지 유형이어야 합니다.
5. **OK**를 클릭합니다.
6. 상세 정보 창에서 **데이터 센터** 탭을 클릭하고 **활성화**를 클릭합니다.

8.7.4. 유지 관리 모드에서 스토리지 도메인 활성화

데이터 센터의 스토리지를 변경할 경우 스토리지 도메인을 유지 관리 모드로 두어야 합니다. 스토리지 도메인을 활성화하여 사용을 재개합니다.

1. 스토리지 리소스 탭을 클릭하고 검색 결과 목록에서 스토리지 도메인 비활성화를 선택합니다.
2. 상세 정보 창에서 **데이터 센터** 탭을 클릭합니다.
3. 해당 스토리지 도메인을 선택하고 **활성화**를 클릭합니다.



중요

데이터 도메인을 활성화하기 전 ISO 도메인을 활성화하려 할 경우 오류 메시지가 표시되고 도메인은 활성화되지 않습니다.

8.7.5. 스토리지 도메인 삭제

가상화 환경에서 삭제하고자 하는 데이터 센터의 스토리지 도메인이 있습니다.

절차 8.22. 스토리지 도메인 삭제

1. 스토리지 리소스 탭을 클릭하고 검색 결과 목록에서 적절한 스토리지 도메인을 선택합니다.

2. 도메인을 유지 관리 모드로 변경하여 비활성화합니다.
3. 데이터 센터에서 도메인을 분리합니다.
4. 삭제를 클릭하면 스토리지 삭제 확인 창이 열립니다.
5. 목록에서 호스트를 선택합니다.
6. **OK**를 클릭하여 스토리지 도메인을 삭제하고 창을 닫습니다.

스토리지 도메인이 환경에서 영구적으로 삭제됩니다.

8.7.6. 스토리지 도메인 삭제

스토리지 도메인에서 발생한 오류는 일반 절차를 통해 삭제할 수 없습니다. 스토리지 도메인을 삭제하면 내보내기 디렉토리를 참조하지 않고 가상 환경에서 스토리지 도메인이 강제로 삭제됩니다.

스토리지 도메인을 삭제하면 이를 다시 사용하기 전 수동으로 스토리지 도메인의 내보내기 디렉토리를 수정해야 합니다.

절차 8.23. 스토리지 도메인 삭제

1. 스토리지 리소스 탭, 트리 모드, 검색 기능을 사용하여 검색 결과 목록에 있는 적절한 스토리지 도메인을 검색 및 선택합니다.
2. 스토리지 도메인을 오른쪽 클릭하고 **삭제** 버튼을 선택하면 스토리지 도메인 삭제 확인 창이 열립니다.
3. **작업 승인** 확인란을 선택하고 **OK**를 클릭하여 스토리지 도메인을 삭제하고 창을 닫습니다.

스토리지 도메인이 삭제되었습니다. 스토리지 도메인의 내보내기 디렉토리를 다시 사용하려면 이를 수동으로 삭제합니다.

8.7.7. 데이터 센터에서 스토리지 도메인 분리

다른 데이터 센터로 가상 머신과 템플릿을 마이그레이션하기 위해 데이터 센터에서 스토리지 도메인을 분리합니다.

절차 8.24. 데이터 센터에서 스토리지 도메인 분리

1. 스토리지 리소스 탭을 클릭하고 검색 결과 목록에서 스토리지 도메인을 선택합니다.
2. 상세 정보 창에서 **데이터 센터** 탭을 클릭하고 스토리지 도메인을 선택합니다.
3. **유지보수**를 클릭하여 스토리지 도메인 관리 확인 창을 엽니다.
4. **OK**를 클릭하여 유지 관리 모드를 시작합니다.
5. **분리**를 클릭하여 스토리지 분리 확인창을 엽니다.
6. **OK**를 클릭하여 스토리지 도메인을 분리합니다.

스토리지 도메인이 데이터 센터에서 분리되어 다른 데이터 센터로 연결할 준비가 되어 있습니다.

8.7.8. 스토리지 도메인을 데이터 센터에 연결

스토리지 도메인을 데이터 센터에 연결합니다.

절차 8.25. 스토리지 도메인을 데이터 센터에 연결

1. 스토리지 리소스 탭을 클릭하고 검색 결과 목록에서 스토리지 도메인을 선택합니다.
2. 상세 정보 창에서 **데이터 센터** 탭을 클릭합니다.
3. **연결**을 클릭하여 **데이터 센터에 연결** 창을 엽니다.
4. 해당 데이터 센터의 라디오 버튼을 클릭합니다.
5. **OK**를 클릭하여 스토리지 도메인을 연결합니다.

스토리지 도메인이 데이터 센터에 연결되어 자동으로 활성화됩니다.

8.7.9. 디스크 프로파일

디스크 프로파일은 스토리지 도메인에 있는 가상 디스크의 최대 입출력 수준 및 처리 가능한 최대 용량을 정의합니다. 디스크 프로파일은 데이터 센터 아래에서 정의된 스토리지 프로파일에 기반하여 생성되며 프로파일을 적용하려면 개별적 가상 디스크에 수동으로 지정해야 합니다.

8.7.9.1. 디스크 프로파일 생성

디스크 프로파일을 생성합니다. 다음 부분에서는 스토리지 도메인이 속한 데이터 센터 아래에 하나 이상의 스토리지 QoS 항목이 이미 정의되어 있음을 전제로 합니다.

절차 8.26. 디스크 프로파일 생성

1. 스토리지 리소스 탭을 클릭하고 데이터 스토리지 도메인을 선택합니다.
2. 상세 정보 창에서 **디스크 프로파일** 하위 탭을 클릭합니다.
3. **새로 만들기**를 클릭합니다.
4. **이름**란에 디스크 프로파일 이름을 입력합니다.
5. **설명**란에 디스크 프로파일 설명을 입력합니다.
6. **QoS** 목록에서 디스크 프로파일에 적용할 QoS를 선택합니다.
7. **OK**를 클릭합니다.

디스크 프로파일이 생성되었습니다. 디스크 프로파일은 데이터 스토리지 도메인에서 호스트되는 새 가상 디스크에 적용할 수 있습니다.

8.7.9.2. 디스크 프로파일 삭제

Red Hat Virtualization 환경에서 기존 디스크 프로파일을 삭제합니다.

절차 8.27. 디스크 프로파일 삭제

1. 스토리지 리소스 탭을 클릭하고 데이터 스토리지 도메인을 선택합니다.
2. 상세 정보 창에서 **디스크 프로파일** 하위 탭을 클릭합니다.

3. 삭제하려는 디스크 프로파일을 선택합니다.
4. 삭제를 클릭합니다.
5. **OK**를 클릭합니다.

디스크 프로파일이 삭제되어 이를 더이상 사용할 수 없습니다. 디스크 프로파일이 가상 디스크에 지정되어 있을 경우 디스크 프로파일은 이러한 가상 디스크에서 삭제됩니다.

8.7.10. 스토리지 도메인 상태 표시

스토리지 도메인은 일반적인 **상태** 외에 외부 상태가 있습니다. 외부 상태는 플러그인 또는 외부 시스템에 의해 보고되거나 관리자가 설정하며 스토리지 도메인 이름 왼쪽에 다음의 아이콘 중에서 하나가 표시됩니다:

- **OK:** 아이콘 없음
- **Info:** 
- **Warning:** 
- **Error:** 
- **Failure:** 

스토리지 도메인 상태에 대한 상세 정보를 표시하기 위해 해당 스토리지 도메인을 선택하고 **이벤트** 하위 탭을 클릭합니다.

스토리지 도메인 상태는 REST API로 표시될 수도 있습니다. 스토리지 도메인에 대한 **GET** 요청에는 호스트 상태가 들어 있는 **external_status** 요소가 포함됩니다.

events 컬렉션을 통해 REST API에서 스토리지 도메인 상태를 설정할 수 있습니다. 자세한 내용은 **REST API 가이드**에 있는 **이벤트 추가**를 참조하십시오.

8.7.11. 스토리지 도메인의 삭제 후 폐기 설정

삭제 후 폐기 확인란을 선택한 경우, 스토리지 도메인이 제거되면 **blkdiscard** 명령이 논리 볼륨에서 호출되고 기본 스토리지에 해당 블록이 사용 가능성이 통보됩니다. 스토리지 배열에서는 여유 공간을 사용하고 요청 시 해당 공간을 할당할 수 있습니다. **삭제 후 폐기**는 블록 스토리지에서만 작동합니다. 파일 스토리지(예: NFS)의 Red Hat Virtualization Manager에서는 해당 플래그를 사용할 수 없습니다.

제한 사항:

- **삭제 후 폐기**는 iSCSI 또는 파이버 채널 등의 블록 스토리지 도메인에서만 사용 가능합니다.
- 기본 스토리지에서 **Discard**를 지원해야 합니다.

삭제 후 폐기는 블록 스토리지 도메인 생성 시 또는 블록 스토리지 도메인 편집 시 활성화할 수 있습니다. 자세한 내용은 **8.5절. "블록 스토리지 추가"** 및 **8.7.3절. "스토리지 도메인 편집"**에서 참조하십시오.

8.8. 스토리지 및 권한

8.8.1. 스토리지 도메인의 시스템 권한 관리

SuperUser로서 시스템 관리자는 관리 포털의 모든 면을 관리합니다. 보다 특정한 관리 역할은 다른 사용자에게 부여될 수 있습니다. 이러한 제한된 관리자 역할은 특정 리소스에 제한하여 사용자 관리 권한을 부여할 경우 유용합니다. 예를 들어 **DataCenterAdmin** 역할은 데이터 센터의 스토리지를 제외한 할당된 데이터 센터에 대해서만 관리자 권한을 갖으며 **ClusterAdmin**은 할당된 클러스터에 대해서만 관리자 권한을 갖습니다.

스토리지 관리자는 특정 스토리지 도메인에 대한 시스템 관리자 역할입니다. 이는 각 스토리지 도메인에 시스템 관리자가 필요한 여러 스토리지 도메인으로 구성된 데이터 센터에서 유용합니다. 머리글 표시줄에 있는 **설정** 버튼을 사용하여 환경의 모든 스토리지 도메인에 스토리지 관리자를 지정할 수 있습니다.

스토리지 도메인 관리자 역할은 다음과 같은 작업을 허용합니다:

- 스토리지 도메인의 설정을 편집합니다.
- 스토리지 도메인을 유지관리 모드로 전환합니다.
- 스토리지 도메인을 삭제합니다.



참고

기존 사용자에게만 역할 및 권한을 할당할 수 있습니다.

기존 시스템 관리자를 삭제하고 새로운 시스템 관리자를 추가하여 스토리지 도메인의 시스템 관리자를 변경할 수 있습니다.

8.8.2. 스토리지 관리자 역할

스토리지 도메인 권한 역할

아래 표에서는 스토리지 도메인 관리에 적용할 수 있는 관리자 역할 및 권한에 대해 설명합니다.

표 8.1. Red Hat Virtualization 시스템 관리자 역할

역할	권한	알림
StorageAdmin	스토리지 관리자	특정 스토리지 도메인을 생성, 삭제, 설정, 관리할 수 있습니다.
GlusterAdmin	Gluster 스토리지 관리자	Gluster 스토리지 볼륨을 생성, 삭제, 설정, 관리할 수 있습니다.

8.8.3. 리소스에 관리자 또는 사용자 역할 할당

리소스에 관리자 또는 사용자 역할을 할당하여 사용자가 리소스에 액세스 및 관리할 수 있게 합니다.

절차 8.28. 리소스에 역할 할당

1. 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 리소스를 검색 및 선택합니다.
2. 상세 정보 창에 있는 **권한** 탭을 클릭하여 할당된 사용자, 사용자 역할, 선택한 리소스에 대해 상속된 권한을 나열합니다.
3. **추가**를 클릭합니다.

4. **검색** 텍스트 상자에 기존 사용자의 이름 또는 사용자 이름을 입력하고 **검색**을 클릭합니다. 검색 결과 목록에서 일치하는 사용자를 선택합니다.
5. **할당할 역할** 드롭 다운 목록에서 역할을 선택합니다.
6. **OK**를 클릭합니다.

사용자에게 역할이 할당되어 이제 사용자는 리소스에 대해 활성화된 역할에 상속된 권한을 갖습니다.

8.8.4. 리소스에서 관리자 또는 사용자 역할 삭제

리소스에서 관리자 또는 사용자 역할을 삭제합니다. 사용자는 리소스에서의 역할과 관련하여 상속된 권한을 손실합니다.

절차 8.29. 리소스에서 역할 삭제

1. 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 리소스를 검색 및 선택합니다.
2. 상세 정보 창에 있는 **권한** 탭을 클릭하여 할당된 사용자 목록, 사용자 역할, 선택한 리소스에서 상속된 권한을 나열합니다.
3. 리소스에서 삭제할 사용자를 선택합니다.
4. **삭제**를 클릭합니다. **권한 삭제** 창이 열리면 권한 삭제를 확인합니다.
5. **OK**를 클릭합니다.

리소스에서 사용자 역할 및 관련된 권한이 삭제됩니다.

9장. RED HAT GLUSTER STORAGE를 사용하여 작업

9.1. RED HAT GLUSTER STORAGE 노드

9.1.1. Red Hat Gluster Storage 노드 추가

Red Hat Gluster Storage 노드를 Gluster 활성화된 클러스터에 추가하고 GlusterFS 볼륨 및 브릭을 Red Hat Virtualization 환경에 통합합니다.

다음 절차에서는 적절한 호환 버전의 Gluster-활성 클러스터가 존재하고 Red Hat Gluster Storage 노드가 이미 설정되어 있다는 것을 전제로 합니다. Red Hat Gluster Storage 노드 설정에 대한 보다 자세한 내용은 [Red Hat Gluster Storage 설치 가이드](#)에서 참조하십시오. 호환 매트릭스에 대한 자세한 내용은 [Red Hat Gluster Storage Version Compatibility and Support](#)에서 참조하십시오.

절차 9.1. Red Hat Gluster Storage 노드 추가

1. 호스트 리소스 탭을 클릭하여 결과 목록에 호스트를 나열합니다.
2. 새로 만들기를 클릭하여 새 호스트 창을 엽니다.
3. 드롭 다운 메뉴를 사용하여 Red Hat Gluster Storage 노드의 데이터 센터 및 호스트 클러스터를 선택합니다.
4. Red Hat Gluster Storage 노드의 이름, 주소, SSH 포트를 입력합니다.
5. Red Hat Gluster Storage 노드와 함께 사용할 인증 방식을 선택합니다.
 - 인증 암호를 사용하기 위해 root 사용자 암호를 입력합니다.
 - SSH 공개키 필드에 표시된 키를 Red Hat Gluster Storage 노드에 있는 `/root/.ssh/authorized_keys`에 복사하여 공개키 인증에 사용합니다.
6. OK를 클릭하여 노드를 추가하고 창을 닫습니다.

Red Hat Virtualization 환경에 Red Hat Gluster Storage 노드가 추가되었습니다. 사용자 환경에서 노드의 볼륨 및 브릭 리소스를 사용할 수 있습니다.

9.1.2. Red Hat Gluster Storage 노드 삭제

Red Hat Virtualization 환경에서 Red Hat Gluster Storage 노드를 삭제합니다.

절차 9.2. Red Hat Gluster Storage 노드 삭제

1. 호스트 리소스 탭, 트리 모드, 검색 기능을 사용하여 검색 결과 목록에 있는 Red Hat Gluster Storage 노드를 검색 및 선택합니다.
2. 유지보수를 클릭하면 호스트 유지관리 모드 확인 창이 열립니다.
3. OK를 클릭하여 호스트를 유지 관리 모드로 전환합니다.
4. 삭제를 클릭하면 호스트 삭제 확인 창이 열립니다.
5. 노드에 볼륨 브릭이 있거나 노드가 응답하지 않을 경우 강제 삭제 확인란을 선택합니다.
6. OK를 클릭하여 노드를 삭제하고 창을 닫습니다.

Red Hat Gluster Storage 노드가 환경에서 삭제되어 더이상 호스트 탭에서 볼 수 없습니다.

9.2. 스토리지 도메인으로 RED HAT GLUSTER STORAGE 사용

9.2.1. Red Hat Gluster Storage (GlusterFS) 볼륨 소개

Red Hat Gluster Storage 볼륨은 하나 이상의 Red Hat Gluster Storage 서버에서의 스토리지를 단일 글로벌 네임스페이스로 통합합니다. 볼륨은 브릭 모음으로 여기서 각 브릭은 신뢰할 수 있는 스토리지 풀에서 Red Hat Gluster Storage Server에 있는 마운트 지점 또는 디렉토리입니다.

Red Hat Gluster Storage의 대부분의 관리 작업은 볼륨에서 실행됩니다.

관리 포털을 사용하여 새 볼륨을 생성 및 시작할 수 있습니다. 볼륨 탭에서 Red Hat Gluster Storage 클러스터에 있는 볼륨을 모니터링할 수 있습니다.

볼륨은 관리 포털에서 생성 및 관리할 수 있지만 브릭은 관리 포털을 사용하여 볼륨에 추가하기 전 개별 Red Hat Gluster Storage 노드에 생성해야 합니다.

9.2.2. Gluster 스토리지 용어

표 9.1. 데이터 센터 속성

용어	정의
브릭	브릭은 신뢰할 수 있는 스토리지 풀의 서버에 있는 내보내기 디렉토리에서 표시되는 기본 GlusterFS 스토리지 단위입니다. 브릭은 다음과 같은 형식으로 된 내보내기 디렉토리가 있는 서버와 결합하여 표시됩니다: SERVER:EXPORT 예: myhostname:/exports/myexportdir/
블록 스토리지	블록 특수 파일 또는 블록 장치는 시스템이 블록 형태로 데이터를 이동할 때 사용하는 장치에 해당합니다. 이러한 장치 노드에는 하드 디스크, CD-ROM 드라이브, 메모리 영역과 같은 주소 지정 가능한 장치가 있습니다. Red Hat Gluster Storage는 확장 속성과 함께 XFS 파일 시스템을 지원합니다.
클러스터	밀접하게 작동하기 위해 여러가지 방법으로 하나의 컴퓨터를 형성하고 있는 링크된 컴퓨터의 신뢰할 수 있는 풀입니다. Red Hat Gluster Storage 용어에서 클러스터는 신뢰할 수 있는 스토리지 풀이라고 합니다.
클라이언트	볼륨을 마운트하는 시스템입니다. (서버가 될 수도 있음)

용어	정의
분산 파일 시스템	신뢰할 수 있는 스토리지 풀에서 여러 서버/브릭 전체에 걸쳐 분산된 데이터에 여러 클라이언트가 동시에 액세스할 수 있는 파일 시스템입니다. 여러 위치에서 데이터를 공유하는 것은 모든 분산 파일 시스템에 필수적입니다.
지역 복제	지역 복제는 로컬 영역 네트워크 (LAN), 광역 네트워크 (WAN), 인터넷을 통해 사이트간 지속적, 비동기식, 증분 복제 서비스를 제공합니다.
glusterd	신뢰할 수 있는 스토리지 풀에 있는 모든 서버에서 실행해야 하는 Gluster 관리 데몬입니다.
메타데이터	메타데이터는 하나 이상의 다른 데이터에 대한 정보를 제공하는 데이터입니다.
N-way 복제	일반적으로 로컬 동기식 데이터 복제는 캠퍼스나 Amazon Web Services Availability Zones에 걸쳐 배포됩니다.
네임 스페이스	네임 스페이스는 고유 식별자나 기호의 논리적 그룹을 저장하기 위해 생성된 추상적 컨테이너 또는 환경입니다. 각각의 Red Hat Gluster Storage 신뢰할 수 있는 스토리지 풀은 신뢰할 수 있는 스토리지 풀의 모든 파일이 들어 있는 POSIX 마운트 지점으로 단일 네임 스페이스를 제공합니다.
POSIX	Portable Operating System Interface (Unix 용)는 UNIX 운영 체제의 다양한 버전과 호환 가능한 소프트웨어의 셸 및 유틸리티 인터페이스와 함께 애플리케이션 프로그래밍 인터페이스 (API)를 정의하는 IEEE에 의해 지정된 관련 표준 제품군 이름입니다. Red Hat Gluster Storage는 POSIX와의 완전하게 호환 가능한 파일 시스템을 내보내기합니다.
RAID	Redundant Array of Inexpensive Disks (RAID)는 낮은 비용, 낮은 안정성 디스크 드라이브 구성요소를 논리 단위로 (어레이에 있는 모든 드라이브가 상호 종속적인) 결합하여 중복을 통해 스토리지 안정성을 증가시키는 기술입니다.
RRDNS	Round Robin Domain Name Service (RRDNS)는 애플리케이션 서버를 통해 부하를 분산하는 방법입니다. RRDNS는 DNS 서버의 영역 파일에 동일한 이름의 다른 IP 주소를 갖는 복수의 A 레코드를 생성하여 구현됩니다.
서버	데이터가 저장되는 실제 파일 시스템을 호스팅하는 시스템 (가상 또는 베어 메탈)입니다.
단일 차원 확장 스토리지	하나의 차원에서만 스토리지 장치의 용량을 증가시킵니다. 예를 들어 신뢰할 수 있는 스토리지 풀에 있는 단일 컴퓨터의 추가 디스크 용량을 늘리는 것입니다.

용어	정의
다차원 확장 스토리지	여러 차원에서 스토리지 장치의 용량을 증가시킵니다. 예를 들어 신뢰할 수 있는 스토리지 풀에 서버를 추가하여 신뢰할 수 있는 스토리지 풀의 CPU, 디스크 용량 및 처리량을 증가시킵니다.
서브 볼륨	서브 볼륨은 최소 하나의 변환기에 의해 처리된 브릭입니다.
변환기	변환기는 하나 이상의 서브볼륨에 연결되어 작업을 수행하고 서브 볼륨 연결을 제공합니다.
신뢰할 수 있는 스토리지 풀	스토리지 풀은 스토리지 서버의 신뢰할 수 있는 네트워크입니다. 첫 번째 서버를 시작하면 스토리지 풀은 단독으로 해당 서버로 구성됩니다.
사용자 공간	사용자 공간에서 실행되고 있는 애플리케이션은 하드웨어와 직접 상호 작용하는 대신 커널을 사용하여 액세스를 중재합니다. 사용자 공간 애플리케이션은 일반적으로 커널 공간 애플리케이션 보다 더 이동적입니다. Gluster는 사용자 공간 애플리케이션입니다.
VFS (Virtual File System)	VFS는 표준 Linux 파일 시스템과 관련된 모든 시스템 호출을 처리하는 커널 소프트웨어 계층입니다. 이는 여러 종류의 파일 시스템에 대해 일반적인 인터페이스를 제공합니다.
볼륨 파일	볼륨 파일은 GlusterFS 프로세스에 의해 사용되는 설정 파일입니다. 일반적으로 볼륨 파일은 <code>/var/lib/glusterd/vols/VOLNAME</code> 에 있습니다.
볼륨	볼륨은 브릭의 논리 집합입니다. 대부분의 Gluster 관리 작업은 볼륨에서 수행됩니다.

9.2.3. 스토리지 도메인으로 Red Hat Gluster Storage 볼륨 연결

스토리지 도메인으로 바로 사용하기 위해 Red Hat Gluster Storage 볼륨을 Red Hat Virtualization Manager에 추가합니다. 이는 Red Hat Virtualization Manager 내에 있는 노드의 볼륨 및 브릭을 통한 제어를 가능하게 하는 Red Hat Storage Gluster 노드를 추가하는 방법과 다르며 Gluster 활성 클러스터가 필요하지 않습니다.

볼륨을 마운트하려면 호스트에 `glusterfs`, `glusterfs-fuse` 및 `glusterfs-cli` 패키지가 필요합니다. `glusterfs-cli` 패키지는 고객 포털의 `rh-common-rpms` 채널에 있습니다.

Red Hat Gluster Storage 노드 설정에 대한 보다 자세한 내용은 [Red Hat Gluster Storage 설치 가이드](#)에서 참조하십시오. Red Hat Storage Gluster 볼륨 으로 사용할 호스트 준비에 대한 보다 자세한 내용은 [Red Hat Gluster Storage 가이드](#)에서 [Red Hat Virtualization 설정](#)에서 참조하십시오. 호환 매트릭스에 대한 보다 자세한 내용은 [Red Hat Gluster Storage Version Compatibility and Support](#)에서 참조하십시오.

절차 9.3. 스토리지 도메인으로 Red Hat Gluster Storage 볼륨 추가

1. 스토리지 리소스 탭을 클릭하면 결과 목록에 기존 스토리지 도메인 목록이 표시됩니다.

2. 새로운 도메인을 클릭하면 새로운 도메인 창이 열립니다.

그림 9.1. Red Hat Gluster Storage

3. 스토리지 도메인의 이름을 입력합니다.
4. 스토리지 도메인에 연결할 데이터 센터를 클릭합니다.
5. 도메인 기능 드롭 다운 목록에서 **Data**를 선택합니다.
6. 스토리지 유형 드롭 다운 목록에서 **GlusterFS**를 선택합니다.
7. 사용 호스트 드롭 다운 목록에서 호스트를 선택합니다. 선택한 데이터 센터 내에 있는 호스트만 표시됩니다. 볼륨을 마운트하려면 선택한 호스트에 **glusterfs** 및 **glusterfs-fuse** 패키지를 설치해야 합니다.
8. 경로 필드에 Red Hat Gluster Storage 서버의 IP 주소 또는 FQDN 및 볼륨 이름을 콜론으로 구분하여 입력합니다.
9. **-o** 인수를 사용하여 **mount** 명령에 지정하는 것 처럼 추가마운트 옵션을 입력합니다. 마운트 옵션은 콤마로 구분합니다. 유효한 마운트 옵션 목록은 **man mount**에서 확인하십시오.
10. 옵션으로 고급 매개 변수를 설정할 수 있습니다.
 - a. 고급 매개 변수를 클릭합니다.

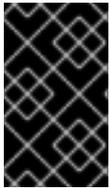
- b. **디스크 공간 부족 경고 표시** 필드에 백분율 값을 입력합니다. 스토리지 도메인에서 사용 가능한 여유 공간이 해당 백분율 값 아래로 내려가면 사용자에게 경고 메시지가 표시되고 기록됩니다.
- c. **심각히 부족한 디스크 공간의 동작 차단** 필드에 **GB** 단위로 값을 입력합니다. 스토리지 도메인에서 사용 가능한 여유 공간이 해당 값 아래로 내려가면 사용자에게 오류 메시지가 표시되고 기록되며 공간을 소비하는 모든 새로운 동작은 일시적이라도 모두 차단됩니다.
- d. **삭제 후 초기화** 확인란을 선택하여 삭제 후 초기화 옵션을 활성화합니다. 이 옵션은 도메인 생성 후 편집할 수 있지만 이러한 경우 이미 존재하는 디스크의 삭제 후 초기화 속성은 변경되지 않습니다.

11. **OK**를 클릭하여 스토리지 도메인으로 볼륨을 마운트하고 창을 닫습니다.

9.2.4. 스토리지 볼륨 생성

관리 포털을 사용하여 새 볼륨을 생성할 수 있습니다. 새 볼륨 생성 시 볼륨을 구성하는 브릭을 지정하고 볼륨이 분산, 복제, 스트라이프되는지를 지정해야 합니다.

브릭을 볼륨에 추가하기 전 브릭 디렉토리 또는 마운트 지점을 생성해야 합니다.



중요

다른 호스트에서 내보내기된 브릭이 볼륨으로 통합된 복제 볼륨을 사용하는 것이 좋습니다. 복제 볼륨은 볼륨에 여러 브릭에 걸쳐 파일 복사본을 만들기 때문에 호스트가 분리된 경우 데이터 손실을 방지할 수 있습니다.

절차 9.4. 스토리지 볼륨 생성

1. 볼륨 리소스 탭을 클릭하여 결과 목록에 있는 기존 볼륨을 나열합니다.
2. **새로 만들기**를 클릭하면 새 볼륨 창이 열립니다.
3. 드롭 다운 메뉴를 사용하여 **데이터 센터** 및 **볼륨 클러스터**를 선택합니다.
4. 볼륨 이름을 입력합니다.
5. 드롭 다운 메뉴에서 볼륨 **유형**을 선택합니다.
6. 활성화된 경우 적절한 **전송 유형** 체크 상자를 선택합니다.
7. **브릭 추가** 버튼을 클릭하여 볼륨에 추가할 브릭을 선택합니다. **Red Hat Gluster Storage** 노드 외부에서 브릭을 생성해야 합니다.
8. 활성화된 경우 **Gluster, NFS, CIFS** 체크 상자를 사용하여 볼륨에 사용되는 적절한 액세스 프로토콜을 선택합니다.
9. **액세스 허용할 호스트** 필드에 볼륨 액세스 제어를 IP 주소 또는 호스트 이름의 콤마로 구분된 목록으로 입력합니다.

IP 주소나 호스트 이름을 범위로 지정하기 위해 *를 와일드 카드로 사용할 수 있습니다.

10. **가상 저장소에 최적화** 옵션을 선택하여 가상 머신 스토리지 볼륨을 최적화하기 위한 매개 변수를 설정합니다. 이 볼륨을 스토리지 도메인으로 사용하고자 할 경우에도 이 옵션을 선택합니다.
11. **OK**를 클릭하여 볼륨을 생성합니다. 새 볼륨이 추가되어 볼륨 탭에 표시됩니다.

Red Hat Gluster Storage 볼륨이 추가되어 이를 스토리지로 사용할 수 있습니다.

9.2.5. 볼륨에 브릭 추가

요약

새로운 브릭을 추가하여 볼륨을 확장할 수 있습니다. 스토리지 공간을 확장할 때 최소 하나의 브릭을 분산 볼륨에 2의 배수의 브릭을 복제 볼륨에 4의 배수의 브릭을 스트라이프 볼륨에 추가해야 합니다.

절차 9.5. 볼륨에 브릭 추가

1. 탐색 창의 볼륨 탭에서 브릭에 추가하고자 하는 볼륨을 선택합니다.
2. 상세 정보 창에서 브릭 탭을 클릭합니다.
3. 브릭 추가를 클릭하여 브릭 추가 창을 엽니다.
4. 서버 드롭 다운 메뉴를 사용하여 브릭을 배치할 서버를 선택합니다.
5. 브릭 디렉토리 경로를 입력합니다. 경로가 이미 존재해야 합니다.
6. 추가를 클릭합니다. 볼륨에 있는 브릭 목록에 서버 주소 및 브릭 디렉토리 이름과 함께 브릭이 표시됩니다.
7. OK를 클릭합니다.

결과

새 브릭이 볼륨에 추가되어 브릭은 볼륨의 브릭 탭에 표시됩니다.

9.2.6. 브릭 추가 창 설정

표 9.2. 브릭 탭 속성 추가

필드 이름	설명
볼륨 유형	볼륨 유형을 표시합니다. 이 필드는 변경할 수 없습니다. 이는 볼륨 생성 시 설정됩니다.
서버	브릭이 호스팅되는 서버입니다.
브릭 디렉토리	브릭 디렉토리 또는 마운트 지점입니다.

9.2.7. 가상 머신 이미지를 저장하기 위해 Red Hat Gluster Storage 볼륨을 최적화

관리 포털을 사용하여 가상 머신 이미지를 저장하기 위해 Red Hat Gluster Storage 볼륨을 최적화합니다.

가상 머신을 저장하기 위해 볼륨을 최적화하려면 Manager는 볼륨에 특정 가상화 매개변수를 설정합니다.

가상 머신을 저장하기 위해 가상 저장소에 최적화 확인란을 선택하거나 볼륨 리소스 탭에서 가상 저장소에 최적화 버튼을 사용하여 볼륨 생성후 이를 최적화할 수 있습니다.

중요

볼륨이 세 개 이상의 노드에 복제되는 경우 노드에서 데이터 불일치되지 않도록 가상 스토리지에서 볼륨을 최적화합니다.

다른 방법은 Red Hat Gluster Storage 노드 중 하나에 액세스하여 볼륨 그룹을 **virt**로 설정하는 것입니다. 이는 **cluster.quorum-type** 매개 변수를 **auto**로 설정하고 **cluster.server-quorum-type** 매개 변수를 **server**로 설정합니다.

```
# gluster volume set VOLUME_NAME group virt
```

볼륨 정보를 나열하여 볼륨 상태를 확인합니다:

```
# gluster volume info VOLUME_NAME
```

9.2.8. 볼륨 시작하기

요약

볼륨을 생성한 후 또는 기존 볼륨을 중지한 후 볼륨을 사용하기 전 이를 시작해야 합니다.

절차 9.6. 볼륨 시작하기

1. 볼륨 탭에서 시작할 볼륨을 선택합니다.

Shift 또는 **Ctrl** 키를 사용하여 시작할 여러 볼륨을 선택할 수 있습니다.

2. 시작 버튼을 클릭합니다.

볼륨 상태를 **Up**으로 변경합니다.

결과

이제 가상 머신 스토리지의 볼륨을 사용할 수 있습니다.

9.2.9. 볼륨 조정

개요

볼륨을 조정하면 성능에 영향을 미칠 수 있습니다. 볼륨을 조정하려면 옵션을 추가합니다.

절차 9.7. 볼륨 조정

1. 볼륨 탭을 클릭합니다.

볼륨 목록이 표시됩니다.

2. 조정하고자 하는 볼륨을 선택하고 상세 정보 창에서 볼륨 옵션 탭을 클릭합니다.

볼륨 옵션 탭에 볼륨 옵션 설정 목록이 표시됩니다.

3. 추가를 클릭하여 옵션을 설정합니다. 옵션 추가 대화 상자 표시됩니다. 드롭 다운 목록에서 옵션 키를 선택하고 옵션 값을 입력합니다.
4. **OK**를 클릭합니다.

옵션이 설정되어 **블륨 옵션** 탭에 표시됩니다.

결과

스토리지 블륨의 옵션이 조정되었습니다.

9.2.10. 블륨 옵션 편집

요약

옵션을 추가하여 블륨을 조정합니다. 스토리지 블륨의 옵션을 변경할 수 있습니다.

절차 9.8. 블륨 옵션 편집

1. **블륨** 탭을 클릭합니다.

블륨 목록이 표시됩니다.

2. 편집하고자 하는 블륨을 선택한 후 상세 정보 창에서 **블륨 옵션** 탭을 클릭합니다.

블륨 옵션 탭에 블륨 옵션 설정 목록이 표시됩니다.

3. 편집하고자 하는 옵션을 선택합니다. **편집**을 클릭하면 **옵션 편집** 대화 상자가 나타납니다. 새 옵션 값을 입력합니다.

4. **OK**를 클릭합니다.

편집된 옵션은 **블륨 옵션** 탭에 표시됩니다.

결과

블륨에서 옵션이 변경됩니다.

9.2.11. 블륨 옵션 재설정

요약

옵션을 재설정하여 기본값으로 되돌리기할 수 있습니다.

1. **블륨** 탭을 클릭합니다.

블륨 목록이 표시됩니다.

2. 블륨을 선택하고 상세 정보 창에서 **블륨 옵션** 탭을 클릭합니다.

블륨 옵션 탭에 블륨 옵션 설정 목록이 표시됩니다.

3. 재설정하고자 하는 옵션을 선택합니다. **재설정**을 클릭합니다. 대화 상자에서 옵션 재설정을 확인하는 메시지가 나타납니다.

4. **OK**를 클릭합니다.

선택한 옵션이 재설정됩니다.



참고

모두 **재설정** 버튼을 클릭하여 모든 볼륨 옵션을 재설정할 수 있습니다. 대화 상자에서 옵션 재 설정을 확인하는 메시지가 나타납니다. **OK**를 클릭합니다. 선택한 볼륨의 모든 볼륨 옵션이 재설정됩니다.

결과

볼륨 옵션이 기본값으로 재설정됩니다.

9.2.12. 볼륨에서 브릭 삭제

요약

클러스터를 온라인에서 사용 가능할 때 필요에 따라 볼륨을 축소할 수 있습니다. 예를 들어 하드웨어나 네트워크 장애로 인해 분산 볼륨에서 액세스할 수 없는 브릭을 삭제해야 할 수도 있습니다.

절차 9.9. 볼륨에서 브릭 삭제

1. 탐색 창의 **볼륨** 탭에서 브릭을 제거하고자 하는 볼륨을 선택합니다.
2. 상세 정보 창에서 **브릭** 탭을 클릭합니다.
3. 삭제하고자 하는 브릭을 선택합니다. **브릭 삭제**를 클릭합니다.
4. 창이 열리고 삭제를 확인하는 메시지가 나타납니다. **OK**를 클릭하여 확인합니다.

결과

브릭이 볼륨에서 삭제됩니다.

9.2.13. Red Hat Gluster Storage 볼륨 중지

볼륨을 시작한 후 이를 중지할 수 있습니다.

절차 9.10. 볼륨 중지

1. **볼륨** 탭에서 중지할 볼륨을 선택합니다.
Shift 또는 **Ctrl** 키를 사용하여 중지할 여러 볼륨을 선택할 수 있습니다.
2. **중지**를 클릭합니다.

9.2.14. Red Hat Gluster Storage 볼륨 삭제

클러스터에서 하나의 볼륨 또는 여러 볼륨을 삭제할 수 있습니다.

1. **볼륨** 탭에서 삭제할 볼륨을 선택합니다.
2. **삭제**를 클릭합니다. 대화 상자에서 삭제를 확인하는 메시지가 나타납니다. **OK**를 클릭합니다.

9.2.15. 볼륨 재조정

요약

브릭을 추가 또는 삭제하여 볼륨을 확장 또는 축소할 경우 볼륨에 있는 데이터를 서버 사이에서 재조정해야 합니다.

절차 9.11. 볼륨 재조정

1. 볼륨 탭을 클릭합니다.
볼륨 목록이 표시됩니다.
2. 재조정하려는 볼륨을 선택합니다.
3. 재조정을 클릭합니다.

결과

선택한 볼륨이 재조정됩니다.

9.3. CLUSTERS 및 GLUSTER 후크

9.3.1. Gluster 후크 관리

Gluster 후크는 볼륨 라이프 사이클 확장입니다. Manager에서 Gluster 후크를 관리할 수 있습니다. 후크 콘텐츠 유형이 **Text**일 경우 후크 콘텐츠를 확인할 수 있습니다.

Manager를 통해 다음과 같은 작업을 수행할 수 있습니다:

- 호스트에서 사용할 수 있는 후크 목록을 확인할 수 있습니다.
- 후크 콘텐츠 및 상태를 확인할 수 있습니다.
- 후크를 활성화 또는 비활성화할 수 있습니다.
- 후크 충돌을 해결할 수 있습니다.

9.3.2. 후크 나열

요약

환경에 Gluster 후크를 나열합니다.

절차 9.12. 후크 나열

1. 클러스터 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 클러스터를 검색 및 선택합니다.
2. **Gluster** 후크 하위 탭을 선택하여 상세 정보 창에 후크를 나열합니다.

결과

환경에 Gluster 후크가 나열됩니다.

9.3.3. 후크 콘텐츠 보기

요약

사용자 환경에 있는 Gluster 후크 콘텐츠를 확인합니다.

절차 9.13. 후크 콘텐츠 보기

1. 클러스터 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 클러스터를 검색 및 선택합니다.
2. **Gluster** 후크 하위 탭을 선택하여 상세 정보 창에 후크를 나열합니다.
3. 콘텐츠 유형이 텍스트인 후크를 선택하고 **콘텐츠 보기** 버튼을 클릭하여 **후크 콘텐츠** 창을 엽니다.

결과

사용자 환경에서 후크 콘텐츠를 확인할 수 있습니다.

9.3.4. 후크 활성화 또는 비활성화

요약

Gluster 후크를 활성화 또는 비활성화하여 Gluster 후크 동작을 전환합니다.

절차 9.14. 후크 활성화 또는 비활성화

1. 클러스터 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 클러스터를 검색 및 선택합니다.
2. **Gluster** 후크 하위 탭을 선택하여 상세 정보 창에 후크를 나열합니다.
3. 후크를 선택하고 **활성화** 또는 **비활성화** 버튼 중 하나를 클릭합니다. 후크는 클러스터의 모든 노드에서 활성화 또는 비활성화됩니다.

결과

사용자 환경에 있는 Gluster 후크 동작을 전환했습니다.

9.3.5. 후크 새로 고침하기

요약

기본값으로 **Manager**는 클러스터에 있는 모든 서버 및 **engine**에 설치된 후크 상태를 확인하고 매 시간마다 정기적으로 작업을 실행하여 새 후크를 감지합니다. **Sync** 버튼을 클릭하여 후크를 수동으로 새로 고침할 수 있습니다.

절차 9.15. 후크 새로 고침하기

1. 클러스터 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 클러스터를 검색 및 선택합니다.
2. **Gluster** 후크 하위 탭을 선택하여 상세 정보 창에 후크를 나열합니다.
3. 동기화 버튼을 클릭합니다.

결과

후크가 상세 정보 창에서 동기화 및 업데이트됩니다.

9.3.6. 충돌 해결

후크는 클러스터 탭의 **Gluster** 후크 하위 탭에 표시됩니다. 충돌의 원인이 되는 후크는 느낌표로 표시

됩니다. 이는 클러스터에 있는 서버 간 후크 콘텐츠 또는 상태에서 충돌이 발생하는지 혹은 하나 이상의 서버에서 후크 스크립트가 누락되어 있는지를 나타냅니다. 이러한 충돌은 **Manager**를 통해 해결할 수 있습니다. 서버에 있는 후크는 **engine** 데이터베이스와 주기적으로 동기화되며 다음과 같은 충돌이 발생할 수 있습니다:

- 콘텐츠 충돌 - 후크 콘텐츠가 서버 간에 다를 경우 발생합니다.
- 누락 충돌 - 클러스터의 하나 이상의 서버에 후크가 없을 경우 발생합니다.
- 상태 충돌 - 서버 간에 후크 상태가 다를 경우 발생합니다.
- 다수 충돌 - 위의 충돌 중 두 개 이상이 조합하여 충돌이 발생합니다.

9.3.7. 콘텐츠 충돌 해결

요약

모든 서버 및 **engine**에서 일관되지 않는 후크는 충돌하는 것으로 플래그 지정됩니다. 충돌을 해결하려면 모든 서버 및 **engine**에 걸쳐 복사할 후크 버전을 선택해야 합니다.

절차 9.16. 콘텐츠 충돌 해결

1. 클러스터 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 클러스터를 검색 및 선택합니다.
2. **Gluster** 후크 하위 탭을 선택하여 상세 정보 창에 후크를 나열합니다.
3. 충돌하는 후크를 선택하고 **충돌 해결** 버튼을 클릭하여 **충돌 해결** 창을 엽니다.
4. 소스 목록에서 **engine**이나 서버를 선택하여 후크 콘텐츠를 확인하고 복사할 후크 버전을 설정합니다.



참고

후크 콘텐츠는 모든 서버 및 **engine**에서 덮어쓰기됩니다.

5. **콘텐츠 사용** 드롭 다운 메뉴에서 선호하는 서버나 **engine**을 선택합니다.
6. **OK**를 클릭하여 충돌을 해결하고 창을 닫습니다.

결과

선택한 서버에서 후크는 모든 서버 및 **engine**에 걸쳐 복사되어 시스템 환경 전반에 걸쳐 일관성을 유지합니다.

9.3.8. 누락된 후크 충돌 해결

요약

모든 서버 및 **engine**에 나타나지 않는 후크는 충돌된 것으로 플래그 지정됩니다. 충돌을 해결하려면 모든 서버 및 **engine**에 걸쳐 복사할 후크 버전을 선택하거나 누락된 후크를 완전히 삭제합니다.

절차 9.17. 누락된 후크 충돌 해결

1. 클러스터 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 클러스터를 검색 및 선택합니다.

2. **Gluster** 후크 하위 탭을 선택하여 상세 정보 창에 후크를 나열합니다.
3. 충돌하는 후크를 선택하고 **충돌 해결** 버튼을 클릭하여 **충돌 해결** 창을 엽니다.
4. **활성화** 상태인 모든 소스를 선택하여 후크 콘텐츠를 확인합니다.
5. 해당 라디오 버튼을 선택하거나 **모든 서버에 후크를 복사** 또는 **누락된 후크 제거**를 선택합니다. 누락된 후크 제거를 선택하면 **engine** 및 모든 서버에서 후크가 삭제됩니다.
6. **OK**를 클릭하여 충돌을 해결하고 창을 닫습니다.

결과

선택한 해결 방법에 따라 후크는 시스템 환경에서 완전히 삭제되거나 모든 서버 및 **engine**에 복사되어 시스템 환경 전반에 걸쳐 일관성을 유지합니다.

9.3.9. 상태 충돌 해결

요약

서버 및 **engine** 전반에 걸쳐 일관된 상태가 아닌 후크는 충돌하는 것으로 플래그 지정됩니다. 충돌을 해결하려면 환경의 모든 서버에 걸쳐 적용할 상태를 선택합니다.

절차 9.18. 상태 충돌 해결

1. 클러스터 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 클러스터를 검색 및 선택합니다.
2. **Gluster** 후크 하위 탭을 선택하여 상세 정보 창에 후크를 나열합니다.
3. 충돌하는 후크를 선택하고 **충돌 해결** 버튼을 클릭하여 **충돌 해결** 창을 엽니다.
4. 후크 상태를 **활성화** 또는 **비활성화**로 설정합니다.
5. **OK**를 클릭하여 충돌을 해결하고 창을 닫습니다.

결과

선택된 후크 상태는 **engine** 및 서버에 적용되며 환경 전반에 걸쳐 일관성을 유지합니다.

9.3.10. 다수 충돌 해결

요약

후크에는 두 개 이상의 충돌이 조합하여 발생할 수 있습니다. 이는 모두 **충돌 해결** 창을 통해 동시에 또는 개별적으로 해결할 수 있습니다. 다음 부분에서는 후크의 모든 충돌을 해결하여 환경의 모든 서버 및 **engine**에 걸쳐 일관성을 유지합니다.

절차 9.19. 다수 충돌 해결

1. 클러스터 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 클러스터를 검색 및 선택합니다.
2. **Gluster** 후크 하위 탭을 선택하여 상세 정보 창에 후크를 나열합니다.
3. 충돌하는 후크를 선택하고 **충돌 해결** 버튼을 클릭하여 **충돌 해결** 창을 엽니다.
4. 적절한 절차에 따라 각각의 영향을 미치는 충돌에 해결 방법을 선택합니다.

5. **OK**를 클릭하여 충돌을 해결하고 창을 닫습니다.

결과

모든 충돌을 해결하여 후크는 **engine** 및 모든 서버에 걸쳐 일관성을 유지합니다.

9.3.11. Gluster 동기화 관리

Gluster 동기화 기능을 통해 GlusterFS에서 주기적으로 최신 클러스터 설정을 가져와 **engine DB**와 동기화합니다. 이러한 절차는 **Manager**를 통해 수행될 수 있습니다. 클러스터를 선택하면 사용자에게 호스트를 가져오기하거나 선택한 클러스터에서 기존 호스트를 분리할 수 있는 옵션이 주어집니다. 클러스터에 호스트가 있을 경우 **Gluster** 동기화를 수행할 수 있습니다.



참고

호스트가 스토리지 클러스터에 추가되거나 삭제되어 있는지를 **Manager**는 지속적으로 모니터링합니다. 호스트 추가 또는 삭제를 선택한 경우 작업 항목은 클러스터의 **일반** 탭에 표시됩니다. 여기서 호스트 **가져오기** 또는 클러스터에서 호스트 **분리**를 선택할 수 있습니다.

10장. 풀

10.1. 가상 머신 풀 소개

가상 머신 풀은 동일한 템플릿에서 복제된 가상 머신 그룹으로 지정된 그룹의 사용자가 요청할 때 사용할 수 있습니다. 가상 머신 풀을 통해 관리자는 사용자의 일반적 가상 머신 모음을 신속하게 설정할 수 있습니다.

사용자는 풀에서 가상 머신을 취득하여 가상 머신 풀에 액세스합니다. 풀에서 사용자가 가상 머신을 취득할 때 풀에 사용 가능한 가상 머신이 있을 경우 가상 머신 중 하나가 사용자에게 제공됩니다. 가상 머신에는 풀의 기반이 되는 템플릿과 동일한 운영 체제 및 설정이 제공되지만 사용자가 가상 머신을 취득할 때 마다 동일한 가상 머신 풀을 수신하지 않습니다. 사용자는 풀 설정에 따라 동일한 가상 머신 풀에서 여러 가상 머신을 취득할 수도 있습니다.

가상 머신 풀에서 가상 머신은 비저장 상태이기 때문에 재부팅 시 데이터가 영구적으로 남아있지 않게 됩니다. 하지만 가상 머신 풀에서 얻은 가상 머신의 콘솔 옵션을 사용자가 설정할 경우 이러한 옵션은 가상 머신 풀의 사용자에게 대해 기본값으로 설정됩니다.

원칙적으로 풀에 있는 가상 머신은 사용자가 취득한 때에 시작되며 사용자가 사용 종료한 때에 종료되지만 가상 머신 풀에는 사전 시작된 가상 머신도 들어 있습니다. 사전 시작된 가상 머신은 **up** 상태로 유지되고 사용자가 취득할 때 까지 유휴 상태로 남아 있게 됩니다. 이를 통해 사용자는 가상 머신을 바로 사용 시작할 수 있지만 이러한 가상 머신은 유휴 상태에서라도 시스템 리소스를 소모합니다.



참고

관리 포털에서 액세스한 경우 풀에서 가져온 가상 머신은 상태 비저장으로 되지 않습니다. 이는 관리자가 필요에 따라 디스크에 변경 사항을 기록할 수 있어야 하기 때문입니다.

10.2. 가상 머신 풀 작업

10.2.1. 가상 머신 풀 생성

일반 템플릿을 기반으로 여러 가상 머신이 들어 있는 가상 머신 풀을 생성할 수 있습니다.

절차 10.1. 가상 머신 풀 생성

1. 풀 탭을 클릭합니다.
2. 새로 만들기 버튼을 클릭하여 새 풀 창을 엽니다.
3. 드롭 다운 목록에서 클러스터를 선택하거나 선택된 기본값을 사용합니다.
4. 템플릿 드롭 다운 메뉴를 사용하여 템플릿과 버전을 선택하거나 선택된 기본값을 사용합니다. 템플릿은 풀에 있는 모든 가상 머신의 표준 설정을 제공합니다.
5. 운영 체제 드롭 다운 목록을 사용하여 운영 체제를 선택하거나 템플릿에서 지정된 기본값을 사용합니다.
6. 최적화 옵션 드롭 다운 목록에서 데스크톱 사용이나 서버 사용을 위해 가상 머신을 최적화합니다.
7. 풀의 이름, 설명, 코멘트 가상 머신 수를 입력합니다.
8. 사전 가동된 가상 머신 필드에서 사전 시작된 가상 머신 수를 입력합니다.

9. 사용자가 세션에서 실행할 수 있는 **사용자당 최대 가상 머신 수**를 선택합니다. 최소 가상 머신 수는 한 대입니다.
10. **삭제 방지** 확인란을 선택하여 삭제 방지 기능을 활성화합니다.
11. 옵션으로 **고급 옵션 표시** 버튼을 클릭하고 다음 절차를 실행합니다:
 - a. **유형** 탭을 클릭하고 **풀 유형**을 선택합니다:
 - **수동** - 관리자는 풀에 가상 머신을 명시적으로 반환해야 합니다. 관리자가 가상 머신을 풀에 반환한 후 가상 머신은 기존의 기본 이미지로 되돌아갑니다.
 - **자동** - 가상 머신 종료 시 이는 자동으로 기본 이미지로 되돌아가고 가상 머신 풀에 반환됩니다.
 - b. **콘솔** 탭을 선택합니다. 탭 하단 창에서 **SPICE** **프록시** **덮어쓰기**란을 선택하고 **SPICE** **프록시** **주소** **덮어쓰기** 텍스트 필드를 활성화합니다. 글로벌 **SPICE** **프록시**를 덮어쓰기할 **SPICE** **프록시** **주소**를 지정합니다.
12. **OK**를 클릭합니다.

지정된 동일한 가상 머신 수가 있는 가상 머신 풀이 생성 및 설정되었습니다. **가상 머신** 리소스 탭이나 풀 리소스 탭의 상세 정보 창에서 이러한 가상 머신을 확인할 수 있습니다. 가상 머신 풀은 아이콘으로된 개별적 가상 머신에서 구별할 수 있습니다.

10.2.2. 새 풀 및 풀 편집 창 설정 및 제어

10.2.2.1. 새 풀 및 풀 편집 일반 설정

다음 표에서는 새 풀 창과 풀 편집 창의 일반 탭에 필요한 가상 머신 풀에 관련된 정보를 설명하고 있습니다. 모든 다른 설정은 새 가상 머신 창에 있는 설정과 동일합니다.

표 10.1. 일반 설정

필드 이름	설명
템플릿	가상 머신 풀의 기반이 되는 템플릿 및 템플릿 하위 버전입니다. 템플릿의 latest 하위 버전을 기반으로 풀을 생성하는 경우 재부팅 시 풀에 있는 모든 가상 머신이 자동으로 최신 템플릿 버전을 받습니다. 가상 머신의 템플릿 설정에 대한 자세한 내용은 가상 머신 관리 가이드 에 있는 가상 머신 일반 설정 및 새 템플릿 설정 및 템플릿 편집 창에 대한 설명 을 참조하십시오.
설명	가상 머신 풀에 대한 설명입니다.
코멘트	가상 머신 풀 관련 일반 텍스트 형식의 사용자가 읽을 수 있는 코멘트를 추가하기 위한 필드입니다.
사전 시작된 가상 머신	사용자가 검색하기 전 시작하여 그 상태로 유지되는 가상 머신 풀에서 가상 머신 수를 지정할 수 있습니다. 이 필드의 값은 0 과 가상 머신 풀에 있는 총 가상 머신 수 사이에 있는 값이어야 합니다.

필드 이름	설명
가상 머신 수/풀에 추가할 가상 머신 수	가상 머신 풀에 생성 및 사용 가능한 가상 머신 수를 지정할 수 있습니다. 편집 창에서 가상 머신 풀의 가상 머신 수를 지정한 수량만큼 추가할 수 있습니다. 기본 값으로 풀에 생성할 수 있는 최대 가상 머신 수는 1000 입니다. 이러한 값은 engine-config 명령의 MaxVmsInPool 키를 사용하여 설정할 수 있습니다.
사용자당 최대 가상 머신 수	단일 사용자가 한 번에 가상 머신 풀에서 검색할 수 있는 최대 가상 머신 수를 지정할 수 있습니다. 이 필드 값은 1 과 32,767 사이에 있는 값이어야 합니다.
삭제 방지	가상 머신 풀에 있는 가상 머신의 삭제를 방지합니다.

10.2.2.2. 새 풀 및 풀 유형 일반 설정

다음 표에서는 새 풀 창과 풀 편집 창의 유형 탭에 필요한 정보에 대해 설명합니다.

표 10.2. 유형 설정

필드 이름	설명
풀 유형	드롭 다운 메뉴에서 가상 머신 풀 유형을 지정할 수 있습니다. 다음과 같은 옵션을 사용할 수 있습니다: <ul style="list-style-type: none"> • 자동: 사용자가 가상 머신 풀에서의 가상 머신 사용을 종료한 후 가상 머신은 가상 머신 풀에 자동으로 반환됩니다. • 수동: 사용자가 가상 머신 풀에서 가상 머신 사용을 종료한 후 관리자가 가상 머신을 수동으로 반환한 경우에만 가상 머신은 가상 머신 풀에 반환됩니다.

10.2.2.3. 새 풀 및 풀 편집 콘솔 설정

다음 표에서는 새 풀 또는 풀 편집 창의 콘솔 탭에 필요한 가상 머신 풀에 관련된 정보를 설명하고 있습니다. 모든 다른 설정은 새 가상 머신 및 가상 머신 편집 창에 있는 설정과 동일합니다.

표 10.3. 콘솔 설정

필드 이름	설명
SPICE 프록시 덮어쓰기	이 옵션을 선택하여 전체 설정에 지정된 SPICE 프록시 덮어쓰기를 활성화할 수 있습니다. 이 기능은 호스트가 있는 네트워크 외부에 사용자 (예를 들어 사용자 포털을 통해 연결된 사용자)가 연결되어 있을 경우에 유용합니다.

필드 이름	설명
SPICE 프록시 주소 덮어쓰기	<p>SPICE 클라이언트는 가상 머신에 연결된 프록시입니다. 이러한 프록시는 Red Hat Virtualization 환경에 정의된 글로벌 SPICE 프록시 및 가상 머신 풀이 속한 클러스터에 대해 정의된 SPICE 프록시를 덮어쓰기합니다. 주소는 다음과 같은 형식이어야 합니다:</p> <pre>protocol://[host]:[port]</pre>

10.2.2.4. 가상 머신 풀 호스트 설정

다음 표에서는 새 풀 창과 풀 편집 창의 호스트 탭에 있는 옵션에 대해 설명합니다.

표 10.4. 가상 머신 풀: 호스트 설정

필드 이름	하위 요소	설명
실행 호스트		<p>가상 머신 실행 시 선호하는 호스트를 지정합니다. 다음 중에서 선택합니다:</p> <ul style="list-style-type: none"> 클러스터 내의 호스트 - 클러스터 내의 사용가능한 호스트에서 가상 머신을 시작 및 실행할 수 있습니다. 특정 호스트 - 클러스터 내의 특정 호스트에서 가상 머신이 실행되기 시작합니다. 하지만 이 가상 머신의 마이그레이션 여부와 고가용성 설정에 따라서 Manager 또는 관리자가 해당 가상 머신을 클러스터 내의 다른 호스트로 마이그레이션할 수 있습니다. 사용 가능한 호스트 목록에서 특정 호스트 또는 호스트 그룹을 선택합니다.

필드 이름	하위 요소	설명
<p>마이그레이션 옵션</p>	<p>마이그레이션 모드</p>	<p>가상 머신의 실행 및 마이그레이션 옵션을 지정합니다. 여기에 있는 옵션을 사용하지 않는 경우 가상 머신은 해당 클러스터의 정책에 따라 실행 또는 마이그레이션됩니다.</p> <ul style="list-style-type: none"> • 수동 및 자동 마이그레이션 허용 - 가상 머신은 해당 환경 상태에 따라 하나의 호스트에서 다른 호스트로 자동으로 마이그레이션이 되거나 관리자에 의해 수동으로 마이그레이션이 됩니다. • 수동 마이그레이션만 허용 - 가상 머신은 관리자에 의해 하나의 호스트에서 다른 호스트로 수동 마이그레이션만 할 수 있습니다. • 마이그레이션을 허용하지 않음 - 가상 머신은 자동 또는 수동으로 마이그레이션을 할 수 없습니다.

필드 이름	하위 요소	설명
	<p>사용자 정의 마이그레이션 정책 사용</p>	<p>마이그레이션 수렴 정책을 지정합니다. 확인란을 선택하지 않은 상태로 두면 호스트가 정책을 결정합니다.</p> <ul style="list-style-type: none"> • Legacy - 3.6 버전의 레거시 동작입니다. vdsm.conf의 덮어쓰기는 여전히 적용됩니다. 게스트 에이전트 후크 메커니즘은 비활성화됩니다. • Minimal downtime - 일반적인 상황에서 가상 머신 마이그레이션을 합니다. 가상 머신의 다운 타임은 길지 않습니다. 가상 머신 마이그레이션이 오랫동안 (QEMU 반복에 따라 최대 500 밀리초까지) 수렴되지 않는 경우 마이그레이션이 중단됩니다. 게스트 에이전트 후크 메커니즘은 활성화됩니다. • Suspend workload if needed - 대부분의 상황에서 가상 머신 마이그레이션을 하며, 가상 머신이 많은 작업량을 실행하는 경우를 포함합니다. 가상 머신의 다운 타임이 길 수 있습니다. 최대 부하시 마이그레이션이 중단될 수도 있습니다. 게스트 에이전트 후크 메커니즘은 활성화됩니다.
	<p>사용자 정의 마이그레이션 다운 타임 사용</p>	<p>이 확인란을 이용하여 라이브 마이그레이션 동안 가상 머신이 다운되는 최대 밀리초를 지정합니다. 각 가상 머신의 작업량 및 SLA 요구사항에 따라 서로 다른 최대 다운타임을 설정합니다. VDSM 기본값을 사용하려면 0을 입력합니다.</p>

필드 이름	하위 요소	설명
	<p>마이그레이션 자동 통합</p>	<p>Legacy 마이그레이션 정책에서 만 활성화됩니다. 가상 머신의 라이브 마이그레이션 중 자동 통합을 사용하도록 설정할 수 있습니다. 워크로드가 큰 대형 가상 머신은 라이브 마이그레이션 중 전송 속도보다 더 빠르게 더티 메모리 상태가 되어 마이그레이션을 컨버전스하지 못하게 합니다. QEMU의 자동 컨버전스 기능을 통해 가상 머신 마이그레이션 컨버전스를 강제할 수 있습니다. QEMU는 자동으로 컨버전스되지 않음을 감지하고 가상 머신에 있는 vCPU의 스로틀을 감소시킵니다. 자동 컨버전스는 전역에서 기본값으로 비활성화되어 있습니다.</p> <ul style="list-style-type: none"> • 클러스터 설정에서 가져오기를 선택하여 클러스터 수준에 설정된 자동 통합 설정을 사용합니다. 이 옵션은 기본값으로 선택되어 있습니다. • 자동 통합을 선택하여 클러스터 또는 전역 설정을 덮어쓰기하고 가상 머신의 자동 통합을 허용합니다. • 자동 통합 해제를 선택하여 클러스터 또는 전역 설정을 덮어쓰기하고 가상 머신이 자동 통합되지 않도록 합니다.

