



Red Hat Virtualization 4.4

관리 가이드

Red Hat Virtualization의 관리 작업

Red Hat Virtualization 4.4 관리 가이드

Red Hat Virtualization의 관리 작업

Enter your first name here. Enter your surname here.

Enter your organisation's name here. Enter your organisational division here.

Enter your email address here.

법적 공지

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Administration_Guide.ent file |.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution-Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

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, the Red Hat 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 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

이 문서에서는 Red Hat Virtualization 관리자와 관련된 정보 및 절차를 설명합니다.

차례

1장. RED HAT VIRTUALIZATION 환경 관리 및 유지 관리	14
1.1. 글로벌 설정	14
1.1.1. 역할	14
1.1.1.1. 새 역할 생성	14
1.1.1.2. 역할 편집 또는 복사	15
1.1.1.3. 사용자 역할 및 권한 부여 예	15
1.1.2. 시스템 권한	17
1.1.2.1. 사용자 속성	18
1.1.2.2. 사용자 및 관리자 역할	18
1.1.2.3. 사용자 역할 설명	19
1.1.2.4. 설명된 관리자 역할	20
1.1.2.5. 리소스에 관리자 또는 사용자 역할 할당	22
1.1.2.6. 리소스에서 관리자 또는 사용자 역할 제거	22
1.1.2.7. 데이터 센터의 시스템 권한 관리	23
1.1.2.8. 설명된 데이터 센터 관리자 역할	23
1.1.2.9. 클러스터의 시스템 권한 관리	24
1.1.2.10. 설명된 클러스터 관리자 역할	24
1.1.2.11. 네트워크의 시스템 권한 관리	25
1.1.2.12. 설명된 네트워크 관리자 및 사용자 역할	25
1.1.2.13. 호스트의 시스템 권한 관리	26
1.1.2.14. 설명된 호스트 관리자 역할	26
1.1.2.15. 스토리지 도메인의 시스템 권한 관리	27
1.1.2.16. 설명된 스토리지 관리자 역할	27
1.1.2.17. 가상 머신 풀의 시스템 권한 관리	28
1.1.2.18. 가상 머신 풀 관리자 역할 설명	28
1.1.2.19. 가상 디스크의 시스템 권한 관리	28
1.1.2.20. 가상 디스크 사용자 역할 설명	29
1.1.2.20.1. 레거시 SPICE 암호 설정	29
1.1.3. 예약 정책	30
1.1.3.1. 스케줄링 정책 생성	32
1.1.3.2. 새 스케줄링 정책의 설정 설명 및 스케줄링 정책 편집 창	32
1.1.4. 인스턴스 유형	36
1.1.4.1. 인스턴스 유형 생성	36
1.1.4.2. 인스턴스 유형 편집	37
1.1.4.3. 인스턴스 유형 제거	37
1.1.5. MAC 주소 풀	38
1.1.5.1. MAC 주소 풀 생성	38
1.1.5.2. MAC 주소 풀 편집	39
1.1.5.3. MAC 주소 풀 권한 편집	39
1.1.5.4. MAC 주소 풀 제거	40
1.2. 대시보드	40
1.2.1. 사전 요구 사항	41
1.2.2. 글로벌 인벤토리	41
1.2.3. 글로벌 사용률	43
1.2.3.1. 사용률 상위 리소스	43
1.2.4. 클러스터 사용률	44
1.2.4.1. CPU	44
1.2.4.2. 메모리	44
1.2.5. 스토리지 사용률	45
1.3. 검색	45
1.3.1. Red Hat Virtualization에서 검색 수행	45

1.3.2. 구문 및 예제 검색	45
1.3.3. 자동 완성 검색	46
1.3.4. 결과 검색 유형 옵션	47
1.3.5. 검색 기준	47
1.3.6. 검색: 다중 기준 및 와일드카드	48
1.3.7. 검색: 검색 순서 확인	49
1.3.8. 데이터 센터 검색	49
1.3.9. 클러스터 검색	49
1.3.10. 호스트 검색	50
1.3.11. 네트워크 검색	52
1.3.12. 스토리지 검색	53
1.3.13. 디스크 검색	54
1.3.14. 볼륨 검색	55
1.3.15. 가상 머신 검색	56
1.3.16. 풀 검색	59
1.3.17. 템플릿 검색	59
1.3.18. 사용자 검색	60
1.3.19. 이벤트 검색	61
1.4. 북마크	63
1.4.1. 북마크로 쿼리 문자열 저장	63
1.4.2. 북마크 편집	63
1.4.3. 북마크 삭제	63
1.5. 태그	64
1.5.1. 태그를 사용하여 Red Hat Virtualization과의 상호 작용 사용자 정의	64
1.5.2. 태그 생성	64
1.5.3. 태그 수정	64
1.5.4. 태그 삭제	64
1.5.5. 오브젝트에 태그 추가 및 제거	65
1.5.6. 태그를 사용하여 오브젝트 검색	65
1.5.7. 태그를 사용하여 호스트 사용자 지정	65
2장. 리소스 관리	66
2.1. 서비스 품질	66
2.1.1. 저장 서비스 품질	66
2.1.1.1. 스토리지 서비스 품질 생성	66
2.1.1.2. 스토리지 서비스 품질 제거	66
2.1.2. 가상 머신 네트워크 서비스 품질	67
2.1.2.1. 가상 머신 네트워크 서비스 품질 생성	67
2.1.2.2. New Virtual Machine Network QoS 및 Edit Virtual Machine Network QoS Windows의 설정 설명	67
2.1.2.3. 가상 머신 네트워크 서비스 품질 제거	68
2.1.3. 호스트 네트워크 서비스 품질	69
2.1.3.1. 호스트 네트워크 서비스 품질 생성	69
2.1.3.2. 새 호스트 네트워크 서비스 품질 및 Edit Host Network of Service Windows의 설정 설명	69
2.1.3.3. 호스트 네트워크 서비스 품질 제거	70
2.1.4. CPU 서비스 품질	70
2.1.4.1. CPU 서비스 품질 입력 생성	70
2.1.4.2. CPU 서비스 품질 제거	71
2.2. 데이터 센터	71
2.2.1. 데이터 센터 소개	71
2.2.2. 스토리지 풀 관리자	72
2.2.3. SPM 우선 순위	72
2.2.4. 데이터 센터 작업	73
2.2.4.1. 새 데이터 센터 생성	73

2.2.4.2. 새 데이터 센터의 설정 설명 및 데이터 센터 편집 창	73
2.2.4.3. 데이터 센터 다시 초기화: 복구 절차	74
2.2.4.4. 데이터 센터 제거	75
2.2.4.5. 데이터 센터를 강제로 제거	75
2.2.4.6. 데이터 센터 스토리지 유형 변경	75
2.2.4.7. 데이터 센터 호환성 버전 변경	76
2.2.5. 데이터 센터 및 스토리지 도메인	76
2.2.5.1. 데이터 센터에 기존 데이터 도메인 연결	76
2.2.5.2. 데이터 센터에 기존 ISO 도메인 연결	77
2.2.5.3. 데이터 센터에 기존 내보내기 도메인 연결	77
2.2.5.4. 데이터 센터에서 스토리지 도메인 분리	78
2.3. 클러스터	78
2.3.1. 클러스터 소개	78
2.3.2. 클러스터 작업	79
2.3.2.1. 새 클러스터 생성	79
2.3.2.2. 설명된 일반 클러스터 설정	81
2.3.2.3. 최적화 설정 설명	84
2.3.2.4. 마이그레이션 정책 설정 설명	86
2.3.2.5. 설명된 스케줄링 정책 설정	89
2.3.2.6. MaxFreeMemoryForOverUtilized 및 MinFreeMemoryForUnderUtilized 클러스터 스케줄링 정책 속성	93
2.3.2.7. 설명된 클러스터 콘솔 설정	94
2.3.2.8. 설명된 펜싱 정책 설정	94
2.3.2.9. 클러스터에서 호스트의 로드 및 전원 관리 정책 설정	95
2.3.2.10. 클러스터의 호스트에서 MoM 정책 업데이트	97
2.3.2.11. CPU 프로파일 생성	97
2.3.2.12. CPU 프로파일 제거	97
2.3.2.13. 기존 Red Hat Gluster Storage 클러스터 가져오기	98
2.3.2.14. 호스트 추가 창 설정 설명	99
2.3.2.15. 클러스터 제거	99
2.3.2.16. 메모리 최적화	99
2.3.2.17. 메모리 최적화 및 메모리 과다 할당	100
2.3.2.18. 스왑 공간 및 메모리 과다 할당	101
2.3.2.19. 메모리 과다 할당 관리자 (MoM)	101
2.3.2.20. 메모리 증대	101
2.3.2.21. KSM(Kernel Same-page Merging)	102
2.3.2.22. UEFI 및 Q35 칩셋	103
2.3.2.23. Q35œset 및 UEFI를 사용하도록 클러스터 구성	103
2.3.2.24. Q35œset 및 UEFI를 사용하도록 가상 머신 구성	104
2.3.2.25. 클러스터 호환성 버전 변경	105
2.4. 논리적 네트워크	106
2.4.1. 논리적 네트워크 작업	106
2.4.1.1. 네트워킹 작업 수행	106
2.4.1.2. 데이터 센터 또는 클러스터에서 새 논리적 네트워크 생성	107
2.4.1.3. 논리적 네트워크 편집	108
2.4.1.4. 논리적 네트워크 제거	109
2.4.1.5. 비관리 논리적 네트워크를 기본 경로로 구성	109
2.4.1.6. 호스트에 정적 경로 추가	110
2.4.1.7. 호스트에서 정적 경로 제거	112
2.4.1.8. 논리적 네트워크의 게이트웨이 보기 또는 편집	113
2.4.1.9. 논리적 네트워크 일반 설정 설명	113
2.4.1.10. 논리적 네트워크 클러스터 설정 설명	115
2.4.1.11. 논리적 네트워크 vNIC 프로파일 설정 설명	116

2.4.1.12. 네트워크 관리 창을 사용하여 논리적 네트워크의 특정 트래픽 유형 지정	116
2.4.1.13. 네트워크 관리 창에서 설정 설명	117
2.4.1.14. NIC에서 가상 기능 구성	117
2.4.2. 가상 네트워크 인터페이스 카드 (vNIC)	118
2.4.2.1. vNIC 프로파일 개요	118
2.4.2.2. vNIC 프로파일 생성 또는 편집	119
2.4.2.3. VM 인터페이스 프로파일 창에서 설정 설명	119
2.4.2.4. vNIC 프로파일에서 패스스루 활성화	121
2.4.2.5. 장애 조치로 SR-IOV 마이그레이션에 대한 vNIC 프로파일 활성화	122
2.4.2.6. vNIC 프로파일 제거	123
2.4.2.7. vNIC 프로파일 보안 그룹 할당	123
2.4.2.8. vNIC 프로파일의 사용자 권한	124
2.4.3. 외부 프로바이더 네트워크	124
2.4.3.1. 외부 공급자에서 네트워크 가져오기	124
2.4.3.2. 외부 프로바이더 네트워크 사용 제한	125
2.4.3.3. 외부 프로바이더 논리적 네트워크에서 서브넷 구성	125
2.4.3.4. 외부 공급자 논리적 네트워크에 서브넷 추가	125
2.4.3.5. 외부 공급자 논리적 네트워크에서 서브넷 제거	126
2.4.3.6. 논리적 네트워크 및 포트에 보안 그룹 할당	126
2.4.4. 호스트 및 네트워킹	127
2.4.4.1. 네트워크 관리자 상태 저장 설정 (nmstate)	127
2.4.4.2. 호스트 기능 새로 고침	128
2.4.4.3. 호스트 네트워크 인터페이스 편집 및 호스트에 논리적 네트워크 할당	128
2.4.4.4. 호스트 네트워크 동기화	132
2.4.4.5. 호스트의 VLAN 설정 편집	134
2.4.4.6. 논리적 네트워크를 사용하여 단일 네트워크 인터페이스에 여러 VLAN 추가	134
2.4.4.6.1. 호스트 네트워크 복사	135
2.4.4.7. 호스트 네트워크에 추가 IPv4 주소 할당	136
2.4.4.8. 호스트 네트워크 인터페이스에 네트워크 레이블 추가	137
2.4.4.8.1. LLDP 라벨러 구성	138
2.4.4.9. 호스트의 FQDN 변경	139
2.4.4.9.1. IPv6 네트워킹 지원	140
2.4.4.9.2. SR-IOV 설정 및 구성	141
2.4.5. 네트워크 연결	143
2.4.5.1. 본딩 방법	143
2.4.5.2. 관리 포털에서 본드 장치 생성	144
2.4.5.3. LLDP 라벨러 서비스를 사용하여 본드 장치 생성	146
2.4.5.3.1. LLDP 라벨러 구성	146
2.4.5.4. 본딩 모드	148
2.5. 호스트	149
2.5.1. 호스트 소개	149
2.5.2. Red Hat Virtualization Host	151
2.5.3. Red Hat Enterprise Linux 호스트	152
2.5.4. Satellite 호스트 공급자 호스트	152
2.5.5. 호스트 작업	153
2.5.5.1. Red Hat Virtualization Manager에 표준 호스트 추가	153
2.5.5.2. Satellite 호스트 공급자 호스트 추가	154
2.5.5.3. 호스트의 Satellite 에라타 보기 설정	156
2.5.5.3.1. PCI 패스스루에 대한 호스트 구성	157
2.5.5.3.2. 모든 가상 머신에 중첩된 가상화 활성화	159
2.5.5.3.3. 개별 가상 머신에 중첩된 가상화 활성화	161
2.5.5.4. 호스트를 유지 관리 모드로 이동	164
2.5.5.5. 유지 관리 모드에서 호스트 활성화	166

2.5.5.5.1. 호스트 방화벽 규칙 구성	166
2.5.5.5.2. 호스트 제거	167
2.5.5.5.3. 마이너 릴리스 간 호스트 업데이트	168
2.5.5.5.4. 호스트 재설치	176
2.5.5.6. 호스트 에라타 보기	178
2.5.5.7. 호스트의 상태 보기	178
2.5.5.8. 호스트 장치 보기	179
2.5.5.9. 관리 포털에서 Cockpit에 액세스	180
2.5.5.9.1. 레거시 SPICE 암호 설정	180
2.5.5.10. 호스트 전원 관리 설정 구성	181
2.5.5.11. 호스트 스토리지 풀 관리자 설정 구성	184
2.5.5.11.1. 자체 호스팅 엔진 호스트를 다른 클러스터로 마이그레이션	184
2.5.6. 새 호스트 및 호스트 편집 창의 설정 및 제어 설명	185
2.5.6.1. 설명된 호스트 일반 설정	185
2.5.6.2. 설명된 호스트 전원 관리 설정	187
2.5.6.3. 설명된 SPM 우선 순위 설정	191
2.5.6.4. 설명된 호스트 콘솔 설정	191
2.5.6.5. 설명된 네트워크 공급자 설정	192
2.5.6.6. 설명된 커널 설정	192
2.5.6.7. 호스트 엔진 설정 설명	194
2.5.7. 호스트 복원력	194
2.5.7.1. 호스트 고가용성	194
2.5.7.2. Red Hat Virtualization에서 프록시로 전원 관리	195
2.5.7.3. 호스트에서 펜싱 매개 변수 설정	196
2.5.7.4. fence_kdump 고급 구성	198
2.5.7.5. fence_kdump 리스너 구성	199
2.5.7.6. Manager에서 fence_kdump 구성	201
2.5.7.7. 소프트 펜싱 호스트	203
2.5.7.8. 호스트 전원 관리 기능 사용	204
2.5.7.9. 응답이 없는 호스트 수동 펜싱 또는 격리	205
2.6. 스토리지	206
2.6.1. Red Hat Virtualization 스토리지 정보	206
2.6.2. 스토리지 도메인 이해	208
2.6.3. NFS 스토리지 준비 및 추가	208
2.6.3.1. NFS 스토리지 준비	208
2.6.3.2. NFS 스토리지 추가	210
2.6.3.3. NFS 스토리지 증가	212
2.6.4. 로컬 스토리지 준비 및 추가	212
2.6.4.1. 로컬 스토리지 준비	213
2.6.4.2. 로컬 스토리지 도메인 추가	213
2.6.5. POSIX 호환 파일 시스템 스토리지 준비 및 추가	215
2.6.5.1. POSIX 호환 파일 시스템 스토리지 준비	215
2.6.5.2. POSIX 호환 파일 시스템 스토리지 추가	215
2.6.6. 블록 스토리지 준비 및 추가	217
2.6.6.1. iSCSI 스토리지 준비	217
2.6.6.2. iSCSI 스토리지 추가	218
2.6.6.3. iSCSI Multipathing 구성	221
2.6.6.4. 논리적 네트워크를 iSCSI 본드로 마이그레이션	222
2.6.6.5. FCP 스토리지 준비	224
2.6.6.6. FCP 스토리지 추가	225
2.6.6.7. iSCSI 또는 FCP 스토리지 증가	227
2.6.6.8. LUN 재사용	229
2.6.6.9. 오래된 LUN 제거	230

2.6.6.10. LVM 필터 생성	231
2.6.7. Red Hat Gluster Storage 준비 및 추가	234
2.6.7.1. Red Hat Gluster Storage 준비	234
2.6.7.2. Red Hat Gluster Storage 추가	234
2.6.8. 기존 스토리지 도메인 가져오기	234
2.6.8.1. 기존 스토리지 도메인 가져오기 개요	234
2.6.8.2. 스토리지 도메인 가져오기	235
2.6.8.3. 동일한 환경에서 데이터 센터 간에 스토리지 도메인 마이그레이션	237
2.6.8.4. 다른 환경에서 데이터 센터 간 스토리지 도메인 마이그레이션	239
2.6.8.5. 가져온 데이터 스토리지 도메인에서 템플릿 가져오기	242
2.6.9. 스토리지 작업	243
2.6.9.1. 데이터 스토리지 도메인에 이미지 업로드	243
2.6.9.2. 스토리지 도메인에 VirtIO 이미지 파일 업로드	244
2.6.9.3. ISO 도메인에 이미지 업로드	245
2.6.9.4. 스토리지 도메인을 유지 관리 모드로 이동	247
2.6.9.5. 스토리지 도메인 편집	248
2.6.9.6. OVF 업데이트	250
2.6.9.7. 유지 관리 모드에서 스토리지 도메인 활성화	250
2.6.9.8. 데이터 센터에서 스토리지 도메인 분리	251
2.6.9.9. 데이터 센터에 스토리지 도메인 연결	252
2.6.9.10. 스토리지 도메인 제거	252
2.6.9.11. 스토리지 도메인 삭제	253
2.6.9.12. 디스크 프로필 생성	254
2.6.9.13. 디스크 프로파일 제거	254
2.6.9.14. 스토리지 도메인의 상태 보기	255
2.6.9.15. 스토리지 도메인 삭제 후 비활성화 설정	256
2.6.9.16. 250개 이상의 호스트가 있는 환경에서 4K 지원 활성화	256
2.6.9.17. 4K 지원 비활성화	257
2.6.9.18. 스토리지 도메인에서 사용 가능한 공간 모니터링	258
2.7. 풀	259
2.7.1. 가상 머신 풀 소개	259
2.7.2. 가상 머신 풀 생성	260
2.7.3. 새 풀 및 풀 편집 창의 설정 및 제어 설명	267
2.7.3.1. 새 풀 및 풀 편집 일반 설정 설명	267
2.7.3.2. 새 풀 및 풀 유형 설정 편집 설명	268
2.7.3.3. 설명된 새 풀 및 풀 콘솔 설정 편집	268
2.7.3.4. 설명된 가상 머신 풀 호스트 설정	269
2.7.3.5. 새 풀 및 풀 리소스 할당 설정 편집 설명	275
2.7.3.6. 가상 머신 풀 편집	276
2.7.3.7. 풀에서 가상 머신 사전 시작	276
2.7.3.8. 가상 머신 풀에 가상 머신 추가	277
2.7.3.9. 가상 머신 풀에서 가상 머신 분리	277
2.7.3.10. 가상 머신 풀 제거	278
2.8. 가상 디스크	278
2.8.1. 가상 머신 스토리지 이해	278
2.8.2. 가상 디스크 이해	279
2.8.3. 삭제 후 가상 디스크를 초기화하는 설정	281
2.8.4. Red Hat Virtualization에서 공유 가능한 디스크	283
2.8.5. Red Hat Virtualization에서 디스크만 읽기	283
2.8.6. 가상 디스크 작업	283
2.8.6.1. 가상 디스크 생성	283
2.8.6.2. New Virtual Disk(새 가상 디스크) 창의 설정 설명	285
2.8.6.3. 실시간 스토리지 마이그레이션 개요	290

2.8.6.4. 가상 디스크 이동	291
2.8.6.5. 디스크 인터페이스 유형 변경	292
2.8.6.6. 가상 디스크 복사	293
2.8.6.7. 디스크 성능 향상	294
2.8.6.8. 데이터 스토리지 도메인에 이미지 업로드	296
2.8.6.9. 가져온 스토리지 도메인에서 디스크 이미지 가져오기	296
2.8.6.10. 가져온 스토리지 도메인에서 등록되지 않은 디스크 이미지 가져오기	297
2.8.6.11. OpenStack 이미지 서비스에서 가상 디스크 가져오기	297
2.8.6.12. OpenStack 이미지 서비스로 가상 디스크 내보내기	298
2.8.6.13. 가상 디스크 공간 회수	299
2.9. 외부 공급자	300
2.9.1. Red Hat Virtualization에서 외부 공급자 소개	300
2.9.2. 외부 공급자 추가	302
2.9.2.1. 호스트 프로비저닝용 Red Hat Satellite 인스턴스 추가	302
2.9.2.2. 이미지 관리를 위한 OpenStack 이미지(Glance) 인스턴스 추가	303
2.9.2.3. KubeVirt/OpenShift Virtualization을 외부 공급자로 추가	304
2.9.2.4. 가상 머신 공급자로 VMware 인스턴스 추가	306
2.9.2.5. 가상 머신 공급자로 RHEL 5 Xen Host 추가	308
2.9.2.6. KVM 호스트를 가상 머신 공급자로 추가	309
2.9.2.7. OVN(Open Virtual Network)을 외부 네트워크 공급자로 추가	311
2.9.2.7.1. 새 OVN 네트워크 공급자 설치	311
2.9.2.7.2. 단일 호스트에서 OVN 터널 네트워크 업데이트	314
2.9.2.7.3. 물리적 네트워크에 OVN 네트워크 연결	314
2.9.2.8. 설명된 공급자 일반 설정 추가	316
2.9.3. 외부 공급자 편집	321
2.9.4. 외부 공급자 제거	321
3장. 환경 관리	322
3.1. 셀프 호스트 엔진 관리	322
3.1.1. 셀프 호스트 엔진 유지 관리	322
3.1.1.1. 자체 호스팅 엔진 유지 관리 모드 설명	322
3.1.1.2. 로컬 유지 관리 모드 설정	322
3.1.1.3. 글로벌 유지 관리 모드 설정	323
3.1.2. Manager 가상 머신 관리	324
3.1.2.1. 셀프 호스트 엔진 구성 업데이트	324
3.1.2.2. 이메일 알림 구성	325
3.1.3. 추가 호스트에서 셀프 호스트 엔진에 대한 메모리 예약 구성	326
3.1.4. Red Hat Virtualization Manager에 자체 호스트 엔진 노드 추가	327
3.1.5. 기존 호스트를 자체 호스팅 엔진 노드로 다시 설치	328
3.1.6. 복구 모드에서 관리자 가상 머신 부팅	329
3.1.7. 자체 호스트 엔진 환경에서 호스트 제거	331
3.1.8. 자체 호스팅 엔진 업데이트	332
글로벌 유지 관리 모드 활성화	332
Red Hat Virtualization Manager 업데이트	332
전역 유지 관리 모드 비활성화	334
3.1.9. 자체 호스팅 엔진에서 관리자의 FQDN 변경	335
3.2. 백업 및 마이그레이션	335
3.2.1. Red Hat Virtualization Manager 백업 및 복원	335
3.2.1.1. Red Hat Virtualization Manager 백업 - 개요	335
3.2.1.2. engine-backup 명령의 구문	335
3.2.1.3. engine-backup 명령으로 백업 생성	337
3.2.1.4. engine-backup 명령을 사용하여 백업 복원	339
3.2.1.5. 이전 설치로 백업 복원	340

3.2.1.6. 기존 설치를 덮어쓰도록 백업 복원	341
3.2.1.7. 다른 인증 정보를 사용하여 백업 복원	342
3.2.1.8. 자체 호스팅 엔진 백업 및 복원	345
3.2.1.8.1. 원래 관리자 백업	346
3.2.1.8.2. 새로운 자체 호스팅 엔진에서 백업 복원	348
3.2.1.8.3. Red Hat Virtualization Manager 리포지토리 활성화	353
3.2.1.8.4. 호스트 재설치	355
3.2.1.8.5. 스토리지 도메인 제거	357
3.2.1.9. 기존 백업에서 자체 호스팅 엔진 복구	358
3.2.1.9.1. 새로운 자체 호스팅 엔진에서 백업 복원	359
3.2.1.9.2. Red Hat Virtualization Manager 리포지토리 활성화	364
3.2.1.9.3. 호스트 재설치	366
3.2.1.9.4. 스토리지 도메인 제거	368
3.2.1.10. 기존 백업에서 자체 호스팅 엔진 덮어쓰기	369
3.2.1.10.1. 글로벌 유지 관리 모드 활성화	369
3.2.1.10.2. 기존 설치를 덮어쓰도록 백업 복원	370
3.2.1.10.3. 전역 유지 관리 모드 비활성화	371
3.2.2. 별도의 머신으로 데이터 software software to a Separate Machine으로 마이그레이션	372
3.2.2.1. 별도의 머신으로 데이터 웨어하우스 데이터베이스 마이그레이션	373
3.2.2.1.1. Red Hat Virtualization Manager 리포지토리 활성화	373
3.2.2.1.2. 별도의 머신으로 데이터 웨어하우스 데이터베이스 마이그레이션	375
3.2.2.2. 별도의 머신으로 데이터 웨어하우스 서비스 마이그레이션	376
3.2.2.2.1. 새 데이터 웨어하우스 머신 설정	377
3.2.2.2.2. 관리자 시스템에서 데이터 웨어하우스 서비스 중지	379
3.2.2.2.3. 새 데이터 웨어하우스 머신 구성	379
3.2.2.2.4. 관리자 시스템에서 데이터 웨어하우스 서비스 비활성화	381
3.2.3. 백업 스토리지 도메인을 사용하여 가상 머신 백업 및 복원	381
3.2.3.1. 백업 스토리지 도메인 설명	382
3.2.3.2. 데이터 스토리지 도메인을 백업 도메인으로 설정	383
3.2.3.3. 백업 도메인을 사용하여 가상 머신 또는 스냅샷 백업 또는 복원	384
3.2.4. 백업 및 복원 API를 사용하여 가상 머신 백업 및 복원	385
3.2.4.1. 백업 및 복원 API	385
3.2.4.2. 가상 머신 백업	385
3.2.4.3. 가상 머신 복원	388
3.2.5. 증분 백업 및 복원 API를 사용하여 가상 머신 백업 및 복원	390
3.2.5.1. 증분 백업 및 복원 API	390
3.2.5.1.1. 증분 백업 흐름	392
3.2.5.1.2. 증분 복원 흐름	393
3.2.5.1.3. 증분 백업 및 복원 API 작업	394
3.2.5.1.4. 새 가상 디스크에서 증분 백업 활성화	395
3.2.5.1.5. 기존 RAW 가상 디스크에서 증분 백업 활성화	396
3.2.5.1.6. 증분 백업 활성화	397
3.2.5.1.7. 증분 백업에 활성화된 디스크 찾기	397
3.2.5.1.8. 전체 백업 시작	398
3.2.5.1.9. 증분 백업 시작	400
3.2.5.1.10. 백업에 대한 정보 가져오기	402
3.2.5.1.11. 백업의 디스크에 대한 정보 가져오기	403
3.2.5.1.12. 백업 종료	404
3.2.5.1.13. 증분 백업을 위한 이미지 전송 오브젝트 생성	405
3.2.5.1.14. 증분 복원을 위한 이미지 전송 오브젝트 생성	406
3.2.5.1.15. 가상 머신의 체크 포인트 나열	407
3.2.5.1.16. 가상 머신의 특정 checkpoint 나열	408
3.2.5.1.17. checkpoint 제거	409

3.2.5.1.18. imageio API를 사용하여 백업 데이터 전송	409
3.3. RED HAT SATELLITE를 사용하여 에라타 보기 설정	410
3.4. 인증서가 만료되기 전에 갱신	412
3.5. ANSIBLE을 사용하여 구성 작업 자동화	414
3.5.1. oVirt Ansible 컬렉션	414
3.5.1.1. RPM 패키지에서 oVirt Ansible 컬렉션 설치	414
3.5.1.2. Automation Hub에서 oVirt Ansible 컬렉션 설치	415
3.5.1.3. oVirt Ansible Collection을 사용하여 Red Hat Virtualization 구성	416
3.6. 사용자 및 역할	417
3.6.1. 사용자 소개	417
3.6.2. 디렉터리 서버 소개	417
3.6.3. 외부 LDAP 공급자 구성	419
3.6.3.1. 외부 LDAP 공급자 구성(Interactive Setup)	419
3.6.3.2. Active Directory 연결	425
3.6.3.3. 외부 LDAP 공급자 구성(수동 방법)	430
3.6.3.4. 외부 LDAP 공급자 제거	433
3.6.4. Single Sign-on용 LDAP 및 Kerberos 구성	434
3.6.4.1. Apache 서비스에 대한 Kerberos 구성	435
3.6.5. Red Hat Single Sign-On 설치 및 구성	440
3.6.5.1. Red Hat SSO 설치	441
3.6.5.2. LDAP 그룹 매핑 구성	441
3.6.5.3. Manager에서 Apache 구성	443
3.6.5.4. OVN 구성	446
3.6.5.5. 모니터링 포털 구성(Grafana)	446
3.6.6. 사용자 권한 부여	448
3.6.6.1. 사용자 권한 부여 모델	448
3.6.6.2. 사용자 작업	449
3.6.7. 관리 포털에서 사용자 작업 관리	449
3.6.7.1. 사용자 추가 및 VM 포털 권한 할당	449
3.6.7.2. 사용자 정보 보기	450
3.6.7.3. 리소스에 대한 사용자 권한 보기	450
3.6.7.4. 사용자 제거	451
3.6.7.5. 로그인된 사용자 보기	451
3.6.7.6. 사용자 세션 종료	451
3.6.8. 명령줄에서 사용자 작업 관리	452
3.6.8.1. 새 사용자 생성	452
3.6.8.2. 사용자 암호 설정	452
3.6.8.3. 사용자 시간 제한 설정	453
3.6.8.4. 사용자 암호 사전 암호화	454
3.6.8.5. 사용자 정보 보기	455
3.6.8.6. 사용자 정보 편집	455
3.6.8.7. 사용자 제거	455
3.6.8.8. 내부 관리 사용자 비활성화	455
3.6.8.9. 그룹 관리	456
3.6.8.10. 사용자 및 그룹 쿼리	457
3.6.8.11. 계정 설정 관리	459
3.6.9. 추가 로컬 도메인 구성	459
3.7. 쿼터 및 서비스 수준 계약 정책	460
3.7.1. 할당량 소개	460
3.7.2. 공유 할당량 및 개별적으로 정의된 할당량	462
3.7.3. 할당량 계정	462
3.7.4. 데이터 센터에서 쿼터 모드 활성화 및 변경	463
3.7.5. 새 할당량 정책 생성	463

3.7.6. 쿼터 임계값 설정 설명	465
3.7.7. 오브젝트에 할당량 할당	466
3.7.8. 할당량을 사용하여 사용자별 리소스 제한	467
3.7.9. 할당량 편집	468
3.7.10. 할당량 제거	468
3.7.11. 서비스 수준 계약 정책 시행	468
3.8. 이벤트 알림	469
3.8.1. 관리 포털에서 이벤트 알림 구성	469
3.8.2. 관리 포털에서 이벤트 알림 취소	471
3.8.3. ovirt-engine-notifier.conf의 이벤트 알림 매개 변수	472
3.8.4. SNMP 트랩을 전송하도록 Red Hat Virtualization Manager 구성 cookie-Always 설정 파일 샘플	477 481
3.9. 유틸리티	483
3.9.1. oVirt 엔진 이름 바꾸기 도구	483
3.9.1.1. oVirt 엔진 이름 바꾸기 도구	483
3.9.1.2. oVirt Engine Rename 명령 구문	485
3.9.1.3. oVirt Engine 이름 바꾸기 도구로 관리자 이름 변경	485
3.9.2. 엔진 설정 도구	487
3.9.2.1. 엔진 설정 도구	487
3.9.2.2. engine-config 명령의 구문	487
3.9.3. USB 필터 편집기	488
3.9.3.1. USB 필터 편집기 설치	488
3.9.3.2. USB 필터 편집기 인터페이스	489
3.9.3.3. USB 정책 추가	490
3.9.3.4. USB 정책 제거	491
3.9.3.5. USB 장치 정책 검색	492
3.9.3.6. USB 정책 내보내기	492
3.9.3.7. USB 정책 가져오기	493
3.9.4. 이미지 불일치 툴	494
3.9.4.1. 이미지 불일치 툴을 사용하여 스냅샷 상태 모니터링	494
3.9.5. 로그 수집기 도구	495
3.9.5.1. Log Collector	495
3.9.5.2. ovirt-log-collector 명령의 구문	496
3.9.5.3. 기본 로그 수집기 사용	500
3.9.6. 엔진 툴	500
3.9.6.1. 엔진 툴	500
3.9.6.2. 엔진 툴킷 모드	501
3.9.6.3. engine-vacuum 명령 구문	501
3.9.7. 네트워크 이름 매핑 도구에 대한 VDSM	502
3.9.7.1. VDSM 이름을 논리적 네트워크 이름에 매핑	502
4장. 환경에 대한 정보 수집	504
4.1. 모니터링 및 관찰 기능	504
4.1.1. 데이터 웨어하우스 및 Grafana를 사용하여 RHV 모니터링	504
4.1.1.1. Grafana 개요	504
4.1.1.2. 설치	505
4.1.1.2.1. Single Sign-on에 대한 Grafana 구성	506
4.1.1.3. 기본 제공 Grafana 대시보드	507
4.1.1.4. 사용자 정의된 Grafana 대시보드	510
4.1.2. Elasticsearch의 원격 인스턴스에 지표 및 로그 전송	510
4.1.2.1. collectd 및 rsyslog 설치	510
4.1.2.2. 로깅 스키마 및 로그 분석	511
4.1.3. Insights 배포	513

4.1.3.1. 시스템을 Red Hat Insights에 등록	513
4.1.3.2. Red Hat Virtualization 환경에서 데이터 수집 활성화	513
4.1.3.3. Insights 콘솔에서 Insights 결과 보기	513
4.2. 로그 파일	514
4.2.1. Manager 설치 로그 파일	514
4.2.2. Red Hat Virtualization Manager 로그 파일	515
4.2.3. SPICE 로그 파일	515
4.2.3.1. 하이퍼바이저 SPICE 서버용 SPICE 로그	516
4.2.3.2. 게스트 머신 용 SPICE 로그	516
4.2.3.3. console.vv 파일을 사용하여 시작되는 SPICE 클라이언트를 위한 SPICE 로그	516
4.2.4. 호스트 로그 파일	517
4.2.5. Red Hat Virtualization 서비스에 대한 디버그 수준 로깅 설정	518
4.2.6. Red Hat Virtualization 서비스의 기본 설정 파일	519
4.2.7. 호스트 로깅 서버 설정	520
4.2.8. SyslogHandler를 활성화하여 RHV Manager 로그를 원격 syslog 서버에 전달	521
부록 A. VDSM 서비스 및 후크	523
A.1. VDSM 후크 설치	523
A.2. 지원되는 VDSM 이벤트	524
A.3. VDSM 후크 환경	527
A.4. VDSM 후크 도메인 XML 객체	527
A.5. 사용자 정의 속성 정의	528
A.6. 가상 머신 사용자 정의 속성 설정	530
A.7. VDSM 후크에서 가상 머신 사용자 정의 속성 평가	530
A.8. VDSM 후크 모듈 사용	531
A.9. VDSM 후크 실행	531
A.10. VDSM 후크 반환 코드	532
A.11. VDSM 후크 예	533
부록 B. 사용자 정의 네트워크 속성	536
B.1. BRIDGE_OPTS 매개변수 설명	536
B.2. ETHTOOL을 사용하도록 RED HAT VIRTUALIZATION MANAGER 설정 방법	538
B.3. FCOE 사용을 위해 RED HAT VIRTUALIZATION MANAGER 설정 방법	538
부록 C. RED HAT VIRTUALIZATION 사용자 인터페이스 플러그인	540
C.1. RED HAT VIRTUALIZATION 사용자 인터페이스 플러그인 정보	540
C.2. RED HAT VIRTUALIZATION 사용자 인터페이스 플러그인 라이프 사이클	540
C.2.1. Red Hat Virtualization 사용자 인터페이스 플러그인 검색	540
C.2.2. Red Hat Virtualization 사용자 인터페이스 플러그인 로딩	541
C.2.3. Red Hat Virtualization 사용자 인터페이스 플러그인 부트스트래핑	541
C.3. 사용자 인터페이스 플러그인 관련 파일 및 위치	542
C.4. 사용자 인터페이스 플러그인 배포 예	543
부록 D. RED HAT VIRTUALIZATION에서 FIPS 활성화	545
D.1. 자체 호스팅 엔진에서 FIPS 활성화	545
D.2. RHV 호스트 및 독립 실행형 관리자에서 FIPS 활성화	546
D.3. 추가 리소스	546
부록 E. RED HAT VIRTUALIZATION 및 암호화된 통신	547
E.1. RED HAT VIRTUALIZATION MANAGER CA 인증서 교체	547
E.1.1. P12 번들에서 인증서 및 개인 키 추출	547
E.1.2. Red Hat Virtualization Manager Apache CA 인증서 교체	548
E.2. 관리자와 LDAP 서버 간의 암호화된 통신 설정	551
E.3. FIPS에 대해 암호화된 VNC 콘솔 활성화	553

E.3.1. VNC 암호화를 활성화하도록 클러스터 구성	553
E.3.2. 각 호스트에 대해 VNC SASL Ansible 플레이북 실행 VNC SASL Ansible Playbook 오류 메시지	554 555
E.3.3. 관리자의 CA 인증서를 신뢰하도록 Remote Viewer 구성	556
부록 F. 프록시	558
F.1. SPICE 프록시	558
F.1.1. SPICE 프록시 개요	558
F.1.2. SPICE 프록시 머신 설정	558
F.1.3. SPICE 프록시 활성화	559
F.1.4. SPICE 프록시 끄기	560
F.2. SQUID 프록시	560
F.2.1. Squid 프록시 설치 및 구성	560
F.3. WEBSOCKET 프록시	564
F.3.1. WebSocket 프록시 개요	564
부록 G. 브랜딩	565
G.1. 브랜딩	565
G.1.1. 관리자 재분산	565
G.1.2. 로그인 화면	565
G.1.3. 관리 포털 화면	565
G.1.4. VM 포털 화면	566
G.1.5. Windows 팝업	567
G.1.6. 탭	567
G.1.7. 시작 페이지	567
G.1.8. 페이지를 찾을 수 없음	568
부록 H. 시스템 계정	570
H.1. RED HAT VIRTUALIZATION MANAGER 사용자 계정	570
H.2. RED HAT VIRTUALIZATION MANAGER 그룹	570
H.3. 가상화 호스트 사용자 계정	571
H.4. 가상화 호스트 그룹	571
부록 I. 법적 공지	573

1장. RED HAT VIRTUALIZATION 환경 관리 및 유지 관리

Red Hat Virtualization 환경에서는 관리자가 계속 실행되도록 해야 합니다. 관리자는 다음과 같은 작업을 수행합니다.

- 호스트 및 가상 시스템 등의 물리적 리소스와 가상 리소스 관리. 여기에는 호스트 업그레이드 및 추가, 도메인 가져오기, 외부 하이퍼바이저에서 생성된 가상 시스템 변환, 가상 시스템 풀 관리 등이 포함됩니다.
- 호스트 중 하나에서 극심한 부하, 메모리 또는 디스크 공간이 부족하고 필요한 작업을 수행하는 등의 잠재적 문제에 대해 전체 시스템 리소스를 모니터링합니다(예: 시스템을 종료하여 가상 시스템을 다른 호스트로 마이그레이션하여 부하를 줄이거나 리소스를 확보하는 등).
- 가상 시스템의 새로운 요구 사항에 대응(예: 운영 체제 업그레이드 또는 메모리 할당).
- 태그를 사용하여 사용자 지정된 오브젝트 속성 관리.
- [공개 북마크](#)로 저장된 검색 관리.
- 사용자 설정 및 권한 수준 설정 관리.
- 전체 시스템 기능을 위한 특정 사용자 또는 가상 시스템의 문제 해결.
- 일반 및 특정 보고서 생성.

1.1. 글로벌 설정

Administration(관리) Configure(구성) 창을 클릭하여 액세스하면 사용자, 역할, 시스템 권한, 스케줄링 정책, 인스턴스 유형 및 MAC 주소 풀과 같은 Red Hat Virtualization 환경에 대한 여러 글로벌 리소스를 구성할 수 있습니다. 이 창을 사용하면 사용자가 환경의 리소스와 상호 작용하는 방법을 사용자 지정하고 여러 클러스터에 적용할 수 있는 옵션을 구성하는 중앙 위치를 제공합니다.

1.1.1. 역할

역할은 Red Hat Virtualization Manager에서 구성할 수 있는 사전 정의된 권한 세트입니다. 역할은 데이터 센터의 다양한 리소스 수준과 특정 실체 및 가상 리소스에 대한 액세스 및 관리 권한을 제공합니다.

다단계 관리를 사용하면 컨테이너 오브젝트에 적용되는 모든 권한이 해당 컨테이너 내의 모든 개별 오브젝트에도 적용됩니다. 예를 들어 호스트 관리자 역할이 특정 호스트의 사용자에게 할당되면 사용자는 할당된 호스트에서만 사용 가능한 호스트 작업을 수행할 수 있는 권한을 얻게 됩니다. 그러나 호스트 관리자 역할이 데이터 센터의 사용자에게 할당되면 사용자는 데이터 센터 클러스터에 있는 모든 호스트에서 호스트 작업을 수행할 수 있는 권한을 얻게 됩니다.

1.1.1.1. 새 역할 생성

Red Hat Virtualization의 기본 역할 목록에 필요한 역할이 없는 경우 새 역할을 생성하고 사용자의 목적에 맞게 사용자 지정할 수 있습니다.

절차

1. **Administration(관리) Configure(구성)** 를 클릭합니다. 그러면 **Configure(구성)** 창이 열립니다. **Roles(역할)** 탭은 기본적으로 선택되어 기본 User 및 Administrator 역할 목록과 사용자 지정 역할을 표시합니다.
2. **New (새로 만들기)**를 클릭합니다.

3. 새 역할의 **Name** (이름) 및 **Description** (설명)을 입력합니다.
4. **Admin**(관리) 또는 **User** (사용자)를 **Account Type**(계정 유형)으로 선택합니다.
5. **Check Boxes**(작업 허용) 목록에 나열된 오브젝트에 대한 권한 수를 보려면 **Expand All** (모두 확장) 또는 **Collapse All** (모든 축소) 버튼을 사용합니다. 각 오브젝트에 대한 옵션을 확장하거나 축소할 수도 있습니다.
6. 각 오브젝트에 대해 설정 중인 역할에 대해 허용하거나 거부할 작업을 선택하거나 지웁니다.
7. **OK**(확인)를 클릭하여 변경 사항을 적용합니다. 새 역할은 역할 목록에 표시됩니다.

1.1.1.2. 역할 편집 또는 복사

생성한 역할의 설정을 변경할 수 있지만 기본 역할은 변경할 수 없습니다. 기본 역할을 변경하려면 요구 사항에 맞게 복제하고 수정합니다.

절차

1. **Administration**(관리) **Configure**(구성)를 클릭합니다. 그러면 기본 User 및 Administrator 역할 목록과 사용자 지정 역할을 표시하는 **Configure** (구성) 창이 열립니다.
2. 변경할 역할을 선택합니다.
3. **Edit**(편집) 또는 **Copy** (복사)를 클릭합니다. 그러면 **Edit Role or Copy Role**(역할 편집 또는 복사 역할 편집) 창이 열립니다.
4. 필요한 경우 역할의 **Name** (이름) 및 **Description** (설명)을 편집합니다.
5. 나열된 오브젝트에 대한 권한 중 하나 이하를 보려면 **Expand All**(모두 확장) 또는 **Collapse All** (모든 축소) 버튼을 사용합니다. 각 오브젝트에 대한 옵션을 확장하거나 축소할 수도 있습니다.
6. 각 오브젝트에 대해 편집 중인 역할에 대해 허용 또는 거부할 작업을 선택하거나 지웁니다.
7. **OK**(확인)를 클릭하여 변경한 내용을 적용합니다.

1.1.1.3. 사용자 역할 및 권한 부여 예

다음 예제에서는 이 장에 설명된 다양한 권한 부여 시스템의 다양한 기능을 사용하여 다양한 시나리오에 권한 부여 제어를 적용하는 방법을 보여줍니다.

예 1.1. 클러스터 권한

Sarah는 회사의 회계 부서의 시스템 관리자입니다. 부서의 모든 가상 리소스는 **Accounts** 라는 Red Hat Virtualization 클러스터에서 구성됩니다. 계정에 **ClusterAdmin** 역할이 할당됩니다. 그러면 가상 시스템이 클러스터의 하위 개체이므로 클러스터의 모든 가상 시스템을 관리할 수 있습니다. 가상 시스템 관리에는 디스크 등의 가상 리소스 편집, 추가 또는 제거 및 스냅샷이 포함됩니다. 이 클러스터 외부의 리소스를 관리할 수 없습니다. **ClusterAdmin** 은 관리자 역할이므로 관리 포털 또는 VM 포털을 사용하여 이러한 리소스를 관리할 수 있습니다.

예 1.2. VM PowerUser 권한

John은 계정 부서의 소프트웨어 개발자입니다. 그는 가상 시스템을 사용하여 소프트웨어를 빌드하고 테스트합니다. Sarah는 **johndesktop** 이라는 가상 데스크탑을 만들었습니다. John은 **johndesktop** 가상 시스템에서 **UserVmManager** 역할을 할당받습니다. 이렇게 하면 VM 포털을 사용하여 이 단일 가상

시스템에 액세스할 수 있습니다. **UserVmManager** 권한이 있으므로 가상 시스템을 수정할 수 있습니다. **UserVmManager** 는 사용자 역할이므로 관리 포털을 사용할 수 없습니다.

예 1.3. 데이터 센터 파워 사용자 역할 권한

Penelope는 사무실 관리자입니다. 자신이 맡은 책임 외에도 인터뷰 예약, 참조 점검 등 인사 작업을 수행하는 데 도움을 주기도 합니다. 기업 정책에 따라 Penelope는 특별한 작업에 특정 애플리케이션을 사용해야 합니다.

Penelope는 사무실 관리 작업을 수행할 수 있는 시스템을 보유하고 있지만, 이 시스템을 사용하여 애플리케이션을 실행할 별도의 가상 시스템을 만들려고 합니다. 새 가상 시스템이 상주할 데이터 센터에 대한 **PowerUserRole** 권한이 할당됩니다. 이는 새 가상 시스템을 생성하려면 스토리지 도메인에 가상 디스크 생성을 포함하여 데이터 센터 내의 여러 구성 요소를 변경해야 하기 때문입니다.

이는 Penelope에 **DataCenterAdmin** 권한을 할당하는 것과 같지 않습니다. 데이터 센터의 **PowerUser** 로 Penelope는 VM 포털에 로그인하고 데이터 센터 내의 가상 시스템에서 가상 시스템 관련 작업을 수행할 수 있습니다. 호스트 또는 스토리지를 데이터 센터에 연결하는 등의 데이터 센터 수준 작업을 수행할 수 없습니다.

예 1.4. 네트워크 관리자 권한

Chris는 IT 부서의 네트워크 관리자로 근무하고 있습니다. 담당 부서의 Red Hat Virtualization 환경에서는 일상적인 네트워크 생성, 조작 및 제거가 포함됩니다. 역할을 위해 리소스와 각 리소스의 네트워크에 대한 관리 권한이 필요합니다. 예를 들어 Chris가 IT 부서의 데이터 센터에 대한 **NetworkAdmin** 권한이 있는 경우 데이터 센터에서 네트워크를 추가 및 제거하고 데이터 센터에 속하는 모든 가상 시스템의 네트워크를 연결 및 분리할 수 있습니다.

예 1.5. 사용자 정의 역할 권한

Rachel은 IT 부서에서 일하며 Red Hat Virtualization에서 사용자 계정을 관리합니다. 사용자 계정을 추가하고 적절한 역할 및 권한을 할당할 수 있는 권한이 필요합니다. 가상 시스템을 사용하지 않으며 호스트, 가상 시스템, 클러스터 또는 데이터 센터의 관리에 액세스할 수 없어야 합니다. 이 특정 권한 세트를 제공하는 기본 제공 역할은 없습니다. Rachel의 위치에 적합한 권한 집합을 정의하려면 사용자 지정 역할을 생성해야 합니다.

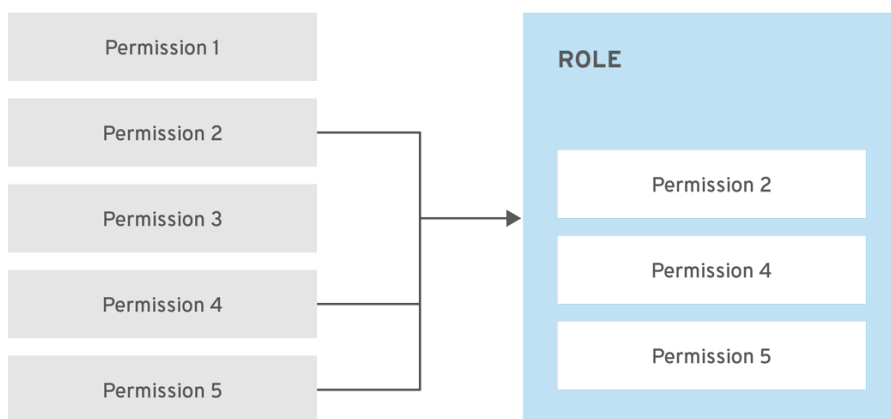
그림 1.1. UserManager 사용자 지정 역할

위에 표시된 **UserManager** 사용자 지정 역할을 사용하면 사용자, 권한 및 역할을 조작할 수 있습니다. 이러한 작업은 **System** (시스템) 아래에 구성됩니다. 오브젝트 계층 구조에 표시된 계층의 최상위 [오브젝트](#)입니다. 즉, 시스템의 다른 모든 개체에 적용됩니다. 역할은 **Account Type(계정 유형)**을 **Admin**으로 설정합니다. 즉, Rachel은 이 역할을 할당하면 관리 포털과 VM 포털을 모두 사용할 수 있습니다.

1.1.2. 시스템 권한

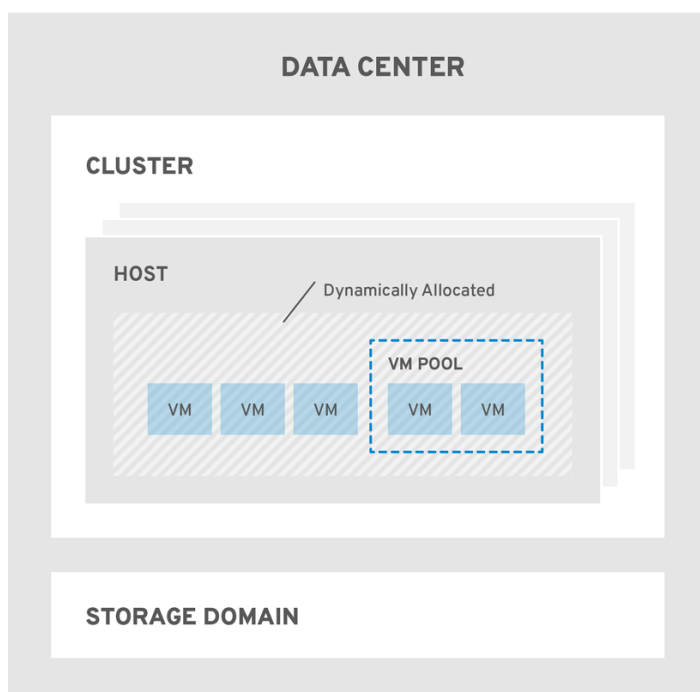
권한을 사용하면 사용자가 오브젝트가 개별 오브젝트 또는 컨테이너 오브젝트인 오브젝트에 대한 작업을 수행할 수 있습니다. 컨테이너 오브젝트에 적용되는 권한은 해당 컨테이너의 모든 멤버에게도 적용됩니다.

그림 1.2. 권한 및 역할



RHV_453537_0219

그림 1.3. Red Hat Virtualization 개체 계층 구조



RHV_453537_0219

1.1.2.1. 사용자 속성

역할 및 권한은 사용자의 속성입니다. 역할은 다양한 수준의 실제 및 가상 리소스에 대한 액세스를 허용하는 사전 정의된 권한 집합입니다. 다단계 관리는 세밀하게 조정된 권한 계층 구조를 제공합니다. 예를 들어 데이터 센터 관리자는 데이터 센터에 있는 모든 오브젝트를 관리할 수 있는 권한이 있는 반면 호스트 관리자에게 단일 물리적 호스트에 대한 시스템 관리자 권한이 있습니다. 사용자는 단일 가상 시스템을 사용할 수 있는 권한을 보유할 수 있지만 가상 시스템 구성을 변경하지 않고 다른 사용자에게 가상 시스템에 시스템 권한을 할당할 수 있습니다.

1.1.2.2. 사용자 및 관리자 역할

Red Hat Virtualization은 시스템 전체 권한이 있는 관리자부터 단일 가상 시스템에 액세스할 수 있는 최종 사용자에게 이르기까지 다양한 사전 구성된 역할을 제공합니다. 기본 역할을 변경하거나 제거할 수는 없지만, 요구 사항에 따라 역할을 복제 및 사용자 지정하거나 새 역할을 생성할 수 있습니다. 역할은 다음 두 가지 유형이 있습니다.

- 관리자 역할: 물리적 및 가상 리소스를 관리하기 위해 관리 포털에 액세스 가능. 관리자 역할은 VM 포털에서 수행할 작업에 대한 권한을 부여하지만 VM 포털에서 볼 수 있는 작업에 대한 권한을 제한하지 않습니다.
- 사용자 역할: VM 포털에 액세스하여 가상 시스템 및 템플릿 관리 및 액세스 가능. 사용자 역할은 VM 포털에서 사용자가 볼 수 있는 사항을 결정합니다. 관리자 역할이 있는 사용자에게 부여된 권한은 VM 포털에서 해당 사용자가 사용할 수 있는 작업에 반영됩니다.

1.1.2.3. 사용자 역할 설명

아래 표에서는 VM 포털에서 가상 시스템에 액세스하고 구성할 권한을 부여하는 기본 사용자 역할을 설명합니다.

표 1.1. Red Hat Virtualization 사용자 역할 - Basic

Role	권한	참고
UserRole	가상 시스템 및 풀에 액세스하고 사용할 수 있음.	VM 포털에 로그인할 수 있음, 할당된 가상 시스템 및 풀을 사용하며, 가상 시스템 상태 및 세부 정보를 확인합니다.
PowerUserRole	가상 시스템과 템플릿을 생성하고 관리할 수 있습니다.	Configure (구성) 창이 있거나 특정 데이터 센터 또는 클러스터에 대해 전체 환경의 사용자에게 이 역할을 적용합니다. 예를 들어 PowerUserRole이 데이터 센터에 적용된 경우 PowerUser는 데이터 센터에서 가상 시스템과 템플릿을 생성할 수 있습니다.
UserVmManager	가상 시스템의 시스템 관리자.	가상 시스템을 관리하고 스냅샷을 만들고 사용할 수 있습니다. VM 포털에서 가상 시스템을 생성하는 사용자에게는 시스템의 UserVmManager 역할이 자동으로 할당됩니다.

아래 표는 VM 포털의 리소스에 대한 권한을 보다 세부적으로 조정할 수 있는 고급 사용자 역할에 대해 설명합니다.

표 1.2. Red Hat Virtualization 사용자 역할 - 고급

Role	권한	참고
UserTemplateBasedVm	템플릿만 사용하는 제한된 권한.	템플릿을 사용하여 가상 시스템을 생성할 수 있음.
DiskOperator	가상 디스크 사용자.	가상 디스크를 사용, 보기 및 편집할 수 있습니다. 가상 디스크가 연결된 가상 시스템을 사용하는 권한을 상속합니다.

Role	권한	참고
VmCreator	VM 포털에서 가상 시스템을 생성할 수 있음.	이 역할은 특정 가상 시스템에 적용되지 않습니다. Configure (구성) 창이 있는 전체 환경의 사용자에게 이 역할을 적용합니다. 또는 특정 데이터 센터 또는 클러스터에 이 역할을 적용합니다. 이 역할을 클러스터에 적용하는 경우 전체 데이터 센터 또는 특정 스토리지 도메인에 DiskCreator 역할을 적용해야 합니다.
TemplateCreator	할당된 리소스 내에서 가상 시스템 템플릿을 생성, 편집, 관리 및 제거할 수 있습니다.	이 역할은 특정 템플릿에 적용되지 않습니다. Configure (구성) 창이 있는 전체 환경의 사용자에게 이 역할을 적용합니다. 또는 특정 데이터 센터, 클러스터 또는 스토리지 도메인에 이 역할을 적용합니다.
DiskCreator	할당된 클러스터 또는 데이터 센터 내에서 가상 디스크를 생성, 편집, 관리 및 제거할 수 있습니다.	이 역할은 특정 가상 디스크에 적용되지 않습니다. Configure (구성) 창이 있는 전체 환경의 사용자에게 이 역할을 적용합니다. 또는 특정 데이터 센터 또는 스토리지 도메인에 이 역할을 적용합니다.
TemplateOwner	템플릿을 편집하고 삭제하고, 템플릿에 대한 사용자 권한을 할당 및 관리할 수 있습니다.	이 역할은 템플릿을 생성하는 사용자에게 자동으로 할당됩니다. 템플릿에 대한 TemplateOwner 권한이 없는 다른 사용자는 템플릿을 보거나 사용할 수 없습니다.
VnicProfileUser	가상 시스템 및 템플릿용 논리적 네트워크 및 네트워크 인터페이스 사용자.	특정 논리적 네트워크에서 네트워크 인터페이스를 연결하거나 연결 해제할 수 있습니다.

1.1.2.4. 설명된 관리자 역할

아래 표는 관리 포털에서 리소스에 액세스하고 구성할 권한을 부여하는 기본 관리자 역할을 설명합니다.

표 1.3. Red Hat Virtualization 시스템 관리자 역할 - Basic

Role	권한	참고
슈퍼유저	Red Hat Virtualization 환경의 시스템 관리자.	에는 모든 오브젝트와 수준에 대한 전체 권한이 있으며, 모든 데이터 센터에서 모든 오브젝트를 관리할 수 있습니다.

Role	권한	참고
ClusterAdmin	클러스터 관리자.	특정 클러스터 아래의 모든 오브젝트에 대한 관리 권한이 있습니다.
DataCenterAdmin	데이터 센터 관리자.	특정 데이터 센터 아래의 모든 오브젝트에 대한 관리 권한을 보유하고 있습니다. 단, 스토리지는 제외됩니다.



중요

디렉터리 서버에 대한 관리자를 Red Hat Virtualization 관리 사용자로 사용하지 마십시오. 특히 Red Hat Virtualization 관리 사용자로 사용하기 위해 디렉터리 서버에서 사용자를 생성합니다.

아래 표는 관리 포털의 리소스에 대한 권한을 보다 세부적으로 조정할 수 있는 고급 관리자 역할을 설명합니다.

표 1.4. Red Hat Virtualization 시스템 관리자 역할 - 고급

Role	권한	참고
TemplateAdmin	가상 머신 템플릿 관리자.	템플릿의 스토리지 도메인과 네트워크 세부 정보를 생성, 삭제 및 구성하고 도메인 간에 템플릿을 이동할 수 있습니다.
StorageAdmin	스토리지 관리자.	할당된 스토리지 도메인을 생성, 삭제, 구성 및 관리할 수 있습니다.
HostAdmin	호스트 관리자.	특정 호스트를 연결, 제거, 구성 및 관리할 수 있습니다.
NetworkAdmin	네트워크 관리자.	특정 데이터 센터 또는 클러스터의 네트워크를 구성하고 관리할 수 있습니다. 데이터 센터 또는 클러스터의 네트워크 관리자는 클러스터 내의 가상 풀에 대한 네트워크 권한을 상속받습니다.
VmPoolAdmin	가상 풀의 시스템 관리자.	가상 풀을 생성, 삭제 및 구성하고, 가상 풀 사용자를 할당 및 제거하고, 풀의 가상 시스템에서 기본 작업을 수행할 수 있습니다.
GlusterAdmin	Gluster 스토리지 관리자.	Gluster 스토리지 볼륨을 생성, 삭제, 구성 및 관리할 수 있습니다.

Role	권한	참고
VmlImporterExporter	가상 시스템의 관리자 가져오기 및 내보내기.	가상 시스템을 가져오고 내보낼 수 있습니다. 다른 사용자가 내보낸 모든 가상 시스템과 템플릿을 볼 수 있습니다.

1.1.2.5. 리소스에 관리자 또는 사용자 역할 할당

사용자가 해당 리소스에 액세스하거나 관리할 수 있도록 관리자 또는 사용자 역할을 리소스에 할당합니다.

절차

1. 리소스 이름을 찾아 클릭합니다. 그러면 세부 정보 보기가 열립니다.
2. **Permissions(권한)** 탭을 클릭하여 할당된 사용자, 각 사용자의 역할 및 선택한 리소스에 대한 상속된 권한을 나열합니다.
3. **추가**를 클릭합니다.
4. 기존 사용자의 이름 또는 사용자 이름을 **Search** (검색) 텍스트 상자에 입력하고 **Go** (이동)를 클릭합니다. 가능한 일치 항목 목록에서 사용자를 선택합니다.
5. **Role to Assign** (할당할 역할) 드롭다운 목록에서 역할을 선택합니다.
6. **OK(확인)**를 클릭합니다.

이제 사용자에게 해당 리소스에 대해 해당 역할의 상속된 권한이 활성화되었습니다.

중요

권한이 시스템 계층 구조에서 낮은 리소스에서 자동으로 상속되므로 클러스터와 같은 리소스에서 일반 사용자에게 글로벌 권한을 할당하지 마십시오. 가상 시스템, 풀 또는 가상 시스템 풀, 특히 후자의 특정 리소스에 대한 **UserRole** 및 기타 모든 사용자 역할 권한을 설정합니다.

글로벌 권한을 할당하면 권한 상속으로 인해 두 가지 문제가 발생할 수 있습니다.

- 일반 사용자는 관리자가 할당 권한을 수행하지 않으려는 경우에도 가상 시스템 풀을 제어하는 권한을 자동으로 부여할 수 있습니다.
- 풀에서 가상 시스템 포털이 예기치 않게 작동할 수 있습니다.

따라서 다른 리소스가 권한을 상속받는 리소스가 아닌 특정 리소스에 대해서만 **UserRole** 및 기타 모든 사용자 역할 권한을 설정하는 것이 좋습니다.

1.1.2.6. 리소스에서 관리자 또는 사용자 역할 제거

리소스에서 관리자 또는 사용자 역할을 제거합니다. 사용자는 해당 리소스의 역할과 연결된 상속된 권한이 손실됩니다.

절차

1. 리소스 이름을 찾아 클릭합니다. 그러면 세부 정보 보기가 열립니다.
2. **Permissions(권한)** 탭을 클릭하여 할당된 사용자, 사용자의 역할 및 선택한 리소스에 대한 상속된 권한을 나열합니다.
3. 리소스에서 제거할 사용자를 선택합니다.
4. **Remove(제거)**를 클릭합니다.
5. **OK(확인)**를 클릭합니다.

1.1.2.7. 데이터 센터의 시스템 권한 관리

SuperUser로서 시스템 관리자는 관리 포털의 모든 측면을 관리합니다. 특정 관리 역할을 다른 사용자에게 할당할 수 있습니다. 이러한 제한된 관리자 역할은 특정 리소스로 제한하는 사용자 관리 권한을 부여하는 데 유용합니다. 예를 들어 **DataCenterAdmin** 역할에는 해당 데이터 센터에 대한 스토리지를 제외하고 할당된 데이터 센터에 대해서만 관리자 권한이 있으며 **ClusterAdmin**에는 할당된 클러스터에 대한 관리자 권한만 있습니다.

데이터 센터 관리자는 특정 데이터 센터에 대해서만 시스템 관리 역할입니다. 이 기능은 각 데이터 센터에 관리자가 필요한 여러 데이터 센터가 있는 가상화 환경에 유용합니다. **DataCenterAdmin** 역할은 계층적 모델입니다. 데이터 센터에 대한 데이터 센터 관리자 역할이 할당된 사용자는 해당 데이터 센터에 대한 스토리지를 제외하고 데이터 센터의 모든 오브젝트를 관리할 수 있습니다. 헤더 표시줄에서 **Configure(구성)** 버튼을 사용하여 환경의 모든 데이터 센터에 대한 데이터 센터 관리자를 할당합니다.

데이터 센터 관리자 역할은 다음 작업을 허용합니다.

- 데이터 센터와 연결된 클러스터 생성 및 제거.
- 데이터 센터와 연결된 호스트, 가상 시스템 및 풀을 추가 및 제거합니다.
- 데이터 센터와 연결된 가상 시스템에 대한 사용자 권한을 편집합니다.



참고

기존 사용자에게만 역할과 권한을 할당할 수 있습니다.

기존 시스템 관리자를 제거하고 새 시스템 관리자를 추가하여 데이터 센터의 시스템 관리자를 변경할 수 있습니다.

1.1.2.8. 설명된 데이터 센터 관리자 역할

데이터 센터 권한 역할

아래 표에서는 데이터 센터 관리에 적용되는 관리자 역할 및 권한을 설명합니다.

표 1.5. Red Hat Virtualization 시스템 관리자 역할

Role	권한	참고

Role	권한	참고
DataCenterAdmin	데이터 센터 관리자	클러스터, 호스트, 템플릿 및 가상 시스템을 포함한 스토리지를 제외하고 특정 데이터 센터 내의 모든 실제 및 가상 리소스를 사용, 생성, 삭제, 관리할 수 있습니다.
NetworkAdmin	네트워크 관리자	특정 데이터 센터의 네트워크를 구성하고 관리할 수 있습니다. 데이터 센터의 네트워크 관리자는 데이터 센터 내의 가상 시스템에 대한 네트워크 권한을 상속받습니다.

1.1.2.9. 클러스터의 시스템 권한 관리

SuperUser로서 시스템 관리자는 관리 포털의 모든 측면을 관리합니다. 특정 관리 역할을 다른 사용자에게 할당할 수 있습니다. 이러한 제한된 관리자 역할은 특정 리소스로 제한하는 사용자 관리 권한을 부여하는 데 유용합니다. 예를 들어 **DataCenterAdmin** 역할에는 해당 데이터 센터에 대한 스토리지를 제외하고 할당된 데이터 센터에 대해서만 관리자 권한이 있으며 **ClusterAdmin**에는 할당된 클러스터에 대한 관리자 권한만 있습니다.

클러스터 관리자는 특정 클러스터에 대해서만 시스템 관리 역할입니다. 이 기능은 각 클러스터에 시스템 관리자가 필요한 여러 클러스터가 있는 데이터 센터에서 유용합니다. **ClusterAdmin** 역할은 계층 구조 모델입니다. 클러스터에 대한 클러스터 관리자 역할이 할당된 사용자가 클러스터의 모든 개체를 관리할 수 있습니다. 헤더 표시줄에서 **Configure(구성)** 버튼을 사용하여 환경에 있는 모든 클러스터에 클러스터 관리자를 할당합니다.

클러스터 관리자 역할은 다음 작업을 허용합니다.

- 연결된 클러스터 생성 및 제거.
- 클러스터와 관련된 호스트, 가상 시스템 및 풀을 추가 및 제거합니다.
- 클러스터와 연결된 가상 시스템에 대한 사용자 권한을 편집합니다.



참고

기존 사용자에게만 역할과 권한을 할당할 수 있습니다.

기존 시스템 관리자를 제거하고 새 시스템 관리자를 추가하여 클러스터의 시스템 관리자를 변경할 수도 있습니다.

1.1.2.10. 설명된 클러스터 관리자 역할

클러스터 권한 역할

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

표 1.6. Red Hat Virtualization 시스템 관리자 역할

Role	권한	참고
ClusterAdmin	클러스터 관리자	호스트, 템플릿 및 가상 시스템을 포함하여 특정 클러스터의 모든 실제 및 가상 리소스를 사용, 생성, 삭제, 관리할 수 있습니다. 는 표시 네트워크 지정과 같은 클러스터 내에서 네트워크 속성을 구성하거나 네트워크를 필수 또는 필요하지 않은 것으로 표시할 수 있습니다. 그러나 ClusterAdmin 에는 클러스터에서 네트워크를 연결하거나 분리할 권한이 없으므로 NetworkAdmin 권한이 필요합니다.
NetworkAdmin	네트워크 관리자	특정 클러스터의 네트워크를 구성하고 관리할 수 있습니다. 클러스터의 네트워크 관리자는 클러스터 내의 가상 시스템에 대한 네트워크 권한을 상속받습니다.

1.1.2.11. 네트워크의 시스템 권한 관리

SuperUser로서 시스템 관리자는 관리 포털의 모든 측면을 관리합니다. 특정 관리 역할을 다른 사용자에게 할당할 수 있습니다. 이러한 제한된 관리자 역할은 특정 리소스로 제한하는 사용자 관리 권한을 부여하는 데 유용합니다. 예를 들어 **DataCenterAdmin** 역할에는 해당 데이터 센터에 대한 스토리지를 제외하고 할당된 데이터 센터에 대해서만 관리자 권한이 있으며 **ClusterAdmin**에는 할당된 클러스터에 대한 관리자 권한만 있습니다.

네트워크 관리자는 특정 네트워크 또는 데이터 센터, 클러스터, 호스트, 가상 시스템 또는 템플릿의 모든 네트워크에 적용할 수 있는 시스템 관리 역할입니다. 네트워크 사용자는 특정 가상 시스템 또는 템플릿에서 네트워크 보기 및 연결과 같은 제한된 관리 역할을 수행할 수 있습니다. 헤더 표시줄에서 **Configure(구성)** 버튼을 사용하여 환경의 모든 네트워크에 대한 네트워크 관리자를 할당할 수 있습니다.

네트워크 관리자 역할은 다음 작업을 허용합니다.

- 네트워크 만들기, 편집 및 제거.
- 포트 미러링 구성을 포함하여 네트워크 설정을 편집합니다.
- 클러스터 및 가상 시스템을 포함한 리소스에서 네트워크를 연결 및 분리합니다.

네트워크를 생성하는 사용자에게는 생성된 네트워크에 대한 **NetworkAdmin** 권한이 자동으로 할당됩니다. 기존 관리자를 제거하고 새 관리자를 추가하여 네트워크 관리자를 변경할 수도 있습니다.

1.1.2.12. 설명된 네트워크 관리자 및 사용자 역할

네트워크 권한 역할

아래 표는 네트워크 관리에 적용할 수 있는 관리자 및 사용자 역할 및 권한을 설명합니다.

표 1.7. Red Hat Virtualization Network 관리자 및 사용자 역할

Role	권한	참고
NetworkAdmin	데이터 센터, 클러스터, 호스트, 가상 시스템 또는 템플릿의 네트워크 관리자. 네트워크를 생성하는 사용자에게는 생성된 네트워크에 대한 NetworkAdmin 권한이 자동으로 할당됩니다.	특정 데이터 센터, 클러스터, 호스트, 가상 시스템 또는 템플릿의 네트워크를 구성하고 관리할 수 있습니다. 데이터 센터 또는 클러스터의 네트워크 관리자는 클러스터 내의 가상 풀에 대한 네트워크 권한을 상속받습니다. 가상 시스템 네트워크에서 포트 미러링을 구성하려면 네트워크에 NetworkAdmin 역할을 적용하고 가상 머신에서 UserVmManager 역할을 적용합니다.
VnicProfileUser	가상 시스템 및 템플릿용 논리적 네트워크 및 네트워크 인터페이스 사용자.	특정 논리적 네트워크에서 네트워크 인터페이스를 연결하거나 연결 해제할 수 있습니다.

1.1.2.13. 호스트의 시스템 권한 관리

SuperUser로서 시스템 관리자는 관리 포털의 모든 측면을 관리합니다. 특정 관리 역할을 다른 사용자에게 할당할 수 있습니다. 이러한 제한된 관리자 역할은 특정 리소스로 제한하는 사용자 관리 권한을 부여하는 데 유용합니다. 예를 들어 **DataCenterAdmin** 역할에는 해당 데이터 센터에 대한 스토리지를 제외하고 할당된 데이터 센터에 대해서만 관리자 권한이 있으며 **ClusterAdmin**에는 할당된 클러스터에 대한 관리자 권한만 있습니다.

호스트 관리자는 특정 호스트에 대해서만 시스템 관리 역할입니다. 이 기능은 각 호스트에 시스템 관리자가 필요한 여러 호스트가 있는 클러스터에서 유용합니다. 헤더 표시줄에서 **Configure(구성)** 버튼을 사용하여 환경의 모든 호스트에 대한 호스트 관리자를 할당할 수 있습니다.

호스트 관리자 역할은 다음 작업을 허용합니다.

- 호스트의 구성을 편집합니다.
- 논리적 네트워크를 설정합니다.
- 호스트를 제거합니다.

기존 시스템 관리자를 제거하고 새 시스템 관리자를 추가하여 호스트의 시스템 관리자를 변경할 수도 있습니다.

1.1.2.14. 설명된 호스트 관리자 역할

호스트 권한 역할

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

표 1.8. Red Hat Virtualization 시스템 관리자 역할

Role	권한	참고

Role	권한	참고
HostAdmin	호스트 관리자	특정 호스트를 구성, 관리 및 제거할 수 있습니다. 또한 네트워크 관련 작업을 특정 호스트에서 수행할 수 있습니다.

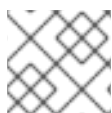
1.1.2.15. 스토리지 도메인의 시스템 권한 관리

SuperUser로서 시스템 관리자는 관리 포털의 모든 측면을 관리합니다. 특정 관리 역할을 다른 사용자에게 할당할 수 있습니다. 이러한 제한된 관리자 역할은 특정 리소스로 제한하는 사용자 관리 권한을 부여하는 데 유용합니다. 예를 들어 **DataCenterAdmin** 역할에는 해당 데이터 센터에 대한 스토리지를 제외하고 할당된 데이터 센터에 대해서만 관리자 권한이 있으며 **ClusterAdmin**에는 할당된 클러스터에 대한 관리자 권한만 있습니다.

스토리지 관리자는 특정 스토리지 도메인에 대해서만 시스템 관리 역할입니다. 이 기능은 스토리지 도메인마다 시스템 관리자가 필요한 여러 스토리지 도메인이 있는 데이터 센터에서 유용합니다. 헤더 표시줄에서 **Configure(구성)** 버튼을 사용하여 환경의 모든 스토리지 도메인에 대한 스토리지 관리자를 할당합니다.

스토리지 도메인 관리자 역할은 다음 작업을 허용합니다.

- 스토리지 도메인의 구성을 편집합니다.
- 스토리지 도메인을 유지 관리 모드로 이동합니다.
- 스토리지 도메인을 제거합니다.



참고

기존 사용자에게만 역할과 권한을 할당할 수 있습니다.

기존 시스템 관리자를 제거하고 새 시스템 관리자를 추가하여 스토리지 도메인의 시스템 관리자를 변경할 수도 있습니다.

1.1.2.16. 설명된 스토리지 관리자 역할

스토리지 도메인 권한 역할

아래 표에서는 스토리지 도메인 관리에 적용할 수 있는 관리자 역할 및 권한을 설명합니다.

표 1.9. Red Hat Virtualization 시스템 관리자 역할

Role	권한	참고
StorageAdmin	스토리지 관리자	특정 스토리지 도메인을 생성, 삭제, 구성 및 관리할 수 있습니다.
GlusterAdmin	Gluster Storage 관리자	Gluster 스토리지 볼륨을 생성, 삭제, 구성 및 관리할 수 있습니다.

Role	권한	참고

1.1.2.17. 가상 머신 풀의 시스템 권한 관리

SuperUser로서 시스템 관리자는 관리 포털의 모든 측면을 관리합니다. 특정 관리 역할을 다른 사용자에게 할당할 수 있습니다. 이러한 제한된 관리자 역할은 특정 리소스로 제한하는 사용자 관리 권한을 부여하는 데 유용합니다. 예를 들어 **DataCenterAdmin** 역할에는 해당 데이터 센터에 대한 스토리지를 제외하고 할당된 데이터 센터에 대해서만 관리자 권한이 있으며 **ClusterAdmin**에는 할당된 클러스터에 대한 관리자 권한만 있습니다.

가상 시스템 풀 관리자는 데이터 센터의 가상 시스템 풀에 대한 시스템 관리 역할입니다. 이 역할은 특정 가상 시스템 풀, 데이터 센터 또는 전체 가상화 환경에 적용할 수 있습니다. 이 역할은 다른 사용자가 특정 가상 시스템 풀 리소스를 관리할 수 있도록 하는 데 유용합니다.

가상 머신 풀 관리자 역할은 다음 작업을 허용합니다.

- 풀 생성, 편집 및 제거.
- 풀에서 가상 머신 추가 및 분리.



참고

기존 사용자에게만 역할과 권한을 할당할 수 있습니다.

1.1.2.18. 가상 머신 풀 관리자 역할 설명

풀 권한 역할

아래 표는 풀 관리에 적용할 수 있는 관리자 역할 및 권한을 설명합니다.

표 1.10. Red Hat Virtualization 시스템 관리자 역할

Role	권한	참고
VmPoolAdmin	가상 풀의 시스템 관리자 역할.	가상 풀을 생성, 삭제 및 구성하고, 가상 풀 사용자를 할당 및 제거하고, 가상 시스템에서 기본 작업을 수행할 수 있습니다.
ClusterAdmin	클러스터 관리자	특정 클러스터의 모든 가상 시스템 풀을 사용, 생성, 삭제, 관리할 수 있습니다.

1.1.2.19. 가상 디스크의 시스템 권한 관리

SuperUser로서 시스템 관리자는 관리 포털의 모든 측면을 관리합니다. 특정 관리 역할을 다른 사용자에게 할당할 수 있습니다. 이러한 제한된 관리자 역할은 특정 리소스로 제한하는 사용자 관리 권한을 부여하는 데 유용합니다. 예를 들어 **DataCenterAdmin** 역할에는 해당 데이터 센터에 대한 스토리지를 제외하고

할당된 데이터 센터에 대해서만 관리자 권한이 있으며 **ClusterAdmin**에는 할당된 클러스터에 대한 관리자 권한만 있습니다.

Red Hat Virtualization Manager는 두 개의 기본 가상 디스크 사용자 역할을 제공하지만 기본 가상 디스크 관리자 역할은 없습니다. 이러한 사용자 역할 중 하나인 **DiskCreator** 역할을 사용하면 VM 포털에서 가상 디스크를 관리할 수 있습니다. 이 역할은 특정 가상 시스템, 데이터 센터, 특정 스토리지 도메인 또는 전체 가상화 환경에 적용할 수 있습니다. 이 역할은 다른 사용자가 다른 가상 리소스를 관리할 수 있도록 하는데 유용합니다.

가상 디스크 생성자 역할은 다음 작업을 허용합니다.

- 가상 시스템 또는 기타 리소스와 연결된 가상 디스크를 생성, 편집 및 제거합니다.
- 가상 디스크에 대한 사용자 권한을 편집합니다.



참고

기존 사용자에게만 역할과 권한을 할당할 수 있습니다.

1.1.2.20. 가상 디스크 사용자 역할 설명

가상 디스크 사용자 권한 역할

아래 표는 VM 포털에서 가상 디스크를 사용하고 관리하는 데 적용할 수 있는 사용자 역할 및 권한을 설명합니다.

표 1.11. Red Hat Virtualization 시스템 관리자 역할

Role	권한	참고
DiskOperator	가상 디스크 사용자.	가상 디스크를 사용, 보기 및 편집할 수 있습니다. 가상 디스크가 연결된 가상 시스템을 사용하는 권한을 상속합니다.
DiskCreator	할당된 클러스터 또는 데이터 센터 내에서 가상 디스크를 생성, 편집, 관리 및 제거할 수 있습니다.	이 역할은 특정 가상 디스크에 적용되지 않습니다. Configure (구성) 창이 있는 전체 환경의 사용자에게 이 역할을 적용합니다. 또는 특정 데이터 센터, 클러스터 또는 스토리지 도메인에 이 역할을 적용합니다.

1.1.2.20.1. 레거시 SPICE 암호 설정

SPICE 콘솔은 기본적으로 암호화 문자열과 함께 FIPS 호환 암호화를 사용합니다. 기본 SPICE 암호화 문자열은 **kECDHE+FIPS:kDHE+FIPS:kRSA+FIPS:!eNULL:!aNULL**입니다.

일반적으로 이 문자열은 충분합니다. 그러나 이전 운영 체제 또는 SPICE 클라이언트가 있는 가상 머신이 하나나 하나라도 FIPS 호환 암호화를 지원하지 않는 경우 더 약한 암호 문자열을 사용해야 합니다. 그렇지 않으면 기존 클러스터에 새 클러스터 또는 새 호스트를 설치하고 해당 가상 시스템에 연결을 시도하면 연결 보안 오류가 발생할 수 있습니다.

Ansible 플레이북을 사용하여 암호 문자열을 변경할 수 있습니다.

암호화 문자열 변경

1. Manager 시스템의 디렉토리 **/usr/share/ovirt-engine/playbooks** 에 파일을 만듭니다. 예를 들면 다음과 같습니다.

```
# vim /usr/share/ovirt-engine/playbooks/change-spice-cipher.yml
```

2. 파일에 다음을 입력하여 저장합니다.

```
name: oVirt - setup weaker SPICE encryption for old clients
hosts: hostname
vars:
  host_deploy_spice_cipher_string: 'DEFAULT:-RC4:-3DES:-DES'
roles:
  - ovirt-host-deploy-spice-encryption
```

3. 방금 만든 파일을 실행합니다.

```
# ansible-playbook -i hostname /usr/share/ovirt-engine/playbooks/change-spice-cipher.yml
```

또는 `host_deploy_spice_cipher_string` 변수와 함께 `--extra-vars` 옵션을 사용하여 **Ansible** 플레이북 **ovirt-host-deploy**로 호스트를 재구성할 수 있습니다.

```
# ansible-playbook -i hostname \
--extra-vars host_deploy_spice_cipher_string="DEFAULT:-RC4:-3DES:-DES" \
/usr/share/ovirt-engine/playbooks/ovirt-host-deploy.yml
```

1.1.3. 예약 정책

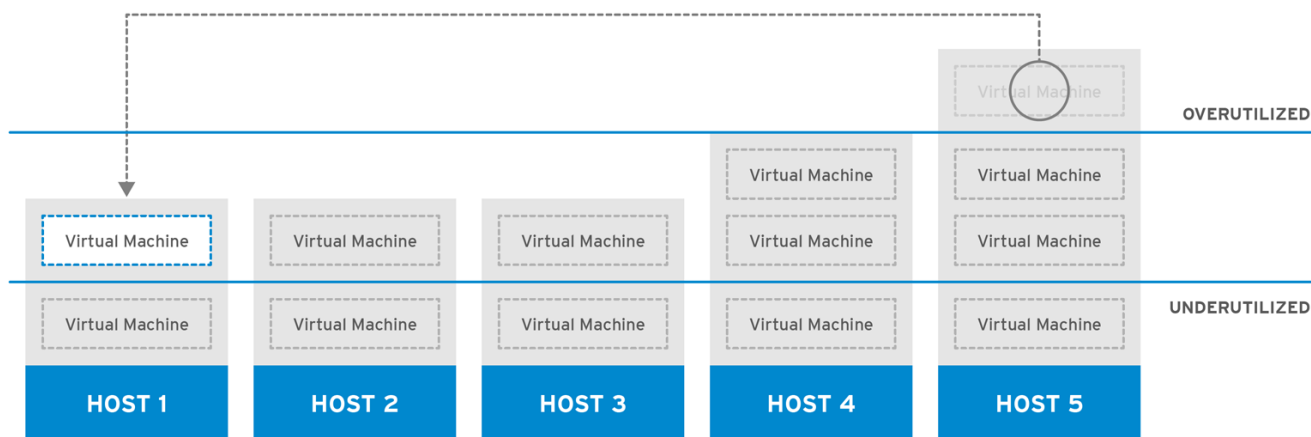
스케줄링 정책은 스케줄링 정책이 적용되는 클러스터의 호스트 간에 가상 시스템이 배포되는 논리를 정의하는 규칙 집합입니다. 스케줄링 정책은 필터, 가중치 및 부하 분산 정책의 조합을 통해 이 논리를 결정합니다. `filter` 모듈은 하드 적용을 적용하고 해당 필터에서 지정한 조건을 충족하지 않는 호스트를 필터링합니다. `weights` 모듈은 소프트 적용을 적용하며, 가상 시스템을 실행할 수 있는 클러스터의 호스트를 결정할 때 고려하는 요인의 상대적 우선 순위를 제어하는 데 사용됩니다.

Red Hat Virtualization Manager는 5가지 기본 스케줄링 정책을 제공합니다.

evenly_Distributed, Cluster_Maintenance, None, Power_Saving 및 **VM_Evenly_Distributed**. 가상 시스템 배포에 대한 세부적인 제어를 제공하는 새로운 스케줄링 정책을 정의할 수도 있습니다. 스케줄링 정책에 관계없이 과부하된 CPU가 있는 호스트에서 가상 시스템이 시작되지 않습니다. 기본적으로 5분 동안 80% 이상의 부하가 있는 경우 호스트의 CPU가 과부하로 간주되지만 스케줄링 정책을 사용하여 이러한 값을 변경할 수 있습니다. 각 [스케줄링 정책](#)의 속성에 대한 자세한 내용은 [관리 가이드](#)의 스케줄링 정책을 참조하십시오.

스케줄링 정책이 작동하는 방법에 대한 자세한 내용은 [클러스터 스케줄링 정책의 작동 방식을 참조하십시오](#).

그림 1.4. 균일하게 분산 스케줄링 정책

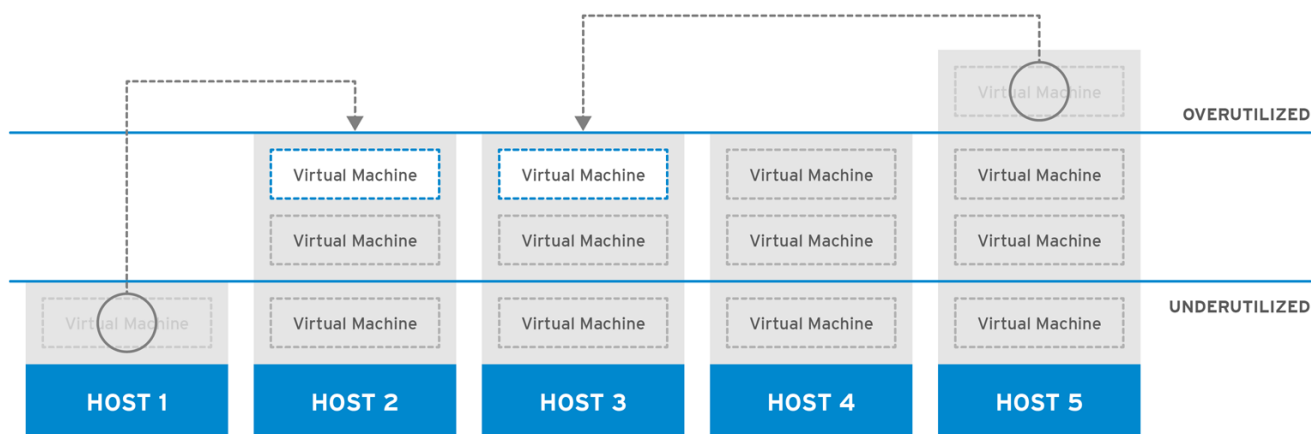


RHV_444396_0417

evenly_Distributed 스케줄링 정책에서는 클러스터의 모든 호스트에서 메모리와 CPU 처리 부하를 균등하게 배포합니다. 해당 호스트가 정의된 **CpuOverCommitDurationMinutes,HighUtilization** 또는 **MaxFreeMemoryForOver Utilized**에 도달하면 호스트에 연결된 추가 가상 시스템이 시작되지 않습니다.

VM_Evenly_Distributed 스케줄링 정책은 가상 시스템 수에 따라 호스트 간에 가상 시스템을 균등하게 배포합니다. 호스트가 **HighVmCount** 보다 더 많은 가상 시스템을 실행 중이고 **MigrationThreshold** 외부에 있는 가상 머신 수가 하나 이상 있는 경우 클러스터가 균형이 맞지 않는 것으로 간주됩니다.

그림 1.5. 절전 예약 정책



RHV_444396_0417

Power_Saving 스케줄링 정책은 활용도가 낮은 호스트의 전력 소비를 줄이기 위해 사용 가능한 호스트의 하위 집합에 메모리 및 CPU 처리 부하를 분산합니다. CPU 부하가 정의된 시간 간격보다 긴 사용률 값이 낮은 호스트는 모든 가상 시스템을 다른 호스트로 마이그레이션하여 전원을 끌 수 있습니다. 호스트가 정의된 높은 사용률 값에 도달한 경우 호스트에 연결된 추가 가상 시스템이 시작되지 않습니다.

가상 시스템을 실행하기 위해 호스트 간에 부하 또는 전원 공유가 없도록 **None** 정책을 설정합니다. 이는 기본값 모드입니다. 가상 시스템이 시작되면 클러스터의 모든 호스트에 메모리 및 CPU 처리 부하가 균등하게 분산됩니다. 해당 호스트가 정의된 **CpuOverCommitDurationMinutes,HighUtilization** 또는 **MaxFreeMemoryForOver Utilized**에 도달하면 호스트에 연결된 추가 가상 시스템이 시작되지 않습니다.

Cluster_Maintenance 스케줄링 정책은 유지 관리 작업 중에 클러스터의 활동을 제한합니다.

Cluster_Maintenance 정책이 설정되면 고가용성 가상 시스템을 제외하고 새 가상 시스템을 시작할 수 없습니다. 호스트 오류가 발생하면 고가용성 가상 시스템이 제대로 다시 시작되고 모든 가상 시스템이 마이그레이션될 수 있습니다.

1.1.3.1. 스케줄링 정책 생성

새 스케줄링 정책을 생성하여 Red Hat Virtualization 환경에서 지정된 클러스터 간에 가상 머신이 배포되는 논리를 제어할 수 있습니다.

절차

1. **Administration(관리) Configure(구성)** 를 클릭합니다.
2. **Scheduling Policies(스케줄링 정책)** 탭을 클릭합니다.
3. **New (새로 만들기)**를 클릭합니다.
4. 스케줄링 정책에 **Name (이름)** 및 **Description (설명)**을 입력합니다.
5. 필터 모듈을 구성합니다.
 - a. **Filter Modules (모듈 필터)** 섹션에서 선호하는 필터 모듈을 드래그 앤 드롭하여 **Disabled Filters (비활성화된 필터)** 섹션에서 스케줄링 정책에 적용합니다.
 - b. 특정 필터 모듈도 기본 최적화를 위해 우선 순위가 가장 높은 첫 번째 또는 가장 낮은 우선 순위를 부여할 수 있습니다. 우선 순위를 설정하려면 필터 모듈을 마우스 오른쪽 단추로 클릭하고 위치 위에 커서를 두고 **First** 또는 **Last** 를 선택합니다.
6. 가중치 모듈을 구성합니다.
 - a. **Weights** 모듈 섹션에서 선호하는 weight 모듈을 드래그 앤 드롭하여 **Disabled Weights (비활성화된 가중치)** 섹션에서 스케줄링 정책에 적용할 수 있습니다.
 - b. 활성화된 weight 모듈의 왼쪽에 + 및 - 버튼을 사용하여 해당 모듈의 가중치를 늘리거나 줄입니다.
7. 로드 밸런싱 정책을 지정합니다.
 - a. **Load Balancer (로드 밸런서 로드)** 섹션의 드롭다운 메뉴에서 스케줄링 정책에 적용할 로드 밸런싱 정책을 선택합니다.
 - b. **Properties (속성)** 섹션의 드롭다운 메뉴에서 스케줄링 정책에 적용할 로드 밸런싱 속성을 선택하고 해당 속성의 오른쪽에 텍스트 필드를 사용하여 값을 지정합니다.
 - c. + 및 - 버튼을 사용하여 추가 속성을 추가하거나 제거합니다.
8. **OK(확인)**를 클릭합니다.

1.1.3.2. 새 스케줄링 정책의 설정 설명 및 스케줄링 정책 편집 창

다음 표에는 **New Scheduling Policy(새 스케줄링 정책)** 및 **Edit Scheduling Policy(스케줄링 정책 편집)** 창에서 사용할 수 있는 옵션이 자세히 나와 있습니다.

표 1.12. 새 스케줄링 정책 및 스케줄링 정책 편집

필드 이름	설명
이름	스케줄링 정책의 이름입니다. Red Hat Virtualization Manager의 스케줄링 정책을 참조하는 데 사용되는 이름입니다.

필드 이름	설명
설명	스케줄링 정책에 대한 설명입니다. 이 필드는 권장되지만 필수는 아닙니다.
필터 모듈	클러스터의 가상 시스템을 실행할 수 있는 호스트를 제어하는 필터 집합입니다. 필터를 활성화하면 아래에 설명된 대로 해당 필터에서 지정한 조건을 충족하지 않는 호스트를 필터링합니다. ● ClusterInMaintenance: 고가용성에 대해 구성되지 않은 호스트에서 시작하는 가상 시스템은 호스트를 필터링합니다. ● CpuPinning: CPU 고정 정의를 충족하지 않는 호스트입니다. ● 마이그레이션: 동일한 호스트로 마이그레이션하는 것을 방지합니다. ● CPUOverloaded: CpuOverCommitDurationMinutes에서 정의한 간격에 대해 정의된 HighUtilization 임계값을 초과하는 CPU 사용량이 있는 호스트입니다. ● PinToHost: 가상 시스템이 고정된 호스트 이외의 호스트입니다. ● CPU 레벨: 가상 시스템의 CPU 토폴로지를 충족하지 않는 호스트입니다. ● VmAffinityGroups: 가상 시스템에 대해 정의된 선호도 규칙을 충족하지 않는 호스트입니다. ● NUMA: 리소스 측면에서 가상 머신 vNUMA 노드를 수용할 수 있는 NUMA 노드가 없는 호스트입니다. ● InClusterUpgrade: 가상 시스템이 현재 실행되는 호스트보다 이전 버전의 운영 체제를 실행 중인 호스트입니다. ● MDevice: 필수 중재 장치를 제공하지 않는 호스트(mDev). ● 메모리: 가상 시스템을 실행하는 데 메모리가 충분하지 않은 호스트입니다. ● CPU: 가상 시스템에 할당된 수보다 CPU 수가 적은 호스트입니다. ● HostedEnginesSpares: 지정된 수의 자체 호스팅 엔진 노드에 있는 Manager 가상 시스템의 공간을 예약합니다. ● 스왑: 임계값 내에서 스왑하지 않는 호스트입니다.

필드 이름	설명
	● VM 리스를 준비합니다: 스토리지 리스를 사용하여 구성된 가상 시스템을 지원하지 않는 호스트. ● VmToHostsAffinityGroups: 선호도 그룹의 멤버인 가상 시스템에 지정된 조건을 충족하지 않는 호스트 그룹입니다. 예를 들어 선호도 그룹의 해당 가상 시스템은 그룹의 호스트 중 하나 또는 그룹에서 제외된 별도의 호스트에서 실행해야 합니다. ● HostDevice: 가상 시스템에 필요한 호스트 장치를 지원하지 않는 호스트입니다. ● HA: 셀프 호스트 엔진 환경에서 Manager 가상 시스템이 양의 고가용성 점수가 있는 호스트에서만 실행되도록 강제 적용합니다. ● 에플레이트된 머신: 에플레이트된 시스템 지원이 없는 호스트. ● HugePages: 가상 시스템의 메모리에 필요한 Huge Pages 수를 충족하지 않는 호스트입니다. ● Migration-Tsc-Frequency: 현재 가상 시스템을 실행 중인 호스트와 TSC 빈도가 동일한 가상 시스템이 없는 호스트입니다. ● 네트워크: 가상 시스템의 네트워크 인터페이스스 컨트롤러에 필요한 네트워크가 설치되어 있지 않거나 클러스터의 디스플레이 네트워크가 설치되지 않은 호스트입니다. ● 레이블: 필수 선호도 레이블이 없는 호스트입니다. ● compatibility-Version: 올바른 클러스터 호환성 버전 지원이 없는 호스트.
weights 모듈	가상 시스템이 실행할 수 있는 클러스터의 호스트를 결정할 때 고려하는 요인의 상대 우선 순위를 제어하는 가중치 집합입니다. ● VmAffinityGroups: 가상 시스템에 정의된 선호도 그룹에 따라 호스트를 가중치화합니다. 이 weight 모듈은 해당 선호도 그룹의 매개변수에 따라 선호도 그룹의 가상 시스템을 동일한 호스트 또는 별도의 호스트에서 실행할 가능성을 결정합니다. ● InClusterUpgrade: 운영 체제 버전에 따라 호스트 가중치. 가중치는 가상 시스템이 현재 실행 중인 호스트와 동일한 운영 체제가 있는 호스트보다 이전 운영 체제가 있는 호스트보다 더 많은 호스트를 사용할 수 있습니다. 이렇게 하면 이후 운영 체제가 있는 호스트에 우선 순위가 항상 부여됩니다. ● OptimalForCpuEvenDistribution: CPU 사용량에 따라 호스트를 가중치로 사용하여 CPU 사용량이 낮은 호스트에 우선 순위를 부여합니다.

필드 이름	설명
	● 고성능 VM의 CPU: VM과 동일한 수의 소켓, 코어 및 스레드가 있는 호스트를 선호합니다. ● HA: 고가용성 점수에 따라 호스트의 가중치를 지정합니다. ● OptimalForCpuPowerSaving: CPU 사용량에 따라 호스트를 가중치로 사용하여 CPU 사용량이 높은 호스트에 우선 순위를 제공합니다. ● OptimalForMemoryPowerSaving: 메모리 사용량에 따라 호스트를 가중치로 사용하여 사용 가능한 메모리가 낮은 호스트에 우선 순위를 제공합니다. ● CPU 및 NUMA 고정 호환성: 호환성 고정에 따른 가중치 호스트. 가상 시스템에 vNUMA와 고정이 정의되어 있는 경우 이 weight 모듈은 CPU 고정이 vNUMA 고정과 충돌하지 않는 호스트를 선호합니다. ● VmToHostsAffinityGroups: 가상 시스템에 정의된 선호도 그룹에 따라 호스트를 가중치화합니다. 이 weight 모듈은 선호도 그룹의 가상 시스템을 그룹의 호스트 중 하나 또는 그룹에서 제외된 별도의 호스트에서 실행할 가능성을 결정합니다. ● OptimalForEvenGuestDistribution: 해당 호스트에서 실행되는 가상 시스템의 수에 따라 호스트를 가중치화합니다. ● OptimalForHaReservation: 고가용성 점수에 따라 호스트의 가중치를 지정합니다. ● OptimalForMemoryEvenDistribution: 메모리 사용량에 따라 호스트를 가중치로 사용하여 사용 가능한 메모리가 높은 호스트에 우선 순위를 제공합니다. ● 단일 호스트 NUMA 노드에 VM 적합: 가상 머신이 단일 NUMA 노드에 적합한지 여부에 따라 호스트를 가중칩니다. 가상 시스템에 vNUMA가 정의되지 않은 경우 이 weight 모듈은 가상 시스템을 하나의 물리적 NUMA에 적합할 수 있는 호스트를 선호합니다. ● PreferredHosts: 가상 시스템을 설정하는 동안 선호되는 호스트에는 우선 순위가 있습니다.
로드 밸런서	이 드롭다운 메뉴에서 적용할 부하 분산 모듈을 선택할 수 있습니다. 부하 분산 모듈은 사용량이 낮은 호스트에서 가상 시스템을 마이그레이션하는 데 사용되는 논리를 판별합니다.

필드 이름	설명
속성	이 드롭다운 메뉴를 사용하면 부하 분산 모듈의 속성을 추가하거나 제거할 수 있으며 스케줄링 정책에 대한 부하 분산 모듈을 선택한 경우에만 사용할 수 있습니다. 속성은 기본적으로 정의되지 않으며 사용 가능한 속성은 선택한 부하 분산 모듈에 따라 다릅니다. + 및 - 버튼을 사용하여 부하 분산 모듈에 추가 속성을 추가하거나 제거합니다.

1.1.4. 인스턴스 유형

인스턴스 유형을 사용하여 가상 시스템의 하드웨어 구성을 정의할 수 있습니다. 가상 시스템을 만들거나 편집할 때 인스턴스 유형을 선택하면 하드웨어 구성 필드가 자동으로 채워집니다. 이를 통해 사용자는 모든 필드를 수동으로 입력하지 않고도 동일한 하드웨어 구성을 사용하여 여러 가상 시스템을 만들 수 있습니다.



참고

인스턴스 유형에 대한 지원은 더 이상 사용되지 않으며 향후 릴리스에서 제거됩니다.

다음 표에 설명된 대로 사전 정의된 인스턴스 유형 집합은 기본적으로 사용할 수 있습니다.

표 1.13. 사전 정의된 인스턴스 유형

이름	메모리	vCPU
작음	512MB	1
소	2GB	1
중간	4GB	2
대	8GB	2
XLarge	16GB	4

관리자는 **Configure** (구성) 창의 **Instance Types**(인스턴스 유형) 탭에서 인스턴스 유형을 생성, 편집 및 제거할 수도 있습니다.

인스턴스 유형에 바인딩된 **New Virtual Machine**(새 가상 머신) 및 **Edit Virtual Machine**(가상 머신 편집) 창의 필드에는 체인 링크 이미지가 있습니다(). 이러한 필드 중 하나의 값이 변경되면 가상 머신이 인스턴스 유형에서 분리되어 **Custom**(사용자 지정)으로 변경되고 체인이 손상됩니다(). 그러나 값이 다시 변경되면 체인이 다시 연결되고 인스턴스 유형이 선택한 항목으로 다시 이동합니다.

1.1.4.1. 인스턴스 유형 생성

관리자는 가상 시스템을 만들거나 편집할 때 사용자가 선택할 수 있는 새 인스턴스 유형을 만들 수 있습니다.

절차

1. **Administration(관리) Configure(구성)** 를 클릭합니다.
2. **Instance Types(인스턴스 유형)** 탭을 클릭합니다.
3. **New** (새로 만들기)를 클릭합니다.
4. 인스턴스 유형에 **Name** (이름) 및 **Description** (설명)을 입력합니다.
5. **Show Advanced Options** (고급 옵션 표시)를 클릭하고 필요에 따라 인스턴스 유형 설정을 구성합니다. **New Instance Type(새 인스턴스 유형)** 창에 표시되는 설정은 **NewVirtual Machine(새 가상 시스템)** 창에 있는 설정과 동일하지만 관련 필드만 사용됩니다. 가상 [머신 관리 가이드에서 새 가상 머신 및 가상 머신 편집의 설정 설명](#)을 참조하십시오.
6. **OK(확인)**를 클릭합니다.

새 인스턴스 유형은 **Configure** (구성) 창의 **Instance Types(인스턴스 유형)** 탭에 표시되며, 가상 시스템을 만들거나 편집할 때 **Instance Type(인스턴스 유형)** 드롭다운 목록에서 선택할 수 있습니다.

1.1.4.2. 인스턴스 유형 편집

관리자는 **Configure** (구성) 창에서 기존 인스턴스 유형을 편집할 수 있습니다.

절차

1. **Administration(관리) Configure(구성)** 를 클릭합니다.
2. **Instance Types(인스턴스 유형)** 탭을 클릭합니다.
3. 편집할 인스턴스 유형을 선택합니다.
4. **Edit(편집)**를 클릭합니다.
5. 필요에 따라 설정을 변경합니다.
6. **OK(확인)**를 클릭합니다.

인스턴스 유형의 구성이 업데이트됩니다. 이 인스턴스 유형을 기반으로 하는 새 가상 시스템이 생성되거나 이 인스턴스 유형에 따라 기존 가상 시스템이 업데이트되면 새 구성이 적용됩니다.

이 인스턴스 유형을 기반으로 하는 기존 가상 시스템은 업데이트될 체인 아이콘으로 표시된 필드가 표시됩니다. 인스턴스 유형이 변경될 때 기존 가상 시스템이 실행 중인 경우, 인스턴스 유형에 따라 **Pending Changes**(보류 중인 변경 사항) 아이콘이 표시되고 체인 아이콘이 있는 필드가 다음 다시 시작할 때 업데이트됩니다.

1.1.4.3. 인스턴스 유형 제거

절차

1. **Administration(관리) Configure(구성)** 를 클릭합니다.
2. **Instance Types(인스턴스 유형)** 탭을 클릭합니다.
3. 제거할 인스턴스 유형을 선택합니다.

4. **Remove(제거)**를 클릭합니다.

5. 제거할 인스턴스 유형을 기반으로 하는 가상 머신이 있는 경우 연결된 가상 머신을 나열하는 경고창이 표시됩니다. 인스턴스 유형을 계속 제거하려면 **Approve Operation(작업 승인)** 확인란을 선택합니다. 그렇지 않으면 **Cancel(취소)**을 클릭합니다.

6. **OK(확인)**를 클릭합니다.

인스턴스 유형은 **Instance Types(인스턴스 유형)** 목록에서 제거되며 새 가상 머신을 만들 때 더 이상 사용할 수 없습니다. 제거된 인스턴스 유형에 연결된 가상 머신은 이제 **Custom** (인스턴스 유형 없음)에 연결됩니다.

1.1.5. MAC 주소 풀

MAC 주소 풀은 각 클러스터에 할당된 MAC 주소의 범위를 정의합니다. 각 클러스터에 대해 MAC 주소 풀이 지정됩니다. Red Hat Virtualization은 MAC 주소 풀을 사용하여 새 가상 네트워크 장치에 MAC 주소를 자동으로 생성하고 할당할 수 있으므로 MAC 주소 중복을 방지할 수 있습니다. 클러스터와 관련된 모든 MAC 주소가 할당된 MAC 주소 풀의 범위 내에 있을 때 MAC 주소 풀이 더 메모리가 더 효율적입니다.

동일한 MAC 주소 풀을 여러 클러스터에서 공유할 수 있지만 각 클러스터에는 단일 MAC 주소 풀이 할당됩니다. 기본 MAC 주소 풀은 Red Hat Virtualization에서 생성하며 다른 MAC 주소 풀이 할당되지 않은 경우 사용됩니다. 클러스터에 MAC 주소 풀을 할당하는 방법에 대한 자세한 내용은 [새 클러스터 생성을 참조하십시오](#).



참고

두 개 이상의 Red Hat Virtualization 클러스터가 네트워크를 공유하는 경우 각 클러스터의 가상 머신이 동일한 범위의 MAC 주소를 사용하여 충돌하기 때문에 기본 MAC 주소 풀에만 의존하지 마십시오. MAC 주소 충돌을 방지하려면 MAC 주소 풀 범위를 확인하여 각 클러스터에 고유한 MAC 주소 범위가 할당되어 있는지 확인합니다.

MAC 주소 풀은 풀에 반환된 마지막 주소 뒤에 사용 가능한 다음 MAC 주소를 할당합니다. 범위에 더 이상 남은 주소가 없으면 범위의 처음부터 검색을 다시 시작합니다. 단일 MAC 주소 풀에 정의된 사용 가능한 MAC 주소가 있는 여러 MAC 주소 범위가 있는 경우, 범위는 사용 가능한 MAC 주소를 선택하는 것과 동일한 방식으로 들어오는 요청을 처리합니다.

1.1.5.1. MAC 주소 풀 생성

새 MAC 주소 풀을 생성할 수 있습니다.

절차

1. **Administration(관리) Configure(구성)**를 클릭합니다.
2. **MAC Address Pools(MA 주소 풀)** 탭을 클릭합니다.
3. **추가**를 클릭합니다.
4. 새 MAC 주소 풀의 **Name** (이름) 및 **Description** (설명)을 입력합니다.
5. MAC 주소를 풀에서 여러 번 사용할 수 있도록 **Allow Duplicates** (중복 허용) 확인란을 선택합니다. MAC 주소 풀은 중복 MAC 주소를 자동으로 사용하지 않지만 중복 옵션을 활성화하면 사용자가 중복 MAC 주소를 수동으로 사용할 수 있습니다.



참고

하나의 MAC 주소 풀에 중복이 비활성화되어 있고 다른 하나는 중복이 활성화된 경우, 중복이 비활성화된 풀에서 각 MAC 주소를 한 번 사용할 수 있지만 중복이 활성화된 풀에서 여러 번 사용할 수 있습니다.

6. 필요한 **MAC 주소 범위를 입력합니다**. 여러 범위를 시작하려면 **From and To(다음에서 및 대상)** 필드 옆의 더하기 버튼을 클릭합니다.
7. **OK(확인)**를 클릭합니다.

1.1.5.2. MAC 주소 풀 편집

MAC 주소 풀을 편집하여 풀에서 사용할 수 있는 MAC 주소 범위 및 중복이 허용되는지 여부를 포함하여 세부 정보를 변경할 수 있습니다.

절차

1. **Administration(관리) Configure(구성)** 를 클릭합니다.
2. **MAC Address Pools(MA 주소 풀)** 탭을 클릭합니다.
3. 편집할 MAC 주소 풀을 선택합니다.
4. **Edit(편집)** 를 클릭합니다.
5. **Name (이름)**, **Description (설명)**, **Allow Duplicates (배포 허용)** 및 **MAC Address Ranges(MAC 주소 범위)** 필드를 필요에 따라 변경합니다.



참고

MAC 주소 범위가 업데이트되면 기존 NIC의 MAC 주소가 다시 할당되지 않습니다. 이미 할당되었지만 새로운 MAC 주소 범위를 벗어나는 MAC 주소는 사용자 지정 MAC 주소로 추가되며 해당 MAC 주소 풀에서 계속 추적됩니다.

6. **OK(확인)**를 클릭합니다.

1.1.5.3. MAC 주소 풀 권한 편집

MAC 주소 풀을 만들고 나면 사용자 권한을 편집할 수 있습니다. 사용자 권한은 MAC 주소 풀을 사용할 수 있는 데이터 센터를 제어합니다. 새 사용자 권한을 추가하는 방법에 대한 자세한 내용은 [역할](#)을 참조하십시오.

절차

1. **Administration(관리) Configure(구성)** 를 클릭합니다.
2. **MAC Address Pools(MA 주소 풀)** 탭을 클릭합니다.
3. 필수 MAC 주소 풀을 선택합니다.
4. MAC 주소 풀에 대한 사용자 권한을 편집합니다.
 - MAC 주소 풀에 사용자 권한을 추가하려면 다음을 수행합니다.

- a. **Configure(구성)** 창의 아래쪽에 있는 사용자 권한 창에서 **Add (추가)**를 클릭합니다.
 - b. 필요한 사용자를 검색하고 선택합니다.
 - c. **Role to Assign** (할당으로 역할) 드롭다운 목록에서 필요한 역할을 선택합니다.
 - d. **OK(확인)**를 클릭하여 사용자 권한을 추가합니다.
- MAC 주소 풀에서 사용자 권한을 제거하려면 다음을 수행합니다.
 - a. **Configure** (구성) 창의 하단에 있는 사용자 권한 창에서 제거할 사용자 권한을 선택합니다.
 - b. **Remove(제거)**를 클릭하여 사용자 권한을 제거합니다.

1.1.5.4. MAC 주소 풀 제거

풀이 클러스터와 연결되어 있지 않지만 기본 MAC 주소 풀을 제거할 수 없는 경우 생성된 MAC 주소 풀을 제거할 수 있습니다.

절차

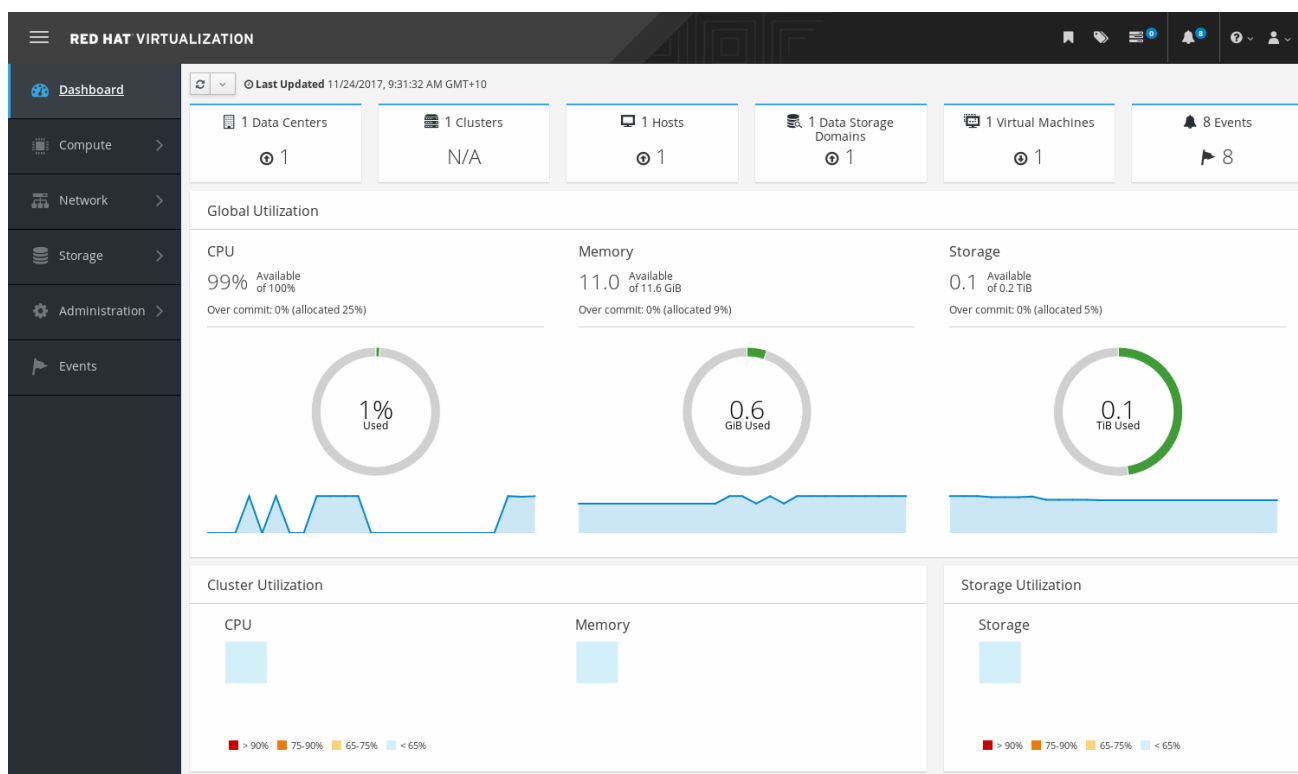
1. **Administration(관리) Configure(구성)**를 클릭합니다.
2. **MAC Address Pools(MA 주소 풀)** 탭을 클릭합니다.
3. 제거할 MAC 주소 풀을 선택합니다.
4. **Remove** (제거)를 클릭합니다.
5. **OK(확인)**를 클릭합니다.

1.2. 대시보드

대시보드는 Red Hat Virtualization의 리소스 및 사용률에 대한 요약을 표시하여 Red Hat Virtualization 시스템 상태에 대한 개요를 제공합니다. 이 요약을 통해 문제에 대해 알리고 문제 영역을 분석할 수 있습니다.

대시보드의 정보는 기본적으로 데이터 웨어하우스에서 15분마다 업데이트되며, 기본적으로 Manager API에서 15초마다 업데이트되거나 대시보드가 새로 고쳐질 때마다 업데이트됩니다. 사용자가 다른 페이지에서 다시 변경하거나 수동으로 새로 고침하면 대시보드가 새로 고쳐집니다. 대시보드가 자동으로 새로 고쳐지지 않습니다. 인벤토리 카드 정보는 관리자 API에서 제공하며, 데이터 웨어하우스에서 사용률 정보를 제공합니다. 대시보드는 Manager와 함께 자동으로 설치 및 업그레이드되는 UI 플러그인 구성 요소로 구현됩니다.

그림 1.6. 대시보드



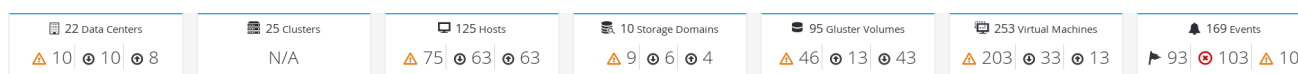
1.2.1. 사전 요구 사항

대시보드를 사용하려면 데이터 웨어하우스가 설치 및 구성되어 있어야 합니다. 데이터 웨어하우스 [가이드](#)의 데이터 웨어하우스 설치 및 구성을 참조하십시오.

1.2.2. 글로벌 인벤토리

대시보드의 상단 섹션에서는 Red Hat Virtualization 리소스의 글로벌 인벤토리를 제공하며 데이터 센터, 클러스터, 호스트, 스토리지 도메인, 가상 시스템 및 이벤트에 대한 항목을 포함합니다. 아이콘은 각 리소스의 상태를 표시하고 숫자에는 해당 상태가 있는 각 리소스의 수량이 표시됩니다.

그림 1.7. 글로벌 인벤토리



제목은 리소스 유형의 수를 표시하며, 해당 상태는 제목 아래 표시됩니다. 리소스 제목을 클릭하면 Red Hat Virtualization Manager의 관련 페이지로 이동합니다. 클러스터의 상태는 항상 N/A로 표시됩니다.

표 1.14. 리소스 상태

아이콘	상태
	Red Hat Virtualization에 추가된 리소스가 없습니다.

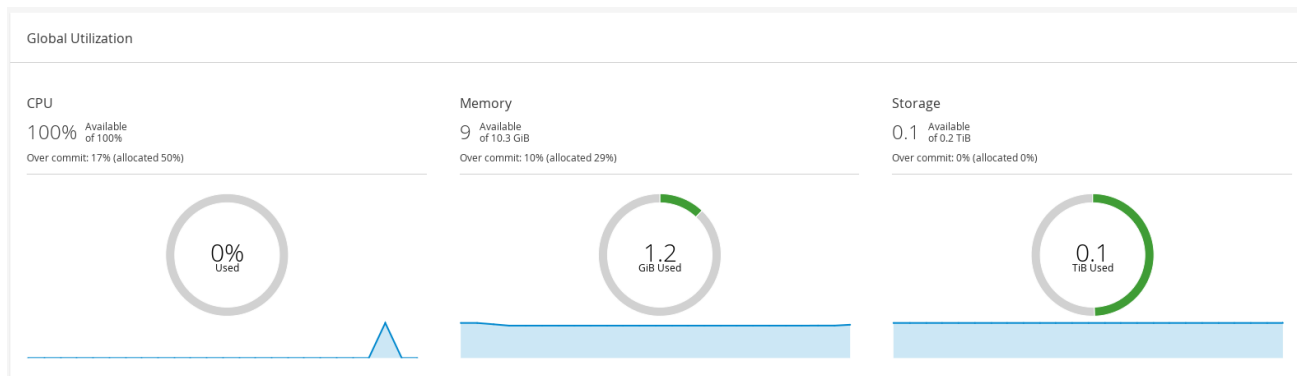
아이콘	상태
	경고 상태의 리소스 수를 표시합니다. 아이콘을 클릭하면 경고 상태로 해당 리소스로 제한된 검색이 있는 적절한 페이지로 이동합니다. 검색은 리소스마다 다르게 제한됩니다. ● 데이터 센터: 검색은 작동하거나 응답하지 않는 데이터 센터로 제한됩니다. ● Gluster 볼륨: 검색은 전원을 켜거나, 일시 중지됨, 마이그레이션, 대기, 일시 중단 또는 전원이 꺼지는 Gluster 볼륨으로 제한됩니다. ● 호스트: 검색은 할당되지 않았거나 유지 관리 모드, 설치, 재부팅, 유지 관리 준비, 보류 중인 승인 또는 연결을 위한 호스트로 제한됩니다. ● 스토리지 도메인: 검색은 초기화되지 않았거나, 연결되지 않음, 비활성, 유지 관리 모드에서 준비, 유지 관리, 분리 또는 활성화를 준비하는 스토리지 도메인으로 제한됩니다. ● 가상 머신: 이 검색은 전원 켜기, 일시 중지, 마이그레이션, 대기, 일시 중단 또는 전원이 꺼지는 가상 머신으로 제한됩니다. ● 이벤트: 검색은 심각도가 warning인 이벤트로 제한됩니다.
	상태가 up인 리소스 수를 표시합니다. 아이콘을 클릭하면 작동 중인 리소스로 제한된 검색으로 적절한 페이지로 이동합니다.
	상태가 down인 리소스 수를 표시합니다. 아이콘을 클릭하면 down 상태로 리소스로 제한된 검색을 사용하여 적절한 페이지로 이동합니다. 검색은 리소스마다 다르게 제한됩니다. ● 데이터 센터: 검색은 초기화되지 않았거나 유지 관리 모드 또는 다운 상태인 데이터 센터로 제한됩니다. ● Gluster 볼륨: 검색은 분리되거나 비활성 볼륨으로 제한됩니다. ● 호스트: 검색은 응답하지 않고 오류가 있으며 설치 오류, 비작동, 초기화 또는 다운이 있는 호스트로 제한됩니다. ● 스토리지 도메인: 검색은 분리되거나 비활성화된 스토리지 도메인으로 제한됩니다. ● 가상 머신: 검색은 다운되거나 응답하지 않거나 재부팅되지 않는 가상 시스템으로 제한됩니다.

아이콘	상태
images:images/Dashboard_Alert.png[title="Alert icon"]	경고 상태가 있는 이벤트 수를 표시합니다. 아이콘을 클릭하면 심각도가 alert인 이벤트 로 제한된 검색이 있는 이벤트로 이동합니다.
images:images/Dashboard_Error.png[title="Error icon"]	오류 상태의 이벤트 수를 표시합니다. 아이콘을 클릭하면 심각도가 error인 이벤트로 제한된 검색이 있는 Events 로 이동합니다.

1.2.3. 글로벌 사용률

Global Utilization(글로벌 사용률) 섹션에는 CPU, Memory, Storage(메모리 및 스토리지)의 시스템 사용률이 표시됩니다.

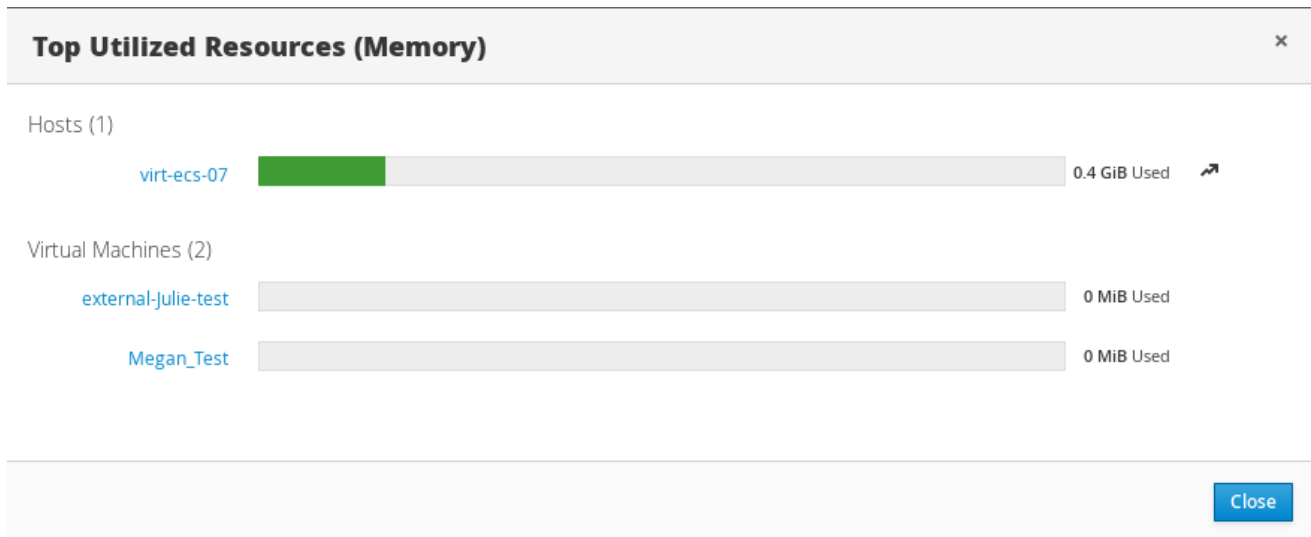
그림 1.8. 글로벌 사용률



- top 섹션에서는 사용 가능한 CPU, 메모리 또는 스토리지의 백분율과 오버 커밋 비율을 보여줍니다. 예를 들어, CPU의 오버 커밋 비율은 데이터 웨어하우스의 최신 데이터에 따라 실행 중인 가상 머신에 사용 가능한 물리적 코어 수를 가상 코어 수를 나누어 계산합니다.
- 도넛은 CPU, 메모리 또는 스토리지의 사용량(%)을 표시하고, 지난 5분 동안 평균 사용량에 따라 모든 호스트의 평균 사용량을 표시합니다. 도넛의 섹션을 가리키면 선택한 섹션의 값이 표시됩니다.
- 하단의 줄 그래프에는 지난 24시간 동안 추세가 표시됩니다. 각 데이터 지점에는 특정 시간 동안 평균 사용량이 표시됩니다. 그래프에서 지점을 가리키면 CPU 그래프에 사용된 시간과 백분율, 메모리 및 스토리지 그래프의 사용량 양이 표시됩니다.

1.2.3.1. 사용률 상위 리소스

그림 1.9. 사용률 상위 리소스 (Memory)

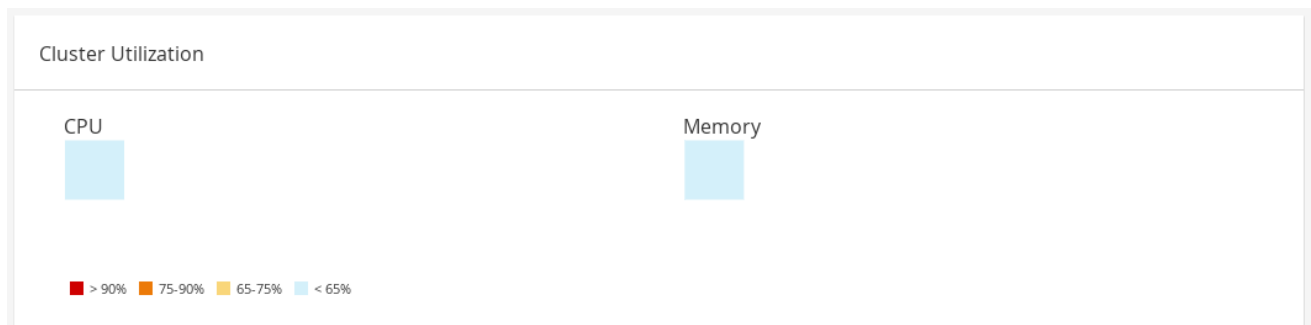


대시보드의 글로벌 사용률 섹션에서 도넛을 클릭하면 CPU, 메모리 또는 스토리지에 가장 많이 사용되는 리소스 목록이 표시됩니다. CPU 및 메모리의 경우 팝업에는 사용량이 가장 높은 10개의 호스트와 가상 시스템 목록이 표시됩니다. 스토리지의 경우 팝업에는 사용된 상위 10개 스토리지 도메인 및 가상 시스템 목록이 표시됩니다. 사용 표시줄 오른쪽에 있는 화살표는 해당 리소스의 사용 추세를 최근 1분 내에 표시합니다.

1.2.4. 클러스터 사용률

Cluster Utilization(클러스터 사용률) 섹션에는 heatmap의 CPU 및 메모리의 클러스터 사용률이 표시됩니다.

그림 1.10. 클러스터 사용률



1.2.4.1. CPU

지난 24시간 동안 CPU의 평균 사용률을 보여주는 특정 클러스터에 대한 CPU 사용률의 heatmap입니다. heatmap을 가리키면 클러스터 이름이 표시됩니다. heatmap을 클릭하면 **Compute → Hosts(호스트)** 로 이동하여 CPU 사용률에 따라 정렬된 특정 클러스터에서 검색 결과가 표시됩니다. 클러스터의 CPU 사용량을 계산하는 데 사용되는 공식은 클러스터의 평균 호스트 CPU 사용률입니다. 이는 클러스터의 CPU 총 사용량을 찾기 위해 지난 24시간 동안 각 호스트에 대한 평균 호스트 CPU 사용률을 사용하여 계산됩니다.

1.2.4.2. 메모리

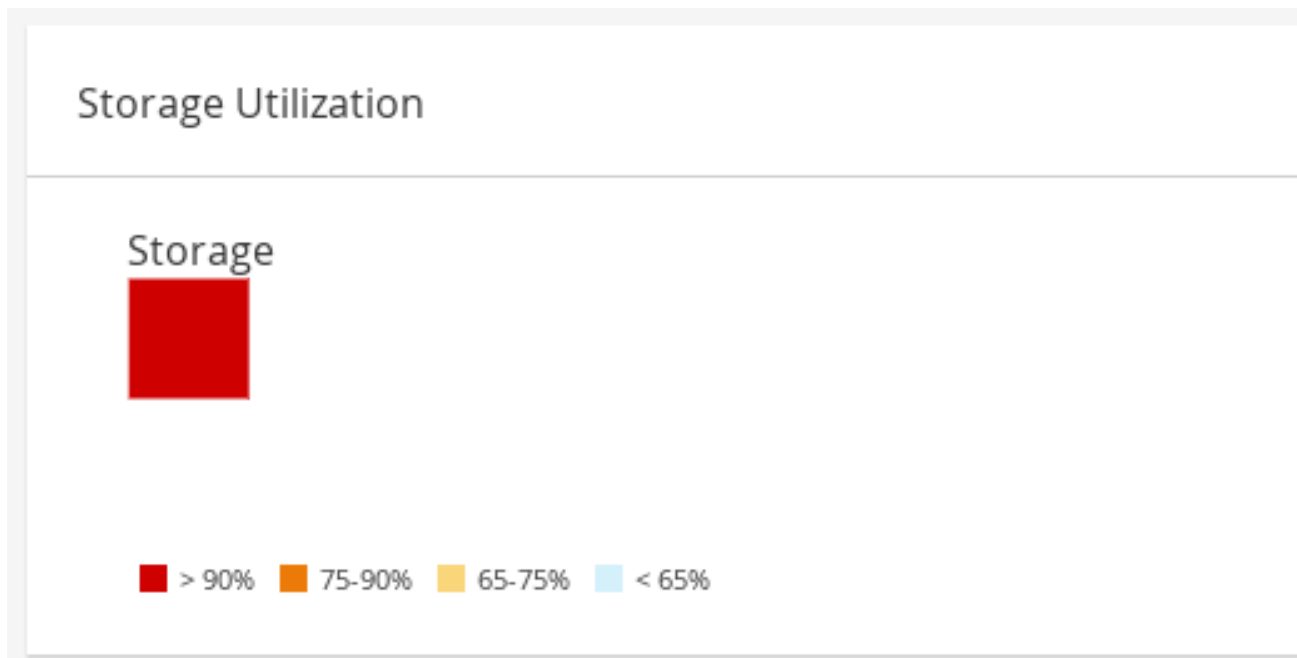
마지막 24시간 동안 메모리의 평균 사용률을 보여주는 특정 클러스터에 대한 메모리 사용률의 heatmap입니다. heatmap을 가리키면 클러스터 이름이 표시됩니다. heatmap을 클릭하면 **Compute → Hosts(호스트)** 로 이동하여 메모리 사용량에 따라 정렬된 특정 클러스터에 대한 검색 결과가 표시됩니다. 클러스터의

메모리 사용량을 계산하는 데 사용되는 공식은 클러스터의 메모리 총 사용률(GB)입니다. 이는 마지막 24 시간 동안 각 호스트에 대한 평균 호스트 메모리 사용률을 사용하여 클러스터의 총 메모리 사용량을 찾아 계산합니다.

1.2.5. 스토리지 사용률

Storage Utilization(스토리지 사용률) 섹션에는 heatmap의 스토리지 사용률이 표시됩니다.

그림 1.11. 스토리지 사용률



heatmap은 지난 24시간 동안 스토리지의 평균 사용률을 보여줍니다. 클러스터의 스토리지 사용량을 계산하는 데 사용하는 공식은 클러스터의 스토리지 총 사용률입니다. 이는 클러스터의 스토리지 총 사용량을 찾기 위해 지난 24시간 동안 각 호스트의 평균 스토리지 사용률을 사용하여 계산됩니다. heatmap을 가리키면 스토리지 도메인 이름이 표시됩니다. heatmap을 클릭하면 사용률에 따라 정렬된 스토리지 도메인을 사용하여 **StorageDomains** (스토리지 도메인)로 이동합니다.

1.3. 검색

1.3.1. Red Hat Virtualization에서 검색 수행

관리 포털을 사용하면 가상 시스템, 호스트, 사용자 등 수천 개의 리소스를 관리할 수 있습니다. 검색을 수행하려면 검색 쿼리(무료 텍스트 또는 구문 기반)를 검색 표시줄에 입력합니다(각 리소스의 기본 페이지에서 사용 가능). 검색 쿼리는 향후 재사용을 위해 북마크로 저장될 수 있으므로 특정 검색 결과가 필요할 때마다 검색 쿼리를 다시 입력할 필요가 없습니다. 검색은 대소문자를 구분하지 않습니다.

1.3.2. 구문 및 예제 검색

Red Hat Virtualization 리소스에 대한 검색 쿼리 구문은 다음과 같습니다.

결과 유형: {critoe} [sortby sort_spec]

구문 예

다음 예제에서는 검색 쿼리를 사용하는 방법을 설명하고 Red Hat Virtualization이 검색 쿼리 구축을 지원하는 방법을 이해하는 데 도움이 됩니다.

표 1.15. 검색 쿼리 예

예제	결과
호스트: VMs.status = 페이지 위로 2	작동 중인 가상 시스템을 실행하는 모든 호스트 목록의 2페이지를 표시합니다.
VM: domain = qa.company.com	지정된 도메인에서 실행 중인 모든 가상 시스템 목록을 표시합니다.
VM: users.name =	사용자 이름에 속하는 모든 가상 시스템 목록을 표시합니다.
이벤트: 심각도 > 일반 정렬	심각도가 Normal 이상인 모든 이벤트 목록을 표시하고 시간별로 정렬됩니다.

1.3.3. 자동 완성 검색

관리 포털은 자동 완성 기능을 제공하여 유효하고 강력한 검색 쿼리 생성에 도움이 됩니다. 검색 쿼리의 각 부분을 입력하면 검색바에서 다음 검색 부분에 대한 선택 드롭다운 목록이 열립니다. 목록에서 선택한 다음 검색의 다음 부분을 계속 입력/선택하거나 옵션을 무시하고 수동으로 쿼리를 입력할 수 있습니다.

다음 테이블에서는 관리 포털을 자동 완성하는 방법을 예제로 지정합니다.

호스트: VMs.status = down

표 1.16. 자동 완성을 사용하여 검색 쿼리의 예

입력	표시된 항목 나열	동작
h	호스트 (1 옵션만 해당)	호스트 선택 또는 호스트 유형
호스트:	모든 호스트 속성	유형 v
호스트: v	v로 시작하는 호스트 속성	Vms를 선택하거나 Vms를 입력합니다.
호스트: Vms	모든 가상 머신 속성	s입력
호스트: VMs.s	모든 가상 머신 속성은 s로 시작합니다	상태 또는 유형 상태 선택
호스트: Vms.status	= !=	선택 또는 유형 =
호스트: Vms.status =	모든 상태 값	선택 또는 입력

1.3.4. 결과 검색 유형 옵션

결과 유형을 사용하면 다음 유형의 리소스를 검색할 수 있습니다.

- 가상 머신 목록의 VM
- 호스트 목록의 호스트
- 풀 목록의 풀
- 템플릿 목록의 템플릿
- 이벤트 목록 이벤트
- 사용자 목록 사용자
- 클러스터 목록의 클러스터
- 데이터 센터 목록의 데이터센터
- 스토리지 도메인 목록 스토리지

각 리소스 유형에는 고유한 속성 집합과 연결된 다른 리소스 유형 집합이 있으므로 각 검색 유형에는 유효한 구문 조합 세트가 있습니다. 자동 완성 기능을 사용하여 유효한 쿼리를 쉽게 만들 수도 있습니다.

1.3.5. 검색 기준

쿼리에서 콜론 뒤에 검색 기준을 지정할 수 있습니다. **{critoe}** 구문은 다음과 같습니다.

<prop><operator><value>

또는

<obj-type><prop><operator><value>

예

다음 표에서는 구문의 부분을 설명합니다.

표 1.17. 검색 기준 예

부분	설명	값	예제	참고
prop	searched-for 리소스의 속성입니다. 또한 리소스 유형의 속성일 수도 있고(obj-type 참조), 태그(custom tag)가 될 수도 있습니다.	특정 속성을 사용하여 개체로 검색을 제한합니다. 예를 들어 status 속성이 있는 오브젝트를 검색합니다.	상태	해당 없음
obj-type	searched-for 리소스와 연결할 수 있는 리소스 유형입니다.	데이터 센터 및 가상 시스템과 같은 시스템 오브젝트입니다.	사용자	해당 없음

부분	설명	값	예제	참고
operator	비교 연산자.	= != (동일하지 않음) > < >= <=	해당 없음	값 옵션은 속성에 따라 다릅니다.
현재의	표현식을 와 비교합니다.	문자열 정수 순위 날짜(지역 설정에 따라 포맷됨)	마케도니아 256 보통	- 문자열 내에서 와일드카드를 사용할 수 있습니다. ""(두 세트의 공백이 없는 따옴표로 묶음)을 사용하여 초기화되지 않은(비어 있음) 문자열을 나타낼 수 있습니다. - 큰따옴표는 공백이 포함된 문자열 또는 날짜와 관련이 있습니다.

1.3.6. 검색: 다중 기준 및 와일드카드

와일드카드는 문자열의 구문의 **<value>** 부분에서 사용할 수 있습니다. 예를 들어 m으로 시작하는 모든 사용자를 찾으려면 **m ***을 입력합니다.

부울 연산자 및 **OR**을 사용하여 두 가지 기준을 검색할 수 있습니다. 예를 들면 다음과 같습니다.

VM: users.name = m* and status = Up

이 쿼리는 이름이 "m"으로 시작하는 사용자에 대해 실행 중인 모든 가상 시스템을 반환합니다.

VMs: users.name = m* AND tag = "paris-loc"

이 쿼리는 이름이 "m"으로 시작하는 사용자에 대해 "paris-loc" 태그가 지정된 모든 가상 머신을 반환합니다.

AND 또는 **OR** 없이 두 가지 기준을 지정하는 경우 **AND** 가 암시됩니다. **OR**, 또는 우선 순위 및 우선 순위.

1.3.7. 검색: 검색 순서 확인

sortby 를 사용하여 반환된 정보의 정렬 순서를 확인할 수 있습니다. 정렬 방향(오름차순의 경우 **asc**, 내림차순의 경우 **desc**)을 포함할 수 있습니다.

예를 들면 다음과 같습니다.

이벤트: severity > normal sortby time desc

이 쿼리는 심각도가 Normal 이상인 모든 이벤트를 반환하고, 시간별로 정렬(준비 순서)을 반환합니다.

1.3.8. 데이터 센터 검색

다음 표에는 데이터 센터의 모든 검색 옵션이 설명되어 있습니다.

표 1.18. 데이터 센터 검색

속성(리소스 또는 리소스 유형)	유형	설명 (참조)
cluster.cluster-prop	속성 유형에 따라 다릅니다.	데이터 센터와 연결된 클러스터의 속성입니다.
name	문자열	데이터 센터의 이름입니다.
description	문자열	데이터 센터에 대한 설명입니다.
type	문자열	데이터 센터의 유형.
status	list	데이터 센터의 가용성.
sortby	list	반환된 결과를 리소스 속성 중 하나로 정렬합니다.
page	정수	표시할 페이지 결과 수입니다.

예제

datacenter: type = nfs 및 status != up

이 예제에서는 스토리지 유형이 NFS이고 up 이외의 상태가 있는 데이터 센터 목록을 반환합니다.

1.3.9. 클러스터 검색

다음 테이블에서는 클러스터의 모든 검색 옵션에 대해 설명합니다.

표 1.19. 클러스터 검색

속성(리소스 또는 리소스 유형)	유형	설명 (참조)
datacenter.datacenter-prop	속성 유형에 따라 다릅니다.	클러스터와 연결된 데이터 센터의 속성입니다.
데이터 센터	문자열	클러스터가 속한 데이터 센터입니다.
name	문자열	네트워크에서 클러스터를 식별하는 고유 이름입니다.
description	문자열	클러스터에 대한 설명입니다.
초기화됨	문자열	참 또는 False는 클러스터 상태를 나타냅니다.
sortby	list	반환된 결과를 리소스 속성 중 하나로 정렬합니다.
page	정수	표시할 페이지 결과 수입니다.

예제

클러스터: **initialized = true** 또는 **name = Default**

이 예에서는 초기화되거나 이름이 Default인 클러스터 목록을 반환합니다.

1.3.10. 호스트 검색

다음 테이블에서는 호스트에 대한 모든 검색 옵션을 설명합니다.

표 1.20. 호스트 검색

속성(리소스 또는 리소스 유형)	유형	설명 (참조)
VM. Vms-prop	속성 유형에 따라 다릅니다.	호스트와 연결된 가상 시스템의 속성입니다.
templates-prop	속성 유형에 따라 다릅니다.	호스트와 연결된 템플릿의 속성입니다.
events.events-prop	속성 유형에 따라 다릅니다.	호스트와 연결된 이벤트의 속성입니다.
users.users-prop	속성 유형에 따라 다릅니다.	호스트와 연결된 사용자의 속성입니다.
name	문자열	호스트의 이름입니다.

속성(리소스 또는 리소스 유형)	유형	설명 (참조)
status	list	호스트의 가용성.
external_status	문자열	외부 시스템 및 플러그인에서 보고한 호스트의 상태입니다.
cluster	문자열	호스트가 속한 클러스터입니다.
address	문자열	네트워크에서 호스트를 식별하는 고유 이름입니다.
cpu_usage	정수	사용된 처리 능력의 백분율.
mem_usage	정수	사용된 메모리의 백분율입니다.
network_usage	정수	네트워크 사용량의 백분율입니다.
load	정수	지정된 시간 슬라이스당 프로세서당 실행 대기열에서 실행되도록 대기 중인 작업.
버전	정수	운영 체제의 버전 번호입니다.
cpus	정수	호스트의 CPU 수입니다.
memory	정수	사용 가능한 메모리 양입니다.
cpu_speed	정수	CPU의 처리 속도입니다.
cpu_model	문자열	CPU 유형입니다.
active_vms	정수	현재 실행 중인 가상 시스템의 수입니다.
migrating_vms	정수	현재 마이그레이션 중인 가상 시스템의 수입니다.
committed_mem	정수	커밋된 메모리의 백분율입니다.
tag	문자열	호스트에 할당된 태그입니다.
type	문자열	호스트 유형입니다.
datacenter	문자열	호스트가 속한 데이터 센터입니다.
sortby	list	반환된 결과를 리소스 속성 중 하나로 정렬합니다.

속성(리소스 또는 리소스 유형)	유형	설명 (참조)
page	정수	표시할 페이지 결과 수입니다.

예제

hosts: cluster = Default 및 Vms.os = rhel6

이 예제에서는 Red Hat Enterprise Linux 6 운영 체제를 실행하는 Default 클러스터 및 호스트 가상 시스템의 일부인 호스트 목록을 반환합니다.

1.3.11. 네트워크 검색

다음 테이블에서는 네트워크의 모든 검색 옵션에 대해 설명합니다.

표 1.21. 네트워크 검색

속성(리소스 또는 리소스 유형)	유형	설명 (참조)
Cluster_network.clusternetwork-prop	속성 유형에 따라 다릅니다.	네트워크와 연결된 클러스터의 속성입니다.
Host_Network.hostnetwork-prop	속성 유형에 따라 다릅니다.	네트워크와 연결된 호스트의 속성입니다.
name	문자열	사람이 읽을 수 있는 네트워크를 식별하는 이름입니다.
description	문자열	네트워크를 설명하는 키워드 또는 텍스트로, 네트워크를 만들 때 선택적으로 사용됩니다.
vlanid	정수	네트워크의 VLAN ID입니다.
stp	문자열	네트워크에 대해 STP(Spanning Tree Protocol)를 활성화하거나 비활성화할지 여부입니다.
mtu	정수	논리적 네트워크의 최대 전송 단위입니다.
vmnetwork	문자열	네트워크가 가상 시스템 트래픽에만 사용되는지 여부.
datacenter	문자열	네트워크를 연결하는 데이터 센터입니다.

속성(리소스 또는 리소스 유형)	유형	설명 (참조)
sortby	list	반환된 결과를 리소스 속성 중 하나로 정렬합니다.
page	정수	표시할 페이지 결과 수입니다.

예제

Network: mtu > 1500 and vmnetwork = true

이 예제에서는 최대 전송 단위가 1500바이트보다 크며 가상 시스템에서만 사용하도록 설정된 네트워크 목록을 반환합니다.

1.3.12. 스토리지 검색

다음 테이블에서는 스토리지의 모든 검색 옵션에 대해 설명합니다.

표 1.22. 스토리지 검색

속성(리소스 또는 리소스 유형)	유형	설명 (참조)
호스트.hosts-prop	속성 유형에 따라 다릅니다.	스토리지와 연결된 호스트의 속성입니다.
cluster.cluster-prop	속성 유형에 따라 다릅니다.	스토리지와 연결된 클러스터의 속성입니다.
name	문자열	네트워크에서 스토리지를 식별하는 고유 이름입니다.
status	문자열	스토리지 도메인의 상태.
external_status	문자열	외부 시스템 및 플러그인에서 보고한 스토리지 도메인의 상태입니다.
datacenter	문자열	스토리지가 속한 데이터 센터입니다.
type	문자열	스토리지 유형입니다.
free-size	정수	사용 가능한 스토리지의 크기(GB).
used-size	정수	사용되는 스토리지의 양(GB)입니다.
total_size	정수	사용 가능한 스토리지의 총 용량(GB).

속성(리소스 또는 리소스 유형)	유형	설명 (참조)
커밋됨	정수	커밋된 스토리지의 양(GB)입니다.
sortby	list	반환된 결과를 리소스 속성 중 하나로 정렬합니다.
page	정수	표시할 페이지 결과 수입니다.

예제

스토리지: **free_size > 6 GB** 및 **total_size < 20 GB**

이 예에서는 사용 가능한 스토리지 공간이 6GB보다 크거나 총 스토리지 공간이 20GB 미만인 스토리지 목록을 반환합니다.

1.3.13. 디스크 검색

다음 테이블에서는 디스크의 모든 검색 옵션에 대해 설명합니다.



참고

디스크 유형 및 콘텐츠 유형 필터링 옵션을 사용하여 표시된 가상 디스크 수를 줄일 수 있습니다.

표 1.23. 디스크 검색

속성(리소스 또는 리소스 유형)	유형	설명 (참조)
datacenters.datacenters-prop	속성 유형에 따라 다릅니다.	디스크와 연결된 데이터 센터의 속성입니다.
storages.storages-prop	속성 유형에 따라 다릅니다.	디스크와 연결된 스토리지의 속성입니다.
alias	문자열	네트워크에서 스토리지를 식별하는 사람이 읽을 수 있는 이름입니다.
description	문자열	디스크를 설명하는 키워드 또는 텍스트(디스크 생성 시 선택적으로 사용됩니다).
provisioned_size	정수	디스크의 가상 크기입니다.
크기	정수	디스크 크기입니다.
actual_size	정수	디스크에 할당된 실제 크기입니다.

속성(리소스 또는 리소스 유형)	유형	설명 (참조)
creation_date	정수	디스크를 만든 날짜입니다.
bootable	문자열	디스크를 부팅할 수 있는지 또는 부팅할 수 있는지 여부입니다. 유효한 값은 0,1,yes 또는 no 중 하나입니다.
공유 가능	문자열	디스크를 한 번에 둘 이상의 가상 머신에 연결할 수 있는지 여부입니다. 유효한 값은 0,1,yes 또는 no 중 하나입니다.
포맷	문자열	디스크 형식입니다. 사용하지 않거나 할당되지 않은 cow 또는 raw 중 하나일 수 있습니다.
status	문자열	디스크 상태입니다. 할당되지 않은,ok,locked,invalid, bad 중 하나일 수 있습니다.
disk_type	문자열	디스크 유형입니다. 이미지 또는 lun 중 하나일 수 있습니다.
number_of_vms	정수	디스크가 연결된 가상 시스템의 수입니다.
vm_names	문자열	디스크가 연결된 가상 시스템의 이름입니다.
할당량	문자열	가상 디스크에 적용된 할당량의 이름입니다.
sortby	list	반환된 결과를 리소스 속성 중 하나로 정렬합니다.
page	정수	표시할 페이지 결과 수입니다.

예제

디스크: 형식 = **cow** 및 **provisioned_size > 8**

이 예에서는 QCOW 형식과 할당된 디스크 크기가 8GB보다 큰 가상 디스크 목록을 반환합니다.

1.3.14. 볼륨 검색

다음 표에는 볼륨에 대한 모든 검색 옵션이 설명되어 있습니다.

표 1.24. 볼륨 검색

속성(리소스 또는 리소스 유형)	유형	설명 (참조)
Cluster	문자열	볼륨과 연결된 클러스터의 이름입니다.
cluster.cluster-prop	속성 유형에 따라 다릅니다(예: name, description, comment, architecture)	볼륨과 연결된 클러스터의 속성입니다.
name	문자열	사람이 읽을 수 있는 볼륨을 식별하는 이름입니다.
type	문자열	배포, 복제, distributed_replicate, 스트라이프 또는 distributed_stripe 중 하나일 수 있습니다.
transport_type	정수	TCP 또는 RDMA 중 하나일 수 있습니다.
REPLICA_COUNT	정수	복제본 수입니다.
stripe_count	정수	스트라이프 수.
status	문자열	볼륨 상태입니다. Up 또는 Down 중 하나일 수 있습니다.
sortby	list	반환된 결과를 리소스 속성 중 하나로 정렬합니다.
page	정수	표시할 페이지 결과 수입니다.

예제

볼륨: transport_type = rdma 및 stripe_count >= 2

이 예에서는 전송 유형이 RDMA로 설정되어 있고 2개 이상의 스트라이프가 있는 볼륨 목록을 반환합니다.

1.3.15. 가상 머신 검색

다음 표에는 가상 시스템의 모든 검색 옵션이 설명되어 있습니다.



참고

현재 **Network Label**(네트워크 레이블), **Custom Emulated Machine**(사용자 지정 에뮬레이션 시스템) 및 **Custom CPU Type** 속성은 지원되지 않습니다.

표 1.25. 가상 머신 검색

속성(리소스 또는 리소스 유형)	유형	설명 (참조)
호스트.<i>hosts-prop</i>	속성 유형에 따라 다릅니다.	가상 시스템과 연결된 호스트의 속성입니다.
<i>templates-prop</i>	속성 유형에 따라 다릅니다.	가상 머신과 연결된 템플릿의 속성입니다.
events.<i>events-prop</i>	속성 유형에 따라 다릅니다.	가상 머신과 연결된 이벤트의 속성입니다.
users.<i>users-prop</i>	속성 유형에 따라 다릅니다.	가상 머신과 연결된 사용자의 속성입니다.
storage.<i>storage-prop</i>	속성 유형에 따라 다릅니다.	가상 머신과 연결된 스토리지 장치의 속성입니다.
vNIC.<i>vnic-prop</i>	속성 유형에 따라 다릅니다.	가상 머신과 연결된 vNIC의 속성입니다.
name	문자열	가상 시스템의 이름입니다.
status	list	가상 시스템의 가용성.
ip	정수	가상 시스템의 IP 주소입니다.
uptime	정수	가상 시스템이 실행 중인 분(분)입니다.
domain	문자열	이러한 시스템을 그룹화하는 도메인(일반적으로 Active Directory 도메인)입니다.
OS	문자열	가상 시스템이 생성될 때 선택한 운영 체제입니다.
creationDate	날짜	가상 시스템이 생성된 날짜입니다.
address	문자열	네트워크에서 가상 시스템을 식별하는 고유 이름입니다.
cpu_usage	정수	사용된 처리 능력의 백분율.
mem_usage	정수	사용된 메모리의 백분율입니다.
network_usage	정수	사용된 네트워크의 백분율입니다.
memory	정수	정의된 최대 메모리입니다.

속성(리소스 또는 리소스 유형)	유형	설명 (참조)
apps	문자열	현재 가상 시스템에 설치된 애플리케이션입니다.
cluster	list	가상 시스템이 속한 클러스터입니다.
pool	list	가상 시스템이 속한 가상 시스템 풀입니다.
loggedinuser	문자열	현재 가상 시스템에 로그인한 사용자의 이름입니다.
tag	list	가상 시스템이 속한 태그입니다.
datacenter	문자열	가상 시스템이 속한 데이터 센터입니다.
type	list	가상 머신 유형(서버 또는 데스크탑).
할당량	문자열	가상 머신과 연결된 할당량의 이름입니다.
description	문자열	가상 시스템을 설명하는 키워드 또는 텍스트로, 가상 시스템을 생성할 때 선택적으로 사용됩니다.
sortby	list	반환된 결과를 리소스 속성 중 하나로 정렬합니다.
page	정수	표시할 페이지 결과 수입니다.
next_run_configuration_exists	부울	가상 시스템에는 보류 중인 구성 변경 사항이 있습니다.

예제

VM: template.name = Win* 및 user.name = ""

이 예제에서는 기본 템플릿 이름이 **Win** 으로 시작되어 사용자에게 할당되는 가상 시스템 목록을 반환합니다.

예제

VM: cluster = Default 및 os = windows7

이 예에서는 **Default** 클러스터에 속하고 Windows 7을 실행 중인 가상 머신 목록을 반환합니다.

1.3.16. 풀 검색

다음 표에는 풀의 모든 검색 옵션이 설명되어 있습니다.

표 1.26. 풀 검색

속성(리소스 또는 리소스 유형)	유형	설명 (참조)
name	문자열	풀의 이름입니다.
description	문자열	풀에 대한 설명입니다.
type	list	풀 유형입니다.
sortby	list	반환된 결과를 리소스 속성 중 하나로 정렬합니다.
page	정수	표시할 페이지 결과 수입니다.

예제

풀: **type = automatic**

이 예에서는 유형이 automatic인 풀 목록을 반환합니다.

1.3.17. 템플릿 검색

다음 표에는 템플릿의 모든 검색 옵션이 설명되어 있습니다.

표 1.27. 템플릿 검색

속성(리소스 또는 리소스 유형)	유형	설명 (참조)
VM. <i>Vms-prop</i>	문자열	템플릿과 연결된 가상 시스템의 속성입니다.
호스트. <i>hosts-prop</i>	문자열	템플릿과 연결된 호스트의 속성입니다.
events. <i>events-prop</i>	문자열	템플릿과 연결된 이벤트의 속성입니다.
users. <i>users-prop</i>	문자열	템플릿과 연결된 사용자의 속성입니다.
name	문자열	템플릿의 이름입니다.
domain	문자열	템플릿의 도메인입니다.
OS	문자열	운영 체제의 유형입니다.

속성(리소스 또는 리소스 유형)	유형	설명 (참조)
creationDate	정수	템플릿을 만든 날짜입니다. 날짜 형식은mm/dd/y입니다.
자식 수	정수	템플릿에서 생성된 가상 시스템의 수입니다.
mem	정수	정의된 메모리.
description	문자열	템플릿에 대한 설명입니다.
status	문자열	템플릿의 상태입니다.
cluster	문자열	템플릿과 연결된 클러스터입니다.
datacenter	문자열	템플릿과 연결된 데이터 센터입니다.
할당량	문자열	템플릿과 연결된 할당량입니다.
sortby	list	반환된 결과를 리소스 속성 중 하나로 정렬합니다.
page	정수	표시할 페이지 결과 수입니다.

예제

템플릿: **events.severity >= normal** 및 **Vms.uptime > 0**

이 예제에서는 템플릿에서 과생된 가상 시스템에서 일반 또는 심각도가 높은 이벤트가 발생하고 가상 시스템이 여전히 실행 중인 템플릿 목록을 반환합니다.

1.3.18. 사용자 검색

다음 표에는 사용자의 모든 검색 옵션이 설명되어 있습니다.

표 1.28. 사용자 검색

속성(리소스 또는 리소스 유형)	유형	설명 (참조)
VM.Vms-prop	속성 유형에 따라 다릅니다.	사용자와 연결된 가상 시스템의 속성입니다.
호스트.hosts-prop	속성 유형에 따라 다릅니다.	사용자와 연결된 호스트의 속성입니다.

속성(리소스 또는 리소스 유형)	유형	설명 (참조)
templates-prop	속성 유형에 따라 다릅니다.	사용자와 연결된 템플릿의 속성입니다.
events.events-prop	속성 유형에 따라 다릅니다.	사용자와 연결된 이벤트의 속성입니다.
name	문자열	사용자 이름.
lastname	문자열	사용자의 성.
username	문자열	사용자의 고유 이름입니다.
부서	문자열	사용자가 속한 부서입니다.
group	문자열	사용자가 속한 그룹입니다.
title	문자열	사용자의 제목입니다.
status	문자열	사용자 상태.
role	문자열	사용자의 역할.
tag	문자열	사용자가 속한 태그입니다.
pool	문자열	사용자가 속한 풀입니다.
sortby	list	반환된 결과를 리소스 속성 중 하나로 정렬합니다.
page	정수	표시할 페이지 결과 수입니다.

예제

사용자: **events.severity > normal** 및 **Vms.status = up** 또는 **Vms.status = pause**

이 예에서는 가상 머신에서 일반 심각도보다 큰 이벤트가 발생하고 가상 시스템이 여전히 실행 중이거나 사용자의 가상 머신이 일시 중지된 사용자 목록을 반환합니다.

1.3.19. 이벤트 검색

다음 테이블에서는 이벤트를 검색하는 데 사용할 수 있는 모든 검색 옵션을 설명합니다. 적절한 여러 옵션에 자동 완성이 제공됩니다.

표 1.29. 이벤트 검색

속성(리소스 또는 리소스 유형)	유형	설명 (참조)
VM. <i>Vms-prop</i>	속성 유형에 따라 다릅니다.	이벤트와 연결된 가상 시스템의 속성입니다.
호스트. <i>hosts-prop</i>	속성 유형에 따라 다릅니다.	이벤트와 연결된 호스트의 속성입니다.
<i>templates-prop</i>	속성 유형에 따라 다릅니다.	이벤트와 연결된 템플릿의 속성입니다.
users. <i>users-prop</i>	속성 유형에 따라 다릅니다.	이벤트와 관련된 사용자의 속성입니다.
cluster. <i>cluster-prop</i>	속성 유형에 따라 다릅니다.	이벤트와 연결된 클러스터의 속성입니다.
볼륨. <i>Volumes-prop</i>	속성 유형에 따라 다릅니다.	이벤트와 연결된 볼륨의 속성입니다.
type	list	이벤트 유형입니다.
심각도	list	이벤트 심각도: 경고/오류/Normal.
message	문자열	이벤트 유형에 대한 설명입니다.
time	list	이벤트가 발생한 날.
username	문자열	이벤트와 연결된 사용자 이름입니다.
event_host	문자열	이벤트와 연결된 호스트입니다.
event_vm	문자열	이벤트와 관련된 가상 머신입니다.
event_template	문자열	이벤트와 연결된 템플릿입니다.
event_storage	문자열	이벤트와 관련된 스토리지입니다.
event_datacenter	문자열	이벤트와 관련된 데이터 센터입니다.
event_volume	문자열	이벤트와 연결된 볼륨입니다.
correlation_id	정수	이벤트 식별 번호입니다.

속성(리소스 또는 리소스 유형)	유형	설명 (참조)
sortby	list	반환된 결과를 리소스 속성 중 하나로 정렬합니다.
page	정수	표시할 페이지 결과 수입니다.

예제

이벤트: **VMs.name = testdesktop** 및 **Hosts.name = gonzo.example.com**

이 예제에서는 이벤트 목록을 반환합니다. 여기서 호스트 **gonzo.example.com** 에서 실행 중 **testdesktop** 이라는 가상 머신에서 이벤트가 발생했습니다.

1.4. 북마크

1.4.1. 북마크로 쿼리 문자열 저장

북마크를 사용하여 검색 쿼리를 기억하고 다른 사용자와 공유할 수 있습니다.

절차

1. 검색바에 원하는 검색 쿼리를 입력하고 검색을 수행합니다.
2. 검색바 오른쪽에 있는 별표 **북마크** 버튼을 클릭합니다. 그러면 **New Bookmark(새 북마크)** 창이 열립니다.
3. 북마크 **의** 이름을 입력합니다.
4. 필요한 경우 **Search string** 필드를 편집합니다.
5. **OK(확인)**를 클릭합니다.

헤더 표시줄에서 **Bookmarks** 아이콘()을 클릭하여 북마크를 찾아 선택합니다.

1.4.2. 북마크 편집

북마크의 이름 및 검색 문자열을 수정할 수 있습니다.

절차

1. 헤더 표시줄에서 **Bookmarks** 아이콘()을 클릭합니다.
2. 북마크를 선택하고 **편집**을 클릭합니다.
3. Name(이름) 및 **Search(검색)** 문자열 필드를 필요에 따라 변경합니다.
4. **OK(확인)**를 클릭합니다.

1.4.3. 북마크 삭제

북마크가 더 이상 필요하지 않으면 제거합니다.

절차

1. 헤더 표시줄에서 **Bookmarks** 아이콘()을 클릭합니다.
2. 북마크를 선택하고 **Remove(제거)**를 클릭합니다.
3. **OK(확인)**를 클릭합니다.

1.5. 태그

1.5.1. 태그를 사용하여 Red Hat Virtualization과의 상호 작용 사용자 정의

Red Hat Virtualization 플랫폼을 사용자의 요구 사항에 맞게 설정한 후 태그를 사용하여 작업 방식을 사용자 지정할 수 있습니다. 태그를 사용하면 시스템 리소스를 그룹 또는 범주로 정렬할 수 있습니다. 이는 가상화 환경에 많은 객체가 존재하고 관리자가 특정 객체 집합에 집중하고자 하는 경우에 유용합니다.

이 섹션에서는 태그를 생성 및 편집하고 호스트 또는 가상 시스템에 할당하며 태그를 기준으로 사용하여 검색하는 방법을 설명합니다. 태그는 기업의 요구 사항에 맞게 구조와 일치하는 계층 구조로 정렬할 수 있습니다.

관리 포털 태그를 생성, 수정 및 제거하려면 헤더 표시줄에서 **태그** 아이콘()을 클릭합니다.

1.5.2. 태그 생성

태그를 사용하여 검색 결과를 필터링할 수 있도록 태그를 생성합니다.

절차

1. 헤더 표시줄에서 **태그** 아이콘()을 클릭합니다.
2. **Add(추가)**를 클릭하여 새 태그를 만들거나 태그를 선택하고 **New (새로 만들기)**를 클릭하여 하위 태그를 만듭니다.
3. 새 태그의 **Name (이름)**과 **Description (설명)**을 입력합니다.
4. **OK(확인)**를 클릭합니다.

1.5.3. 태그 수정

태그의 이름 및 설명을 편집할 수 있습니다.

태그 수정

1. 헤더 표시줄에서 **태그** 아이콘()을 클릭합니다.
2. 수정할 태그를 선택하고 **편집**을 클릭합니다.
3. 필요한 경우 **Name (이름)** 및 **Description (설명)** 필드를 변경합니다.
4. **OK(확인)**를 클릭합니다.

1.5.4. 태그 삭제

태그가 더 이상 필요하지 않으면 제거합니다.

절차

1. 헤더 표시줄에서 **태그** 아이콘()을 클릭합니다.
2. 삭제할 태그를 선택하고 **Remove(제거)**를 클릭합니다. 태그를 제거하면 태그의 하위 항목도 모두 제거된다는 메시지가 표시됩니다.
3. **OK(확인)**를 클릭합니다.

태그와 해당 하위 항목을 모두 제거했습니다. 태그는 연결된 모든 오브젝트에서도 제거됩니다.

1.5.5. 오브젝트에 태그 추가 및 제거

호스트, 가상 시스템 및 사용자의 태그를 할당하고 제거할 수 있습니다.

절차

1. 태그를 지정하거나 태그 취소하려는 객체를 선택합니다.
2. **More Actions(추가 작업)**()를 클릭한 다음 **Assign Tags(태그 할당)**를 클릭합니다.
3. 확인란을 선택하여 오브젝트에 태그를 할당하거나 확인란을 지워 오브젝트에서 태그를 분리합니다.
4. **OK(확인)**를 클릭합니다.

이제 지정된 태그가 선택한 객체의 사용자 지정 속성으로 추가 또는 제거됩니다.

1.5.6. 태그를 사용하여 오브젝트 검색

tag를 속성으로, 원하는 값 또는 검색 기준에 따라 검색 쿼리를 입력합니다.

지정한 기준에 태그된 오브젝트는 결과 목록에 나열됩니다.



참고

tag를 속성으로 사용하여 개체를 검색하는 경우, inequality 연산자 (**!=**) (예: **Host: VMs.tag!=server1**) 결과 목록에 태그되지 않은 오브젝트가 포함되지 않습니다.

1.5.7. 태그를 사용하여 호스트 사용자 지정

태그를 사용하여 호스트에 대한 정보를 저장할 수 있습니다. 그런 다음 태그를 기반으로 호스트를 검색할 수 있습니다. 검색에 대한 자세한 내용은 검색을 [참조하십시오](#).

절차

1. **Compute → Hosts** (컴퓨팅 호스트)를 클릭하고 호스트를 선택합니다.
2. **More Actions(추가 작업)**()를 클릭한 다음 **Assign Tags(태그 할당)**를 클릭합니다.
3. 적용 가능한 태그의 확인란을 선택합니다.
4. **OK(확인)**를 클릭합니다.

태그를 사용하여 호스트에 대한 검색 가능한 추가 정보를 추가했습니다.

2장. 리소스 관리

2.1. 서비스 품질

Red Hat Virtualization을 사용하면 환경에 있는 리소스가 액세스할 수 있는 입력 및 출력 수준, 처리 및 네트워킹 기능을 세부적으로 제어할 수 있는 서비스 품질을 정의할 수 있습니다. 서비스 품질 항목은 데이터 센터 수준에서 정의되며 클러스터 및 스토리지 도메인에서 생성된 프로필에 할당됩니다. 그런 다음 이러한 프로필은 프로필이 생성된 클러스터 및 스토리지 도메인의 개별 리소스에 할당됩니다.

2.1.1. 저장 서비스 품질

스토리지 서비스 품질은 스토리지 도메인의 가상 디스크에 대한 최대 수준의 처리량과 최대 수준의 입력 및 출력 작업을 정의합니다. 가상 디스크에 서비스 품질을 할당하면 스토리지 도메인의 성능을 미세 조정하고 한 가상 디스크와 연결된 스토리지 작업이 동일한 스토리지 도메인에 호스팅된 다른 가상 디스크에 사용 가능한 스토리지 기능에 영향을 미치지 않도록 할 수 있습니다.

2.1.1.1. 스토리지 서비스 품질 생성

절차

1. **Compute(컴퓨팅) → Data Centers** (데이터 센터)를 클릭합니다.
2. 데이터 센터의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **QoS(QoS)** 탭을 클릭합니다.
4. **Storage(스토리지)**에서 **New** (새로 생성)를 클릭합니다.
5. QoS Name(**QoS 이름**)과 서비스 품질 항목에 대한 **설명**을 입력합니다.
6. 라디오 버튼 중 하나를 클릭하여 서비스의 중단 품질을 지정합니다.
 - **없음**
 - **Total - MB/s** 필드에 허용되는 최대 총 처리량을 입력합니다.
 - **읽기/쓰기** - 왼쪽 **MB/s** 필드에 읽기 작업에 대해 허용되는 최대 처리량과 오른쪽 **MB/s** 필드에 쓰기 작업에 대해 허용되는 최대 처리량을 입력합니다.
7. 라디오 버튼 중 하나를 클릭하여 서비스의 **IOps(입력 및 출력)** 품질을 지정합니다.
 - **없음**
 - **합계 - IOps** 필드에 초당 허용되는 최대 입력 및 출력 작업 수를 입력합니다.
 - **읽기/쓰기** - 왼쪽 **IOps** 필드에 초당 허용된 입력 작업 수와 오른쪽 **IOps** 필드에서 초당 허용되는 최대 출력 작업 수를 입력합니다.
8. **OK(확인)**를 클릭합니다.

스토리지 서비스 품질을 생성하고 데이터 센터에 속한 데이터 스토리지 도메인의 해당 항목에 따라 디스크 프로필을 생성할 수 있습니다.

2.1.1.2. 스토리지 서비스 품질 제거

기존 스토리지 서비스 품질 항목을 제거합니다.

절차

1. **Compute(컴퓨팅) → Data Centers (데이터 센터)**를 클릭합니다.
2. 데이터 센터의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **QoS (QoS)** 탭을 클릭합니다.
4. **Storage (스토리지)**에서 스토리지 서비스 품질을 선택하고 **Remove(제거)**를 클릭합니다.
5. **OK(확인)**를 클릭합니다.

디스크 프로필이 해당 항목을 기반으로 하는 경우 해당 프로필의 서비스 품질이 자동으로 **[무제한]**로 설정됩니다.

2.1.2. 가상 머신 네트워크 서비스 품질

가상 시스템 네트워크 서비스 품질은 개별 가상 네트워크 인터페이스 컨트롤러의 인바운드 및 아웃바운드 트래픽을 제한하는 프로필을 생성할 수 있는 기능입니다. 이 기능을 사용하면 네트워크 리소스의 사용을 제어하는 여러 계층의 대역폭을 제한할 수 있습니다.

2.1.2.1. 가상 머신 네트워크 서비스 품질 생성

가상 시스템 네트워크 인터페이스 프로필이라고도 하는 vNIC(가상 네트워크 인터페이스 컨트롤러) 프로필에 적용할 때 네트워크 트래픽을 규제하는 서비스 항목의 가상 시스템 네트워크 품질을 만듭니다.

가상 머신 네트워크 서비스 품질 생성

1. **Compute(컴퓨팅) → Data Centers (데이터 센터)**를 클릭합니다.
2. 데이터 센터의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **QoS (QoS)** 탭을 클릭합니다.
4. **VM Network(VM 네트워크)**에서 **New (새로 생성)**를 클릭합니다.
5. 가상 시스템 네트워크 서비스 품질 항목의 **Name (이름)**을 입력합니다.
6. **인바운드 및 아웃바운드** 네트워크 트래픽에 대한 제한을 입력합니다.
7. **OK(확인)**를 클릭합니다.

가상 네트워크 인터페이스 컨트롤러에서 사용할 수 있는 가상 시스템 네트워크 서비스 품질을 생성했습니다.

2.1.2.2. New Virtual Machine Network QoS 및 Edit Virtual Machine Network QoS Windows의 설정 설명

가상 시스템 네트워크 서비스 품질 설정을 사용하면 인바운드 및 아웃바운드 트래픽에 대한 대역폭 제한을 세 가지 수준에서 구성할 수 있습니다.

표 2.1. 가상 머신 네트워크 QoS 설정

필드 이름	설명
데이터 센터	가상 시스템 네트워크 QoS 정책을 추가하는 데이터 센터입니다. 이 필드는 선택한 데이터 센터에 따라 자동으로 구성됩니다.
이름	Manager 내에서 가상 시스템 네트워크 QoS 정책을 나타내는 이름입니다.
인바운드	인바운드 트래픽에 적용할 설정입니다. 이러한 설정을 활성화 또는 비활성화하려면 Inbound 확인란을 선택하거나 지웁니다. ● 평균: 인바운드 트래픽의 평균 속도. ● 최대값: 피크 시간 동안 인바운드 트래픽의 속도. ● 버스트: 버스트 중에 인바운드 트래픽의 속도.
아웃바운드	아웃바운드 트래픽에 적용할 설정입니다. 이러한 설정을 활성화 또는 비활성화하려면 아웃바운드 확인란을 선택하거나 지웁니다. ● 평균: 아웃바운드 트래픽의 평균 속도. ● 최대값: 피크 시간 동안 아웃바운드 트래픽의 속도. ● 버스트: 버스트 중에 아웃바운드 트래픽 속도.

Average, **Peak** 또는 **Burst** 필드에서 허용되는 최대 값을 변경하려면 **engine-config** 명령을 사용하여 Max **AverageNetworkQoSValue**, **MaxPeakNetworkQoSValue** 또는 **MaxBurstNetworkQoSValue** 구성 키 값을 변경합니다. 변경 사항을 적용하려면 **ovirt-engine** 서비스를 다시 시작해야 합니다. 예를 들면 다음과 같습니다.

```
# engine-config -s MaxAverageNetworkQoSValue=2048
# systemctl restart ovirt-engine
```

2.1.2.3. 가상 머신 네트워크 서비스 품질 제거

기존 가상 시스템 네트워크 서비스 품질 항목을 제거합니다.

절차

1. **Compute(컴퓨팅) → Data Centers (데이터 센터)**를 클릭합니다.
2. 데이터 센터의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **QoS (QoS)** 탭을 클릭합니다.

4. **VM Network**(VM 네트워크)에서 서비스의 가상 시스템 네트워크 품질을 선택하고 **Remove(제거)**를 클릭합니다.
5. **OK(확인)**를 클릭합니다.

2.1.3. 호스트 네트워크 서비스 품질

호스트 네트워크 서비스 품질은 물리적 인터페이스를 통해 네트워크 트래픽 제어를 활성화하도록 호스트의 네트워크를 구성합니다. 호스트 네트워크 서비스 품질은 동일한 물리적 네트워크 인터페이스 컨트롤러에서 네트워크 리소스의 사용을 제어하여 네트워크 성능을 미세 조정할 수 있습니다. 이렇게 하면 트래픽이 많기 때문에 하나의 네트워크가 동일한 실제 네트워크 인터페이스 컨트롤러에 연결된 다른 네트워크가 더 이상 작동하지 않는 상황을 방지할 수 있습니다. 호스트 네트워크 서비스 품질을 구성하여 이러한 네트워크가 혼잡 문제 없이 동일한 실제 네트워크 인터페이스 컨트롤러에서 작동할 수 있습니다.

2.1.3.1. 호스트 네트워크 서비스 품질 생성

호스트 네트워크 품질 서비스 항목을 만듭니다.

절차

1. **Compute(컴퓨팅) → Data Centers** (데이터 센터)를 클릭합니다.
2. 데이터 센터의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **QoS (QoS)** 탭을 클릭합니다.
4. **Host Network(호스트 네트워크)**에서 **New** (새로 생성)를 클릭합니다.
5. **Qos Name** 을 입력하고 서비스 품질 항목에 대한 설명을 입력합니다.
6. 가중 공유에 대해 원하는 값, **Rate Limit [Mbps]** 및 **Committed Rate [Mbps]** 를 입력합니다.
7. **OK(확인)**를 클릭합니다.

2.1.3.2. 새 호스트 네트워크 서비스 품질 및 Edit Host Network of Service Windows의 설정 설명

호스트 네트워크 서비스 품질 설정을 사용하면 아웃바운드 트래픽에 대한 대역폭 제한을 구성할 수 있습니다.

표 2.2. 호스트 네트워크 QoS 설정

필드 이름	설명
데이터 센터	호스트 네트워크 QoS 정책을 추가하는 데이터 센터입니다. 이 필드는 선택한 데이터 센터에 따라 자동으로 구성됩니다.
QoS 이름	Manager 내에서 호스트 네트워크 QoS 정책을 나타내는 이름입니다.
설명	호스트 네트워크 QoS 정책에 대한 설명입니다.

필드 이름	설명
아웃바운드	아웃바운드 트래픽에 적용할 설정입니다. ● 가중치 공유: 동일한 논리적 링크에 연결된 다른 네트워크를 기준으로 특정 네트워크를 할당해야 하는 논리적 링크 용량의 양을 나타냅니다. 정확한 공유는 해당 링크의 모든 네트워크의 공유 합계에 따라 다릅니다. 기본적으로 1~100 범위의 숫자입니다. ● 속도 제한 [Mbps]: 네트워크에서 사용할 최대 대역폭입니다. ● 커밋 비율 [Mbps]: 네트워크에 필요한 최소 대역폭입니다. 요청된 커밋 비율은 보장되지 않으며 네트워크 인프라 및 동일한 논리적 링크의 다른 네트워크에서 요청한 커밋 비율에 따라 달라집니다.

Rate Limit [Mbps] 또는 **Committed Rate [Mbps]**(요금 제한[Mbps]) 필드에서 허용되는 최대 값을 변경하려면 **engine-config** 명령을 사용하여 **MaxAverageNetworkQoSValue** 구성 키 값을 변경합니다. 변경 사항을 적용하려면 **ovirt-engine** 서비스를 다시 시작해야 합니다. 예를 들면 다음과 같습니다.

```
# engine-config -s MaxAverageNetworkQoSValue=2048
# systemctl restart ovirt-engine
```

2.1.3.3. 호스트 네트워크 서비스 품질 제거

기존 네트워크 서비스 품질 항목을 제거합니다.

절차

1. **Compute(컴퓨팅) → Data Centers** (데이터 센터)를 클릭합니다.
2. 데이터 센터의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **QoS(QoS)** 탭을 클릭합니다.
4. **Host Network(호스트 네트워크)**에서 호스트 네트워크 품질 항목을 선택하고 **Remove(제거)**를 클릭합니다.
5. 메시지가 표시되면 **OK(확인)**를 클릭합니다.

2.1.4. CPU 서비스 품질

서비스의 CPU 품질은 가상 시스템이 실행되는 호스트에서 액세스할 수 있는 최대 처리 기능 크기를 해당 호스트에서 사용할 수 있는 총 처리 기능의 백분율로 정의합니다. 가상 머신에 CPU 서비스 품질을 할당하면 클러스터의 한 가상 시스템의 워크로드가 해당 클러스터의 다른 가상 시스템에 사용 가능한 처리 리소스에 영향을 미치지 않도록 할 수 있습니다.

2.1.4.1. CPU 서비스 품질 입력 생성

CPU 서비스 품질 항목을 만듭니다.

절차

1. **Compute(컴퓨팅) → Data Centers (데이터 센터)**를 클릭합니다.
2. 데이터 센터의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **QoS (QoS)** 탭을 클릭합니다.
4. **CPU** 아래에서 **New (새로 만들기)**를 클릭합니다.
5. QoS Name(**QoS 이름**)과 서비스 품질 항목에 대한 **설명을** 입력합니다.
6. **Limit(%) (제한(%))** 필드에 허용되는 서비스 품질을 최대 처리 기능을 입력합니다. % 기호를 포함하지 마십시오.
7. **OK(확인)**를 클릭합니다.

CPU 품질 서비스 항목을 생성하고 데이터 센터에 속한 클러스터에서 해당 항목을 기반으로 CPU 프로필을 생성할 수 있습니다.

2.1.4.2. CPU 서비스 품질 제거

기존 CPU 서비스 품질 항목을 제거합니다.

절차

1. **Compute(컴퓨팅) → Data Centers (데이터 센터)**를 클릭합니다.
2. 데이터 센터의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **QoS (QoS)** 탭을 클릭합니다.
4. **CPU**에서 **CPU quality of service** 항목을 선택하고 **Remove(제거)**를 클릭합니다.
5. **OK(확인)**를 클릭합니다.

CPU 프로필이 해당 항목을 기반으로 하는 경우 해당 프로필의 서비스 품질 항목이 자동으로 **[무제한]**로 설정됩니다.

2.2. 데이터 센터

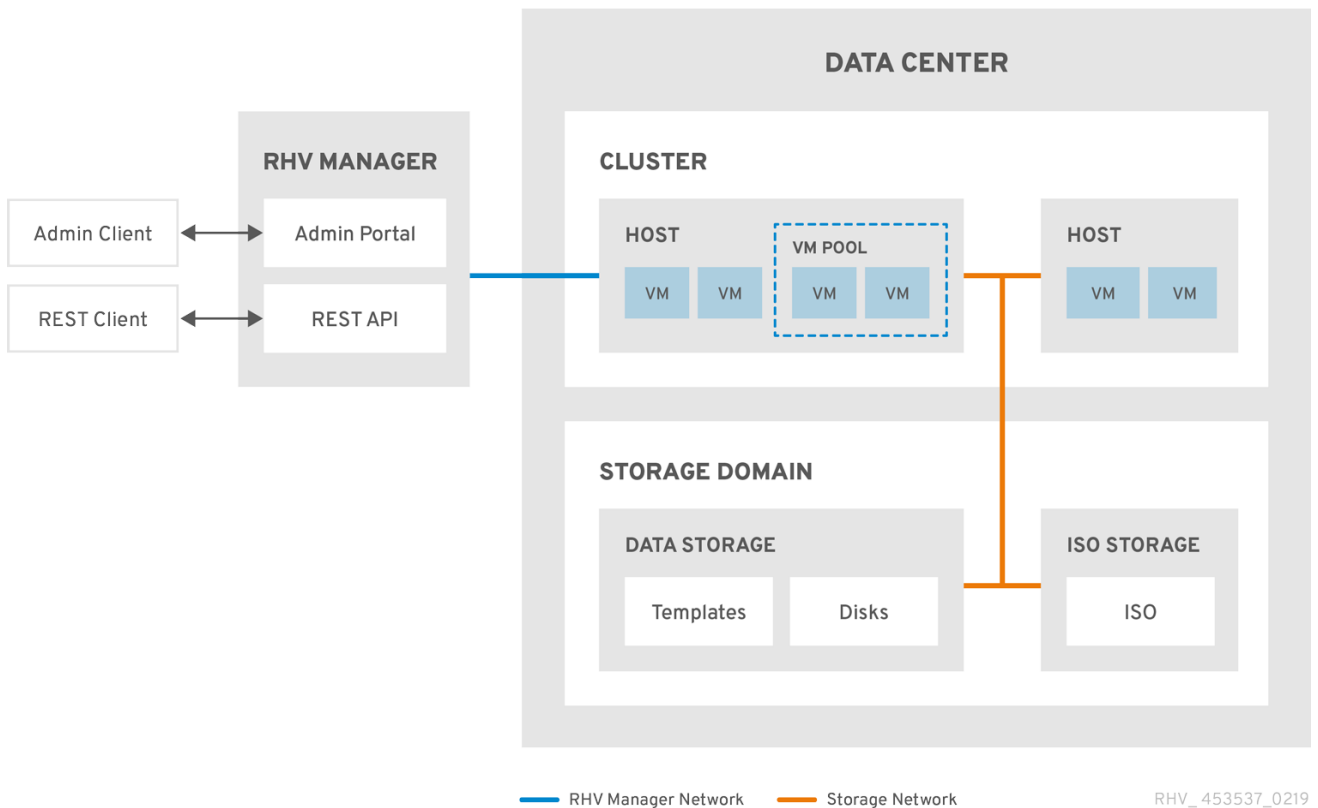
2.2.1. 데이터 센터 소개

데이터 센터는 특정 환경에서 사용되는 리소스 집합을 정의하는 논리적 엔터티입니다. 데이터 센터는 클러스터 및 호스트의 형태로 논리적 리소스, 논리적 네트워크 및 물리적 NIC 형식의 네트워크 리소스, 스토리지 도메인 형식의 스토리지 리소스로 구성된 컨테이너 리소스로 간주됩니다.

데이터 센터에는 여러 호스트가 포함될 수 있는 여러 클러스터가 포함될 수 있으며, 여러 스토리지 도메인이 연결되어 있을 수 있으며 각 호스트에서 여러 가상 시스템을 지원할 수 있습니다. Red Hat Virtualization 환경에는 여러 데이터 센터가 포함될 수 있습니다. 데이터 센터 인프라를 사용하면 이러한 센터를 별도로 유지할 수 있습니다.

모든 데이터 센터는 단일 관리 포털에서 관리됩니다.

그림 2.1. 데이터 센터



Red Hat Virtualization은 설치 중에 기본 데이터 센터를 생성합니다. 기본 데이터 센터를 구성하거나 적절한 이름의 데이터 센터를 새로 설정할 수 있습니다.

2.2.2. 스토리지 풀 관리자

SPM(스토리지 풀 관리자)은 데이터 센터의 스토리지 도메인을 관리할 수 있도록 데이터 센터의 호스트 중 하나에 지정된 역할입니다. SPM 엔터티는 데이터 센터의 모든 호스트에서 실행할 수 있습니다. Red Hat Virtualization Manager는 호스트 중 하나에 역할을 부여합니다. SPM은 표준 작업에서 호스트를 제외하지 않으며, SPM으로 실행되는 호스트에서 여전히 가상 리소스를 호스팅할 수 있습니다.

SPM 엔터티는 스토리지 도메인에서 메타데이터를 조정하여 스토리지에 대한 액세스를 제어합니다. 여기에는 가상 디스크(이미지), 스냅샷 및 템플릿 생성, 삭제 및 조작, SAN에 있는 스푸스 블록 장치에 대한 스토리지 할당이 포함됩니다. 이는 독점적인 책임입니다. 메타데이터 무결성을 보장하기 위해 데이터 센터에서는 한 번에 하나의 호스트만 SPM이 될 수 있습니다.

Red Hat Virtualization Manager를 사용하면 SPM을 항상 사용할 수 있습니다. SPM 호스트가 스토리지에 액세스하는 데 문제가 발생하면 Manager가 SPM 역할을 다른 호스트로 이동합니다. SPM이 시작되면 역할이 부여된 유일한 호스트인지 확인할 수 있으므로 스토리지 중심 리스를 확보하게 됩니다. 이 프로세스는 다소 시간이 걸릴 수 있습니다.

2.2.3. SPM 우선 순위

SPM 역할은 호스트의 사용 가능한 리소스 중 일부를 사용합니다. 호스트의 SPM 우선 순위 설정은 SPM 역할을 할당하는 호스트의 가능성을 변경합니다. SPM 우선 순위가 높은 호스트가 SPM 우선 순위가 낮은 호스트가 할당되기 전에 SPM 역할이 할당됩니다. SPM 우선 순위가 낮은 호스트의 중요한 가상 시스템은 호스트 리소스에 대해 SPM 작업을 계속할 필요가 없습니다.

Edit Host (호스트 편집) 창에서 SPM 탭에서 호스트의 **SPM** 우선 순위를 변경할 수 있습니다.

2.2.4. 데이터 센터 작업

2.2.4.1. 새 데이터 센터 생성

이 절차에서는 가상화 환경에 데이터 센터를 생성합니다. 데이터 센터에서 작동하려면 클러스터, 호스트 및 스토리지 도메인이 작동해야 합니다.



참고

호환성 버전을 설정한 후에는 버전 번호를 낮출 수 없습니다. 버전 회귀는 지원되지 않습니다.

클러스터의 MAC 풀 범위를 지정할 수 있습니다. MAC 풀 범위 설정은 더 이상 지원되지 않습니다.

절차

1. **Compute(컴퓨팅) → Data Centers** (데이터 센터)를 클릭합니다.
2. **New** (새로 만들기)를 클릭합니다.
3. 데이터 센터의 **Name** (이름) 및 **Description** (설명)을 입력합니다.
4. 드롭다운 메뉴에서 데이터 센터의 **Storage Type** (스토리지 유형), **Compatibility Version** (호환 버전), **Quota Mode** (할당량 모드)를 선택합니다.
5. **OK(확인)**를 클릭하여 데이터 센터를 생성하고 **Data Center - Guide Me**(데이터 센터 - 안내) 창을 엽니다.
6. **Guide Me** (안내) 창에는 데이터 센터에 대해 구성해야 하는 엔터티가 나열됩니다. **Configure Later**(나중에 구성) 버튼을 클릭하여 이러한 엔터티 또는 **postpone** 구성을 구성합니다 데이터 센터를 선택하고 추가 작업 ()을 클릭한 다음 **Guide Me** (안내)를 클릭하여 구성을 다시 시작할 수 있습니다.

새 데이터 센터는 클러스터, 호스트 및 스토리지 도메인이 구성 될 때까지 초기화되지 않은 상태로 유지됩니다. **Guide Me** (안내)를 사용하여 이러한 엔터티를 구성합니다.

2.2.4.2. 새 데이터 센터의 설정 설명 및 데이터 센터 편집 창

아래 표는 **New Data Center**(새 데이터 센터) 및 **Edit Data Center**(데이터 센터 편집) 창에 표시된 데이터 센터의 설정을 설명합니다. **OK(확인)**를 클릭하면 유효하지 않은 항목이 노란색으로 설명되어 변경 사항이 수락되지 않습니다. 또한 필드 프롬프트는 예상 값 또는 값 범위를 나타냅니다.

표 2.3. 데이터 센터 속성

필드	설명/액션
이름	데이터 센터의 이름입니다. 이 텍스트 필드에는 40자 제한이 있으며 대문자와 소문자, 숫자, 하이픈, 밑줄이 조합된 고유한 이름이어야 합니다.
설명	데이터 센터에 대한 설명입니다. 이 필드는 권장되지만 필수는 아닙니다.

필드	설명/액션
스토리지 유형	Shared (공유) 또는 Local storage type(로컬 스토리지 유형)을 선택합니다. 스토리지 도메인 유형(iSCSI, NFS, FC, POSIX 및 Gluster)을 동일한 데이터 센터에 추가할 수 있습니다. 그러나 로컬 및 공유 도메인은 혼합할 수 없습니다. 데이터 센터를 초기화한 후 스토리지 유형을 변경할 수 있습니다. 데이터 센터 스토리지 유형 변경을 참조하십시오.
Compatibility Version	Red Hat Virtualization의 버전. Red Hat Virtualization Manager를 업그레이드한 후에도 호스트, 클러스터 및 데이터 센터가 이전 버전에 있을 수 있습니다. 데이터 센터의 호환성 수준을 업그레이드하기 전에 모든 호스트를 업그레이드했는지 확인합니다.
쿼터 모드	쿼터는 Red Hat Virtualization과 함께 제공되는 리소스 제한 도구입니다. 다음 중 하나를 선택하십시오. ● 비활성화됨: 쿼터를 구현하지 않으려면 선택 ● 감사: 쿼터 설정을 편집하려는 경우 선택 ● 시행 됨: 쿼터를 구현하려면 선택
설명	필요한 경우 데이터 센터에 대한 일반 텍스트 주석을 추가합니다.

2.2.4.3. 데이터 센터 다시 초기화: 복구 절차

이 복구 절차에서는 데이터 센터의 **마스터** 데이터 도메인을 새 **마스터** 데이터 도메인으로 교체합니다. 데이터가 손상된 경우 **마스터** 데이터 도메인을 다시 초기화해야 합니다. 데이터 센터를 다시 초기화하면 클러스터, 호스트 및 문제 없는 스토리지 도메인을 포함하여 데이터 센터와 관련된 기타 모든 리소스를 복원할 수 있습니다.

백업 또는 내보낸 가상 머신 또는 템플릿을 새 **마스터** 데이터 도메인으로 가져올 수 있습니다.

절차

1. **Compute(컴퓨팅) → Data Centers** (데이터 센터)를 클릭하고 데이터 센터를 선택합니다.
2. 데이터 센터에 연결된 스토리지 도메인이 유지 관리 모드인지 확인합니다.
3. **More Actions(추가 작업)**()를 클릭한 다음 **Re-Initialize Data Center** (데이터 센터 다시 초기화)를 클릭합니다.

4. **Data Center Re-initialization** (데이터 센터 다시 초기화) 화면에 있는 다음 리소스 목록(승인 관리 목록)

4. **Data Center Re-Initialize** (데이터 센터 다시 초기화) 장에는 사용 가능한 보는(유지 관리 모드) 스토리지 도메인이 나열됩니다. 데이터 센터에 추가하려는 스토리지 도메인의 라디오 버튼을 클릭합니다.
5. **Approve operation(작업 승인)** 확인란을 선택합니다.
6. **OK(확인)**를 클릭합니다.

스토리지 도메인은 **마스터** 데이터 도메인으로 데이터 센터에 연결되고 활성화됩니다. 백업 또는 내보낸 가상 머신 또는 템플릿을 새 **마스터** 데이터 도메인으로 가져올 수 있습니다.

2.2.4.4. 데이터 센터 제거

데이터 센터를 제거하려면 활성 호스트가 필요합니다. 데이터 센터를 제거해도 연결된 리소스는 제거되지 않습니다.

절차

1. 데이터 센터에 연결된 스토리지 도메인이 유지 관리 모드인지 확인합니다.
2. **Compute(컴퓨팅) → Data Centers** (데이터 센터)를 클릭하고 제거할 데이터 센터를 선택합니다.
3. **Remove(제거)**를 클릭합니다.
4. **OK(확인)**를 클릭합니다.

2.2.4.5. 데이터 센터를 강제로 제거

연결된 스토리지 도메인이 손상되거나 호스트가 **Non Responsive** 가 되는 경우 데이터 센터는 무응답이 됩니다. 두 상황에서는 데이터 센터를 제거할 수 없습니다.

force Remove에는 활성 호스트가 필요하지 않습니다. 연결된 스토리지 도메인도 영구적으로 제거합니다.

데이터 센터를 강제로 제거할 수 있으려면 손상된 스토리지 도메인을 삭제해야 할 수 있습니다.

절차

1. **Compute(컴퓨팅) → Data Centers** (데이터 센터)를 클릭하고 제거할 데이터 센터를 선택합니다.
2. 추가 작업 ()을 클릭한 다음 **Force Remove** (강제 제거)를 클릭합니다.
3. **Approve operation(작업 승인)** 확인란을 선택합니다.
4. **OK**를 클릭합니다.

데이터 센터와 연결된 스토리지 도메인은 Red Hat Virtualization 환경에서 영구적으로 제거됩니다.

2.2.4.6. 데이터 센터 스토리지 유형 변경

초기화한 후 데이터 센터의 스토리지 유형을 변경할 수 있습니다. 이는 가상 시스템 또는 템플릿을 이동하는 데 사용되는 데이터 도메인에 유용합니다.

제한

- Local에 공유 - 두 개 이상의 호스트와 둘 이상의 클러스터를 포함하지 않는 데이터 센터의 경우 로컬 데이터 센터에서 지원하지 않기 때문입니다.
- Local to Shared(공유로 로컬) - 로컬 스토리지 도메인을 포함하지 않는 데이터 센터의 경우입니다.

절차

1. **Compute(컴퓨팅) → Data Centers** (데이터 센터)를 클릭하고 변경할 데이터 센터를 선택합니다.
2. **Edit(편집)**를 클릭합니다.
3. 스토리지 유형을 원하는 값으로 변경합니다.
4. **OK(확인)**를 클릭합니다.

2.2.4.7. 데이터 센터 호환성 버전 변경

Red Hat Virtualization 데이터 센터에는 호환성 버전이 있습니다. 호환성 버전은 데이터 센터를 호환하기 위한 Red Hat Virtualization 버전을 나타냅니다. 데이터 센터의 모든 클러스터에서 원하는 호환성 수준을 지원해야 합니다.

사전 요구 사항

- 데이터 센터 호환성 수준을 변경하려면 먼저 데이터 센터에서 모든 클러스터와 가상 시스템의 호환성 버전을 업데이트해야 합니다.

절차

1. 관리 포털에서 **Compute(컴퓨팅) Data Centers(데이터 센터)**를 클릭합니다.
2. 변경할 데이터 센터를 선택하고 **Edit(편집)**를 클릭합니다.
3. **Compatibility Version(호환 버전)**을 원하는 값으로 변경합니다.
4. **OK(확인)**를 클릭합니다. 데이터 센터 호환성 버전 변경 확인 대화 상자가 열립니다.
5. **OK(확인)**를 클릭하여 확인합니다.

2.2.5. 데이터 센터 및 스토리지 도메인

2.2.5.1. 데이터 센터에 기존 데이터 도메인 연결

연결 해제된 데이터 도메인은 데이터 센터에 연결할 수 있습니다. 여러 유형의 공유 스토리지 도메인 (iSCSI, NFS, FC, POSIX 및 Gluster)을 동일한 데이터 센터에 추가할 수 있습니다.

절차

1. **Compute(컴퓨팅) → Data Centers** (데이터 센터)를 클릭합니다.
2. 데이터 센터의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Storage(스토리지)** 탭을 클릭하여 데이터 센터에 이미 연결된 스토리지 도메인을 나열합니다.

4. **Attach Data** (데이터 연결)를 클릭합니다.
5. 데이터 도메인의 확인란을 선택하여 데이터 센터에 연결합니다. 여러 개의 확인란을 선택하여 여러 데이터 도메인을 연결할 수 있습니다.
6. **OK(확인)**를 클릭합니다.

데이터 도메인은 데이터 센터에 연결되며 자동으로 활성화됩니다.

2.2.5.2. 데이터 센터에 기존 ISO 도메인 연결

연결 해제된 ISO 도메인을 데이터 센터에 연결할 수 있습니다. ISO 도메인은 데이터 센터와 동일한 **스토리지 유형** 이어야 합니다.

하나의 ISO 도메인만 데이터 센터에 연결할 수 있습니다.

절차

1. **Compute(컴퓨팅) → Data Centers** (데이터 센터)를 클릭합니다.
2. 데이터 센터의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Storage(스토리지)** 탭을 클릭하여 데이터 센터에 이미 연결된 스토리지 도메인을 나열합니다.
4. **Attach ISO** (ISO 연결)를 클릭합니다.
5. 적절한 ISO 도메인의 라디오 버튼을 클릭합니다.
6. **OK(확인)**를 클릭합니다.

ISO 도메인은 데이터 센터에 연결되며 자동으로 활성화됩니다.

2.2.5.3. 데이터 센터에 기존 내보내기 도메인 연결



참고

내보내기 스토리지 도메인은 더 이상 사용되지 않습니다. 스토리지 데이터 도메인은 데이터 센터에서 연결을 해제하고 동일한 환경이나 다른 환경에서 다른 데이터 센터로 가져올 수 있습니다. 그런 다음 가져온 스토리지 도메인에서 연결된 데이터 센터로 가상 시스템, 유동 가상 디스크 및 템플릿을 업로드할 수 있습니다. 스토리지 도메인 [가져오기에 대한](#) 자세한 내용은 기존 스토리지 도메인 가져오기를 참조하십시오.

연결 해제된 내보내기 도메인을 데이터 센터에 연결할 수 있습니다. 데이터 센터에 하나의 내보내기 도메인만 연결할 수 있습니다.

절차

1. **Compute(컴퓨팅) → Data Centers** (데이터 센터)를 클릭합니다.
2. 데이터 센터의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Storage(스토리지)** 탭을 클릭하여 데이터 센터에 이미 연결된 스토리지 도메인을 나열합니다.
4. **Attach Export** (내보내기 연결)를 클릭합니다.

5. 적절한 내보내기 도메인의 라디오 버튼을 클릭합니다.

6. **OK(확인)**를 클릭합니다.

내보내기 도메인은 데이터 센터에 연결되며 자동으로 활성화됩니다.

2.2.5.4. 데이터 센터에서 스토리지 도메인 분리

데이터 센터에서 스토리지 도메인을 분리하면 데이터 센터가 해당 스토리지 도메인과 연결되지 않습니다. 스토리지 도메인은 Red Hat Virtualization 환경에서 제거되지 않으며 다른 데이터 센터에 연결할 수 있습니다.

가상 시스템 및 템플릿과 같은 데이터는 스토리지 도메인에 계속 연결되어 있습니다.



주의

마지막 마스터 스토리지 도메인을 분리할 수 있지만 권장되지는 않습니다.

마스터 스토리지 도메인을 분리한 경우 다시 초기화해야 합니다.

스토리지 도메인이 다시 초기화되면 모든 데이터가 손실되고 스토리지 도메인이 디스크를 다시 찾지 못할 수 있습니다.

절차

1. **Compute(컴퓨팅) → Data Centers (데이터 센터)**를 클릭합니다.
2. 데이터 센터의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Storage(스토리지)** 탭을 클릭하여 데이터 센터에 연결된 스토리지 도메인을 나열합니다.
4. 분리할 스토리지 도메인을 선택합니다. 스토리지 도메인이 **Active** 이면 **Maintenance(유지 관리)**를 클릭합니다.
5. **OK(확인)**를 클릭하여 유지 관리 모드를 시작합니다.
6. **Detach(분리)**를 클릭합니다.
7. **OK(확인)**를 클릭합니다.

스토리지 도메인이 세부 정보 보기에서 사라지는 데 최대 몇 분이 걸릴 수 있습니다.

2.3. 클러스터

2.3.1. 클러스터 소개

클러스터는 동일한 스토리지 도메인을 공유하고 동일한 유형의 CPU(Intel 또는 AMD)를 갖는 호스트의 논리적 그룹화입니다. 호스트에 다른 CPU 모델이 있는 경우 모든 모델에 있는 기능만 사용합니다.

시스템의 각 클러스터는 데이터 센터에 속해야 하며 시스템의 각 호스트가 클러스터에 속해야 합니다. 가상 시스템은 클러스터의 모든 호스트에 동적으로 할당되며, 가상 시스템의 클러스터 및 설정에 정의된 정

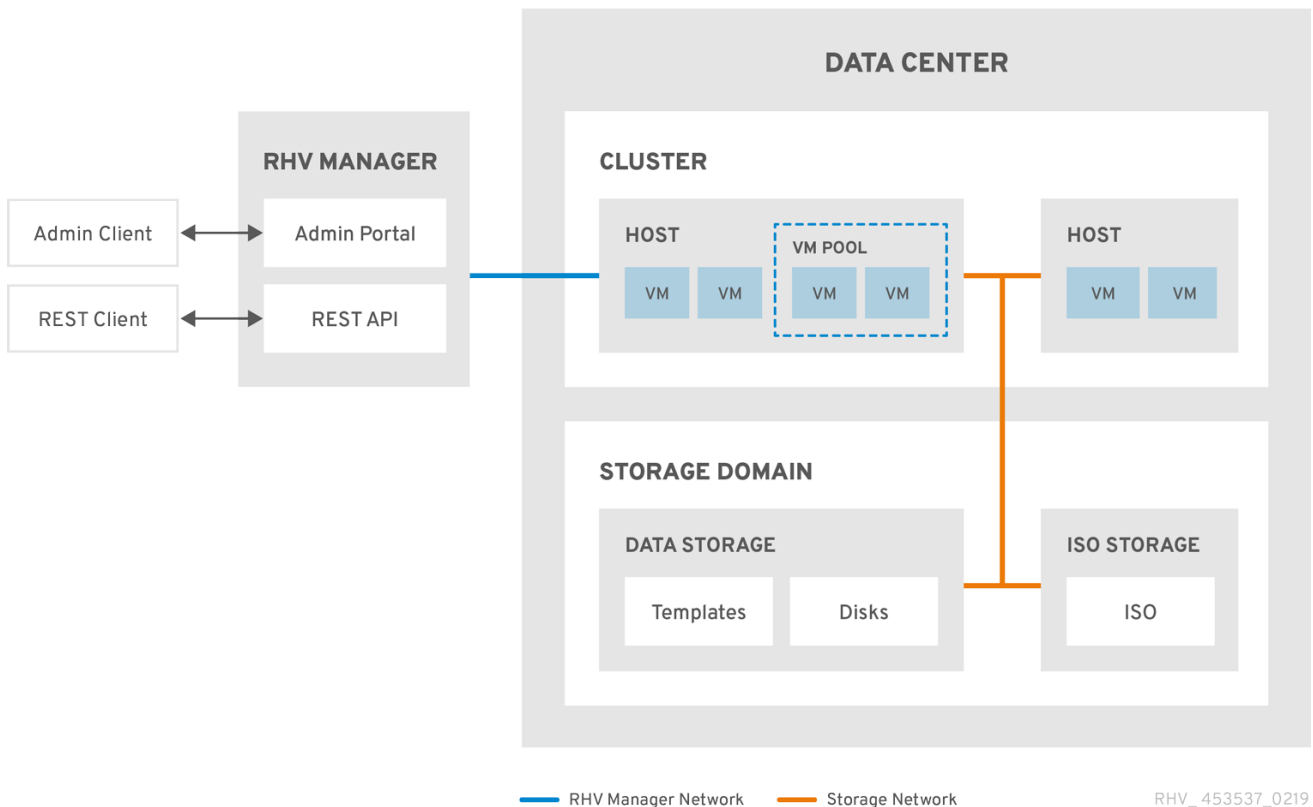
책에 따라 클러스터 간에 마이그레이션할 수 있습니다. 클러스터는 전원 및 로드 공유 정책을 정의할 수 있는 최상위 수준입니다.

클러스터에 속하는 호스트 수와 가상 시스템 수는 각각 **Host Count(호스트 개수)** 및 **VM Count(VM 개수)** 아래의 결과 목록에 표시됩니다.

클러스터는 가상 시스템 또는 Red Hat Gluster Storage 서버를 실행합니다. 이 두 가지 목적은 함께 사용할 수 없습니다. 단일 클러스터는 가상화 및 스토리지 호스트를 함께 지원할 수 없습니다.

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

그림 2.2. Cluster



2.3.2. 클러스터 작업



참고

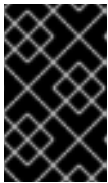
일부 클러스터 옵션은 Gluster 클러스터에 적용되지 않습니다. Red Hat Virtualization과 함께 Red Hat Gluster Storage 사용에 대한 자세한 내용은 Red Hat [Gluster Storage를 사용하여 Red Hat Virtualization](#) 구성을 참조하십시오.

2.3.2.1. 새 클러스터 생성

데이터 센터에 여러 클러스터를 포함할 수 있으며 클러스터에 여러 호스트가 포함될 수 있습니다. 클러스터의 모든 호스트에는 동일한 CPU 아키텍처가 있어야 합니다. CPU 유형을 최적화하려면 클러스터를 생성하기 전에 호스트를 생성합니다. 클러스터를 생성한 후 **Guide Me** (안내) 버튼을 사용하여 호스트를 구성할 수 있습니다.

절차

1. **Compute(컴퓨팅) Clusters(클러스터)** 를 클릭합니다.
2. **New** (새로 만들기)를 클릭합니다.
3. 드롭다운 목록에서 클러스터가 속할 **Data Center** (데이터 센터)를 선택합니다.
4. 클러스터의 **Name** (이름) 및 **Description** (설명)을 입력합니다.
5. **Management Network** (관리 네트워크) 드롭다운 목록에서 네트워크를 선택하여 관리 네트워크 역할을 할당합니다.
6. **CPU Architecture** (CPU 아키텍처)를 선택합니다.
7. **CPU Type** (CPU 유형) 의 경우 이 클러스터의 일부가 될 호스트 중 가장 오래된 CPU 프로세서 제품군을 선택합니다. CPU 유형은 가장 오래된 유형부터 최신 순으로 나열됩니다.



중요

CPU 프로세서 제품군이 **CPU 유형으로 지정한 호스트보다 오래된 호스트는 이 클러스터의 일부가 될 수 없습니다.** 자세한 내용은 [What CPU family should a RHEV3 or RHV4 cluster be set to?](#)를 참조하십시오.

8. 드롭다운 목록에서 클러스터의 **FIPS** 모드를 선택합니다.
9. 드롭다운 목록에서 클러스터의 **Compatibility Version** (호환 버전)을 선택합니다.
10. 드롭다운 목록에서 **Switch Type** (스위치 유형)을 선택합니다.
11. 클러스터에서 **Firewalld (default)** 또는 **iptables** 중 하나를 선택합니다.



참고

iptables 는 호환성 버전 4.2 또는 4.3이 있는 클러스터에서만 Red Hat Enterprise Linux 7 호스트에서만 지원됩니다. 방화벽 유형 **firewalld**가 있는 클러스터에만 Red Hat Enterprise Linux 8 호스트를 추가할 수 있습니다.

12. **Enable Virt Service**(가상 서비스 사용) 또는 **Enable Gluster Service**(Gluster 서비스 활성화) 확인란을 선택하여 클러스터가 가상 시스템 호스트 또는 **Gluster** 지원 노드로 채워질지 여부를 정의합니다.
13. 선택적으로 **Enable to set VM maintenance reason**(VM 유지 관리 이유 설정) 확인란을 선택하여 **Manager**에서 가상 시스템을 종료할 때 선택적 **reason** 필드를 활성화하여 관리자가 유지 관리에 대한 설명을 제공할 수 있습니다.
14. 선택적으로 **Enable to set Host maintenance reason**(호스트 유지 관리 이유 설정) 확인란을 선택하여 **Manager**에서 호스트를 유지 관리 모드로 전환할 때 선택적 **reason** 필드를 활성화하여 관리자가 유지 관리에 대한 설명을 제공할 수 있습니다.
15. 선택적으로 **/dev/hwrng** 소스 (외부 하드웨어 장치) 확인란을 선택하여 클러스터의 모든 호스트에서 사용할 임의 번호 생성기 장치를 지정합니다. **/dev/urandom** 소스 (Linux 제공 장치)는 기본적으로 활성화되어 있습니다.
16. **Optimization**(최적화) 탭을 클릭하여 클러스터의 임계값을 공유하는 메모리 페이지를 선택하고, 클러스터의 호스트에서 **CPU 스레드 처리** 및 **메모리 증대**를 선택적으로 활성화합니다.

17. **Migration Policy**(마이그레이션 정책) 탭을 클릭하여 클러스터의 가상 시스템 마이그레이션 정책을 정의합니다.
18. 선택 사항으로 스케줄링 정책을 구성하고, 스케줄러 최적화 설정을 구성하고, 클러스터에서 호스트에 대해 신뢰할 수 있는 서비스를 활성화하고, HA 예약을 활성화하고, 일련 번호 정책을 선택하려면 **Scheduling Policy** (스케줄링 정책) 탭을 클릭합니다.
19. **Console**(콘솔) 탭을 클릭하여 글로벌 **SPICE** 프록시(있는 경우 선택적으로 재정의)를 클릭하고 클러스터의 호스트에 대한 **SPICE** 프록시 주소를 지정합니다.
20. 펜싱 정책 탭을 클릭하여 클러스터에서 펜싱을 활성화하거나 비활성화하고 펜싱 옵션을 선택합니다.
21. **MAC Address Pool**(MAC 주소 풀) 탭을 클릭하여 클러스터의 기본 풀 이외의 MAC 주소 풀을 지정합니다. MAC 주소 풀 생성, 편집 또는 제거에 대한 자세한 내용은 [MAC Address Pools](#)를 참조하십시오.
22. **OK**(확인)를 클릭하여 클러스터를 생성하고 **Cluster - Guide Me**(클러스터 - 안내) 창을 엽니다.
23. **Guide Me**(안내) 창에는 클러스터에 대해 구성해야 하는 엔터티가 나열됩니다. **Configure Later**(나중에 구성) 버튼을 클릭하여 이러한 엔터티 또는 **postpone** 구성을 구성합니다 클러스터를 선택하고 추가 작업 (■)을 클릭한 다음 **Guide Me**(안내)를 클릭하여 구성을 다시 시작할 수 있습니다.

2.3.2.2. 설명된 일반 클러스터 설정

아래 표는 **New Cluster**(새 클러스터) 및 **Edit Cluster**(클러스터 편집) 창의 **General**(일반) 탭에 대한 설정을 설명합니다. **OK**(확인)를 클릭하면 유효하지 않은 항목이 노란색으로 설명되어 변경 사항이 수락되지 않습니다. 또한 필드 프롬프트는 예상 값 또는 값 범위를 나타냅니다.

표 2.4. 일반 클러스터 설정

필드	설명/액션
데이터 센터	클러스터를 포함할 데이터 센터입니다. 클러스터를 추가하기 전에 데이터 센터를 생성해야 합니다.
이름	클러스터의 이름입니다. 이 텍스트 필드에는 40자 제한이 있으며 대문자와 소문자, 숫자, 하이픈, 밑줄이 조합된 고유한 이름이어야 합니다.
설명/주석	클러스터 또는 추가 노트에 대한 설명입니다. 이러한 필드는 권장되지만 필수는 아닙니다.
관리 네트워크	관리 네트워크 역할이 할당될 논리적 네트워크입니다. 기본값은 ovirtmgmt 입니다. 마이그레이션 네트워크가 소스 또는 대상 호스트에 올바르게 연결되지 않은 경우에도 이 네트워크가 가상 머신을 마이그레이션하는 데 사용됩니다. 기존 클러스터에서 관리 네트워크는 세부 정보 보기의 Logical Networks (논리 네트워크) 탭에서 Manage Networks (네트워크 관리) 버튼을 사용해서만 변경할 수 있습니다.

필드	설명/액션
CPU 아키텍처	클러스터의 CPU 아키텍처입니다. 클러스터의 모든 호스트는 지정한 아키텍처를 실행해야 합니다. 선택한 CPU 아키텍처에 따라 다양한 CPU 유형을 사용할 수 있습니다. ● 정의되지 않음: 기타 모든 CPU 유형. ● x86_64: Intel 및 AMD CPU 유형의 경우. ● ppc64: IBM POWER CPU 유형의 경우.
CPU 유형	클러스터에서 가장 오래된 CPU 제품군. CPU 유형 목록은 계획 및 사전 요구 사항 가이드의 CPU 요구 사항을 참조하십시오. 중요한 중단 없이 클러스터를 생성한 후에는 이를 변경할 수 없습니다. CPU 유형을 클러스터에서 가장 오래된 CPU 모델로 설정합니다. 모든 모델에 있는 기능만 사용할 수 있습니다. Intel 및 AMD CPU 유형의 경우 나열된 CPU 모델은 가장 오래된 CPU 모델에서 최신 버전까지 논리적 순서로 되어 있습니다.
칩셋/방지 유형	이 설정은 클러스터의 CPU 아키텍처가 x86_64로 설정된 경우에만 사용할 수 있습니다. 이 설정은 칩셋 및 펌웨어 유형을 지정합니다. 옵션은 다음과 같습니다. ● 자동 삭제: 이 설정은 칩셋 및 펌웨어 유형을 자동으로 감지합니다. 자동 탐지를 선택하면 클러스터의 첫 번째 호스트에 의해 칩셋 및 펌웨어가 결정됩니다. ● BIOS를 통한 I440FX Chipset BIOS의 펌웨어 유형을 사용하여 칩셋을 I440FX에 지정합니다. ● BIOS를 사용한 Q35 Chipset UEFI가 없는 펌웨어 유형 BIOS(호환 버전 4.4가 있는 클러스터의 경우 기본)를 사용하는 Q35 칩셋을 지정합니다. ● UEFI를 사용한 Q35 Chipset은 UEFI를 사용하는 BIOS의 펌웨어 유형이 있는 Q35 칩셋을 지정합니다. (호환 버전 4.7이 있는 클러스터의 기본값) ● UEFI SecureBoot를 통한 Q35 칩셋은 부트로더의 디지털 서명을 인증하는 SecureBoot를 사용하여 UEFI의 펌웨어 유형을 Q35 칩셋을 지정합니다. 자세한 내용은 관리 가이드의 UEFI 및 Q35 칩셋을 참조하십시오.
BIOS를 사용하여 기존 VM/Templates를 I440fx에서 Q35 Chipset으로 변경	클러스터의 칩셋이 I440FX에서 Q35로 변경될 때 이 확인란을 선택하여 기존 워크로드를 변경합니다.

필드	설명/액션
FIPS 모드	클러스터에서 사용하는 FIPS 모드입니다. 클러스터의 모든 호스트는 사용자가 지정하는 FIPS 모드를 실행해야 합니다. 그렇지 않으면 작동하지 않습니다. ● 자동 삭제: 이 설정은 FIPS 모드가 활성화되었는지 여부를 자동으로 탐지합니다. 자동 탐지를 선택하면 클러스터의 첫 번째 호스트에 의해 FIPS 모드가 결정됩니다. ● 비활성화됨: 이 설정은 클러스터에서 FIPS를 비활성화합니다. ● 활성화됨: 이 설정은 클러스터에서 FIPS를 활성화합니다.
Compatibility Version	Red Hat Virtualization의 버전. 데이터 센터에 지정된 버전보다 이전에 버전을 선택할 수 없습니다.
스위치 유형	클러스터에서 사용하는 스위치 유형입니다. Linux Bridge 는 표준 Red Hat Virtualization 스위치입니다. OVS 는 Open vSwitch 네트워킹 기능을 지원합니다.
방화벽 유형	클러스터의 호스트 방화벽 유형을 firewalld (기본값) 또는 iptables 로 지정합니다. iptables 는 호환성 버전 4.2 또는 4.3 이 있는 클러스터에서만 Red Hat Enterprise Linux 7 호스트에서만 지원됩니다. 방화벽 유형 firewalld 가 있는 클러스터에만 Red Hat Enterprise Linux 8 호스트를 추가할 수 있습니다. 기존 클러스터의 방화벽 유형을 변경하는 경우 변경 사항을 적용하려면 클러스터의 모든 호스트를 다시 설치해야 합니다.
기본 네트워크 공급자	클러스터가 사용할 기본 외부 네트워크 공급자를 지정합니다. OVN(Open Virtual Network)을 선택하면 클러스터에 추가된 호스트가 OVN 공급자와 통신하도록 자동으로 구성됩니다. 기본 네트워크 공급자를 변경하는 경우 변경 사항을 적용하려면 클러스터의 모든 호스트를 다시 설치해야 합니다.
최대 로그 메모리 임계값	최대 메모리 사용량의 로깅 임계값을 백분율로 지정하거나 절대 값으로 MB로 지정합니다. 호스트의 메모리 사용량이 백분율 값을 초과하거나 호스트의 사용 가능한 메모리가 절대 값(MB)보다 낮은 경우 메시지가 기록됩니다. 기본값은 95% 입니다.
가상 서비스 활성화	이 확인란을 선택하면 이 클러스터의 호스트를 사용하여 가상 시스템을 실행합니다.

필드	설명/액션
Gluster 서비스 활성화	이 확인란을 선택하면 이 클러스터의 호스트가 Red Hat Gluster Storage Server 노드로 사용되며 가상 시스템 실행에 대해서는 사용되지 않습니다.
기존 Gluster 구성 가져오기	이 확인란은 Enable Gluster Service (Gluster 서비스 활성화) 라디오 버튼을 선택한 경우에만 사용할 수 있습니다. 이 옵션을 사용하면 기존 Gluster 지원 클러스터 및 연결된 모든 호스트를 Red Hat Virtualization Manager에 가져올 수 있습니다. 가져온 클러스터의 각 호스트에는 다음 옵션이 필요합니다. ● hostname: Gluster 호스트 서버의 IP 또는 정규화된 도메인 이름을 입력합니다. ● Host ssh 공개 키 (PEM) Red Hat Virtualization Manager는 호스트의 SSH 공개 키를 가져와 올바른 호스트에 연결하도록 합니다. ● 암호: 호스트와 통신하는 데 필요한 루트 암호를 입력합니다.
추가 임의 번호 생성기 소스	확인란을 선택하면 클러스터의 모든 호스트에 사용 가능한 추가 임의 번호 생성기 장치가 있습니다. 따라서 난수 생성기 장치에서 가상 머신으로 엔트로피의 패스트루를 사용할 수 있습니다.
Gluster Tuned 프로필	이 확인란은 Gluster Service 사용 확인란 이 선택된 경우에만 사용할 수 있습니다. 이 옵션은 호스트 성능에 도움이 되는 더러운 메모리 페이지를 더 적극적으로 쓸 수 있도록 virtual-host 튜닝 프로필을 지정합니다.

2.3.2.3. 최적화 설정 설명

메모리 고려 사항

메모리 페이지 공유를 통해 가상 머신은 다른 가상 시스템에서 사용하지 않는 메모리를 활용하여 할당된 메모리의 최대 200%를 사용할 수 있습니다. 이 프로세스는 Red Hat Virtualization 환경의 가상 머신이 모두 동시에 실행되는 것이 아니라는 가정을 기반으로 하며, 미사용 메모리를 특정 가상 시스템에 일시적으로 할당할 수 있다는 가정을 토대로 합니다.

CPU 고려 사항

- CPU 사용량이 많은 워크로드의 경우 총 프로세서 코어 수가 호스트의 코어 수보다 큰 가상 시스템을 실행할 수 있습니다. 이렇게 하면 다음을 활성화합니다.
 - 더 많은 수의 가상 시스템을 실행하여 하드웨어 요구 사항을 줄일 수 있습니다.
 - 가상 코어 수가 호스트 코어 수와 호스트 스레드 수 사이의 경우와 같이 가능하지 않은 CPU 토폴로지를 사용하여 가상 시스템을 구성할 수 있습니다.

- 최상의 성능, 특히 CPU 사용량이 많은 워크로드의 경우 호스트와 가상 시스템의 동일한 토폴로지를 사용해야 하므로 호스트와 가상 시스템에 동일한 캐시 사용량이 필요합니다. 호스트에 하이퍼스레딩이 활성화된 경우 QEMU는 호스트의 하이퍼스레드를 코어로 처리하므로 가상 시스템이 여러 스레드가 있는 단일 코어에서 실행되고 있음을 인식하지 못합니다. 이 동작은 가상 시스템의 성능에 영향을 줄 수 있습니다. 호스트 코어의 하이퍼스레드에 실제로 해당하는 가상 코어는 동일한 호스트 코어의 다른 하이퍼스레드와 단일 캐시를 공유할 수 있기 때문입니다. 가상 시스템은 이를 별도의 코어로 취급합니다.

아래 표는 New Cluster(새 클러스터) 및 Edit Cluster(클러스터 편집) 창의 Optimization(최적화) 탭에 대한 설정을 설명합니다.

표 2.5. 최적화 설정

필드	설명/액션
메모리 최적화	● none - 메모리 과다 할당 비활성화: 메모리 페이지 공유를 비활성화합니다. ● 서버 로드의 경우 - 물리적 메모리의 150%의 스케줄링을 허용합니다: 각 호스트에서 시스템 메모리의 150%로 메모리 페이지 공유 임계값을 설정합니다. ● 데스크탑 로드의 경우 - 물리적 메모리의 200% 스케줄링 허용: 각 호스트에서 임계값을 200%의 시스템 메모리로 공유하는 메모리 페이지를 설정합니다.
CPU 스레드	Count Threads As Cores (코어로 개수 스레드) 확인란을 선택하면 호스트가 호스트의 코어 수보다 큰 총 프로세서 코어 수가 있는 가상 시스템을 실행할 수 있습니다. 이 확인란을 선택하면 노출된 호스트 스레드가 가상 시스템에서 사용할 수 있는 코어로 처리됩니다. 예를 들어 코어당 2개 스레드(총 48개 스레드)가 있는 24코어 시스템은 각각 48개 코어의 가상 시스템을 실행할 수 있으며 호스트 CPU 부하를 계산하기 위한 알고리즘은 사용 가능한 코어 수의 두 배에 비해 부하를 비교합니다.

필드	설명/액션
메모리 증대	Enable Memory balloon Optimization 확인란을 선택하면 이 클러스터의 호스트에서 실행되는 가상 시스템에서 메모리 과다 할당이 활성화됩니다. 이 확인란을 선택하면 메모리 과다 할당 관리자(MoM)가 가능한 경우 모든 가상 시스템의 메모리 크기가 보장된 메모리 크기 제한으로 ballooning을 시작합니다. balloon을 실행하려면 가상 시스템에 관련 드라이버가 있는 balloon 장치가 있어야 합니다. 특히 제거되지 않는 한 각 가상 시스템에는 balloon 장치가 포함되어 있습니다. 이 클러스터의 각 호스트는 상태가 Up 으로 변경되면 balloon 정책 업데이트를 수신합니다. 필요한 경우 상태를 변경하지 않고도 호스트에서 balloon 정책을 수동으로 업데이트할 수 있습니다. 클러스터의 호스트에서 MoM 정책 업데이트를 참조하십시오. 일부 시나리오에서 증대는 KSM과 충돌할 수 있다는 점을 이해하는 것이 중요합니다. 이러한 경우 MoM은 충돌을 최소화하기 위해 balloon 크기를 조정하려고 합니다. 또한 일부 시나리오에서는 가상 시스템의 하위 최적화 성능을 유발할 수 있습니다. 관리자는 ballooning 최적화를 주의해서 사용하는 것이 좋습니다.
KSM 제어	Enable KSM(KSM 활성화) 확인란을 선택하면 MoM이 필요할 때 KSM(Kernel Same-page Merging)을 실행하고 CPU 비용을 초과하는 메모리 절약 효과를 얻을 수 있습니다.

2.3.2.4. 마이그레이션 정책 설정 설명

마이그레이션 정책은 호스트 장애 발생 시 가상 시스템을 실시간 마이그레이션하기 위한 조건을 정의합니다. 이러한 조건에는 마이그레이션 중 가상 머신 가동 중지 시간, 네트워크 대역폭, 가상 시스템의 우선 순위 지정 방법이 포함됩니다.

표 2.6. 마이그레이션 정책 설명

policy	설명
클러스터 기본값(최소 다운타임)	vdsmd.conf 의 재정의가 계속 적용됩니다. 게스트 에이전트 후크 메커니즘이 비활성화되어 있습니다.
가동 중지 시간 최소화	일반적인 상황에서 가상 시스템을 마이그레이션할 수 있는 정책입니다. 가상 시스템에는 다운타임이 발생하지 않아야 합니다. 가상 머신 마이그레이션이 오랜 시간 후에 수렴되지 않으면 마이그레이션이 중단됩니다(최대 500밀리초의 QEMU 반복에 종속됨). 게스트 에이전트 후크 메커니즘이 활성화되어 있습니다.

policy	설명
복사 후 마이그레이션	사용 시 사후 복사 마이그레이션은 소스 호스트에서 가상 시스템 vCPU 마이그레이션 일시 중단, 최소 메모리 페이지만 전송하고, 대상 호스트에서 가상 시스템 vCPU를 활성화하며, 가상 시스템이 대상 호스트에서 실행 중인 동안 나머지 메모리 페이지를 전송합니다. 사후 복사 정책은 먼저 사전 복사를 시도하여 수렴이 발생할 수 있는지 확인합니다. 오랜 시간 후에 가상 머신 마이그레이션이 수렴되지 않으면 마이그레이션이 사후 복사로 전환됩니다. 따라서 마이그레이션된 가상 시스템의 다운타임을 크게 줄이고 소스 가상 시스템의 메모리 페이지 변경 속도와 관계없이 마이그레이션을 완료할 수 있습니다. 표준 사전 복사 마이그레이션을 통해 마이그레이션할 수 없는 지속적인 사용으로 가상 시스템을 마이그레이션하는 것이 최적입니다. 이 정책의 단점은 복사 후 단계에서 누락된 메모리 부분이 호스트 간에 전송되므로 가상 시스템이 상당히 느려질 수 있다는 것입니다.  주의 사후 복사 프로세스를 완료하기 전에 네트워크 연결이 끊어지면 Manager가 실행 중인 가상 시스템을 일시 중지한 다음 종료합니다. 가상 머신 가용성이 중요하거나 마이그레이션 네트워크가 불안정한 경우에는 사후 복사 마이그레이션을 사용하지 마십시오.
필요한 경우 워크로드 일시 중단	워크로드가 많은 가상 시스템을 포함하여 대부분의 상황에서 가상 시스템을 마이그레이션할 수 있는 정책입니다. 이로 인해 가상 머신에 다른 일부 설정보다 더 중요한 다운타임이 발생할 수 있습니다. 극심한 워크로드로 인해 마이그레이션이 중단될 수 있습니다. 게스트 에이전트 후크 메커니즘이 활성화되어 있습니다.

대역폭 설정은 호스트당 나가는 마이그레이션과 들어오는 마이그레이션의 최대 대역폭을 정의합니다.

표 2.7. 설명된 대역폭

policy	설명
auto	대역폭은 데이터 센터 Host Network QoS 의 Rate Limit [Mbps] 설정에서 복사됩니다. 속도 제한이 정의되지 않은 경우 네트워크 인터페이스를 보내고 받는 최소 링크 속도로 계산됩니다. 속도 제한을 설정하지 않고 링크 속도를 사용할 수 없는 경우 호스트 전송 시 로컬 VDSM 설정에 의해 결정됩니다.
하이퍼바이저 기본값	대역폭은 호스트 전송 시 로컬 VDSM 설정을 통해 제어됩니다.
사용자 지정	사용자 정의(Mbps). 이 값은 동시 마이그레이션 수로 나뉘니다(기본값은 진행 중 및 나가는 마이그레이션을 고려하는 2). 따라서 사용자 정의 대역폭은 모든 동시 마이그레이션을 수용할 수 있을 만큼 충분히 커야 합니다. 예를 들어 사용자 지정 대역폭이 600Mbps로 정의된 경우 가상 시스템 마이그레이션의 최대 대역폭은 실제로 300Mbps입니다.

복원력 정책은 가상 시스템이 마이그레이션의 우선 순위를 지정하는 방법을 정의합니다.

표 2.8. 복원력 정책 설정

필드	설명/액션
가상 머신 마이그레이션	정의된 우선 순위에 따라 모든 가상 시스템을 마이그레이션합니다.
Migrate only Highly Available Virtual Machines	다른 호스트 과부하를 방지하기 위해고가용성 가상 시스템만 마이그레이션합니다.
가상 머신을 마이그레이션하지 않음	가상 시스템이 마이그레이션되지 않도록 합니다.

표 2.9. 추가 속성 설정

필드	설명/액션
마이그레이션 암호화 활성화	마이그레이션 중에 가상 시스템을 암호화할 수 있습니다. - 클러스터 기본값 - 암호화 - 암호화하지 않음

필드	설명/액션
병렬 마이그레이션	사용할 병렬 마이그레이션 연결의 여부와 수를 지정할 수 있습니다. ● 비활성화됨: 가상 시스템은 파형이 아닌 단일 연결을 사용하여 마이그레이션됩니다. ● Auto: 병렬 연결 수는 자동으로 결정됩니다. 이 설정은 병렬 연결을 자동으로 비활성화할 수 있습니다. ● 자동 병렬: 병렬 연결 수는 자동으로 결정됩니다. ● 사용자 정의: 원하는 병렬 연결 수를 지정할 수 있습니다. Allows you to specify the preferred number of parallel Connections.
VM 마이그레이션 연결 수	이 설정은 Custom 을 선택한 경우에만 사용할 수 있습니다. 2에서 255 사이의 사용자 정의 병렬 마이그레이션 수입니다.

2.3.2.5. 설명된 스케줄링 정책 설정

스케줄링 정책을 사용하면 사용 가능한 호스트 간에 가상 시스템의 사용 및 배포를 지정할 수 있습니다. 클러스터의 호스트 전체에서 자동 로드 밸런싱을 활성화하도록 스케줄링 정책을 정의합니다. 스케줄링 정책에 관계없이 과부하된 CPU가 있는 호스트에서 가상 시스템이 시작되지 않습니다. 기본적으로 5분 동안 80% 이상의 부하가 있는 경우 호스트의 CPU가 과부하로 간주되지만 스케줄링 정책을 사용하여 이러한 값을 변경할 수 있습니다. 자세한 내용은 [내용은 관리 가이드](#)의 스케줄링 정책을 참조하십시오.

표 2.10. 정책 탭 속성 예약

필드	설명/액션

필드	설명/액션
정책 선택	드롭다운 목록에서 정책을 선택합니다. ● none: 이미 실행 중인 가상 시스템의 호스트 간 부하 분산 또는 전원 분배를 비활성화합니다. 이는 기본값 모드입니다. 가상 시스템이 시작되면 클러스터의 모든 호스트에 메모리 및 CPU 처리 부하가 균등하게 분산됩니다. 해당 호스트가 정의된 CpuOverCommitDurationMinutes, HighUtilization 또는 MaxFreeMemoryForOver Utilized에 도달하면 호스트에 연결된 추가 가상 시스템이 시작되지 않습니다. ● evenly_distributed: 클러스터의 모든 호스트에 메모리와 CPU 처리 부하를 균등하게 분산합니다. 해당 호스트가 정의된 CpuOverCommitDurationMinutes, HighUtilization 또는 MaxFreeMemoryForOver Utilized에 도달하면 호스트에 연결된 추가 가상 시스템이 시작되지 않습니다. ● cluster_maintenance: 유지 관리 작업 중 클러스터 활동을 제한합니다. 고가용성 가상 시스템을 제외하고는 새 가상 시스템을 시작할 수 없습니다. 호스트 오류가 발생하면 고가용성 가상 시스템이 제대로 다시 시작되고 모든 가상 시스템이 마이그레이션될 수 있습니다. ● power_saving: 활용도가 낮은 호스트의 전력 소비를 줄이기 위해 사용 가능한 호스트의 하위 집합에 메모리 및 CPU 처리 부하를 분산합니다. CPU 부하가 정의된 시간 간격보다 긴 사용률 값이 낮은 호스트는 모든 가상 시스템을 다른 호스트로 마이그레이션하여 전원을 끌 수 있습니다. 호스트가 정의된 높은 사용률 값에 도달한 경우 호스트에 연결된 추가 가상 시스템이 시작되지 않습니다. ● vm_evenly_distributed: 가상 시스템 수에 따라 호스트 간에 가상 시스템을 균등하게 배포합니다. 호스트가 HighVmCount보다 더 많은 가상 시스템을 실행 중이고 MigrationThreshold 외부에 있는 가상 머신 수가 하나 이상 있는 경우 클러스터가 균형이 맞지 않는 것으로 간주됩니다.
속성	다음 속성은 선택한 정책에 따라 표시됩니다. 필요한 경우 편집합니다. ● HighVmCount: 부하 분산을 활성화하려면 호스트당 실행해야 하는 최소 가상 시스템 수를 설정합니다. 기본값은 한 호스트에서 실행 중인 10개의 가상 시스템입니다. 부하 분산은 가상 시스템을 실행하는 HighVmCount 이상의 호스트가 클러스터에 하나 이상 있는 경우에만 활성화됩니다. ● MigrationThreshold: 호스트에서 가상 시스템을 마이그레이션하기 전에 버퍼를 정의합니다. 가장 활용도가 높은 호스트와 가장 활용도가 가장 적은 호스트 간에 가상 시스템 수의 최대 포함 차이입니다. 클러스터의 모든 호스트에 마이그레이션 임계값 내에 속하는 가상 시스템 수가 있으면 클러스터가 균형을 유지합니다. 기본값은 5입니다. ● SpmVmGrace: SPM 호스트에서 예약할 가상 시스템의 슬롯 수를 정의합니다. SPM 호스트에는 다른 호스트보다 더 낮은 부하가 있으므로 이 변수는 다른 호스트와 비교하여 SPM 호스트를 실행할 수 있는 가상 시스템의 수를 정의합니다. 기본값은 5입니다. ● CpuOverCommitDurationMinutes: 스케줄링 정책이 작업을 수행하기 전에 호스트가 정의된 사용률 값 외부에서 CPU 부하를 실행할 수 있는 시간 (분 단위)을 설정합니다. 정의된 시간 간격을 스케줄링 정책을 활성화하는 CPU 부하의 일시적인 급증과 불필요한 가상 시스템 마이그레이션을 유발하지 않도록 보호합니다. 최대 2자. 기본값은 2입니다. ● HighUtilization: 백분율로 표현됩니다. 호스트가 정의된 시간 간격에 대해 높은 사용률 값을 초과하여 CPU 사용량으로 실행되는 경우 Red Hat

필드	설명/액션
	Virtualization Manager는 호스트의 CPU 로드가 최대 서비스 임계값 미만 이 될 때까지 가상 머신을 클러스터의 다른 호스트로 마이그레이션합니다. 기본값은 80입니다. ● LowUtilization: 백분율로 표현됩니다. 호스트가 정의된 시간 간격 동안 사 용률이 낮은 값보다 낮은 CPU 사용량으로 실행되는 경우 Red Hat Virtualization Manager는 가상 시스템을 클러스터의 다른 호스트로 마이그 레이션합니다. Manager는 원래 호스트 시스템의 전원을 끄고 부하 분산이 필요하거나 클러스터에 사용 가능한 호스트가 충분하지 않을 때 다시 시작 합니다. 기본값은 20 입니다. ● ScaleDown: 호스트의 점수를 지정된 양으로 나누어 HA 예약 가중치 기능 의 영향을 줄입니다. 이는 none 을 포함하여 모든 정책에 추가할 수 있는 선 택적 속성입니다. ● HostsInReserve: 실행 중인 가상 시스템이 없어도 계속 실행 중인 호스트를 지정합니다. 이는 power_saving 정책에 추가할 수 있는 선택적 속성입니다. ● EnableAutomaticHostPowerManagement: 클러스터의 모든 호스트에 대해 자동 전원 관리를 활성화합니다. 이는 power_saving 정책에 추가할 수 있는 선택적 속성입니다. 기본값은 true입니다. ● MaxFreeMemoryForOverUtilized: 호스트에 있어야 하는 최소 사용 가능 한 메모리 양을 MB로 지정합니다. 호스트에 사용 가능한 메모리가 이 양보 다 적으면 RHV Manager는 호스트가 활용도가 높은 것으로 간주합니다. 예 를 들어 이 속성을 1000 으로 설정하면 사용 가능한 메모리가 1GB 미만인 호스트가 활용도가 높습니다. 이 속성이 power_saving 및 evenly_distributed 정책과 상호 작용하는 방 법에 대한 자세한 내용은 MaxFreeMemoryForOverALLOWized 및 MinFreeMemoryForUnder Purposeized 클러스터 스케줄링 정책 속성 을 참조하십시오. power_saving 및 evenly_distributed 정책에 이 속성을 추가할 수 있습니 다. vm_evenly_distributed 정책의 속성 목록에 표시되지만 해당 정책에는 적용되지 않습니다. ● MinFreeMemoryForUnderUtilized: 호스트에서 보유해야 하는 최대 사용 가능한 메모리 양을 MB로 지정합니다. 호스트에 이 양보다 많은 메모리가 있는 경우 RHV Manager 스케줄러는 활용도가 낮은 호스트를 고려합니다. 예를 들어 이 매개변수를 10000 으로 설정하면 사용 가능한 메모리가 10GB를 초과하는 호스트가 활용되지 않습니다. 이 속성이 power_saving 및 evenly_distributed 정책과 상호 작용하는 방 법에 대한 자세한 내용은 MaxFreeMemoryForOverALLOWized 및 MinFreeMemoryForUnder Purposeized 클러스터 스케줄링 정책 속성 을 참조하십시오. power_saving 및 evenly_distributed 정책에 이 속성을 추가할 수 있습니 다. vm_evenly_distributed 정책의 속성 목록에 표시되지만 해당 정책에는 적용되지 않습니다. ● HeSparesCount: 마이그레이션 또는 종료 시 Manager 가상 머신을 시작하 기에 충분한 여유 메모리를 예약해야 하는 추가 자체 호스팅 엔진 노드 수를 설정합니다. 이렇게 하면 다른 가상 머신은 관리자 가상 시스템에 충분한 여 유 메모리를 남겨 두지 않는 경우 자체 호스팅 엔진 노드에서 시작하지 못합 니다. 이는 power_saving, vm_evenly_distributed, evenly_distributed 정 책에 추가할 수 있는 선택적 속성입니다. 기본값은 0입니다.

필드	설명/액션
스케줄러 최적화	호스트 가중치/주문에 대한 스케줄링을 최적화합니다. ● 사용률 최적화: 최적의 선택을 허용하도록 스케줄링에 가중치 모듈이 포함됩니다. ● 속도 최적화: 보류 중인 요청이 10개를 초과하는 경우 호스트 가중치를 건너뜁니다.
실행할 수 있는 서비스 활성화	OpenAttestation 서버와의 통합을 활성화합니다. 이를 활성화하기 전에 engine-config 도구를 사용하여 OpenAttestation 서버의 세부 정보를 시작합니다.중요: OpenAttestation 및 Intel Trusted Execution Technology(Intel TXT)는 더 이상 사용할 수 없습니다.
HA 예약 활성화	Manager를 활성화하여 고가용성 가상 시스템의 클러스터 용량을 모니터링합니다. Manager는 기존 호스트가 예기치 않게 실패하는 경우 마이그레이션하기 위해 고가용성으로 지정된 가상 시스템을 위해 적절한 용량이 클러스터 내에 있도록 합니다.
일련 번호 정책	클러스터의 각 새 가상 머신에 일련 번호를 할당하기 위한 정책을 구성합니다. ● 시스템 기본값: Manager 데이터베이스에서 시스템 전체 기본값을 사용합니다. 이러한 기본값을 구성하려면 엔진 구성 도구를 사용하여 DefaultSerialNumberPolicy 및 DefaultCustomSerialNumber의 값을 설정합니다. 이러한 키-값 쌍은 Manager 데이터베이스의 vdc_options 테이블에 저장됩니다. DefaultSerialNumberPolicy의 경우: ○ 기본값: HOST_ID ○ 가능한 값은 다음과 같습니다. HOST_ID, VM_ID, CUSTOM ○ 명령줄 예: engine-config --set DefaultSerialNumberPolicy=VM_ID ○ 중요: Manager를 다시 시작하여 구성을 적용합니다. ● DefaultCustomSerialNumber의 경우: ○ 기본값: 더미 일련 번호 ○ 가능한 값은 다음과 같습니다. 모든 문자열 (최대 길이 255 자) ○ 명령줄 예: engine-config --set DefaultCustomSerialNumber="My 매우 특별한 문자열 값" ○ 중요: Manager를 다시 시작하여 구성을 적용합니다. ● 호스트 ID: 각각의 새 가상 시스템의 일련 번호를 호스트의 UUID로 설정합니다. ● Vm ID: 각각의 새 가상 머신의 일련 번호를 가상 시스템의 UUID로 설정합니다. ● 사용자 정의 일련 번호: 새 가상 머신의 일련 번호를 다음 Custom Serial Number 매개변수에서 지정한 값으로 설정합니다.
사용자 정의 직렬 번호	클러스터의 새 가상 머신에 적용할 사용자 정의 일련 번호를 지정합니다.

호스트의 사용 가능한 메모리가 20% 미만으로 떨어지면 `metal .Controllers.Balloon - INFO ballooning guest:half1 from 1096400~172580` 과 같은 ballooning 명령이 `/var/log/vdsm/mom.log` 에 기록됩니다. `/var/log/vdsm/mom.log` 는 Memory Overcommit Manager 로그 파일입니다.

2.3.2.6. MaxFreeMemoryForOverUtilized 및 MinFreeMemoryForUnderUtilized 클러스터 스케줄링 정책 속성

스케줄러에는 현재 클러스터 스케줄링 정책 및 해당 매개 변수에 따라 가상 시스템을 마이그레이션하는 백그라운드 프로세스가 있습니다. 정책의 다양한 기준과 상대적 가중치에 따라 스케줄러는 호스트를 소스 호스트 또는 대상 호스트로 계속 분류하고 개별 가상 시스템을 이전에서 후자로 마이그레이션합니다.

다음 설명은 `evenly_distributed` 및 `power_saving` 클러스터 스케줄링 정책이 `MaxFreeMemoryForOverUtilized` 및 `MinFreeMemoryForUnderUtilized` 속성과 상호 작용하는 방법을 설명합니다. 두 정책 모두 CPU 및 메모리 로드를 고려하지만 CPU 로드는 `MaxFreeMemoryForOverUtilized` 및 `MinFreeMemoryForUnderUtilized` 속성과 관련이 없습니다.

`MaxFreeMemoryForOverUtilized` 및 `MinFreeMemoryForUnderUtilized` 속성을 `evenly_distributed` 정책의 일부로 정의하는 경우:

- `MaxFreeMemoryForOverUtilized` 보다 사용 가능한 메모리가 적은 호스트는 활용도가 높으며 소스 호스트가 됩니다.
- `MinFreeMemoryForUnderUtilized` 보다 사용 가능한 메모리가 더 많은 호스트는 활용도가 떨어지고 대상 호스트가 됩니다.
- `MaxFreeMemoryForOverUtilized` 가 정의되지 않은 경우 스케줄러는 메모리 로드를 기반으로 가상 머신을 마이그레이션하지 않습니다. (CPU 로드와 같은 정책의 다른 기준에 따라 가상 머신을 계속 마이그레이션합니다.)
- `MinFreeMemoryForUnderUtilized` 가 정의되지 않은 경우 스케줄러는 대상 호스트가 될 수 있는 모든 호스트를 고려합니다.

`power_saving` 정책의 일부로 `MaxFreeMemoryForOver Utilized` 및 `MinFreeMemoryForUnderUtilized` 속성을 정의하는 경우:

- `MaxFreeMemoryForOverUtilized` 보다 사용 가능한 메모리가 적은 호스트는 활용도가 높으며 소스 호스트가 됩니다.
- `MinFreeMemoryForUnderUtilized` 보다 사용 가능한 메모리가 많은 호스트는 활용도가 떨어지고 소스 호스트가 됩니다.
- `MaxFreeMemoryForOverUtilized` 보다 사용 가능한 메모리가 많은 호스트는 활용도가 높지 않고 대상 호스트가 됩니다.
- `MinFreeMemoryForUnderUtilized` 보다 사용 가능한 메모리가 적은 호스트는 충분히 활용되지 않으며 대상 호스트가 됩니다.
- 스케줄러는 활용도가 떨어지거나 활용도가 낮은 호스트로 가상 시스템을 마이그레이션하는 것을 선호합니다. 이러한 호스트가 충분하지 않은 경우 스케줄러는 가상 시스템을 활용도가 낮은 호스트로 마이그레이션할 수 있습니다. 활용도가 낮은 호스트가 이러한 용도로 필요하지 않은 경우 스케줄러는 전원을 끌 수 있습니다.
- `MaxFreeMemoryForOverUtilized` 가 정의되지 않은 경우 호스트가 과도하게 사용되지 않습니다. 따라서 활용도가 낮은 호스트만 소스 호스트이며 대상 호스트에는 클러스터의 모든 호스트가 포함됩니다.

- `MinFreeMemoryForUnderUtilized` 가 정의되지 않은 경우 활용도가 높은 호스트만 소스 호스트이며 활용도가 높은 호스트는 대상 호스트입니다.

추가 리소스

- [클러스터 스케줄링 정책 설정](#)

2.3.2.7. 설명된 클러스터 콘솔 설정

아래 표는 **New Cluster**(새 클러스터) 및 **Edit Cluster** (클러스터 편집) 창의 **Console**(콘솔) 탭에 대한 설정을 설명합니다.

표 2.11. 콘솔 설정

필드	설명/액션
클러스터용 SPICE 프록시 정의	글로벌 구성에 정의된 SPICE 프록시 재정의를 사용하려면 이 확인란을 선택합니다. 이 기능은 사용자가(예: VM 포털을 통해 연결) 하이퍼바이저가 있는 네트워크 외부에 있는 경우 유용합니다.
재정의된 SPICE 프록시 주소	SPICE 클라이언트가 가상 머신에 연결되는 프록시. 주소는 다음과 같은 형식이어야 합니다. protocol://[host]:[port]

2.3.2.8. 설명된 펜싱 정책 설정

아래 표는 **New Cluster**(새 클러스터) 및 **Edit Cluster** (클러스터 편집) 창의 **Fencing Policy**(펜싱 정책) 탭의 설정을 설명합니다.

표 2.12. 펜싱 정책 설정

필드	설명/액션
펜싱 활성화	클러스터에서 펜싱을 활성화합니다. 펜싱은 기본적으로 활성화되어 있지만 필요한 경우 비활성화할 수 있습니다. 예를 들어 임시 네트워크 문제가 발생하거나 필요한 경우 관리자는 진단 또는 유지 관리 작업이 완료될 때까지 펜싱을 비활성화할 수 있습니다. 펜싱이 비활성화된 경우 무응답 호스트에서 실행 중인 고가용성 가상 시스템은 다른 위치에서는 재시작되지 않습니다.
호스트에 스토리지에 라이브 리스가 있는 경우 펜싱을 건너뛰니다	이 확인란을 선택하면 무응답인 클러스터의 모든 호스트가 펜싱되지 않고 스토리지에 연결된 호스트는 펜싱되지 않습니다.
클러스터 연결 문제에서 펜싱 건너 뛰기	이 확인란을 선택하면 연결 문제가 발생한 클러스터의 호스트 백분율이 정의된 임계값 보다 크거나 같은 경우 펜싱이 일시적으로 비활성화됩니다. 임계값 은 드롭다운 목록에서 선택되며 사용 가능한 값은 25,50,75,100 입니다.

필드	설명/액션
gluster brick이 작동 중인 경우 펜싱을 건너뛰니다	이 옵션은 Red Hat Gluster Storage 기능이 활성화된 경우에만 사용할 수 있습니다. 이 확인란을 선택하면 brick이 실행 중이고 다른 피어에서 도달할 수 있는 경우 펜싱을 건너뛰니다. 새 페이지 2를 참조하십시오. Fencing Policies(펜싱 정책) 및 부록 A를 사용하여 고 가용성을 구성합니다. 자세한 내용은 Red Hat Hyperconverged Infrastructure를 유지 관리하는 Red Hat Gluster Storage용 펜싱 정책 입니다.
gluster 쿼럼이 충족되지 않는 경우 펜싱을 건너뛰니다.	이 옵션은 Red Hat Gluster Storage 기능이 활성화된 경우에만 사용할 수 있습니다. 이 확인란을 선택하면 brick이 실행 중이고 호스트를 종료하면 펜싱을 건너뛰면 쿼럼이 손실됩니다. 새 페이지 2를 참조하십시오. Fencing Policies(펜싱 정책) 및 부록 A를 사용하여 고 가용성을 구성합니다. 자세한 내용은 Red Hat Hyperconverged Infrastructure를 유지 관리하는 Red Hat Gluster Storage용 펜싱 정책 입니다.

2.3.2.9. 클러스터에서 호스트의 로드 및 전원 관리 정책 설정

evenly_distributed 및 power_saving 스케줄링 정책을 사용하면 허용 가능한 메모리 및 CPU 사용량 값을 지정할 수 있으며, 가상 시스템을 호스트로 또는 호스트에서 마이그레이션해야 하는 시점을 지정할 수 있습니다. vm_evenly_distributed 스케줄링 정책은 가상 시스템 수에 따라 호스트 간에 가상 시스템을 균등하게 배포합니다. 클러스터의 호스트 전체에서 자동 로드 밸런싱을 활성화하도록 스케줄링 정책을 정의합니다. 각 스케줄링 정책에 대한 자세한 내용은 클러스터 스케줄링 [정책 설정](#)을 참조하십시오.

절차

1. Compute(컴퓨팅) → Clusters (클러스터)를 클릭하고 클러스터를 선택합니다.
2. Edit(편집)를 클릭합니다.
3. Scheduling Policy(스케줄링 정책) 탭을 클릭합니다.
4. 다음 정책 중 하나를 선택합니다.
 - none
 - vm_evenly_distributed
 - a. HighVmCount 필드에서 부하 분산을 활성화하려면 하나 이상의 호스트에서 실행해야 하는 최소 가상 시스템 수를 설정합니다.
 - b. 가장 활용도가 높은 호스트의 가상 시스템 수와 MigrationThreshold(마이그레이션 Threshold) 필드에서 가장 활용도가 가장 적은 호스트의 가상 시스템 수 간의 허용 가능한 최대 차이를 정의합니다.
 - c. SpmVmGrace 필드의 SPM 호스트에 예약할 가상 시스템의 슬롯 수를 정의합니다.
 - d. 선택적으로 HeSparesCount 필드에 마이그레이션하거나 종료하는 경우 Manager 가상 머신을 시작하기에 충분한 여유 메모리를 예약하는 추가 자체 호스팅 엔진 노드 수를 입력합니다. 자세한 내용은 [Configuring Memory Slots Reserved for the self-hosted](#)

[engine](#) 에서 참조하십시오.

- **evenly_distributed**
 - a. 스케줄링 정책이 `CpuOverCommitDurationMinutes` 필드에서 작업을 수행하기 전에 호스트가 정의된 사용률 값 외부에서 CPU 부하를 실행할 수 있는 시간(분 단위)을 설정합니다.
 - b. **HighUtilization** (고유률) 필드의 다른 호스트로 마이그레이션하기 시작하는 CPU 사용률을 입력합니다.
 - c. 선택적으로 **HeSparesCount** 필드에 마이그레이션하거나 종료하는 경우 Manager 가상 머신을 시작하기에 충분한 여유 메모리를 예약하는 추가 자체 호스팅 엔진 노드 수를 입력합니다. 자세한 내용은 [Configuring Memory Slots Reserved for the self-hosted engine](#) 에서 참조하십시오.
 - **power_saving**
 - a. 스케줄링 정책이 `CpuOverCommitDurationMinutes` 필드에서 작업을 수행하기 전에 호스트가 정의된 사용률 값 외부에서 CPU 부하를 실행할 수 있는 시간(분 단위)을 설정합니다.
 - b. 호스트가 **LowUtilization** (낮음) 필드에서 활용도가 낮은 것으로 간주될 CPU 사용률을 입력합니다.
 - c. **HighUtilization** (고유률) 필드의 다른 호스트로 마이그레이션하기 시작하는 CPU 사용률을 입력합니다.
 - d. 선택적으로 **HeSparesCount** 필드에 마이그레이션하거나 종료하는 경우 Manager 가상 머신을 시작하기에 충분한 여유 메모리를 예약하는 추가 자체 호스팅 엔진 노드 수를 입력합니다. 자세한 내용은 [Configuring Memory Slots Reserved for the self-hosted engine](#) 에서 참조하십시오.
5. 클러스터의 스케줄러 최적화로 다음 중 하나를 선택합니다.
- 최적의 선택을 위해 **weight** 모듈을 스케줄링에 포함하려면 **Optimize for Utilization**(사용률 최적화)을 선택합니다.
 - 보류 중인 요청이 10개를 초과하는 경우 **Optimize for Speed**를 선택하여 호스트 가중치를 건너뛸입니다.
6. **OpenAttestation** 서버를 사용하여 호스트를 확인하고 **engine-config** 도구를 사용하여 서버의 세부 정보를 설정한 경우 **Enable Trusted Service**(신뢰할 수 있는 서비스 활성화) 확인란을 선택합니다.