필드 이름	하위 요소	설명
	마이그레이션 압축 활성화	<p>Legacy 마이그레이션 정책에서만 활성화됩니다. 이 옵션을 통해 가상 머신의 라이브 마이그레이션 중 마이그레이션 압축을 사용하도록 설정할 수 있습니다. 이 기능은 Xor Binary Zero Run-Length-Encoding을 사용하여 가상 머신 다운 타임 및 집약적 메모리 쓰기 작업을 실행하는 가상 머신이나 스파스 메모리 업데이트 패턴이 있는 애플리케이션의 총 라이브 마이그레이션 시간을 단축할 수 있습니다. 마이그레이션 압축은 전역에서 기본값으로 비활성화되어 있습니다.</p> <ul style="list-style-type: none"> • 클러스터 설정에서 가져오기를 선택하여 클러스터 수준에 설정된 압축 설정을 사용합니다. 이 옵션은 기본값으로 선택되어 있습니다. • 압축을 선택하여 클러스터 또는 전역 설정을 덮어쓰기하고 가상 머신의 압축을 허용합니다. • 압축 해제를 선택하여 클러스터 또는 전역 설정을 덮어쓰기하고 가상 머신이 압축되지 않도록 합니다.
	호스트 CPU 통과	<p>이 확인란을 선택하여 가상 머신이 위치한 호스트의 물리 CPU의 기능을 사용할 수 있습니다. 이 옵션은 마이그레이션을 허용하지 않음 선택 시에만 활성화될 수 있습니다.</p>
NUMA 설정	NUMA 노드 수	<p>가상 머신에 할당할 가상 NUMA 노드의 수입니다. 조정 모드가 기본 설정인 경우 해당 값은 1로 설정되어야 합니다.</p>

필드 이름	하위 요소	설명
	조정 모드	메모리 할당에 사용되는 방법입니다. <ul style="list-style-type: none"> • 제한: 메모리가 대상 노드에 할당되지 못하는 경우 메모리 할당이 실패하게 됩니다. • 기본 설정: 단 하나의 기본 노드에서 메모리가 할당됩니다. 사용 가능한 메모리가 충분하지 않은 경우 다른 노드에서 메모리가 할당될 수 있습니다. • 인터리브: 라운드 로빈 알고리즘으로 메모리가 노드 전체에 할당됩니다.
	NUMA 고정	NUMA 토폴로지 창을 엽니다. 이 창에서는 호스트의 총 CPU, 메모리, NUMA 노드, 그리고 가상 머신의 가상 NUMA 노드가 표시됩니다. 오른쪽의 상자에서 왼쪽의 NUMA 노드로 각 vNUMA를 클릭 및 드래그하여 가상 NUMA 노드를 호스트 NUMA 노드에 고정시킵니다.

10.2.3. 가상 머신 풀 편집

10.2.3.1. 가상 머신 풀 편집

가상 머신 풀을 생성한 후 가상 머신 속성을 편집할 수 있습니다. 가상 머신 풀 편집 시 사용 가능한 속성은 새 가상 머신 풀을 생성할 때 사용 가능한 속성과 동일합니다. 여기에는 **풀에 추가할 가상 머신 수**로 대체되는 **가상 머신 수** 속성이 제외되어 있습니다.



참고

가상 머신 풀을 편집 시 변경된 내용은 새로운 가상 머신에만 영향을 미칩니다. 변경된 내용이 적용될 때 이미 존재한 가상 머신은 영향을 받지 않습니다.

절차 10.2. 가상 머신 풀 편집

1. 풀 리소스 탭을 클릭하고 검색 결과 목록에서 가상 머신 풀을 선택합니다.
2. 편집을 클릭하여 풀 편집 창을 엽니다.
3. 가상 머신 풀의 속성을 편집합니다.
4. **OK**를 클릭합니다.

10.2.3.2. 폴에서 가상 머신 사전 시작

가상 머신 폴에서 가상 머신은 기본적으로 전원이 꺼져 있습니다. 사용자가 폴에서 가상 머신을 요청하면 가상 머신은 전원이 켜지고 사용자에게 지정됩니다. 반대로 사전 시작된 가상 머신은 이미 실행되어 사용자에게 할당되기를 대기하고 있기 때문에 사용자가 가상 머신에 액세스할 때 까지의 대기 시간을 단축시킵니다. 사전 시작된 가상 머신이 종료되면 이는 폴에 반환하여 원래 상태로 복원됩니다. 최대 사전 시작 가상 머신 수는 폴에 있는 가상 머신 수입니다.

사전 시작된 가상 머신은 사용자에게 지정되지 않은 가상 머신에 바로 액세스해야 하는 환경에 적합합니다. 자동 폴만 가상 머신을 사전 시작할 수 있습니다.

절차 10.3. 폴에서 가상 머신 사전 시작

1. 폴 리소스 탭, 트리 모드, 검색 기능을 사용하여 검색 결과 목록에 있는 가상 머신 폴을 검색 및 선택합니다.
2. 편집을 클릭하여 폴 편집 창을 엽니다.
3. 사전 시작된 가상 머신 필드에서 사전 시작된 가상 머신 수를 입력합니다.
4. 폴 탭을 선택합니다. 폴 유형이 자동으로 설정되어 있는지 확인합니다.
5. OK를 클릭합니다.

폴에 사전 시작된 가상 머신 수가 설정되었습니다. 사전 시작된 가상 머신이 실행되고 있으며 사용 가능합니다.

10.2.3.3. 가상 머신 폴에 가상 머신 추가

가상 머신 폴에 기존에 제공된 가상 머신 보다 많은 가상 머신이 필요할 경우 이를 추가합니다.

절차 10.4. 가상 머신 폴에 가상 머신 추가

1. 폴 리소스 탭, 트리 모드, 검색 기능을 사용하여 검색 결과 목록에 있는 가상 머신 폴을 검색 및 선택합니다.
2. 편집을 클릭하여 폴 수정 창을 엽니다.
3. 폴에 추가할 가상 머신 수 필드에 추가할 가상 머신 수를 입력합니다.
4. OK를 클릭합니다.

가상 머신 폴에 여러 개의 가상 머신이 추가됩니다.

10.2.3.4. 가상 머신 폴에서 가상 머신 분리

가상 머신 폴에서 가상 머신을 분리할 수 있습니다. 폴에서 가상 머신을 분리하면 독립적 가상 머신이 됩니다.

절차 10.5. 가상 머신 폴에서 가상 머신 분리

1. 폴 리소스 탭, 트리 모드, 검색 기능을 사용하여 검색 결과 목록에 있는 가상 머신 폴을 검색 및 선택합니다.
2. 실행 중인 가상 머신을 분리할 수 없으므로 가상 머신이 **Down** 상태인지 확인합니다.

상세 정보 탭에서 **가상 머신** 탭을 클릭하여 풀에 있는 가상 머신을 나열합니다.

3. 하나 이상의 가상 머신을 선택하고 **분리**를 클릭하여 **가상 머신 분리** 확인 창을 엽니다.
4. **OK**를 클릭하여 풀에서 가상 머신을 분리합니다.



참고

가상 머신이 환경에 여전히 존재하여 **가상 머신 리소스** 탭에서 액세스 및 확인할 수 있습니다. 아이콘을 변경하여 분리된 가상 머신이 독립적 가상 머신임을 표시합니다.

가상 머신 풀에서 가상 머신이 분리됩니다.

10.2.4. 가상 머신 풀 삭제

데이터 센터에서 가상 머신 풀을 삭제할 수 있습니다. 풀에 있는 모든 가상 머신을 삭제하거나 분리합니다. 풀에서 가상 머신을 분리하면 이는 독립적 가상 머신으로 보존됩니다.

절차 10.6. 가상 머신 풀 삭제

1. 풀 리소스 탭, 트리 모드, 검색 기능을 사용하여 검색 결과 목록에 있는 가상 머신 풀을 검색 및 선택합니다.
2. **삭제**를 클릭하면 **풀 삭제** 확인 창이 열립니다.
3. **OK**를 클릭하여 풀을 삭제합니다.

데이터 센터에서 풀이 삭제됩니다.

10.3. 풀 및 권한

10.3.1. 가상 머신 풀의 시스템 권한 관리

SuperUser로서 시스템 관리자는 관리 포털의 모든 면을 관리합니다. 보다 특정한 관리 역할은 다른 사용자에게 부여될 수 있습니다. 이러한 제한된 관리자 역할은 특정 리소스에 제한하여 사용자 관리 권한을 부여할 경우 유용합니다. 예를 들어 **DataCenterAdmin** 역할은 데이터 센터의 스토리지를 제외한 할당된 데이터 센터에 대해서만 관리자 권한을 갖으며 **ClusterAdmin**은 할당된 클러스터에 대해서만 관리자 권한을 갖습니다.

가상 머신 풀 관리자는 데이터 센터에 있는 가상 머신 풀의 시스템 관리 역할입니다. 이 역할은 특정 가상 머신 풀, 데이터 센터, 가상화 환경 전체에 적용할 수 있습니다. 이는 다른 사용자가 특정 가상 머신 풀 리소스를 관리하는데 유용합니다.

가상 머신 풀 관리자 역할은 다음과 같은 작업을 허용합니다:

- 풀을 생성, 편집, 삭제합니다.
- 풀에서 가상 머신을 추가 또는 분리합니다.



참고

기존 사용자에게만 역할 및 권한을 할당할 수 있습니다.

10.3.2. 가상 머신 풀 관리자 역할

풀 권한이 있는 역할

아래 표에서는 풀 관리에 적용할 수 있는 관리자 역할 및 권한에 대해 설명합니다.

표 10.5. Red Hat Virtualization 시스템 관리자 역할

역할	권한	알림
VmPoolAdmin	가상 풀의 시스템 관리자	가상 풀을 생성, 삭제, 구성하고 가상 풀 사용자를 지정 및 삭제하며 가상 머신에서 기본 작업을 수행할 수 있습니다.
ClusterAdmin	클러스터 관리자	특정 클러스터에 있는 모든 가상 머신 풀을 사용, 생성, 삭제, 관리할 수 있습니다.

10.3.3. 리소스에 관리자 또는 사용자 역할 할당

리소스에 관리자 또는 사용자 역할을 할당하여 사용자가 리소스에 액세스 및 관리할 수 있게 합니다.

절차 10.7. 리소스에 역할 할당

1. 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 리소스를 검색 및 선택합니다.
2. 상세 정보 창에 있는 **권한** 탭을 클릭하여 할당된 사용자, 사용자 역할, 선택한 리소스에 대해 상속된 권한을 나열합니다.
3. 추가를 클릭합니다.
4. **검색** 텍스트 상자에 기존 사용자의 이름 또는 사용자 이름을 입력하고 **검색**을 클릭합니다. 검색 결과 목록에서 일치하는 사용자를 선택합니다.
5. **할당할 역할** 드롭 다운 목록에서 역할을 선택합니다.
6. **OK**를 클릭합니다.

사용자에게 역할이 할당되어 이제 사용자는 리소스에 대해 활성화된 역할에 상속된 권한을 갖습니다.

10.3.4. 리소스에서 관리자 또는 사용자 역할 삭제

리소스에서 관리자 또는 사용자 역할을 삭제합니다. 사용자는 리소스에서의 역할과 관련하여 상속된 권한을 손실합니다.

절차 10.8. 리소스에서 역할 삭제

1. 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 리소스를 검색 및 선택합니다.
2. 상세 정보 창에 있는 **권한** 탭을 클릭하여 할당된 사용자 목록, 사용자 역할, 선택한 리소스에서 상속된 권한을 나열합니다.

3. 리소스에서 삭제할 사용자를 선택합니다.
4. 삭제를 클릭합니다. 권한 삭제 창이 열리면 권한 삭제를 확인합니다.
5. OK를 클릭합니다.

리소스에서 사용자 역할 및 관련된 권한이 삭제됩니다.

10.4. 신뢰할 수 있는 컴퓨팅 풀

신뢰할 수 있는 컴퓨팅 풀은 Intel Trusted Execution Technology (Intel TXT) 기반의 보안 클러스터입니다. 신뢰할 수 있는 클러스터는 호스트 하드웨어 및 소프트웨어의 무결성을 White List 데이터베이스와 비교해서 측정하는 인텔 OpenAttestation에 의해 검증된 호스트만 허용합니다. 신뢰할 수 있는 호스트와 거기에 실행 중인 가상 머신은 높은 보안을 요구하는 작업에 할당될 수 있습니다. Intel TXT, 신뢰할 수 있는 시스템, 그리고 인증에 대한 보다 자세한 내용은 <https://software.intel.com/en-us/articles/intel-trusted-execution-technology-intel-txt-enabling-guide>에서 참조하십시오.

신뢰할 수 있는 컴퓨팅 풀을 생성하기 위해 다음의 단계를 거칩니다:

- Manager가 OpenAttestation 서버와 통신하도록 설정합니다.
- 신뢰할 수 있는 호스트만 실행할 수 있는 신뢰할 수 있는 클러스터를 생성합니다.
- 신뢰할 수 있는 클러스터에 신뢰할 수 있는 호스트를 추가합니다. OpenAttestation에 의해 신뢰할 수 있는 호스트로 검증되려면 해당 호스트는 OpenAttestation 에이전트에서 실행중이어야 합니다.

OpenAttestation 서버 설치, 호스트에 OpenAttestation 에이전트 설치, 그리고 White List 데이터베이스 생성에 대한 자세한 내용은 <https://github.com/OpenAttestation/OpenAttestation/wiki>에서 참조하십시오.

10.4.1. OpenAttestation 서버를 Manager에 연결

신뢰할 수 있는 클러스터를 생성하기 전에 Red Hat Virtualization Manager이 OpenAttestation 서버를 인식하도록 설정되어야 합니다. `engine-config`을 이용하여 OpenAttestation 서버의 FQDN 또는 IP 주소를 추가합니다:

```
# engine-config -s AttestationServer=attestationserver.example.com
```

필요한 경우 다음의 설정을 변경할 수 있습니다:

표 10.6. engine-config을 위한 OpenAttestation 설정

옵션	기본값	설명
AttestationServer	oat-server	OpenAttestation 서버의 FQDN 또는 IP 주소입니다. 이것이 설정되어야 Manager가 OpenAttestation 서버와 통신할 수 있습니다.
AttestationPort	8443	OpenAttestation 서버가 Manager와의 통신에 사용하는 포트입니다.

옵션	기본값	설명
AttestationTruststore	TrustStore.jks	OpenAttestation 서버와의 보안 통신에 사용되는 신뢰 저장소입니다.
AttestationTruststorePass	암호	신뢰 저장소에 액세스하기 위한 암호입니다.
AttestationFirstStageSize	10	빠른 설치에 사용됩니다. 타당한 이유 없이 해당 값을 변경하는 것은 권장되지 않습니다.
SecureConnectionWithOATServers	true	OpenAttestation 서버와의 보안 통신을 활성화 또는 비활성화합니다.
PollUri	AttestationService/resources/PollHosts	OpenAttestation 서비스에 액세스하기 위한 URI입니다.

10.4.2. 신뢰할 수 있는 클러스터 생성

신뢰할 수 있는 클러스터는 OpenAttestation 서버와 통신해서 호스트의 보안을 평가합니다. 신뢰할 수 있는 클러스터에 호스트 추가 시 OpenAttestation 서버는 호스트 하드웨어 및 소프트웨어의 무결성을 White List 데이터베이스와 비교해서 측정합니다. 신뢰할 수 있는 클러스터에 있는 신뢰할 수 있는 호스트 사이에 가상 머신을 마이그레이션할 수 있으며, 이를 통해 보안 환경에서 고가용성이 가능해집니다.

절차 10.9. 신뢰할 수 있는 클러스터 생성

1. 클러스터 탭을 선택합니다.
2. 새로 만들기를 클릭합니다.
3. 클러스터의 이름을 입력합니다.
4. Virt 서비스 활성화 라디오 버튼을 선택합니다.
5. 스케줄링 정책 탭에서 신뢰할 수 있는 서비스 활성화 확인란을 선택합니다.
6. OK를 클릭합니다.

10.4.3. 신뢰할 수 있는 호스트 추가

Red Hat Enterprise Linux 호스트가 신뢰할 수 있는 클러스터에 추가될 수 있으며 OpenAttestation 서버에서 White List 데이터베이스와 비교해서 해당 호스트를 측정합니다. OpenAttestation 서버에서 신뢰할 수 있는 호스트가 되려면 다음의 요구 사항을 충족해야 합니다:

- BIOS에서 Intel TXT가 활성화됩니다.
- OpenAttestation 에이전트가 설치되었고 실행중입니다.
- 호스트에 실행중인 소프트웨어가 OpenAttestation 서버의 White List 데이터베이스와 일치합니다.

절차 10.10. 신뢰할 수 있는 호스트 추가

1. 호스트 탭을 선택합니다.
2. 새로 만들기를 클릭합니다.
3. 호스트 클러스터 드롭 다운 목록에서 신뢰할 수 있는 클러스터를 선택합니다.
4. 호스트의 이름을 입력합니다.
5. 호스트의 주소를 입력합니다.
6. 호스트의 root 암호를 입력합니다.
7. **OK**를 클릭합니다.

호스트가 신뢰할 수 있는 클러스터에 추가된 후 OpenAttestation 서버에서 평가됩니다. OpenAttestation 서버가 신뢰할 수 없는 호스트는 **Non Operational** 상태가 되며 신뢰할 수 있는 클러스터에서 제거되어야 합니다.

11장. 가상 디스크

11.1. 가상 머신 스토리지 이해

Red Hat Virtualization은 세 개의 스토리지 유형 (NFS, iSCSI, FCP)을 지원합니다.

각 유형에 있어서 SPM (Storage Pool Manager)라는 호스트는 호스트와 스토리지 간의 액세스를 관리합니다. SPM 호스트는 스토리지 풀 내에서 완전한 액세스를 갖는 유일한 노드입니다. SPM은 스토리지 도메인 메타데이터와 풀의 메타데이터를 수정할 수 있습니다. 기타 다른 모든 호스트는 가상 머신의 하드 디스크 이미지 데이터에만 액세스할 수 있습니다.

기본값으로 NFS, 로컬, POSIX 호환 데이터 센터에서 SPM은 파일 시스템에 있는 파일로 씬 프로비저닝 포맷을 사용하여 가상 디스크를 생성합니다.

iSCSI 및 기타 블록 기반 데이터 센터에서 SPM은 지정된 LUN(Logical Unit Numbers) 상단에 볼륨 그룹을 생성하고 가상 디스크로 사용할 논리 볼륨을 만듭니다. 블록 기반 스토리지에서 가상 디스크는 기본적으로 사전 할당됩니다.

가상 디스크가 사전 할당되어 있을 경우 지정된 크기 (GB 단위)의 논리 볼륨이 생성됩니다. **kpartx, vgscan, vgchange, mount**를 사용하여 가상 머신을 Red Hat Enterprise Linux에 마운트하여 가상 머신의 프로세스 또는 문제를 확인할 수 있습니다.

가상 디스크가 씬 프로비저닝되는 경우 1 G의 논리 볼륨이 생성됩니다. 논리 볼륨은 가상 머신이 실행되는 호스트에서 지속적으로 모니터링됩니다. 사용량이 임계치에 가까워지면 호스트는 SPM에 통지하고 SPM은 논리 볼륨을 1 GB까지 확장합니다. 호스트는 논리 볼륨을 확장한 후 가상 머신을 다시 시작해야 합니다. 가상 머신이 일시 중지 상태가 될 경우 SPM은 적절한 때에 디스크가 확장되지 않을 수 있습니다. 이는 SPM이 너무 바쁜 경우 또는 스토리지 공간이 충분하지 않을 경우에 발생합니다.

사전 할당된 (RAW) 형식의 가상 디스크는 씬 프로비저닝 (QCOW2) 형식의 가상 디스크보다 쓰기 속도가 훨씬 빠릅니다. 씬 프로비저닝은 가상 디스크를 생성하는데 훨씬 적은 시간이 소요됩니다. 씬 프로비저닝 형식은 I/O 이외의 집약적 가상 시스템에 적합합니다. 사전 할당된 형식은 빠른 I/O 쓰기의 가상 머신에 사용하는 것이 좋습니다. 가상 머신이 4 초 마다 1 GB 이상을 쓸 수 있는 경우 가능하면 사전 할당된 디스크를 사용합니다.

11.2. 가상 디스크 이해

Red Hat Virtualization에는 사전 할당 (씬 프로비저닝된) 및 스파스 (씬 프로비저닝된) 스토리지 옵션을 특징으로 합니다.

- 사전 할당

사전 할당된 가상 디스크는 가상 머신에 필요한 모든 스토리지를 할당합니다. 예를 들어 가상 머신의 데이터 파티션을 위해 20 GB의 사전 할당된 논리 볼륨이 생성된 경우 생성 후 바로 20 GB의 스토리지 공간을 차지하게 됩니다.

- 스파스

스파스 할당을 통해 관리자는 가상 머신에 할당된 총 스토리지를 지정할 수 있지만 스토리지는 필요할 경우에만 할당됩니다.

예를 들어 20 GB 씬 프로비저닝 논리 볼륨은 처음 생성 시 0 GB의 스토리지 공간을 차지하게 됩니다. 운영 체제가 설치되면 설치된 파일 크기의 공간을 차지하게 되고 데이터는 최대 20 GB까지 추가할 수 있게 됩니다.

각 가상 머신 및 템플릿의 디스크 하위 탭에 디스크 크기가 나열됩니다. 디스크의 가상 크기는 가상 머신

이 사용할 수 있는 총 디스크 공간입니다. 이는 디스크 생성 또는 편집 시 크기(**GB**) 필드에 입력된 값입니다. 디스크의 **실제 크기**는 지금 까지 가상 머신에 할당된 디스크 공간입니다. 사전 할당된 디스크에서는 이 두 필드에 대해 동일한 값이 표시됩니다. 스파스 디스크는 할당된 디스크 용량에 따라 **실제 크기** 필드에 있는 값과 **가상 크기** 필드에 있는 값이 다를 수 있습니다.



참고

Cinder 가상 디스크 생성 시 디스크 포맷 및 유형은 Cinder에 의해 내부적으로 처리되며 Red Hat Virtualization에 의해 관리되지 않습니다.

다음 표에는 스토리지 유형 및 포맷의 가능한 조합에 대해 기재되어 있습니다.

표 11.1. 허용된 스토리지 조합

스토리지	포맷	유형	알림
NFS 또는 iSCSI/FCP	RAW 또는 QCOW2	스파스 또는 사전 할당	
NFS	RAW	사전 할당	가상 디스크에 대해 정의된 스토리지 용량과 동일한 초기 크기의 파일로 포맷되어 있지 않습니다.
NFS	RAW	스파스	초기 크기가 제로에 가까운 파일로 포맷되어 있지 않습니다.
NFS	QCOW2	스파스	초기 크기가 제로에 가까운 파일로 QCOW2 포맷되어 있습니다. 후속 레이어는 QCOW2로 포맷됩니다.
SAN	RAW	사전 할당	가상 디스크에 대해 지정된 스토리지 용량과 동일한 초기 크기의 블록 장치로 포맷되어 있지 않습니다.
SAN	QCOW2	스파스	가상 디스크 (현재 1 GB)에 대해 지정된 크기보다 작은 초기 크기의 블록 장치로 필요에 따라 공간을 할당하는(현재 1 GB 추가) QCOW2 포맷으로 되어 있습니다.

11.3. 삭제 후 디스크 장치 초기화 설정

관리 포털에서 **삭제 후 초기화** 확인란에 표시되는 **wipe_after_delete** 플래그는 가상 디스크 삭제 시 사용 데이터를 제로로 대체합니다. 기본값인 **false**로 설정되어 있을 경우 디스크 삭제 시 해당 블록을 다시 사용할 수 있지만 데이터를 초기화하는 것이 아닙니다. 블록은 제로로 처리되지 않기 때문에 데이터를

복원할 수 있습니다.

wipe_after_delete 플래그는 블록 스토리지에서만 작동합니다. 파일 시스템에 의해 데이터가 존재하지 않게 되므로 NFS 등의 파일 스토리지에서 해당 옵션은 아무 작업도 수행하지 않습니다.

가상 디스크의 **wipe_after_delete** 활성화는 가상 디스크에 중요한 데이터가 들어 있을 경우 권장되는 옵션입니다. 이는 보다 집약적 작업으로 시스템 성능이 저하되거나 삭제 시간이 오래 걸릴 수 있습니다.



참고

삭제 후 초기화 기능은 보안 삭제와 다릅니다. 이 기능은 데이터가 스토리지에서 제거되는 것을 보장하지 못하며 같은 스토리지에 생성되는 새로운 디스크가 이전 디스크의 데이터를 노출하지 않도록 합니다.

wipe_after_delete 플래그 기본값을 설정 프로세스에서 **true**로 변경(설치 가이드에 있는 [Red Hat Virtualization Manager 설정 참조](#))하거나 Red Hat Virtualization Manager의 engine 설정 도구를 사용하여 변경할 수 있습니다. 설정 변경 사항을 적용하려면 engine을 다시 시작합니다.

절차 11.1. Engine 설정 도구를 사용하여 SANWipeAfterDelete의 기본값을 True로 설정

1. **--set** 동작으로 engine 설정 도구를 실행합니다:

```
# engine-config --set SANWipeAfterDelete=true
```

2. 변경 사항을 적용하려면 engine을 다시 시작합니다:

```
# systemctl restart ovirt-engine.service
```

가상 디스크가 성공적으로 초기화 및 삭제되었는지 확인하기 위해서 호스트에 위치한 `/var/log/vdsm/vdsm.log` 파일을 확인합니다.

성공적으로 초기화되면 로그 파일에 **storage_domain_id/volume_id was zeroed and will be deleted** 항목이 표시됩니다. 예:

```
a9cb0625-d5dc-49ab-8ad1-72722e82b0bf/a49351a7-15d8-4932-8d67-512a369f9d61
was zeroed and will be deleted
```

성공적으로 삭제되면 로그 파일에 **finished with VG:storage_domain_id LVs: list_of_volume_ids, img: image_id** 항목이 표시됩니다. 예:

```
finished with VG:a9cb0625-d5dc-49ab-8ad1-72722e82b0bf LVs: {'a49351a7-15d8-4932-8d67-512a369f9d61':
  ImgsPar(imgs=['11f8b3be-fa96-4f6a-bb83-14c9b12b6e0d'], parent='00000000-0000-0000-0000-000000000000')},
img: 11f8b3be-fa96-4f6a-bb83-14c9b12b6e0d
```

초기화가 실패한 경우 **zeroing storage_domain_id/volume_id failed. Zero and remove this volume manually**라는 로그 메시지가 표시되며, 삭제가 실패한 경우 **Remove failed for some of VG: storage_domain_id zeroed volumes: list_of_volume_ids**라는 로그 메시지가 표시됩니다.

11.4. RED HAT VIRTUALIZATION에서 공유 가능한 디스크

일부 애플리케이션에는 서버간 공유 가능한 스토리지가 필요합니다. Red Hat Virtualization을 통해 가상 머신 하드 디스크를 공유 가능으로 표시하고 이러한 디스크를 가상 머신에 연결할 수 있습니다. 이러한 방법으로 하나의 단일 가상 디스크를 여러 클러스터 인식 게스트가 사용할 수 있습니다.

모든 상황에서 공유 디스크를 사용할 수는 없습니다. 클러스터된 데이터 베이스 서버 및 기타 고가용성 서비스와 같은 애플리케이션의 경우 공유 디스크를 사용하는 것이 적합합니다. 클러스터 인식되지 않는 여러 게스트에 공유 디스크를 연결하면 읽기 및 쓰기가 디스크에 연계되지 않기 때문에 데이터가 손상될 수 있습니다.

공유 디스크의 스냅샷을 생성할 수 없습니다. 스냅샷을 생성한 가상 디스크는 나중에 공유 가능한 디스크로 표시할 수 없습니다.

디스크 생성시 또는 나중에 디스크 편집 시 공유 가능한 디스크를 표시할 수 있습니다.

11.5. RED HAT VIRTUALIZATION에서 읽기 전용 디스크

일부 애플리케이션의 경우 관리자는 읽기 전용 권한이 있는 데이터를 공유해야 합니다. 가상 머신의 상세 정보 창에 있는 디스크 탭을 통해 가상 머신에 연결되는 디스크를 생성 또는 편집 시 읽기 전용 확인란을 선택하여 이를 수행할 수 있습니다. 이 때에 관리자는 쓰기 권한을 유지하면서 단일 디스크는 여러 클러스터 인식 게스트로 읽을 수 있습니다.

가상 머신이 실행되고 있는 동안 읽기 전용 상태를 변경할 수 없습니다.



중요

저널링된 파일 시스템을 마운트하려면 읽기-쓰기 액세스가 필요합니다. 그러한 파일 시스템(예: **EXT3**, **EXT4**, **XFS**)이 있는 가상 디스크에 읽기 전용 옵션을 사용하는 것은 적합하지 않습니다.

11.6. 가상 디스크 작업

11.6.1. 플로팅 가상 디스크 생성

가상 머신에 속하지 않은 가상 디스크를 생성할 수 있습니다. 그 뒤 단일 가상 머신이나 디스크가 공유 가능할 경우 여러 가상 머신에 디스크를 연결할 수 있습니다

이미지 디스크 생성은 전적으로 Manager에 의해 관리됩니다. 직접 LUN 디스크에는 이미 존재하는 외부에 준비된 대상이 필요합니다. Cinder 디스크에는 외부 공급자 창을 사용하여 Red Hat Virtualization 환경에 추가된 OpenStack Volume 인스턴스로의 액세스가 필요합니다. 보다 자세한 내용은 [12.2.4절. "스토리지 관리를 위해 OpenStack Volume \(Cinder\) 인스턴스 추가"](#)에서 참조하십시오.

절차 11.2. 플로팅 가상 디스크 생성

1. 디스크 리소스 탭을 선택합니다.
2. 새로 만들기를 클릭합니다.

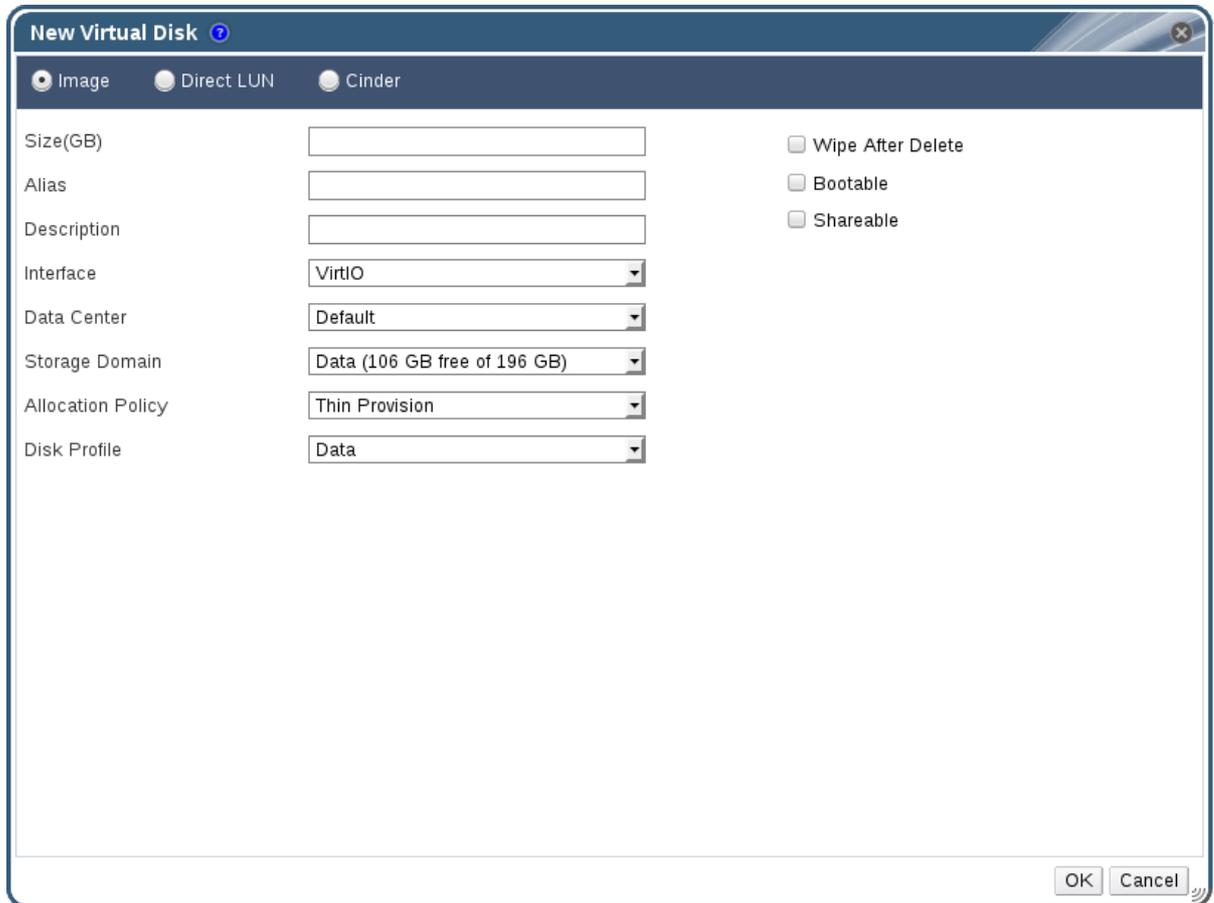


그림 11.1. 가상 디스크 추가 창

3. 라디오 버튼을 사용하여 가상 디스크를 이미지, 직접 LUN, Cinder 디스크 중 하나로 지정합니다.
4. 가상 디스크에 필요한 옵션을 선택합니다. 옵션은 선택한 디스크 유형에 따라 변경할 수 있습니다. 각각의 디스크 유형 별 각 옵션에 대한 자세한 내용은 11.6.2절. “새 가상 디스크 창에서 설정”에서 참조하십시오.
5. OK를 클릭합니다.

11.6.2. 새 가상 디스크 창에서 설정

표 11.2. 새 가상 디스크 설정: 이미지

필드 이름	설명
크기 (GB)	새 가상 디스크의 크기 (GB 단위)입니다.
별칭	가상 디스크 이름으로 최대 길이는 40 자로 제한되어 있습니다.
설명	가상 디스크에 대한 설명입니다. 이 필드는 권장 입력 사항이지 필수 입력 사항은 아닙니다.

필드 이름	설명
인터페이스	<p>디스크가 가상 머신에 표시되는 가상 인터페이스입니다. VirtIO는 빠르지만 드라이버가 필요합니다. Red Hat Enterprise Linux 5 및 이후 버전에는 이러한 드라이버가 포함되어 있습니다. Windows에는 이러한 드라이버가 포함되어 있지 않지만 게스트 도구 ISO 또는 가상 플로피 디스크에서 설치할 수 있습니다. IDE 장치에는 특정 드라이버가 필요하지 않습니다.</p> <p>디스크가 연결된 모든 가상 머신을 중지한 후 인터페이스 유형을 업데이트할 수 있습니다.</p>
데이터 센터	가상 디스크를 사용할 수 있는 데이터 센터입니다.
스토리지 도메인	가상 디스크가 저장될 스토리지 도메인입니다. 드롭다운 목록에는 지정된 데이터 센터에서 사용 가능한 모든 스토리지 도메인이 표시되어 있으며 스토리지 도메인에서 현재 사용 가능한 용량 및 총 용량이 표시되어 있습니다.
할당 정책	<p>새 가상 디스크의 프로비저닝 정책입니다.</p> <ul style="list-style-type: none"> • 사전 할당에서는 가상 디스크가 생성될 때 스토리지 도메인에 있는 전체 디스크 크기를 할당합니다. 사전 할당된 디스크의 실제 크기는 가상 크기와 동일합니다. 사전 할당된 가상 디스크는 쉐 프로비저닝 가상 디스크보다 생성 시간이 더 오래 걸리지만 읽기 및 쓰기 성능이 더 좋습니다. 서버 및 기타 다른 I/O 집약적 가상 디스크의 경우 사전 할당된 가상 디스크를 사용하는 것이 좋습니다. 가상 머신이 4 초마다 1 GB 이상을 쓰기 가능한 경우 가능하면 사전 할당된 디스크를 사용합니다. • 쉐 프로비저닝은 가상 디스크가 생성될 때 1 GB를 할당하고 디스크가 확장될 수 있는 최대 상한 크기를 설정합니다. 디스크의 가상 크기는 최대 상한 크기이고 디스크의 실제 크기는 지금까지 할당된 용량입니다. 쉐 프로비저닝 디스크는 사전 할당된 디스크보다 보다 빠르게 생성되며 스토리지 오버 커밋을 허용합니다. 데스크탑의 경우 쉐 프로비저닝 가상 디스크를 권장합니다.
디스크 프로파일	가상 디스크에 할당된 디스크 프로파일입니다. 디스크 프로파일은 스토리지 도메인에 있는 가상 디스크의 최대 처리량과 최대 입출력 수준을 정의합니다. 디스크 프로파일은 데이터 센터에 생성된 스토리지 QoS 항목에 기반하여 스토리지 도메인 수준에서 정의됩니다.
삭제 후 초기화	가상 디스크 삭제 시 중요 자료 삭제를 위해 보안을 강화할 수 있습니다.

필드 이름	설명
부팅 가능	가상 디스크에 부팅 가능한 플래그를 설정할 수 있습니다.
공유 가능	두 개 이상의 가상 머신에 동시에 가상 디스크를 연결할 수 있습니다.

직접 LUN 설정은 대상 > LUN 또는 LUN > 대상에 표시할 수 있습니다. 대상 > LUN은 LUN이 발견된 호스트에 따라 사용가능한 LUN을 정렬하며 LUN > 대상은 하나의 LUN 목록을 표시합니다.

표 11.3. 새 가상 디스크 설정: 직접 LUN

필드 이름	설명
별칭	가상 디스크 이름으로 최대 길이는 40 자로 제한되어 있습니다.
설명	가상 디스크에 대한 설명입니다. 이 필드는 권장 입력 사항이지 필수 입력 사항은 아닙니다. 기본값으로 LUN ID의 마지막 4자를 필드에 입력합니다. 기본 동작은 PopulateDirectLUNDiskDescriptionWithLUNId 설정 키를 engine-config 명령을 사용하여 적절한 값으로 설정할 수 있습니다. 전체 LUN ID를 사용할 경우 설정키를 -1 로 이러한 기능을 무시하고자 할 경우 0 으로 설정할 수 있습니다. 양의 정수로 해당 LUN ID와 설명을 입력합니다. 보다 자세한 내용은 18.2.2절. “ engine-config 명령 구문”에서 참조하십시오.
인터페이스	디스크가 가상 머신에 표시되는 가상 인터페이스입니다. VirtIO 는 빠르지만 드라이버가 필요합니다. Red Hat Enterprise Linux 5 및 이후 버전에는 이러한 드라이버가 포함되어 있습니다. Windows 에는 이러한 드라이버가 포함되어 있지 않지만 게스트 도구 ISO 또는 가상 플로피 디스크에서 설치할 수 있습니다. IDE 장치에는 특정 드라이버가 필요하지 않습니다. 디스크가 연결된 모든 가상 머신을 중지한 후 인터페이스 유형을 업데이트할 수 있습니다.
데이터 센터	가상 디스크를 사용할 수 있는 데이터 센터입니다.
사용 호스트	LUN이 마운트되는 호스트입니다. 데이터 센터에 있는 모든 호스트를 선택할 수 있습니다.
스토리지 유형	추가할 외부 LUN 유형입니다. iSCSI 또는 파이버 채널 중 하나를 선택할 수 있습니다.

필드 이름	설명
<p>대상 검색</p>	<p>이 부분은 iSCSI 외부 LUN 사용 시 확장되어 대상 > LUN이 선택됩니다.</p> <p>주소 - 대상 서버의 호스트 이름 또는 IP 주소입니다.</p> <p>포트 - 대상 서버에 연결 시도하는 포트입니다. 기본 포트는 3260입니다.</p> <p>사용자 인증 - iSCSI 서버에는 사용자 인증이 필요합니다. iSCSI 외부 LUN을 사용하는 경우 사용자 인증 필드를 볼 수 있습니다.</p> <p>CHAP 사용자 이름 - LUN에 로그인할 수 있는 권한을 갖는 사용자의 사용자 이름입니다. 사용자 인증 확인란을 선택하면 이 필드에 액세스할 수 있습니다.</p> <p>CHAP 암호 - LUN에 로그인할 수 있는 권한을 갖는 사용자의 암호입니다. 사용자 인증 확인란을 선택하면 이 필드에 액세스할 수 있습니다.</p>
<p>부팅 가능</p>	<p>가상 디스크에 부팅 가능한 플래그를 설정할 수 있습니다.</p>
<p>공유 가능</p>	<p>두 개 이상의 가상 머신에 동시에 가상 디스크를 연결할 수 있습니다.</p>
<p>SCSI 통과 활성화</p>	<p>인터페이스가 VirtIO-SCSI로 설정 시 사용 가능합니다. 이 확인란을 선택하면 물리적 SCSI 장치가 가상 디스크로 통과할 수 있습니다. VirtIO-SCSI 인터페이스에 SCSI 통과를 활성화하는 경우 자동으로 SCSI 폐기가 지원됩니다. 이 확인란을 선택 해제하면 가상 디스크가 에뮬레이트된 SCSI 장치를 사용합니다.</p>
<p>권한 부여된 SCSI I/O 허용</p>	<p>SCSI 통과 활성화 확인란 선택 시 사용 가능합니다. 이 확인란을 선택하면 필터링되지 않은 SCSI Generic I/O (SG_IO) 액세스가 활성화되어 권한이 부여된 SG_IO 명령이 디스크에서 허용됩니다. 영구적인 예약에 필요합니다.</p>

대상 검색 섹션에 있는 필드를 입력하고 검색을 클릭하여 대상 서버를 검색합니다. 전체 로그인 버튼을 클릭하여 대상 서버에 사용 가능한 LUN을 나열하고 각 LUN 옆에 있는 라디오 버튼을 사용하여 추가할 LUN을 선택할 수 있습니다.

가상 머신 하드 디스크 이미지로 LUN을 직접 사용하여 가상 머신과 데이터 사이에 추상화 계층을 삭제합니다.

가상 머신 하드 디스크 이미지로 직접 LUN을 사용하는 경우 다음과 같은 사항을 고려해야 합니다.

- 직접 LUN 하드 디스크 이미지의 라이브 스토리지 마이그레이션은 지원되지 않습니다.
- 직접 LUN 디스크는 가상 머신 내보내기에 포함되지 않습니다.
- 직접 LUN 디스크는 가상 머신 스냅샷에 포함되지 않습니다.

관련 데이터 센터에 있는 디스크를 생성할 수 있는 권한이 있는 사용 가능한 OpenStack 볼륨 스토리지 도메인이 없을 경우 **Cinder** 설정 양식을 사용할 수 없습니다. **Cinder** 디스크는 **외부 공급자** 창을 사용하는 Red Hat Virtualization 환경에 추가된 OpenStack 볼륨 인스턴스에 액세스할 수 있어야 합니다. 보다 자세한 내용은 [12.2.4절. “스토리지 관리를 위해 OpenStack Volume \(Cinder\) 인스턴스 추가”](#)에서 참조하십시오.

표 11.4. 새 가상 디스크 설정: **Cinder**

필드 이름	설명
크기 (GB)	새 가상 디스크의 크기 (GB 단위)입니다.
별칭	가상 디스크 이름으로 최대 길이는 40 자로 제한되어 있습니다.
설명	가상 디스크에 대한 설명입니다. 이 필드는 권장 입력 사항이지 필수 입력 사항은 아닙니다.
인터페이스	디스크가 가상 머신에 표시되는 가상 인터페이스입니다. VirtIO 는 빠르지만 드라이버가 필요합니다. Red Hat Enterprise Linux 5 및 이후 버전에는 이러한 드라이버가 포함되어 있습니다. Windows에는 이러한 드라이버가 포함되어 있지 않지만 게스트 도구 ISO 또는 가상 플로피 디스크에서 설치할 수 있습니다. IDE 장치에는 특정 드라이버가 필요하지 않습니다. 디스크가 연결된 모든 가상 머신을 중지한 후 인터페이스 유형을 업데이트할 수 있습니다.
데이터 센터	가상 디스크를 사용할 수 있는 데이터 센터입니다.
스토리지 도메인	가상 디스크가 저장될 스토리지 도메인입니다. 드롭 다운 목록에는 지정된 데이터 센터에서 사용 가능한 모든 스토리지 도메인이 표시되어 있으며 스토리지 도메인에서 현재 사용 가능한 용량 및 총 용량이 표시되어 있습니다.
볼륨 유형	가상 디스크의 볼륨 유형입니다. 드롭 다운 목록에 사용 가능한 모든 볼륨 유형이 표시됩니다. 볼륨 유형은 OpenStack Cinder에서 관리 및 설정됩니다.
부팅 가능	가상 디스크에 부팅 가능한 플래그를 설정할 수 있습니다.
공유 가능	두 개 이상의 가상 머신에 동시에 가상 디스크를 연결할 수 있습니다.

11.6.3. 라이브 스토리지 마이그레이션 개요

연결된 가상 머신이 실행되고 있는 동안 가상 디스크를 하나의 스토리지 도메인에서 다른 스토리지 도메인으로 마이그레이션할 수 있습니다. 이를 라이브 스토리지 마이그레이션이라고 합니다. 실행 중인 가상 머신에 연결된 디스크를 마이그레이션할 경우 디스크 이미지 체인의 스냅샷이 소스 스토리지 도메인에 생성되고 전체 이미지 체인이 대상 스토리지 도메인에 복제됩니다. 따라서 소스 스토리지 도메인과 대상 스

토리지 도메인 모두에 디스크 이미지 체인과 스냅샷 둘 다를 호스트하기에 충분한 스토리지 공간이 있어야 합니다. 마이그레이션이 실패하는 경우에도 라이브 스토리지 마이그레이션을 시도할 때마다 새 스냅샷이 생성됩니다.

라이브 스토리지 마이그레이션 사용 시 다음과 같은 사항을 고려해야 합니다:

- 한 번에 여러 디스크를 라이브 마이그레이션할 수 있습니다.
- 동일한 가상 머신의 여러 디스크를 여러 스토리지 도메인에 걸쳐 배치할 수 있지만 각 디스크의 이미지 체인은 하나의 스토리지 도메인에 있어야 합니다.
- 동일한 데이터 센터의 두 스토리지 도메인 간에 디스크를 라이브 마이그레이션할 수 있습니다.
- 직접 LUN 하드 디스크 이미지 또는 공유 가능으로 표시된 디스크는 라이브 마이그레이션할 수 없습니다.

11.6.4. 가상 디스크 이동

가상 머신에 연결되어 있거나 하나의 스토리지 도메인에서 다른 스토리지 도메인으로 플로팅 가상 디스크처럼 동작하는 가상 디스크를 이동합니다. 연결된 가상 디스크를 실행 중인 가상 머신에 이동할 수 있습니다. 이는 라이브 스토리지 마이그레이션이라고 합니다. 이를 계속 진행하기 전 가상 머신을 종료합니다.

디스크를 이동할 때 다음과 같은 사항을 고려해야 합니다:

- 동시에 여러 디스크를 이동할 수 있습니다.
- 동일한 데이터 센터의 두 스토리지 도메인 간에 디스크를 이동할 수 있습니다.
- 가상 디스크가 템플릿을 기반으로 생성되어 썸 프로비저닝 스토리지 할당 옵션을 사용하여 생성된 가상 머신에 연결되어 있을 경우 가상 머신의 기반이 되는 템플릿의 디스크를 가상 디스크와 동일한 스토리지 도메인에 복사해야 합니다.

절차 11.3. 가상 디스크 이동

1. 디스크 탭을 선택합니다.
2. 이동할 하나 이상의 가상 디스크를 선택합니다.
3. 이동을 클릭하여 **디스크 이동** 창을 엽니다.
4. 대상 목록에서 가상 디스크를 이동할 스토리지 도메인을 선택합니다.
5. 디스크 프로파일 목록에서 디스크의 프로파일을 선택합니다.
6. **OK**를 클릭합니다.

가상 디스크는 대상 스토리지 도메인으로 이동됩니다. 이동 절차 동안 **상태** 열에는 **Locked** 및 이동 작업의 진행 상황을 보여주는 진행 상태 표시줄이 표시됩니다.

11.6.5. 디스크 인터페이스 유형 변경

사용자는 디스크를 생성한 후 디스크의 인터페이스 유형을 변경할 수 있습니다. 이를 통해 다른 인터페이스 유형이 필요한 가상 머신에 기존 디스크를 연결할 수 있습니다. 예를 들어 **VirtIO** 인터페이스를 사용하는 디스크를 **VirtIO-SCSI** 또는 **IDE** 인터페이스가 필요한 가상 머신에 연결할 수 있습니다. 그러면 백

업 및 복원 또는 재해 복구를 목적으로 디스크를 유연하게 마이그레이션할 수 있습니다. 또한 공유 가능한 디스크의 디스크 인터페이스를 가상 머신별로 업데이트할 수 있습니다. 따라서 공유 디스크를 사용하는 각 가상 머신이 다른 인터페이스 유형을 사용할 수 있습니다.

디스크 인터페이스 유형을 업데이트하려면 디스크를 사용하는 모든 가상 머신을 먼저 중지해야 합니다.

절차 11.4. 디스크 인터페이스 유형 변경

1. **가상 머신** 탭을 선택하고 해당하는 가상 머신을 중지합니다.
2. **디스크** 하위 탭에서 디스크를 선택하고 **편집**을 클릭합니다.
3. **인터페이스** 목록에서 새 인터페이스 유형을 선택하고 **OK**를 클릭합니다.

이제 가상 머신에서 해당 디스크에 대해 다른 가상 인터페이스를 사용합니다.

다음 절차는 다른 인터페이스 유형이 필요한 다른 가상 머신에 디스크를 연결하는 방법을 보여줍니다.

절차 11.5. 다른 인터페이스 유형을 사용하여 다른 가상 머신에 디스크 연결

1. **가상 머신** 탭을 선택하고 해당하는 가상 머신을 중지합니다.
2. 디스크를 분리할 가상 머신을 선택합니다.
3. **디스크** 하위 탭에서 디스크를 선택하고 **제거**를 클릭합니다.
4. **가상 머신** 탭에서 디스크를 연결할 새 가상 머신을 선택합니다.
5. **연결**을 클릭합니다.
6. **가상 디스크 연결** 창에서 디스크를 선택하고 **인터페이스** 드롭 다운에서 해당하는 인터페이스를 선택합니다.
7. **OK**를 클릭합니다.

11.6.6. 가상 디스크 복사

요약

하나의 스토리지 도메인에서 다른 도메인으로 가상 디스크를 복사할 수 있습니다. 복사된 디스크는 가상 머신에 연결될 수 있습니다.

절차 11.6. 가상 디스크 복사

1. **디스크** 탭을 선택합니다.
2. 복사할 가상 디스크를 선택합니다.
3. **복사** 버튼을 클릭하여 **디스크 복사** 창을 엽니다.
4. 옵션으로 **별칭** 텍스트 필드에 별칭을 입력합니다.
5. **대상** 드롭 다운 메뉴를 사용하여 가상 머신을 복사할 스토리지 도메인을 선택합니다.
6. **OK**를 클릭합니다.

결과

가상 디스크가 대상 스토리지 도메인에 복사되며 복사되는 동안 **Locked** 상태가 됩니다.

11.6.7. 디스크 이미지를 스토리지 도메인에 업로드 및 다운로드

QEMU 호환 가능 가상 디스크 이미지를 로컬 시스템에서 Red Hat Virtualization 스토리지 도메인으로 업로드하여 가상 머신에 연결할 수 있습니다.

가상 디스크 이미지 유형은 QCOW2 또는 Raw여야 합니다. QCOW2 디스크 이미지에서 생성한 디스크는 공유할 수 없으며 QCOW2 디스크 이미지 파일에는 지원 파일이 있어서는 안 됩니다.

디스크 이미지는 Manager 또는 REST API를 사용하여 업로드할 수 있지만 다운로드는 REST API를 사용해서만 가능합니다. REST API를 사용할 경우 **IMAGETRANSFERS** 서비스를 사용하여 전송을 하고 **IMAGETRANSFER** 서비스를 사용하여 이미지를 업로드할지 또는 다운로드할지를 지정합니다.

이러한 서비스와 함께 사용할 수 있는 사용 가능한 모든 방법에 관한 자세한 내용은 *REST API 가이드*에 있는 **IMAGETRANSFERS** 및 **IMAGETRANSFER**를 참조하십시오.

전제 조건:

- **engine-setup** 실행 시 이미지 I/O 프록시를 설정해야 합니다. 자세한 내용은 *설치 가이드*에 있는 **Red Hat Virtualization Manager 설정**을 참조하십시오.
- 관리 포털 액세스에 사용되는 웹 브라우저로 필수 인증 기관을 가져와야 합니다.
- 이 업로드 절차를 수행하려면 Internet Explorer 10, Firefox 35 또는 Chrome 13 이상이 필요합니다. 이전 브라우저 버전은 필수 HTML5 API를 지원하지 않습니다.



참고

인증 기관을 가져오려면 https://engine_address/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA로 이동하고 신뢰할 수 있는 모든 설정을 선택합니다. 지침을 참조하여 **Firefox**, **Internet Explorer** 또는 **Google Chrome**에서 인증 기관을 설치하십시오.

절차 11.7. 디스크 이미지를 스토리지 도메인에 업로드

1. 이미지 업로드 화면을 엽니다.
 - 디스크 탭의 **업로드** 드롭 다운에서 **시작**을 선택합니다.
 - 또는 스토리지 탭에서 스토리지 도메인을 선택한 다음 **디스크** 하위 탭을 선택하고 **업로드** 드롭 다운에서 **시작**을 선택합니다.

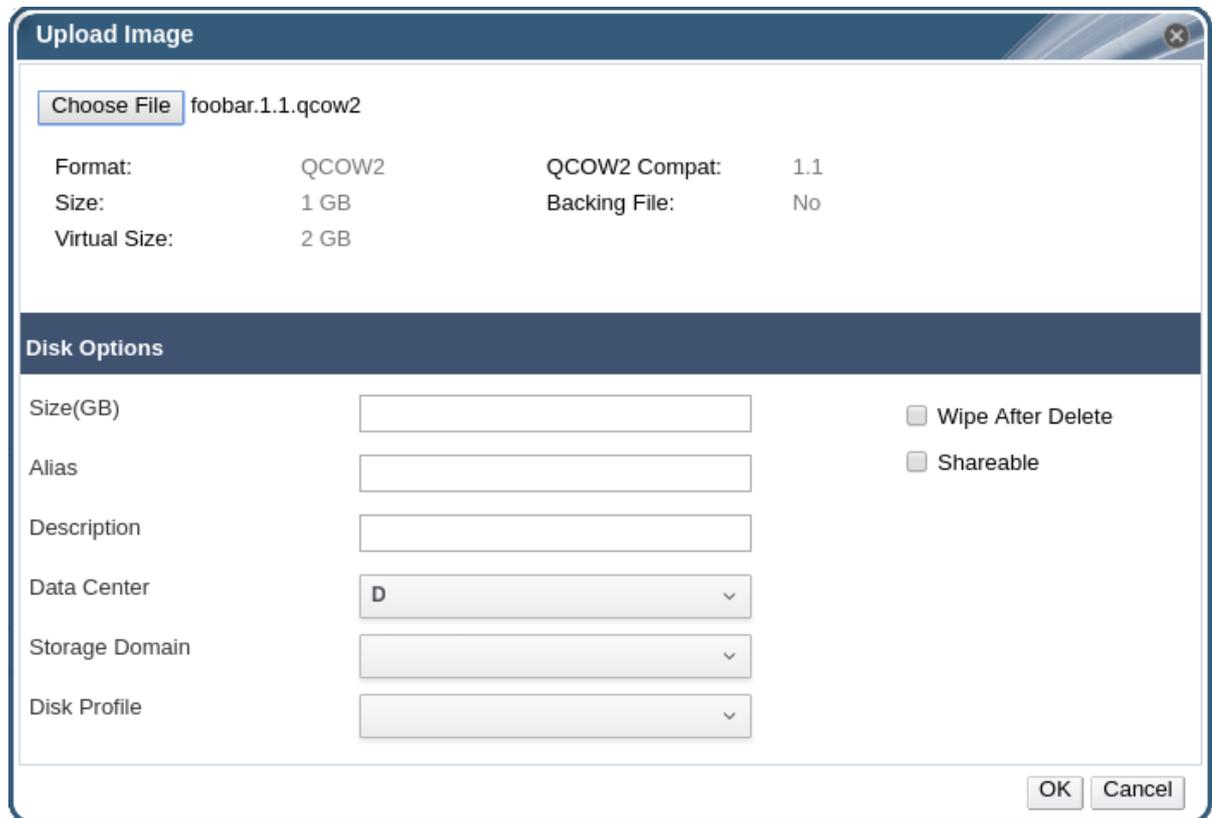


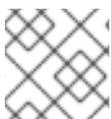
그림 11.2. 이미지 업로드 화면

2. 이미지 업로드 화면에서 파일 선택을 클릭하고 로컬 디스크에서 이미지를 선택합니다. 선택한 파일에 대한 정보가 표시됩니다.
3. 디스크 옵션 필드를 작성합니다. 관련 필드의 설명에 대한 내용은 11.6.2절. “새 가상 디스크 창에서 설정”를 참조하십시오.
4. **OK**를 클릭합니다.

진행률 표시줄은 업로드 상태를 나타냅니다. 또한 업로드 드롭 다운에서 업로드를 일시 중지, 취소 또는 다시 시작할 수 있습니다.

11.6.8. 가져온 스토리지 도메인에서 디스크 이미지 가져오기

가져온 스토리지 도메인에서 플로팅 가상 디스크를 가져오기 위해 상세 정보 창의 **디스크 불러오기** 탭을 사용합니다.



참고

QEMU와 호환되는 디스크만 Manager로 불러올 수 있습니다.

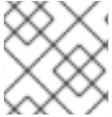
절차 11.8. 디스크 이미지 가져오기

1. 데이터 센터로 가져온 스토리지 도메인을 선택합니다.
2. 상세 정보 창에서 **디스크 불러오기**를 클릭합니다.
3. 하나 이상의 디스크 이미지를 선택 후 **가져오기**를 클릭하여 **디스크 불러오기** 창을 엽니다.
4. 각 디스크의 적절한 **디스크 프로파일**을 선택합니다.

5. **OK**를 클릭하여 선택된 디스크를 가져옵니다.

11.6.9. 가져온 스토리지 도메인에서 미등록된 디스크 이미지 가져오기

스토리지 도메인에서 플로팅 가상 디스크를 가져오기 위해 상세 정보 창의 **디스크 불러오기** 탭을 사용합니다. Red Hat Virtualization 환경 외부(outside)에서 생성된 플로팅 디스크는 **Manager**에 등록되어 있지 않습니다. 미등록된 플로팅 디스크를 찾아서 가져오기 위하여 스토리지 도메인을 검색합니다.



참고

QEMU와 호환되는 디스크만 **Manager**로 가져올 수 있습니다.

절차 11.9. 디스크 이미지 불러오기

1. 데이터 센터로 가져온 스토리지 도메인을 선택합니다.
2. 스토리지 도메인을 오른쪽 클릭하고 **디스크 검사**를 선택하여 **Manager**가 미등록된 디스크를 찾습니다.
3. 상세 정보 창에서 **디스크 불러오기**를 클릭합니다.
4. 하나 이상의 디스크 이미지를 선택 후 **가져오기**를 클릭하여 **디스크 불러오기** 창을 엽니다.
5. 각 디스크의 적절한 **디스크 프로파일**을 선택합니다.
6. **OK**를 클릭하여 선택된 디스크를 가져옵니다.

11.6.10. OpenStack 이미지 서비스에서 가상 디스크 이미지 가져오기

요약

OpenStack 이미지 서비스가 외부 공급자로 **Manager**에 추가될 경우 OpenStack 이미지 서비스에 의해 관리되는 가상 디스크 이미지를 Red Hat Virtualization **Manager**로 가져올 수 있습니다.

1. 스토리지 리소스 탭을 클릭하고 검색 결과 목록에서 **OpenStack** 이미지 서비스 도메인을 선택합니다.
2. 상세 정보 창의 **이미지** 탭에 가져오기할 이미지를 선택합니다.
3. **가져오기** 버튼을 클릭하여 **이미지 가져오기** 창을 엽니다.
4. **데이터 센터** 드롭 다운 메뉴에서 가상 디스크 이미지를 가져오기할 데이터 센터를 선택합니다.
5. **도메인 이름** 드롭 다운 메뉴에서 가상 디스크 이미지를 저장할 스토리지 도메인을 선택합니다.
6. 옵션으로 **쿼터** 드롭 다운 메뉴에서 가상 디스크 이미지에 적용할 쿼터를 선택합니다.
7. **OK**를 클릭하여 이미지를 가져옵니다.

결과

이미지가 플로피 디스크로 가져오기되어 **디스크 리소스** 탭의 결과 목록에 표시됩니다. 이제 이를 가상 머신에 연결할 수 있습니다.

11.6.11. OpenStack 이미지 서비스에 가상 디스크 내보내기

요약

외부 공급자로 Manager에 추가된 OpenStack 이미지 서비스에 가상 디스크를 내보낼 수 있습니다.

1. 디스크 리소스 탭을 선택합니다.
2. 내보내기할 디스크를 선택합니다.
3. 내보내기 버튼을 클릭하여 이미지 내보내기 창을 엽니다.
4. 도메인 이름 드롭 다운 메뉴에서 디스크를 내보내기할 OpenStack 이미지를 선택합니다.
5. 쿼터를 설정할 경우 쿼터 드롭 다운 목록에서 해당 디스크 쿼터를 선택합니다.
6. OK를 클릭합니다.

결과

가상 디스크가 지정된 OpenStack 이미지 서비스로 내보내기되어 해당 서비스에서 가상 디스크 이미지로 관리됩니다.



중요

가상 디스크는 볼륨이 여러 개가 아니고, 썸 프로비저닝되어 있지 않으며, 스냅샷이 없을 경우에만 내보낼 수 있습니다.

11.6.12. 가상 머신 디스크 공간 확보

썸 프로비저닝을 사용하는 가상 머신 디스크는 파일 삭제 후 자동으로 축소되지 않습니다. 예를 들어 실제 디스크 크기가 100GB이고 50GB의 파일을 삭제하는 경우 할당된 디스크 크기는 100GB로 남아 있으며 나머지 50GB는 호스트에 반환되지 않으므로 다른 가상 머신에서 사용할 수 없습니다. 가상 머신 디스크에서 스파스(sparse) 형식으로 변환하는 작업을 수행하면 사용되지 않는 디스크 공간을 호스트에서 확보할 수 있습니다. 그러면 디스크 이미지에서 호스트로 여유 공간이 전송됩니다.

가상 머신을 복제하거나 가상 머신을 기반으로 템플릿을 생성하거나 스토리지 도메인의 디스크 공간을 정리하기 전에 이 작업을 수행하는 것이 좋습니다.

제한 사항

- NFS 스토리지 도메인은 NFS 버전 4.2 이상을 사용해야 합니다.
- 직접 LUN 또는 Cinder를 사용하는 디스크를 스파스(sparse) 형식으로 변환할 수 없습니다.
- 사전 할당된 할당 정책을 사용하는 디스크를 스파스(sparse) 형식으로 변환할 수 없습니다. 템플릿에서 가상 머신을 생성 중인 경우 스토리지 할당 필드에서 썸 프로비저닝을 선택해야 합니다. 또는 복제를 선택하는 경우 템플릿이 썸 프로비저닝이 있는 가상 머신을 기반으로 하는지 확인해야 합니다.
- 활성 스냅샷만 스파스(sparse) 형식으로 변환할 수 있습니다.

절차 11.10. 디스크를 스파스(sparse) 형식으로 변환

1. 가상 머신 탭을 클릭하고 가상 머신을 선택합니다. 상태가 Down으로 표시되는지 확인합니다. 가상 머신이 실행 중인 경우 진행하기 전에 종료해야 합니다.
2. 상세 정보 창에서 디스크 탭을 선택합니다. 상태가 OK로 표시되는지 확인합니다.

3. **스파스 형식으로 변환** 버튼을 선택합니다. **디스크 스파스(sparse) 변환** 창에 선택한 디스크의 스파스 형식 변환 작업을 확인하도록 메시지가 표시됩니다.

4. **OK**를 클릭합니다.

Started to sparsify 이벤트가 스파스(sparse) 변환 작업 동안 창 하단에 있는 **이벤트** 탭에 나타나며 디스크 상태가 **Locked**로 표시됩니다. 작업이 완료되면 **Sparsified successfully** 이벤트가 **이벤트** 탭에 나타나며 디스크 상태가 **OK**로 표시됩니다. 사용되지 않는 디스크 공간이 호스트에 반환되었으며 다른 가상 머신에서 사용 가능합니다.



참고

병렬로 여러 가상 머신 디스크를 스파스(sparse) 형식으로 변환할 수 있습니다.

11.7. 가상 디스크 및 권한

11.7.1. 가상 디스크의 시스템 권한 관리

SuperUser로서 시스템 관리자는 관리 포털의 모든 면을 관리합니다. 보다 특정한 관리 역할은 다른 사용자에게 부여될 수 있습니다. 이러한 제한된 관리자 역할은 특정 리소스에 제한하여 사용자 관리 권한을 부여할 경우 유용합니다. 예를 들어 **DataCenterAdmin** 역할은 데이터 센터의 스토리지를 제외한 할당된 데이터 센터에 대해서만 관리자 권한을 갖으며 **ClusterAdmin**은 할당된 클러스터에 대해서만 관리자 권한을 갖습니다.

Red Hat Virtualization Manager는 두 개의 기본 가상 디스크 사용자 역할을 제공하지만 기본 가상 디스크 관리자 역할은 제공하지 않습니다. 이러한 사용자 역할 중 하나는 **DiskCreator** 역할로 사용자 포털에서 가상 디스크를 관리할 수 있게 합니다. 이 역할은 특정 가상 머신, 데이터 센터, 특정 스토리지 도메인, 전체 가상화 환경에 적용할 수 있습니다. 이는 다른 사용자가 다른 가상 리소스를 관리할 수 있도록 하는데 유용합니다.

가상 디스크 생성자 (creator) 역할은 다음과 같은 작업을 허용합니다:

- 가상 머신 또는 다른 리소스에 연결된 가상 머신 생성, 편집, 삭제
- 가상 디스크의 사용자 권한 편집



참고

기존 사용자에게만 역할 및 권한을 할당할 수 있습니다.

11.7.2. 가상 디스크 사용자 역할

가상 디스크 사용자 권한 역할

아래 표에서는 사용자 포털에서 가상 디스크의 사용 및 관리를 위해 적용할 수 있는 사용자 역할 및 권한에 대해 설명합니다.

표 11.5. **Red Hat Virtualization** 시스템 관리자 역할

역할	권한	알림
----	----	----

역할	권한	알림
DiskOperator	가상 디스크 사용자입니다.	가상 디스크를 사용, 보기, 편집할 수 있습니다. 가상 디스크가 연결된 가상 머신을 사용하기 위해 권한을 상속합니다.
DiskCreator	할당된 클러스터 또는 데이터 센터 내에서 가상 디스크를 생성, 편집, 관리, 제거할 수 있습니다.	이 역할은 특정 가상 디스크에는 적용되지 않습니다. 설정 창을 사용하여 전체 환경에 대한 사용자에게 이 역할을 적용할 수 있습니다. 또는 특정 데이터 센터, 클러스터, 스토리지 도메인에 이 역할을 적용할 수 있습니다.

11.7.3. 리소스에 관리자 또는 사용자 역할 할당

리소스에 관리자 또는 사용자 역할을 할당하여 사용자가 리소스에 액세스 및 관리할 수 있게 합니다.

절차 11.11. 리소스에 역할 할당

1. 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 리소스를 검색 및 선택합니다.
2. 상세 정보 창에 있는 **권한** 탭을 클릭하여 할당된 사용자, 사용자 역할, 선택한 리소스에 대해 상속된 권한을 나열합니다.
3. **추가**를 클릭합니다.
4. **검색** 텍스트 상자에 기존 사용자의 이름 또는 사용자 이름을 입력하고 **검색**을 클릭합니다. 검색 결과 목록에서 일치하는 사용자를 선택합니다.
5. **할당할 역할** 드롭 다운 목록에서 역할을 선택합니다.
6. **OK**를 클릭합니다.

사용자에게 역할이 할당되어 이제 사용자는 리소스에 대해 활성화된 역할에 상속된 권한을 갖습니다.

11.7.4. 리소스에서 관리자 또는 사용자 역할 삭제

리소스에서 관리자 또는 사용자 역할을 삭제합니다. 사용자는 리소스에서의 역할과 관련하여 상속된 권한을 손실합니다.

절차 11.12. 리소스에서 역할 삭제

1. 리소스 탭, 트리 모드 또는 검색 기능을 사용하여 검색 결과 목록에서 리소스를 검색 및 선택합니다.
2. 상세 정보 창에 있는 **권한** 탭을 클릭하여 할당된 사용자 목록, 사용자 역할, 선택한 리소스에서 상속된 권한을 나열합니다.
3. 리소스에서 삭제할 사용자를 선택합니다.
4. **삭제**를 클릭합니다. **권한 삭제** 창이 열리면 권한 삭제를 확인합니다.

5. **OK**를 클릭합니다.

리소스에서 사용자 역할 및 관련된 권한이 삭제됩니다.

12장. 외부 공급자

12.1. RED HAT VIRTUALIZATION에서 외부 공급자 소개

Red Hat Virtualization Manager 자체에 의해 관리되는 리소스에 더하여 Red Hat Virtualization은 외부 소스에 의해 관리되는 리소스를 이용할 수 있습니다. 외부 공급자로 알려진 이러한 리소스 공급자는 가상화 호스트, 가상 머신 이미지, 네트워크와 같은 리소스를 제공할 수 있습니다.

Red Hat Virtualization은 현재 다음과 같은 외부 공급자를 지원하고 있습니다:

호스트 프로비저닝을 위한 Red Hat Satellite

Satellite는 물리 및 가상 호스트의 모든 라이프 사이클 측면을 관리하기 위한 도구입니다. Red Hat Virtualization에서 Satellite에 의해 관리되는 호스트는 Red Hat Virtualization Manager에 의해 가상화 호스트로 추가 및 사용될 수 있습니다. Manager에 Satellite 인스턴스를 추가한 후 Satellite에 의해 관리되는 호스트는 새 호스트 추가 시 Satellite 인스턴스에서 사용 가능한 호스트를 검색하여 추가할 수 있습니다. For more information on installing Red Hat Satellite 설치 및 Red Hat Satellite을 사용한 호스트 관리에 대한 보다 자세한 내용은 [Installation Guide](#) 및 [Host Configuration Guide](#)에서 참조하십시오.

이미지 관리 용 OpenStack Image Service (Glance)

OpenStack Image Service는 가상 머신 이미지 카탈로그를 제공합니다. Red Hat Virtualization에서 이러한 이미지를 Red Hat Virtualization Manager로 가져와 플로팅 디스크로 사용하거나 가상 머신에 연결하여 템플릿으로 변환할 수 있습니다. OpenStack Image Service를 Manager에 추가하면 데이터 센터에 연결되지 않는 스토리지 도메인으로 나타납니다. Red Hat Virtualization 환경에서 가상 디스크는 가상 디스크 이미지로 OpenStack Image Service에 내보낼 수도 있습니다.

네트워크 프로비저닝 용 OpenStack Networking (Neutron)

OpenStack Networking은 소프트웨어 정의 네트워크를 제공합니다. Red Hat Virtualization에서 OpenStack Networking이 제공하는 네트워크를 Red Hat Virtualization Manager로 가져올 수 있으며 모든 트래픽 유형을 전송하고 복잡한 네트워크 토폴로지를 생성하는데 사용할 수 있습니다. Manager에 OpenStack Networking을 추가한 후 OpenStack Networking이 제공하는 네트워크를 수동으로 가져오기하여 액세스할 수 있습니다.

스토리지 관리 용 OpenStack Volume (Cinder)

OpenStack Volume은 가상 하드 드라이브의 영구 블록 스토리지 관리를 제공합니다. OpenStack Cinder 볼륨은 OpenStack Cinder에 의해 제공됩니다. Red Hat Virtualization에서는 OpenStack Volume 스토리지에 플로팅 디스크로 사용하거나 가상 머신에 연결할 디스크를 생성할 수 있습니다. Manager에 OpenStack Volume을 추가한 후 OpenStack Volume에서 제공하는 스토리지에 디스크를 생성할 수 있습니다.

가상 머신 프로비저닝 용 VMware

VMware에 생성된 가상 머신은 V2V (virt-v2v)를 사용하여 변환한 후 Red Hat Virtualization 환경으로 가져올 수 있습니다. Manager에 VMware 공급자를 추가한 후 해당 공급자가 제공하는 가상 머신을 가져올 수 있습니다. V2V 변환은 가져오기 작업의 일부로 지정된 프로시 호스트에서 실행됩니다.

네트워크 프로비저닝용 외부 네트워크 공급자

지원되는 외부 소프트웨어 정의 네트워크 공급자에는 OpenStack Neutron REST API를 구현하는 모든 공급자가 포함됩니다. OpenStack Networking(Neutron)과 달리 Neutron 에이전트는 호스트에서 가상 인터페이스 드라이버 구현으로 사용되지 않으며 외부 네트워크 공급자의 작업 구현자가 가상 인터페이스 드라이버를 제공해야 합니다.

모든 외부 리소스 공급자는 하나의 창을 사용하여 입력에 따라 추가됩니다. Red Hat Virtualization 환경에서 제공하는 리소스를 사용하기 전 리소스 공급자를 추가해야 합니다.

12.2. 외부 공급자 추가

12.2.1. 호스트 프로비저닝을 위한 Red Hat Satellite 인스턴스 추가

호스트 프로비저닝을 위한 Satellite 인스턴스를 Red Hat Virtualization Manager에 추가합니다. Red Hat Satellite 6.1에서는 Red Hat Virtualization 4.1이 지원됩니다.

절차 12.1. 호스트 프로비저닝을 위한 Satellite 인스턴스 추가

1. 트리 창에서 **외부 공급자** 항목을 선택합니다.
2. 추가를 클릭하여 공급자 추가 창을 엽니다.

그림 12.1. 공급자 추가 창

3. 이름 및 설명을 입력합니다.
4. 유형 목록에서 **Foreman/Satellite**가 선택되어 있는지 확인합니다.
5. 공급자 URL 텍스트 필드에 Satellite 인스턴스가 설치된 시스템의 URL 또는 정규화된 도메인 이름을 입력합니다. 포트 번호를 지정할 필요는 없습니다.



중요

Satellite 인스턴스를 추가하는 데 IP 주소를 사용할 수 없습니다.

6. **Satellite** 인스턴스의 **사용자 이름** 및 **암호**를 입력합니다. **Satellite** 프로비저닝 포털 로그인에 사용하고자 하는 동일한 사용자 이름 및 암호를 사용해야 합니다.
7. 인증 정보 테스트:
 - a. **테스트**를 클릭하여 지정된 인증 정보로 **Satellite** 인스턴스를 성공적으로 인증할 수 있는지 테스트합니다.
 - b. **Satellite** 인스턴스가 **SSL**을 사용할 경우 **공급자 인증서 가져오기** 창을 엽니다. **OK**를 클릭하여 **Satellite** 인스턴스가 제공하는 인증서를 가져옵니다.



중요

Manager가 인스턴스와 통신할 수 있는지를 확인하기 위해 **Satellite** 인스턴스가 제공하는 인증서를 가져와야 합니다.

8. **OK**를 클릭합니다.

Red Hat Virtualization Manager에 **Satellite** 인스턴스를 추가하여 인스턴스가 제공하는 호스트를 사용하여 작업할 수 있습니다.

12.2.2. 이미지 관리를 위해 **OpenStack Image (Glance)** 인스턴스 추가

이미지 관리를 위해 Red Hat Virtualization Manager에 **OpenStack Image (Glance)** 인스턴스를 추가합니다.

절차 12.2. 이미지 관리를 위해 **OpenStack Image (Glance)** 인스턴스 추가

1. 트리 창에서 **외부 공급자** 항목을 선택합니다.
2. **추가**를 클릭하여 **공급자 추가** 창을 엽니다.

그림 12.2. 공급자 추가 창

3. 이름 및 설명을 입력합니다.
4. 유형 목록에서 **OpenStack Image**를 선택합니다.
5. 공급자 **URL** 텍스트 필드에 OpenStack Image 인스턴스가 설치된 시스템의URL 또는 정규화된 도메인 이름(FQDN)을 입력합니다.
6. 옵션으로 인증 필요 확인란을 선택하고 OpenStack Image 인스턴스의 사용자 이름, 암호, 테넌트 이름, 인증 URL을 입력합니다. Keystone에 등록된 OpenStack Image 사용자의 사용자 이름 및 암호와 OpenStack Image 인스턴스가 속한 테넌트 및 Keystone 서버 포트 및 URL을 사용해야 합니다.
7. 인증 정보 테스트:
 - a. 테스트를 클릭하여 지정된 인증 정보로 OpenStack Image 인스턴스를 성공적으로 인증할 수 있는지 테스트합니다.
 - b. OpenStack Image 인스턴스가 SSL을 사용할 경우 공급자 인증서 가져오기 창이 열리면 **OK**를 클릭하여 OpenStack Image 인스턴스가 제공하는 인증서를 가져옵니다.



중요

Manager가 인스턴스와 통신할 수 있는지를 확인하려면 OpenStack Image 인스턴스가 제공하는 인증서를 가져오기해야 합니다.

8. **OK**를 클릭합니다.

OpenStack Image 인스턴스를 Red Hat Virtualization Manager에 추가하여 인스턴스가 제공하는 이미지로 작업할 수 있습니다.

12.2.3. 네트워크 프로비저닝을 위해 **OpenStack Networking (Neutron)** 인스턴스 추가

네트워크 프로비저닝을 위해 Red Hat Virtualization Manager에 OpenStack Networking (Neutron) 인스턴스를 추가합니다. OpenStack Neutron REST API를 구현하는 타사 네트워크 공급자를 추가하는 방법은 12.2.6절. “외부 네트워크 공급자 추가”에서 참조하십시오.



중요

Red Hat Virtualization은 Red Hat OpenStack Platform 8, 9, 10을 외부 네트워크 공급자로 지원합니다.

절차 12.3. 네트워크 프로비저닝을 위해 **OpenStack Networking (Neutron)** 인스턴스 추가

1. 트리 창에서 **외부 공급자** 항목을 선택합니다.
2. 추가를 클릭하여 공급자 추가 창을 엽니다.

그림 12.3. 공급자 추가 창

3. 이름 및 설명을 입력합니다.
4. 유형 목록에서 **OpenStack Networking**을 선택합니다.
5. **Open vSwitch**가 네트워킹 플러그인 필드에 선택되어 있는지 확인합니다.

6. 공급자 URL 텍스트 필드에 OpenStack Networking 인스턴스가 설치된 시스템의 URL 또는 정규화된 도메인 이름을 입력하고 뒤에 포트 번호를 입력합니다. 기본적으로 읽기 전용 확인란이 선택되어 있으며 이는 사용자가 OpenStack Networking 인스턴스를 수정하는 것을 방지합니다.



중요

Red Hat 지원을 받으려면 설정에 읽기 전용 확인란을 선택된 상태로 두어야 합니다.

7. 옵션으로 인증 필요 확인란을 선택하고 OpenStack Networking 인스턴스의 사용자 이름, 암호, 테넌트 이름, 인증 URL을 입력합니다. Keystone에 등록된 OpenStack Networking 사용자의 사용자 이름 및 암호와 OpenStack Networking 인스턴스가 속한 테넌트 및 Keystone 서버의 포트 및 URL을 사용해야 합니다.
8. 인증 정보 테스트:
 - a. 테스트를 클릭하여 지정된 인증 정보로 OpenStack Networking 인스턴스를 성공적으로 인증할 수 있는지 테스트합니다.
 - b. OpenStack Networking 인스턴스에서 SSL을 사용하는 경우 공급자 인증서 가져오기 창이 열리면 Manager가 해당 인스턴스와 통신할 수 있도록 OK를 클릭하여 OpenStack Networking 인스턴스가 제공하는 인증서를 가져옵니다.



주의

다음 단계는 기술 프리뷰로만 제공됩니다. Red Hat Virtualization은 사전 설정된 Neutron 호스트만 지원합니다.

9. 에이전트 설정 탭을 클릭합니다.

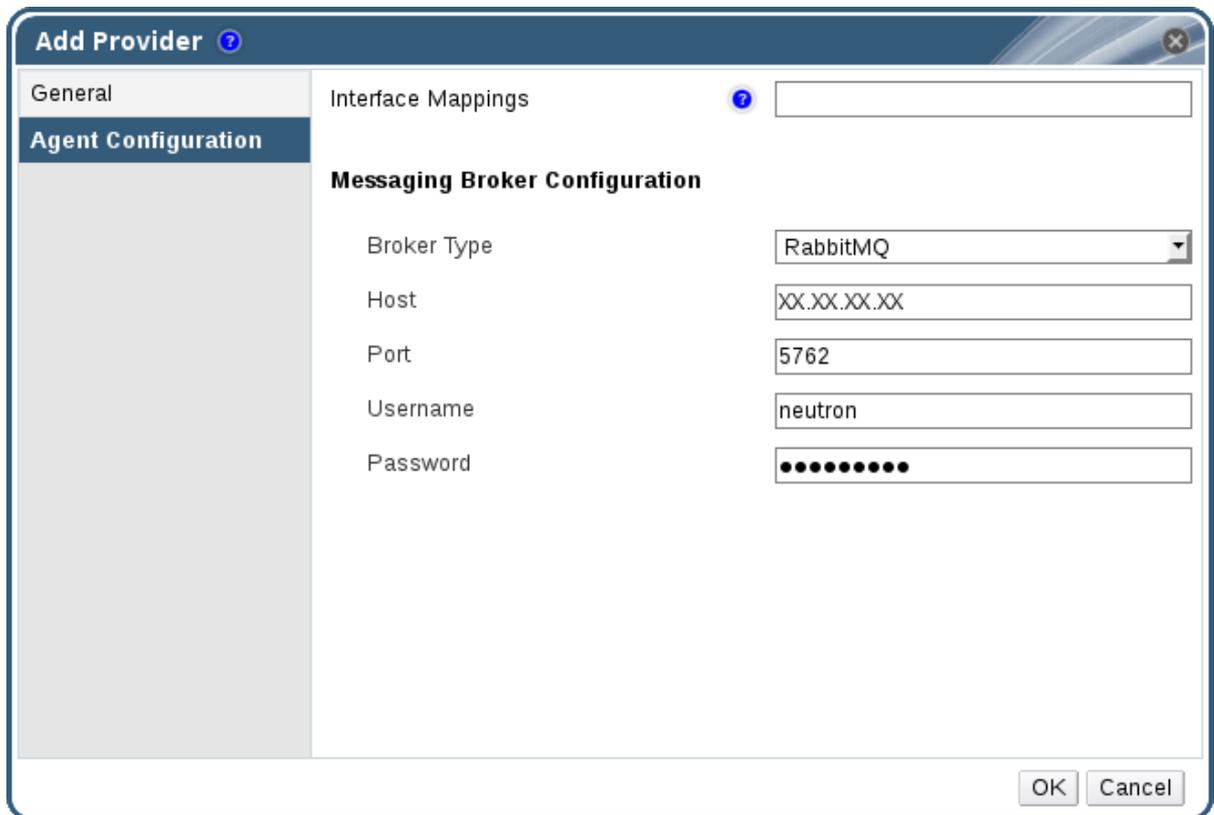


그림 12.4. 에이전트 설정 탭

10. 인터페이스 매핑 필드에 있는 Open vSwitch 에이전트의 콤마로 구분한 인터페이스 매핑 목록을 입력합니다.
11. 브로커 유형 목록에서 OpenStack Networking 인스턴스가 사용하는 메시지 브로커 유형을 선택합니다.
12. 호스트 필드에 메시지 브로커가 호스팅되는 호스트의 URL 또는 정규화된 도메인 이름을 입력합니다.
13. 메시지 브로커에 연결할 포트를 입력합니다. 메시지 브로커가 SSL을 사용하도록 설정되어 있지 않을 경우 이 포트 번호는 기본값으로 5762가 되며 SSL을 사용하도록 설정되어 있을 경우 포트 번호는 5761이 됩니다.
14. 메시지 브로커 인스턴스에 등록된 OpenStack Networking 사용자의 사용자 이름 및 암호를 입력합니다.
15. OK를 클릭합니다.

Red Hat Virtualization Manager에 OpenStack Networking 인스턴스가 추가됩니다. 해당 인스턴스가 제공하는 네트워크를 사용할 수 있으려면 Manager로 네트워크를 가져오기합니다. 6.3.1절. “외부 공급자에서 네트워크 가져오기”에서 참조하십시오.

12.2.4. 스토리지 관리를 위해 OpenStack Volume (Cinder) 인스턴스 추가

Red Hat Virtualization Manager에 스토리지 관리를 위한 OpenStack Volume (Cinder) 인스턴스를 추가합니다. OpenStack Cinder 볼륨은 Ceph Storage에 의해 구축됩니다.

절차 12.4. 스토리지 관리를 위해 OpenStack Volume (Cinder) 인스턴스 추가

1. 트리 창에서 외부 공급자 항목을 선택합니다.

2. 추가를 클릭하여 공급자 추가 창을 엽니다.

그림 12.5. 공급자 추가 창

3. 이름 및 설명을 입력합니다.
4. 유형 목록에서 **OpenStack Volume**을 선택합니다.
5. OpenStack Volume 스토리지 볼륨을 연결할 데이터 센터를 선택합니다.
6. 공급자 URL 텍스트 필드에 OpenStack Volume 인스턴스가 설치된 시스템의 URL 또는 정규화된 도메인 이름을 입력하고 그 뒤에 포트 번호를 입력합니다.
7. 옵션으로 인증 필요 확인란을 선택하고 OpenStack Volume 인스턴스의 사용자 이름, 암호, 테넌트 이름, 인증 URL을 입력합니다. Keystone에 등록된 OpenStack Volume 사용자의 사용자 이름 및 암호와 OpenStack Volume 인스턴스가 속한 테넌트 및 Keystone 서버의 API 버전, 포트, URL을 사용해야 합니다.
8. 테스트를 클릭하여 지정된 인증 정보로 OpenStack Volume 인스턴스를 성공적으로 인증할 수 있는지 테스트합니다.
9. **OK**를 클릭합니다.
10. 클라이언트 Ceph 인증 (**cephx**)이 활성화되어 있을 경우 다음 단계를 완료해야 합니다. **cephx** 프로토콜은 기본적으로 활성화되어 있습니다.
 - a. Ceph 서버에서 **ceph auth get-or-create** 명령을 사용하여 **client.cinder** 사용자에 대한 새로운 보안 키를 생성합니다. **cephx**에 대한 보다 자세한 내용은 [Ceph Config Reference](#) 에서 참조하시고 새로운 사용자를 위한 키 생성에 대한 보다 자세한 내용은 [Managing Users](#)에서 참조하십시오. **client.cinder** 사용자에 대한 키가 이미 존재할 경우 동일한 명령을 사용하여 이를 검색합니다.

- b. 관리 포털에 있는 **공급자** 목록에서 새로 생성된 **Cinder** 외부 공급자를 선택합니다.
- c. **인증키** 하위 탭을 클릭합니다.
- d. **새로 만들기**를 클릭합니다.
- e. **값**란에 보안 키를 입력합니다.
- f. 자동 생성된 **UUID**를 복사하거나 기존 **UUID**를 텍스트 필드에 입력합니다.
- g. Cinder 서버에서 이전 단계에서의 **UUID**를 추가하고 **/etc/cinder/cinder.conf**에 **cinder** 사용자를 추가합니다:

```

| rbd_secret_uuid = UUID
| rbd_user = cinder

```

Red Hat Virtualization Manager에 OpenStack Volume 인스턴스를 추가하고 인스턴스가 제공하는 스토리지 볼륨을 사용하여 작업합니다. OpenStack Volume (Cinder) 디스크 생성에 대한 보다 자세한 내용은 11.6.1절. “플로팅 가상 디스크 생성”에서 참조하십시오.

12.2.5. 가상 머신 공급자로 VMware 인스턴스 추가

VMware vCenter 인스턴스를 추가하여 VMware에서 Red Hat Virtualization Manager로 가상 머신을 가져옵니다.

Red Hat Virtualization은 VMware 가상 머신을 가져오기 전에 V2V를 사용하여 올바른 형식으로 변환합니다. virt-v2v 패키지는 하나 이상의 호스트에 설치해야 합니다. virt-v2v 패키지는 Red Hat Virtualization Hosts(RHVH)에서 기본적으로 사용할 수 있지만 Red Hat Enterprise Linux 호스트에서는 설치해야 합니다. Red Hat Enterprise Linux 호스트는 Red Hat Enterprise Linux 7.2 이상이어야 합니다.

절차 12.5. 가상 머신 공급자로 VMware vCenter 인스턴스를 추가

1. 트리 창에서 **외부 공급자** 항목을 선택합니다.
2. **추가**를 클릭하여 **공급자 추가** 창을 엽니다.

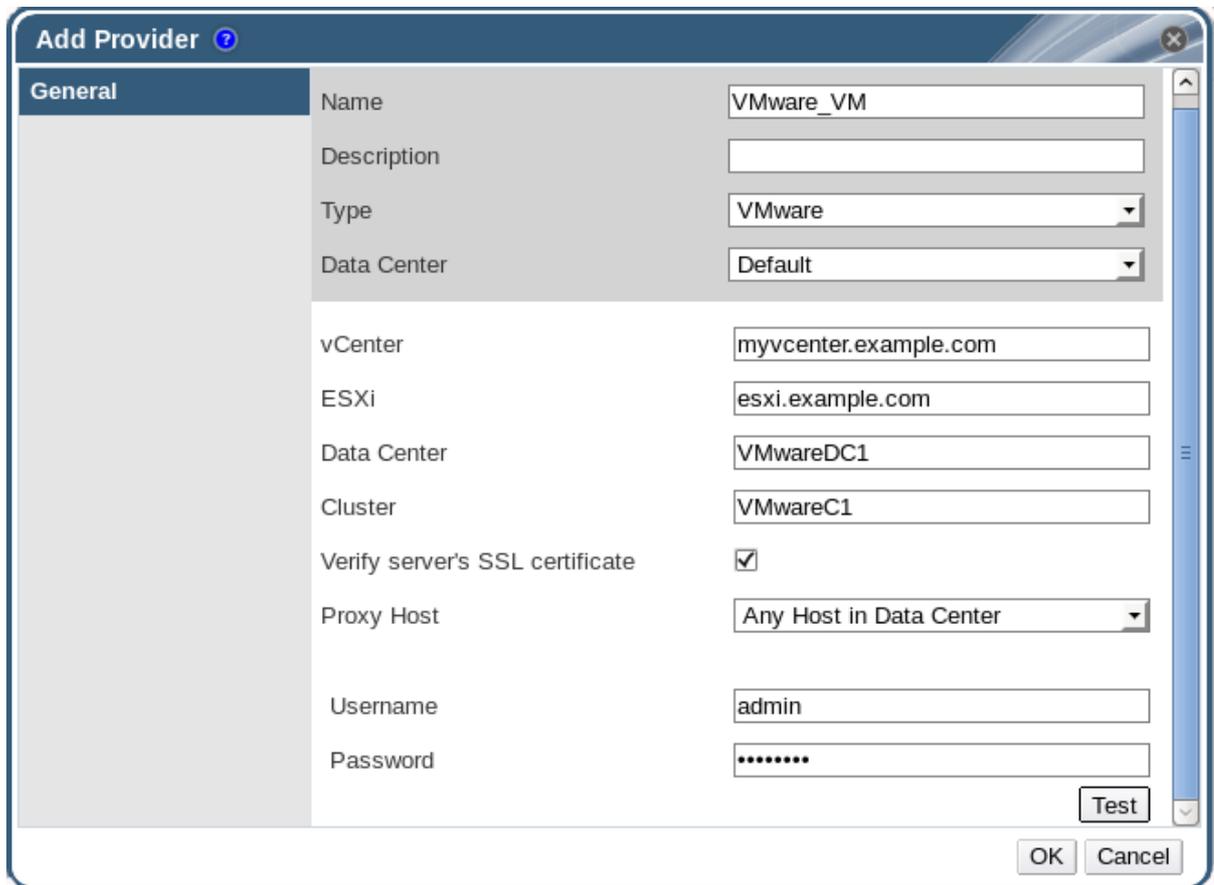


그림 12.6. 공급자 추가 창

3. 이름 및 설명을 입력합니다.
4. 유형 목록에서 **VMware**를 선택합니다.
5. VMware 가상 머신을 가져오기할 데이터 센터를 선택하거나 개별적으로 가져오기 작업을 실행하는 동안 대상 데이터 센터를 지정하기 위해 모든 데이터 센터를 선택합니다 (가상 머신 탭에서 가져오기 기능 사용).
6. vCenter 필드에 VMware vCenter 인스턴스의 IP 주소 또는 정규화된 도메인 이름을 입력합니다.
7. ESXi 필드에 가상 머신을 가져오기할 호스트의 IP 주소 또는 정규화된 도메인 이름을 입력합니다.
8. 데이터 센터 필드에 지정된 ESXi 호스트가 있는 데이터 센터의 이름을 입력합니다.
9. ESXi 호스트와 Manager 간에 SSL 인증서를 교환한 경우 ESXi 호스트의 인증서를 확인하려면 서버 **SSL 인증서 확인**을 선택한 상태로 둡니다. 그렇지 않은 경우 옵션을 선택 취소합니다.
10. 선택한 데이터 센터에 있는 virt-v2v가 설치된 호스트를 선택하여 가상 머신을 가져오는 동안 프록시 호스트로 동작하게 합니다. 이 호스트는 VMware vCenter 외부 공급자의 네트워크에 연결할 수 있어야 합니다. 위에서 모든 데이터 센터를 선택한 경우 여기서 호스트를 선택할 수 없지만 개별 가져오기 작업 중에 호스트를 지정할 수 있습니다 (가상 머신 탭에서 가져오기 기능 사용).
11. VMware vCenter 인스턴스의 사용자 이름 및 암호를 입력합니다. 사용자는 가상 머신이 있는 VMware 데이터 센터 및 ESXi 호스트에 액세스해야 합니다.
12. 인증 정보 테스트:

- a. 테스트를 클릭하여 지정된 인증 정보로 VMware vCenter 인스턴스를 성공적으로 인증할 수 있는지 테스트합니다.
- b. VMware vCenter 인스턴스가 SSL을 사용할 경우 공급자 인증서 가져오기 창이 열리면 OK를 클릭하여 VMware vCenter 인스턴스가 제공하는 인증서를 가져옵니다.



중요

Manager가 인스턴스와 통신할 수 있는지를 확인하려면 VMware vCenter 인스턴스가 제공하는 인증서를 가져오기해야 합니다.

13. OK를 클릭합니다.

VMware vCenter 인스턴스를 Red Hat Virtualization Manager에 추가하고 가상 머신을 가져올 수 있습니다. 자세한 내용은 *가상 머신 관리 가이드*에 있는 **VMware 공급자에서 가상 머신 가져오기**를 참조하십시오.

12.2.6. 외부 네트워크 공급자 추가

OpenStack Neutron REST API를 구현하는 모든 네트워크를 Red Hat Virtualization에 추가할 수 있습니다. 외부 네트워크 공급자의 작업 구현자가 가상 인터페이스 드라이버를 제공해야 합니다. 네트워크 공급자 및 가상 인터페이스 드라이버의 참조 구현에 대한 내용은 <https://github.com/mmirecki/ovirt-provider-mock> 및 https://github.com/mmirecki/ovirt-provider-mock/blob/master/docs/driver_installation에서 참조하십시오.

절차 12.6. 네트워크 프로비저닝용 외부 네트워크 공급자 추가

1. 트리 창에서 **외부 공급자** 항목을 선택합니다.
2. **추가**를 클릭합니다.

그림 12.7. 공급자 추가 창

3. 이름 및 설명을 입력합니다.
4. 유형 목록에서 **외부 네트워크 공급자**를 선택합니다.
5. 공급자 **URL** 텍스트 필드에 외부 네트워크 공급자가 설치된 시스템의 **URL** 또는 정규화된 도메인 이름을 입력하고 뒤에 포트 번호를 지정합니다. **읽기전용** 체크 상자가 기본으로 선택되어 있습니다. 이를 통해 외부 네트워크 공급자를 수정하는 것을 방지합니다.



중요

셋업 시 Red Hat 지원을 받으려면 **읽기전용** 체크 상자를 선택된 상태로 두어야 합니다.

6. 옵션으로 **인증 필요** 확인란을 선택하고 외부 네트워크 공급자의 **사용자 이름, 암호, 테넌트 이름, 인증 URL**을 입력합니다.
7. 인증 정보 테스트:
 - a. **테스트**를 클릭하여 지정된 인증 정보로 외부 네트워크 공급자를 성공적으로 인증할 수 있는지 테스트합니다.
 - b. 외부 네트워크 공급자가 **SSL**을 사용할 경우 **공급자 인증서 가져오기** 창이 열리면 **Manager**가 해당 인스턴스와 통신할 수 있도록 **OK**를 클릭하여 외부 네트워크 공급자가 제공하는 인증서를 가져옵니다.

Red Hat Virtualization Manager에 외부 네트워크 공급자가 추가됩니다. 해당 공급자가 제공하는 네트워크를 사용할 수 있으려면 호스트에 가상 인터페이스 드라이버를 설치하고 네트워크를 가져와야 합니다. 네트워크를 가져오는 방법은 [6.3.1절. "외부 공급자에서 네트워크 가져오기"](#)에서 참조하십시오.

12.2.7. 공급자 추가 일반 설정

공급자 추가 창에 있는 **일반** 탭에서 외부 공급자의 주요 정보를 등록할 수 있습니다.

표 12.1. 공급자 추가: 일반 설정

설정	설명
이름	Manager에서 공급자를 표시하기 위한 이름입니다.
설명	일반 텍스트 형식의 읽을 수 있는 공급자에 대한 설명입니다.
유형	<p>외부 공급자 유형입니다. 이 설정을 변경하면 공급자 설정을 위한 필드가 변경됩니다.</p> <p>Foreman/Satellite</p> <ul style="list-style-type: none"> • 공급자 URL: Satellite 인스턴스가 호스팅 되는 시스템의 URL 또는 정규화된 도메인 이름입니다. URL 또는 정규화된 도메인 이름의 마지막에 포트 번호를 추가할 필요가 없습니다. • 인증 필요: 공급자에 인증 필요 여부를 지정할 수 있습니다. Foreman/Satellite가 선택되어 있을 시 인증이 필요합니다. • 사용자 이름: Satellite 인스턴스에 연결하기 위한 사용자 이름입니다. 사용자 이름은 Satellite 인스턴스에 있는 프로비저닝 포털에 로그인 시 사용하는 사용자 이름이어야 합니다. 기본적으로 이 사용자 이름은 admin입니다. • 암호: 위의 사용자를 인증하기 위한 암호입니다. 이 암호는 Satellite 인스턴스에 있는 프로비저닝 포털에 로그인 시 사용하는 암호이어야 합니다. <p>OpenStack 이미지</p> <ul style="list-style-type: none"> • 공급자 URL: OpenStack Image 서비스를 호스팅하는 시스템의 URL 또는 정규화된 도메인 이름입니다. URL 또는 정규화된 도메인 이름의 마지막에 OpenStack Image 서비스의 포트 번호를 추가해야 합니다. 기본적으로 이 포트 번호는 9292입니다. • 인증 필요: OpenStack Image 서비스에 액세스하기 위한 인증 필요 여부를 지정할 수 있습니다. • 사용자 이름: OpenStack Image 서비스에 연결하기 위한 사용자 이름입니다. 이 사용자 이름은 OpenStack Image가 속해 있는 Keystone 인스턴스에 등록된 OpenStack Image 서비스의 사용자 이름이어야 합니다. 기본적으로 이 사용자 이름은 glance입니다.

설정	설명
	<ul style="list-style-type: none"> • 암호: 위의 사용자를 인증하기 위한 암호입니다. 이 암호는 OpenStack Image 서비스가 속해 있는 Keystone 인스턴스에 등록된 OpenStack Image 서비스의 암호이어야 합니다. • 테넌트 이름: OpenStack Image 서비스가 속해 있는 OpenStack 테넌트 이름입니다. 기본값으로 이는 services입니다. • 인증 URL: OpenStack Image 서비스가 인증하는 Keystone 서버의 URL 및 포트입니다. <p>OpenStack 네트워크</p> <ul style="list-style-type: none"> • 네트워크 플러그인: OpenStack Networking 서버에 연결하려는 네트워크 플러그인입니다. Open vSwitch는 옵션으로 기본값으로 선택됩니다. • 공급자 URL: OpenStack Networking 인스턴스를 호스팅하는 시스템의 URL 또는 정규화된 도메인 이름입니다. URL 또는 정규화된 도메인 이름의 마지막에 OpenStack Networking 인스턴스의 포트 번호를 추가해야 합니다. 기본값으로 이 포트 번호는 9696입니다. • 읽기 전용: 관리 포털에서 OpenStack Networking 인스턴스의 수정을 허용하는지 지정할 수 있습니다. • 인증 필요: OpenStack Networking 서비스에 액세스하기 위한 인증 필요 여부를 지정할 수 있습니다. • 사용자 이름: OpenStack Networking 인스턴스에 연결하기 위한 사용자 이름입니다. 이 사용자 이름은 OpenStack Networking 인스턴스가 속해 있는 Keystone 인스턴스에 등록된 OpenStack Networking의 사용자 이름이어야 합니다. 기본값으로 이 사용자 이름은 neutron입니다. • 암호: 위의 사용자를 인증하기 위한 암호입니다. 이 암호는 OpenStack Networking 인스턴스가 속해 있는 Keystone 인스턴스에 등록된 OpenStack Networking의 암호이어야 합니다. • 테넌트 이름: OpenStack Networking 인스턴스가 속해 있는 OpenStack 테넌트 이름입니다. 기본값으로 이는 services입니다. • 인증 URL: OpenStack Networking 인스턴스가 인증하는 Keystone 서버의 URL 및 포트입니다. <p>OpenStack 볼륨</p> <ul style="list-style-type: none"> • 데이터 센터: OpenStack Volume 스토리지 볼륨이 연결된 데이터 센터입니다.

설정	설명
	<ul style="list-style-type: none"> ● 공급자 URL: OpenStack Volume 인스턴스를 호스팅하는 시스템의 URL 또는 정규화된 도메인 이름입니다. URL 또는 정규화된 도메인 이름의 마지막에 OpenStack Volume 인스턴스의 포트 번호를 추가해야 합니다. 기본값으로 이 포트 번호는 8776입니다. ● 인증 필요: OpenStack Volume 서비스에 액세스하기 위한 인증 필요 여부를 지정할 수 있습니다. ● 사용자 이름: OpenStack Volume 인스턴스에 연결하기 위한 사용자 이름입니다. 이 사용자 이름은 OpenStack Volume 인스턴스가 속해 있는 Keystone 인스턴스에 등록된 OpenStack Volume의 사용자 이름이어야 합니다. 기본값으로 이 사용자 이름은 cinder입니다. ● 암호: 위의 사용자를 인증하기 위한 암호입니다. 이 암호는 OpenStack Volume 인스턴스가 속해 있는 Keystone 인스턴스에 등록된 OpenStack Volume의 암호이어야 합니다. ● 테넌트 이름: OpenStack Volume 인스턴스가 속해 있는 OpenStack 테넌트 이름입니다. 기본값으로 이는 services입니다. ● 인증 URL: OpenStack Volume 인스턴스가 인증하는 Keystone 서버의 URL 및 포트입니다. <p>VMware</p> <ul style="list-style-type: none"> ● 데이터 센터: VMware 가상 머신을 가져오기할 데이터 센터를 지정하거나 개별적으로 가져오기 작업을 실행하는 동안 대상 데이터 센터를 지정하기 위해 모든 데이터 센터를 선택합니다 (가상 머신 탭에서 가져오기 기능 사용). ● vCenter: VMware vCenter 인스턴스의 IP 주소 또는 정규화된 도메인 이름입니다. ● ESXi: 가상 머신을 가져오기할 호스트의 IP 주소 또는 정규화된 도메인 이름입니다. ● 데이터 센터: 지정된 ESXi 호스트가 있는 데이터 센터의 이름입니다. ● 클러스터: 지정한 ESXi 호스트가 속해 있는 클러스터의 이름입니다. ● 서버 SSL 인증서 확인: 연결 시 ESXi 호스트의 인증서를 확인할지를 지정합니다. ● 프록시 호스트: 선택한 데이터 센터에 있는 virt-v2v가 설치된 호스트를 선택하여 가상 머신을 가져오는 동안 호스트로 동작하게 합니다. 이 호스트는 VMware vCenter 외부 공급자의 네트워크에 연결할 수 있어야 합니다. 모든 데이터 센터를 선택한 경우

설정	설명
	<p>여기서 호스트를 선택할 수 없지만 개별 가져오기 작업 중에 호스트를 지정할 수 있습니다 (가상 머신 탭에서 가져오기 기능 사용).</p> <ul style="list-style-type: none"> • 사용자 이름: VMware vCenter 인스턴스에 연결하기 위한 사용자 이름입니다. 사용자는 가상 머신이 있는 VMware 데이터 센터 및 ESXi 호스트에 액세스해야 합니다. • 암호: 위의 사용자 이름을 인증하기 위한 암호입니다. <p>외부 네트워크 공급자</p> <ul style="list-style-type: none"> • 공급자 URL: 외부 네트워크 공급자를 호스팅하는 시스템의 URL 또는 정규화된 도메인 이름입니다. URL 또는 정규화된 도메인 이름의 마지막에 외부 네트워크 공급자의 포트 번호를 추가해야 합니다. 기본적으로 이 포트 번호는 9696입니다. • 읽기 전용: 관리 포털에서 외부 네트워크 공급자의 수정을 허용하는지 지정할 수 있습니다. • 인증 필요: 외부 네트워크 공급자에 액세스하기 위한 인증 필요 여부를 지정할 수 있습니다. • 사용자 이름: 외부 네트워크 공급자에 연결하기 위한 사용자 이름입니다. • 암호: 위의 사용자 이름을 인증하기 위한 암호입니다. • 인증 URL: 외부 네트워크 공급자가 인증하는 인증 서버의 URL 및 포트입니다.
테스트	<p>사용자는 지정된 인증 정보를 테스트할 수 있습니다. 이 버튼은 모든 공급자 유형에서 사용할 수 있습니다.</p>

12.2.8. 공급자 에이전트 설정 추가

공급자 추가 창에 있는 에이전트 설정 탭에서 사용자는 네트워크 플러그인의 상세 정보를 등록할 수 있습니다. 이 탭은 **OpenStack Networking** 공급자 유형에서만 사용 가능합니다.

표 12.2. 공급자: 일반 설정 추가

설정	설명
인터페이스 매핑	<code>label:interface</code> 형식의 콤마로 구분된 매핑 목록입니다.
브로커 유형	OpenStack Networking 인스턴스가 사용하는 메시지 브로커 유형입니다. RabbitMQ 또는 Qpid 를 선택합니다.

설정	설명
호스트	메세지 브로커가 설치된 URL 또는 정규화된 도메인 이름입니다.
포트	위의 호스트와 연결된 원격 포트입니다. 기본값으로 이 포트는 SSL이 호스트에서 활성화되어 있지 않은 경우 5762가 되며 SSL이 활성화되어 있을 경우 5671이 됩니다.
사용자 이름	위의 메세지 브로커로 OpenStack Networking 인스턴스를 인증하기 위한 사용자 이름입니다. neutron 은 기본 사용자 이름입니다.
암호	위의 사용자 이름에 대한 인증 암호입니다.

12.3. 외부 공급자 편집

12.3.1. 외부 공급자 편집

절차 12.7. 외부 공급자 편집

1. 트리 창에서 **외부 공급자** 항목을 선택합니다.
2. 편집할 외부 공급자를 선택합니다.
3. **편집** 버튼을 클릭하여 **공급자 편집** 창을 엽니다.
4. 공급자의 현재 값을 원하는 값으로 변경합니다.
5. **OK**를 클릭합니다.

12.4. 외부 공급자 삭제

12.4.1. 외부 공급자 삭제

절차 12.8. 외부 공급자 삭제

1. 트리 창에서 **외부 공급자** 항목을 선택합니다.
2. 삭제할 외부 공급자를 선택합니다.
3. **삭제**를 클릭합니다.
4. **공급자 삭제** 창에서 **OK**를 클릭하여 공급자 삭제를 확인합니다.

III 부. 환경 관리

13장. 백업 및 마이그레이션

13.1. RED HAT VIRTUALIZATION MANAGER 백업 및 복구

13.1.1. Red Hat Virtualization Manager 백업 - 개요

engine-backup 도구를 사용하여 Red Hat Virtualization Manager의 일반적인 백업을 수행합니다. 도구를 사용하여 **engine** 데이터 베이스 및 설정 파일을 단일 파일로 백업할 수 있으며 **ovirt-engine** 서비스를 중단하지 않고 실행할 수 있습니다.

13.1.2. engine-backup 명령 구문

engine-backup 명령은 두 가지 기본 모드 중 하나에서 작동합니다:

```
# engine-backup --mode=backup
```

```
# engine-backup --mode=restore
```

이 두 가지 모드는 매개 변수 집합으로 추가 확장되어 **engine** 데이터베이스에 대한 백업 범위 및 다른 인증 정보를 지정할 수 있습니다. 전체 매개 변수 목록 및 기능을 보려면 **engine-backup --help**를 실행하십시오.

기본 옵션

--mode

명령이 백업 작업을 수행하거나 복원 작업을 수행할 지에 대한 여부를 지정합니다. **backup** 및 **restore**의 두 가지 옵션을 사용할 수 있습니다. 이는 필수 매개 변수입니다.

--file

백업 모드에서 백업된 파일 이름 및 경로와 복원 모드에서 백업 데이터를 읽기 위한 파일 이름 및 경로를 지정합니다. 이는 백업 모드 및 복원 모드 모두에서 필수 매개 변수입니다.

--log

백업 기록 또는 복원 작업이 기록될 파일 경로와 이름을 지정합니다. 이 매개 변수는 백업 모드 및 복원 모드 모두에서 필요합니다.

--scope

백업 또는 복원 작업 범위를 지정합니다. 다음과 같은 네 가지 옵션이 있습니다. **all**은 모든 데이터베이스 및 설정 데이터를 백업 또는 복원합니다. **files**는 시스템에 있는 파일만 백업 또는 복원합니다. **db**는 **Manager** 데이터베이스만 백업 또는 복원합니다. **dwhdb**는 **Data Warehouse** 데이터베이스만 백업 또는 복원합니다. 기본 범위는 **all**입니다.

--scope 매개 변수는 같은 **engine-backup** 명령에서 여러 번 지정할 수 있습니다.

Manager 데이터베이스 옵션

다음 옵션은 **restore** 모드에서 **engine-backup** 명령을 사용하는 경우에만 사용할 수 있습니다. 아래의 옵션 구문은 **Manager** 데이터베이스 복원에 적용됩니다. 데이터 웨어하우스 데이터베이스 복원에도 동일한 옵션이 존재합니다. 데이터 웨어하우스 옵션 구문은 **engine-backup --help**를 참조하십시오.

--provision-db

복원할 Manager 데이터베이스 백업에 대해 PostgreSQL 데이터베이스를 만듭니다. 이는 원격 호스트에서 백업을 복원하거나 PostgreSQL 데이터베이스가 이미 설정되어 있지 않은 새 설치 시 필요한 매개 변수입니다.

--change-db-credentials

백업 자체에 저장된 항목 이외의 인증 정보를 사용하여 Manager 데이터베이스를 복원하는 데 사용할 대체 인증 정보를 지정할 수 있습니다. 이 매개 변수에서 필요한 추가 매개 변수에 대한 내용은 **engine-backup --help**를 참조하십시오.

--restore-permissions 또는 **--no-restore-permissions**

데이터베이스 사용자의 권한을 복원하거나 복원하지 않습니다. 백업 복원 시 이러한 매개 변수 중 하나가 필요합니다.

**참고**

백업에 추가 데이터베이스 사용자에게 대한 권한이 포함된 경우 **--restore-permissions** 및 **--provision-db**(또는 **--provision-dwh-db**) 옵션을 사용하여 백업을 복원하면 임의의 암호로 추가 사용자가 만들어집니다. 추가 사용자에게 복원된 시스템에 대한 액세스가 필요한 경우 이러한 암호를 수동으로 변경해야 합니다. 자세한 내용은 <https://access.redhat.com/articles/2686731>에서 참조하십시오.

13.1.3. engine-backup 명령으로 백업 생성

Manager가 활성화되어 있는 상태에서 **engine-backup** 명령을 사용하여 Red Hat Virtualization Manager를 백업할 수 있습니다. **--scope**에 다음 옵션 중 하나를 추가하여 수행할 백업 범위를 지정합니다:

- **all**: Manager에 있는 모든 데이터 베이스 및 설정 파일의 전체 백업
- **files**: 시스템에 있는 파일만 백업
- **db**: Manager 데이터베이스만 백업
- **dwhdb**: 데이터 웨어하우스 데이터만 백업

**중요**

Red Hat Virtualization Manager를 새로 설치하기 위해 데이터 베이스를 복원하려면 데이터 베이스 백업 하나만으로는 충분하지 않습니다. Manager는 설정 파일에 액세스해야 합니다. 기본값인 **all** 이외의 범위를 지정하는 모든 백업은 **files** 범위 또는 **filesystem** 백업과 함께 복원해야 합니다.

절차 13.1. engine-backup 명령 사용 예

1. Red Hat Virtualization Manager를 실행하는 시스템에 로그인합니다.
2. 백업을 생성합니다:

예 **13.1. 전체 백업 생성**

```
# engine-backup --scope=all --mode=backup --file=file_name --
log=log_file_name
```

예 13.2. Manager 데이터베이스 백업 생성

```
# engine-backup --scope=files --scope=db --mode=backup --
file=file_name --log=log_file_name
```

db 옵션을 **dwhdb**로 변경하여 데이터 웨어하우스 데이터 베이스를 백업합니다.

지정된 경로 및 파일 이름을 사용하여 백업이 들어있는 **tar** 파일이 생성됩니다.

백업이 들어 있는 **tar** 파일은 환경을 복원하는데 사용할 수 있습니다.

13.1.4. engine-backup 명령으로 백업 복원

engine-backup 명령을 사용하여 백업을 복원하는 절차는 복원 대상에 따라 백업 생성 절차와 비교해 볼 때 몇 가지 추가 절차가 필요합니다. 예를 들어 **engine-backup** 명령으로 로컬 또는 원격 데이터 베이스를 사용하여 기존 Red Hat Virtualization 설치에 Red Hat Virtualization을 새로 설치하기 위해 백업을 복원할 수 있습니다.



중요

백업은 백업과 동일한 메이저 릴리스 환경으로만 복원할 수 있습니다. 예를 들어, Red Hat Virtualization 버전 4.1 환경의 백업은 다른 Red Hat Virtualization 버전 4.1 환경으로만 복원할 수 있습니다. 백업 파일에 들어 있는 Red Hat Virtualization 버전을 확인하려면 백업 파일의 압축을 풀고 압축을 푼 파일의 **root** 디렉토리에 있는 **version** 파일 값을 읽습니다.

13.1.5. 백업을 복원하여 새로 설치하기

engine-backup 명령을 사용하여 Red Hat Virtualization Manager를 새로 설치하기 위한 백업을 복원할 수 있습니다. 다음 절차는 기본 운영 체제 및 Red Hat Virtualization Manager에 필요한 패키지가 설치되어 있으나 **engine-setup** 명령은 아직 실행되지 않은 시스템에서 실행해야 합니다. 다음 절차에서는 백업이 복원되어 있는 컴퓨터에서 백업 파일에 액세스할 수 있다고 간주합니다.

절차 13.2. 백업을 복원하여 새로 설치하기

1. Manager 시스템에 로그인합니다. 원격 호스트에 **engine** 데이터베이스를 복원하는 경우 해당 호스트에 로그인하여 관련 작업을 수행해야 합니다. 또한 원격 호스트에 데이터 웨어하우스를 복원하는 경우에도 마찬가지로 해당 호스트에 로그인하여 관련 작업을 수행해야 합니다.
2. 전체 백업을 복원하거나 데이터베이스만 백업을 복원합니다.
 - 전체 백업을 복원하려면 다음을 수행합니다:

```
# engine-backup --mode=restore --file=file_name --
log=log_file_name --provision-db --restore-permissions
```

데이터 웨어하우스도 전체 백업의 일부로 복원하는 경우 추가 데이터베이스를 프로비저닝합니다.

```
engine-backup --mode=restore --file=file_name --log=log_file_name
--provision-db --provision-dwh-db --restore-permissions
```

- 설정 파일을 복원하고 데이터베이스 백업을 복원하여 데이터베이스만 백업을 복원하려면 다음을 수행합니다:

```
# engine-backup --mode=restore --scope=files --scope=db --
file=file_name --log=log_file_name --provision-db --restore-
permissions
```

위의 예시는 Manager 데이터베이스 백업을 복원합니다.

```
# engine-backup --mode=restore --scope=files --scope=dwhdb --
file=file_name --log=log_file_name --provision-dwh-db --restore-
permissions
```

위의 예시는 데이터 웨어하우스 데이터베이스의 백업을 복원합니다.

완료시 다음과 같은 출력 결과가 표시됩니다:

```
You should now run engine-setup.
Done.
```

3. 다음 명령을 실행하고 프롬프트에 따라 복원된 Manager를 설정합니다.

```
# engine-setup
```

Red Hat Virtualization Manager가 백업에 저장된 버전에 복원되었습니다. 새로운 Red Hat Virtualization 시스템의 정규화된 도메인 이름을 변경하는 방법은 [18.1.1절. “oVirt Engine Rename 도구”](#)에서 참조하십시오.

13.1.6. 기존 설치를 덮어쓰기하여 백업 복원하기

engine-backup 명령을 사용하여 Red Hat Virtualization Manager가 이미 설치 및 설정된 머신에 백업을 복원할 수 있습니다. 설치를 백업하고 설치를 변경한 후 백업에서 설치를 복원하고자 하는 경우에 유용합니다.



중요

기존 설치를 덮어쓰기하기 위해 백업을 복원할 때 **engine-backup** 명령을 사용하기 전 **engine-cleanup** 명령을 실행하여 기존 설치를 정리해야 합니다. **engine-cleanup** 명령은 engine 데이터베이스만을 정리하고 데이터베이스를 삭제하거나 데이터 베이스를 소유하고 있는 사용자를 삭제하지 않기 때문입니다. 사용자 및 데이터베이스가 이미 존재하고 있기 때문에 새로운 데이터베이스를 생성하거나 데이터베이스 인증을 지정할 필요가 없습니다.

절차 13.3. 기존 설치를 덮어쓰기하여 백업 복원하기

1. Red Hat Virtualization Manager 시스템에 로그인합니다.
2. 설정 파일을 삭제하고 Manager에 연결된 데이터베이스를 정리합니다:

```
# engine-cleanup
```

3. 전체 백업 또는 데이터베이스만 백업을 복원합니다:

- 전체 백업을 복원하려면 다음을 수행합니다:

```
# engine-backup --mode=restore --file=file_name --
log=log_file_name --restore-permissions
```

- 설정 파일을 복원하고 데이터베이스 백업을 복원하여 데이터베이스만 백업을 복원하려면 다음을 수행합니다:

```
# engine-backup --mode=restore --scope=files --scope=db --
file=file_name --log=log_file_name --restore-permissions
```

위의 예시는 **Manager** 데이터베이스 백업을 복원합니다. 필요한 경우 데이터 웨어하우스 데이터베이스도 복원합니다.

```
# engine-backup --mode=restore --scope=dwhdb --file=file_name --
log=log_file_name --restore-permissions
```

완료시 다음과 같은 출력 결과가 표시됩니다:

```
You should now run engine-setup.
Done.
```

4. 다음 명령을 실행하고 프롬프트에 따라 방화벽을 다시 설정한 후 **ovirt-engine** 서비스가 올바르게 설정되어 있는지 확인합니다:

```
# engine-setup
```

13.1.7. 다른 인증 정보를 사용하여 백업 복원하기

engine-backup 명령을 사용하여 Red Hat Virtualization Manager가 이미 설치 및 설정된 컴퓨터에 백업을 복원할 수 있지만 백업에 있는 데이터 베이스의 인증 정보는 백업이 복원된 컴퓨터에 있는 데이터 베이스와 다릅니다. 이는 설치에서 백업을 취하여 백업에서 다른 시스템으로 설치를 복원하고자 하는 경우 유용합니다.

중요

기존 설치를 덮어쓰기하기 위해 백업을 복원할 때 **engine-backup** 명령을 사용하기 전 **engine-cleanup** 명령을 실행하여 기존 설치를 정리해야 합니다. **engine-cleanup** 명령은 **engine** 데이터베이스만을 정리하고 데이터베이스를 삭제하거나 데이터 베이스를 소유하고 있는 사용자를 삭제하지 않기 때문입니다. 사용자 및 데이터베이스가 이미 존재하고 있기 때문에 새로운 데이터베이스를 생성하거나 데이터베이스 인증 정보를 지정할 필요가 없습니다. 하지만 **engine** 데이터 베이스 소유자의 인증 정보를 알 수 없는 경우 백업을 복원하기 전 이를 변경해야 합니다.

절차 13.4. 다른 인증 정보를 사용하여 백업 복원하기

1. Red Hat Virtualization Manager가 설치된 시스템에 로그인합니다.

- 다음 명령을 실행하여 프롬프트에 따라 설정 파일을 삭제하고 Manager에 연결된 데이터베이스를 정리합니다:

```
# engine-cleanup
```

- 사용자 인증 정보를 알 수 없는 경우 engine 데이터베이스 소유자의 암호를 변경합니다:

1. postgresql 명령행에 들어갑니다:

```
# su postgres
$ psql
```

2. engine 데이터베이스를 소유한 사용자의 암호를 변경합니다:

```
postgres=# alter role user_name encrypted password
'new_password';
```

필요한 경우 **ovirt_engine_dwh** 데이터베이스를 소유하는 사용자에게 대해 이 명령을 반복 실행합니다.

4. **--change-db-credentials** 매개 변수를 사용하여 전체 백업 또는 데이터베이스만 백업을 복구하여 새 데이터베이스의 인증을 전달합니다. Manager에 로컬로 설정된 데이터베이스의 **database_location**은 **localhost**입니다.



참고

다음 예에서는 각 데이터 베이스마다 암호를 입력하라는 프롬프트에 따라 암호를 지정하지 않고 각 데이터베이스마다 **--*password** 옵션을 사용합니다. 이러한 옵션의 명령 자체에 암호를 지정할 수 있지만 암호는 셸 기록에 저장되므로 권장되지 않습니다. 다른 방법으로 각 데이터베이스에 대해 **--*passfile=password_file** 옵션을 사용하여 인터랙티브 (interactive) 프롬프트없이 **engine-backup** 도구에 암호를 안전하게 전달할 수 있습니다.

- 전체 백업을 복원하려면 다음을 수행합니다:

```
# engine-backup --mode=restore --file=file_name --
log=log_file_name --change-db-credentials --db-
host=database_location --db-name=database_name --db-user=engine -
-db-password --no-restore-permissions
```

데이터 웨어하우스도 전체 백업의 일부로 복원하는 경우 추가되는 두 가지 데이터 베이스의 변경된 인증 정보를 포함시켜야 합니다:

```
engine-backup --mode=restore --file=file_name --log=log_file_name
--change-db-credentials --db-host=database_location --db-
name=database_name --db-user=engine --db-password --change-dwh-
db-credentials --dwh-db-host=database_location --dwh-db-
name=database_name --dwh-db-user=ovirt_engine_history --dwh-db-
password --no-restore-permissions
```

- 설정 파일을 복원하고 데이터베이스 백업을 복원하여 데이터베이스만 백업을 복원하려면 다음을 수행합니다:

```
# engine-backup --mode=restore --scope=files --scope=db --
file=file_name --log=log_file_name --change-db-credentials --db-
host=database_location --db-name=database_name --db-user=engine -
-db-password --no-restore-permissions
```

위의 예시는 Manager 데이터베이스의 백업을 복원합니다.

```
# engine-backup --mode=restore --scope=files --scope=dwhdb --
file=file_name --log=log_file_name --change-dwh-db-credentials --
dwh-db-host=database_location --dwh-db-name=database_name --dwh-
db-user=ovirt_engine_history --dwh-db-password --no-restore-
permissions
```

위의 예시는 데이터 웨어하우스 데이터베이스의 백업을 복원합니다.