OpenAttestation 및 **Intel Trusted Execution Technology(Intel TXT)**는 더 이상 사용할 수 없습니다.

1. 선택적으로 관리자가 고가용성 가상 시스템의 클러스터 용량을 모니터링할 수 있도록 **Enable HA reserved**(HA 예약 사용) 확인란을 선택합니다.
2. 클러스터의 가상 머신에 대한 직렬 번호 정책을 선택적으로 선택합니다.
 - 시스템 기본값: **엔진 구성 도구** 및 **DefaultSerialNumberPolicy** 및 **DefaultCustomSerialNumber** 키 이름을 사용하여 Manager 데이터베이스에 구성된 시스템 전체 기본값을 사용합니다. **DefaultSerialNumberPolicy**의 기본값은 호스트 ID를 사용하는 것입니다. 자세한 내용은 [관리 가이드](#)의 스케줄링 정책을 참조하십시오.
 - 호스트 ID: 각 가상 시스템의 일련 번호를 호스트의 UUID로 설정합니다.

- Vm ID: 각 가상 머신의 일련 번호를 가상 머신의 UUID로 설정합니다.
- 사용자 정의 일련 번호: 각 가상 머신의 일련 번호를 다음 Custom Serial Number 매개변수에서 지정한 값으로 설정합니다.

3. **OK(확인)**를 클릭합니다.

2.3.2.10. 클러스터의 호스트에서 MoM 정책 업데이트

Memory Overcommit Manager는 호스트에서 메모리 balloon 및 KSM 기능을 처리합니다. 클러스터의 이러한 기능에 대한 변경 사항은 다음에 호스트가 재부팅된 후 또는 유지 관리 모드로 Up 상태로 이동할 때 호스트에 전달합니다. 그러나 필요한 경우 호스트가 Up 인 동안 MoM 정책을 동기화하여 호스트에 중요한 변경 사항을 즉시 적용할 수 있습니다. 다음 절차는 각 호스트에서 개별적으로 수행해야 합니다.

절차

1. **Compute(컴퓨팅) Clusters(클러스터)** 를 클릭합니다.
2. 클러스터 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Hosts(호스트)** 탭을 클릭하고 업데이트된 MoM 정책이 필요한 호스트를 선택합니다.
4. **Sync MoM Policy(모M 정책 동기화)**를 클릭합니다.

호스트를 유지 관리 모드로 이동하고 백업할 필요 없이 호스트의 MoM 정책이 업데이트됩니다.

2.3.2.11. CPU 프로파일 생성

CPU 프로파일은 클러스터의 가상 시스템이 실행되는 호스트에서 액세스할 수 있는 최대 처리 기능을 정의합니다. 이는 해당 호스트에서 사용할 수 있는 총 처리 기능의 백분율로 표시됩니다. CPU 프로파일은 데이터 센터에 정의된 CPU 프로파일을 기반으로 생성되며 클러스터의 모든 가상 시스템에 자동으로 적용되지 않습니다. 프로파일을 적용하려면 개별 가상 시스템에 수동으로 할당해야 합니다.

이 절차에서는 클러스터가 속한 데이터 센터 아래에 하나 이상의 CPU 품질을 이미 정의했다고 가정합니다.

절차

1. **Compute(컴퓨팅) Clusters(클러스터)** 를 클릭합니다.
2. 클러스터 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **CPU Profiles(CPU 프로파일)** 탭을 클릭합니다.
4. **New (새로 만들기)**를 클릭합니다.
5. CPU 프로파일에 **Name (이름)**과 **Description (설명)**을 입력합니다.
6. **QoS (QoS)** 목록에서 CPU 프로파일에 적용할 서비스 품질을 선택합니다.
7. **OK(확인)**를 클릭합니다.

2.3.2.12. CPU 프로파일 제거

Red Hat Virtualization 환경에서 기존 CPU 프로파일을 제거합니다.

절차

1. **Compute(컴퓨팅) Clusters(클러스터)** 를 클릭합니다.
2. 클러스터 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **CPU Profiles(CPU 프로파일)** 탭을 클릭하고 제거할 **CPU 프로파일**을 선택합니다.
4. **Remove(제거)**를 클릭합니다.
5. **OK(확인)**를 클릭합니다.

CPU 프로파일은 모든 가상 시스템에 할당되면 해당 가상 시스템에 기본 CPU 프로파일은 자동으로 할당됩니다.

2.3.2.13. 기존 Red Hat Gluster Storage 클러스터 가져오기

Red Hat Gluster Storage 클러스터와 클러스터에 속하는 모든 호스트를 Red Hat Virtualization Manager 로 가져올 수 있습니다.

클러스터에 있는 모든 호스트의 IP 주소 또는 호스트 이름 및 암호와 같은 세부 정보를 제공하면 **gluster** 피어 상태 명령이 SSH를 통해 해당 호스트에서 실행된 다음 클러스터의 일부인 호스트 목록을 표시합니다. 각 호스트의 지문을 수동으로 확인하고 암호를 제공해야 합니다. 클러스터의 호스트 중 하나가 다운되거나 연결할 수 없는 경우 클러스터를 가져올 수 없습니다. 새로 가져온 호스트에 VDSM이 설치되지 않으므로 부트 스트랩 스크립트는 가져온 후 호스트에 필요한 모든 VDSM 패키지를 설치하고 재부팅합니다.

절차

1. **Compute(컴퓨팅) Clusters(클러스터)** 를 클릭합니다.
2. **New (새로 만들기)**를 클릭합니다.
3. 클러스터가 속할 **Data Center (데이터 센터)**를 선택합니다.
4. 클러스터의 **Name (이름)** 및 **Description (설명)**을 입력합니다.
5. **Enable Gluster Service(Gluster 서비스 사용)** 확인란을 선택하고 **Import existing gluster configuration (기존 Gluster 구성 가져오기)** 확인란을 선택합니다.
Import existing Gluster configuration(기존 Gluster 구성 가져오기) 필드는 **Enable Gluster Service (Gluster 서비스 활성화)**가 선택된 경우에만 표시됩니다.
6. **Hostname(호스트 이름)** 필드에 클러스터에 있는 서버의 호스트 이름 또는 IP 주소를 입력합니다.
호스트 **SSH Fingerprint**가 올바른 호스트와 연결되도록 표시됩니다. 호스트에 연결할 수 없거나 네트워크 오류가 있는 경우 **Error in fetching fingerprint**가 **Fingerprint** 필드에 표시됩니다.
7. 서버의 암호를 입력하고 **OK(확인)**를 클릭합니다.
8. **Add Hosts(호스트 추가)** 창이 열리고 클러스터의 일부인 호스트 목록이 표시됩니다.
9. 각 호스트에 대해 **Name (이름)** 및 **Root Password(루트 암호)**를 입력합니다.
10. 모든 호스트에 대해 동일한 암호를 사용하려면 **Use a Common Password (일반 암호 사용)** 확인란을 선택하여 제공된 텍스트 필드에 암호를 입력합니다.
Apply(적용)를 클릭하여 입력한 암호를 모든 호스트를 설정합니다.

지문이 유효한지 확인하고 **OK(확인)**를 클릭하여 변경 사항을 제출합니다.

부트스트랩 스크립트는 가져온 후 호스트에 필요한 모든 VDSM 패키지를 설치하고 재부팅합니다. 이제 기존 Red Hat Gluster Storage 클러스터를 Red Hat Virtualization Manager로 성공적으로 가져왔습니다.

2.3.2.14. 호스트 추가 창 설정 설명

Add Hosts(호스트 추가) 창을 사용하면 Gluster 지원 클러스터의 일부로 가져온 호스트의 세부 정보를 지정할 수 있습니다. 이 창은 New Cluster (새 클러스터) 창에서 Enable Gluster Service(Gluster 서비스 활성화) 확인란을 선택하고 필요한 호스트 세부 정보를 제공한 후에 나타납니다.

표 2.13. Gluster 호스트 설정 추가

필드	설명
공통 암호 사용	클러스터에 속하는 모든 호스트에 대해 동일한 암호를 사용하려면 이 확인란을 선택하십시오. Password (암호) 필드에 암호를 입력한 다음 Apply (적용) 버튼을 클릭하여 모든 호스트에서 암호를 설정합니다.
이름	호스트 이름을 입력합니다.
호스트 이름/IP	이 필드는 New Cluster (새 클러스터) 창에서 제공한 호스트의 정규화된 도메인 이름 또는 IP로 자동으로 채워집니다.
Root 암호	각 호스트에 다른 루트 암호를 사용하려면 이 필드에 암호를 입력합니다. 이 필드는 클러스터의 모든 호스트에 제공된 공통 암호를 재정의합니다.
지문	호스트 지문이 표시되어 올바른 호스트와 연결 중인지 확인합니다. 이 필드는 New Cluster (새 클러스터) 창에서 제공한 호스트의 지문으로 자동으로 채워집니다.

2.3.2.15. 클러스터 제거

제거하기 전에 모든 호스트를 클러스터에서 이동합니다.



참고

Blank 템플릿을 보유하고 있으므로 Default 클러스터를 제거할 수 없습니다. 그러나 Default 클러스터의 이름을 변경하고 새 데이터 센터에 추가할 수 있습니다.

절차

1. **Compute**(컴퓨팅) → **Clusters** (클러스터)를 클릭하고 클러스터를 선택합니다.
2. 클러스터에 호스트가 없는지 확인합니다.
3. **Remove**(제거)를 클릭합니다.
4. **OK**를 클릭합니다.

2.3.2.16. 메모리 최적화

호스트에서 가상 시스템 수를 늘리려면 가상 시스템에 할당한 메모리가 RAM을 초과하고 스왑 공간을 사용하는 메모리 과다 할당을 사용할 수 있습니다.

그러나 메모리 과다 할당에 잠재적인 문제가 있습니다.

- 스왑 성능 - 스왑 공간이 더 느리고 RAM보다 많은 CPU 리소스를 소비하므로 가상 시스템 성능에 영향을 미칩니다. 과도한 스왑으로 인해 CPU 스레싱이 발생할 수 있습니다.
- OOM(메모리 부족) 킬러 - 호스트에 스왑 공간이 부족하면 새 프로세스를 시작할 수 없으며 커널의 OOM 킬러 데몬이 가상 시스템 게스트와 같은 활성 프로세스 종료를 시작합니다.

이러한 단점을 극복하기 위해 다음을 수행할 수 있습니다.

- Memory Optimization 설정 및 MemoryOvercommit Manager(MoM)를 사용하여 메모리 과다 할당을 제한합니다.
- 가상 메모리에 대한 최대 잠재적인 수요를 수용하고 안전 마진을 유지할 수 있을 만큼 충분한 스왑 공간을 만듭니다.
- 메모리 증대 및 KSM(Kernel Same-page Merging)을 활성화하여 가상 메모리 크기를 줄입니다.

2.3.2.17. 메모리 최적화 및 메모리 과다 할당

Memory Optimization 설정 중 하나를 선택하여 메모리 과다 할당 양을 제한할 수 있습니다(없음 (0%), 150% 또는 200%).

각 설정은 RAM의 백분율을 나타냅니다. 예를 들어 64GB RAM이 있는 호스트를 사용하면 150%를 선택하면 총 가상 메모리에서 총 96GB의 메모리를 추가로 32GB까지 과다 할당할 수 있습니다. 호스트가 총 4GB를 사용하는 경우 나머지 92GB를 사용할 수 있습니다. 대부분의 가상 머신(시스템의 Memory Size(메모리 크기))을 가상 머신에 할당할 수 있지만 일부 할당되지 않은 상태로 두는 것을 안전한 여백으로 두는 것이 좋습니다.

가상 메모리에 대한 수요가 급증하면 MoM, 메모리 증대 및 KSM이 가상 메모리를 다시 최적화하기 전에 성능에 영향을 미칠 수 있습니다. 해당 영향을 줄이려면 실행 중인 애플리케이션 및 워크로드 유형에 적합한 제한을 선택합니다.

- 메모리 수요 증가를 유발하는 워크로드의 경우 200% 또는 150%와 같이 더 높은 백분율을 선택합니다.
- 메모리 수요 증가를 유발하는 중요한 애플리케이션 또는 워크로드의 경우 150% 또는 None (0%)과 같이 더 낮은 백분율을 선택합니다. None을 선택하면 메모리 과다 할당을 방지할 수 있지만 MoM, 메모리 증대 장치 및 KSM이 가상 메모리를 계속 최적화할 수 있습니다.



중요

항상 구성을 프로덕션에 배포하기 전에 광범위한 조건 하에서 스트레스 테스트를 통해 메모리 최적화 설정을 테스트합니다.

Memory Optimization(메모리 최적화) 설정을 구성하려면 New Cluster(새 클러스터) 또는 Edit Cluster(클러스터 편집) 창에서 Optimization(최적화) 탭을 클릭합니다. [클러스터 최적화 설정 설명](#)을 참조하십시오.

추가 코멘트:

- [Host Statistics\(호스트 통계\) 뷰](#)는 오버 커밋 비율의 크기를 조정하는 데 유용한 기록 정보가 표시됩니다.

- KSM에서 달성한 메모리 최적화 양과 메모리 증대(Memory ballooning) 변경이 지속적으로 이루어지기 때문에 실제 메모리는 실시간으로 결정할 수 없습니다.
- 가상 머신이 가상 메모리 제한에 도달하면 새 앱을 시작할 수 없습니다.
- 호스트에서 실행할 가상 시스템 수를 계획하는 경우 최대 가상 메모리(물리 메모리 크기 및 메모리 최적화 설정)를 시작점으로 사용합니다. 메모리 증대 및 KSM과 같은 메모리 최적화에 의해 달성되는 더 작은 가상 메모리를 고려하지 마십시오.

2.3.2.18. 스왑 공간 및 메모리 과다 할당

Red Hat은 [스왑 공간을 구성하기 위한 권장 사항을](#) 제공합니다.

이러한 권장 사항을 적용하는 경우 지침에 따라 스왑 공간의 크기를 최악의 경우 "마지막 작업 메모리"로 조정합니다. 실제 메모리 크기 및 메모리 최적화 설정을 총 가상 메모리 크기를 추정하기 위해 기준으로 사용합니다. MoM, 메모리 증대 및 KSM에 의해 최적화된 가상 메모리 크기 감소를 제외합니다.



중요

OOM 조건을 방지하려면 스왑 공간을 활용하여 최악의 시나리오를 처리할 수 있으며 여전히 안전한 여백을 사용할 수 있습니다. 프로덕션에 배포하기 전에 항상 광범위한 조건 하에서 구성을 과부하 테스트를 수행하십시오.

2.3.2.19. 메모리 과다 할당 관리자 (MoM)

MM (Memory Overcommit Manager)은 다음 두 가지를 수행합니다.

- 이전 섹션에 설명된 대로 Memory Optimization(메모리 최적화) 설정을 클러스터의 호스트에 적용하여 메모리 과다 할당을 제한합니다.
- 다음 섹션에 설명된 대로 *메모리 ballooning* 및 KSM 을 관리하여 메모리를 최적화합니다.

MoM을 활성화 또는 비활성화할 필요가 없습니다.

호스트의 사용 가능한 메모리가 20% 미만으로 떨어지면 ballooning 명령(예: ballooning). **Controllers.Ballooning - INFO ballooning guest:half1 from 1096400~172580** 은 /var/log/vdsm/mom.log 에 기록되며 Memory Overcommit Manager 로그 파일입니다.

2.3.2.20. 메모리 증대

가상 머신은 가상 메모리에 할당한 전체 양의 가상 메모리로 시작합니다. 가상 메모리 사용량이 RAM을 초과하므로 호스트는 스왑 공간에 더 많이 의존합니다. *메모리 증대* 기능을 사용하면 가상 머신에서 사용하지 않는 메모리 부분을 포기할 수 있습니다. 사용 가능한 메모리는 호스트의 다른 프로세스 및 가상 시스템에서 재사용할 수 있습니다. 메모리 점유율이 감소하면 스왑 가능성이 줄어들고 성능이 향상됩니다.

메모리 증대 장치 및 드라이버를 제공하는 *virtio-balloon* 패키지는 로드 가능한 커널 모듈(LKM)으로 제공됩니다. 기본적으로 자동으로 로드되도록 구성됩니다. 거부 또는 언로드에 모듈을 추가하면 풍선이 비활성화됩니다.

메모리 증대 장치는 서로 직접 조정되지 않습니다. 호스트의 MOM(메모리 과다 할당 관리자) 프로세스를 사용하여 각 가상 시스템의 요구 사항을 지속적으로 모니터링하고 balloon 장치에 가상 메모리를 늘리거나 줄이도록 지시합니다.

성능 고려 사항:

- Red Hat은 지속적인 고성능과 짧은 대기 시간이 필요한 워크로드에 대해 메모리 증대 및 과다 할당을 권장하지 않습니다. [고성능 가상 머신, 템플릿 및 풀](#) 구성을 참조하십시오.
- 가상 시스템 밀도(ecographic)를 늘릴 때 메모리 증대를 사용하는 것이 성능보다 더 중요합니다.
- 메모리 증대는 CPU 사용률에 큰 영향을 미치지 않습니다. (KSM은 일부 CPU 리소스를 사용하지만 사용량은 지속적으로 부족합니다.)

메모리 증대를 사용하려면 New Cluster(새 클러스터) 또는 Edit Cluster(클러스터 편집) 창에서 Optimization(최적화) 탭을 클릭합니다. 그런 다음 Enable Memory balloon Optimization(메모리 balloon 최적화 활성화) 확인란을 선택합니다. 이 설정을 사용하면 이 클러스터의 호스트에서 실행되는 가상 머신의 메모리 과다 할당이 가능합니다. 이 확인란을 선택하면 MoM은 모든 가상 시스템의 메모리 크기 보장된 제한과 함께 가능한 경우 ballooning을 시작합니다. [클러스터 최적화 설정 설명](#)을 참조하십시오.

이 클러스터의 각 호스트는 상태가 Up으로 변경되면 balloon 정책 업데이트를 수신합니다. 필요한 경우 상태를 변경하지 않고도 호스트에서 balloon 정책을 수동으로 업데이트할 수 있습니다. [클러스터의 호스트에서 MoM 정책 업데이트를 참조하십시오.](#)

2.3.2.21. KSM(Kernel Same-page Merging)

가상 시스템이 실행되면 공통 라이브러리 및 사용량이 많은 데이터와 같은 항목에 대한 중복 메모리 페이지를 생성하는 경우가 많습니다. 또한 유사한 게스트 운영 체제 및 애플리케이션을 실행하는 가상 머신은 가상 메모리에서 중복 메모리 페이지를 생성합니다.

활성화된 경우 KSM(Kernel Same-page Merging)은 호스트에서 가상 메모리를 검사하고 중복 메모리 페이지를 제거하고 여러 애플리케이션과 가상 시스템에서 나머지 메모리 페이지를 공유합니다. 이러한 공유 메모리 페이지는 COW(Copy-On-Write)로 표시됩니다. 가상 시스템이 페이지에 변경 사항을 작성해야 하는 경우 해당 복사본에 수정 사항을 작성하기 전에 먼저 복사본을 만듭니다.

KSM이 활성화되는 동안 MoM은 KSM을 관리합니다. KSM을 수동으로 구성하거나 제어할 필요가 없습니다.

KSM은 두 가지 방식으로 가상 메모리 성능을 향상시킵니다. 공유 메모리 페이지가 더 자주 사용되므로 호스트는 캐시 또는 주 메모리에 저장할 가능성이 높기 때문에 메모리 액세스 속도가 향상됩니다. 또한 메모리 과다 할당을 통해 KSM은 가상 메모리 공간을 줄여 스왑을 줄이고 성능을 개선할 수 있습니다.

KSM은 메모리 증대기보다 더 많은 CPU 리소스를 사용합니다. CPU KSM 소비 양은 계속 압박을 받고 있습니다. 호스트에서 동일한 가상 머신 및 애플리케이션을 실행하면 KSM이 다른 가상 시스템보다 더 많은 메모리 페이지를 병합할 수 있습니다. 대부분 다른 가상 시스템 및 애플리케이션을 실행하는 경우 KSM 사용의 CPU 비용이 그 이점을 상쇄할 수 있습니다.

성능 고려 사항:

- KSM 데몬이 많은 메모리를 병합한 후 커널 메모리 계정 통계가 결국 서로 모순될 수 있습니다. 시스템에 사용 가능한 메모리가 많은 경우 KSM을 비활성화하여 성능을 향상시킬 수 있습니다.
- Red Hat은 지속적인 고성능과 짧은 대기 시간이 필요한 워크로드에 KSM 및 과다 할당을 권장하지 않습니다. [고성능 가상 머신, 템플릿 및 풀](#) 구성을 참조하십시오.
- KSM을 성능보다 더 중요시하는 가상 머신 밀도(보안)를 늘리는 경우 KSM을 사용합니다.

KSM을 활성화하려면 New Cluster(새 클러스터) 또는 Edit Cluster(클러스터 편집) 창에서 Optimization(최적화) 탭을 클릭합니다. 그런 다음 Enable KSM 확인란을 선택합니다. 이 설정을 사용하면 필요한 경우 MoM이 KSM을 실행할 수 있으며 CPU 비용보다 더 큰 메모리를 절약할 수 있습니다. [클러스터 최적화 설정 설명](#)을 참조하십시오.

2.3.2.22. UEFI 및 Q35 칩셋

새 가상 시스템의 기본 칩셋인 Intel Q35 칩셋에는 레거시 BIOS를 대체하는 UEFI(Unified Extensible Firmware Interface) 지원이 포함되어 있습니다.

또는 UEFI를 지원하지 않는 레거시 Intel i440fx 칩셋을 사용하도록 가상 시스템 또는 클러스터를 구성할 수도 있습니다.

UEFI는 다음을 포함하여 기존 BIOS에 비해 몇 가지 이점을 제공합니다.

- 최신 부트 로더
- SecureBoot: 부트 로더의 디지털 서명을 인증
- 2TB보다 큰 디스크를 활성화하는 GUID 파티션 테이블 (GPT)

가상 머신에서 UEFI를 사용하려면 4.4 이상의 호환성을 위해 가상 머신의 클러스터를 구성해야 합니다. 그런 다음 기존 가상 시스템에 대해 UEFI를 설정하거나 클러스터의 새 가상 시스템의 기본 BIOS 유형으로 설정할 수 있습니다. 다음 옵션을 사용할 수 있습니다.

표 2.14. 사용 가능한 BIOS 유형

BIOS 유형	설명
Legacy BIOS를 사용한 Q35set	UEFI가 없는 레거시 BIOS (호환 버전 4.4가 있는 클러스터의 경우 기본값)
UEFI BIOS를 사용한 Q35æset	UEFI 사용 BIOS
SecureBoot를 사용한 Q35æset	UEFI SecureBoot와 함께, 부트 로더의 디지털 서명을 인증
레거시	레거시 BIOS가 있는 i440fx 칩셋

운영 체제를 설치하기 전에 BIOS 유형 설정

운영 체제를 설치하기 전에 Q35 칩셋 및 UEFI를 사용하도록 가상 머신을 구성할 수 있습니다. 운영 체제를 설치한 후에는 가상 시스템을 레거시 BIOS에서 UEFI로 변환하는 것은 지원되지 않습니다.

2.3.2.23. Q35æset 및 UEFI를 사용하도록 클러스터 구성

클러스터를 Red Hat Virtualization 4.4로 업그레이드한 후 클러스터의 모든 가상 머신은 4.4 버전의 VDSM을 실행합니다. 해당 클러스터에서 생성한 새 가상 시스템의 기본 BIOS 유형을 결정하는 클러스터의 기본 BIOS 유형을 구성할 수 있습니다. 필요한 경우 가상 머신을 생성할 때 다른 BIOS 유형을 지정하여 클러스터의 기본 BIOS 유형을 재정의할 수 있습니다.

절차

1. VM 포털 또는 관리 포털에서 **Compute → Clusters** (클러스터) 를 클릭합니다.
2. 클러스터를 선택하고 **Edit(편집)** 를 클릭합니다.
3. **General(일반)** 을 클릭합니다.

4. BIOS Type(OSOS 유형) 드롭다운 메뉴를 클릭하고 다음 중 하나를 선택하여 클러스터에서 새 가상 머신의 기본 BIOS 유형을 정의합니다.
 - 레저시
 - Legacy BIOS를 사용한 Q35set
 - UEFI BIOS를 사용한 Q35æset
 - SecureBoot를 사용한 Q35æset
5. Compatibility Version(호환 버전) 드롭다운 메뉴에서 4.4 를 선택합니다. 관리자는 실행 중인 모든 호스트가 4.4와 호환되는지 확인하고, 해당 호스트가 있는 경우 관리자는 4.4 기능을 사용합니다.
6. 클러스터의 기존 가상 시스템이 새 BIOS 유형을 사용해야 하는 경우 이를 수행하도록 구성합니다. BIOS 유형 클러스터 기본값 을 사용하도록 구성된 클러스터의 새 가상 머신은 이제 선택한 BIOS 유형을 사용합니다. 자세한 내용은 [Q35æset 및 UEFI를 사용하도록 가상 머신 구성](#)을 참조하십시오.



참고

운영 체제를 설치하기 전에만 BIOS 유형을 변경할 수 있으므로 BIOS 유형 클러스터 기본값 을 사용하도록 구성된 기존 가상 머신에 대해 BIOS 유형을 이전 기본 클러스터 BIOS 유형으로 변경합니다. 그렇지 않으면 가상 시스템이 부팅되지 않을 수 있습니다. 또는 가상 시스템의 운영 체제를 다시 설치할 수 있습니다.

2.3.2.24. Q35æset 및 UEFI를 사용하도록 가상 머신 구성

운영 체제를 설치하기 전에 Q35 칩셋 및 UEFI를 사용하도록 가상 머신을 구성할 수 있습니다. 가상 시스템을 레저시 BIOS에서 UEFI로 변환하거나 UEFI에서 레저시 BIOS로 변환하면 가상 시스템이 부팅되지 않을 수 있습니다. 기존 가상 머신의 BIOS 유형을 변경하는 경우 운영 체제를 다시 설치합니다.



주의

가상 시스템의 BIOS 유형이 클러스터 기본값으로 설정된 경우 클러스터의 BIOS 유형을 변경하면 가상 시스템의 BIOS 유형이 변경됩니다. 가상 시스템에 운영 체제가 설치되어 있는 경우 클러스터 BIOS 유형을 변경하면 가상 시스템이 부팅되지 않을 수 있습니다.

절차

Q35 칩셋 및 UEFI를 사용하도록 가상 머신을 구성하려면 다음을 수행합니다.

1. VM 포털 또는 관리 포털에서 Compute(컴퓨팅) Virtual Machines(가상 시스템) 를 클릭합니다.
2. 가상 시스템을 선택하고 Edit(편집) 를 클릭합니다.
3. General(일반) 탭에서 Show Advanced Options(고급 옵션 표시)를 클릭합니다.
4. System → Advanced Parameters (시스템 고급 매개 변수)를 클릭합니다.

5. BIOS 유형 드롭다운 메뉴에서 다음 중 하나를 선택합니다.
 - 클러스터 기본값
 - Legacy BIOS를 사용한 Q35set
 - UEFI BIOS를 사용한 Q35æset
 - SecureBoot를 사용한 Q35æset
6. OK(확인)를 클릭합니다.
7. 가상 시스템 포털 또는 관리 포털에서 가상 시스템의 전원을 끕니다. 다음에 가상 시스템을 시작하면 선택한 새 BIOS 유형으로 실행됩니다.

2.3.2.25. 클러스터 호환성 버전 변경

Red Hat Virtualization 클러스터에는 호환성 버전이 있습니다. 클러스터 호환성 버전은 클러스터의 모든 호스트에서 지원하는 Red Hat Virtualization의 기능을 나타냅니다. 클러스터 호환성은 클러스터에서 가장 적게 사용할 수 있는 호스트 운영 체제 버전에 따라 설정됩니다.

사전 요구 사항

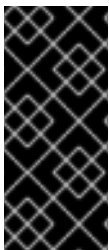
- 클러스터 호환성 수준을 변경하려면 먼저 클러스터의 모든 호스트를 원하는 호환성 수준을 지원하는 수준으로 업데이트해야 합니다. 호스트 옆에 업데이트를 사용할 수 있음을 나타내는 아이콘이 있는지 확인합니다.

제한

- VirtIO NIC는 클러스터 호환성 수준을 4.6으로 업그레이드한 후 다른 장치로 열거됩니다. 따라서 NIC를 재구성해야 할 수 있습니다. Red Hat은 가상 머신에서 클러스터 호환성 수준을 4.6으로 설정하고 네트워크 연결을 확인하여 클러스터를 업그레이드하기 전에 가상 머신을 테스트하는 것이 좋습니다. 가상 시스템의 네트워크 연결이 실패하면 클러스터를 업그레이드하기 전에 현재 에뮬레이트된 시스템과 일치하는 사용자 지정 에뮬레이트 시스템(예: 4.5 호환성 버전의 pc-q35-rhel8.3.0)을 사용하여 가상 머신을 구성합니다.

절차

1. 관리 포털에서 Compute(컴퓨팅) Clusters(클러스터) 를 클릭합니다.
2. 변경할 클러스터를 선택하고 **Edit(편집)**를 클릭합니다.
3. **General(일반)** 탭에서 **Compatibility Version (호환 버전)**을 원하는 값으로 변경합니다.
4. **OK(확인)**를 클릭합니다. 클러스터 호환성 버전 변경 확인 대화 상자가 열립니다.
5. **OK(확인)**를 클릭하여 확인합니다.



중요

일부 가상 시스템 및 템플릿이 잘못 구성되었다고 경고하는 오류 메시지가 표시될 수 있습니다. 이 오류를 수정하려면 각 가상 시스템을 수동으로 편집합니다. **Edit Virtual Machine(가상 시스템 편집)** 창에서 수정할 항목을 보여주는 추가 검증 및 경고를 제공합니다. 문제가 자동으로 수정되고 가상 시스템의 구성을 다시 저장하면 되는 경우가 있습니다. 각 가상 시스템을 편집한 후 클러스터 호환성 버전을 변경할 수 있습니다.

클러스터의 호환성 버전을 업데이트한 후 게스트 운영 체제 대신 관리 포털에서 재부팅하거나 REST API를 사용하여 실행 중인 모든 가상 시스템의 클러스터 호환성 버전을 업데이트해야 합니다. 재부팅해야 하는 가상 머신은 보류 중인 변경 사항 아이콘()으로 표시됩니다. 미리 보기 중인 가상 머신 스냅샷의 클러스터 호환성 버전을 변경할 수 없습니다. 먼저 프리뷰를 커밋하거나 실행 취소해야 합니다.

자체 호스팅 엔진 환경에서는 Manager 가상 시스템을 다시 시작할 필요가 없습니다.

편리한 시간에 가상 시스템을 재부팅할 수 있지만 가상 시스템이 최신 구성을 사용하도록 즉시 재부팅하는 것이 좋습니다. 업데이트되지 않은 가상 시스템은 이전 구성으로 실행되며 재부팅하기 전에 가상 시스템을 다른 변경하면 새 구성을 덮어쓸 수 있습니다.

데이터 센터에서 모든 클러스터 및 가상 시스템의 호환성 버전을 업데이트한 후에는 데이터 센터 자체의 호환성 버전을 변경할 수 있습니다.

2.4. 논리적 네트워크

2.4.1. 논리적 네트워크 작업

2.4.1.1. 네트워킹 작업 수행

Network → Networks 는 사용자가 논리적 네트워크 관련 작업을 수행하고 각 네트워크의 속성 또는 다른 리소스와의 연결을 기반으로 논리적 네트워크를 검색할 수 있는 중앙 위치를 제공합니다. New (새로 생성), Edit (편집), Remove (제거) 버튼을 사용하면 데이터 센터 내의 논리적 네트워크를 생성, 변경, 변경 및 삭제할 수 있습니다.

각 네트워크 이름을 클릭하고 세부 정보 보기에서 탭을 사용하여 다음을 포함한 기능을 수행합니다.

- 클러스터 및 호스트에 네트워크 연결 또는 분리
- 가상 머신 및 템플릿에서 네트워크 인터페이스 제거
- 사용자가 네트워크에 액세스 및 관리할 수 있는 권한 추가 및 제거

이러한 기능은 각 개별 리소스를 통해서도 액세스할 수 있습니다.



주의

이와 같이 호스트가 실행 중이면 호스트에 연결할 수 없는 위험이 있는 경우 데이터 센터 또는 클러스터의 네트워킹을 변경하지 마십시오.

중요

Red Hat Virtualization 노드를 사용하여 서비스를 제공하려는 경우 Red Hat Virtualization 환경 운영을 중지하면 서비스가 중지됩니다.

이는 모든 서비스에 적용되지만 Red Hat Virtualization에서 다음을 실행할 위험이 특히 인 지해야 합니다.

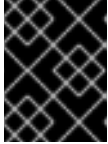
- 디렉터리 서비스
- DNS
- 스토리지

2.4.1.2. 데이터 센터 또는 클러스터에서 새 논리적 네트워크 생성

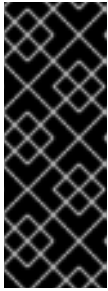
논리적 네트워크를 생성하고 데이터 센터 또는 데이터 센터의 클러스터에서 사용을 정의합니다.

절차

1. **Compute**(컴퓨팅) → **Data Centers** (데이터 센터) 또는 **Compute Clusters**(컴퓨팅 클러스터)를 클릭합니다.
2. 데이터 센터 또는 클러스터 이름을 클릭합니다. **Details**(세부 정보) 보기가 열립니다.
3. **Logical Networks**(논리적 네트워크) 탭을 클릭합니다.
4. **New Logical Network** 창을 엽니다.
 - 데이터 센터 세부 정보 보기에서 **New** (새로 생성)를 클릭합니다.
 - 클러스터 세부 정보 보기에서 **네트워크 추가**를 클릭합니다.
5. 논리적 네트워크에 **Name** (이름), **Description** (설명) 및 **Comment** (주석)를 입력합니다.
6. 선택 사항: **VLAN 태그 지정** 활성화.
7. 선택 사항: **VM 네트워크 비활성화**.
8. 선택 사항: **Create on external provider** (외부 공급업체에 생성) 확인란을 선택합니다. 이렇게 하면 네트워크 레이블과 VM 네트워크가 비활성화됩니다. 자세한 내용은 [외부 공급자](#)를 참조하십시오.
 - a. **External Provider** (외부 프로바이더)를 선택합니다. **External Provider**(외부 프로바이더) 목록에는 읽기 전용 모드에 있는 외부 프로바이더가 포함되지 않습니다.
 - b. 격리된 내부 네트워크를 생성하려면 외부 프로바이더 목록에서 **ovirt-provider-ovn** 을 선택하고 물리적 네트워크에 연결을 지웁니다.
9. 새 레이블을 입력하거나 **Network Label** (네트워크 레이블) 텍스트 필드에 논리적 네트워크의 기존 레이블을 선택합니다.
10. **MTU**의 경우 **Default(1500)**를 선택하거나 **Custom** (사용자 지정) 을 선택하고 사용자 지정 값을 지정합니다.

**중요**

외부 프로바이더에서 네트워크를 생성한 후에는 네트워크의 MTU 설정을 변경할 수 없습니다.

**중요**

네트워크의 MTU 설정을 변경하는 경우 이 변경 사항을 네트워크에서 실행 중인 가상 머신으로 전파해야 합니다. MTU 설정을 적용하거나 가상 시스템을 다시 시작해야 하는 모든 가상 시스템의 vNIC의 핫플러그 및 재플러그. 그렇지 않으면 가상 시스템이 다른 호스트로 마이그레이션될 때 이러한 인터페이스가 실패합니다. 자세한 내용은 [네트워크 MTU가 변경된 후 일부 VM과 브리지에는 이전 MTU가 있으며 패킷 삭제와 BZ#1766414](#)를 참조하십시오.

11. 외부 프로바이더 드롭다운 목록에서 `ovirt-provider-ovn` 을 선택한 경우 네트워크에서 보안 그룹을 구현할지 여부를 정의합니다. 자세한 내용은 [Logical Network General Settings](#)에서 참조하십시오.
12. **Cluster**(클러스터) 탭에서 네트워크를 할당할 클러스터를 선택합니다. 논리적 네트워크가 필수 네트워크인지 여부를 지정할 수도 있습니다.
13. **Create on external provider**(외부 공급업체에 생성) 확인란이 선택되면 **Subnet**(서브넷) 탭이 표시됩니다. **Subnet**(서브넷) 탭에서 **Create subnet**(서브넷 만들기)을 선택하고 **Name**(이름), **CIDR**, **Gateway**(게이트웨이 주소)를 입력한 다음 논리적 네트워크에서 제공할 서브넷의 **IP Version**(IP 버전)을 선택합니다. 필요에 따라 **DNS** 서버를 추가할 수도 있습니다.
14. **vNIC Profiles**(vNIC 프로필) 탭에서 필요에 따라 vNIC 프로필을 논리적 네트워크에 추가합니다.
15. **OK**(확인)를 클릭합니다.

논리적 네트워크의 레이블을 입력한 경우 해당 레이블이 있는 모든 호스트 네트워크 인터페이스에 자동으로 추가됩니다.

**참고**

새 논리적 네트워크를 만들거나 디스플레이 네트워크로 사용되는 기존 논리적 네트워크를 변경할 때 해당 네트워크를 사용하는 실행 중인 가상 시스템을 네트워크를 사용할 수 있게 되기 전에 재부팅해야 합니다.

2.4.1.3. 논리적 네트워크 편집

**중요**

논리적 네트워크는 호스트의 네트워크 구성과 동기화되지 않은 경우 다른 인터페이스로 편집하거나 이동할 수 없습니다. [네트워크 동기화 방법에 대한 자세한 내용은 호스트 네트워크 인터페이스 편집 및 호스트에 논리적 네트워크 할당](#)을 참조하십시오.

절차

1. **Compute**(컴퓨팅) → **Data Centers**(데이터 센터)를 클릭합니다.
2. 데이터 센터의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Logical Networks**(논리적 네트워크) 탭을 클릭하고 논리적 네트워크를 선택합니다.

4. **Edit(편집)**를 클릭합니다.

5. 필요한 설정을 편집합니다.



참고

가상 시스템을 중지하지 않고도 기본 네트워크를 제외하고 새 또는 기존 네트워크의 이름을 편집할 수 있습니다.

6. **OK(확인)**를 클릭합니다.



참고

다중 호스트 네트워크 구성은 네트워크가 할당되는 데이터 센터 내의 모든 호스트에 업데이트된 네트워크 설정을 자동으로 적용합니다. 변경 사항은 네트워크를 사용하는 가상 머신이 중단된 경우에만 적용할 수 있습니다. 호스트에 이미 구성된 논리적 네트워크의 이름을 변경할 수 없습니다. 해당 네트워크를 사용하는 가상 시스템 또는 템플릿은 실행 중인 동안 VM 네트워크 옵션을 비활성화할 수 없습니다.

2.4.1.4. 논리적 네트워크 제거

네트워크 네트워크 또는 →계산 →데이터 센터에서 논리적 네트워크를 제거할 수 있습니다. 다음 절차에서는 데이터 센터와 연결된 논리적 네트워크를 제거하는 방법을 보여줍니다. 작동 중인 Red Hat Virtualization 환경의 경우 ovirtmgmt 관리 네트워크로 사용되는 논리적 네트워크가 하나 이상 있어야 합니다.

절차

1. **Compute(컴퓨팅) → Data Centers (데이터 센터)**를 클릭합니다.
2. 데이터 센터의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Logical Networks(논리적 네트워크)** 탭을 클릭하여 데이터 센터의 논리적 네트워크를 나열합니다.
4. 논리적 네트워크를 선택하고 **Remove(제거)**를 클릭합니다.
5. 선택적으로 **Remove external network(s) from provider(공급업체)** 및 외부 프로바이더가 네트워크를 제공하는 경우 **Manager(관리자)** 및 외부 프로바이더에서 논리적 네트워크를 모두 제거하려면 **Remove external network(s)(외부 네트워크 제거)** 확인란을 선택합니다. 외부 프로바이더가 읽기 전용 모드인 경우 확인란이 회색으로 표시됩니다.
6. **OK(확인)**를 클릭합니다.

논리적 네트워크는 Manager에서 제거되며 더 이상 사용할 수 없습니다.

2.4.1.5. 비관리 논리적 네트워크를 기본 경로로 구성

클러스터의 호스트에서 사용하는 기본 경로는 관리 네트워크(ovirtmgmt)를 사용하는 것입니다. 다음 절차에서는 비 관리 논리적 네트워크를 기본 경로로 구성하는 지침을 제공합니다.

사전 요구 사항:

- **default_route** 사용자 지정 속성을 사용하는 경우 연결된 모든 호스트에서 사용자 지정 속성을 지운 다음 다음 절차를 따라야 합니다.

기본 경로 역할 구성

1. **Network → Networks** (네트워크) 를 클릭합니다.
2. 비관리 논리적 네트워크의 이름을 클릭하여 세부 정보에 액세스할 기본 경로로 를 구성합니다.
3. **Clusters**(클러스터) 탭을 클릭합니다.
4. **Manage Network**(네트워크 관리)를 클릭합니다. 그러면 **Manage Network**(네트워크 관리) 창이 열립니다.
5. 적절한 클러스터의 기본 경로 확인란을 선택합니다.
6. **OK**(확인)를 클릭합니다.

네트워크가 호스트에 연결되면 선택한 네트워크에 호스트의 기본 경로가 설정됩니다. 호스트가 클러스터에 추가되기 전에 기본 경로 역할을 구성하는 것이 좋습니다. 클러스터에 호스트가 이미 포함되어 있는 경우 변경 사항을 동기화할 때까지 동기화되지 않을 수 있습니다.

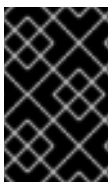
IPv6의 중요한 제한 사항

- IPv6의 경우 Red Hat Virtualization은 정적 주소 지정만 지원합니다.
- 두 네트워크에서 단일 게이트웨이(동일한 서브넷에 있음)를 공유하는 경우 기본 경로 역할을 관리 네트워크(ovirtmgmt)에서 다른 논리적 네트워크로 이동할 수 있습니다.
- 호스트와 관리자가 동일한 서브넷에 있지 않으면 IPv6 게이트웨이가 제거되었으므로 관리자가 호스트와의 연결이 끊어집니다.
- 기본 경로 역할을 비관리 네트워크로 이동하면 네트워크 인터페이스에서 IPv6 게이트웨이가 제거되고 경고를 생성합니다. "클러스터 클러스터에서 '기본 경로 역할' 네트워크가 더 이상 네트워크 ovirtmgmt가 아닙니다. 이 네트워크에서 IPv6 게이트웨이가 제거됩니다."

2.4.1.6. 호스트에 정적 경로 추가

nmstate를 사용하여 호스트에 정적 경로를 추가할 수 있습니다. 이 방법을 사용하려면 Red Hat Virtualization Manager를 사용하지 않고 호스트를 직접 구성해야 합니다.

추가한 static-routes는 관련 라우팅된 브리지, 인터페이스 또는 본당이 존재하고 IP 주소가 있는 한 보존됩니다. 그렇지 않으면 시스템은 정적 경로를 제거합니다.



중요

호스트에서 정적 경로를 추가하거나 제거하는 것을 제외하고 항상 RHV Manager를 사용하여 클러스터에서 호스트 네트워크 설정을 구성합니다. 자세한 내용은 [Network Manager Stateful Configuration\(nmstate\)](#) 을 참조하십시오.

참고

사용자 지정 **static-route**는 인터페이스/**bond**가 존재하고 IP 주소가 있는 한 보존됩니다. 그렇지 않으면 제거됩니다.

결과적으로 VM 네트워크는 VM 이외의 네트워크와 다르게 작동합니다.

- VM 네트워크는 브리지를 기반으로 합니다. 하나의 인터페이스/결정에서 다른 인터페이스로 네트워크를 이동해도 VM 네트워크의 경로에는 영향을 미치지 않습니다.
- VM 이외의 네트워크는 인터페이스를 기반으로 합니다. 네트워크를 하나의 인터페이스/결정에서 다른 인터페이스로 이동하면 Non-VM 네트워크와 관련된 경로가 삭제됩니다.

사전 요구 사항

이 절차에는 **nmstate**가 필요하며, 해당 환경에서만 사용 가능합니다.

- Red Hat Virtualization Manager 버전 4.4
- Red Hat Enterprise Linux 8을 기반으로 하는 Red Hat Enterprise Linux 호스트 및 Red Hat Virtualization 호스트

절차

1. 구성할 호스트에 연결합니다.
2. 호스트에서 다음 예제 콘텐츠를 사용하여 **static_route.yml** 파일을 생성합니다.

```
routes:
  config:
    - destination: 192.168.123.0/24
      next-hop-address: 192.168.178.1
      next-hop-interface: eth1
```

3. 표시된 예제 값을 네트워크의 실제 값으로 바꿉니다.
4. 트래픽을 보조 추가 네트워크로 라우팅하려면 **next-hop-interface** 를 사용하여 인터페이스 또는 네트워크 이름을 지정합니다.
 - 비가상 시스템 네트워크를 사용하려면 **eth1** 과 같은 인터페이스를 지정합니다.
 - 가상 머신 네트워크를 사용하려면 **net1** 과 같은 브리지 이름이기도 한 네트워크 이름을 지정합니다.
5. 다음 명령을 실행하십시오.

```
$ nmstatectl set static_route.yml
```

검증 단계

- **static_route.yml** 에 설정한 대상 매개 변수 값을 사용하여 **IProute** 명령 **ip route** 를 실행합니다. 그러면 원하는 경로가 표시되어야 합니다. 예를 들어 다음 명령을 실행합니다.

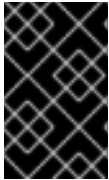
```
$ ip route | grep 192.168.123.0`
```

추가 리소스

- [네트워크 관리자 상태 저장 설정 \(nmstate\)](#)
- [호스트에서 정적 경로 제거](#)

2.4.1.7. 호스트에서 정적 경로 제거

nmstate를 사용하여 호스트에서 정적 경로를 제거할 수 있습니다. 이 방법을 사용하려면 Red Hat Virtualization Manager를 사용하지 않고 호스트를 직접 구성해야 합니다.



중요

호스트에서 정적 경로를 추가하거나 제거하는 것을 제외하고 항상 RHV Manager를 사용하여 클러스터에서 호스트 네트워크 설정을 구성합니다. 자세한 내용은 [Network Manager Stateful Configuration\(nmstate\)](#) 을 참조하십시오.



참고

사용자 지정 static-route는 인터페이스/bond가 존재하고 IP 주소가 있는 한 보존됩니다. 그렇지 않으면 제거됩니다.

결과적으로 VM 네트워크는 VM 이외의 네트워크와 다르게 작동합니다.

- VM 네트워크는 브리지를 기반으로 합니다. 하나의 인터페이스/결정에서 다른 인터페이스로 네트워크를 이동해도 VM 네트워크의 경로에는 영향을 미치지 않습니다.
- VM 이외의 네트워크는 인터페이스를 기반으로 합니다. 네트워크를 하나의 인터페이스/결정에서 다른 인터페이스로 이동하면 Non-VM 네트워크와 관련된 경로가 삭제됩니다.

사전 요구 사항

이 절차에는 nmstate가 필요하며, 해당 환경에서만 사용 가능합니다.

- Red Hat Virtualization Manager 버전 4.4
- Red Hat Enterprise Linux 8을 기반으로 하는 Red Hat Enterprise Linux 호스트 및 Red Hat Virtualization 호스트

절차

1. 재구성할 호스트에 연결합니다.
2. 호스트에서 **static_route.yml** 파일을 편집합니다.
3. 다음 예에 표시된 대로 line **state: absent** 를 삽입합니다.
4. 인터페이스: [] 사이에 **next-hop-interface** 값을 추가합니다. 결과는 여기에 표시된 예와 유사해야 합니다.

```
routes:
  config:
    - destination: 192.168.123.0/24
      next-hop-address: 192.168.178.
```

```
next-hop-interface: eth1
state: absent
interfaces: [{"name": eth1}]
```

5. 다음 명령을 실행하십시오.

```
$ nmstatectl set static_route.yml
```

검증 단계

- **static_route.yml**에 설정한 대상 매개 변수 값을 사용하여 **IProute** 명령 **ip route**를 실행합니다. 더 이상 원하는 경로가 표시되지 않습니다. 예를 들어 다음 명령을 실행합니다.

```
$ ip route | grep 192.168.123.0`
```

추가 리소스

- [네트워크 관리자 상태 저장 설정 \(nmstate\)](#)
- [호스트에 정적 경로 추가](#)

2.4.1.8. 논리적 네트워크의 게이트웨이 보기 또는 편집

사용자가 논리적 네트워크에 대한 IP 주소 및 서브넷 마스크와 함께 게이트웨이를 정의할 수 있습니다. 이 작업은 호스트에 여러 네트워크가 있고 기본 게이트웨이가 아니라 지정된 네트워크를 통해 트래픽을 라우팅해야 하는 경우 필요합니다.

호스트에 여러 네트워크가 있고 게이트웨이가 정의되지 않은 경우 기본 게이트웨이를 통해 반환 트래픽이 라우팅되며 의도한 대상에 도달하지 못할 수 있습니다. 이로 인해 사용자가 호스트를 ping할 수 없습니다.

Red Hat Virtualization은 인터페이스가 시작되거나 중단될 때마다 자동으로 여러 게이트웨이를 처리합니다.

절차

1. **Compute(컴퓨팅) Hosts(호스트)**를 클릭합니다.
2. 호스트 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Network Interfaces(네트워크 인터페이스)** 탭을 클릭하여 호스트에 연결된 네트워크 인터페이스와 해당 구성을 나열합니다.
4. **Setup Host Networks(호스트 네트워크 설정)**를 클릭합니다.
5. 할당된 논리적 네트워크 위로 커서를 가리키고 연필 아이콘을 클릭합니다. 그러면 **Edit Management Network(관리 네트워크 편집)** 창이 열립니다.

Edit Management Network(관리 네트워크 편집) 창에는 네트워크 이름, 부팅 프로토콜 및 IP, 서브넷 마스크 및 게이트웨이 주소가 표시됩니다. 주소 정보는 정적 부팅 프로토콜을 선택하여 수동으로 편집할 수 있습니다.

2.4.1.9. 논리적 네트워크 일반 설정 설명

아래 표는 New Logical Network(새 논리적 네트워크) 및 Edit Logical Network(논리 네트워크 편집) 창의 General (일반) 탭에 대한 설정을 설명합니다.

표 2.15. 새로운 논리적 네트워크 및 논리적 네트워크 설정 편집

필드 이름	설명
이름	논리적 네트워크의 이름입니다. 이 텍스트 필드는 대문자와 소문자, 숫자, 하이픈, 밑줄이 조합된 고유한 이름이어야 합니다. 논리적 네트워크의 이름은 15자를 초과하고 ASCII가 아닌 문자를 포함할 수 있지만 호스트 ID(vdsm_name)는 정의한 이름과 다릅니다. 이러한 이름의 매핑을 표시하는 방법에 대한 자세한 내용은 논리적 네트워크 이름으로 매핑 VDSM 이름을 참조하십시오.
설명	논리적 네트워크에 대한 설명입니다. 이 텍스트 필드에는 40자 제한이 있습니다.
설명	논리적 네트워크와 관련된 일반 텍스트인 사람이 읽을 수 있는 주석을 추가하는 필드입니다.
외부 공급자에서 생성	Manager에 외부 프로바이더로 추가된 OpenStack Networking 인스턴스에 논리적 네트워크를 생성할 수 있습니다. External Provider (외부 프로바이더) - 논리적 네트워크가 생성될 외부 공급자를 선택할 수 있습니다.
VLAN 태그 지정 활성화	VLAN 태그 지정은 논리적 네트워크에서 전달되는 모든 네트워크 트래픽에 특별한 특성을 부여하는 보안 기능입니다. VLAN 태그 지정 트래픽은 이러한 특징이 없는 인터페이스에서 읽을 수 없습니다. 논리적 네트워크에서 VLAN을 사용하면 단일 네트워크 인터페이스를 다양한 다른 VLAN 태그 지정 논리적 네트워크와 연결할 수 있습니다. VLAN 태그 지정이 활성화된 경우 텍스트 항목 필드에 숫자 값을 입력합니다.
VM 네트워크	이 네트워크를 사용하는 가상 시스템만 사용하는 경우 이 옵션을 선택합니다. 네트워크가 가상 시스템이 필요하지 않은 트래픽(예: 스토리지 통신)에 사용되는 경우 이 확인란을 선택하지 마십시오.
포트 격리	이 설정을 설정하면 동일한 호스트의 가상 시스템이 이 논리적 네트워크에서 서로 통신하고 볼 수 없습니다. 이 옵션이 다른 하이퍼바이저에서 작동하려면 하이퍼바이저에 연결된 각 포트/VLAN에서 PVLAN/Port Isolation을 사용하여 스위치를 구성해야 하며 Hairpin 설정을 사용하여 프레임을 다시 반영하지 않아야 합니다.

필드 이름	설명
MTU	최대 전송 단위(MTU)를 괄호()에 지정된 값으로 설정하는 Default (기본값)를 선택하거나 Custom 을 선택하여 논리적 네트워크의 사용자 지정 MTU를 설정합니다. 이를 사용하여 새 논리적 네트워크에서 지원되는 MTU를 인터페이스하는 하드웨어에서 지원하는 MTU와 일치시킬 수 있습니다. Custom 이 선택된 경우 텍스트 항목 필드에 숫자 값을 입력합니다. 중요: 네트워크의 MTU 설정을 변경하는 경우 이 변경 사항을 네트워크에서 실행 중인 가상 머신으로 전파해야 합니다. MTU 설정을 적용하거나 가상 시스템을 다시 시작해야 하는 모든 가상 시스템의 vNIC의 핫플러그 및 재플러그. 그렇지 않으면 가상 시스템이 다른 호스트로 마이그레이션될 때 이러한 인터페이스가 실패합니다. 자세한 내용은 네트워크 MTU가 변경된 후 일부 VM과 브리지에는 이전 MTU가 있으며 패킷 삭제와 BZ#1766414 를 참조하십시오.
네트워크 레이블	네트워크에 새 레이블을 지정하거나 호스트 네트워크 인터페이스에 이미 연결된 기존 라벨 중에서 선택할 수 있습니다. 기존 레이블을 선택하면 논리적 네트워크가 해당 레이블이 있는 모든 호스트 네트워크 인터페이스에 자동으로 할당됩니다.
보안 그룹	이 논리적 네트워크의 포트에 보안 그룹을 할당할 수 있습니다. disabled 는 보안 그룹 기능을 비활성화합니다. Enable(활성화) 기능을 활성화합니다. 포트를 만들고 이 네트워크에 연결하면 포트 보안이 활성화된 상태로 정의됩니다. 즉, 가상 시스템에 대한 액세스는 현재 배포 중인 보안 그룹의 적용을 받습니다. Configuration(구성)에서 상속 하면 포트가 모든 네트워크에 대해 정의된 구성 파일에서 동작을 상속할 수 있습니다. 기본적으로 파일은 보안 그룹을 비활성화합니다. 자세한 내용은 Security Groups to Logical Networks 를 참조하십시오.

2.4.1.10. 논리적 네트워크 클러스터 설정 설명

아래 표는 New Logical Network(새 논리적 네트워크) 창의 **Cluster(클러스터)** 탭에 대한 설정을 설명합니다.

표 2.16. 새로운 논리적 네트워크 설정

필드 이름	설명

필드 이름	설명
클러스터에 네트워크 연결/연결	데이터 센터의 클러스터에서 논리적 네트워크를 연결하거나 분리하고 논리적 네트워크가 개별 클러스터에 필요한 네트워크인지 여부를 지정할 수 있습니다. name - 설정이 적용할 클러스터의 이름입니다. 이 값을 편집할 수 없습니다. Attach All(모두 연결) - 데이터 센터의 모든 클러스터에 논리적 네트워크를 연결하거나 분리할 수 있습니다. 또는 지정된 클러스터에 논리적 네트워크를 연결하거나 분리할 각 클러스터의 이름 옆에 있는 Attach (연결) 확인란을 선택하거나 지웁니다. 필수 모두 - 논리적 네트워크가 모든 클러스터에서 필수 네트워크인지 여부를 지정할 수 있습니다. 또는 각 클러스터의 이름 옆에 있는 Required (필수) 확인란을 선택하거나 지워서 논리적 네트워크가 지정된 클러스터에 필요한 네트워크인지 여부를 지정합니다.

2.4.1.11. 논리적 네트워크 vNIC 프로파일 설정 설명

아래 표에서는 New Logical Network(새 논리적 네트워크) 창의 vNIC Profiles(vNIC 프로파일) 탭에 대한 설정을 설명합니다.

표 2.17. 새로운 논리적 네트워크 설정

필드 이름	설명
vNIC 프로파일	논리적 네트워크에 대해 하나 이상의 vNIC 프로파일을 지정할 수 있습니다. vNIC 프로파일 옆에 있는 더하기 또는 빼기 버튼을 클릭하여 논리적 네트워크에 vNIC 프로파일을 추가하거나 제거할 수 있습니다. 첫 번째 필드는 vNIC 프로파일의 이름을 입력하기 위한 것입니다. public - 모든 사용자가 프로파일을 사용할 수 있는지 여부를 지정할 수 있습니다. QoS - vNIC 프로파일에 네트워크 서비스 품질(QoS) 프로파일을 지정할 수 있습니다.

2.4.1.12. 네트워크 관리 창을 사용하여 논리적 네트워크의 특정 트래픽 유형 지정

논리적 네트워크의 트래픽 유형을 지정하여 네트워크 트래픽 흐름을 최적화합니다.

절차

1. **Compute(컴퓨팅) Clusters(클러스터)** 를 클릭합니다.
2. 클러스터 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Logical Networks(논리적 네트워크)** 탭을 클릭합니다.

4. **Manage Networks**(네트워크 관리)를 클릭합니다.
5. 적절한 확인란과 라디오 버튼을 선택합니다.
6. **OK**(확인)를 클릭합니다.



참고

외부 프로바이더가 제공하는 논리적 네트워크는 가상 시스템 네트워크로 사용해야 합니다. 디스플레이 또는 마이그레이션과 같은 특수 클러스터 역할을 할당할 수 없습니다.

2.4.1.13. 네트워크 관리 창에서 설정 설명

아래 표에서는 **Manage Networks**(네트워크 관리) 창에 대한 설정을 설명합니다.

표 2.18. 네트워크 설정 관리

필드	설명/액션
할당	논리적 네트워크를 클러스터의 모든 호스트에 할당합니다.
필수 항목	연결된 호스트가 제대로 작동하려면 "필수됨"으로 표시된 네트워크가 계속 작동해야 합니다. 필수 네트워크가 작동하지 않으면 연결된 모든 호스트가 작동하지 않습니다.
VM 네트워크	"VM 네트워크"라고 표시된 논리적 네트워크는 가상 시스템 네트워크와 관련된 네트워크 트래픽을 전송합니다.
디스플레이 네트워크	"Display Network"라고 표시된 논리적 네트워크는 SPICE 및 가상 네트워크 컨트롤러와 관련된 네트워크 트래픽을 전송합니다.
마이그레이션 네트워크	"마이그레이션 네트워크"라고 표시된 논리적 네트워크는 가상 시스템 및 스토리지 마이그레이션 트래픽을 전송합니다. 이 네트워크에서 중단되면 관리 네트워크(기본적으로 ovirtmgmt)가 대신 사용됩니다.

2.4.1.14. NIC에서 가상 기능 구성



참고

이는 Red Hat Virtualization에서 SR-IOV를 설정하고 구성하는 방법을 보여주는 일련의 주제 중 하나입니다. 자세한 내용은 [SR-IOV 설정 및 구성](#)을 참조하십시오.

SR-IOV(Single Root I/O Virtualization)를 사용하면 물리적 기능(PF) 및 VF(가상 기능)를 사용하여 각 PCIe 끝점을 여러 개의 개별 장치로 사용할 수 있습니다. PCIe 카드는 하나에서 8개의 PF를 가질 수 있습니다. 각 PF에는 많은 VF가 있을 수 있습니다. 보유할 수 있는 VF 수는 PCIe 장치의 특정 유형에 따라 다릅니다.

SR-IOV 사용 가능한 NIC(네트워크 인터페이스 컨트롤러)를 구성하려면 Red Hat Virtualization Manager를 사용합니다. 여기에서 각 NIC에서 VF 수를 구성할 수 있습니다.

다음은 포함하여 독립 실행형 NIC를 구성하는 것과 같이 VF를 구성할 수 있습니다.

- 하나 이상의 논리적 네트워크를 VF에 할당.
- VF를 사용하여 결합된 인터페이스 생성.
- 직접 장치 패스스루를 위해 vNIC를 VF에 할당.

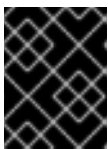
기본적으로 모든 가상 네트워크는 가상 기능에 액세스할 수 있습니다. 이 기본값을 비활성화하고 가상 기능에 액세스할 수 있는 네트워크를 지정할 수 있습니다.

사전 요구 사항

- vNIC를 VF에 연결하려면 passthrough 속성을 활성화해야 합니다. 자세한 내용은 [Enabling_Passthrough_on_a_vNIC_Profile](#) 을 참조하십시오.

절차

1. Compute(컴퓨팅) Hosts(호스트) 를 클릭합니다.
2. SR-IOV 가능 호스트의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. 네트워크 인터페이스 탭을 클릭합니다.
4. Setup Host Networks (호스트 네트워크 설정)를 클릭합니다.
5.  로 표시된 SR-IOV 가능 NIC를 선택하고 연필 아이콘을 클릭합니다.
6. 선택 사항: 가상 함수 수를 변경하려면 Number of VFs setting(VFs 설정 수) 드롭다운 버튼을 클릭하고 Number of VFs(VFs 수) 텍스트 필드를 편집합니다.



중요

VF 수를 변경하면 새 VF를 생성하기 전에 네트워크 인터페이스에서 이전 VF를 모두 삭제합니다. 여기에는 가상 머신이 직접 연결된 VF가 포함됩니다.

7. 선택 사항: 가상 기능에 액세스할 수 있는 가상 네트워크를 제한하려면 특정 네트워크를 선택합니다.
 - a. VF에 액세스해야 하는 네트워크를 선택하거나 레이블을 사용하여 네트워크 레이블을 기반으로 네트워크를 선택합니다.
8. OK(확인)를 클릭합니다.
9. Setup Host Networks(호스트 네트워크 설정) 창에서 OK(확인)를 클릭합니다.

2.4.2. 가상 네트워크 인터페이스 카드 (vNIC)

2.4.2.1. vNIC 프로파일 개요

vNIC(가상 네트워크 인터페이스 카드) 프로파일은 관리자의 개별 가상 네트워크 인터페이스 카드에 적용할

수 있는 설정 컬렉션입니다. vNIC 프로필을 사용하면 네트워크 QoS 프로필을 vNIC에 적용하고, 포트 미러링을 활성화 또는 비활성화하고, 사용자 지정 속성을 추가하거나 제거할 수 있습니다. 또한 vNIC 프로필은 이러한 프로필을 특정 사용자에게 부여할 수 있는 사용 권한(소비)에 추가되는 관리 유연성 계층을 제공합니다. 이렇게 하면 지정된 네트워크에서 다른 사용자가 수신하는 서비스의 품질을 제어할 수 있습니다.

2.4.2.2. vNIC 프로필 생성 또는 편집

vNIC(Virtual Network Interface Controller) 프로필을 생성하거나 편집하여 사용자와 그룹의 네트워크 대역폭을 조정합니다.



참고

포트 미러링을 활성화하거나 비활성화하는 경우 연결된 프로필을 사용하는 모든 가상 머신이 편집하기 전에 down 상태여야 합니다.

절차

1. Network → Networks (네트워크) 를 클릭합니다.
2. 논리적 네트워크의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. vNIC Profiles(vNIC 프로필) 탭을 클릭합니다.
4. New (새로 생성) 또는 Edit (편집)를 클릭합니다.
5. 프로필의 Name (이름) 및 Description (설명)을 입력합니다.
6. QoS(서비스 품질) 목록에서 관련 QoS(서비스 품질) 정책을 선택합니다.
7. 드롭다운 목록에서 Network Filter (네트워크 필터)를 선택하여 가상 시스템과의 네트워크 패킷 트래픽을 관리합니다. 네트워크 필터에 대한 자세한 내용은 *Red Hat Enterprise Linux Virtualization 배포 및 관리 가이드*에서 [네트워크 필터링 적용](#)을 참조하십시오.
8. Passthrough 확인란을 선택하여 vNIC의 패스스루를 활성화하고 가상 함수의 직접 장치 할당을 허용합니다. passthrough 속성을 활성화하면 QoS, 네트워크 필터링 및 포트 미러링이 호환되지 않으므로 QoS, 네트워크 필터링 및 포트 미러링이 비활성화됩니다. passthrough에 대한 자세한 내용은 [vNIC 프로파일에서 통과 활성화](#)를 참조하십시오.
9. Passthrough 를 선택한 경우 선택적으로Migratable 확인란을 선택 취소하여 이 프로필을 사용하여 vNIC에 대한 마이그레이션을 비활성화합니다. 이 확인란을 선택한 경우 [가상 머신 관리 가이드의 SR-IOV-Enabled vNIC를 사용하는 가상 머신의 추가 사전 요구 사항](#)을 참조하십시오.
10. 포트 미러링 및 모든 사용자가 이 프로필을 사용하도록 허용 확인란을 사용하여 이러한 옵션을 전환합니다.
11. 표시되는 사용자 정의 속성 목록에서 사용자 정의 속성을 선택하십시오. 키를 선택하십시오. 기본적으로, + 및 - 버튼을 사용하여 사용자 지정 속성을 추가하거나 제거합니다.
12. OK(확인)를 클릭합니다.

사용자 및 그룹에 이 프로필을 적용하여 네트워크 대역폭을 조정합니다. vNIC 프로필을 편집한 경우 가상 시스템을 재시작하거나 게스트 운영 체제에서 vNIC 핫 플러그 및 핫 언플러그를 지원하는 경우 vNIC를 핫 플러그로 연결해야 합니다.

2.4.2.3. VM 인터페이스 프로필 창에서 설정 설명

표 2.19. VM 인터페이스 프로파일 창

필드 이름	설명
네트워크	vNIC 프로필을 적용할 사용 가능한 네트워크의 드롭다운 목록입니다.
이름	vNIC 프로필의 이름입니다. 1~50자 사이에 대문자와 소문자, 숫자, 하이픈, 밑줄이 조합된 고유한 이름이어야 합니다.
설명	vNIC 프로필에 대한 설명입니다. 이 필드는 권장되지만 필수는 아닙니다.
QoS	vNIC 프로필에 적용할 사용 가능한 네트워크 품질 정책의 드롭다운 목록입니다. QoS 정책은 vNIC의 인바운드 및 아웃바운드 네트워크 트래픽을 규제합니다.
네트워크 필터	vNIC 프로필에 적용할 사용 가능한 네트워크 필터의 드롭다운 목록입니다. 네트워크 필터는 가상 머신으로 또는 가상 머신에서 전송할 수 있는 패킷 유형을 필터링하여 네트워크 보안을 향상시킵니다. 기본 필터는 vdsm-no-mac-spoofing 으로, no-mac-spoofing 및 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 본딩에는 <네트워크 필터 없음> 을 사용합니다. 신뢰할 수 있는 가상 시스템에서 네트워크 필터를 사용하지 않는 경우 성능이 향상됩니다.  참고 Red Hat은 engine-config 도구를 사용하여 EnableMACAntiSpoofingFilterRules 매개변수를 false 로 설정하여 필터 비활성화를 지원하지 않습니다. 대신 <No Network Filter> 옵션을 사용합니다.
Passthrough	passthrough 속성을 토글하는 확인란입니다. 통과를 사용하면 vNIC가 호스트 NIC의 가상 기능에 직접 연결할 수 있습니다. vNIC 프로필이 가상 머신에 연결된 경우 passthrough 속성을 편집할 수 없습니다. 통과가 활성화된 경우 vNIC 프로필에서 QoS, 네트워크 필터 및 포트 미러링이 비활성화됩니다.

필드 이름	설명
마이그레이션 가능	이 프로필을 사용하는 vNIC를 사용하는지 여부를 토글하는 확인란은 마이그레이션할 수 있습니다. 마이그레이션은 일반 vNIC 프로필에서 기본적으로 활성화되어 있습니다. 확인란은 선택되며 변경할 수 없습니다. Passthrough 확인란을 선택하면 Migratable 을 사용할 수 있게 되며 필요한 경우 passthrough vNIC의 마이그레이션을 비활성화할 수 있습니다.
페일오버	장애 조치 장치 역할을 하는 사용 가능한 vNIC 프로필을 선택하는 드롭다운 메뉴입니다. Passthrough 및 Migratable 확인란이 선택된 경우에만 사용할 수 있습니다.
포트 미러링	포트 미러링을 토글하는 확인란입니다. 포트 미러링은 논리적 네트워크의 계층 3 네트워크 트래픽을 가상 시스템의 가상 인터페이스에 복사합니다. 기본적으로 선택되지 않습니다. 자세한 내용은 Port Mirroring in the Technical Reference 를 참조하십시오.
장치 사용자 정의 속성	vNIC 프로필에 적용할 사용 가능한 사용자 지정 속성을 선택하는 드롭다운 메뉴입니다. + 및 - 버튼을 사용하여 각각 속성을 추가하고 제거합니다.
모든 사용자가 이 프로파일을 사용하도록 허용	프로필의 가용성을 환경의 모든 사용자에게 토글하는 확인란을 선택합니다. 기본적으로 선택됩니다.

2.4.2.4. vNIC 프로필에서 패스스루 활성화



참고

이는 Red Hat Virtualization에서 SR-IOV를 설정하고 구성하는 방법을 보여주는 일련의 주제 중 하나입니다. 자세한 내용은 [SR-IOV 설정 및 구성](#)을 참조하십시오.

vNIC 프로필의 passthrough 특성을 사용하면 vNIC가 SR-IOV 지원 NIC의 VF(가상 기능)에 직접 연결할 수 있습니다. 그런 다음 vNIC는 소프트웨어 네트워크 가상화를 무시하고 직접 장치 할당을 위해 VF에 직접 연결합니다.

vNIC 프로필이 vNIC에 이미 연결되어 있으면 passthrough 속성을 활성화할 수 없습니다. 이 절차에서는 이를 방지하는 새 프로필을 생성합니다. vNIC 프로필에 통과가 활성화된 경우 동일한 프로필에서 QoS, 네트워크 필터 및 포트 미러링을 활성화할 수 없습니다.

SR-IOV, 직접 장치 할당 및 Red Hat Virtualization에서 이러한 구현을 위한 하드웨어 고려 사항에 대한 자세한 내용은 [SR-IOV 구현을 위한 하드웨어 고려 사항](#)을 참조하십시오.

절차

1. Network → Networks (네트워크) 를 클릭합니다.
2. 논리적 네트워크의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.

3. vNIC Profiles(vNIC 프로필) 탭을 클릭하여 해당 논리적 네트워크의 모든 vNIC 프로필을 나열합니다.
4. New (새로 만들기)를 클릭합니다.
5. 프로필의 Name (이름) 및 Description (설명)을 입력합니다.
6. Passthrough(통과) 확인란을 선택합니다.
7. 선택적으로 이 프로필을 사용하여 vNIC에 대한 마이그레이션을 비활성화하려면 Migratable 확인란을 선택 취소합니다. 이 확인란을 선택한 경우 [가상 머신 관리 가이드의 SR-IOV-Enabled vNIC를 사용하는 가상 머신의 추가 사전 요구사항](#)을 참조하십시오.
8. 필요한 경우 키를 선택하십시오. 기본적으로, + 및 - 버튼을 사용하여 사용자 지정 속성을 추가하거나 제거합니다.
9. OK(확인)를 클릭합니다.

vNIC 프로필이 passthrough-capable로 변경되었습니다. 이 프로필을 사용하여 NIC 또는 PCI VF에 가상 머신을 직접 연결하려면 논리적 네트워크를 NIC에 연결하고 passthrough vNIC 프로필을 사용하는 원하는 가상 머신에 새 PCI Passthrough vNIC를 생성합니다. 이러한 절차에 대한 자세한 내용은 [호스트 네트워크 인터페이스 편집 및 호스트에 논리 네트워크 할당 및 가상 시스템 관리 가이드에서 새 네트워크 인터페이스 추가](#)를 참조하십시오.

2.4.2.5. 장애 조치로 SR-IOV 마이그레이션에 대한 vNIC 프로필 활성화

장애 조치(failover)를 사용하면 VF를 분리하여 최소한의 중단으로 가상 머신 통신을 보존하여 가상 머신 마이그레이션 중에 장애 조치 장치 역할을 하는 프로필을 선택할 수 있습니다.



참고

페일오버는 기술 프리뷰 기능 전용입니다. 기술 프리뷰 기능은 Red Hat 프로덕션 서비스 수준 계약(SLA)에서 지원되지 않으며 기능적으로 완전하지 않을 수 있으며 프로덕션에 사용하지 않는 것이 좋습니다. 이러한 기능을 사용하면 향후 제품 기능을 조기에 이용할 수 있어 개발 과정에서 고객이 기능을 테스트하고 피드백을 제공할 수 있습니다. 자세한 내용은 [Red Hat 기술 프리뷰 기능 지원 범위를 참조하십시오](#).

사전 요구 사항

- 프로필의 Passthrough 및 Migratable 확인란이 선택됩니다.
- 페일오버 네트워크가 호스트에 연결되어 있습니다.
- 장애 조치(failover)를 편집할 수 있는 vNIC 프로필을 만들려면 먼저 페일오버 참조를 제거해야 합니다.
- 장애 조치(failover) 역할을 할 수 있는 vNIC 프로필은 Passthrough로 선택되지 않거나 외부 네트워크에 연결되어 있지 않은 프로필입니다.

절차

1. 관리 포털의 Network → vNIC 프로필로 이동하여 vNIC 프로필을 선택하고 Edit(편집)를 클릭하고 드롭다운 목록에서 Failover vNIC 프로필을 선택합니다.
2. OK(확인)를 클릭하여 프로필 설정을 저장합니다.



참고

동일한 장애 조치 vNIC 프로필을 동일한 가상 시스템에 참조하는 두 개의 vNIC 프로필을 libvirt에서 연결할 수 없습니다.

2.4.2.6. vNIC 프로필 제거

vNIC 프로필을 제거하여 가상화된 환경에서 삭제합니다.

절차

1. Network → Networks (네트워크) 를 클릭합니다.
2. 논리적 네트워크의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. vNIC Profiles(vNIC 프로필) 탭을 클릭하여 사용 가능한 vNIC 프로필을 표시합니다.
4. 하나 이상의 프로필을 선택하고 Remove(제거)를 클릭합니다.
5. OK(확인)를 클릭합니다.

2.4.2.7. vNIC 프로필에 보안 그룹 할당



참고

이 기능은 **ovirt-provider-ovn** 이 외부 네트워크 프로바이더로 추가된 경우에만 사용할 수 있습니다. 보안 그룹은 Red Hat Virtualization Manager를 통해 만들 수 없습니다. **ovirt-provider-ovn** 에서 OpenStack 네트워킹을 통해 보안 그룹을 생성해야 합니다. 자세한 내용은 *Red Hat OpenStack Platform 사용자 및 ID 관리 가이드*의 [Project Security Management](#) 를 참조하십시오.

OpenStack Networking 인스턴스에서 가져온 네트워크의 vNIC 프로필에 보안 그룹을 할당하고 Open vSwitch 플러그인을 사용할 수 있습니다. 보안 그룹은 네트워크 인터페이스를 통해 인바운드 및 아웃바운드 트래픽을 필터링할 수 있는 엄격하게 적용된 규칙 컬렉션입니다. 다음 절차에서는 보안 그룹을 vNIC 프로필에 연결하는 방법을 간략하게 설명합니다.



참고

보안 그룹은 OVN(Open Virtual Network) 외부 네트워크 프로바이더에 등록된 해당 보안 그룹의 ID를 사용하여 식별됩니다. OpenStack Networking API를 사용하여 지정된 테넌트에 대한 보안 그룹의 ID는 *OpenStack API 참조*의 [List Security Groups](#) 를 참조하십시오.

절차

1. Network → Networks (네트워크) 를 클릭합니다.
2. 논리적 네트워크의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. vNIC Profiles(vNIC 프로필) 탭을 클릭합니다.
4. 새로 생성을 클릭하거나 기존 vNIC 프로필을 선택하고 Edit(편집)를 클릭합니다.
5. 사용자 지정 속성 드롭다운 목록에서 SecurityGroups 를 선택합니다. 사용자 지정 속성 드롭다운을 비워 두면 기본 보안 설정이 적용되므로 모든 아웃바운드 트래픽 및 상호 통신이 허용되지만 기본 보

안 그룹 외부의 모든 인바운드 트래픽은 거부됩니다. 나중에 SecurityGroups 속성을 제거해도 적용된 보안 그룹에는 영향을 미치지 않습니다.

6. 텍스트 필드에 vNIC 프로필에 연결할 보안 그룹의 ID를 입력합니다.
7. OK(확인)를 클릭합니다.

보안 그룹을 vNIC 프로필에 연결했습니다. 해당 보안 그룹에 대해 정의된 규칙에 따라 해당 프로필이 연결된 논리적 네트워크를 통한 모든 트래픽이 필터링됩니다.

2.4.2.8. vNIC 프로필의 사용자 권한

특정 vNIC 프로필에 사용자를 할당하도록 사용자 권한을 구성합니다. VnicProfileUser 역할을 사용자에게 할당하여 프로필을 사용하도록 설정합니다. 해당 프로필에 대한 권한을 제거하여 특정 프로필에서 사용자를 제한합니다.

vNIC 프로필의 사용자 권한

1. Network vNIC Profile(네트워크vNIC 프로필)을 클릭합니다.
2. vNIC 프로필의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. Permissions(권한) 탭을 클릭하여 프로필의 현재 사용자 권한을 표시합니다.
4. Add(추가) 또는 Remove(제거)를 클릭하여 vNIC 프로필에 대한 사용자 권한을 변경합니다.
5. Add Permissions to User(사용자에게 권한 추가) 창에서 My Groups(내 그룹)를 클릭하여 사용자 그룹을 표시합니다. 이 옵션을 사용하여 그룹의 다른 사용자에게 권한을 부여할 수 있습니다.

vNIC 프로필에 대한 사용자 권한이 구성되어 있습니다.

2.4.3. 외부 프로바이더 네트워크

2.4.3.1. 외부 공급자에서 네트워크 가져오기

OVN(Open Virtual Network)에서 네트워크를 사용하려면 Manager(관리자)에 프로바이더를 등록합니다. 자세한 내용은 [External Network Provider 추가](#)를 참조하십시오. 그런 다음 다음 절차에 따라 가상 시스템에서 네트워크를 사용할 수 있도록 해당 공급업체가 제공한 네트워크를 Manager로 가져옵니다.

절차

1. Network → Networks(네트워크)를 클릭합니다.
2. Import(가져오기)를 클릭합니다.
3. Network Provider(네트워크 프로바이더) 드롭다운 목록에서 외부 프로바이더를 선택합니다. 해당 프로바이더가 제공하는 네트워크는 자동으로 검색되고 Provider Networks(프로바이더 네트워크) 목록에 나열됩니다.
4. 확인란을 사용하여 Provider Networks(프로바이더 네트워크) 목록에서 가져올 네트워크를 선택하고 아래쪽 화살표를 클릭하여 해당 네트워크를 Networks to Import(가져오기할 네트워크) 목록으로 이동합니다.
5. 가져올 네트워크의 이름을 사용자 지정할 수 있습니다. 이름을 사용자 지정하려면 Name(이름) 열에서 네트워크 이름을 클릭하고 텍스트를 변경합니다.

6. Data Center (데이터 센터) 드롭다운 목록에서 네트워크를 가져올 데이터 센터를 선택합니다.
7. 선택 사항: Allow All(모든 허용) 확인란을 선택 취소하여 해당 네트워크를 모든 사용자가 사용할 수 없도록 합니다.
8. Import(가져오기)를 클릭합니다.

선택한 네트워크는 대상 데이터 센터로 가져오고 가상 시스템에 연결할 수 있습니다. 자세한 내용은 *가상 머신 관리 가이드*에서 [새 네트워크 인터페이스](#) 추가를 참조하십시오.

2.4.3.2. 외부 프로바이더 네트워크 사용 제한

다음 제한 사항은 Red Hat Virtualization 환경에서 외부 프로바이더에서 가져온 논리적 네트워크를 사용하는 데 적용됩니다.

- 외부 프로바이더가 제공하는 논리적 네트워크는 가상 시스템 네트워크로 사용해야 하며 디스플레이 네트워크로 사용할 수 없습니다.
- 동일한 논리적 네트워크를 두 번 이상 가져올 수 있지만 다른 데이터 센터로만 가져올 수 있습니다.
- Manager에서 외부 프로바이더가 제공하는 논리적 네트워크를 편집할 수 없습니다. 외부 프로바이더가 제공하는 논리적 네트워크의 세부 정보를 편집하려면 해당 논리적 네트워크를 제공하는 외부 프로바이더에서 직접 논리적 네트워크를 편집해야 합니다.
- 외부 프로바이더가 제공하는 논리적 네트워크에 연결된 가상 네트워크 인터페이스 카드에는 포트 미러링을 사용할 수 없습니다.
- 가상 시스템이 외부 프로바이더가 제공하는 논리적 네트워크를 사용하는 경우 논리적 네트워크는 여전히 가상 시스템에서 사용 중인 동안 Manager에서 해당 프로바이더를 삭제할 수 없습니다.
- 외부 프로바이더가 제공하는 네트워크는 필요하지 않습니다. 따라서 이러한 논리적 네트워크를 가져온 클러스터 예약은 호스트 선택 중에 해당 논리적 네트워크를 고려하지 않습니다. 또한 사용자가 논리적 네트워크를 가져온 클러스터에 있는 호스트에서 논리적 네트워크를 사용할 수 있도록 해야 합니다.

2.4.3.3. 외부 프로바이더 논리적 네트워크에서 서브넷 구성

외부 프로바이더가 제공하는 논리적 네트워크는 해당 논리적 네트워크에 하나 이상의 서브넷이 정의된 경우에만 가상 시스템에 IP 주소를 할당할 수 있습니다. 서브넷을 정의하지 않으면 가상 시스템에 할당된 IP 주소가 할당되지 않습니다. 서브넷이 하나 있는 경우 가상 시스템에 해당 서브넷의 IP 주소가 할당되며 서브넷이 여러 개인 경우 사용 가능한 서브넷의 IP 주소가 가상 시스템에 할당됩니다. 논리적 네트워크가 호스팅되는 외부 네트워크 프로바이더가 제공하는 DHCP 서비스는 이러한 IP 주소를 할당합니다.

Red Hat Virtualization Manager는 가져온 논리적 네트워크에서 사전 정의된 서브넷을 자동으로 검색하는 반면, 관리자 내에서 논리적 네트워크에 서브넷을 추가하거나 제거할 수도 있습니다.

OVN(Open Virtual Network)(ovirt-provider-ovn)을 외부 네트워크 프로바이더로 추가하는 경우 라우터를 통해 여러 서브넷을 서로 연결할 수 있습니다. 이러한 라우터를 관리하려면 [OpenStack Networking API v2.0](#)을 사용할 수 있습니다. 그러나 ovirt-provider-ovn에는 제한이 있습니다. 소스 NAT(OpenStack API의 enable_snat)가 구현되지 않았습니다.

2.4.3.4. 외부 공급자 논리적 네트워크에 서브넷 추가

외부 프로바이더가 제공하는 논리적 네트워크에 서브넷을 생성합니다.

절차

1. **Network → Networks** (네트워크) 를 클릭합니다.
2. 논리적 네트워크의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Subnets**(서브넷) 탭을 클릭합니다.
4. **New** (새로 만들기)를 클릭합니다.
5. 새 서브넷에 **Name** (이름) 및 **CIDR** 을 입력합니다.
6. **IP Version** (IP 버전) 드롭다운 목록에서 **IPv4** 또는 **IPv6** 을 선택합니다.
7. **OK**(확인)를 클릭합니다.



참고

IPv6의 경우 Red Hat Virtualization은 정적 주소 지정만 지원합니다.

2.4.3.5. 외부 공급자 논리적 네트워크에서 서브넷 제거

외부 프로바이더가 제공하는 논리적 네트워크에서 서브넷을 제거합니다.

절차

1. **Network → Networks** (네트워크) 를 클릭합니다.
2. 논리적 네트워크의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Subnets**(서브넷) 탭을 클릭합니다.
4. 서브넷을 선택하고 **Remove**(제거)를 클릭합니다.
5. **OK**(확인)를 클릭합니다.

2.4.3.6. 논리적 네트워크 및 포트에 보안 그룹 할당



참고

이 기능은 OVN(Open Virtual Network)이 외부 네트워크 프로바이더(`ovirt-provider-ovn`)로 추가된 경우에만 사용할 수 있습니다. 보안 그룹은 Red Hat Virtualization Manager를 통해 만들 수 없습니다. OpenStack Networking API v2.0 또는 Ansible을 통해 보안 그룹을 생성해야 합니다.

보안 그룹은 네트워크를 통해 인바운드 및 아웃바운드 트래픽을 필터링할 수 있는 엄격하게 적용되는 규칙 컬렉션입니다. 보안 그룹을 사용하여 포트 수준에서 트래픽을 필터링할 수도 있습니다.

Red Hat Virtualization 4.2.7에서는 기본적으로 보안 그룹이 비활성화되어 있습니다.

절차

1. **Compute**(컴퓨팅) **Clusters**(클러스터) 를 클릭합니다.
2. 클러스터 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Logical Networks**(논리적 네트워크) 탭을 클릭합니다.

4. 네트워크 추가를 클릭하고 속성을 정의하여 외부 프로바이더 드롭다운 목록에서 **ovirt-provider-ovn** 을 선택했는지 확인합니다. 자세한 내용은 [데이터 센터 또는 클러스터에서 새 논리적 네트워크 생성](#) 을 참조하십시오.
5. **Security Group** (보안 그룹) 드롭다운 목록에서 **Enabled** (활성화)를 선택합니다. 자세한 내용은 [Logical Network General Settings](#)에서 참조하십시오.
6. **OK(확인)**를 클릭합니다.
7. [OpenStack Networking API v2.0](#) 또는 [Ansible](#) 을 사용하여 보안 그룹을 만듭니다.
8. [OpenStack Networking API v2.0](#) 또는 [Ansible](#) 을 사용하여 보안 그룹 규칙을 만듭니다.
9. [OpenStack Networking API v2.0](#) 또는 [Ansible](#) 을 사용하여 정의한 보안 그룹으로 포트를 업데이트합니다.
10. 선택 사항: 포트 수준에서 보안 기능이 활성화되었는지를 정의합니다. 현재는 [OpenStack Networking API](#) 만 사용할 수 있습니다. **port_security_enabled** 특성이 설정되지 않은 경우 기본적으로 해당 특성이 속한 네트워크에 지정된 값으로 설정됩니다.

2.4.4. 호스트 및 네트워킹

2.4.4.1. 네트워크 관리자 상태 저장 설정 (nmstate)

RHV(Red Hat Virtualization 4.4)에서는 NTP(*Network Manager Stateful Configuration*)를 사용하여 RHEL 8을 기반으로 하는 RHV 호스트에 대한 네트워킹을 구성합니다. RHV 버전 4.3 이상에서는 인터페이스 구성(ifcfg) 네트워크 스크립트를 사용하여 호스트 네트워킹을 관리합니다.

nmstate를 사용하려면 [RHV 업그레이드 가이드](#)에 설명된 대로 [Red Hat Virtualization Manager](#) 및 [호스트](#)를 업그레이드합니다.

관리자는 nmstate를 설치하거나 구성할 필요가 없습니다. 기본적으로 활성화되어 있으며 백그라운드에서 실행됩니다.



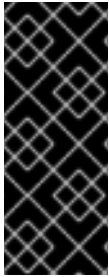
중요

항상 RHV Manager를 사용하여 클러스터에 있는 호스트의 네트워크 구성을 수정합니다. 그렇지 않으면 지원되지 않는 구성을 만들 수 있습니다.

nmstate로의 변경은 거의 투명합니다. 다음과 같은 방식으로 호스트 네트워킹을 구성하는 방법만 변경합니다.

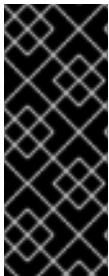
- 클러스터에 호스트를 추가한 후 항상 RHV Manager를 사용하여 호스트 네트워크를 수정합니다.
- Manager를 사용하지 않고 호스트 네트워크를 수정하면 지원되지 않는 구성이 생성될 수 있습니다.
- 지원되지 않는 구성을 수정하려면 Manager를 사용하여 호스트 네트워크를 동기화하여 지원되는 구성으로 바꿉니다. 자세한 내용은 호스트 네트워크 [동기화](#)를 참조하십시오.
- 관리자 외부에서 호스트 네트워크를 수정하는 유일한 상황은 호스트에서 정적 경로를 구성하는 것입니다. 자세한 내용은 [호스트에 정적 경로 추가](#)를 참조하십시오.

nmstate를 변경하면 Manager에 호스트를 추가하기 전에 RHV Manager에서 Cockpit 및 Anaconda에서 구성 변경 사항을 적용하는 방법이 향상되었습니다. 이는 [NM가 인터페이스를 관리하는 경우 호스트 배포에서 BZ#1680970 정적 IPv6 주소와 같은 몇 가지 문제가 해결되었습니다](#).

**중요**

dnf 또는 **yum** 을 사용하여 **nmstate** 패키지를 수동으로 업데이트하는 경우 호스트에서 **vdsmd** 및 **supervdsm** 를 다시 시작하십시오. 예를 들면 다음과 같습니다.

```
# dnf update nmstate
# systemctl restart vdsmd supervdsm
```

**중요**

dnf 또는 **yum** 을 사용하여 **Network Manager** 패키지를 수동으로 업데이트하는 경우 호스트에서 **NetworkManager** 를 다시 시작합니다. 예를 들면 다음과 같습니다.

```
# dnf update NetworkManager
# systemctl restart NetworkManager
```

2.4.4.2. 호스트 기능 새로 고침

네트워크 인터페이스 카드가 호스트에 추가되면 Manager에 해당 네트워크 인터페이스 카드를 표시하도록 호스트의 기능을 새로 고쳐야 합니다.

절차

1. **Compute → Hosts** (컴퓨팅 호스트)를 클릭하고 호스트를 선택합니다.
2. **Management(관리) Refresh capabilities(새로 고침 기능)** 를 클릭합니다.

선택한 호스트의 **Network Interfaces**(네트워크 인터페이스) 탭의 네트워크 인터페이스 카드 목록이 업데이트됩니다. 이제 Manager에서 새 네트워크 인터페이스 카드를 사용할 수 있습니다.

2.4.4.3. 호스트 네트워크 인터페이스 편집 및 호스트에 논리적 네트워크 할당

물리적 호스트 네트워크 인터페이스의 설정을 변경하고, 관리 네트워크를 하나의 물리적 호스트 네트워크 인터페이스에서 다른 물리적 호스트 네트워크 인터페이스로 이동하고, 논리적 네트워크를 물리적 호스트 네트워크 인터페이스에 할당할 수 있습니다. **bridge** 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 [VLAN 설정 편집](#) 을 참조하십시오.

**중요**

외부 프로바이더가 제공하는 논리적 네트워크를 물리적 호스트 네트워크 인터페이스에 할당할 수 없습니다. 이러한 네트워크는 가상 시스템에 필요하므로 호스트에 동적으로 할당됩니다.



참고

LLDP(링크 계층 검색 프로토콜) 정보를 제공하도록 스위치가 구성된 경우 실제 네트워크 인터페이스에 커서를 가리키면 스위치 포트의 현재 구성을 볼 수 있습니다. 이렇게 하면 잘못된 구성을 방지하는 데 도움이 될 수 있습니다. 논리적 네트워크를 할당하기 전에 다음 정보를 확인하십시오.

- 포트 설명(TLV 유형 4) 및 System Name(TLV 유형 5)은 호스트의 인터페이스가 패치된 포트와 스위치하는 포트를 감지하는 데 도움이 됩니다.
- 포트 VLAN ID는 태그되지 않은 이더넷 프레임의 스위치 포트에 구성된 기본 VLAN ID를 표시합니다. 스위치 포트에 구성된 모든 VLAN은 VLAN 이름 및 VLANID 조합으로 표시됩니다.

절차

1. Compute(컴퓨팅) Hosts(호스트) 를 클릭합니다.
2. 호스트 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. 네트워크 인터페이스 탭을 클릭합니다.
4. Setup Host Networks (호스트 네트워크 설정)를 클릭합니다.
5. 선택적으로, 커서를 호스트 네트워크 인터페이스로 이동하여 스위치에서 제공한 구성 정보를 확인합니다.
6. 논리적 네트워크를 선택하고 물리적 호스트 네트워크 인터페이스 옆의 Assigned Logical Networks(논리 네트워크 할당) 영역으로 끌어서 물리적 호스트 네트워크 인터페이스에 논리적 네트워크를 연결합니다.



참고

NIC가 논리적 네트워크에 연결되어 있는 경우 VLAN이 아닌 네트워크 중 하나만 있을 수 있습니다. 기타 모든 논리적 네트워크는 고유한 VLAN이어야 합니다.

7. 논리적 네트워크를 구성합니다.
 - a. 할당된 논리적 네트워크 위로 커서를 가리키고 연필 아이콘을 클릭합니다. 그러면 Edit Management Network (관리 네트워크 편집) 창이 열립니다.
 - b. IPv4 탭에서 None,DHCP 또는 Static 에서 Boot Protocol(부팅 프로토콜)을 선택합니다. Static (정적)을 선택한 경우 IP, Netmask / Routing Prefix(IP, 넷마스크/라우팅 접두사) 및 Gateway (게이트웨이)를 입력합니다.



참고

IPv6의 경우 정적 IPv6 주소 지정만 지원됩니다. 논리적 네트워크를 구성하려면 IPv6 탭을 선택하고 다음 항목을 만듭니다.

- 부팅 프로토콜을 정적으로 설정합니다.
- Routing Prefix의 경우 슬래시와 10진수를 사용하여 접두사길이를 입력합니다. 예: /48
- IP: 호스트 네트워크 인터페이스의 전체 IPv6 주소입니다. 예를 들면 다음과 같습니다. 2001:db8::1:0:0:6
- 게이트웨이: 소스 라우터의 IPv6 주소입니다. 예를 들면 다음과 같습니다. 2001:db8::1:0:0:1



참고

호스트의 관리 네트워크 IP 주소를 변경하는 경우 구성할 새 IP 주소를 위해 [호스트를 다시 설치해야](#) 합니다.

각 논리적 네트워크에는 관리 네트워크 게이트웨이에서 정의된 별도의 게이트웨이가 있을 수 있습니다. 이렇게 하면 관리 네트워크에서 사용하는 기본 게이트웨이 대신 논리적 네트워크의 게이트웨이를 사용하여 논리적 네트워크에 도달하는 트래픽이 전달됩니다.



중요

관리 네트워크에 동일한 IP 스택을 사용하도록 클러스터의 모든 호스트를 설정합니다(IPv4 또는 IPv6만 해당). 듀얼 스택은 지원되지 않습니다.

- c. QoS (QoS) 탭을 사용하여 서비스의 기본 호스트 네트워크 품질을 재정의합니다.Override QoS (QoS 재정의)를 선택하고 다음 필드에 원하는 값을 입력합니다.

- 가중치 공유: 동일한 논리적 링크에 연결된 다른 네트워크를 기준으로 특정 네트워크를 할당해야 하는 논리적 링크 용량의 양을 나타냅니다. 정확한 공유는 해당 링크의 모든 네트워크의 공유 합계에 따라 다릅니다. 기본적으로 1~100 범위의 숫자입니다.
- 속도 제한 [Mbps]: 네트워크에서 사용할 최대 대역폭입니다.
- 커밋 비율 [Mbps]: 네트워크에 필요한 최소 대역폭입니다. 요청된 커밋 비율은 보장되지 않으며 네트워크 인프라 및 동일한 논리적 링크의 다른 네트워크에서 요청한 커밋 비율에 따라 달라집니다.

- d. 네트워크 브리지를 구성하려면 Custom Properties(사용자 지정 속성) 탭을 클릭하고 드롭다운 목록에서 bridge_opts를 선택합니다. 다음 구문을 사용하여 유효한 키와 값을 입력합니다. key=value. 공백 문자를 사용하여 여러 항목을 구분합니다. 다음 키는 예제로 제공된 값을 사용하여 유효합니다. 이러한 매개변수에 대한 자세한 내용은 [bridge_opts Parameters 설명](#)을 참조하십시오.

```
forward_delay=1500
group_addr=1:80:c2:0:0:0
group_fwd_mask=0x0
hash_max=512
hello_time=200
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 구성하려면 Custom Properties(사용자 지정 속성) 탭을 클릭하고 드롭다운 목록에서 `ethtool_opts` 를 선택합니다. `ethtool`의 명령줄 인수 형식을 사용하여 유효한 값을 입력합니다. 예:

```

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

```

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

```

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

```

`ethtool_opts` 옵션은 기본적으로 사용할 수 없습니다. 엔진 구성 도구를 사용하여 추가해야 합니다. 자세한 내용은 [How to Set Up Manager to Use Ethtool](#)을 참조하십시오. `ethtool` 속성에 대한 자세한 내용은 명령줄에 `man ethtool` 을 입력하여 도움말 페이지를 참조하십시오.

- f. FCoE(Fibre Channel over Ethernet)를 구성하려면 Custom Properties(사용자 지정 속성) 탭을 클릭하고 드롭다운 목록에서 `fcoe` 를 선택합니다. 다음 구문을 사용하여 유효한 키와 값을 입력합니다. `key=value`. 최소 `enable=yes` 가 필요합니다. `dcb=[yes|no]` 및 `'auto_vlan=[yes|no]`를 추가할 수도 있습니다. 공백 문자를 사용하여 여러 항목을 구분합니다. `fcoe` 옵션은 기본적으로 사용할 수 없습니다. 엔진 구성 도구를 사용하여 추가해야 합니다. 자세한 내용은 [How to Set Up Manager to Use FCoE](#)를 참조하십시오.



참고

FCoE와 함께 사용하려면 별도의 전용 논리적 네트워크를 사용하는 것이 좋습니다.

- g. 호스트에서 사용하는 기본 네트워크를 관리 네트워크(`ovirtmgmt`)에서 비관리 네트워크로 변경하려면 비관리 네트워크의 기본 경로를 구성합니다. [자세한 내용은 기본 경로](#) 구성을 참조하십시오.
- h. 논리적 네트워크 정의가 호스트의 네트워크 구성과 동기화되지 않은 경우 Sync network (네트워크 동기화) 확인란을 선택합니다. 동기화되지 않은 호스트 및 동기화에 대한 자세한 내용은 [호스트 네트워크 동기화](#)를 참조하십시오.
8. Verify connectivity between Host and Engine(호스트와 엔진간 연결 확인) 확인란을 선택하여 네트워크 연결을 선택합니다. 이 작업은 호스트가 유지 관리 모드인 경우에만 작동합니다.
9. OK(확인)를 클릭합니다.



참고

호스트의 일부 네트워크 인터페이스 카드가 표시되지 않으면 Management(관리 → Refresh capabilities(새로 고침 기능))를 클릭하여 해당 호스트에 사용할 수 있는 네트워크 인터페이스 카드 목록을 업데이트합니다.

문제 해결

경우에 따라 Setup Host Networks(호스트 네트워크 설정) 창 또는 **setupNetwork** 명령을 사용하여 호스트 네트워크 구성을 여러 번 동시에 변경하면 **Operation(작업) 실패: [Cannot setup Networks]**(네트워크를 설정할 수 없음) 오류가 발생하는 경우도 있습니다. 호스트에서 또 다른 설정 네트워크 또는 호스트 새로 고침 프로세스가 진행 중입니다. 이벤트 로그에서 나중에 시도하십시오.] 오류. 이 오류는 일부 변경 사항이 호스트에 구성되지 않았음을 나타냅니다. 이러한 문제는 구성 상태의 무결성을 유지하기 위해 한 번에 단일 설정 **network** 명령만 처리할 수 있기 때문입니다. 다른 동시 구성 명령은 기본 제한 시간 20초까지 대기합니다. 위의 오류가 발생하지 않도록 하려면 **engine-config** 명령을 사용하여 **SetupNetworksWaitTimeoutSeconds**의 시간 제한을 20초 이상 늘립니다. 예를 들면 다음과 같습니다.

```
# engine-config --set SetupNetworksWaitTimeoutSeconds=40
```

추가 리소스

- [engine-config 명령 구문](#)
- [setupnetworks POST](#)

2.4.4.4. 호스트 네트워크 동기화

호스트의 인터페이스 정의가 Manager에 저장된 정의와 다를 때 Manager는 네트워크 인터페이스를 동기화 외부로 정의합니다.

비동기 네트워크는 호스트의 네트워크 인터페이스 탭과 함께 와 함께 비동기 아이콘 을(가) Setup Host Networks (호스트 네트워크 설정) 창에서 로 표시됩니다.

호스트의 네트워크가 동기화되지 않은 경우 Setup Host Networks(호스트 네트워크 설정) 창의 동기화되지 않은 네트워크에서 수행할 수 있는 유일한 활동은 네트워크 인터페이스에서 논리적 네트워크를 분리하거나 네트워크를 동기화하는 것입니다.

호스트가 동기화되지 않는 방법 이해

다음과 같은 경우 호스트가 동기화되지 않습니다.

- 다음과 같이 Edit Logical Networks(논리 네트워크 편집) 창을 사용하지 않고 호스트에서 구성을 변경합니다.
 - 물리적 호스트에서 VLAN 식별자 변경.
 - 물리적 호스트의 사용자 지정 MTU 변경.
- 동일한 네트워크 이름이 있지만 값/매개 변수를 사용하여 호스트를 다른 데이터 센터로 이동합니다.
- 호스트에서 브리지를 수동으로 제거하여 네트워크의 VM 네트워크 속성을 변경합니다.



중요

네트워크의 MTU 설정을 변경하는 경우 이 변경 사항을 네트워크에서 실행 중인 가상 머신으로 전파해야 합니다. MTU 설정을 적용하거나 가상 시스템을 다시 시작해야 하는 모든 가상 시스템의 vNIC의 핫플러그 및 재플러그. 그렇지 않으면 가상 시스템이 다른 호스트로 마이그레이션될 때 이러한 인터페이스가 실패합니다. 자세한 내용은 [네트워크 MTU가 변경된 후 일부 VM과 브리지에는 이전 MTU가 있으며 패킷 삭제와 BZ#1766414](#) 를 참조하십시오.

호스트 동기화되지 않음 방지

이러한 모범 사례를 따르면 호스트가 동기화되지 않도록 합니다.

1. 호스트에서 로컬로 변경하는 대신 관리 포털을 사용하여 변경합니다.
2. VLAN 설정 [편집 지침에 따라 VLAN](#) 설정을 편집합니다.

호스트 동기화

호스트의 네트워크 인터페이스 정의를 동기화하려면 Manager의 정의를 사용하여 호스트에 적용하는 작업이 포함됩니다. 필요한 정의가 아닌 경우 호스트를 동기화한 후 관리 포털에서 정의를 업데이트합니다. 호스트의 네트워크를 다음 세 수준에서 동기화할 수 있습니다.

- 논리적 네트워크당
- 호스트당
- 클러스터당

논리적 네트워크 수준에서 호스트 네트워크 동기화

1. Compute(컴퓨팅) Hosts(호스트) 를 클릭합니다.
2. 호스트 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. 네트워크 인터페이스 탭을 클릭합니다.
4. Setup Host Networks (호스트 네트워크 설정)를 클릭합니다.
5. 동기화되지 않은 네트워크 위로 커서를 가리키고 연필 아이콘을 클릭합니다. 그러면 Edit Network(네트워크 편집) 창이 열립니다.
6. Sync network(네트워크 동기화) 확인란을 선택합니다.
7. OK(확인)를 클릭하여 네트워크 변경 사항을 저장합니다.
8. OK(확인)를 클릭하여 Setup Host Networks(호스트 네트워크 설정) 창을 닫습니다.

호스트 수준에서 호스트의 네트워크 동기화

- 호스트의 Network Interfaces(네트워크 인터페이스) 탭에서 Sync All Networks(모든 네트워크 동기화) 버튼을 클릭하여 동기화되지 않은 모든 호스트의 네트워크 인터페이스를 동기화합니다.

클러스터 수준에서 호스트의 네트워크 동기화

- 클러스터의 Logical Networks(논리 네트워크) 탭에서 Sync All Networks(모든 네트워크 동기화) 버튼을 클릭하여 전체 클러스터에 대해 동기화되지 않은 모든 논리적 네트워크 정의를 동기화합니다.



참고

REST API를 통해 호스트의 네트워크를 동기화할 수도 있습니다. *REST API 가이드*의 [syncallnetworks](#) 를 참조하십시오.

2.4.4.5. 호스트의 VLAN 설정 편집

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

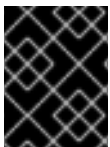
네트워킹을 동기화된 상태로 유지하려면 다음을 수행합니다.

1. 호스트를 유지 관리 모드로 설정합니다.
2. 호스트에서 관리 네트워크를 수동으로 제거합니다. 그러면 새 VLAN을 통해 호스트에 연결할 수 있습니다.
3. 클러스터에 호스트를 추가합니다. 관리 네트워크에 직접 연결되지 않은 가상 시스템은 호스트 간에 안전하게 마이그레이션할 수 있습니다.

관리 네트워크의 VLAN ID가 변경되면 다음 경고 메시지가 표시됩니다.

Changing certain properties (e.g. VLAN, MTU) of the management network could lead to loss of connectivity to hosts in the data center, if its underlying network infrastructure isn't configured to accommodate the changes. Are you sure you want to proceed?

계속 진행하면 데이터 센터의 모든 호스트가 Manager에 대한 연결이 끊어지고 호스트를 새 관리 네트워크로 마이그레이션하는 데 실패합니다. 관리 네트워크는 "out-of-sync"로 보고됩니다.

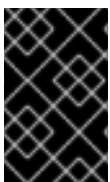


중요

관리 네트워크의 VLAN ID를 변경하는 경우 새 VLAN ID를 적용하려면 호스트를 다시 설치해야 합니다.

2.4.4.6. 논리적 네트워크를 사용하여 단일 네트워크 인터페이스에 여러 VLAN 추가

단일 네트워크 인터페이스에 여러 VLAN을 추가하여 한 호스트에서 트래픽을 분리할 수 있습니다.



중요

New Logical Network(새 논리적 네트워크) 또는 Edit Logical Network(논리 네트워크 편집) 창에서 모두 VLAN 태그 지정 활성화 확인란이 있는 논리적 네트워크를 두 개 이상 생성해야 합니다.

절차

1. Compute(컴퓨팅) Hosts(호스트)를 클릭합니다.
2. 호스트 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. 네트워크 인터페이스 탭을 클릭합니다.
4. Setup Host Networks(호스트 네트워크 설정)를 클릭합니다.

5. VLAN 태그가 지정된 논리적 네트워크를 물리적 네트워크 인터페이스 옆의 **Assigned Logical Networks**(할당 논리적 네트워크) 영역으로 끌어 옵니다. 실제 네트워크 인터페이스에 VLAN 태그 지정으로 인해 논리적 네트워크가 여러 개 할당될 수 있습니다.
6. 논리적 네트워크를 편집합니다.
 - a. 할당된 논리적 네트워크 위로 커서를 가리키고 연필 아이콘을 클릭합니다.
 - b. 논리적 네트워크 정의가 호스트의 네트워크 구성과 동기화되지 않은 경우 **Sync network** (네트워크 동기화) 확인란을 선택합니다.
 - c. 부팅 프로토콜 선택 :
 - 없음
 - DHCP
 - 고정
 - d. IP 및 서브넷 마스크를 제공합니다.
 - e. **OK(확인)**를 클릭합니다.
7. **Verify connectivity between Host and Engine**(호스트와 엔진 간 연결 확인) 확인란을 선택하여 네트워크 확인란을 실행합니다. 이는 호스트가 유지 관리 모드인 경우에만 작동합니다.
8. **OK(확인)**를 클릭합니다.

클러스터의 각 호스트에서 NIC를 편집하여 클러스터의 각 호스트에 논리적 네트워크를 추가합니다. 이 작업이 완료되면 네트워크가 작동합니다.

이 프로세스는 여러 번 반복하여 각 호스트에서 동일한 네트워크 인터페이스를 선택하고 편집하여 다양한 VLAN 태그가 있는 논리적 네트워크를 단일 네트워크 인터페이스에 추가할 수 있습니다.

2.4.4.6.1. 호스트 네트워크 복사

시간을 절약하기 위해 동일한 클러스터의 대상 호스트에 소스 호스트의 네트워크 구성을 복사할 수 있습니다.

네트워크 구성을 복사하는 작업은 다음과 같습니다.

- **ovirtmgmt** 관리 네트워크를 제외하고 호스트에 연결된 논리적 네트워크
- 인터페이스에 연결된 본딩

제한

- 고정 IP 주소가 포함된 네트워크 구성을 복사하지 마십시오. 이렇게 하면 대상 호스트의 부팅 프로토콜이 **none** 으로 설정됩니다.
- 소스 호스트와 동일한 인터페이스 이름을 사용하여 대상 호스트에 구성을 복사하면 다른 물리적 네트워크 연결에서 잘못된 구성이 생성됩니다.
- 대상 호스트에는 소스 호스트와 동일한 수 이상의 인터페이스가 있어야 합니다. 그렇지 않으면 작업이 실패합니다.
- **QoS, DNS 및 custom_properties** 복사는 지원되지 않습니다.

- 네트워크 인터페이스 레이블은 복사되지 않습니다.



주의

호스트 네트워크를 복사하면 **ovirtmgmt** 관리 네트워크에 대한 연결을 제외하고 대상 호스트의 모든 네트워크 설정이 대체됩니다.

사전 요구 사항

- 대상 호스트의 NIC 수는 소스 호스트의 수보다 같거나 커야 합니다. 그렇지 않으면 작업이 실패합니다.
- 호스트는 동일한 클러스터에 있어야 합니다.

절차

1. 관리 포털에서 **Compute → Hosts** (호스트) 를 클릭합니다.
2. 복사할 구성이 있는 소스 호스트를 선택합니다.
3. **Copy Host Networks** (호스트 네트워크 복사)를 클릭합니다. 그러면 **Copy Host Networks**(호스트 네트워크 복사) 창이 열립니다.
4. **Target Host**(대상 호스트)를 사용하여 구성을 수신해야 하는 호스트를 선택합니다. 목록에는 동일한 클러스터에 있는 호스트만 표시됩니다.
5. **Copy Host Networks** (호스트 네트워크 복사)를 클릭합니다.
6. 대상 호스트의 네트워크 설정을 확인합니다

팁

- 여러 호스트를 선택하면 **Copy Host Networks**(호스트 네트워크 복사) 버튼 및 컨텍스트 메뉴를 비활성화합니다.
- **Copy Host Networks**(호스트 네트워크 복사) 버튼을 사용하는 대신 호스트를 마우스 오른쪽 버튼으로 클릭하고 컨텍스트 메뉴에서 **Copy Host Networks**(호스트 네트워크 복사)를 선택할 수 있습니다.
- **Copy Host Networks**(호스트 네트워크 복사) 버튼은 모든 호스트의 세부 정보 보기에서도 사용할 수 있습니다.

2.4.4.7. 호스트 네트워크에 추가 IPv4 주소 할당

ovirtmgmt 관리 네트워크와 같은 호스트 네트워크는 처음 설정할 때 하나의 IP 주소만으로 생성됩니다. 즉, NIC의 구성 파일이 여러 IP 주소로 구성된 경우 첫 번째로 나열된 IP 주소만 호스트 네트워크에 할당됩니다. 스토리지에 연결하거나 동일한 NIC를 사용하는 별도의 사설 서브넷의 서버에 연결하는 경우 추가 IP 주소가 필요할 수 있습니다.

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

다음 절차에서는 추가 IP 주소를 구성하려는 각 호스트에서 호스트별 작업을 수행해야 합니다.

절차

1. 에 추가 IPv4 주소를 구성하려는 호스트에서 VDSM 후크 패키지를 설치합니다. 패키지는 기본적으로 Red Hat Virtualization 호스트에서 사용할 수 있지만 Red Hat Enterprise Linux 호스트에 설치해야 합니다.

```
# dnf install vdsd-hook-extra-ipv4-addr
```

2. Manager에서 다음 명령을 실행하여 키를 추가합니다.

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

3. ovirt-engine 서비스를 다시 시작하십시오.

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

4. 관리 포털에서 Compute → Hosts (호스트) 를 클릭합니다.
5. 호스트 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
6. Network Interfaces(네트워크 인터페이스) 탭을 클릭하고 Setup Host Networks(호스트 네트워크 설정)를 클릭합니다.
7. 할당된 논리적 네트워크를 가리키고 연필 아이콘을 클릭하여 호스트 네트워크 인터페이스를 편집합니다.
8. Custom Properties (사용자 지정 속성) 드롭다운 목록에서 ipv4_addr 을 선택하고 추가 IP 주소와 접두사(예: 5.5.5.5/24)를 추가합니다. 여러 IP 주소는 쉼표로 구분되어야 합니다.
9. OK(확인) 를 클릭하여 Edit Network(네트워크 편집) 창을 닫습니다.
10. OK(확인) 를 클릭하여 Setup Host Networks(호스트 네트워크 설정) 창을 닫습니다.

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

2.4.4.8. 호스트 네트워크 인터페이스에 네트워크 레이블 추가

네트워크 레이블을 사용하면 논리적 네트워크를 호스트 네트워크 인터페이스에 할당하는 것과 관련된 관리 워크로드를 크게 단순화할 수 있습니다. 역할 네트워크(예: 마이그레이션 네트워크 또는 디스플레이 네트워크)에서 레이블을 설정하면 모든 호스트에서 해당 네트워크를 대량으로 배포합니다. 이러한 네트워크 추가는 DHCP를 사용하여 수행됩니다. 이 대량 배포 방법은 많은 정적 IP 주소를 입력하는 작업의 확장 불가능한 특성 때문에 정적 주소를 입력하는 방법에 대해 선택되었습니다.

호스트 네트워크 인터페이스에 레이블을 추가하는 방법은 두 가지가 있습니다.

- 관리 포털에서 수동으로
- LLDP 라벨러 서비스를 사용하여 자동으로

절차

1. Compute(컴퓨팅) Hosts(호스트) 를 클릭합니다.

2. 호스트 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. 네트워크 인터페이스 탭을 클릭합니다.
4. **Setup Host Networks** (호스트 네트워크 설정)를 클릭합니다.
5. **Labels** (레이블)를 클릭하고 **[New Label]** 을 마우스 오른쪽 버튼으로 클릭합니다. 레이블을 지정할 물리적 네트워크 인터페이스를 선택합니다.
6. **Label** (레이블) 텍스트 필드에 네트워크 레이블의 이름을 입력합니다.
7. **OK**(확인)를 클릭합니다.

절차

LLDP Labeler 서비스를 사용하여 구성된 클러스터 목록에서 호스트 네트워크 인터페이스에 레이블을 할당하는 프로세스를 자동화할 수 있습니다.

2.4.4.8.1. LLDP 라벨러 구성

기본적으로 LLDP 레이블은 시간별 서비스로 실행됩니다. 이 옵션은 하드웨어(예: NIC, 스위치 또는 케이블)를 변경하거나 스위치 구성을 변경하는 경우 유용합니다.

사전 요구 사항

- 인터페이스는 Juniper 스위치에 연결되어야 합니다.
- Juniper 스위치는 LLDP를 사용하여 포트 **VLAN** 을 제공하도록 구성해야 합니다.

절차

1. `/etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf`에서 사용자 이름과 암호를 구성합니다.
 - **username** - Manager 관리자의 사용자 이름입니다. 기본값은 **admin@internal** 입니다.
 - **password** - 관리자 관리자의 암호입니다. 기본값은 **123456** 입니다.
2. `etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf`에서 다음 값을 업데이트하여 LLDP 레이블 서비스를 구성합니다.
 - - cluster** - 서비스를 실행해야 하는 쉼표로 구분된 클러스터 목록입니다. 와일드카드가 지원됩니다. 예를 들어 **Cluster*** 는 **Cluster** 라는 단어로 시작하는 모든 클러스터에서 실행할 LLDP 레이블 프로그램을 정의합니다. 데이터 센터의 모든 클러스터에서 서비스를 실행하려면 ***** 를 입력합니다. 기본값은 **Def*** 입니다.
 - - api_url** - 관리자 API의 전체 URL입니다. 기본값은 **https://Manager_FQDN/ovirt-engine/api**입니다.
 - - ca_file** - 사용자 정의 CA 인증서 파일의 경로입니다. 사용자 정의 인증서를 사용하지 않는 경우 이 값을 비워 둡니다. 기본값은 비어 있습니다.

- **auto_bonding** - LLDP 라벨러의 본딩 기능을 활성화합니다. 기본값은 **true**입니다.
 - **auto_labeling** - LLDP 라벨러의 레이블링 기능을 활성화합니다. 기본값은 **true**입니다.
3. 선택적으로 **etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-labeler.timer** 에서 **OnUnitActiveSec** 값을 변경하여 다른 간격으로 실행되도록 서비스를 구성할 수 있습니다. 기본값은 **1h** 입니다.
 4. 다음 명령을 입력하여 지금 및 부팅 시 서비스를 설정합니다.

```
# systemctl enable --now ovirt-lldp-labeler
```

서비스를 수동으로 호출하려면 다음 명령을 입력합니다.

```
# /usr/bin/python /usr/share/ovirt-lldp-labeler/ovirt_lldp_labeler_cli.py
```

호스트 네트워크 인터페이스에 네트워크 레이블을 추가했습니다. 동일한 레이블이 있는 새로 생성된 논리적 네트워크는 해당 레이블이 있는 모든 호스트 네트워크 인터페이스에 자동으로 할당됩니다. 논리적 네트워크에서 레이블을 제거하면 해당 레이블이 있는 모든 호스트 네트워크 인터페이스에서 해당 논리적 네트워크가 자동으로 제거됩니다.

2.4.4.9. 호스트의 FQDN 변경

다음 절차에 따라 호스트의 정규화된 도메인 이름을 변경합니다.

절차

1. 가상 시스템이 다른 호스트로 실시간 마이그레이션되도록 호스트를 유지 관리 모드로 전환합니다. 자세한 내용은 [호스트를 유지 관리 모드로 전환하기](#)를 참조하십시오. 또는 모든 가상 시스템을 수동으로 종료하거나 다른 호스트로 마이그레이션합니다. 자세한 내용은 [가상 머신 관리 가이드에서 가상 머신 수동 마이그레이션](#)을 참조하십시오.
2. **Remove(제거)**를 클릭하고 **OK(확인)**를 클릭하여 관리 포털에서 호스트를 제거합니다.
- 3.

hostnamectl 도구를 사용하여 호스트 이름을 업데이트합니다. 자세한 내용은 *Red Hat Enterprise Linux 7 네트워킹 가이드*의 [호스트 이름](#) 구성을 참조하십시오.

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

4.

호스트를 재부팅합니다.

5.

Manager를 사용하여 호스트를 다시 등록합니다. 자세한 내용은 [Manager에 표준 호스트 추가](#)를 참조하십시오.

2.4.4.9.1. IPv6 네트워킹 지원

Red Hat Virtualization은 대부분의 컨텍스트에서 정적 **IPv6** 네트워킹을 지원합니다.



참고

Red Hat Virtualization에서는 관리자를 실행 중인 컴퓨터 또는 가상 머신("관리자 시스템"이라고도 함)에서 **IPv6**를 사용하도록 유지해야 합니다. [시스템에서 IPv6를 사용하지 않더라도 Manager 시스템에서 IPv6를 비활성화](#) 하지 마십시오.

IPv6 제한 사항

- 정적 **IPv6** 주소 지정만 지원됩니다. **DHCP** 또는 상태 비저장 주소 자동 구성을 사용하는 동적 **IPv6** 주소는 지원되지 않습니다.
- 듀얼 스택 주소 지정, **IPv4** 및 **IPv6**는 지원되지 않습니다.
- **OVN** 네트워킹은 **IPv4** 또는 **IPv6**에서만 사용할 수 있습니다.
- 클러스터를 **IPv4**에서 **IPv6**로 전환하는 것은 지원되지 않습니다.
- 호스트당 단일 게이트웨이만 **IPv6**에 대해 설정할 수 있습니다.
- 두 네트워크에서 단일 게이트웨이(동일한 서브넷에 있음)를 공유하는 경우 기본 경로 역할을 관리 네트워크(**ovirtmgmt**)에서 다른 논리적 네트워크로 이동할 수 있습니다. 호스트와

Manager에는 동일한 **IPv6** 게이트웨이가 있어야 합니다. 호스트와 관리자가 동일한 서브넷에 있지 않으면 **IPv6** 게이트웨이가 제거되었으므로 **Manager**에서 호스트와의 연결이 끊어질 수 있습니다.

- **IPv6** 주소 지정 **Gluster** 서버와 함께 **gluster** 스토리지 도메인을 사용하는 것은 지원되지 않습니다.

2.4.4.9.2. SR-IOV 설정 및 구성

이 항목에는 **SR-IOV**를 설정하고 구성하는 단계가 요약되어 있으며 각 단계에 대해 자세히 다루는 링크와 함께 구성됩니다.

사전 요구 사항

SR-IOV 구현을 위한 하드웨어 고려사항에 따라 하드웨어 설정

절차

SR-IOV를 설정하고 구성하려면 다음 작업을 완료합니다.

1. **PCI 패스스루용 호스트 구성.**
2. **NIC에서 가상 기능 구성 편집.**
3. **vNIC 프로파일에서 패스스루 활성화.**
4. 마이그레이션 중에 네트워크 중단을 줄이기 위해 **SR-IOV-Enabled vNIC**를 사용하여 가상 머신 구성.

참고

- 'passthrough' vNIC의 수는 호스트에서 사용 가능한 **VF**(가상 기능) 수에 따라 다릅니다. 예를 들어 vNIC(**SR-IOV** 카드)가 3개 이상인 VM(가상 머신)을 실행하려면 호스트에 3개 이상의 **VF**가 활성화되어 있어야 합니다.
- 핫플러그 및 언플러그가 지원됩니다.

- 실시간 마이그레이션이 지원됩니다.
- VM을 마이그레이션하려면 대상 호스트에 VM을 받을 수 있는 충분한 VF가 있어야 합니다. 마이그레이션 중에 VM은 소스 호스트에서 다수의 VF를 해제하고 대상 호스트의 동일한 수의 VF를 차지합니다.
- 호스트에 다른 인터페이스와 마찬가지로 장치, 링크 또는 **ifcae**가 표시됩니다. 이 장치는 VM에 연결되면 사라지고 릴리스되면 다시 나타납니다.
- SR-IOV 기능을 위해 호스트 장치를 VM에 직접 연결하지 마십시오.
- 여러 VLAN이 있는 트렁크 포트에 VF를 사용하고 게스트 내에 VLAN을 구성하려면 가상 머신 내의 SR-IOV VF 인터페이스에서 VLAN을 구성할 수 없음을 참조하십시오.

인터페이스의 libvirt XML은 다음과 같은 예입니다.

```
----
<interface type='hostdev'>
  <mac address='00:1a:yy:xx:vv:xx'/>
  <driver name='vfio'/>
  <source>
    <address type='pci' domain='0x0000' bus='0x05' slot='0x10' function='0x0'/>
  </source>
  <alias name='ua-18400536-5688-4477-8471-be720e9efc68'/>
  <address type='pci' domain='0x0000' bus='0x00' slot='0x08' function='0x0'/>
</interface>
----
```

문제 해결

다음 예제에서는 인터페이스에 연결된 VF에 대한 진단 정보를 가져오는 방법을 보여줍니다.

```
# ip -s link show dev enp5s0f0
```

```
1: enp5s0f0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9000 qdisc mq state UP mode
DEFAULT qlen 1000
    link/ether 86:e2:ba:c2:50:f0 brd ff:ff:ff:ff:ff:ff
    RX: bytes  packets  errors  dropped  overrun  mcast
    30931671  218401  0      0      0      19165434
    TX: bytes  packets  errors  dropped  carrier  collsns
    997136    13661  0      0      0      0
```

```
vf 0 MAC 02:00:00:00:00:01, spoof checking on, link-state auto, trust off, query_rss off
vf 1 MAC 00:1a:4b:16:01:5e, spoof checking on, link-state auto, trust off, query_rss off
vf 2 MAC 02:00:00:00:00:01, spoof checking on, link-state auto, trust off, query_rss off
```

2.4.4.9.2.1. 추가 리소스

- **RHV VM에 대해 SR-IOV 패스스루를 구성하는 방법**
- **RHV에서 SR-IOV VF(Virtual Function)와의 본딩 구성 방법**
- **RHV의 가상 머신에 전용 가상 NIC를 할당할 수 있도록 호스트 장치 패스스루 및 SR-IOV를 활성화하는 방법**

2.4.5. 네트워크 연결

2.4.5.1. 본딩 방법

네트워크 본딩은 여러 **NIC**를 본딩 장치에 결합하고 다음과 같은 이점을 제공합니다.

- 본딩된 **NIC**의 전송 속도는 단일 **NIC**보다 큽니다.
- 네트워크 본딩은 모든 **NIC**가 실패하지 않는 한 본딩 장치가 실패하지 않으므로 내결함성을 제공합니다.

동일한 **make** 및 모델의 **NIC**를 사용하면 동일한 본딩 옵션 및 모드를 지원할 수 있습니다.

중요

Red Hat Virtualization의 기본 본딩 모드 (Mode 4) 동적 링크 집계에는 802.3ad를 지원하는 스위치가 필요합니다.

본딩의 논리적 네트워크는 호환 가능해야 합니다. 본딩은 VLAN이 아닌 논리적 네트워크 1개만 지원할 수 있습니다. 나머지 논리적 네트워크에는 고유한 VLAN ID가 있어야 합니다.

스위치 포트에 본딩을 활성화해야 합니다. 특정 지침은 스위치 벤더가 제공한 설명서를 참조하십시오.

다음 방법 중 하나를 사용하여 네트워크 본딩 장치를 생성할 수 있습니다.

- [관리 포털에서](#) 수동으로 특정 호스트
- 클러스터 또는 데이터 센터에 있는 모든 호스트의 연결되지 않은 NIC에 대해 [LLDP 라벨러](#)를 자동으로 사용합니다.

환경에서 iSCSI 스토리지를 사용하고 중복을 구현하려면 [iSCSI 다중 경로 구성](#) 지침을 따르십시오.

2.4.5.2. 관리 포털에서 본드 장치 생성

관리 포털의 특정 호스트에 본딩 장치를 생성할 수 있습니다. 본딩 장치는 VLAN 태그 지정 및 태그 지정되지 않은 트래픽을 모두 전송할 수 있습니다.

절차

1. **Compute(컴퓨팅) Hosts(호스트)** 를 클릭합니다.
2. 호스트 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Network Interfaces(네트워크 인터페이스)** 탭을 클릭하여 호스트에 연결된 실제 네트워크 인터페이스를 나열합니다.

4.

Setup Host Networks (호스트 네트워크 설정)를 클릭합니다.

5.

스위치 구성을 확인합니다. **LLDP**(링크 계층 검색 프로토콜) 정보를 제공하도록 스위치가 구성된 경우 물리적 **NIC**를 통해 커서를 가리키면 스위치 포트의 집계 구성을 확인합니다.

6.

NIC를 다른 **NIC** 또는 본딩으로 끌어다 놓습니다.



참고

두 개의 **NIC**는 새 본딩을 형성합니다. **NIC** 및 본딩은 **NIC**를 기존 본딩에 추가합니다.

논리적 네트워크가 **호환되지** 않으면 본딩 작업이 차단됩니다.

7.

드롭다운 메뉴에서 **Bond Name** (결합 이름) 및 **Bonding Mode** (결합 모드)를 선택합니다. 자세한 내용은 **본딩** 모드를 참조하십시오.

Custom bonding 모드를 선택하는 경우 다음 예와 같이 텍스트 필드에 본딩 옵션을 입력할 수 있습니다.

•

환경에서 **ethtool** 로 링크 상태를 보고하지 않는 경우 **mode=1 arp_interval= 1 arp_ip_target=192.168.0.2**를 입력하여 **ARP** 모니터링을 설정할 수 있습니다.

•

mode=1 primary=eth0 을 입력하여 더 높은 처리량으로 **NIC**를 기본 인터페이스로 지정할 수 있습니다.

본딩 옵션 및 해당 설명에 대한 포괄적인 목록은 Kernel.org의 [Linux Ethernet Bonding Driver HOWTO](#)를 참조하십시오.

8.

OK(확인)를 클릭합니다.

9.

새 본딩에 논리적 네트워크를 연결하고 구성합니다. 자세한 내용은 **호스트 네트워크 인터페이스 편집** 및 **호스트에 논리적 네트워크 할당**을 참조하십시오.



참고

논리적 네트워크를 본딩의 개별 **NIC**에 직접 연결할 수 없습니다.

10.

선택적으로 호스트가 유지 관리 모드인 경우 **Verify connectivity between Host and Engine**(호스트와 엔진 간 연결 확인)을 선택할 수 있습니다.

11.

OK(확인)를 클릭합니다.

2.4.5.3. LLDP 라벨러 서비스를 사용하여 본드 장치 생성

LLDP 레이블 서비스를 사용하면 하나 이상의 클러스터 또는 전체 데이터 센터에 있는 모든 호스트에 대해 결합되지 않은 모든 **NIC**를 사용하여 본딩 장치를 자동으로 생성할 수 있습니다. 본딩 모드는 **(Mode 4) 동적 링크 집계(802.3ad)**입니다.

호환되지 않는 논리적 네트워크가 있는 **NIC**는 결합할 수 없습니다.

2.4.5.3.1. LLDP 라벨러 구성

기본적으로 **LLDP** 레이블은 시간별 서비스로 실행됩니다. 이 옵션은 하드웨어(예: **NIC**, 스위치 또는 케이블)를 변경하거나 스위치 구성을 변경하는 경우 유용합니다.

사전 요구 사항

- 인터페이스는 **Juniper** 스위치에 연결되어야 합니다.
- **LLDP**를 사용하여 **LACP**(링크 집계 제어 프로토콜)에 대해 **Juniper** 스위치를 구성해야 합니다.

절차

1.

`/etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf`에서 사용자 이름과 암호를 구성합니다.

- **username - Manager** 관리자의 사용자 이름입니다. 기본값은 **admin@internal**입니다.

- **password** - 관리자 관리자의 암호입니다. 기본값은 **123456** 입니다.
2. **etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-credentials.conf**에서 다음 값을 업데이트하여 **LLDP** 레이블 서비스를 구성합니다.
- **cluster** - 서비스를 실행해야 하는 쉼표로 구분된 클러스터 목록입니다. 와일드카드가 지원됩니다. 예를 들어 **Cluster*** 는 **Cluster** 라는 단어로 시작하는 모든 클러스터에서 실행할 **LLDP** 레이블 프로그램을 정의합니다. 데이터 센터의 모든 클러스터에서 서비스를 실행하려면 ***** 를 입력합니다. 기본값은 **Def*** 입니다.
 - **api_url** - 관리자 **API**의 전체 **URL**입니다. 기본값은 **https://Manager_FQDN/ovirt-engine/api**입니다.
 - **ca_file** - 사용자 정의 **CA** 인증서 파일의 경로입니다. 사용자 정의 인증서를 사용하지 않는 경우 이 값을 비워 둡니다. 기본값은 비어 있습니다.
 - **auto_bonding** - **LLDP** 라벨러의 본딩 기능을 활성화합니다. 기본값은 **true**입니다.
 - **auto_labeling** - **LLDP** 라벨러의 레이블링 기능을 활성화합니다. 기본값은 **true**입니다.
3. 선택적으로 **etc/ovirt-lldp-labeler/conf.d/ovirt-lldp-labeler.timer** 에서 **OnUnitActiveSec** 값을 변경하여 다른 간격으로 실행되도록 서비스를 구성할 수 있습니다. 기본값은 **1h** 입니다.
4. 다음 명령을 입력하여 지금 및 부팅 시 서비스를 설정합니다.
- ```
systemctl enable --now ovirt-lldp-labeler
```
- 서비스를 수동으로 호출하려면 다음 명령을 입력합니다.
- ```
# /usr/bin/python /usr/share/ovirt-lldp-labeler/ovirt_lldp_labeler_cli.py
```
1. 새 본딩에 논리적 네트워크를 연결하고 구성합니다. 자세한 내용은 [호스트 네트워크 인터페이스](#)

이스 편집 및 호스트에 논리적 네트워크 할당을 참조하십시오.



참고

논리적 네트워크를 본당의 개별 **NIC**에 직접 연결할 수 없습니다.

2.4.5.4. 본딩 모드

패킷 디스퍼스 알고리즘은 본딩 모드로 결정됩니다. (자세한 내용은 [Linux 이더넷 본딩 드라이버 HOWTO](#) 참조). Red Hat Virtualization의 기본 본딩 모드는 (Mode 4) Dynamic Link Aggregation(802.3ad)입니다.

Red Hat Virtualization은 가상 머신(bridged) 네트워크에서 사용할 수 있으므로 다음과 같은 결합 모드를 지원합니다.

(모드 1) Active-Backup

하나의 **NIC**가 활성화되어 있습니다. 활성 **NIC**가 실패하면 백업 **NIC** 중 하나가 본당의 유일한 활성 **NIC**로 교체됩니다. 이 본당의 **MAC** 주소는 네트워크 어댑터 포트에만 표시됩니다. 이렇게 하면 새 활성 **NIC**의 **MAC** 주소를 반영하여 본당의 **MAC** 주소가 변경되면 발생할 수 있는 **MAC** 주소 혼동이 방지됩니다.

(Mode 2) 로드 밸런서(balance-xor)

소스 **MAC** 주소와 대상 **MAC** 주소에서 **XOR** 작업을 수행하여 패킷을 전송하는 **NIC**를 총 **NIC** 수의 모듈로 곱합니다. 이 알고리즘을 사용하면 각 대상 **MAC** 주소에 대해 동일한 **NIC**를 선택할 수 있습니다.

(모드 3) 방송

패킷이 모든 **NIC**로 전송됩니다.

(모드 4) 동적 링크 집계(802.3ad) (기본값)

NIC는 동일한 속도 및 이중 설정을 공유하는 그룹으로 집계됩니다. 활성 집계 그룹의 모든 **NIC**가 사용됩니다.

참고

(모드 4) 동적 링크 집계(802.3ad)에는 802.3ad를 지원하는 스위치가 필요합니다.

본딩된 NIC에는 동일한 집계기 ID가 있어야 합니다. 그렇지 않으면 Manager가 Network Interfaces(네트워크 인터페이스) 탭의 본딩에 경고 느낌표 아이콘을 표시하고 본딩의 ad_partner_mac 값은 00:00:00:00:00:00 으로 보고됩니다. 다음 명령을 입력하여 집계기 ID를 확인할 수 있습니다.

```
# cat /proc/net/bonding/bond0
```

가상 머신 게스트 또는 컨테이너가 연결되는 브리지와 함께 사용할 때 Which 본딩 모드가 작동합니다.?

다음 본딩 모드는 가상 머신 논리적 네트워크와 호환되지 않으므로 이러한 모드를 사용하여 VM이 아닌 논리적 네트워크만 본딩에 연결할 수 있습니다.

(Mode 0) 라운드 로빈

NIC는 패킷을 순차적으로 전송합니다. 본딩에서 처음 사용 가능한 NIC로 패킷이 전송되고 본딩에서 마지막 사용 가능한 NIC로 끝납니다. 후속 반복문은 사용 가능한 첫 번째 NIC로 시작합니다.

(모드 5) Balance-TLB, Transmit Load-Balance라고도 합니다.

나가는 트래픽은 본딩의 모든 NIC를 통해 부하를 기반으로 분산됩니다. 들어오는 트래픽은 활성 NIC에서 수신합니다. 들어오는 트래픽을 수신하는 NIC가 실패하면 다른 NIC가 할당됩니다.

(Mode 6) Balance-ALB, Adaptive Load-Balance라고도 함

(모드 5) Balance-TLB 는 IPv4 트래픽에 대한 수신 부하 분산과 결합됩니다. ARP 협상은 수신 부하의 균형을 조정하는 데 사용됩니다.

2.5. 호스트

2.5.1. 호스트 소개

하이퍼바이저라고도 하는 호스트는 가상 시스템이 실행되는 물리 서버입니다. 전체 가상화는 KVM(커널 기반 가상 시스템)이라는 로드 가능한 Linux 커널 모듈을 사용하여 제공됩니다.

KVM은 Windows 또는 Linux 운영 체제를 실행하는 여러 가상 시스템을 동시에 호스팅할 수 있습니다. 가상 시스템은 호스트 시스템에서 개별 Linux 프로세스 및 스레드로 실행되며 Red Hat Virtualization Manager에서 원격으로 관리합니다. Red Hat Virtualization 환경에는 하나 이상의 호스트가 연결되어 있습니다.

Red Hat Virtualization에서는 두 가지 호스트 설치 방법을 지원합니다. RHVH(Red Hat Virtualization Host) 설치 미디어를 사용하거나 표준 Red Hat Enterprise Linux 설치 시 하이퍼바이저 패키지를 설치할 수 있습니다.



참고

Red Hat Virtualization Manager에서 호스트 이름을 선택하여 개별 호스트의 호스트 유형을 식별할 수 있습니다. 그러면 세부 정보 보기가 열립니다. 그런 다음 **Software** (소프트웨어)에서 **OS Description(OS 설명)**을 확인합니다.

호스트는 가상화 최적화를 제공하는 **tuned** 프로필을 사용합니다. **tuned**에 대한 자세한 내용은 *Red Hat Enterprise Linux 모니터링 및 시스템 상태 및 성능 관리*에서 **TuneD 프로필**을 참조하십시오.

Red Hat Virtualization Host에는 보안 기능이 활성화되어 있습니다. SELinux(Security Enhanced Linux) 및 방화벽은 기본적으로 완전히 구성되어 있습니다. 선택한 호스트의 SELinux 상태는 세부 정보 보기의 **General(일반)** 탭의 SELinux 모드에서 보고됩니다. 관리자는 Red Hat Enterprise Linux 호스트에서 해당 포트를 환경에 추가할 때 필요한 포트를 열 수 있습니다.

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

Red Hat Virtualization 플랫폼의 물리적 호스트:

- 은 시스템의 클러스터에만 속해야 합니다.
- AMD-V 또는 Intel VT 하드웨어 가상화 확장 기능을 지원하는 CPU가 있어야 합니다.
- 클러스터 생성 시 가상 CPU 유형에 의해 노출되는 모든 기능을 지원하는 CPU가 있어야 합니다.

- 에는 최소 2GB RAM이 있습니다.
- 시스템 권한이 있는 할당된 시스템 관리자가 있을 수 있음.

관리자는 **Red Hat Virtualization** 감시 목록에서 최신 보안 공지를 받을 수 있습니다. 이메일로 **Red Hat Virtualization** 제품에 대한 새 보안 공지를 받으려면 **Red Hat Virtualization** 감시 목록에 가입하십시오. 이 양식을 작성하여 구독하십시오.

<https://www.redhat.com/mailman/listinfo/rhsa-announce>

2.5.2. Red Hat Virtualization Host

RHVH(Red Hat Virtualization Host)는 가상 시스템을 호스팅하는 데 필요한 패키지만 포함하는 특수 **Red Hat Enterprise Linux** 빌드를 사용하여 설치됩니다. **Red Hat Enterprise Linux** 호스트에서 사용하는 인터페이스를 기반으로 **Anaconda** 설치 인터페이스를 사용하며 **Red Hat Virtualization Manager** 또는 **yum** 을 통해 업데이트할 수 있습니다. **yum** 명령을 사용하면 추가 패키지를 설치하고 업그레이드 후에도 지속되도록 할 수 있습니다.

RHVH에는 호스트의 리소스를 모니터링하고 관리 작업을 수행하기 위한 **Cockpit** 웹 인터페이스가 있습니다. **SSH** 또는 콘솔을 통해 **RHVH**에 직접 액세스하는 것은 지원되지 않으므로 **Cockpit** 웹 인터페이스는 호스트가 **Red Hat Virtualization Manager**에 추가되기 전에 수행되는 작업에 대한 그래픽 사용자 인터페이스를 제공합니다(예: 터미널 하위 탭을 통한 네트워킹 구성 또는 터미널 명령 실행).

웹 브라우저의 <https://HostFQDNorIP:9090>에서 **Cockpit** 웹 인터페이스에 액세스합니다. **RHVH**용 **Cockpit**에는 호스트 상태, **SSH** 호스트 키, 자체 호스팅 엔진 상태, 가상 시스템 및 가상 시스템 통계를 표시하는 사용자 지정 가상화 대시보드가 포함되어 있습니다.

Red Hat Virtualization 버전 4.4 SP1부터 **RHVH**에서는 **systemd-coredump** 를 사용하여 코어 덤프를 수집, 저장 및 처리합니다. 자세한 내용은 [코어 덤프 스토리지 구성 파일](#) 및 [systemd-coredump 서비스](#) 설명서를 참조하십시오.

Red Hat Virtualization 4.4 및 이전 **RHVH**에서는 **ABRT(Automatic Bug Reporting Tool)**를 사용하여 애플리케이션 충돌에 대한 의미 있는 디버그 정보를 수집합니다. 자세한 내용은 [Red Hat Enterprise Linux 시스템 관리자 가이드를 참조하십시오](#).



참고

grubby 툴을 사용하여 사용자 지정 부팅 커널 인수를 **Red Hat Virtualization Host**에 추가할 수 있습니다. **grubby** 도구는 **grub.cfg** 파일을 영구적으로 변경합니다. 호스트의 **Cockpit** 웹 인터페이스에서 **Terminal** (터미널) 하위 탭으로 이동하여 **grubby** 명령을 사용합니다. 자세한 내용은 [Red Hat Enterprise Linux 시스템 관리자 가이드](#)를 참조하십시오.



주의

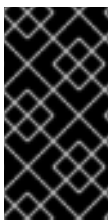
RHVH에서 신뢰할 수 없는 사용자를 생성하지 마십시오. 이로 인해 로컬 보안 취약점이 악용될 수 있습니다.

2.5.3. Red Hat Enterprise Linux 호스트

가능 하드웨어에 **Red Hat Enterprise Linux 7** 설치를 호스트로 사용할 수 있습니다. **Red Hat Virtualization**은 **Intel VT** 또는 **AMD-V** 확장 기능을 통해 **Red Hat Enterprise Linux 7 Server AMD64/Intel 64** 버전을 실행하는 호스트를 지원합니다. **Red Hat Enterprise Linux** 시스템을 호스트로 사용하려면 **Red Hat Enterprise Linux Server** 및 **Red Hat Virtualization** 서브스크립션도 연결해야 합니다.

가상화 확인, 패키지 설치 및 브리지 생성과 같이 다음 단계를 플랫폼에서 완료하므로 호스트를 추가하는 데 다소 시간이 걸릴 수 있습니다. 세부 정보 보기를 사용하여 호스트 및 관리 시스템에서 연결을 설정할 때 프로세스를 모니터링합니다.

선택적으로 호스트의 리소스를 모니터링하고 관리 작업을 수행하기 위해 **Cockpit** 웹 인터페이스를 설치할 수 있습니다. **Cockpit** 웹 인터페이스는 호스트가 **Red Hat Virtualization Manager**에 추가되기 전에 수행되는 작업에 대한 그래픽 사용자 인터페이스를 제공합니다(예: 네트워킹 구성 또는 터미널 명령 실행) 하위 탭을 통해.



중요

타사 위치독은 **VDSM**에서 제공하는 위치독 데몬을 방해할 수 있으므로 **Red Hat Enterprise Linux** 호스트에 설치해서는 안 됩니다.

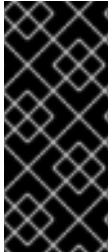
2.5.4. Satellite 호스트 공급자 호스트

Satellite 호스트 프로바이더가 제공하는 호스트는 **Red Hat Virtualization Manager**에서 가상화 호스

트로 사용할 수도 있습니다. **Satellite** 호스트 프로바이더를 외부 프로바이더로 **Manager**에 추가한 후에는 **RHVH(Red Hat Virtualization Hosts)** 및 **Red Hat Enterprise Linux** 호스트와 동일한 방식으로 제공하는 모든 호스트를 **Red Hat Virtualization**에 추가하고 사용할 수 있습니다.

2.5.5. 호스트 작업

2.5.5.1. Red Hat Virtualization Manager에 표준 호스트 추가



중요

항상 **RHV Manager**를 사용하여 클러스터에 있는 호스트의 네트워크 구성을 수정합니다. 그렇지 않으면 지원되지 않는 구성을 만들 수 있습니다. 자세한 내용은 [Network Manager Stateful Configuration\(nmstate\)](#) 을 참조하십시오.

Red Hat Virtualization 환경에 호스트를 추가하는 데는 가상화 점검, 패키지 설치 및 브리지 생성과 같은 플랫폼에서 다음 단계를 완료하므로 다소 시간이 걸릴 수 있습니다.

절차

1. 관리 포털에서 **Compute** → **Hosts (호스트)** 를 클릭합니다.
2. **New (새로 만들기)**를 클릭합니다.
3. 드롭다운 목록을 사용하여 새 호스트의 **Data Center** (데이터 센터) 및 **Host Cluster**(호스트 클러스터) 를 선택합니다.
4. 새 호스트의 **Name** (이름) 및 **Address** (주소)를 입력합니다. 표준 **SSH** 포트인 **port 22**는 **SSH Port(SSH 포트)** 필드에 자동으로 채워집니다.
5. **Manager(관리자)**에 사용할 인증 방법을 선택하여 호스트에 액세스합니다.
 - 암호 인증을 사용하려면 **root** 사용자의 암호를 입력합니다.
 - 또는 **SSH PublicKey** 필드에 표시된 키를 호스트의 **/root/.ssh/authorized_keys** 에 복사하여 공개 키 인증을 사용합니다.

6.

선택적으로 **Advanced Parameters**(고급 매개 변수) 버튼을 클릭하여 다음 고급 호스트 설정을 변경합니다.

●

자동 방화벽 구성을 비활성화합니다.

●

호스트 **SSH** 지문을 추가하여 보안을 강화합니다. 수동으로 추가하거나 자동으로 가져올 수 있습니다.

7.

선택적으로 호스트에 지원되는 전원 관리 카드가 있는 전원 관리를 구성합니다. 전원 관리 구성에 대한 자세한 내용은 [관리 가이드에 설명된 호스트 전원 관리 설정을 참조하십시오](#).

8.

OK(확인)를 클릭합니다.

새 호스트는 **Installing** (설치 중) 상태로 호스트 목록에 표시되며 **Notification Drawer** (



알림)의 **Events** (이벤트) 섹션에서 설치 진행 상황을 볼 수 있습니다. 잠시 지연된 후 호스트 상태가 **Up** 으로 변경됩니다.

2.5.5.2. Satellite 호스트 공급자 호스트 추가

Satellite 호스트 프로바이더 호스트를 추가하는 프로세스는 관리자에서 호스트를 식별하는 방법을 제외하고 **Red Hat Enterprise Linux** 호스트를 추가하는 프로세스와 거의 동일합니다. 다음 절차에서는 **Satellite** 호스트 프로바이더에서 제공하는 호스트를 추가하는 방법을 간략하게 설명합니다.

절차

1.

Compute(컴퓨팅) **Hosts**(호스트) 를 클릭합니다.

2.

New (새로 만들기)를 클릭합니다.

3.

드롭다운 메뉴를 사용하여 새 호스트의 호스트 클러스터 를 선택합니다.

4.

Foreman/Satellite (Foreman/Satellite) 확인란을 선택하여 **Satellite** 호스트 프로바이더 호스트를 추가하는 옵션을 표시하고 호스트를 추가할 프로바이더를 선택합니다.

5.

Discovered Hosts(검색된 호스트) 또는 **Provisioned Hosts** (프로비저닝된 호스트)를 선택합니다.

•

검색된 호스트 (기본 옵션): 드롭다운 목록에서 호스트, 호스트 그룹 및 컴퓨팅 리소스를 선택합니다.

•

프로비저닝된 호스트: **Providers Hosts**(공급업체 호스트) 드롭다운 목록에서 호스트를 선택합니다.

외부 프로바이더에서 검색할 수 있는 호스트와 관련된 모든 세부 정보는 자동으로 설정되며 원하는 대로 편집할 수 있습니다.

6.

새 호스트의 이름 및 **SSH 포트** (프로비저닝된 호스트만 해당)를 입력합니다.

7.

호스트에서 사용할 인증 방법을 선택합니다.

•

암호 인증을 사용하려면 **root** 사용자의 암호를 입력합니다.

•

공개 키 인증을 사용하도록 **SSH PublicKey** 필드에 표시된 키를 호스트의 `/root/.ssh/authorized_hosts` 에 복사합니다(프로비저닝된 호스트만 해당).

8.

이제 **Red Hat Enterprise Linux** 호스트를 추가하는 필수 단계를 완료했습니다. **Advanced Parameters** (고급 매개 변수) 드롭다운 버튼을 클릭하여 고급 호스트 설정을 표시합니다.

a.

선택적으로 자동 방화벽 구성을 비활성화합니다.

b.

선택적으로 호스트 **SSH** 지문을 추가하여 보안을 강화합니다. 수동으로 추가하거나 자동으로 가져올 수 있습니다.

9.

지금 해당하는 탭을 사용하여 전원 관리, **SPM**, 콘솔 및 네트워크 공급자를 구성할 수 있습니다. 그러나 **Red Hat Enterprise Linux** 호스트를 추가하는 것은 기본이 아니기 때문에 이 절차에서는 다루지 않습니다.

10.

OK(확인)를 클릭하여 호스트를 추가하고 창을 닫습니다.

새 호스트가 **Installing**(설치 중) 상태로 호스트 목록에 표시되고 세부 정보 보기에서 설치 진행 상황을 볼 수 있습니다. 설치가 완료되면 상태가 **Reboot** (재부팅)로 업데이트됩니다. 상태가 **Up** 으로 변경되면 호스트를 활성화해야 합니다.

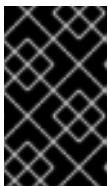
2.5.5.3. 호스트의 **Satellite** 에라타 보기 설정

관리 포털에서는 **Red Hat Satellite**에서 에라타를 볼 수 있도록 호스트를 구성할 수 있습니다. 호스트를 **Red Hat Satellite** 공급자와 연결한 후 사용 가능한 에라타 및 중요성에 대한 호스트 구성 대시보드의 업데이트를 수신하고 업데이트를 적용할 시기를 결정할 수 있습니다.

Red Hat Virtualization 4.4에서는 **Red Hat Satellite 6.6**으로 에라타 보기를 지원합니다.

사전 요구 사항

- **Satellite** 서버를 외부 프로바이더로 추가해야 합니다.
- 에라타를 보고자 하는 **Manager**(관리자)와 모든 호스트는 해당 **FQDN**을 통해 **Satellite** 서버에 등록해야 합니다. 이렇게 하면 **Red Hat Virtualization**에서 외부 콘텐츠 호스트 ID를 유지 관리할 필요가 없습니다.



중요

IP 주소를 사용하여 추가된 호스트는 에라타를 보고할 수 없습니다.

- 호스트를 관리하는 **Satellite** 계정에는 관리자 권한과 기본 조직 세트가 있어야 합니다.
- 호스트를 **Satellite** 서버에 등록해야 합니다.
- **Red Hat Satellite** 원격 실행을 사용하여 호스트의 패키지 관리.



참고

Katello 에이전트는 더 이상 사용되지 않으며 향후 **Satellite** 버전에서 제거됩니다. 프로세스를 마이그레이션하여 원격 실행 기능을 사용하여 클라이언트를 원격으로 업데이트합니다.

절차

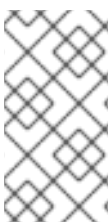
1. **Compute**(컴퓨팅) → **Hosts**(호스트) 를 클릭하고 호스트를 선택합니다.
2. **Edit**(편집)를 클릭합니다.
3. **Use Foreman/Satellite**(Foreman/Satellite 사용) 확인란을 선택합니다.
4. 드롭다운 목록에서 필수 **Satellite** 서버를 선택합니다.
5. **OK**(확인)를 클릭합니다.

호스트는 이제 호스트 구성을 관리하는 데 사용되는 것과 동일한 대시보드에 사용 가능한 에라타와 그 중요성이 표시되도록 구성됩니다.

추가 리소스

- [호스트 프로비저닝을 위한 Red Hat Satellite 인스턴스 추가](#)
- [Red Hat Satellite 문서 관리 호스트 관리 문서의 Goferd 및 Katello Agent를 사용하지 않는 호스트 관리](#)

2.5.5.3.1. PCI 패스스루에 대한 호스트 구성



참고

이는 **Red Hat Virtualization**에서 **SR-IOV**를 설정하고 구성하는 방법을 보여주는 일련의 주제 중 하나입니다. 자세한 내용은 [SR-IOV 설정 및 구성](#)을 참조하십시오.

PCI 패스스루를 활성화하면 가상 머신에서 장치가 가상 머신에 직접 연결된 것처럼 호스트 장치를 사용할 수 있습니다. **PCI** 통과 기능을 활성화하려면 가상화 확장 및 **IOMMU** 기능을 활성화해야 합니다. 다음 절차에 따라 호스트를 재부팅해야 합니다. 호스트가 이미 **Manager**에 연결되어 있는 경우 먼저 호스트를 유지 관리 모드에 배치해야 합니다.

사전 요구 사항

- 호스트 하드웨어가 **PCI** 장치 패스스루 및 할당에 대한 요구 사항을 충족하는지 확인합니다. 자세한 내용은 **PCI 장치 요구 사항**을 참조하십시오.

PCI 패스스루에 대한 호스트 구성

1. **BIOS**에서 가상화 확장 및 **IOMMU** 확장 활성화. 자세한 내용은 *Red Hat Enterprise Linux Virtualization Deployment and Administration Guide*의 **BIOS에서 Intel VT-x 및 AMD-V 가상화 하드웨어 확장 활성화**를 참조하십시오.
2. **Manager**에 호스트를 추가하거나 **grub** 구성 파일을 수동으로 편집할 때 **Hostdev Passthrough & SR-IOV** 확인란을 선택하여 커널에서 **IOMMU** 플래그를 활성화합니다.
 - 관리 포털에서 **IOMMU** 플래그를 활성화하려면 **Red Hat Virtualization Manager** 및 **Kernel Settings**에 표준 호스트 추가를 참조하십시오.
 - **grub** 구성 파일을 수동으로 편집하려면 **IOMMU 수동 활성화**를 참조하십시오.
3. **GPU** 패스스루의 경우 호스트 및 게스트 시스템 둘 다에서 추가 구성 단계를 실행해야 합니다. **GPU** 장치 통과를 참조하십시오. 자세한 내용은 *Red Hat Virtualization*의 가상 머신용 **NVIDIA GPU 설정**에서 단일 가상 머신에 호스트 **GPU** 할당

수동으로 IOMMU 활성화

1. **grub** 구성 파일을 편집하여 **IOMMU**를 활성화합니다.



참고

IBM POWER8 하드웨어를 사용하는 경우 기본적으로 **IOMMU**가 활성화되므로 이 단계를 건너뛰십시오.

- Intel의 경우 시스템을 부팅하고 **grub** 구성 파일의 **GRUB_CMDLINE_LINUX** 행 끝에 **intel_iommu=on** 을 추가합니다.

```
# vi /etc/default/grub
...
GRUB_CMDLINE_LINUX="nofb splash=quiet console=tty0 ... intel_iommu=on
...
```

- AMD의 경우 시스템을 부팅하고 **grub** 구성 파일의 **GRUB_CMDLINE_LINUX** 행 끝에 **amd_iommu=on** 을 추가합니다.

```
# vi /etc/default/grub
...
GRUB_CMDLINE_LINUX="nofb splash=quiet console=tty0 ... amd_iommu=on
...
```

참고

intel_iommu=on 또는 **AMD IOMMU**가 감지되면 **add iommu=pt** 를 사용해 볼 수 있습니다. **pt** 옵션은 **passthrough**에 사용되는 장치에만 **IOMMU**를 활성화하고 호스트 성능을 향상시킵니다. 그러나 모든 하드웨어에서 옵션이 지원되지 않을 수 있습니다. **pt** 옵션이 호스트에 대해 작동하지 않는 경우 이전 옵션으로 되돌립니다.

하드웨어가 인터럽트 다시 매핑을 지원하지 않기 때문에 패스스루가 실패하면 가상 시스템을 신뢰하는 경우 **allow_unsafe_interrupts** 옵션을 활성화하는 것이 좋습니다. **allow_unsafe_interrupts**는 기본적으로 활성화되어 있지 않습니다. 활성화하면 호스트를 가상 시스템의 **MSI** 공격에 노출할 수 있기 때문입니다. 옵션을 활성화하려면 다음을 수행합니다.

```
# vi /etc/modprobe.d
options vfio_iommu_type1 allow_unsafe_interrupts=1
```

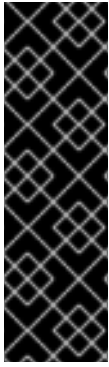
2.

grub.cfg 파일을 새로 고치고 호스트를 재부팅하여 이러한 변경 사항을 적용합니다.

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

```
# reboot
```

2.5.5.3.2. 모든 가상 머신에 중첩된 가상화 활성화



중요

후크를 사용하여 중첩된 가상화를 활성화하는 것은 기술 프리뷰 기능입니다. 기술 프리뷰 기능은 **Red Hat** 프로덕션 서비스 수준 계약(SLA)에서 지원되지 않으며 기능적으로 완전하지 않을 수 있으며 프로덕션에 사용하지 않는 것이 좋습니다. 이러한 기능을 사용하면 향후 제품 기능을 조기에 이용할 수 있어 개발 과정에서 고객이 기능을 테스트하고 피드백을 제공할 수 있습니다. 자세한 내용은 [Red Hat 기술 프리뷰 기능 지원 범위를 참조하십시오](#).

중첩된 가상화를 사용하면 가상 시스템이 다른 가상 시스템을 호스팅할 수 있습니다. 명확성을 위해 이러한 가상 시스템을 *상위 가상 시스템*과 *중첩된 가상 시스템*을 호출합니다.

하위 가상 시스템은 상위 가상 시스템에 액세스할 수 있는 사용자만 볼 수 있고 관리합니다. RHV(Red Hat Virtualization) 관리자는 볼 수 없습니다.

기본적으로 RHV에서는 중첩된 가상화가 활성화되지 않습니다. 중첩된 가상화를 활성화하려면 클러스터의 모든 호스트에 **VDSM** 후크 **vds-hook-nestedvt**를 설치합니다. 그런 다음 이러한 호스트에서 실행되는 모든 가상 시스템은 상위 가상 시스템으로 작동할 수 있습니다.

중첩된 가상화를 지원하는 호스트에서 상위 가상 시스템만 실행해야 합니다. 상위 가상 시스템이 중첩된 가상화를 지원하지 않는 호스트로 마이그레이션되는 경우 하위 가상 시스템이 실패합니다. 이 문제가 발생하지 않도록 하려면 중첩된 가상화를 지원하도록 클러스터의 모든 호스트를 구성합니다. 그렇지 않으면 중첩된 가상화를 지원하지 않는 호스트로 상위 가상 시스템이 마이그레이션되지 않도록 제한합니다.



주의

상위 가상 시스템이 중첩된 가상화를 지원하지 않는 호스트로 마이그레이션되지 않도록 예방하십시오.

절차

1. 관리 포털에서 **Compute** → **Hosts** (호스트)를 클릭합니다.
2. 중첩된 가상화를 활성화하려는 클러스터에서 호스트를 선택하고 **Management Maintenance**(유지 관리 유지관리) 및 **OK** (확인)를 클릭합니다.

3. 호스트를 다시 선택하고 호스트 콘솔을 클릭하고 호스트 콘솔에 로그인합니다.

4. **VDSM** 후크를 설치합니다.

```
# dnf install vdsmd-hook-nestedvt
```

5. 호스트를 재부팅합니다.

6. 호스트 콘솔에 다시 로그인하고 중첩된 가상화가 활성화되었는지 확인합니다.

```
$ cat /sys/module/kvm*/parameters/nested
```

이 명령에서 **Y** 또는 **1** 을 반환하면 기능이 활성화됩니다.

7. 클러스터의 모든 호스트에 대해 이 절차를 반복합니다.

추가 리소스



VDSM 후크

2.5.5.3.3. 개별 가상 머신에 중첩된 가상화 활성화



중요

중첩된 가상화는 기술 프리뷰 기능입니다. 기술 프리뷰 기능은 **Red Hat** 프로덕션 서비스 수준 계약(**SLA**)에서 지원되지 않으며 기능적으로 완전하지 않을 수 있으며 프로덕션에 사용하지 않는 것이 좋습니다. 이러한 기능을 사용하면 향후 제품 기능을 조기에 이용할 수 있어 개발 과정에서 고객이 기능을 테스트하고 피드백을 제공할 수 있습니다. 자세한 내용은 [Red Hat 기술 프리뷰 기능 지원 범위를 참조하십시오](#).

중첩된 가상화를 사용하면 가상 시스템이 다른 가상 시스템을 호스팅할 수 있습니다. 명확성을 위해 이러한 가상 시스템을 **상위 가상 시스템과 중첩된 가상 시스템**을 호출합니다.

하위 가상 시스템은 상위 가상 시스템에 액세스할 수 있는 사용자만 볼 수 있고 관리합니다. RHV(Red Hat Virtualization) 관리자는 볼 수 없습니다.

일부 가상 시스템이 아닌 *특정 가상 시스템에서* 중첩된 가상화를 활성화하려면 중첩된 가상화를 지원하도록 호스트 또는 호스트를 구성합니다. 그런 다음 특정 호스트에서 실행되는 에서 가상 시스템 또는 가상 시스템을 구성하고 **Pass-Through Host CPU** 를 활성화합니다. 이 옵션을 사용하면 가상 시스템에서 호스트에서 방금 구성한 중첩된 가상화 설정을 사용할 수 있습니다. 또한 이 옵션은 가상 시스템에서 실행할 수 있는 호스트를 제한하며 수동 마이그레이션이 필요합니다.

또는 클러스터 *의 모든 가상 머신에* 중첩된 가상화를 사용하려면 **모든 가상 머신에 중첩된 가상화 활성화**를 참조하십시오.

중첩된 가상화를 지원하는 호스트에서 상위 가상 시스템만 실행합니다. 상위 가상 시스템을 중첩된 가상화를 지원하지 않는 호스트로 마이그레이션하면 하위 가상 머신이 실패합니다.



주의

중첩된 가상화를 지원하지 않는 호스트로 상위 가상 시스템을 마이그레이션하지 마십시오.

하위 가상 시스템을 실행 중인 상위 가상 시스템의 실시간 마이그레이션 방지. 소스 및 대상 호스트가 동일하고 중첩된 가상화를 지원하는 경우에도 실시간 마이그레이션으로 인해 하위 가상 머신이 실패할 수 있습니다. 대신 마이그레이션 전에 가상 시스템을 종료합니다.

절차

중첩된 가상화를 지원하도록 호스트를 구성합니다.

1. 관리 포털에서 **Compute** → **Hosts** (호스트) 를 클릭합니다.
2. 중첩된 가상화를 활성화하려는 클러스터에서 호스트를 선택하고 **Management Maintenance**(유지 관리 유지관리) 및 **OK** (확인)를 클릭합니다.

3. 호스트를 다시 선택하고 호스트 콘솔을 클릭하고 호스트 콘솔에 로그인합니다.
4. **Edit Host**(호스트 편집) 창에서 **Kernel** (커널) 탭을 선택합니다.
5. **Kernel boot parameters** (커널 부팅 매개 변수)에서 확인란을 선택 취소하는 경우 **RESET** (재설정)을 클릭합니다.
6. 중첩된 가상화를 선택하고 **OK**(확인)를 클릭합니다.

이 작업은 커널 명령줄에서 **kvm-<architecture>.nested=1** 매개 변수를 표시합니다. 다음 단계에서는 이 매개 변수를 **Current kernel CMD** 행에 추가합니다.
7. **Installation → Reinstall** (재설치)을 클릭합니다.
8. 호스트 상태가 **Up** 으로 반환되면 **Power Management**(전원 관리) 또는 **SSH Management**(SSH 관리 (관리) **Restart** (재시작))를 클릭합니다.
9. 중첩된 가상화가 활성화되었는지 확인합니다. 호스트 콘솔에 로그인하여 다음을 입력합니다.

```
$ cat /sys/module/kvm*/parameters/nested
```

이 명령에서 **Y** 또는 **1** 을 반환하면 기능이 활성화됩니다.

10. 상위 가상 시스템을 실행하는 데 필요한 모든 호스트에 대해 이 절차를 반복합니다.

특정 가상 머신에서 중첩된 가상화를 활성화합니다.

1. 관리 포털에서 **Compute**(컴퓨팅) **Virtual Machines**(가상 시스템) 를 클릭합니다.
2. 가상 머신을 선택하고 편집을 클릭합니다.

3.

Edit Virtual Machine(논리 시스템 편집) 창에서 **Show Advanced Options** (고급 옵션 표시)를 클릭하고 **Host**(호스트) 탭을 선택합니다.

4.

Start Running On (실행 시작)에서 **Specific Host** (특정 호스트)를 클릭하고 중첩된 가상화를 지원하도록 구성된 호스트 또는 호스트를 선택합니다.

5.

CPU Options (CPU 옵션)에서 **Pass-Through Host CPU**(호스트 CPU 통과)를 선택합니다. 이 작업은 수동 마이그레이션만 허용하도록 마이그레이션 모드를 자동으로 설정합니다.



참고

RHV 버전 4.2에서는 마이그레이션을 허용하지 않는 경우에만 호스트 **CPU** 패스쓰루(**Pass-Through Host CPU**)를 활성화할 수 있습니다.

추가 리소스

•

[VDSM 후크](#)

•

[RHEL 설명서에서 중첩된 가상 머신 생성.](#)

2.5.5.4. 호스트를 유지 관리 모드로 이동

네트워크 구성 및 소프트웨어 업데이트 배포를 비롯한 많은 유지 관리 작업을 수행하려면 호스트를 유지 관리 모드로 전환해야 합니다. **VDSM**이 재부팅 또는 네트워킹 또는 스토리지 관련 문제와 같이 제대로 작동하지 않을 수 있는 이벤트를 수행하기 전에 호스트를 유지 관리 모드로 전환해야 합니다.

호스트가 유지 관리 모드로 전환되면 **Red Hat Virtualization Manager**는 실행 중인 모든 가상 시스템을 대체 호스트로 마이그레이션하려고 시도합니다. 실시간 마이그레이션을 위한 표준 사전 요구 사항이 적용됩니다. 특히 마이그레이션된 가상 시스템을 실행할 용량을 갖춘 호스트가 클러스터에 하나 이상 활성 상태여야 합니다.



참고

호스트에 고정되어 마이그레이션할 수 없는 가상 시스템은 종료됩니다. 호스트 세부 정보 보기의 **Virtual Machines** (가상 시스템) 탭에서 **Pinned to Host** (호스트에 고정됨)를 클릭하여 호스트에 고정된 가상 시스템을 확인할 수 있습니다.

호스트를 유지 관리 모드로 전환

1. **Compute → Hosts** (컴퓨팅 호스트)를 클릭하고 원하는 호스트를 선택합니다.
2. **Management(관리 → Maintenance (유지 관리))**를 클릭합니다. 그러면 **Maintenance Host(s)**(유지 관리 호스트) 확인 창이 열립니다.
3. 선택적으로, 호스트를 유지 관리 모드로 이동하는 **Reason** 을 입력합니다. 그러면 로그에 호스트가 다시 활성화될 때 표시됩니다. **OK**를 클릭합니다.



참고

호스트 유지 관리 **Reason**(호스트 유지 관리 이유) 필드는 클러스터 설정에서 활성화된 경우에만 표시됩니다. 자세한 내용은 [클러스터 일반 설정](#)을 참조하십시오.

4. 선택적으로 **Gluster**를 지원하는 호스트에 필요한 옵션을 선택합니다.

기본 점검을 방지하려면 **Ignore Gluster Quorum** 및 **self-Heal Validations** 옵션을 선택합니다. 기본적으로 **Manager**는 호스트가 유지 관리 모드로 이동하면 **Gluster** 쿼럼이 손실되지 않았는지 확인합니다. 또한 관리자는 호스트를 유지 관리 모드로 이동하여 영향을 받는 자동 복구 활동이 없는지 확인합니다. **Gluster** 쿼럼이 손실되거나 영향을 받는 자체 복구 활동이 있는 경우 관리자는 호스트가 유지 관리 모드로 전환되지 않도록 합니다. 호스트를 유지 관리 모드로 배치하는 다른 방법이 없는 경우에만 이 옵션을 사용합니다.

호스트를 유지 관리 모드로 이동하는 동안 모든 **Gluster** 서비스를 중지하려면 **Stop Gluster Service (Gluster 서비스 중지)** 옵션을 선택합니다.

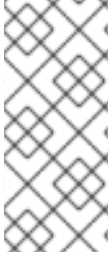


참고

이러한 필드는 선택한 호스트에서 **Gluster**를 지원하는 경우에만 호스트 유지 관리 창에 표시됩니다. 자세한 내용은 [기본 Gluster Storage 노드](#) 교체 *Red Hat Hyperconverged Infrastructure* 유지 관리에서 참조하십시오.

5. **OK(확인)**를 클릭하여 유지 관리 모드를 시작합니다.

실행 중인 모든 가상 시스템은 대체 호스트로 마이그레이션됩니다. 호스트가 **SPM(Storage Pool Manager)**인 경우 **SPM** 역할은 다른 호스트로 마이그레이션됩니다. 호스트의 **Status(상태)** 필드가 **Preparing for Maintenance** (유지 관리 준비 중)로 변경되고 작업이 성공적으로 완료되면 마지막으로 **Maintenance** (유지 관리)가 변경됩니다. 호스트가 유지 관리 모드에 있는 동안 **VDSM**이 중지되지 않습니다.



참고

가상 시스템에서 마이그레이션이 실패하면 **Management(관리 → Activate (활성화))**를 클릭하여 해당 작업을 유지 관리 모드로 전환한 다음 가상 시스템에서 마이그레이션 취소 를 클릭하여 마이그레이션을 중지합니다.

2.5.5.5. 유지 관리 모드에서 호스트 활성화

유지 관리 모드로 설정되었거나 최근에 환경에 추가된 호스트는 사용할 수 있기 전에 활성화해야 합니다. 호스트가 준비되지 않은 경우 활성화에 실패할 수 있습니다. 호스트 활성화를 시도하기 전에 모든 작업이 완료되었는지 확인합니다.

절차

1. **Compute(컴퓨팅) → Hosts(호스트)** 를 클릭하고 호스트를 선택합니다.
2. **Management(관리 → Activate (활성화))** 를 클릭합니다.

호스트 상태가 **Unassigned(할당되지 않음)** 로 변경되고 작업이 완료되면 결국 **Up** 으로 변경됩니다. 이제 가상 시스템을 호스트에서 실행할 수 있습니다. 유지 관리 모드로 전환되었을 때 호스트에서 마이그레이션된 가상 시스템은 활성화 시 호스트로 자동으로 마이그레이션되지 않지만 수동으로 마이그레이션할 수 있습니다. 호스트가 유지 관리 모드로 전환되기 전에 **SPM(Storage Pool Manager)**인 경우 호스트를 활성화할 때 **SPM** 역할이 자동으로 반환되지 않습니다.

2.5.5.5.1. 호스트 방화벽 규칙 구성

Ansible을 사용하여 호스트 방화벽 규칙을 영구적으로 구성할 수 있습니다. **firewalld** 를 사용하도록 클러스터를 구성해야 합니다.



참고

firewalld 영역 변경은 지원되지 않습니다.

호스트의 방화벽 규칙 구성

1. **Manager** 시스템에서 **ovirt-host-deploy-post-tasks.yml.example** 을 편집하여 사용자 지정 방화벽 포트를 추가합니다.

```
# vi /etc/ovirt-engine/ansible/ovirt-host-deploy-post-tasks.yml.example
---
#
# Any additional tasks required to be executing during host deploy process can
# be added below
#
- name: Enable additional port on firewall
  firewallld:
    port: "12345/tcp"
    permanent: yes
    immediate: yes
    state: enabled
```

2. 파일을 다른 위치에 **ovirt-host-deploy-post-tasks.yml** 로 저장합니다.

새로운 또는 재설치 호스트는 업데이트된 방화벽 규칙을 사용하여 구성됩니다.

Installation → **Reinstall** (재설치)을 클릭하고 **Automatically configure host firewall**(호스트 방화벽 자동 구성)을 선택하여 기존 호스트를 다시 설치해야 합니다.

2.5.5.5.2. 호스트 제거

호스트를 다시 설치해야 하는 경우와 같이 **Red Hat Virtualization** 환경에서 호스트를 제거해야 하는 경우가 있습니다.

절차

1. **Compute**(컴퓨팅) → **Hosts**(호스트) 를 클릭하고 호스트를 선택합니다.
2. **Management**(관리 → **Maintenance** (유지 관리))를 클릭합니다.
3. 호스트가 유지 관리 모드이면 **Remove**(제거)를 클릭합니다. **Remove Host(s)**(호스트 제거) 확인 창이 열립니다.
- 4.

호스트가 **Red Hat Gluster Storage** 클러스터의 일부이고 볼륨 **brick**이 있고 호스트가 응답하지 않는 경우 **Force Remove** (강제 제거) 확인란을 선택합니다.

5.

OK(확인)를 클릭합니다.

2.5.5.5.3. 마이너 릴리스 간 호스트 업데이트

클러스터의 모든 호스트를 업데이트하거나 개별 호스트를 업데이트할 수 있습니다.

2.5.5.5.3.1. 클러스터의 모든 호스트 업데이트

호스트를 개별적으로 업데이트하는 대신 클러스터의 모든 호스트를 업데이트할 수 있습니다. 이는 **Red Hat Virtualization**의 새 버전으로 업그레이드하는 동안 특히 유용합니다. 업데이트 자동화에 사용되는 **Ansible** 역할에 대한 자세한 내용은 [oVirt Cluster Upgrade](#)를 참조하십시오.

한 번에 하나의 클러스터를 업데이트합니다.

제한

- **RHVH**의 업데이트는 **/etc** 및 **/var** 디렉토리에서만 수정된 콘텐츠만 유지합니다. 다른 경로의 수정된 데이터는 업데이트 중에 덮어씁니다.
- 클러스터가 활성화된 마이그레이션이 활성화된 경우 가상 시스템이 클러스터의 다른 호스트로 자동으로 마이그레이션됩니다.
- 자체 호스팅 엔진 환경에서 **Manager** 가상 시스템은 동일한 클러스터의 자체 호스팅 엔진 노드 간에만 마이그레이션할 수 있습니다. 표준 호스트로 마이그레이션할 수 없습니다.
- 클러스터에는 호스트가 유지 관리를 수행할 수 있도록 충분한 메모리가 있어야 합니다. 그렇지 않으면 가상 시스템 마이그레이션이 중단되고 실패합니다. 호스트를 업데이트하기 전에 일부 또는 모든 가상 시스템을 종료하여 호스트 업데이트의 메모리 사용량을 줄일 수 있습니다.
- 고정된 가상 시스템(예: **vGPU**를 사용하는 가상 머신)은 다른 호스트로 마이그레이션할 수 없습니다. 대신 해당 호스트를 건너뛰지 않는 한, 고정된 가상 시스템은 업데이트 중에 종료됩니다.

절차

1. 관리 포털에서 **Compute** → **Clusters** (클러스터) 를 클릭하고 클러스터를 선택합니다.
Upgrade status 옆에는 클러스터의 모든 호스트에 업그레이드를 사용할 수 있는지 표시됩니다.
2. **Upgrade** (업그레이드)를 클릭합니다.
3. 업데이트할 호스트를 선택한 다음 **Next** (다음)를 클릭합니다.
4. 옵션을 설정합니다.
 - 고정된 **VM**을 중지하면 클러스터의 호스트에 고정된 모든 가상 시스템이 종료되며 기본적으로 선택됩니다. 고정된 가상 시스템이 중요한 서비스 또는 프로세스를 실행하는 경우와 같이 고정된 가상 시스템이 실행되도록 해당 호스트 업데이트를 건너뛰도록 이 확인란을 지우고 업데이트 중에 알 수 없는 시간에 종료하지 않도록 할 수 있습니다.
 - **Upgrade Timeout(Minutes)** (업그레이드 시간 제한(Minutes))은 클러스터 업그레이드가 실패하기 전에 개별 호스트가 업데이트될 때까지 대기하는 시간을 설정합니다. 기본값은 **60** 입니다. 60분에 충분하지 않은 대규모 클러스터에서는 클러스터를 늘리거나 호스트가 빠르게 업데이트되는 소규모 클러스터에서 줄일 수 있습니다.
 - 업그레이드 프로세스를 실행하기 전에 업그레이드에서 사용 가능한 업데이트가 있는지 확인합니다. 기본적으로 선택되지 않지만, 기본값보다 덜 자주 호스트 업데이트를 확인하도록 **Manager**를 구성한 경우와 같이 최신 업데이트가 포함되어 있는지 확인해야 하는 경우 선택할 수 있습니다.
 - **Rebooting after Upgrade**(업그레이드 후 재부팅)는 업데이트한 후 각 호스트를 재부팅하고 기본적으로 선택됩니다. 호스트 재부팅이 필요한 보류 중인 업데이트가 없는 경우 프로세스의 속도를 높이기 위해 이 확인란을 지울 수 있습니다.
 - **Maintenance Policy**를 사용하여 업데이트 중에 클러스터의 스케줄링 정책을 **cluster_maintenance** 로 설정합니다. 기본적으로 선택되므로 활동은 제한되며 고가용성이 아니면 가상 시스템을 시작할 수 없습니다. 업데이트 중에 계속 사용하려는 사용자 지정 스케줄링 정책이 있는 경우 이 확인란을 지울 수 있지만 이는 알 수 없는 결과를 초래할 수 있습니다. 이 옵션을 비활성화하기 전에 사용자 정의 정책이 클러스터 업그레이드 활동과 호환되는지 확인하십시오.

5.

다음을 클릭합니다.

6.

영향을 받을 호스트 및 가상 시스템의 요약을 검토합니다.

7.

Upgrade (업그레이드)를 클릭합니다.

호스트 업데이트 진행 상황을 추적할 수 있습니다.

•

Compute(컴퓨팅) **Clusters**(클러스터) 보기에서 **Upgrade Status**(업그레이드 상태) 열에 **Upgrade in progress**가 표시됩니다.

•

Compute Hosts(컴퓨팅 호스트) 보기

•

알림 다이내믹의 이벤트 섹션에서(



확인할 수 있습니다.

Compute → **Virtual Machines** (컴퓨팅 가상 시스템) 보기의 **Status**(상태) 열에서 개별 가상 머신 마 이그레이션의 진행 상황을 추적할 수 있습니다. 대규모 환경에서는 결과를 필터링하여 특정 가상 시스템 그룹을 표시해야 할 수도 있습니다.

2.5.5.5.3.2. 개별 호스트 업데이트

호스트 업그레이드 관리자를 사용하여 관리 포털에서 직접 개별 호스트를 업데이트합니다.



참고

업그레이드 관리자는 **Up** 또는 **Non-operational** (유지 관리가 아님) 상태의 호스트 만 확인합니다.

제한

•

RHVH의 업데이트는 **/etc** 및 **/var** 디렉토리에서만 수정된 콘텐츠만 유지합니다. 다른 경로의 수정된 데이터는 업데이트 중에 덮어씁니다.

- 클러스터가 활성화된 마이그레이션이 활성화된 경우 가상 시스템이 클러스터의 다른 호스트로 자동으로 마이그레이션됩니다. 사용량이 상대적으로 낮은 경우 호스트를 업데이트합니다.
- 자체 호스팅 엔진 환경에서 **Manager** 가상 시스템은 동일한 클러스터의 자체 호스팅 엔진 노드 간에만 마이그레이션할 수 있습니다. 표준 호스트로 마이그레이션할 수 없습니다.
- 클러스터에는 호스트가 유지 관리를 수행할 수 있도록 충분한 메모리가 있어야 합니다. 그렇지 않으면 가상 시스템 마이그레이션이 중단되고 실패합니다. 호스트를 업데이트하기 전에 일부 또는 모든 가상 시스템을 종료하여 호스트 업데이트의 메모리 사용량을 줄일 수 있습니다.
- 하나의 호스트에서 **SPM(Storage Pool Manager)** 작업을 수행하기 위해 하나의 호스트를 계속 사용할 수 있어야 하므로 모든 호스트를 동시에 업데이트하지 마십시오.
- 고정된 가상 시스템(예: **vGPU**를 사용하는 가상 머신)은 다른 호스트로 마이그레이션할 수 없습니다. 고정된 가상 시스템은 호스트를 업데이트하기 전에 종료해야 합니다.

절차

1.

올바른 리포지토리가 활성화되어 있는지 확인합니다. 현재 활성화된 리포지토리 목록을 보려면 **dnf repolist**를 실행합니다.

•

Red Hat Virtualization 호스트의 경우:

```
# subscription-manager repos --enable=rhvh-4-for-rhel-8-x86_64-rpms
```

•

Red Hat Enterprise Linux 호스트의 경우:

```
# subscription-manager repos \
  --enable=rhel-8-for-x86_64-baseos-rpms \
  --enable=rhel-8-for-x86_64-appstream-rpms \
  --enable=rhvh-4-mgmt-agent-for-rhel-8-x86_64-rpms \
  --enable=advanced-virt-for-rhel-8-x86_64-rpms \
  --enable=fast-datapath-for-rhel-8-x86_64-rpms
```

2.

관리 포털에서 **Compute**(컴퓨팅 → **Hosts**(호스트))를 클릭하고 업데이트할 호스트를 선택합니다.

3.

Installation → **Check for Upgrade** (업그레이드용 설치 확인)를 클릭하고 **OK(확인)**를 클릭합니다.

Notification Drawer (



)를 열고 **Events**(이벤트) 섹션을 확장하여 결과를 확인합니다.

4.

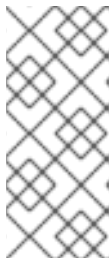
업데이트를 사용할 수 있는 경우 **Installation** → **Upgrade** (업그레이드)를 클릭합니다.

5.

OK(확인)를 클릭하여 호스트를 업데이트합니다. 마이그레이션 정책에 따라 가상 시스템 실행이 마이그레이션됩니다. 모든 가상 시스템에 대한 마이그레이션이 비활성화된 경우 가상 시스템을 종료하라는 메시지가 표시됩니다.

호스트의 세부 정보는 **Compute Hosts**(컴퓨팅 호스트)에서 업데이트되고 상태는 다음 단계를 통해 전환됩니다.

유지 관리 > 설치 > 재부팅 > 위로



참고

업데이트에 실패하면 호스트 상태가 **Install Failed**로 변경됩니다. **Install Failed** (설치 실패)에서 **Installation** → **Upgrade** (업그레이드)를 다시 클릭할 수 있습니다.

Red Hat Virtualization 환경의 각 호스트에 대해 이 절차를 반복합니다.



참고

관리 포털에서 호스트를 업데이트해야 합니다. 대신 **dnf** 업그레이드를 사용하여 호스트를 업데이트할 수 있습니다.

2.5.5.5.3.3. 수동으로 호스트 업데이트

경고

이 정보는 호스트를 수동으로 업데이트해야 하지만 **Red Hat**은 이 방법을 지원하지 않는 고급 시스템 관리자를 위해 제공됩니다. 이 항목에 설명된 절차에는 인증서 갱신을 포함하여 이러한 정보에 대한 고급 지식이 있을 경우 중요한 단계가 포함되지 않습니다. **Red Hat**은 관리 포털을 사용하여 호스트 업데이트를 지원합니다. 자세한 내용은 [관리 가이드에서 개별 호스트 업데이트 또는 클러스터의 모든 호스트 업데이트를 참조하십시오.](#)

dnf 명령을 사용하여 호스트를 업데이트할 수 있습니다. 보안 및 버그 픽스를 적시에 적용할 수 있도록 시스템을 정기적으로 업데이트합니다.

제한

- **RHVH**의 업데이트는 **/etc** 및 **/var** 디렉토리에서만 수정된 콘텐츠만 유지합니다. 다른 경로의 수정된 데이터는 업데이트 중에 덮어씁니다.
- 클러스터가 활성화된 마이그레이션이 활성화된 경우 가상 시스템이 클러스터의 다른 호스트로 자동으로 마이그레이션됩니다. 사용량이 상대적으로 낮은 경우 호스트를 업데이트합니다.
- 자체 호스팅 엔진 환경에서 **Manager** 가상 시스템은 동일한 클러스터의 자체 호스팅 엔진 노드 간에만 마이그레이션할 수 있습니다. 표준 호스트로 마이그레이션할 수 없습니다.
- 클러스터에는 호스트가 유지 관리를 수행할 수 있도록 충분한 메모리가 있어야 합니다. 그렇지 않으면 가상 시스템 마이그레이션이 중단되고 실패합니다. 호스트를 업데이트하기 전에 일부 또는 모든 가상 시스템을 종료하여 호스트 업데이트의 메모리 사용량을 줄일 수 있습니다.
- 하나의 호스트에서 **SPM(Storage Pool Manager)** 작업을 수행하기 위해 하나의 호스트를 계속 사용할 수 있어야 하므로 모든 호스트를 동시에 업데이트하지 마십시오.
- 고정된 가상 시스템(예: **vGPU**를 사용하는 가상 머신)은 다른 호스트로 마이그레이션할 수 없습니다. 고정된 가상 시스템은 호스트를 업데이트하기 전에 종료해야 합니다.

절차

1. 올바른 리포지토리가 활성화되었는지 확인합니다. **dnf repolist** 를 실행하여 현재 활성화된 리포지토리를 확인할 수 있습니다.

•

Red Hat Virtualization 호스트의 경우:

```
# subscription-manager repos --enable=rhvh-4-for-rhel-8-x86_64-rpms
```

•

Red Hat Enterprise Linux 호스트의 경우:

```
# subscription-manager repos \
  --enable=rhel-8-for-x86_64-baseos-rpms \
  --enable=rhel-8-for-x86_64-appstream-rpms \
  --enable=rhv-4-mgmt-agent-for-rhel-8-x86_64-rpms \
  --enable=advanced-virt-for-rhel-8-x86_64-rpms \
  --enable=fast-datapath-for-rhel-8-x86_64-rpms
```

2.

관리 포털에서 **Compute**(컴퓨팅 → **Hosts**(호스트) 를 클릭하고 업데이트할 호스트를 선택합니다.

3.

Management(관리 → **Maintenance** (유지 관리) 및 **OK** (확인)를 클릭합니다.

4.

Red Hat Enterprise Linux 호스트의 경우:

a.

Red Hat Enterprise Linux의 현재 버전을 확인합니다.

```
# cat /etc/redhat-release
```

b.

사용 가능한 **redhat-release** 패키지 버전을 확인합니다.

```
# dnf --refresh info --available redhat-release
```

이 명령은 사용 가능한 업데이트를 모두 표시합니다. 예를 들어 **Red Hat Enterprise Linux 8.2.z**에서 **8.3**으로 업그레이드하는 경우 패키지 버전을 현재 설치된 버전과 비교합니다.

```
Available Packages
Name      : redhat-release
Version   : 8.3
Release   : 1.0.el8
...
```

경고

Red Hat Enterprise Linux Advanced Virtualization 모듈은 일반적으로 **Red Hat Enterprise Linux y-stream**보다 나중에 출시됩니다. 아직 새로운 **Advanced Virtualization** 모듈을 사용할 수 없거나 오류가 있는 경우 여기를 중지하고 업그레이드를 취소하십시오. 그렇지 않으면 호스트가 손상될 위험이 있습니다.

c.

Red Hat Enterprise Linux 8.3 이상에서 **Advanced Virtualization** 스트림을 사용할 수 있는 경우 **virt** 모듈을 재설정합니다.

```
# dnf module reset virt
```



참고

이 모듈이 **Advanced Virtualization** 스트림에서 이미 활성화된 경우 이 단계는 필요하지 않지만 부정적인 영향은 없습니다.

다음을 입력하여 스트림의 값을 확인할 수 있습니다.

```
# dnf module list virt
```

d.

다음 명령을 사용하여 **Advanced Virtualization** 스트림에서 **virt** 모듈을 활성화합니다.

•

RHV 4.4.2:

```
# dnf module enable virt:8.2
```

•

RHV 4.4.3에서 **4.4.5**로의 경우:

```
# dnf module enable virt:8.3
```

•

RHV 4.4.6에서 **4.4.10**으로의 경우:

```
# dnf module enable virt:av
```

•

RHV 4.4 이상의 경우:

```
# dnf module enable virt:rhel
```

**참고**

RHEL 8.6부터 고급 가상화 패키지는 표준 **virt:rhel** 모듈을 사용합니다.
RHEL 8.4 및 **8.5**의 경우 하나의 고급 가상화 스트림만 사용됩니다. **rhel:av**.

1. 호스트를 업데이트합니다.

```
# dnf upgrade --nobest
```

2. 호스트를 재부팅하여 모든 업데이트가 올바르게 적용되었는지 확인합니다.

**참고**

img 기반 로그를 확인하여 **Red Hat Virtualization Host**에 대한 추가 패키지 업데이트가 실패했는지 확인합니다. 업데이트 후 일부 패키지가 성공적으로 다시 설치되지 않은 경우 패키지가 **/var/imagbased/persisted-rpms**에 나열되어 있는지 확인합니다. 누락된 패키지를 추가한 다음 **rpm -Uvh /var/imagbased/persisted-rpms/***를 실행합니다.

Red Hat Virtualization 환경에서 각 호스트에 대해 이 프로세스를 반복합니다.

2.5.5.5.4. 호스트 재설치

관리 포털에서 **RHVH(Red Hat Virtualization Host)** 및 **Red Hat Enterprise Linux** 호스트를 다시 설치합니다. 절차에는 호스트를 중지하고 다시 시작하는 작업이 포함됩니다.



주의

호스트 운영 체제를 설치하거나 다시 설치하는 경우 먼저 이러한 디스크를 실수로 초기화하지 않도록 호스트에 연결된 기존 비OS 스토리지를 분리하는 것이 좋습니다.

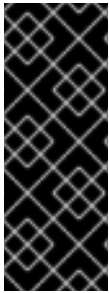
사전 요구 사항

- 클러스터의 마이그레이션이 활성화된 경우 가상 시스템은 클러스터의 다른 호스트로 자동 마이그레이션할 수 있습니다. 따라서 사용량이 상대적으로 낮은 상태에서 호스트를 다시 설치합니다.
- 클러스터에 호스트에서 유지 관리를 수행할 수 있는 메모리가 충분한지 확인합니다. 클러스터에 메모리가 없으면 가상 시스템 마이그레이션이 중단되고 실패합니다. 메모리 사용량을 줄이면 호스트를 유지 관리로 이동하기 전에 일부 또는 모든 가상 시스템을 종료합니다.
- 재설치를 수행하기 전에 클러스터에 호스트가 두 개 이상 포함되어 있는지 확인합니다. 모든 호스트를 동시에 다시 설치하지 마십시오. 스토리지 풀 관리자(SPM) 작업을 수행하려면 하나의 호스트를 사용할 수 있어야 합니다.

절차

1. **Compute(컴퓨팅) → Hosts(호스트)** 를 클릭하고 호스트를 선택합니다.
2. **Management(관리 → Maintenance (유지 관리) 및 OK (확인))**를 클릭합니다.
3. **Installation → Reinstall (재설치)**을 클릭합니다. 그러면 **Install Host(호스트 설치)** 창이 열립니다.
4. **OK(확인)**를 클릭하여 호스트를 다시 설치합니다.

호스트를 다시 설치하고 해당 상태가 **Up** 으로 돌아간 후 가상 시스템을 호스트로 다시 마이그레이션할 수 있습니다.



중요

Red Hat Virtualization Host를 Red Hat Virtualization Manager에 등록하고 다시 설치한 후 관리 포털에 **Install Failed** (설치 실패) 상태로 잘못 표시될 수 있습니다. **Management**(관리 → **Activate** (활성화) 를 클릭하면 호스트가 **Up** 상태로 변경되고 사용할 준비가 됩니다.

2.5.5.6. 호스트 에라타 보기

각 호스트에 대한 에라타는 Red Hat Satellite 서버에서 에라타 정보를 수신하도록 호스트를 구성한 후 볼 수 있습니다. 에라타를 수신하도록 호스트를 구성하는 방법에 대한 자세한 내용은 [Configuring Satellite Errata Management for a Host](#)를 참조하십시오.

절차

1. **Compute**(컴퓨팅) **Hosts**(호스트) 를 클릭합니다.
2. 호스트 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Errata** (에라타) 탭을 클릭합니다.

2.5.5.7. 호스트의 상태 보기

호스트에는 일반 상태 외에도 외부 상태가 있습니다. 외부 상태는 플러그인 또는 외부 시스템에서 보고되거나 관리자가 설정하며 호스트 이름 왼쪽에 다음 아이콘 중 하나로 표시됩니다.

- **OK:** 아이콘 없음
- **Info:**

- **경고:**

-

Error:



●

실패:



호스트 상태에 대한 자세한 내용을 보려면 호스트 이름을 클릭합니다. 그러면 세부 정보 보기가 열리고 **Events(이벤트)** 탭을 클릭합니다.

호스트의 상태는 **REST API**를 사용하여 볼 수도 있습니다. 호스트의 **GET** 요청에는 상태가 포함된 **external_status** 요소가 포함됩니다.

이벤트 컬렉션을 통해 **REST API**에서 호스트 상태를 설정할 수 있습니다. 자세한 내용은 [REST API 가이드에서 이벤트 추가](#)를 참조하십시오.

2.5.5.8. 호스트 장치 보기

세부 정보 보기의 **Host Devices(호스트 장치)** 탭에서 각 호스트의 호스트 장치를 볼 수 있습니다. 호스트가 직접 장치 할당을 위해 구성된 경우 성능 향상을 위해 해당 장치를 가상 시스템에 직접 연결할 수 있습니다.

직접 장치 할당을 위한 하드웨어 요구 사항에 대한 자세한 내용은 [SR-IOV 구현을 위한 하드웨어 할당 사용을 위한 추가 하드웨어 고려 사항](#)을 참조하십시오.

직접 장치 할당을 위해 호스트 구성에 대한 자세한 내용은 [PCI 패스스루 호스트 작업](#) 구성을 참조하십시오.

가상 머신에 호스트 장치 연결에 대한 자세한 내용은 [가상 머신 관리 가이드의 호스트 장치를 참조하십시오](#).

절차

1.

Compute(컴퓨팅) Hosts(호스트) 를 클릭합니다.

2. 호스트 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Host Devices**(호스트 장치) 탭을 클릭합니다.

이 탭에는 장치가 가상 시스템에 연결되어 있는지 여부와 해당 가상 시스템에서 현재 사용 중인 호스트 장치의 세부 정보가 나열됩니다.

2.5.5.9. 관리 포털에서 Cockpit에 액세스

Cockpit은 RHVH(Red Hat Virtualization Host) 및 Red Hat Enterprise Linux 호스트에서 기본적으로 사용할 수 있습니다. 브라우저에 주소를 입력하거나 관리 포털을 통해 **Cockpit** 웹 인터페이스에 액세스할 수 있습니다.

절차

1. 관리 포털에서 **Compute** → **Hosts** (호스트)를 클릭하고 호스트를 선택합니다.
2. 호스트 콘솔을 클릭합니다.

Cockpit 로그인 페이지가 새 브라우저 창에서 열립니다.

2.5.5.9.1. 레거시 SPICE 암호 설정

SPICE 콘솔은 기본적으로 암호화 문자열과 함께 **FIPS** 호환 암호화를 사용합니다. 기본 **SPICE** 암호화 문자열은 **kECDHE+FIPS:kDHE+FIPS:kRSA+FIPS:!eNULL:!aNULL**입니다.

일반적으로 이 문자열은 충분합니다. 그러나 이전 운영 체제 또는 **SPICE** 클라이언트가 있는 가상 머신이 하나나 하나라도 **FIPS** 호환 암호화를 지원하지 않는 경우 더 약한 암호 문자열을 사용해야 합니다. 그렇지 않으면 기존 클러스터에 새 클러스터 또는 새 호스트를 설치하고 해당 가상 시스템에 연결을 시도하면 연결 보안 오류가 발생할 수 있습니다.

Ansible 플레이북을 사용하여 암호 문자열을 변경할 수 있습니다.

암호화 문자열 변경

1.

Manager 시스템의 디렉토리 `/usr/share/ovirt-engine/playbooks` 에 파일을 만듭니다. 예를 들면 다음과 같습니다.

```
# vim /usr/share/ovirt-engine/playbooks/change-spice-cipher.yml
```

2.

파일에 다음을 입력하여 저장합니다.

```
name: oVirt - setup weaker SPICE encryption for old clients
hosts: hostname
vars:
  host_deploy_spice_cipher_string: 'DEFAULT:-RC4:-3DES:-DES'
roles:
  - ovirt-host-deploy-spice-encryption
```

3.

방금 만든 파일을 실행합니다.

```
# ansible-playbook -i hostname /usr/share/ovirt-engine/playbooks/change-spice-cipher.yml
```

또는 `host_deploy_spice_cipher_string` 변수와 함께 `--extra-vars` 옵션을 사용하여 **Ansible** 플레이북 `ovirt-host-deploy`로 호스트를 재구성할 수 있습니다.

```
# ansible-playbook -i hostname \
  --extra-vars host_deploy_spice_cipher_string="DEFAULT:-RC4:-3DES:-DES" \
  /usr/share/ovirt-engine/playbooks/ovirt-host-deploy.yml
```

2.5.5.10. 호스트 전원 관리 설정 구성

관리 포털에서 호스트 라이프사이클 작업(중지, 시작, 다시 시작)을 수행하도록 호스트 전원 관리 장치 설정을 구성합니다.

호스트 고가용성 및 가상 시스템 고가용성을 활용하려면 호스트 전원을 구성해야 합니다. 전원 관리 장치에 대한 자세한 내용은 [Power Management in the Technical Reference](#)를 참조하십시오.

절차

1.

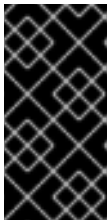
Compute → **Hosts** (컴퓨팅 호스트)를 클릭하고 호스트를 선택합니다.

2.

Management(관리 → **Maintenance** (유지 관리))를 클릭하고 **OK**(확인)를 클릭하여 확인합

니다.

3. 호스트가 유지 관리 모드인 경우 **Edit(편집)**를 클릭합니다.
4. **Power Management(전원 관리)** 탭을 클릭합니다.
5. **Enable Power Management (전원 관리 활성화)** 확인란을 선택하여 필드를 활성화합니다.
6. **Kdump** 통합 확인란을 선택하여 커널 크래시 덤프를 수행하는 동안 호스트가 펜싱되지 않도록 합니다.



중요

기존 호스트에서 **Kdump** 통합을 활성화하거나 비활성화하는 경우 구성할 **kdump**에 대해 [호스트를 다시 설치해야](#) 합니다.

7. 선택적으로 호스트 클러스터의 스케줄링 정책에서 호스트의 전원 관리를 제어하지 않으면 전원 관리의 정책 제어 비활성화 확인란을 선택합니다.
8. 더하기(+)버튼을 클릭하여 새 전원 관리 장치를 추가합니다. **Edit fence agent(펜스 에이전트 편집)** 창이 열립니다.
9. 전원 관리 장치의 **User Name (사용자 이름)** 및 **Password(암호)**를 적절한 필드에 입력합니다.
10. 드롭다운 목록에서 전원 관리 장치 유형을 선택합니다.
11. **Address (주소)** 필드에 **IP** 주소를 입력합니다.
12. 전원 관리 장치에서 사용하는 **SSH** 포트 번호를 입력하여 호스트와 통신합니다.

13.

전원 관리 장치의 블레이드를 식별하는 데 사용되는 번호 입력.

14.

전원 관리 장치의 옵션을 입력합니다. 쉼표로 구분된 '**key=value**' 항목 목록을 사용합니다.

- **IPv4 및 IPv6 IP** 주소를 모두 사용할 수 있는 경우 **Options** (옵션) 필드를 비워 둡니다.
- **IPv4 IP** 주소만 사용할 수 있는 경우 **inet4_only=1** 을 입력합니다.
- **IPv6 IP** 주소만 사용할 수 있는 경우 **inet6_only=1** 을 입력합니다.

15.

Secure (보안) 확인란을 선택하여 전원 관리 장치를 호스트에 안전하게 연결할 수 있습니다.

16.

Test (테스트)를 클릭하여 설정이 올바른지 확인합니다. 테스트 성공, 호스트 상태는: **on** 이 성공적으로 확인되면 표시됩니다.

17.

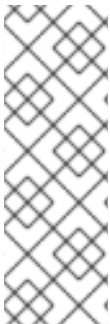
OK(확인)를 클릭하여 **Edit fence agent**(펜스 에이전트 편집) 창을 닫습니다.

18.

Power Management(전원 관리) 탭에서 **Advanced Parameters** (고급 매개 변수)를 확장하고 **up** 및 **down** 버튼을 사용하여 관리자가 펜싱 프록시에 대해 호스트의 클러스터 및 **dc** (**datacenter**)를 검색하는 순서를 지정합니다.

19.

OK(확인)를 클릭합니다.



참고

- **IPv6**의 경우 **Red Hat Virtualization**은 정적 주소 지정만 지원합니다.
- 듀얼 스택 **IPv4** 및 **IPv6** 주소 지정은 지원되지 않습니다.

이제 관리 포털에서 **Management** → **Power Management** (전원 관리) 드롭다운 메뉴가 활성화되었습니다.

2.5.5.11. 호스트 스토리지 풀 관리자 설정 구성

스토리지 풀 관리자(**SPM**)는 스토리지 도메인에 대한 액세스 제어를 유지하기 위해 데이터 센터의 호스트 중 하나에 제공되는 관리 역할입니다. **SPM** 호스트를 사용할 수 없게 되면 항상 **SPM** 역할을 사용할 수 있어야 하며 **SPM** 역할은 다른 호스트에 할당됩니다. **SPM** 역할은 일부 호스트의 사용 가능한 리소스를 사용하므로 리소스를 보유할 수 있는 호스트에 우선 순위를 지정하는 것이 중요합니다.

호스트의 **SPM(Storage Pool Manager)** 우선 순위 설정은 **SPM** 역할을 할당하는 호스트의 가능성을 변경합니다. **SPM** 우선 순위가 높은 호스트가 **SPM** 우선 순위가 낮은 호스트 전에 **SPM** 역할이 할당됩니다.

절차

1. **Compute(컴퓨팅) Hosts(호스트)** 를 클릭합니다.
2. **Edit(편집)** 를 클릭합니다.
3. **SPM** 탭을 클릭합니다.
4. 라디오 버튼을 사용하여 호스트의 적절한 **SPM** 우선 순위를 선택합니다.
5. **OK(확인)**를 클릭합니다.

2.5.5.11.1. 자체 호스팅 엔진 호스트를 다른 클러스터로 마이그레이션

자체 호스팅 엔진 호스트로 구성된 호스트를 자체 호스팅 엔진 가상 시스템이 실행 중인 이외의 데이터 센터 또는 클러스터로 마이그레이션할 수 없습니다. 모든 셀프 호스팅 엔진 호스트는 동일한 데이터 센터와 클러스터에 있어야 합니다.

호스트에서 셀프 호스팅 엔진 구성을 배포 취소하여 호스트가 자체 호스팅 엔진 호스트가 되지 않도록 비활성화해야 합니다.

절차

1. **Compute(컴퓨팅) → Hosts(호스트)** 를 클릭하고 호스트를 선택합니다.
2. **Management(관리 → Maintenance (유지 관리))**를 클릭합니다. 호스트 상태가 **Maintenance(유지 관리)**로 변경됩니다.
3. **Reinstall (재설치)**에서 **Hosted Engine UNDEPLOY(호스팅 엔진 UNDEPLOY)**를 선택합니다.
4. **Reinstall (재설치)**을 클릭합니다.

작은 정보

또는 **REST API undeploy_hosted_engine** 매개변수를 사용할 수 있습니다.

5. **Edit(편집)**를 클릭합니다.
6. 대상 데이터 센터와 클러스터를 선택합니다.
7. **OK(확인)**를 클릭합니다.
8. **Management(관리 → Activate (활성화))** 를 클릭합니다.

추가 리소스

- [호스트를 유지 관리 모드로 이동](#)
- [유지 관리 모드에서 호스트 활성화](#)

2.5.6. 새 호스트 및 호스트 편집 창의 설정 및 제어 설명

2.5.6.1. 설명된 호스트 일반 설정

이러한 설정은 호스트의 세부 정보를 편집하거나 새로운 **Red Hat Enterprise Linux** 호스트 및 **Satellite** 호스트 공급자 호스트를 추가할 때 적용됩니다.

General settings(일반 설정) 테이블에는 **New Host**(새 호스트) 또는 **Edit Host** (호스트 편집) 창의 **General**(일반) 탭에 필요한 정보가 포함되어 있습니다.

표 2.20. 일반 설정

필드 이름	설명
호스트 클러스터	호스트가 속한 클러스터 및 데이터 센터입니다.
Foreman/Satellite 사용	이 확인란을 선택하거나 지워서 Satellite 호스트 공급 업체가 제공한 호스트를 추가하기 위한 옵션을 보거나 숨깁니다. 다음 옵션도 사용할 수 있습니다. 검색된 호스트 ● Discover Hosts(검색된 호스트) - 엔진에서 검색한 Satellite 호스트 이름으로 채워진 드롭다운 목록입니다. ● 호스트 그룹 - 사용 가능한 호스트 그룹의 드롭다운 목록. ● Compute Resources(컴퓨팅 리소스) - 컴퓨팅 리소스를 제공하는 하이퍼바이저의 드롭다운 목록입니다. 프로비저닝된 호스트 ● Provider Hosts(프로바이더 호스트) - 선택한 외부 프로바이더가 제공하는 호스트 이름으로 채워진 드롭다운 목록입니다. 이 목록의 항목은 공급자 검색 필터에 입력된 검색 쿼리에 따라 필터링 됩니다. ● 공급자 검색 필터 - 선택한 외부 공급자가 제공한 호스트를 검색할 수 있는 텍스트 필드입니다. 이 옵션은 공급자에 따라 다릅니다. 특정 공급자에 대한 검색 쿼리를 검색하는 방법에 대한 자세한 내용은 공급자 설명서를 참조하십시오. 사용 가능한 모든 호스트를 보려면 이 필드를 비워 둡니다.
이름	호스트의 이름입니다. 이 텍스트 필드에는 40자 제한이 있으며 대문자와 소문자, 숫자, 하이픈, 밑줄이 조합된 고유한 이름이어야 합니다.
설명	호스트와 관련된 일반 텍스트인 사람이 읽을 수 있는 주석을 추가하는 필드입니다.

필드 이름	설명
호스트 이름	호스트의 IP 주소 또는 확인 가능한 호스트 이름입니다. 확인 가능한 호스트 이름이 사용되는 경우 호스트의 관리 네트워크에서 사용하는 IP 주소인 IPv4 및 IPv6와 일치하도록 호스트 이름이 확인되는 모든 주소를 확인해야 합니다.
암호	호스트의 root 사용자의 암호입니다. 호스트를 추가할 때 암호를 설정합니다. 암호는 나중에 편집할 수 없습니다.
설치 후 호스트 활성화	성공적으로 설치한 후 호스트를 활성화하려면 이 확인란을 선택합니다. 이는 기본적으로 활성화되어 있으며 하이퍼바이저를 성공적으로 활성화하는 데 필요합니다. 성공적으로 설치되면 이 확인란을 지워 호스트 상태를 유지 관리로 전환할 수 있습니다. 이를 통해 관리자는 하이퍼바이저에서 추가 구성 작업을 수행할 수 있습니다.
설치 후 호스트 재부팅	이 확인란을 선택하여 호스트를 설치한 후 재부팅합니다. 이는 기본적으로 활성화되어 있습니다. 참고 호스트의 커널 명령줄 매개 변수를 변경하거나 클러스터의 방화벽 유형을 변경하려면 호스트를 재부팅해야 합니다.
SSH 공개 키	텍스트 상자의 콘텐츠를 호스트로 인증하기 위해 암호 대신 Manager의 SSH 키를 사용하도록 호스트의 <code>/root/.ssh/authorized_hosts</code> 파일에 복사합니다.
호스트 방화벽 자동 설정	새 호스트를 추가할 때 관리자는 호스트 방화벽에서 필요한 포트를 열 수 있습니다. 이는 기본적으로 활성화되어 있습니다. 이는 고급 매개 변수 입니다.
SSH 지문	호스트의 SSH 지문을 가져와 호스트가 반환할 지문과 비교하여 일치하는지 확인할 수 있습니다. 이는 고급 매개 변수 입니다.

2.5.6.2. 설명된 호스트 전원 관리 설정

Power Management settings(전원 관리 설정) 테이블에는 **New Host**(새 호스트) 또는 **Edit Host** (호스트 편집) 창의 **Power Management**(전원 관리) 탭에 필요한 정보가 포함되어 있습니다. 호스트에 지원

되는 전원 관리 카드가 있는 경우 전원 관리를 구성할 수 있습니다.

표 2.21. 전원 관리 설정

필드 이름	설명
전원 관리 활성화	호스트에서 전원 관리를 활성화합니다. Power Management(전원 관리) 탭에서 나머지 필드를 활성화하려면 이 확인란을 선택합니다.
Kdump 통합	크래시 덤프가 중단되지 않도록 커널 크래시 덤프를 수행하는 동안 호스트가 펜싱되지 않도록 방지합니다. Red Hat Enterprise Linux 7.1 이상에서는 기본적으로 kdump를 사용할 수 있습니다. kdump를 호스트에서 사용할 수 있지만 구성이 올바르지 않은 경우(kdump 서비스를 시작할 수 없음) Kdump 통합 을 활성화하면 호스트(재) 설치에 실패합니다. 기존 호스트에서 Kdump 통합 을 활성화하거나 비활성화하는 경우 호스트를 다시 설치해야 합니다.
전원 관리 정책 제어 비활성화	전원 관리는 호스트 클러스터의 스케줄링 정책에 의해 제어됩니다. 전원 관리가 활성화되고 정의된 낮은 사용률 값에 도달하면 관리자가 호스트 시스템의 전원을 끄고 부하 분산이 필요하거나 클러스터에 사용 가능한 호스트가 충분하지 않은 경우 다시 시작합니다. 이 확인란을 선택하여 정책 제어를 비활성화합니다.
순서별 에이전트	호스트의 펜스 에이전트를 나열합니다. 펜스 에이전트는 순차적으로, 동시 또는 둘 다 혼합될 수 있습니다. ● 펜스 에이전트를 순차적으로 사용하는 경우 기본 에이전트는 먼저 호스트를 중지하거나 시작하는 데 사용되며 실패하는 경우 보조 에이전트가 사용됩니다. ● 펜스 에이전트를 동시에 사용하는 경우 두 펜스 에이전트 모두 호스트가 중지되도록 Stop 명령에 응답해야 합니다. 한 에이전트가 Start 명령에 응답하면 호스트가 시작됩니다. 펜스 에이전트는 기본적으로 순차적입니다. up 및 down 버튼을 사용하여 펜스 에이전트를 사용하는 시퀀스를 변경합니다. 두 펜스 에이전트를 동시에 수행하려면 Concurrent(콘술)에서 다른 펜스 에이전트 옆에 있는 드롭다운 목록을 사용하여 하나의 펜스 에이전트를 선택합니다. 추가 펜스 에이전트 옆에 있는 드롭다운 목록에서 Concurrent (조건)에서 그룹을 선택하여 동시 펜스 에이전트 그룹에 추가 펜스 에이전트를 추가할 수 있습니다.

필드 이름	설명
펜스 에이전트 추가	+ 버튼을 클릭하여 새 펜스 에이전트를 추가합니다. Edit fence agent(펜스 에이전트 편집) 창이 열립니다. 이 창의 필드에 대한 자세한 내용은 아래 표를 참조하십시오.
전원 관리 프록시 환경 설정	기본적으로 Manager가 호스트와 동일한 클러스터 내에서 펜싱 프록시를 검색하도록 지정하며 펜싱 프록시를 찾을 수 없는 경우 Manager는 동일한 dc (데이터 센터)에서 검색합니다. up 및 down 버튼을 사용하여 이러한 리소스를 사용하는 시퀀스를 변경합니다. 이 필드는 Advanced Parameters (고급 매개 변수)에서 사용할 수 있습니다.

다음 테이블에는 **Edit fence agent(펜스 에이전트 편집)** 창에 필요한 정보가 포함되어 있습니다.

표 2.22. 펜스 에이전트 설정 편집

필드 이름	설명
주소	호스트의 전원 관리 장치에 액세스할 주소입니다. 확인 가능한 호스트 이름 또는 IP 주소 중 하나입니다.
사용자 이름	전원 관리 장치에 액세스할 사용자 계정입니다. 장치에서 사용자를 설정하거나 기본 사용자를 사용할 수 있습니다.
암호	전원 관리 장치에 액세스하는 사용자의 암호입니다.

필드 이름	설명
유형	호스트의 전원 관리 장치 유형입니다. 다음 중 하나를 선택합니다. ● APC - APC MasterSwitch 네트워크 전원 스위치. APC 5.x 전원 스위치 장치와 함께 사용하지 않습니다. ● apc_snmp - APC 5.x 전원 스위치 장치에 사용됩니다. ● BladeCenter - IBM Bladecenter 원격 관리자 어댑터. ● cisco_ucs - Cisco 통합 컴퓨팅 시스템. ● drac5 - Dell 컴퓨터용 Dell Remote Access Controller. ● drac7 - Dell 컴퓨터용 Dell 원격 액세스 컨트롤러. ● EPS - ePowerSwitch 8M+ 네트워크 전원 스위치. ● hpblade - HP BladeSystem. ● iLO,ilo2,ilo3,ilo4 - HP Integrated Lights-Out. ● ipmilan - 지능형 플랫폼 관리 인터페이스 및 Sun Integrated Lights Out Management 장치. ● RSA - IBM Remote Supervisor Adapter. ● RSB - Fujitsu-Siemens RSB 관리 인터페이스. ● WTI - WTI 네트워크 전원 스위치. 전원 관리 장치에 대한 자세한 내용은 Power Management in the <i>Technical Reference</i> 를 참조하십시오.
포트	전원 관리 장치에서 호스트와 통신하는 데 사용하는 포트 번호입니다.
슬롯	전원 관리 장치의 블레이드를 식별하는 데 사용되는 번호입니다.
서비스 프로파일	전원 관리 장치의 블레이드를 식별하는 데 사용되는 서비스 프로파일 이름입니다. 장치 유형이 cisco_ucs 인 경우 이 필드는 var 대신 표시됩니다.

필드 이름	설명
옵션	전원 관리 장치별 옵션. 'key=value'로 입력합니다. 사용 가능한 옵션은 호스트의 전원 관리 장치 설명서를 참조하십시오. Red Hat Enterprise Linux 7 호스트의 경우 <code>cisco_ucs</code> 를 전원 관리 장치로 사용하는 경우 <code>ssl_insecure=1</code> 을 Options (옵션) 필드에 추가해야 합니다.
보안	전원 관리 장치가 호스트에 안전하게 연결할 수 있도록 하려면 이 확인란을 선택합니다. 이 작업은 전원 관리 에이전트에 따라 <code>ssh</code> , <code>ssl</code> 또는 기타 인증 프로토콜을 통해 수행할 수 있습니다.

2.5.6.3. 설명된 SPM 우선 순위 설정

SPM 설정 테이블에는 **New Host**(새 호스트) 또는 **Edit Host** (호스트 편집) 창의 **SPM** 탭에 필요한 정보가 자세히 설명되어 있습니다.

표 2.23. SPM 설정

필드 이름	설명
SPM 우선 순위	호스트에 SPM(Storage Pool Manager) 역할이 제공될 가능성을 정의합니다. 옵션은 낮음 , 보통 및 높음 우선 순위입니다. 낮은 우선 순위는 SPM의 역할이 할당된 호스트가 줄어든다는 의미이며, 높은 우선 순위는 호스트가 더 큰 가능성이 있음을 의미합니다. 기본 설정은 Normal입니다.

2.5.6.4. 설명된 호스트 콘솔 설정

콘솔 설정 테이블에는 **New Host**(새 호스트) 또는 **Edit Host** (호스트 편집) 창의 **Console**(콘솔) 탭에 필요한 정보가 자세히 설명되어 있습니다.

표 2.24. 콘솔 설정

필드 이름	설명
표시 주소 덮어쓰기	이 확인란을 선택하여 호스트의 표시 주소를 재정의합니다. 이 기능은 호스트가 내부 IP로 정의하고 NAT 방화벽 뒤에 있는 경우에 유용합니다. 사용자가 가상 시스템이 실행 중인 호스트의 사설 주소를 반환하지 않고 내부 네트워크 외부에서 가상 시스템에 연결하는 경우 시스템은 공용 IP 또는 FQDN(외부 네트워크에서 공용 IP)을 반환합니다.

필드 이름	설명
주소 표시	여기에 지정된 표시 주소는 이 호스트에서 실행되는 모든 가상 시스템에 사용됩니다. 주소는 정규화된 도메인 이름 또는 IP의 형식이어야 합니다.
vGPU Placement	vGPUs의 기본 배치를 지정합니다. ● 통합: 사용 가능한 물리적 카드에서 더 많은 vGPU를 실행하려면 이 옵션을 선택합니다. ● 분리됨: 별도의 물리적 카드에서 각 vGPU를 실행하려면 이 옵션을 선택합니다.

2.5.6.5. 설명된 네트워크 공급자 설정

Network Provider settings(네트워크 프로바이더 설정) 테이블에는 **New Host**(새 호스트) 또는 **Edit Host** (호스트 편집) 창의 **Network Provider**(네트워크 공급업체) 탭에 필요한 정보가 자세히 설명되어 있습니다.

표 2.25. 네트워크 공급자 설정

필드 이름	설명
외부 네트워크 공급자	외부 네트워크 공급자를 추가하고 외부 네트워크 프로바이더가 호스트의 네트워크를 프로비저닝하려면 목록에서 하나를 선택합니다.

2.5.6.6. 설명된 커널 설정

커널 설정 테이블에는 **New Host**(새 호스트) 또는 **Edit Host** (호스트 편집) 창의 **Kernel** (커널) 탭에 필요한 정보를 자세히 설명합니다. 일반적인 커널 부팅 매개 변수 옵션은 체크박스로 나열되므로 쉽게 선택할 수 있습니다.

좀 더 복잡한 변경 사항을 위해 **Kernel** 명령행 옆에 있는 무료 텍스트 항목 필드를 사용하여 필요한 추가 매개 변수에 를 추가합니다. 커널 명령줄 매개변수를 변경하는 경우 **호스트를 다시 설치해야 합니다**.



중요

호스트가 **Manager**에 연결된 경우 변경하기 전에 호스트를 유지 관리 모드에 배치해야 합니다. 변경한 후 **호스트를 다시 설치하여** 변경 사항을 적용합니다.

표 2.26. 커널 설정

필드 이름	설명
hostdev 패스스루 및 SR-IOV	가상 머신이 가상 머신에 직접 연결된 것처럼 호스트 장치를 사용할 수 있도록 커널에서 IOMMU 플래그를 활성화합니다. 호스트 하드웨어 및 펌웨어도 IOMMU를 지원해야 합니다. 가상화 확장 및 IOMMU 확장 기능을 하드웨어에서 활성화해야 합니다. PCI 패스스루에 대한 호스트 구성을 참조하십시오 . IBM POWER8에는 기본적으로 IOMMU가 활성화되어 있습니다.
중첩된 가상화	가상 머신을 가상 머신 내에서 실행할 수 있도록 vmx 또는 svm 플래그를 활성화합니다. 이 옵션은 기술 프리뷰 기능입니다. 평가 목적으로만 사용됩니다. 운영 목적으로 지원되지 않습니다. 이 설정을 사용하려면 호스트에 vdsms-hook-nestedvt 후크를 설치해야 합니다. 자세한 내용은 모든 가상 머신에 대해 중첩된 가상화 활성화 및 개별 가상 머신의 중첩된 가상화 활성화 를 참조하십시오.
안전하지 않은 인터럽트	하드웨어가 인터럽트 재 매핑을 지원하지 않기 때문에 IOMMU가 활성화되어 있지만 통과가 실패하면 이 옵션을 활성화하는 것이 좋습니다. 호스트의 가상 시스템이 신뢰할 수 있는 경우에만 이 옵션을 활성화해야 합니다. 옵션을 활성화하면 가상 시스템에서 호스트를 MSI 공격에 노출할 수 있습니다. 이 옵션은 평가를 위해 인증되지 않은 하드웨어를 사용할 때만 해결 방법으로 사용할 수 있습니다.
PCI 제한당	SR-IOV NIC가 메모리 문제로 인해 가상 기능을 할당할 수 없는 경우 이 옵션을 활성화하는 것이 좋습니다. 호스트 하드웨어 및 펌웨어에서도 PCI 제한당을 지원해야 합니다. 이 옵션은 평가를 위해 인증되지 않은 하드웨어를 사용할 때만 해결 방법으로 사용할 수 있습니다.
블랙리스트 노바로	부트로니를 차단합니다. Nvidia GPU는 공급업체가 제공하는 드라이버와 충돌하는 NVIDIA GPU를 위한 커뮤니티 드라이버입니다. 벤더 드라이버가 우선하는 경우 no rules driver는 차단해야 합니다.
SMT 비활성화	SMT(동시 멀티 스레드)를 비활성화합니다. SMT를 비활성화하면 L1TF 또는 MDS와 같은 보안 취약점이 완화될 수 있습니다.
FIPS 모드	FIPS 모드를 활성화합니다. 자세한 내용은 Manager를 사용하여 FIPS 활성화 를 참조하십시오.
커널 명령줄	이 필드를 사용하면 기본 매개변수에 커널 매개변수를 추가할 수 있습니다.



참고

커널 부팅 매개 변수가 회색으로 표시되면 **reset** (재설정) 버튼을 클릭하면 옵션을 사용할 수 있습니다.

2.5.6.7. 호스트 엔진 설정 설명

Hosted Engine settings(호스팅 엔진 설정) 테이블에는 **New Host**(새 호스트) 또는 **Edit Host** (호스트 편집) 창의 **Hosted Engine**(호스팅 엔진) 탭에 필요한 정보가 자세히 설명되어 있습니다.

표 2.27. 호스트 엔진 설정

필드 이름	설명
호스팅 엔진 배포 작업 선택	다음 세 가지 옵션을 사용할 수 있습니다. ● none - 작업이 필요하지 않습니다. ● 배포 - 호스트를 자체 호스팅 엔진 노드로 배포하려면 이 옵션을 선택합니다. ● 배포 취소 - 셀프 호스팅 엔진 노드의 경우 이 옵션을 선택하여 호스트를 배포 취소하고 자체 호스팅 엔진 관련 구성을 제거할 수 있습니다.

2.5.7. 호스트 복원력

2.5.7.1. 호스트 고가용성

Red Hat Virtualization Manager는 펜싱을 사용하여 클러스터의 호스트 응답성을 유지합니다. 무 응답 호스트는 비작동 호스트와 다릅니다. 비작동 호스트는 관리자에서 와 통신할 수 있지만 잘못된 구성이 있습니다(예: 논리적 네트워크가 누락됨). 비응답 호스트는 관리자가 와 통신할 수 없습니다.

펜싱을 사용하면 클러스터가 예기치 않은 호스트 오류에 대응하고 절전, 로드 밸런싱 및 가상 시스템 가용성 정책을 시행할 수 있습니다. 호스트의 전원 관리 장치에 대한 펜싱 매개 변수를 구성하고 수시로 정확성을 테스트해야 합니다. 펜싱 작업에서 무응답 호스트는 재부팅되며 호스트가 규정된 시간 내에 활성 상태로 반환되지 않으면 대기 중인 수동 개입 및 문제 해결이 그대로 유지됩니다.

참고

펜싱 매개 변수를 자동으로 확인하려면 **PMHealthCheckEnabled**(기본적으로 **False**) 및 **PMHealthCheck IntervalInSec** (기본값으로 3600초) **engine-config** 옵션을 구성할 수 있습니다.

true로 설정하면 **PMHealthCheckEnabled** 는 **PMHealthCheckIntervalInSec** 에서 지정한 간격으로 모든 호스트 에이전트를 확인하고 문제를 탐지하는 경우 경고를 표시합니다. **engine-config** 옵션 구성에 대한 자세한 내용은 **engine-config** 명령의 **Syntax** 를 참조하십시오.

전원 관리 작업은 **Red Hat Virtualization Manager**가 재부팅한 후 프록시 호스트에서 수행하거나 관리 포털에서 수동으로 수행할 수 있습니다. 무응답 호스트에서 실행되는 모든 가상 시스템이 중지되고 고가용성 가상 시스템이 다른 호스트에서 시작됩니다. 전원 관리 작업에는 두 개 이상의 호스트가 필요합니다.

Manager가 시작되면 유휴 시간(기본값 5분)이 경과한 후 전원 관리가 활성화된 무응답 호스트를 자동으로 펜싱하려고 합니다. **DisableFenceAtStartupInSec engine-config** 옵션을 업데이트하여 유휴 시간을 구성할 수 있습니다.

참고

DisableFenceAtStartupInSec engine-config 옵션은 관리자가 부팅하는 동안 호스트를 펜싱하려고 하는 시나리오를 방지하는 데 도움이 됩니다. 이는 일반적으로 호스트의 부팅 프로세스가 관리자 부팅 프로세스보다 길기 때문에 데이터 센터 중단 후에 발생할 수 있습니다.

호스트는 전원 관리 매개 변수를 사용하여 프록시 호스트에서 자동으로 펜싱하거나, 호스트를 마우스 오른쪽 버튼으로 클릭하고 메뉴에서 옵션을 사용하여 수동으로 펜싱할 수 있습니다.

중요

호스트에서 고가용성 가상 시스템을 실행하는 경우 전원 관리를 활성화하고 구성해야 합니다.

2.5.7.2. Red Hat Virtualization에서 프록시로 전원 관리

Red Hat Virtualization Manager는 펜싱 에이전트와 직접 통신하지 않습니다. 대신 **Manager**는 프록시를 사용하여 전원 관리 명령을 호스트 전원 관리 장치로 전송합니다. **Manager**는 **VDSM**을 사용하여 전

원 관리 장치 작업을 실행하므로 환경의 다른 호스트를 펜싱 프록시로 사용합니다.

다음 중 선택할 수 있습니다.

- 펜싱을 필요로 하는 호스트와 동일한 클러스터에 있는 모든 호스트입니다.
- 펜싱을 필요로 하는 호스트와 동일한 데이터 센터에 있는 모든 호스트입니다.

실행 가능한 펜싱 프록시 호스트의 상태는 **UP** 또는 **Maintenance** 입니다.

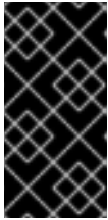
2.5.7.3. 호스트에서 펜싱 매개 변수 설정

호스트 펜싱의 매개 변수는 **New Host**(새 호스트) 또는 **Edit Host** (호스트 편집) 창의 **Power Management** (전원 관리) 필드를 사용하여 설정됩니다. 전원 관리를 사용하면 시스템은 **RAC(Remote Access Card)**와 같은 추가 인터페이스를 사용하여 문제가 있는 호스트를 펜싱할 수 있습니다.

모든 전원 관리 작업은 **Red Hat Virtualization Manager**에서 직접 사용하는 것과 달리 프록시 호스트를 사용하여 수행됩니다. 전원 관리 작업에는 두 개 이상의 호스트가 필요합니다.

절차

1. **Compute**(컴퓨팅) → **Hosts**(호스트) 를 클릭하고 호스트를 선택합니다.
2. **Edit**(편집)를 클릭합니다.
3. **Power Management**(전원 관리) 탭을 클릭합니다.
4. **Enable Power Management** (전원 관리 활성화) 확인란을 선택하여 필드를 활성화합니다.
5. **Kdump** 통합 확인란을 선택하여 커널 크래시 덤프를 수행하는 동안 호스트가 펜싱되지 않도록 합니다.



중요

기존 호스트에서 **Kdump** 통합을 활성화하거나 비활성화하는 경우 호스트를 다시 설치해야 합니다.

6. 선택적으로 호스트 클러스터의 스케줄링 정책에서 호스트의 전원 관리를 제어하지 않으려면 전원 관리의 정책 제어 비활성화 확인란을 선택합니다.
7. **+** 버튼을 클릭하여 새 전원 관리 장치를 추가합니다. **Edit fence agent**(펜스 에이전트 편집) 창이 열립니다.
8. 전원 관리 장치의 **Address** (주소), **User Name** (사용자 이름) 및 **Password** (암호)를 입력합니다.
9. 드롭다운 목록에서 전원 관리 장치 유형을 선택합니다.
10. 전원 관리 장치에서 사용하는 **SSH** 포트 번호를 입력하여 호스트와 통신합니다.
11. 전원 관리 장치의 블레이드를 식별하는 데 사용되는 번호 입력.
12. 전원 관리 장치의 옵션을 입력합니다. 쉼표로 구분된 '**key=value**' 항목 목록을 사용합니다.
13. **Secure** (보안) 확인란을 선택하여 전원 관리 장치를 호스트에 안전하게 연결할 수 있습니다.
14. **Test**(테스트) 버튼을 클릭하여 설정이 올바른지 확인합니다. 테스트 성공, 호스트 상태는: **on** 이 성공적으로 확인되면 표시됩니다.



주의

전원 관리 매개 변수(사용자, 암호, 옵션 등)는 **Red Hat Virtualization Manager**에서 설치 및 수동으로 테스트한 후에만 테스트됩니다. 잘못된 매개 변수에 대한 경고를 무시하거나 **Red Hat Virtualization Manager**의 해당 변경 없이 전원 관리 하드웨어에서 매개 변수가 변경되면 펜싱이 실패할 수 있습니다.

15.

OK(확인)를 클릭하여 **Edit fence agent**(펜스 에이전트 편집) 창을 닫습니다.

16.

Power Management(전원 관리) 탭에서 **Advanced Parameters** (고급 매개 변수)를 확장하고 **up** 및 **down** 버튼을 사용하여 관리자가 펜싱 프록시에 대해 호스트의 클러스터 및 **dc** (**datacenter**)를 검색하는 순서를 지정합니다.

17.

OK(확인)를 클릭합니다.

호스트 목록으로 돌아갑니다. 이제 호스트 이름 옆에 느낌표가 사라졌고 전원 관리가 성공적으로 구성되었음을 나타냅니다.

2.5.7.4. fence_kdump 고급 구성

kdump

호스트 이름을 클릭하여 세부 정보 보기의 **General**(일반) 탭에서 **kdump** 서비스의 상태를 확인합니다.

- **enabled:** kdump가 올바르게 구성되고 kdump 서비스가 실행됩니다.
- **Disabled:** kdump 서비스가 실행되고 있지 않습니다(이 경우 kdump 통합이 제대로 작동하지 않음).

•

unknown: kdump 상태를 보고하지 않는 이전 **VDSM** 버전이 있는 호스트에만 발생합니다.

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

fence_kdump

New Host(새 호스트) 또는 **Edit Host** (호스트 편집) 창의 **Power Management**(전원 관리) 탭에서 **Kdump** 통합을 활성화하면 표준 **fence_kdump** 설정이 구성됩니다. 환경의 네트워크 구성이 단순하고 **Manager**의 **FQDN**이 모든 호스트에서 확인할 수 있는 경우 기본 **fence_kdump** 설정을 사용하기에 충분합니다.

그러나 **fence_kdump**의 고급 구성이 필요한 몇 가지 경우가 있습니다. 더 복잡한 네트워킹이 있는 환경에는 **Manager**, **fence_kdump** 리스너 또는 둘 다의 구성을 수동으로 변경해야 할 수 있습니다. 예를 들어, 관리자의 **FQDN**이 **Kdump** 통합이 활성화된 모든 호스트에서 확인할 수 없는 경우 **engine-config**를 사용하여 적절한 호스트 이름 또는 **IP** 주소를 설정할 수 있습니다.

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

다음 예제 사례에는 구성 변경이 필요할 수도 있습니다.

•

Manager에는 두 개의 **NIC**가 있습니다. 여기서 하나는 공용입니다. 두 번째는 **fence_kdump** 메시지의 기본 대상입니다.

•

다른 **IP** 또는 포트에서 **fence_kdump** 리스너를 실행해야 합니다.

•

가능한 패킷 손실을 방지하기 위해 **fence_kdump** 알림 메시지에 대한 사용자 지정 간격을 설정해야 합니다.

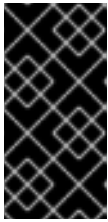
기본 구성 변경은 더 복잡한 네트워킹 설정에만 필요하므로 사용자 지정 **fence_kdump** 탐지 설정이 고급 사용자에게만 권장됩니다.

2.5.7.5. fence_kdump 리스너 구성

fence_kdump 리스너의 구성을 편집합니다. 기본 구성이 충분하지 않은 경우에만 필요합니다.

절차

1. `/etc/ovirt-engine/ovirt-fence-kdump-listener.conf.d`에서 새 파일(예: `my-fence-kdump.conf.conf`)을 만듭니다.
2. **OPTION=** 구문으로 사용자 지정을 입력하고 파일을 저장합니다.



중요

관리자의 **fence-kdump** 구성의 **fence_kdump** 구성 옵션 표에 설명된 대로 **engine-config**에서 편집된 값도 변경해야 합니다.

3. **fence_kdump** 리스너를 다시 시작합니다.

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

필요한 경우 다음 옵션을 사용자 지정할 수 있습니다.

표 2.28. **fence_kdump** 리스너 구성 옵션

Variable	설명	Default	참고
LISTENER_ADDRESS	fence_kdump 메시지를 수신할 IP 주소를 정의합니다.	0.0.0.0	이 매개 변수의 값이 변경되면 engine-config 의 FenceKdumpDestinationAddress 값과 일치해야 합니다.
LISTENER_PORT	에서 fence_kdump 메시지를 받을 포트를 정의합니다.	7410	이 매개 변수의 값이 변경되면 engine-config 의 FenceKdumpDestinationPort 값과 일치해야 합니다.
HEARTBEAT_INTERVAL	리스너의 하트비트 업데이트 간격(초)을 정의합니다.	30	이 매개 변수의 값이 변경되면 engine-config 의 FenceKdumpListenerTimeout 값보다 크기 절반 이하이어야 합니다.

Variable	설명	Default	참고
SESSION_SYNC_INTERVAL	메모리의 리스너 호스트 kdumping 세션을 데이터 베이스에 동기화하는 간격(초)을 정의합니다.	5	이 매개 변수의 값이 변경 되면 engine-config 의 KdumpStartedTimeout 값보다 크기 절반 이하 이어야 합니다.
REOPEN_DB_CONNECTION_INTERVAL	이전에 사용할 수 없는 데이터베이스 연결을 다시 열 수 있는 간격(초)을 정의합니다.	30	-
KDUMP_FINISHED_TIMEOUT	호스트 kdump 흐름이 FINISHED로 표시된 후 kdump 호스트에서 마지막으로 수신된 메시지 이후 최대 시간 초과(초)를 정의합니다.	60	이 매개 변수의 값이 변경 되면 engine-config 의 FenceKdumpMessageInterval 값보다 크기가 두 배 이상이어야 합니다.

2.5.7.6. Manager에서 fence_kdump 구성

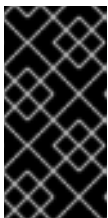
Manager의 **kdump** 구성을 편집합니다. 기본 구성이 충분하지 않은 경우에만 필요합니다. 현재 구성 값은 다음을 사용하여 찾을 수 있습니다.

engine-config -g *OPTION*

절차

1. **engine-config** 명령을 사용하여 **kdump** 구성을 편집합니다.

engine-config -s *OPTION=value*



중요

편집된 값은 **Kdump** 구성 옵션 테이블에 설명된 대로 **fence_kdump** 리스너 구성 파일에서도 변경해야 합니다. **fence_kdump** 리스너 구성을 참조하십시오.

2. **ovirt-engine** 서비스를 다시 시작하십시오.

systemctl restart ovirt-engine.service

3.

필요한 경우 **Kdump** 통합이 활성화된 모든 호스트를 다시 설치합니다(아래 표 참조).

다음 옵션은 **engine-config** 를 사용하여 구성할 수 있습니다.

표 2.29. kdump 구성 옵션

Variable	설명	Default	참고
FenceKdumpDestinationAddress	fence_kdump 메시지를 보낼 호스트 이름 또는 IP 주소를 정의합니다. 비어 있는 경우 Manager의 FQDN이 사용됩니다.	빈 문자열 (Manager FQDN 사용)	이 매개 변수의 값이 변경되면 fence_kdump 리스너 구성 파일의 LISTENER_ADDRESS 값과 일치해야 하며 Kdump 통합 이 활성화된 모든 호스트를 다시 설치해야 합니다.
FenceKdumpDestinationPort	fence_kdump 메시지를 보낼 포트를 정의합니다.	7410	이 매개 변수의 값이 변경된 경우 fence_kdump 리스너 구성 파일의 LISTENER_PORT 값과 일치해야 하며 Kdump 통합 이 활성화된 모든 호스트를 다시 설치해야 합니다.
FenceKdumpMessageInterval	fence_kdump에서 보낸 메시지 간 간격(초)을 정의합니다.	5	이 매개 변수의 값이 변경된 경우 fence_kdump 리스너 구성 파일에서 KDUMP_FINISHED_TIMEOUT 값보다 크기 절반 이하이어야 하며 Kdump 통합 이 활성화된 모든 호스트를 다시 설치해야 합니다.
FenceKdumpListenerTimeout	fence_kdump 리스너를 활성 상태로 간주하기 위해 마지막 하트비트 이후 최대 시간 초과(초)를 정의합니다.	90	이 매개 변수의 값이 변경된 경우 fence_kdump 리스너 구성 파일의 HEARTBEAT_INTERVAL 값보다 크기 두 배 이상이어야 합니다.

Variable	설명	Default	참고
KdumpStartedTimeout	kdumping 호스트의 첫 번째 메시지가 수신될 때까지 대기하는 최대 시간 초과 시간(초)을 정의합니다(호스트 kdump 흐름이 시작됨).	30	이 매개 변수의 값이 변경된 경우 fence_kdump 리스너 구성 파일에서 SESSION_SYNC_INTERVAL 값보다 크기 두 배 이상이어야 하며 FenceKdumpMessageInterval 가 있어야 합니다.

2.5.7.7. 소프트 펜싱 호스트

예기치 않은 문제로 인해 호스트는 응답하지 않을 수 있으며 **VDSM**은 요청에 응답할 수 없지만 **VDSM**에 의존하는 가상 시스템은 활성 상태로 유지되고 액세스가 가능합니다. 이러한 상황에서 **VDSM**을 다시 시작하면 **VDSM**이 응답 상태가 되고 이 문제가 해결됩니다.

"SSH 소프트 펜싱"은 관리자가 응답하지 않는 호스트에서 SSH를 통해 **VDSM**을 다시 시작하려고 하는 프로세스입니다. 관리자가 SSH를 통해 **VDSM**을 다시 시작하지 못하면 외부 펜싱 에이전트가 구성된 경우 펜싱이 외부 펜싱 에이전트로 전환됩니다.

SSH를 통한 소프트 펜싱은 다음과 같이 작동합니다. 호스트에서 펜싱을 구성하고 활성화해야 하며 유효한 프록시 호스트(두 번째 호스트, 데이터 센터에는 **UP** 상태)가 있어야 합니다. **Manager**와 호스트 간의 연결이 시간 초과되면 다음이 수행됩니다.

1. 첫 번째 네트워크 오류 시 호스트 상태가 "연결 중"으로 변경됩니다.
2. 그런 다음 관리자는 **VDSM**에 상태를 요청하거나 호스트의 부하에 의해 결정된 간격을 대기하는 세 번의 시도를 합니다. 간격의 길이를 결정하는 공식은 구성 값 **TimeoutToResetVdsInSeconds** (기본값은 60 초) + [**DelayResetPerVmInSeconds** (기본값은 0.5초)]*(호스트에서 실행 중인 가상 시스템의 개수) + [**DelayResetForSpmlnSeconds**(기본값은 20초임)] * 1 (호스트가 **SPM**으로 실행되는 경우) 또는 0 (호스트가 **SPM**으로 실행되지 않는 경우). **VDSM**에 응답할 최대 시간을 제공하기 위해 관리자는 위에서 언급한 두 옵션 중 더 긴 시간을 선택합니다(**VDSM**의 상태 검색 또는 위의 공식에 의해 결정된 간격 검색).
3. 간격이 경과하면 호스트가 응답하지 않으면 SSH를 통해 **vdsm**이 다시 시작됩니다.
4. 호스트와 관리자 간의 연결을 다시 설정할 때 **vdsm** 재시작에 성공하지 못하면 호스트 상태가 **Non Responsive** (응답 없음)로 변경되고 전원 관리가 구성된 경우 펜싱이 외부 펜싱 에이전

트에 전달됩니다.



참고

전원 관리가 구성되지 않은 호스트에서 **SSH**를 통한 소프트웨어 펜싱을 실행할 수 있습니다. "펜싱"과 다릅니다. 펜싱은 전원 관리가 구성된 호스트에서만 실행할 수 있습니다.

2.5.7.8. 호스트 전원 관리 기능 사용

호스트에 전원 관리가 구성된 경우 관리 포털 인터페이스에서 여러 옵션에 액세스할 수 있습니다. 각 전원 관리 장치에는 사용자 지정 가능한 고유한 옵션이 있지만, 모두 호스트를 시작, 중지 및 다시 시작하는 기본 옵션을 지원합니다.

절차

1.

Compute(컴퓨팅) → **Hosts**(호스트) 를 클릭하고 호스트를 선택합니다.

2.

Management(관리) 드롭다운 메뉴를 클릭하고 다음 **Power Management** 옵션 중 하나를 선택합니다.

•

재시작: 이 옵션은 호스트를 중지하고 호스트 상태가 **Down** 으로 변경될 때까지 기다립니다. 에이전트에서 호스트가 다운되었음을 확인하면 클러스터의 다른 호스트에서 고가용성 가상 시스템이 다시 시작됩니다. 그런 다음 에이전트는 이 호스트를 다시 시작합니다. 호스트가 사용 준비가 되면 상태가 **Up** 으로 표시됩니다.

•

시작: 이 옵션은 호스트를 시작하고 클러스터에 참여할 수 있도록 합니다. 사용할 준비가 되면 상태가 **Up** 으로 표시됩니다.

•

중지: 이 옵션은 호스트 전원을 끕니다. 이 옵션을 사용하기 전에 호스트에서 실행 중인 가상 시스템이 클러스터의 다른 호스트로 마이그레이션되었는지 확인합니다. 그렇지 않으면 가상 시스템이 충돌하고 고가용성 가상 시스템만 다른 호스트에서 다시 시작됩니다. 호스트가 중지되면 상태가 **Non-Operational** (비작동)으로 표시됩니다.



참고

Power Management(전원 관리)가 활성화되지 않으면 호스트를 선택하고, **Management**(관리) 드롭다운 메뉴를 클릭하고, **SSH Management** (SSH 관리) 옵션인 **Restart** (재시작) 또는 **Stop** (중지)을 선택하여 호스트를 다시 시작하거나 중지할 수 있습니다.



중요

호스트에 두 개의 펜싱 에이전트를 정의하면 동시에 또는 순차적으로 사용할 수 있습니다. 동시 에이전트의 경우 두 에이전트 모두 호스트가 중지되도록 **Stop** 명령에 응답해야 하며, 한 에이전트가 **Start** 명령에 응답하면 호스트가 시작됩니다. 순차 에이전트의 경우 호스트를 시작하거나 중지하려면 먼저 기본 에이전트를 사용합니다. 실패하면 보조 에이전트가 사용됩니다.

3.

OK(확인)를 클릭합니다.

2.5.7.9. 응답이 없는 호스트 수동 펜싱 또는 격리

예를 들어 하드웨어 장애로 인해 호스트가 예기치 않게 응답하지 않는 상태가 되면 환경의 성능에 큰 영향을 줄 수 있습니다. 전원 관리 장치가 없거나 잘못 구성된 경우 호스트를 수동으로 재부팅할 수 있습니다.



주의

호스트를 수동으로 재부팅하지 않은 경우 '**Host has been Rebooted**' (호스트가 재부팅되었는지 확인)를 선택하지 마십시오. 호스트가 실행되는 동안 이 옵션을 사용하면 가상 시스템 이미지가 손상될 수 있습니다.

절차

1. 관리 포털에서 **Compute**(컴퓨팅 → **Hosts** (호스트))를 클릭하고 호스트 상태가 **Non Responsive** (응답 없음)인지 확인합니다.
2. 수동으로 호스트를 재부팅합니다. 물리적으로 랩에 진입하고 호스트를 재부팅할 수 있습니다.

3.

관리 포털에서 호스트를 선택하고 **More Actions** (추가 작업)(



)를 클릭한 다음 **Confirm 'Host has been Rebooted'**(호스트가 재부팅됨)를 클릭합니다.

4.

Approve Operation(작업 승인) 확인란을 선택하고 **OK**(확인)를 클릭합니다.

5.

호스트를 부팅하는 데 시간이 오래 걸리는 경우 **ServerRebootTimeout** 을 설정하여 호스트가 무응답임을 확인하기 전에 대기 할 초 (초)를 지정할 수 있습니다.

```
# engine-config --set ServerRebootTimeout=integer
```

2.6. 스토리지

2.6.1. Red Hat Virtualization 스토리지 정보

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

- 네트워크 파일 시스템(**NFS**)
- 기타 **POSIX** 호환 파일 시스템
- **iSCSI**(Internet Small Computer System Interface)
- 가상화 호스트에 직접 연결된 로컬 스토리지
- **FCP**(Fibre Channel Protocol)
- 병렬 **NFS**(**pNFS**)

스토리지 도메인을 연결하고 활성화하지 않는 한 데이터 센터를 초기화할 수 없기 때문에 스토리지 설정은 새 데이터 센터의 전제 조건입니다.

Red Hat Virtualization 시스템 관리자는 가상화된 엔터프라이즈용 스토리지를 생성, 구성, 연결 및 유지 관리합니다. 스토리지 유형과 그 용도를 잘 알고 있어야 합니다. 스토리지 어레이 벤더의 가이드를 읽고 [스토리지 장치의 개념, 프로토콜, 요구 사항 및 일반적인 사용 방법에 대한 자세한 내용은 Red Hat Enterprise Linux 관리](#) 스토리지 장치를 참조하십시오.

스토리지 도메인을 추가하려면 관리 포털에 성공적으로 액세스할 수 있어야 하며 **Up** 상태와 연결된 호스트가 하나 이상 있어야 합니다.

Red Hat Virtualization에는 세 가지 유형의 스토리지 도메인이 있습니다.

•

데이터 도메인: 데이터 도메인에는 모든 가상 시스템 및 템플릿의 가상 하드 디스크와 **OVF** 파일이 데이터 센터에 있습니다. 또한 가상 시스템의 스냅샷도 데이터 도메인에 저장됩니다.

데이터 도메인은 데이터 센터에서 공유할 수 없습니다. 여러 유형의 데이터 도메인(**iSCSI, NFS, FC, POSIX, Gluster**)은 로컬 도메인이 아닌 공유된 경우 동일한 데이터 센터에 추가할 수 있습니다.

다른 유형의 도메인을 연결하려면 데이터 도메인을 데이터 센터에 연결해야 합니다.

•

ISO 도메인: **ISO** 도메인은 가상 시스템의 운영 체제와 애플리케이션을 설치하고 부팅하는 데 사용되는 **ISO** 파일(또는 논리적 **CD**)을 저장합니다. **ISO** 도메인은 물리적 미디어에 대한 데이터 센터의 필요성을 제거합니다. **ISO** 도메인은 여러 데이터 센터에서 공유할 수 있습니다. **ISO** 도메인은 **NFS** 기반만 가능합니다. 하나의 **ISO** 도메인만 데이터 센터에 추가할 수 있습니다.

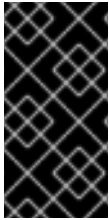
•

도메인 내보내기: 내보내기 도메인은 데이터 센터와 **Red Hat Virtualization** 환경 간에 이미지를 복사하고 이동하는 데 사용되는 임시 스토리지 리포지토리입니다. 내보내기 도메인을 사용하여 가상 시스템을 백업할 수 있습니다. 내보내기 도메인은 데이터 센터 간에 이동할 수 있지만 한 번에 하나의 데이터 센터에서만 활성화할 수 있습니다. 내보내기 도메인은 **NFS** 기반만 가능합니다. 데이터 센터에 하나의 내보내기 도메인만 추가할 수 있습니다.



참고

내보내기 스토리지 도메인은 더 이상 사용되지 않습니다. 스토리지 데이터 도메인은 데이터 센터에서 연결을 해제하고 동일한 환경이나 다른 환경에서 다른 데이터 센터로 가져올 수 있습니다. 그런 다음 가져온 스토리지 도메인에서 연결된 데이터 센터로 가상 시스템, 유동 가상 디스크 및 템플릿을 업로드할 수 있습니다. 스토리지 도메인 [가져오기에 대한](#) 자세한 내용은 기존 스토리지 도메인 가져오기를 참조하십시오.



중요

데이터 센터의 스토리지 요구 사항을 확인한 후에만 **Red Hat Virtualization** 환경에 대한 스토리지 구성 및 연결을 시작합니다.

2.6.2. 스토리지 도메인 이해

스토리지 도메인은 공통 스토리지 인터페이스가 있는 이미지 컬렉션입니다. 스토리지 도메인에는 템플릿 및 가상 시스템(스냅샷 포함) 또는 **ISO** 파일의 전체 이미지가 포함되어 있습니다. 스토리지 도메인은 블록 장치(**SAN - iSCSI** 또는 **FCP**) 또는 파일 시스템(**NAS - NFS, GlusterFS** 또는 기타 **POSIX** 호환 파일 시스템)으로 만들 수 있습니다.

기본적으로 **GlusterFS** 도메인 및 로컬 스토리지 도메인은 **4K** 블록 크기를 지원합니다. 특히 대용량 작업을 사용할 때 **4K** 블록 크기는 더 나은 성능을 제공할 수 있으며 **VDO**와 같은 **4K** 호환성이 필요한 툴을 사용할 수도 있습니다.



참고

GlusterFS 스토리지는 더 이상 사용되지 않으며 향후 릴리스에서 더 이상 지원되지 않습니다.

NFS에서 모든 가상 디스크, 템플릿 및 스냅샷은 파일입니다.

SAN(iSCSI/FCP)에서 각 가상 디스크, 템플릿 또는 스냅샷은 논리 볼륨입니다. 블록 장치는 볼륨 그룹이라는 논리 엔터티로 집계된 다음 **LVM**(논리 볼륨 관리자)으로 나누어 가상 하드 디스크로 사용합니다. **LVM**에 대한 자세한 내용은 [Red Hat Enterprise Linux 구성 및 논리 볼륨 관리](#)를 참조하십시오.

가상 디스크는 **QCOW2** 또는 **raw**의 두 가지 형식 중 하나를 가질 수 있습니다. 스토리지 유형은 스파스이거나 사전 할당할 수 있습니다. 스냅샷은 항상 스파스이지만 두 형식 모두 디스크에 대해 취할 수 있습니다.

동일한 스토리지 도메인을 공유하는 가상 시스템은 동일한 클러스터에 속하는 호스트 간에 마이그레이션할 수 있습니다.

2.6.3. NFS 스토리지 준비 및 추가

2.6.3.1. NFS 스토리지 준비

Red Hat Enterprise Virtualization Host 시스템에서 스토리지 도메인 역할을 할 파일 스토리지 스토리지 또는 원격 서버에 **NFS** 공유를 설정합니다. 원격 스토리지에서 공유를 내보내 **Red Hat Virtualization Manager**에서 구성한 후 **Red Hat Virtualization** 호스트에서 공유를 자동으로 가져옵니다.

NFS 설정, 구성, 마운트 및 내보내기에 대한 자세한 내용은 **Red Hat Enterprise Linux 8**의 [파일 시스템](#) 관리를 참조하십시오.

Red Hat Virtualization에는 특정 시스템 사용자 계정 및 시스템 사용자 그룹이 필요하므로 관리자가 내보낸 디렉토리로 표시된 스토리지 도메인에 데이터를 저장할 수 있습니다. 다음 절차에서는 하나의 디렉터리에 대한 권한을 설정합니다. **Red Hat Virtualization**에서 스토리지 도메인으로 사용할 모든 디렉터리에 대해 **chown** 및 **chmod** 단계를 반복해야 합니다.

사전 요구 사항

1. **NFS utils** 패키지를 설치합니다.

```
# dnf install nfs-utils -y
```

2. 활성화된 버전을 확인하려면 다음을 수행합니다.

```
# cat /proc/fs/nfsd/versions
```

3. 다음 서비스를 활성화합니다.

```
# systemctl enable nfs-server
# systemctl enable rpcbind
```

절차

1. 그룹 **kvm** 을 만듭니다.

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

2. **kvm** 그룹에 **vdsm** 사용자를 생성합니다.