완료시 다음과 같은 출력 결과가 표시됩니다:

```
You should now run engine-setup.
Done.
```

- 다음 명령을 실행하고 프롬프트에 따라 방화벽을 다시 설정한 후 **ovirt-engine** 서비스가 올바르게 설정되어 있는지 확인합니다:

```
# engine-setup
```

13.1.8. Engine 데이터 베이스를 원격 서버 데이터 베이스로 마이그레이션

Red Hat Virtualization Manager를 처음에 설정하고 나면 **engine** 데이터베이스를 원격 데이터베이스 서버로 마이그레이션해야 합니다. **engine-backup**을 사용하여 데이터베이스 백업을 생성하고 새 데이터베이스 서버에서 복원합니다. 이 절차에서는 새 데이터베이스 서버에 Red Hat Enterprise Linux 7이 설치되어 있으며 적절한 서브스크립션이 설정되어 있다고 가정합니다. 자세한 내용은 [설치 가이드](#)에 있는 [필요한 서브스크립션을 등록](#)을 참조하십시오.

절차 13.5. 데이터베이스 마이그레이션

- Red Hat Virtualization Manager 시스템에 로그인하고 **ovirt-engine** 서비스를 중지하여 engine 백업을 방해하지 않도록 합니다:

```
# systemctl stop ovirt-engine.service
```

- engine** 데이터베이스 백업을 만듭니다.

```
# engine-backup --scope=files --scope=db --mode=backup --
file=file_name --log=log_file_name
```

- 백업 파일을 새 데이터베이스 서버에 복사합니다.

```
# scp /tmp/engine.dump root@new.database.server.com:/tmp
```

- 새 데이터베이스 서버에 로그인하고 **engine-backup**을 설치합니다.

```
# yum install ovirt-engine-tools-backup
```

- 5. 새 데이터베이스 서버에서 데이터베이스를 복원합니다. `file_name`은 Manager에서 복사한 백업 파일입니다.

```
# engine-backup --mode=restore --scope=files --scope=db --
file=file_name --log=log_file_name --provision-db --no-restore-
permissions
```

- 6. 이제 데이터베이스가 마이그레이션되었습니다. **ovirt-engine** 서비스를 시작합니다:

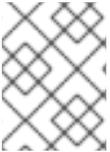
```
# systemctl start ovirt-engine.service
```

13.2. 백업 및 복구 API를 사용하여 가상 머신 백업 및 복구

13.2.1. 백업 및 복원 API

백업 및 복원 API는 전체 또는 파일 수준에서 가상 머신의 백업 및 복원을 실행할 수 있게 하는 기능 모음입니다. API는 라이브 스냅샷 및 REST API와 같이 Red Hat Virtualization의 여러 구성 요소로 결합되어 독립적인 소프트웨어 공급자에 의해 제공되는 백업 소프트웨어가 포함된 가상 머신에 연결할 수 있는 임시 볼륨을 생성하고 작업할 수 있습니다.

지원되는 타사 백업 벤더의 경우 [Red Hat Marketplace](#)에 있는 Red Hat Virtualization 에코시스템에서 참조하십시오.



참고

REST API로 작업하는 방법에 대한 자세한 내용은 [REST API 가이드](#)에 있는 [백업 및 복구 API](#)를 참조하십시오.

13.2.2. 가상 머신 백업

가상 머신을 백업하려면 백업 및 복원 API를 사용합니다. 다음 절차에서는 백업을 위한 가상 머신 및 백업 관리를 위한 소프트웨어가 설치된 가상 머신 이렇게 두 가지 가상 머신이 있음을 전제로 합니다.

절차 13.6. 가상 머신 백업

1. REST API를 사용하여 백업할 가상 머신의 스냅샷을 생성합니다:

```
POST /api/vms/11111111-1111-1111-1111-111111111111/snapshots/
HTTP/1.1
Accept: application/xml
Content-type: application/xml

<snapshot>
  <description>BACKUP</description>
</snapshot>
```



참고

가상 머신의 스냅샷 생성 시 스냅샷이 생성되는 시점에 가상 머신의 설정 데이터 복사본은 스냅샷 아래의 **initialization**에 있는 **configuration** 속성의 **data** 속성에 저장됩니다.



중요

공유 가능으로 표시된 디스크나 직접 LUN 디스크에 기반하는 디스크의 스냅샷을 생성할 수 없습니다.

- 스냅샷 아래의 데이터 속성에서 가상 머신의 설정 데이터를 검색합니다:

```
GET /api/vms/11111111-1111-1111-1111-111111111111/snapshots/11111111-1111-1111-1111-111111111111 HTTP/1.1
Accept: application/xml
Content-type: application/xml
```

- 스냅샷의 디스크 ID 및 스냅샷 ID를 확인합니다:

```
GET /api/vms/11111111-1111-1111-1111-111111111111/snapshots/11111111-1111-1111-1111-111111111111/disks
HTTP/1.1
Accept: application/xml
Content-type: application/xml
```

- 백업 가상 머신에 스냅샷을 첨부하고 디스크를 활성화합니다:

```
POST /api/vms/22222222-2222-2222-2222-222222222222/disks/ HTTP/1.1
Accept: application/xml
Content-type: application/xml

<disk id="11111111-1111-1111-1111-111111111111">
  <snapshot id="11111111-1111-1111-1111-111111111111"/>
  <active>true</active>
</disk>
```

- 백업 가상 머신에 있는 백업 소프트웨어를 사용하여 스냅샷 디스크에 있는 데이터를 백업합니다.
- 백업 가상 머신에서 스냅샷 디스크를 분리합니다:

```
DELETE /api/vms/22222222-2222-2222-2222-222222222222/disks/11111111-1111-1111-1111-111111111111 HTTP/1.1
Accept: application/xml
Content-type: application/xml

<action>
  <detach>true</detach>
</action>
```

- 옵션으로 스냅샷을 삭제합니다:

```
DELETE /api/vms/11111111-1111-1111-1111-
```

```
111111111111/snapshots/11111111-1111-1111-1111-111111111111 HTTP/1.1
Accept: application/xml
Content-type: application/xml
```

다른 가상 머신에 설치된 백업 소프트웨어를 사용하여 일정 시점의 가상 머신 상태가 백업되었습니다.

13.2.3. 가상 머신 복구

백업 및 복구 API를 사용하여 백업한 가상 머신을 복구합니다. 이러한 절차에서는 이전 백업 관리에 사용된 소프트웨어가 설치된 백업 가상 머신이 준비되어 있음을 전제로 합니다.

절차 13.7. 가상 머신 복구

1. 관리 포털에서 백업을 복구하기 위한 플로팅 디스크를 생성합니다. 플로팅 디스크를 생성하는 방법에 대한 보다 자세한 내용은 [11.6.1절. “플로팅 가상 디스크 생성”](#)에서 참조하십시오.
2. 백업 가상 머신에 디스크를 연결합니다:

```
POST /api/vms/22222222-2222-2222-2222-222222222222/disks/ HTTP/1.1
Accept: application/xml
Content-type: application/xml

<disk id="11111111-1111-1111-1111-111111111111">
</disk>
```

3. 백업 소프트웨어를 사용하여 디스크에 백업을 복원합니다.
4. 디스크를 백업 가상 머신에서 분리합니다:

```
DELETE /api/vms/22222222-2222-2222-2222-222222222222/disks/11111111-
1111-1111-1111-111111111111 HTTP/1.1
Accept: application/xml
Content-type: application/xml

<action>
  <detach>true</detach>
</action>
```

5. 복원된 가상 머신의 설정 데이터를 사용하여 새 가상 머신을 생성합니다:

```
POST /api/vms/ HTTP/1.1
Accept: application/xml
Content-type: application/xml

<vm>
  <cluster>
    <name>cluster_name</name>
  </cluster>
  <name>NAME</name>
  ...
</vm>
```

6. 새 가상 머신에 디스크를 연결합니다:

■

```
POST /api/vms/33333333-3333-3333-3333-333333333333/disks/ HTTP/1.1
Accept: application/xml
Content-type: application/xml

<disk id="11111111-1111-1111-1111-111111111111">
</disk>
```

백업 및 복원 API를 사용하여 생성된 백업을 사용하여 가상 머신이 복원되었습니다.

14장. RED HAT SATELLITE을 사용한 에라타 관리

Red Hat Virtualization 설정 시 Red Hat Virtualization Manager의 Red Hat Satellite에서 에라타를 볼 수 있습니다. 이를 통해 Red Hat Satellite 공급자에 연결된 호스트, 가상 머신, 그리고 Manager를 위해 관리자가 사용 가능한 에라타와 그 중요성에 대한 업데이트를 받을 수 있습니다. 해당 업데이트를 적용하기 위해 관리자가 대상 호스트, 가상 머신, 또는 Manager에 업데이트를 실행합니다. Red Hat Satellite에 대한 보다 자세한 내용은 [Red Hat Satellite User Guide](#)에서 참조하십시오.

Red Hat Virtualization 4.1은 Red Hat Satellite 6.1을 사용한 에라타 관리를 지원합니다.



중요

Satellite 서버에서 Manager, 호스트, 그리고 가상 머신을 FQDN로 식별합니다. 이를 통해 외부 콘텐츠 호스트 ID가 Red Hat Virtualization에서 유지되지 않아도 됩니다.

Manager, 호스트, 그리고 가상 머신 관리에 사용되는 Satellite 계정은 관리자 권한이 있고 기본 조직이 설정되어야 합니다.

절차 14.1. Red Hat Virtualization 에라타 설정

Manager, 호스트, 그리고 가상 머신을 Red Hat Satellite 공급자와 연결하기 위해 우선 Manager가 공급자에 연결되어야 합니다. 그리고 나서 호스트가 같은 공급자에 연결 및 설정됩니다. 마지막으로 가상 머신이 같은 공급자에 연결 및 설정됩니다.

1. Satellite 서버를 외부 공급자로 추가해서 Manager를 연결합니다. 보다 자세한 내용은 [12.2.1절. “호스트 프로비저닝을 위한 Red Hat Satellite 인스턴스 추가”](#)에서 참조하십시오.



참고

Manager가 해당 Satellite 서버에 콘텐츠 호스트로 등록되어 있고 katello-agent 패키지가 설치되어야 합니다.

호스트 등록 설정 방법에 대한 보다 자세한 내용은 [Red Hat Satellite User Guide](#)에 있는 [Configuring a Host for Registration](#)에서 참조하고 호스트 등록 및 katello-agent 패키지 설치에 대한 보다 자세한 내용은 [Red Hat Satellite User Guide](#)에 있는 [Registration](#)에서 참조하십시오.

2. 옵션으로 호스트를 설정해서 사용 가능한 에라타를 표시합니다. 보다 자세한 내용은 [7.5.3절. “호스트에 대한 Satellite 에라타 관리 설정”](#)에서 참조하십시오.
3. 선택적으로 필요한 가상 머신을 설정하여 사용 가능한 에라타를 표시합니다. 필요한 가상 머신을 설정하기 전에 먼저 연결된 호스트를 설정해야 합니다. 자세한 내용은 [가상 머신 관리 가이드](#)에 있는 [가상 머신의 Red Hat Satellite 에라타 관리 설정](#)을 참조하십시오.

절차 14.2. Red Hat Virtualization Manager 에라타 표시

1. 트리 창에서 **에라타** 항목을 선택합니다.
2. **보안, 버그, 또는 기능 강화** 확인란을 선택하여 해당 에라타 유형만 표시합니다.

호스트에 대해 사용 가능한 에라타를 보는 방법에 대한 자세한 내용은 [7.5.13절. “호스트 에라타 표시”](#)를 참조하고 가상 머신에 대해 사용 가능한 에라타를 표시하는 방법에 대한 자세한 내용은 [가상 머신 관리 가이드](#)에 있는 [가상 머신의 Red Hat Satellite 에라타 보기](#)를 참조하십시오.

15장. 사용자 및 역할

15.1. 사용자에게 대한 소개

Red Hat Virtualization은 로컬 도메인 및 외부 도메인의 두 가지 유형의 사용자 도메인이 있습니다. Manager 설치 과정에서 **internal** 도메인이라는 기본 로컬 도메인과 기본 사용자 **admin**이 생성됩니다.

ovirt-aaa-jdbc-tool을 사용하여 **internal** 도메인에 추가 사용자를 생성합니다. 로컬 도메인에 생성된 사용자 계정은 로컬 사용자라고 부릅니다. 또한 Red Hat Directory Server, Active Directory, OpenLDAP 등의 외부 디렉토리 서버 및 지원되는 다른 옵션을 사용자의 Red Hat Virtualization 환경에 연결해서 외부 도메인으로 사용할 수 있습니다. 외부 도메인에 생성된 사용자 계정은 디렉토리 사용자라고 부릅니다.

로컬 사용자와 디렉토리 사용자 모두 관리 포털에서 적절한 역할 및 권한이 부여되어야 해당 환경에서 동작할 수 있습니다. 사용자 역할은 최종 사용자와 관리자의 두 가지 주요 유형이 있습니다. 최종 사용자 역할은 사용자 포털에서 가상 리소스를 사용 및 관리합니다. 관리자 역할은 관리 포털에서 시스템 인프라를 관리합니다. 가상 머신 및 호스트와 같은 개별 리소스 또는 클러스터 및 데이터 센터와 같은 개체 계층에 대해 역할을 할당할 수 있습니다.

15.2. 디렉토리 서버 소개

설치 과정에서 Red Hat Virtualization Manager는 **internal** 도메인에 **admin** 사용자를 생성합니다. 이 사용자는 **admin@internal**이라고 부르기도 합니다. 이 계정은 초기 환경 설정 시 및 문제 해결 시 사용됩니다. 외부 디렉토리 서버를 연결하고, 디렉토리 서버를 추가하고, 적절한 역할 및 권한을 할당하고 나서 **admin@internal** 사용자가 필요하지 않으면 비활성화합니다. 지원되는 디렉토리 서버는 다음과 같습니다:

- 389ds
- 389ds RFC-2307 스키마
- Active Directory
- FreeIPA
- Red Hat Identity Management (IdM)
- Novell eDirectory RFC-2307 스키마
- OpenLDAP RFC-2307 스키마
- OpenLDAP Standard 스키마
- Oracle Unified Directory RFC-2307 스키마
- RFC-2307 스키마 (일반)
- Red Hat Directory Server (RHDS)
- Red Hat Directory Server (RHDS) RFC-2307 스키마
- iPlanet

**중요**

동일한 시스템에 Red Hat Virtualization Manager (rhev) 및 IdM (ipa-server)을 설치할 수 없습니다. IdM은 mod_ssl 패키지와 호환되지 않으며 Red Hat Virtualization Manager가 필요합니다.

**중요**

디렉토리 서버로 Active Directory를 사용하고 있고 템플릿 및 가상 머신 생성에 **sysprep**을 사용하고자 할 경우 Red Hat Virtualization 관리자에게 다음과 같은 도메인 제어 권한을 위임해야 합니다:

- 컴퓨터를 도메인에 가입
- 그룹 멤버십 수정

Active Directory에 사용자 계정 생성에 대한 보다 자세한 내용은 <http://technet.microsoft.com/en-us/library/cc732336.aspx>에서 확인하십시오.

Active Directory에서 관리 제어 권한 위임에 대한 보다 자세한 내용은 <http://technet.microsoft.com/en-us/library/cc732524.aspx>에서 참조하십시오.

15.3. 외부 LDAP 공급자 설정

15.3.1. 외부 LDAP 공급자 설정 (대화형 설정)

ovirt-engine-extension-aaa-ldap 확장자를 사용하여 사용자 지정 외부 디렉토리를 쉽게 설정합니다. **ovirt-engine-extension-aaa-ldap** 확장자는 여러 다른 LDAP 서버 유형을 지원하며 사용자에게 제공되는 대화형 (interactive) 설정 스크립트를 사용하여 대부분의 LDAP 유형을 설정할 수 있습니다.

LDAP 서버 유형이 대화형 설정 스크립트 목록에 없거나 보다 많은 사용자 정의 설정을 원하는 경우 설정 파일을 수동으로 편집할 수 있습니다. 보다 자세한 내용은 **15.3.3절. “외부 LDAP 공급자 설정 (수동 설정)”**에서 참조하십시오.

Active Directory의 예는 **15.3.2절. “Active Directory 연결”**에서 참조하십시오.

전제 조건:

- DNS 또는 LDAP 서버의 도메인 이름을 알아야 합니다. Round-robin 및 장애 조치 failover 정책이 지원됩니다.
- LDAP 서버와 Manager 간의 보안 연결을 설정하려면 PEM 인코딩된 CA 인증서가 준비되었는지 확인합니다.
- LDAP 서버에 검색 및 로그인 쿼리를 수행할 수 있는 계정 이름과 암호를 최소한 하나 준비해 놓습니다.

절차 15.1. 외부 LDAP 공급자 설정

1. Red Hat Virtualization Manager에서 LDAP 확장 패키지를 설치합니다:

```
# yum install ovirt-engine-extension-aaa-ldap-setup
```

2. **ovirt-engine-extension-aaa-ldap-setup** 명령을 실행해서 대화형 설정을 시작합니다:

```
# ovirt-engine-extension-aaa-ldap-setup
```

3. 해당하는 번호를 입력해서 LDAP 유형을 선택합니다. 사용자의 LDAP 서버의 스키마가 확실하지 않다면 사용자 LDAP 서버 유형의 표준 스키마를 선택합니다. Active Directory의 경우 [15.3.2 절. “Active Directory 연결”](#)의 절차를 사용합니다.

```
Available LDAP implementations:
1 - 389ds
2 - 389ds RFC-2307 Schema
3 - Active Directory
4 - IPA
5 - Novell eDirectory RFC-2307 Schema
6 - OpenLDAP RFC-2307 Schema
7 - OpenLDAP Standard Schema
8 - Oracle Unified Directory RFC-2307 Schema
9 - RFC-2307 Schema (Generic)
10 - RHDS
11 - RHDS RFC-2307 Schema
12 - iPlanet
Please select: 10
```

4. **Enter**를 눌러서 기본값을 수락하고 LDAP 서버 이름의 도메인 이름 확인을 설정합니다:

```
It is highly recommended to use DNS resolution for LDAP server.
If for some reason you intend to use hosts or plain address disable
DNS usage.
Use DNS (Yes, No) [Yes]:
```

5. 해당하는 번호를 입력해서 DNS 정책 방식을 선택합니다:

```
1 - Single server
2 - DNS domain LDAP SRV record
3 - Round-robin between multiple hosts
4 - Failover between multiple hosts
Please select:
```

- 1번 옵션의 경우 **/etc/resolv.conf**에 표시된 DNS 서버를 사용하여 IP 주소를 확인합니다. **/etc/resolv.conf** 파일이 올바른 DNS 서버를 업데이트했는지 확인합니다.

LDAP 서버의 정규화된 도메인 이름(FQDN) 또는 IP 주소를 입력합니다. SRV 레코드와 **dig** 명령을 사용하여 도메인 이름을 찾을 수 있습니다. SRV 레코드 형식은 다음과 같습니다: **_service._protocol.domain name**. 예: **dig _ldap._tcp.redhat.com SRV**.
- 2번 옵션의 경우 DNS 서버의 도메인 이름을 입력합니다. DNS 검색을 실행하여 SRV 레코드를 검색해서 LDAP 서버의 도메인 이름을 찾습니다.
- 3번 옵션의 경우 공백으로 구분된 LDAP 서버 목록을 입력합니다. 서버의 FQDN 또는 IP 주소를 사용합니다. 이 정책을 통해 LDAP 서버 간 로드 밸런싱이 제공됩니다. 쿼리는 round-robin 알고리즘을 바탕으로 모든 LDAP 서버에 분배됩니다.
- 4번 옵션의 경우 공백으로 구분된 LDAP 서버 목록을 입력합니다. 서버의 FQDN 또는 IP 주소를 사용합니다. 이 정책을 통해 첫 LDAP 서버를 쿼리에 응답하는 기본 LDAP 서버로 정의합니다. 첫 서버를 사용할 수 없는 경우 쿼리는 목록에 있는 다음 LDAP 서버로 갑니다.

6. 사용자의 LDAP 서버가 지원하는 보안 연결 방식을 선택하고 PEM 인코딩된 CA 인증서를 취득하는 방법을 지정합니다. 파일 옵션을 사용하여 인증서로의 전체 경로를 지정할 수 있습니다. URL 옵션을 사용하여 인증서로의 URL을 지정할 수 있습니다. 인라인 옵션을 사용하여 인증서 내용을 터미널에 복사할 수 있습니다. 시스템 옵션을 사용하여 모든 CA 파일의 기본 위치를 지정할 수 있습니다. 비보안 (insecure) 모드를 선택하는 경우에도 TLS를 사용하여 연결이 암호화되지만 인증서 확인은 건너뛰니다.

NOTE:

It is highly recommended to use secure protocol to access the LDAP server.

Protocol startTLS is the standard recommended method to do so.

Only in cases in which the startTLS is not supported, fallback to non standard ldaps protocol.

Use plain for test environments only.

Please select protocol to use (startTLS, ldaps, plain) [startTLS]:
startTLS

Please select method to obtain PEM encoded CA certificate (File, URL, Inline, System, Insecure): *File*

Please enter the password:

**참고**

LDAPS는 Lightweight Directory Access Protocol Over Secure Socket Links의 약자입니다. SSL 연결의 경우 **ldaps** 옵션을 선택합니다.

7. 검색 사용자 고유 이름을 입력합니다. 해당 사용자는 디렉토리 서버에서 모든 사용자 및 그룹에 대한 검색 권한이 있어야 합니다. LDAP 어노테이션(annotation)에 검색 사용자를 지정해야 합니다. 익명 검색이 허용되는 경우 아무것도 입력하지 않고 **Enter**를 누릅니다.

Enter search user DN (empty for anonymous):

uid=user1,ou=Users,dc=test,dc=redhat,dc=com

Enter search user password:

8. 기본 DN을 입력합니다.

Please enter base DN (dc=redhat,dc=com) [dc=redhat,dc=com]:

9. 가상 머신에 단일 로그인을 설정하려면 **Yes**를 입력합니다. 해당 기능은 관리 포털 및 사용자 포털 기능에 대한 단일 로그인과 함께 사용할 수 없습니다. 스크립트에서는 프로필 이름이 도메인 이름과 일치해야 함을 미리 알립니다. [가상 머신 관리 가이드](#)에 있는 [가상 머신에 대한 단일 로그인 설정](#)의 지침을 계속해서 따라야 합니다.

Are you going to use Single Sign-On for Virtual Machines (Yes, No)

[No]:

10. 프로파일 이름을 지정합니다. 프로파일 이름은 로그인 페이지에서 사용자에게 표시됩니다. 다음의 예시에서는 **redhat.com**을 사용합니다.



참고

`/etc/ovirt-engine/extensions.d/redhat.com-authn.properties` 파일에 있는 `ovirt.engine.aaa.authn.profile.name` 속성을 편집해서 도메인 설정 후 프로파일 이름을 변경합니다. 변경 사항을 적용하려면 engine 서비스를 다시 시작합니다.

Please specify profile name that will be visible to users:`redhat.com`

그림 15.1. 관리 포털 로그인 페이지



참고

처음 로그인 시 드롭 다운 목록에서 원하는 프로파일을 선택해야 합니다. 해당 정보는 브라우저 쿠키에 저장되어 다음 로그인 시 미리 선택됩니다.

11. 검색 및 로그인 기능을 테스트해서 사용자의 LDAP 서버가 Red Hat Virtualization 환경에 올바르게 연결되었는지 확인합니다. 로그인 쿼리를 위해 계정 이름 및 암호를 입력합니다. 검색 쿼리를 위해 사용자 계정의 경우 **Principal**을 선택하고 그룹 계정의 경우 **Group**을 선택합니다. **Resolve Groups**에 대해 **Yes**로 대답하면 사용자 계정의 그룹 계정 정보가 반환됩니다. **Done**을 선택하여 설정을 완료합니다. 세 개의 설정 파일이 생성되며 출력 화면에 표시됩니다.

NOTE:

It is highly recommended to test drive the configuration before applying it into engine.

Perform at least one Login sequence and one Search sequence.

Select test sequence to execute (Done, Abort, Login, Search)

[Abort]: Login

Enter search user name: `testuser1`

Enter search user password:

[INFO] Executing login sequence...

...

Select test sequence to execute (Done, Abort, Login, Search)

[Abort]: Search

Select entity to search (Principal, Group) [Principal]:

```

Term to search, trailing '*' is allowed: testuser1
Resolve Groups (Yes, No) [No]:
[ INFO ] Executing login sequence...
...
Select test sequence to execute (Done, Abort, Login, Search)
[Abort]: Done
[ INFO ] Stage: Transaction setup
[ INFO ] Stage: Misc configuration
[ INFO ] Stage: Package installation
[ INFO ] Stage: Misc configuration
[ INFO ] Stage: Transaction commit
[ INFO ] Stage: Closing up
CONFIGURATION SUMMARY
Profile name is: redhat.com
The following files were created:
    /etc/ovirt-engine/aaa/redhat.com.properties
    /etc/ovirt-engine/extensions.d/redhat.com-
authz.properties
    /etc/ovirt-engine/extensions.d/redhat.com-
authn.properties
[ INFO ] Stage: Clean up
    Log file is available at /tmp/ovirt-engine-extension-aaa-
ldap-setup-20160114064955-1yar9i.log:
[ INFO ] Stage: Pre-termination
[ INFO ] Stage: Termination

```

12. engine 서비스를 다시 시작합니다. 생성된 프로파일이 관리 포털과 사용자 포털의 로그인 페이지에서 사용 가능합니다. LDAP 서버의 사용자 계정에 예를 들어 사용자 포털 로그인과 같이 적절한 역할 및 권한을 할당하는 방법은 15.6절. “관리 포털에서 사용자 작업 관리”에서 참조하십시오.

```
# systemctl restart ovirt-engine.service
```



참고

보다 자세한 내용은 `/usr/share/doc/ovirt-engine-extension-aaa-ldap-version`에 있는 LDAP 인증 확장 README 파일에서 참조하십시오.

15.3.2. Active Directory 연결

전제 조건:

- Active Directory 포리스트 이름을 알아야 합니다. 포리스트 이름은 root 도메인 이름이라고도 합니다.
- Active Directory 포리스트 이름을 확인할 수 있는 DNS 서버를 Manager에 있는 `/etc/resolv.conf` 파일에 추가하거나 Active Directory DNS 서버를 적어 놓았다가 대화형 (interactive) 설정 스크립트에서 메시지가 나타나면 해당 서버를 입력합니다.
- LDAP 서버와 Manager 간의 보안 연결을 설정하려면 PEM 인코딩된 CA 인증서를 준비합니다. 보다 자세한 내용은 D.2절. “Manager 및 LDAP 서버 간의 SSL 또는 TLS 연결 설정”을 참조하십시오.
- 익명 검색이 지원되지 않는 경우 모든 사용자 및 그룹에 대한 검색 권한이 있는 사용자가 Active Directory에서 검색 사용자로 사용 가능해야 합니다. 검색 사용자의 고유 이름(DN)을 적어 놓습니다. Active Directory의 관리 사용자를 사용하지 않습니다.

- Active Directory에 검색 및 로그인 쿼리를 수행할 수 있는 계정 이름과 암호를 최소한 하나 준비해 놓습니다.

절차 15.2. 외부 LDAP 공급자 설정

1. Red Hat Virtualization Manager에서 LDAP 확장 패키지를 설치합니다:

```
# yum install ovirt-engine-extension-aaa-ldap-setup
```

2. **ovirt-engine-extension-aaa-ldap-setup** 명령을 실행해서 대화형 설정을 시작합니다:

```
# ovirt-engine-extension-aaa-ldap-setup
```

3. 해당하는 번호를 입력해서 LDAP 유형을 선택합니다. LDAP 유형에 따라 이후의 단계에 있는 LDAP 관련 질문이 다릅니다.

```
Available LDAP implementations:
1 - 389ds
2 - 389ds RFC-2307 Schema
3 - Active Directory
4 - IPA
5 - Novell eDirectory RFC-2307 Schema
6 - OpenLDAP RFC-2307 Schema
7 - OpenLDAP Standard Schema
8 - Oracle Unified Directory RFC-2307 Schema
9 - RFC-2307 Schema (Generic)
10 - RHDS
11 - RHDS RFC-2307 Schema
12 - iPlanet
Please select: 3
```

4. Active Directory 포리스트 이름을 입력합니다. Manager의 DNS에서 포리스트 이름을 확인할 수 없는 경우 스크립트의 메시지에 따라 공백으로 구분된 Active Directory DNS 서버 이름 목록을 입력합니다.

```
Please enter Active Directory Forest name: ad-example.redhat.com
[ INFO ] Resolving Global Catalog SRV record for ad-
example.redhat.com
[ INFO ] Resolving LDAP SRV record for ad-example.redhat.com
```

5. 사용자의 LDAP 서버가 지원하는 보안 연결 방식을 선택하고 PEM 인코딩된 CA 인증서를 취득하는 방법을 지정합니다. 파일 옵션을 사용하여 인증서로의 전체 경로를 지정할 수 있습니다. URL 옵션을 사용하여 인증서로의 URL을 지정할 수 있습니다. 인라인 옵션을 사용하여 인증서 내용을 터미널에 복사할 수 있습니다. 시스템 옵션을 사용하여 모든 CA 파일의 위치를 지정할 수 있습니다. 비보안 (insecure) 옵션을 사용하여 비보안 (insecure) 모드에서 startTLS를 사용합니다.

NOTE:

It is highly recommended to use secure protocol to access the LDAP server.

Protocol startTLS is the standard recommended method to do so.

Only in cases in which the startTLS is not supported, fallback to non standard ldaps protocol.

Use plain for test environments only.

Please select protocol to use (startTLS, ldaps, plain) [startTLS]:

startTLS

Please select method to obtain PEM encoded CA certificate (File, URL, Inline, System, Insecure): *File*
Please enter the password:



참고

LDAPS는 Lightweight Directory Access Protocol Over Secure Socket Links의 약자입니다. SSL 연결의 경우 **ldaps** 옵션을 선택합니다.

PEM 인코딩된 CA 인증서 생성에 대한 보다 자세한 내용은 [D.2절. “Manager 및 LDAP 서버 간의 SSL 또는 TLS 연결 설정”](#)에서 참조하시기 바랍니다.

6. 검색 사용자 고유 이름을 입력합니다. 해당 사용자는 디렉토리 서버에서 모든 사용자 및 그룹에 대한 검색 권한이 있어야 합니다. 이 검색 사용자는 LDAP 어노테이션(annotation)에 지정되어 있어야 합니다. 익명 검색이 허용되는 경우 아무것도 입력하지 않고 **Enter**를 누릅니다.

Enter search user DN (empty for anonymous):
uid=user1,ou=Users,dc=test,dc=redhat,dc=com
Enter search user password:

7. 프로파일 이름을 지정합니다. 프로파일 이름은 로그인 페이지에서 사용자에게 표시됩니다. 다음의 예시에서는 **redhat.com**을 사용합니다.

Please specify profile name that will be visible to users:*redhat.com*

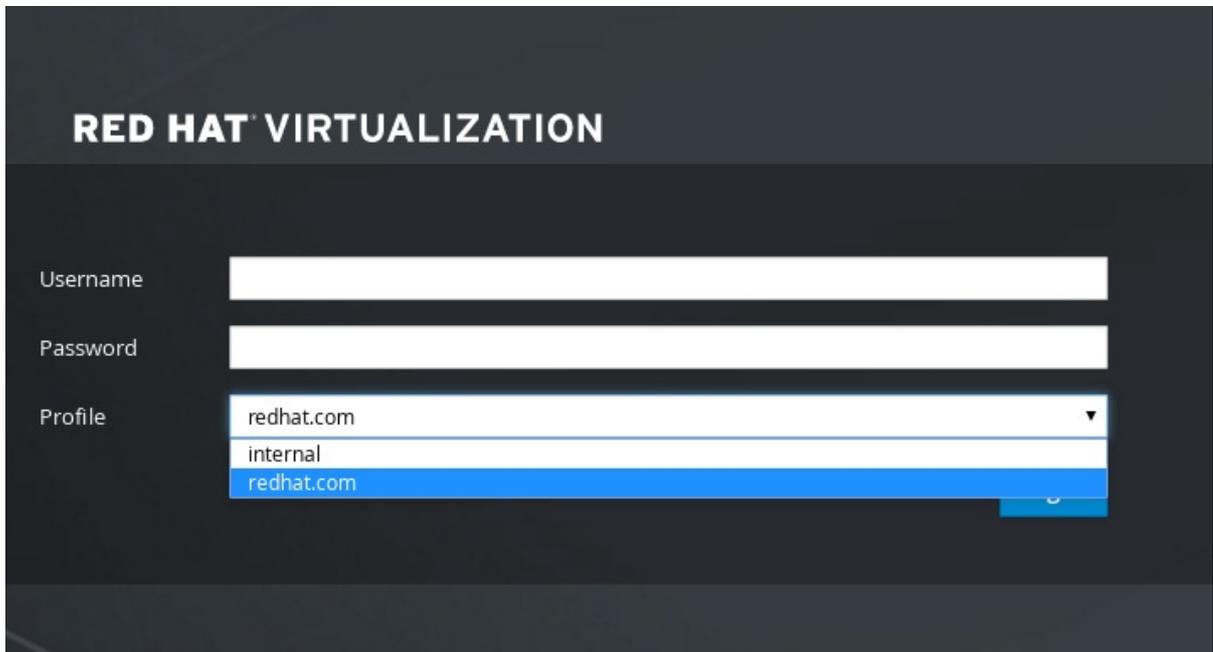


그림 15.2. 관리 포털 로그인 페이지



참고

처음 로그인 시 드롭 다운 목록에서 원하는 프로파일을 선택해야 합니다. 해당 정보는 브라우저 쿠키에 저장되어 다음 로그인 시 미리 선택됩니다.

8. 검색 및 로그인 기능을 테스트해서 사용자의 LDAP 서버가 Red Hat Virtualization 환경에 올바

르게 연결되었는지 확인합니다. 로그인 쿼리를 위해 계정 이름 및 암호를 입력합니다. 검색 쿼리를 위해 사용자 계정의 경우 **Principal**을 선택하고 그룹 계정의 경우 **Group**을 선택합니다. **Resolve Groups**에 대해 **Yes**로 대답하면 사용자 계정의 그룹 계정 정보가 반환됩니다. **Done**을 선택하여 설정을 완료합니다. 세 개의 설정 파일이 생성되며 출력 화면에 표시됩니다.

NOTE:

It is highly recommended to test drive the configuration before applying it into engine.

Perform at least one Login sequence and one Search sequence.

Select test sequence to execute (Done, Abort, Login, Search)

[Abort]: Login

Enter search user name: *testuser1*

Enter search user password:

[INFO] Executing login sequence...

...

Select test sequence to execute (Done, Abort, Login, Search)

[Abort]: Search

Select entity to search (Principal, Group) [Principal]:

Term to search, trailing '*' is allowed: *testuser1*

Resolve Groups (Yes, No) [No]:

[INFO] Executing login sequence...

...

Select test sequence to execute (Done, Abort, Login, Search)

[Abort]: Done

[INFO] Stage: Transaction setup

[INFO] Stage: Misc configuration

[INFO] Stage: Package installation

[INFO] Stage: Misc configuration

[INFO] Stage: Transaction commit

[INFO] Stage: Closing up

CONFIGURATION SUMMARY

Profile name is: *redhat.com*

The following files were created:

/etc/ovirt-engine/aaa/redhat.com.properties

/etc/ovirt-engine/extensions.d/redhat.com-

authz.properties

/etc/ovirt-engine/extensions.d/redhat.com-

authn.properties

[INFO] Stage: Clean up

Log file is available at */tmp/ovirt-engine-extension-aaa-*

ldap-setup-20160114064955-1yar9i.log:

[INFO] Stage: Pre-termination

[INFO] Stage: Termination

9. 생성된 프로파일이 관리 포털과 사용자 포털의 로그인 페이지에서 사용 가능합니다. LDAP 서버의 사용자 계정에 예를 들어 사용자 포털 로그인과 같이 적절한 역할 및 권한을 할당하는 방법은 [15.6절. “관리 포털에서 사용자 작업 관리”](#)에서 참조하십시오.

**참고**

보다 자세한 내용은 */usr/share/doc/ovirt-engine-extension-aaa-ldap-version*에 있는 LDAP 인증 확장 README 파일에서 참조하십시오.

15.3.3. 외부 LDAP 공급자 설정 (수동 설정)

ovirt-engine-extension-aaa-ldap 확장은 LDAP 프로토콜을 사용하여 디렉토리 서버에 액세스하며 사용자 정의 가능합니다. 사용자 포털 또는 관리 포털에 단일 사용 승인(single sign-on)을 활성화하는 경우를 제외하면 Kerberos 인증을 하지 않아도 됩니다.

이전 부분의 대화형 설정 방식이 사용자의 경우에 해당되지 않으면 설정 파일을 수동으로 수정해서 LDAP 서버를 연결합니다. 다음의 절차는 일반적인 내용입니다. 사용자의 설정에 맞도록 해당 값을 변경합니다.

절차 15.3. 외부 LDAP 공급자 수동 설정

1. Red Hat Virtualization Manager에서 LDAP 확장 패키지를 설치합니다:

```
# yum install ovirt-engine-extension-aaa-ldap
```

2. LDAP 설정 템플릿 파일을 **/etc/ovirt-engine** 디렉토리에 복사합니다. 템플릿 파일은 Active Directory (**ad**) 및 기타 다른 디렉토리 유형 (**simple**)에서 사용할 수 있습니다. 다음 예에서는 간단한 설정 템플릿을 사용합니다.

```
# cp -r /usr/share/ovirt-engine-extension-aaa-ldap/examples/simple/.
/etc/ovirt-engine
```

3. 관리 포털 및 사용자 포털 로그인 페이지에서 표시되길 원하는 이름으로 설정 파일의 이름을 변경합니다:

```
# mv /etc/ovirt-engine/aaa/profile1.properties /etc/ovirt-
engine/aaa/example.properties
# mv /etc/ovirt-engine/extensions.d/profile1-authn.properties
/etc/ovirt-engine/extensions.d/example-authn.properties
# mv /etc/ovirt-engine/extensions.d/profile1-authz.properties
/etc/ovirt-engine/extensions.d/example-authz.properties
```

4. LDAP 서버 유형을 주석 해제하고 도메인 및 암호 필드를 업데이트하여 LDAP 속성 설정 파일을 편집합니다:

```
# vi /etc/ovirt-engine/aaa/example.properties
```

예 15.1. 프로파일 예: LDAP 서버 부분

```
# Select one
#
include = <openldap.properties>
#include = <389ds.properties>
#include = <rhds.properties>
#include = <ipa.properties>
#include = <iplanet.properties>
#include = <rfc2307-389ds.properties>
#include = <rfc2307-rhds.properties>
#include = <rfc2307-openldap.properties>
#include = <rfc2307-edir.properties>
#include = <rfc2307-generic.properties>

# Server
#
vars.server = ldap1.company.com
```

```
# Search user and its password.
#
vars.user = uid=search,cn=users,cn=accounts,dc=company,dc=com
vars.password = 123456

pool.default.serverset.single.server = ${global:vars.server}
pool.default.auth.simple.bindDN = ${global:vars.user}
pool.default.auth.simple.password = ${global:vars.password}
```

LDAP 서버와 통신하는 TLS 또는 SSL 프로토콜을 사용하려면 LDAP 서버의 root CA 인증서를 취득하고 이를 사용하여 공개 keystore 파일을 생성합니다. 다음 행을 주석 해제 처리하고 공개 keystore 파일로의 완전 경로 및 파일에 액세스하기 위한 암호를 지정합니다.



참고

공개 keystore 파일 생성에 대한 보다 자세한 내용은 [D.2절. “Manager 및 LDAP 서버 간의 SSL 또는 TLS 연결 설정”](#)에서 참조하십시오.

예 15.2. 프로파일 예: keystore 부분

```
# Create keystore, import certificate chain and uncomment
# if using tls.
pool.default.ssl.startTLS = true
pool.default.ssl.truststore.file = /full/path/to/myrootca.jks
pool.default.ssl.truststore.password = password
```

- 인증 설정 파일을 확인합니다. 관리 포털 및 사용자 포털 로그인 페이지에서 사용자가 볼 수 있는 프로파일 이름은 **ovirt.engine.aaa.authn.profile.name**에 정의되어 있습니다. 설정 프로파일 위치는 LDAP 설정 파일 위치와 일치해야 합니다. 모든 필드는 기본값으로 둘 수 있습니다.

```
# vi /etc/ovirt-engine/extensions.d/example-authn.properties
```

예 15.3. 인증 설정 파일의 예

```
ovirt.engine.extension.name = example-authn
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module =
org.ovirt.engine-extensions.aaa ldap
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engineextensions.aaa ldap.AuthnExtension
ovirt.engine.extension.provides =
org.ovirt.engine.api.extensions.aaa.Authn
ovirt.engine.aaa.authn.profile.name = example
ovirt.engine.aaa.authn.authz.plugin = example-authz
config.profile.file.1 = ../aaa/example.properties
```

- 인증 설정 파일을 확인합니다. 설정 프로파일 위치는 LDAP 설정 파일 위치와 일치해야 합니다. 모든 필드는 기본값으로 둘 수 있습니다.

```
# vi /etc/ovirt-engine/extensions.d/example-authz.properties
```

예 15.4. 인증 설정 파일의 예

```
ovirt.engine.extension.name = example-authz
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module =
org.ovirt.engine-extensions.aaa.ldap
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engineextensions.aaa.ldap.AuthzExtension
ovirt.engine.extension.provides =
org.ovirt.engine.api.extensions.aaa.Authz
config.profile.file.1 = ../aaa/example.properties
```

7. 설정 파일의 소유권 및 권한이 적절한지 확인합니다:

```
# chown ovirt:ovirt /etc/ovirt-engine/aaa/example.properties
```

```
# chmod 600 /etc/ovirt-engine/aaa/example.properties
```

8. engine 서비스를 다시 시작합니다:

```
# systemctl restart ovirt-engine.service
```

9. 생성된 *example* 프로파일이 관리 포털과 사용자 포털의 로그인 페이지에서 사용 가능합니다. LDAP 서버의 사용자 계정에 예를 들어 사용자 포털 로그인과 같이 적절한 권한을 할당하는 방법은 15.6절. “관리 포털에서 사용자 작업 관리”에서 참조하십시오.



참고

보다 자세한 내용은 `/usr/share/doc/ovirt-engine-extension-aaa-ldap-version`에 있는 LDAP 인증 확장 README 파일에서 참조하십시오.

15.4. 단일 사용 승인(SSO)을 위해 LDAP 및 KERBEROS 설정

단일 로그인을 사용하면 암호를 다시 입력하지 않고도 사용자 포털 또는 관리 포털에 로그인할 수 있습니다. 인증 정보는 Kerberos 서버에서 얻습니다. 관리 포털 및 사용자 포털에 단일 로그인을 설정하려면 `ovirt-engine-extension-aaa-misc` 및 `ovirt-engine-extension-aaa-ldap`라는 두 개의 확장 파일과 `mod_auth_gssapi` 및 `mod_session`이라는 두 개의 Apache 모듈을 설정해야 합니다. Kerberos를 사용하지 않는 단일 로그인을 설정할 수도 있지만 이 문서에서는 해당 내용을 다루지 않습니다.



참고

사용자 포털에 단일 사용 승인이 활성화되어 있을 경우 가상 머신으로의 단일 사용 승인은 사용할 수 없게 됩니다. 사용자 포털로의 단일 사용 승인이 활성화되어 있으면 사용자 포털에서는 암호를 확인할 필요가 없기 때문에 암호는 가상 머신에 사용 승인하도록 위임될 수 없습니다.

예시에서는 다음을 전제로 합니다:

- 기존 KDC (Key Distribution Center) 서버는 Kerberos 5의 MIT 버전을 사용합니다.
- KDC 서버의 관리자 권한이 있어야 합니다.
- Red Hat Virtualization Manager 및 사용자 시스템에 Kerberos 클라이언트가 설치되어 있어야 합니다.
- **kadmin** 유틸리티를 사용하여 Kerberos 서비스 사용자 및 **keytab** 파일을 생성합니다.

이는 다음과 같은 요소로 구성되어 있어야 합니다:

KDC 서버

- Red Hat Virtualization Manager에서 Apache 서비스의 **keytab** 파일 및 서비스 사용자를 생성합니다.

Red Hat Virtualization Manager

- 인증 확장 패키지 및 Apache Kerberos 인증 모듈을 설치합니다.
- 확장 파일을 설정합니다.

절차 15.4. Apache 서비스의 Kerberos 설정

1. KDC 서버에서 **kadmin** 유틸리티를 사용하여 Red Hat Virtualization Manager에서 Apache 서비스에 대한 서비스 사용자를 생성합니다. 서비스 사용자는 Apache 서비스에 대한 KDC의 참조 ID입니다.

```
# kadmin
kadmin> addprinc -randkey HTTP/fqdn-of-rhevm@REALM.COM
```

2. Apache 서비스의 **keytab** 파일을 생성합니다. **keytab** 파일은 공유 비밀 키를 저장합니다.

```
kadmin> ktadd -k /tmp/http.keytab HTTP/fqdn-of-rhevm@REALM.COM
```

```
kadmin> quit
```

3. KDC 서버에서 Red Hat Virtualization Manager로 **keytab** 파일을 복사합니다:

```
# scp /tmp/http.keytab root@rhevm.example.com:/etc/httpd
```

절차 15.5. 사용자 포털 또는 관리 포털에 단일 사용 승인 (SSO) 설정

1. Red Hat Virtualization Manager에서 **keytab**의 소유권 및 권한이 적절한지 확인합니다:

```
# chown apache /etc/httpd/http.keytab
```

```
# chmod 400 /etc/httpd/http.keytab
```

2. 인증 확장 패키지, LDAP 확장 패키지, **mod_auth_gssapi** 및 **mod_session** Apache 모듈을 설치합니다.

```
# yum install ovirt-engine-extension-aaa-misc ovirt-engine-
extension-aaa-ldap mod_auth_gssapi mod_session
```

3. SSO 설정 템플릿 파일을 **/etc/ovirt-engine** 디렉토리에 복사합니다. 템플릿 파일은 Active Directory (**ad-ss0**) 및 기타 다른 디렉토리 유형 (**simple-ss0**)에서 사용할 수 있습니다. 다음 예에서는 간단한 SSO 설정 템플릿을 사용합니다.

```
# cp -r /usr/share/ovirt-engine-extension-aaa-ldap/examples/simple-
sso/. /etc/ovirt-engine
```

4. **ovirt-ss0.conf**를 Apache 설정 디렉토리로 이동합니다.

```
# mv /etc/ovirt-engine/aaa/ovirt-ss0.conf /etc/httpd/conf.d
```

5. 인증 방식 파일을 검토합니다. 영역은 **keytab** 파일에서 자동으로 가져오므로 이 파일을 편집할 필요는 없습니다.

```
# vi /etc/httpd/conf.d/ovirt-ss0.conf
```

예 15.5. 인증 방식 파일의 예

```
<LocationMatch ^/ovirt-engine/sso/(interactive-login-
negotiate|oauth/token-http-auth)|^/ovirt-engine/api>
  <If "req('Authorization') !~ /^(Bearer|Basic)/i">
    RewriteEngine on
    RewriteCond %{LA-U:REMOTE_USER} ^(.*)$
    RewriteRule ^(.*)$ - [L,NS,P,E=REMOTE_USER:%1]
    RequestHeader set X-Remote-User %{REMOTE_USER}s

    AuthType GSSAPI
    AuthName "Kerberos Login"

    # Modify to match installation
    GssapiCredStore keytab:/etc/httpd/http.keytab
    GssapiUseSessions On
    Session On
    SessionCookieName ovirt_gssapi_session
    path=/private;httponly;secure;

    Require valid-user
    ErrorDocument 401 "<html><meta http-equiv=\"refresh\"
content=\"0; url=/ovirt-engine/sso/login-unauthorized\"/><body><a
href=\"/ovirt-engine/sso/login-unauthorized\">Here</a></body>
</html>"
  </If>
</LocationMatch>
```

6. 관리 포털 및 사용자 포털 로그인 페이지에서 표시되길 원하는 이름으로 설정 파일의 이름을 변경합니다:

```
# mv /etc/ovirt-engine/aaa/profile1.properties /etc/ovirt-
engine/aaa/example.properties
```

```
# mv /etc/ovirt-engine/extensions.d/profile1-http-authn.properties
/etc/ovirt-engine/extensions.d/example-http-authn.properties
```

```
# mv /etc/ovirt-engine/extensions.d/profile1-http-mapping.properties
/etc/ovirt-engine/extensions.d/example-http-mapping.properties
```

```
# mv /etc/ovirt-engine/extensions.d/profile1-authz.properties
/etc/ovirt-engine/extensions.d/example-authz.properties
```

7. LDAP 서버 유형을 주석 해제하고 도메인 및 암호 필드를 업데이트하여 LDAP 속성 설정 파일을 편집합니다:

```
# vi /etc/ovirt-engine/aaa/example.properties
```

예 15.6. 프로파일 예: LDAP 서버 부분

```
# Select one
include = <openldap.properties>
#include = <389ds.properties>
#include = <rhds.properties>
#include = <ipa.properties>
#include = <iplanet.properties>
#include = <rfc2307-389ds.properties>
#include = <rfc2307-rhds.properties>
#include = <rfc2307-openldap.properties>
#include = <rfc2307-edir.properties>
#include = <rfc2307-generic.properties>

# Server
#
vars.server = ldap1.company.com

# Search user and its password.
#
vars.user = uid=search,cn=users,cn=accounts,dc=company,dc=com
vars.password = 123456

pool.default.serverset.single.server = ${global:vars.server}
pool.default.auth.simple.bindDN = ${global:vars.user}
pool.default.auth.simple.password = ${global:vars.password}
```

LDAP 서버와 통신하는 TLS 또는 SSL 프로토콜을 사용하려면 LDAP 서버의 root CA 인증서를 취득하고 이를 사용하여 공개 keystore 파일을 생성합니다. 다음 행을 주석 해제 처리하고 공개 keystore 파일로의 완전 경로 및 파일에 액세스하기 위한 암호를 지정합니다.



참고

공개 keystore 생성에 대한 보다 자세한 내용은 [D.2절. “Manager 및 LDAP 서버 간의 SSL 또는 TLS 연결 설정”](#)에서 참조하십시오.

예 15.7. 프로파일 예: keystore 부분

```
# Create keystore, import certificate chain and uncomment
# if using ssl/tls.
pool.default.ssl.startTLS = true
pool.default.ssl.truststore.file = /full/path/to/myrootca.jks
pool.default.ssl.truststore.password = password
```

8. 인증 설정 파일을 확인합니다. 관리 포털 및 사용자 포털 로그인 페이지에서 사용자가 볼 수 있는 프로파일 이름은 **ovirt.engine.aaa.authn.profile.name**에 정의되어 있습니다. 설정 프로파일 위치는 LDAP 설정 파일 위치와 일치해야 합니다. 모든 필드는 기본값으로 둘 수 있습니다.

```
# vi /etc/ovirt-engine/extensions.d/example-http-authn.properties
```

예 15.8. 인증 설정 파일의 예

```
ovirt.engine.extension.name = example-http-authn
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module =
org.ovirt.engine-extensions.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engineextensions.aaa.misc.http.AuthnExtension
ovirt.engine.extension.provides =
org.ovirt.engine.api.extensions.aaa.Authn
ovirt.engine.aaa.authn.profile.name = example-http
ovirt.engine.aaa.authn.authz.plugin = example-authz
ovirt.engine.aaa.authn.mapping.plugin = example-http-mapping
config.artifact.name = HEADER
config.artifact.arg = X-Remote-User
```

9. 인증 설정 파일을 확인합니다. 설정 프로파일 위치는 LDAP 설정 파일 위치와 일치해야 합니다. 모든 필드는 기본값으로 둘 수 있습니다.

```
# vi /etc/ovirt-engine/extensions.d/example-authz.properties
```

예 15.9. 인증 설정 파일 예

```
ovirt.engine.extension.name = example-authz
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module =
org.ovirt.engine-extensions.aaa.ldap
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engineextensions.aaa.ldap.AuthzExtension
ovirt.engine.extension.provides =
org.ovirt.engine.api.extensions.aaa.Authz
config.profile.file.1 = ../aaa/example.properties
```

10. 인증 매핑 설정 파일을 검토합니다. 설정 프로파일 위치는 LDAP 설정 파일 위치와 일치해야 합니다.


```
# systemctl restart ovirt-engine.service
```

15.5. 사용자 인증

15.5.1. 사용자 인증 모델

Red Hat Virtualization에서는 다음의 세 가지 구성 요소의 조합에 따라 인증 제어를 적용합니다:

- 작업을 수행하는 사용자
- 수행할 작업 유형
- 작업이 수행되고 있는 개체

15.5.2. 사용자 작업

작업을 성공적으로 수행하려면 **사용자에게 개체에 대한 적절한 권한**이 있어야 합니다. 작업 유형은 **권한**에 따라 다릅니다. 시스템에는 여러 다른 권한이 있습니다:

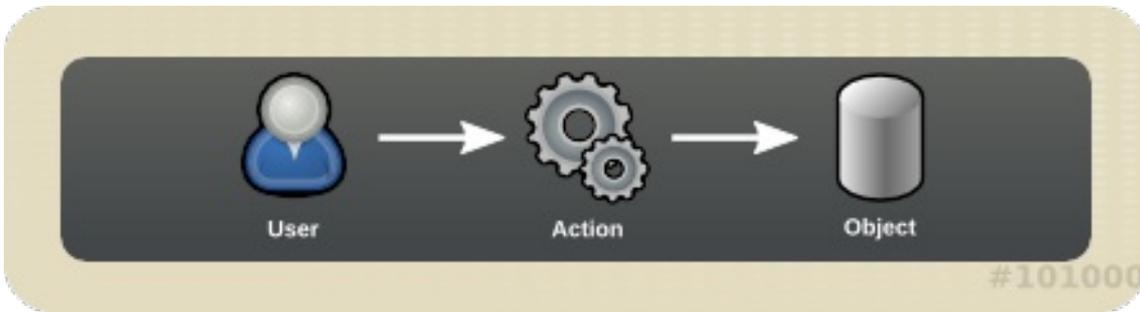


그림 15.3. 작업



중요

일부 작업은 하나 이상의 개체에서 수행됩니다. 예를 들어 템플릿을 다른 스토리지 도메인에 복사할 경우 템플릿 및 대상 스토리지 도메인 모두에 영향을 미치게 됩니다. 작업을 수행하는 사용자는 작업이 영향을 미치는 모든 개체에 대해 적절한 권한이 있어야 합니다.

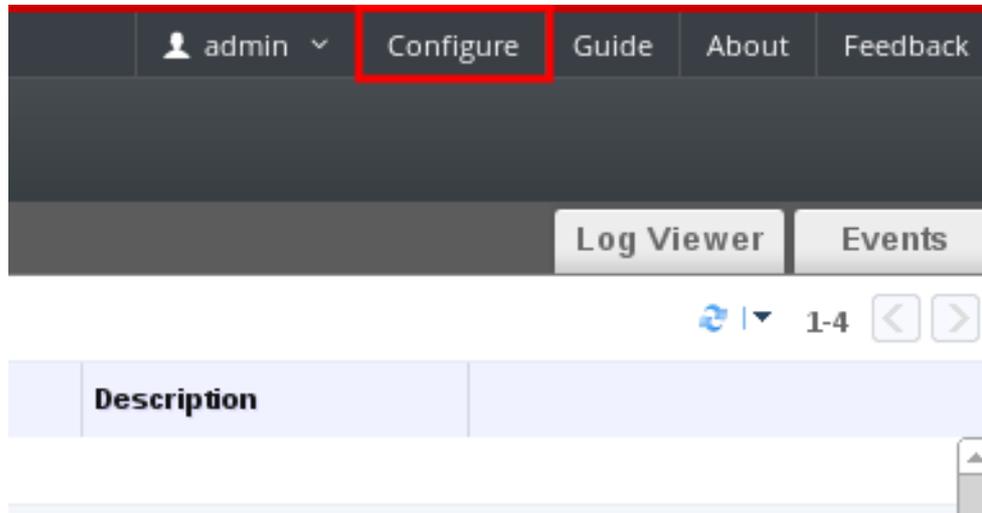
15.6. 관리 포털에서 사용자 작업 관리

15.6.1. 사용자 포털에 사용자 추가 및 권한 부여

사용자 계정을 먼저 생성한 후 사용자 포털에 해당 사용자를 추가하고 역할 및 권한을 할당합니다. 이 절차를 통해 할당된 역할 및 권한을 사용하여 사용자 포털에 로그인해서 가상 머신을 생성할 수 있습니다. 이러한 절차는 그룹 계정에도 적용됩니다.

절차 15.6. 사용자 포털에 사용자 추가 및 권한 부여

1. 머릿글 표시줄에서 **설정** 버튼을 클릭하여 **설정** 창을 엽니다. **시스템 권한**을 클릭합니다.



2. 추가를 클릭하여 사용자에게 시스템 권한 추가 창을 엽니다.
3. 검색 드롭 다운 메뉴에서 프로파일을 선택합니다. 이 프로파일은 사용자가 검색하려는 도메인입니다. 검색 텍스트 필드에 이름 또는 이름의 일부를 입력하고 **검색**을 클릭합니다. 다른 방법으로 **검색**을 클릭하여 모든 사용자 및 그룹 목록을 표시합니다.
4. 해당 사용자 또는 그룹의 확인란을 선택합니다.
5. 할당할 역할을 **할당된 역할**에서 선택합니다. **UserRole** 역할이 할당된 사용자 계정은 사용자 포털에 로그인 권한이 있습니다.
6. **OK**를 클릭합니다.

사용자 포털에 로그인해서 해당 사용자 계정이 로그인 권한이 있는지 확인합니다.

15.6.2. 사용자 정보 확인

사용자 탭에서 각 사용자에게 대한 상세 정보를 확인할 수 있습니다.

절차 15.7. 사용자 정보 확인

1. 사용자 탭을 클릭하여 권한이 부여된 사용자 목록을 표시합니다.
2. 사용자를 선택하거나 사용자가 검색 결과 목록에 표시되지 않으면 검색을 수행할 수 있습니다.
3. 상세 정보 창에서는 선택된 사용자에게 대해 표시합니다. 일반적으로 **일반 정보** 탭에서는 도메인 이름, 사용자 이메일 및 상태와 같은 일반적인 정보를 표시합니다.
4. 다른 탭에서는 사용자의 그룹, 권한, 쿼터, 이벤트를 확인할 수 있습니다.

예를 들어 사용자가 속한 그룹을 확인하려면 **디렉토리 그룹** 탭을 클릭합니다.

15.6.3. 리소스에서 사용자 권한 보기

사용자는 특정 리소스 또는 리소스 계층에 권한을 할당할 수 있습니다. 할당된 사용자 및 각 리소스에 권한을 확인할 수 있습니다.

절차 15.8. 리소스에서 사용자 권한 보기

1. 리소스 탭을 클릭하여 검색 결과 목록에서 리소스를 선택합니다.

- 상세 정보 창에 있는 **권한** 탭을 클릭하여 할당된 사용자, 사용자 역할, 선택한 리소스에 대해 상속된 권한을 나열합니다.

15.6.4. 사용자 삭제

사용자 계정이 더이상 필요하지 않을 경우 Red Hat Virtualization에서 삭제합니다.

절차 15.9. 사용자 삭제

- 사용자 탭을 클릭하여 권한이 부여된 사용자 목록을 표시합니다.
- 삭제할 사용자를 선택합니다. 사용자가 가상 머신을 실행하고 있지 않은지 확인합니다.
- 삭제** 버튼을 클릭합니다. 삭제할 지를 묻는 메시지가 나타나면 **OK**를 클릭합니다.

사용자가 외부 디렉토리에서가 아닌 Red Hat Virtualization에서 삭제됩니다.

15.6.5. 로그인한 사용자 확인

현재 로그인한 사용자의 세션 시간 및 기타 상세 정보를 볼 수 있습니다. 트리 창에서 **활성 사용자 세션** 항목을 클릭하여 각 로그인한 사용자의 세션 정보를 확인합니다.

15.6.6. 사용자 세션 종료

현재 로그인한 사용자 세션을 종료할 수 있습니다.

절차 15.10. 사용자 세션 종료

- 트리 창에서 **활성 사용자 세션** 항목을 클릭합니다.
- 종료할 사용자 세션을 선택합니다.
- 세션 종료**를 클릭합니다.
- OK**를 클릭합니다.

15.7. 명령행에서 사용자 작업 관리

15.7.1. 사용자 관리

ovirt-aaa-jdbc-tool 도구를 사용하여 내부 도메인에서 사용자 계정을 관리합니다. 이러한 도구를 사용하여 변경된 내용은 바로 적용되며 **ovirt-engine** 서비스를 다시 시작하지 않아도 됩니다. 사용자 옵션의 전체 목록을 보려면 **ovirt-aaa-jdbc-tool user --help** 명령을 실행합니다. 다음 부분에는 일반적인 예가 있습니다.

절차 15.11. 사용자 생성

다음 절차에서는 사용자 생성, 사용자 암호 설정, 그리고 사용자를 Red Hat Virtualization environment에 추가하는 방법에 대해 설명합니다.