```
# useradd vdsm -u 36 -g kvm
```

3.

스토리지 디렉토리를 생성하고 액세스 권한을 수정합니다.

```
# mkdir /storage
# chmod 0755 /storage
# chown 36:36 /storage/
```

4.

관련 권한을 사용하여 스토리지 디렉토리를 **/etc/exports**에 추가합니다.

```
# vi /etc/exports
# cat /etc/exports
/storage *(rw)
```

5.

다음 서비스를 다시 시작하십시오.

```
# systemctl restart rpcbind
# systemctl restart nfs-server
```

6.

특정 IP 주소에 사용할 수 있는 내보내기를 보려면 다음을 수행합니다.

```
# exportfs
/nfs_server/srv
10.46.11.3/24
/nfs_server <world>
```



참고

서비스를 시작한 후 **/etc/exports**를 변경한 경우 **exportfs -ra** 명령을 사용하여 변경 사항을 다시 로드할 수 있습니다. 위의 모든 단계를 수행하고 나면 **exports** 디렉터리가 준비되고 다른 호스트에서 테스트하여 사용할 수 있는지 확인할 수 있습니다.

2.6.3.2. NFS 스토리지 추가

다음 절차에서는 기존 NFS 스토리지를 Red Hat Virtualization 환경에 데이터 도메인으로 연결하는 방법을 설명합니다.

ISO 또는 내보내기 도메인이 필요한 경우 다음 절차를 사용하되 **Domain Function** (도메인 기능) 목록에서 **ISO** 또는 **Export** (내보내기)를 선택합니다.

절차

1. 관리 포털에서 **Storage** → **Domains** (도메인) 를 클릭합니다.
2. **New Domain** (새 도메인)을 클릭합니다.
3. 스토리지 도메인 의 이름을 입력합니다.
4. **Data Center** (데이터 센터),**Domain Function** (도메인 기능),**Storage Type** (스토리지 유형),**Format** (형식) 및 **Host**(호스트) 목록의 기본값을 수락합니다.
5. 스토리지 도메인에 사용할 **Export Path** (내보내기 경로)를 입력합니다. 내보내기 경로는 **123.123.0.10:/data** (IPv4), **[2001:0:0:0:0:0:0:5db1]:/data** (IPv6) 또는 **domain.example.com:/data** 형식이어야 합니다.
6. 선택적으로 고급 매개변수를 구성할 수 있습니다.
 - a. **Advanced Parameters** (고급 매개 변수)를 클릭합니다.
 - b. **Warninglow Space Indicator**(낮은 공간 표시기) 필드에 백분율 값을 입력합니다. 스토리지 도메인에서 사용 가능한 여유 공간이 이 백분율 미만인 경우 경고 메시지가 사용자에게 표시되고 기록됩니다.
 - c. **Critical Space Action Blocker** (심각 공간 작업 블록) 필드에 **GB** 값을 입력합니다. 스토리지 도메인에서 사용 가능한 여유 공간이 이 값보다 작으면 사용자에게 오류 메시지가 표시되고 기록되고 공간을 소비하는 새 작업이 차단됩니다.
 - d. **Wipe after Delete**(삭제 후 **Wipe after Delete**) 확인란을 선택하여 삭제 후 지우기 옵션을 활성화합니다. 이 옵션은 도메인을 만든 후에 편집할 수 있지만, 이렇게 하면 이미 존재하는 디스크의 삭제 속성 후에는 **wipe**가 변경되지 않습니다.
7. **OK**(확인)를 클릭합니다.

새 **NFS** 데이터 도메인의 상태는 디스크가 준비될 때까지 **Locked**(잠김) 입니다. 그러면 데이터 도메인이 자동으로 데이터 센터에 연결됩니다.

2.6.3.3. NFS 스토리지 증가

NFS 스토리지의 양을 늘리려면 새 스토리지 도메인을 생성하여 기존 데이터 센터에 추가하거나 **NFS** 서버에서 사용 가능한 여유 공간을 늘릴 수 있습니다. 이전 옵션의 경우 [NFS 스토리지 추가](#)를 참조하십시오. 다음 절차에서는 기존 **NFS** 서버에서 사용 가능한 여유 공간을 늘리는 방법을 설명합니다.

절차

1. **Storage**(스토리지 → **Domains** (도메인) 를 클릭합니다.
2. **NFS** 스토리지 도메인의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Data Center**(데이터 센터) 탭을 클릭하고 **Maintenance**(유지 관리)를 클릭하여 스토리지 도메인을 유지 관리 모드로 전환합니다. 이렇게 하면 기존 공유를 마운트 해제하고 스토리지 도메인의 크기를 조정할 수 있습니다.
4. **NFS** 서버에서 스토리지의 크기를 조정합니다. **Red Hat Enterprise Linux 6** 시스템의 경우 [Red Hat Enterprise Linux 6 스토리지 관리 가이드](#)를 참조하십시오. **Red Hat Enterprise Linux 7** 시스템의 경우 [Red Hat Enterprise Linux 7 스토리지 관리 가이드](#)를 참조하십시오. **Red Hat Enterprise Linux 8** 시스템의 경우 [파티션 재설정을 참조](#)하십시오.
5. 세부 정보 보기에서 **Data Center**(데이터 센터) 탭을 클릭하고 **Activate**(활성화)를 클릭하여 스토리지 도메인을 마운트합니다.

2.6.4. 로컬 스토리지 준비 및 추가

가상 시스템의 호스트에 물리적으로 설치된 스토리지 장치를 사용하는 가상 시스템의 디스크를 로컬 스토리지 장치라고 합니다.

스토리지 장치는 스토리지 도메인의 일부여야 합니다. 로컬 스토리지의 스토리지 도메인 유형을 로컬 스토리지 도메인이라고 합니다.

로컬 스토리지를 사용하도록 호스트를 구성하면 자동으로 생성되고, 다른 호스트를 추가할 수 없는 새 로컬 스토리지 도메인, 데이터 센터 및 클러스터에 호스트를 추가합니다. 다중 호스트 클러스터에서는 모든 호스트가 로컬 스토리지에서 사용할 수 없는 모든 스토리지 도메인에 액세스할 수 있어야 합니다. 단일 호스트 클러스터에서 생성된 가상 시스템은 마이그레이션, 펜싱 또는 예약할 수 없습니다.

2.6.4.1. 로컬 스토리지 준비

RHVH(Red Hat Virtualization Host)에서는 항상 / (root)와 별도의 파일 시스템에 로컬 스토리지를 정의해야 합니다. 별도의 논리 볼륨 또는 디스크를 사용하여 업그레이드 중 데이터 손실을 방지합니다.

Red Hat Enterprise Linux 호스트 절차

1. 호스트에서 로컬 스토리지에 사용할 디렉터리를 생성합니다.

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

2. 디렉터리에 **vdsm** 사용자(**UID 36**) 및 **kvm** 그룹(**GID 36**)에 대한 읽기/쓰기 액세스를 허용하는 권한이 있는지 확인합니다.

```
# chown 36:36 /data /data/images
# chmod 0755 /data /data/images
```

Red Hat Virtualization Host 절차

논리 볼륨에 로컬 스토리지를 생성합니다.

1. 로컬 스토리지 디렉터리를 생성합니다.

```
# mkdir /data
# lvcreate -L $SIZE rhvh -n data
# mkfs.ext4 /dev/mapper/rhvh-data
# echo "/dev/mapper/rhvh-data /data ext4 defaults,discard 1 2" >> /etc/fstab
# mount /data
```

2. 새 로컬 스토리지를 마운트합니다.

```
# mount -a
```

3. 디렉터리에 **vdsm** 사용자(**UID 36**) 및 **kvm** 그룹(**GID 36**)에 대한 읽기/쓰기 액세스를 허용하는 권한이 있는지 확인합니다.

```
# chown 36:36 /data /rhvh-data
# chmod 0755 /data /rhvh-data
```

2.6.4.2. 로컬 스토리지 도메인 추가

로컬 스토리지 도메인을 호스트에 추가할 때 로컬 스토리지 디렉터리에 경로를 설정하면 로컬 데이터 센터, 로컬 클러스터, 로컬 스토리지 도메인에 호스트가 자동으로 생성됩니다.

절차

1. **Compute**(컴퓨팅) → **Hosts**(호스트) 를 클릭하고 호스트를 선택합니다.
2. **Management**(관리 → **Maintenance** (유지 관리) 및 **OK** (확인)를 클릭합니다. 호스트의 상태가 **Maintenance** (유지 관리)로 변경됩니다.
3. **Management**(관리 → **Configure Local Storage** (로컬 스토리지 구성)를 클릭합니다.
4. **Data Center** (데이터 센터), **Cluster** (클러스터) 및 **Storage** (스토리지) 필드 옆에 있는 **Edit** (편집) 버튼을 클릭하여 로컬 스토리지 도메인을 구성하고 이름을 지정합니다.
5. 텍스트 항목 필드에 로컬 스토리지의 경로를 설정합니다.
6. 해당하는 경우 **Optimization**(최적화) 탭을 클릭하여 새 로컬 스토리지 클러스터에 대한 메모리 최적화 정책을 구성합니다.
7. **OK**(확인)를 클릭합니다.

관리자는 로컬 클러스터 로컬 스토리지 도메인으로 로컬 데이터 센터를 설정합니다. 또한 호스트의 상태를 **Up** 으로 변경합니다.

검증

1. **Storage**(스토리지 → **Domains** (도메인) 를 클릭합니다.
2. 방금 추가한 로컬 스토리지 도메인을 찾습니다.

도메인의 상태는 **Active** (



)여야 하며 **Storage Type** (스토리지 유형) 열의 값은 **Local on Host**(호스트의 로컬)여야 합니다.

이제 새 로컬 스토리지 도메인에 디스크 이미지를 업로드할 수 있습니다.

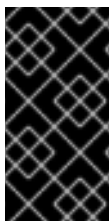
2.6.5. POSIX 호환 파일 시스템 스토리지 준비 및 추가

2.6.5.1. POSIX 호환 파일 시스템 스토리지 준비

POSIX 파일 시스템 지원을 사용하면 명령줄에서 수동으로 마운트할 때 일반적으로 사용하는 것과 동일한 마운트 옵션을 사용하여 파일 시스템을 마운트할 수 있습니다. 이 기능은 **NFS**, **iSCSI** 또는 **FCP**를 사용하여 노출되지 않은 스토리지에 대한 액세스를 허용하기 위한 것입니다.

Red Hat Virtualization의 스토리지 도메인으로 사용되는 **POSIX** 호환 파일 시스템은 **GFS2**(**Global File System 2**)와 같은 클러스터형 파일 시스템이어야 하며 스파스 파일과 직접 **I/O**를 지원해야 합니다. 예를 들어 **CIFS**(**Common Internet File System**)는 직접 **I/O**를 지원하지 않으므로 **Red Hat Virtualization**과 호환되지 않습니다.

POSIX 규격 파일 시스템 스토리지 설정 및 구성에 대한 자세한 내용은 [Red Hat Enterprise Linux Global File System 2](#)를 참조하십시오.



중요

POSIX 호환 파일 시스템 스토리지 도메인을 생성하여 **NFS** 스토리지를 마운트 하지 마십시오. 대신 항상 **NFS** 스토리지 도메인을 생성합니다.

2.6.5.2. POSIX 호환 파일 시스템 스토리지 추가

다음 절차에서는 기존 **POSIX** 규격 파일 시스템 스토리지를 **Red Hat Virtualization** 환경에 데이터 도메인으로 연결하는 방법을 보여줍니다.

절차

1. **Storage**(스토리지 → **Domains** (도메인) 를 클릭합니다.
2. **New Domain** (새 도메인)을 클릭합니다.

3.

스토리지 도메인의 **Name** (이름)을 입력합니다.

4.

스토리지 도메인과 연결할 **Data Center** (데이터 센터)를 선택합니다. 선택한 데이터 센터는 **POSIX**(POSIX 호환 **FS**) 유형이어야 합니다. 또는 (없음) 을 선택합니다.

5.

Domain Function (도메인 기능) 드롭다운 목록에서 **Data** (데이터)를 선택하고 **Storage Type** (스토리지 유형) 드롭다운 목록에서 **POSIX 호환 FS** 를 선택합니다.

해당하는 경우 드롭다운 메뉴에서 **Format** (형식)을 선택합니다.

6.

Host(호스트) 드롭다운 목록에서 호스트를 선택합니다.

7.

일반적으로 **mount** 명령에 제공하는 것처럼 **POSIX** 파일 시스템의 경로를 입력합니다.

8.

일반적으로 **-t** 인수를 사용하여 **mount** 명령에 제공하는 것처럼 **VFS** 유형을 입력합니다. 유효한 **VFS** 유형 목록은 **man mount** 를 참조하십시오.

9.

일반적으로 **-o** 인수를 사용하여 **mount** 명령에 제공하는 추가 마운트 옵션을 입력합니다. 마운트 옵션은 쉼표로 구분된 목록으로 제공해야 합니다. 유효한 마운트 옵션 목록은 **man mount** 를 참조하십시오.

10.

선택적으로 고급 매개 변수를 구성할 수 있습니다.

a.

Advanced Parameters (고급 매개 변수)를 클릭합니다.

b.

Warninglow Space Indicator(낮은 공간 표시기) 필드에 백분율 값을 입력합니다. 스토리지 도메인에서 사용 가능한 여유 공간이 이 백분율 미만인 경우 경고 메시지가 사용자에게 표시되고 기록됩니다.

c.

Critical Space Action Blocker (심각 공간 작업 블록) 필드에 **GB** 값을 입력합니다. 스토리지 도메인에서 사용 가능한 여유 공간이 이 값보다 작으면 사용자에게 오류 메시지가 표시되고 기록되고 공간을 소비하는 새 작업이 차단됩니다.

d.

Wipe after Delete(삭제 후 **Wipe after Delete**) 확인란을 선택하여 삭제 후 지우기 옵션을 활성화합니다. 이 옵션은 도메인을 만든 후에 편집할 수 있지만, 이렇게 하면 이미 존재하는 디스크의 삭제 속성 후에는 **wipe**가 변경되지 않습니다.

11.

OK(확인)를 클릭합니다.

2.6.6. 블록 스토리지 준비 및 추가

2.6.6.1. iSCSI 스토리지 준비

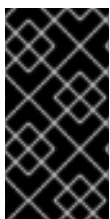
Red Hat Virtualization은 **LUN**으로 구성된 볼륨 그룹에서 생성된 스토리지 도메인인 **iSCSI** 스토리지를 지원합니다. 볼륨 그룹 및 **LUN**은 한 번에 둘 이상의 스토리지 도메인에 연결할 수 없습니다.

iSCSI 스토리지 설정 및 구성에 대한 자세한 내용은 **Red Hat Enterprise Linux 8**의 *스토리지 장치 관리*에서 **iSCSI로 시작하기**를 참조하십시오.



중요

블록 스토리지를 사용하고 원시 장치 또는 직접 **LUN**에 가상 머신을 배포하고 **LVM(Logical Volume Manager)**을 사용하여 관리하려는 경우 게스트 논리 볼륨을 숨기는 필터를 생성해야 합니다. 이렇게 하면 호스트가 부팅될 때 게스트 논리 볼륨이 활성화되지 않으며 논리 볼륨이 오래될 수 있고 데이터 손상이 발생할 수 있습니다. **vdsm-tool config-lvm-filter** 명령을 사용하여 **LVM**에 대한 필터를 생성합니다.



중요

Red Hat Virtualization은 현재 블록 크기가 **4K**인 블록 스토리지를 지원하지 않습니다. 레거시(**512b** 블록) 모드에서 블록 스토리지를 구성해야 합니다.

중요

호스트가 **SAN** 스토리지에서 부팅되고 스토리지에 대한 연결이 끊어지면 스토리지 파일 시스템이 읽기 전용으로 되어 연결이 복원된 후에도 이 상태로 유지됩니다.

이러한 상황을 방지하려면 연결이 있을 때 대기하도록 부팅 **LUN**에 대해 **SAN**의 루트 파일 시스템에 드롭인 다중 경로 구성 파일을 추가합니다.

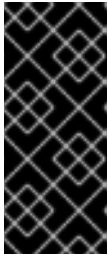
```
# cat /etc/multipath/conf.d/host.conf
multipaths {
    multipath {
        wwid boot_LUN_wwid
        no_path_retry queue
    }
}
```

2.6.6.2. iSCSI 스토리지 추가

다음 절차에서는 기존 **iSCSI** 스토리지를 **Red Hat Virtualization** 환경에 데이터 도메인으로 연결하는 방법을 설명합니다.

절차

1. **Storage**(스토리지 → **Domains** (도메인) 를 클릭합니다.
2. **New Domain** (새 도메인)을 클릭합니다.
3. 새 스토리지 도메인의 **Name** (이름)을 입력합니다.
4. 드롭다운 목록에서 **Data Center** (데이터 센터)를 선택합니다.
5. **Domain Function** (도메인 기능)로 **Data**(데이터)를 선택하고 **Storage Type** (스토리지 유형)으로 **iSCSI** 를 선택합니다.
6. **호스트로 활성 호스트**를 선택합니다.



중요

스토리지 도메인과의 통신은 선택한 호스트에서 이루어지며 **Manager**에서 직접 통신하지 않습니다. 따라서 스토리지 도메인을 구성하려면 모든 호스트에 스토리지 장치에 액세스할 수 있어야 합니다.

7.

관리자는 **iSCSI** 대상을 **LUN** 또는 **LUN**에 매핑할 수 있습니다. **iSCSI** 스토리지 유형을 선택하면 **New Domain** (새 도메인) 창에서 사용되지 않는 **LUN**이 있는 알려진 타겟을 자동으로 표시합니다. 스토리지를 추가하는 데 사용하는 대상이 나타나지 않으면 대상 검색을 사용하여 찾을 수 있습니다. 그렇지 않으면 다음 단계로 진행합니다.

a.

Discover Targets (대상 검색)를 클릭하여 대상 검색 옵션을 활성화합니다. 대상이 검색되어 에 로그인되면 **New Domain**(새 도메인) 창에 환경에서 사용하지 않는 **LUN**이 있는 대상이 자동으로 표시됩니다.



참고

환경에 외부적으로 사용하는 **LUN**도 표시됩니다.

Discover Targets(대상 검색) 옵션을 사용하여 여러 대상 또는 여러 경로에 **LUN**을 동일한 **LUN**에 추가할 수 있습니다.



중요

REST API 메서드 **discoveriscsi** 을 사용하여 **iscsi** 대상을 검색할 경우 **FQDN** 또는 **IP** 주소를 사용할 수 있지만 검색된 대상의 **iscsi** 세부 정보를 사용하여 **REST API** 메서드 **iscsilogin** 을 사용하여 로그인해야 합니다. 자세한 내용은 **REST API 가이드**의 **discoveriscsi** 을 참조하십시오.

b.

Address (주소) 필드에 **iSCSI** 호스트의 **FQDN** 또는 **IP** 주소를 입력합니다.

c.

Port(포트) 필드에서 대상을 찾을 때 호스트에 연결할 포트를 입력합니다. 기본값은 **3260**입니다.

d.

CHAP를 사용하여 스토리지를 보호하는 경우 **User Authentication** (사용자 인증) 확인란을 선택합니다. **CHAP** 사용자 이름과 **CHAP** 암호를 입력합니다.



참고

REST API를 사용하여 특정 호스트에 대한 **iSCSI** 대상에 대한 자격 증명을 정의할 수 있습니다. 자세한 내용은 ***REST API 가이드***에 **StorageServerConnectionExtensions: add** 를 참조하십시오.

e.

Discover(검색)를 클릭합니다.

f.

검색 결과에서 하나 이상의 대상을 선택하고 하나의 대상에 대해 **Login**(로그인) 또는 여러 대상에 대해 **Login All** (모두 로그인)을 클릭합니다.



중요

둘 이상의 경로 액세스가 필요한 경우 필요한 모든 경로를 통해 대상을 검색하고 로그인해야 합니다. 스토리지 도메인을 변경하여 추가 경로를 추가하는 것은 현재 지원되지 않습니다.



중요

REST API iscsilogin 메서드를 사용하여 로그인하는 경우 검색된 대상의 **iscsi** 세부 정보를 사용해야 합니다. 그러면 **discoveriscsi** 메서드가 생성됩니다. 자세한 내용은 ***REST API 가이드***에서 **iscsilogin** 을 참조하십시오.

8.

원하는 대상 옆에 있는 **+** 버튼을 클릭합니다. 이렇게 하면 항목이 확장되고 대상에 연결된 사용하지 않는 모든 **LUN**이 표시됩니다.

9.

스토리지 도메인을 생성하기 위해 사용 중인 각 **LUN**의 확인란을 선택합니다.

10.

선택적으로 고급 매개변수를 구성할 수 있습니다.

a.

Advanced Parameters (고급 매개 변수)를 클릭합니다.

b.

Warninglow Space Indicator(낮은 공간 표시기) 필드에 백분율 값을 입력합니다. 스토리지 도메인에서 사용 가능한 여유 공간이 이 백분율 미만인 경우 경고 메시지가 사용자에게 표시되고 기록됩니다.

c.

Critical Space Action Blocker (심각 공간 작업 블록) 필드에 **GB** 값을 입력합니다. 스토리지 도메인에서 사용 가능한 여유 공간이 이 값보다 작으면 사용자에게 오류 메시지가 표시되고 기록되고 공간을 소비하는 새 작업이 차단됩니다.

d.

Wipe after Delete(삭제 후 **Wipe after Delete**) 확인란을 선택하여 삭제 후 지우기 옵션을 활성화합니다. 이 옵션은 도메인을 만든 후에 편집할 수 있지만, 이렇게 하면 이미 존재하는 디스크의 삭제 속성 후에는 **wipe**가 변경되지 않습니다.

e.

삭제 후 삭제 옵션을 활성화하려면 **Discard after Delete**(삭제 후 카드 비활성화) 확인란을 선택합니다. 이 옵션은 도메인을 생성한 후 편집할 수 있습니다. 이 옵션은 블록 스토리지 도메인에서만 사용할 수 있습니다.

11.

OK(확인)를 클릭합니다.

동일한 대상에 여러 스토리지 연결 경로를 구성한 경우 **iSCSI Multipathing** 구성의 절차에 따라 **iSCSI** 본딩을 완료합니다.

현재 스토리지 네트워크를 **iSCSI** 본딩으로 **마이그레이션**하려면 논리적 네트워크를 **iSCSI** 본드로 마이그레이션을 참조하십시오.

2.6.6.3. iSCSI Multipathing 구성

iSCSI 다중 경로를 사용하면 논리적 네트워크 및 **iSCSI** 스토리지 연결 그룹을 생성하고 관리할 수 있습니다. 호스트와 **iSCSI** 스토리지 간의 여러 네트워크 경로는 네트워크 경로 실패로 인한 호스트 다운타임을 방지합니다.

관리자는 **iSCSI** 본딩의 논리적 네트워크에 할당된 **NIC** 또는 **VLAN**을 사용하여 데이터 센터의 각 호스트를 각 대상에 연결합니다.

중복성을 위해 여러 대상 및 논리적 네트워크를 사용하여 **iSCSI** 본딩을 생성할 수 있습니다.

사전 요구 사항

- 하나 이상의 **iSCSI** 대상

- 다음 요구 사항을 충족하는 하나 이상의 **논리적 네트워크**:
 - **Required** 또는 **VM Network**로 정의되어 있지 않습니다
 - **호스트 인터페이스에 할당**
 - **iSCSI** 본딩의 다른 논리적 네트워크와 동일한 **VLAN** 및 서브넷의 **고정 IP 주소 할당**

절차

1. **Compute**(컴퓨팅) → **Data Centers** (데이터 센터)를 클릭합니다.
2. 데이터 센터 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **iSCSI Multipathing** 탭에서 **Add** (추가)를 클릭합니다.
4. **Add iSCSI Bond**(iSCSI 본드 추가) 창에 **Name** (이름) 및 **Description** (설명)을 입력합니다.
5. 논리적 네트워크에서 논리적 네트워크를 선택하고 **Storage Targets** (스토리지 대상)에서 스토리지 도메인을 선택합니다. 동일한 대상에 대한 모든 경로를 선택해야 합니다.
6. **OK**(확인)를 클릭합니다.

데이터 센터의 호스트는 **iSCSI** 본딩의 논리적 네트워크를 통해 **iSCSI** 대상에 연결됩니다.

2.6.6.4. 논리적 네트워크를 iSCSI 본드로 마이그레이션

iSCSI 트래픽을 위해 만든 논리적 네트워크가 있고 기존 **네트워크 본딩** 위에 구성된 경우 중단이나 다운타임 없이 동일한 서브넷에서 **iSCSI** 본딩으로 마이그레이션할 수 있습니다.

절차

1.

현재 논리적 네트워크가 필요하지 않도록 수정합니다 :

 - a.

Compute(컴퓨팅) Clusters(클러스터) 를 클릭합니다.
 - b.

클러스터 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
 - c.

Logical Networks(논리 네트워크) 탭에서 현재 논리적 네트워크(**net-1**)를 선택하고 **Manage Networks (네트워크 관리)**를 클릭합니다.
 - d.

Require (필수) 확인란을 지우고 **OK(확인)**를 클릭합니다.
2.

VM 네트워크가 아닌 새로운 논리적 네트워크를 생성하십시오 :

 - a.

네트워크 추가를 클릭합니다. 그러면 **New Logical Network(새 논리적 네트워크)** 창이 열립니다.
 - b.

General(일반) 탭에서 **Name (이름) (net-2)**을 입력하고 **VM network (VM 네트워크)** 확인란을 지웁니다.
 - c.

Cluster(클러스터) 탭에서 **Require (필수)** 확인란을 지우고 **OK(확인)**를 클릭합니다.
3.

현재 네트워크 본딩을 제거하고 논리적 네트워크를 다시 할당합니다.

 - a.

Compute(컴퓨팅) Hosts(호스트) 를 클릭합니다.
 - b.

호스트 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
 - c.

Network Interfaces(네트워크 인터페이스) 탭에서 **Setup Host Networks(호스트 네트워크 설정)**를 클릭합니다.

- u. **net-1** 을 오른쪽으로 끌어 할당 해제합니다.
 - e. 현재 본딩을 오른쪽으로 끌어서 제거합니다.
 - f. **net-1** 및 **net-2** 를 왼쪽으로 끌어서 물리적 인터페이스에 할당합니다.
 - g. **net-2** 의 연필 아이콘을 클릭합니다. 그러면 **Edit Network**(네트워크 편집) 창이 열립니다.
 - h. **IPV4** 탭에서 **Static** (정적)을 선택합니다.
 - i. 서브넷의 **IP** 및 넷마스크/라우팅 접두사 를 입력하고 **OK**(확인)를 클릭합니다.
4. **iSCSI** 본딩을 생성합니다.
- a. **Compute**(컴퓨팅) → **Data Centers** (데이터 센터)를 클릭합니다.
 - b. 데이터 센터 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
 - c. **iSCSI Multipathing** 탭에서 **Add** (추가)를 클릭합니다.
 - d. **Add iSCSI Bond** (iSCSI 본드 추가) 창에서 **Name** (이름)을 입력하고 **network**, **net-1** 및 **net -2** 를 선택한 다음 **OK**(확인)를 클릭합니다.

데이터 센터에는 이전 및 새 논리적 네트워크가 포함된 **iSCSI** 본딩이 있습니다.

2.6.6.5. FCP 스토리지 준비

Red Hat Virtualization은 기존 **LUN**으로 구성된 볼륨 그룹에서 스토리지 도메인을 생성하여 **SAN** 스토리지를 지원합니다. 한 번에 둘 이상의 스토리지 도메인에 볼륨 그룹과 **LUN**을 연결할 수 없습니다.

Red Hat Virtualization 시스템 관리자에게는 **SAN(Storage Area Networks)** 개념에 대한 지식이 필요합니다. **SAN**은 일반적으로 호스트와 공유 외부 스토리지 간의 트래픽에 **FCP(Fibre Channel Protocol)**를 사용합니다. 이러한 이유로 **SAN**을 종종 **FCP** 스토리지라고 할 수 있습니다.

Red Hat Enterprise Linux에서 **FCP** 또는 다중 경로를 설정하고 구성하는 방법에 대한 자세한 내용은 [스토리지 관리 가이드](#) 및 [DM 다중 경로 가이드](#)를 참조하십시오.

중요

블록 스토리지를 사용하고 원시 장치 또는 직접 **LUN**에 가상 머신을 배포하고 **LVM(Logical Volume Manager)**을 사용하여 관리하려는 경우 게스트 논리 볼륨을 숨기는 필터를 생성해야 합니다. 이렇게 하면 호스트가 부팅될 때 게스트 논리 볼륨이 활성화되지 않으며 논리 볼륨이 오래될 수 있고 데이터 손상이 발생할 수 있습니다. **vdsm-tool config-lvm-filter** 명령을 사용하여 **LVM**에 대한 필터를 생성합니다.

중요

Red Hat Virtualization은 현재 블록 크기가 **4K**인 블록 스토리지를 지원하지 않습니다. 레거시(**512b** 블록) 모드에서 블록 스토리지를 구성해야 합니다.

중요

호스트가 **SAN** 스토리지에서 부팅되고 스토리지에 대한 연결이 끊어지면 스토리지 파일 시스템이 읽기 전용으로 되어 연결이 복원된 후에도 이 상태로 유지됩니다.

이러한 상황을 방지하려면 연결이 있을 때 대기하도록 부팅 **LUN**에 대해 **SAN**의 루트 파일 시스템에 드롭인 다중 경로 구성 파일을 추가합니다.

```
# cat /etc/multipath/conf.d/host.conf
multipaths {
    multipath {
        wwid boot_LUN_wwid
        no_path_retry queue
    }
}
```

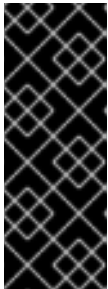
2.6.6.6. FCP 스토리지 추가

다음 절차에서는 기존 **FCP** 스토리지를 Red Hat Virtualization 환경에 데이터 도메인으로 연결하는 방법을 보여줍니다.

절차

1. **Storage**(스토리지 → **Domains** (도메인) 를 클릭합니다.
2. **New Domain** (새 도메인)을 클릭합니다.
3. 스토리지 도메인의 **Name** (이름)을 입력합니다.
4. 드롭다운 목록에서 **FCP Data Center** (**FCP** 데이터 센터)를 선택합니다.

아직 적절한 **FCP** 데이터 센터가 없는 경우 (없음) 을 선택합니다.
5. 드롭다운 목록에서 **Domain Function** (도메인 기능) 및 **Storage Type** (스토리지 유형)을 선택합니다. 선택한 데이터 센터와 호환되지 않는 스토리지 도메인 유형을 사용할 수 없습니다.
6. **Host**(호스트) 필드에서 활성 호스트를 선택합니다. 데이터 센터의 첫 번째 데이터 도메인이 아닌 경우 데이터 센터의 **SPM** 호스트를 선택해야 합니다.



중요

스토리지 도메인과의 모든 통신은 **Red Hat Virtualization Manager**에서 직접 전송하지 않은 선택된 호스트를 통해 이루어집니다. 시스템에 하나 이상의 활성 호스트가 있어야 하며 선택한 데이터 센터에 연결해야 합니다. 스토리지 도메인을 구성하려면 모든 호스트에 스토리지 장치에 액세스할 수 있어야 합니다.

7. **New Domain**(새 도메인) 창은 파이버 채널을 스토리지 유형으로 선택하면 사용되지 않는 **LUN**을 사용하여 알려진 타겟을 자동으로 표시합니다. **LUN ID** 확인란을 선택하여 사용 가능한 **LUN**을 모두 선택합니다.
8. 선택적으로 고급 매개 변수를 구성할 수 있습니다.
 - a. **Advanced Parameters** (고급 매개 변수)를 클릭합니다.
 - b. **Warninglow Space Indicator**(낮은 공간 표시기) 필드에 백분율 값을 입력합니다. 스

스토리지 도메인에서 사용 가능한 여유 공간이 이 백분을 미만인 경우 경고 메시지가 사용자에게 표시되고 기록됩니다.

c.

Critical Space Action Blocker (심각 공간 작업 블록) 필드에 **GB** 값을 입력합니다. 스토리지 도메인에서 사용 가능한 여유 공간이 이 값보다 작으면 사용자에게 오류 메시지가 표시되고 기록되고 공간을 소비하는 새 작업이 차단됩니다.

d.

Wipe after Delete(삭제 후 **Wipe after Delete**) 확인란을 선택하여 삭제 후 지우기 옵션을 활성화합니다. 이 옵션은 도메인을 만든 후에 편집할 수 있지만, 이렇게 하면 이미 존재하는 디스크의 삭제 속성 후에는 **wipe**가 변경되지 않습니다.

e.

삭제 후 삭제 옵션을 활성화하려면 **Discard after Delete**(삭제 후 카드 비활성화) 확인란을 선택합니다. 이 옵션은 도메인을 생성한 후 편집할 수 있습니다. 이 옵션은 블록 스토리지 도메인에서만 사용할 수 있습니다.

9.

OK(확인)를 클릭합니다.

새로운 **FCP** 데이터 도메인은 사용할 준비가 되어 있는 동안 **Locked** 상태로 유지됩니다. 준비가 되면 데이터 센터에 자동으로 연결됩니다.

2.6.6.7. iSCSI 또는 FCP 스토리지 증가

iSCSI 또는 FCP 스토리지 크기를 늘리는 방법은 다음과 같습니다.

- 기존 **LUN**을 현재 스토리지 도메인에 추가합니다.
- 새 **LUN**을 사용하여 새 스토리지 도메인을 생성하고 기존 데이터 센터에 추가합니다. **iSCSI 스토리지 추가**를 참조하십시오.
- 기본 **LUN**의 크기를 조정하여 스토리지 도메인을 확장합니다.

Red Hat Enterprise Linux 7 시스템에서 iSCSI 스토리지 생성, 구성 또는 크기 조정에 대한 자세한 내용은 [Red Hat Enterprise Linux 7 스토리지 관리 가이드](#)를 참조하십시오.

다음 절차에서는 기존 스토리지 도메인에 새 **LUN**을 추가하여 **SAN(Storage Area Network)** 스토리지를 확장하는 방법을 설명합니다.

사전 요구 사항

- 스토리지 도메인의 상태는 **UP** 이어야 합니다.
- 상태가 **UP** 인 모든 호스트에서 **LUN**에 액세스할 수 있어야 합니다. 그렇지 않으면 작업이 실패하고 **LUN**이 도메인에 추가되지 않습니다. 그러나 호스트 자체는 영향을 받지 않습니다. 새로 추가된 호스트 또는 유지 관리 상태가 아니거나 비작동 상태인 호스트가 **LUN**에 액세스할 수 없는 경우 호스트의 상태가 **Non Operational** 이 됩니다.

기존 iSCSI 또는 FCP 스토리지 도메인 증가

1. **Storage → Domains** (스토리지 도메인)를 클릭하고 **iSCSI** 또는 **FCP** 도메인을 선택합니다.
2. **Manage Domain** (도메인 관리)을 클릭합니다.
3. **Targets(대상) → LUNs** 를 클릭하고 **Discover Targets(대상 검색)** 확장 버튼을 클릭합니다.
4. 스토리지 서버의 연결 정보를 입력하고 **Discover(검색)**를 클릭하여 연결을 시작합니다.
5. **LUNs Targets → (대상)**를 클릭하고 새로 사용 가능한 **LUN**의 확인란을 선택합니다.
6. **OK(확인)**를 클릭하여 선택한 스토리지 도메인에 **LUN**을 추가합니다.

그러면 추가된 **LUN**의 크기만큼 스토리지 도메인이 증가합니다.

기본 **LUN**을 변경하여 스토리지 도메인을 확장하는 경우 관리 포털에서 **LUN**도 새로 고쳐야 합니다.

LUN 크기 새로 고침

1. **Storage → Domains** (스토리지 도메인)를 클릭하고 **iSCSI** 또는 **FCP** 도메인을 선택합니다.
2. **Manage Domain** (도메인 관리)을 클릭합니다.
3. **LUNs** 대상을 → 클릭합니다.
4. 추가 크기 열에서 새로 고침할 LUN의 **Add additional _Storage_Size** 버튼을 클릭합니다.
5. **OK(확인)**를 클릭하여 LUN을 새로 고쳐 새 스토리지 크기를 나타냅니다.

2.6.6.8. LUN 재사용

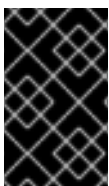
LUN은 스토리지 도메인 또는 가상 디스크를 생성하기 위해 그대로 재사용할 수 없습니다. LUN을 재사용하려는 경우 관리 포털에 다음과 같은 오류 메시지가 표시됩니다.

Physical device initialization failed. Please check that the device is empty and accessible by the host.

자체 호스팅 엔진은 설치 중에 다음과 같은 오류를 표시합니다.

```
[ ERROR ] Error creating Volume Group: Failed to initialize physical device: ("
[u'/dev/mapper/00000000000000000000000000000000']"),)
[ ERROR ] Failed to execute stage 'Misc configuration': Failed to initialize physical device: ("
[u'/dev/mapper/00000000000000000000000000000000']"),)
```

LUN을 재사용하려면 이전 파티션 테이블을 지워야 합니다.



절차

실수로 데이터를 삭제하지 않도록 올바른 LUN에서 다음 절차를 실행해야 합니다.

1.

<LUN_ID> 에서 파티션 매핑을 삭제합니다.

```
kpartx -dv /dev/mapper/<LUN_ID>
```

2.

<LUN_ID>에서 *filesystem* 또는 *raid* 서명을 지웁니다:

```
wipefs -a /dev/mapper/<LUN_ID>
```

3.

운영 체제에 <LUN_ID> 의 파티션 테이블 변경 사항을 알립니다.

```
partprobe
```

2.6.6.9. 오래된 LUN 제거

스토리지 도메인을 제거하면 오래된 LUN 링크가 스토리지 서버에 남아 있을 수 있습니다. 이로 인해 다중 경로 검사, 복잡한 로그 파일 및 LUN ID 충돌 속도가 느릴 수 있습니다.

Red Hat Virtualization은 iSCSI 서버를 관리하지 않으므로 스토리지 도메인을 제거할 때 LUN을 자동으로 제거할 수 없습니다. 관리자는 `remove_stale_lun.yml` Ansible 역할을 사용하여 오래된 LUN 링크를 수동으로 제거할 수 있습니다. 이 역할은 지정된 데이터 센터에 속한 모든 호스트에서 오래된 LUN 링크를 제거합니다. 이 역할 및 해당 변수에 대한 자세한 내용은 [oVirt Ansible 컬렉션에서 LUN 역할 제거](#)를 참조하십시오.



참고

엔진 ssh 키가 모든 호스트에 이미 추가되었으므로 엔진 시스템에서 `remove_stale_lun.yml` 을 실행 중이라고 가정합니다. 플레이북이 엔진 시스템에서 실행되지 않는 경우 사용자의 SSH 키를 데이터 센터에 속하는 모든 호스트에 추가하거나 사용자가 적절한 인벤토리 파일을 제공해야 합니다.

절차

1.

Storage(스토리지 → Domains (도메인) 를 클릭합니다.

2.

스토리지 도메인의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.

3. **Data Center**(데이터 센터) 탭을 클릭합니다.
4. **Maintenance**(유지 관리)를 클릭한 다음 **OK**(확인)를 클릭합니다.
5. **Detatch** (분리)를 클릭한 다음 **OK**(확인)를 클릭합니다.
6. **Remove**(제거)를 클릭합니다.
7. **OK**(확인)를 클릭하여 소스 환경에서 스토리지 도메인을 제거합니다.
8. 스토리지 서버에서 **LUN**을 제거합니다.
9. **Ansible**을 사용하여 호스트에서 오래된 **LUN**을 제거합니다.

```
# ansible-playbook --extra-vars "lun=<LUN>"
/usr/share/ansible/collections/ansible_collections/ovirt/ovirt/roles/remove_stale_lun/examples/remove_stale_lun.yml
```

여기서 **LUN**은 위 단계에서 스토리지 서버에서 **LUN**이 제거되었습니다.



참고

스토리지 서버에서 **LUN**을 먼저 제거하지 않고 **Ansible**을 사용하여 호스트에서 오래된 **LUN**을 제거하면 **VDSM**이 다음에 **iSCSI** 재검사를 수행할 때 오래된 **LUN**이 호스트에 다시 나타납니다.

2.6.6.10. LVM 필터 생성

LVM 필터는 **regex** 쿼리에 따라 볼륨 목록에서 장치를 수락하거나 거부하도록 **/etc/lvm/lvm.conf** 에 설정할 수 있는 기능입니다. 예를 들어 **/dev/cdrom** 을 무시하려면 **filter=["r|^/dev/cdrom\$"]** 을 사용하거나 **lvm** 명령에 다음 매개 변수를 추가합니다. **lvs --config 'devices{filter=["r|cdrom"]}'**.

이렇게 하면 호스트가 호스트에서 직접 필요하지 않은 논리 볼륨을 검색 및 활성화하지 못하도록 간편하게 할 수 있습니다. 특히 이 솔루션은 **RHV**에서 관리하는 공유 스토리지의 논리 볼륨과 **RHV** 원시 볼륨

의 게스트가 생성한 논리 볼륨을 처리합니다. 다른 논리 볼륨 검색 및 활성화로 인해 데이터 손상, 느린 부팅 또는 기타 문제가 발생할 수 있으므로 이 솔루션이 필요합니다.

해결책은 각 호스트에 **LVM** 필터를 구성하여 호스트의 **LVM**에서 호스트에 필요한 논리 볼륨만 스캔할 수 있도록 하는 것입니다.

vdsmd-tool config-lvm-filter 명령을 사용하여 현재 **LVM** 구성을 분석하고 필터를 구성해야 하는지 결정할 수 있습니다.

LVM 필터가 아직 구성되지 않은 경우 명령은 호스트에 대한 **LVM** 필터 옵션을 생성하고 **LVM** 구성에 옵션을 추가합니다.

시나리오 1: 구성되지 않은 호스트

호스트에서 아직 구성할 경우 사용자가 작업을 확인하면 명령이 자동으로 **LVM**을 구성합니다.

```
# vdsmd-tool config-lvm-filter
```

```
Analyzing host...
```

```
Found these mounted logical volumes on this host:
```

```
logical volume: /dev/mapper/vg0-lv_home
mountpoint:    /home
devices:       /dev/vda2
```

```
logical volume: /dev/mapper/vg0-lv_root
mountpoint:     /
devices:        /dev/vda2
```

```
logical volume: /dev/mapper/vg0-lv_swap
mountpoint:     [SWAP]
devices:        /dev/vda2
```

```
This is the recommended LVM filter for this host:
```

```
filter = [ "a|^/dev/vda2$", "r|.*)" ]
```

This filter will allow LVM to access the local devices used by the hypervisor, but not shared storage owned by VDSM. If you add a new device to the volume group, you will need to edit the filter manually.

```
Configure LVM filter? [yes,NO] ? [NO/yes] yes
Configuration completed successfully!
```

Please reboot to verify the LVM configuration.

시나리오 2: 구성된 호스트

호스트가 이미 구성된 경우 명령은 **LVM 필터**가 이미 구성되었음을 사용자에게 알립니다.

```
# vdsim-tool config-lvm-filter
```

Analyzing host...

LVM filter is already configured for Vdsm

시나리오 3: 수동 설정 필요

호스트 구성이 **VDSM**에 필요한 구성과 일치하지 않으면 **LVM 필터**를 수동으로 구성해야 합니다.

```
# vdsim-tool config-lvm-filter
```

Analyzing host...

Found these mounted logical volumes on this host:

logical volume: /dev/mapper/vg0-lv_home

mountpoint: /home

devices: /dev/vda2

logical volume: /dev/mapper/vg0-lv_root

mountpoint: /

devices: /dev/vda2

logical volume: /dev/mapper/vg0-lv_swap

mountpoint: [SWAP]

devices: /dev/vda2

This is the recommended LVM filter for this host:

```
filter = [ "a|^/dev/vda2$", "r|.*)" ]
```

This filter will allow LVM to access the local devices used by the hypervisor, but not shared storage owned by VDSM. If you add a new device to the volume group, you will need to edit the filter manually.

This is the current LVM filter:

```
filter = [ "a|^/dev/vda2$", "a|^/dev/vdb1$", "r|.*)" ]
```

WARNING: The current LVM filter does not match the recommended filter, Vdsm cannot configure the filter automatically.

Please edit `/etc/lvm/lvm.conf` and set the 'filter' option in the 'devices' section to the recommended value.

It is recommended to reboot after changing LVM filter.

2.6.7. Red Hat Gluster Storage 준비 및 추가

2.6.7.1. Red Hat Gluster Storage 준비

Red Hat Gluster Storage 설정 및 구성에 대한 자세한 내용은 [Red Hat Gluster Storage 설치 가이드를 참조하십시오.](#)

Red Hat Virtualization에서 지원되는 Red Hat Gluster Storage 버전은 [Red Hat Gluster Storage 버전 호환성 및 지원을 참조하십시오.](#)

2.6.7.2. Red Hat Gluster Storage 추가

Red Hat Virtualization과 함께 Red Hat Gluster Storage를 사용하려면 [Red Hat Gluster Storage를 사용하여 Red Hat Virtualization 구성을 참조하십시오.](#)

Red Hat Virtualization에서 지원되는 Red Hat Gluster Storage 버전은 [Red Hat Gluster Storage 버전 호환성 및 지원을 참조하십시오.](#)

2.6.8. 기존 스토리지 도메인 가져오기

2.6.8.1. 기존 스토리지 도메인 가져오기 개요

데이터가 포함되지 않은 새 스토리지 도메인을 추가하는 것 외에도 기존 스토리지 도메인을 가져오고 포함된 데이터에 액세스할 수 있습니다. 스토리지 도메인을 가져오면 **Manager** 데이터베이스의 오류가 발생할 때 데이터를 복구하고 한 데이터 센터 또는 환경에서 다른 데이터 센터로 데이터를 마이그레이션할 수 있습니다.

다음은 각 스토리지 도메인 유형을 가져오는 개요입니다.

데이터

기존 데이터 스토리지 도메인을 가져오면 데이터 스토리지 도메인에 포함된 모든 가상 시스템 및 템플릿에 액세스할 수 있습니다. 스토리지 도메인을 가져온 후 가상 시스템, 유동 디스크 이미지 및 템플릿을 대상 데이터 센터로 수동으로 가져와야 합니다. 데이터 스토리지 도메인에 포함된 가상 시스템 및 템플릿을 가져오는 프로세스는 내보내기 스토리지 도메인의 프로세스와 유사합니다. 그러나 데이

터 스토리지 도메인에는 지정된 데이터 센터에 있는 모든 가상 시스템과 템플릿이 포함되어 있으므로 데이터 센터 또는 환경 간에 가상 시스템의 데이터 복구 또는 대규모 마이그레이션에 데이터 스토리지 도메인을 가져오는 것이 좋습니다.



중요

지원되는 올바른 호환성 수준을 사용하여 데이터 센터에 연결된 기존 데이터 스토리지 도메인을 가져올 수 있습니다. 자세한 내용은 [이전 RHV 버전에서 스토리지 도메인 및 가상 시스템 가져오기와 관련된 지원 가능성 및 제약 조건](#)을 참조하십시오.

ISO

기존 ISO 스토리지 도메인을 가져오면 ISO 스토리지 도메인에 포함된 모든 ISO 파일 및 가상 디스크 세트에 액세스할 수 있습니다. 이러한 리소스에 액세스하기 위해 스토리지 도메인을 가져온 후에는 추가 작업이 필요하지 않습니다. 필요에 따라 가상 머신에 연결할 수 있습니다.

내보내기

기존 내보내기 스토리지 도메인을 가져오면 내보내기 스토리지 도메인에 포함된 모든 가상 시스템 이미지와 템플릿에 액세스할 수 있습니다. 내보내기 도메인은 가상 시스템 이미지와 템플릿을 내보내고 가져오도록 설계되었으므로 내보내기 스토리지 도메인을 가져오려면 환경 내에서 또는 환경 간에 소수의 가상 시스템과 템플릿을 마이그레이션하는 것이 좋습니다. 스토리지 도메인으로 가상 머신 및 템플릿을 내보내고 가져오는 방법에 대한 자세한 내용은 가상 머신 [관리 가이드](#)에서 [가상 머신 및 템플릿 내보내기 및 가져오기](#)를 참조하십시오.



참고

내보내기 스토리지 도메인은 더 이상 사용되지 않습니다. 스토리지 데이터 도메인은 데이터 센터에서 연결을 해제하고 동일한 환경이나 다른 환경에서 다른 데이터 센터로 가져올 수 있습니다. 그런 다음 가져온 스토리지 도메인에서 연결된 데이터 센터로 가상 시스템, 유동 가상 디스크 및 템플릿을 업로드할 수 있습니다.



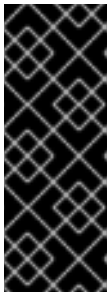
주의

대상 데이터 센터에 스토리지 도메인을 연결할 때 최신 스토리지 도메인 형식으로 업그레이드할 수 있으며 소스 데이터 센터에 다시 연결할 수 없습니다. 이렇게 하면 **Data-Domain**을 내보내기 도메인 대신 사용할 수 있습니다.

동일한 환경 또는 다른 환경에서 이전에 데이터 센터에 연결된 스토리지 도메인을 가져옵니다. 이 절차에서는 데이터 손상을 방지하기 위해 스토리지 도메인이 모든 환경의 데이터 센터에 더 이상 연결되지 않는다고 가정합니다. 기존 데이터 스토리지 도메인을 데이터 센터에 가져와 연결하려면 대상 데이터 센터를 초기화해야 합니다.

절차

1. **Storage**(스토리지 → **Domains** (도메인) 를 클릭합니다.
2. **Import Domain** (도메인 가져오기)을 클릭합니다.
3. 스토리지 도메인을 가져올 데이터 센터를 선택합니다.
4. 스토리지 도메인 의 이름을 입력합니다.
5. 드롭다운 목록에서 **Domain Function** (도메인 기능) 및 **Storage Type** (스토리지 유형)을 선택합니다.
6. **Host**(호스트) 드롭다운 목록에서 호스트를 선택합니다.



중요

스토리지 도메인과의 모든 통신은 **Red Hat Virtualization Manager**에서 직접 전송하지 않은 선택된 호스트를 통해 이루어집니다. 시스템에 하나 이상의 활성 호스트가 있어야 하며 선택한 데이터 센터에 연결해야 합니다. 스토리지 도메인을 구성하려면 모든 호스트에 스토리지 장치에 액세스할 수 있어야 합니다.

7. 스토리지 도메인의 세부 정보를 입력합니다.



참고

Domain Function (도메인 기능) 및 **Storage Type** (스토리지 유형) 목록에서 선택한 값에 따라 스토리지 도메인 변경의 세부 사항을 지정하는 필드입니다. 이러한 필드는 새 스토리지 도메인을 추가하는 데 사용할 수 있는 항목과 동일합니다.

8.

Activate Domain in Data Center (데이터 센터에서 도메인 활성화) 확인란을 선택하여 선택한 데이터 센터에 연결한 후 스토리지 도메인을 활성화합니다.

9.

OK(확인)를 클릭합니다.

이제 스토리지 도메인에서 데이터 센터로 가상 머신 및 템플릿을 가져올 수 있습니다.



주의

대상 데이터 센터에 스토리지 도메인을 연결할 때 최신 스토리지 도메인 형식으로 업그레이드할 수 있으며 소스 데이터 센터에 다시 연결할 수 없습니다. 이렇게 하면 **Data-Domain**을 내보내기 도메인 대신 사용할 수 있습니다.

관련 정보



[데이터 도메인에서 가상 머신 가져오기](#)



[가져온 데이터 스토리지 도메인에서 템플릿 가져오기](#)

2.6.8.3. 동일한 환경에서 데이터 센터 간에 스토리지 도메인 마이그레이션

스토리지 도메인을 같은 **Red Hat Virtualization** 환경에 있는 한 데이터 센터에서 다른 데이터 센터로 마이그레이션하여 대상 데이터 센터가 스토리지 도메인에 포함된 데이터에 액세스할 수 있도록 합니다. 이 절차에서는 한 데이터 센터에서 스토리지 도메인을 분리하고 다른 데이터 센터에 연결하는 작업을 수행해야 합니다.



주의

원래 데이터 센터보다 호환성 수준이 더 높은 데이터 센터로 데이터 스토리지 도메인을 마이그레이션하면 스토리지 도메인의 스토리지 형식 버전이 업그레이드됩니다.

가상 시스템을 새 데이터 센터로 마이그레이션하는 등의 이유로 스토리지 도메인을 원래 데이터 센터로 다시 이동하려는 경우 더 높은 버전으로 데이터 스토리지 도메인을 원래 데이터 센터에 다시 첨부하지 않도록 해야 합니다.

관리 포털에서 스토리지 도메인 형식(예: **V3**에서 **V 5**로)을 업데이트하라는 메시지가 표시됩니다. 또한 **DC** 수준이 낮은 이전 데이터 센터에 다시 연결할 수 없다는 경고도 표시됩니다.

이 문제를 해결하기 위해 소스 데이터 센터와 동일한 호환성 버전이 있는 대상 데이터 센터를 만들 수 있습니다. 더 이상 호환성이 낮은 버전을 유지 관리할 필요가 없는 경우 대상 데이터 센터의 호환성 버전을 늘릴 수 있습니다.

자세한 내용은 [이전 RHV 버전에서 스토리지 도메인 및 가상 시스템 가져오기와 관련된 지원 가능성 및 제약 조건](#)을 참조하십시오.

절차

1. 필요한 스토리지 도메인에서 실행 중인 모든 가상 시스템을 종료합니다.
2. **Storage**(스토리지 → **Domains** (도메인))를 클릭합니다.
3. 스토리지 도메인의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
4. **Data Center**(데이터 센터) 탭을 클릭합니다.
5. **Maintenance**(유지 관리)를 클릭한 다음 **OK**(확인)를 클릭합니다.

6.

Detach(분리) 를 클릭한 다음 **OK(확인)**를 클릭합니다.

7.

Attach(연결)를 클릭합니다.

8.

대상 데이터 센터를 선택하고 **OK(확인)**를 클릭합니다.

스토리지 도메인은 대상 데이터 센터에 연결되며 자동으로 활성화됩니다. 이제 스토리지 도메인에서 대상 데이터 센터로 가상 머신 및 템플릿을 가져올 수 있습니다.

2.6.8.4. 다른 환경에서 데이터 센터 간 스토리지 도메인 마이그레이션

스토리지 도메인을 한 **Red Hat Virtualization** 환경에서 다른 환경으로 마이그레이션하여 대상 환경이 스토리지 도메인에 포함된 데이터에 액세스할 수 있도록 합니다. 다음 절차에서는 하나의 **Red Hat Virtualization** 환경에서 스토리지 도메인을 제거하고 다른 환경으로 가져오는 작업을 수행해야 합니다. 기존 데이터 스토리지 도메인을 **Red Hat Virtualization** 데이터 센터에 가져와 연결하려면 스토리지 도메인의 소스 데이터 센터에 올바른 지원 호환성 수준이 있어야 합니다.



주의

원래 데이터 센터보다 호환성 수준이 더 높은 데이터 센터로 데이터 스토리지 도메인을 마이그레이션하면 스토리지 도메인의 스토리지 형식 버전이 업그레이드됩니다.

가상 시스템을 새 데이터 센터로 마이그레이션하는 등의 이유로 스토리지 도메인을 원래 데이터 센터로 다시 이동하려는 경우 더 높은 버전으로 데이터 스토리지 도메인을 원래 데이터 센터에 다시 첨부하지 않도록 해야 합니다.

관리 포털에서 스토리지 도메인 형식(예: **V3**에서 **V 5** 로)을 업데이트하라는 메시지가 표시됩니다. 또한 **DC** 수준이 낮은 이전 데이터 센터에 다시 연결할 수 없다는 경고도 표시됩니다.

이 문제를 해결하기 위해 소스 데이터 센터와 동일한 호환성 버전이 있는 대상 데이터 센터를 만들 수 있습니다. 더 이상 호환성이 낮은 버전을 유지 관리할 필요가 없는 경우 대상 데이터 센터의 호환성 버전을 늘릴 수 있습니다.

자세한 내용은 [이전 RHV 버전에서 스토리지 도메인 및 가상 시스템 가져오기와 관련된 지원 가능성 및 제약 조건](#)을 참조하십시오.

절차

1. 소스 환경의 관리 포털에 로그인합니다.
2. 필요한 스토리지 도메인에서 실행 중인 모든 가상 시스템을 종료합니다.
3. **Storage**(스토리지 → **Domains** (도메인))를 클릭합니다.
4. 스토리지 도메인의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
5. **Data Center**(데이터 센터) 탭을 클릭합니다.
6. **Maintenance**(유지 관리)를 클릭한 다음 **OK**(확인)를 클릭합니다.
7. **Detach**(분리) 를 클릭한 다음 **OK**(확인)를 클릭합니다.
8. **Remove**(제거)를 클릭합니다.
9. **Remove Storage(s)**(스토리지 제거) 창에서 **Format Domain**(형식 도메인)을 확인합니다. 즉, **Storage Content**(스토리지 콘텐츠가 손실됨!) 확인란이 선택되지 않았는지 확인합니다. 이 단계에서는 나중에 사용하기 위해 스토리지 도메인의 데이터를 보존합니다.
10. **OK**(확인)를 클릭하여 소스 환경에서 스토리지 도메인을 제거합니다.
11. 대상 환경의 관리 포털에 로그인합니다.
12. **Storage**(스토리지 → **Domains** (도메인))를 클릭합니다.

13. **Import Domain (도메인 가져오기)**을 클릭합니다.
14. **Data Center (데이터 센터)** 드롭다운 목록에서 대상 데이터 센터를 선택합니다.
15. 스토리지 도메인의 이름을 입력합니다.
16. 적절한 드롭다운 목록에서 **Domain Function (도메인 기능)** 및 **Storage Type (스토리지 유형)**을 선택합니다.
17. **Host(호스트)** 드롭다운 목록에서 호스트를 선택합니다.
18. 스토리지 도메인의 세부 정보를 입력합니다.



참고

스토리지 도메인의 세부 정보를 지정하는 필드는 **Storage Type (스토리지 유형)** 드롭다운 목록에서 선택한 값에 따라 변경됩니다. 이러한 필드는 새 스토리지 도메인을 추가하는 데 사용할 수 있는 항목과 동일합니다.

19. **Activate Domain in Data Center (데이터 센터에서 도메인 활성화)** 확인란을 선택하여 스토리지 도메인을 연결할 때 자동으로 활성화합니다.
20. **OK(확인)**를 클릭합니다.

스토리지 도메인은 새로운 **Red Hat Virtualization** 환경의 대상 데이터 센터에 연결되며 자동으로 활성화됩니다. 이제 가져온 스토리지 도메인에서 대상 데이터 센터로 가상 머신 및 템플릿을 가져올 수 있습니다.



주의

대상 데이터 센터에 스토리지 도메인을 연결할 때 최신 스토리지 도메인 형식으로 업그레이드할 수 있으며 소스 데이터 센터에 다시 연결할 수 없습니다. 이렇게 하면 **Data-Domain**을 내보내기 도메인 대신 사용할 수 있습니다.

2.6.8.5. 가져온 데이터 스토리지 도메인에서 템플릿 가져오기

Red Hat Virtualization 환경으로 가져온 데이터 스토리지 도메인에서 템플릿을 가져옵니다. 이 절차에서는 가져온 데이터 스토리지 도메인이 데이터 센터에 연결되었으며 활성화되었다고 가정합니다.

절차

1. **Storage**(스토리지 → **Domains** (도메인))를 클릭합니다.
2. 가져온 스토리지 도메인의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Template Import**(템플릿 가져오기) 탭을 클릭합니다.
4. 가져올 하나 이상의 템플릿을 선택합니다.
5. **Import**(가져오기)를 클릭합니다.
6. **Import Templates(s)**(템플릿 가져오기) 창의 각 템플릿에 대해 클러스터 목록에서 올바른 대상 클러스터가 선택되어 있는지 확인합니다.
7. 외부 가상 머신 **vNIC** 프로필을 대상 클러스터에 있는 프로필에 매핑합니다.
 - a. **vNic Profiles Mapping**을 클릭합니다.
 - b. **Target vNic Profile**(대상 vNic Profile) 드롭다운 목록에서 사용할 **vNIC** 프로필을 선택

택합니다.

c.

Import Templates (템플릿 가져오기) 창에서 여러 대상 클러스터를 선택한 경우 **Target Cluster** (대상 클러스터) 드롭다운 목록에서 각 대상 클러스터를 선택하고 매핑이 올바른지 확인합니다.

d.

OK(확인)를 클릭합니다.

8.

OK(확인)를 클릭합니다.

가져온 템플릿은 **Template Import**(템플릿 가져오기) 탭의 목록에 더 이상 표시되지 않습니다.

2.6.9. 스토리지 작업

2.6.9.1. 데이터 스토리지 도메인에 이미지 업로드

관리 포털 또는 **REST API**에서 데이터 스토리지 도메인에 가상 디스크 이미지 및 **ISO** 이미지를 업로드할 수 있습니다.



참고

REST API를 사용하여 이미지를 업로드하려면 **REST API 가이드에서 IMAGETRANSFERS** 및 **IMAGETRANSFER**를 참조하십시오.

QEMU 호환 가상 디스크를 가상 머신에 연결할 수 있습니다. 가상 디스크 유형은 **QCOW2** 또는 **raw**여야 합니다. **QCOW2** 가상 디스크에서 생성된 디스크를 공유할 수 없으며 **QCOW2** 가상 디스크 파일에 백업 파일이 없어야 합니다.

ISO 이미지는 가상 머신에 **CDROM**으로 연결하거나 가상 시스템을 부팅하는 데 사용할 수 있습니다.

사전 요구 사항

업로드 기능은 **HTML 5 API**를 사용하며, 이를 위해 사용자 환경에서 다음을 수행해야 합니다.

- 인증 기관 - 관리 포털에 액세스하는 데 사용되는 웹 브라우저로 가져옵니다.

인증 기관을 가져오려면 https://engine_address/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA 로 이동하여 모든 신뢰 설정을 활성화합니다. [Firefox](#), [Internet Explorer](#) 또는 [Google Chrome](#) 에 인증 기관을 설치하려면 지침을 참조하십시오.
- **Firefox 35, Internet Explorer 10, Chrome 13** 이상과 같은 **HTML 5**를 지원하는 브라우저.

절차

1. **Storage** → **Disks** (스토리지 디스크)를 클릭합니다.
2. **Upload**(업로드) 메뉴에서 **Start**(시작)를 선택합니다.
3. **Choose File** (파일 선택)을 클릭하고 업로드할 이미지를 선택합니다.
4. **Disk Options**(디스크 옵션) 필드를 입력합니다. 관련 필드에 [대한 설명은 새 가상 디스크 창의 설정](#) 계획을 참조하십시오.
5. **OK**(확인)를 클릭합니다.

진행률 표시줄은 업로드 상태를 나타냅니다. 업로드 메뉴에서 업로드를 일시 중지, 취소 또는 다시 시작할 수 있습니다.

작은 정보

메시지와 함께 업로드 시간이 초과되는 경우, 전송 비활성으로 인한 이유: 시간 초과는 시간 초과 값을 늘리고 **ovirt-engine** 서비스를 다시 시작합니다.

```
# engine-config -s TransferImageClientInactivityTimeoutInSeconds=6000
# systemctl restart ovirt-engine
```

2.6.9.2. 스토리지 도메인에 VirtIO 이미지 파일 업로드

virtio-win_version.iso 이미지에는 **Windows** 가상 머신의 성능과 유용성을 향상시키기 위한 다음이

포함되어 있습니다.

- **Virtio 드라이버**
- **게스트 에이전트용 설치 프로그램**
- **드라이버 설치 프로그램**

virtio-win_version.iso 의 최신 버전을 설치하고 업로드하려면 :

1. **Manager 시스템에 이미지 파일을 설치합니다.**

```
# dnf -y install virtio-win
```

Manager 시스템에 설치한 후 이미지 파일은 /usr/share/virtio-win/virtio-win/virtio-win_version.iso입니다.

2. 설치 중에 로컬로 생성되지 않은 데이터 스토리지 도메인에 이미지 파일을 업로드합니다. 자세한 내용은 [관리 가이드](#) 의 [데이터 스토리지 도메인에 이미지 업로드](#) 를 참조하십시오.
3. 이미지 파일을 가상 시스템에 연결합니다.

이제 가상 시스템에서 **virtio** 드라이버 및 에이전트를 사용할 수 있습니다.

가상 머신에 이미지 파일 연결에 대한 자세한 내용은 [가상 머신 관리 가이드](#) 의 [Windows에서 게스트 에이전트, 툴 및 드라이버 설치](#) 를 참조하십시오.

2.6.9.3. ISO 도메인에 이미지 업로드



참고

ISO 도메인은 더 이상 사용되지 않는 스토리지 도메인 유형입니다. Red Hat Virtualization 4.4에서는 ISO 업로더 도구 **ovirt-iso-uploader**가 제거되었습니다. 관리 포털 또는 **REST API**를 사용하여 데이터 도메인에 ISO 이미지를 업로드해야 합니다. 자세한 내용은 [데이터 스토리지 도메인에 이미지 업로드](#)를 참조하십시오.

ISO 도메인은 더 이상 사용되지 않지만, ISO 도메인을 사용해야 하는 경우 이 정보에 제공됩니다.

관리자 내에서 사용할 수 있도록 ISO 스토리지 도메인에 ISO 이미지를 업로드하려면 다음 단계를 따르십시오.

절차

1. ISO 스토리지 도메인이 있는 데이터 센터에 속한 호스트에 **root**로 로그인합니다.
2. `/rhev/data-center`의 디렉토리 트리 가져오기 :

```
# tree /rhev/data-center
.
|-- 80dfacc7-52dd-4d75-ab82-4f9b8423dc8b
|   |-- 76d1ecba-b61d-45a4-8eb5-89ab710a6275 → /rhev/data-center/mnt/10.10.10.10:_rhevnfssd/76d1ecba-b61d-45a4-8eb5-89ab710a6275
|   |-- b835cd1c-111c-468d-ba70-fec5346af227 → /rhev/data-center/mnt/10.10.10.10:_rhevisosd/b835cd1c-111c-468d-ba70-fec5346af227
|   |-- mastersd → 76d1ecba-b61d-45a4-8eb5-89ab710a6275
|   |-- tasks → mastersd/master/tasks
|   `-- vms → mastersd/master/vms
|-- hsm-tasks
`-- mnt
    |-- 10.10.10.10:_rhevisosd
    |   |-- b835cd1c-111c-468d-ba70-fec5346af227
    |   |   |-- dom_md
    |   |   |   |-- ids
    |   |   |   |-- inbox
    |   |   |   |-- leases
    |   |   |   |-- metadata
    |   |   |   `-- outbox
    |   |   `-- images
    |   |       `-- 11111111-1111-1111-1111-111111111111
    |   `-- lost+found [error opening dir]
```

(output trimmed)

3.

소스 위치에서 이미지를 11111111-1111-1111-1111-111111111111 의 전체 경로로 안전하게 복사하십시오.

```
# scp root@isosource:/isos/example.iso /rhev/data-center/mnt/10.96.4.50:_rhevisosd/b835cd1c-111c-468d-ba70-fec5346af227/images/11111111-1111-1111-1111-111111111111
```

4.

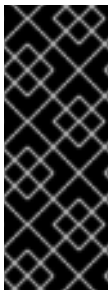
새로 복사한 ISO 이미지의 파일 권한은 36:36(vdsm:kvm)이어야 합니다. 그렇지 않은 경우 ISO 파일의 사용자 및 그룹 소유권을 36:36 (vdsm의 사용자 및 그룹)으로 변경합니다.

```
# cd /rhev/data-center/mnt/10.96.4.50:_rhevisosd/b835cd1c-111c-468d-ba70-fec5346af227/images/11111111-1111-1111-1111-111111111111
# chown 36.36 example.iso
```

이제 데이터 센터의 ISO 도메인에서 ISO 이미지를 사용할 수 있어야 합니다.

2.6.9.4. 스토리지 도메인을 유지 관리 모드로 이동

스토리지 도메인을 유지 관리 모드로 전환해야 분리 및 제거할 수 있습니다. 다른 데이터 도메인을 마스터 데이터 도메인으로 다시 설계하는 데 필요합니다.



중요

가상 머신의 스토리지 도메인에 리스가 있는 경우 스토리지 도메인을 유지 관리 모드로 이동할 수 없습니다. 가상 시스템을 종료하거나 먼저 리스를 제거하거나 다른 스토리지 도메인으로 이동해야 합니다. [가상 머신 리스를 위한 자세한 내용은 가상 머신 관리 가이드를 참조하십시오.](#)

LUN을 추가하여 iSCSI 도메인 확장은 도메인이 활성화된 경우에만 수행할 수 있습니다.

절차

1.

스토리지 도메인에서 실행 중인 모든 가상 시스템을 종료합니다.

2.

Storage(스토리지 → **Domains** (도메인) 를 클릭합니다.

3.

스토리지 도메인의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.

4.

Data Center(데이터 센터) 탭을 클릭합니다.

5.

Maintenance(유지 관리)를 클릭합니다.



참고

Ignore OVF 업데이트 실패 확인란을 통해 **OVF** 업데이트가 실패하더라도 스토리지 도메인이 유지 관리 모드로 전환됩니다.

6.

OK(확인)를 클릭합니다.

스토리지 도메인은 비활성화되고 결과 목록에 비활성 상태가 있습니다. 이제 데이터 센터에서 비활성 스토리지 도메인을 편집, 분리, 제거 또는 다시 활성화할 수 있습니다.



참고

연결된 데이터 센터의 세부 정보 보기에 있는 **Storage**(스토리지) 탭을 사용하여 도메인을 유지 관리 모드로 활성화, 분리 및 배치할 수도 있습니다.

2.6.9.5. 스토리지 도메인 편집

관리 포털을 통해 스토리지 도메인 매개 변수를 편집할 수 있습니다. 스토리지 도메인의 상태에 따라 **active** 또는 **inactive** 중 하나에 따라 다양한 필드를 편집할 수 있습니다. **Data Center** (데이터 센터), **Domain Function**(도메인 기능), **Storage Type** (스토리지 유형) 및 **Format** 과 같은 필드는 변경할 수 없습니다.

•

활성: 스토리지 도메인이 활성 상태인 경우 **Name**, **Description**, **Comment**, **Warning Low Space Indicator**(%), **Critical Space Action Blocker**(GB), **Wipe after Delete**(삭제 후 Wipe) 및 삭제 후 카드 비활성화 필드를 편집할 수 있습니다. **Name** (이름) 필드는 스토리지 도메인이 활성화된 경우에만 편집할 수 있습니다. 스토리지 도메인이 비활성화되는 동안 다른 모든 필드를 편집할 수도 있습니다.

•

비활성: 스토리지 도메인이 유지 관리 모드이거나 연결 해제된 상태이므로 비활성 상태인 경우 이름, 데이터 센터, 도메인 기능, 스토리지 유형, 형식을 제외한 모든 필드를 편집할 수 있습니다.

스토리지 연결, 마운트 옵션 및 기타 고급 매개 변수를 편집하려면 스토리지 도메인을 비활성화해야 합니다. 이는 **NFS, POSIX** 및 로컬 스토리지 유형에서만 지원됩니다.



참고

관리 포털을 통해 **iSCSI** 스토리지 연결을 편집할 수는 없지만 **REST API**를 통해 편집할 수 있습니다. **REST API 가이드**에서 **스토리지 연결 업데이트**를 참조하십시오.

활성 스토리지 도메인 편집*

1. **Storage → Domains** (스토리지 도메인)를 클릭하고 스토리지 도메인을 선택합니다.
2. **Manage Domain** (도메인 관리)을 클릭합니다.
3. 필요에 따라 사용 가능한 필드를 편집합니다.
4. **OK(확인)**를 클릭합니다.

비활성 스토리지 도메인 편집

1. **Storage**(스토리지 → **Domains** (도메인))를 클릭합니다.
2. 스토리지 도메인이 활성화된 경우 유지 관리 모드로 이동합니다.
 - a. 스토리지 도메인의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
 - b. **Data Center**(데이터 센터) 탭을 클릭합니다.
 - c. **Maintenance**(유지 관리)를 클릭합니다.
 - d. **OK(확인)**를 클릭합니다.

3.

Manage Domain (도메인 관리)을 클릭합니다.

4.

필요에 따라 스토리지 경로 및 기타 세부 정보를 편집합니다. 새 연결 세부 정보는 원래 연결과 동일한 스토리지 유형이어야 합니다.

5.

OK(확인)를 클릭합니다.

6.

스토리지 도메인을 활성화합니다.

a.

스토리지 도메인의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.

b.

Data Center(데이터 센터) 탭을 클릭합니다.

c.

Activate(활성화)를 클릭합니다.

2.6.9.6. OVF 업데이트

기본적으로 **OVF**는 60분마다 업데이트됩니다. 그러나 중요한 가상 머신을 가져오거나 중요한 업데이트를 수행한 경우 **OVF**를 수동으로 업데이트할 수 있습니다.

절차

1.

Storage(스토리지 → **Domains** (도메인))를 클릭합니다.

2.

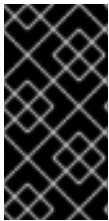
스토리지 도메인을 선택하고 추가 작업 ()을 클릭한 다음 **Update OVF**(확인)를 클릭합니다.

OVF가 업데이트되고 **Events**에 메시지가 표시됩니다.

2.6.9.7. 유지 관리 모드에서 스토리지 도메인 활성화

데이터 센터의 스토리지를 변경한 경우 스토리지 도메인을 유지 관리 모드로 전환해야 합니다. 스토리지 도메인을 활성화하여 사용을 재개합니다.

1. **Storage**(스토리지 → **Domains** (도메인) 를 클릭합니다.
2. 비활성 스토리지 도메인의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Data Centers**(데이터 센터) 탭을 클릭합니다.
4. **Activate**(활성화)를 클릭합니다.



중요

데이터 도메인을 활성화하기 전에 **ISO** 도메인을 활성화하려고 하면 오류 메시지가 표시되고 도메인이 활성화되지 않습니다.

2.6.9.8. 데이터 센터에서 스토리지 도메인 분리

한 데이터 센터에서 스토리지 도메인을 분리하여 다른 데이터 센터로 마이그레이션합니다.

절차

1. **Storage**(스토리지 → **Domains** (도메인) 를 클릭합니다.
2. 스토리지 도메인의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Data Center**(데이터 센터) 탭을 클릭합니다.
4. **Maintenance**(유지 관리)를 클릭합니다.
5. **OK**(확인)를 클릭하여 유지 관리 모드를 시작합니다.
6. **Detach**(분리) 를 클릭합니다.

7.

OK(확인)를 클릭하여 스토리지 도메인을 분리합니다.

스토리지 도메인이 데이터 센터에서 분리되어 다른 데이터 센터에 연결할 준비가 되었습니다.

2.6.9.9. 데이터 센터에 스토리지 도메인 연결

데이터 센터에 스토리지 도메인을 연결합니다.

절차

1.

Storage(스토리지 → **Domains** (도메인) 를 클릭합니다.

2.

스토리지 도메인의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.

3.

Data Center(데이터 센터) 탭을 클릭합니다.

4.

Attach(연결)를 클릭합니다.

5.

적절한 데이터 센터를 선택합니다.

6.

OK(확인)를 클릭합니다.

스토리지 도메인은 데이터 센터에 연결되며 자동으로 활성화됩니다.

2.6.9.10. 스토리지 도메인 제거

데이터 센터에 가상화된 환경에서 제거하려는 스토리지 도메인이 있습니다.

절차

1.

Storage(스토리지 → **Domains** (도메인) 를 클릭합니다.

2. 스토리지 도메인을 유지 관리 모드로 이동하고 분리합니다.
 - a. 스토리지 도메인의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
 - b. **Data Center**(데이터 센터) 탭을 클릭합니다.
 - c. **Maintenance**(유지 관리)를 클릭한 다음 **OK**(확인)를 클릭합니다.
 - d. **Detach**(분리)를 클릭한 다음 **OK**(확인)를 클릭합니다.
3. **Remove**(제거)를 클릭합니다.
4. 선택적으로 **Format Domain**(형식 도메인)을 선택합니다. 즉, 스토리지 콘텐츠가 손실됩니다! 도메인의 내용을 지우려면 확인란을 선택합니다.
5. **OK**(확인)를 클릭합니다.

스토리지 도메인은 환경에서 영구적으로 제거됩니다.

2.6.9.11. 스토리지 도메인 삭제

오류가 발생하는 스토리지 도메인은 일반적인 절차를 통해 제거할 수 없습니다. 스토리지 도메인을 삭제하면 가상화된 환경에서 스토리지 도메인이 강제로 제거됩니다.

절차

1. **Storage**(스토리지 → **Domains** (도메인))를 클릭합니다.
2. 스토리지 도메인을 선택하고 추가 작업 (



)을 클릭한 다음 **Destroy** (폐기)를 클릭합니다.

3. **Approve operation**(작업 승인) 확인란을 선택합니다.
4. **OK**(확인)를 클릭합니다.

2.6.9.12. 디스크 프로파일 생성

디스크 프로파일은 최대 처리량 수준과 스토리지 도메인의 가상 디스크에 대한 최대 입력 및 출력 작업을 정의합니다. 디스크 프로파일은 데이터 센터에 정의된 스토리지 프로파일을 기반으로 생성되며 프로파일을 적용하려면 개별 가상 디스크에 수동으로 할당해야 합니다.

이 절차에서는 스토리지 도메인이 속한 데이터 센터 아래에 서비스 항목의 하나 이상의 스토리지 품질을 이미 정의했다고 가정합니다.

절차

1. **Storage**(스토리지 → **Domains** (도메인) 를 클릭합니다.
2. 데이터 스토리지 도메인의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Disk Profiles**(디스크 프로파일) 탭을 클릭합니다.
4. **New** (새로 만들기)를 클릭합니다.
5. 디스크 프로파일에 **Name** (이름)과 **Description** (설명)을 입력합니다.
6. **QoS** (**QoS**) 목록에서 디스크 프로파일에 적용할 서비스 품질을 선택합니다.
7. **OK**(확인)를 클릭합니다.

2.6.9.13. 디스크 프로파일 제거

Red Hat Virtualization 환경에서 기존 디스크 프로파일을 제거합니다.

절차

1. **Storage**(스토리지 → **Domains** (도메인) 를 클릭합니다.
2. 데이터 스토리지 도메인의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Disk Profiles**(디스크 프로파일) 탭을 클릭합니다.
4. 제거할 디스크 프로파일을 선택합니다.
5. **Remove**(제거)를 클릭합니다.
6. **OK**(확인)를 클릭합니다.

디스크 프로파일이 모든 가상 디스크에 할당된 경우 해당 가상 디스크에서 디스크 프로파일이 제거됩니다.

2.6.9.14. 스토리지 도메인의 상태 보기

스토리지 도메인에는 일반 상태 외에 외부 상태가 있습니다. 외부 상태는 플러그인 또는 외부 시스템에서 보고하거나 관리자가 설정하며 스토리지 도메인 이름 왼쪽에 다음 아이콘 중 하나로 표시됩니다.

- **OK:** 아이콘 없음
- **Info:**

- **경고:**

- **Error:**


-

실패:



스토리지 도메인의 상태에 대한 자세한 내용을 보려면 스토리지 도메인의 이름을 클릭합니다. 그러면 세부 정보 보기가 열리고 **Events**(이벤트) 탭을 클릭합니다.

REST API를 사용하여 스토리지 도메인의 상태도 볼 수 있습니다. 스토리지 도메인의 **GET** 요청에는 상태가 포함된 **external_status** 요소가 포함됩니다.

이벤트 컬렉션을 통해 **REST API**에서 스토리지 도메인의 상태를 설정할 수 있습니다. 자세한 내용은 [REST API 가이드에서 이벤트 추가를 참조하십시오](#).

2.6.9.15. 스토리지 도메인 삭제 후 비활성화 설정

Discard after Delete(삭제 후 카드 비활성화) 확인란을 선택하면 논리 볼륨에서 **blkdiscard** 명령이 호출되고 기본 스토리지에 블록이 사용 가능함을 알리는 알림이 표시됩니다. 스토리지 어레이는 사용 가능한 공간을 사용하여 요청 시 할당할 수 있습니다. 삭제 후 삭제는 블록 스토리지에서만 작동합니다. **Red Hat Virtualization Manager** 파일 스토리지(예: **NFS**)에서는 플래그를 사용할 수 없습니다.

제한 사항:

-

삭제 후 삭제는 **iSCSI** 또는 파이버 채널과 같은 블록 스토리지 도메인에서만 사용할 수 있습니다.

-

기본 스토리지는 **Discard** 를 지원해야 합니다.

블록 스토리지 도메인을 만들 때 또는 블록 스토리지 도메인을 편집할 때 삭제 후 삭제 를 활성화할 수 있습니다. [블록 스토리지 준비 및 추가 및 스토리지 도메인 편집](#)을 참조하십시오.

2.6.9.16. 250개 이상의 호스트가 있는 환경에서 4K 지원 활성화

기본적으로 **GlusterFS** 도메인 및 로컬 스토리지 도메인은 최대 250개의 호스트가 있는 **Red Hat Virtualization** 환경에서 4K 블록 크기를 지원합니다. 특히 대용량 파일을 사용할 때 4K 블록 크기는 더 나

은 성능을 제공할 수 있으며 VDO와 같은 4K 호환성이 필요한 툴을 사용할 수도 있습니다.



참고

GlusterFS 스토리지는 더 이상 사용되지 않으며 향후 릴리스에서 더 이상 지원되지 않습니다.

Sanlock이 할당하는 **lockspace** 영역은 최대 호스트 수가 기본 250인 경우 1MB입니다. 4K 스토리지를 사용할 때 최대 호스트 수를 늘리면 **lockspace** 영역이 더 커집니다. 예를 들어 2000개의 호스트를 사용하는 경우 **lockspace** 영역은 8MB만큼 클 수 있습니다.

엔진 구성 매개 변수 **MaxNumberOfHostsInStoragePool** 을 설정하여 250개 이상의 호스트가 있는 환경에서 4K 블록 지원을 활성화할 수 있습니다.

절차

1. **Manager** 시스템에서 필요한 최대 호스트 수를 활성화합니다.

```
# engine-config -s MaxNumberOfHostsInStoragePool=NUMBER_OF_HOSTS
```

2. **JBoss Application Server**를 다시 시작하십시오.

```
# service jboss-as restart
```

예를 들어, 300개의 호스트가 있는 클러스터가 있는 경우 다음을 입력합니다.

```
# engine-config -s MaxNumberOfHostsInStoragePool=300
# service jboss-as restart
```

검증

Manager에서 **MaxNumberOfHostsInStoragePool** 매개 변수 값을 확인합니다.

```
# engine-config --get=MaxNumberOfHostsInStoragePool
MaxNumberOfHostsInStoragePool: 250 version: general
```

2.6.9.17. 4K 지원 비활성화

기본적으로 **GlusterFS** 도메인 및 로컬 스토리지 도메인은 **4K** 블록 크기를 지원합니다. 특히 대용량 파일을 사용할 때 **4K** 블록 크기는 더 나은 성능을 제공할 수 있으며 **VDO**와 같은 **4K** 호환성이 필요한 툴을 사용할 수도 있습니다.



참고

GlusterFS 스토리지는 더 이상 사용되지 않으며 향후 릴리스에서 더 이상 지원되지 않습니다.

4K 블록 지원을 비활성화할 수 있습니다.

절차

1. **4K** 블록 지원이 활성화되어 있는지 확인합니다.

```
$ vdsd-client Host getCapabilities
...
{
  "GLUSTERFS" : [
    0,
    512,
    4096,
  ]
  ...
}
```

2. `/etc/vdsm/vdsm.conf.d/gluster.conf` 를 편집하고 `enable_4k_storage` 를 `false`로 설정합니다. 예를 들면 다음과 같습니다.

```
$ vi /etc/vdsm/vdsm.conf.d/gluster.conf

[gluster]
# Use to disable 4k support
# if needed.
enable_4k_storage = false
```

2.6.9.18. 스토리지 도메인에서 사용 가능한 공간 모니터링

스토리지 도메인에서 사용 가능한 공간을 모니터링하고 스토리지 도메인이 용량에 가까운 경우 경고하도록 경고를 만들 수 있습니다. 도메인이 종료되는 에서 중요한 임계값을 정의할 수도 있습니다.

VDO(가상 데이터 최적화 도구) 및 썬 폴 지원을 사용하면 물리적으로 사용 가능한 것보다 더 많은 사

용 가능한 공간이 표시될 수 있습니다. VDO의 경우 이 동작이 예상되지만 관리자는 실제로 작성할 수 있는 데이터 양을 예측할 수 없습니다. **Warning Low Confirmed Space Indicator** 매개변수는 도메인이 물리적 공간 용량에 가까운 경우 알림을 받고 확인된 공간이 남아 있는 양을 보여줍니다. 확인된 공간은 데이터를 작성하는 데 사용할 수 있는 실제 공간을 나타냅니다.

절차

1. 관리 포털에서 **Storage(스토리지) Storage → Domain (스토리지 도메인)**을 클릭하고 스토리지 도메인의 이름을 클릭합니다.
2. **Manage Domain (도메인 관리)**을 클릭합니다. **Manage Domains(도메인 관리)** 대화 상자가 열립니다.
3. **Advanced Parameters (고급 매개 변수) 확장.**
4. **Warning low Space Indicator(%)**의 경우 백분율 값을 입력합니다. 스토리지 도메인의 사용 가능한 공간이 이 값에 도달하면 관리자는 도메인이 용량에 가까운 것으로 경고합니다.
5. **Critical Space Action Blocker(GB)**의 경우 값을 기가바이트 단위로 입력합니다. 스토리지 도메인에서 사용 가능한 공간이 이 값에 도달하면 **Manager**가 종료됩니다.
6. **Warning Low Confirmed Space Indicator(%)**의 경우 백분율 값을 입력합니다. 스토리지 도메인의 사용 가능한 공간이 이 값에 도달하면 관리자는 데이터 쓰기에 사용할 수 있는 실제 공간이 용량에 가까운 것으로 경고합니다.

2.7. 풀

2.7.1. 가상 머신 풀 소개

가상 시스템 풀은 모두 동일한 템플릿의 복제본이며 지정된 그룹의 모든 사용자가 필요에 따라 사용할 수 있는 가상 시스템 그룹입니다. 가상 시스템 풀을 사용하면 관리자가 사용자를 위한 일반화된 가상 시스템 세트를 신속하게 구성할 수 있습니다.

사용자는 풀에서 가상 머신을 가져와 가상 시스템 풀에 액세스합니다. 사용자가 풀에서 가상 시스템을 가져오는 경우 사용 가능한 경우 풀에 가상 시스템 중 하나가 제공됩니다. 해당 가상 시스템에는 풀을 기반으로 하는 템플릿의 운영 체제와 구성이 동일하지만, 사용자가 가상 시스템을 사용할 때마다 동일한 풀의 멤버를 받지 못할 수 있습니다. 사용자는 해당 풀의 구성에 따라 동일한 가상 머신 풀에서 여러 가상 머신을 사용할 수도 있습니다.

가상 머신 풀은 기본적으로 상태 비저장이므로 재부팅 시 가상 머신 데이터와 구성 변경 사항이 유지되지 않습니다. 그러나 풀을 상태 저장으로 구성하여 이전 사용자가 변경한 내용을 유지할 수 있습니다. 그러나 사용자가 가상 시스템 풀에서 가져온 가상 머신의 콘솔 옵션을 구성하는 경우 해당 옵션은 해당 가상 머신 풀의 기본값으로 설정됩니다.



참고

관리 포털에서 액세스할 때 풀에서 가져온 가상 시스템은 상태 비저장 방식이 아닙니다. 필요한 경우 관리자가 디스크에 변경 사항을 작성할 수 있어야 하기 때문입니다.

기본적으로 풀의 가상 시스템은 사용자가 가져올 때 시작하고 사용자가 완료되면 종료합니다. 그러나 가상 시스템 풀에는 사전 시작된 가상 머신도 포함될 수 있습니다. 사전 시작된 가상 시스템은 **up** 상태로 유지되며 사용자가 사용할 때까지 유휴 상태로 유지됩니다. 따라서 사용자는 이러한 가상 시스템을 즉시 사용할 수 있지만, 이러한 가상 시스템은 유휴 상태로 인해 사용하지 않는 경우에도 시스템 리소스를 사용합니다.

2.7.2. 가상 머신 풀 생성

공통 템플릿을 기반으로 여러 가상 머신이 포함된 가상 머신 풀을 생성할 수 있습니다. *가상 머신 봉인 및 템플릿 생성에 대한 정보는 가상 머신 관리 가이드의 템플릿을 참조하십시오.*

Windows 가상 머신의 sysprep 파일 구성 옵션

요구 사항에 따라 여러 **sysprep** 파일 구성 옵션을 사용할 수 있습니다.

풀에서 도메인에 참여할 필요가 없는 경우 `/usr/share/ovirt-engine/conf/sysprep/`에 있는 기본 **sysprep** 파일을 사용할 수 있습니다.

풀이 도메인에 참여해야 하는 경우 각 **Windows** 운영 체제에 대해 사용자 지정 **sysprep**을 생성할 수 있습니다.

1. `/usr/share/ovirt-engine/conf/osinfo-defaults.properties`에서 각 운영 체제의 관련 섹션을 새 파일로 복사하고 **99-defaults.properties**로 저장합니다.
2. **99-defaults.properties**에서 **Windows** 제품 활성화 키와 새 사용자 지정 **sysprep** 파일의 경로를 지정합니다.


```
os.operating_system.productKey.value=Windows_product_activation_key ...
OS.operating_system.sysprepPath.value =
${ENGINE_USR}/conf/sysprep/sysprep.operating_system
```

3. 도메인, 도메인 암호 및 도메인 관리자를 지정하여 새 **sysprep** 파일을 생성합니다.

```
<Credentials>
  <Domain>__AD_Domain__</Domain>
  <Password>__Domain_Password__</Password>
  <Username>__Domain_Administrator__</Username>
</Credentials>
```

다른 **Windows** 가상 머신 풀에 대해 다른 **sysprep** 설정을 구성해야 하는 경우 관리 포털에서 사용자 지정 **sysprep** 파일을 만들 수 있습니다(아래의 [가상 머신 풀 생성](#)을 참조하십시오). [자세한 내용은 가상 머신 가이드에서 가상 머신 구성 자동화에 Sysprep 사용](#)을 참조하십시오.

절차

1. **Compute → Pools** (컴퓨팅 풀)를 클릭합니다.
2. **New** (새로 만들기)를 클릭합니다.
3. 드롭다운 목록에서 클러스터 를 선택합니다.
4. 드롭다운 메뉴에서 **Template**(템플릿) 및 **version**(버전)을 선택합니다. 템플릿은 풀의 모든 가상 시스템에 대한 표준 설정을 제공합니다.
5. 드롭다운 목록에서 **Operating System** (운영 체제)을 선택합니다.
6. **Use Optimized for to optimize virtual machine for Desktop or Server.**



참고

고성능 가상 시스템이 단일 호스트 및 구체적인 리소스에 고정되므로 고성능 최적화는 풀에 권장되지 않습니다. 이러한 구성이 포함된 여러 가상 시스템이 포함된 풀이 제대로 실행되지 않습니다.

7.

Name(이름)을 입력하고 선택적으로 **Description** (설명)과 **Comment** (주석)를 입력합니다.

풀의 이름은 숫자 접미사가 있는 풀의 각 가상 머신에 적용됩니다. 플레이스 홀더로 ? 을 사용하여 가상 머신의 번호를 사용자 지정할 수 있습니다.

예 2.1. 풀 이름 및 가상 머신 번호 지정 예

•

풀: **MyPool**

가상 머신: **MyPool-1, MyPool-2, ... MyPool-10**

•

풀: **MyPool-???**

가상 머신: **MyPool-001, MyPool-002, ... MyPool-010**

8.

풀에 대한 **VM** 수를 입력합니다.

9.

Prestarted (사전 시작됨) 필드에 사전 시작할 가상 시스템 수를 입력합니다.

10.

단일 사용자가 세션에서 실행할 수 있는 사용자당 최대 **VM** 수를 선택합니다. 최소값은 **1** 입니다.

11.

Delete Protection (보호 삭제) 확인란을 선택하여 삭제 보호를 활성화합니다.

12.

Windows 이외의 가상 머신 풀을 생성 중이거나 기본 **sysprep** 을 사용하는 경우 이 단계를 건너뛰니다. **Windows** 가상 머신 풀에 대한 사용자 지정 **sysprep** 파일을 생성하는 경우 다음을 수행합니다.

a.

Show Advanced Options (고급 옵션 표시) 버튼을 클릭합니다.

b.

Initial Run(최초 실행) 탭을 클릭하고 **Use Cloud-Init/Sysprep**(Cloud-Init/Sysprep 사용) 확인란을 선택합니다.

c.

Authentication (인증) 화살표를 클릭하고 **User Name** (사용자 이름) 및 **Password** (암호)를 입력하거나 **Use already configured password** (이미 구성된 암호 사용)를 선택합니다.



참고

이 사용자 이름은 로컬 관리자의 이름입니다. 인증 섹션 또는 사용자 지정 **sysprep** 파일의 기본값(사용자)에서 해당 값을 변경할 수 있습니다.

d.

Custom Script (사용자 지정 스크립트) 화살표를 클릭하고 **/usr/share/ovirt-engine/conf/sysprep/**에 있는 기본 **sysprep** 파일의 내용을 텍스트 상자에 붙여넣습니다.

e.

sysprep 파일의 다음 값을 수정할 수 있습니다.

•

키. 사전 정의된 **Windows** 활성화 제품 키를 사용하지 않으려면 **<![CDATA[\$ProductKey\$]>**를 유효한 제품 키로 바꿉니다.

```
<ProductKey>
  <Key><![CDATA[$ProductKey$]]></Key>
</ProductKey>
```

예 2.2. Windows 제품 키 예

```
<ProductKey>
  <Key>0000-000-000-000</Key>
</ProductKey>
```

•

Windows 가상 머신이 참여할 도메인, 도메인의 암호 및 도메인 관리자의 사용자 이름:

```
<Credentials>
  <Domain>__AD_Domain__</Domain>
```

```
<Password>__Domain_Password__</Password>
<Username>__Domain_Administrator__</Username>
</Credentials>
```

예 2.3. 도메인 인증 정보 예

```
<Credentials>
  <Domain>addomain.local</Domain>
  <Password>12345678</Password>
  <Username>Sarah_Smith</Username>
</Credentials>
```

참고

도메인에 가입하려면 **Domain** (도메인), **Password** (암호), **Username**(사용자 이름)이 필요합니다. **Key**(키)는 활성화를 위한 것입니다. 둘 다 필요하지는 않습니다.

Initial Run(최초 실행) 탭에서 도메인 및 자격 증명을 수정할 수 없습니다.

- 로컬 관리자의 전체 이름:

```
<UserData>
...
  <FullName>__Local_Administrator__</FullName>
...
</UserData>
```

- 로컬 관리자의 **DisplayName** 및 **Name**:

```
<LocalAccounts>
  <LocalAccount wcm:action="add">
    <Password>
      <Value><![CDATA[$AdminPassword$]]></Value>
      <PlainText>true</PlainText>
    </Password>
    <DisplayName>__Local_Administrator__</DisplayName>
    <Group>administrators</Group>
    <Name>__Local_Administrator__</Name>
  </LocalAccount>
</LocalAccounts>
```

sysprep 파일의 나머지 변수는 **Initial Run**(최초 실행) 탭에 입력할 수 있습니다.

13.

선택 사항: 풀 유형 설정 :

a.

Type(유형) 탭을 클릭하고 **Pool Type**(풀 유형)을 선택합니다.

-

Manual (수동) - 관리자가 가상 머신을 풀에 명시적으로 반환합니다.

-

automatic - 가상 머신이 자동으로 가상 머신 풀로 반환됩니다.

b.

Stateful Pool (상태 저장 풀) 확인란을 선택하여 가상 시스템이 상태 저장 모드로 시작되었는지 확인합니다. 이렇게 하면 이전 사용자가 변경한 사항이 가상 시스템에 지속됩니다.

c.

OK(확인)를 클릭합니다.

14.

선택 사항: **SPICE** 프록시 재정의:

a.

Console(콘솔) 탭에서 **Override SPICE Proxy**(**SPICE** 프록시 재정의) 확인란을 선택합니다.

b.

Overridden SPICE 프록시 주소 텍스트 필드에서 글로벌 **SPICE** 프록시를 재정의할 **SPICE** 프록시 주소를 지정합니다.

c.

OK(확인)를 클릭합니다.

15.

Windows 가상 머신 풀의 경우 **Compute**(컴퓨팅 → **Virtual Machines** (가상 머신) 를 클릭하고 풀에서 각 가상 머신을 선택한 다음 **Run Once**(한 번 실행)를 클릭합니다.

참고

가상 머신이 시작되지 않고 정보 [windeploy.exe]가 %WINDIR%\panther\UnattendGC\setupact.log 에 표시되지 않는 경우 폴의 템플릿을 생성하는 데 사용된 Windows 가상 머신의 레지스트리에 UnattendFile 키를 추가합니다.

1. Windows 가상 머신에 unattend 파일이 있는 보조 CD-ROM 장치가 연결되어 있는지 확인합니다(예: A:\Unattend.xml).
2. 가상 시스템을 선택하고 Run(실행)을 한 번 클릭합니다.
3. Boot Options(부팅 옵션)에서 Attach Windows guest tools CD(Windows 게스트 도구 CD 연결)를 선택합니다.
4. Start(시작)를 클릭하고 Run(실행)을 클릭하고 Open (열기) 텍스트 상자에 있는 regedit 를 입력한 다음 OK(확인)를 클릭합니다.
5. 왼쪽 창에서 HKEY_LOCAL_MACHINE → SYSTEM → Setup 으로 이동합니다.
6. 오른쪽 창을 마우스 오른쪽 버튼으로 클릭하고 New → String Value (새 문자열 값)를 선택합니다.
7. 키 이름으로 UnattendFile 을 입력합니다.
8. 새 키를 두 번 클릭하고 무인 파일 이름과 경로를 입력합니다(예: 키의 값으로 A:\Unattend.xml).
9. 레지스트리를 저장하고, Windows 가상 머신을 봉인하고, 새 템플릿을 생성합니다. 자세한 내용은 가상 머신 관리 가이드의 [템플릿](#) 을 참조하십시오.

지정된 수의 동일한 가상 머신으로 가상 머신 폴을 생성하고 구성했습니다. 이러한 가상 시스템은 Compute Virtual Machines(컴퓨팅 가상 시스템) 에서 보거나 폴 이름을 클릭하여 세부 정보 보기를 열

수 있습니다. 풀의 가상 시스템은 아이콘에 따라 독립 가상 시스템과 구분됩니다.

2.7.3. 새 풀 및 풀 편집 창의 설정 및 제어 설명

2.7.3.1. 새 풀 및 풀 편집 일반 설정 설명

다음 표에서는 가상 머신 풀과 관련된 **New Pool**(새 풀) 및 **Edit Pool** (풀 편집) 창의 **General**(일반) 탭에 필요한 정보를 자세히 설명합니다. 기타 모든 설정은 **New Virtual Machine**(새 가상 시스템) 창의 설정과 동일합니다.

표 2.30. 일반 설정

필드 이름	설명
템플릿	가상 머신 풀을 기반으로 하는 template 및 template 하위 버전입니다. 템플릿의 최신 하위 버전을 기반으로 풀을 생성하면 풀의 모든 가상 시스템이 재부팅되면 최신 템플릿 버전이 자동으로 수신됩니다. 가상 머신 의 템플릿 구성에 대한 자세한 내용은 가상 머신 일반 설정 설명 및 설명 에서 새 템플릿 및 템플릿 편집 창의 가상 머신 관리 가이드 를 참조하십시오.
설명	가상 시스템 풀에 대한 의미 있는 설명입니다.
설명	가상 시스템 풀과 관련된 일반 텍스트를 사람이 읽을 수 있는 주석을 추가하는 필드입니다.
사전 시작된 VM	가상 머신 풀에서 시작할 가상 머신 수를 지정한 후 사용자가 해당 상태를 유지할 수 있습니다. 이 필드의 값은 가상 머신 풀의 총 가상 머신 수와 0 사이여야 합니다.
VM 수/풀 내 VM 수를 기준으로 계산	가상 머신 풀에서 생성하고 사용할 수 있는 가상 머신 수를 지정할 수 있습니다. 편집 창에서 가상 머신 풀의 가상 머신 수를 지정된 수만큼 늘릴 수 있습니다. 기본적으로 풀에서 생성할 수 있는 최대 가상 머신 수는 1000개입니다. 이 값은 engine-config 명령의 MaxVmsInPool 키를 사용하여 구성할 수 있습니다.
사용자당 최대 VM 수	단일 사용자가 한 번에 가상 머신 풀에서 가져올 수 있는 최대 가상 머신 수를 지정할 수 있습니다. 이 필드의 값은 1 에서 32,767 사이여야 합니다.
보호 삭제	풀의 가상 머신이 삭제되지 않도록 할 수 있습니다.

필드 이름	설명
봉인됨	템플릿의 시스템별 설정이 템플릿에서 프로비저닝된 가상 시스템에서 재현되지 않도록 합니다. 봉인 프로세스에 대한 자세한 내용은 템플릿으로 Windows 가상 머신 봉인에서 참조하십시오. https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.4/html-single/virtual_machine_management_guide#Sealing_a_Windows_Virtual_Machine_for_Deployment_as_a_Template

2.7.3.2. 새 풀 및 풀 유형 설정 편집 설명

다음 표에서는 **New Pool**(새 풀) 및 **Edit Pool** (풀 편집) 창의 **Type**(유형) 탭에 필요한 정보를 자세히 설명합니다.

표 2.31. 설정 입력

필드 이름	설명
풀 유형	이 드롭다운 메뉴에서는 가상 머신 풀의 유형을 지정할 수 있습니다. 다음 옵션을 사용할 수 있습니다. ● 자동: 사용자가 가상 머신 풀에서 가져온 가상 머신 사용을 완료하면 해당 가상 머신이 자동으로 가상 머신 풀로 반환됩니다. ● 수동: 사용자가 가상 머신 풀에서 가져온 가상 머신 사용을 마치고 나면 관리자가 가상 머신을 수동으로 반환할 때만 가상 머신이 가상 머신 풀로 반환됩니다.
상태 저장 풀	가상 머신이 다른 사용자에게 전달될 때 풀의 가상 머신 상태가 보존되는지 여부를 지정합니다. 즉, 이전 사용자가 변경한 내용은 가상 시스템에 지속됩니다.

2.7.3.3. 설명된 새 풀 및 풀 콘솔 설정 편집

다음 표에는 가상 머신 풀과 관련된 **New Pool**(새 풀) 또는 **Edit Pool** (풀 편집) 창의 **Console**(콘솔) 탭에 필요한 정보가 자세히 나와 있습니다. 다른 모든 설정은 **New Virtual Machine**(새 가상 시스템) 및 **Edit Virtual Machine** (가상 시스템 편집) 창의 설정과 동일합니다.

표 2.32. 콘솔 설정

필드 이름	설명
SPICE 프록시 재정의	글로벌 구성에 정의된 SPICE 프록시 재정의의 사용하려면 이 확인란을 선택합니다. 이 기능은 사용자가(예: VM 포털을 통해 연결) 호스트가 있는 네트워크 외부에 있는 경우 유용합니다.
재정의된 SPICE 프록시 주소	SPICE 클라이언트가 가상 머신에 연결되는 프록시. 이 프록시는 Red Hat Virtualization 환경에 정의된 글로벌 SPICE 프록시와 가상 머신 풀이 속하는 클러스터에 대해 정의된 SPICE 프록시(있는 경우)를 재정의합니다. 주소는 다음과 같은 형식이어야 합니다. <pre>protocol://host:port</pre>

2.7.3.4. 설명된 가상 머신 풀 호스트 설정

다음 표에는 **New Pool**(새 풀) 및 **Edit Pool** (풀 편집) 창의 **Host**(호스트) 탭에서 사용할 수 있는 옵션이 자세히 나와 있습니다.

표 2.33. 가상 머신 풀: 호스트 설정

필드 이름	서브 요소	설명
실행 시작		가상 시스템을 실행할 기본 호스트를 정의합니다. 다음 중 하나를 선택합니다. ● 클러스터의 모든 호스트 - 가상 시스템은 클러스터의 사용 가능한 모든 호스트에서 시작하고 실행할 수 있습니다. ● 특정 호스트 - 가상 시스템은 클러스터의 특정 호스트에서 실행을 시작합니다. 그러나 관리자 또는 관리자는 가상 시스템의 마이그레이션 및 고가용성 설정에 따라 가상 시스템을 클러스터의 다른 호스트로 마이그레이션할 수 있습니다. 사용 가능한 호스트 목록에서 특정 호스트 또는 호스트 그룹을 선택합니다.

필드 이름	서브 요소	설명
CPU 옵션	패스쓰루(Pass-Through) 호스트 CPU	를 선택하면 가상 시스템에서 호스트의 CPU 플래그를 사용할 수 있습니다. 선택하면 마이그레이션 옵션 은 수동 마이그레이션만 허용하도록 설정됩니다.
	동일한 TSC 빈도가 있는 호스트로만 마이그레이션	이 가상 시스템을 선택하면 동일한 TSC 빈도가 있는 호스트로만 마이그레이션할 수 있습니다. 이 옵션은 고성능 가상 시스템에만 유효합니다.
마이그레이션 옵션	마이그레이션 모드	가상 시스템을 실행하고 마이그레이션하는 옵션을 정의합니다. 여기에 있는 옵션을 사용하지 않으면 클러스터 정책에 따라 가상 시스템이 실행되거나 마이그레이션됩니다. ● 수동 및 자동 마이그레이션 허용 - 환경 상태에 따라 가상 시스템을 한 호스트에서 다른 호스트로 자동으로 마이그레이션하거나 관리자가 수동으로 마이그레이션할 수 있습니다. ● 수동 마이그레이션만 허용 - 가상 시스템은 관리자가 수동으로 한 호스트에서 다른 호스트로만 마이그레이션할 수 있습니다. ● 마이그레이션을 허용하지 마십시오. 가상 시스템을 자동으로 또는 수동으로 마이그레이션할 수 없습니다.
	마이그레이션 정책	마이그레이션 통합 정책을 정의합니다. 확인란을 선택하지 않은 상태로 두면 호스트에서 정책을 결정합니다. ● 클러스터 기본값 (Minimal downtime) - vdsm.conf의 덮어쓰기가 여전히 적용됩니다. 게스트 에이전트 후크 메커니즘이 비활성화되어 있습니다. ● 가동 중지 시간 최소화 - 일반적인 상황에서 가상

필드 이름	서브 요소	설명
		머신을 마이그레이션할 수 있습니다. 가상 시스템에는 다운타임이 발생하지 않아야 합니다. 가상 머신 마이그레이션이 오랜 시간 후에 수렴되지 않으면 마이그레이션이 중단됩니다(최대 500밀리초의 QEMU 반복에 따라). 게스트 에이전트 후크 메커니즘이 활성화되어 있습니다. ● Post-copy migration - 사용된 후 복사 후 마이그레이션은 소스 호스트의 가상 시스템 vCPU 마이그레이션 일시 중단, 최소 메모리 페이지만 전송하고, 대상 호스트에서 가상 시스템 vCPU를 활성화한 후 대상 호스트에서 가상 시스템 vCPU를 활성화하며, 가상 시스템이 대상에서 실행되는 동안 나머지 메모리 페이지를 전송합니다. 사후 복사 정책은 먼저 사전 복사를 시도하여 수렴이 발생할 수 있는지 확인합니다. 오랜 시간 후에 가상 머신 마이그레이션이 수렴되지 않으면 마이그레이션이 사후 복사로 전환됩니다. 따라서 마이그레이션된 가상 시스템의 다운타임을 크게 줄이고 소스 가상 시스템의 메모리 페이지 변경 속도와 관계없이 마이그레이션을 완료할 수 있습니다. 표준 사전 복사 마이그레이션을 통해 마이그레이션할 수 없는 지속적인 사용으로 가상 시스템을 마이그레이션하는 것이 최적입니다. 이 정책의 단점은 복사 후 단계에서 누락된 메모리 부분이 호스트 간에 전송되므로 가상 시스템이 상당히 느려질 수 있다는 것입니다.



주의
사후복

필드 이름	서브 요소	설명	사 프 르 세 스 를 완 료 하 기 전 에 네 트 워 크 연 결 이 끊 어 지 면 M a n a g e r 가 실행 중인 가상 시스템을 일시 중지한 다음 종료합니다. 가상 머신 가용성이 중요하거나 마 이 그

필드 이름	서브 요소	설명
		레이션 네트워크가 불안정한 경우에는 사후복사 마이그레이션을 사용하지 마십시오. ● 필요한 경우 워크로드 일시 중단 - 가상 시스템이 많은 워크로드를 실행하는 시기를 포함하여 대부분의 상황에서 가상 시스템을 마이그레이션할 수 있습니다. 이로 인해 가상 시스템에는 다른 설정보다 더 중요한 다운타임이 발생할 수 있습니다. 극심한 워크로드로 인해 마이그레이션이 중단될 수 있습니다. 게스트 에이전트 후크 메커니즘이 활성화되어 있습니다.

필드 이름	서브 요소	설명
	마이그레이션 암호화 활성화	마이그레이션 중에 가상 시스템을 암호화할 수 있습니다. ● 클러스터 기본값 ● 암호화 ● 암호화하지 않음
	병렬 마이그레이션	사용할 병렬 마이그레이션 연결의 여부와 수를 지정할 수 있습니다. ● 클러스터 기본값: 병렬 마이그레이션 연결은 클러스터 기본값에 따라 결정됩니다. ● 비활성화됨: 가상 시스템은 파형이 아닌 단일 연결을 사용하여 마이그레이션됩니다. ● Auto: 병렬 연결 수는 자동으로 결정됩니다. 이 설정은 병렬 연결을 자동으로 비활성화할 수 있습니다. ● 자동 병렬: 병렬 연결 수는 자동으로 결정됩니다. ● 사용자 정의: 기본 병렬 연결 수를 지정할 수 있으므로 실제 수가 더 낮을 수 있습니다.
	VM 마이그레이션 연결 수	이 설정은 Custom 을 선택한 경우에만 사용할 수 있습니다. 2에서 255 사이의 사용자 정의 병렬 마이그레이션 수입니다.
NUMA 설정	NUMA 노드 수	가상 시스템에 할당할 수 있는 호스트에서 사용 가능한 가상 NUMA 노드 수입니다.

필드 이름	서브 요소	설명
	NUMA 고정	NUMA 토폴로지 창을 엽니다. 이 창에는 호스트의 총 CPU, 메모리, NUMA 노드 및 가상 머신의 가상 NUMA 노드가 표시됩니다. 오른쪽에 있는 상자에서 각 vNUMA를 왼쪽의 NUMA 노드로 드래그하여 NUMA 노드를 호스팅하는 데 가상 NUMA 노드를 수동으로 고정할 수 있습니다. 메모리 할당에 Tune 모드를 설정할 수도 있습니다. strict - 메모리 할당을 대상 노드에 할당할 수 없는 경우 실패합니다. 기본 - 하나의 기본 노드에서 메모리가 할당됩니다. 충분한 메모리를 사용할 수 없는 경우 다른 노드에서 메모리를 할당할 수 있습니다. interleave - 메모리는 라운드 로빈 알고리즘의 노드에 할당됩니다. NUMA 고정을 정의하는 경우 수동 마이그레이션 만 허용하도록 마이그레이션 옵션이 설정됩니다.

2.7.3.5. 새 풀 및 풀 리소스 할당 설정 편집 설명

다음 표에서는 가상 머신 풀에 고유한 **New Pool**(새 풀) 및 **Edit Pool** (풀 편집) 창의 **Resource Allocation**(리소스 할당) 탭에 필요한 정보를 자세히 설명합니다. 기타 모든 설정은 **New Virtual Machine**(새 가상 시스템) 창의 설정과 동일합니다. 자세한 내용은 [가상 머신 관리 가이드에 설명된 Virtual Machine Resource Allocation Settings](#)에서 참조하십시오.

표 2.34. 리소스 할당 설정

필드 이름	서브 요소	설명
디스크 할당	자동 선택 대상	이 확인란을 선택하여 사용 가능한 공간이 가장 많은 스토리지 도메인을 자동으로 선택합니다. Target(대상) 및 Disk Profile(디스크 프로파일) 필드가 비활성화되어 있습니다.
	형식	이 필드는 읽기 전용이며 항상 QCOW2를 표시합니다.

2.7.3.6. 가상 머신 풀 편집

가상 시스템 풀을 만들고 나면 해당 속성을 편집할 수 있습니다. 가상 시스템 풀을 편집할 때 사용할 수 있는 속성은 새 가상 시스템 풀을 만들 때 사용 가능한 항목과 동일합니다. 단, **Number of VMs (VM 수)**가 풀의 VM 수 증가로 대체됩니다.



참고

가상 시스템 풀을 편집할 때 도입된 변경 사항은 새 가상 머신에만 적용됩니다. 도입된 변경 당시 이미 존재하는 가상 머신은 영향을 받지 않습니다.

절차

1. **Compute** → **Pools** (컴퓨팅 풀)를 클릭하고 가상 머신 풀을 선택합니다.
2. **Edit**(편집)를 클릭합니다.
3. 가상 머신 풀의 속성을 편집합니다.
4. **OK**(확인)를 클릭합니다.

2.7.3.7. 풀에서 가상 머신 사전 시작

가상 시스템 풀의 가상 머신은 기본적으로 전원이 꺼집니다. 사용자가 풀에서 가상 시스템을 요청하면 시스템의 전원이 켜져 사용자에게 할당됩니다. 반면, 사전 시작된 가상 시스템은 이미 실행 중이며 사용자에게 할당되기를 기다리고 있으므로 시스템에 액세스하기 전에 사용자가 기다려야 하는 시간을 줄입니다. 사전 시작된 가상 시스템을 종료하면 풀로 반환되고 원래 상태로 복원됩니다. 사전 시작된 가상 시스템의 최대 수는 풀의 가상 머신 수입니다.

사전 시작된 가상 시스템은 사용자가 구체적으로 할당되지 않은 가상 시스템에 즉시 액세스해야 하는 환경에 적합합니다. 자동 풀만 사전 시작되어 있을 수 있습니다.

절차

1. **Compute** → **Pools** (컴퓨팅 풀)를 클릭하고 가상 머신 풀을 선택합니다.

2. **Edit(편집)**를 클릭합니다.
3. **Prestarted VMs** (사전 시작된 VM) 필드에 사전 시작할 가상 시스템 수를 입력합니다.
4. **Type(유형)** 탭을 클릭합니다. **Pool Type(풀 유형)**이 **Automatic(자동)**으로 설정되어 있는지 확인합니다 .
5. **OK(확인)**를 클릭합니다.

2.7.3.8. 가상 머신 풀에 가상 머신 추가

가상 머신 풀에서 원래 프로비저닝된 것보다 많은 가상 머신이 필요한 경우 풀에 머신을 추가합니다.

절차

1. **Compute → Pools** (컴퓨팅 풀)를 클릭하고 가상 머신 풀을 선택합니다.
2. **Edit(편집)**를 클릭합니다.
3. 증가한 VM 수 필드에 추가 가상 시스템 수를 입력합니다.
4. **OK(확인)**를 클릭합니다.

2.7.3.9. 가상 머신 풀에서 가상 머신 분리

가상 머신 풀에서 가상 머신을 분리할 수 있습니다. 가상 머신을 분리하면 풀에서 가상 머신을 제거하여 독립적인 가상 머신이 됩니다.

절차

1. **Compute → Pools** (컴퓨팅 풀)를 클릭합니다.

2. 풀의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Virtual Machines** (가상 시스템) 탭을 클릭하여 풀의 가상 시스템을 나열합니다.
4. 가상 머신의 상태가 **Down** 인지 확인합니다. 실행 중인 가상 머신을 분리할 수 없습니다.
5. 하나 이상의 가상 시스템을 선택하고 **Detach**(분리)를 클릭합니다.
6. **OK**(확인)를 클릭합니다.



참고

가상 시스템은 여전히 환경에 존재하며 **Compute**(컴퓨팅) → **Virtual Machines** (가상 시스템)에서 보고 액세스할 수 있습니다. 분리된 가상 시스템이 독립 가상 시스템임을 나타내도록 아이콘이 변경됩니다.

2.7.3.10. 가상 머신 풀 제거

데이터 센터에서 가상 머신 풀을 제거할 수 있습니다. 먼저 풀의 모든 가상 머신을 삭제하거나 분리해야 합니다. 풀에서 가상 머신을 분리하면 해당 머신이 독립 가상 시스템으로 유지됩니다.

절차

1. **Compute** → **Pools** (컴퓨팅 풀)를 클릭하고 가상 머신 풀을 선택합니다.
2. **Remove**(제거)를 클릭합니다.
3. **OK**(확인)를 클릭합니다.

2.8. 가상 디스크

2.8.1. 가상 머신 스토리지 이해

Red Hat Virtualization은 다음과 같은 세 가지 스토리지 유형을 지원합니다. **NFS**, **iSCSI** 및 **FCP**.

각 유형에서 **SPM(Storage Pool Manager)**이라는 호스트는 호스트와 스토리지 간 액세스를 관리합니다. **SPM** 호스트는 스토리지 풀 내에서 전체 액세스 권한이 있는 유일한 노드입니다. **SPM**은 스토리지 도메인 메타데이터와 풀의 메타데이터를 수정할 수 있습니다. 다른 모든 호스트는 가상 시스템 하드 디스크 이미지 데이터에만 액세스할 수 있습니다.

기본적으로 **NFS**, 로컬 또는 **POSIX** 호환 데이터 센터에서 **SPM**은 썸 프로비저닝된 형식을 파일 시스템에 파일로 사용하여 가상 디스크를 생성합니다.

iSCSI 및 기타 블록 기반 데이터 센터에서 **SPM**은 제공된 논리 단위 번호(**LUN**) 위에 볼륨 그룹을 만들고 논리적 볼륨을 가상 디스크로 사용하도록 만듭니다. 블록 기반 스토리지의 가상 디스크는 기본적으로 사전 할당됩니다.

가상 디스크가 사전 할당되면 지정된 크기(**GB**)의 논리 볼륨이 생성됩니다. 가상 시스템은 **kpartx**, **vgscan**, **vg change** 또는 **mount**를 사용하여 **Red Hat Enterprise Linux** 서버에 마운트 하여 가상 시스템의 프로세스 또는 문제를 조사할 수 있습니다.

가상 디스크가 썸 프로비저닝되면 **1GB** 논리 볼륨이 생성됩니다. 논리 볼륨은 가상 시스템이 실행 중인 호스트에서 지속적으로 모니터링됩니다. 사용량이 임계값에 다다르면 호스트에서 **SPM**에 알리는 즉시 논리 볼륨을 **1GB**까지 확장합니다. 호스트는 논리 볼륨이 확장된 후 가상 시스템을 다시 시작합니다. 가상 머신이 일시 중지된 상태가 되면 **SPM**에서 디스크를 시간 단위로 확장할 수 없음을 의미합니다. 이는 **SPM**이 과도하게 사용되거나 스토리지 공간이 충분하지 않은 경우 발생합니다.

사전 할당(**raw**) 형식의 가상 디스크는 썸 프로비저닝(**QCOW2**) 형식의 가상 디스크보다 쓰기 속도가 훨씬 빠릅니다. 썸 프로비저닝은 가상 디스크를 만드는 데 소요되는 시간이 크게 단축됩니다. 썸 프로비저닝 형식은 **I/O** 집약적이지 않은 가상 시스템에 적합합니다. **I/O** 쓰기가 많은 가상 머신에는 사전 할당된 형식을 사용하는 것이 좋습니다. 4초마다 **1GB** 이상을 작성할 수 있는 경우 가능한 경우 사전 할당된 디스크를 사용합니다.

2.8.2. 가상 디스크 이해

Red Hat Virtualization에는 사전 할당(썸 프로비저닝됨) 및 스 패스(썸 프로비저닝됨) 스토리지 옵션이 포함되어 있습니다.

-

사전 할당됨

사전 할당된 가상 디스크는 가상 시스템에 필요한 모든 스토리지를 할당합니다. 예를 들어 가

상 시스템의 데이터 파티션용으로 생성된 **20GB**의 논리 볼륨은 생성 시 즉시 **20GB**의 스토리지 공간을 차지합니다.

-

스파스

관리자는 스파스 할당을 통해 전체 스토리지를 가상 시스템에 할당할 수 있지만 필요한 경우에만 스토리지가 할당됩니다.

예를 들어 **20GB** 씩 프로비저닝 논리 볼륨은 처음 생성할 때 **0GB**의 스토리지 공간을 차지합니다. 운영 체제가 설치되면 설치된 파일의 크기를 조정할 수 있으며 데이터가 최대 **20GB** 크기까지 추가되므로 계속 커질 수 있습니다.

스토리지 디스크에서 가상 디스크의 **ID** 를 볼 수 → 있습니다. 장치 이름(예: **/dev/vda0**)이 변경되어 디스크 손상이 발생할 수 있으므로 **ID** 를 사용하여 가상 디스크를 식별합니다. **/dev/disk/by-id** 에서 가상 디스크 **ID**를 볼 수도 있습니다.

스토리지 → 및 템플릿에 대한 세부 정보 보기의 **Disks(디스크)** 탭에서 볼 수 있습니다. 가상 크기는 가상 시스템에서 사용할 수 있는 총 디스크 공간입니다. 가상 디스크를 만들거나 편집할 때 **Size(GB)(크기(GB))** 필드에 입력한 번호입니다.

스토리지 도메인 및 템플릿 세부 정보 보기의 **Disks(디스크)** 탭에서 디스크의 실제 크기를 볼 수 있습니다. 지금까지 가상 시스템에 할당된 디스크 공간 크기입니다. 사전 할당된 디스크에는 가상 크기 및 실제 크기에 대해 동일한 값이 표시됩니다. 스파스 디스크는 할당된 디스크 공간 크기에 따라 다른 값을 표시할 수 있습니다.

가능한 스토리지 유형 및 형식 조합은 다음 표에 설명되어 있습니다.

표 2.35. 허용된 스토리지 조합

스토리지	형식	유형	참고
NFS	원시	사전 할당됨	초기 크기가 가상 디스크에 대해 정의된 스토리지 크기와 같고 형식 지정이 없는 파일입니다.
NFS	원시	스파스	초기 크기가 0에 가까워 포맷이 없는 파일.

스토리지	형식	유형	참고
NFS	QCOW2	스파스	초기 크기가 0에 가까워 QCOW2 형식이 있는 파일. 후속 계층은 QCOW2 형식이 됩니다.
SAN	원시	사전 할당됨	초기 크기가 있는 블록 장치는 가상 디스크에 대해 정의된 스토리지 크기와 동일하며 형식 지정이 없습니다.
SAN	QCOW2	스파스	초기 크기가 가상 디스크에 대해 정의된 크기(현재 1GB)보다 훨씬 작은 블록 장치이며 필요한 경우(현재 1GB 단위) 공간이 할당되는 QCOW2 포맷이 있습니다.

2.8.3. 삭제 후 가상 디스크를 초기화하는 설정

가상 디스크를 삭제할 때 관리 포털에서 **Wipe after Delete**(삭제 후) 확인란으로 표시된 **wipe_after_delete** 플래그가 0으로 바뀝니다. 기본값인 **false**로 설정된 경우 디스크를 삭제하면 재사용을 위해 이러한 블록이 열리지만 데이터가 지워지지 않습니다. 따라서 블록이 0으로 반환되지 않았기 때문에 이 데이터를 복구할 수 있습니다.

wipe_after_delete 플래그는 블록 스토리지에서만 작동합니다. 파일 스토리지(예: NFS)에서는 파일 시스템이 데이터가 없는지 확인하기 때문에 옵션은 아무 작업도 수행하지 않습니다.

가상 디스크에 **wipe_after_delete**를 활성화하는 것이 더 안전하며, 가상 디스크에 중요한 데이터가 포함되어 있는 경우 사용하는 것이 좋습니다. 이는 보다 집약적인 작업이며 사용자는 성능 저하 및 삭제 시간이 길어질 수 있습니다.



참고

삭제 후 초기화 기능은 **secure delete**와 동일하지 않으며, 동일한 스토리지에서 생성된 새 디스크만 이전 디스크의 데이터를 노출하지 않는다는 점에서 데이터가 스토리지에서 제거되도록 보장할 수 없습니다.

wipe_after_delete 플래그 기본값은 설정 프로세스 중에 **true**로 변경되거나([Red Hat Virtualization Manager 구성 참조](#)) 또는 [Red Hat Virtualization Manager](#)에서 **engine-config** 도구를 사용하여 변경할

수 있습니다. **ovirt-engine** 서비스를 다시 시작하여 설정이 변경되도록 합니다.



참고

wipe_after_delete 플래그의 기본 설정을 변경해도 이미 존재하는 디스크의 삭제 후 Wipe 에는 영향을 미치지 않습니다.

엔진 구성 도구를 사용하여 **SANWipeAfterDelete**를 기본값으로 설정합니다.

1.

set 작업을 사용하여 **engine-config** 툴 을 실행합니다.

```
# engine-config --set SANWipeAfterDelete=true
```

2.

ovirt-engine 서비스를 다시 시작하여 변경 사항을 적용합니다.

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

호스트에 있는 **/var/log/vdsm/vdsm.log** 파일을 확인하여 가상 디스크가 성공적으로 지워지고 삭제되었는지 확인할 수 있습니다.

성공적으로 초기화하기 위해 로그 파일에는 **storage_domain_id/volume_id** 항목이 0이 되어 삭제됩니다. 예를 들면 다음과 같습니다.

```
a9cb0625-d5dc-49ab-8ad1-72722e82b0bf/a49351a7-15d8-4932-8d67-512a369f9d61 was zeroed and will be deleted
```

성공적으로 삭제하려면 로그 파일에 **VG:storage_domain_id LVs: list_of_volume_ids, img:image_id** 로 완료된 항목이 포함됩니다. 예를 들면 다음과 같습니다.

```
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
```

초기화 실패하면 로그 메시지 **0ing storage_domain_id/volume_id** 실패를 표시합니다. 0 및 제거 이 볼륨을 수동으로, 실패한 삭제는 일부 VG에서 제거 실패로 표시됩니다. **storage_domain_id 0ed** 볼륨: **list_of_volume_ids**.

2.8.4. Red Hat Virtualization에서 공유 가능한 디스크

일부 애플리케이션은 서버 간에 스토리지를 공유해야 합니다. **Red Hat Virtualization**을 사용하면 가상 머신 하드 디스크를 공유 가능으로 표시하고 해당 디스크를 가상 머신에 연결할 수 있습니다. 이러한 방식으로 여러 클러스터 인식 게스트에서 단일 가상 디스크를 사용할 수 있습니다.

공유 디스크는 모든 상황에서 사용되지 않습니다. 클러스터된 데이터베이스 서버 및 기타고가용성 서비스와 같은 애플리케이션의 경우 공유 디스크가 적합합니다. 공유 디스크를 클러스터를 인식하지 않는 여러 게스트에 연결하는 경우 디스크에 대한 읽기 및 쓰기가 조정되지 않기 때문에 데이터 손상이 발생할 수 있습니다.

공유 디스크의 스냅샷을 만들 수 없습니다. 스냅샷이 생성된 가상 디스크는 나중에 공유할 수 없습니다.

디스크를 생성할 때 또는 나중에 디스크를 편집하여 공유할 수 있는 디스크를 표시할 수 있습니다.

2.8.5. Red Hat Virtualization에서 디스크만 읽기

일부 애플리케이션에서는 관리자가 읽기 전용 권한으로 데이터를 공유해야 합니다. 가상 머신의 세부 정보 보기에 있는 **Disks(디스크)** 탭을 통해 가상 머신에 연결된 디스크를 만들거나 편집한 후 읽기 전용 확인란을 선택할 때 이 작업을 수행할 수 있습니다. 이렇게 하면 관리자가 쓰기 권한을 유지 관리하는 동안 단일 디스크를 여러 클러스터 인식 게스트에서 읽을 수 있습니다.

가상 머신이 실행되는 동안 디스크의 읽기 전용 상태를 변경할 수 없습니다.



중요

저널링된 파일 시스템을 마운트하려면 읽기-쓰기 액세스 권한이 필요합니다. **Read Only** (읽기 전용) 옵션은 이러한 파일 시스템을 포함하는 가상 디스크에는 적합하지 않습니다(예: **EXT3**, **EXT4** 또는 **XFS**).

2.8.6. 가상 디스크 작업

2.8.6.1. 가상 디스크 생성

이미지 디스크 생성은 전적으로 **Manager**에서 관리합니다. 직접 **LUN** 디스크에는 이미 존재하는 외부에서 준비된 대상이 필요합니다.

특정 가상 머신에 연결된 가상 디스크를 생성할 수 있습니다. 연결된 가상 디스크를 만들 때 [새 가상 디스크 창의 설정](#) 계획에 지정된 대로 추가 옵션을 사용할 수 있습니다.

가상 머신에 연결된 가상 디스크 생성

1. **Compute(컴퓨팅) Virtual Machines(가상 시스템)** 를 클릭합니다.
2. 가상 시스템의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. 디스크 탭을 클릭합니다.
4. **New (새로 만들기)**를 클릭합니다.
5. 적절한 버튼을 클릭하여 가상 디스크가 이미지 인지 또는 **LUN** 디스크 직접 디스크인지 지정합니다.
6. 가상 디스크에 필요한 옵션을 선택합니다. 옵션은 선택한 디스크 유형에 따라 변경됩니다. 각 [디스크 유형에 대한 각 옵션에 대한 자세한 내용은 새 가상 디스크 창의 설정](#) 계획을 참조하십시오.
7. **OK(확인)**를 클릭합니다.

또한 가상 머신에 속하지 않는 유동 가상 디스크를 생성할 수 있습니다. 디스크를 공유할 수 있는 경우 단일 가상 머신 또는 여러 가상 머신에 이 디스크를 연결할 수 있습니다. [새 가상 디스크 창에서 설정 계획](#)에서 지정한 대로 가상 디스크를 만들 때 일부 옵션을 사용할 수 없습니다.

유동 가상 디스크 생성

1. **Storage → Disks (스토리지 디스크)**를 클릭합니다.
2. **New (새로 만들기)**를 클릭합니다.

3. 적절한 버튼을 클릭하여 가상 디스크가 이미지 인지 또는 **LUN** 디스크 직접 디스크인지 지정합니다.
4. 가상 디스크에 필요한 옵션을 선택합니다. 옵션은 선택한 디스크 유형에 따라 변경됩니다. 각 **디스크 유형에 대한 각 옵션에 대한 자세한 내용은 새 가상 디스크 창의 설정** 계획을 참조하십시오.
5. **OK(확인)**를 클릭합니다.

2.8.6.2. New Virtual Disk(새 가상 디스크) 창의 설정 설명

유동 및 연결된 가상 디스크를 생성하기 위한 **New Virtual Disk(새 가상 디스크)** 창이 매우 유사하기 때문에 해당 설정은 단일 섹션에 설명되어 있습니다.

표 2.36. 새로운 가상 디스크 및 편집 가상 디스크 설정: Image

필드 이름	설명
크기(GB)	새 가상 디스크의 크기(GB)입니다.
alias	가상 디스크의 이름입니다. 40자로 제한됩니다.
설명	가상 디스크에 대한 설명입니다. 이 필드는 권장되지만 필수는 아닙니다.
인터페이스	이 필드는 연결된 디스크를 만들 때만 표시됩니다. 디스크가 가상 시스템에 제공하는 가상 인터페이스입니다. VirtIO는 더 빠르지만 드라이버가 필요합니다. Red Hat Enterprise Linux 5 이상에는 다음과 같은 드라이버가 포함되어 있습니다. Windows에는 이러한 드라이버가 포함되지 않지만 virtio-win ISO 이미지에서 설치할 수 있습니다. IDE 및 SATA 장치에는 특수 드라이버가 필요하지 않습니다. 디스크가 연결된 모든 가상 머신을 중지한 후 인터페이스 유형을 업데이트할 수 있습니다.
데이터 센터	이 필드는 유동 디스크를 만들 때만 표시됩니다. 가상 디스크를 사용할 수 있는 데이터 센터입니다.

필드 이름	설명
스토리지 도메인	가상 디스크를 저장할 스토리지 도메인입니다. 드롭다운 목록은 지정된 데이터 센터에서 사용할 수 있는 모든 스토리지 도메인을 표시하며, 스토리지 도메인에서 현재 사용 가능한 총 공간과 공간을 표시합니다.
할당 정책	새 가상 디스크에 대한 배포 정책입니다. - 가상 디스크를 생성할 때 스토리지 도메인에 디스크의 전체 크기를 사전 할당합니다. 가상 크기와 사전 할당된 디스크의 실제 크기는 동일합니다. 사전 할당된 가상 디스크는 썸 프로비저닝된 가상 디스크보다 생성하는 데 더 많은 시간이 소요되지만 읽기 및 쓰기 성능이 향상됩니다. 서버 및 기타 I/O 집약적인 가상 시스템에 사전 할당된 가상 디스크가 권장됩니다. 4초마다 1GB 이상을 작성할 수 있는 경우 가능한 경우 사전 할당된 디스크를 사용합니다. 썸 프로비저닝은 가상 디스크를 만들 때 1GB를 할당하며, 디스크가 증가할 수 있는 크기에 대한 최대 제한을 설정합니다. 디스크의 가상 크기는 최대 한도입니다. 실제 디스크 크기는 지금까지 할당된 공간입니다. 썸 프로비저닝된 디스크는 사전 할당된 디스크보다 빠르게 생성되고 과다 할당 스토리지를 허용합니다. 데스크탑에는 썸 프로비저닝된 가상 디스크가 권장됩니다.
디스크 프로파일	가상 디스크에 할당된 디스크 프로파일입니다. 디스크 프로파일은 스토리지 도메인의 가상 디스크에 대한 최대 처리량 양과 최대 입력 및 출력 작업을 정의합니다. 디스크 프로파일은 데이터 센터에 대해 생성된 서비스 항목의 스토리지 품질에 따라 스토리지 도메인 수준에서 정의됩니다.
디스크 활성화	이 필드는 연결된 디스크를 만들 때만 표시됩니다. 생성 후 즉시 가상 디스크를 활성화합니다.
삭제 후 지우기	가상 디스크를 삭제할 때 중요한 자료의 삭제를 위한 강화된 보안을 활성화할 수 있습니다.
부팅 가능	이 필드는 연결된 디스크를 만들 때만 표시됩니다. 가상 디스크에서 부팅 가능한 플래그를 활성화할 수 있습니다.
공유 가능	한 번에 둘 이상의 가상 머신에 가상 디스크를 연결할 수 있습니다.

필드 이름	설명
Read-Only	이 필드는 연결된 디스크를 만들 때만 표시됩니다. 를 사용하여 디스크를 읽기 전용으로 설정할 수 있습니다. 동일한 디스크는 한 가상 시스템에 읽기 전용으로 연결할 수 있으며 다른 가상 시스템에 다시 쓸 수 있습니다.
중분 백업 활성화	가상 디스크에서 중분 백업을 활성화합니다. 중분 백업에서는 RAW 형식 대신 QCOW2 형식으로 디스크를 포맷해야 합니다. 중분 백업 및 복원 을 참조하십시오.
카드 비활성화 활성화	이 필드는 연결된 디스크를 만들 때만 표시됩니다. 가상 시스템이 가동되는 동안 썸 프로비저닝된 디스크를 축소할 수 있습니다. 블록 스토리지의 경우 기본 스토리지 장치는 삭제 호출을 지원해야 하며 기본 스토리지에서 discard_zeroes_data 속성을 지원하지 않는 한 옵션은 Wipe after Delete 와 함께 사용할 수 없습니다. 파일 스토리지의 경우 기본 파일 시스템 및 블록 장치에서 삭제 호출을 지원해야 합니다. 모든 요구 사항이 충족되면 게스트 가상 머신에서 발행된 SCSI UNMAP 명령이 QEMU에 의해 기본 스토리지로 전달되어 사용되지 않는 공간을 확보합니다.

직접 LUN 설정은 대상 > LUN 또는 LUN > 대상에 표시할 수 있습니다. 대상 > LUN은 검색된 호스트에 따라 사용 가능한 LUN을 정렬하는 반면 LUN > 대상은 단일 LUN 목록을 표시합니다.

Discover Targets(대상 검색) 섹션에서 필드를 입력하고 **Discover** (검색)를 클릭하여 대상 서버를 검색합니다. 그런 다음 **Login All** (로그인 모두) 버튼을 클릭하여 대상 서버에서 사용 가능한 LUN을 나열하고 각 LUN 옆에 있는 라디오 버튼을 사용하여 추가할 LUN을 선택할 수 있습니다.

LUN을 가상 시스템 하드 디스크 이미지로 직접 사용하면 가상 시스템과 해당 데이터 간의 추상화 계층이 제거됩니다.

직접 LUN을 가상 머신 하드 디스크 이미지로 사용할 때는 다음과 같은 사항을 고려해야 합니다.

- 직접 LUN 하드 디스크 이미지의 실시간 스토리지 마이그레이션은 지원되지 않습니다.
- 직접 LUN 디스크는 가상 머신 내보내기에 포함되지 않습니다.

● 직접 LUN 디스크는 가상 머신 스냅샷에 포함되지 않습니다.

표 2.37. 새로운 가상 디스크 및 편집 가상 디스크 설정: 직접 LUN

필드 이름	설명
alias	가상 디스크의 이름입니다. 40자로 제한됩니다.
설명	가상 디스크에 대한 설명입니다. 이 필드는 권장되지만 필수는 아닙니다. 기본적으로 LUN ID의 마지막 4자가 필드에 삽입됩니다. 기본 동작은 engine-config 명령을 사용하여 PopulateDirectLUNDiskDescriptionWithLUNID 구성 키를 적절한 값으로 설정하여 구성할 수 있습니다. 전체 LUN ID를 사용하려면 구성 키를 -1 로, 이 기능을 무시하려면 0 으로 설정할 수 있습니다. 양의 정수는 설명을 LUN ID의 해당 문자로 채웁니다.
인터페이스	이 필드는 연결된 디스크를 만들 때만 표시됩니다. 디스크가 가상 시스템에 제공하는 가상 인터페이스입니다. VirtIO 는 더 빠르지만 드라이버가 필요합니다. Red Hat Enterprise Linux 5 이상에는 다음과 같은 드라이버가 포함되어 있습니다. Windows에는 이러한 드라이버가 포함되지 않지만 virtio-win ISO에서 설치할 수 있습니다. IDE 및 SATA 장치에는 특수 드라이버가 필요하지 않습니다. 디스크가 연결된 모든 가상 머신을 중지한 후 인터페이스 유형을 업데이트할 수 있습니다.
데이터 센터	이 필드는 유동 디스크를 만들 때만 표시됩니다. 가상 디스크를 사용할 수 있는 데이터 센터입니다.
호스트	LUN이 마운트될 호스트입니다. 데이터 센터에서 호스트를 선택할 수 있습니다.
스토리지 유형	추가할 외부 LUN의 유형입니다. iSCSI 또는 Fibre 채널 중 하나를 선택할 수 있습니다.

필드 이름	설명
검색 대상	이 섹션은 iSCSI 외부 LUN 및 대상 > LUN 을 사용할 때 확장할 수 있습니다. address - 대상 서버의 호스트 이름 또는 IP 주소입니다. port - 대상 서버에 대한 연결을 시도할 포트입니다. 기본 포트는 3260입니다. User Authentication(사용자 인증) - iSCSI 서버에는 사용자 인증이 필요합니다. iSCSI 외부 LUN을 사용하는 경우 User Authentication (사용자 인증) 필드가 표시됩니다. CHAP 사용자 이름 - LUN에 로그인할 권한이 있는 사용자의 사용자 이름입니다. 이 필드는 User Authentication (사용자 인증) 확인란이 선택된 경우 액세스할 수 있습니다. CHAP 암호 - LUN에 로그인할 권한이 있는 사용자의 암호입니다. 이 필드는 User Authentication (사용자 인증) 확인란이 선택된 경우 액세스할 수 있습니다.
디스크 활성화	이 필드는 연결된 디스크를 만들 때만 표시됩니다. 생성 후 즉시 가상 디스크를 활성화합니다.
부팅 가능	이 필드는 연결된 디스크를 만들 때만 표시됩니다. 가상 디스크에서 부팅 가능한 플래그를 활성화할 수 있습니다.
공유 가능	한 번에 둘 이상의 가상 머신에 가상 디스크를 연결할 수 있습니다.
Read-Only	이 필드는 연결된 디스크를 만들 때만 표시됩니다. 를 사용하여 디스크를 읽기 전용으로 설정할 수 있습니다. 동일한 디스크는 한 가상 시스템에 읽기 전용으로 연결할 수 있으며 다른 가상 시스템에 다시 쓸 수 있습니다.
카드 비활성화 활성화	이 필드는 연결된 디스크를 만들 때만 표시됩니다. 가상 시스템이 가동되는 동안 켜진 프로비저닝된 디스크를 축소할 수 있습니다. 이 옵션을 활성화하면 게스트 가상 머신에서 발행된 SCSI UNMAP 명령이 QEMU에 의해 기본 스토리지로 전달되어 사용되지 않는 공간을 확보할 수 있습니다.

필드 이름	설명
SCSI 패스쓰루 활성화	이 필드는 연결된 디스크를 만들 때만 표시됩니다. Interface (인터페이스)가 VirtIO-SCSI 로 설정된 경우 사용 가능. 이 확인란을 선택하면 가상 디스크에 대한 물리적 SCSI 장치를 통과할 수 있습니다. SCSI 패스쓰루가 활성화된 VirtIO-SCSI 인터페이스에는 SCSI 삭제 지원이 자동으로 포함됩니다. 이 확인란을 선택하면 읽기 전용 이 지원되지 않습니다. 이 확인란을 선택하지 않으면 가상 디스크에서 에뮬레이트된 SCSI 장치를 사용합니다. 읽기 전용 은 에뮬레이트된 VirtIO-SCSI 디스크에서 지원됩니다.
Privileged SCSI I/O 허용	이 필드는 연결된 디스크를 만들 때만 표시됩니다. Enable SCSI Pass-Through(SCSI 패스쓰루 사용) 확인란이 선택되면 사용할 수 있습니다. 이 확인란을 선택하면 필터링되지 않은 SCSI 일반 I/O(SG_IO) 액세스를 활성화하여 디스크에 권한 있는 SG_IO 명령을 허용합니다. 이는 지속적인 예약에 필요합니다.
SCSI 예약 사용	이 필드는 연결된 디스크를 만들 때만 표시됩니다. Enable SCSI Pass-Through and Allow Privileged SCSI I/O 확인란이 선택되면 사용할 수 있습니다. 이 확인란을 선택하면 SCSI 예약을 사용하는 가상 머신이 디스크에 대한 액세스가 손실되지 않도록 이 디스크를 사용하는 모든 가상 시스템의 마이그레이션이 비활성화됩니다.

중요

저널링된 파일 시스템을 마운트하려면 읽기-쓰기 액세스 권한이 필요합니다. **Read-Only** 옵션을 사용하는 것은 이러한 파일 시스템을 포함하는 가상 디스크에 적합하지 않습니다(예: EXT3,EXT4 또는 XFS).

2.8.6.3. 실시간 스토리지 마이그레이션 개요

연결된 가상 시스템이 실행되는 동안 가상 디스크를 한 스토리지 도메인에서 다른 스토리지 도메인으로 마이그레이션할 수 있습니다. 이를 실시간 스토리지 마이그레이션이라고 합니다. 실행 중인 가상 시스템에 연결된 디스크를 마이그레이션하면 해당 디스크의 이미지 체인의 스냅샷이 소스 스토리지 도메인에 생성되고 전체 이미지 체인이 대상 스토리지 도메인에 복제됩니다. 따라서 디스크 이미지 체인과 스냅샷을 모두 호스팅할 대상 스토리지 도메인과 소스 스토리지 도메인 모두에 충분한 스토리지 공간이 있는지 확인합니다. 마이그레이션이 실패하더라도 각 실시간 스토리지 마이그레이션 시도에 새 스냅샷이 생성됩니다.

실시간 스토리지 마이그레이션을 사용하는 경우 다음을 고려하십시오.

- 한 번에 여러 디스크를 실시간으로 마이그레이션할 수 있습니다.
- 동일한 가상 시스템의 여러 디스크는 둘 이상의 스토리지 도메인에 있을 수 있지만 각 디스크의 이미지 체인은 단일 스토리지 도메인에 있어야 합니다.
- 동일한 데이터 센터에 있는 두 스토리지 도메인 간에 디스크를 실시간 마이그레이션할 수 있습니다.
- 공유 가능으로 표시된 직접 LUN 하드 디스크 이미지 또는 디스크를 실시간 마이그레이션할 수 없습니다.

2.8.6.4. 가상 디스크 이동

가상 시스템에 연결된 가상 디스크를 이동하거나 한 스토리지 도메인에서 다른 스토리지 도메인으로 유동 가상 디스크 역할을 합니다. 실행 중인 가상 머신에 연결된 가상 디스크를 이동할 수 있습니다. 이를 실시간 스토리지 마이그레이션이라고 합니다. 또는 계속하기 전에 가상 시스템을 종료합니다.

디스크를 이동할 때 다음을 고려하십시오.

- 동시에 여러 디스크를 이동할 수 있습니다.
- 동일한 데이터 센터에 있는 두 스토리지 도메인 간에 디스크를 이동할 수 있습니다.
- 가상 디스크가 템플릿을 기반으로 생성된 가상 머신에 연결되어 있고 켜진 프로비저닝 스토리지 할당 옵션을 사용하는 경우 가상 시스템이 가상 디스크와 동일한 스토리지 도메인을 기반으로 하는 템플릿의 디스크를 복사해야 합니다.

절차

1. **Storage** → **Disks** (스토리지 디스크)를 클릭하고 이동할 하나 이상의 가상 디스크를 선택합니다.

2. **Move(이동)**를 클릭합니다.
3. **Target(대상)** 목록에서 가상 디스크를 이동할 스토리지 도메인을 선택합니다.
4. **Disk Profile (디스크 프로파일)** 목록에서 해당하는 경우 디스크의 프로필을 선택합니다.
5. **OK(확인)**를 클릭합니다.

가상 디스크는 대상 스토리지 도메인으로 이동합니다. 이동 절차 중에 **Status(상태)** 열에 **Locked(잠김)** 열에 이동 작업의 진행률을 나타내는 진행 표시줄이 표시됩니다.

2.8.6.5. 디스크 인터페이스 유형 변경

사용자는 디스크를 만든 후 디스크의 인터페이스 유형을 변경할 수 있습니다. 이를 통해 기존 디스크를 다른 인터페이스 유형이 필요한 가상 머신에 연결할 수 있습니다. 예를 들어 **VirtIO** 인터페이스를 사용하는 디스크를 **VirtIO -SCSI** 또는 **IDE** 인터페이스가 필요한 가상 시스템에 연결할 수 있습니다. 따라서 백업 및 복원 또는 재해 복구를 위해 디스크를 마이그레이션할 수 있는 유연성이 제공됩니다. 공유 가능한 디스크 인터페이스도 가상 시스템별로 업데이트할 수 있습니다. 즉, 공유 디스크를 사용하는 각 가상 시스템은 다른 인터페이스 유형을 사용할 수 있습니다.

디스크 인터페이스 유형을 업데이트하려면 디스크를 사용하는 모든 가상 시스템을 먼저 중지해야 합니다.

디스크 인터페이스 유형 변경*

1. **Compute(컴퓨팅) → Virtual Machines (가상 시스템)**를 클릭하고 적절한 가상 시스템을 중지합니다.
2. 가상 시스템의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Disks(디스크)** 탭을 클릭하고 디스크를 선택합니다.
4. **Edit(편집)**를 클릭합니다.

5.

Interface (인터페이스) 목록에서 새 인터페이스 유형을 선택하고 **OK**(확인)를 클릭합니다.

다른 인터페이스 유형이 필요한 다른 가상 머신에 디스크를 연결할 수 있습니다.

다른 인터페이스 유형을 사용하여 다른 가상 머신에 디스크 연결

1.

Compute(컴퓨팅) → **Virtual Machines** (가상 시스템)를 클릭하고 적절한 가상 시스템을 중지합니다.

2.

가상 시스템의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.

3.

Disks(디스크) 탭을 클릭하고 디스크를 선택합니다.

4.

Remove(제거)를 클릭한 다음 **OK**(확인)를 클릭합니다.

5.

Virtual Machines(가상 시스템)로 돌아가서 디스크가 연결될 새 가상 시스템의 이름을 클릭합니다.

6.

Disks(디스크) 탭을 클릭한 다음 **Attach**(연결)를 클릭합니다.

7.

Attach Virtual Disks(가상 디스크 연결) 창에서 디스크를 선택하고 **Interface** (인터페이스) 드롭다운에서 적절한 인터페이스를 선택합니다.

8.

OK(확인)를 클릭합니다.

2.8.6.6. 가상 디스크 복사

스토리지 도메인 간에 가상 디스크를 복사할 수 있습니다. 복사된 디스크를 가상 시스템에 연결할 수 있습니다.

절차

1. **Storage** → **Disks** (스토리지 디스크)를 클릭하고 가상 디스크를 선택합니다.
2. **Copy** 를 클릭합니다.
3. 선택적으로 **Alias**(별칭) 필드에 새 이름을 입력합니다.
4. **Target**(대상) 목록에서 가상 디스크를 복사할 스토리지 도메인을 선택합니다.
5. **Disk Profile** (디스크 프로파일) 목록에서 해당하는 경우 디스크의 프로파일을 선택합니다.
6. **OK**(확인)를 클릭합니다.

복사하는 동안 가상 디스크의 상태가 **Locked**(잠김) 입니다.

2.8.6.7. 디스크 성능 향상

관리 포털의 가상 시스템의 **Resource Allocation**(리소스 할당) 탭에서 기본 **I/O 스레드 활성화** 설정이 확인(활성화)되고 스레드 수는 **1** 입니다.

가상 시스템에 **VirtIO** 컨트롤러가 있는 여러 디스크가 있으며, 해당 워크로드가 이러한 컨트롤러를 상당 부분 활용하고 있다고 가정합니다. 이 경우 **I/O 스레드** 수를 늘려 성능을 향상시킬 수 있습니다.

그러나 **I/O 스레드** 수를 늘리면 가상 시스템의 스레드 풀이 줄어들습니다. 워크로드가 **VirtIO** 컨트롤러와 해당 컨트롤러에 할당한 스레드를 사용하지 않는 경우 **I/O 스레드** 수가 증가하면 전반적인 성능이 저하될 수 있습니다.

스레드 수를 최적화하려면 스레드 수를 조정하기 전후에 워크로드를 실행하는 가상 머신의 성능을 벤치마킹합니다.

절차

1. **Compute**(컴퓨팅) → **Virtual Machines**(가상 시스템)에서 가상 시스템의 전원을 끕니다.

2. 가상 시스템의 이름을 클릭합니다.
3. 세부 정보 창에서 **Vm Devices** 탭을 클릭합니다.
4. **Type(유형)**이 **virtio** 또는 **virtio -scsi**인 컨트롤러 수를 계산합니다.
5. **Edit(편집)**를 클릭합니다.
6. **Edit Virtual Machine(가상 시스템 편집)** 창에서 **Resource Allocation(리소스 할당)** 탭을 클릭합니다.
7. **I/O 스레드 활성화**가 선택되었는지 확인합니다(활성화됨).
8. 사용 가능한 **I/O 스레드** 오른쪽으로 스레드 수를 늘리지만, 유형이 **virtio** 또는 **virtio -scsi**인 컨트롤러 수를 초과하지 않습니다.
9. **OK(확인)**를 클릭합니다.
10. 세부 정보 창에서 **Disks (디스크)** 탭을 클릭합니다.
11. 각 디스크에 대해 추가 작업 ()을 사용하여 디스크 비활성화 및 활성화를 해제합니다. 이 작업은 디스크를 컨트롤러에 다시 매핑합니다.
12. **Run(실행)**을 클릭하여 가상 시스템을 시작합니다.

검증 단계

- **I/O 스레드**가 있는 컨트롤러를 보려면 세부 정보 창에서 **Vm Devices**를 클릭하고 **Spec Params** 열에서 **for ioThreadid=**를 찾습니다.

- 컨트롤러에 디스크 매핑을 보려면 호스트 시스템에 로그인하고 다음 명령을 입력합니다.

```
# virsh -r dumpxml virtual_machine_name
```

추가 리소스

- [고성능 가상 머신, 템플릿 및 풀 구성](#)
- [가상 머신 리소스 할당 설정 설명](#)

2.8.6.8. 데이터 스토리지 도메인에 이미지 업로드

관리 포털 또는 **REST API**에서 데이터 스토리지 도메인에 가상 디스크 이미지 및 **ISO** 이미지를 업로드할 수 있습니다. 자세한 내용은 데이터 스토리지 [도메인에 이미지 업로드](#)를 참조하십시오.

2.8.6.9. 가져온 스토리지 도메인에서 디스크 이미지 가져오기

가져온 스토리지 도메인에서 유동 가상 디스크를 가져옵니다.



참고

QEMU 호환 디스크만 Manager로 가져올 수 있습니다.

절차

1. **Storage**(스토리지 → **Domains** (도메인))를 클릭합니다.
2. 가져온 스토리지 도메인의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Disk Import**(디스크 가져오기) 탭을 클릭합니다.
4. 하나 이상의 디스크를 선택하고 **Import**(가져오기)를 클릭합니다.

5. 각 디스크에 적절한 디스크 프로필을 선택합니다.
6. **OK(확인)**를 클릭합니다.

2.8.6.10. 가져온 스토리지 도메인에서 등록되지 않은 디스크 이미지 가져오기

스토리지 도메인에서 유동 가상 디스크를 가져옵니다. **Red Hat Virtualization** 환경 외부에서 생성된 유동 디스크는 **Manager**에 등록되지 않습니다. 스토리지 도메인을 스캔하여 가져올 등록되지 않은 유동 디스크를 식별합니다.



참고

QEMU 호환 디스크만 **Manager**로 가져올 수 있습니다.

절차

1. **Storage**(스토리지 → **Domains** (도메인))를 클릭합니다.
2. 스토리지 도메인의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. 관리자가 등록되지 않은 디스크를 식별할 수 있도록 **More Actions**(추가 작업 ())를 클릭한 다음 **Scan Disks** (디스크 스캔)를 클릭합니다.
4. **Disk Import**(디스크 가져오기) 탭을 클릭합니다.
5. 하나 이상의 디스크 이미지를 선택하고 **Import**(가져오기)를 클릭합니다.
6. 각 디스크에 적절한 디스크 프로필을 선택합니다.
7. **OK(확인)**를 클릭합니다.

2.8.6.11. OpenStack 이미지 서비스에서 가상 디스크 가져오기

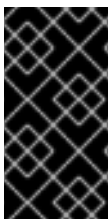
OpenStack Image Service에서 관리하는 가상 디스크는 **OpenStack Image Service**가 외부 공급업체로 **Manager**에 추가된 경우 **Red Hat Virtualization Manager**로 가져올 수 있습니다.

1. **Storage**(스토리지 → **Domains** (도메인) 를 클릭합니다.
2. **OpenStack Image Service** 도메인의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Images**(이미지) 탭을 클릭하고 이미지를 선택합니다.
4. **Import**(가져오기)를 클릭합니다.
5. 이미지를 가져올 **Data Center** (데이터 센터)를 선택합니다.
6. **Domain Name** (도메인 이름) 드롭다운 목록에서 이미지를 저장할 스토리지 도메인을 선택합니다.
7. 선택적으로 **Quota** (할당량) 드롭다운 목록에서 이미지에 적용할 할당량을 선택합니다.
8. **OK**(확인)를 클릭합니다.

이제 디스크를 가상 머신에 연결할 수 있습니다.

2.8.6.12. OpenStack 이미지 서비스로 가상 디스크 내보내기

가상 디스크를 외부 공급업체로 **Manager**에 추가된 **OpenStack** 이미지 서비스로 내보낼 수 있습니다.



중요

가상 디스크는 여러 볼륨이 없고 썸 프로비저닝되지 않은 경우에만 내보낼 수 있으며 스냅샷이 없는 경우에만 내보낼 수 있습니다.

1. **Storage** → **Disks** (스토리지 디스크)를 클릭하고 내보낼 디스크를 선택합니다.
2. **More Actions**(추가 작업) ()를 클릭한 다음 **Export**(내보내기)를 클릭합니다.
3. **Domain Name** (도메인 이름) 드롭다운 목록에서 디스크를 내보낼 **OpenStack** 이미지 서비스를 선택합니다.
4. **Quota**(할당량) 드롭다운 목록에서 할당량을 적용할 경우 디스크 할당량을 선택합니다.
5. **OK**(확인)를 클릭합니다.

2.8.6.13. 가상 디스크 공간 회수

썬 프로비저닝을 사용하는 가상 디스크는 파일을 삭제해도 자동으로 축소되지 않습니다. 예를 들어 실제 디스크 크기가 **100GB**이고 **50GB**의 파일을 삭제하면 할당된 디스크 크기가 **100GB**로 유지되고 나머지 **50GB**가 호스트에 반환되지 않으므로 다른 가상 시스템에서 사용할 수 없습니다. 이 사용하지 않는 디스크 공간은 가상 머신의 디스크에서 스파스 작업을 수행하여 호스트에서 회수할 수 있습니다. 디스크 이미지에서 호스트로 사용 가능한 공간을 전송합니다. 여러 가상 디스크를 동시에 스파스할 수 있습니다.

가상 시스템을 복제하거나, 가상 시스템을 기반으로 템플릿을 생성하거나, 스토리지 도메인의 디스크 공간을 정리하기 전에 이 작업을 수행합니다.

제한

- **NFS** 스토리지 도메인에서는 **NFS** 버전 **4.2** 이상을 사용해야 합니다.
- 직접 **LUN**을 사용하는 디스크를 스파스할 수 없습니다.
- 사전 할당된 할당 정책을 사용하는 디스크를 스파스할 수 없습니다. 템플릿에서 가상 시스템을 생성하는 경우 **Storage Allocation** (스토리지 할당) 필드에서 **Thin** (썬)을 선택하거나 **Clone** (복제)을 선택하는 경우 템플릿이 썬 프로비저닝이 있는 가상 시스템을 기반으로 해야 합니다.

- 활성 스냅샷만 스파스할 수 있습니다.

디스크 범위 지정

1. **Compute**(컴퓨팅) → **Virtual Machines** (가상 시스템)를 클릭하고 필요한 가상 시스템을 종료합니다.
2. 가상 시스템의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. 디스크 탭을 클릭합니다. 디스크 상태가 **OK** 인지 확인합니다.
4. 추가 작업 ()을 클릭한 다음 **Sparsify**(스포함)를 클릭합니다.
5. **OK**(확인)를 클릭합니다.

스파스화 작업 중 **Events**(이벤트) 탭에 **Started to sparsify** 이벤트가 표시되고 디스크 상태가 **Locked**(잠김)로 표시됩니다. 작업이 완료되면 **Events**(이벤트) 탭에 **Sparsified successfully** 이벤트가 표시되고 디스크 상태가 **OK**로 표시됩니다. 사용되지 않은 디스크 공간이 호스트에 반환되었으며 다른 가상 시스템에서 사용할 수 있습니다.

2.9. 외부 공급자

2.9.1. Red Hat Virtualization에서 외부 공급자 소개

Red Hat Virtualization Manager 자체에서 관리하는 리소스 외에도 **Red Hat Virtualization**은 외부 소스에서 관리하는 리소스를 활용할 수도 있습니다. 외부 프로바이더라고 하는 이러한 리소스의 프로바이더는 가상화 호스트, 가상 시스템 이미지 및 네트워크와 같은 리소스를 제공할 수 있습니다.

Red Hat Virtualization은 현재 다음과 같은 외부 공급자를 지원합니다.

호스트 프로비저닝용 Red Hat Satellite

Satellite는 물리적 호스트와 가상 호스트의 라이프사이클의 모든 측면을 관리하는 툴입니다.

Red Hat Virtualization에서는 Red Hat Virtualization Manager에서 Satellite에서 관리하는 호스트를 가상화 호스트로 추가하고 사용할 수 있습니다. Manager에 Satellite 인스턴스를 추가하고 나면 새 호스트를 추가할 때 해당 Satellite 인스턴스에서 사용 가능한 호스트를 검색하여 Satellite 인스턴스에서 관리하는 호스트를 추가할 수 있습니다. Red Hat Satellite 설치 및 Red Hat Satellite를 사용하여 호스트 관리에 대한 자세한 내용은 [Red Hat Satellite 빠른 시작 가이드](#) 및 [Red Hat Satellite 관리 호스트를 참조하십시오](#).

KubeVirt/OpenShift Virtualization

OpenShift Virtualization(이전의 컨테이너 네이티브 가상화 또는 "CNV")을 통해 VM(가상 머신)을 컨테이너 워크플로우로 가져올 수 있으므로 컨테이너 및 서버리스와 나란히 가상 머신을 개발, 관리 및 배포할 수 있습니다. RHV Manager에서 이 공급자를 추가하는 것은 OpenShift Virtualization을 사용하는 데 필요한 요구 사항 중 하나입니다. 자세한 내용은 [KubeVirt/OpenShift Virtualization을 외부 공급자로 추가](#)를 참조하십시오.

이미지 관리를 위한 OpenStack Image Service(Glance)

OpenStack Image Service는 가상 시스템 이미지 카탈로그를 제공합니다. Red Hat Virtualization에서는 이러한 이미지를 Red Hat Virtualization Manager로 가져와 유동 디스크로 사용하거나 가상 머신에 연결하고 템플릿으로 변환할 수 있습니다. OpenStack Image Service를 Manager에 추가하면 데이터 센터에 연결되지 않은 스토리지 도메인으로 표시됩니다. Red Hat Virtualization 환경의 가상 디스크도 가상 디스크로 OpenStack 이미지 서비스로 내보낼 수 있습니다.



참고

OpenStack Glance에 대한 지원은 더 이상 사용되지 않습니다. 이 기능은 이후 릴리스에서 제거됩니다.

가상 머신 프로비저닝용 VMware

VMware에서 생성된 가상 시스템은 V2V(virt-v2v)를 사용하여 변환하고 Red Hat Virtualization 환경으로 가져올 수 있습니다. 관리자에 VMware 공급업체를 추가한 후 제공하는 가상 시스템을 가져올 수 있습니다. V2V 변환은 가져오기 작업의 일부로 지정된 프록시 호스트에서 수행됩니다.

가상 머신 프로비저닝 용 RHEL 5 Xen

RHEL 5 Xen에서 생성된 가상 머신은 V2V(virt-v2v)를 사용하여 변환하고 Red Hat Virtualization 환경으로 가져올 수 있습니다. RHEL 5 Xen 호스트를 Manager에 추가한 후 제공하는 가상 머신을 가져올 수 있습니다. V2V 변환은 가져오기 작업의 일부로 지정된 프록시 호스트에서 수행됩니다.

가상 머신 프로비저닝을 위한 KVM

KVM에서 생성된 가상 머신을 Red Hat Virtualization 환경으로 가져올 수 있습니다. KVM 호스트를 Manager에 추가한 후 제공하는 가상 머신을 가져올 수 있습니다.

네트워크 프로비저닝을 위한 OVN(Open Virtual Network)

OVN(Open Virtual Network)은 소프트웨어 정의 네트워크를 제공하는 **OVS(Open vSwitch)** 확장입니다. 관리자에 **OVN**을 추가한 후 기존 **OVN** 네트워크를 가져오고 관리자에서 새 **OVN** 네트워크를 생성할 수 있습니다. **engine-setup** 을 사용하여 **Manager**에 **OVN**을 자동으로 설치할 수도 있습니다.

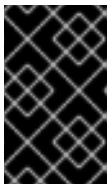
2.9.2. 외부 공급자 추가

2.9.2.1. 호스트 프로비저닝용 Red Hat Satellite 인스턴스 추가

호스트 프로비저닝을 위한 **Satellite** 인스턴스를 **Red Hat Virtualization Manager**에 추가합니다. **Red Hat Satellite 6.1**에서는 **Red Hat Virtualization 4.2**가 지원됩니다.

절차

1. **Administration(관리) Providers(공급업체)** 를 클릭합니다.
2. **추가**를 클릭합니다.
3. **Name (이름)** 및 **Description (설명)**을 입력합니다.
4. **Type(유형)** 드롭다운 목록에서 **Foreman/Satellite** 를 선택합니다.
5. **Satellite** 인스턴스가 **Provider URL** 텍스트 필드에 설치된 시스템의 **URL** 또는 정규화된 도메인 이름을 입력합니다. 포트 번호를 지정할 필요가 없습니다.



중요

IP 주소는 **Satellite** 인스턴스를 추가하는 데 사용할 수 없습니다.

6. **Requires Authentication (인증 필요)** 확인란을 선택합니다.
7. **Satellite** 인스턴스에 **Username (사용자 이름)** 및 **Password (암호)**를 입력합니다. **Satellite** 프로비저닝 포털에 로그인하는 데 사용하는 것과 동일한 사용자 이름 및 암호를 사용해야 합니다.

8.

인증 정보를 테스트합니다.

a.

Test (테스트)를 클릭하여 제공된 자격 증명을 사용하여 **Satellite** 인스턴스를 사용하여 인증할 수 있는지 테스트합니다.

b.

Satellite 인스턴스에서 **SSL**을 사용하는 경우 **Import provider certificates** (프로바이더 인증서 가져오기) 창이 열립니다. **OK**(확인)를 클릭하여 관리자가 인스턴스와 통신할 수 있도록 **Satellite** 인스턴스에서 제공하는 인증서를 가져옵니다.

9.

OK(확인)를 클릭합니다.

2.9.2.2. 이미지 관리를 위한 OpenStack 이미지(Glance) 인스턴스 추가



참고

OpenStack Glance에 대한 지원은 더 이상 사용되지 않습니다. 이 기능은 이후 릴리스에서 제거됩니다.

이미지 관리를 위해 **OpenStack** 이미지(**Glance**) 인스턴스를 **Red Hat Virtualization Manager**에 추가합니다.

절차

1.

Administration(관리) **Providers**(공급업체) 를 클릭합니다.

2.

Add(추가)를 클릭하고 **General Settings**(일반 설정) 탭에서 세부 정보를 입력합니다. 이러한 필드에 대한 자세한 내용은 [공급자의 일반 설정 추가를 참조하십시오](#).

3.

Name (이름) 및 **Description** (설명)을 입력합니다.

4.

Type(유형) 드롭다운 목록에서 **OpenStack Image** (**OpenStack** 이미지)를 선택합니다.

5.

OpenStack Image 인스턴스가 **Provider URL** 텍스트 필드에 설치된 시스템의 **URL** 또는 정규화된 도메인 이름을 입력합니다.

6.

선택적으로 **Requires Authentication** (인증 필요) 확인란을 선택하고 **Keystone**에 등록된 **OpenStack Image** 인스턴스 사용자에게 대해 **Username** (사용자 이름) 및 **Password**(암호)를 입력합니다. 프로토콜 (**HTTP**), 호스트 이름 및 **API** 포트를 정의하여 **Keystone** 서버의 인증 **URL**도 정의해야 합니다.

OpenStack Image 인스턴스의 테넌트 를 입력합니다.

7.

인증 정보를 테스트합니다.

a.

Test (테스트)를 클릭하여 제공된 자격 증명을 사용하여 **OpenStack** 이미지 인스턴스로 성공적으로 인증할 수 있는지 테스트합니다.

b.

OpenStack Image 인스턴스에서 **SSL**을 사용하는 경우 **Import provider certificates** (프로바이더 인증서 가져오기) 창이 열립니다. **OK**(확인)를 클릭하여 관리자가 인스턴스와 통신할 수 있도록 **OpenStack** 이미지 인스턴스에서 제공하는 인증서를 가져옵니다.

8.

OK(확인)를 클릭합니다.

2.9.2.3. KubeVirt/Openshift Virtualization을 외부 공급자로 추가

OpenShift Container Platform의 컨테이너에서 가상 머신을 실행하려면 **Red Hat Virtualization**에서 **OpenShift**를 외부 공급자로 추가합니다.



참고

이 기능을 **OpenShift Virtualization** 이라고 합니다.

사전 요구 사항

•

OpenShift Container Platform에서 클러스터는 **OpenShift Virtualization**용으로 구성됩니다.

절차

1. **RHV 관리 포털**에서 관리 공급업체로 이동하여 **New (→ 생성)**를 클릭합니다.
2. **Add Provider(프로바이더 추가)** 에서 **Type (유형)**을 **KubeVirt/Openshift Virtualization** 으로 설정합니다.
3. 필요한 공급자 **URL** 및 토큰을 입력합니다.
4. 선택 사항: 인증 기관,**Prometheus URL** 및 **Prometheus** 인증 기관과 같은 고급 매개변수 값을 입력합니다.
5. **Test (테스트)**를 클릭하여 새 공급업체에 대한 연결을 확인합니다.
6. **OK(확인)**를 클릭하여 이 새 공급업체 추가를 완료합니다.

검증 단계

1. **RHV 관리 포털**에서 **Compute(컴퓨팅) Clusters(클러스터)** 를 클릭합니다.
2. 방금 생성한 새 클러스터의 이름을 클릭합니다. 예를 들어 이 클러스터 이름은 공급자의 이름을 기반으로 합니다. 이 작업은 클러스터 세부 정보 보기를 엽니다.
3. **Hosts** 탭을 클릭하여 **OpenShift Container Platform** 작업자 노드의 상태가 **up** 인지 확인합니다.



참고

컨트롤 플레인 노드의 상태는 가상 머신을 호스팅할 수 없기 때문에 실행 중인 경우에도 다운 됩니다.

4. **Compute Virtual Machines(컴퓨팅 가상 시스템)**를 사용하여 새 클러스터에 가상 시스템을 배포합니다.
5. **OpenShift Container Platform** 웹 콘솔에서 관리자 관점에서 워크로드 가상 머신을 사용하

여 배포한 가상 머신을 확인합니다.

추가 리소스

- [OpenShift Virtualization 정보](#)
- [공급자 일반 설정 추가](#)

2.9.2.4. 가상 머신 공급자로 VMware 인스턴스 추가

VMware vCenter 인스턴스를 추가하여 VMware에서 Red Hat Virtualization Manager로 가상 머신을 가져옵니다.

Red Hat Virtualization은 V2V를 사용하여 VMware 가상 머신을 가져오기 전에 올바른 형식으로 변환합니다. virt-v2v 패키지는 하나 이상의 호스트에 설치되어 있어야 합니다. virt-v2v 패키지는 RHVH(Red Hat Virtualization Hosts)에서 기본적으로 사용할 수 있으며 Red Hat Virtualization 환경에 추가될 때 Red Hat Enterprise Linux 호스트에 VDSM에 종속된 상태로 설치됩니다. Red Hat Enterprise Linux 호스트는 Red Hat Enterprise Linux 7.2 이상이어야 합니다.



참고

ppc64le 아키텍처에서는 virt-v2v 패키지를 사용할 수 없습니다. 이러한 호스트는 프록시 호스트로 사용할 수 없습니다.

절차

1. **Administration(관리) Providers(공급업체)** 를 클릭합니다.
2. **추가**를 클릭합니다.
3. **Name (이름)** 및 **Description (설명)**을 입력합니다.
4. **Type(유형)** 드롭다운 목록에서 **VMware** 를 선택합니다.
5. **VMware** 가상 시스템을 가져올 **Data Center (데이터 센터)**를 선택하거나 개별 가져오기 작

업 중에 대상 데이터 센터를 지정하려면 **Any Data Center** (모든 데이터 센터)를 선택합니다.

6. **vCenter** 필드에 **VMware vCenter** 인스턴스의 **IP** 주소 또는 정규화된 도메인 이름을 입력합니다.
7. **ESXi** 필드에 가상 머신을 가져올 호스트의 **IP** 주소 또는 정규화된 도메인 이름을 입력합니다.
8. 지정된 **ESXi** 호스트가 **Data Center**(데이터 센터) 필드에 있는 데이터 센터의 이름을 입력합니다.
9. **ESXi** 호스트와 **Manager** 간에 **SSL** 인증서를 교환한 경우, **ESXi** 호스트의 인증서를 확인하도록 **Verify** 서버의 **SSL** 인증서 확인란을 선택한 상태로 둡니다. 그렇지 않은 경우 확인란을 지웁니다.
10. 가상 시스템 가져오기 작업 중 **virt-v2v** 가 설치된 상태에서 선택한 데이터 센터에서 호스트를 선택하여 프록시 호스트로 작동합니다. 또한 이 호스트는 **VMware vCenter** 외부 공급자의 네트워크에 연결할 수 있어야 합니다. 위의 모든 데이터 센터를 선택한 경우 여기에서 호스트를 선택할 수 없지만, 대신 개별 가져오기 작업 중에 호스트를 지정할 수 있습니다.
11. **VMware vCenter** 인스턴스에 **Username** (사용자 이름) 및 **Password** (암호)를 입력합니다. 사용자는 가상 시스템이 상주하는 **VMware** 데이터 센터 및 **ESXi** 호스트에 액세스할 수 있어야 합니다.
12. 인증 정보를 테스트합니다.
 - a. **Test** (테스트)를 클릭하여 제공된 자격 증명을 사용하여 **VMware vCenter** 인스턴스로 인증할 수 있는지 테스트합니다.
 - b. **VMware vCenter** 인스턴스에서 **SSL**을 사용하는 경우 **Import provider certificates** (프로바이더 인증서 가져오기) 창이 열립니다. **OK**(확인)를 클릭하여 관리자가 인스턴스와 통신할 수 있도록 **VMware vCenter** 인스턴스에서 제공하는 인증서를 가져옵니다.
13. **OK**(확인)를 클릭합니다.

VMware 외부 공급자에서 가상 머신을 가져오려면 [가상 머신 관리 가이드의 VMware 공급자에서 가상 머신 가져오기](#)를 참조하십시오.

2.9.2.5. 가상 머신 공급자로 RHEL 5 Xen Host 추가

Xen에서 Red Hat Virtualization으로 가상 시스템을 가져오기 위해 RHEL 5 Xen 호스트를 추가합니다.

Red Hat Virtualization은 V2V를 사용하여 RHEL 5 Xen 가상 머신을 가져오기 전에 올바른 형식으로 변환합니다. virt-v2v 패키지는 하나 이상의 호스트에 설치되어 있어야 합니다. virt-v2v 패키지는 RHVH(Red Hat Virtualization Hosts)에서 기본적으로 사용할 수 있으며 Red Hat Virtualization 환경에 추가될 때 Red Hat Enterprise Linux 호스트에 VDSM에 종속된 상태로 설치됩니다. Red Hat Enterprise Linux 호스트는 Red Hat Enterprise Linux 7.2 이상이어야 합니다.



참고

ppc64le 아키텍처에서는 virt-v2v 패키지를 사용할 수 없습니다. 이러한 호스트는 프록시 호스트로 사용할 수 없습니다.

절차

1.

프록시 호스트와 RHEL 5 Xen 호스트 간의 공개 키 인증을 활성화합니다.

a.

프록시 호스트에 로그인하고 vdsim 사용자에게 대한 SSH 키를 생성합니다.

```
# sudo -u vdsim ssh-keygen
```

b.

vdsim 사용자의 공개 키를 RHEL 5 Xen 호스트에 복사합니다. RHEL 5 Xen 호스트의 호스트 키를 포함하도록 프록시 호스트의 known_hosts 파일도 업데이트됩니다.

```
# sudo -u vdsim ssh-copy-id root@xenhost.example.com
```

c.

RHEL 5 Xen 호스트에 로그인하여 로그인이 올바르게 작동하는지 확인합니다.

```
# sudo -u vdsim ssh root@xenhost.example.com
```

2.

Administration(관리) Providers(공급업체)를 클릭합니다.

3. 추가를 클릭합니다.
4. **Name (이름)** 및 **Description (설명)**을 입력합니다.
5. **Type(유형)** 드롭다운 목록에서 **XEN** 을 선택합니다.
6. **Xen** 가상 머신을 가져올 데이터 센터를 선택하거나 **Any Data Center** (모든 데이터 센터)를 선택하여 개별 가져오기 작업 중에 대상 데이터 센터를 지정합니다.
7. **URI** 필드에 **RHEL 5 Xen** 호스트의 **URI** 를 입력합니다.
8. 가상 시스템 가져오기 작업 중 **virt-v2v** 가 설치된 상태에서 선택한 데이터 센터에서 호스트를 선택하여 프록시 호스트로 작동합니다. 또한 이 호스트는 **RHEL 5 Xen** 외부 공급자의 네트워크에 연결할 수 있어야 합니다. 위의 모든 데이터 센터를 선택한 경우 여기에서 호스트를 선택할 수 없지만, 대신 개별 가져오기 작업 중에 호스트를 지정할 수 있습니다.
9. **Test (테스트)**를 클릭하여 **RHEL 5 Xen** 호스트를 사용하여 인증할 수 있는지 테스트합니다.
10. **OK(확인)**를 클릭합니다.

RHEL 5 Xen 외부 공급자에서 가상 머신을 가져오려면 [가상 머신 관리 가이드의 RHEL 5 Xen 호스트에서 가상 머신 가져오기를 참조하십시오](#).

2.9.2.6. KVM 호스트를 가상 머신 공급자로 추가

KVM 호스트를 추가하여 **KVM**에서 **Red Hat Virtualization Manager**로 가상 머신을 가져옵니다.

절차

1. 프록시 호스트와 **KVM** 호스트 간의 공개 키 인증을 활성화합니다.
 - a. 프록시 호스트에 로그인하고 **vdsm** 사용자에게 대한 **SSH** 키를 생성합니다.

```
# sudo -u vdsmd ssh-keygen
```

b.

vdsmd 사용자의 공개 키를 **KVM** 호스트에 복사합니다. **KVM** 호스트의 호스트 키를 포함하도록 프록시 호스트의 **known_hosts** 파일도 업데이트됩니다.

```
# sudo -u vdsmd ssh-copy-id root@kvmhost.example.com
```

c.

KVM 호스트에 로그인하여 로그인이 올바르게 작동하는지 확인합니다.

```
# sudo -u vdsmd ssh root@kvmhost.example.com
```

2.

Administration(관리) Providers(공급업체) 를 클릭합니다.

3.

추가를 클릭합니다.

4.

Name (이름) 및 **Description (설명)**을 입력합니다.

5.

유형 드롭다운 목록에서 **KVM** 을 선택합니다.

6.

KVM 가상 머신을 가져올 **Data Center (데이터 센터)**를 선택하거나 **Any Data Center (모든 데이터 센터)**를 선택하여 개별 가져오기 작업 중에 대상 데이터 센터를 지정합니다.

7.

URI 필드에 **KVM** 호스트의 **URI** 를 입력합니다.

```
qemu+ssh://root@host.example.com/system
```

8.

선택한 데이터 센터에서 호스트를 선택하여 가상 시스템 가져오기 작업 중에 프록시 호스트 역할을 합니다. 또한 이 호스트는 **KVM** 외부 프로바이더의 네트워크에 연결할 수 있어야 합니다. 위의 **Data Center(데이터 센터)** 필드에서 **Any Data Center (모든 데이터 센터)**를 선택한 경우 여기에서 호스트를 선택할 수 없습니다. 이 필드는 데이터 센터의 **Any Host(모든 호스트)**를 표시하며 출력됩니다. 대신 개별 가져오기 작업 중에 호스트를 지정할 수 있습니다.

9.

선택적으로 **Requires Authentication (인증 필요)** 확인란을 선택하고 **KVM** 호스트에 **Username(사용자 이름)** 및 **Password(암호)** 를 입력합니다. 사용자는 가상 시스템이 상주하는 **KVM** 호스트에 대한 액세스 권한이 있어야 합니다.

10.

Test (테스트)를 클릭하여 제공된 자격 증명을 사용하여 **KVM** 호스트로 인증할 수 있는지 테스트합니다.

11.

OK(확인)를 클릭합니다.

KVM 외부 공급자에서 가상 머신을 가져오려면 [가상 머신 관리 가이드의 KVM 호스트에서 가상 머신 가져오기](#)를 참조하십시오.

2.9.2.7. OVN(Open Virtual Network)을 외부 네트워크 공급자로 추가

OVN(Open Virtual Network)을 사용하여 **VLAN**을 추가하거나 인프라를 변경하지 않고도 가상 머신 간 통신을 활성화하는 오버레이 가상 네트워크를 생성할 수 있습니다. **OVN**은 가상 **L2** 및 **L3** 오버레이에 대한 기본 지원을 제공하는 **OVS(Open vSwitch)**의 확장입니다.

OVN 네트워크를 기본 **Red Hat Virtualization** 네트워크에 연결할 수도 있습니다. [자세한 내용은 OVN Network를 물리적 네트워크에 연결](#)을 참조하십시오. 이 기능은 기술 프리뷰로만 사용할 수 있습니다.

ovirt-provider-ovn 은 **OpenStack Networking REST API**를 노출합니다. 이 **API**를 사용하여 네트워크, 서브넷, 포트 및 라우터를 만들 수 있습니다. 자세한 내용은 [OpenStack Networking API v2.0](#)을 참조하십시오.

자세한 내용은 [Open vSwitch 문서](#) 및 [Open vSwitch Manpages](#)를 참조하십시오.

2.9.2.7.1. 새 OVN 네트워크 공급자 설치

engine-setup 을 사용하여 **OVN**을 설치하면 다음 단계를 수행합니다.

- **Manager** 머신에서 **OVN** 중앙 서버를 설정합니다.
- **Red Hat Virtualization**에 **OVN**을 외부 네트워크 공급자로 추가합니다.
- **Default** 클러스터에서만 **Default Network Provider** 를 **ovirt-provider-ovn** 으로 설정합니다.

중요

- **OVN**을 설치하면 다른 클러스터가 아닌 **Default** 클러스터에만 기본 네트워크 공급자 설정이 변경됩니다.
- 기본 네트워크 프로바이더 설정을 변경해도 해당 클러스터의 호스트가 **Default Network Provider**를 사용하도록 업데이트되지 않습니다.
- 호스트 및 가상 머신이 **OVN**을 사용하려면 이 주제 끝에 있는 "다음 단계"에 설명된 추가 작업을 수행합니다.

절차

1.

선택 사항: **engine-setup**으로 사전 구성된 응답 파일을 사용하는 경우 다음 항목을 추가하여 **OVN**을 설치합니다.

```
OVESETUP_OVN/ovirtProviderOvn=bool:True
```

2.

Manager 시스템에서 **engine-setup**을 실행합니다.

3.

사전 구성된 응답 파일을 사용하지 않는 경우 **engine-setup**이 질문할 때 **Yes**로 응답합니다.

Configuring ovirt-provider-ovn also sets the Default cluster's default network provider to ovirt-provider-ovn.

Non-Default clusters may be configured with an OVN after installation.

Configure ovirt-provider-ovn (Yes, No) [Yes]:

4.

다음 질문에 답변하십시오.

Use default credentials (admin@internal) for ovirt-provider-ovn (Yes, No) [Yes]?:

예, **engine-setup**은 설정 프로세스 초기에 지정한 기본 엔진 사용자와 암호를 사용합니다. 이 옵션은 새 설치 중에만 사용할 수 있습니다.

oVirt OVN provider user[admin]:

oVirt OVN provider password[empty]:

기본값을 사용하거나 **oVirt OVN provider** 사용자 및 암호를 지정할 수 있습니다.



참고

나중에 인증 방법을 변경하려면 `/etc/ovirt-provider-ovn/conf.d/10_engine_setup.conf` 파일을 편집하거나 새 `/etc/ovirt-provider-ovn/conf.d/20_engine_setup.conf` 파일을 만들 수 있습니다. **ovirt-provider-ovn** 서비스를 다시 시작하여 변경 사항을 적용합니다. **OVN 인증에 대한 자세한 내용은 [oVirt external network provider for OVN](#)에서 참조하십시오.**

다음 단계

새로 설치한 **OVN** 네트워크를 사용하는 가상 머신을 생성하려면 먼저 다음 추가 단계를 완료합니다.

1.

Default 클러스터에 네트워크를 추가합니다.

a.

이렇게 하는 동안 **Create on external provider** (외부 공급업체에 생성) 확인란을 선택합니다. 이렇게 하면 **ovirt-provider-ovn** 을 기반으로 네트워크가 생성됩니다.

b.

선택 사항: **OVN** 네트워크를 물리적 네트워크에 연결하려면 **물리적 네트워크에 연결 확인란을 선택**하고 사용할 **Red Hat Virtualization** 네트워크를 지정합니다.

c.

선택 사항: 네트워크가 보안 그룹을 사용해야 하는지 여부를 확인하고 **Security Groups** (보안 그룹) 드롭다운에서 하나를 선택합니다. 사용 가능한 옵션에 대한 자세한 내용은 **Logical Network General Settings**에서 참조하십시오.

2.

클러스터 의 새 기본 네트워크 공급자인 **ovirt-provider-ovn** 을 사용하도록 호스트를 기본 클러스터에 추가하거나 다시 설치합니다.

3.

선택 사항: 기본이 아닌 클러스터를 편집하고 기본 네트워크 프로바이더 를 **ovirt-provider-ovn** 으로 설정합니다.

a.

선택 사항: 클러스터의 새 기본 네트워크 공급자 **ovirt-provider-ovn**을 사용하도록 기본이 아닌 각 클러스터에 호스트를 다시 설치합니다.

추가 리소스

•

기본이 아닌 기존 네트워크를 사용하도록 호스트를 구성하려면 [OVN 터널 네트워크의 호스트 구성](#)을 참조하십시오.

2.9.2.7.2. 단일 호스트에서 OVN 터널 네트워크 업데이트

vdsms-tool 을 사용하여 단일 호스트에서 OVN 터널 네트워크를 업데이트할 수 있습니다.

```
# vdsms-tool ovn-config OVN_Central_IP Tunneling_IP_or_Network_Name Host_FQDN
```



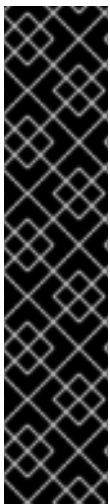
참고

Host_FQDN은 이 호스트의 엔진에 지정된 **FQDN**과 일치해야 합니다.

예 2.4. **vdsms-tool**로 호스트 업데이트

```
# vdsms-tool ovn-config 192.168.0.1 MyNetwork MyFQDN
```

2.9.2.7.3. 물리적 네트워크에 OVN 네트워크 연결



중요

이 기능은 **Red Hat Virtualization**에서 기술 프리뷰로만 제공되는 **Open vSwitch** 지원을 사용합니다. 기술 프리뷰 기능은 **Red Hat** 프로덕션 서비스 수준 계약(SLA)에서 지원되지 않으며 기능적으로 완전하지 않을 수 있으며 프로덕션에는 사용하지 않는 것이 좋습니다. 이러한 기능을 사용하면 향후 제품 기능을 조기에 이용할 수 있어 개발 과정에서 고객이 기능을 테스트하고 피드백을 제공할 수 있습니다.

Red Hat 기술 프리뷰 기능 지원 범위에 대한 자세한 내용은 [기술 프리뷰 기능 지원 범위를 참조하십시오](#).

기본 **Red Hat Virtualization** 네트워크를 오버레이하는 외부 프로바이더 네트워크를 생성하여 각 가상 머신이 동일한 서브넷을 공유하도록 할 수 있습니다.



중요

OVN 네트워크의 서브넷을 생성하면 해당 네트워크를 사용하는 가상 머신에서 IP 주소를 수신합니다. 물리적 네트워크에서 IP 주소를 할당하려면 OVN 네트워크의 서브넷을 생성하지 마십시오.

사전 요구 사항

- 클러스터에 OVS를 **Switch Type**으로 선택해야 합니다 . 이 클러스터에 추가된 호스트에는 **ovirtmgmt** 브리지와 같이 기존 **Red Hat Virtualization** 네트워크가 구성되어 있지 않아야 합니다.
- 호스트에서 물리적 네트워크를 사용할 수 있어야 합니다. 클러스터에 필요한 대로 실제 네트워크를 설정합니다(네트워크 관리 창 또는 **New Logical Network** 창의 **Cluster**(클러스터) 탭).

절차

1. **Compute(컴퓨팅) Clusters(클러스터)** 를 클릭합니다.
 2. 클러스터 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
 3. **Logical Networks(논리적 네트워크)** 탭을 클릭하고 **Add Network(네트워크 추가)**를 클릭합니다.
 4. 네트워크의 이름을 입력합니다.
 5. **Create on external provider(외부 프로바이더에 생성)** 확인란을 선택합니다. 기본적으로 **ovirt-provider-ovn** 이 선택됩니다.
 6. 기본적으로 아직 선택되지 않은 경우 물리적 네트워크에 연결 확인란을 선택합니다.
 7. 새 네트워크를 연결할 물리적 네트워크를 선택합니다.
- **Data Center Network (데이터 센터 네트워크)** 라디오 버튼을 클릭하고 드롭다운 목록

에서 물리적 네트워크를 선택합니다. 이 옵션을 사용하는 것이 좋습니다.

•

Custom(사용자 지정) 라디오 버튼을 클릭하고 물리적 네트워크의 이름을 입력합니다. 실제 네트워크에 **VLAN** 태그 지정이 활성화된 경우 **VLAN** 태그 지정 활성화 확인란을 선택하고 실제 네트워크의 **VLAN** 태그를 입력해야 합니다.



중요

실제 네트워크의 이름은 **15**자를 초과하거나 특수 문자를 포함해서는 안 됩니다.

8.

OK(확인)를 클릭합니다.

////Removing for BZ2006228

include::topics/Adding_an_External_Network_Provider.adoc[leveloffset=+2]

2.9.2.8. 설명된 공급자 일반 설정 추가

Add Provider (프로바이더 추가) 창의 **General(일반)** 탭에서는 외부 프로바이더의 핵심 세부 정보를 등록할 수 있습니다.

표 2.38. 공급자 추가: 일반 설정

설정	설명
이름	관리자의 공급업체를 나타내는 이름입니다.
설명	프로바이더에 대한 사용자가 읽을 수 있는 일반 텍스트 설명입니다.
유형	외부 프로바이더의 유형입니다. 이 설정을 변경하면 공급업체 구성에 사용 가능한 필드가 변경됩니다. 외부 네트워크 공급자 ● 네트워킹 플러그인: 호스트에서 NIC 작업을 처리하는 데 사용할 드라이버의 구현을 결정합니다. OVN 플러그인용 oVirt Network Provider가 클러스터의 기본 네트워크 공급자로 추가되면 클러스터에 추가된 호스트에 설치할 드라이버도 결정됩니다. ● 자동 동기화: 공급업체가 기존 네트워크와 자동으로 동기화되는지 여부를 지정할 수 있습니다.

설정	설명
	● 공급자 URL: 외부 네트워크 프로바이더가 호스팅되는 시스템의 URL 또는 정규화된 도메인 이름입니다. 외부 네트워크 프로바이더의 포트 번호를 URL 또는 정규화된 도메인 이름의 끝에 추가해야 합니다. 기본적으로 이 포트 번호는 9696입니다. ● 읽기 전용: 관리 포털에서 외부 네트워크 프로바이더를 수정할 수 있는지 여부를 지정할 수 있습니다. ● 인증 필요: 인증이 외부 네트워크 공급자에 액세스해야 하는지 여부를 지정할 수 있습니다. ● 사용자 이름: 외부 네트워크 프로바이더에 연결하는 사용자 이름입니다. Active Directory로 인증하는 경우 사용자 이름은 기본 사용자 이름 @ domain 대신 <code>username@domain@auth_profile</code> 형식이어야 합니다. ● 암호: 위의 사용자 이름을 인증해야 하는 암호입니다. ● 프로토콜: Keystone 서버와 통신하는 데 사용되는 프로토콜입니다. 기본값은 HTTPS입니다. ● hostname: Keystone 서버의 IP 주소 또는 호스트 이름. ● API 포트: Keystone 서버의 API 포트 번호입니다. ● API 버전: Keystone 서버의 버전. 값은 v2.0이고 필드가 비활성화되어 있습니다. ● 테넌트 이름: 선택 사항: 외부 네트워크 프로바이더가 멤버인 테넌트의 이름입니다. Foreman/Satellite ● 공급자 URL: Satellite 인스턴스를 호스팅하는 시스템의 URL 또는 정규화된 도메인 이름입니다. URL 또는 정규화된 도메인 이름의 끝에 포트 번호를 추가할 필요가 없습니다. ● 인증 필요: 공급자에 인증이 필요한지 여부를 지정할 수 있습니다. Foreman/Satellite가 선택되면 인증이 필요합니다. ● 사용자 이름: Satellite 인스턴스에 연결할 사용자 이름입니다. 이 사용자 이름은 Satellite 인스턴스에서 프로비저닝 포털에 로그인하는 데 사용되는 사용자 이름이어야 합니다. ● 암호: 위의 사용자 이름을 인증해야 하는 암호입니다. 이 암호는 Satellite 인스턴스에서 프로비저닝 포털에 로그인하는 데 사용되는 암호여야 합니다. KubeVirt/OpenShift Virtualization ● 공급자 URL: OpenShift Container Platform API의 URL 또는 정규화된 도메인 이름 및 포트 번호입니다. 기본적으로 이 포트 번호는

설정	설명
	6443입니다. ● 토큰 API에 대한 이 연결을 인증하기 위한 OAuth 액세스 토큰입니다. ● 인증 기관 https 요청을 만들 때 신뢰할 CA 인증서입니다. ● Prometheus URL OpenShift 클러스터의 prometheus 서비스의 URL입니다. 이 URL을 제공하지 않으면 소프트웨어는 이 URL을 자동으로 탐지합니다. ● prometheus의 X509 인증서 Prometheus 인증 기관. 이 CA를 지정하지 않으면 공급자는 KubeVirt CA를 대신 사용합니다. OpenStack Image ● 공급자 URL: OpenStack 이미지 서비스가 호스팅되는 시스템의 URL 또는 정규화된 도메인 이름입니다. URL 또는 정규화된 도메인 이름의 끝에 OpenStack 이미지 서비스의 포트 번호를 추가해야 합니다. 기본적으로 이 포트 번호는 9292입니다. ● 인증 필요: OpenStack 이미지 서비스에 액세스하는 데 인증이 필요한지 여부를 지정할 수 있습니다. ● 사용자 이름: Keystone 서버 연결에 사용되는 사용자 이름입니다. 이 사용자 이름은 OpenStack 이미지 서비스가 멤버인 Keystone 인스턴스에 등록된 OpenStack 이미지 서비스의 사용자 이름이어야 합니다. ● 암호: 위의 사용자 이름을 인증해야 하는 암호입니다. 이 암호는 OpenStack 이미지 서비스가 멤버인 Keystone 인스턴스에 등록된 OpenStack 이미지 서비스의 암호여야 합니다. ● 프로토콜: Keystone 서버와 통신하는 데 사용되는 프로토콜입니다. HTTP로 설정해야 합니다. ● hostname: Keystone 서버의 IP 주소 또는 호스트 이름. ● API 포트: Keystone 서버의 API 포트 번호입니다. ● API 버전: Keystone 서비스의 버전. 값은 v2.0이고 필드가 비활성화되어 있습니다. ● 테넌트 이름: OpenStack 이미지 서비스가 멤버인 OpenStack 테넌트의 이름입니다. OpenStack 볼륨 ● 데이터 센터: OpenStack 볼륨 스토리지 볼륨이 연결될 데이터 센터입니다. ● 공급자 URL: OpenStack Volume 인스턴스가 호스팅되는 시스템의 URL 또는 정규화된 도

설정	설명
	메인 이름입니다. URL 또는 정규화된 도메인 이름의 끝에 OpenStack 볼륨 인스턴스의 포트 번호를 추가해야 합니다. 기본적으로 이 포트 번호는 8776입니다. ● 인증 필요: OpenStack 볼륨 서비스에 액세스하는 데 인증이 필요한지 여부를 지정할 수 있습니다. ● 사용자 이름: Keystone 서버 연결에 사용되는 사용자 이름입니다. 이 사용자 이름은 OpenStack Volume 인스턴스가 멤버인 Keystone 인스턴스에 등록된 OpenStack 볼륨의 사용자 이름이어야 합니다. ● 암호: 위의 사용자 이름을 인증해야 하는 암호입니다. 이 암호는 OpenStack Volume 인스턴스가 멤버인 Keystone 인스턴스에 등록된 OpenStack 볼륨의 암호여야 합니다. ● 프로토콜: Keystone 서버와 통신하는 데 사용되는 프로토콜입니다. HTTP 로 설정해야 합니다. ● hostname: Keystone 서버의 IP 주소 또는 호스트 이름. ● API 포트: Keystone 서버의 API 포트 번호입니다. ● API 버전: Keystone 서버의 버전. 값은 v2.0 이고 필드가 비활성화되어 있습니다. ● 테넌트 이름: OpenStack Volume 인스턴스가 멤버인 OpenStack 테넌트의 이름입니다. VMware ● 데이터 센터: VMware 가상 시스템을 가져올 데이터 센터를 지정하거나 Any Data Center (모든 데이터 센터)를 선택하여 개별 가져오기 작업 중에 대상 데이터 센터를 지정합니다(Virtual Machines (가상 시스템) 탭에서 가져오기 기능을 사용). ● vCenter: VMware vCenter 인스턴스의 IP 주소 또는 정규화된 도메인 이름입니다. ● ESXi: 가상 시스템을 가져올 호스트의 IP 주소 또는 정규화된 도메인 이름입니다. ● 데이터 센터: 지정된 ESXi 호스트가 상주하는 데이터 센터의 이름입니다. ● 클러스터: 지정된 ESXi 호스트가 있는 클러스터의 이름입니다. ● 서버의 SSL 인증서를 확인합니다: 연결 시 ESXi 호스트의 인증서를 확인할지 여부를 지정합니다. ● 프록시 호스트: 가상 시스템 가져오기 작업 중에 호스트 역할을 수행하도록 virt-v2v 가 설치된 선택한 데이터 센터에서 호스트를 선택합니다. 또한 이 호스트는 VMware vCenter 외

설정	설명
	부 공급자의 네트워크에 연결할 수 있어야 합니다. Any Data Center (모든 데이터 센터)를 선택한 경우 여기에서 호스트를 선택할 수 없지만 개별 가져오기 작업(Virtual Machines (가상 시스템) 탭에서 가져오기 기능을 사용하여) 동안 호스트를 지정할 수 있습니다. ● 사용자 이름: VMware vCenter 인스턴스에 연결하는 사용자 이름입니다. 사용자는 가상 시스템이 상주하는 VMware 데이터 센터 및 ESXi 호스트에 액세스할 수 있어야 합니다. ● 암호: 위의 사용자 이름을 인증해야 하는 암호입니다. RHEL 5 Xen ● 데이터 센터: Xen 가상 머신을 가져올 데이터 센터를 지정하거나 개별 가져오기 작업 중에 대상 데이터 센터를 지정합니다 (가상 머신 탭에서 가져오기 기능을 사용). ● URI: RHEL 5 Xen 호스트의 URI입니다. ● 프록시 호스트: 가상 시스템 가져오기 작업 중에 호스트 역할을 수행하도록 virt-v2v가 설치된 선택한 데이터 센터에서 호스트를 선택합니다. 또한 이 호스트는 RHEL 5 Xen 외부 공급자의 네트워크에 연결할 수 있어야 합니다. Any Data Center (모든 데이터 센터를 선택한 경우 여기에서 호스트를 선택할 수 없지만, 개별 가져오기 작업(Virtual Machines (가상 시스템) 탭에서 가져오기 기능 사용) 동안 호스트를 지정할 수 있습니다. KVM ● 데이터 센터: KVM 가상 머신을 가져올 데이터 센터를 지정하거나 개별 가져오기 작업 중에 대상 데이터 센터를 대신 지정합니다(가상 머신 탭에서 가져오기 기능 사용). ● URI: KVM 호스트의 URI입니다. ● 프록시 호스트: 선택한 데이터 센터에서 호스트를 선택하여 가상 시스템 가져오기 작업 중에 호스트 역할을 합니다. 또한 이 호스트는 KVM 외부 프로바이더의 네트워크에 연결할 수 있어야 합니다. Any Data Center (모든 데이터 센터를 선택한 경우 여기에서 호스트를 선택할 수 없지만, 개별 가져오기 작업(Virtual Machines (가상 시스템) 탭에서 가져오기 기능 사용) 동안 호스트를 지정할 수 있습니다. ● 인증 필요: 인증이 KVM 호스트에 액세스해야 하는지 여부를 지정할 수 있습니다. ● 사용자 이름: KVM 호스트에 연결하는 사용자 이름입니다. ● 암호: 위의 사용자 이름을 인증해야 하는 암호입니다.

설정	설명
테스트	사용자가 지정된 자격 증명을 테스트할 수 있습니다. 이 버튼은 모든 공급업체 유형에서 사용할 수 있습니다.

2.9.3. 외부 공급자 편집

절차

1. **Administration(관리 → Providers (공급업체))** 를 클릭하고 편집할 외부 공급업체를 선택합니다.
2. **Edit(편집)**를 클릭합니다.
3. **프로바이더의 현재 값을 기본 값으로 변경합니다.**
4. **OK(확인)**를 클릭합니다.

2.9.4. 외부 공급자 제거

절차

1. **Administration(관리 → Providers (공급업체))** 를 클릭하고 제거할 외부 공급업체를 선택합니다.
2. **Remove(제거)**를 클릭합니다.
3. **OK(확인)**를 클릭합니다.

3장. 환경 관리

3.1. 셀프 호스트 엔진 관리

3.1.1. 셀프 호스트 엔진 유지 관리

3.1.1.1. 자체 호스팅 엔진 유지 관리 모드 설명

유지 관리 모드를 사용하면 고가용성 에이전트의 간섭 없이 **Manager** 가상 시스템을 시작, 중지 및 수정하고 **Manager**를 방해하지 않고 환경에서 셀프 호스트 엔진 노드를 다시 시작하고 수정할 수 있습니다.

다음과 같은 세 가지 유지 관리 모드가 있습니다.

- **global** - 클러스터의 모든 고가용성 에이전트가 **Manager** 가상 시스템의 상태 모니터링에서 비활성화됩니다. 이후 버전의 **Red Hat Virtualization**으로 업그레이드하는 등 **ovirt-engine** 서비스가 중지되어야 하는 모든 설정 또는 업그레이드 작업에 글로벌 유지 관리 모드를 적용해야 합니다.
- **로컬** - 명령을 실행한 노드의 고가용성 에이전트는 **Manager** 가상 시스템의 상태를 모니터링하지 못하도록 비활성화되어 있습니다. 노드는 로컬 유지 관리 모드에서 관리자 가상 머신을 호스팅하는 것에서 제외됩니다. 이 모드에 배치할 때 **Manager** 가상 시스템을 호스팅하는 경우 사용 가능한 한 개가 있는 경우 관리자는 다른 노드로 마이그레이션합니다. 시스템 변경 또는 업데이트를 자체 호스팅 엔진 노드에 적용할 때 로컬 유지 관리 모드를 사용하는 것이 좋습니다.
- **none** - 유지 관리 모드를 비활성화하여 고가용성 에이전트가 작동하는지 확인합니다.

3.1.1.2. 로컬 유지 관리 모드 설정

로컬 유지 관리 모드를 활성화하면 단일 자체 호스팅 엔진 노드에서 고가용성 에이전트가 중지됩니다.

관리 포털에서 로컬 유지 관리 모드 설정

1.

자체 호스팅 엔진 노드를 로컬 유지 관리 모드에 넣으십시오.

a.

관리 포털에서 **Compute**(컴퓨팅 → **Hosts**(호스트))를 클릭하고 자체 호스팅 엔진 노드를 선택합니다.

b.

Management(관리 → **Maintenance** (유지 관리) 및 **OK** (확인)를 클릭합니다. 해당 노드에 대해 로컬 유지 관리 모드가 자동으로 트리거됩니다.

2.

유지 관리 작업을 완료한 후 유지 관리 모드를 비활성화합니다.

a.

관리 포털에서 **Compute**(컴퓨팅 → **Hosts**(호스트) 를 클릭하고 자체 호스팅 엔진 노드를 선택합니다.

b.

Management(관리 → **Activate** (활성화) 를 클릭합니다.

명령줄에서 로컬 유지 관리 모드 설정

1.

자체 호스팅 엔진 노드에 로그인하여 로컬 유지 관리 모드로 전환합니다.

```
# hosted-engine --set-maintenance --mode=local
```

2.

유지 관리 작업을 완료한 후 유지 관리 모드를 비활성화합니다.

```
# hosted-engine --set-maintenance --mode=none
```

3.1.1.3. 글로벌 유지 관리 모드 설정

글로벌 유지 관리 모드를 활성화하면 클러스터의 모든 자체 호스팅 엔진 노드에서 고가용성 에이전트가 중지됩니다.

관리 포털에서 글로벌 유지 관리 모드 설정

1.

모든 셀프 호스팅 엔진 노드를 전역 유지 관리 모드로 전환합니다.

a.

관리 포털에서 **Compute**(컴퓨팅 → **Hosts**(호스트) 를 클릭하고 자체 호스팅 엔진 노드를 선택합니다.

b.

추가 작업 (

⋮

)을 클릭한 다음 **Enable Global HA Maintenance**(글로벌 HA 유지 관리 활성화)를 클릭합니다.

2.

유지 관리 작업을 완료한 후 유지 관리 모드를 비활성화합니다.

a.

관리 포털에서 **Compute**(컴퓨팅 → **Hosts**(호스트)를 클릭하고 자체 호스팅 엔진 노드를 선택합니다.

b.

추가 작업 (



)을 클릭한 다음 **Disable Global HA Maintenance**(글로벌 HA 유지 관리 비활성화)를 클릭합니다.

명령줄에서 전역 유지 관리 모드 설정

1.

자체 호스팅 엔진 노드에 로그인하여 전역 유지 관리 모드로 설정합니다.

```
# hosted-engine --set-maintenance --mode=global
```

2.

유지 관리 작업을 완료한 후 유지 관리 모드를 비활성화합니다.

```
# hosted-engine --set-maintenance --mode=none
```

3.1.2. Manager 가상 머신 관리

hosted-engine 유틸리티는 **Manager** 가상 시스템을 관리하는 데 도움이 되는 여러 명령을 제공합니다. 모든 자체 호스팅 엔진 노드에서 호스팅 엔진을 실행할 수 있습니다. 사용 가능한 모든 명령을 보려면 **hosted-engine --help**를 실행합니다. 특정 명령에 대한 추가 정보를 보려면 **hosted-engine --command --help**를 실행합니다.

3.1.2.1. 셀프 호스트 엔진 구성 업데이트

셀프 호스트 엔진 구성을 업데이트하려면 **hosted-engine --set-shared-config** 명령을 사용합니다. 이 명령은 초기 배포 후 공유 스토리지 도메인에서 자체 호스팅 엔진 구성을 업데이트합니다.

현재 구성 값을 보려면 **hosted-engine --get-shared-config** 명령을 사용합니다.

사용 가능한 모든 구성 키 및 해당 유형을 보려면 다음 명령을 입력합니다.

```
# hosted-engine --set-shared-config key--type=type --help
```

여기서 **type** 은 다음 중 하나입니다.

he_local	호스트가 새 값을 사용하도록 로컬 호스트에서 /etc/ovirt-hosted-engine/hosted-engine.conf 의 로컬 인스턴스에서 값을 설정합니다. 새 값을 활성화하려면 ovirt-ha-agent 및 ovirt-ha-broker 서비스를 다시 시작합니다.
he_shared	공유 스토리지에 /etc/ovirt-hosted-engine/hosted-engine.conf 의 값을 설정하여 구성 변경 후 배포된 모든 호스트에서 이러한 값을 사용합니다. 호스트에서 새 값을 활성화하려면 해당 호스트를 다시 배포합니다.
ha	로컬 스토리지의 /var/lib/ovirt-hosted-engine-ha/ha.conf 에 값을 설정합니다. 새 설정은 즉시 적용됩니다.
broker	로컬 스토리지의 /var/lib/ovirt-hosted-engine-ha/broker.conf 에 값을 설정합니다. ovirt-ha-broker 서비스를 다시 시작하여 새 설정을 활성화합니다.

3.1.2.2. 이메일 알림 구성

셀프 호스팅 엔진 노드에서 **HA** 상태 전환에 **SMTP**를 사용하여 이메일 알림을 구성할 수 있습니다. 업데이트할 수 있는 키에는 **smtp-server,smtp-port,source-email,destination-emails** 및 **state_transition** 이 포함됩니다.

이메일 알림을 구성하려면 다음을 수행합니다.

1.

자체 호스팅 엔진 노드에서 **smtp-server** 키를 원하는 **SMTP** 서버 주소로 설정합니다.

```
# hosted-engine --set-shared-config smtp-server smtp.example.com --type=broker
```



참고

자체 호스팅 엔진 구성 파일이 업데이트되었는지 확인하려면 다음을 실행합니다.

```
# hosted-engine --get-shared-config smtp-server --type=broker
broker : smtp.example.com, type : broker
```

2.

기본 **SMTP** 포트(25 포트)가 구성되었는지 확인합니다.

```
# hosted-engine --get-shared-config smtp-port --type=broker
broker : 25, type : broker
```

3.

SMTP 서버가 이메일 알림을 보내는 데 사용할 이메일 주소를 지정합니다. 주소 하나만 지정할 수 있습니다.

```
# hosted-engine --set-shared-config source-email source@example.com --type=broker
```

4.

이메일 알림을 받을 대상 이메일 주소를 지정합니다. 여러 이메일 주소를 지정하려면 각 주소를 쉼표로 구분합니다.

```
# hosted-engine --set-shared-config destination-emails
destination1@example.com,destination2@example.com --type=broker
```

SMTP가 자체 호스팅 엔진 환경에 맞게 올바르게 구성되었는지 확인하려면 셀프 호스트 엔진 노드에서 **HA** 상태를 변경하고 이메일 알림이 전송되었는지 확인합니다. 예를 들어 **HA** 에이전트를 유지 관리 모드로 전환하여 **HA** 상태를 변경할 수 있습니다. 자세한 내용은 [자체 호스팅 엔진 유지](#) 관리를 참조하십시오.

3.1.3. 추가 호스트에서 셀프 호스트 엔진에 대한 메모리 예약 구성

Manager 가상 시스템을 종료하거나 마이그레이션해야 하는 경우 **Manager** 가상 시스템을 다시 시작하거나 마이그레이션할 수 있도록 자체 호스팅 엔진 노드에 충분한 메모리가 있어야 합니다. 이 메모리는 스케줄링 정책을 사용하여 여러 자체 호스팅 엔진 노드에 예약할 수 있습니다. 스케줄링 정책은 가상 머신을 시작하거나 마이그레이션하기 전에 **Manager** 가상 머신을 시작하는 데 충분한 메모리가 지정된 수의 추가 자체 호스팅 엔진 노드에 남아 있는지 확인합니다. [스케줄링 정책](#)에 대한 자세한 내용은 [관리 가이드](#)에서 스케줄링 정책 생성을 참조하십시오.

Red Hat Virtualization Manager에 자체 호스팅 엔진 노드를 추가하려면 **Manager**에 [자체 호스팅 엔진 노드 추가](#)를 참조하십시오.

추가 호스트에서 셀프 호스트 엔진에 대한 메모리 예약 구성

1.

Compute(컴퓨팅) → **Clusters** (클러스터) 를 클릭하고 자체 호스팅 엔진 노드가 포함된 클러스터를 선택합니다.

2. **Edit(편집)**를 클릭합니다.
3. **Scheduling Policy(스케줄링 정책)** 탭을 클릭합니다.
4. **+**를 클릭하고 **HeSparesCount**를 선택합니다.
5. **Manager** 가상 시스템을 시작하는 데 충분한 여유 메모리를 예약하는 추가 자체 호스팅 엔진 노드 수를 입력합니다.
6. **OK(확인)**를 클릭합니다.

3.1.4. Red Hat Virtualization Manager에 자체 호스팅 엔진 노드 추가

자체 호스팅 엔진 노드로 호스트를 배포하는 추가 단계를 사용하여 표준 호스트와 동일한 방식으로 셀프 호스팅 엔진 노드를 추가합니다. 공유 스토리지 도메인이 자동으로 감지되고 필요한 경우 **Manager** 가상 시스템을 호스팅하기 위해 노드를 장애 조치 호스트로 사용할 수 있습니다. 자체 호스팅 엔진 환경에 표준 호스트를 연결할 수도 있지만 **Manager** 가상 시스템을 호스팅할 수는 없습니다. **Manager** 가상 시스템을 고가용성으로 사용할 수 있도록 두 개 이상의 자체 호스팅 엔진 노드가 있어야 합니다. **REST API**를 사용하여 호스트를 추가할 수도 있습니다. [REST API 가이드에서 호스트](#)를 참조하십시오.

사전 요구 사항

- 모든 자체 호스팅 엔진 노드는 동일한 클러스터에 있어야 합니다.
- 자체 호스팅 엔진 노드를 재사용하는 경우 기존 셀프 호스팅 엔진 구성을 제거합니다. [셀프 호스팅 엔진 환경에서 호스트 제거](#)를 참조하십시오.

절차

1. 관리 포털에서 **Compute** → **Hosts (호스트)**를 클릭합니다.
2. **New (새로 만들기)**를 클릭합니다.

추가 호스트 설정에 대한 자세한 내용은 [관리 가이드의 새 호스트 및 호스트 편집 창의 설정](#)을 참조하십시오.

3.
드롭다운 목록을 사용하여 새 호스트의 **Data Center** (데이터 센터) 및 **Host Cluster**(호스트 클러스터) 를 선택합니다.
4.
새 호스트의 **Name** (이름) 및 **Address** (주소)를 입력합니다. 표준 SSH 포트인 **port 22**는 **SSH Port**(SSH 포트) 필드에 자동으로 채워집니다.
5.
Manager(관리자)에 사용할 인증 방법을 선택하여 호스트에 액세스합니다.
 - 암호 인증을 사용하려면 **root** 사용자의 암호를 입력합니다.
 - 또는 **SSH PublicKey** 필드에 표시된 키를 호스트의 **/root/.ssh/authorized_keys** 에 복사하여 공개 키 인증을 사용합니다.
6.
선택적으로 호스트에 지원되는 전원 관리 카드가 있는 전원 관리를 구성합니다. 전원 관리 구성에 대한 자세한 내용은 [관리 가이드에 설명된 호스트 전원 관리 설정을 참조하십시오](#).
7.
Hosted Engine(호스팅 엔진) 탭을 클릭합니다.
8.
Deploy (배포)를 선택합니다.
9.
OK(확인)를 클릭합니다.

3.1.5. 기존 호스트를 자체 호스팅 엔진 노드로 다시 설치

자체 호스팅 엔진 환경의 기존 표준 호스트를 **Manager** 가상 시스템을 호스팅할 수 있는 자체 호스팅 엔진 노드로 변환할 수 있습니다.



주의

호스트 운영 체제를 설치하거나 다시 설치하는 경우 먼저 이러한 디스크를 실수로 초기화하지 않도록 호스트에 연결된 기존 비OS 스토리지를 분리하는 것이 좋습니다.

절차

1. **Compute(컴퓨팅) → Hosts(호스트)** 를 클릭하고 호스트를 선택합니다.
2. **Management(관리 → Maintenance (유지 관리) 및 OK (확인)**를 클릭합니다.
3. **Installation → Reinstall (재설치)**을 클릭합니다.
4. **Hosted Engine(호스팅 엔진)** 탭을 클릭하고 드롭다운 목록에서 **DEPLOY (배포)**를 선택합니다.
5. **OK(확인)**를 클릭합니다.

호스트는 자체 호스팅 엔진 구성으로 다시 설치되며 관리 포털에서 오른쪽 아이콘으로 플래그가 지정됩니다.

3.1.6. 복구 모드에서 관리자 가상 머신 부팅

이 주제에서는 **Manager** 가상 시스템을 시작하지 않을 때 복구 모드로 부팅하는 방법을 설명합니다. 자세한 내용은 **Red Hat Enterprise Linux 시스템 관리자 가이드의 복구 모드로 부팅** 을 참조하십시오.

1. 호스팅 엔진 노드 중 하나에 연결합니다.

```
$ ssh root@host_address
```

2. 자체 호스팅 엔진을 전역 유지 관리 모드에 넣으십시오.

```
# hosted-engine --set-maintenance --mode=global
```

3. **Manager** 가상 머신의 실행 중인 인스턴스가 이미 있는지 확인합니다.

```
# hosted-engine --vm-status
```

Manager 가상 머신 인스턴스가 실행 중인 경우 해당 호스트에 연결합니다.

```
# ssh root@host_address
```

4. 가상 머신을 종료합니다.

```
# hosted-engine --vm-shutdown
```



참고

가상 머신이 종료되지 않으면 다음 명령을 실행합니다.

```
# hosted-engine --vm-poweroff
```

5. 일시 중지 모드에서 **Manager** 가상 머신을 시작합니다.

```
hosted-engine --vm-start-paused
```

6. 임시 **VNC** 암호를 설정합니다.

```
hosted-engine --add-console-password
```

명령은 **VNC**를 사용하여 **Manager** 가상 머신에 로그인하는 데 필요한 정보를 출력합니다.

7. **VNC**를 사용하여 **Manager** 가상 시스템에 로그인합니다. **Manager**(관리자) 가상 시스템이 여전히 일시 중지되어 있으므로 해당 시스템이 정지된 것처럼 보입니다.

8.

호스트에서 다음 명령을 사용하여 **Manager** 가상 머신을 다시 시작합니다.



주의

다음 명령을 실행하면 부트 로더 메뉴가 나타납니다. 부트 로더가 정상적인 부팅 프로세스를 진행하기 전에 복구 모드로 전환해야 합니다. 이 명령을 계속 진행하기 전에 복구 모드로 들어가는 방법에 대한 다음 단계를 읽어 보십시오.

```
# /usr/bin/virsh -c qemu:///system?authfile=/etc/ovirt-hosted-engine/virsh_auth.conf
resume HostedEngine
```

9.

복구 모드에서 **Manager** 가상 시스템을 부팅합니다.

10.

글로벌 유지 관리 모드 비활성화

```
# hosted-engine --set-maintenance --mode=none
```

이제 **Manager** 가상 머신에서 복구 작업을 실행할 수 있습니다.

3.1.7. 자체 호스트 엔진 환경에서 호스트 제거

사용자 환경에서 자체 호스팅 엔진 노드를 제거하려면 노드를 유지보수 모드에 배치하고 노드 배포를 취소한 다음 선택적으로 제거합니다. **HA** 서비스가 중지되고 자체 호스팅 엔진 구성 파일이 제거된 후 노드는 일반 호스트로 관리할 수 있습니다.

절차

1.

관리 포털에서 **Compute**(컴퓨팅 → **Hosts**(호스트))를 클릭하고 자체 호스팅 엔진 노드를 선택합니다.

2.

Management(관리 → **Maintenance** (유지 관리) 및 **OK** (확인))를 클릭합니다.

3. **Installation → Reinstall (재설치)**을 클릭합니다.
4. **Hosted Engine(호스팅 엔진)** 탭을 클릭하고 드롭다운 목록에서 **UNDEPLOY (UNDEPLOY)**를 선택합니다. 이 작업은 **ovirt-ha-agent** 및 **ovirt-ha-broker** 서비스를 중지하고 자체 호스팅 엔진 구성 파일을 제거합니다.
5. **OK(확인)**를 클릭합니다.
6. 선택적으로 **Remove(제거)**를 클릭합니다. 그러면 **Remove Host(s)(호스트 제거)** 확인 창이 열립니다.
7. **OK(확인)**를 클릭합니다.

3.1.8. 자체 호스팅 엔진 업데이트

현재 버전에서 최신 버전으로 자체 호스팅 엔진을 업데이트하려면 환경을 전역 유지 관리 모드로 전환한 다음 마이너 버전 간에 업데이트를 위한 표준 절차를 따라야 합니다.

글로벌 유지 관리 모드 활성화

Manager 가상 시스템에서 설정 또는 업그레이드 작업을 수행하기 전에 자체 호스팅 엔진 환경을 전역 유지 관리 모드에 배치해야 합니다.

절차

1. 셀프 호스트 엔진 노드 중 하나에 로그인하고 글로벌 유지 관리 모드를 활성화합니다.

```
# hosted-engine --set-maintenance --mode=global
```

2. 계속하기 전에 환경이 글로벌 유지 관리 모드에 있는지 확인합니다.

```
# hosted-engine --vm-status
```

클러스터가 전역 유지 관리 모드에 있음을 나타내는 메시지가 표시되어야 합니다.

Red Hat Virtualization Manager 업데이트

절차

1. **Manager** 시스템에서 업데이트된 패키지가 사용 가능한지 확인합니다.

```
# engine-upgrade-check
```

2. 설정 패키지를 업데이트합니다.

```
# yum update ovirt-*setup* rh*vm-setup-plugins
```

3. **Red Hat Virtualization Manager**를 **engine-setup** 스크립트로 업데이트합니다. **engine-setup** 스크립트에서는 몇 가지 설정 질문을 표시한 다음 **ovirt-engine** 서비스를 중지하고, 업데이트된 패키지를 다운로드 및 설치하고, 데이터베이스를 백업 및 업데이트하고, 설치 후 구성을 수행하고, **ovirt-engine** 서비스를 시작합니다.

```
# engine-setup
```

스크립트가 성공적으로 완료되면 다음 메시지가 표시됩니다.

```
Execution of setup completed successfully
```

참고

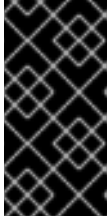
engine-setup 스크립트는 **Red Hat Virtualization Manager** 설치 프로세스 중에도 사용되며 제공된 구성 값을 저장합니다. 업데이트 중에 구성을 프리뷰할 때 저장된 값이 표시되며 설치 후 **engine-config**를 사용하여 구성을 업데이트한 경우 최신 상태가 아닐 수 있습니다. 예를 들어 설치 후 **engine-config**를 **SANWipeAfterDelete**를 **true**로 업데이트하는 경우 **engine-setup**은 "삭제 후 기본 SAN 와이프(Default SAN wipe after delete)를 출력합니다. **False**"를 설정합니다. 그러나 업데이트된 값은 **engine-setup**으로 덮어쓰지 않습니다.

중요

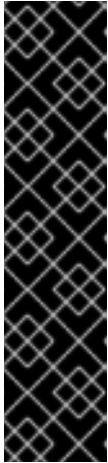
업데이트 프로세스에 다소 시간이 걸릴 수 있습니다. 완료하기 전에 프로세스를 중지하지 마십시오.

4. 기본 운영 체제 및 **Manager**에 설치된 선택적 패키지를 업데이트합니다.

```
# yum update --nobest
```

**중요**

업데이트 중에 필요한 **Ansible** 패키지 충돌이 발생하면 **RHV 관리자**에서 **yum update**를 수행할 수 없음(적용 충돌)을 참조하십시오.

**중요**

커널 패키지가 업데이트된 경우 다음을 수행합니다.

1. 글로벌 유지 관리 모드 비활성화
2. 시스템을 재부팅하여 업데이트를 완료합니다.

관련 정보

전역 유지 관리 모드 비활성화

전역 유지 관리 모드 비활성화

절차

1. **Manager** 가상 시스템에 로그인하여 종료합니다.
2. 자체 호스팅 엔진 노드 중 하나에 로그인하고 글로벌 유지 관리 모드를 비활성화합니다.

```
# hosted-engine --set-maintenance --mode=none
```

글로벌 유지 관리 모드를 종료하면 **ovirt-ha-agent**가 **Manager** 가상 시스템을 시작한 다음 **Manager**가 자동으로 시작됩니다. **Manager**가 시작하는 데 최대 10분이 걸릴 수 있습니다.

3. 환경이 실행 중인지 확인합니다.

```
# hosted-engine --vm-status
```

나열된 정보에는 **Engine Status**가 포함됩니다. **Engine** 상태 값은 다음과 같아야 합니다.

```
{ "health": "good", "vm": "up", "detail": "Up" }
```

참고

가상 머신이 여전히 부팅되고 **Manager**가 아직 시작되지 않은 경우 **Engine** 상태는 다음과 같습니다.

```
{ "reason": "bad vm status", "health": "bad", "vm": "up", "detail": "Powering up" }
```

이 경우 몇 분 기다렸다가 다시 시도합니다.

3.1.9. 자체 호스팅 엔진에서 관리자의 FQDN 변경

ovirt-engine-rename 명령을 사용하여 관리자의 **FQDN**(정규화된 도메인 이름) 레코드를 업데이트할 수 있습니다.

자세한 내용은 [Ovirt Engine Rename Tool을 사용하여 관리자 Renaming](#) 을 참조하십시오.

3.2. 백업 및 마이그레이션

3.2.1. Red Hat Virtualization Manager 백업 및 복원

3.2.1.1. Red Hat Virtualization Manager 백업 - 개요

engine-backup 도구를 사용하여 **Red Hat Virtualization Manager**의 정기적 백업을 수행합니다. 툴은 엔진 데이터베이스와 구성 파일을 단일 파일로 백업하고 **ovirt-engine** 서비스를 중단하지 않고 실행할 수 있습니다.

3.2.1.2. engine-backup 명령의 구문

engine-backup 명령은 다음 두 가지 기본 모드 중 하나로 작동합니다.

```
# engine-backup --mode=backup
```

```
# engine-backup --mode=restore
```

이러한 두 모드는 엔진 데이터베이스의 백업 범위와 다른 자격 증명을 지정할 수 있는 매개 변수 집합에 의해 확장됩니다. 전체 매개 변수 및 해당 기능을 보려면 **engine-backup --help** 를 실행합니다.

기본 옵션

--mode

명령이 백업 작업을 수행할지 또는 복원 작업을 수행할지 여부를 지정합니다. 두 가지 옵션 (**backup** 및 **restore**)을 사용할 수 있습니다. 필수 매개변수입니다.

--file

백업 모드에서 백업을 수행할 파일의 경로와 이름과 복원 모드에서 백업 데이터를 읽을 파일의 경로와 이름을 지정합니다. 이는 백업 모드와 복원 모드 모두에서 필수 매개 변수입니다.

--log

백업 또는 복원 작업의 로그를 작성할 파일의 경로와 이름을 지정합니다. 이 매개 변수는 백업 모드와 복원 모드에서 모두 필요합니다.

--scope

backup 또는 **restore** 작업의 범위를 지정합니다. 네 가지 옵션이 있습니다. **all** 은 모든 데이터베이스와 구성 데이터를 백업하거나 복원합니다. 시스템에서 파일만 백업하거나 복원하는 파일, 관리자 데이터베이스만 백업하거나 복원하는 **db**, 데이터 웨어하우스 데이터베이스만 백업하거나 복원하는 **and dwhdb**. 기본 범위는 모두입니다.

--scope 매개 변수는 동일한 **engine-backup** 명령에서 여러 번 지정할 수 있습니다.

관리자 데이터베이스 옵션

다음 옵션은 복원 모드에서 **engine-backup** 명령을 사용하는 경우에만 사용할 수 있습니다. 아래 옵션 구문은 **Manager** 데이터베이스를 복원하는 데 적용됩니다. 데이터 웨어하우스 데이터베이스를 복원하는 데도 동일한 옵션이 있습니다. 데이터 웨어하우스 옵션 구문은 **engine-backup --help** 를 참조하십시오.

--provision-db

복원할 **Manager** 데이터베이스 백업에 사용할 **PostgreSQL** 데이터베이스를 생성합니다. 원격 호스트에서 백업을 복원하거나 **PostgreSQL** 데이터베이스가 아직 구성되지 않은 새 설치에 백업을 복원할 때 필수 매개 변수입니다.

--change-db-credentials

백업 자체에 저장된 자격 증명 이외의 자격 증명을 사용하여 **Manager** 데이터베이스를 복원하기 위한 대체 자격 증명을 지정할 수 있습니다. 이 매개변수에 필요한 추가 매개변수는 **engine-backup --**

help 를 참조하십시오.

--restore-permissions 또는 **--no-restore-permissions**

데이터베이스 사용자의 권한을 복원하거나 복원하지 않습니다. 백업을 복원할 때는 이러한 매개 변수 중 하나가 필요합니다.



참고

백업에 추가 데이터베이스 사용자에게 대한 권한이 포함된 경우 **--restore-permissions** 및 **--provision-db**(또는 **--provision-dwh-db**) 옵션으로 백업을 복원하면 임의 암호가 있는 추가 사용자가 생성됩니다. 추가 사용자가 복원된 시스템에 액세스해야 하는 경우 이러한 암호를 수동으로 변경해야 합니다. 백업에서 **Red Hat Virtualization**을 복원한 후 추가 데이터베이스 사용자에게 액세스 권한을 부여하는 방법을 참조하십시오.

3.2.1.3. engine-backup 명령으로 백업 생성

Manager가 활성화된 동안 **engine-backup** 명령을 사용하여 **Red Hat Virtualization Manager**를 백업할 수 있습니다. 백업할 항목을 지정하려면 다음 값 중 하나를 **--scope** 옵션에 추가합니다.

all

Manager의 모든 데이터베이스 및 구성 파일의 전체 백업

파일

시스템의 파일 만 백업

db

Manager 데이터베이스만 백업

dwhdb

데이터 웨어하우스 데이터베이스만 백업

cinderlibdb

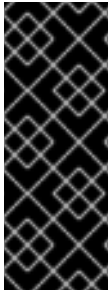
Cinderlib 데이터베이스만 백업

grafanadb

Grafana 데이터베이스만 백업

--scope 옵션을 두 번 이상 지정할 수 있습니다.

추가 파일을 백업하도록 **engine-backup** 명령을 구성할 수도 있습니다. 백업하는 모든 항목을 복원합니다.



중요

Red Hat Virtualization Manager의 새로운 설치에 데이터베이스를 복원하려면 데이터베이스 백업만으로는 충분하지 않습니다. **Manager**는 구성 파일에 대한 액세스도 필요합니다. **all** 이외의 범위를 지정하는 경우 **--scope=files**를 포함하거나 파일 시스템을 백업해야 합니다.

engine-backup 명령에 대한 전체 설명을 보려면 **Manager** 시스템에 **engine-backup --help**를 입력하십시오.

절차

1. **Manager** 시스템에 로그인합니다.
2. 백업을 생성합니다.

```
# engine-backup --scope=all --mode=backup --file=file_name --log=log_file_name
```

이 명령은 **file_name.tar**에 백업과 **log_file_name**에 로그 파일을 생성합니다.

file_name.tar을 사용하여 환경을 복원합니다.

다음 예제에서는 여러 가지 백업 시나리오를 보여줍니다.

예 3.1. 전체 백업

```
# engine-backup --scope=all --mode=backup --file=file_name --log=log_file_name
```

예 3.2. 데이터베이스 백업 관리자

```
# engine-backup --scope=files --scope=db --mode=backup --file=file_name --
log=log_file_name
```

예 3.3. 데이터 웨어하우스 데이터베이스 백업

```
# engine-backup --scope=files --scope=dwhdb --mode=backup --file=file_name --
log=log_file_name
```

예 3.4. 백업에 특정 파일 추가

1.

engine-backup 명령에 대한 구성 사용자 지정을 저장할 디렉터리를 만듭니다.

```
# mkdir -p /etc/ovirt-engine-backup/engine-backup-config.d
```

2.

다음 내용을 사용하여 새 디렉터리에 **ntp-chroney.sh** 라는 텍스트 파일을 생성합니다.

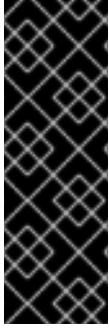
```
BACKUP_PATHS="${BACKUP_PATHS}
/etc/chrony.conf
/etc/ntp.conf
/etc/ovirt-engine-backup"
```

3.

engine-backup 명령을 실행할 때 **--scope=files** 를 사용합니다. 백업 및 복원에는 **/etc/chrony.conf**, **/etc/ntp.conf**, **/etc/ovirt-engine-backup** 이 포함됩니다.

3.2.1.4. engine-backup 명령을 사용하여 백업 복원

engine-backup 명령을 사용하여 백업을 복원하려면 복원 대상에 따라 백업을 생성하는 것보다 더 많은 단계가 필요합니다. 예를 들어 **engine-backup** 명령을 사용하여 **Red Hat Virtualization**의 기존 설치 위에 새로 설치한 **Red Hat Virtualization** 설치의 백업을 복원하고 로컬 또는 원격 데이터베이스를 사용할 수 있습니다.



중요

백업을 복원하는 데 사용되는 Red Hat Virtualization Manager 버전 (예: 4.4.8)은 백업을 생성하는 데 사용되는 Red Hat Virtualization Manager 버전 (예: 4.4.7) 이상이어야 합니다. Red Hat Virtualization 4.4.7부터 이 정책은 **engine-backup** 명령에 의해 엄격하게 적용됩니다. 백업 파일에 포함된 Red Hat Virtualization 버전을 보려면 백업 파일의 압축을 풀고 압축을 푼 파일의 루트 디렉터리에 있는 버전 파일의 값을 읽습니다.

3.2.1.5. 이전 설치로 백업 복원

engine-backup 명령을 사용하여 Red Hat Virtualization Manager의 새로운 설치로 백업을 복원할 수 있습니다. 다음 절차는 기본 운영 체제가 설치되어 있고 Red Hat Virtualization Manager에 필요한 패키지가 설치되었지만 **engine-setup** 명령이 아직 실행되지 않은 시스템에서 수행해야 합니다. 이 절차에서는 백업을 복원할 시스템에서 백업 파일 또는 파일에 액세스할 수 있다고 가정합니다.

절차

1.

Manager 시스템에 로그인합니다. 엔진 데이터베이스를 원격 호스트에 복원하는 경우에 로그인하고 해당 호스트에서 관련 작업을 수행해야 합니다. 마찬가지로 데이터 웨어하우스를 원격 호스트로 복원하는 경우에도 에 로그인하고 해당 호스트에서 관련 작업을 수행해야 합니다.

2.

전체 백업 또는 데이터베이스 전용 백업을 복원합니다.

•

전체 백업을 복원하십시오.

```
# engine-backup --mode=restore --file=file_name --log=log_file_name --provision-db --restore-permissions
```

데이터 웨어하우스가 전체 백업의 일부로 복원되는 경우 추가 데이터베이스를 프로비저닝합니다.

```
engine-backup --mode=restore --file=file_name --log=log_file_name --provision-db --provision-dwh-db --restore-permissions
```

•

구성 파일과 데이터베이스 백업을 복원하여 데이터베이스 전용 백업을 복원합니다.

```
# engine-backup --mode=restore --scope=files --scope=db --file=file_name --log=log_file_name --provision-db --restore-permissions
```


위의 예제에서는 **Manager** 데이터베이스의 백업을 복원합니다.

```
# engine-backup --mode=restore --scope=files --scope=dwhdb --file=file_name --
log=log_file_name --provision-dwh-db --restore-permissions
```

위의 예제에서는 데이터 웨어하우스 데이터베이스의 백업을 복원합니다.

성공하면 다음 출력이 표시됩니다.

```
You should now run engine-setup.
Done.
```

3.

다음 명령을 실행하고 프롬프트에 따라 복원된 관리자를 구성합니다.

```
# engine-setup
```

Red Hat Virtualization Manager가 백업에 보존된 버전으로 복원되었습니다. 새로운 **Red Hat Virtualization** 시스템의 정규화된 도메인 이름을 변경하려면 **oVirt Engine Rename Tool** 을 참조하십시오.

3.2.1.6. 기존 설치를 덮어쓰도록 백업 복원

engine-backup 명령을 사용하면 **Red Hat Virtualization Manager**가 이미 설치되어 설정된 머신에 백업을 복원할 수 있습니다. 이 기능은 환경을 백업하고 해당 환경에 대한 변경 사항을 수행한 다음 백업에서 환경을 복원하여 변경 사항을 취소하려는 경우에 유용합니다.

호스트 추가 또는 제거와 같은 백업이 수행되었으므로 환경의 변경 사항이 복원된 환경에 표시되지 않습니다. 이러한 변경 사항을 다시 실행해야 합니다.

절차

1. **Manager** 시스템에 로그인합니다.
2. 구성 파일을 제거하고 **Manager**와 연결된 데이터베이스를 정리합니다.

```
# engine-cleanup
```

engine-cleanup 명령은 관리자 데이터베이스만 정리합니다. 데이터베이스를 삭제하거나 해당 데이터베이스를 소유한 사용자를 삭제하지 않습니다.

3.

전체 백업 또는 데이터베이스 전용 백업을 복원합니다. 사용자와 데이터베이스가 이미 있으므로 새 데이터베이스를 만들거나 데이터베이스 자격 증명을 지정할 필요가 없습니다.

-

전체 백업을 복원하십시오.

```
# engine-backup --mode=restore --file=file_name --log=log_file_name --restore-permissions
```

-

구성 파일과 데이터베이스 백업을 복원하여 데이터베이스 전용 백업을 복원합니다.

```
# engine-backup --mode=restore --scope=files --scope=db --scope=dwhdb --file=file_name --log=log_file_name --restore-permissions
```



참고

Manager 데이터베이스만 복원하려면(예: 데이터 웨어하우스 데이터베이스가 다른 시스템에 있는 경우) **--scope=dwhdb** 매개 변수를 생략하면 됩니다.

성공하면 다음 출력이 표시됩니다.

```
You should now run engine-setup.
Done.
```

4.

Manager를 재구성합니다.

```
# engine-setup
```

3.2.1.7. 다른 인증 정보를 사용하여 백업 복원

engine-backup 명령은 **Red Hat Virtualization Manager**가 이미 설치 및 설정된 머신에 백업을 복원할 수 있지만 백업의 데이터베이스 자격 증명은 백업을 복원할 시스템의 데이터베이스와 다릅니다. 이 기능은 설치 백업을 수행하고 백업에서 다른 시스템으로 설치를 복원하려는 경우에 유용합니다.

중요

기존 설치를 덮어쓰도록 백업을 복원할 때는 **engine- backup** 명령을 사용하기 전에 **engine -cleanup** 명령을 실행하여 기존 설치를 정리해야 합니다. **engine-cleanup** 명령은 엔진 데이터베이스만 정리하며 데이터베이스를 삭제하거나 해당 데이터베이스를 소유한 사용자를 삭제하지 않습니다. 따라서 새 데이터베이스를 만들거나 데이터베이스 자격 증명을 지정할 필요가 없습니다. 그러나 엔진 데이터베이스의 소유자 자격 증명을 알 수 없는 경우 백업을 복원하기 전에 변경해야 합니다.

절차

1.

Red Hat Virtualization Manager 시스템에 로그인합니다.

2.

다음 명령을 실행하고 프롬프트에 따라 **Manager**의 구성 파일을 제거하고 **Manager**의 데이터베이스를 정리합니다.

```
# engine-cleanup
```

3.

해당 사용자의 자격 증명을 알 수 없는 경우 엔진 데이터베이스의 소유자 암호를 변경합니다.

a.

postgresql 명령줄을 입력합니다.

```
# su - postgres -c 'psql'
```

b.

엔진 데이터베이스를 소유한 사용자의 암호를 변경합니다.

```
postgres=# alter role user_name encrypted password 'new_password';
```

필요한 경우 **ovirt_engine_history** 데이터베이스를 소유한 사용자에게 대해 이 작업을 반복합니다.

4.

change- db-credentials 매개변수를 사용하여 전체 백업 또는 데이터베이스 전용 백업을 복원하여 새 데이터베이스의 자격 증명을 전달합니다. **Manager**에 로컬로 있는 데이터베이스의 **database_location**은 **localhost**입니다.



참고

다음 예제에서는 암호를 지정하지 않고 각 데이터베이스에 대해 **--password** 옵션을 사용하여 각 데이터베이스의 암호를 묻는 메시지를 표시합니다. 또는 각 데이터베이스에 대해 **--passfile=password_file** 옵션을 사용하여 대화형 프롬프트 없이도 **engine-backup** 도구에 암호를 안전하게 전달할 수 있습니다.

•

전체 백업을 복원하십시오.

```
# 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 웨어하우스가 전체 백업의 일부로 복원되는 경우 추가 데이터베이스에 대한 수정된 인증 정보를 포함합니다.

```
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
```

•

구성 파일과 데이터베이스 백업을 복원하여 데이터베이스 전용 백업을 복원합니다.

```
# 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 예제에서는 **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 예제에서는 데이터 웨어하우스 데이터베이스의 백업을 복원합니다.

성공하면 다음 출력이 표시됩니다.

**You should now run engine-setup.
Done.**

5.

다음 명령을 실행하고 프롬프트에 따라 방화벽을 재구성하고 **ovirt-engine** 서비스가 올바르게 구성되었는지 확인합니다.

engine-setup

3.2.1.8. 자체 호스팅 엔진 백업 및 복원

자체 호스팅 엔진을 백업하고 새로운 자체 호스팅 환경에서 복원할 수 있습니다. 환경을 다른 스토리지 유형의 새로운 자체 호스팅 엔진 스토리지 도메인으로 마이그레이션하는 등의 작업을 수행하려면 다음 절차를 사용하십시오.

배포 중에 백업 파일을 지정하면 자체 호스팅 엔진 스토리지 도메인과 함께 새 **Manager** 가상 시스템에 백업이 복원됩니다. 이전 관리자가 제거되고 기존의 자체 호스팅 엔진 스토리지 도메인의 이름이 변경되며 새 환경이 올바르게 작동하는지 확인한 후 수동으로 제거할 수 있습니다. 새 호스트에 배포하는 것이 좋습니다. 백업된 환경에 배포에 사용된 호스트가 있는 경우 새 환경의 충돌을 피하기 위해 복원된 데이터베이스에서 제거됩니다. 새 호스트에 배포하는 경우 고유한 이름을 호스트에 할당해야 합니다. 백업에 포함된 기존 호스트의 이름을 재사용하면 새 환경에서 충돌이 발생할 수 있습니다.

백업 및 복원 작업에는 다음과 같은 주요 작업이 포함됩니다.

1.

engine-backup 도구를 사용하여 원래 관리자를 백업합니다.

2.

새 자체 호스팅 엔진을 배포하고 백업을 복원합니다.

3.

새 관리자 가상 시스템에서 **Manager** 리포지토리를 활성화합니다.

4.

셀프 호스팅 엔진 노드를 다시 설치하여 구성을 업데이트합니다.

5.

기존의 자체 호스팅 엔진 스토리지 도메인을 제거합니다.

이 절차에서는 액세스 권한이 있다고 가정하고 원래 관리자를 변경할 수 있습니다.

사전 요구 사항

- 관리자와 호스트에 대해 준비된 정규화된 도메인 이름입니다. 정방향 및 역방향 조회 레코드는 모두 **DNS**에 설정해야 합니다. 새 관리자는 원래 **Manager**와 동일한 정규화된 도메인 이름을 가져야 합니다.
- 원래 관리자는 최신 마이너 버전으로 업데이트해야 합니다. 백업을 복원하는 데 사용되는 **Red Hat Virtualization Manager** 버전 (예: 4.4.8)은 백업을 생성하는 데 사용되는 **Red Hat Virtualization Manager** 버전 (예: 4.4.7) 이상이어야 합니다. **Red Hat Virtualization 4.4.7**부터 이 정책은 **engine-backup** 명령에 의해 엄격하게 적용됩니다. [업그레이드 가이드에서 Red Hat Virtualization Manager](#) 업데이트를 참조하십시오.



참고

백업을 복원해야 하지만 새 어플라이언스가 없으면 복원 프로세스가 일시 중지되고 **SSH**를 통해 임시 관리자 시스템에 로그인하고 필요에 따라 채널을 등록하고, 관리자 패키지를 업그레이드한 후 복원 프로세스를 다시 시작할 수 있습니다.

- 업데이트된 스토리지 버전과의 호환성을 보장하려면 데이터 센터 호환성 수준을 최신 버전으로 설정해야 합니다.
- 환경에는 하나 이상의 일반 호스트가 있어야 합니다. 이 호스트(및 기타 일반 호스트)는 **SPM** 역할 및 실행 중인 가상 시스템을 호스팅하도록 활성 상태로 유지됩니다. 일반 호스트가 아직 **SPM**이 아닌 경우 일반 호스트를 선택하고 **Management** → **Select as SPM**(**SPM** 선택)을 클릭하여 백업을 만들기 전에 **SPM** 역할을 이동합니다.

일반 호스트를 사용할 수 없는 경우 다음 두 가지 방법으로 호스트를 추가할 수 있습니다.

- 노드에서 자체 호스팅 엔진 구성을 제거합니다(하지만 환경에서 노드를 제거하지 마십시오). [셀프 호스팅 엔진 환경에서 호스트 제거를 참조하십시오.](#)
- 새 일반 호스트를 추가합니다. [Manager 호스트 작업에 표준 호스트 추가를 참조하십시오.](#)

3.2.1.8.1. 원래 관리자 백업

engine-backup 명령을 사용하여 원래 관리자를 백업하고, 프로세스 중 언제든지 액세스할 수 있도록 백업 파일을 별도의 위치에 복사합니다.

engine-backup --mode=backup 옵션에 대한 자세한 내용은 *관리 가이드의 [Backing Up](#) 및 [Restoring the Red Hat Virtualization Manager](#)* 를 참조하십시오.

절차

1. 셀프 호스트 엔진 노드 중 하나에 로그인하여 환경을 전역 유지 관리 모드로 이동합니다.

```
# hosted-engine --set-maintenance --mode=global
```

2. 원래 관리자에 로그인하여 **ovirt-engine** 서비스를 중지합니다.

```
# systemctl stop ovirt-engine
# systemctl disable ovirt-engine
```



참고

원래 관리자가 실행되지 않도록 중지하는 것은 필수 사항이 아니지만 백업을 만든 후 환경을 변경하지 않도록 하는 것이 좋습니다. 또한 원래 관리자와 새 관리자가 기존 리소스를 동시에 관리하지 못하게 합니다.

3. **engine-backup** 명령을 실행하여 생성할 백업 파일의 이름과 백업 로그를 저장하도록 만들 로그 파일의 이름을 지정합니다.

```
# engine-backup --mode=backup --file=file_name --log=log_file_name
```

4. 파일을 외부 서버에 복사합니다. 다음 예에서 **storage.example.com** 은 필요할 때까지 백업을 저장할 네트워크 스토리지 서버의 정규화된 도메인 이름이며 **/backup/** 는 지정된 폴더 또는 경로입니다.

```
# scp -p file_name log_file_name storage.example.com:/backup/
```

5. 다른 용도로 관리자 시스템이 필요하지 않은 경우 **Red Hat** 서브스크립션 관리자에서 등록 취소합니다.

```
# subscription-manager unregister
```

6. 자체 호스팅 엔진 노드 중 하나에 로그인하고 원래 **Manager** 가상 머신을 종료합니다.

hosted-engine --vm-shutdown

Manager를 백업한 후 새 자체 호스팅 엔진을 배포하고 새 가상 시스템에 백업을 복원합니다.

3.2.1.8.2. 새로운 자체 호스팅 엔진에서 백업 복원

새 호스트에서 **hosted-engine** 스크립트를 실행하고 **--restore-from-file=path/to/file_name** 옵션을 사용하여 배포 중에 **Manager** 백업을 복원합니다.

중요

iSCSI 스토리지를 사용하고 있고 **iSCSI** 대상에서 이니시에이터의 **ACL**에 따라 연결을 필터링하는 경우 **STORAGE_DOMAIN_UNREACHABLE** 오류로 배포가 실패할 수 있습니다. 이 문제를 방지하려면 자체 호스팅 엔진 배포를 시작하기 전에 **iSCSI** 구성을 업데이트해야 합니다.

- 기존 호스트에 재배포하는 경우 **/etc/iscsi/initiatorname.iscsi**에서 호스트의 **iSCSI** 이니시에이터 설정을 업데이트해야 합니다. 이니시에이터 **IQN**은 이전에 **iSCSI** 타겟에 매핑된 것과 동일하거나 해당하는 경우 새 **IQN**으로 업데이트되어야 합니다.
- 새 호스트에 배포하는 경우 해당 호스트의 연결을 수락하도록 **iSCSI** 대상 구성을 업데이트해야 합니다.

IQN은 호스트 측(**iSCSI** 이니시에이터) 또는 스토리지 측(**iSCSI** 대상)에서 업데이트할 수 있습니다.

절차

1. 백업 파일을 새 호스트에 복사합니다. 다음 예에서 **host.example.com**은 호스트의 **FQDN**이며 **/backup/**는 지정된 폴더 또는 경로입니다.

```
# scp -p file_name host.example.com:/backup/
```

2. 새 호스트에 로그인합니다.

3. **Red Hat Virtualization Host**에 배포하는 경우 **ovirt-hosted-engine-setup**이 이미 설치되어 있으므로 이 단계를 건너뛰니다. **Red Hat Enterprise Linux**에 배포하는 경우 **ovirt-hosted-**

engine-setup 패키지를 설치합니다.

```
# dnf install ovirt-hosted-engine-setup
```

4.

네트워크 또는 터미널 중단 시 세션 손실을 방지하기 위해 **tmux** 창 관리자를 사용하여 스크립트를 실행합니다.

tmux 를 설치하고 실행합니다.

```
# dnf -y install tmux
# tmux
```

5.

백업 파일의 경로를 지정하여 **hosted-engine** 스크립트를 실행합니다.

```
# hosted-engine --deploy --restore-from-file=backup/file_name
```

언제든지 스크립트를 이스케이프하려면 **CTRL+D** 를 사용하여 배포를 중단합니다.

6.

Yes (예)를 선택하여 배포를 시작합니다.

7.

네트워크를 구성합니다. 스크립트는 환경에 대한 관리 브리지로 사용할 수 있는 **NIC**를 탐지합니다.

8.

가상 머신 설치에 사용자 지정 어플라이언스를 사용하려면 **OVA** 아카이브 경로를 입력합니다. 그렇지 않으면 **RHV-M** 어플라이언스를 사용하려면 이 필드를 비워 둡니다.

9.

Manager의 루트 암호를 입력합니다.

10.

root 사용자로 **Manager**에 로그인할 수 있는 **SSH** 공개 키를 입력하고 **root** 사용자에게 대해 **SSH** 액세스를 활성화할지 여부를 지정합니다.

11.

가상 시스템의 **CPU** 및 메모리 구성을 입력합니다.

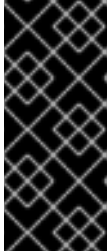
12.

Manager 가상 시스템의 **MAC** 주소를 입력하거나 무작위로 생성된 가상 시스템의 수락을

수락합니다. **DHCP**를 통해 **Manager** 가상 머신에 **IP** 주소를 제공하려면 이 **MAC** 주소에 유효한 **DHCP** 예약이 있는지 확인합니다. 배포 스크립트는 **DHCP** 서버를 구성하지 않습니다.

13.

가상 시스템의 네트워킹 세부 정보를 입력합니다. 정적을 지정하는 경우 **Manager**의 **IP** 주소를 입력합니다.



중요

정적 **IP** 주소는 호스트와 동일한 서브넷에 속해야 합니다. 예를 들어 호스트가 **10.1.1.0/24**에 있는 경우 **Manager** 가상 시스템의 **IP**는 동일한 서브넷 범위 (**10.1.1.1-254/24**)에 있어야 합니다.

14.

Manager 가상 시스템 및 기본 호스트에 대한 항목을 가상 시스템의 **/etc/hosts** 파일에 추가할지 여부를 지정합니다. 호스트 이름을 확인할 수 있는지 확인해야 합니다.

15.

SMTP 서버의 이름 및 **TCP** 포트 번호, 이메일 알림을 보내는 데 사용되는 이메일 주소 및 이러한 알림을 수신하기 위해 쉼표로 구분된 이메일 주소 목록을 제공합니다.

16.

admin@internal 사용자의 암호를 입력하여 관리 포털에 액세스합니다.

이 스크립트는 가상 시스템을 생성합니다. **RHV-M** 어플라이언스를 설치해야 하는 경우 다소 시간이 걸릴 수 있습니다.

참고

필수 네트워크 또는 유사한 문제가 없어 호스트가 작동하지 않는 경우 배포가 일시 중지되고 다음과 같은 메시지가 표시됩니다.

```
[ INFO ] You can now connect to https://<host name>:6900/ovirt-engine/ and
check the status of this host and eventually remediate it, please continue only
when the host is listed as 'up'
[ INFO ] TASK [ovirt.ovirt.hosted_engine_setup : include_tasks]
[ INFO ] ok: [localhost]
[ INFO ] TASK [ovirt.ovirt.hosted_engine_setup : Create temporary lock file]
[ INFO ] changed: [localhost]
[ INFO ] TASK [ovirt.ovirt.hosted_engine_setup : Pause execution until
/tmp/ansible.<random>_he_setup_lock is removed, delete it once ready to
proceed]
```

프로세스를 일시 중지하면 다음을 수행할 수 있습니다.

- 제공된 **URL**을 사용하여 관리 포털에 연결합니다.
- 상황을 평가하고 호스트가 작동하지 않는 이유를 확인하고 필요한 사항을 수정합니다. 예를 들어 이 배포가 백업에서 복원되고 호스트 클러스터에 필요한 네트워크가 포함된 백업이 네트워크를 구성하여 관련 호스트 **NIC**를 이러한 네트워크에 연결합니다.
- 모든 항목이 확인되고 호스트 상태가 **Up** 이면 위의 메시지에 표시된 잠금 파일을 제거합니다. 배포는 계속됩니다.

17.

사용할 스토리지 유형을 선택합니다.

- **NFS**의 경우 버전, 전체 주소 및 스토리지의 경로 및 모든 마운트 옵션을 입력합니다.



주의

가상 시스템 데이터가 손실될 위험이 있으므로 기존의 자체 호스팅 엔진 스토리지 도메인의 마운트 지점을 새 스토리지 도메인에 사용하지 마십시오.

- **iSCSI**의 경우 포털 세부 정보를 입력하고 자동 감지 목록에서 대상 및 **LUN**을 선택합니다. 배포 중에 하나의 **iSCSI** 대상만 선택할 수 있지만 다중 경로는 동일한 포털 그룹의 모든 포털을 연결하도록 지원됩니다.



참고

iSCSI 대상을 두 개 이상 지정하려면 셀프 호스트 엔진을 배포하기 전에 다중 경로를 활성화해야 합니다. 자세한 내용은 [Red Hat Enterprise Linux DM Multipath](#)를 참조하십시오. 다양한 옵션으로 다중 경로를 설치하고 구성하는 스크립트를 생성하는 [Multipath Helper](#) 툴도 있습니다.

- **Gluster** 스토리지의 경우 전체 주소와 스토리지 경로 및 모든 마운트 옵션을 입력합니다.



주의

가상 시스템 데이터가 손실될 위험이 있으므로 기존의 자체 호스팅 엔진 스토리지 도메인의 마운트 지점을 새 스토리지 도메인에 사용하지 마십시오.



중요

복제본 1과 복제본 3 **Gluster** 스토리지만 지원됩니다. 다음과 같이 볼륨을 구성했는지 확인합니다.