- Red Hat Virtualization Manager가 설치된 시스템에 로그인합니다.
- 새 사용자 계정을 만듭니다. 옵션으로 **--attribute**를 사용하여 계정 상세 정보를 지정합니다. 전체 옵션 목록을 보려면 **ovirt-aaa-jdbc-tool user add --help** 명령을 실행합니다.

```
# ovirt-aaa-jdbc-tool user add test1 --attribute=firstName=John --
attribute=lastName=Doe
adding user test1...
user added successfully
```

3. 암호를 설정합니다. `--password-valid-to` 값을 설정하지 않으면 암호 만료 시간이 기본값인 현재 시간으로 설정됩니다. 날짜 형식은 `yyyy-MM-dd HH:mm:ssX`입니다. 다음의 예에서 `-0800`은 GMT에서 8시간을 빼는 것을 의미합니다. 더 많은 옵션을 보려면 `ovirt-aaa-jdbc-tool user password-reset --help`를 실행합니다.

```
# ovirt-aaa-jdbc-tool user password-reset test1 --password-valid-
to="2025-08-01 12:00:00-0800"
Password:
updating user test1...
user updated successfully
```



참고

기본적으로 내부 도메인의 사용자 계정 암호에 대한 정책은 다음과 같은 제한 사항이 있습니다:

- 최소 6글자
- 이전에 사용된 3개의 암호를 암호 변경 시 다시 사용할 수 없습니다.

암호 정책 및 다른 기본 설정에 대한 보다 자세한 내용을 보려면 `ovirt-aaa-jdbc-tool settings show`를 실행합니다.

4. 새로 만든 사용자를 관리 포털에 추가하고 적절한 역할 및 권한을 할당합니다. 보다 자세한 내용은 [15.6.1절. “사용자 포털에 사용자 추가 및 권한 부여”](#)에서 참조하십시오.

절차 15.12. 사용자 정보 확인

다음 절차에서는 사용자 계정 정보를 확인하는 방법에 대해 설명합니다. 관리 포털의 사용자 탭보다 더 많은 정보가 표시됩니다.

1. Red Hat Virtualization Manager가 설치된 시스템에 로그인합니다.
2. 다음 명령을 실행합니다:

```
# ovirt-aaa-jdbc-tool user show test1
```

절차 15.13. 사용자 정보 편집

다음 절차에서는 사용자 계정 정보를 업데이트하는 방법에 대해 설명합니다.

1. Red Hat Virtualization Manager가 설치된 시스템에 로그인합니다.
2. 사용자 정보를 편집하기 위해 다음 명령을 실행하십시오. 다음 예에서는 이메일 주소를 업데이트합니다.

```
# ovirt-aaa-jdbc-tool user edit test1 --
attribute=email=jdoe@example.com
```

절차 15.14. 사용자 삭제

다음 절차에서는 사용자 계정을 삭제하는 방법에 대해 설명합니다.

1. Red Hat Virtualization Manager가 설치된 시스템에 로그인합니다.
2. 사용자를 삭제합니다:

```
# ovirt-aaa-jdbc-tool user delete test1
```

3. 관리 포털에서 사용자를 삭제합니다. 보다 자세한 내용은 [15.6.4절. "사용자 삭제"](#)에서 참조하십시오.

15.7.2. 내부 관리자 암호 변경

내부 관리자 (**admin@internal**) 암호를 변경하려면 **ovirt-aaa-jdbc-tool** 도구를 사용합니다. **ovirt-engine** 서비스를 다시 시작하지 않아도 암호 변경 사항이 적용됩니다.

기본적으로 내부 도메인의 사용자 계정 암호에 대한 정책은 다음과 같은 제한 사항이 있습니다:

- 최소 6글자
- 이전에 사용된 3개의 암호를 암호 변경 시 다시 사용할 수 없습니다.

암호 정책 및 다른 기본 설정에 대한 보다 자세한 내용을 보려면 **ovirt-aaa-jdbc-tool settings show**를 실행합니다.

절차 15.15. 내부 관리자 암호 변경

1. Red Hat Virtualization Manager가 설치된 시스템에 로그인합니다.
2. 대화형 (interactive) 모드에서 암호를 변경하려면 다음의 명령을 실행합니다. **--password-valid-to** 값을 설정하지 않으면 암호 만료 시간이 기본값인 현재 시간으로 설정됩니다. 날짜 형식은 **yyyy-MM-dd HH:mm:ssX**입니다. 다음의 예에서 **Z**는 UTC 시간을 의미합니다. 더 많은 옵션을 보려면 **ovirt-aaa-jdbc-tool user password-reset --help**를 실행합니다.

```
# ovirt-aaa-jdbc-tool user password-reset admin --password-valid-to="2025-08-01 12:00:00Z"
```

15.7.3. 내부 관리자 비활성화

engine-setup 시 생성된 **admin@internal** 사용자를 포함한 로컬 도메인의 사용자를 비활성화할 수 있습니다. **admin** 사용자를 비활성화하기 전에 사용자 환경에 전체 관리 권한이 있는 사용자가 하나 이상인 것을 확인합니다.

절차 15.16. 내부 관리자 비활성화

1. Red Hat Virtualization Manager가 설치된 시스템에 로그인합니다.
2. **SuperUser** 역할이 있는 다른 사용자가 사용자 환경에 추가되었는지 확인합니다. 보다 자세한 내용은 [15.6.1절. "사용자 포털에 사용자 추가 및 권한 부여"](#)에서 참조하십시오.
3. 기본 **admin** 사용자를 비활성화합니다:

```
# ovirt-aaa-jdbc-tool user edit admin --flag=+disabled
```



참고

사용자를 다시 활성화하려면 **ovirt-aaa-jdbc-tool user edit username --flag=-disabled** 명령을 실행합니다.

15.7.4. 그룹 관리

ovirt-aaa-jdbc-tool 도구를 사용하여 사용자의 내부 도메인에서 그룹 계정을 관리합니다. 그룹 계정 관리는 사용자 계정 관리와 그 방법이 비슷합니다. 그룹 옵션의 전체 목록을 보려면 **ovirt-aaa-jdbc-tool group --help** 명령을 실행합니다. 다음 부분에는 일반적인 예가 있습니다.

절차 15.17. 그룹 생성

다음 절차에서는 그룹 계정 생성, 그룹에 사용자 추가, 그리고 그룹 상세 정보를 확인하는 방법에 대해 설명합니다.

1. Red Hat Virtualization Manager가 설치된 시스템에 로그인합니다.
2. 새 그룹을 생성합니다:

```
# ovirt-aaa-jdbc-tool group add group1
```

3. 그룹에 사용자를 추가합니다. 이미 생성된 사용자만 추가할 수 있습니다.

```
# ovirt-aaa-jdbc-tool group-manage useradd group1 --user=test1
```



참고

전체 **group-manage** 옵션 목록을 보려면 **ovirt-aaa-jdbc-tool group-manage --help** 명령을 실행합니다.

4. 그룹 계정 상세 정보를 표시합니다:

```
# ovirt-aaa-jdbc-tool group show group1
```

5. 새로 만든 그룹을 관리 포털에 추가하고 적절한 역할 및 권한을 할당합니다. 그룹의 사용자는 해당 그룹의 역할 및 권한을 상속(**inherit**)합니다. 보다 자세한 내용은 [15.6.1절. “사용자 포털에 사용자 추가 및 권한 부여”](#)에서 참조하십시오.

절차 15.18. 중첩된 그룹 생성

다음 절차에서는 그룹 내에서 그룹을 생성하는 방법에 대해 설명합니다.

1. Red Hat Virtualization Manager가 설치된 시스템에 로그인합니다.
2. 첫 번째 그룹을 생성합니다:

```
# ovirt-aaa-jdbc-tool group add group1
```

3. 두 번째 그룹을 생성합니다:

```
# ovirt-aaa-jdbc-tool group add group1-1
```

4. 첫 번째 그룹에 두 번째 그룹을 추가합니다:

```
# ovirt-aaa-jdbc-tool group-manage groupadd group1 --group=group1-1
```

5. 첫 번째 그룹을 관리 포털에 추가하고 적절한 역할 및 권한을 할당합니다. 보다 자세한 내용은 [15.6.1절. “사용자 포털에 사용자 추가 및 권한 부여”](#)에서 참조하십시오.

15.7.5. 사용자 및 그룹 쿼리

query 모듈을 사용하여 사용자 및 그룹 정보를 쿼리합니다. 전체 옵션 목록을 보려면 **ovirt-aaa-jdbc-tool query --help** 명령을 실행합니다.

절차 15.19. 모든 사용자 또는 그룹 계정 상세 정보 표시

다음 절차에서는 모든 계정 정보를 표시하는 방법에 대해 설명합니다.

1. Red Hat Virtualization Manager가 설치된 시스템에 로그인합니다.
2.
 - 모든 사용자 계정 상세 정보를 나열합니다:

```
# ovirt-aaa-jdbc-tool query --what=user
```

- 모든 그룹 계정 상세 정보를 나열합니다:

```
# ovirt-aaa-jdbc-tool query --what=group
```

절차 15.20. 필터링된 계정 상세 정보 표시

다음 절차에서는 계정 정보 나열 시 필터를 적용하는 방법에 대해 설명합니다.

1. Red Hat Virtualization Manager가 설치된 시스템에 로그인합니다.
2.
 - 글자 *j*로 시작하는 이름의 사용자 계정 상세 정보를 표시합니다.

```
# ovirt-aaa-jdbc-tool query --what=user --pattern="name=j*"
```

- 부서의 속성을 *marketing*으로 설정한 그룹을 표시합니다:

```
# ovirt-aaa-jdbc-tool query --what=group --pattern="department=marketing"
```

15.7.6. 계정 설정 관리

계정 기본 설정을 변경하려면 **ovirt-aaa-jdbc-tool settings** 모듈을 사용합니다.

절차 15.21. 계정 설정 업데이트

다음 절차에서는 계정 기본 설정을 업데이트하는 방법에 대해 설명합니다.

1. Red Hat Virtualization Manager가 설치된 시스템에 로그인합니다.

2. 다음 명령을 실행해서 사용 가능한 모든 설정을 표시합니다:

```
# ovirt-aaa-jdbc-tool setting show
```

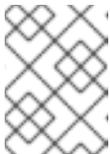
3. 설정을 변경합니다:

- 다음 예시에서는 모든 사용자 계정의 기본 로그인 세션 시간을 60분으로 업데이트합니다. 기본값은 10080분입니다.

```
# ovirt-aaa-jdbc-tool setting set --name=MAX_LOGIN_MINUTES --value=60
```

- 다음 예시에서는 사용자 계정이 잠기기 전까지 최대 로그인 시도 횟수를 업데이트합니다. 기본값은 5입니다.

```
# ovirt-aaa-jdbc-tool setting set --name=MAX_FAILURES_SINCE_SUCCESS --value=3
```



참고

사용자 계정을 잠금 해제하려면 **ovirt-aaa-jdbc-tool user unlock test1** 명령을 실행합니다.

15.8. 추가 로컬 도메인 설정

기본 **internal** 도메인 이외의 추가적인 로컬 도메인 생성이 지원됩니다. **ovirt-engine-extension-aaa-jdbc** 확장을 사용하여 외부 디렉토리 서버를 연결하지 않고 여러 개의 도메인을 생성할 수 있지만, 기업 환경에서 이렇게 사용하는 경우는 흔하지 않습니다.

추가적으로 생성된 로컬 도메인은 일반적인 Red Hat Virtualization 업그레이드 시 자동으로 업그레이드되지 않으며 앞으로 새로운 릴리즈가 있을 때마다 수동으로 업그레이드해야 합니다. 추가 로컬 도메인을 생성하고 업그레이드하는 방법은 **/usr/share/doc/ovirt-engine-extension-aaa-jdbc-version/README.admin**에 있는 README 파일에서 참조하십시오.

16장. 쿼터 및 서비스 수준 계약 정책

16.1. 쿼터 소개

쿼터는 Red Hat Virtualization에서 제공되는 리소스 제한 도구입니다. 쿼터는 사용자 권한에 따라 설정되는 계층 제한 상부에 있는 제한 설정 층으로 생각할 수 있습니다.

쿼터는 데이터 센터 개체입니다.

쿼터를 통해 Red Hat Virtualization 환경 관리자는 메모리, CPU, 스토리지에 대한 사용자 액세스를 제한할 수 있습니다. 쿼터는 관리자가 사용자를 지정할 수 있는 메모리 리소스 및 스토리지 리소스를 정의합니다. 이로 인해 사용자는 자신에게 할당된 리소스만 사용할 수 있게 됩니다. 쿼터 리소스가 모두 사용되면 Red Hat Virtualization은 더 이상 사용자 작업을 허용하지 않습니다.

다음과 같은 두 가지 유형의 쿼터가 있습니다:

표 16.1. 두 가지 유형의 쿼터

쿼터 유형	정의
런타임 쿼터	이 쿼터는 CPU와 메모리와 같은 런타임 리소스 소비를 제한합니다.
스토리지 쿼터	이 쿼터는 사용 가능한 스토리지 용량을 제한합니다.

쿼터는 SELinux와 같이 3 개의 모드가 있습니다:

표 16.2. 쿼터 모드

쿼터 모드	기능
강제 적용	이 모드는 감사 모드에 설정한 쿼터의 영향을 받으며 쿼터의 영향을 받는 그룹 또는 사용자의 리소스를 제한합니다.
감사	이 모드에서 쿼터 설정을 변경할 수 있습니다. 런타임 쿼터 양 및 쿼터의 영향을 받는 사용자가 사용 가능한 스토리지 쿼터 양을 증가 또는 감소하려면 이 모드를 선택합니다.
사용 해제	이 모드는 쿼터에 의해 정의된 런타임 및 스토리지 제한을 해제합니다.

사용자가 가상 머신을 실행하려 할 경우 가상 머신 사양은 쿼터에 설정된 사용 가능 스토리지 및 사용 가능 런타임과 비교됩니다.

가상 머신을 시작하면 쿼터에서 제공하는 실행중인 모든 가상 머신의 리소스가 쿼터에 지정된 허용 한도를 초과하여 Manager는 가상 머신을 실행 거부하게 됩니다.

사용자가 새 디스크를 생성할 경우 필요한 디스크 크기는 해당 쿼터에 포함된 기타 다른 디스크의 집계된 디스크 사용량에 추가됩니다. 새로운 디스크가 쿼터에서 허용하는 양 보다 많은 총 디스크 용량을 사용할 경우 디스크 생성에 실패합니다.

쿼터는 동일한 하드웨어의 리소스 공유를 허용합니다. 이는 하드 및 소프트웨어 임계값을 지원합니다. 관리자는 쿼터를 사용하여 리소스에서 임계값을 설정할 수 있습니다. 이러한 임계값은 사용자 측에서 리소스 100% 사용으로 나타납니다. 사용자가 예기치 않게 이러한 임계값을 초과할 경우 오류가 발생하지 않도록 하기 위해 인터페이스는 임계값을 약간 초과할 수 있는 "유예" 용량을 지원합니다. 임계값을 초과하면 사용자에게 경고 메시지가 전송됩니다.

중요

쿼터는 가상 머신 실행에 제한을 둡니다. 이러한 제한을 무시할 경우 가상 머신 및 가상 디스크를 사용할 수 없는 상황이 발생할 수 있습니다.

쿼터가 강제 적용 모드에서 실행되고 있을 경우 쿼터가 할당되지 않은 가상 머신 및 디스크는 사용할 수 없습니다.

가상 머신의 전원을 켜려면 가상 머신에 쿼터를 할당해야 합니다.

가상 머신의 스냅샷을 생성하려면 가상 머신에 연결된 디스크에 쿼터를 할당해야 합니다.

가상 머신에서 템플릿 생성 시 템플릿을 소비하고자 하는 쿼터를 선택하라는 메시지가 표시됩니다. 이를 통해 템플릿이 생성된 디스크 및 가상 머신 이외에 다른 쿼터를 소비하기 위한 템플릿 (및 템플릿에서 차후 생성되는 모든 가상 머신)을 설정할 수 있습니다.

16.2. 공유된 쿼터 및 개별적으로 정의된 쿼터

SuperUser 권한이 있는 사용자는 개별 사용자에게 쿼터 또는 그룹 쿼터를 생성할 수 있습니다.

그룹 쿼터는 Active Directory 사용자에게 대해 설정할 수 있습니다. 10 명의 사용자로 된 그룹에 1 TB 스토리지 쿼터가 할당되고 10 명의 사용자 중 한 명이 전체 테라바이트를 사용한 경우 전치 그룹은 쿼터를 초과하고 10 명 중 어느 누구도 그룹과 연관된 스토리지를 사용할 수 없게 됩니다.

개별 사용자에게 대해 정의된 쿼터는 개별적으로만 설정할 수 있습니다. 개별 사용자가 스토리지 쿼터 또는 런타임 쿼터 모두를 사용하면 사용자는 쿼터를 초과하여 사용자 쿼터에 연결된 스토리지를 사용할 수 없게 됩니다.

16.3. 쿼터 계산

소비자 또는 리소스에 쿼터 할당 시 스토리지, vCPU, 메모리에 관련된 리소스 또는 소비자에 의한 작업으로 인해 쿼터 소비 또는 쿼터 반환이 발생합니다.

쿼터는 사용자 리소스에 대한 액세스를 제한하는 상한 값으로 작동하기 때문에 쿼터 계산은 사용자의 현재 실제 사용량과는 다를 수 있습니다. 쿼터는 현재 사용량이 아니라 잠재적으로 증가할 수 있는 최대 사용량으로 산출됩니다.

예 16.1. 쿼터 계산 예

사용자는 1 vCPU 및 1024 MB 메모리로 가상 머신을 실행하고 있습니다. 작업에서는 사용자에게 할당된 1 vCPU 및 1024 MB의 쿼터가 소비됩니다. 가상 머신이 중지하면 1 vCPU 및 1024 MB RAM이 사용자에게 할당된 쿼터로 다시 반환됩니다. 런타임 쿼터 소비량은 소비자의 실제 런타임 동안에만 계산됩니다.

사용자는 10 GB의 썸 프로비저닝 가상 디스크를 생성합니다. 실제 디스크 사용량은 실제 디스크가 사용하고 있는 3 GB 만 표시될 수 있습니다. 하지만 쿼터 소비량은 잠재적으로 증가할 수 있는 최대 용량인 10 GB가 됩니다.

16.4. 데이터 센터에서 쿼터 모드 활성화 및 변경

다음 부분에서는 데이터 센터에서 쿼터 모드를 활성화 또는 변경하는 방법에 대해 설명합니다. 쿼터를 정의하기 전 쿼터 모드를 선택해야 합니다. 관리 포털로 로그인하여 이러한 단계를 수행하기 위한 절차를 따릅니다.

감사 모드를 사용하여 쿼터가 예상대로 작동하는지 테스트합니다. 쿼터를 생성하거나 변경하기 위해 감사 모드로 실행할 필요는 없습니다.

절차 16.1. 데이터 센터에서 쿼터 활성화 및 변경

1. 탐색 창에서 **데이터 센터** 탭을 클릭합니다.
2. 탐색 창에 출력된 데이터 센터 목록에서 편집하려는 쿼터 정책이 있는 데이터 센터를 선택합니다.
3. 탐색 창의 왼쪽 상단에 있는 **편집**을 클릭합니다.

데이터 센터 편집 창이 열립니다.
4. 쿼터 모드 드롭 다운 메뉴에서 쿼터 모드를 **강제 적용**으로 변경합니다.
5. **OK**를 클릭합니다.

데이터 센터에서 쿼터 모드가 활성화되었습니다. 테스트 도중 쿼터 모드를 감사로 설정한 경우 이를 **강제 적용**으로 변경하여 쿼터 설정을 적용해야 합니다.

16.5. 새 쿼터 정책 생성

감사 또는 강제 적용 모드에서 쿼터 모드를 활성화했습니다. 쿼터 정책을 정의하여 데이터 센터에 있는 리소스 사용량을 관리합니다.

절차 16.2. 새 쿼터 정책 생성

1. 트리 모드에서 데이터 센터를 선택합니다. 탐색 창에 **쿼터** 탭이 표시됩니다.
2. 탐색 창에서 **쿼터** 탭을 클릭합니다.
3. 탐색 창에서 **추가**를 클릭합니다. **새 쿼터** 창이 열립니다.
4. **이름 필드**에 이름을 입력합니다.

설명 필드에 설명을 입력합니다.
5. **새 쿼터** 창의 **메모리 & CPU** 부분에 초록색 슬라이더를 사용하여 **클러스터 임계값**을 설정합니다.
6. **새 쿼터** 창의 **메모리 & CPU** 부분에 파란색 슬라이더를 사용하여 **클러스터 유예**를 설정합니다.
7. **모든 클러스터** 라디오 버튼 또는 **특정 클러스터** 라디오 버튼 중 하나를 선택합니다. **특정 클러스터** 선택 시 쿼터 정책을 추가하려는 클러스터의 체크 상자를 선택합니다.
8. **편집**을 클릭하여 **쿼터 편집** 창을 엽니다.
9. **메모리 필드**에서 **제한없음** 라디오 버튼 (클러스터에서 메모리 리소스 사용에 제한 없음) 또는 **제한있음** 라디오 버튼 중 하나를 선택하여 쿼터가 설정한 메모리 양을 설정합니다. **제한있음** 라디오 버튼을 선택한 경우 **MB** 필드에 메가바이트 (MB) 단위로 메모리 쿼터를 입력합니다.

10. CPU 필드에서 **제한없음** 라디오 버튼 또는 **제한있음** 라디오 버튼 중 하나를 선택하여 쿼터가 설정한 CPU 양을 설정합니다. **제한있음** 라디오 버튼을 선택한 경우 **vCpus** 필드에 vCPU 수를 입력합니다.
11. 쿼터 편집 창에서 **OK**를 클릭합니다.
12. 새 쿼터 창의 스토리지 부분에서 초록색 슬라이더를 사용하여 **스토리지 임계값**을 설정합니다.
13. 새 쿼터 창의 스토리지 부분에서 파란색 슬라이더를 사용하여 **스토리지 유예**를 설정합니다.
14. 모든 스토리지 도메인 라디오 버튼 또는 **특정 스토리지 도메인** 라디오 버튼 중 하나를 선택합니다. **특정 스토리지 도메인** 선택 시 쿼터 정책을 추가하려는 스토리지 도메인의 체크 상자를 선택합니다.
15. 편집을 클릭하여 쿼터 편집 창을 엽니다.
16. 스토리지 쿼터 필드에서 **제한없음** 라디오 버튼 (스토리지 사용에 제한 없음) 또는 **제한있음** 라디오 버튼 중 하나를 선택하여 사용자를 제한할 스토리지 양을 설정할 수 있습니다. **제한있음** 라디오 버튼을 선택한 경우 **GB** 필드에 기가바이트 (GB) 단위로 스토리지 쿼터 크기를 입력합니다.
17. 새 쿼터 창에서 **OK**를 클릭합니다. 새 쿼터 창으로 되돌아갑니다.
18. 새 쿼터 창에서 **OK**를 클릭합니다.

결과

새 쿼터 정책이 생성되었습니다.

16.6. 쿼터 임계값 설정

표 16.3. 쿼터 임계값 및 유예

설정	정의
클러스터 임계값	데이터 센터 마다 사용 가능한 클러스터 리소스 용량입니다.
클러스터 유예	데이터 센터의 클러스터 임계값을 모두 사용한 후 데이터 센터에서 사용 가능한 클러스터 용량입니다.
스토리지 임계값	데이터 센터 마다 사용 가능한 클러스터 리소스 용량입니다.
스토리지 유예	데이터 센터의 스토리지 임계값을 모두 사용한 후 데이터 센터에서 사용 가능한 스토리지 용량입니다.

쿼터가 100 GB, 20% 유예로 설정되어 있을 경우 소비자가 스토리지의 120 GB를 사용한 후 스토리지를 사용할 수 없게 됩니다. 동일한 쿼터에 임계값이 70%로 설정되어 있을 경우 소비자가 스토리지 소비량의 70 GB를 초과하면 경고를 받습니다. (스토리지 소비량의 120 GB가 될 때 까지 스토리지를 사용할 수 있습니다.) "임계값" 및 "유예" 모두 해당 쿼터에 설정됩니다. "임계값"은 "소프트 한도"로 이를 초과 시 경고가 발생합니다. "유예"는 "하드 한도"로 이를 초과시 더이상 스토리지 리소스를 사용할 수 없습니다.

16.7. 개체에 쿼터 지정

요약

다음 절차에서는 가상 머신을 쿼터에 연결하는 방법에 대해 설명합니다.

절차 16.3. 가상 머신에 쿼터 할당

1. 탐색 창에서 쿼터를 추가하고자 하는 가상 머신을 선택합니다.
2. 편집을 클릭하여 가상 머신 편집 창을 엽니다.
3. 가상 머신이 사용할 쿼터를 선택합니다. 쿼터 드롭 다운 메뉴를 사용합니다.
4. **OK**를 클릭합니다.

결과

선택한 가상 머신에 대한 쿼터가 지정됩니다.

요약

다음 절차에서는 가상 디스크를 쿼터에 연결하는 방법에 대해 설명합니다.

절차 16.4. 가상 디스크에 쿼터 할당

1. 탐색 창에서 쿼터를 추가하고자 하는 디스크의 가상 머신을 선택합니다.
2. 상세 정보 창에서 쿼터에 연결하고자 하는 디스크를 선택합니다.
3. 편집을 클릭하여 가상 디스크 수정 창을 엽니다.
4. 가상 디스크가 사용할 쿼터를 선택합니다.
5. **OK**를 클릭합니다.

결과

선택한 가상 디스크에 쿼터가 지정됩니다.

**중요**

가상 머신이 작동하려면 가상 머신에 연결된 모든 개체에 대한 쿼터를 선택해야 합니다. 가상 머신에 연결된 개체의 쿼터를 선택하지 않은 경우 가상 머신은 제대로 작동하지 않습니다. 이러한 경우 **Manager**가 표시하는 오류는 일반적인 것이기 때문에 가상 머신에 연결된 모든 개체에 쿼터를 연결하지 않은 것으로 인해 오류가 발생했다고 보기는 어렵습니다. 쿼터가 할당되지 않은 가상 머신의 스냅샷을 생성할 수 없습니다. 또한 쿼터가 할당되지 않은 가상 디스크가 있는 가상 머신의 템플릿을 생성할 수 없습니다.

16.8. 쿼터를 사용하여 사용자에게 따라 리소스를 제한**요약**

다음 절차에서는 사용자가 액세스할 수 있는 리소스를 제한하기 위해 쿼터를 사용하는 방법에 대해 설명합니다.

절차 16.5. 사용자에게 쿼터 할당

1. 트리에서 사용자와 연결하려는 쿼터가 있는 데이터 센터를 클릭합니다.

2. 탐색 창에서 **쿼터** 탭을 클릭합니다.
3. 탐색 창에 있는 목록에서 대상 쿼터를 선택합니다.
4. 상세 정보 창에서 **소비자** 탭을 클릭합니다.
5. 상세 정보 창 상단에 **추가**를 클릭합니다.
6. 검색 필드에 쿼터와 연결하려는 사용자 이름을 입력합니다.
7. 검색을 클릭합니다.
8. 대상 사용자 이름이 들어 있는 행의 왼쪽에 있는 확인란을 선택합니다.
9. 쿼터에 **사용자/그룹 할당** 창의 오른쪽 하단에 있는 **OK**를 클릭합니다.

결과

잠시 후 상세 정보 창의 **소비자** 탭에 사용자가 표시됩니다.

16.9. 쿼터 편집

개요

다음 부분에서는 기존 쿼터를 변경하는 방법에 대해 설명합니다.

절차 16.6. 쿼터 편집

1. 트리 창에서 편집하고자 하는 쿼터가 있는 데이터 센터를 클릭합니다.
2. 탐색 창에서 **쿼터** 탭을 클릭합니다.
3. 편집하고자 하는 쿼터 이름을 클릭합니다.
4. 탐색 창에서 **편집**을 클릭합니다.
5. **쿼터 편집** 창을 엽니다. 필요한 경우 **이름** 필드에 적절한 이름을 입력합니다.
6. 필요한 경우 **설명** 필드에 적절한 설명을 입력합니다.
7. 모든 **클러스터** 라디오 버튼 또는 **특정 클러스터** 라디오 버튼 중 하나를 선택합니다. **클러스터 임계값** 및 **클러스터 유예 기간** 슬라이더를 **메모리 & CPU** 슬라이더 상의 원하는 위치로 이동합니다.
8. 모든 **스토리지 도메인** 라디오 버튼 또는 **특정 스토리지 도메인** 라디오 버튼 중 하나를 선택합니다. **클러스터 임계값** 및 **클러스터 유예 기간** 슬라이더를 **메모리 & CPU** 슬라이더 상의 원하는 위치로 이동합니다.
9. **쿼터 편집** 창에서 **OK**를 클릭하여 새로운 쿼터 설정을 확인합니다.

결과

기존 쿼터가 변경됩니다.

16.10. 쿼터 삭제

개요

다음 부분에서는 쿼터 삭제 방법에 대해 설명합니다.

절차 16.7. 쿼터 삭제

1. 트리 창에서 편집하고자 하는 쿼터가 있는 데이터 센터를 클릭합니다.
2. 탐색 창에서 **쿼터** 탭을 클릭합니다.
3. 삭제하고자 하는 쿼터 이름을 클릭합니다.
4. 탭 열 아래에 있는 탐색 창 상단의 **제거**를 클릭합니다.
5. **쿼터 삭제** 창에서 **OK**를 클릭하여 쿼터 삭제를 확인합니다.

결과

쿼터가 삭제됩니다.

16.11. 서비스 수준 계약 정책 적용

요약

다음 부분에서는 서비스 수준 계약 CPU 기능을 설정하는 방법에 대해 설명합니다.

절차 16.8. 서비스 수준 계약 CPU 정책 설정

1. 탐색 창에서 **새 가상 머신**을 선택합니다.
2. **고급 옵션 표시**를 선택합니다.
3. **리소스 할당** 탭을 선택합니다.

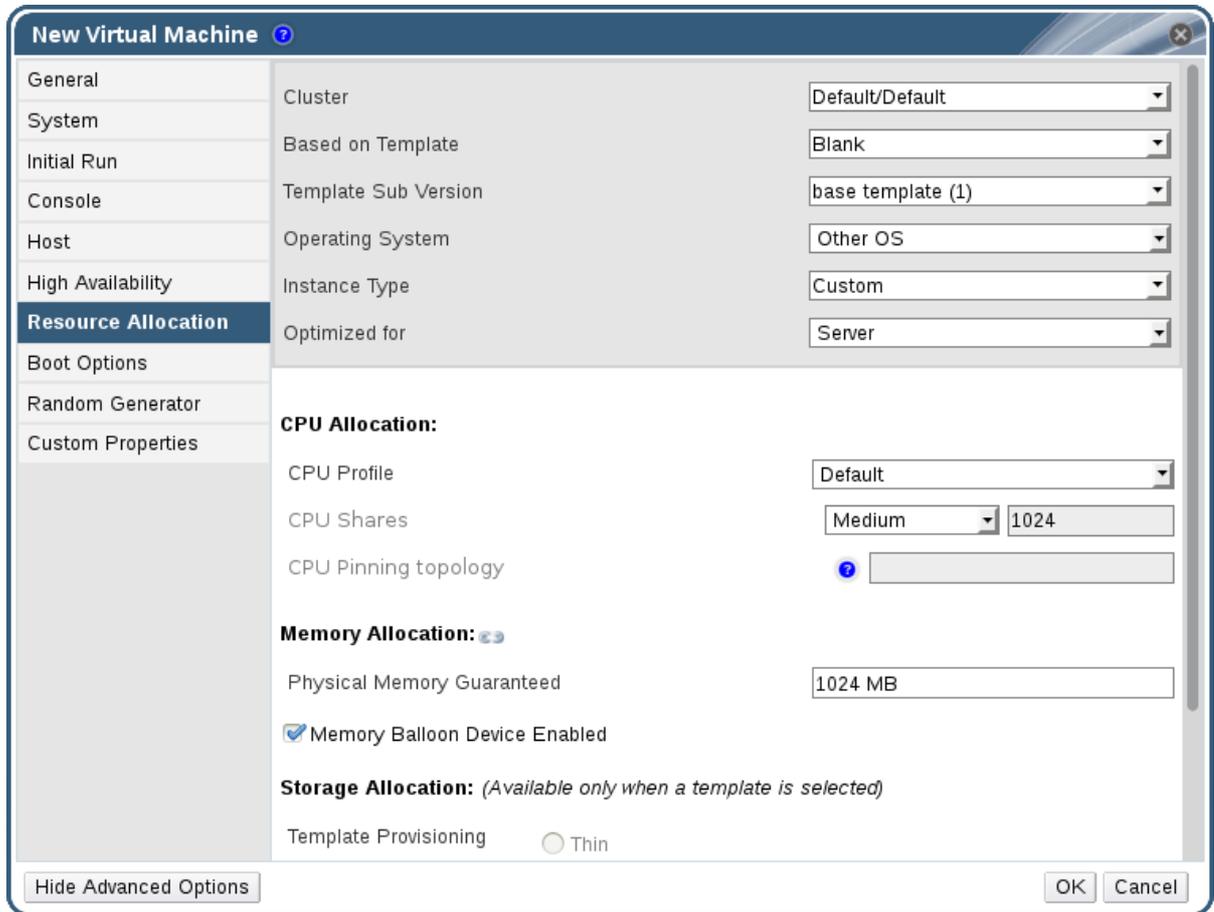


그림 16.1. 서비스 수준 계약 정책 적용 - CPU 할당 메뉴

4. CPU 공유를 지정합니다. 설정 가능한 옵션에는 낮음, 중간, 높음, 사용자 지정, 비활성화됨이 있습니다. 높음으로 설정된 가상 머신은 중간으로 설정된 가상 머신 보다 두 배 많은 공유를 수신하게 되며 중간으로 설정된 가상 머신은 낮음으로 설정된 가상 머신 보다 두 배 많은 공유를 수신하게 됩니다. 비활성화됨으로 설정되어 있을 경우 VDSM을 통해 공유 분배를 설정하기 위해 이전 알고리즘을 사용하게 됩니다; 일반적으로 이러한 조건에서 분배되는 공유 수는 1020입니다.

결과

서비스 수준 계약 CPU 정책이 설정되었습니다. 사용자의 CPU 소비는 설정된 정책에 따라 관리됩니다.

17장. 이벤트 알림

17.1. 관리 포털에서 이벤트 알림 설정

요약

Red Hat Virtualization Manager가 관리하는 환경에서 특정 이벤트가 발생했을 경우 Red Hat Virtualization Manager는 이메일을 통해 지정된 사용자에게 통지할 수 있습니다. 이러한 기능을 사용하려면 메일 전송 에이전트를 설정하여 메시지를 전달할 수 있습니다. 이메일 알림만 관리 포털을 통해 설정할 수 있습니다. Manager 시스템에서 SNMP 트랩을 설정해야 합니다.

절차 17.1. 이벤트 알림 설정

1. 적절한 매개 변수로 메일 전송 에이전트를 설정했는지 확인합니다.
2. 사용자 리소스 탭, 트리 모드, 검색 기능을 사용하여 이벤트 알림을 받을 사용자를 검색 및 선택할 수 있습니다.
3. 상세 정보 창에서 **이벤트 공지** 탭을 클릭하여 사용자가 알림 받을 이벤트 목록을 나열합니다. 사용자 이벤트 알림을 설정하지 않은 경우 이 목록은 비어 있게 됩니다.
4. **이벤트 관리**를 클릭하여 **이벤트 알림 추가** 창을 엽니다.

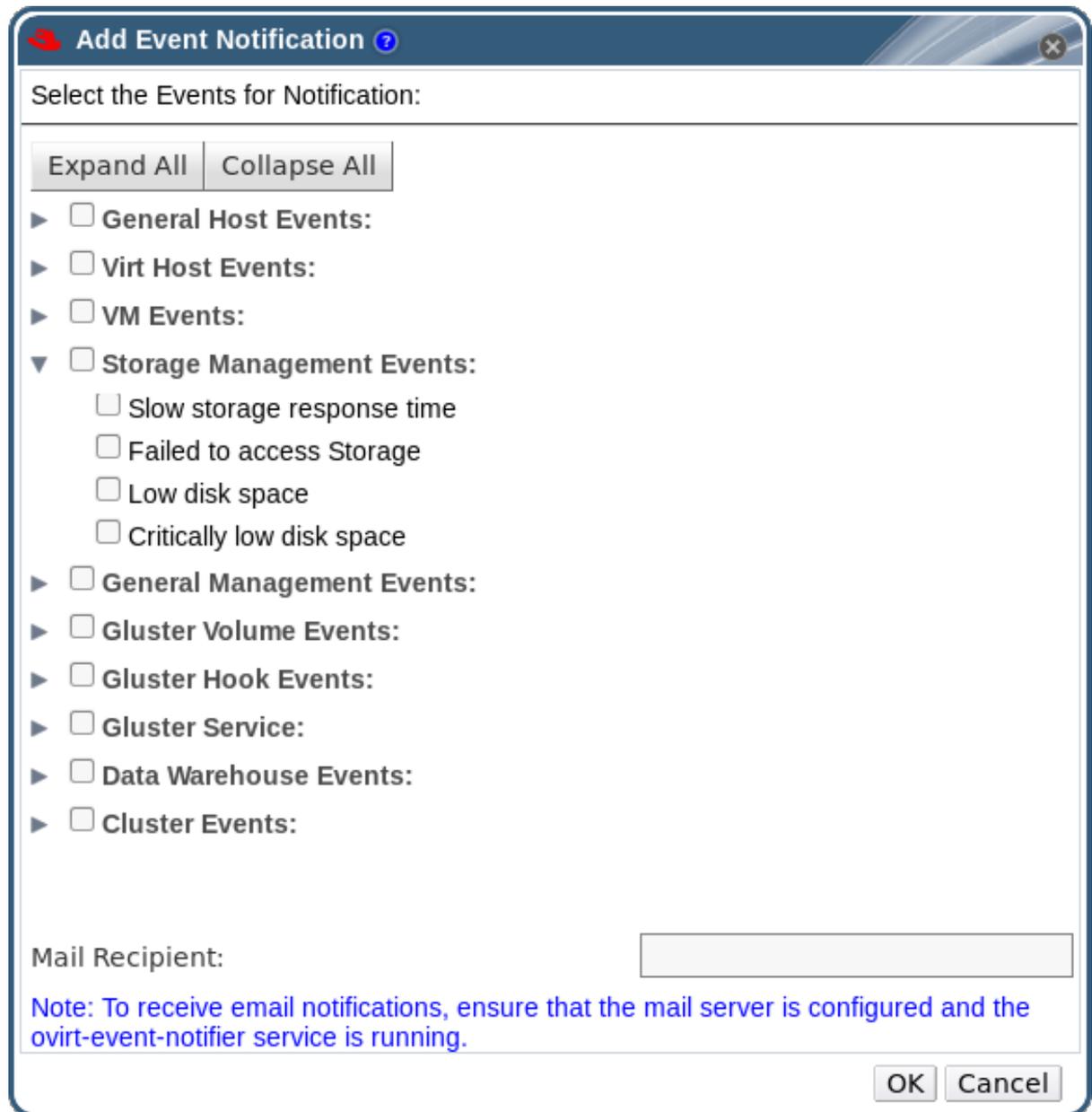


그림 17.1. 이벤트 알림 추가 창

5. 모두 확장 버튼이나 특정 대상에 대한 확장 버튼을 사용하여 이벤트를 확인합니다.
6. 해당 확인란을 선택합니다.
7. 메일 수신인 필드에 이메일 주소를 입력합니다.
8. **OK**를 클릭하여 변경 사항을 저장하고 창을 닫습니다.
9. Red Hat Virtualization Manager에 있는 **ovirt-engine-notifier** 서비스를 추가 및 시작하면 변경 사항이 활성화됩니다:

```
# systemctl daemon-reload
# systemctl enable ovirt-engine-notifier.service
# systemctl restart ovirt-engine-notifier.service
```

결과

Red Hat Virtualization 환경에서의 이벤트를 기반으로 지정된 사용자에게 이메일이 수신됩니다. 선택한 이벤트는 사용자의 이벤트 공지 탭에 표시됩니다.

17.2. 관리 포털에서 이벤트 공지 취소

요약

사용자는 일부 불필요한 이메일 공지 설정을 취소할 수 있습니다.

절차 17.2. 이벤트 공지 취소

1. 사용자 탭에서 사용자 또는 사용자 그룹을 선택합니다.
2. 상세 정보 창에서 **이벤트 공지** 탭을 선택하여 사용자가 메일 공지를 받는 이벤트 목록을 나열합니다.
3. **이벤트 관리**를 클릭하여 **이벤트 알림 추가** 창을 엽니다.
4. 모두 **확장** 버튼이나 특정 대상에 대한 확장 버튼을 사용하여 이벤트를 확인합니다.
5. 이벤트 공지를 삭제하려면 해당 확인란을 선택 취소합니다.
6. **OK**를 클릭하여 변경 사항을 저장하고 창을 닫습니다.

결과

사용자의 불필요한 이벤트 공지가 취소되었습니다.

17.3. OVIRT-ENGINE-NOTIFIER.CONF에서 이벤트 공지 매개 변수

이벤트 공지 설정 파일은 `/usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf`에 있습니다.

표 17.1. ovirt-engine-notifier.conf 변수

변수 이름	기본값	설명
SENSITIVE_KEYS	없음	콤마로 구분된 기록되지 않을 키 목록
JBASS_HOME	/usr/share/jbossas	Manager가 사용하는 JBoss 애플리케이션 서버 위치입니다.
ENGINE_ETC	/etc/ovirt-engine	Manager가 사용하는 etc 디렉토리 위치입니다.
ENGINE_LOG	/var/log/ovirt-engine	Manager가 사용하는 logs 디렉토리 위치입니다.
ENGINE_USR	/usr/share/ovirt-engine	Manager가 사용하는 usr 디렉토리 위치입니다.
ENGINE_JAVA_MODULEPATH	\${ENGINE_USR}/modules	JBoss 모듈이 추가되는 파일 경로입니다.

변수 이름	기본값	설명
NOTIFIER_DEBUG_ADDRESS	없음	통지 기능을 사용하는 Java 가상 머신의 원격 디버깅을 수행하는데 사용할 수 있는 시스템의 주소입니다.
NOTIFIER_STOP_TIME	30	서비스가 종료되는 시간 (초 단위)입니다.
NOTIFIER_STOP_INTERVAL	1	시간 제한 카운터가 증가하는 시간 (초 단위)입니다.
INTERVAL_IN_SECONDS	120	가입자에게 메시지를 발송하는 인스턴스의 간격 (초 단위)입니다.
IDLE_INTERVAL	30	우선순위가 낮은 작업이 실행되는 간격 (초 단위)입니다.
DAYS_TO_KEEP_HISTORY	0	이 매개 변수는 발송된 이벤트가 기록 표에 보관되는 기간을 설정합니다. 이러한 변수가 설정되어 있지 않은 경우 이벤트는 기록 표에 무기한으로 남아있게 됩니다.
FAILED_QUERIES_NOTIFICATION_THRESHOLD	30	통지 이메일이 전송된 후 오류가 발생한 쿼리 수입니다. 첫 번째 전송 오류 후 통지 이메일이 전송되며 이러한 변수에 지정된 오류 횟수에 도달할 때 마다 한 번의 통지 이메일이 전송됩니다. 0 또는 1 로 값을 지정할 경우 오류 발생 마다 이메일이 전송됩니다.
FAILED_QUERIES_NOTIFICATION_RECIPIENTS	없음	통지 이메일이 전송될 수신자의 이메일 주소입니다. 콤마로 이메일 주소를 구분합니다. 이 항목은 FILTER 변수로 인해 더 이상 사용되지 않습니다.
DAYS_TO_SEND_ON_STARTUP	0	통지 시작 시 처리 및 전송된 이전 이벤트의 기간입니다.
FILTER	exclude:*	이메일 통지 트리거 및 수신자를 지정하는데 사용되는 알고리즘입니다. 이러한 변수 값은 include 또는 exclude , 이벤트 및 수신자로 구성됩니다. 예: include:VDC_START(smtp:mail@example.com) \${FILTER}
MAIL_SERVER	없음	SMTP 메일 서버 주소입니다. 필수 항목입니다.

변수 이름	기본값	설명
MAIL_PORT	25	통신에 사용되는 포트입니다. 일반 SMTP의 경우 25 , SSL을 사용하는 SMTP의 경우 465 , TLS를 사용하는 SMTP의 경우 587 로 값을 설정할 수 있습니다.
MAIL_USER	없음	사용자 인증에 SSL이 활성화되어 있을 경우 반드시 이러한 변수를 설정해야 합니다. 이 변수는 MAIL_FROM 변수가 설정되어 있지 않을 때 "from" 사용자 주소를 지정하는데 사용됩니다. 일부 메일 서버는 이러한 기능을 지원하지 않습니다 주소는 RFC822 형식입니다.
SENSITIVE_KEYS	\${SENSITIVE_KEYS},MAIL_PASSWORD	메일 서버에 인증이 필요하거나 SSL 또는 TLS가 활성화되어 있을 경우 사용자 인증이 필요합니다.
MAIL_PASSWORD	없음	메일 서버에 인증이 필요하거나 SSL 또는 TLS가 활성화되어 있을 경우 사용자 인증이 필요합니다.
MAIL_SMTP_ENCRYPTION	없음	통신에 사용할 암호화 유형입니다. 사용 가능한 값은 none, ssl, tls 입니다.
HTML_MESSAGE_FORMAT	false	이 변수가 true 로 설정되어 있을 경우 메일 서버는 HTML 형식으로 메시지를 전송합니다.
MAIL_FROM	없음	메일 서버가 지원하는 경우 이 변수는 보낸 사람의 주소를 RFC822 형식으로 지정합니다.
MAIL_REPLY_TO	없음	메일 서버가 지원하는 경우 이 변수는 수신자 주소를 RFC822 형식으로 지정합니다.
MAIL_SEND_INTERVAL	1	각 IDLE_INTERVAL에 대해 전송되는 SMTP 메시지 수
MAIL_RETRIES	4	이메일 전송 시도 횟수입니다.
SNMP_MANAGER	없음	SNMP 관리자로 작동하게 될 컴퓨터의 정규화된 도메인 이름 또는 IP 주소입니다. 항목은 공백으로 구분해야 하며 포트 번호를 넣을 수 있습니다. 예: manager1.example.com manager2.example.com:164
SNMP_COMMUNITY	public	기본 SNMP 커뮤니티입니다.

변수 이름	기본값	설명
SNMP_OID	1.3.6.1.4.1.2312.13.1.1	경고 용 기본 트랩 개체 식별자입니다. OID가 지정되면 SNMP 관리자에게 이벤트 정보와 함께 모든 트랩 유형이 전송됩니다. 기본 트랩을 변경할 경우 생성된 트랩은 Manager의 관리 정보 기반에 준수하지 않게 됨에 유의합니다.
ENGINE_INTERVAL_IN_SECONDS	300	Manager가 설치된 시스템의 모니터링 간격 (초 단위)입니다. 간격은 모니터링이 완료된 시점에서 측정됩니다.
ENGINE_MONITOR_RETRIES	3	오류 발생 후 통지 기능이 지정된 간격으로 Manager가 설치된 시스템 상태를 모니터링하는 횟수입니다.
ENGINE_TIMEOUT_IN_SECONDS	30	오류 발생 후 통지 기능이 지정된 간격으로 Manager가 설치된 시스템 상태를 모니터링할 때 까지의 대기 시간 (초 단위)입니다.
IS_HTTPS_PROTOCOL	false	JBoss가 보안 모드에서 실행되고 있을 경우 이 항목은 true 로 설정해야 합니다.
SSL_PROTOCOL	TLS	SSL이 활성화되어 있을 경우 JBoss 설정 커넥터가 사용하는 프로토콜입니다.
SSL_IGNORE_CERTIFICATE_ERRORS	false	JBoss가 보안 모드에서 실행되고 있고 SSL 오류를 무시하려는 경우 이 값은 true 로 설정해야 합니다.
SSL_IGNORE_HOST_VERIFICATION	false	JBoss가 보안 모드에서 실행되고 있고 호스트 이름 확인이 생략되어 있을 경우 이 값은 true 로 설정해야 합니다.
REPEAT_NON_RESPONSIVE_NOTIFICATION	false	이러한 변수는 Manager가 설치된 시스템이 응답하지 않음 (non-responsive) 상태일 경우 가입자에게 오류 메시지를 반복하여 전송할 지에 대한 여부를 지정합니다.
ENGINE_PID	/var/lib/ovirt-engine/ovirt-engine.pid	Manager의 PID 경로 및 파일 이름입니다.

17.4. RED HAT VIRTUALIZATION MANAGER를 설정하여 SNMP 트랩 전송

하나 이상의 외부 SNMP 관리자에게 SNMP (Simple Network Management Protocol) 트랩을 전송하기 위해 Red Hat Virtualization Manager를 설정합니다. SNMP 트랩에는 시스템 이벤트 정보가 들어

있으며 Red Hat Virtualization 환경을 모니터링하는데 사용됩니다. SNMP 관리자에 전송된 트랩 수와 유형은 Red Hat Virtualization Manager 내에서 정의할 수 있습니다.

다음 절차에서는 트랩을 수신하기 위해 하나 이상의 외부 SNMP 관리자가 설정되어 있으며 다음과 같은 내용이 준비되어 있음을 전제로 합니다:

- SNMP 관리자로 작동하게 될 컴퓨터의 정규화된 도메인 이름 또는 IP 주소입니다. 옵션으로 관리자가 트랩 알림을 수신하는 포트를 지정합니다. 기본값으로 이는 UDP 포트 162입니다.
- SNMP 커뮤니티입니다. 여러 SNMP 관리자는 단일 커뮤니티에 속해 있을 수 있습니다. 관리 시스템 및 에이전트는 동일한 커뮤니티내에 있을 경우에만 통신할 수 있습니다. 기본 커뮤니티는 **public**입니다.
- 경고 용 트랩 객체 식별자입니다. Red Hat Virtualization Manager는 1.3.6.1.4.1.2312.13.1.1의 기본 OID를 제공합니다. OID가 지정되어 있을 때 이벤트 정보에 첨부된 모든 트랩 유형은 SNMP 관리자에게 전송됩니다. 기본 트랩을 변경하면 생성된 트랩이 관리자의 관리 정보 기반을 준수하지 않을 수 있습니다.



참고

Red Hat Virtualization Manager는 `/usr/share/doc/ovirt-engine/mibs/OVIRT-MIB.txt` 및 `/usr/share/doc/ovirt-engine/mibs/REDHAT-MIB.txt`에 관리 정보 기반을 제공합니다. 작업 절차를 수행하기 전 SNMP 관리자의 MIB를 로딩합니다.

기본 SNMP 설정 값은 이벤트 통지 데몬 설정 파일 `/usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf`에 있는 Manager에 있습니다. 다음 절차에서 설명된 값은 해당 파일에서 제공하는 기본값 또는 예시 값을 기반으로 합니다. `ovirt-engine-notifier.conf` 파일을 편집하는 것 보다 덮어쓰기한 파일을 지정하여 업그레이드와 같이 시스템 변경에 대한 설정 옵션을 영구적으로 유지하는 것이 좋습니다.

절차 17.3. Manager에서 SNMP 트랩 설정

1. Manager에서 SNMP 설정 파일을 생성합니다:

```
# vi /etc/ovirt-engine/notifier/notifier.conf.d/20-snmf.conf
```

2. 다음과 같은 형식으로 SNMP 관리자, SNMP 커뮤니티, OID를 지정합니다:

```
SNMP_MANAGERS="manager1.example.com manager2.example.com:162"
SNMP_COMMUNITY=public
SNMP_OID=1.3.6.1.4.1.2312.13.1.1
```

3. SNMP 관리자로 전송할 이벤트를 정의합니다:

예 17.1. 이벤트 예

모든 이벤트를 기본 SNMP 프로파일로 전송합니다:

```
FILTER="include:*(snmp:) ${FILTER}"
```

ERROR 또는 **ALERT** 심각도로된 모든 이벤트를 기본 SNMP 프로파일로 전송합니다:

```
FILTER="include:*ERROR(snmp:) ${FILTER}"
```

```
FILTER="include:*ALERT(snmp:) ${FILTER}"
```

`VDC_START`의 이벤트를 특정 이메일 주소로 전송합니다:

```
FILTER="include:VDC_START(snmp:mail@example.com) ${FILTER}"
```

`VDC_START`를 제외한 모든 이벤트를 기본 SNMP 프로파일에 전송합니다:

```
FILTER="exclude:VDC_START include:*(snmp:) ${FILTER}"
```

이러한 기본 필터는 `ovirt-engine-notifier.conf`에 정의됩니다. 이러한 필터를 비활성화하지 않거나 필터 덮어쓰기를 적용하지 않을 경우 아무런 통지도 전송되지 않습니다:

```
FILTER="exclude:*"
```

`VDC_START`는 사용 가능한 감시 로그 메시지의 예입니다. 감시 로그 메시지의 전체 목록은 `/usr/share/doc/ovirt-engine/AuditLogMessages.properties`에서 확인할 수 있습니다. 다른 방법으로 SNMP 관리자 내에서 결과를 필터링합니다.

4. 파일을 저장합니다.

5. `ovirt-engine-notifier` 서비스를 시작하고 부팅 시 이러한 서비스가 시작되는지 확인합니다:

```
# systemctl start ovirt-engine-notifier.service
# systemctl enable ovirt-engine-notifier.service
```

트랩이 수신되고 있는지 확인하려면 SNMP 관리자를 살펴봅니다.



참고

`SNMP_MANAGERS`, `MAIL_SERVER` 또는 두 가지 모두 `/usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf`에 지정하거나 덮어쓰기 파일에 지정하여 통지 서비스가 실행되도록 합니다.

18장. 유틸리티

18.1. OVIRT ENGINE RENAME 도구

18.1.1. oVirt Engine Rename 도구

engine-setup 명령을 실행하면 설정 프로세스에서 지정한 **Manager**의 정규화된 도메인 이름을 사용하는 인증서와 키가 생성됩니다. **Manager**의 정규화된 도메인 이름은 나중에 변경해야 할 경우 (예를 들어 **Manager**를 호스팅하는 머신을 다른 도메인으로 마이그레이션하는 경우) 정규화된 도메인 이름의 레코드가 새 이름을 반영하도록 업데이트해야 합니다. **ovirt-engine-rename** 명령으로 이러한 작업을 자동화합니다.

ovirt-engine-rename 명령은 다음 위치에 있는 **Manager**의 정규화된 도메인 이름 레코드를 업데이트합니다:

- /etc/ovirt-engine/engine.conf.d/10-setup-protocols.conf
- /etc/ovirt-engine/imageuploader.conf.d/10-engine-setup.conf
- /etc/ovirt-engine/isouploader.conf.d/10-engine-setup.conf
- /etc/ovirt-engine/logcollector.conf.d/10-engine-setup.conf
- /etc/pki/ovirt-engine/cert.conf
- /etc/pki/ovirt-engine/cert.template
- /etc/pki/ovirt-engine/certs/apache.cer
- /etc/pki/ovirt-engine/keys/apache.key.nopass
- /etc/pki/ovirt-engine/keys/apache.p12



주의

ovirt-engine-rename 명령으로 **Manager**를 실행하는 웹 서버의 새 인증서를 생성합니다. 이는 engine 인증서 또는 인증 기관에 영향을 미치지 않습니다. 이로 인해 **ovirt-engine-rename** 명령을 사용하는데 위험 요소가 있으며 특히 Red Hat Enterprise Virtualization 3.2 버전 및 그 이전 버전에서 업그레이드한 환경에서 그러합니다. 따라서 가능하면 **engine-cleanup** 및 **engine-setup**를 실행하여 **Manager**의 정규화된 도메인 이름을 변경하는 것이 좋습니다.

18.1.2. oVirt Engine Rename 명령 구문

ovirt-engine-rename 명령의 기본 구문은 다음과 같습니다:

```
# /usr/share/ovirt-engine/setup/bin/ovirt-engine- rename
```

명령은 다음과 같은 옵션을 허용합니다:

--newname=[new name]

사용자 조작없이 Manager의 새로운 FQDN (fully qualified domain name)을 지정할 수 있습니다.

--log=[file]

이름 변경 작업의 로그를 기록할 수 있는 파일의 경로 및 이름을 지정할 수 있습니다.

--config=[file]

이름 변경 작업에 로딩할 설정 파일의 경로 및 파일 이름을 지정할 수 있습니다.

--config-append=[file]

이름 변경 작업에 추가할 설정 파일 경로 및 이름을 지정할 수 있습니다. 이 옵션은 응답 파일의 경로 및 파일 이름을 지정하는데 사용할 수 있습니다.

--generate-answer=[file]

ovirt-engine-rename 명령에 의해 변경된 값 및 응답이 기록되는 파일의 경로 및 파일 이름을 지정할 수 있습니다.

18.1.3. oVirt Engine Rename 도구 사용

요약

ovirt-engine-rename 명령을 사용하여 Manager의 정규화된 도메인 이름 레코드를 업데이트합니다.

이 도구를 사용하여 Manager에 로컬 ISO 또는 데이터 스토리지 도메인이 있는지 확인합니다. 도메인이 있다면 이 도구의 프롬프트에 따라 작업을 계속하기 전에 해당 스토리지에 연결된 모든 가상 머신 또는 스토리지 도메인을 빼거나, 종료하거나, 혹은 유지 보수 모드로 전환합니다. 이를 통해 이름 변경 과정에서 가상 머신이 가상 디스크와 연결이 끊어지거나 ISO 스토리지 도메인 연결이 끊어지는 것을 방지할 수 있습니다.

절차 18.1. Red Hat Virtualization Manager 이름 변경

1. 새로운 정규화된 도메인 이름의 모든 DNS 및 기타 관련 레코드를 준비합니다.
2. DHCP를 사용할 경우 DHCP 서버 설정을 업데이트합니다.
3. Manager에서 호스트 이름을 업데이트합니다.
4. 다음 명령을 실행합니다:

```
# /usr/share/ovirt-engine/setup/bin/ovirt-engine-rename
```

5. 프롬프트가 나타나면 **Enter** 를 눌러 engine 서비스를 중지합니다:

```
During execution engine service will be stopped (OK, Cancel) [OK]:
```

6. 프롬프트가 나타나면 Manager의 새로운 정규화된 도메인 이름을 입력합니다:

```
New fully qualified server name:[new name]
```

결과

ovirt-engine-rename 명령은 Manager의 정규화된 도메인 이름 레코드를 업데이트합니다.

18.2. ENGINE 설정 도구

18.2.1. Engine 설정 도구

Engine 설정 도구는 Red Hat Virtualization 환경의 글로벌 설정을 위한 명령행 유틸리티입니다. 이 도구는 engine 데이터베이스에 지정된 키값 매핑 목록과 상호 작용하여 개별 키를 검색 및 설정하고 사용 가능한 모든 설정 키 및 값 목록을 검색할 수 있습니다. 또한 Red Hat Virtualization 환경에서 각 설정 수준에 따라 다른 값을 저장할 수 있습니다.



참고

설정 키 값을 설정하거나 검색하기 위해 Red Hat Virtualization Manager 또는 Red Hat JBoss Enterprise Application Platform을 실행할 필요는 없습니다. 설정 키 값과 키 매핑은 engine 데이터 베이스에 저장되어 있기 때문에 **postgresql** 서비스가 실행되고 있는 동안 이를 업데이트할 수 있습니다. 변경사항은 **ovirt-engine** 서비스를 다시 시작할 때 적용됩니다.

18.2.2. engine-config 명령 구문

Red Hat Virtualization Manager가 설치된 시스템에서 engine 설정 도구를 실행할 수 있습니다. 사용법에 대한 보다 자세한 내용은 help 명령 출력 결과에서 확인합니다:

```
# engine-config --help
```

일반 작업

사용 가능한 설정 키 목록 나열

```
# engine-config --list
```

사용 가능한 설정 값 나열

```
# engine-config --all
```

설정키 값 검색

```
# engine-config --get [KEY_NAME]
```

지정된 버전의 키 값을 검색하기 위해 **[KEY_NAME]**을 원하는 키 이름으로 변경합니다. **--cver** 매개 변수를 사용하여 검색할 설정 버전 값을 지정합니다. 버전이 지정되어 있지 않을 경우 모든 기존 버전에 대한 값이 반환됩니다.

설정키 값 설정

```
# engine-config --set [KEY_NAME]=[KEY_VALUE] --cver=[VERSION]
```

[KEY_NAME]을 설정할 특정 키 이름으로 변경하고 **[KEY_VALUE]**를 설정할 값으로 변경합니다. 여러 설정 버전이 있는 환경의 경우 **[VERSION]**을 지정해야 합니다.

변경 사항을 적용하기 위해 **ovirt-engine** 서비스 다시 시작

변경 사항을 적용하기 위해 **ovirt-engine** 서비스를 다시 시작합니다.

```
# service ovirt-engine restart
```

18.3. 이미지 업로더 도구

18.3.1. 이미지 업로더 도구



참고

내보내기 스토리지 도메인은 사용되지 않습니다. 스토리지 데이터 도메인을 데이터 센터에서 분리한 후 같은 환경이나 다른 환경의 데이터 센터로 가져오기할 수 있습니다. 그 후에 가상 머신, 플로팅 가상 디스크 이미지, 그리고 템플릿을 가져오기한 스토리지 도메인에서 연결된 데이터 센터로 업로드할 수 있습니다. 스토리지 도메인을 가져오기하는 방법에 대한 자세한 내용은 [8.6절. “기존 스토리지 도메인 가져오기”](#)에서 참조하십시오.

engine-image-uploader 명령을 사용하여 내보내기할 스토리지 도메인을 나열하고 가상 머신 이미지를 OVF 또는 OVA 형식으로 내보내기 스토리지 도메인에 업로드하여 Red Hat Virtualization Manager에서 자동으로 인식할 수 있습니다.

OVA는 OVF 파일의 **tar** 아카이브(archive)입니다.



참고

이미지 업로더는 Red Hat Virtualization에 의해 생성된 gzip으로 압축된 OVF 또는 OVA 파일만 지원합니다.

OVF에는 다음과 같은 형식의 이미지와 마스터 디렉토리가 들어 있습니다:

```
|-- images
|   |-- [Image Group UUID]
|       |-- [Image UUID (this is the disk image)]
|       |-- [Image UUID (this is the disk image)].meta
|-- master
|   |--vms
|       |-- [UUID]
|       |-- [UUID].ovf
```

18.3.2. engine-image-uploader 명령 구문

이미지 업로더 명령의 기본 구문은 다음과 같습니다:

```
engine-image-uploader [options] list
engine-image-uploader [options] upload [file].[file]...[file]
```

이미지 업로더 명령은 **list** 및 **upload** 두 동작을 지원합니다.