```
gluster volume set VOLUME_NAME group virt
gluster volume set VOLUME_NAME performance.strict-o-direct on
gluster volume set VOLUME_NAME network.remote-dio off
gluster volume set VOLUME_NAME storage.owner-uid 36
gluster volume set VOLUME_NAME storage.owner-gid 36
gluster volume set VOLUME_NAME network.ping-timeout 30
```

•

파이버 채널의 경우 자동 감지 목록에서 **LUN**을 선택합니다. 호스트 버스 어댑터를 구성하고 연결해야 하며 **LUN**에 기존 데이터가 없어야 합니다. 기존 **LUN**을 재사용하려면 [관리 가이드에서 LUN 재사용](#)을 참조하십시오.

18.

Manager 디스크 크기를 입력합니다.

스크립트는 배포가 완료될 때까지 계속됩니다.

19.

배포 프로세스는 관리자의 **SSH** 키를 변경합니다. 클라이언트 시스템이 **SSH** 오류 없이 새 관리자에 액세스할 수 있도록 하려면 원래 관리자에 액세스한 클라이언트 시스템에서 **.ssh/known_hosts** 파일에서 원래 관리자 항목을 제거하십시오.

배포가 완료되면 새 **Manager** 가상 시스템에 로그인하고 필요한 리포지토리를 활성화합니다.

3.2.1.8.3. Red Hat Virtualization Manager 리포지토리 활성화

Red Hat Subscription Manager에 관리자 시스템에 로그인하고 등록하고 **Red Hat Virtualization Manager** 서브스크립션을 연결한 다음 **Manager** 리포지토리를 활성화해야 합니다.

절차

1.

시스템을 **Content Delivery Network**에 등록하고 메시지가 표시되면 고객 포털 사용자 이름과 암호를 입력합니다.

```
# subscription-manager register
```



참고

IPv6 네트워크를 사용하는 경우 IPv6 전환 메커니즘을 사용하여 콘텐츠 전달 네트워크 및 서브스크립션 관리자에게 액세스합니다.

2.

Red Hat Virtualization Manager 서브스크립션 풀을 찾아 풀 ID를 기록합니다.

```
# subscription-manager list --available
```

3.

풀 ID를 사용하여 서브스크립션을 시스템에 연결합니다.

```
# subscription-manager attach --pool=pool_id
```



참고

현재 첨부된 서브스크립션을 보려면 다음을 수행합니다.

```
# subscription-manager list --consumed
```

활성화된 리포지토리를 모두 나열하려면 다음을 수행합니다.

```
# dnf repolist
```

4.

리포지토리를 구성합니다.

```
# subscription-manager repos \
  --disable='*' \
  --enable=rhel-8-for-x86_64-baseos-rpms \
  --enable=rhel-8-for-x86_64-appstream-rpms \
  --enable=rhv-4.4-manager-for-rhel-8-x86_64-rpms \
  --enable=fast-datapath-for-rhel-8-x86_64-rpms \
  --enable=jb-eap-7.4-for-rhel-8-x86_64-rpms \
  --enable=openstack-16.2-cinderlib-for-rhel-8-x86_64-rpms \
  --enable=rhceph-4-tools-for-rhel-8-x86_64-rpms
```

5.

pki-deps 모듈을 활성화합니다.

```
# dnf module -y enable pki-deps
```

6. **postgresql** 모듈 버전 12를 활성화합니다.

```
# dnf module -y enable postgresql:12
```

7. **nodejs** 모듈의 버전 14를 활성화합니다.

```
# dnf module -y enable nodejs:14
```

8. 설치된 패키지를 동기화하여 사용 가능한 최신 버전으로 업데이트합니다.

```
# dnf distro-sync --nobest
```

추가 리소스

모듈 및 모듈 스트림에 대한 자세한 내용은 *사용자 공간 구성 요소 설치, 관리 및 제거*의 다음 섹션을 참조하십시오.

- [모듈 스트림](#)
- [패키지 설치 전에 스트림 선택](#)
- [모듈 스트림 재설정](#)
- [이후 스트림으로 전환](#)

이제 **Manager**와 해당 리소스가 자체 호스팅 환경에서 실행됩니다. 자체 호스팅 엔진 구성을 업데이트하려면 **Manager**에 자체 호스팅 엔진 노드를 다시 설치해야 합니다. 표준 호스트는 영향을 받지 않습니다. 각 셀프 호스트 엔진 노드에 대해 다음 절차를 수행합니다.

3.2.1.8.4. 호스트 재설치

관리 포털에서 **RHVH(Red Hat Virtualization Host)** 및 **Red Hat Enterprise Linux** 호스트를 다시 설치합니다. 절차에는 호스트를 중지하고 다시 시작하는 작업이 포함됩니다.



주의

호스트 운영 체제를 설치하거나 다시 설치하는 경우 먼저 이러한 디스크를 실수로 초기화하지 않도록 호스트에 연결된 기존 비OS 스토리지를 분리하는 것이 좋습니다.

사전 요구 사항

- 클러스터의 마이그레이션이 활성화된 경우 가상 시스템은 클러스터의 다른 호스트로 자동 마이그레이션할 수 있습니다. 따라서 사용량이 상대적으로 낮은 상태에서 호스트를 다시 설치합니다.
- 클러스터에 호스트에서 유지 관리를 수행할 수 있는 메모리가 충분한지 확인합니다. 클러스터에 메모리가 없으면 가상 시스템 마이그레이션이 중단되고 실패합니다. 메모리 사용량을 줄이면 호스트를 유지 관리로 이동하기 전에 일부 또는 모든 가상 시스템을 종료합니다.
- 재설치를 수행하기 전에 클러스터에 호스트가 두 개 이상 포함되어 있는지 확인합니다. 모든 호스트를 동시에 다시 설치하지 마십시오. 스토리지 풀 관리자(SPM) 작업을 수행하려면 하나의 호스트를 사용할 수 있어야 합니다.

절차

1. **Compute(컴퓨팅) → Hosts(호스트)** 를 클릭하고 호스트를 선택합니다.
2. **Management(관리 → Maintenance (유지 관리) 및 OK(확인))**를 클릭합니다.
3. **Installation → Reinstall (재설치)**을 클릭합니다. 그러면 **Install Host(호스트 설치)** 창이 열립니다.
4. **Hosted Engine(호스팅 엔진)** 탭을 클릭하고 드롭다운 목록에서 **DEPLOY (배포)**를 선택합니다.
5. **OK(확인)**를 클릭하여 호스트를 다시 설치합니다.

호스트를 다시 설치하고 해당 상태가 **Up** 으로 돌아간 후 가상 시스템을 호스트로 다시 마이그레이션 할 수 있습니다.



중요

Red Hat Virtualization Host를 **Red Hat Virtualization Manager**에 등록하고 다시 설치한 후 관리 포털에 **Install Failed** (설치 실패) 상태로 잘못 표시될 수 있습니다. **Management**(관리 → **Activate** (활성화) 를 클릭하면 호스트가 **Up** 상태로 변경되고 사용할 준비가 됩니다.

자체 호스팅 엔진 노드를 다시 설치한 후 노드 중 하나에서 다음 명령을 실행하여 새 환경의 상태를 확인할 수 있습니다.

```
# hosted-engine --vm-status
```

복원하는 동안 기존의 자체 호스팅 엔진 스토리지 도메인의 이름이 변경되었지만 복원에 문제가 있는 경우 새 환경에서 제거되지 않았습니다. 환경이 정상적으로 실행 중인지 확인한 후 기존의 자체 호스팅 엔진 스토리지 도메인을 제거할 수 있습니다.

3.2.1.8.5. 스토리지 도메인 제거

데이터 센터에 가상화된 환경에서 제거하려는 스토리지 도메인이 있습니다.

절차

1. **Storage**(스토리지 → **Domains** (도메인) 를 클릭합니다.
2. 스토리지 도메인을 유지 관리 모드로 이동하고 분리합니다.
 - a. 스토리지 도메인의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
 - b. **Data Center**(데이터 센터) 탭을 클릭합니다.
 - c. **Maintenance**(유지 관리)를 클릭한 다음 **OK**(확인)를 클릭합니다.

d.

Detach(분리) 를 클릭한 다음 **OK(확인)**를 클릭합니다.

3.

Remove(제거)를 클릭합니다.

4.

선택적으로 **Format Domain(형식 도메인)**을 선택합니다. 즉, 스토리지 콘텐츠가 손실됩니다! 도메인의 내용을 지우려면 확인란을 선택합니다.

5.

OK(확인)를 클릭합니다.

스토리지 도메인은 환경에서 영구적으로 제거됩니다.

3.2.1.9. 기존 백업에서 자체 호스팅 엔진 복구

복구할 수 없는 문제로 인해 자체 호스팅 엔진을 사용할 수 없는 경우 문제가 발생하기 전에 수행한 백업을 사용하여 새로운 자체 호스팅 환경에서 복원할 수 있습니다(사용 가능한 경우).

배포 중에 백업 파일을 지정하면 자체 호스팅 엔진 스토리지 도메인과 함께 새 **Manager** 가상 시스템에 백업이 복원됩니다. 이전 관리자가 제거되고 기존의 자체 호스팅 엔진 스토리지 도메인의 이름이 변경되며 새 환경이 올바르게 작동하는지 확인한 후 수동으로 제거할 수 있습니다. 새 호스트에 배포하는 것이 좋습니다. 백업된 환경에 배포에 사용된 호스트가 있는 경우 새 환경의 충돌을 피하기 위해 복원된 데이터베이스에서 제거됩니다. 새 호스트에 배포하는 경우 고유한 이름을 호스트에 할당해야 합니다. 백업에 포함된 기존 호스트의 이름을 재사용하면 새 환경에서 충돌이 발생할 수 있습니다.

자체 호스팅 엔진을 복원하려면 다음과 같은 주요 작업이 포함됩니다.

1.

새 자체 호스팅 엔진을 배포하고 백업을 복원합니다.

2.

새 관리자 가상 시스템에서 **Manager** 리포지토리를 활성화합니다.

3.

셀프 호스트 엔진 노드를 다시 설치하여 구성을 업데이트합니다.

4.

기존의 자체 호스팅 엔진 스토리지 도메인을 제거합니다.

이 절차에서는 원래 관리자에 대한 액세스 권한이 없고 새 호스트에서 백업 파일에 액세스할 수 있다고 가정합니다.

사전 요구 사항

- 관리자와 호스트에 대해 준비된 정규화된 도메인 이름입니다. 정방향 및 역방향 조회 레코드는 모두 DNS에 설정해야 합니다. 새 관리자는 원래 **Manager**와 동일한 정규화된 도메인 이름을 가져야 합니다.

3.2.1.9.1. 새로운 자체 호스팅 엔진에서 백업 복원

새 호스트에서 **hosted-engine** 스크립트를 실행하고 **--restore-from-file=path/to/file_name** 옵션을 사용하여 배포 중에 **Manager** 백업을 복원합니다.

중요

iSCSI 스토리지를 사용하고 있고 iSCSI 대상에서 이니시에이터의 **ACL**에 따라 연결을 필터링하는 경우 **STORAGE_DOMAIN_UNREACHABLE** 오류로 배포가 실패할 수 있습니다. 이 문제를 방지하려면 자체 호스팅 엔진 배포를 시작하기 전에 iSCSI 구성을 업데이트해야 합니다.

- 기존 호스트에 재배포하는 경우 **/etc/iscsi/initiatorname.iscsi**에서 호스트의 iSCSI 이니시에이터 설정을 업데이트해야 합니다. 이니시에이터 **IQN**은 이전에 iSCSI 타겟에 매핑된 것과 동일하거나 해당하는 경우 새 **IQN**으로 업데이트되어야 합니다.

- 새 호스트에 배포하는 경우 해당 호스트의 연결을 수락하도록 iSCSI 대상 구성을 업데이트해야 합니다.

IQN은 호스트 측(iSCSI 이니시에이터) 또는 스토리지 측(iSCSI 대상)에서 업데이트할 수 있습니다.

절차

1.

백업 파일을 새 호스트에 복사합니다. 다음 예에서 **host.example.com**은 호스트의 **FQDN**이며 **/backup/**는 지정된 폴더 또는 경로입니다.

```
# scp -p file_name host.example.com:/backup/
```

2.

새 호스트에 로그인합니다.

3.

Red Hat Virtualization Host에 배포하는 경우 **ovirt-hosted-engine-setup** 이 이미 설치되어 있으므로 이 단계를 건너뛰니다. **Red Hat Enterprise Linux**에 배포하는 경우 **ovirt-hosted-engine-setup** 패키지를 설치합니다.

```
# dnf install ovirt-hosted-engine-setup
```

4.

네트워크 또는 터미널 중단 시 세션 손실을 방지하기 위해 **tmux** 창 관리자를 사용하여 스크립트를 실행합니다.

tmux 를 설치하고 실행합니다.

```
# dnf -y install tmux
# tmux
```

5.

백업 파일의 경로를 지정하여 **hosted-engine** 스크립트를 실행합니다.

```
# hosted-engine --deploy --restore-from-file=backup/file_name
```

언제든지 스크립트를 이스케이프하려면 **CTRL+D** 를 사용하여 배포를 중단합니다.

6.

Yes (예)를 선택하여 배포를 시작합니다.

7.

네트워크를 구성합니다. 스크립트는 환경에 대한 관리 브리지로 사용할 수 있는 **NIC**를 탐지합니다.

8.

가상 머신 설치에 사용자 지정 어플라이언스를 사용하려면 **OVA** 아카이브 경로를 입력합니다. 그렇지 않으면 **RHV-M** 어플라이언스를 사용하려면 이 필드를 비워 둡니다.

9.

Manager의 루트 암호를 입력합니다.

10.

root 사용자로 **Manager**에 로그인할 수 있는 **SSH** 공개 키를 입력하고 **root** 사용자에게 대해 **SSH** 액세스를 활성화할지 여부를 지정합니다.

11. 가상 시스템의 **CPU** 및 메모리 구성을 입력합니다.
 12. **Manager** 가상 시스템의 **MAC** 주소를 입력하거나 무작위로 생성된 가상 시스템의 수락을 수락합니다. **DHCP**를 통해 **Manager** 가상 머신에 **IP** 주소를 제공하려면 이 **MAC** 주소에 유효한 **DHCP** 예약이 있는지 확인합니다. 배포 스크립트는 **DHCP** 서버를 구성하지 않습니다.
 13. 가상 시스템의 네트워킹 세부 정보를 입력합니다. 정적을 지정하는 경우 **Manager**의 **IP** 주소를 입력합니다.
- 

중요

정적 **IP** 주소는 호스트와 동일한 서브넷에 속해야 합니다. 예를 들어 호스트가 **10.1.1.0/24**에 있는 경우 **Manager** 가상 시스템의 **IP**는 동일한 서브넷 범위 (**10.1.1.1-254/24**)에 있어야 합니다.
14. **Manager** 가상 시스템 및 기본 호스트에 대한 항목을 가상 시스템의 **/etc/hosts** 파일에 추가할지 여부를 지정합니다. 호스트 이름을 확인할 수 있는지 확인해야 합니다.
 15. **SMTP** 서버의 이름 및 **TCP** 포트 번호, 이메일 알림을 보내는 데 사용되는 이메일 주소 및 이러한 알림을 수신하기 위해 쉽표로 구분된 이메일 주소 목록을 제공합니다.
 16. **admin@internal** 사용자의 암호를 입력하여 관리 포털에 액세스합니다.

이 스크립트는 가상 시스템을 생성합니다. **RHV-M** 어플라이언스를 설치해야 하는 경우 다소 시간이 걸릴 수 있습니다.

참고

필수 네트워크 또는 유사한 문제가 없어 호스트가 작동하지 않는 경우 배포가 일시 중지되고 다음과 같은 메시지가 표시됩니다.

```
[ INFO ] You can now connect to https://<host name>:6900/ovirt-engine/ and
check the status of this host and eventually remediate it, please continue only
when the host is listed as 'up'
[ INFO ] TASK [ovirt.ovirt.hosted_engine_setup : include_tasks]
[ INFO ] ok: [localhost]
[ INFO ] TASK [ovirt.ovirt.hosted_engine_setup : Create temporary lock file]
[ INFO ] changed: [localhost]
[ INFO ] TASK [ovirt.ovirt.hosted_engine_setup : Pause execution until
/tmp/ansible.<random>_he_setup_lock is removed, delete it once ready to
proceed]
```

프로세스를 일시 중지하면 다음을 수행할 수 있습니다.

- 제공된 **URL**을 사용하여 관리 포털에 연결합니다.
- 상황을 평가하고 호스트가 작동하지 않는 이유를 확인하고 필요한 사항을 수정합니다. 예를 들어 이 배포가 백업에서 복원되고 호스트 클러스터에 필요한 네트워크가 포함된 백업이 네트워크를 구성하여 관련 호스트 **NIC**를 이러한 네트워크에 연결합니다.
- 모든 항목이 확인되고 호스트 상태가 **Up** 이면 위의 메시지에 표시된 잠금 파일을 제거합니다. 배포는 계속됩니다.

17.

사용할 스토리지 유형을 선택합니다.

- **NFS**의 경우 버전, 전체 주소 및 스토리지의 경로 및 모든 마운트 옵션을 입력합니다.



주의

가상 시스템 데이터가 손실될 위험이 있으므로 기존의 자체 호스팅 엔진 스토리지 도메인의 마운트 지점을 새 스토리지 도메인에 사용하지 마십시오.

- **iSCSI**의 경우 포털 세부 정보를 입력하고 자동 감지 목록에서 대상 및 **LUN**을 선택합니다. 배포 중에 하나의 **iSCSI** 대상만 선택할 수 있지만 다중 경로는 동일한 포털 그룹의 모든 포털을 연결하도록 지원됩니다.



참고

iSCSI 대상을 두 개 이상 지정하려면 셀프 호스트 엔진을 배포하기 전에 다중 경로를 활성화해야 합니다. 자세한 내용은 [Red Hat Enterprise Linux DM Multipath](#)를 참조하십시오. 다양한 옵션으로 다중 경로를 설치하고 구성하는 스크립트를 생성하는 [Multipath Helper](#) 툴도 있습니다.

- **Gluster** 스토리지의 경우 전체 주소와 스토리지 경로 및 모든 마운트 옵션을 입력합니다.



주의

가상 시스템 데이터가 손실될 위험이 있으므로 기존의 자체 호스팅 엔진 스토리지 도메인의 마운트 지점을 새 스토리지 도메인에 사용하지 마십시오.



중요

복제본 1과 복제본 3 Gluster 스토리지만 지원됩니다. 다음과 같이 볼륨을 구성했는지 확인합니다.

```
gluster volume set VOLUME_NAME group virt
gluster volume set VOLUME_NAME performance.strict-o-direct on
gluster volume set VOLUME_NAME network.remote-dio off
gluster volume set VOLUME_NAME storage.owner-uid 36
gluster volume set VOLUME_NAME storage.owner-gid 36
gluster volume set VOLUME_NAME network.ping-timeout 30
```

•

파이버 채널의 경우 자동 감지 목록에서 **LUN**을 선택합니다. 호스트 버스 어댑터를 구성하고 연결해야 하며 **LUN**에 기존 데이터가 없어야 합니다. 기존 **LUN**을 재사용하려면 [관리 가이드에서 LUN 재사용](#)을 참조하십시오.

18.

Manager 디스크 크기를 입력합니다.

스크립트는 배포가 완료될 때까지 계속됩니다.

19.

배포 프로세스는 관리자의 **SSH** 키를 변경합니다. 클라이언트 시스템이 **SSH** 오류 없이 새 관리자에 액세스할 수 있도록 하려면 원래 관리자에 액세스한 클라이언트 시스템에서 **.ssh/known_hosts** 파일에서 원래 관리자 항목을 제거하십시오.

배포가 완료되면 새 **Manager** 가상 시스템에 로그인하고 필요한 리포지토리를 활성화합니다.

3.2.1.9.2. Red Hat Virtualization Manager 리포지토리 활성화

Red Hat Subscription Manager에 관리자 시스템에 로그인하고 등록하고 **Red Hat Virtualization Manager** 서브스크립션을 연결한 다음 **Manager** 리포지토리를 활성화해야 합니다.

절차

1.

시스템을 **Content Delivery Network**에 등록하고 메시지가 표시되면 고객 포털 사용자 이름과 암호를 입력합니다.

```
# subscription-manager register
```




참고

IPv6 네트워크를 사용하는 경우 IPv6 전환 메커니즘을 사용하여 콘텐츠 전달 네트워크 및 서브스크립션 관리자에게 액세스합니다.

2.

Red Hat Virtualization Manager 서브스크립션 풀을 찾아 풀 ID를 기록합니다.

```
# subscription-manager list --available
```

3.

풀 ID를 사용하여 서브스크립션을 시스템에 연결합니다.

```
# subscription-manager attach --pool=pool_id
```



참고

현재 첨부된 서브스크립션을 보려면 다음을 수행합니다.

```
# subscription-manager list --consumed
```

활성화된 리포지토리를 모두 나열하려면 다음을 수행합니다.

```
# dnf repolist
```

4.

리포지토리를 구성합니다.

```
# subscription-manager repos \
  --disable='*' \
  --enable=rhel-8-for-x86_64-baseos-rpms \
  --enable=rhel-8-for-x86_64-appstream-rpms \
  --enable=rhv-4.4-manager-for-rhel-8-x86_64-rpms \
  --enable=fast-datapath-for-rhel-8-x86_64-rpms \
  --enable=jb-eap-7.4-for-rhel-8-x86_64-rpms \
  --enable=openstack-16.2-cinderlib-for-rhel-8-x86_64-rpms \
  --enable=rhceph-4-tools-for-rhel-8-x86_64-rpms
```

5.

pki-deps 모듈을 활성화합니다.

```
# dnf module -y enable pki-deps
```

6.

postgresql 모듈 버전 12를 활성화합니다.

```
# dnf module -y enable postgresql:12
```

7.

nodejs 모듈의 버전 14를 활성화합니다.

```
# dnf module -y enable nodejs:14
```

8.

설치된 패키지를 동기화하여 사용 가능한 최신 버전으로 업데이트합니다.

```
# dnf distro-sync --nobest
```

추가 리소스

모듈 및 모듈 스트림에 대한 자세한 내용은 *사용자 공간 구성 요소 설치, 관리 및 제거*의 다음 섹션을 참조하십시오.

- [모듈 스트림](#)
- [패키지 설치 전에 스트림 선택](#)
- [모듈 스트림 재설정](#)
- [이후 스트림으로 전환](#)

이제 **Manager**와 해당 리소스가 자체 호스팅 환경에서 실행됩니다. 자체 호스팅 엔진 구성을 업데이트하려면 **Manager**에 자체 호스팅 엔진 노드를 다시 설치해야 합니다. 표준 호스트는 영향을 받지 않습니다. 각 셀프 호스팅 엔진 노드에 대해 다음 절차를 수행합니다.

3.2.1.9.3. 호스트 재설치

관리 포털에서 **RHVH(Red Hat Virtualization Host)** 및 **Red Hat Enterprise Linux** 호스트를 다시 설치합니다. 절차에는 호스트를 중지하고 다시 시작하는 작업이 포함됩니다.



주의

호스트 운영 체제를 설치하거나 다시 설치하는 경우 먼저 이러한 디스크를 실수로 초기화하지 않도록 호스트에 연결된 기존 비OS 스토리지를 분리하는 것이 좋습니다.

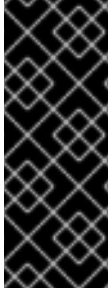
사전 요구 사항

- 클러스터의 마이그레이션이 활성화된 경우 가상 시스템은 클러스터의 다른 호스트로 자동 마이그레이션할 수 있습니다. 따라서 사용량이 상대적으로 낮은 상태에서 호스트를 다시 설치합니다.
- 클러스터에 호스트에서 유지 관리를 수행할 수 있는 메모리가 충분한지 확인합니다. 클러스터에 메모리가 없으면 가상 시스템 마이그레이션이 중단되고 실패합니다. 메모리 사용량을 줄이면 호스트를 유지 관리로 이동하기 전에 일부 또는 모든 가상 시스템을 종료합니다.
- 재설치를 수행하기 전에 클러스터에 호스트가 두 개 이상 포함되어 있는지 확인합니다. 모든 호스트를 동시에 다시 설치하지 마십시오. 스토리지 풀 관리자(SPM) 작업을 수행하려면 하나의 호스트를 사용할 수 있어야 합니다.

절차

1. **Compute(컴퓨팅) → Hosts(호스트)** 를 클릭하고 호스트를 선택합니다.
2. **Management(관리 → Maintenance (유지 관리) 및 OK(확인))**를 클릭합니다.
3. **Installation → Reinstall (재설치)**을 클릭합니다. 그러면 **Install Host(호스트 설치)** 창이 열립니다.
4. **Hosted Engine(호스팅 엔진)** 탭을 클릭하고 드롭다운 목록에서 **DEPLOY (배포)**를 선택합니다.
5. **OK(확인)**를 클릭하여 호스트를 다시 설치합니다.

호스트를 다시 설치하고 해당 상태가 **Up** 으로 돌아간 후 가상 시스템을 호스트로 다시 마이그레이션 할 수 있습니다.



중요

Red Hat Virtualization Host를 **Red Hat Virtualization Manager**에 등록하고 다시 설치한 후 관리 포털에 **Install Failed** (설치 실패) 상태로 잘못 표시될 수 있습니다. **Management**(관리 → **Activate** (활성화) 를 클릭하면 호스트가 **Up** 상태로 변경되고 사용할 준비가 됩니다.

자체 호스팅 엔진 노드를 다시 설치한 후 노드 중 하나에서 다음 명령을 실행하여 새 환경의 상태를 확인할 수 있습니다.

```
# hosted-engine --vm-status
```

복원하는 동안 기존의 자체 호스팅 엔진 스토리지 도메인의 이름이 변경되었지만 복원에 문제가 있는 경우 새 환경에서 제거되지 않았습니다. 환경이 정상적으로 실행 중인지 확인한 후 기존의 자체 호스팅 엔진 스토리지 도메인을 제거할 수 있습니다.

3.2.1.9.4. 스토리지 도메인 제거

데이터 센터에 가상화된 환경에서 제거하려는 스토리지 도메인이 있습니다.

절차

1. **Storage**(스토리지 → **Domains** (도메인) 를 클릭합니다.
2. 스토리지 도메인을 유지 관리 모드로 이동하고 분리합니다.
 - a. 스토리지 도메인의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
 - b. **Data Center**(데이터 센터) 탭을 클릭합니다.
 - c. **Maintenance**(유지 관리)를 클릭한 다음 **OK**(확인)를 클릭합니다.

d.

Detach(분리) 를 클릭한 다음 **OK(확인)**를 클릭합니다.

3.

Remove(제거)를 클릭합니다.

4.

선택적으로 **Format Domain(형식 도메인)**을 선택합니다. 즉, 스토리지 콘텐츠가 손실됩니다! 도메인의 내용을 지우려면 확인란을 선택합니다.

5.

OK(확인)를 클릭합니다.

스토리지 도메인은 환경에서 영구적으로 제거됩니다.

3.2.1.10. 기존 백업에서 자체 호스팅 엔진 덮어쓰기

자체 호스팅 엔진에 액세스할 수 있지만 데이터베이스 손상이나 롤백하기 어려운 구성 오류와 같은 문제가 발생하는 경우 문제를 시작한 백업을 사용하여 환경을 이전 상태로 복원할 수 있습니다(사용 가능한 경우).

자체 호스팅 엔진의 이전 상태를 복원하려면 다음 단계를 수행해야 합니다.

1.

글로벌 유지 관리 모드로 환경을 배치합니다.

2.

Manager 가상 시스템에서 백업을 복원합니다.

3.

글로벌 유지 관리 모드를 비활성화합니다.

engine-backup --mode=restore 옵션에 대한 자세한 내용은 **Manager 백업 및 복원**을 참조하십시오.

3.2.1.10.1. 글로벌 유지 관리 모드 활성화

Manager 가상 시스템에서 설정 또는 업그레이드 작업을 수행하기 전에 자체 호스팅 엔진 환경을 전역 유지 관리 모드에 배치해야 합니다.

절차

1. 셀프 호스트 엔진 노드 중 하나에 로그인하고 글로벌 유지 관리 모드를 활성화합니다.

```
# hosted-engine --set-maintenance --mode=global
```

2. 계속하기 전에 환경이 글로벌 유지 관리 모드에 있는지 확인합니다.

```
# hosted-engine --vm-status
```

클러스터가 전역 유지 관리 모드에 있음을 나타내는 메시지가 표시되어야 합니다.

3.2.1.10.2. 기존 설치를 덮어쓰도록 백업 복원

engine-backup 명령을 사용하면 **Red Hat Virtualization Manager**가 이미 설치되어 설정된 머신에 백업을 복원할 수 있습니다. 이 기능은 환경을 백업하고 해당 환경에 대한 변경 사항을 수행한 다음 백업에서 환경을 복원하여 변경 사항을 취소하려는 경우에 유용합니다.

호스트 추가 또는 제거와 같은 백업이 수행되었으므로 환경의 변경 사항이 복원된 환경에 표시되지 않습니다. 이러한 변경 사항을 다시 실행해야 합니다.

절차

1. **Manager** 시스템에 로그인합니다.
2. 구성 파일을 제거하고 **Manager**와 연결된 데이터베이스를 정리합니다.

```
# engine-cleanup
```

engine-cleanup 명령은 관리자 데이터베이스만 정리합니다. 데이터베이스를 삭제하거나 해당 데이터베이스를 소유한 사용자를 삭제하지 않습니다.

3. 전체 백업 또는 데이터베이스 전용 백업을 복원합니다. 사용자와 데이터베이스가 이미 있으므로 새 데이터베이스를 만들거나 데이터베이스 자격 증명을 지정할 필요가 없습니다.

•

전체 백업을 복원하십시오.

```
# engine-backup --mode=restore --file=file_name --log=log_file_name --restore-
permissions
```

•

구성 파일과 데이터베이스 백업을 복원하여 데이터베이스 전용 백업을 복원합니다.

```
# engine-backup --mode=restore --scope=files --scope=db --scope=dwhdb --
file=file_name --log=log_file_name --restore-permissions
```



참고

Manager 데이터베이스만 복원하려면(예: 데이터 웨어하우스 데이터 베이스가 다른 시스템에 있는 경우) **--scope=dwhdb** 매개 변수를 생략하면 됩니다.

성공하면 다음 출력이 표시됩니다.

```
You should now run engine-setup.
Done.
```

4.

Manager를 재구성합니다.

```
# engine-setup
```

3.2.1.10.3. 전역 유지 관리 모드 비활성화

절차

1.

Manager 가상 시스템에 로그인하여 종료합니다.

2.

자체 호스팅 엔진 노드 중 하나에 로그인하고 글로벌 유지 관리 모드를 비활성화합니다.

```
# hosted-engine --set-maintenance --mode=none
```

글로벌 유지 관리 모드를 종료하면 **ovirt-ha-agent**가 **Manager** 가상 시스템을 시작한 다음 **Manager**가 자동으로 시작됩니다. **Manager**가 시작하는 데 최대 10분이 걸릴 수 있습니다.

3.

환경이 실행 중인지 확인합니다.

```
# hosted-engine --vm-status
```

나열된 정보에는 **Engine Status** 가 포함됩니다. **Engine** 상태 값은 다음과 같아야 합니다.

```
{"health": "good", "vm": "up", "detail": "Up"}
```

참고

가상 머신이 여전히 부팅되고 **Manager**가 아직 시작되지 않은 경우 **Engine** 상태는 다음과 같습니다.

```
{"reason": "bad vm status", "health": "bad", "vm": "up", "detail": "Powering up"}
```

이 경우 몇 분 기다렸다가 다시 시도합니다.

환경이 다시 실행되면 중지된 모든 가상 시스템을 시작하고 환경의 리소스가 예상대로 작동하는지 확인할 수 있습니다.

3.2.2. 별도의 머신으로 데이터 **software** **software** to a Separate Machine으로 마이그레이션

이 섹션에서는 데이터 웨어하우스 데이터베이스 및 서비스를 **Red Hat Virtualization Manager** 시스템에서 별도의 시스템으로 마이그레이션하는 방법에 대해 설명합니다. 별도의 시스템에서 데이터 웨어하우스 서비스를 호스팅하면 각 개별 시스템의 부하가 줄어들고 **CPU** 및 메모리 리소스를 다른 프로세스와 공유하여 발생할 수 있는 충돌을 방지합니다.

참고

Red Hat은 이러한 구성 요소를 서로 별도의 시스템에 설치할 수 있더라도 데이터 웨어하우스 데이터베이스, 데이터 웨어하우스 서비스 및 **Grafana** 모두에만 설치할 수 있도록 지원합니다.

다음과 같은 마이그레이션 옵션이 있습니다.

-

Manager 시스템에서 데이터 웨어하우스 서비스를 마이그레이션하고 기존 데이터 웨어하우스

스 데이터베이스(**ovirt_engine_history**)와 연결할 수 있습니다.

-

Manager 시스템에서 데이터 웨어하우스 데이터베이스를 마이그레이션한 다음 데이터 웨어하우스 서비스를 마이그레이션할 수 있습니다.

3.2.2.1. 별도의 머신으로 데이터 웨어하우스 데이터베이스 마이그레이션

데이터 웨어하우스 서비스를 마이그레이션하기 전에 데이터 웨어하우스 데이터베이스(**ovirt_engine_history**)를 마이그레이션합니다. **engine-backup** 을 사용하여 데이터베이스 백업을 생성하고 새 데이터베이스 시스템에서 복원합니다. **engine-backup** 에 대한 자세한 내용을 보려면 **engine-backup --help** 를 실행합니다.



참고

Red Hat은 이러한 구성 요소를 서로 별도의 시스템에 설치할 수 있더라도 데이터 웨어하우스 데이터베이스, 데이터 웨어하우스 서비스 및 **Grafana** 모두에만 설치할 수 있도록 지원합니다.

새 데이터베이스 서버에 **Red Hat Enterprise Linux 8**이 설치되어 있어야 합니다.

새 데이터베이스 서버에서 필요한 리포지토리를 활성화합니다.

3.2.2.1.1. Red Hat Virtualization Manager 리포지토리 활성화

Red Hat Subscription Manager에 데이터 웨어하우스 시스템에 로그인하고 등록하고 **Red Hat Virtualization Manager** 서브스크립션을 연결한 다음 **Manager** 리포지토리를 활성화해야 합니다.

절차

- 1.

시스템을 **Content Delivery Network**에 등록하고 메시지가 표시되면 고객 포털 사용자 이름과 암호를 입력합니다.

```
# subscription-manager register
```



참고

IPv6 네트워크를 사용하는 경우 **IPv6** 전환 메커니즘을 사용하여 콘텐츠 전달 네트워크 및 서브스크립션 관리자에게 액세스합니다.

2.

Red Hat Virtualization Manager 서브스크립션 풀을 찾아 풀 ID를 기록합니다.

```
# subscription-manager list --available
```

3.

풀 ID를 사용하여 서브스크립션을 시스템에 연결합니다.

```
# subscription-manager attach --pool=pool_id
```



참고

현재 첨부된 서브스크립션을 보려면 다음을 수행합니다.

```
# subscription-manager list --consumed
```

활성화된 리포지토리를 모두 나열하려면 다음을 수행합니다.

```
# dnf repolist
```

4.

리포지토리를 구성합니다.

```
# subscription-manager repos \
  --disable='*' \
  --enable=rhel-8-for-x86_64-baseos-rpms \
  --enable=rhel-8-for-x86_64-appstream-rpms \
  --enable=rhv-4.4-manager-for-rhel-8-x86_64-rpms
```

5.

postgresql 모듈 버전 12를 활성화합니다.

```
# dnf module -y enable postgresql:12
```

6.

nodejs 모듈의 버전 14를 활성화합니다.

```
# dnf module -y enable nodejs:14
```

7.

설치된 패키지를 동기화하여 사용 가능한 최신 버전으로 업데이트합니다.

```
# dnf distro-sync --nobest
```

추가 리소스

모듈 및 모듈 스트림에 대한 자세한 내용은 *사용자 공간 구성 요소 설치, 관리 및 제거*의 다음 섹션을 참조하십시오.

- [모듈 스트림](#)
- [패키지 설치 전에 스트림 선택](#)
- [모듈 스트림 재설정](#)
- [이후 스트림으로 전환](#)

3.2.2.1.2. 별도의 머신으로 데이터 웨어하우스 데이터베이스 마이그레이션

절차

1.

Manager에서 데이터 웨어하우스 데이터베이스 및 구성 파일의 백업을 생성합니다.

```
# engine-backup --mode=backup --scope=dwhdb --scope=files --file=file_name --log=log_file_name
```

2.

Manager의 백업 파일을 새 시스템으로 복사합니다.

```
# scp /tmp/file_name root@new.dwh.server.com:/tmp
```

3.

새 시스템에 **engine-backup** 을 설치합니다.

```
# dnf install ovirt-engine-tools-backup
```

4.

PostgreSQL 서버 패키지를 설치합니다.

```
# dnf install postgresql-server postgresql-contrib
```

5.

PostgreSQL 데이터베이스를 초기화하고, **postgresql** 서비스를 시작한 다음, 이 서비스가 부팅 시 시작되는지 확인합니다.

```
# su - postgres -c 'initdb'
# systemctl enable postgresql
# systemctl start postgresql
```

6.

새 시스템에서 데이터 웨어하우스 데이터베이스를 복원합니다. **file_name** 은 **Manager**에서 복사한 백업 파일입니다.

```
# engine-backup --mode=restore --scope=files --scope=dwhdb --file=file_name --
log=log_file_name --provision-dwh-db --restore-permissions
```

데이터 웨어하우스 데이터베이스는 이제 **Manager**가 호스팅되는 별도의 시스템에서 호스팅됩니다. 데이터 웨어하우스 데이터베이스를 복원한 후 프롬프트에서 **engine-setup** 명령을 실행하도록 지시합니다. 이 명령을 실행하기 전에 데이터 웨어하우스 서비스를 마이그레이션합니다.

3.2.2.2. 별도의 머신으로 데이터 웨어하우스 서비스 마이그레이션

Red Hat Virtualization Manager에 설치 및 구성된 데이터 웨어하우스 서비스를 별도의 시스템으로 마이그레이션할 수 있습니다. 별도의 시스템에서 데이터 웨어하우스 서비스를 호스팅하면 **Manager** 시스템의 부하를 줄이는 데 도움이 됩니다.

이 절차에서는 데이터 웨어하우스 서비스만 마이그레이션합니다.

데이터 웨어하우스 서비스를 마이그레이션하기 전에 데이터 웨어하우스 데이터베이스 (**ovirt_engine_history**)를 [마이그레이션하려면 데이터장 데이터베이스를 분리 머신으로 마이그레이션을 참조하십시오.](#)



참고

Red Hat은 이러한 구성 요소를 서로 별도의 시스템에 설치할 수 있더라도 데이터 웨어하우스 데이터베이스, 데이터 웨어하우스 서비스 및 **Grafana** 모두에만 설치할 수 있도록 지원합니다.

사전 요구 사항

- 동일한 시스템에 **Manager** 및 **Data** 웨어하우스를 설치하고 구성해야 합니다.
 - 새 데이터 웨어하우스 시스템을 설정하려면 다음이 있어야 합니다.
 - **Manager**의 `/etc/ovirt-engine/engine.conf.d/10-setup-database.conf` 파일의 암호입니다.
 - 데이터 웨어하우스 시스템에서 관리자 데이터베이스 시스템의 **TCP** 포트 **5432**로 액세스할 수 있습니다.
 - **Manager**의 `/etc/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/10-setup-database.conf` 파일에서 데이터 웨어하우스 데이터베이스의 사용자 이름과 암호.
- 데이터 웨어하우스 데이터베이스를 분리 머신으로 마이그레이션하는 데 설명된 절차를 사용하여 **ovirt_engine_history** 데이터베이스를 마이그레이션하면 해당 시스템에 데이터베이스 설정 중에 정의한 이러한 자격 증명이 포함됩니다.

이 시나리오를 설치하려면 다음 네 가지 단계가 필요합니다.

1. 새 데이터 웨어하우스 머신 설정
2. **Manager** 시스템에서 데이터 **installer** 서비스 중지
3. 새 데이터 저장소 머신 구성
4. **Manager** 시스템에서 데이터 **installer** 패키지 비활성화

3.2.2.2.1. 새 데이터 웨어하우스 머신 설정

Red Hat Virtualization 리포지토리를 활성화하고 **Red Hat Enterprise Linux 8** 시스템에 데이터 웨어하우스 설치 패키지를 설치합니다.

1.

필요한 리포지토리를 활성화합니다.

a.

시스템을 **Content Delivery Network**에 등록하고 메시지가 표시되면 고객 포털 사용자 이름과 암호를 입력합니다.

```
# subscription-manager register
```

b.

Red Hat Virtualization Manager 서브스크립션 풀을 찾아 풀 ID를 기록합니다.

```
# subscription-manager list --available
```

c.

풀 ID를 사용하여 서브스크립션을 시스템에 연결합니다.

```
# subscription-manager attach --pool=pool_id
```

d.

리포지토리를 구성합니다.

```
# subscription-manager repos \
  --disable='*' \
  --enable=rhel-8-for-x86_64-baseos-rpms \
  --enable=rhel-8-for-x86_64-appstream-rpms \
  --enable=rhv-4.4-manager-for-rhel-8-x86_64-rpms \
  --enable=fast-datapath-for-rhel-8-x86_64-rpms \
  --enable=jb-eap-7.4-for-rhel-8-x86_64-rpms
```

2.

pki-deps 모듈을 활성화합니다.

```
# dnf module -y enable pki-deps
```

3.

현재 설치된 모든 패키지가 최신 상태인지 확인합니다.

```
# dnf upgrade --nobest
```

4.

ovirt-engine-dwh-setup 패키지를 설치합니다.

```
# dnf install ovirt-engine-dwh-setup
```

3.2.2.2. 관리자 시스템에서 데이터 웨어하우스 서비스 중지

절차

1. 데이터 웨어하우스 서비스를 중지합니다.

```
# systemctl stop ovirt-engine-dwhd.service
```

2. 데이터베이스가 원격 시스템에서 호스팅되는 경우 **postgres.conf** 파일을 편집하여 액세스 권한을 수동으로 부여해야 합니다. **/var/lib/pgsql/data/postgresql.conf** 파일을 편집하고 다음과 일치하도록 **listen_addresses** 행을 수정합니다.

```
listen_addresses = '*'
```

행이 없거나 주석 처리된 경우 수동으로 추가합니다.

데이터베이스가 **Manager** 시스템에서 호스팅되고 **Red Hat Virtualization Manager**를 새로 설정하는 동안 구성된 경우 기본적으로 액세스 권한이 부여됩니다.

3. **postgresql** 서비스를 다시 시작하십시오.

```
# systemctl restart postgresql
```

3.2.2.3. 새 데이터 웨어하우스 머신 구성

이 섹션에 표시된 옵션 또는 설정의 순서는 환경에 따라 다를 수 있습니다.

1. **ovirt_engine_history** 데이터베이스와 데이터 웨어하우스 서비스를 모두 동일한 시스템으로 마이그레이션하는 경우 다음을 실행하십시오. 그렇지 않으면 다음 단계를 진행합니다.

```
# sed -i '/^ENGINE_DB_/d' \
    /etc/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/10-setup-database.conf

# sed -i \
    -e 's;^\(OVESETUP_ENGINE_CORE/enable=bool\):True;\1:False;' \
    -e '/^OVESETUP_CONFIG/fqdn/d' \
    /etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf
```

2.

engine-setup 명령을 실행하여 시스템에서 데이터 웨어하우스 구성을 시작합니다.

```
# engine-setup
```

3.

Enter 를 눌러 자동으로 감지된 호스트 이름을 승인하거나 대체 호스트 이름을 입력한 후 **Enter** 키를 누릅니다.

```
Host fully qualified DNS name of this server [autodetected host name]:
```

4.

Enter 를 눌러 방화벽을 자동으로 구성하거나 **No** 를 입력하고 **Enter** 를 눌러 기존 설정을 유지 관리합니다.

```
Setup can automatically configure the firewall on this system.
Note: automatic configuration of the firewall may overwrite current settings.
Do you want Setup to configure the firewall? (Yes, No) [Yes]:
```

방화벽을 자동으로 구성하도록 선택하고 방화벽 관리자가 활성화되지 않은 경우 지원되는 옵션 목록에서 선택한 방화벽 관리자를 선택하라는 메시지가 표시됩니다. 방화벽 관리자 이름을 입력하고 **Enter** 키를 누릅니다. 이는 하나의 옵션만 나열되는 경우에도 적용됩니다.

5.

관리자에 대해 정규화된 도메인 이름과 암호를 입력합니다. **Enter** 를 눌러 서로 필드의 기본값을 적용합니다.

```
Host fully qualified DNS name of the engine server []: engine-fqdn
Setup needs to do some actions on the remote engine server. Either automatically,
using ssh as root to access it, or you will be prompted to manually perform each such
action.
Please choose one of the following:
1 - Access remote engine server using ssh as root
2 - Perform each action manually, use files to copy content around
(1, 2) [1]:
ssh port on remote engine server [22]:
root password on remote engine server engine-fqdn: password
```

6.

Manager 데이터베이스 시스템의 **FQDN** 및 암호를 입력합니다. **Enter** 를 눌러 서로 필드의 기본값을 적용합니다.

```
Engine database host []: manager-db-fqdn
Engine database port [5432]:
Engine database secured connection (Yes, No) [No]:
Engine database name [engine]:
Engine database user [engine]:
Engine database password: password
```


7.

설치 설정을 확인합니다.

Please confirm installation settings (OK, Cancel) [OK]:

데이터 웨어하우스 서비스가 이제 원격 시스템에 구성되어 있습니다. **Manager** 시스템에서 데이터 웨어하우스 서비스를 비활성화합니다.

3.2.2.2.4. 관리자 시스템에서 데이터 웨어하우스 서비스 비활성화

절차

1.

Manager 시스템에서 **Manager**를 다시 시작합니다.

```
# service ovirt-engine restart
```

2.

다음 명령을 실행하여 `/etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf` 파일을 수정하고 옵션을 **False**로 설정합니다.

```
# sed -i \
-e 's;^\(OVESETUP_DWH_CORE/enable=bool\):True;\1:False;' \
-e 's;^\(OVESETUP_DWH_CONFIG/remoteEngineConfigured=bool\):True;\1:False;' \
/etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf

# sed -i \
-e 's;^\(OVESETUP_GRAFANA_CORE/enable=bool\):True;\1:False;' \
/etc/ovirt-engine-setup.conf.d/20-setup-ovirt-post.conf
```

3.

데이터 웨어하우스 서비스를 비활성화합니다.

```
# systemctl disable ovirt-engine-dwhd.service
```

4.

데이터 웨어하우스 파일을 제거합니다.

```
# rm -f /etc/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/*.conf /var/lib/ovirt-engine-dwh/backups/*
```

데이터 웨어하우스 서비스는 이제 **Manager**와 별도의 시스템에서 호스팅됩니다.

3.2.3. 백업 스토리지 도메인을 사용하여 가상 머신 백업 및 복원

3.2.3.1. 백업 스토리지 도메인 설명

백업 스토리지 도메인은 재해 복구, 마이그레이션 또는 기타 백업/복원 사용 모델을 위해 백업 및 복원을 위해 가상 머신 및 가상 머신 템플릿을 저장 및 마이그레이션하는 데 특히 사용할 수 있습니다. 백업 도메인은 백업 도메인의 모든 가상 시스템이 전원 다운 상태라는 점에서 백업이 아닌 도메인과 다릅니다. 가상 시스템은 백업 도메인에서 실행할 수 없습니다.

데이터 스토리지 도메인을 백업 도메인으로 설정할 수 있습니다. **Manage Domain**(도메인 관리) 대화 상자에서 확인란을 선택하거나 선택 취소하여 이 설정을 활성화하거나 비활성화할 수 있습니다. 이 설정은 해당 스토리지 도메인의 모든 가상 시스템이 중지된 후에만 활성화할 수 있습니다.

백업 도메인에 저장된 가상 머신을 시작할 수 없습니다. 관리자는 이 작업을 차단하고 백업을 무효화할 수 있는 기타 모든 작업을 차단합니다. 그러나 가상 시스템의 디스크가 백업 도메인의 일부가 아닌 경우 백업 도메인에 저장된 템플릿을 기반으로 가상 머신을 실행할 수 있습니다.

다른 유형의 스토리지 도메인과 마찬가지로 데이터 센터에 백업 도메인을 연결하거나 분리할 수 있습니다. 따라서 백업 저장 외에도 백업 도메인을 사용하여 데이터 센터 간에 가상 시스템을 마이그레이션할 수 있습니다.

이점

내보내기 도메인이 아닌 백업 도메인을 사용하는 몇 가지 이유는 다음과 같습니다.

- 하나의 내보내기 도메인과 달리 데이터 센터에 여러 백업 스토리지 도메인을 가질 수 있습니다.
- 백업 및 재해 복구에 사용할 백업 스토리지 도메인을 전용으로 지정할 수 있습니다.
- 가상 머신, 템플릿 또는 스냅샷의 백업을 백업 스토리지 도메인으로 전송할 수 있습니다.
- 내보내기 도메인보다 백업 도메인을 사용하면 다수의 가상 시스템, 템플릿 또는 **OVF** 파일을 마이그레이션하는 속도가 훨씬 빠릅니다.
- 백업 도메인은 내보내기 도메인보다 디스크 공간을 더 효율적으로 사용합니다.
- 백업 도메인은 파일 스토리지(**NFS, Gluster**) 및 블록 스토리지(**Fiber Channel** 및 **iSCSI**)를

모두 지원합니다. 이는 파일 스토리지만 지원하는 내보내기 도메인과 대조됩니다.

- 제한 사항을 고려하여 스토리지 도메인의 백업 설정을 동적으로 활성화 및 비활성화할 수 있습니다.

제한 사항

- 백업 도메인의 모든 가상 시스템 또는 템플릿은 동일한 도메인에 모든 디스크가 있어야 합니다.
- 스토리지 도메인의 모든 가상 시스템의 전원을 꺼야 백업 도메인으로 설정할 수 있습니다.
- 이렇게 하면 디스크의 데이터를 조작할 수 있기 때문에 백업 도메인에 저장된 가상 시스템을 실행할 수 없습니다.
- 메모리 볼륨은 활성 가상 머신에서만 지원되므로 백업 도메인이 메모리 볼륨의 대상이 될 수 없습니다.
- 백업 도메인에서 가상 머신을 미리 볼 수 없습니다.
- 가상 머신을 백업 도메인으로 실시간 마이그레이션할 수 없습니다.
- 백업 도메인을 마스터 도메인이 되도록 설정할 수 없습니다.
- 자체 호스팅 엔진의 도메인을 백업 도메인으로 설정할 수 없습니다.
- **default** 스토리지 도메인을 백업 도메인으로 사용하지 마십시오.

3.2.3.2. 데이터 스토리지 도메인을 백업 도메인으로 설정

사전 요구 사항

- 스토리지 도메인의 가상 시스템 또는 템플릿에 속하는 모든 디스크는 동일한 도메인에 있어야 합니다.

- 도메인의 모든 가상 시스템의 전원을 꺼야 합니다.

절차

1. 관리 포털에서 **Storage** → **Domains** (스토리지 도메인)를 선택합니다.
2. 새 스토리지 도메인을 생성하거나 기존 스토리지 도메인을 선택하고 **Manage Domain**(도메인 관리)을 클릭합니다. **Manage Domains**(도메인 관리) 대화 상자가 열립니다.
3. **Advanced Parameters**(고급 매개 변수)에서 **Backup**(백업) 확인란을 선택합니다.

도메인은 이제 백업 도메인입니다.

3.2.3.3. 백업 도메인을 사용하여 가상 머신 또는 스냅샷 백업 또는 복원

전원이 꺼진 가상 시스템 또는 스냅샷을 백업할 수 있습니다. 그런 다음, 동일한 데이터 센터에 백업을 저장하고 필요에 따라 복원하거나 다른 데이터 센터로 마이그레이션할 수 있습니다.

절차: 가상 머신 백업

1. 백업 도메인을 생성합니다. [스토리지 도메인 설정을 백업 도메인 백업 도메인으로 설정합니다.](#)
2. 백업할 가상 머신을 기반으로 새 가상 머신을 생성합니다.
- 스냅샷을 백업하려면 먼저 스냅샷에서 가상 시스템을 만듭니다. [가상 머신 관리 가이드의 스냅샷에서 가상 머신 생성을 참조하십시오.](#)
- 가상 시스템을 백업하려면 먼저 가상 시스템을 복제합니다. [가상 머신 관리 가이드에서 가상 머신 복제를 참조하십시오.](#) 계속하기 전에 복제본의 전원이 꺼져 있는지 확인합니다.
3. 새 가상 시스템을 백업 도메인으로 내보냅니다. [가상 머신 관리 가이드에서 데이터 도메인으로 가상 머신 내보내기](#)를 참조하십시오.

절차: 가상 머신 복원

1. 가상 시스템 백업을 저장하는 백업 스토리지 도메인이 데이터 센터에 연결되어 있는지 확인합니다.
2. 백업 도메인에서 가상 시스템을 가져옵니다. [데이터 도메인에서 가상 머신 가져오기를 참조하십시오.](#)

관련 정보

- [스토리지 도메인 가져오기](#)
- [동일한 환경에서 데이터 센터 간에 스토리지 도메인 마이그레이션](#)
- [다른 환경의 데이터 센터 간에 스토리지 도메인 마이그레이션](#)

3.2.4. 백업 및 복원 API를 사용하여 가상 머신 백업 및 복원

3.2.4.1. 백업 및 복원 API

백업 및 복원 API는 가상 머신의 전체 또는 파일 수준 백업 및 복원을 수행할 수 있는 기능 컬렉션입니다. API는 라이브 스냅샷 및 REST API와 같은 Red Hat Virtualization의 여러 구성 요소를 결합하여 독립 소프트웨어 공급자가 제공하는 백업 소프트웨어가 포함된 가상 머신에 연결할 수 있는 임시 볼륨을 생성하고 작업합니다.

지원되는 타사 백업 벤더는 [Red Hat Virtualization 에코시스템](#) 을 참조하십시오.

3.2.4.2. 가상 머신 백업

백업 및 복원 API를 사용하여 가상 머신을 백업합니다. 이 절차에서는 백업할 가상 시스템과 백업을 관리하는 소프트웨어를 설치하는 가상 시스템이 두 개 있다고 가정합니다.

절차

1.

REST API를 사용하여 백업할 가상 머신의 스냅샷을 생성합니다.

POST /api/vms/{vm:id}/snapshots/ HTTP/1.1

Accept: application/xml

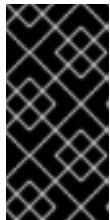
Content-type: application/xml

```
<snapshot>
  <description>BACKUP</description>
</snapshot>
```



참고

- 여기서 **{vm:id}** 를 스냅샷이 있는 가상 시스템의 **VM ID**로 바꿉니다. 이 ID는 관리 포털 및 VM 포털의 **New Virtual Machine**(새 가상 시스템) 및 **Edit Virtual Machine**(가상 시스템 편집) 창의 **General**(일반) 탭에서 사용할 수 있습니다.
- 가상 시스템의 스냅샷을 저장하면 현재 구성 데이터가 구성 특성의 **data** 속성에 스냅샷 아래의 초기화 에 저장됩니다.



중요

공유 가능 또는 직접 **LUN** 디스크에 따라 디스크 스냅샷을 가져올 수 없습니다.

2.

스냅샷 아래의 **data** 속성에서 가상 머신의 구성 데이터를 검색합니다.

GET /api/vms/{vm:id}/snapshots/{snapshot:id} HTTP/1.1

All-Content: true

Accept: application/xml

Content-type: application/xml



참고

- 여기에서 `{vm:id}` 를 이전에 만든 가상 시스템의 ID로 바꿉니다. `{snapshot:id}` 를 스냅샷 ID로 바꿉니다.
- **All-Content: true** 헤더를 추가하여 응답에서 추가 OVF 데이터를 검색합니다. XML 응답의 OVF 데이터는 VM 구성 요소 `<initialization>` `<configuration>` 내에 있습니다. 나중에 이 데이터를 사용하여 가상 시스템을 복원합니다.

3.

스냅샷 ID를 가져옵니다.

```
GET /api/vms/{vm:id}/snapshots/ HTTP/1.1
Accept: application/xml
Content-type: application/xml
```

4.

스냅샷의 디스크 ID를 식별합니다.

```
GET /api/vms/{vm:id}/snapshots/{snapshot:id}/disks HTTP/1.1
Accept: application/xml
Content-type: application/xml
```

5.

올바른 인터페이스 유형(예: `virtio_scsi`)을 사용하여 백업 가상 머신에 액티브 디스크 연결로 스냅샷을 연결합니다.

```
POST /api/vms/{vm:id}/diskattachments/ HTTP/1.1
Accept: application/xml
Content-type: application/xml
```

```
<disk_attachment>
  <active>true</active>
  <interface>_virtio_scsi_</interface>
  <disk id="{disk:id}">
    <snapshot id="{snapshot:id}" />
  </disk>
</disk_attachment>
```



참고

여기에서 `{vm:id}` 를 이전에 스냅샷이 아닌 백업 가상 시스템의 ID로 바꿉니다. `{disk:id}` 를 디스크 ID로 바꿉니다. `{snapshot:id}` 를 스냅샷 ID로 바꿉니다.

6.

백업 가상 시스템에서 백업 소프트웨어를 사용하여 스냅샷 디스크의 데이터를 백업합니다.

7.

백업 가상 머신에서 스냅샷 디스크 연결을 제거합니다.

```
DELETE /api/vms/{vm:id}/diskattachments/{snapshot:id} HTTP/1.1
Accept: application/xml
Content-type: application/xml
```



참고

여기에서 `{vm:id}` 를 이전에 스냅샷이 아닌 **백업** 가상 시스템의 ID로 바꿉니다. `{snapshot:id}` 를 스냅샷 ID로 바꿉니다.

8.

선택적으로 스냅샷을 삭제합니다.

```
DELETE /api/vms/{vm:id}/snapshots/{snapshot:id} HTTP/1.1
Accept: application/xml
Content-type: application/xml
```



참고

여기에서 `{vm:id}` 를 이전에 만든 가상 시스템의 ID로 바꿉니다. `{snapshot:id}` 를 스냅샷 ID로 바꿉니다.

별도의 가상 시스템에 설치된 백업 소프트웨어를 사용하여 고정 지점에서 가상 머신의 상태를 백업했습니다.

3.2.4.3. 가상 머신 복원

백업 및 복원 **API**를 사용하여 백업된 가상 머신을 복원합니다. 이 절차에서는 이전 백업을 관리하는데 사용한 소프트웨어가 설치된 백업 가상 시스템이 있다고 가정합니다.

절차

1.

관리 포털에서 백업을 복원할 유동 디스크를 생성합니다. 유동 **디스크를 생성하는 방법에 대한 자세한 내용은 가상** 디스크 생성을 참조하십시오.

2.

백업 가상 머신에 디스크를 연결합니다.

POST /api/vms/{vm:id}/disks/ HTTP/1.1

Accept: application/xml

Content-type: application/xml

```
<disk id="{disk:id}">
</disk>
```



참고

여기에서 {vm:id} 를 이전에 스냅샷이 아닌 이 백업 가상 시스템의 ID로 바꿉니다. {disk:id} 를 가상 머신을 백업하는 동안 얻은 디스크 ID로 바꿉니다.

3.

백업 소프트웨어를 사용하여 백업을 디스크에 복원합니다.

4.

백업 가상 머신에서 디스크를 분리합니다.

DELETE /api/vms/{vm:id}/disks/{disk:id} HTTP/1.1

Accept: application/xml

Content-type: application/xml

```
<action>
  <detach>true</detach>
</action>
```



참고

여기에서 {vm:id} 를 이전에 스냅샷이 아닌 이 백업 가상 시스템의 ID로 바꿉니다. {disk:id} 를 디스크 ID로 바꿉니다.

5.

복원 중인 가상 머신의 구성 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>
<initialization>
<configuration>
<data>
<!-- omitting long ovf data -->
</data>
<type>ovf</type>
</configuration>
</initialization>
...
</vm>

```



참고

가상 시스템을 생성하는 동안 **ovf**의 값을 재정의하려면 초기화 요소 **전후**에 요소를 재정의합니다. 초기화 요소 **내**에 없습니다.

6.

새 가상 머신에 디스크를 연결합니다.

```

POST /api/vms/{vm:id}/disks/ HTTP/1.1
Accept: application/xml
Content-type: application/xml

```

```

<disk id="{disk:id}">
</disk>

```



참고

여기에서 **{vm:id}** 를 이전에 스냅샷이 있는 가상 머신이 아닌 새 가상 시스템의 ID로 바꿉니다. **{disk:id}** 를 디스크 ID로 바꿉니다.

백업 및 복원 **API**를 사용하여 생성된 백업을 사용하여 가상 머신을 복원했습니다.

3.2.5. 증분 백업 및 복원 **API**를 사용하여 가상 머신 백업 및 복원

3.2.5.1. 증분 백업 및 복원 **API**

Red Hat Virtualization은 임시 스냅샷 없이 **QCOW2** 또는 **RAW** 가상 디스크의 전체 백업 또는 **QCOW 2** 가상 디스크의 증분 백업 백업에 사용할 수 있는 증분 백업 **API**를 제공합니다. 백업 중인 가상 디스크가 **QCOW2**인지 **RAW**인지 여부에 관계없이 **RAW** 형식으로 데이터가 백업됩니다. **RAW** 게스트 데이터와 **RAW** 또는 **QCOW2** 디스크를 복원할 수 있습니다. 증분 백업 **API**는 **RHV REST API**의 일부입니다. 실행 중이거나 그렇지 않은 가상 머신을 백업할 수 있습니다.

개발자는 **API**를 사용하여 백업 애플리케이션을 개발할 수 있습니다.

기능

백업은 **Backup** 및 **Restore API**를 사용할 때보다 더 간단하고 빠르고 강력합니다. 증분형 백업 **API**를 사용하면 백업 애플리케이션과의 통합이 향상되고 기본 디스크 형식에 관계없이 **RAW** 게스트 데이터를 백업하고 복원하는 새로운 지원이 제공됩니다.

잘못된 비트맵으로 인해 백업이 실패하는 경우 백업 체인에서 특정 **checkpoint**를 제거할 수 있습니다. 전체 백업을 실행할 필요는 없습니다.

제한 사항:

- **QCOW2** 형식의 디스크만 **RAW** 형식 디스크가 아닌 증분적으로 백업할 수 있습니다. 백업 프로세스는 백업된 데이터를 **RAW** 형식으로 저장합니다.
 - **RAW** 형식으로 백업된 데이터만 복원할 수 있습니다.
 - 증분 복원은 백업 시 스냅샷 복원을 지원하지 않으며, 증분 복원은 백업 시 스냅샷의 볼륨 또는 이미지의 구조가 아닌 데이터만 복원합니다. 이 제한은 다른 시스템의 백업 솔루션에서 일반적입니다.
 - 일반적으로 백업 솔루션과 마찬가지로 증분 복원은 백업 시 스냅샷의 볼륨 또는 이미지의 구조가 아닌 데이터만 복원합니다.
 - 가상 시스템의 불명확한 종료 원인으로 인해 디스크의 비트맵이 무효화되어 전체 백업 체인이 무효화될 수 있습니다. 잘못된 비트맵을 사용하여 증분 백업을 복원하면 가상 머신 데이터가 손상됩니다.
- 백업을 시작하는 것 외에 잘못된 비트맵을 감지할 방법은 없습니다. 디스크에 잘못된 비트맵이 포함된 경우 작업이 실패합니다.

다음 표에서는 증분 백업을 지원하는 디스크 구성을 설명합니다.



참고

관리 포털을 사용하여 디스크를 생성할 때 스토리지 유형, 프로비저닝 유형 및 증분 백업의 활성화 또는 비활성화 여부를 설정합니다. 이러한 설정에 따라 관리자는 가상 디스크 형식을 결정합니다.

표 3.1. 증분 백업에 지원되는 디스크 구성

스토리지 유형	프로비저닝 유형	증분 백업이..	가상 디스크 형식은...
블록	썬	enabled	qcow2
블록	사전 할당됨	enabled	qcow2 (preallocated)
file	썬	enabled	qcow2
file	사전 할당됨	enabled	qcow2 (preallocated)
블록	썬	비활성화됨	qcow2
블록	사전 할당됨	비활성화됨	원시 (사전 할당됨)
file	썬	비활성화됨	raw (sparse)
file	사전 할당됨	비활성화됨	원시 (사전 할당됨)
network	해당 없음	비활성화됨	원시
LUN	해당 없음	비활성화됨	원시

3.2.5.1.1. 증분 백업 흐름

증분 백업 API를 사용하는 백업 애플리케이션은 증분 백업을 위해 이미 활성화된 가상 머신 디스크를 백업하려면 다음 시퀀스를 따라야 합니다.

1.

백업 애플리케이션은 **REST API**를 사용하여 백업에 포함되어야 하는 **가상 시스템 디스크**를 찾습니다. **QCOW2** 형식의 디스크만 포함됩니다.

2.

백업 애플리케이션은 **전체 백업** 또는 **증분 백업**을 시작합니다. **API** 호출은 가상 시스템 ID, 선택적 이전 체크포인트 ID 및 백업할 디스크 목록을 지정합니다. **API** 호출에서 이전 **checkpoint ID**를 지정하지 않으면 각 디스크의 현재 상태에 따라 지정된 디스크의 모든 데이터를 포함하는 전체 백업이 시작됩니다.

3. 엔진은 백업을 위해 가상 시스템을 준비합니다. 가상 시스템은 백업 중에 계속 실행될 수 있습니다.
4. 백업 애플리케이션은 엔진에서 백업을 시작할 준비가 되었다고 보고할 때까지 엔진의 백업 상태를 폴링합니다.
5. 백업을 시작할 준비가 되면 백업 애플리케이션에서 백업에 포함된 모든 디스크에 대해 **이미지 전송 오브젝트를 생성합니다.**
6. 백업 애플리케이션은 모든 이미지 전송에 대해 **ovirt-imageio**에서 변경된 블록 목록을 가져옵니다. 변경 목록을 사용할 수 없는 경우 백업 애플리케이션에 오류가 발생합니다.
7. 백업 애플리케이션은 **ovirt-imageio**에서 변경된 블록을 **RAW** 형식으로 다운로드하여 백업 미디어에 저장합니다. 변경된 블록 목록을 사용할 수 없는 경우 백업 애플리케이션을 대체하여 전체 디스크를 복사할 수 있습니다.
8. 백업 애플리케이션은 모든 이미지 전송을 완료합니다.
9. 백업 애플리케이션은 **REST API**를 사용하여 백업을 완료합니다.

3.2.5.1.2. 증분 복원 흐름

증분 백업 **API**를 사용하는 백업 애플리케이션은 다음 시퀀스에 따라 백업된 가상 머신 디스크를 복원해야 합니다.

1. 사용자는 백업 애플리케이션을 사용하여 사용 가능한 백업을 기반으로 복원 지점을 선택합니다.
2. 백업 애플리케이션에서는 복원된 데이터를 보유할 기존 디스크가 있는 새 디스크 또는 스냅샷을 생성합니다.
3. 백업 애플리케이션은 모든 디스크에 대해 업로드 이미지 전송을 시작하여 형식을 지정하는 것은 **raw**입니다. 이를 통해 **RAW** 데이터를 **QCOW2** 디스크에 업로드할 때 형식 변환이 가능합니다.

4. 백업 애플리케이션은 **API를 사용하여 이 복원 지점에 포함된 데이터를 imageio 로 전송합니다.**
5. 백업 애플리케이션은 이미지 전송을 완료합니다.

3.2.5.1.3. 증분 백업 및 복원 API 작업

증분 백업 및 복원 API는 **Red Hat Virtualization REST API 가이드**에 설명되어 있습니다. 백업 및 복원 흐름에는 다음 작업이 필요합니다.

- 새 가상 디스크 또는 기존 가상 디스크에서 증분 백업을 활성화합니다.
 - **관리 포털을 사용하는 새 디스크**
 - **관리 포털을 사용하는 기존 디스크**
 - **API 호출을 사용하는 새 디스크 또는 기존 디스크**
- **증분 백업에 활성화된 디스크 찾기**
- **전체 백업 시작**
- **증분 백업 시작**
- **백업 종료**
- **백업에 대한 정보 가져오기**
- **백업의 디스크에 대한 정보 가져오기**

- 가상 머신의 모든 체크포인트 나열
- 특정 가상 머신 체크포인트에 대한 정보 나열
- 특정 가상 머신의 체크포인트 제거
- 백업 아카이브를 위해 이미지 전송 오브젝트 다운로드
- 백업 복원을 위해 이미지 전송 오브젝트 업로드
- 변경된 블록 나열
- 변경된 블록 다운로드 및 업로드

3.2.5.1.4. 새 가상 디스크에서 증분 백업 활성화

가상 디스크에 대해 증분 백업을 활성화하여 증분 백업에 포함된 대로 표시합니다. 디스크를 추가할 때 **REST API** 또는 관리 포털을 사용하여 모든 디스크에 대해 증분 백업을 활성화할 수 있습니다. 전체 백업을 사용하여 또는 이전과 동일한 방식으로 증분 백업에 활성화되지 않은 기존 디스크를 백업할 수 있습니다.



참고

관리자는 증분 백업에 디스크를 활성화할 필요가 없지만 활성화된 디스크를 추적하도록 활성화할 수 있습니다.

증분 백업에는 **QCOW2**로 디스크를 포맷해야 하므로 **RAW** 형식 대신 **QCOW2** 형식을 사용하십시오.

절차

1. 새 가상 디스크를 추가합니다. 자세한 내용은 [가상 디스크 생성](#)을 참조하십시오.

2.

디스크를 구성할 때 **Enable Incremental Backup** (분산 백업 사용) 확인란을 선택합니다.

추가 리소스

-

[API를 사용하여 디스크의 증분 백업을 활성화합니다.](#)

3.2.5.1.5. 기존 RAW 가상 디스크에서 증분 백업 활성화

RAW 형식의 디스크에는 증분 백업이 지원되지 않으므로 증분 백업을 사용하려면 **RAW** 형식 디스크에 **QCOW2** 형식 계층이 있어야 합니다. 스냅샷을 생성하면 **QCOW2** 계층이 생성되므로 스냅샷이 생성되는 지점에서 스냅샷에 포함된 모든 디스크에서 증분 백업을 활성화합니다.



주의

디스크의 기본 계층에서 **RAW** 형식을 사용하는 경우 마지막 스냅샷을 삭제하고 최상위 **QCOW2** 계층을 기본 계층으로 병합하여 디스크를 **RAW** 형식으로 변환하여 설정된 경우 증분 백업을 비활성화합니다. 증분 백업을 다시 활성화하려면 이 디스크를 포함한 새 스냅샷을 만들 수 있습니다.

절차

- 1.

관리 포털에서 **Compute(컴퓨팅) Virtual Machines(가상 시스템)** 를 클릭합니다.

- 2.

가상 머신을 선택하고 **Disks** (디스크) 탭을 클릭합니다.

- 3.

Edit(편집) 버튼을 클릭합니다. 디스크 편집 대화 상자가 열립니다.

- 4.

Enable Incremental Backup 확인란을 선택합니다.

추가 리소스

-

[API를 사용하여 디스크의 증분 백업 활성화](#)

3.2.5.1.6. 증분 백업 활성화

REST API 요청을 사용하여 가상 머신 디스크의 증분 백업을 활성화할 수 있습니다.

절차

- 새 디스크에 대해 증분 백업을 활성화합니다. 예를 들어 ID가 123 인 가상 머신의 새 디스크의 경우 이 요청을 보냅니다.

POST /ovirt-engine/api/vms/123/diskattachments

요청 본문에는 다음과 같이 디스크 오브젝트의 일부로 **incremental** 로 설정된 백업이 포함되어야 합니다.

```
<disk_attachment>
...
<disk>
...
<backup>incremental</backup>
...
</disk>
</disk_attachment>
```

응답은 다음과 같습니다.

```
<disk_attachment>
...
<disk href="/ovirt-engine/api/disks/456" id="456"/>
...
</disk_attachment>
```

추가 리소스

- **RHV용 REST API 가이드**의 [DiskBackup 열거 형](#)

3.2.5.1.7. 증분 백업에 활성화된 디스크 찾기

지정된 가상 머신의 경우 **backup** 속성에 따라 필터링된 증분 백업에 활성화된 디스크를 나열할 수 있습니다.

절차

1.

가상 머신에 연결된 디스크를 나열합니다. 예를 들어 ID가 123 인 가상 머신의 경우 이 요청을 보냅니다.

GET /ovirt-engine/api/vms/123/diskattachments

응답에는 모든 **disk_attachment** 오브젝트가 포함되며, 각 오브젝트에는 하나 이상의 디스크 오브젝트가 포함됩니다. 예를 들면 다음과 같습니다.

```
<disk_attachments>
  <disk_attachment>
    ...
    <disk href="/ovirt-engine/api/disks/456" id="456"/>
    ...
  </disk_attachment>
  ...
</disk_attachments>
```

2.

디스크 서비스를 사용하여 이전 단계의 디스크 속성을 확인합니다. 예를 들어 ID 456 이 있는 디스크의 경우 다음 요청을 보냅니다.

GET /ovirt-engine/api/disks/456

응답에는 디스크의 모든 속성이 포함됩니다. 백업 은 **none** 또는 증분식 으로 설정됩니다. 예를 들면 다음과 같습니다.

```
<disk href="/ovirt-engine/api/disks/456" id="456">
  ...
  <backup>incremental</backup>
  ...
</disk>
```

추가 리소스

- [디스크 구조의 백업 특성](#)
- [DiskBackup 열거값](#)

3.2.5.1.8. 전체 백업 시작

전체 백업 후 결과 검사점 ID를 다음 증분 백업의 시작 지점으로 사용할 수 있습니다. **After a full backup you can use the resulting checkpoint ID as the start point in the next incremental**

backup.

실행 중인 가상 머신을 백업할 때 프로세스는 백업 중인 디스크와 동일한 스토리지 도메인에 스크래치 디스크를 생성합니다. 백업 프로세스에서는 이 디스크를 생성하여 백업 중에 실행 중인 가상 시스템에 새 데이터를 작성할 수 있습니다. 이 스크래치 디스크는 백업 중에 관리 포털에서 확인할 수 있습니다. 백업이 완료되면 자동으로 삭제됩니다.

전체 백업을 시작하려면 본문을 사용한 요청 호출이 필요하며 응답이 포함됩니다.

절차

1.

백업할 가상 시스템을 지정하는 요청을 전송합니다. 예를 들어 ID가 **123** 인 가상 머신을 다음과 같이 지정합니다.

```
POST /ovirt-engine/api/vms/123/backups
```

2.

요청 본문에서 백업할 디스크를 지정합니다. 예를 들어 ID **456** 으로 디스크의 전체 백업을 시작하려면 다음 요청 본문을 보냅니다.

```
<backup>
<disks>
  <disk id="456" />
  ...
</disks>
</backup>
```

응답 본문은 다음과 유사해야 합니다.

```
<backup id="789">
<disks>
  <disk id="456" />
  ...
</disks>
<status>initializing</status>
<creation_date>
</backup>
```

응답에는 다음이 포함됩니다.

- **백업 ID**

- 백업의 상태: 백업이 초기화 중임을 나타냅니다.

3.

상태가 준비될 때까지 백업을 폴링합니다. 응답에는 `to_checkpoint_id` 가 포함됩니다. 이 ID를 기록해 두고 다음 증분 백업에서 `from_checkpoint_id` 에 사용합니다.

추가 리소스

- [RHV의 REST API 가이드에 VmBackups 서비스 방법추가](#)

3.2.5.1.9. 증분 백업 시작

지정된 가상 디스크에 대해 전체 백업이 완료되면 해당 디스크에 마지막 백업 이후의 변경 사항만 포함하는 후속 증분 백업입니다. 최신 백업의 `to_checkpoint_id` 값을 요청 본문의 `from_checkpoint_id` 값으로 사용합니다.

실행 중인 가상 머신을 백업할 때 프로세스는 백업 중인 디스크와 동일한 스토리지 도메인에 스크래치 디스크를 생성합니다. 백업 프로세스에서는 이 디스크를 생성하여 백업 중에 실행 중인 가상 시스템에 새 데이터를 작성할 수 있습니다. 이 스크래치 디스크는 백업 중에 관리 포털에서 확인할 수 있습니다. 백업이 완료되면 자동으로 삭제됩니다.

증분 백업 또는 혼합 백업을 시작하려면 본문을 사용한 요청 호출이 필요하며 응답이 포함됩니다.

절차

1.

백업할 가상 시스템을 지정하는 요청을 전송합니다. 예를 들어 ID가 123 인 가상 머신을 다음과 같이 지정합니다.

```
POST /ovirt-engine/api/vms/123/backups
```

2.

요청 본문에서 백업할 디스크를 지정합니다. 예를 들어 ID 456 가 있는 디스크의 증분 백업을 시작하려면 다음 요청 본문을 보냅니다.

```
<backup>
  <from_checkpoint_id>previous-checkpoint-uuid</from_checkpoint_id>
  <disks>
    <disk id="456" />
```

```
...
</disks>
</backup>
```

참고

요청 본문에서 이전 확인 지점에 포함되지 않은 디스크를 포함하는 경우 요청은 이 디스크의 전체 백업도 실행합니다. 예를 들어 ID 789 가 있는 디스크는 아직 백업되지 않았습니다. 위의 요청 본문에 전체 백업을 추가하려면 다음과 같은 요청 본문을 보냅니다.

```
<backup>
  <from_checkpoint_id>previous-checkpoint-
  uuid</from_checkpoint_id>
  <disks>
    <disk id="456" />
    <disk id="789" />
    ...
  </disks>
</backup>
```

응답 본문은 다음과 유사해야 합니다.

```
<backup id="101112">
  <from_checkpoint_id>previous-checkpoint-uuid</from_checkpoint_id>
  <to_checkpoint_id>new-checkpoint-uuid</to_checkpoint_id>
  <disks>
    <disk id="456" />
    <disk id="789" />
    ...
  </disks>
  <status>initializing</status>
  <creation_date>
</backup>
```

응답에는 다음이 포함됩니다.

- 백업 ID입니다.
- 백업에 포함된 디스크의 ID입니다.

- 백업이 초기화 중임을 나타내는 상태입니다.

3. 상태가 준비될 때까지 백업을 폴링합니다. 응답에는 `to_checkpoint_id`가 포함됩니다. 이 ID를 기록해 두고 다음 증분 백업에서 `from_checkpoint_id`에 사용합니다.

추가 리소스

- [RHV용 REST API 가이드](#)에 VmBackups 서비스의 메서드를 추가합니다.

3.2.5.1.10. 백업에 대한 정보 가져오기

새 증분 백업을 시작하는 데 사용할 수 있는 백업에 대한 정보를 가져올 수 있습니다.

VmBackups 서비스의 목록 방법은 백업에 대한 다음 정보를 반환합니다.

- 백업한 각 디스크의 ID입니다.
- 백업의 시작 및 끝 검사점의 ID입니다.
- 백업에 포함된 각 디스크에 대해 백업의 디스크 이미지 ID입니다.
- 백업의 상태입니다.
- 백업이 생성된 날짜입니다.

<status> 값이 준비되면 응답에는 다음 증분 백업에서 <from_checkpoint_id>로 사용해야 하는 <to_checkpoint_id>가 포함되고 디스크 다운로드를 시작하여 가상 머신 스토리지를 백업할 수 있습니다.

절차

- ID가 123인 가상 머신의 ID 456이 있는 백업에 대한 정보를 얻으려면 다음과 같은 요청을 보냅니다.

GET /ovirt-engine/api/vms/456/backups/123

응답에는 ID 456이 포함된 백업과 <from_checkpoint_id> 999 및 <to_checkpoint_id> 666가 포함됩니다. 백업에 포함된 디스크는 <link> 요소에서 참조됩니다.

```
<backup id="456">
  <from_checkpoint_id>999</from_checkpoint_id>
  <to_checkpoint_id>666</to_checkpoint_id>
  <link href="/ovirt-engine/api/vms/456/backups/123/disks" rel="disks"/>
  <status>ready</status>
  <creation_date>
</backup>
```

추가 리소스

- [VmBackups 서비스의 메서드 나열](#)

3.2.5.1.11. 백업의 디스크에 대한 정보 가져오기

백업의 각 디스크에 사용된 백업 모드를 포함하여 백업의 일부인 디스크에 대한 정보를 가져올 수 있습니다. 이는 백업을 다운로드하는 데 사용하는 모드를 결정하는 데 도움이 됩니다.

VmBackupDisks 서비스의 목록 방법은 백업에 대한 다음 정보를 반환합니다.

- 백업한 각 디스크의 ID와 이름입니다.
- 백업에 포함된 각 디스크에 대해 백업의 디스크 이미지 ID입니다.
- 디스크 형식입니다.
- 디스크에서 지원하는 백업 동작입니다.
- 디스크에 대해 가져온 백업 유형(전체/부위)입니다.

절차

-

ID가 123인 가상 머신의 ID 456이 있는 백업에 대한 정보를 얻으려면 다음과 같은 요청을 보냅니다.

GET /ovirt-engine/api/vms/456/backups/123/disks

응답에는 ID 789가 있는 디스크와 디스크 이미지의 ID가 555입니다.

```
<disks>
  <disk id="789">
    <name>vm1_Disk1</name>
    <actual_size>671744</actual_size>
    <backup>incremental</backup>
    <backup_mode>full</backup_mode>
    <format>cow</format>
    <image_id>555</image_id>
    <qcow_version>qcow2_v3</qcow_version>
    <status>locked</status>
    <storage_type>image</storage_type>
    <total_size>0</total_size>
  </disk>
</disks>
```

추가 리소스

- [VmBackupDisks 서비스의 메서드 나열](#)

3.2.5.1.12. 백업 종료

백업을 완료하면 백업을 종료하고, 리소스를 잠금 해제하고, 정리 작업을 수행합니다. 최종 백업 서비스 방법 사용

절차

- ID가 123인 가상 머신에서 ID 456이 있는 디스크 백업을 종료하려면 다음과 같은 요청을 보냅니다.

POST /vms/123/backups/456/finalize

추가 리소스

- [REST API 가이드에서 POST 종료.](#)

3.2.5.1.13. 증분 백업을 위한 이미지 전송 오브젝트 생성

백업을 다운로드할 준비가 되면 백업 애플리케이션에서 증분 백업에 대한 전송을 시작하는 **imagetransfer** 오브젝트를 생성해야 합니다.

이미지 전송 오브젝트를 생성하려면 본문이 있는 요청 호출이 필요합니다.

절차

1.

다음과 같은 요청을 보냅니다.

POST /ovirt-engine/api/imagetransfers

2.

요청 본문에서 다음 매개변수를 지정합니다.

- 디스크 ID.
- 백업 ID.
- 다운로드할 디스크 세트의 방향.
- 디스크 형식을 **raw** 로 설정합니다.

예를 들어 디스크 ID가 123 이고 백업 ID가 456 인 디스크의 백업을 전송하려면 다음 요청 본문을 보냅니다.

```
<image_transfer>
  <disk id="123"/>
  <backup id="456"/>
  <direction>download</direction>
  <format>raw</format>
</image_transfer>
```

추가 리소스

-

RHV의 **REST API** 가이드에서 이미지 전송 오브젝트를 생성하는 방법을 추가합니다.

3.2.5.1.14. 증분 복원을 위한 이미지 전송 오브젝트 생성

증분 백업 **API**를 사용하여 백업된 원시 데이터를 **QCOW2** 형식의 디스크에 복원하려면 백업 애플리케이션에서 **imagetransfer** 오브젝트를 생성해야 합니다.

전송 형식이 **raw** 이고 기본 디스크 형식이 **QCOW2**이면 업로드된 데이터는 스토리지에 쓸 때 즉시 **QCOW2** 형식으로 변환됩니다. **QCOW2** 디스크에서 **RAW** 디스크로 데이터를 업로드하는 것은 지원되지 않습니다.

이미지 전송 오브젝트를 생성하려면 본문이 있는 요청 호출이 필요합니다.

절차

- 1.

다음과 같은 요청을 보냅니다.

```
POST /ovirt-engine/api/imagetransfers
```

- 2.

요청 본문에서 다음 매개변수를 지정합니다.

-

디스크 **ID** 또는 스냅샷 **ID**.

-

업로드할 디스크 세트의 방향입니다.

-

디스크 형식을 **raw** 로 설정합니다.

예를 들어 디스크 **ID**가 **123** 인 디스크의 백업을 전송하려면 다음 요청 본문을 보냅니다.

```
<image_transfer>
<disk id="123"/>
<direction>upload</direction>
<format>raw</format>
</image_transfer>
```

수가 리소스

- **RHV의 REST API 가이드에서 이미지 전송 오브젝트를 생성하는 방법을 추가합니다.**

3.2.5.1.15. 가상 머신의 체크 포인트 나열

요청 호출을 보내면 각 검사 지점에 대한 정보를 포함하여 가상 시스템의 모든 **checkpoints**를 나열할 수 있습니다.

절차

- 가상 시스템을 지정하는 요청을 전송합니다. 예를 들어 ID가 123인 가상 머신을 다음과 같이 지정합니다.

GET /vms/123/checkpoints/

응답에는 모든 가상 시스템 체크포인트가 포함됩니다. 각 검사 지점에는 다음 정보가 포함됩니다.

- 검사점의 디스크입니다.
- 부모 검사점의 ID입니다.
- 검사점 생성 날짜입니다.
- 속한 가상 머신입니다.

예를 들면 다음과 같습니다.

```
<parent_id>, <creation_date> and the virtual machine it belongs to <vm>:
<checkpoints>
  <checkpoint id="456">
    <link href="/ovirt-engine/api/vms/vm-uuid/checkpoints/456/disks" rel="disks"/>
    <parent_id>parent-checkpoint-uuid</parent_id>
    <creation_date>xxx</creation_date>
    <vm href="/ovirt-engine/api/vms/123" id="123"/>
  </checkpoint>
</checkpoints>
```

추가 리소스

- **RHV의 REST API 가이드에 가상 시스템 체크포인트를 나열하는 방법을 나열합니다.**

3.2.5.1.16. 가상 머신의 특정 checkpoint 나열

요청 호출을 보내 가상 머신의 특정 검사 지점에 대한 정보를 나열할 수 있습니다.

절차

- 가상 시스템을 지정하는 요청을 전송합니다. 예를 들어 ID가 123 이고 검사점 ID 456 이 있는 가상 머신을 다음과 같이 지정합니다.

```
GET /vms/123/checkpoints/456
```

응답에는 체크포인트에 대한 다음 정보가 포함됩니다.

- 검사점의 디스크입니다.
- 부모 검사점의 ID입니다.
- 검사점 생성 날짜입니다.
- 속한 가상 머신입니다.

예를 들면 다음과 같습니다.

```
<checkpoint id="456">
  <link href="/ovirt-engine/api/vms/vm-uuid/checkpoints/456/disks" rel="disks"/>
  <parent_id>parent-checkpoint-uuid</parent_id>
  <creation_date>xxx</creation_date>
  <vm href="/ovirt-engine/api/vms/123" id="123"/>
</checkpoint>
```

추가 리소스

•

• RHV의 REST API 가이드에 가상 시스템 체크포인트를 나열하는 방법을 나열합니다.

3.2.5.1.17. checkpoint 제거

DELETE 요청을 보내 가상 머신의 **checkpoint**를 제거할 수 있습니다. 실행 여부에 관계없이 가상 머신의 **checkpoint**를 제거할 수 있습니다.

절차

- 가상 시스템 및 **checkpoint**를 지정하는 요청을 전송합니다. 예를 들어 ID가 123 인 가상 머신과 ID 456 이 있는 검사점을 지정합니다.

DELETE /vms/123/checkpoints/456/

추가 리소스

- [VmCheckpoint 방법 제거](#)

3.2.5.1.18. imageio API를 사용하여 백업 데이터 전송

이미지 전송 API는 이미지 전송을 시작하고 중지합니다. 결과적으로 전송 URL이 표시됩니다.

imageio API를 사용하여 전송 URL에서 데이터를 전송합니다.

imageio API 사용에 대한 전체 정보는 [ovirt-imageio Images API 참조](#)를 참조하십시오.

표 3.2. 증분 백업 및 복원에 사용되는 Imageio Image API 방법

API 요청	설명	Imageio Image API 참조 섹션
OPTIONS /images/{ticket-id} HTTP/1.1	서버에서 지원하는 기능을 확인하기 위해 서버 옵션을 가져옵니다.	옵션보기
GET /images/{ticket-id}/extents	디스크 이미지 콘텐츠 및 할당 또는 증분 백업 중에 변경된 블록에 대한 정보를 가져옵니다. 이 정보를 확장 영역 정보라고 합니다.	추가 정보

API 요청	설명	Imageio Image API 참조 섹션
GET /images/{ticket-id}/extent?context=dirty	이미지 전송을 수행하는 프로그램은 백업에서 변경 사항을 다운로드해야 합니다. 이러한 변경 사항은 더티 확장 영역으로 알려져 있습니다. 변경 사항을 다운로드하려면 다음과 같은 요청을 보냅니다.	EXTENT S→ 예제→ 더티 확장 요청 보기
PUT /images/{ticket-id}	백업 애플리케이션에서는 복원된 데이터를 보유할 기존 디스크가 있는 새 디스크 또는 스냅샷을 생성합니다.	PUT 보기

추가 리소스

Red Hat Virtualization Python SDK에는 백업 전송을 시작하는 데 사용할 수 있는 몇 가지 구현 예제가 포함되어 있습니다.

- [ovirt-imageio Images API 참조](#)
- [디스크 생성](#)
- [Calling imagetransfer.create_transfer\(\)](#)
- [전송 생성을 간소화하는 도우미](#)
- [Red Hat Virtualization Python SDK 사용](#)

3.3. RED HAT SATELLITE를 사용하여 에라타 보기 설정

관리 포털에서는 **Red Hat Virtualization Manager**의 **Red Hat Satellite**에서 에라타를 확인하도록 **Red Hat Virtualization**을 구성할 수 있습니다. 호스트, 가상 시스템, 관리자와 **Red Hat Satellite** 공급자를 연결한 후 사용 가능한 에라타와 그 중요성에 대한 업데이트를 수신하고 적용 시기를 결정할 수 있습니다. **Red Hat Satellite**에 대한 자세한 내용은 [Red Hat Satellite 설명서를 참조하십시오](#).

Red Hat Virtualization 4.4에서는 Red Hat Satellite 6.6으로 에라타 보기를 지원합니다.

사전 요구 사항

- **Satellite 서버를 외부 프로바이더로 추가해야 합니다.**
- **Manager(관리자), 호스트 및 가상 시스템은 모두 해당 FQDN으로 Satellite 서버에 등록해야 합니다. 이렇게 하면 Red Hat Virtualization에서 외부 콘텐츠 호스트 ID를 유지 관리할 필요가 없습니다.**
- **Manager, 호스트 및 가상 시스템을 관리하는 Satellite 계정에는 관리자 권한과 기본 조직 세트가 있어야 합니다.**



참고

Katello 에이전트는 더 이상 사용되지 않으며 향후 Satellite 버전에서 제거됩니다. 프로세스를 마이그레이션하여 원격 실행 기능을 사용하여 클라이언트를 원격으로 업데이트합니다.

Red Hat Virtualization 에라타 구성

Manager, host 및 가상 머신을 Red Hat Satellite 공급자와 연결하려면 다음 작업을 완료합니다.

1. **필요한 Satellite 서버를 Manager에 외부 프로바이더로 추가합니다.**
2. **사용 가능한 에라타를 표시하도록 필요한 호스트를 구성합니다.**
3. **사용 가능한 에라타를 표시하도록 필요한 가상 시스템을 구성합니다.**

Red Hat Virtualization Manager 에라타 보기

1. **Administration(관리) Errata(에라타) 를 클릭합니다.**
2. **Security,Bugs 또는 Enhancements(보안, 버그 또는 개선 사항) 확인란을 선택하여 해당 에라타 유형만 확인합니다.**

추가 리소스

- [호스트에 대한 Satellite 에라타 관리 구성](#)
- **Red Hat Enterprise Linux** 가상 시스템용 가상 시스템 관리 가이드에 [Linux에 게스트 에이전트, 툴 및 드라이버 설치](#).
- **Windows** 가상 시스템용 가상 머신 관리 가이드를 통해 **Windows**에 게스트 에이전트, 툴 및 드라이버 설치.
- [호스트 에라타 보기](#)
- 자세한 내용은 가상 시스템 관리 가이드에서 가상 시스템에 대한 **Satellite** 에라타 보기 구성.
- 가상 시스템 관리 가이드에서 가상 시스템에 대한 **Red Hat Satellite** 에라타 보기.

3.4. 인증서가 만료되기 전에 갱신

Red Hat Virtualization 인증서는 이제 표준 398 일 라이프 사이클을 따르며 1년에 한 번 갱신되어야 합니다.



주의

인증서가 만료되지 않도록 합니다. 만료되면 호스트 및 관리자의 응답이 중지되고 복구는 오류가 발생하기 쉽고 시간이 많이 걸리는 프로세스입니다.

절차

1. 호스트 인증서를 갱신합니다.

- a. 관리 포털에서 **Compute** → **Hosts** (호스트) 를 클릭합니다.
- b. **Management** → **Maintenance** (유지 관리)를 클릭한 다음 **OK** (확인)를 클릭합니다. 가상 시스템이 호스트에서 자동으로 마이그레이션되어야 합니다. 고정되었거나 다른 경우 마이그레이션할 수 없는 경우 해당 파일을 종료해야 합니다.
- c. 호스트가 유지 관리 모드에 있고 이 호스트에 더 이상 가상 시스템이 남아 있지 않으면 **Installation** → **Enroll Certificate** 을 클릭합니다.
- d. 등록이 완료되면 **Management** → 클릭합니다.

2.

Manager 인증서를 갱신합니다.

- a. 셀프 호스트 엔진만 해당: 호스트에 로그인하여 글로벌 유지 관리 모드로 전환합니다.

```
# hosted-engine --set-maintenance --mode=global
```

- b. 셀프 호스트 엔진 및 독립 실행형 관리자: **Manager**에 로그인하고 **engine-setup** 을 실행합니다.

```
# engine-setup --offline
```

engine-setup 스크립트에서 구성 질문을 표시합니다. 질문에 적절히 응답하거나 응답 파일을 사용합니다.

- c. 다음 **engine-setup** 프롬프트 뒤에 **Yes** 를 입력합니다.

```
Renew certificates? (Yes, No) [Yes]:
```

- d. 셀프 호스트 엔진만 해당: 호스트에 로그인하고 글로벌 유지 관리 모드를 비활성화합니다.

```
# hosted-engine --set-maintenance --mode=none
```

만료된 경우 **RHV 호스트 SSL 인증서**를 수동으로 갱신하는 방법은 무엇입니까?

3.5. ANSIBLE을 사용하여 구성 작업 자동화

Ansible은 시스템을 구성하고, 소프트웨어를 배포하고, 롤링 업데이트를 수행하는 데 사용되는 자동화 도구입니다. **Red Hat Virtualization**에는 설치 후 **RHV** 작업(예: 데이터 센터 설정 및 구성, 사용자 관리, 가상 시스템 작업)을 자동화하는 제한된 버전의 **Ansible**이 포함되어 있습니다.

Ansible은 **REST API** 및 **SDK**와 비교하여 **Red Hat Virtualization** 구성을 더 쉽게 자동화하고 다른 **Ansible** 모듈과 통합할 수 있습니다. **Red Hat Virtualization**에 사용할 수 있는 **Ansible** 모듈에 대한 자세한 내용은 **Red Hat Ansible Automation Hub** 설명서의 **oVirt Ansible Collection**을 참조하십시오.



참고

Ansible Tower는 **Ansible**용 웹 인터페이스 및 **REST API**를 통해 액세스할 수 있는 그래픽으로 활성화된 프레임워크입니다. **Ansible Tower**에 대한 지원을 받으려면 **Red Hat Virtualization** 서브스크립션에 속하지 않는 **Ansible Tower** 라이선스가 있어야 합니다.

대체 설치 지침은 **Ansible 설명서** 및 **Ansible** 사용에 대한 정보를 참조하십시오.

3.5.1. oVirt Ansible 컬렉션

ovirt Ansible Collection은 **Red Hat Virtualization** 인프라의 다양한 부분을 관리하기 위한 모듈, 역할 및 플러그인을 제공합니다. 모듈은 **Ansible**과 **Red Hat Virtualization Manager** 간의 통신에 사용됩니다. **Ansible** 역할은 대규모 플레이북을 다른 사용자와 공유할 수 있는 작은 재사용 가능한 파일로 분리하여 **Ansible** 코드를 모듈화하는 방법을 제공합니다. **oVirt Ansible Collection**에 대한 자세한 내용은 **Automation Hub** 설명서를 참조하십시오.

3.5.1.1. RPM 패키지에서 oVirt Ansible 컬렉션 설치

Red Hat Virtualization Manager 리포지토리에서 **oVirt Ansible Collection for Red Hat Virtualization**을 설치할 수 있습니다.

사전 요구 사항

oVirt Ansible Collection을 설치하려면 다음 서브스크립션 채널 중 하나에 가입해야 합니다.

- **Red Hat Virtualization 서브스크립션 사용 - rhv-4.4-manager-for-rhel-8-x86_64-rpms**
- **Red Hat Enterprise Linux 서브스크립션 사용 - rhv-4-tools-for-rhel-8-x86_64-rpms**

절차

1. 다음 명령을 실행하여 **Manager** 시스템에 **oVirt Ansible Collection** 을 설치합니다.

```
# dnf install ovirt-ansible-collection
```

2. 기본적으로 컬렉션은 다음을 위해 설치됩니다.

```
/usr/share/ansible/collections/ansible_collections/redhat/rhv.
```

ovirt-ansible-collection 패키지의 구조는 다음과 같습니다.

```
/usr/share/ansible/collections/ansible_collections/redhat/rhv /usr/share/doc/ovirt-ansible-collection/
```

3.5.1.2. Automation Hub에서 oVirt Ansible 컬렉션 설치

Automation Hub는 **oVirt Ansible Collection** 을 설치하는 데 사용할 수 있는 새로운 곳입니다. 환경을 구성하려면 **oVirt Ansible Collection 설명서**의 지침을 따르십시오.

절차

1. 컬렉션 설치

```
# ansible-galaxy collection install redhat.rhv
```

2. **Automation Hub**는 현재 **RPM** 종속성을 설치하지 않습니다. 플레이북을 실행하는 호스트에 이러한 패키지가 있는지 확인합니다.

- **python3-ovirt-engine-sdk4**

- **`python3-netaddr`**
- **`python3-jmespath`**
- **`python3-passlib`**

3.5.1.3. oVirt Ansible Collection을 사용하여 Red Hat Virtualization 구성

다음 절차에서는 **oVirt Ansible Collection** 을 사용하여 **Red Hat Virtualization**을 구성하는 플레이북을 생성 및 실행하는 방법을 안내합니다. 이 예제에서는 **Ansible**을 사용하여 로컬 시스템의 **Manager**에 연결하고 새 데이터 센터를 생성합니다.

사전 요구 사항

- 플레이북을 실행하는 시스템에 **Python SDK**가 설치되어 있는지 확인합니다.

절차

1.

플레이북을 생성합니다.

```
- name: RHV infrastructure
  hosts: localhost
  connection: local
  gather_facts: false

vars_files:
  # Contains variables to connect to the Manager
  - engine_vars.yml
  # Contains encrypted engine_password variable using ansible-vault
  - passwords.yml

pre_tasks:
  # The use of redhat.rhv before ovirt_auth is to check if oVirt Ansible Collection is correctly
  loaded
  - name: Login to RHV
    redhat.rhv.ovirt_auth:
      hostname: "{{ engine_fqdn }}"
      username: "{{ engine_user }}"
      password: "{{ engine_password }}"
      ca_file: "{{ engine_cafile | default(omit) }}"
      insecure: "{{ engine_insecure | default(true) }}"
    tags:
      - always
```

```

vars:
  data_center_name: mydatacenter
  data_center_description: mydatacenter
  data_center_local: false
  compatibility_version: 4.4

roles:
  - infra
collections:
  - redhat.rhv
post_tasks:
  - name: Logout from RHV
    ovirt_auth:
      state: absent
      ovirt_auth: "{{ ovirt_auth }}"
tags:
  - always

```

oVirt Ansible Collection 에서 **infra Ansible** 역할을 사용하여 **mydatacenter**라는 데이터 센터를 생성했습니다.

3.6. 사용자 및 역할

3.6.1. 사용자 소개

Red Hat Virtualization에는 로컬 도메인과 외부 도메인의 두 가지 유형의 사용자 도메인이 있습니다. **Manager** 설치 프로세스 중에 **internal** 도메인 및 기본 사용자 **admin**이라는 기본 로컬 도메인이 생성됩니다.

ovirt-aaa-jdbc-tool 을 사용하여 내부 도메인에 추가 사용자를 생성할 수 있습니다. 로컬 도메인에서 생성된 사용자 계정을 로컬 사용자라고 합니다. **Red Hat Directory Server, Active Directory, OpenLDAP** 및 기타 지원되는 여러 옵션과 같은 외부 디렉터리 서버를 **Red Hat Virtualization** 환경에 연결하고 외부 도메인으로 사용할 수도 있습니다. 외부 도메인에서 생성된 사용자 계정을 디렉터리 사용자라고 합니다.

로컬 사용자와 디렉터리 사용자 모두 환경에서 작동할 수 있으려면 관리 포털을 통해 적절한 역할과 권한으로 할당해야 합니다. 사용자 역할은 최종 사용자와 관리자의 두 가지 주요 유형이 있습니다. 최종 사용자 역할은 **VM** 포털의 가상 리소스를 사용하고 관리합니다. 관리자 역할은 관리 포털을 사용하여 시스템 인프라를 유지 관리합니다. 이 역할은 가상 시스템 및 호스트와 같은 개별 리소스 또는 클러스터 및 데이터 센터와 같은 개체 계층 구조에 대해 사용자에게 할당할 수 있습니다.

3.6.2. 디렉터리 서버 소개

설치하는 동안 **Red Hat Virtualization Manager**는 내부 도메인에 **admin** 사용자를 생성합니다. 이 사

용자를 **admin@internal** 이라고도 합니다. 이 계정은 처음 환경 구성 시 및 문제 해결을 위해 사용하기 위한 것입니다. 외부 디렉터리 서버를 연결한 후 디렉터리 사용자를 추가하고 적절한 역할 및 권한으로 할당한 후 **admin@internal** 사용자는 필요하지 않은 경우 비활성화할 수 있습니다. 지원되는 디렉터리 서버는 다음과 같습니다.

- **389ds**
- **389DS RFC-2307 스키마**
- **Active Directory**
- **IBM Security Directory Server**
- **IBM Security Directory Server RFC-2307 스키마**
- **FreeIPA**
- **iDM**
- **Novell eDirectory RFC-2307 스키마**
- **OpenLDAP RFC-2307 Schema**
- **OpenLDAP 표준 스키마**
- **Oracle Unified Directory RFC-2307 스키마**
- **RFC-2307 스키마 (Generic)**
- **Red Hat Directory Server (RHDS)**

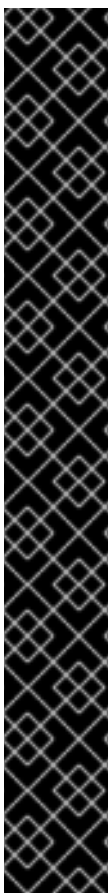
•

RHDS(Red Hat Directory Server) RFC-2307 스키마

•

iPlanet**중요**

Red Hat Virtualization Manager(rhev) 및 **IdM(ipa-server)**을 동일한 시스템에 설치할 수 없습니다. **IdM**은 **Red Hat Virtualization Manager**에 필요한 **mod_ssl** 패키지와 호환되지 않습니다.

**중요**

Active Directory를 디렉터리 서버로 사용하고 템플릿 및 가상 시스템을 생성할 때 **sysprep**를 사용하려는 경우 **Red Hat Virtualization** 관리 사용자를 도메인에 대한 제어 권한을 위임하여 에 위임해야 합니다.

•

도메인에 컴퓨터에 가입

•

그룹 구성원을 수정합니다

Active Directory에서 사용자 계정 만들기에 대한 자세한 내용은 [새 사용자 계정 만들기](#)를 참조하십시오.

Active Directory에서 제어 위임에 대한 자세한 내용은 [조직 단위의 위임 제어](#)를 참조하십시오.

3.6.3. 외부 LDAP 공급자 구성

3.6.3.1. 외부 LDAP 공급자 구성(Interactive Setup)

**참고**

ovirt-engine-extension-aaa-ldap는 더 이상 사용되지 않습니다. 새로 설치하는 경우 **Red Hat Single Sign On**을 사용하십시오. 자세한 내용은 관리 가이드의 [Red Hat Single Sign-On 설치 및 구성](#)을 참조하십시오.

ovirt-engine-extension-aaa-ldap 확장을 사용하면 외부 디렉터리 설정을 쉽게 사용자 지정할 수 있습니다. **ovirt-engine-extension-aaa-ldap** 확장은 다양한 **LDAP** 서버 유형을 지원하며 대부분의 **LDAP** 유형에 대한 설정을 지원하기 위해 대화형 설정 스크립트가 제공됩니다.

LDAP 서버 유형이 대화형 설정 스크립트에 나열되지 않거나 더 많은 사용자 지정을 수행하려면 구성 파일을 수동으로 편집할 수 있습니다. [자세한 내용은 외부 LDAP 공급자 구성](#)을 참조하십시오.

Active Directory에 대한 예제는 [Attaching an Active Directory](#)를 참조하십시오.

사전 요구 사항

- **DNS** 또는 **LDAP** 서버의 도메인 이름을 알아야 합니다.
- **LDAP** 서버와 관리자 간에 보안 연결을 설정하려면 **PEM** 인코딩 **CA** 인증서가 준비되었는지 확인합니다.
- **LDAP** 서버에 대한 검색 및 로그인 쿼리를 수행할 준비가 된 계정 이름과 암호가 하나 이상 있어야 합니다.

절차

1. **Red Hat Virtualization Manager**에서 **LDAP** 확장 패키지를 설치합니다.

```
# dnf install ovirt-engine-extension-aaa-ldap-setup
```

2. **ovirt-engine-extension-aaa-ldap-setup**을 실행하여 대화형 설정을 시작합니다.

```
# ovirt-engine-extension-aaa-ldap-setup
```

3. 해당 번호를 입력하여 **LDAP** 유형을 선택합니다. **LDAP** 서버가 어떤 스키마인지 확실하지 않은 경우 **LDAP** 서버 유형의 표준 스키마를 선택합니다. **Active Directory**의 경우 [Attaching an Active Directory](#)에 있는 절차를 따릅니다.

Available LDAP implementations:

1 - 389ds

2 - 389ds RFC-2307 Schema

3 - Active Directory

4 - IBM Security Directory Server
 5 - IBM Security Directory Server RFC-2307 Schema
 6 - IPA
 7 - Novell eDirectory RFC-2307 Schema
 8 - OpenLDAP RFC-2307 Schema
 9 - OpenLDAP Standard Schema
 10 - Oracle Unified Directory RFC-2307 Schema
 11 - RFC-2307 Schema (Generic)
 12 - RHDS
 13 - RHDS RFC-2307 Schema
 14 - iPlanet
 Please select:

4.

Enter 를 눌러 기본값을 승인하고 **LDAP** 서버 이름에 대한 도메인 이름 확인을 구성합니다.

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.

DNS 정책 방법을 선택합니다.

- 옵션 1의 경우 **/etc/resolv.conf** 에 나열된 **DNS** 서버를 사용하여 **IP** 주소를 확인합니다. **/etc/resolv.conf** 파일이 올바른 **DNS** 서버로 업데이트되었는지 확인합니다.
- 옵션 2의 경우 **FQDN**(정규화된 도메인 이름) 또는 **LDAP** 서버의 **IP** 주소를 입력합니다. **dig** 명령을 **SRV** 레코드와 함께 사용하여 도메인 이름을 확인할 수 있습니다. **SRV** 레코드는 다음 형식을 취합니다.


```
_service._protocol.domain_name
```

예: **dig _ldap._tcp.redhat.com SRV.**
- 옵션 3의 경우 공백으로 구분된 **LDAP** 서버 목록을 입력합니다. 서버의 **FQDN** 또는 **IP** 주소를 사용합니다. 이 정책은 **LDAP** 서버 간에 부하 분산을 제공합니다. 쿼리는 라운드 로빈 알고리즘에 따라 모든 **LDAP** 서버에 분산됩니다.
- 옵션 4의 경우 공백으로 구분된 **LDAP** 서버 목록을 입력합니다. 서버의 **FQDN** 또는 **IP** 주소를 사용합니다. 이 정책은 쿼리에 응답할 첫 번째 **LDAP** 서버를 기본 **LDAP** 서버로 정의합니다. 첫 번째 서버를 사용할 수 없는 경우 쿼리는 목록의 다음 **LDAP** 서버로 이동합니다.

1 - Single server

2 - DNS domain LDAP SRV record
 3 - Round-robin between multiple hosts
 4 - Failover between multiple hosts
 Please select:

6.

LDAP 서버에서 지원하는 보안 연결 방법을 선택하고 PEM 인코딩 CA 인증서를 가져올 방법을 지정합니다.

- 파일을 사용하면 인증서의 전체 경로를 제공할 수 있습니다.
- URL 을 사용하면 인증서의 URL을 지정할 수 있습니다.
- 인라인 을 사용하면 인증서의 내용을 터미널에 붙여넣을 수 있습니다.
- 시스템을 사용하면 모든 CA 파일의 기본 위치를 지정할 수 있습니다.
- 안전하지 않은 경우 인증서 유효성 검사를 건너뛰지만 연결은 계속 TLS를 사용하여 암호화됩니다.

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):

Please enter the password:



참고

LDAPS는 Lightweight Directory Access Protocol over Secure Socket Links의 약어입니다. SSL 연결의 경우 ldaps 옵션을 선택합니다.

7.

검색 사용자 고유 이름(DN)을 입력합니다. 사용자는 디렉터리 서버에서 모든 사용자와 그룹을 찾아볼 수 있는 권한이 있어야 합니다. **LDAP** 주석에 검색 사용자를 지정해야 합니다. 익명 검색이 허용되는 경우 입력 없이 **Enter**를 누릅니다.

Enter search user DN (for example uid=username,dc=example,dc=com or leave empty for anonymous): uid=user1,ou=Users,ou=department-1,dc=example,dc=com
Enter search user password:

8.

기본 DN을 입력합니다.

Please enter base DN (dc=redhat,dc=com) [dc=redhat,dc=com]: ou=department-1,dc=redhat,dc=com

9.

가상 시스템에 대해 **Single Sign-On**을 구성하려면 **Yes** 를 선택합니다. 이 기능은 관리 포털 기능에 대한 **SSO(Single Sign-On)**와 함께 사용할 수 없습니다. 스크립트에서 프로필 이름이 도메인 이름과 일치해야 함을 상기시킵니다. 가상 시스템 관리 가이드의 [가상 시스템에 대한 SSO\(Single Sign-On\)](#) 구성의 지침을 따라야 합니다.

Are you going to use Single Sign-On for Virtual Machines (Yes, No) [Yes]:

10.

프로필 이름을 지정합니다. 프로필 이름은 로그인 페이지에 있는 사용자에게 표시됩니다. 이 예에서는 **redhat.com** 을 사용합니다.



참고

도메인을 구성한 후 프로필 이름을 바꾸려면 `/etc/ovirt-engine/extensions.d/redhat.com-authn.properties` 파일에서 `ovirt.engine.aaa.authn.profile.name` 속성을 편집합니다. `ovirt-engine` 서비스를 다시 시작하여 변경 사항을 적용합니다.

Please specify profile name that will be visible to users: redhat.com

그림 3.1. 관리 포털 로그인 페이지



참고

사용자는 처음 로그인할 때 드롭다운 목록에서 프로필을 선택해야 합니다. 정보는 브라우저 쿠키에 저장되며 다음에 로그인할 때 미리 선택됩니다.

11.

로그인 기능을 테스트하여 **LDAP** 서버가 **Red Hat Virtualization** 환경에 올바르게 연결되어 있는지 확인합니다. 로그인 쿼리의 경우 사용자 이름과 암호를 입력합니다 :

NOTE:

It is highly recommended to test drive the configuration before applying it into engine. Login sequence is executed automatically, but it is recommended to also execute Search sequence manually after successful Login sequence.

Please provide credentials to test login flow:

Enter user name:

Enter user password:

[INFO] Executing login sequence...

...

[INFO] Login sequence executed successfully

12.

사용자 세부 정보가 올바른지 확인합니다. 사용자 세부 정보가 올바르지 않으면 **Abort:**를 선택합니다.

Please make sure that user details are correct and group membership meets expectations (search for PrincipalRecord and GroupRecord titles).

Abort if output is incorrect.

Select test sequence to execute (Done, Abort, Login, Search) [Abort]:

13.

수동으로 검색 기능을 테스트하는 것이 좋습니다. 검색 쿼리의 경우 **Principal for user accounts** 또는 **Group for group accounts**를 선택합니다. 사용자 계정의 그룹 계정 정보를 반환하려면 **Yes to Resolve Groups**를 선택합니다. 3개의 구성 파일이 생성되고 화면 출력에 표시됩니다.

```
Select test sequence to execute (Done, Abort, Login, Search) [Search]: Search
Select entity to search (Principal, Group) [Principal]:
Term to search, trailing '*' is allowed: testuser1
Resolve Groups (Yes, No) [No]:
```

14.

Done(완료)을 선택하여 설정을 완료합니다.

```
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.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-20171004101225-
mmneib.log:
[ INFO ] Stage: Pre-termination
[ INFO ] Stage: Termination
```

15.

ovirt-engine 서비스를 다시 시작합니다. 생성한 프로필을 이제 관리 포털 및 VM 포털 로그인 페이지에서 사용할 수 있습니다. 예를 들어 VM 포털에 로그인하는 것과 같이 LDAP 서버의 사용자 계정에 적절한 역할 및 권한을 할당하려면 **Manager User Tasks**를 참조하십시오.

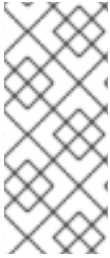
```
# systemctl restart ovirt-engine.service
```



참고

자세한 내용은 `/usr/share/doc/ovirt-engine-extension-aaa-ldap-버전의 LDAP 인증 및 권한 확장 README` 파일을 참조하십시오.

3.6.3.2. Active Directory 연결



참고

ovirt-engine-extension-aaa-ldap 는 더 이상 사용되지 않습니다. 새로 설치하는 경우 **Red Hat Single Sign On**을 사용하십시오. 자세한 내용은 관리 가이드의 **Red Hat Single Sign-On 설치 및 구성**을 참조하십시오.

사전 요구 사항

- **Active Directory forest** 이름을 알아야 합니다. 포레스트 이름은 루트 도메인 이름이라고도 합니다.



참고

ovirt-engine-extension-aaa-ldap-setup 도구를 사용하여 구성할 수 없는 가장 일반적인 **Active Directory** 구성의 예는 `/usr/share/ovirt-engine-extension-aaa-ldap/examples/README.md`에 제공됩니다.

- **Active Directory forest** 이름을 **Manager**의 `/etc/resolv.conf` 파일에 분석할 수 있는 **DNS** 서버를 추가하거나 **Active Directory DNS** 서버를 기록한 후 대화형 설정 스크립트에서 메시지가 표시되면 입력해야 합니다.
- **LDAP** 서버와 관리자 간에 보안 연결을 설정하려면 **PEM** 인코딩 **CA** 인증서가 준비되었는지 확인합니다. 자세한 내용은 **Manager와 LDAP 서버 간 SSL 연결** 설정에서 참조하십시오.
- 익명 검색이 지원되는 경우가 아니면 검색 사용자로 **Active Directory**에서 모든 사용자와 그룹을 찾아볼 수 있는 권한이 있는 사용자를 사용할 수 있어야 합니다. 검색 사용자의 고유 이름 (**DN**)을 기록해 둡니다. **Active Directory**에 관리자를 사용하지 마십시오.
- **Active Directory**에 대한 검색 및 로그인 쿼리를 수행하려면 하나 이상의 계정 이름과 암호가 있어야 합니다.
- **Active Directory** 배포가 여러 도메인에 걸쳐 있는 경우 `/usr/share/ovirt-engine-extension-aaa-ldap/profiles/ad.properties` 파일에 설명된 제한 사항을 숙지하십시오.

절차

1.

Red Hat Virtualization Manager에서 **LDAP** 확장 패키지를 설치합니다.

```
# dnf install ovirt-engine-extension-aaa-ldap-setup
```

2.

ovirt-engine-extension-aaa-ldap-setup 을 실행하여 대화형 설정을 시작합니다.

```
# ovirt-engine-extension-aaa-ldap-setup
```

3.

해당 번호를 입력하여 **LDAP** 유형을 선택합니다. 이 단계 이후의 **LDAP** 관련 질문은 **LDAP** 유형에 따라 다릅니다.

Available LDAP implementations:

- 1 - 389ds
 - 2 - 389ds RFC-2307 Schema
 - 3 - Active Directory
 - 4 - IBM Security Directory Server
 - 5 - IBM Security Directory Server RFC-2307 Schema
 - 6 - IPA
 - 7 - Novell eDirectory RFC-2307 Schema
 - 8 - OpenLDAP RFC-2307 Schema
 - 9 - OpenLDAP Standard Schema
 - 10 - Oracle Unified Directory RFC-2307 Schema
 - 11 - RFC-2307 Schema (Generic)
 - 12 - RHDS
 - 13 - RHDS RFC-2307 Schema
 - 14 - iPlanet
- Please select: 3

4.

Active Directory forest 이름을 입력합니다. **Manager**의 **DNS**에서 포레스트 이름을 확인할 수 없는 경우 스크립트에서 공백으로 구분된 **Active Directory DNS** 서버 이름을 입력하라는 메시지를 표시합니다.

```
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.

LDAP 서버에서 지원하는 보안 연결 방법을 선택하고 **PEM** 인코딩 **CA** 인증서를 가져올 방법을 지정합니다. **file** 옵션을 사용하면 인증서의 전체 경로를 제공할 수 있습니다. **URL** 옵션을 사용하면 인증서에 **URL**을 지정할 수 있습니다. 인라인 옵션을 사용하여 터미널에 인증서의 콘텐츠를 붙여넣습니다. 시스템 옵션을 사용하면 모든 **CA** 파일의 위치를 지정할 수 있습니다. 비보안 옵션을 사용하면 비보안 모드에서 **startTLS**를 사용할 수 있습니다.

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 Links**의 약어입니다. **SSL** 연결의 경우 **ldaps** 옵션을 선택합니다.

PEM 인코딩 **CA** 인증서를 만드는 방법에 대한 자세한 내용은 [Manager와 LDAP 서버 간 SSL 또는 TLS 연결 설정](#)을 참조하십시오.

6.

검색 사용자 고유 이름(DN)을 입력합니다. 사용자는 디렉터리 서버에서 모든 사용자와 그룹을 찾아볼 수 있는 권한이 있어야 합니다. 검색 사용자는 **LDAP** 주석이어야 합니다. 익명 검색이 허용되는 경우 입력 없이 **Enter**를 누릅니다.

Enter search user DN (empty for anonymous):
 cn=user1,ou=Users,dc=test,dc=redhat,dc=com
 Enter search user password:

7.

가상 시스템에 **Single Sign-On** 사용 여부를 지정합니다. 이 기능은 기본적으로 활성화되어 있지만 관리 포털에 대한 **SSO(Single Sign-On)**가 활성화된 경우에는 사용할 수 없습니다. 스크립트에서 프로필 이름이 도메인 이름과 일치해야 함을 상기시킵니다. 가상 시스템 관리 가이드의 [가상 시스템에 대한 SSO\(Single Sign-On\)](#) 구성의 지침을 따라야 합니다.

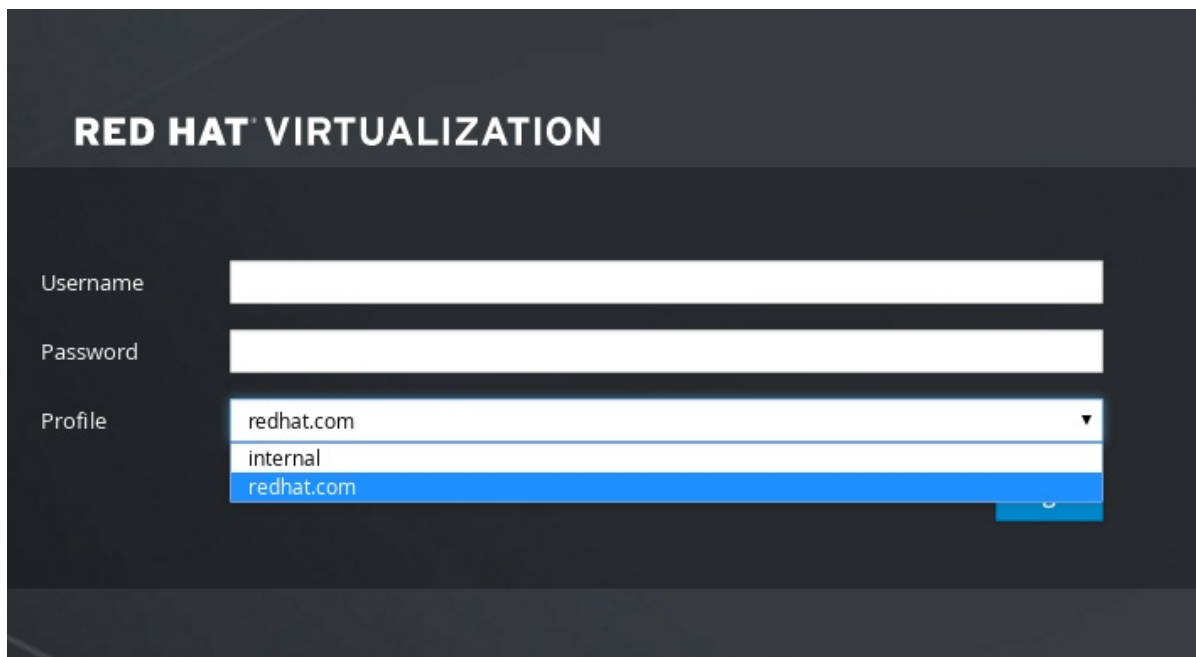
Are you going to use Single Sign-On for Virtual Machines (Yes, No) [Yes]:

8.

프로필 이름을 지정합니다. 프로필 이름은 로그인 페이지에 있는 사용자에게 표시됩니다. 이 예에서는 **redhat.com** 을 사용합니다.

Please specify profile name that will be visible to users:redhat.com

그림 3.2. 관리 포털 로그인 페이지



The image shows the Red Hat Virtualization login page. It has a dark background with the title 'RED HAT VIRTUALIZATION' in white. Below the title, there are three input fields: 'Username', 'Password', and 'Profile'. The 'Profile' field is a dropdown menu with three options: 'redhat.com', 'internal', and 'redhat.com' (which is highlighted in blue). There is a blue button to the right of the 'Profile' dropdown.



참고

사용자는 처음 로그인할 때 드롭다운 목록에서 원하는 프로필을 선택해야 합니다. 정보가 브라우저 쿠키에 저장되고 다음에 로그인할 때 미리 선택됩니다.

9.

검색 및 로그인 기능을 테스트하여 **LDAP** 서버가 **Red Hat Virtualization** 환경에 올바르게 연결되어 있는지 확인합니다. 로그인 쿼리에는 계정 이름과 암호를 입력합니다. 검색 쿼리의 경우 **Principal for user accounts**(사용자 계정에 대해 **Principal**)를 선택하고 그룹 계정의 **Group**(그룹)을 선택합니다. 사용자 계정의 그룹 계정 정보를 반환하려면 **Yes**를 입력하여 그룹을 복구합니다. **Done**(완료)을 선택하여 설정을 완료합니다. 3개의 구성 파일이 생성되고 화면 출력에 표시됩니다.

NOTE:

It is highly recommended to test drive the configuration before applying it into engine.

Login sequence is executed automatically, but it is recommended to also execute Search sequence manually after successful Login 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
```

10.

생성한 프로필을 이제 관리 포털 및 VM 포털 로그인 페이지에서 사용할 수 있습니다. 예를 들어 VM 포털에 로그인하는 것과 같이 **LDAP** 서버의 사용자 계정에 적절한 역할 및 권한을 할당하려면 **Manager User Tasks** 를 참조하십시오.



참고

자세한 내용은 `/usr/share/doc/ovirt-engine-extension-aaa-ldap-버전`의 **LDAP** 인증 및 권한 확장 **README** 파일을 참조하십시오.

3.6.3.3. 외부 LDAP 공급자 구성(수동 방법)



참고

ovirt-engine-extension-aaa-ldap 는 더 이상 사용되지 않습니다. 새로 설치하는 경우 **Red Hat Single Sign On**을 사용하십시오. 자세한 내용은 관리 가이드의 **Red Hat Single Sign-On 설치 및 구성**을 참조하십시오.

ovirt-engine-extension-aaa-ldap 확장에서는 **LDAP** 프로토콜을 사용하여 디렉터리 서버에 액세스 하며 완전히 사용자 지정할 수 있습니다. VM 포털 또는 관리 포털 기능에 대한 **SSO(Single Sign-On)**를 활성화하려는 경우를 제외하고 **Kerberos** 인증은 필요하지 않습니다.

이전 섹션의 대화형 설정 방법이 사용 사례를 다루지 않으면 구성 파일을 수동으로 수정하여 **LDAP** 서버를 연결할 수 있습니다. 다음 절차에서는 일반 세부 정보를 사용합니다. 특정 값은 설정에 따라 다릅니다.

절차

1.

Red Hat Virtualization Manager에서 **LDAP** 확장 패키지를 설치합니다.

```
# dnf install ovirt-engine-extension-aaa-ldap
```

2.

LDAP 구성 템플릿 파일을 **/etc/ovirt-engine** 디렉터리에 복사합니다. 템플릿 파일은 활성 디렉토리(**ad**) 및 기타 디렉토리 유형(단순)에 사용할 수 있습니다. 이 예에서는 간단한 구성 템플릿을 사용합니다.

```
# cp -r /usr/share/ovirt-engine-extension-aaa-ldap/examples/simple/. /etc/ovirt-engine
```

3.