- **list** 동작은 이미지를 업로드할 수 있는 내보내기 스토리지 도메인을 나열합니다.

- **upload** 동작은 지정된 내보내기 스토리지 도메인에 이미지를 업로드합니다.

이미지 업로더 명령을 사용하는 경우 위의 동작 중 하나를 지정해야 합니다. 또한 **upload** 동작을 사용하려면 최소 하나의 로컬 파일을 지정해야 합니다.

engine-image-uploader 명령을 자세히 지정하기 위한 여러 매개 변수가 있습니다. 이러한 매개 변수의 기본값은 **/etc/ovirt-engine/imageuploader.conf** 파일에서 설정할 수 있습니다.

일반 옵션

-h, --help

이미지 업로더 명령을 사용하는 방법에 대한 정보를 표시합니다.

--conf-file=[PATH]

명령을 사용할 설정 파일로 **[PATH]**를 설정합니다. 기본값은 **etc/ovirt-engine/imageuploader.conf**입니다.

--log-file=[PATH]

로그 출력 결과를 작성하기 위해 명령이 사용할 특정 파일 이름으로 **[PATH]**를 설정합니다. 기본값은 **/var/log/ovirt-engine/ovirt-image-uploader-[date].log**입니다.

--cert-file=[PATH]

engine을 검증하기 위한 인증서로 **[PATH]**를 설정합니다. 기본값은 **/etc/pki/ovirt-engine/ca.pem**입니다.

--insecure

engine 검증을 시도하지 않도록 지정합니다.

--quiet

콘솔 출력을 최소로 감소시키는 자동 모드 (quiet mode)를 설정합니다.

-v, --verbose

보다 자세한 콘솔 출력을 표시하는 상세 표시 모드 (verbose mode)를 설정합니다.

-f, --force

강제 모드 (Force mode)는 업로드된 소스 파일이 내보내기 도메인에 있는 기존 파일과 동일한 파일 이름일 경우에 사용해야 합니다. 이 옵션은 기존 파일을 강제로 덮어쓰기합니다.

Red Hat Virtualization Manager 옵션

-u [USER], --user=[USER]

명령 실행에 사용할 사용자 인증을 지정합니다. **[USER]**은/는 **[username]@[domain]** 형식으로 지정합니다. 사용자는 지정된 도메인에 존재해야 하며 Red Hat Virtualization Manager가 알고 있어야 합니다.

-r [FQDN], --engine=[FQDN]

이미지가 업로드될 Red Hat Virtualization Manager의 IP 주소 또는 정규화된 도메인 이름을 지정합니다. 이미지 업로더는 Red Hat Virtualization Manager가 설치된 시스템과 동일한 컴퓨터에서 실행되는 것을 전제로 합니다. 기본값은 **localhost:443**입니다.

내보내기 스토리지 도메인 옵션

다음 옵션은 이미지를 업로드할 내보내기 도메인을 지정합니다. 이러한 옵션은 동시에 함께 사용할 수 없습니다. **-e** 또는 **-n** 옵션 중 하나를 사용해야 합니다.

-e [EXPORT_DOMAIN], --export-domain=[EXPORT_DOMAIN]

스토리지 도메인 *EXPORT_DOMAIN*을 업로드할 대상으로 설정합니다.

-n [NFSSERVER], --nfs-server=[NFSSERVER]

NFS path *[NFSSERVER]*을/를 업로드할 대상으로 설정합니다.

가져오기 옵션

다음 옵션을 사용하여 이미지를 내보내기 도메인에 업로드할 때 포함된 업로드할 이미지 속성을 사용자 정의할 수 있습니다.

-i, --ovf-id

이미지의 UUID가 업데이트되지 않도록 지정합니다. 기본값으로 명령은 업로드된 이미지의 새 UUID를 생성합니다. 이는 업로드된 이미지와 환경에 이미 존재하는 이미지 사이에서 ID충돌이 발생하지 않게 합니다.

-d, --disk-instance-id

이미지에 있는 각 디스크의 인스턴스 ID 이름이 변경되지 않도록 지정합니다. 기본값으로 명령은 업로드된 이미지에 있는 디스크의 새 UUID를 생성합니다. 이는 업로드된 이미지에 있는 디스크와 환경에 이미 존재하는 디스크 간의 충돌이 발생하지 않게 합니다.

-m, --mac-address

이미지의 네트워크 구성 요소가 해당 이미지에서 제거되지 않도록 지정합니다. 기본값으로 명령은 업로드된 이미지에서 네트워크 인터페이스 카드를 제거하여 환경에 이미 존재하는 다른 가상 머신의 네트워크 카드와 충돌하지 않게 합니다. 이 옵션을 사용하지 않은 경우 관리 포털을 사용하여 네트워크 인터페이스 카드를 새로 가져오기한 이미지에 추가하여 Manager가 MAC 주소 충돌이 발생하지 않게 할 수 있습니다.

-N [NEW_IMAGE_NAME], --name=[NEW_IMAGE_NAME]

업로드될 이미지의 새 이름을 지정합니다.

18.3.3. 이미지 업로더와 호환하는 OVF 아카이브 만들기

개요

engine-image-uploader 도구를 사용하여 업로드할 수 있는 파일을 만들 수 있습니다.

절차 18.2. 이미지 업로더와 호환하는 OVF 아카이브 만들기

1. Manager를 사용하여 빈 내보내기 도메인을 생성합니다. 빈 내보내기 도메인을 통해 어떤 디렉토리에 가상 머신이 들어 있는지를 쉽게 확인할 수 있습니다.

2. 생성한 비어있는 내보내기 도메인에 가상 머신을 내보냅니다.
3. 내보내기 도메인으로 사용되는 스토리지 서버에 로그인하여 NFS 공유의 **root**를 찾아 마운트 지점 아래의 서브 디렉토리로 변경합니다. 새 내보내기 도메인으로 시작했으므로 내보내기된 디렉토리 아래에는 하나의 디렉토리만 있습니다. 이에는 **images/** 및 **master/** 디렉토리가 포함되어 있습니다.
4. **tar -zcvf my.ovf images/ master/** 명령을 실행하여 tar/gzip OVF 아카이브를 생성합니다.
5. 만든 OVF 파일 (예에서는 **my.ovf**로 부름)을 전달 받으면 누구나 **engine-image-uploader** 명령을 사용하여 Red Hat Virtualization Manager로 가져오기할 수 있습니다.

결과

배포할 수 있는 압축된 OVF 이미지 파일이 생성되었습니다. 이 파일을 받으면 누구나 **engine-image-uploader** 명령을 사용하여 이미지를 Red Hat Virtualization 환경에 업로드할 수 있습니다.

18.3.4. 기본적인 **engine-image-uploader** 사용 예

다음은 내보내기 스토리지 도메인을 나열하기 위해 **engine** 업로더 명령을 사용하는 방법의 예입니다:

예 18.1. 이미지 업로더를 사용하여 내보내기 스토리지 도메인 목록 보기

```
# engine-image-uploader list
Please provide the REST API password for the admin@internal oVirt Engine
user (CTRL+D to abort):
Export Storage Domain Name | Datacenter | Export Domain Status
myexportdom                | Myowndc   | active
```

다음은 OVF (Open Virtualization Format) 파일을 업로드하는 방법의 예입니다:

예 18.2. 이미지 업로더를 사용하여 파일 업로드

```
# engine-image-uploader -e myexportdom upload myrhel6.ovf
Please provide the REST API password for the admin@internal oVirt Engine
user (CTRL+D to abort):
```

18.4. USB 필터 편집기

18.4.1. USB 필터 편집기 설치

USB 필터 편집기는 Windows 용 도구로 **usbfilter.txt** 정책 파일을 설정하는데 사용됩니다. 이 파일에서 지정된 정책 규칙을 통해 클라이언트 머신에서 Red Hat Virtualization Manager를 사용하여 관리되는 가상 머신으로 특정 USB 장치 자동 통과를 허용 또는 거부할 수 있습니다. 정책 파일은 Red Hat Virtualization Manager에 있는 다음과 같은 위치에 저장됩니다:

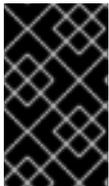
/etc/ovirt-engine/usbfilter.txt

USB 필터 정책 변경 사항은 Red Hat Virtualization Manager 서버에 있는 **ovirt-engine** 서비스를 다시 시작할 때 까지 적용되지 않습니다.

컨텐츠 전송 네트워크에서 **USBFilterEditor.msi** 파일을 다운로드합니다:
<https://rhn.redhat.com/rhn/software/channel/downloads/Download.do?cid=20703>.

절차 18.3. USB 필터 편집기 설치

1. Windows 시스템에서 컨텐츠 전송 네트워크에서 가져온 **USBFilterEditor.msi** 설치 프로그램을 시작합니다.
2. 설치 마법사에 있는 절차를 따릅니다. 설치 위치를 지정하지 않은 경우 USB 필터 편집기는 Windows 버전에 따라 기본값으로 **C:\Program Files\RedHat\USB Filter Editor** 또는 **C:\Program Files(x86)\RedHat\USB Filter Editor**에 설치됩니다.
3. 바탕 화면에 USB 필터 편집기 바로가기 아이콘이 생성됩니다.



중요

Secure Copy (SCP) 클라이언트를 사용하여 Red Hat Virtualization Manager에서 필터 정책을 가져오기 및 내보내기합니다. Windows 시스템 용 Secure Copy 도구는 WinSCP (<http://winscp.net>)입니다.

기본 USB 장치 정책은 USB 장치로의 기본 액세스를 갖는 가상 머신을 제공합니다. 추가 USB 장치를 사용하려면 정책을 업데이트합니다.

18.4.2. USB 필터 편집기 인터페이스

- 바탕화면에서 USB 필터 편집기 바로가기 아이콘을 두 번 클릭합니다.

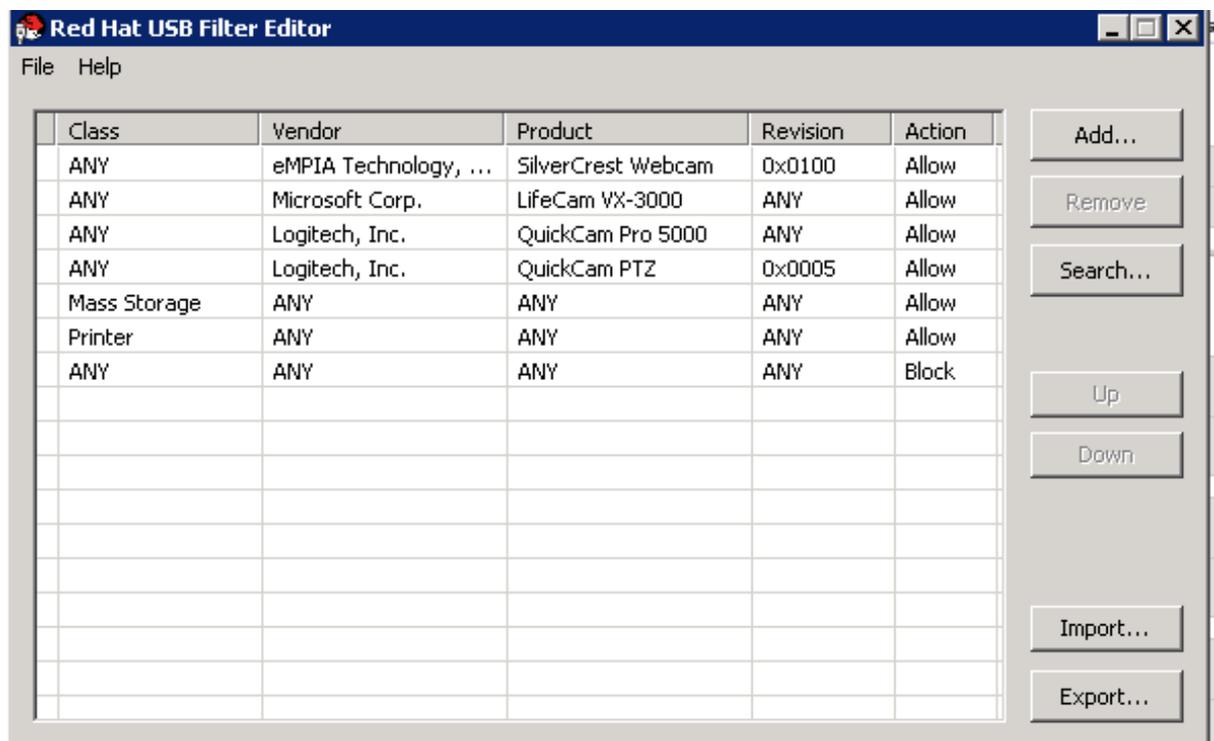


그림 18.1. Red Hat USB 필터 편집기

Red Hat USB 필터 편집기 인터페이스에서는 각 USB 장치의 **Class**, **Vendor**, **Product**, **Revision**, **Action**을 표시합니다. 허용된 USB 장치는 **Action** 란에 **Allow**로 설정되며 차단된 장치는 **Block**으로 설정됩니다.

표 18.1. USB 편집기 필드

이름	설명
Class	USB 장치 유형으로 프린터, 대용량 저장 컨트롤러 등입니다.
Vendor	선택한 장치 유형의 제조업체입니다.
Product	특정 USB 장치 모델입니다.
Revision	제품 버전입니다.
Action	지정된 장치를 허용 또는 차단합니다.

USB 장치 정책 규칙은 나열된 순서로 처리됩니다. **Up** 및 **Down** 버튼을 사용하여 규칙을 목록의 위 또는 아래로 이동합니다. 범용 **Block** 규칙은 USB 필터 편집기에서 명시적으로 허용하지 않는 경우 모든 USB 장치를 거부하기 위해 목록 하단에 배치해야 합니다.

18.4.3. USB 정책 추가

요약

USB 필터 편집기에 USB 정책을 추가합니다.

데스크탑에서 USB 필터 편집기 바로가기 아이콘을 두 번 클릭하여 편집기를 엽니다.

절차 18.4. USB 정책 추가

1. 추가 버튼을 클릭합니다. **USB 기준 편집 창**을 엽니다:

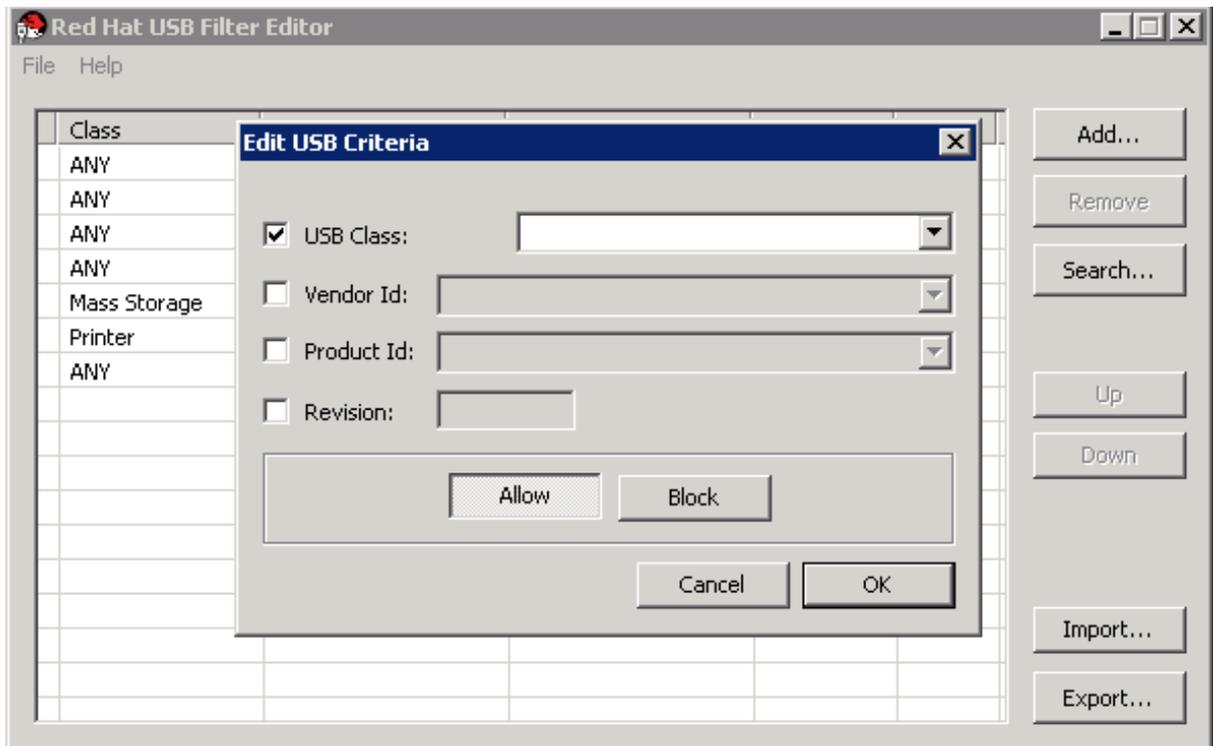


그림 18.2. USB 기준 편집

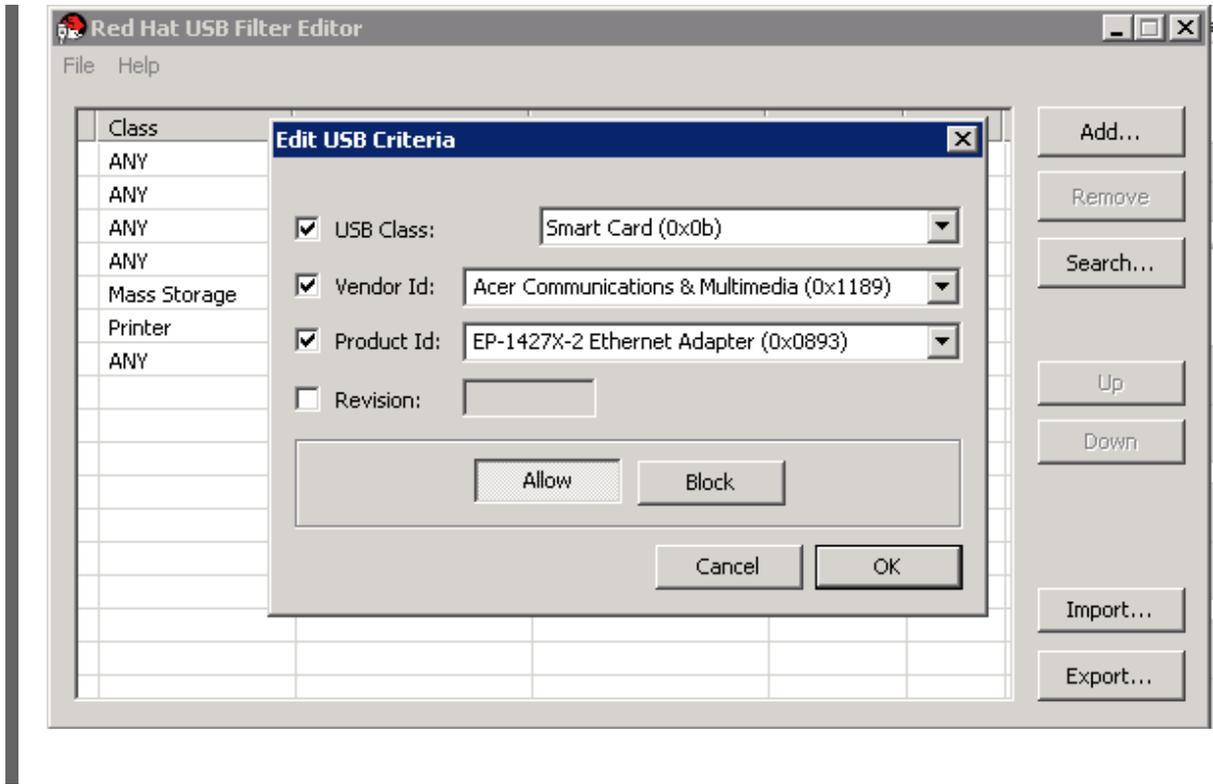
2. **USB 클래스, 벤더 ID, 제품 ID, 버전** 확인란을 사용하여 지정할 장치 목록을 나열합니다.

허용 버튼을 클릭하여 USB 장치의 가상 머신 사용을 허용합니다. **차단** 버튼을 클릭하여 가상 머신에서 USB 장치 사용을 금지합니다.

OK를 클릭하여 선택한 필터 규칙을 목록에 추가하고 창을 닫습니다.

예 18.3. 장치 추가

다음 예에서는 제조업체 **Acer Communications & Multimedia**에서 허용되는 장치 목록으로 USB 클래스 **Smartcard**, 장치 **EP-1427X-2 Ethernet Adapter**를 추가하는 방법에 대해 설명합니다.



3. 파일 →저장을 클릭하여 변경 사항을 저장합니다.

결과

USB 필터 편집기에 USB 정책을 추가합니다. USB 필터 정책을 적용하려면 Red Hat Virtualization Manager에 내보내기해야 합니다.

18.4.4. USB 정책 삭제

요약

USB 필터 편집기에서 USB 정책을 삭제합니다.

편집기를 열려면 바탕화면의 USB 필터 편집기 바로가기 아이콘을 두 번 클릭합니다.

절차 18.5. USB 정책 삭제

1. 삭제할 정책을 선택합니다.

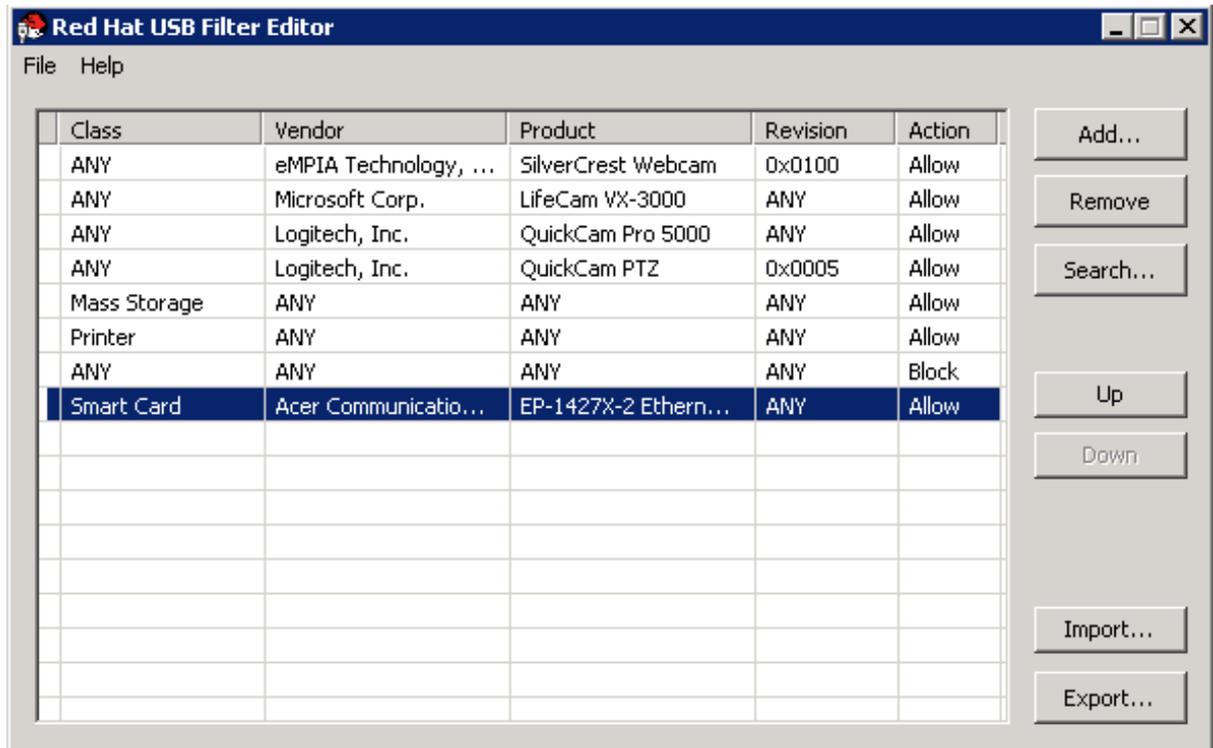


그림 18.3. USB 정책 선택

2. 삭제 버튼을 클릭합니다. 정책을 삭제할 지를 묻는 메시지가 나타납니다.

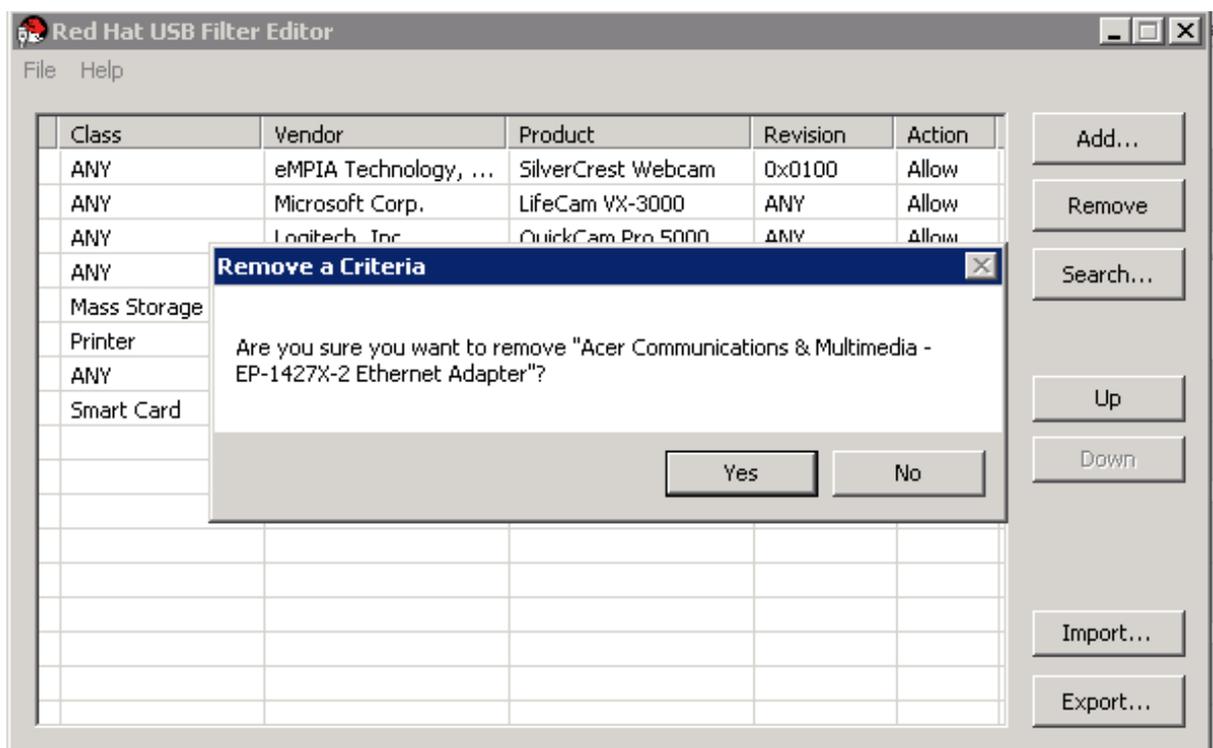


그림 18.4. USB 기준 편집

3. **Yes**를 클릭하여 정책 삭제를 확인합니다.
4. **파일** → **저장**을 클릭하여 변경 사항을 저장합니다.

결과

USB 필터 편집기에서 USB 정책이 삭제되었습니다. USB 필터 정책을 적용하려면 Red Hat Virtualization Manager로 내보내기해야 합니다.

18.4.5. USB 장치 정책 검색

요약

USB 필터 편집기에서 허용하거나 차단할 연결된 USB 장치를 검색합니다.

바탕 화면에 있는 USB 필터 편집기 바로가기 아이콘을 두 번 클릭하여 편집기를 엽니다.

절차 18.6. USB 장치 정책 검색

1. 검색을 클릭합니다. 연결된 USB 장치 창에 연결된 모든 장치 목록이 표시됩니다.

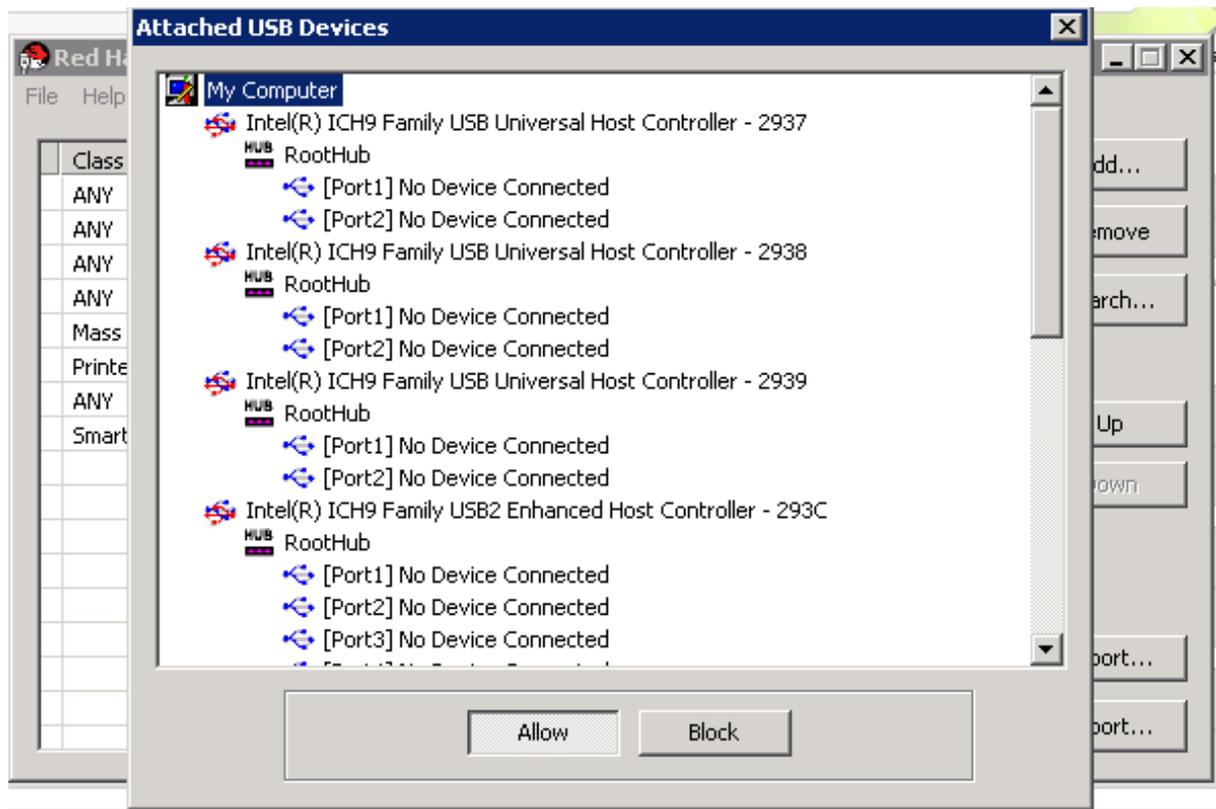


그림 18.5. 연결된 USB 장치

2. 장치를 선택하고 허용 또는 차단을 클릭합니다. 창을 닫으려면 선택한 장치를 두 번 클릭합니다. 장치의 정책 규칙은 목록에 추가됩니다.
3. Up 및 Down 버튼을 사용하여 목록에 있는 새로운 정책 규칙의 위치를 변경합니다.
4. 파일 → 저장을 클릭하여 변경 사항을 저장합니다.

결과

연결된 USB 장치가 검색됩니다. USB 필터 정책을 적용하려면 Red Hat Virtualization Manager로 내보내기해야 합니다.

18.4.6. USB 정책 내보내기

요약

USB 장치 정책 변경 사항을 적용하려면 Red Hat Virtualization Manager로 내보내기 및 업로드해야

합니다. 정책을 업로드하고 **ovirt-engine** 서비스를 다시 시작합니다.

바탕화면에서 USB 필터 편집기 바로가기 아이콘을 두 번 클릭하여 편집기를 엽니다.

절차 18.7. USB 정책 내보내기

1. 내보내기를 클릭합니다. 다른 이름으로 저장 창이 열립니다.
2. **usbfilter.txt** 파일 이름으로 파일을 저장합니다.
3. WinSCP와 같은 Secure Copy 클라이언트를 사용하여 **usbfilter.txt** 파일을 Red Hat Virtualization Manager를 실행하고 있는 서버에 업로드합니다. 파일은 서버 상의 다음과 같은 디렉토리에 배치해야 합니다:

```
/etc/ovirt-engine/
```

4. Red Hat Virtualization Manager를 실행하고 있는 서버에서 **root** 사용자로 **ovirt-engine** 서비스를 다시 시작합니다.

```
# systemctl restart ovirt-engine.service
```

결과

USB 장치 정책이 Red Hat Virtualization 환경에서 실행되는 가상 머신에서 구현됩니다.

18.4.7. USB 정책 가져오기

요약

기존 USB 장치 정책을 다운로드하고 편집하기 전 USB 필터 편집기로 가져옵니다.

절차 18.8. USB 정책 가져오기

1. WinSCP와 같은 Secure Copy 클라이언트를 사용하여 **usbfilter.txt** 파일을 Red Hat Virtualization Manager를 실행하고 있는 서버에 업로드합니다. 파일은 서버 상의 다음과 같은 디렉토리에 배치해야 합니다:

```
/etc/ovirt-engine/
```

2. 바탕화면에서 USB 필터 편집기 바로가기 아이콘을 두 번 클릭하여 편집기를 엽니다.
3. 가져오기를 클릭하여 열기 창을 엽니다.
4. 서버에서 다운로드한 **usbfilter.txt** 파일을 엽니다.

결과

USB 필터 편집기에서 USB 장치 정책을 편집할 수 있습니다.

18.5. 로그 수집 도구

18.5.1. 로그 수집기

로그 수집 도구는 Red Hat Virtualization Manager에 포함되어 있습니다. 이러한 도구를 사용하여 지원 요청 시 Red Hat Virtualization 환경에서 관련 로그를 쉽게 수집할 수 있습니다.

로그 수집 명령은 **ovirt-log-collector**입니다. **root** 사용자로 로그인하여 Red Hat Virtualization 환경의 관리 인증 정보를 입력합니다. **ovirt-log-collector -h** 명령을 실행하면 **ovirt-log-collector** 명령에 유효한 모든 옵션 목록을 포함하여 사용 정보가 표시됩니다.

18.5.2. ovirt-log-collector 명령 구문

로그 수집 명령의 기본 구문은 다음과 같습니다:

```
ovirt-log-collector [options] list [all, clusters, datacenters]
ovirt-log-collector [options] collect
```

작업이 지원되는 두 가지 모드는 **list** 및 **collect**입니다.

- **list** 매개 변수는 Red Hat Virtualization Manager에 연결된 호스트, 클러스터, 또는 데이터 센터를 나열합니다. 나열된 개체에 기반하여 로그 수집을 필터링할 수 있습니다.
- **collect** 매개 변수는 Red Hat Virtualization Manager에서 로그를 수집합니다. 수집된 로그는 **/tmp/logcollector** 디렉토리 아래의 아카이브 파일에 저장됩니다. **ovirt-log-collector** 명령은 각 로그에 특정 파일 이름을 할당합니다.

다른 매개 변수를 지정하지 않을 경우 기본적으로 자신이 속한 데이터 센터 및 클러스터와 함께 사용할 수 있는 호스트가 나열됩니다. 특정 로그를 검색하려면 사용자 이름 및 암호를 입력하라는 메시지가 표시됩니다.

ovirt-log-collector 명령을 상세 지정하기 위한 여러 매개 변수가 있습니다.

일반 옵션

--version

사용 중인 명령의 버전 번호를 표시하고 프롬프트로 돌아갑니다.

-h, --help

명령 사용 정보를 표시하고 프롬프트로 돌아갑니다.

--conf-file=PATH

도구가 사용할 설정 파일로 **PATH**를 설정합니다.

--local-tmp=PATH

로그가 저장된 디렉토리로 **PATH**를 설정합니다. 기본 디렉토리는 **/tmp/logcollector**입니다.

--ticket-number=TICKET

SOS 보고서와 관련된 티켓 또는 기술 문의 번호로 **TICKET**을 설정합니다.

--upload=FTP_SERVER

FTP를 사용하여 전송되는 검색된 로그의 대상으로 **FTP_SERVER**를 설정합니다. Red Hat 지원 담당자가 권장하지 않는 한 이 옵션을 사용하지 마십시오.

--log-file=PATH

명령이 로그 출력을 위해 사용할 특정 파일 이름으로 **PATH**를 설정합니다.

--quiet

콘솔 출력을 최소로 감소시키는 자동 모드 (Quiet mode)를 설정합니다. 기본값으로 자동 모드는 설정 해제되어 있습니다.

-v, --verbose

보다 자세한 콘솔 출력을 표시하는 상세 표시 모드 (Verbose mode)를 설정합니다. 상세 표시 모드는 기본값으로 설정 해제되어 있습니다.

Red Hat Virtualization Manager 옵션

이 옵션은 로그 수집을 필터링하고 Red Hat Virtualization Manager의 인증 정보를 지정합니다.

이러한 매개 변수를 특정 명령을 위해 결합할 수 있습니다. 예를 들어 **ovirt-log-collector --user=admin@internal --cluster ClusterA,ClusterB --hosts "SalesHost"**는 사용자를 **admin@internal**로 지정하고 클러스터 **A** 및 **B**에 있는 **SalesHost** 호스트로만 로그 수집을 제한합니다.

--no-hypervisors

로그 수집에서 가상화 호스트를 제외합니다.

-u USER, --user=USER

사용자 로그인 이름을 설정합니다. **USER**는 **user@domain** 형식으로 지정되며 여기서 **user**는 사용자 이름이고 **domain**은 사용 중인 디렉토리 서비스 도메인입니다. 사용자는 디렉토리 서비스에 존재해야 하며 Red Hat Virtualization Manager가 알고 있어야 합니다.

-r FQDN, --rhevm=FQDN

로그를 수집할 Red Hat Virtualization Manager 서버의 정규화된 도메인 이름을 설정합니다. 여기서 **FQDN**은 Manager의 정규화된 도메인 이름으로 변경합니다. 로그 수집기는 Red Hat Virtualization Manager와 동일한 로컬 호스트에서 실행되는 것으로 간주되며 기본값은 **localhost**입니다.

-c CLUSTER, --cluster=CLUSTER

Red Hat Virtualization Manager의 로그에 더하여 지정된 **CLUSTER**에 있는 가상화 호스트에서 로그를 수집합니다. 클러스터를 포함하려면 클러스터 이름 또는 일치하는 패턴 목록을 콤마로 구분하여 지정합니다.

-d DATACENTER, --data-center=DATACENTER

Red Hat Virtualization Manager의 로그에 더하여 지정된 **DATACENTER**에 있는 가상화 호스트의 로그를 수집합니다. 데이터 센터를 포함하려면 데이터 센터 이름 또는 일치하는 패턴 목록을 콤마로 구분하여 지정합니다.

-H HOSTS_LIST, --hosts=HOSTS_LIST

Red Hat Virtualization Manager의 로그에 더하여 지정된 **HOSTS_LIST**에 있는 가상화 호스트에서 로그를 수집합니다. 호스트를 포함하려면 호스트 이름, 정규화된 도메인 이름, IP 주소, 일치하는 패턴 목록을 콤마로 구분하여 지정합니다.

SOS 보고서 옵션

로그 수집기는 JBoss SOS 플러그인을 사용합니다. 다음 옵션을 사용하여 JMX 콘솔에서 데이터 수집을 활성화합니다.

--jboss-home=JBASS_HOME

JBoss 설치 디렉토리 경로입니다. 기본값은 `/var/lib/jbossas`입니다.

--java-home=JAVA_HOME

Java 설치 디렉토리 경로입니다. 기본값은 `/usr/lib/jvm/java`입니다.

--jboss-profile=JBASS_PROFILE

따옴표 및 공백으로 구분된 서버 프로파일 목록을 표시합니다. 지정된 프로파일로 로그 수집을 제한합니다. 기본값은 `'rhevm-slimmed'`입니다.

--enable-jmx

Red Hat Virtualization의 JBoss JMX 인터페이스에서 런타임 통계 수집을 활성화합니다.

--jboss-user=JBASS_USER

JBoss JMX를 호출할 수 있는 권한을 갖는 사용자입니다. 기본값은 `admin`입니다.

--jboss-logsize=LOG_SIZE

검색된 로그 파일의 최대 크기 (MB 단위)입니다.

--jboss-stdjar=STATE

JBoss 표준 JAR의 JAR 통계 수집을 설정합니다. `STATE`를 `on` 또는 `off`로 변경합니다. 기본값은 `on`입니다.

--jboss-servjar=STATE

모든 서버 설정 디렉토리에서 JAR 통계 수집을 설정합니다. `STATE`를 `on` 또는 `off`로 변경합니다. 기본값은 `on`입니다.

--jboss-twiddle=STATE

twiddle 데이터 수집을 `on` 또는 `off`로 설정합니다. Twiddle은 JMX 호출에서 데이터를 수집하기 위해 사용되는 JBoss 도구입니다. `STATE`를 `on` 또는 `off`로 변경합니다. 기본값은 `on`입니다.

--jboss-appxml=XML_LIST

XML 설명으로 검색할 애플리케이션 목록을 따옴표 및 공백으로 구분하여 표시합니다. 기본값은 `all`입니다.

SSH 설정**--ssh-port=PORT**

가상화 호스트로 SSH 연결 시 사용할 포트로 `PORT`를 설정합니다.

-k KEYFILE, --key-file=KEYFILE

가상화 호스트에 액세스하기 위해 사용할 SSH 공개키로 `KEYFILE`을 설정합니다.

--max-connections=MAX_CONNECTIONS

가상화 호스트에서 로그 수집 시 최대 SSH 동시 연결 수로 `MAX_CONNECTIONS`을 설정합니다. 기본값은 `10`입니다.

PostgreSQL 데이터베이스 옵션

데이터베이스 사용자 이름 및 데이터베이스 이름이 기본값에서 변경되어 있을 경우 **pg-user** 및 **dbname** 매개변수를 사용하여 지정합니다.

데이터베이스가 로컬 호스트에 없는 경우 **pg-dbhost** 매개 변수를 사용합니다. **pg-host-key** 매개 변수 옵션을 사용하여 원격 로그를 수집합니다. 원격 로그 수집을 위해 PostgreSQL SOS 플러그인을 데이터베이스 서버에 설치해야 합니다.

--no-postgresql

데이터베이스 수집을 비활성화합니다. **--no-postgresql** 매개 변수가 지정되어 있지 않을 경우 로그 수집기는 Red Hat Virtualization Manager PostgreSQL 데이터베이스에 연결하고 로그 보고서에 데이터를 추가해야 합니다.

--pg-user=USER

데이터 서버와의 연결에 사용할 사용자 이름으로 **USER**를 설정합니다. 기본값은 **postgres**입니다.

--pg-database=DBNAME

데이터베이스 서버와의 연결에 사용할 데이터베이스 이름으로 **DBNAME**을 설정합니다. 기본값은 **rhevmdb**입니다.

--pg-dbhost=DBHOST

데이터베이스 서버의 호스트 이름으로 **DBHOST**를 설정합니다. 기본값은 **localhost**입니다.

--pg-host-key=KEYFILE

데이터베이스 서버의 공개 ID 파일 (개인 키)로 **KEYFILE**을 설정합니다. 이 값은 기본값으로 설정되어 있지 않습니다. 데이터베이스가 로컬 호스트에 존재하지 않을 경우에만 필요합니다.

18.5.3. 기본 로그 수집기 사용

추가 매개 변수를 지정하지 않고 **ovirt-log-collector** 명령을 실행하면 기본적으로 Red Hat Virtualization Manager 및 연결된 호스트에서의 모든 로그를 수집합니다. **--no-postgresql** 매개 변수를 추가하지 않은 경우 데이터베이스 로그도 수집합니다. 다음 예에서는 로그 수집기를 실행하여 Red Hat Virtualization Manager 및 세 개의 연결된 호스트에서 모든 로그를 수집합니다.

예 18.4. 로그 수집기 사용

```
# ovirt-log-collector
INFO: Gathering oVirt Engine information...
INFO: Gathering PostgreSQL the oVirt Engine database and log files from
localhost...
Please provide REST API password for the admin@internal oVirt Engine
user (CTRL+D to abort):
About to collect information from 3 hypervisors. Continue? (Y/n):
INFO: Gathering information from selected hypervisors...
INFO: collecting information from 192.168.122.250
INFO: collecting information from 192.168.122.251
INFO: collecting information from 192.168.122.252
INFO: finished collecting information from 192.168.122.250
INFO: finished collecting information from 192.168.122.251
INFO: finished collecting information from 192.168.122.252
Creating compressed archive...
```

```
INFO Log files have been collected and placed in
/tmp/logcollector/sosreport-rhn-account-20110804121320-ce2a.tar.xz.
The MD5 for this file is 6d741b78925998caff29020df2b2ce2a and its size
is 26.7M
```

18.6. ISO 업로더 도구

18.6.1. ISO 업로더 도구

ISO 업로더는 ISO 이미지를 ISO 스토리지 도메인에 업로드하기 위한 도구입니다. 이는 Red Hat Virtualization Manager의 일부로 설치됩니다.

ISO 업로더 명령은 **engine-iso-uploader**입니다. **root** 사용자로 로그인하고 Red Hat Virtualization 환경의 관리자 인증 정보를 입력하여 이러한 명령을 사용합니다. **engine-iso-uploader -h** 명령은 **engine-iso-uploader** 명령의 모든 사용 가능한 옵션 목록을 포함하여 사용 방법을 표시합니다.

18.6.2. engine-iso-uploader 명령 구문

ISO 업로더 명령의 기본 구문은 다음과 같습니다:

```
engine-iso-uploader [options] list
engine-iso-uploader [options] upload [file].[file]...[file]
```

ISO 업로더 명령은 **list** 및 **upload**의 두 가지 동작을 지원합니다.

- **list** 동작은 ISO 파일을 업로드할 수 있는 ISO 스토리지 도메인을 나열합니다. Red Hat Virtualization Manager는 설치 프로세스 도중 Manager가 설치된 시스템에 이러한 목록을 생성합니다.
- **upload** 동작은 특정 ISO 스토리지 도메인에 공백으로 구분된 단일 ISO 파일 또는 여러 ISO 파일을 업로드합니다. 기본값으로 NFS가 사용되지만 SSH 또한 사용할 수 있습니다.

ISO 업로더 명령을 사용하는 경우 위의 동작 중 하나를 지정해야 합니다. 또한 **upload** 동작을 사용하려면 최소 하나의 로컬 파일을 지정해야 합니다.

engine-iso-uploader 명령을 상세 지정하기 위한 여러 매개 변수가 있습니다.

일반 옵션

--version

ISO 업로더 명령의 버전 정보를 표시합니다.

-h, --help

ISO 업로더 명령을 사용하는 방법에 대한 정보를 표시합니다.

--conf-file=[PATH]

명령이 사용할 설정 파일로 **[PATH]**를 설정합니다. 기본값은 **/etc/ovirt-engine/isouploader.conf**입니다.

--log-file=[PATH]

로그 출력 결과를 작성하기 위해 명령이 사용할 특정 파일 이름으로 *[PATH]*를 설정합니다. 기본값은 `/var/log/ovirt-engine/ovirt-iso-uploader/ovirt-iso-uploader[date].log`입니다.

--cert-file=[PATH]

engine을 검증하기 위한 인증서로 *[PATH]*를 설정합니다. 기본값은 `/etc/pki/ovirt-engine/ca.pem`입니다.

--insecure

engine 검증을 시도하지 않도록 지정합니다.

--nossll

engine에 연결에 SSL을 사용하지 않도록 지정합니다.

--quiet

콘솔 출력을 최소로 감소시키는 자동 모드 (quiet mode)를 설정합니다.

-v, --verbose

보다 자세한 콘솔 출력을 표시하는 상세 표시 모드 (verbose mode)를 설정합니다.

-f, --force

강제 모드 (Force mode)는 업로드된 소스 파일이 ISO 도메인에 있는 기존 파일과 동일한 파일 이름 일 경우에 사용해야 합니다. 이 옵션은 기존 파일을 강제로 덮어쓰기합니다.

Red Hat Virtualization Manager 옵션

-u [USER], --user=[USER]

명령 실행에 사용할 사용자 인증을 지정합니다. *[USER]*은/는 `[username]@[domain]` 형식으로 지정합니다. 사용자는 지정된 도메인에 존재해야 하며 Red Hat Virtualization Manager가 알고 있어야 합니다.

-r [FQDN], --engine=[FQDN]

이미지가 업로드될 Red Hat Virtualization Manager의 IP 주소 또는 정규화된 도메인 이름을 지정합니다. 이미지 업로더는 Red Hat Virtualization Manager가 설치된 시스템과 동일한 컴퓨터에서 실행되는 것을 전제로 합니다. 기본값은 `localhost:443`입니다.

ISO 스토리지 도메인 옵션

다음 옵션은 이미지를 업로드할 ISO 도메인을 지정합니다. 이러한 옵션은 동시에 함께 사용할 수 없습니다. **-i** 또는 **-n** 옵션 중 하나를 사용해야 합니다.

-i, --iso-domain=[ISODOMAIN]

스토리지 도메인 *[ISODOMAIN]*을 업로드할 대상으로 설정합니다.

-n, --nfs-server=[NFSSERVER]

NFS 경로 *[NFSSERVER]*을/를 업로드할 대상으로 설정합니다.

연결 옵션

ISO 업로더는 파일을 업로드하기 위해 기본적으로 NFS를 사용합니다. 이러한 옵션은 SSH 파일 전송을 지정합니다.

--ssh-user=[USER]

업로드에 사용할 SSH 사용자 이름으로 **[USER]**를 설정합니다. 기본값은 **root**입니다.

--ssh-port=[PORT]

SSH에 연결 시 사용할 포트 **[PORT]**를 설정합니다.

-k [KEYFILE], --key-file=[KEYFILE]

SSH 인증에 사용할 공개키로 **[KEYFILE]**을 설정합니다. 키가 설정되어 있지 않을 경우 **--ssh-user=[USER]**로 지정된 사용자의 암호를 입력해야 합니다.

18.6.3. NFS 서버 지정

예 18.5. NFS 서버에 업로드

```
# engine-iso-uploader --nfs-server=storage.demo.redhat.com:/iso/path
upload RHEL6.0.iso
```

18.6.4. 기본 ISO 업로더 사용

다음은 ISO 업로더와 list 매개 변수의 예입니다. 첫 번째 명령은 사용 가능한 ISO 스토리지 도메인을 나열하며 명령에 사용자가 지정되어 있지 않기 때문에 **admin@internal** 사용자가 사용됩니다. 두 번째 명령은 NFS를 통해 지정된 ISO 도메인에 ISO 파일을 업로드합니다.

예 18.6. 도메인 목록 및 이미지 업로드

```
# engine-iso-uploader list
Please provide the REST API password for the admin@internal oVirt Engine
user (CTRL+D to abort):
ISO Storage Domain Name | Datacenter          | ISO Domain Status
ISODomain                | Default             | active

# engine-iso-uploader --iso-domain=[ISODomain] upload [RHEL6.iso]
Please provide the REST API password for the admin@internal oVirt Engine
user (CTRL+D to abort):
```

18.6.5. ISO 스토리지 도메인에 VirtIO 및 게스트 도구 이미지 파일 업로드

다음 예에서는 **ISODomain**에 **virtio-win.iso**, **virtio-win_x86.vfd**, **virtio-win_amd64.vfd**, **rhev-tools-setup.iso** 이미지 파일을 업로드하는 명령을 보여줍니다.

예 18.7. VirtIO 및 게스트 도구 이미지 파일 업로드

```
# engine-iso-uploader --iso-domain=[ISODomain] upload
```

```
/usr/share/virtio-win/virtio-win.iso /usr/share/virtio-win/virtio-win_x86.vfd /usr/share/virtio-win/virtio-win_amd64.vfd /usr/share/rhev-guest-tools-iso/rhev-tools-setup.iso
```

18.6.6. VirtIO 및 게스트 도구 이미지 파일

Windows 가상 머신 용 VirtIO 드라이버가 들어 있는 virtio-win ISO 및 VFD (Virtual Floppy Drive) 이미지와 Windows 가상 머신용 Red Hat Virtualization 게스트 도구가 들어 있는 rhev-tools-setup ISO 가 도메인 설치 및 설정 시 ISO 스토리지 도메인에 복사됩니다.

이러한 이미지 파일은 가상 머신에 설치할 수 있는 소프트웨어를 제공하여 성능 및 유용성을 향상시킵니다. 가장 최근의 virtio-win 및 rhev-tools-setup 파일은 Red Hat Virtualization Manager의 파일 시스템에 있는 다음과 같은 심볼릭 링크를 통해 액세스할 수 있습니다:

- **/usr/share/virtio-win/virtio-win.iso**
- **/usr/share/virtio-win/virtio-win_x86.vfd**
- **/usr/share/virtio-win/virtio-win_amd64.vfd**
- **/usr/share/rhev-guest-tools-iso/rhev-tools-setup.iso**

이러한 이미지 파일은 설치 프로세스에 의해 로컬로 생성되지 않은 ISO 스토리지 도메인에 수동으로 업로드해야 합니다. **engine-iso-uploader** 명령을 사용하여 이러한 이미지를 ISO 스토리지 도메인에 업로드합니다. 업로드한 후 이미지 파일은 가상 머신에 연결하여 사용할 수 있습니다.

IV 부. 환경 정보

19장. 로그 파일

19.1. RED HAT VIRTUALIZATION MANAGER 설치 로그 파일

표 19.1. 설치

로그 파일	설명
<code>/var/log/ovirt-engine/engine-cleanup-yyyy_mm_dd_hh_mm_ss.log</code>	engine-cleanup 명령에서의 로그입니다. 이는 Red Hat Virtualization Manager 설치를 재설정하는데 사용되는 명령입니다. 로그는 명령이 실행될 때 마다 생성됩니다. 파일 이름으로 실행 날짜와 시간이 사용되므로 동시에 여러 개의 로그가 가능합니다.
<code>/var/log/ovirt-engine/engine-db-install-yyyy_mm_dd_hh_mm_ss.log</code>	rhev 데이터 베이스 생성 및 설정을 자세히 설명하는 engine-setup 명령의 로그입니다.
<code>/var/log/ovirt-engine/ovirt-engine-dwh-setup-yyyy_mm_dd_hh_mm_ss.log</code>	ovirt-engine-dwh-setup 명령의 로그입니다. 보고 용 ovirt_engine_history 데이터베이스를 생성하기 위해 사용되는 명령입니다. 로그는 명령이 실행될 때 마다 생성됩니다. 파일 이름으로 실행 날짜와 시간이 사용되므로 동시에 여러 개의 로그가 가능합니다.
<code>/var/log/ovirt-engine/setup/ovirt-engine-setup-yyyymmddhhmmss.log</code>	engine-setup 명령에서의 로그입니다. 명령이 실행될 때 마다 로그가 생성됩니다. 파일 이름으로 실행 날짜와 시간이 사용되므로 동시에 여러 개의 로그가 가능합니다.

19.2. RED HAT VIRTUALIZATION MANAGER 로그 파일

표 19.2. 서비스 작업

로그 파일	설명
<code>/var/log/ovirt-engine/engine.log</code>	모든 Red Hat Virtualization Manager GUI 충돌, Active Directory 검색, 데이터 베이스 문제 및 기타 다른 이벤트 모두를 반영합니다.
<code>/var/log/ovirt-engine/host-deploy</code>	Red Hat Virtualization Manager에서 배포된 호스트의 로그 파일입니다.
<code>/var/lib/ovirt-engine/setup-history.txt</code>	Red Hat Virtualization Manager와 관련된 패키지 설치 및 업그레이드를 추적합니다.

로그 파일	설명
<code>/var/log/httpd/ovirt-requests-log</code>	<p>각 요청에 걸린 시간을 포함하여 HTTPS를 통해 Red Hat Virtualization Manager에 생성된 요청의 로그 파일입니다.</p> <p>로그 파일을 <code>/var/log/ovirt-engine/engine.log</code>와 비교할 때 요청을 비교할 수 있도록 Correlation-Id 헤더가 포함됩니다.</p>

19.3. SPICE 로그 파일

SPICE 로그 파일은 SPICE 연결 문제를 해결할 때 유용하게 사용될 수 있습니다. SPICE 디버깅을 시작하려면 로그 레벨을 **debugging**으로 변경한 후 로그 위치를 확인합니다.

게스트 시스템에 액세스하는 데 사용되는 클라이언트와 게스트 시스템 자체에는 모두 SPICE 로그 파일이 있습니다. 클라이언트측 로그를 보려면 네이티브 클라이언트를 사용하여 SPICE 클라이언트를 시작한 경우 **console.vv** 파일이 다운로드되고 **remote-viewer** 명령을 사용하여 디버깅을 활성화하고 로그 출력을 생성합니다.

19.3.1. 하이퍼바이저 SPICE 서버의 SPICE 로그

표 19.3. 하이퍼바이저 SPICE 서버의 SPICE 로그

로그 유형	로그 위치	로그 레벨을 변경하려면 다음을 실행합니다:
호스트/하이퍼바이저 SPICE 서버	<code>/var/log/libvirt/qemu/(guest_name).log</code>	게스트 시작 전에 호스트/하이퍼바이저에서 export SPICE_DEBUG_LEVEL=5 를 실행합니다. 이 변수는 QEMU에서 구문 분석되며 시스템 전체에서 실행되는 경우 시스템의 모든 가상 머신에 대한 디버깅 정보가 출력됩니다. 이 명령은 클러스터의 각 호스트에서 실행해야 합니다. 이 명령은 클러스터 기반이 아니라 호스트/하이퍼바이저 기반으로만 작동됩니다.

19.3.2. 게스트 머신의 SPICE 로그

표 19.4. 게스트 머신의 spice-vdagent 로그

로그 유형	로그 위치	로그 레벨을 변경하려면 다음을 실행합니다:
Windows 게스트	<code>C:\Windows\Temp\vdagent.log</code> <code>C:\Windows\Temp\vdservice.log</code>	해당 없음

로그 유형	로그 위치	로그 레벨을 변경하려면 다음을 실행합니다:
Red Hat Enterprise Linux 게스트	journalctl 을 root 사용자로 사용합니다.	<p>디버그 모드에서 spice- vdagentd 서비스를 실행하려면 root 사용자는 SPICE_VDAGENTD_EXTRA_ARGS="-d -d" 항목으로 /etc/sysconfig/spice- vdagentd 파일을 만듭니다.</p> <p>디버그 모드로 spice- vdagent를 실행하려면 명령행에서 다음 명령을 실행합니다:</p> <pre>\$ killall -u \$USER spice- vdagent \$ spice- vdagent -x - d [-d] [& tee spice- vdagent.log]</pre>

19.3.3. console.vv 파일을 사용하여 시작되는 SPICE 클라이언트의 SPICE 로그

Linux 클라이언트 시스템의 경우:

1. **remote-viewer** 명령을 **--spice-debug** 옵션과 함께 실행하여 SPICE 디버깅을 활성화합니다. 프롬프트가 나타나면 연결 URL을 (예: `spice://[virtual_machine_IP]:[port]`) 입력합니다.

```
# remote-viewer --spice-debug
```

2. 디버그 매개 변수를 사용하여 SPICE 클라이언트를 실행하고 .vv 파일을 전달하려면 **console.vv** 파일을 다운로드하고 **remote-viewer** 명령을 **--spice-debug** 옵션과 함께 실행한 다음 전체 경로를 **console.vv** 파일에 지정합니다.

```
# remote-viewer --spice-debug /path/to/console.vv
```

Windows 클라이언트 시스템의 경우:

1. **virt-viewer 2.0-11.el7ev** 이상의 버전에서 **virt-viewer.msi**는 **virt-viewer** 및 **debug-viewer.exe**를 설치합니다.
2. **remote-viewer** 명령을 **spice-debug** 인수와 함께 실행하고 명령의 경로를 콘솔로 지정합니다.

```
remote-viewer --spice-debug path\to\console.vv
```

3. 로그를 확인을 위해 가상 머신에 연결하면 GDB를 실행 중인 명령 프롬프트에서 **remote-viewer**의 표준 오류와 표준 출력이 표시됩니다.

19.4. RED HAT VIRTUALIZATION HOST 로그 파일

표 19.5.

로그 파일	설명
<code>/var/log/vdsm/libvirt.log</code>	libvirt 로그 파일입니다.
<code>/var/log/vdsm/spm-lock.log</code>	스토리지 풀 관리자 역할에 임대를 얻을 수 있는 호스트의 기능에 대한 상세 정보가 있는 로그 파일입니다. 로그에는 호스트 취득, 릴리즈, 갱신, 갱신 실패에 대한 로그 정보가 기록됩니다.
<code>/var/log/vdsm/vdsm.log</code>	VDSM 용 로그 파일로 가상 호스트에 있는 관리자 에이전트입니다.
<code>/tmp/ovirt-host-deploy-Date.log</code>	호스트가 성공적으로 배포된 후 <code>/var/log/ovirt-engine/host-deploy/ovirt-Date-Host-Correlation_ID.log</code> 로 Manager에 복사된 호스트 배포 로그입니다.
<code>/var/log/vdsm/import/import-UUID-Date.log</code>	가져오기 실패 정보를 비롯하여 KVM 호스트, VMWare 공급업체 또는 Xen 호스트에서의 가상 머신 가져오기를 상세히 설명하는 로그 파일입니다. UUID 는 가져온 가상 머신의 UUID이며 Date 는 가져오기가 시작된 날짜와 시간입니다.

19.5. 가상화 호스트 로깅 서버 설정

호스트는 호스트의 동작 및 문제를 기록하는 로그 파일을 생성 및 업데이트합니다. 이러한 로그 파일을 중앙 수집하면 디버깅을 단순화할 수 있습니다.

이러한 절차는 중앙 로그 서버에서 사용할 것을 권장합니다. 다른 로깅 서버를 사용하거나 이 절차를 사용하여 Red Hat Virtualization Manager에서 호스트 로깅을 활성화할 수 있습니다.

절차 19.1. 가상화 호스트 로깅 서버 설정

1. **rsyslog** 트래픽을 허용하기 위해 SELinux를 설정합니다.

```
# semanage port -a -t syslogd_port_t -p udp 514
```

2. 다음과 같은 행을 추가하여 `/etc/rsyslog.conf`를 편집합니다:

```
$template TmplAuth, "/var/log/%fromhost%/secure"
$template TmplMsg, "/var/log/%fromhost%/messages"

$RuleSet remote
authpriv.* ?TmplAuth
*.info,mail.none;authpriv.none,cron.none ?TmplMsg
$RuleSet RSYSLOG_DefaultRuleset
$InputUDPServerBindRuleset remote
```

다음 행을 주석 해제 처리합니다:

```
#$ModLoad imudp
#$UDPServerRun 514
```

3. rsyslog 서비스를 다시 시작합니다:

```
# systemctl restart rsyslog.service
```

가상화 호스트에서 **messages** 및 **secure** 로그를 수신 및 저장하도록 중앙 로그 서버가 설정됩니다.

20장. 프록시

20.1. SPICE 프록시

20.1.1. SPICE 프록시 개요

SPICE 프록시는 SPICE 클라이언트가 하이퍼바이저를 연결하는 네트워크의 외부에 있을 때 가상 머신에 SPICE 클라이언트를 연결하기 위해 사용되는 도구입니다. SPICE를 설정하려면 컴퓨터에 **Squid**를 설치하고 **iptables**를 설정하여 프록시 트래픽이 방화벽을 통과할 수 있게 합니다. SPICE 프록시를 사용하려면 Manager에서 **engine-config**를 사용하여 프록시 이름과 포트로 구성된 값으로 **SpiceProxyDefault** 키를 설정합니다. SPICE 프록시를 사용 해제하려면 Manager에서 **engine-config**를 사용하여 **SpiceProxyDefault**에 설정된 값을 삭제합니다.



중요

SPICE 프록시는 독립형 SPICE 클라이언트와 함께만 사용할 수 있으며 SPICE HTML5 또는 noVNC를 사용하여 가상 머신에 연결하는데 사용할 수 없습니다.

20.1.2. SPICE 프록시 설정

다음 부분에서는 SPICE 프록시로 시스템을 설정하는 방법에 대해 설명합니다. SPICE 프록시는 외부 네트워크에서 Red Hat Virtualization 네트워크에 연결할 수 있게 합니다. 이 부분에서는 **Squid**를 사용하여 프록시 서비스를 제공합니다.

절차 20.1. Red Hat Enterprise Linux에 Squid 설치

1. 프록시 시스템에 **Squid**를 설치하려면 다음을 실행합니다:

```
# yum install squid
```

2. **/etc/squid/squid.conf** 파일을 엽니다:

```
http_access deny CONNECT !SSL_ports
```

다음과 같이 변경합니다:

```
http_access deny CONNECT !Safe_ports
```

3. 프록시를 시작합니다:

```
# service squid start
```

4. 기본값 squid 포트를 엽니다:

```
# iptables -A INPUT -p tcp --dport 3128 -j ACCEPT
```

5. iptables 규칙을 영구적으로 설정합니다:

```
# service iptables save
```

SPICE 프록시로 시스템을 설정했습니다. 네트워크 외부에서 Red Hat Virtualization 네트워크로 연결하기 전 SPICE 프록시를 활성화합니다.

20.1.3. SPICE 프록시 활성화

다음 부분에서는 SPICE 프록시를 활성화하는 방법에 대해 설명합니다.

절차 20.2. SPICE 프록시 활성화

1. Manager에서 engine-config 도구를 사용하여 프록시를 설정합니다:

```
# engine-config -s SpiceProxyDefault=someProxy
```

2. **ovirt-engine** 서비스를 다시 시작합니다:

```
# service ovirt-engine restart
```

프록시는 다음과 같은 형식이어야 합니다:

```
protocol://[host]:[port]
```



참고

Red Hat Enterprise Linux 6.7, Red Hat Enterprise Linux 7.2, 또는 최신 지원 HTTPS 프록시에 탑재된 SPICE 클라이언트만 가능합니다. 이전 클라이언트는 HTTP만 지원합니다. 이전 클라이언트에 HTTPS가 지정되어 있을 경우 클라이언트는 프록시 설정을 무시하고 호스트에 직접 연결을 시도합니다.

SPICE 프록시가 활성화되었습니다. SPICE 프록시를 통해 Red Hat Virtualization 네트워크에 연결할 수 있습니다.

20.1.4. SPICE 프록시 비활성화

다음 부분에서는 SPICE 프록시를 비활성화하는 방법에 대해 설명합니다.

절차 20.3. SPICE 프록시 비활성화

1. Manager에 로그인합니다:

```
$ ssh root@[IP of Manager]
```

2. 다음 명령을 실행하여 SPICE 프록시를 삭제합니다:

```
# engine-config -s SpiceProxyDefault=""
```

3. Manager를 다시 시작합니다:

```
# service ovirt-engine restart
```

SPICE 프록시가 비활성화되었습니다. SPICE 프록시를 통해 Red Hat Virtualization 네트워크에 더 이상 연결할 수 없습니다.

20.2. SQUID 프록시

20.2.1. Squid 프록시 설치 및 설정

요약

다음 부분에서는 사용자 포털에서 Squid 프록시를 설치 및 설정하는 방법에 대해 설명합니다. Squid 프록시 서버는 콘텐츠 가속기로 사용됩니다. 이는 대역폭을 감소시키고 응답 시간을 개선하여 자주 확인되는 콘텐츠를 캐시합니다.

절차 20.4. Squid 프록시 설정

1. Squid 프록시 서버의 HTTPS 포트 용 키 쌍 및 인증서를 가져옵니다. 이러한 키 쌍은 다른 SSL/TLS 서비스의 키 쌍을 얻는 방법과 동일한 방법으로 획득할 수 있습니다. 키 쌍은 개인 키 및 서명된 인증서가 들어 있는 두 개의 PEM 파일 형식으로 되어 있습니다. 이러한 절차에서는 이러한 파일 이름이 **proxy.key** 및 **proxy.cer**라고 지정되어 있다고 전제합니다.



참고

키 쌍 및 인증서는 engine 인증 기관을 사용하여 생성될 수 있습니다. 프록시에 대해 개인키와 인증서가 있어 engine 인증 기관을 통해 이를 생성하지 않으려면 다음 단계를 생략합니다.

2. 프록시의 호스트 이름을 선택합니다. 그 후 프록시 용 고유의 인증서 이름의 다른 구성 요소를 선택합니다.



참고

engine 자체적으로 사용하는 것과 동일한 나라와 조직 이름을 사용하는 것이 좋습니다. Manager가 설치된 시스템에 로그인하고 다음과 같은 명령을 실행하여 정보를 찾을 수 있습니다:

```
# openssl x509 -in /etc/pki/ovirt-engine/ca.pem -noout -subject
```

이러한 명령의 출력 결과는 다음과 같습니다:

```
subject= /C=US/O=Example Inc./CN=engine.example.com.81108
```

여기서 관련된 부분은 **/C=US/O=Example Inc.**입니다. 이를 사용하여 프록시 인증서의 고유한 이름을 작성합니다:

```
/C=US/O=Example Inc./CN=proxy.example.com
```

3. 프록시 시스템에 로그인하고 인증서 서명 요청을 생성합니다:

```
# openssl req -newkey rsa:2048 -subj '/C=US/O=Example Inc./CN=proxy.example.com' -nodes -keyout proxy.key -out proxy.req
```



중요

인용 부호를 사용하여 인증서 이름을 구별합니다. **-nodes** 옵션으로 개인키가 암호화되지 않도록합니다. 이는 프록시 서버를 시작할 때 암호를 입력할 필요가 없음을 의미합니다.

이 명령은 **proxy.key** 및 **proxy.req**라는 두 개의 파일을 생성합니다. **proxy.key**는 개인키입니다. 이 파일을 안전한 장소에 보관합니다. **proxy.req**는 인증서 서명 요청 파일입니다. **proxy.req**에는 특별한 보안이 필요하지 않습니다.

- 서명된 인증서를 생성하려면 프록시 시스템에서 Manager 시스템으로 인증서 서명 요청 파일을 복사합니다:

```
# scp proxy.req engine.example.com:/etc/pki/ovirt-engine/requests/.
```

- Manager 시스템에 로그인하고 인증서에 서명합니다:

```
# /usr/share/ovirt-engine/bin/pki-enroll-request.sh --name=proxy --days=3650 --subject='/C=US/O=Example Inc./CN=proxy.example.com'
```

이는 인증서를 서명하고 10년 (3650일) 동안 사용할 수 있습니다. 필요에 따라 인증서 만료 기간을 짧게 설정할 수 있습니다.

- 생성된 인증서 파일은 **/etc/pki/ovirt-engine/certs** 디렉토리에서 사용할 수 있으며 **proxy.cer**라고 이름을 지정해야 합니다. 프록시 시스템에 있는 Manager 시스템에서 현재 디렉토리로 이 파일을 복사합니다:

```
# scp engine.example.com:/etc/pki/ovirt-engine/certs/proxy.cer .
```

- 프록시 시스템에 **proxy.key** 및 **proxy.cer** 모두가 표시되는지 확인합니다:

```
# ls -l proxy.key proxy.cer
```

- 프록시 머신에 Squid 프록시 서버 패키지를 설치합니다:

```
# yum install squid
```

- 개인키 및 서명된 인증서를 **/etc/squid** 디렉토리와 같이 프록시가 액세스할 수 있는 위치로 옮깁니다:

```
# cp proxy.key proxy.cer /etc/squid/.
```

- squid** 사용자가 이러한 파일을 읽을 수 있도록 권한을 설정합니다:

```
# chgrp squid /etc/squid/proxy.*
# chmod 640 /etc/squid/proxy.*
```

- Squid 프록시는 engine에 의해 사용되는 인증서를 확인합니다. Manager 인증서를 프록시 시스템에 복사합니다. 다음 예에서는 **/etc/squid** 파일 경로를 사용합니다:

```
# scp engine.example.com:/etc/pki/ovirt-engine/ca.pem /etc/squid/.
```



참고

기본값 CA 인증서는 Manager 시스템 상의 `/etc/pki/ovirt-engine/ca.pem`에 위치합니다.

12. **squid** 사용자가 인증서 파일을 읽을 수 있도록 권한을 설정합니다:

```
# chgrp squid /etc/squid/ca.pem
# chmod 640 /etc/squid/ca.pem
```

13. SELinux가 강제 적용 모드일 경우 Squid가 포트 443을 사용할 수 있도록 허용하기 위해 **semanage** 도구를 사용하여 포트 443의 컨텍스트를 변경합니다:

```
# yum install polycoreutils-python
# semanage port -m -p tcp -t http_cache_port_t 443
```

14. 기존 Squid 설정 파일을 다음으로 대체합니다:

```
https_port 443 key=/etc/squid/proxy.key cert=/etc/squid/proxy.cer
ssl-bump defaultsite=engine.example.com
cache_peer engine.example.com parent 443 0 no-query originserver ssl
sslcafile=/etc/squid/ca.pem name=engine
cache_peer_access engine allow all
ssl_bump allow all
http_access allow all
```

15. Squid 프록시 서버를 다시 시작합니다:

```
# systemctl restart squid.service
```

16. 전체 URL을 사용하여 사용자 포털에 연결합니다. 예:

```
https://proxy.example.com/UserPortal/org.ovirt.engine.ui.userportal.
UserPortal/UserPortal.html
```



참고

`https://proxy.example.com/UserPortal`과 같이 짧은 형식의 URL은 작동하지 않습니다. 이러한 짧은 형식의 URL은 302 응답 코드와 위치 헤더를 사용하여 애플리케이션 서버에서 긴 형식의 URL로 리디렉션됩니다. Red Hat Enterprise Linux에서 **Squid** 버전은 이러한 헤더를 다시 작성하는 것을 지원하지 않습니다.



참고

기본 설정에서 Squid 프록시는 15 분 대기 상태 후 연결을 종료합니다. Squid 프록시가 연결 대기 상태를 종료하기 전 대기 시간을 늘리려면 `squid.conf`에 있는 `read_timeout` 옵션을 조정합니다 (예: `read_timeout 10 hours`).

20.3. WEBSOCKET 프록시

20.3.1. Websocket 프록시 개요

websocket 프록시를 사용해서 noVNC 및 SPICE HTML5 콘솔을 통해 가상 머신에 연결할 수 있습니다. 이전에 websocket 프록시는 Red Hat Virtualization Manager 시스템에서만 실행할 수 있었지만 이제는 네트워크에 액세스할 수 있는 모든 시스템에서 해당 프록시를 실행할 수 있습니다.

초기 설정 과정에서 Websocket 프록시를 Red Hat Virtualization Manager 시스템에 설치 및 설정하거나 (설치 가이드에 있는 [Red Hat Virtualization Manager 설정 참조](#)) 별도의 시스템에 설치 및 설정할 수 있습니다(설치 가이드에 있는 [별도의 시스템에 Websocket 프록시 설치 참조](#)).

websocket 프록시를 Manager 시스템에서 다른 시스템으로 마이그레이션할 수 있습니다. [20.3.2절. “다른 시스템으로 Websocket 프록시 마이그레이션”](#)에서 참조하십시오.



참고

SPICE HTML5 지원은 기술 프리뷰 기능입니다. 기술 프리뷰 기능은 Red Hat 서브스크립션 서비스 수준 계약 (SLA: Subscription Service Level Agreement)에서 완전 지원되지 않으며 기능이 완전하게 작동하지 않을 수 있고 프로덕션 환경에서의 사용을 목적으로 하지 않습니다. 하지만 이러한 기능을 통해 예정된 제품 기능을 미리 사용해 볼 수 있으므로 고객은 개발 과정에서 기능을 테스트하고 피드백을 보낼 수 있습니다.

20.3.2. 다른 시스템으로 Websocket 프록시 마이그레이션

보안과 성능을 위해 Red Hat Virtualization Manager를 실행하지 않는 다른 시스템에 websocket 프록시를 실행할 수 있습니다. Manager 시스템에서 다른 시스템으로 websocket 프록시를 마이그레이션하는 이 절차를 통해 Manager 시스템에서 websocket 프록시 설정을 삭제한 후 다른 시스템에 해당 프록시를 설치합니다.

engine-cleanup 명령을 사용하여 Manager 시스템에서 websocket 프록시를 제거합니다.

절차 20.5. 다른 시스템으로 Websocket 프록시 마이그레이션

1. Manager 시스템에서 **engine-cleanup** 명령을 실행해서 관련 설정을 제거합니다.

```
# engine-cleanup
```

2. 모든 구성 요소 제거 여부를 묻으면 **No**를 입력하고 **Enter**를 누릅니다.

```
Do you want to remove all components? (Yes, No) [Yes]: No
```

3. engine 제거 여부를 묻으면 **No**를 입력하고 **Enter**를 누릅니다.

```
Do you want to remove the engine? (Yes, No) [Yes]: No
```

4. websocket 프록시 제거 여부를 묻으면 **Yes**를 입력하고 **Enter**를 누릅니다.

```
Do you want to remove the WebSocket proxy? (Yes, No) [No]: Yes
```

다른 구성 요소 제거 여부를 묻으면 **No**를 선택합니다.

5. 프록시를 별도의 시스템에 설치 및 설정합니다. 자세한 내용은 [설치 가이드에 있는 별도의 시스템에 Websocket 프록시 설치](#)를 참조하십시오.

부록 A. VDSM 및 후크

A.1. VDSM

VDSM 서비스는 Red Hat Virtualization Host (RHVH) 및 Red Hat Enterprise Linux 호스트를 관리하기 위해 Red Hat Virtualization Manager에 의해 사용됩니다. VDSM은 호스트의 스토리지, 메모리, 네트워크 리소스를 관리 및 모니터링합니다. 또한 가상 머신 생성, 통계 수집, 로그 수집, 기타 호스트 관리 작업을 수행합니다. VDSM은 Red Hat Virtualization Manager에 의해 관리되는 각각의 호스트에서 데몬으로 실행됩니다. 이는 클라이언트에서 XML-RPC 호출에 응답합니다. Red Hat Virtualization Manager는 VDSM 클라이언트처럼 기능합니다.

A.2. VDSM 후크

VDSM은 후크를 통해 확장 가능합니다. 후크는 중요 이벤트가 발생했을 때 호스트에서 실행되는 스크립트입니다. 지원되는 이벤트 발생 시 VDSM은 영숫자 순서로 호스트에서 `/usr/libexec/vdsm/hooks/nn_event-name/`에 있는 실행 가능한 후크 스크립트를 실행합니다. 규칙에 따라 각 후크 스크립트는 파일 이름이 앞에 포함된 두 자리 숫자로 할당되어 스크립트가 실행되는 순서를 명확히 합니다. 프로그래밍 언어로 후크 스크립트를 생성할 수 있지만 다음의 예에서는 Python을 사용하고 있습니다.

이벤트에 대해 호스트에서 정의된 모든 스크립트가 실행된다는 점에 유의합니다. 호스트에서 실행되는 가상 머신의 일부분에 대해 지정된 후크만 실행해야 할 경우 후크 스크립트 자체가 가상 머신에 연결된 사용자 정의 속성을 평가하여 이러한 요구사항을 처리하는지 확인해야 합니다.



주의

VDSM 후크는 Red Hat Virtualization 작동을 방해할 수 있습니다. VDSM 후크에 있는 버그는 가상 머신 중지 및 데이터 손상의 원인이 될 수 있습니다. VDSM 후크는 신중하고 엄격하게 테스트해야 합니다. 후크 API는 새로운 기능으로 차후에 변경될 수 있습니다.

A.3. 후크로 VDSM 확장

다음 부분에서는 이벤트 구동 방식의 후크로 VDSM을 확장하는 방법에 대해 설명합니다. 후크로 VDSM을 확장하는 것은 실험적인 기술로 이는 숙련된 개발자를 위한 것입니다. 가상 머신에 사용자 등록 정보를 설정하여 (지정된 가상 머신 고유의) 추가 매개 변수를 후크 스크립트에 전달할 수 있습니다.

A.4. 지원되는 VDSM 이벤트

표 A.1. 지원되는 VDSM 이벤트

이름	설명
before_vm_start	가상 머신 시작하기 전
after_vm_start	가상 머신을 시작한 후

이름	설명
before_vm_cont	가상 머신을 계속 실행하기 전
after_vm_cont	가상 머신을 계속 실행한 후
before_vm_pause	가상 머신 일시 정지 전
after_vm_pause	가상 머신 일시 정지 후
before_vm_hibernate	가상 머신 최대 절전 모드 사용 전
after_vm_hibernate	가상 머신 최대 절전 모드 사용 후
before_vm_dehibernate	가상 머신 최대 절전 모드 해제 전
after_vm_dehibernate	가상 머신 최대 절전 모드 해제 후
before_vm_migrate_source	가상 머신 마이그레이션 전 마이그레이션이 진행되는 소스 호스트에서 실행합니다.
after_vm_migrate_source	가상 머신 마이그레이션 후 마이그레이션이 진행되는 소스 호스트에서 실행합니다.
before_vm_migrate_destination	가상 머신 마이그레이션 전 마이그레이션이 진행되는 대상 호스트에서 실행합니다.
after_vm_migrate_destination	가상 머신 마이그레이션 후 마이그레이션이 진행되는 대상 호스트에서 실행합니다.
after_vm_destroy	가상 머신 파괴 후
before_vdsm_start	VDSM이 호스트에서 시작되기 전입니다. before_vdsm_start 후크는 root 사용자로 실행되며 VDSM 프로세스 환경을 상속하지 않습니다.
after_vdsm_stop	VDSM이 호스트에서 중지된 후입니다. after_vdsm_stop 후크는 root 사용자로 실행되며 VDSM 프로세스 환경을 상속하지 않습니다.
before_nic_hotplug	NIC가 가상 머신으로 핫플러그되기 전입니다.
after_nic_hotplug	NIC가 가상 머신으로 핫 플러그된 후입니다.
before_nic_hotunplug	NIC가 가상 머신에서 핫언플러그되기 전입니다.
after_nic_hotunplug	NIC가 가상 머신에서 핫 언플러그된 후입니다.

이름	설명
after_nic_hotplug_fail	NIC를 가상 머신으로 핫 플러그 실패한 후입니다.
after_nic_hotunplug_fail	NIC를 가상 머신에서 핫언플러그 실패한 후입니다.
before_disk_hotplug	디스크가 가상 머신으로 핫플러그되기 전입니다.
after_disk_hotplug	디스크가 가상 머신으로 핫플러그된 후입니다.
before_disk_hotunplug	디스크가 가상 머신에서 핫언플러그되기 전입니다.
after_disk_hotunplug	디스크가 가상 머신에서 핫 언플러그된 후입니다.
after_disk_hotplug_fail	가상 머신으로 디스크를 핫플러그 실패한 후입니다.
after_disk_hotunplug_fail	가상 머신에서 디스크를 핫 언플러그 실패 후입니다.
before_device_create	사용자 정의 속성을 지원하는 장치 생성 전입니다.
after_device_create	사용자 정의 속성을 지원하는 장치 생성 후입니다.
before_update_device	사용자 정의 속성을 지원하는 장치 업데이트 전입니다.
after_update_device	사용자 정의 속성을 지원하는 장치 업데이트 후입니다.
before_device_destroy	사용자 정의 속성을 지원하는 장치 삭제 전입니다.
after_device_destroy	사용자 정의 속성을 지원하는 장치 삭제 후입니다.
before_device_migrate_destination	장치 마이그레이션 전 마이그레이션이 진행되고 있는 대상 호스트에서 실행합니다.
after_device_migrate_destination	장치 마이그레이션 후 마이그레이션이 진행되고 있는 대상 호스트에서 실행합니다.
before_device_migrate_source	장치 마이그레이션 전 마이그레이션이 진행되고 있는 소스 호스트에서 실행합니다.
after_device_migrate_source	장치 마이그레이션 후 마이그레이션이 진행되고 있는 소스 호스트에서 실행합니다.
after_network_setup	호스트 시스템 시작 시 네트워크를 설정한 후입니다.
before_network_setup	호스트 시스템 시작 시 네트워크를 설정하기 전입니다.

A.5. VDSM 후크 환경

대부분의 후크 스크립트는 **vds**m 사용자로 실행되고 VDSM 프로세스 환경을 상속합니다.

before_vdsm_start 및 **after_vdsm_stop** 이벤트에 의해 트리거된 후크 스크립트는 예외입니다. 이러한 이벤트에 의해 트리거된 후크 스크립트는 **root** 사용자로 실행되며 VDSM 프로세스의 환경을 상속하지 않습니다.

A.6. VDSM 후크 도메인 XML 개체

후크 스크립트 시작 시 **_hook_domxml** 변수가 환경에 추가됩니다. 이러한 변수에는 관련 가상 머신의 libvirt 도메인 XML 표현식 경로가 포함되어 있습니다. 아래에 설명되어 있듯이 일부 후크는 이러한 규칙에 예외가 됩니다.

다음 후크의 **_hook_domxml** 변수에는 가상 머신이 아닌 NIC의 XML 표현이 포함되어 있습니다.

- ***_nic_hotplug_***
- ***_nic_hotunplug_***
- ***_update_device**
- ***_device_create**
- ***_device_migrate_***



중요

before_migration_destination 및 **before_dehibernation** 후크는 현재 소스 호스트에서 도메인의 XML을 수신합니다. 대상 도메인의 XML은 다양한 차이가 있습니다.

VDSM은 libvirt 도메인 XML인 형식을 사용하여 가상 머신을 정의합니다. libvirt 도메인 XML 형식에 대한 보다 자세한 내용은 <http://libvirt.org/formatdomain.html>에서 확인하실 수 있습니다. 가상 머신의 UUID는 XML 도메인에서 확인할 수 있지만 환경 변수 **vmId**로 사용할 수 있습니다.

A.7. 사용자 정의 속성 정의

Red Hat Virtualization Manager에 의해 허용되어 사용자 정의 후크에 차례로 전달되는 사용자 정의 속성은 **engine-config** 명령을 사용하여 정의합니다. Red Hat Virtualization Manager가 설치된 호스트에서 **root** 사용자로 이 명령을 실행합니다.

UserDefinedVMProperties 및 **CustomDeviceProperties** 설정 키는 사용자 정의 속성 정보 이름을 저장하는데 사용됩니다. 각 이름이 지정된 사용자 정의 속성의 유효한 값을 정의하는 정규 표현식도 이러한 설정 키에 포함되어 있습니다.

여러 사용자 정의 속성은 세미 콜론에 의해 구분됩니다. 설정 키 설정 시 기존 값은 덮어 쓰기됨에 유의합니다. 새로운 속성 및 기존 사용자 정의 속성을 조합 시 키 값 설정에 사용되는 명령에 있는 모든 사용자 정의 속성을 입력해야 합니다.

설정 키를 업데이트한 후 새 값을 적용하려면 **ovirt-engine** 서비스를 다시 시작해야 합니다.

예 A.1. 가상 머신 속성 - *smartcard* 사용자정의 속성 정의

1. 다음 명령을 사용하여 **UserDefinedVMProperties** 설정 키로 정의된 기존 사용자 정의 속성을 확인합니다:

```
# engine-config -g UserDefinedVMProperties
```

아래의 출력 결과에서 볼 수 있듯이 사용자 정의 속성 **memory**는 이미 정의되어 있습니다. 정규 표현식 **^[0-9]+\$**은 사용자 정의 속성에 숫자만 포함되도록 되어 있는지를 확인합니다.

```
# engine-config -g UserDefinedVMProperties
UserDefinedVMProperties: version: 3.6
UserDefinedVMProperties: version: 4.0
UserDefinedVMProperties : memory=^[0-9]+$ version: 4.0
```

2. **메모리** 사용자 정의 속성은 **UserDefinedVMProperties** 설정키에 이미 정의되어 있으며 새 사용자 정의 속성은 이곳에 추가해야 합니다. 추가 사용자 정의 속성, **smartcard**는 설정 키 값에 추가됩니다. 새 사용자 정의 속성에는 **true** 또는 **false** 값을 지정할 수 있습니다.

```
# engine-config -s UserDefinedVMProperties='memory=^[0-9]+$;smartcard=^(true|false)$' --cver=4.0
```

3. **UserDefinedVMProperties** 설정 키에 의해 정의된 사용자 정의 속성이 올바르게 업데이트되어 있는지를 확인합니다.

```
# engine-config -g UserDefinedVMProperties
UserDefinedVMProperties: version: 3.6
UserDefinedVMProperties: version: 4.0
UserDefinedVMProperties : memory=^[0-9]+$;smartcard=^(true|false)$
version: 4.0
```

4. 마지막으로 **ovirt-engine** 서비스를 다시 시작하여 설정 변경 사항을 적용합니다.

```
# systemctl restart ovirt-engine.service
```

예 A.2. 장치 속성 - **interface** 사용자 정의 속성 정의

1. 다음 명령을 사용하여 **CustomDeviceProperties** 설정 키에 의해 정의되는 기존 사용자 정의 속성을 확인합니다:

```
# engine-config -g CustomDeviceProperties
```

다음 출력값에서 볼 수 있듯이 사용자 정의 속성은 아직 정의되어 있지 않습니다.

```
# engine-config -g CustomDeviceProperties
CustomDeviceProperties: version: 3.6
CustomDeviceProperties: version: 4.0
```

2. **interface** 사용자 정의 속성이 존재하지 않기 때문에 그대로 추가될 수 있습니다. 다음 예에서 **speed** 하위 속성 값은 0에서 99999 사이의 범위로 설정하고 **duplex** 하위 속성 값은 **full** 또는 **half** 중 하나를 선택하여 설정합니다.

```
# engine-config -s CustomDeviceProperties="{type=interface;prop={speed=^[0-9]{1,5}$;duplex=^(full|half)$}}" --cver=4.0
```

3. **CustomDeviceProperties** 설정 키에 의해 정의된 사용자 정의 속성이 올바르게 업데이트 되어 있는지를 확인합니다.

```
# engine-config -g CustomDeviceProperties
UserDefinedVMProperties: version: 3.6
UserDefinedVMProperties: version: 4.0
UserDefinedVMProperties : {type=interface;prop={speed=^([0-9]{1,5})$;duplex=^(full|half)$} version: 4.0
```

4. 마지막으로 **ovirt-engine** 서비스를 다시 시작하여 설정 변경 사항을 적용합니다.

```
# systemctl restart ovirt-engine.service
```

A.8. 가상 머신 사용자 정의 속성 설정

Red Hat Virtualization Manager에서 사용자 정의 속성을 지정한 후 가상 머신에 이를 설정할 수 있습니다. 사용자 정의 속성은 관리 포털에서 새 가상 머신 및 가상 머신 편집 창의 사용자 정의 속성 탭에서 설정합니다.

또한 가상 머신 실행 대화 상자에서 사용자 정의 속성을 설정할 수 있습니다. 가상 머신 실행 대화 상자에서 사용자 정의 속성을 설정하면 가상 머신이 종료되기 전 까지만 적용됩니다.

사용자 정의 속성 탭에서는 지정된 사용자 정의 속성 목록에서 선택할 수 있는 기능을 제공합니다. 사용자 정의 속성 키를 선택하면 키 값을 입력할 수 있는 추가 필드가 표시됩니다. + 버튼을 클릭하여 키 쌍 값을 추가하고 - 버튼을 클릭하여 제거합니다.

A.9. VDSM 후크에서 가상 머신 사용자 정의 속성 평가

가상 머신의 사용자 정의 속성 필드에 있는 각각의 키 설정은 후크 스크립트를 호출할 때 환경 변수로 추가됩니다. 사용자 정의 속성 필드를 검증하기 위해 사용되는 정규 표현식은 일부 보안을 제공하지만 스크립트가 제공하는 입력이 올바른지 확인해야 합니다.

예 A.3. 사용자 정의 속성 평가

다음에는 사용자 정의 속성 **key1**의 존재를 확인하기 위한 간단한 Python 예입니다. 사용자 정의 속성이 설정되어 있을 경우에 값은 표준 오류에 출력됩니다. 사용자 정의 속성이 설정되어 있지 않을 경우 아무 동작도 하지 않게 됩니다.

```
#!/usr/bin/python

import os
import sys

if os.environ.has_key('key1'):
    sys.stderr.write('key1 value was : %s\n' % os.environ['key1'])
else:
    sys.exit(0)
```

A.10. VDSM 후킹 모듈 사용

VDSM은 Python 후킹 모듈과 함께 제공되며 VDSM 후크 스크립트의 도움말 기능을 제공합니다. 이 모듈은 예제로 제공되며 Python에 작성된 VDSM 후크에만 관련됩니다.

후킹 모듈은 가상 머신의 libvirt XML을 DOM 개체로 읽기를 지원합니다. 후크 스크립트는 Python의 내장 `xml.dom` 라이브러리 (<http://docs.python.org/release/2.6/library/xml.dom.html>)를 사용하여 개체를 조작할 수 있습니다.

수정된 개체는 후킹 모듈을 사용하여 libvirt XML에 다시 저장할 수 있습니다. 후킹 모듈은 후크 개발을 지원하기 위해 다음과 같은 함수를 제공합니다:

표 A.2. 후킹 모듈 함수

이름	인수	설명
<code>tobool</code>	문자열	문자열 "true" 또는 "false"를 부울 값으로 변환합니다
<code>read_domxml</code>	-	가상 머신의 libvirt XML을 DOM 개체로 읽습니다
<code>write_domxml</code>	DOM 개체	DOM 개체에서 가상 머신의 libvirt XML를 씁니다

A.11. VDSM 후크 실행

`before_vm_start` 스크립트는 도메인 XML을 편집하여 libvirt에 도달하기 전 가상 머신의 VDSM 정의를 변경할 수 있습니다. 이러한 과정을 실행할 때 주의해야 합니다. 후크 스크립트는 VDSM의 동작을 방해할 수 있으며 버그 스크립트로 인해 Red Hat Virtualization 환경이 중단될 수 있습니다. 특히 도메인의 UUID를 변경해서는 안되며 충분한 배경 지식 없이 도메인에서 장치를 삭제해서는 안됩니다.

`before_vdsm_start` 및 `after_vdsm_stop` 후크 스크립트 모두 `root` 사용자로 실행됩니다. 시스템에 `root` 액세스가 필요한 다른 후크 스크립트는 권한 에스컬레이션을 위해 `sudo` 명령을 사용하도록 작성해야 합니다. 이를 지원하려면 `/etc/sudoers`를 업데이트하여 `vdsm` 사용자가 암호를 다시 입력하지 않고 `sudo`를 사용할 수 있게 합니다. 후크 스크립트는 대화형이 아닌 방식으로 실행되므로 이러한 설정이 필요합니다.

예 A.4. VDSM 후크에 sudo 설정

다음 예에서는 `vdsm` 사용자가 `root`로 `/bin/chown` 명령을 실행하기 위해 `sudo` 명령을 설정합니다.

1. `root`로 가상화 호스트에 로그인합니다.
2. 텍스트 편집기에서 `/etc/sudoers` 파일을 엽니다.
3. 파일에 다음 행을 추가합니다:

```
vdsm ALL=(ALL) NOPASSWD: /bin/chown
```

이는 `vdsm` 사용자가 `root` 사용자로 `/bin/chown` 명령을 실행할 수 있는 기능을 지정합니다. `NOPASSWD` 매개 변수를 사용하여 `sudo` 호출 시 사용자에게 암호를 입력하라는 메시지가 나타나지 않도록 합니다.

설정이 변경되면 VDSM 후크는 `sudo` 명령을 사용하여 `root`로 `/bin/chown`을 사용할 수 있게 됩니다. Python 코드는 `sudo`를 사용하여 파일 `/my_file`에서 `root`로 `/bin/chown`을 실행합니다.

```
retcode = subprocess.call( ["/usr/bin/sudo", "/bin/chown", "root",
"/my_file"] )
```

후크 스크립트의 표준 오류 스트림은 VDSM 로그에서 수집됩니다. 이러한 정보는 후크 스크립트를 디버깅하는데 사용됩니다.

A.12. VDSM 후크 반환 코드

후크 스크립트는 표 A.3. “후크 반환 코드”에 있는 반환 코드 중 하나를 반환해야 합니다. 반환 코드는 VDSM로 다른 후크 스크립트를 처리할 지에 대한 여부를 지정합니다.

표 A.3. 후크 반환 코드

코드	설명
0	후크 스크립트가 성공적으로 종료되었습니다
1	후크 스크립트가 실패했습니다. 다른 후크를 처리해야 합니다
2	후크 스크립트가 실패했습니다. 다른 후크를 처리할 수 없습니다.
>2	예약됨

A.13. VDSM 후크 예

이 부분에서 지정된 후크 스크립트 예는 Red Hat에서 완전 지원되지 않습니다. 소스에 관계없이 시스템에 설치한 모든 후크 스크립트를 환경에서 완전히 테스트해야 합니다.

예 A.5. NUMA 노드 튜닝

목적:

이러한 후크 스크립트를 사용하여 **numaset** 사용자 정의 속성에 기반하는 NUMA 호스트에서 메모리 할당을 조정합니다. 사용자 정의 속성이 설정되어 있지 않은 경우 동작하지 않게 됩니다.

설정 문자열:

```
numaset=^(interleave|strict|preferred):[\^]?\d+(-\d+)?(,[\^]?\d+(-\d+)?)*$
```

정규 표현식을 사용하여 지정된 가상 머신의 **numaset** 사용자 정의 속성을 통해 할당 모드 (**interleave**, **strict**, **preferred**) 및 사용할 노드 모두를 지정할 수 있습니다. 두 값은 콜론 (:)으로 구분됩니다. 정규 표현식을 통해 다음과 같이 **nodeset** 사양을 지정할 수 있습니다:

- 특정 노드 (**numaset=strict:1**, 노드 1만 사용하도록 지정)
- 사용할 노드 범위 (**numaset=strict:1-4**, 노드 1에서 4 까지 사용하도록 지정)
- 사용하지 않을 특정 노드 (**numaset=strict:^3**, 노드 3을 사용하지 않도록 지정)

- 위의 사양을 콤마로 구분하여 조합 (**numaset=strict:1-4,6**, 노드 1에서 4 그리고 6을 사용하도록 지정)

스크립트:

/usr/libexec/vdsm/hooks/before_vm_start/50_numa

```
#!/usr/bin/python

import os
import sys
import hooking
import traceback

...

numa hook
=====
add numa support for domain xml:

<numatune>
  <memory mode="strict" nodeset="1-4,^3" />
</numatune>

memory=interleave|strict|preferred

numaset="1" (use one NUMA node)
numaset="1-4" (use 1-4 NUMA nodes)
numaset="^3" (don't use NUMA node 3)
numaset="1-4,^3,6" (or combinations)

syntax:
  numa=strict:1-4
  ...

if os.environ.has_key('numa'):
    try:
        mode, nodeset = os.environ['numa'].split(':')

        domxml = hooking.read_domxml()

        domain = domxml.getElementsByTagName('domain')[0]
        numas = domxml.getElementsByTagName('numatune')

        if not len(numas) > 0:
            numatune = domxml.createElement('numatune')
            domain.appendChild(numatune)

            memory = domxml.createElement('memory')
            memory.setAttribute('mode', mode)
            memory.setAttribute('nodeset', nodeset)
            numatune.appendChild(memory)

            hooking.write_domxml(domxml)
        else:
            sys.stderr.write('numa: numa already exists in domain xml')
            sys.exit(2)
    except:
```

```
sys.stderr.write('numa: [unexpected error]: %s\n' %  
traceback.format_exc())  
sys.exit(2)
```

부록 B. 사용자 정의 네트워크 속성

B.1. BRIDGE_OPTS 매개 변수

표 B.1. bridge_opts 매개 변수

매개 변수	설명
forward_delay	브리지가 리스닝(listening) 및 러닝(learning) 상태에 있는 시간을 0.1초 단위로 설정합니다. 이렇게 설정된 시간 내로 스위치 루프(switching loop)가 발견되지 않는 경우 브리지는 포워딩(forwarding) 상태가 됩니다. 그 결과 네트워크가 정상적으로 작동하기 전에 트래픽 및 네트워크 레이아웃을 확인할 수 있는 시간이 있습니다.
gc_timer	가비지(garbage) 수집 시간을 0.1초 단위로 설정해서 이 시간이 지나면 포워딩 데이터베이스를 확인하고 시간이 초과된 항목을 삭제합니다.
group_addr	일반적인 쿼리를 보낼 때 제로로 설정합니다. 특정 그룹 또는 그룹과 소스 관련 쿼리를 보낼 때 IP 멀티캐스트 주소로 설정합니다.
group_fwd_mask	브리지가 로컬 그룹 주소를 포워드 링크(forward link)할 수 있게 합니다. 기본값을 변경 시 비표준(non-standard) 브리징 동작이 허용됩니다.
hash_elasticity	해시(hash) 테이블 상에서 허용되는 최대 체인의 길이입니다. 이 값은 새로운 멀티캐스트 그룹이 추가되기 전까지는 적용되지 않습니다. 리해쉬 후 해당 값이 충족되지 않는 경우 해시 충돌이 발생하고 스누핑(snooping)이 비활성화됩니다.
hash_max	해시(hash) 테이블에서 허용되는 최대 버킷(bucket) 수량입니다. 설정 시 즉시 적용되며 현재 멀티캐스트 그룹 항목의 수보다 작은 값으로 설정할 수 없습니다. 이 값은 2의 거듭제곱이어야 합니다.
hello_time	네트워크 토폴로지(topology)에서 브리지 위치를 알리는 'hello' 메시지를 전송하는 시간 간격을 0.1초 단위로 설정합니다. 브리지가 Spanning Tree root 브리지인 경우에만 해당됩니다.
hello_timer	마지막 'hello' 메시지 전송 후 경과 시간을 0.1초 단위로 표시합니다.
max_age	0.1초 단위로 시간을 설정해서 다른 root 브리지로부터 마지막으로 'hello' 메시지를 받은 후 설정 시간이 지나면 해당 브리지가 정지된 것으로 간주하며 테이크오버(takeover)가 시작됩니다.

매개 변수	설명
multicast_last_member_count	호스트에서 'leave group' 메시지를 받은 후 멀티캐스트 그룹으로 보낸 'last member' 쿼리의 수를 설정합니다.
multicast_last_member_interval	'last member' 쿼리 간의 시간을 0.1초 단위로 설정합니다.
multicast_membership_interval	브릿지가 멀티캐스트 그룹 멤버의 통신을 기다리는 시간을 0.1초 단위로 설정해서 이 설정 시간이 지나면 브릿지는 호스트에 멀티캐스트 트래픽을 더 이상 보내지 않습니다.
multicast_querier	브릿지가 적극적으로 멀티캐스트 쿼리어(querier)를 실행하는지 여부를 설정합니다. 브릿지가 다른 네트워크 호스트로부터 'multicast host membership' 쿼리를 받은 경우 해당 호스트는 쿼리를 받은 시간에 멀티캐스트 쿼리 시간 간격을 더해서 추적됩니다. 나중에 브릿지가 이 멀티캐스트 멤버십의 트래픽을 포워딩하려고 시도하거나 쿼리를 보내는 멀티캐스트 라우터와 통신하는 경우 이러한 타이머가 해당 쿼리어가 유효한지 확인합니다. 유효한 경우 멀티캐스트 트래픽이 브릿지의 기존 멀티캐스트 멤버십 테이블을 통해서 전송됩니다. 더 이상 유효하지 않은 경우 트래픽이 모든 브리지 포트를 통해서 전송됩니다. 멀티캐스트 멤버십이 있거나 예상되는 브로드캐스트(broadcast) 도메인은 성능 향상을 위해서 하나 이상의 멀티캐스트 쿼리어를 실행하는 것이 좋습니다.
multicast_querier_interval	호스트로부터 'multicast host membership' 쿼리를 수신한 후에 그 호스트가 유효한지를 확인할 때까지의 최대 시간을 0.1초 단위로 설정합니다.
multicast_query_use_ifaddr	Boolean. 기본값인 '0'으로 설정되며, 이때 쿼리어가 0.0.0.0을 IPv4 메시지의 소스 주소로 사용합니다. 이 값을 변경하면 브리지 IP가 소스 주소로 설정됩니다.
multicast_query_interval	멀티캐스트 멤버십이 유효한지 확인할 수 있도록 브리지에서 전송된 쿼리 메시지 간의 시간 간격을 0.1초 단위로 설정합니다. 설정된 시간이 되거나 브릿지가 해당 멤버십의 멀티캐스트 쿼리를 전송하도록 요청 받으면 브릿지가 확인이 요청된 시간에 multicast_query_interval을 더해서 자체 멀티캐스트 쿼리어를 확인합니다. 해당 멤버십의 멀티캐스트 쿼리가 마지막 multicast_query_interval 내로 전송된 경우 다시 전송되지 않습니다.
multicast_query_response_interval	쿼리 전송 후 호스트가 응답해야 하는 시간을 0.1초 단위로 설정합니다. multicast_query_interval값보다 작거나 같아야 합니다.

매개 변수	설명
multicast_router	포트의 멀티캐스트 라우터 연결을 활성화 또는 비활성화할 수 있습니다. 포트에 하나 이상의 멀티캐스트 라우터가 연결되어 있는 경우 모든 멀티캐스트 트래픽을 수신합니다. 이러한 값을 0으로 하면 완전히 비활성화되며, 1로 하면 쿼리를 바탕으로 시스템이 라우터의 존재 여부를 자동으로 감지하도록 활성화되고, 2로 하면 포트가 항상 모든 멀티캐스트 트래픽을 수신하도록 활성화됩니다.
multicast_snooping	스누핑 (snooping) 활성화/비활성화를 변경합니다. 스누핑을 사용하여 브리지가 라우터와 호스트 간의 네트워크 트래픽을 들어서 만드는 맵으로 멀티캐스트 트래픽을 적절한 링크로 필터링합니다. 이러한 옵션을 사용하여 해시 (hash) 충돌로 인해 스누핑이 자동으로 비활성화된 경우 이를 다시 활성화할 수 있지만 해시 충돌이 해결되지 않으면 스누핑을 다시 활성화할 수 없습니다.
multicast_startup_query_count	멤버십 정보를 확인하기 위해 시작 시 전송되는 쿼리의 수를 설정합니다.
multicast_startup_query_interval	멤버십 정보를 확인하기 위해 시작 시 전송되는 쿼리 간 간격을 0.1초 단위로 설정합니다.

B.2. ETHTOOL 사용을 위해 RED HAT VIRTUALIZATION MANAGER 설정

관리 포털의 호스트 네트워크 인터페이스 카드 `ethtool` 속성을 설정합니다. `ethtool_opts` 키는 기본적으로 제공되지 않으며 `engine` 설정 도구를 사용하여 `Manager`에 추가해야 합니다. 또한 필요한 `VDSM` 후크 패키지를 호스트에 설치해야 합니다.

절차 B.1. Manager에 ethtool_opts 키 추가

1. Manager에서 키를 추가하기 위해 다음의 명령을 실행합니다:

```
# engine-config -s
UserDefinedNetworkCustomProperties=ethtool_opts=. * --cver=4.0
```

2. `ovirt-engine` 서비스를 다시 시작합니다:

```
# systemctl restart ovirt-engine.service
```

3. `ethtool` 속성을 설정하려는 호스트에 `VDSM` 후크 패키지를 설치합니다. 이러한 패키지는 `Red Hat Virtualization Host`에서 기본적으로 사용 가능하지만 `Red Hat Enterprise Linux` 호스트에 설치해야 합니다.

```
# yum install vds-hook-ethtool-options
```

이제 관리 포털에서 `ethtool_opts` 키를 사용할 수 있습니다. 논리 네트워크에 `ethtool` 속성을 적용하려

면 [6.5.2절. “호스트 네트워크 인터페이스 편집 및 호스트에 논리 네트워크 할당”](#)을 참조하십시오.

B.3. FCOE를 사용하기 위해 RED HAT VIRTUALIZATION MANAGER를 설정하는 방법

관리 포털에서 호스트 네트워크 인터페이스 카드에 대해 FCoE(Fibre Channel over Ethernet) 속성을 설정할 수 있습니다. **fcoe** 키는 기본적으로 사용할 수 없으며 **engine** 설정 도구를 사용하여 **Manager**에 추가해야 합니다. 다음 명령을 실행하여 **fcoe**가 이미 활성화되어 있는지 여부를 확인할 수 있습니다.

```
# engine-config -g UserDefinedNetworkCustomProperties
```

호스트에 필수 VDSM 후크 패키지를 설치해야 합니다. 호스트의 FCoE 카드에 따라 특정 설정이 필요할 수도 있습니다. 자세한 내용은 *Red Hat Enterprise Linux 스토리지 관리 가이드*에 있는 [FCoE\(Fibre Channel over Ethernet\) 인터페이스 설정](#)을 참조하십시오.

절차 B.2. Manager에 fcoe 키 추가

1. Manager에서 키를 추가하기 위해 다음의 명령을 실행합니다:

```
# engine-config -s
UserDefinedNetworkCustomProperties='fcoe=^((enable|dcb|auto_vlan)=
(yes|no),?)*$'
```

2. **ovirt-engine** 서비스를 다시 시작합니다:

```
# systemctl restart ovirt-engine.service
```

3. FCoE 속성을 설정하려는 각 Red Hat Enterprise Linux 호스트에 VDSM 후크 패키지를 설치합니다. 패키지는 Red Hat Virtualization Host(RHVH)에서 기본적으로 사용 가능합니다.

```
# yum install vdsm-hook-fcoe
```

이제 관리 포털에서 **fcoe** 키를 사용할 수 있습니다. [6.5.2절. “호스트 네트워크 인터페이스 편집 및 호스트에 논리 네트워크 할당”](#)을 참조하여 논리 네트워크에 FCoE 속성을 적용하십시오.

B.4. 비관리 네트워크를 사용하기 위해 RED HAT VIRTUALIZATION MANAGER를 설정하는 방법

기본 관리 네트워크(ovirtmgmt) 대신 비관리 네트워크를 기본 네트워크로 사용하도록 데이터 센터의 각 호스트를 구성할 수 있습니다. **default_route** 속성은 관리 포털에서 호스트 네트워크 인터페이스 카드에 대해 정의됩니다. **default_route** 키는 기본적으로 사용할 수 없으며 엔진 설정 도구를 사용하여 **Manager**에 추가해야 합니다. 다음 명령을 실행하여 **default_route**가 이미 활성화되어 있는지 여부를 확인할 수 있습니다.

```
# engine-config -g UserDefinedNetworkCustomProperties
```

절차 B.3. default_route 키를 Manager에 추가

1. Manager에서 키를 추가하기 위해 다음의 명령을 실행합니다:

```
# engine-config -s # engine-config -s
UserDefinedNetworkCustomProperties='default_route:^(true|false)$'
# engine-config -g UserDefinedNetworkCustomProperties
```

2. **ovirt-engine** 서비스를 다시 시작합니다:

```
# systemctl restart ovirt-engine
```

이제 **default_route** 키를 관리 포털에서 사용할 수 있습니다. [6.5.2절](#). “호스트 네트워크 인터페이스 편집 및 호스트에 논리 네트워크 할당”을 참조하여 비관리 네트워크를 정의하십시오.

부록 C. RED HAT VIRTUALIZATION 사용자 인터페이스 플러그인

C.1. RED HAT VIRTUALIZATION 사용자 인터페이스 플러그인

Red Hat Virtualization은 비표준 기능을 제공하는 플러그인을 지원합니다. 이를 통해 Red Hat Virtualization 관리 포털을 다른 시스템과 쉽게 통합할 수 있습니다. 각 인터페이스 플러그인은 Red Hat Virtualization과 함께 사용하기 위해 패키지 설정 및 배포할 수 있는 사용자 인터페이스 확장 기능 모음을 제공합니다.

Red Hat Virtualization의 사용자 인터페이스 플러그인은 JavaScript 프로그래밍 언어를 사용하여 클라이언트에서 직접 관리 포털과 통합할 수 있습니다. 관리 포털이 플러그인을 호출하고 웹 브라우저의 JavaScript 런타임에서 실행됩니다. 사용자 인터페이스 플러그인은 JavaScript 언어 및 라이브러리를 사용할 수 있습니다.

런타임 시 중요 이벤트에서 관리 포털은 관리 포털 플러그인 간의 통신을 제공하는 이벤트 처리 함수를 통해 개별 플러그인을 호출합니다. 관리 포털이 여러 이벤트 처리 함수를 지원하지만 플러그인은 구현에만 초점을 두고 있는 함수만을 지정합니다. 관리 포털에서 플러그인을 사용하기 전 각각의 플러그인은 플러그인 부트 스트랩 순서의 일부로 관련 이벤트 처리 함수에 등록해야 합니다.

사용자 인터페이스 확장을 구동하는 관리 포털 플러그인이 통신을 용이하게 하기 위해 관리 포털은 개별 플러그인이 소비할 수 있는 글로벌 (상위 레벨) pluginApi JavaScript 객체로 플러그인 API를 표시하고 있습니다. 각각의 플러그인에는 별도의 pluginApi 인스턴스가 있어 관리 포털은 플러그인의 라이프 사이클과 관련하여 각 플러그인에 대해 plug-in API- 함수 호출을 제어할 수 있습니다.

C.2. RED HAT VIRTUALIZATION 사용자 인터페이스 플러그인 라이프 사이클

C.2.1. Red Hat Virtualization 사용자 인터페이스 플러그인 라이프 사이클

사용자 인터페이스 플러그인의 기본 라이프 사이클은 다음의 세 단계로 나누어집니다:

1. 플러그인 검색
2. 플러그인 로딩
3. 플러그인 부트스트랩

C.2.2. Red Hat Virtualization 사용자 인터페이스 플러그인 검색

플러그인 검색 프로세스에서 첫 번째 단계는 플러그인 설명자를 생성하는 것입니다. 플러그인 설명자에는 중요한 플러그인 메타데이터 및 플러그인 관련 기본 옵션 설정이 들어 있습니다.

관리 포털 HTML 페이지 요청 (HTTP GET) 처리의 일부분으로 사용자 인터페이스 플러그인 인프라는 로컬 파일 시스템에서 플러그인 설명자를 검색 및 로딩 시도합니다. 각각의 플러그인 설명자의 경우 인프라는 플러그인 관련 기본 설정 (존재할 경우)을 덮어쓰기하고 플러그인 런타임 동작을 조정하기 위해 사용되는 해당 플러그인 사용자 설정도 로딩 시도합니다. 플러그인 사용자 설정은 옵션 사항입니다. 설명자 및 해당 사용자 설정 파일을 로딩한 후 oVirt Engine은 사용자 인터페이스 플러그인 데이터를 집계하고 런타임 평가를 위해 관리 포털 HTML 페이지에 포함합니다.

기본값으로 플러그인 설명자는 oVirt Engine 로컬 설정에 의해 정의된

`ENGINE_USR=/usr/share/ovirt-engine`의 기본 매핑과 함께 `$ENGINE_USR/ui-plug-ins`에 있습니다. 플러그인 설명자는 JSON 형식 사양을 준수해야 하지만 플러그인 설명자는 JSON 형식 사양 이외

에 Java/C++ 형식의 코멘트 (`/*` 및 `//` 변수 모두)를 허용합니다.

기본값으로 플러그인 사용자 설정 파일은 oVirt Engine 로컬 설정에 의해 정의된 `ENGINE_ETC=/etc/ovirt-engine`의 기본 매핑과 함께 `$ENGINE_ETC/ui-plug-ins`에 있습니다. 플러그인 사용자 설정 파일은 플러그인 설명자와 동일한 컨텐츠 형식 규칙을 준수해야 합니다.



참고

일반적으로 플러그인 사용자 설정 파일은 `<descriptorFileName>-config.json` 이름 지정 규칙을 따릅니다.

C.2.3. Red Hat Virtualization 사용자 인터페이스 플러그인 로딩

플러그인이 검색되어 데이터가 관리 포털 HTML 페이지에 포함된 후 관리 포털은 (애플리케이션 시작의 일부로 로딩하지 않도록 설정하지 않는 한) 애플리케이션 시작의 일부로 플러그인을 로딩 시도합니다.

검색된 각 플러그인에 대해 관리 포털은 호스트 페이지를 로딩하는데 사용되는 HTML `iframe` 요소를 생성합니다. 플러그인 호스트 페이지는 플러그인 부트스트랩 프로세스를 시작하는데 필요하며 부트스트랩 프로세스는 플러그인의 `iframe` 요소의 문맥에서 플러그인 코드를 평가하는데 사용됩니다. 사용자 인터페이스 플러그인 인프라는 로컬 파일 시스템에서 플러그인 호스트 페이지와 같은 플러그인 리소스 파일을 지원합니다. 플러그인 호스트 페이지는 `iframe` 요소에 로딩되어 플러그인 코드가 평가됩니다. 플러그인 코드가 평가된 후 플러그인은 플러그인 API를 통해 관리 포털과 통신합니다.

C.2.4. Red Hat Virtualization 사용자 인터페이스 플러그인 부트스트랩

일반적인 플러그인 부트스트랩 순서는 다음과 같습니다:

절차 C.1. 플러그인 부트스트랩 순서

1. 지정된 플러그인의 `pluginApi` 인스턴스 가져오기
2. 런타임 플러그인 설정 개체 가져오기 (옵션)
3. 관련 이벤트 처리기 함수 등록
4. 플러그인 초기화를 실행하도록 UI 플러그인 인프라에 통지

다음 코드 조각은 위에서 설명한 단계가 사용된 예를 보여줍니다:

```
// Access plug-in API using 'parent' due to this code being evaluated
// within the context of an iframe element.
// As 'parent.pluginApi' is subject to Same-Origin Policy, this will only
// work when WebAdmin HTML page and plug-in
// host page are served from same origin. WebAdmin HTML page and plug-in
// host page will always be on same origin
// when using UI plug-in infrastructure support to serve plug-in resource
// files.
var api = parent.pluginApi('MyPlugin');

// Runtime configuration object associated with the plug-in (or an empty
// object).
var config = api.configObject();

// Register event handler function(s) for later invocation by UI plug-in
```

```

infrastructure.
api.register({
  // UiInit event handler function.
  UiInit: function() {
    // Handle UiInit event.
    window.alert('Favorite music band is ' + config.band);
  }
});

// Notify UI plug-in infrastructure to proceed with plug-in
initialization.
api.ready();

```

C.3. 사용자 인터페이스 플러그인 관련 파일 및 위치

표 C.1. UI 플러그인 관련 파일 및 위치

파일	위치	설명
플러그인 설명자 파일 (메타-데이터)	<code>/usr/share/ovirt-engine/ui-plugins/my-plugin.json</code>	
플러그인 사용자 설정 파일	<code>/etc/ovirt-engine/ui-plugins/my-plugin-config.json</code>	
플러그인 리소스 파일	<code>/usr/share/ovirt-engine/ui-plugins/<resourcePath>/PluginHostPage.html</code>	<code><resourcePath></code> 는 플러그인 설명자에 있는 해당 속성에 의해 정의됩니다.

C.4. 사용자 인터페이스 플러그인 배포 예

Red Hat Virtualization Manager 관리 포털에 로그인 시 **Hello World!** 프로그램을 실행하는 사용자 인터페이스 플러그인을 생성하기 위해 다음과 같은 지시 사항을 따릅니다.

절차 C.2. Hello World! 플러그인 배포

1. `/usr/share/ovirt-engine/ui-plugins/helloWorld.json`에 있는 Manager에 다음과 같은 파일을 생성하여 플러그인 설명자를 생성합니다:

```

{
  "name": "HelloWorld",
  "url": "/ovirt-engine/webadmin/plugin/HelloWorld/start.html",
  "resourcePath": "hello-files"
}

```

2. `/usr/share/ovirt-engine/ui-plugins/hello-files/start.html`에 있는 Manager에 다음과 같은 파일을 생성하여 플러그인 호스트 페이지를 생성합니다:

```

<!DOCTYPE html><html><head>

```

```

<script>
  var api = parent.pluginApi('HelloWorld');
  api.register({
    UiInit: function() { window.alert('Hello world'); }
  });
  api.ready();
</script>
</head><body></body></html>

```

Hello World! 플러그인을 성공적으로 구현했을 경우 관리 포털에 로그인했을 때 다음과 같은 화면이 표시됩니다:

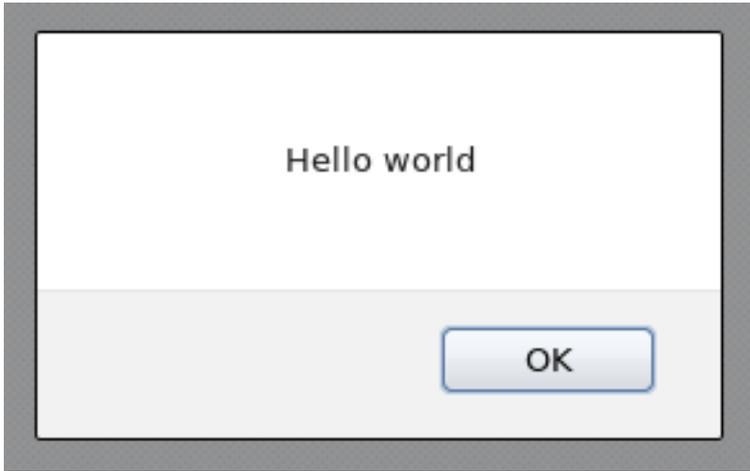


그림 C.1. Hello World! 플러그인의 구현

C.5. RED HAT SUPPORT 플러그인 사용

Red Hat Access 플러그인을 사용하여 Red Hat Virtualization 관리 포털에서 Red Hat 액세스 서비스를 사용할 수 있습니다. Red Hat 로그인을 사용하여 로그인해야 합니다. Red Hat Access 플러그인은 사용자가 로그인되어 있지 않을 때 이를 감지하고 로그인하지 않은 경우 로그인 창이 열립니다.



참고

Red Hat Virtualization 관리 포털 인증 정보는 사용자의 Red Hat 로그인과 일치하지 않습니다.

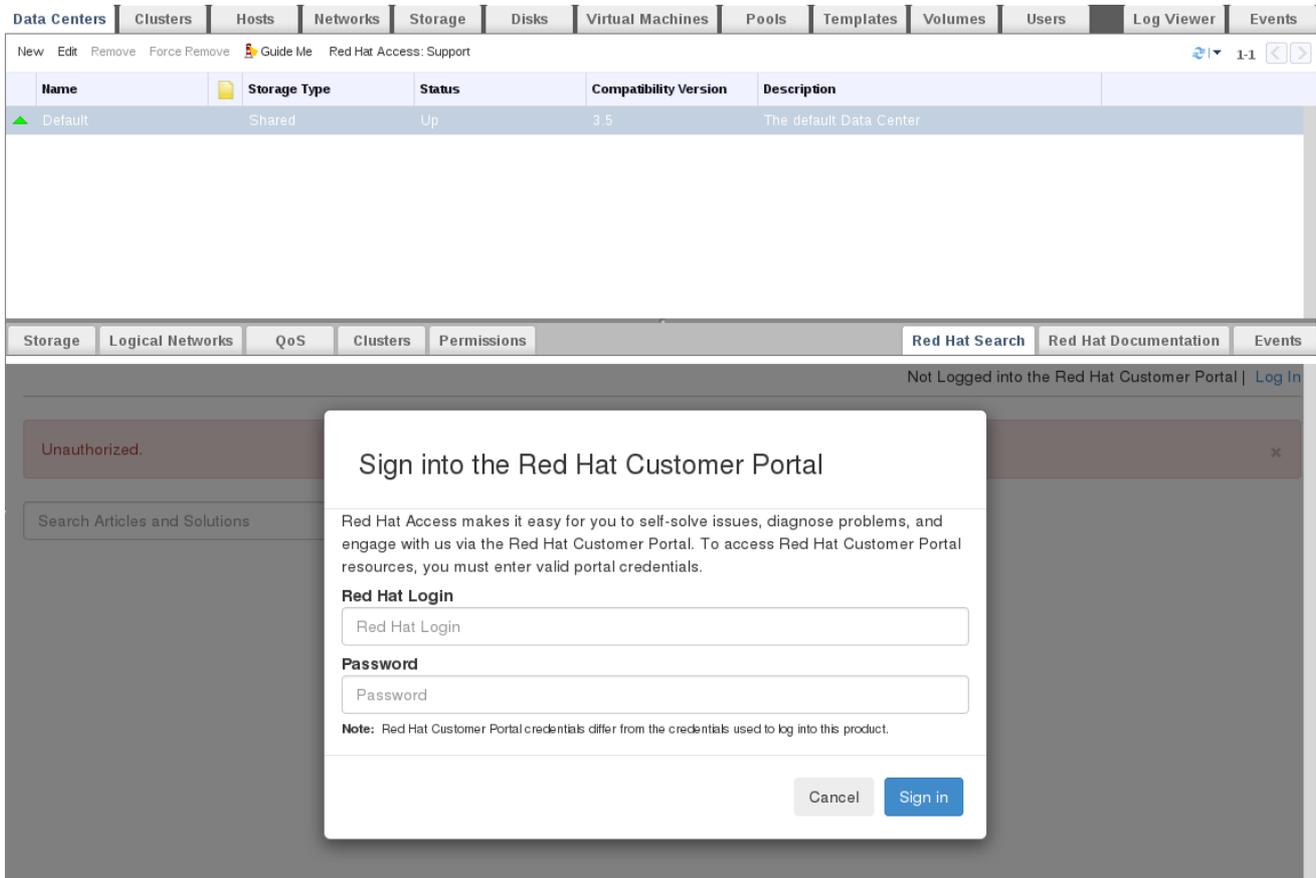


그림 C.2. Red Hat Support 플러그인 로그인 창

로그인 후 Red Hat 고객 포털에 액세스할 수 있습니다. Red Hat Support 플러그인은 Red Hat Virtualization 관리 포털에 있는 여러 다른 메뉴와 함께 상세 정보 창에서 사용할 수 있습니다. 검색 바를 사용하여 Red Hat Access 데이터베이스를 검색합니다. 검색 결과가 상세 정보 창의 왼쪽 탐색 목록에 표시됩니다.

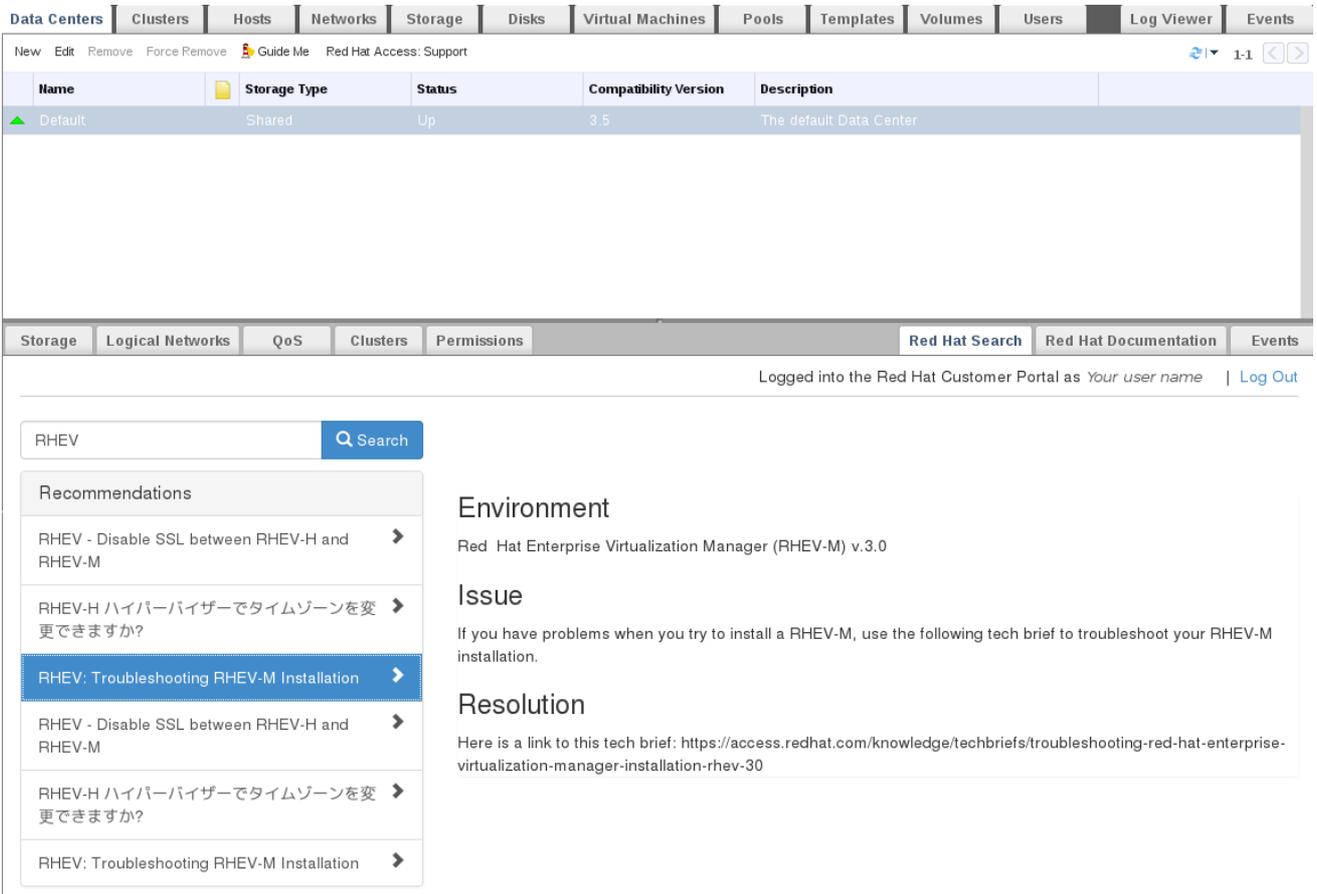


그림 C.3. Red Hat Support 플러그인 - 왼쪽 탐색 목록에 있는 쿼리 결과

Red Hat Virtualization 관리 포털에 있는 컨텍스트 메뉴에서 오른쪽 클릭하여 Red Hat Support 플러그인에 액세스합니다.

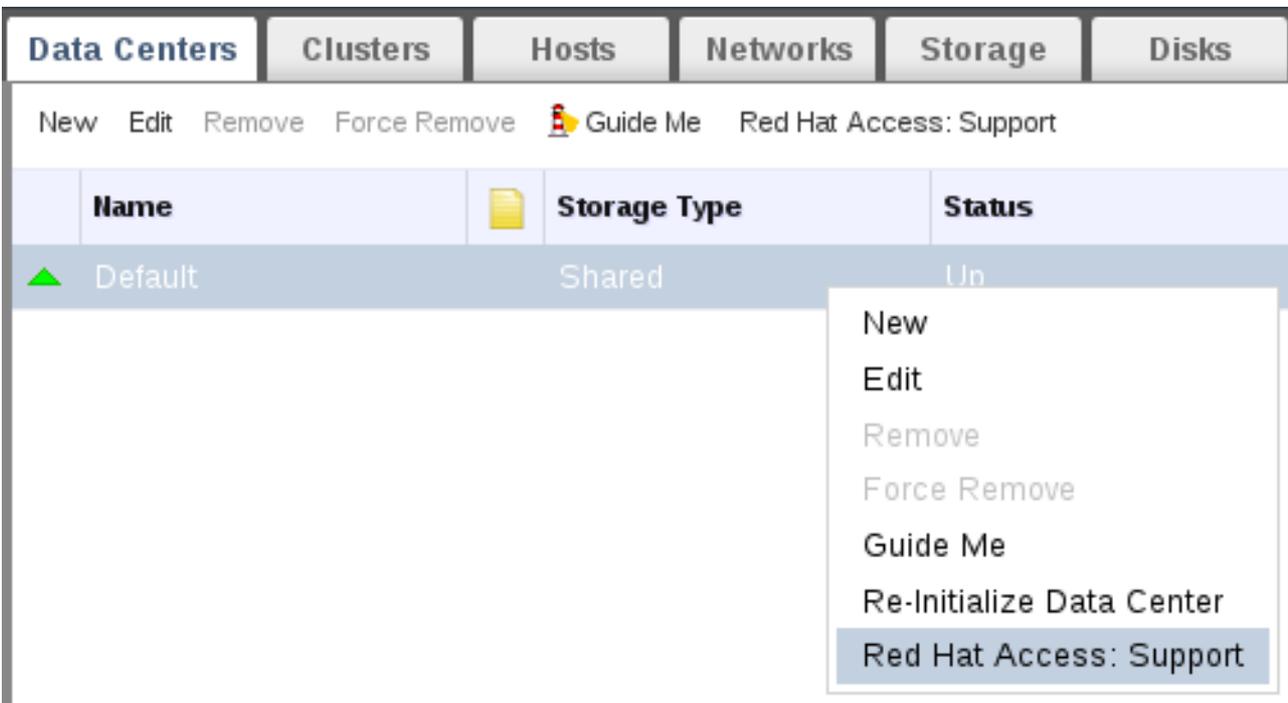


그림 C.4. 컨텍스트 메뉴에서 오른쪽 클릭하여 Red Hat Support 플러그인에 액세스

새 기술 지원 열기 또는 기존 기술 지원 수정 버튼을 선택하여 새 기술 지원을 열거나 기존 기술 지원을 수정합니다.

The screenshot shows the 'Red Hat Access: Support' portal. At the top, there are buttons for 'Open Case' and 'Modify Case'. Below these, it says 'Logged into the Red Hat Customer Portal as *Your user name* | [Log Out](#)'. The main content is divided into two columns. The left column contains form fields for 'Account:' (with a 'My Account' button), 'Owner:' (with a dropdown showing 'No results match'), 'Product:' (with a dropdown showing 'Red Hat Enterprise Virtualization'), and 'Product Version:' (with a dropdown showing '3.5'). Below these are 'Summary:' and 'Description:' text input areas. The right column is titled 'Recommendations' and contains three items, each with a right-pointing arrow icon: 'Does Red Hat support SuSE as a virtual machine?', 'Error message from subscription-manager when attempting to auto-attach shows No Installed products on system. No need to attach subscriptions.', and 'Signal 17 (CHLD) caught by ps (procps version 3.2.8)'.

그림 C.5. Red Hat Support 플러그인 - 새 기술 지원 열기

Red Hat Documentation 탭을 선택하여 현재 화면에 있는 관리 포털 부분과 연관된 문서를 엽니다.

Name	Storage Type	Status	Compatibility Version	Description
Default	Shared	Up	3.5	The default Data Center

Storage
Logical Networks
QoS
Clusters
Permissions
Red Hat Search
Red Hat Documentation
Events




◀ Prev

Administration Guide

Next ▶

Chapter 4. Data Centers

- [4.1. Introduction to Data Centers](#)
- [4.2. The Storage Pool Manager](#)
- [4.3. SPM Priority](#)
- [4.4. Using the Events Tab to Identify Problem Objects in Data Centers](#)
- [4.5. Data Center Tasks](#)
- [4.6. Data Centers and Storage Domains](#)
- [4.7. Data Centers and Permissions](#)

4.1. Introduction to Data Centers

A data center is a logical entity that defines the set of resources used in a specific environment. A data center is considered a container resource, in that it is comprised of logical resources, in the form of clusters and hosts; network resources, in the form of logical networks and physical NICs; and storage resources, in the form of storage domains.

그림 C.6. Red Hat Support 플러그인 액세스 문서

부록 D. RED HAT VIRTUALIZATION 및 SSL

D.1. RED HAT VIRTUALIZATION MANAGER SSL 인증서 변경



주의

/etc/pki 디렉토리 또는 서브 디렉토리의 권한 및 소유권을 변경하지 않습니다. **/etc/pki** 및 **/etc/pki/ovirt-engine** 디렉토리의 권한은 기본 755를 유지해야 합니다.

조직의 상용 서명 인증서를 사용하여 HTTPS를 통해 연결하는 사용자에게 Red Hat Virtualization Manager를 식별하게 할 수 있습니다.



참고

상용 발행된 HTTPS 연결용 인증서를 사용하면 Manager와 호스트 간의 인증에 사용되는 인증서에 영향을 주지 않습니다. Manager에서 생성한 자체 서명된 인증서가 계속 사용됩니다.

전제 조건

이 절차에서는 상용 인증서 발급 기관에서의 PEM 형식 인증서인 **.nokey** 파일 및 **.cer** 파일이 필요합니다. **.nokey** 및 **.cer** 파일은 P12 형식의 인증키 번들로 배포됩니다.

이 절차에서는 P12 형식의 인증키 번들이 있다는 것을 전제로 합니다.



중요

새로운 Red Hat Virtualization 설치에 대해 이 절차의 모든 단계를 완료해야 합니다. 이미 설정된 상용 서명된 인증서가 있는 Red Hat Enterprise Virtualization 3.6 환경에서 업그레이드한 경우 1, 8, 9 단계만 필요합니다.

절차 D.1. Red Hat Virtualization Manager Apache SSL 인증서 교체

1. 상용 발행된 인증서를 호스트 전체 신뢰 저장소에 추가합니다.

```
# cp YOUR-3RD-PARTY-CERT.pem /etc/pki/ca-trust/source/anchors
```

```
# update-ca-trust
```

2. Manager는 **/etc/pki/ovirt-engine/ca.pem**에 심볼릭 링크된 **/etc/pki/ovirt-engine/apache-ca.pem**을 사용하도록 설정되어 있습니다. 심볼릭 링크를 제거합니다.

```
# rm /etc/pki/ovirt-engine/apache-ca.pem
```

3. 상용 발행된 인증서를 **/etc/pki/ovirt-engine/apache-ca.pem**으로 저장합니다. 인증서 체인은 **root** 인증서 까지 완료해야 합니다. 체인 순서는 중요하며 중간 인증서에서 **root** 인증서

로 되어 있어야 합니다.

```
mv YOUR-3RD-PARTY-CERT.pem /etc/pki/ovirt-engine/apache-ca.pem
```

4. **P12** 번들을 백업한 다음 **/etc/pki/ovirt-engine/keys/apache.p12**로 이동합니다.

5. 번들에서 키를 추출합니다.

```
# openssl pkcs12 -in /etc/pki/ovirt-engine/keys/apache.p12 -nocerts  
-nodes > /etc/pki/ovirt-engine/keys/apache.key.nopass
```

6. 번들에서 인증서를 추출합니다.

```
# openssl pkcs12 -in /etc/pki/ovirt-engine/keys/apache.p12 -nokeys >  
/etc/pki/ovirt-engine/certs/apache.cer
```

7. Apache 서버를 다시 시작합니다.

```
# systemctl restart httpd.service
```

8. 새로운 신뢰 저장소 설정 파일을 생성합니다.

```
# vi /etc/ovirt-engine/engine.conf.d/99-custom-truststore.conf
```

다음 콘텐츠를 추가하고 파일을 저장합니다.

```
ENGINE_HTTPS_PKI_TRUST_STORE="/etc/pki/java/cacerts"  
ENGINE_HTTPS_PKI_TRUST_STORE_PASSWORD=""
```

9. **ovirt-engine** 서비스를 다시 시작합니다.

```
systemctl restart ovirt-engine.service
```

이제 사용자가 **HTTPS** 트래픽을 암호화하는 데 사용되는 인증서의 인증에 대한 경고 없이 관리 포털 및 사용자 포털에 연결할 수 있습니다.

중요

인증서를 변경하면 <https://access.redhat.com/solutions/458713>에서 설명되어 있듯이 로그 수집기에서 오류가 발생할 수 있습니다. 이러한 오류가 발생하지 않게 하려면 로그 수집기의 설정을 다음과 같이 편집합니다:

1. CA 서버에서 CA 인증서를 내보내기하여 Red Hat Virtualization Manager 서버에 복사합니다.
2. **/etc/ovirt-engine/logcollector.conf**에 다음 행을 추가하면 로그 수집기가 새 위치를 가리킵니다:

```
cert-file=/path/to/new/CA/file
```

D.2. MANAGER 및 LDAP 서버 간의 SSL 또는 TLS 연결 설정

Red Hat Enterprise Virtualization Manager와 LDAP 서버 간의 보안 연결을 설정하려면 LDAP 서버의 root CA 인증서를 취득하고 root CA 인증서를 Manager로 복사해서 PEM 인코딩된 CA 인증서를 생성합니다. 모든 Java 지원 keystore 유형을 사용할 수 있습니다. 다음의 절차에서는 Java KeyStore (JKS) 형식을 사용합니다.



참고

PEM 인코딩된 CA 인증서 생성 및 인증서를 가져오는 방법에 대한 보다 자세한 내용은 `/usr/share/doc/ovirt-engine-extension-aaa-ldap-version`에서 README 파일의 **X.509 CERTIFICATE TRUST STORE** 섹션에서 참조하십시오..

절차 D.2. PEM 인코딩된 CA 인증서 생성

1. Red Hat Virtualization Manager에서 LDAP 서버의 root CA 인증서를 복사해서 `/tmp` 디렉토리에 넣고 **keytool** 명령을 실행하여 root CA 인증서를 가져와서 PEM 인코딩된 CA 인증서를 생성합니다. 다음의 명령을 사용하여 root CA 인증서를 `/tmp/myrootca.pem`에 가져오고 PEM 인코딩된 CA 인증서인 `myrootca.jks`를 `/etc/ovirt-engine/aaa/` 밑에 생성합니다. 인증서 위치 및 암호를 적어 놓습니다. 대화형 설정 도구를 사용하는 경우 이 정보만 있으면 됩니다. LDAP 서버를 수동 설정 시 다음 절차를 마저 따라서 설정 파일을 업데이트합니다.

```
$ keytool -importcert -noprompt -trustcacerts -alias myrootca -file
/tmp/myrootca.pem -keystore /etc/ovirt-engine/aaa/myrootca.jks -
storepass password
```

2. 인증서 정보로 `/etc/ovirt-engine/aaa/profile1.properties` 파일을 업데이트합니다:



참고

`${local:_basedir}`는 LDAP 속성 설정 파일이 있는 디렉토리이며 `/etc/ovirt-engine/aaa` 디렉토리를 가리킵니다. 다른 디렉토리에 PEM 인코딩된 CA 인증서를 생성할 경우 `${local:_basedir}`를 해당 인증서의 전체 경로로 변경합니다.

- startTLS를 사용하려면 다음을 실행합니다 (권장사항):

```
# Create keystore, import certificate chain and uncomment
pool.default.ssl.startTLS = true
pool.default.ssl.truststore.file = ${local:_basedir}/myrootca.jks
pool.default.ssl.truststore.password = password
```

- SSL을 사용하려면 다음을 실행합니다:

```
# Create keystore, import certificate chain and uncomment
pool.default.serverset.single.port = 636
pool.default.ssl.enable = true
pool.default.ssl.truststore.file = ${local:_basedir}/myrootca.jks
pool.default.ssl.truststore.password = password
```

외부 LDAP 공급자 설정을 계속하려면 15.3.1절. “외부 LDAP 공급자 설정 (대화형 설정)”를 참조하십시오. 단일 사용 승인 (SSO)을 위한 LDAP 및 Kerberos 설정에 대한 자세한 내용은 15.4절. “단일 사용 승인(SSO)을 위해 LDAP 및 Kerberos 설정”에서 참조하십시오.

부록 E. 검색, 북마크, 태그 사용

E.1. 검색

E.1.1. Red Hat Virtualization에서 검색 실행

관리 포털에서는 가상 머신, 호스트, 사용자 등과 같은 수천 가지의 리소스를 관리할 수 있습니다. 검색을 수행하려면 검색 창에 검색 쿼리 (자유 텍스트 또는 구문 기반)를 입력합니다. 검색 쿼리는 차후 재사용을 위해 북마크로 저장해 둘 수 있으므로 특정 검색 결과가 필요할 때 마다 검색 쿼리를 재입력할 필요가 없습니다. 검색은 대소문자를 구분하지 않습니다.

E.1.2. 검색 구문 및 예

Red Hat Virtualization 리소스의 검색 쿼리 구문은 다음과 같습니다:

result type: {criteria} [sortby sort_spec]

구문 예

다음 예에서는 검색 쿼리 사용 방법 및 Red Hat Virtualization에서 검색 쿼리를 구축하는 방법에 대해 설명합니다.

표 E.1. 검색 쿼리 예

예	결과
Hosts: Vms.status = up	사용 중인 가상 머신을 실행하고 있는 모든 호스트 목록을 나열합니다.
Vms: domain = qa.company.com	지정된 도메인에서 실행 중인 모든 가상 머신 목록을 나열합니다.
Vms: users.name = Mary	사용자 이름이 Mary 인 사용자에게 속한 모든 가상 머신 목록을 나열합니다.
events: severity > normal sortby time desc	심각도가 Normal 이상인 모든 이벤트 목록을 시간 순으로 나열합니다.

E.1.3. 검색 자동 완료

관리 포털에서는 효과적이고 강력한 검색 쿼리를 생성할 수 있도록 검색 자동 완료 기능을 제공합니다. 검색 쿼리 일부를 입력하면 검색 창 아래에 검색의 다음 부분을 선택할 수 있는 드롭 다운 목록이 표시됩니다. 이 목록에서 선택하여 검색의 다음 부분을 입력/선택하거나 옵션을 무시하고 수동으로 검색 쿼리를 입력할 수 있습니다.

다음 표에서는 쿼리 구축을 위해 고객 포털에서 검색 자동 완료를 사용하는 방법에 대한 예를 설명합니다.

Hosts: Vms.status = down

표 E.2. 자동 완료 기능을 사용하는 검색 쿼리의 예

입력	표시되는 항목 목록	동작
h	Hosts (옵션 1 개만)	Hosts 를 선택하거나 또는 Hosts 입력
Hosts:	모든 호스트 속성	v 입력
Hosts: v	v 로 시작하는 호스트 속성	Vms 를 선택하거나 Vms 입력
Hosts: Vms	모든 가상 머신 속성	s 입력
Hosts: Vms.s	s 로 시작하는 모든 가상 머신 속성	status 를 선택하거나 status 입력
Hosts: Vms.status	= =!	= 을 선택하거나 입력
Hosts: Vms.status =	모든 상태 값	down 을 선택하거나 입력

E.1.4. 검색 결과 유형 옵션

결과 유형으로 다음과 같은 유형의 리소스를 검색할 수 있습니다:

- **Vms** 가상 머신 목록의 경우
- **Host** 호스트 목록의 경우
- **Pools** 풀 목록의 경우
- **Template** 템플릿 목록의 경우
- **Event** 이벤트 목록의 경우
- **Users** 사용자 목록의 경우
- **Cluster** 클러스터 목록의 경우
- **Datacenter** 데이터 센터 목록의 경우
- **Storage** 스토리지 도메인 목록의 경우

각 리소스 유형에는 고유한 속성 모음 및 이와 관련된 다른 리소스 유형 모음이 있으며 각 검색 유형에는 유효한 구문 조합 모음이 있습니다. 자동 완료 기능을 사용하여 쿼리를 쉽게 생성할 수 있습니다.

E.1.5. 검색 기준

쿼리에서 콜론 다음에 검색 기준을 지정할 수 있습니다. **{criteria}** 구문은 다음과 같습니다:

<prop><operator><value>

또는

<obj-type><prop><operator><value>

예

다음 표에서는 구문의 각 속성에 대해 설명합니다:

표 E.3. 검색 기준 예

요소	설명	값	예	알림
prop	검색 대상이 되는 리소스의 속성입니다. 리소스 유형 (obj-type 참조), 또는 <i>tag</i> (사용자 정의 태그)의 속성이 될 수 있습니다.	검색 범위를 특정 속성을 갖는 개체로 제한합니다. (예: <i>status</i> 속성이 있는 개체를 검색)	Status	해당 없음
obj-type	검색 대상 리소스에 연결할 수 있는 리소스 유형입니다.	데이터 센터, 가상 머신과 같은 시스템 개체입니다.	Users	해당 없음
operator	비교 연산자입니다.	= != (not equal) > < >= <=	해당 없음	obj-type 따라 다른 값 옵션입니다.

요소	설명	값	예	알림
Value	비교 대상이 되는 표현식입니다.	문자열 정수 검색 순위 날짜 (지역 설정에 따라 표기)	Jones 256 normal	<ul style="list-style-type: none"> 문자열에서 와일드카드를 사용할 수 있습니다. " (중간에 공백없는 따옴표)을 사용하여 최적화되지 않은 (빈) 문자열을 표시할 수 있습니다. 공백이 있는 문자열 또는 날짜는 큰 따옴표를 사용합니다.

E.1.6. 검색: 여러 검색 기준 및 와일드 카드

와일드 카드는 문자열의 `<value>` 구문 부분에 사용할 수 있습니다. 예를 들어 `m*`을 입력하여 `m`으로 시작하는 모든 사용자를 검색할 수 있습니다.

부울 연산자 **AND** 및 **OR**를 사용하여 두 개의 검색 기준으로 검색할 수 있습니다. 예:

```
Vms: users.name = m* AND status = Up
```

이 쿼리는 사용자 이름이 "m"으로 시작하는 사용자의 실행 중인 모든 가상 머신을 반환합니다.

```
Vms: users.name = m* AND tag = "paris-loc"
```

이 쿼리는 사용자 이름이 "m"으로 시작하는 사용자의 "paris-loc"으로 태그된 모든 가상 머신을 반환합니다.

AND 또는 **OR**을 사용하지 않고 두 개의 검색 기준을 지정할 경우, **AND**가 묵시적으로 적용됩니다. **AND**는 **OR**에 우선하며 **OR**은 묵시적인 **AND**에 우선합니다.

E.1.7. 검색: 검색 순서 지정

`sortby`를 사용하여 검색 결과 정보의 정렬 순서를 지정할 수 있습니다. 정렬 방향 (오름 차순의 경우 `asc`, 내림 차순의 경우 `desc`)을 지정할 수도 있습니다.

예:

```
events: severity > normal sortby time desc
```

이 쿼리는 심각도가 Normal 이상인 모든 이벤트를 시간 순 (내림 차순)으로 정렬하여 반환합니다.

E.1.8. 데이터 센터 검색

다음 표에서는 데이터 센터의 모든 검색 옵션에 대해 설명합니다.

표 E.4. 데이터 센터 검색

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
<code>Clusters.clusters-prop</code>	속성 유형에 따라	데이터 센터에 연결된 클러스터의 속성입니다.
<code>name</code>	문자열	데이터 센터의 이름입니다.
<code>description</code>	문자열	데이터 센터의 설명입니다.
<code>type</code>	문자열	데이터 센터의 유형입니다.
<code>status</code>	목록	데이터 센터의 사용 가능 상태입니다.
<code>sortby</code>	목록	리소스 속성 중 하나에 따라 반환된 검색 결과를 정렬합니다.
<code>page</code>	정수	표시할 결과의 페이지 번호입니다.

예

Datacenter: type = nfs and status != up

이 예는 다음과 같은 데이터 센터 목록을 반환합니다:

- NFS 스토리지 유형이고 up 이외의 상태인 데이터 센터

E.1.9. 클러스터 검색

다음 표에서는 클러스터의 모든 검색 옵션에 대해 설명합니다.

표 E.5. 클러스터 검색

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
<code>Datacenter.datacenter-prop</code>	속성 유형에 따라	클러스터에 연결된 데이터 센터의 속성입니다.
<code>Datacenter</code>	문자열	클러스터가 속해 있는 데이터 센터입니다.
<code>name</code>	문자열	네트워크에서 클러스터를 구별하는 고유한 이름입니다.
<code>description</code>	문자열	클러스터에 대한 설명입니다.

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
initialized	문자열	클러스터 상태를 True 또는 False 로 표시합니다.
sortby	목록	리소스 속성 중 하나에 따라 반환된 검색 결과를 정렬합니다.
page	정수	표시할 결과의 페이지 번호입니다.

예

Clusters: initialized = true or name = Default

다음 예에서는 다음과 같은 조건에 일치하는 클러스터의 목록을 반환합니다:

- 초기화된 클러스터
- 기본값으로 지정된 클러스터

E.1.10. 호스트 검색

다음 표에서는 호스트의 모든 검색 옵션에 대해 설명합니다.

표 E.6. 호스트 검색

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
Vms.Vms-prop	속성 유형에 따라	호스트에 연결된 가상 머신 속성입니다.
Templates.templates-prop	속성 유형에 따라	호스트에 연결된 템플릿 속성입니다.
Events.events-prop	속성 유형에 따라	호스트에 연결된 이벤트 속성입니다.
Users.users-prop	속성 유형에 따라	호스트에 연결된 사용자 속성입니다.
name	문자열	호스트 이름입니다.
status	목록	호스트의 사용 가능 상태입니다.
external_status	문자열	외부 시스템 및 플러그인에 의해 보고되는 호스트 상태입니다.
cluster	문자열	호스트가 속한 클러스터입니다.

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
address	문자열	네트워크에서 호스트를 구별하는 고유한 이름입니다.
cpu_usage	정수	처리 장치 사용률입니다.
mem_usage	정수	메모리 사용률입니다.
network_usage	정수	네트워크 사용률입니다.
load	정수	지정된 타임 슬라이스에서 프로세서 당 <i>run-queue</i> 실행 대기 중인 작업입니다.
version	정수	운영 체제의 버전 번호입니다.
cpus	정수	호스트의 CPU 수입니다.
memory	정수	사용 가능한 메모리 용량입니다.
cpu_speed	정수	CPU 처리 속도입니다.
cpu_model	문자열	CPU 유형입니다.
active_vms	정수	현재 실행되고 있는 가상 머신 수입니다.
migrating_vms	정수	현재 마이그레이션되고 있는 가상 머신 수입니다.
committed_mem	정수	커밋된 메모리 백분율입니다.
tag	문자열	호스트에 할당된 태그입니다.
type	문자열	호스트 유형입니다.
datacenter	문자열	호스트가 속해 있는 데이터 센터입니다.
sortby	목록	리소스 속성 중 하나에 따라 반환된 검색 결과를 정렬합니다.
page	정수	표시할 결과의 페이지 번호입니다.

예

Hosts: cluster = Default and Vms.os = rhel6

이 예는 다음과 같은 호스트 목록을 반환합니다:

- Default 클러스터의 부분으로 Red Hat Enterprise Linux 6 운영 체제를 실행 중인 가상 머신을 호스팅하는 호스트

E.1.11. 네트워크 검색

다음 표에서는 네트워크의 모든 검색 옵션에 대해 설명합니다.

표 E.7. 네트워크 검색

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
Cluster_network.clusternetwor k-prop	속성 유형에 따라	네트워크와 연결된 클러스터의 속성입니다.
Host_Network.hostnetwork- prop	속성 유형에 따라	네트워크와 연결된 호스트의 속성입니다.
name	문자열	네트워크를 구별하는 읽기 쉬운 형식의 이름입니다.
description	문자열	네트워크를 설명하는 키워드 또는 텍스트로 네트워크 생성 시 옵션으로 사용할 수 있습니다.
vlanid	정수	네트워크의 VLAN ID입니다.
stp	문자열	네트워크의 STP (Spanning Tree Protocol)를 활성화 또는 비활성화할 지에 대한 여부입니다.
mtu	정수	논리 네트워크의 최대 전송 단위입니다.
vmnetwork	문자열	네트워크를 가상 머신 트래픽으로만 사용할 지에 대한 여부입니다.
datacenter	문자열	네트워크가 연결된 데이터 센터입니다.
sortby	목록	리소스 속성 중 하나에 따라 반환된 검색 결과를 정렬합니다.
page	정수	표시할 결과의 페이지 번호입니다.

예

Network: mtu > 1500 and vmnetwork = true

다음 예에서는 네트워크 목록을 반환합니다:

- 최대 전송 단위가 1500 바이트 이상
- 가상 머신 전용으로 사용 설정됨

E.1.12. 스토리지 검색

다음 표에서는 스토리지의 모든 검색 옵션에 대해 설명합니다.

표 E.8. 스토리지 검색

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
Hosts. <i>hosts-prop</i>	속성 유형에 따라	스토리지에 연결된 호스트 속성입니다.
Clusters. <i>clusters-prop</i>	속성 유형에 따라	스토리지에 연결된 클러스터 속성입니다.
name	문자열	네트워크에서 스토리지를 구별하는 고유한 이름입니다.
status	문자열	스토리지 도메인 상태입니다.
external_status	문자열	외부 시스템 및 플러그인에 의해 보고되는 스토리지 도메인 상태입니다.
datacenter	문자열	스토리지가 속한 데이터 센터입니다.
type	문자열	스토리지 유형입니다.
size	정수	스토리지 크기입니다.
used	정수	사용된 스토리지 용량입니다.
committed	정수	커밋된 스토리지 용량입니다.
sortby	목록	리소스 속성 중 하나에 따라 반환된 검색 결과를 정렬합니다.
page	정수	표시할 결과의 페이지 번호입니다.

예

Storage: size > 200 or used < 50

이 예는 다음과 같은 스토리지 목록을 반환합니다:

- 총 스토리지 공간이 200 GB 이상인 스토리지

- 사용된 스토리지 공간이 50 GB 미만인 스토리지

E.1.13. 디스크 검색

다음 표에서는 디스크의 모든 검색 옵션에 대해 설명합니다.

표 E.9. 디스크 검색

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
<code>Datacenters.datacenters-prop</code>	속성 유형에 따라	디스크와 관련된 데이터 센터 속성입니다.
<code>Storages.storages-prop</code>	속성 유형에 따라	디스크와 관련된 스토리지 속성입니다.
<code>alias</code>	문자열	네트워크 상의 스토리지를 구별하는 읽기 쉬운 형식의 이름입니다.
<code>description</code>	문자열	디스크를 설명하는 키워드 또는 텍스트로 디스크 생성 시 옵션으로 사용할 수 있습니다.
<code>provisioned_size</code>	정수	디스크의 가상 크기입니다.
<code>size</code>	정수	디스크의 크기입니다.
<code>actual_size</code>	정수	디스크에 할당된 실제 크기입니다.
<code>creation_date</code>	정수	디스크가 생성된 날짜입니다.
<code>bootable</code>	문자열	디스크를 부팅할 수 있는지 또는 부팅할 수 없는지에 대한 여부입니다. 유효한 값은 0 , 1 , yes , 또는 no 중 하나가 됩니다.
<code>shareable</code>	문자열	디스크를 동시에 여러 개의 가상 머신에 연결할 수 있는지에 대한 여부입니다. 유효한 값은 0 , 1 , yes , no 중 하나가 됩니다.
<code>format</code>	문자열	디스크 형식입니다. unused , unassigned , cow , 또는 raw 중 하나가 될 수 있습니다.
<code>status</code>	문자열	디스크 상태입니다. unassigned , ok , locked , invalid , 또는 illegal 중 하나가 될 수 있습니다.

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
disk_type	문자열	디스크 유형입니다. image 또는 lun 중 하나가 될 수 있습니다.
number_of_vms	정수	디스크가 연결된 가상 머신 수입니다.
vm_names	문자열	디스크가 연결된 가상 머신의 이름입니다.
quota	문자열	가상 디스크에 사용되는 쿼터 이름입니다.
sortby	목록	리소스 속성 중 하나에 따라 반환된 검색 결과를 정렬합니다.
page	정수	표시할 결과의 페이지 번호입니다.

예

Disks: format = cow and provisioned_size > 8

이 예는 다음과 같은 조건에 일치하는 가상 디스크 목록을 반환합니다:

- QCOW, 썸 프로비저닝이라고도 알려짐, 형식
- 할당된 디스크 크기가 8 GB 이상

E.1.14. 볼륨 검색

다음 표에서는 볼륨의 모든 검색 옵션에 대해 설명합니다.

표 E.10. 볼륨 검색

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
Volume.cluster-prop	속성 유형에 따라	볼륨과 관련된 클러스터 속성입니다.
Cluster	문자열	볼륨과 관련된 클러스터 이름입니다.
name	문자열	볼륨을 구별하는 읽기 쉬운 형식의 이름입니다.
type	문자열	distribute, replicate, distributed_replicate, stripe, distributed_stripe 중 하나를 지정할 수 있습니다.

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
transport_type	정수	TCP 또는 RDMA 중 하나를 지정할 수 있습니다.
replica_count	정수	복제 수입니다.
stripe_count	정수	스트라이프 수입니다.
status	문자열	블롭 상태입니다. Up 또는 Down 중 하나를 지정할 수 있습니다.
sortby	목록	리소스 속성 중 하나에 따라 반환된 검색 결과를 정렬합니다.
page	정수	표시할 결과의 페이지 번호입니다.

예

Volume: transport_type = rdma and stripe_count >= 2

이 예는 다음과 같은 블롭 목록을 반환합니다:

- RDMA로 설정된 전송 유형
- 스트라이프가 2 개 이상

E.1.15. 가상 머신 검색

다음 표에서는 가상 머신의 모든 검색 옵션에 대해 설명합니다.

표 E.11. 가상 머신 검색

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
Hosts.hosts-prop	속성 유형에 따라	가상 머신에 연결된 호스트의 속성입니다.
Templates.templates-prop	속성 유형에 따라	가상 머신에 연결된 템플릿의 속성입니다.
Events.events-prop	속성 유형에 따라	가상 머신에 연결된 이벤트의 속성입니다.
Users.users-prop	속성 유형에 따라	가상 머신에 연결된 사용자 속성입니다.
Storage.storage-prop	속성 유형에 따라	가상 머신에 연결된 스토리지 장치의 속성입니다.

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
Vnic.mac-prop	속성 유형에 따라	가상 머신에 연결된 MAC 주소 속성입니다.
name	문자열	가상 머신의 이름입니다.
status	목록	가상 머신의 사용 가능 상태입니다.
ip	정수	가상 머신의 IP 주소입니다.
uptime	정수	가상 머신이 실행되고 있는 시간 (분)입니다.
domain	문자열	이러한 시스템을 그룹화하는 도메인 (주로 Active Directory 도메인)입니다.
os	문자열	가상 머신 생성 시 선택한 운영 체제입니다.
creationdate	날짜	가상 머신이 생성된 날짜입니다.
address	문자열	네트워크 상에서 가상 머신을 구별하는 고유한 이름입니다.
cpu_usage	정수	처리 장치 사용률입니다.
mem_usage	정수	메모리 사용률입니다.
network_usage	정수	네트워크 사용률입니다.
memory	정수	정의된 최대 메모리입니다.
apps	문자열	가상 머신에 현재 설치되어 있는 애플리케이션입니다.
cluster	목록	가상 머신이 속한 클러스터입니다.
pool	목록	가상 머신이 속한 가상 머신 풀입니다.
loggedinuser	문자열	현재 가상 머신에 로그인된 사용자 이름입니다.
tag	목록	가상 머신이 속한 태그입니다.

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
datacenter	문자열	가상 머신이 속한 데이터 센터입니다.
type	목록	가상 머신 유형 (서버 또는 데스크톱)입니다.
quota	문자열	가상 머신에 연결된 쿼터 이름입니다.
description	문자열	가상 머신을 설명하는 키워드 또는 텍스트입니다. 가상 머신 생성 시 옵션으로 사용할 수 있습니다.
sortby	목록	리소스 속성 중 하나에 따라 반환된 검색 결과를 정렬합니다.
page	정수	표시할 결과의 페이지 번호입니다.

예

Vms: template.name = Win* and user.name = ""

이 예는 다음과 같은 조건에 일치하는 가상 머신 목록을 반환합니다:

- 가상 머신이 기반으로 하는 템플릿이 Win으로 시작하고 가상 머신이 다른 사용자에게 할당된 경우.

예

Vms: cluster = Default and os = windows7

이 예는 다음과 같은 조건에 일치하는 가상 머신 목록을 반환합니다:

- 가상 머신이 속한 클러스터 이름이 Default이고 가상 머신이 Windows 7 운영 체제를 실행하고 있는 경우.

E.1.16. 풀 검색

다음 표에서는 풀의 모든 검색 옵션에 대해 설명합니다.

표 E.12. 풀 검색

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
name	문자열	풀 이름입니다.
description	문자열	풀 설명입니다.
type	목록	풀 유형입니다.

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
sortBy	목록	리소스 속성 중 하나에 따라 반환된 검색 결과를 정렬합니다.
page	정수	표시할 결과의 페이지 번호입니다.

예

Pools: type = automatic

이 예는 다음과 같은 풀 목록을 반환합니다:

- 자동(automatic) 유형의 풀

E.1.17. 템플릿 검색

다음 표에서는 템플릿의 모든 검색 옵션에 대해 설명합니다.

표 E.13. 템플릿 검색

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
Vms.Vms-prop	문자열	템플릿에 연결된 가상 머신 속성입니다.
Hosts.hosts-prop	문자열	템플릿에 연결된 호스트 속성입니다.
Events.events-prop	문자열	템플릿에 연결된 이벤트 속성입니다.
Users.users-prop	문자열	템플릿에 연결된 사용자 속성입니다.
name	문자열	템플릿 이름입니다.
domain	문자열	템플릿 도메인입니다.
os	문자열	운영 체제 유형입니다.
creationdate	정수	템플릿이 생성된 날짜입니다. 날짜 형식은 mm/dd/yy입니다.
childcount	정수	템플릿에서 생성된 가상 머신 수입니다.
mem	정수	정의된 메모리입니다.

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
description	문자열	템플릿 설명입니다.
status	문자열	템플릿 상태입니다.
cluster	문자열	템플릿에 연결된 클러스터입니다.
datacenter	문자열	템플릿에 연결된 데이터 센터입니다.
quota	문자열	템플릿에 연결된 쿼터입니다.
sortby	목록	리소스 속성 중 하나에 따라 반환된 검색 결과를 정렬합니다.
page	정수	표시할 결과의 페이지 번호입니다.

예

Template: Events.severity >= normal and Vms.uptime > 0

이 예에서는 다음과 같은 템플릿 목록을 반환합니다:

- 템플릿에서 파생된 가상 머신에서 심각도가 보통 수준 이상인 이벤트가 발생하고 가상 머신이 여전히 가동되고 있는 경우.

E.1.18. 사용자 검색

다음 표에서는 사용자 용 모든 검색 옵션에 대해 설명합니다.

표 E.14. 사용자 검색

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
Vms.Vms-prop	속성 유형에 따라	사용자에 연결된 가상 머신 속성입니다.
Hosts.hosts-prop	속성 유형에 따라	사용자에 연결된 호스트 속성입니다.
Templates.templates-prop	속성 유형에 따라	사용자에 연결된 템플릿 속성입니다.
Events.events-prop	속성 유형에 따라	사용자에 연결된 이벤트 속성입니다.
name	문자열	사용자 이름입니다.

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
lastname	문자열	사용자 이름 (성)입니다.
username	문자열	사용자 고유 이름입니다.
department	문자열	사용자가 속한 부서입니다.
group	문자열	사용자가 속한 그룹입니다.
title	문자열	사용자의 직함입니다.
status	문자열	사용자의 상태입니다.
role	문자열	사용자의 역할입니다.
tag	문자열	사용자가 속한 태그입니다.
pool	문자열	사용자가 속한 풀입니다.
sortby	목록	리소스 속성 중 하나에 따라 반환된 검색 결과를 정렬합니다.
page	정수	표시할 결과의 페이지 번호입니다.

예

Users: Events.severity > normal and Vms.status = up or Vms.status = pause

이 예에서는 다음과 같은 사용자 목록을 반환합니다:

- 사용자 가상 머신에서 심각도가 중간 이상 수준인 이벤트가 발생하고 가상 머신이 여전히 가동되고 있는 경우.
- 사용자의 가상 머신이 일시 정지 되어 있는 경우.

E.1.19. 이벤트 검색

다음 표에서는 이벤트를 검색하기 위해 사용할 수 있는 모든 검색 옵션에 대해 설명합니다. 자동 입력 기능을 사용하여 여러 적절한 옵션을 표시할 수 있습니다.

표 E.15. 이벤트 검색

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
Vms.Vms-prop	속성 유형에 따라	이벤트에 연결된 가상 머신 속성입니다.
Hosts.hosts-prop	속성 유형에 따라	이벤트에 연결된 호스트 속성입니다.

속성 (리소스 또는 리소스 유형)	유형	설명 (참조)
Templates.templates-prop	속성 유형에 따라	이벤트에 연결된 템플릿 속성입니다.
Users.users-prop	속성 유형에 따라	이벤트에 연결된 사용자 속성입니다.
Clusters.clusters-prop	속성 유형에 따라	이벤트에 연결된 클러스터 속성입니다.
Volumes.Volumes-prop	속성 유형에 따라	이벤트에 연결된 볼륨 속성입니다.
type	목록	이벤트 유형입니다.
severity	목록	이벤트 심각도 (Warning/Error/Normal)입니다.
message	문자열	이벤트 유형 설명입니다.
time	목록	이벤트가 발생한 날짜입니다.
username	문자열	이벤트에 연결된 사용자 이름입니다.
event_host	문자열	이벤트에 연결된 호스트입니다.
event_vm	문자열	이벤트에 연결된 가상 머신입니다.
event_template	문자열	이벤트에 연결된 템플릿입니다.
event_storage	문자열	이벤트에 연결된 스토리지입니다.
event_datacenter	문자열	이벤트에 연결된 데이터 센터입니다.
event_volume	문자열	이벤트에 연결된 볼륨입니다.
correlation_id	정수	이벤트 식별 번호입니다.
sortby	목록	리소스 속성 중 하나에 따라 반환된 검색 결과를 정렬합니다.
page	정수	표시할 결과의 페이지 번호입니다.

예

Events: Vms.name = testdesktop and Hosts.name = gonzo.example.com

이 예에서는 다음과 같은 이벤트 목록을 반환합니다:

- **gonzo.example.com** 호스트에서 실행되는 동안 **testdesktop**이라는 가상 머신에서 발생한 이벤트입니다.

E.2. 북마크

E.2.1. 북마크로 쿼리 문자열 저장

북마크를 사용하여 검색 쿼리를 저장하고 다른 사용자와 공유할 수 있습니다.

절차 E.1. 북마크로 쿼리 문자열 저장

1. 검색 창에 원하는 검색 쿼리를 입력하고 검색을 실행합니다.
2. 검색 창 오른쪽에 있는 별표 모양의 **북마크** 버튼을 클릭하여 새 **북마크** 창을 엽니다.

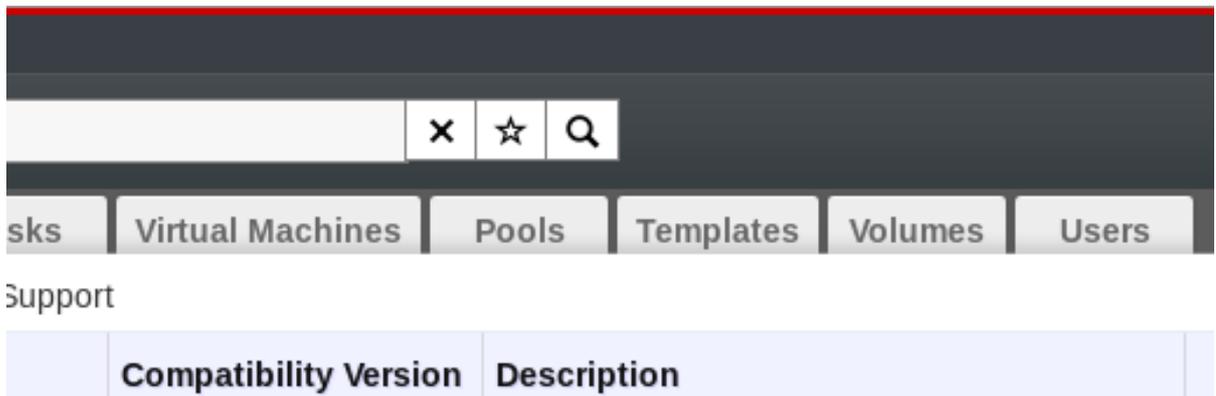


그림 E.1. 북마크 아이콘

3. 북마크의 이름을 입력합니다.
4. 검색 문자열 필드를 편집합니다 (필요한 경우).
5. **OK**를 클릭하여 쿼리를 북마크로 저장하고 창을 닫습니다.
6. 검색 쿼리가 저장되어 **북마크** 창에 표시됩니다.

북마크로 검색 쿼리를 저장하여 차후 다시 사용할 수 있습니다. **북마크** 창을 통해 북마크를 검색 및 선택합니다.

E.2.2. 북마크 편집

북마크 이름 및 검색 문자열을 수정할 수 있습니다.

절차 E.2. 북마크 편집

1. 화면 왼쪽에 있는 **북마크** 탭을 클릭합니다.
2. 편집하고자 하는 북마크를 선택합니다.

3. **편집** 버튼을 클릭하여 **북마크 편집** 창을 엽니다.
4. 필요한 경우 **이름** 및 **검색 문자열**을 변경합니다.
5. **OK**를 클릭하여 편집된 북마크를 저장합니다.

검색 쿼리의 북마크가 편집됩니다.

E.2.3. 북마크 삭제

북마크가 더이상 필요하지 않을 경우 이를 삭제합니다.

절차 E.3. 북마크 삭제

1. 화면 왼쪽의 **북마크** 탭을 클릭합니다.
2. 삭제하고자 하는 북마크를 선택합니다.
3. **삭제** 버튼을 클릭하여 **북마크 삭제** 창을 엽니다.
4. **OK**를 클릭하여 선택된 북마크를 삭제합니다.

검색 쿼리의 북마크가 삭제됩니다.

E.3. 태그

E.3.1. 태그를 사용하여 **Red Hat Virtualization**과의 상호작용을 사용자 정의

Red Hat Virtualization 플랫폼을 설치하고 요구 조건에 맞게 설정한 후 태그를 사용하여 작업할 방법을 사용자 정의할 수 있습니다. 태그는 시스템 관리자에게 중요한 장점을 제공하여 시스템 리소스를 그룹화 또는 카테고리화 할 수 있게 합니다. 이는 가상 환경에 여러 개체가 존재할 경우에 유용하며 관리자는 특정 집합 대상에 대해 집중 관리할 수 있습니다.

다음 부분에서는 태그를 생성 및 편집하여 이를 호스트 또는 가상 머신에 지정하고 태그를 사용하여 검색 기준에 따라 검색하는 방법에 대해 설명합니다. 태그는 엔터프라이즈의 요구에 맞게 구조에 따라 계층화하여 지정할 수 있습니다.

관리 포털 태그는 **태그** 창에서 생성, 수정, 삭제할 수 있습니다.

E.3.2. 태그 생성

태그를 생성하여 검색 결과를 필터링할 수 있습니다.

절차 E.4. 태그 생성

1. 화면 왼쪽의 **태그** 탭을 클릭합니다.
2. 태그를 생성하고자 하는 노드를 선택합니다. 예를 들어 최상위 레벨에 태그를 생성하려면 **root** 노드를 클릭합니다.
3. **새로 만들기** 버튼을 클릭하여 **새 태그** 창을 엽니다.
4. 새 태그의 **이름** 및 **설명**을 입력합니다.
5. **OK**를 클릭하여 태그를 생성합니다.

새 태그가 생성되어 **태그** 탭에 표시됩니다.

E.3.3. 태그 수정

태그 이름 및 설명을 수정할 수 있습니다.

절차 E.5. 태그 수정

1. 화면 왼쪽의 **태그** 탭을 클릭합니다.
2. 수정하고자 하는 태그를 선택합니다.
3. **편집**을 클릭하여 **태그 편집** 창을 엽니다.
4. 필요에 따라 **이름** 및 **설명**란을 변경합니다.
5. **OK**를 클릭하여 편집된 태그를 저장합니다.

태그 속성이 수정됩니다.

E.3.4. 태그 삭제

태그가 더 이상 필요하지 않을 경우 이를 삭제합니다.

절차 E.6. 태그 삭제

1. 화면 왼쪽의 **태그** 탭을 클릭합니다.
2. 삭제하고자 하는 태그를 선택합니다.
3. **삭제**를 클릭하여 **태그 삭제** 창을 엽니다. 태그를 삭제하면 태그의 모든 하위 항목도 삭제될 것이라는 경고 메시지가 표시됩니다.
4. **OK**를 클릭하여 선택된 태그를 삭제합니다.

태그 및 태그의 모든 하위 항목이 삭제됩니다. 태그된 모든 객체에서의 태그도 삭제됩니다.

E.3.5. 객체에서 태그 추가 및 삭제

호스트, 가상 머신, 사용자에서 태그를 지정하거나 삭제할 수 있습니다.

절차 E.7. 객체에서 태그 추가 및 삭제

1. 리소스 탭을 클릭하여 태그 지정하거나 태그 분리할 객체를 선택합니다.
2. **태그 설정** 버튼을 클릭하여 **태그 설정** 창을 엽니다.
3. 객체에 태그를 지정하기 위해 확인란을 선택하거나 객체에서 태그를 분리하기 위해 확인란을 선택 해제합니다.
4. **OK**를 클릭합니다.

선택된 객체의 사용자 정의 속성으로 지정된 태그가 추가되거나 삭제됩니다.

E.3.6. 태그를 사용하여 객체 검색

- **태그**를 사용하여 속성 및 원하는 값이나 검색 기준 값을 설정하여 검색 쿼리를 입력합니다.

지정된 기준으로 태그된 객체가 검색 결과 목록에 나열됩니다.

부록 F. 브랜딩

F.1. 브랜딩

F.1.1. Manager 재브랜딩

사용 아이콘, 팝업 창에 표시되는 텍스트, 환영 페이지에 표시되는 링크와 같이 Red Hat Virtualization Manager의 다양한 측면을 사용자 정의할 수 있습니다. 이를 통해 Manager를 재브랜딩하여 관리자 및 사용자에게 표시되는 모양을 보다 정교하게 제어할 수 있습니다.

Manager를 사용자 정의하기 위해 필요한 파일은 Manager가 설치된 시스템의 `/etc/ovirt-engine/branding/` 디렉토리에 있습니다. 이러한 파일은 그래픽 사용자 인터페이스의 다양한 측면을 스타일 설정하는데 사용하는 CSS 스타일시트 세트와 다양한 Manager 구성요서에 통합된 메시지 및 링크가 포함된 속성 파일 세트로 구성됩니다.

구성 요소를 사용자 정의하려면 구성 요소의 파일을 편집하고 변경 사항을 저장합니다. 다음 번에 구성 요소를 열거나 새로 고침한 후 변경 사항이 적용됩니다.

F.1.2. 로그인 화면

로그인 화면은 관리 포털 및 사용자 포털 모두에서 사용하는 로그인 화면입니다. 사용자 정의할 수 있는 로그인 화면 요소는 다음과 같습니다:

- 테두리
- 왼쪽의 헤더 이미지
- 오른쪽의 헤더 이미지
- 헤더 텍스트

로그인 화면 클래스는 `common.css`에 있습니다.

F.1.3. 관리 포털 화면

관리 포털 화면은 관리 포털에 로그인 시 표시되는 메인 화면입니다. 사용자 정의할 수 있는 관리 포털 화면 요소는 다음과 같습니다:

- 로고
- 왼쪽 배경 화면 이미지
- 중앙 배경 화면 이미지
- 오른쪽 배경 화면 이미지
- 로고 오른쪽 텍스트

관리 포털 화면의 클래스는 `web_admin.css`에 있습니다.

F.1.4. 사용자 포털 화면

사용자 포털 화면은 사용자 포털에 로그인 시 표시되는 화면입니다. 사용자 정의할 수 있는 사용자 포털 화면 요소는 다음과 같습니다:

- 로고
- 중앙 배경 화면 이미지
- 오른쪽 배경 화면 이미지
- 메인 그리드의 테두리
- 로그인 사용자 레이블 위의 텍스트

사용자 포털 화면의 클래스는 **user_portal.css**에 있습니다.

F.1.5. 팝업 창

팝업 창은 **Manager**에 있는 모든 창으로 호스트 또는 가상 머신과 같은 엔티티를 생성, 편집, 업데이트할 수 있습니다. 사용자 정의할 수 있는 팝업 창 요소는 다음과 같습니다:

- 테두리
- 왼쪽의 헤더 이미지
- 중앙 헤더 이미지 (반복)

팝업 창 클래스는 **common.css**에 있습니다.

F.1.6. 탭

사용자 포털에는 두 가지 유형의 탭이 있습니다. 기본 보기와 확장 보기 사이를 전환하는 주요 탭과 확장 보기 선택 시 화면 왼쪽에 표시되는 탭입니다. 관리 포털의 많은 팝업 창에도 탭이 포함되어 있습니다. 사용자 정의할 수 있는 탭 요소는 다음과 같습니다:

- 활성화
- 비활성

탭 클래스는 **common.css** 및 **user_portal.css**에 있습니다.

F.1.7. 환영 페이지

환영 페이지는 **Manager**의 홈페이지 방문 시 처음 표시되는 페이지입니다. 템플릿 파일을 편집하여 전체 모양을 사용자 지정할 수 있으며 추가 문서나 내부 웹사이트의 링크를 추가하는 것과 같은 작업을 할 수 있습니다. 사용자 지정할 수 있는 환영 페이지 요소는 다음과 같습니다:

- 페이지 제목
- 헤더 (왼쪽, 중앙, 오른쪽)
- 오류 메시지
- 대상 링크 및 링크와 관련된 메시지

환영 페이지 클래스는 **welcome_style.css**에 있습니다.

템플릿 파일

환영 페이지의 템플릿 파일은 **HTML**, **HEAD** 또는 **BODY** 태그가 포함되어 있지 않은 **welcome_page.template**이라는 일반 HTML 파일입니다. 이 파일은 환영 페이지에 직접 삽입되어 환

영 페이지에 표시되는 내용의 컨테이너로 작동합니다. 따라서 새 링크를 추가하거나 내용 자체를 변경하려면 이 파일을 편집해야 합니다. 템플릿 파일의 다른 기능은 환영 페이지 처리 시 **messages.properties** 파일에서 해당 텍스트로 변경되는 **{user_portal}**과 같은 자리 표시자 텍스트 기능입니다.

F.1.8. 페이지를 찾을 수 없음 페이지

페이지를 찾을 수 없음 (Page Not Found) 페이지는 Red Hat Virtualization Manager에서 찾을 수 없는 페이지에 대한 링크를 열 때 표시되는 페이지입니다. 페이지를 찾을 수 없음 페이지에서 사용자 정의할 수 있는 요소는 다음과 같습니다.

- 페이지 제목
- 헤더 (왼쪽, 중앙, 오른쪽)
- 오류 메시지
- 대상 링크 및 링크와 관련된 메시지

페이지를 찾을 수 없음 (Page Not Found) 페이지 클래스는 **welcome_style.css**에 있습니다.

부록 G. 시스템 계정

G.1. 시스템 계정

G.1.1. Red Hat Virtualization Manager 사용자 계정

rhev 패키지 설치 시 Red Hat Virtualization 지원을 위해 여러 개의 시스템 사용자 계정이 생성됩니다. 각 시스템 사용자는 기본 사용자 식별자(UID)가 있습니다. 다음과 같은 시스템 사용자 계정이 생성됩니다:

- **vds**m 사용자(UID 36). NFS 스토리지 도메인을 마운트하고 액세스하는 지원 도구에 필요합니다.
- **ovirt** 사용자(UID 108). **ovirt-engine** Red Hat JBoss Enterprise Application Platform 인스턴스의 소유자입니다.
- **ovirt-vmconsole** 사용자(UID 498). 게스트 시리얼 콘솔에 필요합니다.

G.1.2. Red Hat Virtualization Manager 그룹

rhev 패키지 설치 시 Red Hat Virtualization 지원을 위해 여러 개의 시스템 사용자 그룹이 생성됩니다. 각 시스템 사용자 그룹은 기본 그룹 식별자(GID)가 있습니다. 다음과 같은 시스템 사용자 그룹이 생성됩니다:

- **kvm** 그룹 (GID 36). 그룹 구성원은 다음과 같습니다:
 - **vds**m 사용자
- **ovirt** 그룹 (GID 108). 그룹 구성원은 다음과 같습니다:
 - **ovirt** 사용자
- **ovirt-vmconsole** 그룹 (GID 498). 그룹 구성원은 다음과 같습니다:
 - **ovirt-vmconsole** 사용자

G.1.3. 가상화 호스트 사용자 계정

vds 및 qemu-kvm-rhev 패키지 설치 시 가상화 호스트에 여러 개의 시스템 사용자 계정이 생성됩니다. 각 시스템 사용자는 기본 사용자 식별자(UID)가 있습니다. 다음과 같은 시스템 사용자 계정이 생성됩니다:

- **vds**m 사용자 (UID 36)
- **qemu** 사용자 (UID 107)
- **sanlock** 사용자 (UID 179)
- **ovirt-vmconsole** 사용자 (UID 498)



중요

시스템마다 사용자 식별자(UID) 및 그룹 식별자(GID)가 다를 수 있습니다. **vdsm** 사용자의 UID는 **36**으로 고정되며 **kvm** 그룹의 GID는 **36**으로 고정됩니다.

시스템의 다른 계정에서 이미 UID를 **36**으로 사용중이거나 GID를 **36**으로 사용중인 경우 **vdsm** 및 **qemu-kvm-rhev** 패키지 설치 도중 충돌이 발생합니다.

G.1.4. 가상화 호스트 그룹

vdsm 및 **qemu-kvm-rhev** 패키지 설치 시 가상화 호스트에 여러 개의 시스템 사용자 그룹이 생성됩니다. 각 시스템 사용자 그룹은 기본 그룹 식별자(GID)가 있습니다. 다음과 같은 시스템 사용자 그룹이 생성됩니다:

- **kvm** 그룹 (GID **36**). 그룹 구성원은 다음과 같습니다:
 - **qemu** 사용자
 - **sanlock** 사용자
- **qemu** 그룹 (GID **107**). 그룹 구성원은 다음과 같습니다:
 - **vdsm** 사용자
 - **sanlock** 사용자
- **ovirt-vmconsole** 그룹 (GID **498**). 그룹 구성원은 다음과 같습니다:
 - **ovirt-vmconsole** 사용자



중요

시스템마다 사용자 식별자(UID) 및 그룹 식별자(GID)가 다를 수 있습니다. **vdsm** 사용자의 UID는 **36**으로 고정되며 **kvm** 그룹의 GID는 **36**으로 고정됩니다.

시스템의 다른 계정에서 이미 UID를 **36**으로 사용중이거나 GID를 **36**으로 사용중인 경우 **vdsm** 및 **qemu-kvm-rhev** 패키지 설치 도중 충돌이 발생합니다.