관리 포털 및 VM 포털 로그인 페이지의 사용자에게 표시할 프로필 이름과 일치하도록 구성 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 유형의 주석 처리를 제거하고 도메인 및 암호 필드를 업데이트하여 **LDAP** 속성 구성 파일을 편집합니다.

```
# vi /etc/ovirt-engine/aaa/example.properties
```

예 3.5. 프로필 예: LDAP 서버 섹션

```
# 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}
```

TLS 또는 SSL 프로토콜을 사용하여 **LDAP** 서버와 상호 작용하려면 **LDAP** 서버의 루트 **CA** 인증서를 가져와 공개 키 저장소 파일을 만드는 데 사용합니다. 다음 행의 주석을 제거하고 공개 키 저장소 파일의 전체 경로와 암호를 지정하여 파일에 액세스합니다.



참고

공개 키 저장소 파일 생성에 대한 자세한 내용은 [Manager와 LDAP Server 간의 SSL 또는 TLS 연결 설정](#)을 참조하십시오.

예 3.6. profile: keystore 섹션 예

```
# 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
```

5.

인증 구성 파일을 검토합니다. 관리 포털의 사용자에게 표시되는 프로파일 이름과 **VM** 포털 로그인 페이지는 **ovirt.engine.aaa.authn.profile.name** 에서 정의합니다. 구성 프로파일 위치는 **LDAP** 구성 파일 위치와 일치해야 합니다. 모든 필드는 기본값으로 둘 수 있습니다.

```
# vi /etc/ovirt-engine/extensions.d/example-authn.properties
```

예 3.7. 인증 구성 파일 예

```
ovirt.engine.extension.name = example-authn
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module =
org.ovirt.engine.extension.aaa.Ldap
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.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
```

6.

권한 부여 구성 파일을 검토합니다. 구성 프로파일 위치는 **LDAP** 구성 파일 위치와 일치해야 합니다. 모든 필드는 기본값으로 둘 수 있습니다.

```
# vi /etc/ovirt-engine/extensions.d/example-authz.properties
```

예 3.8. 권한 부여 구성 파일의 예

```
ovirt.engine.extension.name = example-authz
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module =
org.ovirt.engine.extension.aaa ldap
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa ldap.AuthzExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Authz
config.profile.file.1 = ../aaa/example.properties
```

7.

구성 프로파일의 소유권과 사용 권한이 적절한지 확인합니다.

```
# chown ovirt:ovirt /etc/ovirt-engine/aaa/example.properties
# chmod 600 /etc/ovirt-engine/aaa/example.properties
```

8.

engine 서비스를 다시 시작하십시오.

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

9.

생성한 예제 프로파일을 이제 관리 포털 및 **VM** 포털 로그인 페이지에서 사용할 수 있습니다. 예를 들어 **VM** 포털에 로그인하는 것과 같이 **LDAP** 서버의 사용자 계정에 적절한 권한을 부여하려면 [Manager User Tasks](#) 를 참조하십시오.



참고

자세한 내용은 `/usr/share/doc/ovirt-engine-extension-aaa-ldap-버전의 LDAP 인증 및 권한 확장 README` 파일을 참조하십시오.

3.6.3.4. 외부 LDAP 공급자 제거

다음 절차에서는 외부 구성된 **LDAP** 프로바이더 및 해당 사용자를 제거하는 방법을 설명합니다.

절차

1.

LDAP 공급자 구성 파일을 제거하고 기본 이름 **profile1** 을 교체합니다.

```
# rm /etc/ovirt-engine/extensions.d/profile1-authn.properties
# rm /etc/ovirt-engine/extensions.d/profile1-authz.properties
# rm /etc/ovirt-engine/aaa/profile1.properties
```

2.

ovirt-engine 서비스를 다시 시작하십시오.

```
# systemctl restart ovirt-engine
```

3.

관리 포털의 **Users** (사용자) 리소스 탭에서 이 공급업체의 사용자(권한 프로바이더가 **profile 1-authz**인 사용자)를 선택하고 **Remove**(제거)를 클릭합니다.

3.6.4. Single Sign-on용 LDAP 및 Kerberos 구성

SSO(Single Sign-On)를 통해 사용자는 암호를 다시 입력하지 않고도 **VM** 포털 또는 관리 포털에 로그인할 수 있습니다. 인증 자격 증명은 **Kerberos** 서버에서 가져옵니다. 관리 포털과 **VM** 포털에 대한 **SSO(Single Sign-On)**를 구성하려면 **ovirt-engine-extension-aaa-misc** 및 **ovirt-engine-extension-aaa-ldap** 및 두 개의 **Apache** 모듈(**mod_auth_gssapi** 및 **mod_session**)을 구성해야 합니다. **Kerberos**가 포함되지 않은 **Single Sign-On**을 구성할 수 있지만 이 설명서의 범위를 벗어납니다.

참고

VM 포털의 **SSO(Single Sign-On)**가 활성화되면 가상 시스템에 대한 **SSO(Single Sign-On)**가 불가능합니다. **VM** 포털에 대한 **SSO(Single Sign-On)**를 활성화하면 **VM** 포털에서 암호를 수락할 필요가 없으므로 가상 시스템에 로그인하기 위해 암호를 위임할 수 없습니다.

이 예제에서는 다음을 가정합니다.

•

기존 **KDC**(키 배포 센터) 서버는 **Kerberos 5**의 **MIT** 버전을 사용합니다.

•

KDC 서버에 대한 관리 권한이 있습니다.

•

Kerberos 클라이언트는 **Red Hat Virtualization Manager** 및 사용자 시스템에 설치됩니다.

- **kadmin** 유틸리티는 **Kerberos** 서비스 주체 및 키탭 파일을 만드는 데 사용됩니다.

이 절차에는 다음 구성 요소가 포함됩니다.

- **KDC 서버에서**
 - **Red Hat Virtualization Manager**에서 **Apache** 서비스에 대한 서비스 주체 및 키탭 파일을 만듭니다.
- **Red Hat Virtualization Manager에서**
 - 인증 및 권한 부여 확장 패키지와 **Apache Kerberos** 인증 모듈을 설치합니다.
 - 확장 파일을 구성합니다.

3.6.4.1. Apache 서비스에 대한 Kerberos 구성

1. **KDC 서버에서 kadmin** 유틸리티를 사용하여 **Red Hat Virtualization Manager**에서 **Apache** 서비스에 대한 서비스 주체를 만듭니다. 서비스 주체는 **Apache** 서비스의 **KDC**에 대한 참조 ID입니다.

```
# kadmin
kadmin> addprinc -randkey HTTP/fqdn-of-rhevm@REALM.COM
```

2. **Apache** 서비스에 대한 키탭 파일을 생성합니다. **keytab** 파일은 공유 비밀 키를 저장합니다.



참고

engine-backup 명령에는 백업 및 복원 시 **/etc/httpd/http.keytab** 파일이 포함되어 있습니다. **keytab** 파일에 다른 이름을 사용하는 경우 백업하고 복원해야 합니다.

```
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@rhev.example.com:/etc/httpd
```

== VM 포털 또는 관리 포털에 대한 SSO(Single Sign-on) 구성

4.

Red Hat Virtualization Manager에서 keytab의 소유권 및 권한이 적절한지 확인합니다.

```
# chown apache /etc/httpd/http.keytab
# chmod 400 /etc/httpd/http.keytab
```

5.

인증 확장 패키지, LDAP 확장 패키지 및 mod_auth_gssapi 및 mod_session Apache 모듈을 설치합니다.

```
# dnf install ovirt-engine-extension-aaa-misc ovirt-engine-extension-aaa-ldap
mod_auth_gssapi mod_session
```



참고

ovirt-engine-extension-aaa-ldap 는 더 이상 사용되지 않습니다. 새로 설치하는 경우 **Red Hat Single Sign On**을 사용하십시오. 자세한 내용은 관리 가이드의 [Red Hat Single Sign-On 설치 및 구성](#)을 참조하십시오.

6.

SSO 구성 템플릿 파일을 /etc/ovirt-engine 디렉터리에 복사합니다. 템플릿 파일은 Active Directory(ad-ss) 및 기타 디렉토리 유형(Simple-ss)에서 사용할 수 있습니다. 이 예에서는 간단한 SSO 구성 템플릿을 사용합니다.

```
# cp -r /usr/share/ovirt-engine-extension-aaa-ldap/examples/simple-ss/. /etc/ovirt-engine
```

7.

ovirt-ss.conf 를 Apache 구성 디렉터리로 이동합니다.



참고

engine-backup 명령에는 백업 및 복원 시 **/etc/httpd/conf.d/ovirt-ss.conf** 파일이 포함되어 있습니다. 이 파일에 다른 이름을 사용하는 경우 백업하고 복원해야 합니다.


```
# mv /etc/ovirt-engine/aaa/ovirt-sso.conf /etc/httpd/conf.d
```

8.

인증 방법 파일을 검토합니다. 영역이 **keytab** 파일에서 자동으로 가져오기 때문에 이 파일을 편집할 필요가 없습니다.

```
# vi /etc/httpd/conf.d/ovirt-sso.conf
```

예 3.9. 인증 방법 파일 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>
```

9.

관리 포털 및 VM 포털 로그인 페이지의 사용자에게 표시할 프로필 이름과 일치하도록 구성 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
```

10.

LDAP 서버 유형의 주석 처리를 제거하고 도메인 및 암호 필드를 업데이트하여 **LDAP** 속성 구성 파일을 편집합니다.

```
# vi /etc/ovirt-engine/aaa/example.properties
```

예 3.10. 프로필 예: LDAP 서버 섹션

```
# 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}
```

TLS 또는 **SSL** 프로토콜을 사용하여 **LDAP** 서버와 상호 작용하려면 **LDAP** 서버의 루트 **CA** 인증서를 가져와 공개 키 저장소 파일을 만드는 데 사용합니다. 다음 행의 주석을 제거하고 공개 키 저장소 파일의 전체 경로와 암호를 지정하여 파일에 액세스합니다.



참고

공개 키 저장소 파일 생성에 대한 자세한 내용은 [Manager와 LDAP Server 간의 SSL 또는 TLS 연결 설정](#)을 참조하십시오.

예 3.11. profile: keystore 섹션 예

```
# 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
```

11.

인증 구성 파일을 검토합니다. 관리 포털의 사용자에게 표시되는 프로필 이름과 VM 포털 로그인 페이지는 `ovirt.engine.aaa.authn.profile.name` 에서 정의합니다. 구성 프로필 위치는 LDAP 구성 파일 위치와 일치해야 합니다. 모든 필드는 기본값으로 둘 수 있습니다.

```
# vi /etc/ovirt-engine/extensions.d/example-http-authn.properties
```

예 3.12. 인증 구성 파일 예

```
ovirt.engine.extension.name = example-http-authn
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module =
org.ovirt.engine.extension.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.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
```

12.

권한 부여 구성 파일을 검토합니다. 구성 프로필 위치는 LDAP 구성 파일 위치와 일치해야 합니다. 모든 필드는 기본값으로 둘 수 있습니다.

```
# vi /etc/ovirt-engine/extensions.d/example-authz.properties
```

예 3.13. 권한 부여 구성 파일의 예

```
ovirt.engine.extension.name = example-authz
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module =
org.ovirt.engine.extension.aaa.Ldap
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.Ldap.AuthzExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Authz
config.profile.file.1 = ../aaa/example.properties
```

13.

인증 매핑 구성 파일을 검토합니다. 구성 프로필 위치는 LDAP 구성 파일 위치와 일치해야 합니다. 구성 프로필 확장 이름은 인증 구성 파일의 `ovirt.engine.aaa.authn.mapping.plugin` 값과 일치해야 합니다. 모든 필드는 기본값으로 둘 수 있습니다.

```
# vi /etc/ovirt-engine/extensions.d/example-http-mapping.properties
```

예 3.14. 인증 매핑 구성 파일의 예

```
ovirt.engine.extension.name = example-http-mapping
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module = org.ovirt.engine.extension.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.misc.mapping.MappingExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Mapping
config.mapAuthRecord.type = regex
config.mapAuthRecord.regex.mustMatch = true
config.mapAuthRecord.regex.pattern = ^(?<user>.*?)(\\|\\|\\|(?<at>@)(?<suffix>.*?)@.*/(?<realm>@.*/.*))$
config.mapAuthRecord.regex.replacement = ${user}${at}${suffix}
```

14.

구성 파일의 소유권과 사용 권한이 적절한지 확인합니다.

```
# chown ovirt:ovirt /etc/ovirt-engine/aaa/example.properties
```

```
# chown ovirt:ovirt /etc/ovirt-engine/extensions.d/example-http-authn.properties
```

```
# chown ovirt:ovirt /etc/ovirt-engine/extensions.d/example-http-mapping.properties
```

```
# chown ovirt:ovirt /etc/ovirt-engine/extensions.d/example-authz.properties
```

```
# chmod 600 /etc/ovirt-engine/aaa/example.properties
```

```
# chmod 640 /etc/ovirt-engine/extensions.d/example-http-authn.properties
```

```
# chmod 640 /etc/ovirt-engine/extensions.d/example-http-mapping.properties
```

```
# chmod 640 /etc/ovirt-engine/extensions.d/example-authz.properties
```

15.

Apache 서비스와 ovirt-engine 서비스를 다시 시작하십시오.

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

3.6.5. Red Hat Single Sign-On 설치 및 구성

Red Hat Single Sign-On을 인증 방법으로 사용하려면 다음을 수행해야 합니다.

- **Red Hat SSO 설치.**
- **LDAP 그룹 매핑을 구성합니다.**
- **Manager에서 Apache를 구성합니다.**
- **OVN 공급자 자격 증명을 구성합니다.**
- **모니터링 포털 구성(Grafana)**



참고

Red Hat SSO가 구성된 경우 한 번에 단일 권한 부여 프로토콜만 사용할 수 있으므로 이전 LDAP 서명이 작동하지 않습니다.

3.6.5.1. Red Hat SSO 설치

ZIP 파일을 다운로드하고 압축을 풀거나 RPM 파일을 사용하여 Red Hat Single Sign-On을 설치할 수 있습니다.

Red Hat SSO설치의 설치 지침을 따르십시오.

다음 정보를 준비합니다.

- **Open ID Connect 서버의 경로/위치.**
- **올바른 리포지토리의 서브스크립션 채널입니다.**
- **유효한 Red Hat 서브스크립션 로그인 자격 증명.**

3.6.5.2. LDAP 그룹 매핑 구성

절차

1. 다음 정보를 사용하여 **LDAP** 그룹 매퍼를 추가합니다.
 - 이름: **ldapgroups**
 - 매퍼 유형: **group-ldap-mapper**
 - **LDAP** 그룹 DN: **ou=groups,dc=example,dc=com**
 - 그룹 객체 클래스: **groupofuniqueNames** (**LDAP** 서버 설정에 따라이 클래스를 조정)
 - 멤버십 **LDAP** 속성: **uniquemember** (**LDAP** 서버 설정에 따라이 클래스 조정)
2. 저장을 클릭합니다.
3. **Sync LDAP Groups to KeyCloak (LDAP 그룹으로 동기화)**을 클릭합니다.
4. **User Federation Provider** (사용자 페더) 페이지 하단에서 **Synchronize all users**(모든 사용자 동기화)를 클릭합니다.
5. **Clients** (클라이언트) 탭에서 **Add Client** (클라이언트 추가) 탭에서 **ovirt-engine** 을 클라이언트 ID 로 추가하고 엔진 URL 을 루트 URL 로 입력합니다.
6. 클라이언트 프로토콜을 **openid-connect** 로 수정하고 액세스 유형을 기밀 로 수정합니다.
7. **Clients**(클라이언트) 탭의 **Ovirt-engine** > 고급 설정에서 **Access Token Lifespan** 을 늘립니다.
8. **https://rhvm.example.com:443/*** 을 유효한 리디렉션 URL로 추가합니다.

9. 클라이언트 시크릿이 생성되며 **Credentials**(자격 증명) 탭에서 볼 수 있습니다.
10. **Create Mapper Protocol** (매퍼 프로토콜 생성)의 **Clients** (클라이언트) 탭에서 다음 설정을 사용하여 매퍼를 생성합니다.
 - 이름: 그룹
 - 매퍼 유형: **Group Membership**
 - 토큰 클레임 이름: 그룹
 - 전체 그룹 경로: **ON**
 - ID 토큰에 추가: **ON**
 - 액세스 토큰에 추가: **ON**
 - **userinfo**에 추가합니다. **ON**
11. **username**에 대한 **builtin Protocol Mapper**를 추가합니다.
12. **ovirt-engine**, **ovirt-app- api**, **ovirt-app- admin** 및 **ovirt-ext=auth:sequence-priority=~**에 필요한 범위를 만듭니다.
13. 이전 단계에서 생성된 범위를 사용하여 **ovirt-engine** 클라이언트에 대한 선택적 클라이언트 범위를 설정합니다.

3.6.5.3. Manager에서 Apache 구성

1. **mod_auth_openidc** 모듈을 활성화합니다.

```
# dnf module enable mod_auth_openidc:2.3 -y
```

2.

Manager에서 Apache 설정

```
# dnf install mod_auth_openidc
```

3.

다음 콘텐츠를 사용하여 `/etc/httpd/conf.d/`에 새 `httpd` 구성 파일 `ovirt-openidc.conf` 를 만듭니다.

```
LoadModule auth_openidc_module modules/mod_auth_openidc.so
```

```
OIDCProviderMetadataURL https://SSO.example.com/auth/realms/master/.well-known/openid-configuration
OIDCSSLValidateServer Off
```

```
OIDCClientID ovirt-engine
OIDCClientSecret <client_SSO_generated_key>
OIDCRedirectURI https://rhvm.example.com/ovirt-engine/callback
OIDCDefaultURL https://rhvm.example.com/ovirt-engine/login?scope=ovirt-app-admin+ovirt-app-portal+ovirt-ext%3Dauth%3Asequence-priority%3D%7E
```

```
# maps the preferred_username claim to the REMOTE_USER environment variable:
```

```
OIDCRemoteUserClaim <preferred_username>
OIDCCryptoPassphrase <random1234>
```

```
<LocationMatch ^/ovirt-engine/sso/(interactive-login-negotiate|oauth/token-http-auth)/^/ovirt-engine/callback>
  <If "req('Authorization') !~ /^(Bearer|Basic)/i">
```

```
    Require valid-user
    AuthType openid-connect
```

```
    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>
```

```
OIDCOAuthIntrospectionEndpoint
https://SSO.example.com/auth/realms/master/protocol/openid-connect/token/introspect
OIDCOAuthSSLValidateServer Off
OIDCOAuthIntrospectionEndpointParams token_type_hint=access_token
OIDCOAuthClientID ovirt-engine
OIDCOAuthClientSecret <client_SSO_generated_key>
OIDCOAuthRemoteUserClaim sub
```

```
<LocationMatch ^/ovirt-engine/(api$/api)>
  AuthType oauth20
  Require valid-user
</LocationMatch>
```


4.

구성 변경 사항을 저장하려면 **httpd** 및 **ovirt-engine** 을 다시 시작하십시오 :

```
# systemctl restart httpd
# systemctl restart ovirt-engine
```

5.

다음 콘텐츠를 사용하여 **/etc/ovirt -engine/extensions.d/**에 **openidc-authn. properties** 파일을 생성합니다.

```
ovirt.engine.extension.name = openidc-authn
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module = org.ovirt.engine.extension.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.misc.http.AuthnExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Authn
ovirt.engine.aaa.authn.profile.name = openidc-http
ovirt.engine.aaa.authn.authz.plugin = openidc-authz
ovirt.engine.aaa.authn.mapping.plugin = openidc-http-mapping
config.artifact.name = HEADER
config.artifact.arg = OIDC_CLAIM_preferred_username
```

6.

다음 콘텐츠를 사용하여 **/etc/ovirt -engine/extensions.d/**에 **openidc-http-mapping. properties** 파일을 생성합니다.

```
ovirt.engine.extension.name = openidc-http-mapping
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module = org.ovirt.engine.extension.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.misc.mapping.MappingExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Mapping
config.mapAuthRecord.type = regex
config.mapAuthRecord.regex.mustMatch = false
config.mapAuthRecord.regex.pattern = ^(<user>.*?)(\\|(?<at>@)(?<suffix>.*?)@.*?)(?<realm>@.*?)$
config.mapAuthRecord.regex.replacement = ${user}${at}${suffix}
```

7.

다음 콘텐츠를 사용하여 **/etc/ovirt -engine/extensions.d/**에 **openidc-authz. properties** 파일을 생성합니다.

```
ovirt.engine.extension.name = openidc-authz
ovirt.engine.extension.bindings.method = jbossmodule
ovirt.engine.extension.binding.jbossmodule.module = org.ovirt.engine.extension.aaa.misc
ovirt.engine.extension.binding.jbossmodule.class =
org.ovirt.engine.extension.aaa.misc.http.AuthzExtension
ovirt.engine.extension.provides = org.ovirt.engine.api.extensions.aaa.Authz
config.artifact.name.arg = OIDC_CLAIM_preferred_username
config.artifact.groups.arg = OIDC_CLAIM_groups
```

8.

다음 콘텐츠를 사용하여 `/etc/ovirt-engine/engine.conf`에 `99-enable-external-auth.conf` 파일을 생성합니다.

```
ENGINE_SSO_ENABLE_EXTERNAL_SSO=true
ENGINE_SSO_EXTERNAL_SSO_LOGOUT_URI="${ENGINE_URI}/callback"
EXTERNAL_OIDC_USER_INFO_END_POINT=https://SSO.example.com/auth/realms/master/protocol/openid-connect/userinfo
EXTERNAL_OIDC_TOKEN_END_POINT=https://SSO.example.com/auth/realms/master/protocol/openid-connect/token
EXTERNAL_OIDC_LOGOUT_END_POINT=https://SSO.example.com/auth/realms/master/protocol/openid-connect/logout
EXTERNAL_OIDC_CLIENT_ID=ovirt-engine
EXTERNAL_OIDC_CLIENT_SECRET="<client_SSO_generated_key>"
EXTERNAL_OIDC_HTTPS_PKI_TRUST_STORE="/etc/pki/java/cacerts"
EXTERNAL_OIDC_HTTPS_PKI_TRUST_STORE_PASSWORD=""
EXTERNAL_OIDC_SSL_VERIFY_CHAIN=false
EXTERNAL_OIDC_SSL_VERIFY_HOST=false
```

3.6.5.4. OVN 구성

Manager에서 `ovirt-ovn-provider` 를 구성하는 경우 **OVN** 공급자 자격 증명을 구성해야 합니다.

절차

1.

`/etc/ovirt-provider-ovn/conf`에 파일 `20setup-ovirt-provider-ovn.conf`를 만듭니다. 여기서 `user1` 은 **LDAP** 그룹 `ovirt-administrator` 에 속하고 `openidhttp` 는 `aaa-ldap-misc` 에 구성된 프로필입니다.

```
[OVIRT]
# ovirt-admin-user-name=user1@openidhttp
```

2.

ovirt-provider-ovn 을 다시 시작하십시오.

```
# systemctl restart ovirt-provider-ovn
```

3.

관리 포털에 로그인하고 **Administration** → **Providers** (관리 공급업체) 로 이동하여 **ovirt-provider-ovn** 을 선택한 다음 **Edit** (편집)를 클릭하여 **ovn** 공급자의 암호를 업데이트합니다.

3.6.5.5. 모니터링 포털 구성(Grafana)

절차

1.

클라이언트의 유효한 리디렉션 **URL**을 구성합니다.

a.

이전 단계에서 구성한 클라이언트 선택(예: **ovirt-engine**)

b.

모니터링 포털(**Grafana**)에 유효한 리디렉션 **URI**를 추가합니다. 유효한 리디렉션 **URI**:
https://rhvm.example.com:443/ovirt-engine-grafana/login/generic_oauth/

c.

Mappers 탭을 선택합니다.

d.

생성을 클릭하여 새 매퍼를 만들고 다음 필드를 작성합니다.

•

이름: 영역 역할

•

매퍼 유형: 사용자 **Realm** 역할

•

토큰 클레임 이름: **realm_access.roles**

•

Claim JSON 유형: 문자열

2.

Grafana 특정 역할을 구성합니다.

a.

주 메뉴에서 **Roles**(역할)를 선택합니다.

b.

admin,editor,viewer 역할을 추가합니다.

3.

원하는 그룹에 **Grafana** 특정 역할을 할당합니다.

a.

주 메뉴에서 **Groups** (그룹)를 선택하고 원하는 그룹을 선택합니다.

L

D.

Role Mappings (역할 매핑)를 선택합니다.

C.

원하는 역할을 **Available Roles**(사용 가능한 역할)에서 **Assigned Roles** (할당된 역할)로 이동합니다.

4.

Grafana 구성 - 다음과 같이 `/etc/grafana/grafana.ini`에서 `auth.generic_oauth` 섹션을 수정합니다. 필요에 따라 화살표 괄호에서 `<>` 값을 바꿉니다.

```
(...)
##### Generic OAuth #####
[auth.generic_oauth]
name = oVirt Engine Auth
enabled = true
allow_sign_up = true
client_id = ovirt-engine
client_secret = <client-secret-of-RH-SSO>
scopes = openid,ovirt-app-admin,ovirt-app-portal,ovirt-ext=auth:sequence-priority=~
email_attribute_name = email:primary
role_attribute_path = "contains(realm_access.roles[*], 'admin') && 'Admin' ||
contains(realm_access.roles[*], 'editor') && 'Editor' || 'Viewer'"
auth_url = https://<rh-sso-hostname>/auth/realms/<RH-SSO-REALM>/protocol/openid-
connect/auth
token_url = https://<rh-sso-hostname>/auth/realms/<RH-SSO-REALM>/protocol/openid-
connect/token
api_url = https://<rh-sso-hostname>/auth/realms/<RH-SSO-REALM>/protocol/openid-
connect/userinfo
team_ids =
allowed_organizations =
tls_skip_verify_insecure = false
tls_client_cert =
tls_client_key =
tls_client_ca = /etc/pki/ovirt-engine/apache-ca.pem
send_client_credentials_via_post = false
(...)
```

3.6.6. 사용자 권한 부여

3.6.6.1. 사용자 권한 부여 모델

Red Hat Virtualization은 세 가지 구성 요소의 조합에 따라 권한 부여 제어를 적용합니다.

•

작업을 수행하는 사용자

- 수행 중인 작업 유형
- 작업이 수행 중인 객체

3.6.6.2. 사용자 작업

조치를 성공적으로 수행하려면 사용자에게 작업 중인 오브젝트에 적절한 권한이 있어야 합니다. 각 작업 유형에는 해당 권한이 있습니다.

일부 작업은 두 개 이상의 오브젝트에서 수행됩니다. 예를 들어 템플릿을 다른 스토리지 도메인에 복사하면 템플릿과 대상 스토리지 도메인 모두에 영향을 미칩니다. 작업을 수행하는 사용자는 작업에 영향을 미치는 모든 오브젝트에 적절한 권한이 있어야 합니다.

3.6.7. 관리 포털에서 사용자 작업 관리

3.6.7.1. 사용자 추가 및 VM 포털 권한 할당

사용자는 역할 및 권한을 추가하고 권한을 할당하기 전에 이미 생성해야 합니다. 이 절차에서 할당된 역할 및 권한은 VM 포털에 로그인하고 가상 시스템 생성을 시작할 수 있는 권한을 사용자에게 제공합니다. 절차는 그룹 계정도 적용됩니다.

절차

1. 헤더 표시줄에서 **Administration**(관리 → **Configure** (구성) 를 클릭합니다. 그러면 **Configure**(구성) 창이 열립니다.
2. **System Permissions** (시스템 권한)를 클릭합니다.
3. 추가를 클릭합니다. 그러면 **Add System Permission to User** (사용자에게 시스템 권한 추가) 창이 열립니다.
4. **Search** (검색)에서 프로필을 선택합니다. 프로필은 검색할 도메인입니다. 검색 텍스트 필드에 이름 또는 부분을 입력하고 **GO** (이동)를 클릭합니다. 또는 **GO** (이동)를 클릭하여 모든 사용자와 그룹 목록을 봅니다.

5.

적절한 사용자 또는 그룹의 확인란을 선택합니다.

6.

Role to Assign (할당할 역할)에서 할당할 적절한 역할을 선택합니다. **UserRole** 역할은 VM 포털에 로그인할 수 있는 권한을 사용자에게 제공합니다.

7.

OK(확인)를 클릭합니다.

VM 포털에 로그인하여 사용자 계정에 로그인할 권한이 있는지 확인합니다.

3.6.7.2. 사용자 정보 보기

절차

1.

Administration(관리 → **Users** (사용자))를 클릭하여 권한 있는 사용자 목록을 표시합니다.

2.

사용자 이름을 클릭합니다. 그러면 일반적으로 **General**(일반) 탭과 함께 세부 정보 보기가 열립니다. 이때 사용자의 도메인 이름, 이메일 및 상태와 같은 일반 정보가 표시됩니다.

3.

기타 탭에서는 사용자의 그룹, 권한, 할당량 및 이벤트를 볼 수 있습니다.

예를 들어 사용자가 속한 그룹을 보려면 **Directory Groups** (디렉토리 그룹) 탭을 클릭합니다.

3.6.7.3. 리소스에 대한 사용자 권한 보기

사용자에게 특정 리소스 또는 리소스 계층 구조에 대한 권한을 할당할 수 있습니다. 할당된 사용자와 각 리소스에 대한 권한을 볼 수 있습니다.

절차

1.

리소스 이름을 찾아 클릭합니다. 그러면 세부 정보 보기가 열립니다.

2.

Permissions(권한) 탭을 클릭하여 할당된 사용자, 사용자의 역할 및 선택한 리소스에 대한 상속된 권한을 나열합니다.

3.6.7.4. 사용자 제거

사용자 계정이 더 이상 필요하지 않은 경우 **Red Hat Virtualization**에서 제거합니다.

절차

1. **Administration**(관리 → **Users** (사용자) 를 클릭하여 권한 있는 사용자 목록을 표시합니다.
2. 제거할 사용자를 선택합니다. 사용자가 가상 시스템을 실행 중이 아닌지 확인합니다.
3. **Remove**(제거)를 클릭한 다음 **OK**(확인)를 클릭합니다.

사용자는 **Red Hat Virtualization**에서 제거되지만 외부 디렉터리에서는 제거되지 않습니다.

3.6.7.5. 로그인된 사용자 보기

현재 로그인한 사용자를 세션 시간 및 기타 세부 정보와 함께 볼 수 있습니다. **Administration** → **Active User Sessions** (활성 사용자 세션 관리)를 클릭하여 로그인한 각 사용자에게 대한 세션 **DB ID**, 사용자 이름, 권한 부여 공급자, 사용자 **ID**, 소스 **IP**, 세션 시작 시간 및 세션 마지막 활성 시간을 확인합니다.

3.6.7.6. 사용자 세션 종료

현재 로그인한 사용자의 세션을 종료할 수 있습니다.

사용자 세션 종료

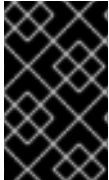
1. **Administration**(관리 → **Active User Sessions** (활성 사용자 세션) 를 클릭합니다.
2. 종료할 사용자 세션을 선택합니다.
3. **Terminate Session** (종료 세션)을 클릭합니다.

4.

OK(확인)를 클릭합니다.

3.6.8. 명령줄에서 사용자 작업 관리

ovirt-aaa-jdbc-tool 툴을 사용하여 내부 도메인에서 사용자 계정을 관리할 수 있습니다. 툴을 사용하여 변경한 내용은 즉시 적용되며 **ovirt-engine** 서비스를 다시 시작할 필요가 없습니다. 전체 사용자 옵션 목록은 **ovirt-aaa-jdbc-tool user --help** 를 실행합니다. 일반적인 예제는 이 섹션에 나와 있습니다.

**중요**

관리자 시스템에 로그인해야 합니다.

3.6.8.1. 새 사용자 생성

새 사용자 계정을 만들 수 있습니다. 선택적 **--attribute** 명령은 계정 세부 정보를 지정합니다. 전체 옵션 목록은 **ovirt-aaa-jdbc-tool 사용자 add --help** 를 실행합니다.

```
# ovirt-aaa-jdbc-tool user add test1 --attribute=firstName=John --attribute=lastName=Doe
adding user test1...
user added successfully
```

관리 포털에 새로 생성된 사용자를 추가하고 사용자에게 적절한 역할 및 권한을 할당할 수 있습니다. 자세한 내용은 [사용자 추가](#) 를 참조하십시오.

3.6.8.2. 사용자 암호 설정

암호를 생성할 수 있습니다. **--password-valid-to** 의 값을 설정해야 합니다. 그렇지 않으면 암호 만료 시간이 현재 시간으로 설정됩니다. 날짜 형식 **isy yyyy-MM-dd HH:mm:ssX**. 이 예에서 **-0800** 은 **-8시간**을 나타냅니다. 자세한 옵션은 **ovirt-aaa-jdbc-tool 사용자 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 **internal** 도메인의 사용자 계정에 대한 암호 정책에는 다음과 같은 제한 사항이 있습니다.

- 최소 6자.
- 사용된 세 개의 이전 암호는 암호 변경 중에 다시 설정할 수 없습니다.

암호 정책 및 기타 기본 설정에 대한 자세한 내용을 보려면 **ovirt-aa-jdbc-tool settings show** 를 실행합니다.

관리자 암호가 업데이트되면 변경 사항을 수동으로 **ovirt-provider-ovn** 으로 전파해야 합니다. 그렇지 않으면 **Red Hat Virtualization Manager**에서 **ovirt-provider-ovn** 의 네트워크를 동기화하는 데 이전 암호를 계속 사용하므로 관리자가 잠깁니다. 새 암호를 **ovirt-provider-ovn** 에 전파하려면 다음을 수행합니다.

1. 관리 포털에서 **Administration(관리) Providers** → (공급업체) 를 클릭합니다.
2. **ovirt-provider-ovn** 을 선택합니다.
3. **Edit(편집)**를 클릭하고 **Password(암호)** 필드에 새 암호를 입력합니다.
4. **Test (테스트)**를 클릭하여 제공한 자격 증명을 사용하여 인증이 성공했는지 테스트합니다.
5. 인증 테스트에 성공하면 **OK(확인)**를 클릭합니다.

3.6.8.3. 사용자 시간 제한 설정

사용자 시간 초과 기간을 설정할 수 있습니다.

```
# engine-config --set UserSessionTimeOutInterval=integer
```

3.6.8.4. 사용자 암호 사전 암호화

ovirt-engine-crypto-tool 스크립트를 사용하여 미리 암호화된 사용자 암호를 생성할 수 있습니다. 이 옵션은 스크립트를 사용하여 데이터베이스에 사용자와 암호를 추가하는 경우 유용합니다.

참고

암호는 관리자 데이터베이스에 암호화된 형태로 저장됩니다. **ovirt-engine-crypto-tool** 스크립트는 모든 암호를 동일한 알고리즘으로 암호화해야 하기 때문에 사용됩니다.

암호가 미리 암호화되면 암호 유효성 테스트를 수행할 수 없습니다. 암호 유효성 검사 정책을 준수하지 않더라도 암호가 수락됩니다.

1.

다음 명령을 실행합니다.

```
# /usr/share/ovirt-engine/bin/ovirt-engine-crypto-tool.sh pbe-encode
```

스크립트에서 암호를 입력하라는 메시지를 표시합니다.

또는 **--password=file:file** 옵션을 사용하여 파일의 첫 번째 행으로 표시되는 단일 암호를 암호화할 수 있습니다. 이 옵션은 자동화에 유용합니다. 다음 예제에서 **file** 은 암호화를 위해 단일 암호를 포함하는 텍스트 파일입니다.

```
# /usr/share/ovirt-engine/bin/ovirt-engine-crypto-tool.sh pbe-encode --password=file:file
```

2.

--encrypted 옵션을 사용하여 **ovirt-aaa-jdbc-tool** 스크립트를 사용하여 새 암호를 설정합니다.

```
# ovirt-aaa-jdbc-tool user password-reset test1 --password-valid-to="2025-08-01 12:00:00-0800" --encrypted
```

3.

암호화된 암호를 입력하고 확인합니다.

```
Password:
Reenter password:
updating user test1...
user updated successfully
```

3.6.8.5. 사용자 정보 보기

자세한 사용자 계정 정보를 볼 수 있습니다.

```
# ovirt-aaa-jdbc-tool user show test1
```

이 명령은 관리 포털의 **Administration Users**(관리 포털)의 **Administration** → **Users** (사용자) 화면보다 더 많은 정보를 표시합니다.

3.6.8.6. 사용자 정보 편집

이메일 주소와 같은 사용자 정보를 업데이트할 수 있습니다.

```
# ovirt-aaa-jdbc-tool user edit test1 --attribute=email=jdoe@example.com
```

3.6.8.7. 사용자 제거

사용자 계정을 제거할 수 있습니다.

```
# ovirt-aaa-jdbc-tool user delete test1
```

관리 포털에서 사용자를 제거합니다. 자세한 내용은 [사용자 제거](#)를 참조하십시오.

3.6.8.8. 내부 관리 사용자 비활성화

engine-setup 중에 생성된 **admin@internal** 사용자를 포함하여 로컬 도메인에서 사용자를 비활성화할 수 있습니다. 기본 **admin** 사용자를 비활성화하기 전에 전체 관리 권한이 있는 **environment**에 하나 이상의 사용자가 있는지 확인합니다.

절차

1. **Red Hat Virtualization Manager**가 설치된 시스템에 로그인합니다.
2. **SuperUser** 역할의 다른 사용자가 환경에 추가되었는지 확인합니다. 자세한 내용은 [사용자 추가](#)를 참조하십시오.

3.

기본 **admin** 사용자를 비활성화합니다.

```
# ovirt-aaa-jdbc-tool user edit admin --flag=+disabled
```



참고

비활성화된 사용자를 활성화하려면 **ovirt-aaa-jdbc-tool user edit username --flag=disabled**를 실행합니다.

3.6.8.9. 그룹 관리

ovirt-aaa-jdbc-tool 툴을 사용하여 내부 도메인의 그룹 계정을 관리할 수 있습니다. 그룹 계정 관리는 사용자 계정 관리와 유사합니다. 전체 그룹 옵션 목록은 **ovirt-aaa-jdbc-tool group --help**를 실행합니다. 일반적인 예제는 이 섹션에 나와 있습니다.

그룹 생성

다음 절차에서는 그룹 계정을 생성하고, 사용자를 그룹에 추가하고, 그룹의 세부 정보를 확인하는 방법을 보여줍니다.

1.

Red Hat Virtualization Manager가 설치된 시스템에 로그인합니다.

2.

새 그룹을 생성합니다.

```
# ovirt-aaa-jdbc-tool group add group1
```

3.

사용자를 그룹에 추가합니다. 사용자를 이미 만들어야 합니다.

```
# ovirt-aaa-jdbc-tool group-manage useradd group1 --user=test1
```



참고

group-manage 옵션의 전체 목록은 **ovirt-aaa-jdbc-tool group-manage --help**를 실행합니다.

4.

그룹 계정 세부 정보 보기:

```
# ovirt-aaa-jdbc-tool group show group1
```

5.

관리 포털에 새로 생성된 그룹을 추가하고 그룹에 적절한 역할과 권한을 할당합니다. 그룹의 사용자는 그룹의 역할 및 권한을 상속받습니다. 자세한 내용은 [사용자 추가](#)를 참조하십시오.

중첩 그룹 생성

다음 절차에서는 그룹 내에 그룹을 만드는 방법을 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.

두 번째 그룹을 첫 번째 그룹에 추가합니다.

```
# ovirt-aaa-jdbc-tool group-manage groupadd group1 --group=group1-1
```

5.

관리 포털에 첫 번째 그룹을 추가하고 그룹에 적절한 역할 및 권한을 할당합니다. 자세한 내용은 [사용자 추가](#)를 참조하십시오.

3.6.8.10. 사용자 및 그룹 쿼리

query 모듈을 사용하면 사용자 및 그룹 정보를 쿼리할 수 있습니다. 전체 옵션 목록은 **ovirt-aaa-jdbc-tool 쿼리 --help**를 실행합니다.

모든 사용자 또는 그룹 계정 정보 나열

다음 절차에서는 모든 계정 정보를 나열하는 방법을 설명합니다.

1. **Red Hat Virtualization Manager**가 설치된 시스템에 로그인합니다.
2. 계정 세부 정보를 나열합니다.

- 모든 사용자 계정 세부 정보:

```
# ovirt-aaa-jdbc-tool query --what=user
```

- 모든 그룹 계정 세부 사항:

```
# ovirt-aaa-jdbc-tool query --what=group
```

필터링된 계정 정보 나열

다음 절차에서는 계정 정보를 나열할 때 필터를 적용하는 방법을 설명합니다.

1. **Red Hat Virtualization Manager**가 설치된 시스템에 로그인합니다.
2. **pattern** 매개 변수를 사용하여 계정 세부 정보를 필터링합니다.

- **j** 문자로 시작하는 이름으로 사용자 계정 세부 정보를 나열합니다.

```
# ovirt-aaa-jdbc-tool query --what=user --pattern="name=j*"
```

- **marketing** 으로 설정된 **department** 속성이 있는 그룹을 나열합니다 :

```
# ovirt-aaa-jdbc-tool query --what=group --pattern="department=marketing"
```

3.6.8.11. 계정 설정 관리

기본 계정 설정을 변경하려면 **ovirt-aaa-jdbc-tool** 설정 모듈을 사용합니다.

계정 설정 업데이트 중

다음 절차에서는 기본 계정 설정을 업데이트하는 방법을 설명합니다.

1. **Red Hat Virtualization Manager**가 설치된 시스템에 로그인합니다.
2. 사용 가능한 모든 설정을 표시하려면 다음 명령을 실행합니다.

```
# ovirt-aaa-jdbc-tool settings show
```

3. 원하는 설정을 변경합니다.

- 이 예제에서는 모든 사용자 계정의 기본 로그인 세션 시간을 60분으로 업데이트합니다. 기본값은 10080분입니다.

```
# ovirt-aaa-jdbc-tool settings set --name=MAX_LOGIN_MINUTES --value=60
```

- 이 예제에서는 사용자 계정을 잠그기 전에 사용자가 수행할 수 있는 실패한 로그인 시도 횟수를 업데이트합니다. 기본값은 5입니다.

```
# ovirt-aaa-jdbc-tool settings set --name=MAX_FAILURES_SINCE_SUCCESS --value=3
```



참고

잠긴 사용자 계정을 잠금 해제하려면 **ovirt-aaa-jdbc-tool user unlock test1** 을 실행합니다.

3.6.9. 추가 로컬 도메인 구성

기본 내부 도메인 이외의 추가 로컬 도메인 생성도 지원됩니다. 이 작업은 **ovirt-engine-extension-**

aaa-jdbc 확장을 사용하여 수행될 수 있으며, 엔터프라이즈 환경에서는 사용 사례가 일반적이 아닐 수도 있지만 외부 디렉터리 서버를 연결하지 않고 여러 도메인을 만들 수 있습니다.

또한 생성된 로컬 도메인은 표준 **Red Hat Virtualization** 업그레이드 중에 자동으로 업그레이드되지 않으며 향후 각 릴리스에 대해 수동으로 업그레이드해야 합니다. 추가 로컬 도메인 생성 및 도메인 업그레이드 방법에 대한 자세한 내용은 `/usr/share/doc/ovirt-engine-extension-aaa-jdbc-버전/README.admin` 에서 **README** 파일을 참조하십시오.



참고

ovirt-engine-extension-aaa-jdbc 확장은 더 이상 사용되지 않습니다. 새로 설치하는 경우 **Red Hat Single Sign On**을 사용하십시오. 자세한 내용은 관리 가이드의 [Red Hat Single Sign-On 설치 및 구성](#)을 참조하십시오.

3.7. 쿼터 및 서비스 수준 계약 정책

3.7.1. 할당량 소개

쿼터는 **Red Hat Virtualization**과 함께 제공되는 리소스 제한 도구입니다. 할당량은 사용자 권한에서 설정한 제한 계층의 최상위에 대한 제한 계층으로 간주될 수 있습니다.

쿼터는 데이터 센터 오브젝트입니다.

쿼터를 사용하면 **Red Hat Virtualization** 환경의 관리자가 메모리, **CPU** 및 스토리지에 대한 사용자 액세스를 제한할 수 있습니다. 할당량은 관리자가 사용자를 할당할 수 있는 메모리 리소스 및 스토리지 리소스를 정의합니다. 결과적으로 사용자는 할당된 리소스만 활용할 수 있습니다. 할당량 리소스가 고갈되면 **Red Hat Virtualization**은 추가 사용자 작업을 허용하지 않습니다.

쿼터에는 두 가지 종류가 있습니다.

표 3.3. 쿼터의 두 가지 종류

할당량 유형	정의
런타임 쿼터	이 할당량은 CPU 및 메모리와 같은 런타임 리소스의 사용을 제한합니다.
스토리지 할당량	이 할당량은 사용 가능한 스토리지 양을 제한합니다.

SELinux와 같은 쿼터에는 다음 세 가지 모드가 있습니다.

표 3.4. 쿼터 모드

쿼터 모드	함수
강제됨	이 모드에서는 감사 모드에서 설정한 할당량에 영향을 미치므로 할당량의 영향을 받는 그룹 또는 사용자로 리소스를 제한합니다.
감사	이 모드에서는 사용자를 차단하지 않고 할당량 위반을 기록하고 할당량을 테스트하는 데 사용할 수 있습니다. 감사 모드에서는 런타임 할당량 양과 해당 사용자의 영향을 받는 사용자가 사용할 수 있는 스토리지 할당량 양을 늘리거나 줄일 수 있습니다.
비활성화됨	이 모드에서는 할당량에서 정의한 런타임 및 스토리지 제한 사항을 비활성화합니다.

사용자가 가상 머신을 실행하려고 하면 가상 머신의 사양은 해당 할당량에 설정된 스토리지 허용값 및 런타임 허용 값과 비교됩니다.

가상 시스템을 시작하면 할당량에서 다루는 모든 실행 중인 가상 시스템의 집계 리소스가 할당량에 정의된 허용값을 초과하면 **Manager**가 가상 시스템 실행을 거부합니다.

사용자가 새 디스크를 생성하면 해당 할당량으로 적용되는 기타 모든 디스크의 집계된 디스크 사용량에 요청된 디스크 크기가 추가됩니다. 새 디스크가 할당량에서 허용하는 양보다 높은 총 집계 디스크 사용량을 사용하는 경우 디스크 생성이 실패합니다.

할당량을 사용하면 동일한 하드웨어의 리소스를 공유할 수 있습니다. 하드 및 소프트웨어 임계값을 지원합니다. 관리자는 할당량을 사용하여 리소스에 임계값을 설정할 수 있습니다. 사용자 관점에서 이러한 임계값은 해당 리소스를 **100%** 사용하므로 표시됩니다. 고객이 이 임계값을 예기치 않게 초과할 때 실패를 방지하기 위해 인터페이스에서 임계값을 간단히 초과할 수 있는 **"grace"** 양을 지원합니다. 임계값을 초과하면 고객에게 경고가 전송됩니다.

중요

할당량은 가상 시스템 실행에 제한이 있습니다. 이러한 제한 사항을 무시하면 가상 시스템 및 가상 디스크를 사용할 수 없는 상황이 발생할 수 있습니다.

할당량이 강제 모드로 실행 중인 경우 할당량이 할당되지 않은 가상 시스템과 디스크를 사용할 수 없습니다.

가상 시스템의 전원을 켜려면 해당 가상 시스템에 할당량을 할당해야 합니다.

가상 시스템의 스냅샷을 생성하려면 가상 시스템과 연결된 디스크에 할당량이 할당되어야 합니다.

가상 시스템에서 템플릿을 생성할 때 템플릿에서 사용할 할당량을 선택하라는 메시지가 표시됩니다. 이를 통해 템플릿(및 템플릿에서 생성된 모든 이후 시스템)을 설정하여 템플릿이 생성되는 가상 시스템 및 디스크와 다른 할당량을 사용할 수 있습니다.

3.7.2. 공유 할당량 및 개별적으로 정의된 할당량

SuperUser 권한이 있는 사용자는 개별 사용자 또는 그룹의 할당량을 생성할 수 있습니다.

Active Directory 사용자에게 대해 그룹 할당량을 설정할 수 있습니다. 10명의 사용자 그룹에 1TB 스토리지의 할당량이 부여되고 10명의 사용자 중 하나가 전체 테라바이트를 채우면 전체 그룹이 할당량을 초과하게 되며, 10명의 사용자 중 어느 것도 해당 그룹과 연결된 스토리지를 사용할 수 없습니다.

개별 사용자의 할당량은 개인용으로만 설정됩니다. 개별 사용자가 스토리지 또는 런타임 할당량을 모두 사용했으면 사용자는 할당량을 초과하게 되며 사용자는 더 이상 자신의 쿼터와 연결된 스토리지를 사용할 수 없게 됩니다.

3.7.3. 할당량 계정

소비자 또는 리소스에 할당량을 할당하면 해당 소비자 또는 스토리지, vCPU 또는 메모리와 관련된 리소스에 의해 각 조치에 따라 할당량 소비 또는 할당량 릴리스가 발생합니다.

할당량은 리소스에 대한 사용자의 액세스를 제한하는 상한값 역할을 하므로 할당량 계산은 사용자의 실제 사용과 다를 수 있습니다. 할당량은 현재 사용량이 아닌 최대 성장 잠재력에 대해 계산됩니다.

예 3.15. 계정 예

사용자는 1개의 vCPU 및 1024MB 메모리의 가상 시스템을 실행합니다. 이 작업은 해당 사용자에게 할당된 할당량 1개 및 1024MB를 사용합니다. 가상 시스템이 1 vCPU 및 1024MB의 RAM이 중지되면 해당 사용자에게 할당된 할당량으로 다시 릴리스됩니다. 런타임 할당량 소비는 실제 소비자 실행 시간에 대해서만 계산됩니다.

사용자가 10GB의 가상 썬 프로비저닝 디스크를 생성합니다. 실제 디스크 사용량은 해당 디스크의 3GB만 실제로 사용 중임을 나타낼 수 있습니다. 그러나 할당량 소비는 해당 디스크의 최대 성장 잠재력인 10GB가 될 수 있습니다.

3.7.4. 데이터 센터에서 쿼터 모드 활성화 및 변경

이 절차에서는 데이터 센터에서 할당량 모드를 활성화하거나 변경합니다. 할당량을 정의하려면 먼저 할당량 모드를 선택해야 합니다. 이 절차의 단계에 따라 관리 포털에 로그인해야 합니다.

감사 모드를 사용하여 할당량을 테스트하여 다음과 같이 작동하는지 테스트합니다. 할당량을 생성하거나 변경하려면 감사 모드에서 할당량이 없어도 됩니다.

절차

1. **Compute(컴퓨팅) → Data Centers (데이터 센터)**를 클릭하고 데이터 센터를 선택합니다.
2. **Edit(편집)**를 클릭합니다.
3. 쿼터 모드 드롭다운 목록에서 할당량 모드를 강제 모드로 변경합니다.
4. **OK(확인)**를 클릭합니다.

테스트 중에 할당량 모드를 감사로 설정하는 경우 할당량 설정이 적용되도록 강제 모드로 변경해야 합니다.

3.7.5. 새 할당량 정책 생성

Audit 또는 **Enforcing** 모드에서 할당량 모드를 활성화했습니다. 데이터 센터에서 리소스 사용량을 관

리할 할당량 정책을 정의하려고 합니다.

절차

1. **Administration(관리) Quota(할당량)** 를 클릭합니다.
2. **추가**를 클릭합니다.
3. **Name(이름)** 및 **Description (설명)** 필드를 작성합니다.
4. 데이터 센터를 선택합니다.
5. **Memory & CPU(메모리 및 CPU)** 섹션에서 녹색 슬라이더를 사용하여 **Cluster Threshold** 를 설정합니다.
6. **Memory & CPU(메모리 및 CPU)** 섹션에서 파란색 슬라이더를 사용하여 **Cluster Grace** 를 설정합니다.
7. **All Clusters(모든 클러스터)** 또는 **Specific Clusters (특정 클러스터)** 라디오 버튼을 클릭합니다. **Specific Clusters (특정 클러스터)**를 선택하는 경우 할당량 정책을 추가할 클러스터의 확인란을 선택합니다.
8. **Edit(편집)**를 클릭합니다. 그러면 **Edit Quota(할당량 편집)** 창이 열립니다.
 - a. **Memory (메모리)** 필드에서 **Unlimited (무제한)** 라디오 버튼(클러스터에서 **Memory** 리소스를 무제한으로 사용하도록 허용) 버튼을 선택하거나 제한을 라디오 버튼을 선택하여 이 할당량에서 설정한 메모리 양을 설정합니다. 단일 라디오 버튼을 선택하는 경우 **MB** 필드에 메모리 할당량(MB)을 입력합니다.
 - b. **CPU** 필드에서 **Unlimited** 라디오 버튼 또는 단일 라디오 버튼을 선택하여 이 할당량으로 설정된 **CPU** 양을 설정합니다. 라디오 제한을 선택하는 경우 **vCpus** 필드에 다수의 **vCPU**를 입력합니다.
 - c. **Edit Quota (할당량 편집)** 창에서 **OK (확인)**를 클릭합니다.

9. **Storage(스토리지)** 섹션에서 녹색 슬라이더를 사용하여 스토리지 임계값 을 설정합니다.
10. **Storage(스토리지)** 섹션에서 파란색 슬라이더를 사용하여 **Storage Grace** 를 설정합니다.
11. **All Storage Domains(모든 스토리지 도메인)** 또는 **Specific Storage Domains (특정 스토리지 도메인)** 라디오 버튼을 클릭합니다. **Specific Storage Domains (특정 스토리지 도메인)**를 선택하는 경우 할당량 정책을 추가할 스토리지 도메인의 확인란을 선택합니다.
12. **Edit(편집)**를 클릭합니다. 그러면 **Edit Quota(할당량 편집)** 창이 열립니다.
 - a. **Storage Quota(스토리지 할당량)** 필드에서 **Unlimited (무제한 스토리지)** 버튼(스토리지 무제한 사용을 허용) 버튼을 선택하거나 제한을 라디오 버튼으로 선택하여 사용자를 제한 할 스토리지 양을 설정합니다. 라디오 제한을 선택하는 경우 **GB** 필드에 스토리지 할당량 크기(GB)를 입력합니다.
 - b. **Edit Quota (할당량 편집)** 창에서 **OK (확인)**를 클릭합니다.
13. **New Quota (새 할당량)** 창에서 **OK (확인)**를 클릭합니다.

3.7.6. 쿼터 임계값 설정 설명

표 3.5. 할당량 임계값 및 유예

설정	정의
클러스터 임계값	데이터 센터당 사용 가능한 클러스터 리소스의 양입니다.
클러스터 Grace	데이터 센터의 클러스터 임계값을 고갈시킨 후 데이터 센터에 사용할 수 있는 클러스터의 양입니다.
스토리지 임계값	데이터 센터당 사용 가능한 스토리지 리소스의 양입니다.
스토리지 컨트롤러	데이터 센터의 스토리지 임계값을 고갈시킨 후 데이터 센터에 사용할 수 있는 스토리지 용량.

할당량이 20% Grace인 100GB로 설정된 경우 120GB의 스토리지를 사용한 후 소비자가 스토리지를 사용하지 못하게 차단됩니다. 동일한 할당량이 70%로 설정된 경우, 소비자는 스토리지 소비가 70GB를

초과하면 경고를 받습니다(하지만 스토리지 사용량 120GB에 도달할 때까지 스토리지를 소비할 수 있습니다.) **"Threshold"** 및 **"Grace"**는 모두 할당량을 기준으로 설정됩니다. **"threshold"**는 "소프트 제한"으로 간주될 수 있으며 이를 초과하면 경고를 생성합니다. **"Grace"**는 "하드 한도"로 간주될 수 있으며 초과하면 더 이상 스토리지 리소스를 사용할 수 없습니다.

3.7.7. 오브젝트에 할당량 할당

가상 머신에 쿼터 할당

1. **Compute(컴퓨팅) → Virtual Machines(가상 시스템)**를 클릭하고 가상 시스템을 선택합니다.
2. **Edit(편집)**를 클릭합니다.
3. **Quota (할당량)** 드롭다운 목록에서 사용할 가상 머신 할당량을 선택합니다.
4. **OK(확인)**를 클릭합니다.

디스크에 할당량 할당

1. **Compute(컴퓨팅) Virtual Machines(가상 시스템)**를 클릭합니다.
2. 가상 시스템의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Disks(디스크)** 탭을 클릭하고 할당량과 연결할 디스크를 선택합니다.
4. **Edit(편집)**를 클릭합니다.
5. **Quota (할당량)** 드롭다운 목록에서 사용할 가상 디스크 할당량을 선택합니다.
6. **OK(확인)**를 클릭합니다.

중요

해당 가상 시스템이 작동하려면 가상 머신과 연결된 모든 오브젝트에 대해 할당량을 선택해야 합니다. 가상 머신과 연결된 오브젝트의 할당량을 선택하지 못하면 가상 머신이 작동하지 않습니다. 이러한 상황에서 **Manager**가 발생하는 오류는 일반이므로 가상 시스템과 연결된 모든 오브젝트와 할당량을 연결하지 않았기 때문에 오류가 발생했는지 확인하기 어렵습니다. 할당량이 할당되지 않은 가상 시스템의 스냅샷을 가져올 수 없습니다. 가상 디스크에 할당량이 할당되지 않은 가상 시스템의 템플릿을 생성할 수 없습니다.

3.7.8. 할당량을 사용하여 사용자별 리소스 제한

다음 절차에서는 할당량을 사용하여 사용자가 액세스할 수 있는 리소스를 제한하는 방법을 설명합니다.

절차

1. **Administration(관리) Quota(할당량)** 를 클릭합니다.
2. 대상 할당량의 이름을 클릭합니다. 그러면 세부 정보 보기가 열립니다.
3. **Consumers (사용자)** 탭을 클릭합니다.
4. **추가**를 클릭합니다.
5. **Search (검색)** 필드에 할당량과 연결할 사용자의 이름을 입력합니다.
6. **GO (이동)**를 클릭합니다.
7. 사용자 이름 옆의 확인란을 선택합니다.
8. **OK(확인)**를 클릭합니다.

잠시 후에 세부 정보 보기의 **Consumers(사용자)** 탭에 사용자가 표시됩니다.

3.7.9. 할당량 편집

다음 절차에서는 기존 할당량을 변경하는 방법을 설명합니다.

절차

1. **Administration(관리 → Quota (할당량))** 를 클릭하고 할당량을 선택합니다.
2. **Edit(편집)**를 클릭합니다.
3. 필요에 따라 필드를 편집합니다.
4. **OK(확인)**를 클릭합니다.

3.7.10. 할당량 제거

다음 절차에서는 할당량을 제거하는 방법을 설명합니다.

절차

1. **Administration(관리 → Quota (할당량))** 를 클릭하고 할당량을 선택합니다.
2. **Remove(제거)**를 클릭합니다.
3. **OK(확인)**를 클릭합니다.

3.7.11. 서비스 수준 계약 정책 시행

다음 절차에서는 서비스 수준 계약 **CPU** 기능을 설정하는 방법을 설명합니다.

절차

1. **Compute(컴퓨팅) Virtual Machines(가상 시스템)** 를 클릭합니다.

2.

New (새로 만들기)를 클릭하거나 가상 시스템을 선택한 다음 **Edit(편집)**를 클릭합니다.

3.

Resource Allocation(리소스 할당) 탭을 클릭합니다.

4.

CPU 공유를 지정합니다. 가능한 옵션은 낮음, 중간, 높음, 사용자 지정, 비활성화 입니다. 가상 머신은 **High(고급)**로 설정된 공유 수를 두 배로 수신하고 **media(중간)**로 설정된 가상 시스템은 **Low(낮음)**로 설정된 가상 시스템 수의 두 배를 받습니다. **Disable** 은 **VDSM**에 이전 알고리즘을 사용하여 공유 분산을 결정하도록 지시합니다. 일반적으로 이러한 조건에 따라 계산된 공유 수는 1020입니다.

이제 사용자의 **CPU** 사용량이 설정한 정책에 의해 관리됩니다.

3.8. 이벤트 알림

3.8.1. 관리 포털에서 이벤트 알림 구성

Red Hat Virtualization Manager는 **Red Hat Virtualization Manager**가 관리하는 환경에서 특정 이벤트가 발생하는 경우 이메일을 통해 지정된 사용자에게 알릴 수 있습니다. 이 기능을 사용하려면 메시지를 전송하도록 메일 전송 에이전트를 설정해야 합니다. 관리 포털을 통해 이메일 알림만 구성할 수 있습니다. 관리자 시스템에 **SNMP** 트랩을 구성해야 합니다.

절차

1.

Manager에서 자동화된 메시지를 수락하고 배포 목록에 전달할 수 있는 이메일 서버에 액세스할 수 있는지 확인합니다.

2.

Administration(관리 → Users (사용자)) 를 클릭하고 사용자를 선택합니다.

3.

사용자의 **User Name(사용자 이름)**을 클릭하여 세부 정보 페이지로 이동합니다.

4.

Event Notifier (이벤트 알림기) 탭에서 **Manage Events(이벤트 관리)**를 클릭합니다.

5.

이벤트를 보려면 **Expand All(모두 확장 확장)** 버튼 또는 제목별 확장 버튼을 사용합니다.

6.

적절한 확인란을 선택합니다.

7.

Mail Recipient (메일 수신자) 필드에 이메일 주소를 입력합니다.



참고

이메일 주소는 텍스트 메시지 이메일 주소(예:)이거나 이메일 주소와 텍스트 메시지 이메일 주소를 포함하는 이메일 그룹 주소가 될 수 있습니다.

8.

OK(확인)를 클릭합니다.

9.

Manager 시스템에서 **ovirt-engine-notifier.conf**를 **90-email-notify.conf**라는 새 파일에 복사합니다.

```
# cp /usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf
/etc/ovirt-engine/notifier/notifier.conf.d/90-email-notify.conf
```

10.

90-email-notify.conf를 편집하여 **EMAIL** 알림 섹션을 제외한 모든 내용을 삭제합니다.

11.

아래 예제와 같이 올바른 이메일 변수를 입력합니다. 이 파일은 원본 **ovirt-engine-notifier.conf** 파일의 값을 재정의합니다.

```
#-----#
# EMAIL Notifications #
#-----#

# The SMTP mail server address. Required.
MAIL_SERVER=myemailserver.example.com

# The SMTP port (usually 25 for plain SMTP, 465 for SMTP with SSL, 587 for SMTP with
# TLS)
MAIL_PORT=25

# Required if SSL or TLS enabled to authenticate the user. Used also to specify 'from' user
# address if mail server
# supports, when MAIL_FROM is not set. Address is in RFC822 format
MAIL_USER=

# Required to authenticate the user if mail server requires authentication or if SSL or TLS is
# enabled
SENSITIVE_KEYS="${SENSITIVE_KEYS},MAIL_PASSWORD"
```

```
MAIL_PASSWORD=
```

```
# Indicates type of encryption (none, ssl or tls) should be used to communicate with mail server.
```

```
MAIL_SMTP_ENCRYPTION=none
```

```
# If set to true, sends a message in HTML format.
```

```
HTML_MESSAGE_FORMAT=false
```

```
# Specifies 'from' address on sent mail in RFC822 format, if supported by mail server.
```

```
MAIL_FROM=rhev2017@example.com
```

```
# Specifies 'reply-to' address on sent mail in RFC822 format.
```

```
MAIL_REPLY_TO=
```

```
# Interval to send smtp messages per # of IDLE_INTERVAL
```

```
MAIL_SEND_INTERVAL=1
```

```
# Amount of times to attempt sending an email before failing.
```

```
MAIL_RETRIES=4
```



참고

자세한 옵션은 `/etc/ovirt-engine/notifier/notifier.conf.d/README` 를 참조하십시오.

12.

ovirt-engine-notifier 서비스를 활성화하고 다시 시작하여 변경한 내용을 활성화합니다.

```
# systemctl daemon-reload
```

```
# systemctl enable ovirt-engine-notifier.service
```

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

이제 지정된 사용자가 **Red Hat Virtualization** 환경의 이벤트를 기반으로 이메일을 받습니다. 선택한 이벤트는 해당 사용자의 **Event Notifier** (이벤트 알림기) 탭에 표시됩니다.

3.8.2. 관리 포털에서 이벤트 알림 취소

사용자가 불필요한 이메일 알림을 구성했으며 이를 취소하려고 합니다.

절차

1.

Administration(관리) Users(사용자) 를 클릭합니다.

2.

사용자의 **User Name**(사용자 이름)을 클릭합니다. 그러면 세부 정보 보기가 열립니다.

3.

Event Notifier (이벤트 알림기) 탭을 클릭하여 사용자가 이메일 알림을 수신하는 이벤트를 나열합니다.

4.

Manage Events (이벤트 관리)를 클릭합니다.

5.

이벤트를 보려면 **Expand All**(모두 확장) 버튼 또는 제목별 확장 버튼을 사용합니다.

6.

해당 이벤트 알림을 제거하려면 적절한 확인란을 지웁니다.

7.

OK(확인)를 클릭합니다.

3.8.3. ovirt-engine-notifier.conf의 이벤트 알림 매개 변수

이벤트 알림기 구성 파일은 `/usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf` 에서 찾을 수 있습니다.

표 3.6. ovirt-engine-notifier.conf variables

변수 이름	Default	비고
SENSITIVE_KEYS	none	섬표로 구분되어 기록되지 않는 키 목록입니다.
JBOSS_HOME	/opt/rh/eap7/root/usr/share/wildfly	Manager에서 사용하는 JBoss 애플리케이션 서버의 위치.
ENGINE_ETC	/etc/ovirt-engine	Manager에서 사용하는 etc 디렉토리의 위치.
ENGINE_LOG	/var/log/ovirt-engine	Manager에서 사용하는 logs 디렉토리의 위치.
ENGINE_USR	/usr/share/ovirt-engine	Manager에서 사용하는 usr 디렉토리의 위치입니다.
ENGINE_JAVA_MODULEPATH	\${ENGINE_USR}/modules	JBoss 모듈이 추가되는 파일 경로입니다.

변수 이름	Default	비고
NOTIFIER_DEBUG_ADDRESS	none	알림기에서 사용하는 Java 가상 시스템의 원격 디버깅을 수행하는 데 사용할 수 있는 머신의 주소입니다.
NOTIFIER_STOP_TIME	30	서비스가 시간 초과되는 시간(초)입니다.
NOTIFIER_STOP_INTERVAL	1	시간 제한 카운터가 증가하게 되는 시간(초)입니다.
INTERVAL_IN_SECONDS	120	구독자에게 메시지를 디스패치하는 인스턴스 간 간격(초)입니다.
IDLE_INTERVAL	30	우선순위가 낮은 작업이 수행될 간격(초)입니다.
DAYS_TO_KEEP_HISTORY	0	이 변수는 디스패치된 이벤트의 날짜 수를 기록 테이블에 보존합니다. 이 변수를 설정하지 않으면 이벤트가 기록 테이블에 무기한 유지됩니다.
FAILED_QUERIES_NOTIFICATION_THRESHOLD	30	알림 이메일이 전송된 실패한 쿼리 수입니다. 알림을 가져온 첫 번째 실패 후에는 알림 이메일이 전송되며, 이 변수에서 지정한 실패 수에 도달할 때마다 한 번씩 전송됩니다. 값을 0 또는 1 로 지정하면 실패마다 이메일이 전송됩니다.
FAILED_QUERIES_NOTIFICATION_RECIPIENTS	none	알림 이메일을 보낼 수신자의 이메일 주소입니다. 이메일 주소는 쉼표로 구분해야 합니다. 이 항목은 FILTER 변수에서 더 이상 사용되지 않습니다.
DAYS_TO_SEND_ON_STARTUP	0	알림 프로그램이 시작될 때 처리되고 전송할 이전 이벤트의 일 수입니다.
필터	제외:*	이메일 알림의 트리거 및 수신자를 결정하는 데 사용되는 알고리즘입니다. 이 변수의 값은 include 또는 exclude , 이벤트 및 수신자의 조합으로 구성됩니다. 예를 들어 :VDC_START(smtp:mail@example.com) \${FILTER}

변수 이름	Default	비고
MAIL_SERVER	none	SMTP 메일 서버 주소. 필수 항목입니다.
MAIL_PORT	25	통신에 사용되는 포트입니다. 사용 가능한 값에는 일반 SMTP의 경우 25 , SSL을 사용하는 SMTP의 경우 465 , TLS를 사용하는 SMTP의 경우 587 이 포함됩니다.
MAIL_USER	none	사용자를 인증하기 위해 SSL이 활성화된 경우 이 변수를 설정해야 합니다. 이 변수는 MAIL_FROM 변수가 설정되지 않은 경우 "from" 사용자 주소를 지정하는 데도 사용됩니다. 일부 메일 서버는 이 기능을 지원하지 않습니다. 주소는 RFC822 형식입니다.
SENSITIVE_KEYS	\${SENSITIVE_KEYS},MAIL_PASSWORD	메일 서버에 인증이 필요한 경우 또는 SSL 또는 TLS가 활성화된 경우 사용자를 인증하는 데 필요합니다.
MAIL_PASSWORD	none	메일 서버에 인증이 필요한 경우 또는 SSL 또는 TLS가 활성화된 경우 사용자를 인증하는 데 필요합니다.
MAIL_SMTP_ENCRYPTION	none	통신에 사용할 암호화 유형입니다. 가능한 값은 none,ssl,tls 입니다.
HTML_MESSAGE_FORMAT	false	이 변수가 true 로 설정된 경우 메일 서버는 HTML 형식으로 메시지를 전송합니다.
MAIL_FROM	none	이 변수는 메일 서버에서 지원하는 경우 RFC822 형식의 발신자 주소를 지정합니다.
MAIL_REPLY_TO	none	이 변수는 메일 서버가 지원하는 경우 전송된 메일의 RFC822 형식의 응답 주소를 지정합니다.
MAIL_SEND_INTERVAL	1	각 IDLE_INTERVAL에 대해 전송할 SMTP 메시지 수
MAIL_RETRIES	4	실패하기 전에 이메일 전송을 시도하는 횟수입니다.

변수 이름	Default	비고
SNMP_MANAGERS	none	SNMP 관리자 역할을 할 시스템의 IP 주소 또는 정규화된 도메인 이름입니다. 항목은 공백으로 구분해야 하며 포트 번호를 포함할 수 있습니다. 예를 들어 manager1.example.com manager2.example.com:164
SNMP_COMMUNITY	공용	(SNMP 버전 2만) SNMP 커뮤니티입니다.
SNMP_OID	1.3.6.1.4.1.2312.13.1.1	경고에 대한 기본 트랩 개체 식별자입니다. 이 OID가 정의된 경우 모든 트랩 유형이 이벤트 정보를 사용하여 SNMP 관리자에게 전송됩니다. 기본 트랩을 변경하면 생성된 트랩이 관리자의 관리 정보 기반을 준수하지 못합니다.
SNMP_VERSION	2	사용할 Keycloak 버전을 정의합니다. 중첩 버전 2 및 버전 3 트랩이 지원됩니다. 가능한 값은 다음과 같습니다. 2 또는 3 .
SNMP_ENGINE_ID	none	(SNMPv3) flushv3 트랩에 사용되는 관리자 ID입니다. 이 ID는 SNMP를 통해 연결된 장치의 고유 식별자입니다.
SNMP_USERNAME	none	(SNMPv3) flushv3 트랩에 사용되는 사용자 이름입니다.
SNMP_AUTH_PROTOCOL	none	(SNMPv3) SNMPv3 권한 부여 프로토콜. 가능한 값은 다음과 같습니다. MD5, SHA
SNMP_AUTH_PASSPHRASE	none	(SNMPv3) flush_SECURITY_LEVEL이 AUTH_NOPRIV 및 AUTH_PRIV로 설정된 경우 사용되는 암호입니다.

변수 이름	Default	비고
SNMP_PRIVACY_PROTOCOL	none	(SNMPv3) flushv3 개인 정보 보호 프로토콜. 가능한 값은 다음과 같습니다. AES128, AES192, AES256  중요 AES192 및 AES256은 RFC3826에 정의되어 있지 않으므로 Keycloak 서버가 해당 프로토콜을 활성화하기 전에 해당 프로토콜을 지원하는지 확인합니다.
SNMP_PRIVACY_PASSPHRASE	none	flush SECURITY_LEVEL 이 AUTH_PRIV 로 설정된 경우 사용되는 flushv3 개인 정보 보호 암호입니다.
SNMP_SECURITY_LEVEL	1	(SNMPv3) 블로그의 보안 수준입니다. 가능한 값: * 1 - NOAUTH_NOPRIV * 2 - AUTH_NOPRIV * 3 - AUTH_PRIV
ENGINE_INTERVAL_IN_SECONDS	300	Manager가 설치된 시스템을 모니터링하는 간격(초)입니다. 간격은 모니터링이 완료된 시간부터 측정됩니다.
ENGINE_MONITOR_RETRIES	3	알림 프로그램이 실패 후 지정된 간격으로 Manager가 설치된 시스템의 상태를 모니터링하려고 하는 횟수입니다.
ENGINE_TIMEOUT_IN_SECONDS	30	알림 프로그램이 실패 후 지정된 간격으로 Manager를 설치하는 시스템의 상태를 모니터링하려고 시도하기 전에 대기하는 시간(초)입니다.
IS_HTTPS_PROTOCOL	false	JBoss가 보안 모드에서 실행 중인 경우 이 항목을 true 로 설정해야 합니다.

변수 이름	Default	비고
SSL_PROTOCOL	TLS	SSL을 활성화할 때 JBoss 구성 컨텍스트에서 사용하는 프로토콜입니다.
SSL_IGNORE_CERTIFICATE_ERRORS	false	JBoss가 보안 모드에서 실행되고 있고 SSL 오류가 무시되는 경우 이 값을 true 로 설정해야 합니다.
SSL_IGNORE_HOST_VERIFICATION	false	JBoss가 보안 모드에서 실행 중이고 호스트 이름 확인을 무시하는 경우 이 값을 true 로 설정해야 합니다.
REPEAT_NON_RESPONSIVE_NOTIFICATION	false	이 변수는 Manager가 설치된 시스템이 응답하지 않는 경우 반복된 실패 메시지가 구독자에게 전송되는지 여부를 지정합니다.
ENGINE_PID	/var/lib/ovirt-engine/ovirt-engine.pid	Manager의 PID 경로 및 파일 이름입니다.

3.8.4. SNMP 트랩을 전송하도록 Red Hat Virtualization Manager 구성

SNMP(Simple Network Management Protocol) 트랩을 하나 이상의 외부 **Keycloak** 관리자에게 보내도록 **Red Hat Virtualization Manager**를 구성합니다. **SNMP** 트랩에는 시스템 이벤트 정보가 포함되어 있으며 **Red Hat Virtualization** 환경을 모니터링하는 데 사용됩니다. **SNMP** 관리자에게 전송되는 트랩 수와 유형을 **Red Hat Virtualization Manager** 내에서 정의할 수 있습니다.

Red Hat Virtualization은 **SNMP** 버전 2 및 버전 3을 지원합니다. 중첩 버전 3은 다음과 같은 보안 수준을 지원합니다.

NoAuthNoPriv

SCSI 트랩은 권한 부여 또는 개인 정보 보호없이 전송됩니다.

AuthNoPriv

SCSI 트랩은 암호 권한 부여와 함께 전송되지만 개인 정보는 제공되지 않습니다.

AuthPriv

SCSI 트랩은 암호 권한 부여 및 개인 정보를 사용하여 전송됩니다.

사전 요구 사항

- 하나 이상의 외부 **SNMP** 관리자가 트랩을 수신하도록 구성되어 있습니다.
- **SNMP** 관리자 역할을 할 시스템의 **IP** 주소 또는 정규화된 도메인 이름입니다. 선택적으로 **Manager**가 트랩 알람을 수신하는 포트를 결정합니다. 기본값은 **UDP** 포트 **162**입니다.
- **SNMP** 커뮤니티(**SNMP** 버전 2만 해당). 여러 **SNMP** 관리자는 단일 커뮤니티에 속할 수 있습니다. 관리 시스템과 에이전트는 동일한 커뮤니티 내에서만 통신할 수 있습니다. 기본 커뮤니티는 공용입니다.
- 경고에 대한 트랩 개체 식별자입니다. **Red Hat Virtualization Manager**는 **1.3.6.1.4.1.2312.13.1.1**의 기본 **OID**를 제공합니다. 이 **OID**가 정의된 경우 모든 트랩 유형이 이벤트 정보를 사용하여 **SNMP** 관리자에게 전송됩니다. 기본 트랩을 변경하면 생성된 트랩이 관리자의 관리 정보 기반을 준수하지 못합니다.
- **Thunderbolt** 버전 3의 경우, 보안 수준 1, 2, 3에 대해 **SNMP** 사용자 이름입니다.
- **SNMP** 암호(**SNA** 버전 3의 경우, 보안 수준 2 및 3).
- **SNMP** 버전 3, 보안 수준 3용 **SNMP** 개인 암호입니다.

참고

Red Hat Virtualization Manager는 `/usr/share/doc/ovirt-engine/mibs/OVIRT-MIB.txt` 및 `/usr/share/doc/ovirt-engine/mibs/REDHAT-MIB.txt.txt`의 관리 정보 기반을 제공합니다. 계속하기 전에 **SNMP** 관리자에 **MIB**를 로드합니다.

기본 **SNMP** 구성 값은 이벤트 알람 데몬 구성 파일 `/usr/share/ovirt-engine/services/ovirt-engine-notifier.conf`의 **Manager**에 있습니다. 다음 절차에 설명된 값은 이 파일에 제공된 기본값 또는 예제 값을 기반으로 합니다. 업그레이드와 같은 시스템 변경 사항이 이 파일에 대한 변경 사항이 제거될 수 있으므로 이 파일을 직접 편집하지 마십시오. 대신 이 파일을 `/etc/ovirt-engine/notifier.conf.d/<정수>-snmp.conf.d/<정수>-snmp.conf`. 여기서 <정수>는 파일이 실행되어야 하는 우선 순위를 나타내는 번호입니다.

절차

1.

Manager에서 파일 이름 **<integer>-snmp.conf**, 여기서 **<integer>** 은 파일이 처리되는 순서를 나타내는 정수입니다. 예를 들면 다음과 같습니다.

```
# vi /etc/ovirt-engine/notifier/notifier.conf.d/20-snmp.conf
```

작은 정보

이벤트 알림 데몬 구성 파일 **/usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf** 에서 기본 **Keycloak** 설정을 복사합니다. 이 파일에는 모든 설정에 대한 인라인 주석이 포함되어 있습니다.

2.

다음 예제의 형식에 **OID (SNMP 버전 2만 해당)** 및 **verynMP 커뮤니티 (SNMP 버전 2에만 해당)**를 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 버전 2(기본값) 또는 **3**을 사용할지 여부를 정의합니다.

```
SNMP_VERSION=3
```

4.

SNMP_ENGINE_ID 값을 지정합니다. 예를 들면 다음과 같습니다.

```
SNMP_ENGINE_ID="80:00:00:00:01:02:05:05"
```

5.

SNMP 버전 3을 사용하여 **SNMP 트랩의 보안 수준**을 지정합니다.

보안 수준 1, **NoAuthNoPriv** 트랩:

```
SNMP_USERNAME=NoAuthNoPriv
SNMP_SECURITY_LEVEL=1
```

보안 수준 2, **AuthNoPriv** 트랩, 사용자 **ovirtengine**, 및 **SNMP Auth** 암호 **authpass**.

```
SNMP_USERNAME=ovirtengine
SNMP_AUTH_PROTOCOL=MD5
SNMP_AUTH_PASSPHRASE=authpass
SNMP_SECURITY_LEVEL=2
```

security level 3, AuthPriv 트랩(AuthPriv)은 **SNMP Auth 암호 authpass** 및 **SNMP Priv 암호 privpass** 를 사용하는 사용자 **ovirtengine** 입니다. 예를 들면 다음과 같습니다.

```
SNMP_USERNAME=ovirtengine
SNMP_AUTH_PROTOCOL=MD5
SNMP_AUTH_PASSPHRASE=authpass
SNMP_PRIVACY_PROTOCOL=AES128
SNMP_PRIVACY_PASSPHRASE=privpass
SNMP_SECURITY_LEVEL=3
```

6.

SNMP 관리자에게 전송할 이벤트를 정의합니다.

예 3.16. 이벤트 예

모든 이벤트를 기본 **SNMP** 프로파일로 보냅니다.

```
FILTER="include:*(snmp:) ${FILTER}"
```

심각도 **ERROR** 또는 **ALERT** 가 있는 모든 이벤트를 기본 **SNMP** 프로파일로 보냅니다.

```
FILTER="include:*.ERROR(snmp:) ${FILTER}"
```

```
FILTER="include:*.ALERT(snmp:) ${FILTER}"
```

VDC_START 에 대한 이벤트를 지정된 이메일 주소로 보냅니다.

```
FILTER="include:VDC_START(snmp:mail@example.com) ${FILTER}"
```

VDC_START 를 제외한 모든 이벤트를 기본 **SNMP** 프로파일로 보냅니다.

```
FILTER="exclude:VDC_START include:*(snmp:) ${FILTER}"
```

ovirt-engine-notifier.conf 에 정의된 기본 필터를 사용합니다. 이 필터를 비활성화하지 않거나 덮어쓰기 필터를 적용하지 않으면 알림이 전송되지 않습니다.

```
FILTER="exclude:*"
```

VDC_START 는 사용 가능한 감사 로그 메시지의 예입니다. 전체 감사 로그 메시지 목록은 `/usr/share/doc/ovirt-engine/AuditLogMessages.properties` 에서 확인할 수 있습니다. 또는 **SNMP** 관리자 내에서 결과를 필터링합니다.

7.

파일을 저장합니다.

8.

ovirt-engine-notifier 서비스를 시작하고 이 서비스가 부팅 시 시작되는지 확인합니다.

```
# systemctl start ovirt-engine-notifier.service
# systemctl enable ovirt-engine-notifier.service
```

SNMP 관리자를 확인하여 트랩이 수신되고 있는지 확인합니다.



참고

protocol_MANAGERS, **MAIL_SERVER** 또는 둘 다 `/usr/share/ovirt-engine/services/ovirt-engine-notifier.conf` 에 올바르게 정의되어야 합니다.

cookie-Always 설정 파일 샘플

이 샘플 구성 파일은 **ovirt-engine-notifier.conf** 의 설정을 기반으로 합니다. 이 파일과 같은 전용 **Keycloak** 구성 파일은 **ovirt-engine-notifier.conf** 의 설정을 덮어씁니다.

작은 정보

이벤트 알람 데몬 구성 파일 `/usr/share/ovirt-engine/services/ovirt-engine-notifier.conf`에서 `/etc/ovirt-engine/notifier.conf.d/<_integer_>-snmp.conf`에서 실행 우선 순위를 지정합니다. 이 파일에는 모든 설정에 대한 인라인 주석이 포함되어 있습니다.

`/etc/ovirt-engine/notifier/notifier.conf.d/20-snmp.conf`

```
SNMP_MANAGERS="manager1.example.com manager2.example.com:162" 1
SNMP_COMMUNITY=public 2
SNMP_OID=1.3.6.1.4.1.2312.13.1.1 3
FILTER="include:*(snmp:)" 4
SNMP_VERSION=3 5
SNMP_ENGINE_ID="80:00:00:00:01:02:05:05" 6
```

```
SNMP_USERNAME=<username> 7
SNMP_AUTH_PROTOCOL=MD5 8
SNMP_AUTH_PASSPHRASE=<authpass> 9
SNMP_PRIVACY_PROTOCOL=AES128 10
SNMP_PRIVACY_PASSPHRASE=<privpass> 11
SNMP_SECURITY_LEVEL=3 12
```

1

SNMP 관리자 역할을 할 시스템의 **IP** 주소 또는 정규화된 도메인 이름입니다. 항목은 공백으로 구분해야 하며 포트 번호를 포함할 수 있습니다. 예를 들어 **manager1.example.com**
manager2.example.com:164

2

(**SNMP** 버전 2만) 기본 **SNMP** 커뮤니티 문자열.

3

발신 알림용 **Fast Trap Object Identifier**. **iso(1) org(3) dod(6) Internet(1) private(4) enterprise(1) redhat(2312) ovirt(13) engine(1) notifier(1)**



참고

기본값을 변경하면 생성된 트랩이 **OVIRT-MIB.txt**를 준수하지 않습니다.

4

Keycloak 알림 및 수신자의 트리거를 결정하는 데 사용되는 알고리즘입니다.

5

중첩 버전. 중첩 버전 2 및 버전 3 트랩이 지원됩니다. 2 = **SNMPv2**, 3 = **SNMPv3**.

6

(**SNMP** 버전 3만) **SNMP** 트랩에 사용된 엔진 ID입니다.

7

(**SNMP** 버전 3만 해당) **SCSI** 트랩에 사용되는 사용자 이름입니다.

8

(SNMP 버전 3만) **SNMP** 인증 프로토콜입니다. 지원되는 값은 **MD5** 및 **SHA**입니다. **broker_SECURITY_LEVEL** 이 2(**AUTH_NOPRIV**) 또는 3(**AUTH_PRIV**)으로 설정된 경우 필요합니다.

9

(SNMP 버전 3만 해당) **SNMP** 인증 암호입니다. **broker_SECURITY_LEVEL** 이 2(**AUTH_NOPRIV**) 또는 3(**AUTH_PRIV**)으로 설정된 경우 필요합니다.

10

(SNMP 버전 3만) **flush** 개인 정보 보호 프로토콜. 지원되는 값은 **AES128**, **AES192** 및 **AES256**입니다. **AES192** 및 **AES256**은 **RFC3826**에 정의되어 있지 않으므로 **Keycloak** 서버가 해당 프로토콜을 활성화하기 전에 해당 프로토콜을 지원하는지 확인합니다. **SNMP_SECURITY_LEVEL** 이 3(**AUTH_PRIV**)으로 설정된 경우 필요합니다.

11

(SNMP 버전 3만) **flush** 개인 정보 보호 암호입니다. **SNMP_SECURITY_LEVEL** 이 3(**AUTH_PRIV**)으로 설정된 경우 필요합니다.

12

(SNMP 버전 3만) **SNMP** 보안 수준입니다. 1 = **NOAUTH_NOPRIV**, 2 = **AUTH_NOPRIV**, 3 = **AUTH_PRIV**.

3.9. 유틸리티

3.9.1. oVirt 엔진 이름 바꾸기 도구

3.9.1.1. oVirt 엔진 이름 바꾸기 도구

engine-setup 명령이 클린 환경에서 실행되면 명령은 설정 프로세스 중에 제공된 **Manager**의 정규화된 도메인 이름을 사용하는 여러 인증서와 키를 생성합니다. 관리자가 다른 도메인으로 호스팅하는 시스템의 마이그레이션으로 인해 관리자의 정규화된 도메인 이름을 나중에 변경해야 하는 경우 새 이름을 반영하도록 정규화된 도메인 이름의 레코드를 업데이트해야 합니다. **ovirt-engine-rename** 명령은 이 작업을 자동화합니다.

ovirt-engine-rename 명령은 다음 위치에서 관리자의 정규화된 도메인 이름에 대한 레코드를 업데이트합니다.

•

/etc/ovirt-engine/engine.conf.d/10-setup-protocols.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 명령은 **Manager**가 실행하는 웹 서버에 대한 새 인증서를 생성하지만 관리자 또는 인증 기관의 인증서에는 영향을 미치지 않습니다. 이로 인해 **ovirt-engine-rename** 명령을 사용하는 경우 특히 **Red Hat Enterprise Virtualization 3.2** 및 이전 버전에서 업그레이드된 환경에서 약간의 위험이 있습니다. 따라서 **engine -cleanup** 및 **engine- setup** 을 실행하여 **Manager**의 정규화된 도메인 이름을 변경하는 것이 좋습니다.



주의

업그레이드 프로세스 중에 이전 호스트 이름을 확인할 수 있어야 합니다. **oVirt Engine Rename** 툴이 실패하고 **[ERROR]** 호스트 이름이 유효하지 않습니다. **<OLD FQDN>**이 IP 주소가 확인되지 않은 경우 이전 호스트 이름을 **/etc/hosts** 파일에 추가하고 **oVirt Engine Rename** 도구를 사용한 다음 **/etc/hosts** 파일에서 이전 호스트 이름을 제거합니다.

3.9.1.2. oVirt Engine Rename 명령 구문

ovirt-engine-rename 명령의 기본 구문은 다음과 같습니다.

```
# /usr/share/ovirt-engine/setup/bin/ovirt-engine-rename
```

명령은 다음 옵션도 허용합니다.

--newname=[새 이름]

사용자 상호 작용 없이 **Manager**에 대해 정규화된 새 도메인 이름을 지정할 수 있습니다.

--log=[file]

파일 이름 바꾸기 작업의 로그를 작성할 파일의 경로와 이름을 지정할 수 있습니다.

--config=[file]

파일 이름 변경 작업에 로드할 구성 파일의 경로와 파일 이름을 지정할 수 있습니다.

--config-append=[file]

파일 이름 작업에 추가할 구성 파일의 경로와 파일 이름을 지정할 수 있습니다. 이 옵션을 사용하여 기존 응답 파일의 경로와 파일 이름을 지정하여 이름 변경 작업을 자동화할 수 있습니다.

--generate-answer=[file]

ovirt-engine-rename 명령으로 변경된 값과 응답이 기록되는 파일의 경로와 파일 이름을 지정할 수 있습니다.

3.9.1.3. oVirt Engine 이름 바꾸기 도구로 관리자 이름 변경

ovirt-engine-rename 명령을 사용하여 관리자의 **FQDN**(정규화된 도메인 이름) 레코드를 업데이트할 수 있습니다.

틀은 관리자가 로컬 **ISO** 또는 데이터 스토리지 도메인을 제공하는지 확인합니다. 이 도구가 있는 경우 작업을 계속하기 전에 스토리지에 연결된 가상 시스템 또는 스토리지 도메인을 유지 관리 모드로 제거, 종료 또는 배치하라는 메시지를 사용자에게 표시합니다. 이렇게 하면 가상 시스템이 가상 디스크와의 연결이 끊어지지 않으며 이름 변경 프로세스 중에 **ISO** 스토리지 도메인이 연결이 손실되지 않도록 합니다.

절차

1. 새 **FQDN**에 대해 모든 **DNS** 및 기타 관련 레코드를 준비합니다.
2. **DHCP**를 사용하는 경우 **DHCP** 서버 구성을 업데이트합니다.
3. **Manager**에서 호스트 이름을 업데이트합니다.
4. 다음 명령을 실행합니다.

```
# /usr/share/ovirt-engine/setup/bin/ovirt-engine-rename
```

5. 메시지가 표시되면 **Enter** 키를 눌러 엔진 서비스를 중지합니다.

```
During execution engine service will be stopped (OK, Cancel) [OK]:
```

6. 메시지가 표시되면 **Manager**에 새 **FQDN**을 입력합니다.

```
New fully qualified server name:new_engine_fqdn
```

ovirt-engine-rename 명령은 **Manager**의 **FQDN** 레코드를 업데이트합니다.

자체 호스팅 엔진의 경우 다음 추가 단계를 완료합니다.

1. 기존의 모든 자체 호스팅 엔진 노드에서 다음 명령을 실행합니다.

```
# hosted-engine --set-shared-config fqdn new_engine_fqdn --type=he_local
```

이 명령은 각 자체 호스팅 엔진 노드의 로컬 `/etc/ovirt-hosted-engine-ha/hosted-engine.conf`에서 **FQDN**을 수정합니다.

2.

자체 호스팅 엔진 노드 중 하나에서 다음 명령을 실행합니다.

```
# hosted-engine --set-shared-config fqdn new_engine_fqdn --type=he_shared
```

이 명령은 공유 스토리지 도메인의 `/etc/ovirt-hosted-engine-ha/hosted-engine.conf`의 기본 사본에 있는 **FQDN**을 수정합니다.

이제 모든 신규 및 기존 자체 호스팅 엔진 노드에서 새 **FQDN**을 사용합니다.

3.9.2. 엔진 설정 도구

3.9.2.1. 엔진 설정 도구

엔진 구성 도구는 **Red Hat Virtualization** 환경에 대한 글로벌 설정을 구성하는 명령줄 유틸리티입니다. 톨은 엔진 데이터베이스에 저장된 키-값 매핑 목록과 상호 작용하며 개별 키의 값을 검색 및 설정하고 사용 가능한 모든 구성 키와 값 목록을 검색할 수 있습니다. 또한 **Red Hat Virtualization** 환경의 각 구성 수준에 대해 다양한 값을 저장할 수 있습니다.



참고

구성 키의 값을 검색하거나 설정하기 위해 **Red Hat Virtualization Manager**와 **Red Hat JBoss Enterprise Application Platform**을 실행하지 않아도 됩니다. 구성 키 값 매핑은 엔진 데이터베이스에 저장되므로 **postgresql** 서비스가 실행되는 동안 업데이트할 수 있습니다. 그런 다음 **ovirt-engine** 서비스를 다시 시작할 때 변경 사항이 적용됩니다.

3.9.2.2. engine-config 명령의 구문

Red Hat Virtualization Manager가 설치된 시스템에서 엔진 구성 도구를 실행할 수 있습니다. 사용법에 대한 자세한 정보를 보려면 명령의 도움말 출력을 출력합니다.

```
# engine-config --help
```

일반적인 작업:

- 사용 가능한 구성 키 나열

```
# engine-config --list
```

- 사용 가능한 구성 값 나열

```
# engine-config --all
```

- 구성 키 검색 값

```
# engine-config --get KEY_NAME
```

KEY_NAME 을 지정된 버전의 키에 대한 값을 검색하도록 기본 키의 이름으로 교체합니다. **c ver** 매개 변수를 사용하여 검색할 값의 구성 버전을 지정합니다. 버전을 제공하지 않으면 기존 버전의 값이 모두 반환됩니다.

- 구성 키의 값 설정

```
# engine-config --set KEY_NAME=KEY_VALUE --cver=VERSION
```

KEY_NAME 을 설정할 특정 키의 이름으로 바꾸고 **KEY_VALUE** 를 설정할 값으로 바꿉니다. 둘 이상의 구성 버전이 있는 환경에서 **VERSION** 을 지정해야 합니다.

- **ovirt-engine** 서비스를 다시 시작하여 변경 사항을 로드합니다.

변경 사항을 적용하려면 **ovirt-engine** 서비스를 다시 시작해야 합니다.

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

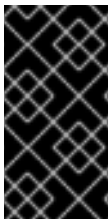
3.9.3. USB 필터 편집기**3.9.3.1. USB 필터 편집기 설치**

USB 필터 편집기는 `usbfilter.txt` 정책 파일을 구성하는 데 사용되는 **Windows** 도구입니다. 이 파일에 정의된 정책 규칙은 **Red Hat Virtualization Manager**를 사용하여 관리되는 가상 시스템으로 클라이언트 시스템에서 특정 **USB** 장치의 자동 패스스루를 허용하거나 거부합니다. 정책 파일은 **Red Hat Virtualization Manager**에 있는 `/etc/ovirt-engine/usbfilter.txt` 에서 **Red Hat Virtualization Manager**의 `ovirt-engine` 서비스를 다시 시작하지 않는 한 적용되지 않습니다.

이 "**Red Hat Virtualization Manager**용 설치 프로그램 및 이미지" 항목에서 **USB 필터 편집기** 설치 프로그램을 다운로드합니다.

절차

1. **Windows** 시스템에서. `zip` 파일에서 `.msi` intaller를 추출하고. `msi` 설치 프로그램을 실행합니다.
2. 설치 마법사의 단계를 따릅니다. 별도로 명시하지 않는 한, 기본적으로 **USB 필터 편집기**는 **Windows** 버전에 따라 `C:\Program Files\RedHat\ Filter Editor` 또는 `C:\Program Files(x86)\RedHat\jpg Filter Editor` 에 설치됩니다.
3. 바탕 화면에 **USB 필터 편집기** 바로 가기 아이콘이 생성됩니다.



중요

WinSCP 와 같은 **SCP(Secure Copy)** 클라이언트를 사용하여 **Red Hat Virtualization Manager**에서 필터 정책을 가져오고 내보냅니다.

기본 **USB** 장치 정책에서는 가상 시스템에 **USB** 장치에 대한 기본 액세스 권한을 제공합니다. 추가 **USB** 장치를 사용하도록 정책을 업데이트합니다.

3.9.3.2. USB 필터 편집기 인터페이스

바탕 화면에서 **USB 필터 편집기** 바로 가기 아이콘을 두 번 클릭합니다.

Red Hat USB 필터 편집기 인터페이스는 각 **USB** 장치에 대한 클래스, 벤더, 제품, 버전 및 작업을 표시합니다. 허용되는 **USB** 장치는 **Action** 열에서 **Allow** 로 설정됩니다. 금지된 장치는 **Block** 으로 설정됩니다.

표 3.7. **USB** 편집기 필드

이름	설명
클래스	USB 장치 유형(예: 프린터, 대용량 스토리지 컨트롤러).
벤더	선택한 장치 유형의 제조업체입니다.
제품	특정 USB 장치 모델.
버전	제품의 버전입니다.
동작	지정된 장치를 허용하거나 차단합니다.

USB 장치 정책 규칙은 나열된 순서대로 처리됩니다. Up 및 Down 버튼을 사용하여 목록에서 규칙을 더 높이거나 아래로 이동합니다. 범용 블록 규칙은 USB 필터 편집기에서 명시적으로 허용되지 않는 한 모든 USB 장치가 거부되도록 하려면 가장 낮은 항목으로 유지해야 합니다.

3.9.3.3. USB 정책 추가

바탕 화면에서 **USB 필터 편집기** 바로 가기 아이콘을 두 번 클릭합니다. 그러면 편집기가 열립니다.

절차

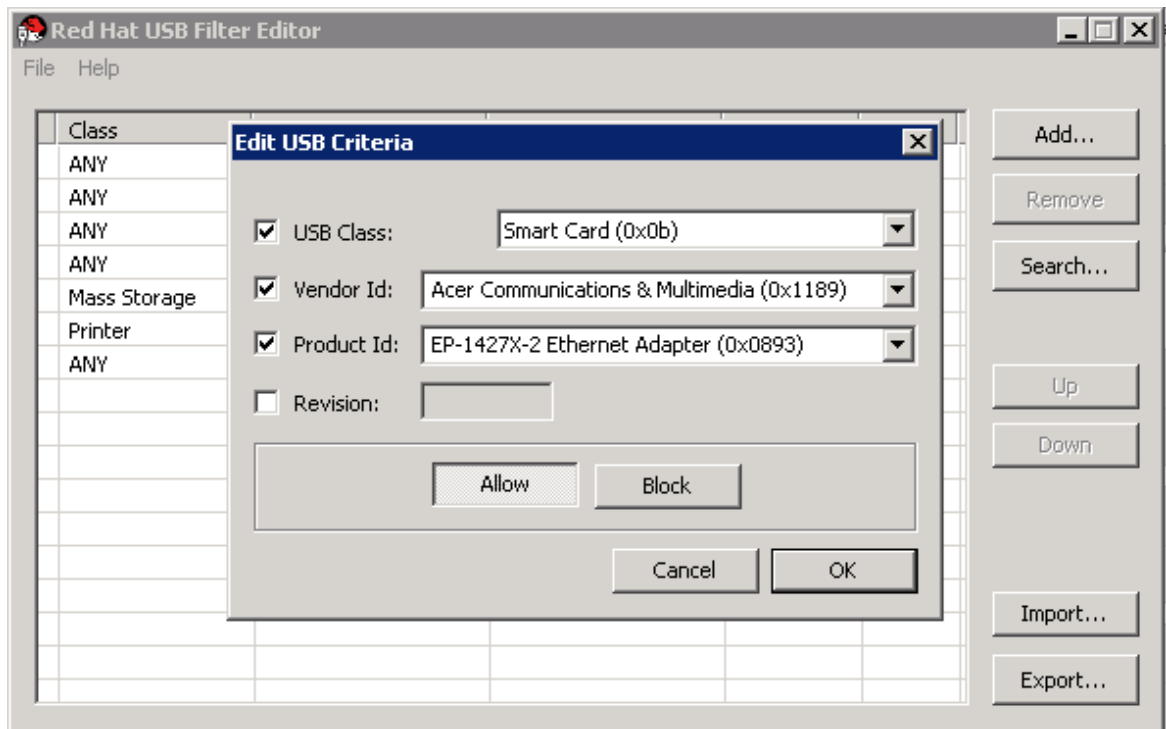
1. **추가**를 클릭합니다.
2. **USB 클래스, 벤더 ID, 제품 ID 및 버전 확인란을 사용하고 목록을 사용하여 장치를 지정합니다.**

USB 장치의 가상 시스템 사용을 허용하려면 Allow (허용) 버튼을 클릭합니다. Block (블록) 버튼을 클릭하여 USB 장치가 가상 시스템의 사용을 금지합니다.

OK(확인)를 클릭하여 선택한 필터 규칙을 목록에 추가하고 창을 닫습니다.

예 3.17. 장치 추가

다음은 제조업체 **Acer Communications & Multimedia** 에서 허용되는 장치 목록에 **USB 클래스 스마트 카드, 장치 EP-1427X-2 이더넷 어댑터** 를 추가하는 방법의 예입니다.



3.

File → Save (저장) 를 클릭하여 변경 사항을 저장합니다.

USB 필터 편집기에 USB 정책을 추가했습니다. USB 필터 정책을 Red Hat Virtualization Manager 로 내보내야 적용됩니다.

추가 리소스

•

[USB 정책 내보내기](#)

3.9.3.4. USB 정책 제거

바탕 화면에서 **USB 필터 편집기** 바로 가기 아이콘을 두 번 클릭합니다. 그러면 편집기가 열립니다.

절차

1.

제거할 정책을 선택합니다.

2.

Remove(제거)를 클릭합니다. 정책을 제거할지 확인하라는 메시지가 표시됩니다.

~

3.

Yes (예)를 클릭하여 정책을 제거할지 확인합니다.

4.

File → **Save (저장)** 를 클릭하여 변경 사항을 저장합니다.

USB 필터 편집기에서 USB 정책을 제거했습니다. USB 필터 정책을 Red Hat Virtualization Manager로 내보내야 적용됩니다.

추가 리소스

•

[USB 정책 내보내기](#)

3.9.3.5. USB 장치 정책 검색

연결된 **USB** 장치를 검색하여 **USB 필터 편집기**에서 허용하거나 차단합니다.

바탕 화면에서 **USB 필터 편집기** 바로 가기 아이콘을 두 번 클릭합니다. 그러면 편집기가 열립니다.

절차

1.

Search를 클릭합니다 연결된 **USB** 장치 창에 연결된 모든 장치 목록이 표시됩니다.

2.

장치를 선택하고 필요에 따라 **Allow or Block**(허용 또는 차단)을 클릭합니다. 선택한 장치를 두 번 클릭하여 창을 닫습니다. 장치의 정책 규칙이 목록에 추가됩니다.

3.

Up 및 **Down** 버튼을 사용하여 목록에서 새 정책 규칙의 위치를 변경합니다.

4.

File → **Save (저장)** 를 클릭하여 변경 사항을 저장합니다.

연결된 **USB** 장치를 검색했습니다. 적용하려면 **USB 필터 정책**을 **Red Hat Virtualization Manager**에 내보내야 합니다.

3.9.3.6. USB 정책 내보내기

업데이트된 정책을 적용하려면 **USB** 장치 정책 변경 사항을 내보내고 **Red Hat Virtualization Manager**에 업로드해야 합니다. 정책을 업로드하고 **ovirt-engine** 서비스를 다시 시작합니다.

바탕 화면에서 **USB** 필터 편집기 바로 가기 아이콘을 두 번 클릭합니다. 그러면 편집기가 열립니다.

절차

1. **Export(내보내기)**를 클릭합니다. **Save As** (다른 이름으로 저장) 창이 열립니다.
2. 파일 이름이 **usbfilter.txt** 인 파일을 저장합니다.
3. **WinSCP**와 같은 보안 복사 클라이언트를 사용하여 **usbfilter.txt** 파일을 **Red Hat Virtualization Manager**를 실행하는 서버에 업로드합니다. 파일은 서버의 다음 디렉토리에 위치해야 합니다. **/etc/ovirt-engine/**
4. **Red Hat Virtualization Manager**를 실행하는 서버에서 **root** 사용자로 **ovirt-engine** 서비스를 다시 시작합니다.

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

3.9.3.7. USB 정책 가져오기

기존 **USB** 장치 정책을 다운로드하여 **USB** 필터 편집기로 가져와야 편집할 수 있습니다.

절차

1. **WinSCP**와 같은 보안 복사 클라이언트를 사용하여 **Red Hat Virtualization Manager**를 실행하는 서버에서 **usbfilter.txt** 파일을 다운로드합니다. 파일은 서버의 다음 디렉토리에 있습니다. **/etc/ovirt-engine/**
2. 바탕 화면에서 **USB** 필터 편집기 바로 가기 아이콘을 두 번 클릭합니다. 그러면 편집기가 열립니다.
3. **Import(가져오기)**를 클릭합니다. 그러면 **Open** 창이 열립니다.

4.

서버에서 다운로드한 **usbfilter.txt** 파일을 엽니다.

3.9.4. 이미지 불일치 툴

3.9.4.1. 이미지 불일치 툴을 사용하여 스냅샷 상태 모니터링

RHV 이미지 논의 툴은 스토리지 도메인 및 **RHV** 데이터베이스의 이미지 데이터를 분석합니다. 볼륨 및 볼륨 속성에서 불일치를 발견하더라도 이러한 불일치를 수정하지 않는 경우 경고합니다. 다음과 같은 다양한 시나리오에서 이 도구를 사용합니다.

- 버전을 업그레이드하기 전에 손상된 볼륨 또는 체인을 새 버전으로 전달하지 않도록 합니다.
- 실패한 스토리지 작업을 수행한 후 상태가 잘못된 상태에서 볼륨 또는 속성을 감지합니다.
- 백업에서 **RHV** 데이터베이스 또는 스토리지를 복원한 후 다음을 수행합니다.
- 정기적으로 잠재적인 문제를 보다 먼저 감지합니다.
- 스냅샷 또는 실시간 스토리지 마이그레이션 관련 문제를 분석하고 이러한 유형의 문제를 해결한 후 시스템 상태를 확인하려면 다음을 수행합니다.

사전 요구 사항

- 필수 버전: 이 도구는 **rhv-log-collector-analyzer-0.2.15-0.el7ev** 와 함께 **RHV** 버전 **4.3.8**에서 도입되었습니다.
- 데이터 컬렉션은 서로 다른 위치에서 동시에 실행되며 원자성이 아니므로 스토리지 도메인을 수정할 수 있는 환경의 모든 활동을 중지합니다. 즉, 스냅샷을 생성하거나 제거하거나, 디스크를 편집, 이동, 생성 또는 제거하지 마십시오. 그렇지 않으면 불일치에 대한 잘못된 탐지가 발생할 수 있습니다. 가상 머신은 프로세스 중에 정상적으로 실행되도록 유지할 수 있습니다.

절차

1.

툴을 실행하려면 **RHV Manager**에 다음 명령을 입력합니다.

rhv-image-discrepancies

2.

툴에서 불일치를 발견하는 경우, 특히 도구를 실행하는 동안 일부 작업을 수행할 가능성이 있는 경우 결과를 확인하기 위해 다시 실행합니다.



참고

이 툴에는 모든 내보내기 및 ISO 스토리지 도메인이 포함되어 있으며 불일치를 보고할 수 있습니다. 이러한 스토리지 도메인에는 RHV 데이터베이스의 이미지에 대한 항목이 없으므로 해당 스토리지 도메인은 무시할 수 있습니다.

결과 이해

도구는 다음을 보고합니다.

- 스토리지에 표시되지만 데이터베이스에 표시되지 않거나 데이터베이스에 표시되지만 스토리지에 없는 블록이 있는 경우.
- 스토리지와 데이터베이스 간에 일부 블록 특성이 다른 경우.

샘플 출력:

```
Checking storage domain c277ad93-0973-43d9-a0ca-22199bc8e801
Looking for missing images...
No missing images found
Checking discrepancies between SD/DB attributes...
image ef325650-4b39-43cf-9e00-62b9f7659020 has a different attribute capacity on
storage(2696984576) and on DB(2696986624)
image 852613ce-79ee-4adc-a56a-ea650dcb4cfa has a different attribute capacity on
storage(5424252928) and on DB(5424254976)

Checking storage domain c64637b4-f0e8-408c-b8af-6a52946113e2
Looking for missing images...
No missing images found
Checking discrepancies between SD/DB attributes...
No discrepancies found
```

3.9.5. 로그 수집기 도구

3.9.5.1. Log Collector

로그 수집 툴은 **Red Hat Virtualization Manager**에 포함되어 있습니다. 이를 통해 지원을 요청할 때 **Red Hat Virtualization** 환경에서 관련 로그를 쉽게 수집할 수 있습니다.

로그 수집 명령은 **ovirt-log-collector** 입니다. **root** 사용자로 로그인하고 **Red Hat Virtualization** 환경에 대한 관리 자격 증명을 제공해야 합니다. **ovirt-log-collector -h** 명령은 **ovirt-log-collector** 명령에 유효한 모든 옵션 목록을 포함하여 사용 정보를 표시합니다.

3.9.5.2. ovirt-log-collector 명령의 구문

로그 수집기의 기본 구문은 다음과 같습니다.

```
# ovirt-log-collector options list all|clusters/datacenters
# ovirt-log-collector options collect
```

지원되는 두 가지 작업 모드는 목록 및 수집입니다.

- **list** 매개 변수는 **Red Hat Virtualization Manager**에 연결된 호스트, 클러스터 또는 데이터 센터를 나열합니다. 나열된 오브젝트를 기반으로 로그 컬렉션을 필터링할 수 있습니다.
- **collect** 매개 변수는 **Red Hat Virtualization Manager**에서 로그 수집을 수행합니다. 수집된 로그는 **/tmp/logcollector** 디렉토리 아래에 있는 아카이브 파일에 저장됩니다. **ovirt-log-collector** 명령은 각 로그에 특정 파일 이름을 할당합니다.

다른 매개 변수를 지정하지 않는 한 기본 작업은 사용 가능한 호스트를 보유한 데이터 센터 및 클러스터와 함께 나열하는 것입니다. 특정 로그를 검색하려면 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다.

ovirt-log-collector 명령을 추가로 구체화하기 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

도구에서 사용할 구성 파일로 **PATH** 를 설정합니다.

--local-tmp=PATH

로그가 저장되는 디렉터리로 **PATH** 를 설정합니다. 기본 디렉토리는 **/tmp/logcollector** 입니다.

--ticket-number=TICKET

TICKET 을 티켓 또는 케이스 번호로 설정하여 **SOS** 보고서와 연결합니다.

--upload=FTP_SERVER

FTP를 사용하여 **FTP_SERVER** 를 검색된 로그의 대상으로 설정합니다.

Red Hat 지원 담당자에게 문의하지 않는 한 이 옵션을 사용하지 마십시오.

--log-file=PATH

명령이 로그 출력에 사용해야 하는 특정 파일 이름으로 **PATH** 를 설정합니다.

--quiet

자동 모드를 설정하여 콘솔 출력을 최소한으로 줄입니다. 자동 모드는 기본적으로 꺼져 있습니다.

-v, --verbose

더 많은 콘솔 출력을 제공하는 자세한 정보 표시 모드를 설정합니다. 자세한 정보 표시 모드는 기본적으로 꺼져 있습니다.

--time-only

전체 **SOS** 보고서를 생성하지 않고 호스트 간 시간 차이에 대한 정보만 표시합니다.

Red Hat Virtualization Manager 옵션

이러한 옵션은 로그 컬렉션을 필터링하고 **Red Hat Virtualization Manager**의 인증 세부 정보를 지정합니다.

이러한 매개 변수는 특정 명령에 결합할 수 있습니다. 예를 들어 **ovirt-log-collector --user=admin@internal --cluster ClusterA,ClusterB --hosts "SalesHost"*** 는 사용자를 **admin@internal** 로 지정하고 **A** 및 **B** 클러스터의 **SalesHost** 호스트로만 로그 컬렉션을 제한합니다.

--no-hypervisors

로그 컬렉션에서 가상화 호스트를 생략합니다.

--one-hypervisor-per-cluster

각 클러스터에서 하나의 호스트(SPM)의 로그를 수집합니다.

-u USER, --user=USER

로그인에 사용할 사용자 이름을 설정합니다. **USER** 는 형식 **user@domain** 에서 지정됩니다. 여기서 **user** 는 사용자 이름이며 **domain** 은 사용 중인 디렉터리 서비스 도메인입니다. 사용자는 디렉터리 서비스에 있어야 하며 **Red Hat Virtualization Manager**에 알려져 있습니다.

-r FQDN, --rhevm=FQDN

로그를 수집할 **Red Hat Virtualization Manager**의 정규화된 도메인 이름을 설정합니다. 여기서 **FQDN** 은 **Manager**의 정규화된 도메인 이름으로 대체됩니다. 로그 수집기가 **Red Hat Virtualization Manager**와 동일한 로컬 호스트에서 실행되고 있다고 가정합니다. 기본값은 **localhost** 입니다.

-c CLUSTER, --cluster=CLUSTER

Red Hat Virtualization Manager의 로그 외에도 **nominated CLUSTER** 의 가상화 호스트에서 로그를 수집합니다. 포함하기 위한 클러스터를 쉼표로 구분된 클러스터 이름 또는 일치 패턴 목록에 지정해야 합니다.

-d DATACENTER, --data-center=DATACENTER

Red Hat Virtualization Manager의 로그 외에도 지정된 **DATACENTER** 의 가상화 호스트에서 로그를 수집합니다. 포함을 위한 데이터 센터를 쉼표로 구분된 데이터 센터 이름 또는 일치 패턴 목록에 지정해야 합니다.

-H HOSTS_LIST, --hosts=HOSTS_LIST

Red Hat Virtualization Manager의 로그 외에도 후보가 지정된 **HOSTS_LIST** 의 가상화 호스트에서 로그를 수집합니다. 포함시킬 호스트는 쉼표로 구분된 호스트 이름, 정규화된 도메인 이름 또는 IP 주소 목록에 지정해야 합니다. 일치 패턴도 유효합니다.

SSH 설정

--ssh-port=PORT

가상화 호스트와 함께 **SSH** 연결에 사용할 포트로 **PORT** 를 설정합니다.

-k KEYFILE, --key-file=KEYFILE

KEYFILE 을 가상화 호스트에 액세스하는 데 사용할 공용 **SSH** 키로 설정합니다.

--max-connections=MAX_CONNECTIONS

MAX_CONNECTIONS 를 가상화 호스트의 로그에 대한 최대 동시 **SSH** 연결로 설정합니다. 기본값은 10입니다.

PostgreSQL 데이터베이스 옵션

pg-user 및 **dbname** 매개 변수를 사용하여 데이터베이스 사용자 이름과 데이터베이스 이름을 기본값에서 변경된 경우 지정해야 합니다.

데이터베이스가 로컬 호스트에 없는 경우 **pg-dbhost** 매개 변수를 사용합니다. 선택적 **pg-host-key** 매개 변수를 사용하여 원격 로그를 수집합니다. 원격 로그 수집이 성공하려면 데이터베이스 서버에 **PostgreSQL SOS** 플러그인을 설치해야 합니다.

--no-postgresql

데이터베이스 컬렉션을 비활성화합니다. 로그 수집기는 **Red Hat Virtualization Manager PostgreSQL** 데이터베이스에 연결하고 **--no-postgresql** 매개 변수를 지정하지 않는 한 로그 보고서에 데이터를 포함합니다.

--pg-user=USER

데이터베이스 서버와 연결에 사용할 사용자 이름으로 **USER** 를 설정합니다. 기본값은 **postgres** 입니다.

--pg-database=DATABASE

데이터베이스 서버와의 연결에 사용할 데이터베이스 이름으로 **DATABASE** 을 설정합니다. 기본값은 **rhevm** 입니다.

--pg-dbhost=DBHOST

DBHOST 를 데이터베이스 서버의 호스트 이름으로 설정합니다. 기본값은 **localhost** 입니다.

--pg-host-key=KEYFILE

KEYFILE 을 데이터베이스 서버에 대한 공용 **ID** 파일(개인 키)으로 설정합니다. 이 값은 기본적으로 설정되지 않습니다. 로컬 호스트에 데이터베이스가 없는 경우에만 필요합니다.

3.9.5.3. 기본 로그 수집기 사용

추가 매개 변수를 지정하지 않고 **ovirt-log-collector** 명령이 실행되면 기본 동작은 **Red Hat Virtualization Manager** 및 연결된 호스트에서 모든 로그를 수집하는 것입니다. **no -postgresql** 매개 변수를 추가하지 않는 한 데이터베이스 로그를 수집합니다. 다음 예에서 로그 수집기는 **Red Hat Virtualization Manager** 및 연결된 호스트 3개에서 모든 로그를 수집하기 위해 실행됩니다.

예 3.18. 로그 수집기 사용량

```
# 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
```

3.9.6. 엔진 툴

3.9.6.1. 엔진 툴

Engine HFScuum 툴은 테이블을 업데이트하고 배달된 행을 제거하여 **PostgreSQL** 데이터베이스를 유지 관리하므로 디스크 공간을 재사용할 수 있습니다. **VACUUM** 명령 및 해당 매개 변수에 대한 정보는 [PostgreSQL 설명서](#)를 참조하십시오.

Engine HFScuum 명령은 **engine-vacuum**입니다. **root** 사용자로 로그인하고 **Red Hat Virtualization** 환경에 대한 관리 자격 증명을 제공해야 합니다.

또는 **engine-setup** 명령을 사용하여 기존 설치를 사용자 지정하는 동안 **Engine collectdcuum** 도구를 실행할 수 있습니다.

```
$ engine-setup
```

```
...
```


[INFO] Stage: Environment customization

...

Perform full vacuum on the engine database engine@localhost?

This operation may take a while depending on this setup health and the configuration of the db vacuum process.

See <https://www.postgresql.org/docs/12/static/sql-vacuum.html>

(Yes, No) [No]:

Yes 옵션은 전체 세부 정보 표시 모드에서 **Engineecuum** 도구를 실행합니다.

3.9.6.2. 엔진 툴킷 모드

엔진 스케줄링에는 두 가지 모드가 있습니다.

표준 비우기

정규 표준 사용 권장.

표준 채우기는 테이블과 색인에서 데드라인 버전을 제거하고 향후 재사용에 사용할 수 있는 공간을 표시합니다. 자주 업데이트되는 테이블은 정기적으로 잠겨야 합니다. 그러나 표준 설비는 공간을 운영 체제로 반환하지 않습니다.

표준 밀도는 매개 변수 없이 현재 데이터베이스의 모든 테이블을 처리합니다.

전체 검색

일상적인 사용에는 전체 제약이 권장되지 않지만, 테이블 내에서 상당한 공간을 회수해야 하는 경우에만 실행해야 합니다.

전체 프레임은 잘못된 공간이 없는 테이블 파일의 새 사본을 작성하여 테이블을 압축하므로 운영 체제에서 공간을 회수할 수 있습니다. 전체 장애는 오랜 시간이 걸릴 수 있습니다.

전체 조작에는 새 테이블 복사본을 위해 추가 디스크 공간이 필요합니다. 작업이 완료되고 이전 복사본이 삭제될 때까지 추가 디스크 공간이 필요합니다. 전체 조작에는 테이블의 배타적 잠금이 필요하기 때문에 테이블의 다른 용도와 병렬로 실행할 수 없습니다.

3.9.6.3. engine-vacuum 명령 구문

engine-vacuum 명령의 기본 구문은 다음과 같습니다.

```
# engine-vacuum
```

```
# engine-vacuum option
```

옵션 없이 **engine-vacuum** 명령을 실행하면 표준 문제가 수행됩니다.

engine-vacuum 명령을 추가로 구체화하기 위한 몇 가지 매개 변수가 있습니다.

일반 옵션

-h --help

engine-vacuum 명령을 사용하는 방법에 대한 정보를 표시합니다.

-a

표준 제약을 실행하고, 데이터베이스를 분석하며, 최적화자 통계를 업데이트합니다.

-A

데이터베이스를 분석하고 최적화자 통계를 업데이트합니다.

-f

전체 화면 실행.

-v

더 많은 콘솔 출력을 제공하는 자세한 정보 표시 모드로 을 실행합니다.

-t table_name

특정 테이블 또는 테이블을 조작합니다.

```
# engine-vacuum -f -v -t vm_dynamic -t vds_dynamic
```

3.9.7. 네트워크 이름 매핑 도구에 대한 VDSM

3.9.7.1. VDSM 이름을 논리적 네트워크 이름에 매핑

논리적 네트워크의 이름이 15자를 초과하거나 **ASCII**가 아닌 문자를 포함하는 경우 시스템은 자동으

로 호스트 ID(**vdsd_name**) 이름을 생성합니다. 이는 의 문자 와 네트워크 고유 식별자의 처음 13자(예: **ona1b2c3d4e5f6g**)로 구성됩니다. 호스트의 로그 파일에 표시되는 이 이름입니다. 논리적 네트워크 이름 목록과 자동 생성된 네트워크 이름 목록을 보려면 **/usr/share/ovirt-engine/bin/**에 있는 **VDSM-to-Network-Name** 매핑 도구를 사용합니다.

절차

1.

도구를 처음 실행하는 경우 **Manager** 데이터베이스에 대한 읽기 액세스 권한이 있는 데이터베이스 사용자의 암호인 **PASSWORD** 환경 변수를 정의합니다. 예를 들어 다음을 실행합니다.

```
# export PASSWORD=DatabaseUserPassword
```

2.

VDSM-to-Network-Name 매핑 도구를 실행합니다.

```
# vdsd_to_network_name_map --user USER
```

여기서 **USER** 는 **Manager** 데이터베이스에 대한 읽기 액세스 권한이 있는 데이터베이스 사용자이며, 해당 암호는 **PASSWORD** 환경 변수에 할당됩니다.

틀에는 동일한 호스트 식별자에 매핑되는 논리적 네트워크 이름 목록이 표시됩니다.

추가 플래그

다음 플래그를 사용하여 틀을 실행할 수 있습니다.

--host 는 데이터베이스 서버의 호스트 이름/IP 주소입니다. 기본값은 **localhost** 입니다.

--port 는 데이터베이스 서버의 포트 번호입니다. 기본값은 **5432** 입니다.**--database** 는 데이터베이스의 이름입니다. 기본값은 **Manager** 데이터베이스인 **engine** 입니다.

--secure 는 데이터베이스와 보안 연결을 활성화합니다. 기본적으로 도구는 보안 연결 없이 실행됩니다.

4장. 환경에 대한 정보 수집

4.1. 모니터링 및 관찰 기능

이 장에서는 **Red Hat Virtualization** 시스템에서 지표와 로그를 모니터링하고 가져올 수 있는 여러 가지 방법을 제공합니다. 이러한 방법에는 다음이 포함됩니다.

- 데이터 웨어하우스 및 **Grafana**를 사용하여 **RHV** 모니터링
- **Elasticsearch**의 원격 인스턴스에 메트릭 전송
- **Red Hat Virtualization Manager**에 **Insights** 배포

4.1.1. 데이터 웨어하우스 및 **Grafana**를 사용하여 **RHV** 모니터링

4.1.1.1. **Grafana** 개요

Grafana는 **ovirt_engine_history**의 **oVirt** 데이터 웨어하우스 **PostgreSQL** 데이터베이스에서 수집한 데이터를 기반으로 보고서를 표시하는 데 사용되는 웹 기반 **UI** 도구입니다. 사용 가능한 보고서 대시보드에 대한 자세한 내용은 [Grafana 대시보드 및 Grafana 웹 사이트 - 대시보드](#)를 참조하십시오.

Manager의 데이터는 1분마다 수집되며 시간별 및 일별 집계로 집계됩니다. 데이터는 **engine-setup** (**Basic** 또는 **Full scale**) 중 데이터 웨어하우스 구성에 정의된 스케일링 설정에 따라 유지됩니다.

- 기본 (기본값) - 24시간 동안 저장된 샘플 데이터, 1개월 동안 저장되는 시간별 데이터, 일별 데이터 - 매일 저장되지 않은 집계.
- full (권장) - 24시간 동안 저장된 샘플 데이터, 2개월 동안 저장되는 시간별 데이터, 매일 5년간 저장되는 집계.

전체 샘플 확장을 위해서는 데이터 웨어하우스를 별도의 가상 시스템으로 마이그레이션해야 할 수 있습니다.

- 데이터 웨어하우스 확장 지침은 [데이터 웨어하우스 Sampling Scale 변경에서](#) 참조하십시오.

•

데이터 웨어하우스를 별도의 시스템으로 마이그레이션하거나 별도의 시스템에 설치하는 방법은 데이터 웨어하우스에서 별도의 머신으로 마이그레이션 및 데이터 웨어하우스 설치 및 구성을 참조하십시오.



참고

Red Hat은 이러한 구성 요소를 서로 별도의 시스템에 설치할 수 있더라도 데이터 웨어하우스 데이터베이스, 데이터 웨어하우스 서비스 및 **Grafana** 모두에만 설치할 수 있도록 지원합니다.

4.1.1.2. 설치

Grafana 통합은 독립 실행형 관리자 설치 및 셀프 호스트 엔진 설치에서 **Red Hat Virtualization Manager** 엔진 설정을 실행할 때 기본적으로 활성화되어 설치됩니다.



참고

Grafana는 기본적으로 설치되지 않으며 이전 버전의 **RHV**에서 업그레이드를 수행하거나 백업을 복원하거나 데이터 웨어하우스가 별도의 시스템으로 마이그레이션되는 경우와 같은 일부 시나리오에서 수동으로 설치해야 할 수 있습니다.

Grafana 통합을 수동으로 활성화하려면 다음을 수행합니다.

1.

환경을 전역 유지 관리 모드로 설정합니다.

```
# hosted-engine --set-maintenance --mode=global
```

2.

Grafana를 설치할 시스템에 로그인합니다. 데이터 웨어하우스가 구성된 시스템과 동일한 시스템(일반적으로 **Manager** 시스템)이어야 합니다.

3.

다음과 같이 **engine-setup** 명령을 실행합니다.

```
# engine-setup --reconfigure-optional-components
```

4.

답변 예: 이 시스템에 **Grafana**를 설치합니다.

```
Configure Grafana on this host (Yes, No) [Yes]:
```

5.

글로벌 유지 관리 모드를 비활성화합니다.

```
# hosted-engine --set-maintenance --mode=none
```

Grafana 대시보드에 액세스하려면 다음을 수행합니다.

•

`https://<engine FQDN 또는 IP address>/ovirt-engine-grafana`로 이동합니다.

또는

•

관리 포털의 웹 관리 시작 페이지에서 **Monitoring Portal** (포털 모니터링)을 클릭합니다.

4.1.1.2.1. Single Sign-on에 대한 Grafana 구성

Manager engine-setup은 **Manager**의 기존 사용자가 관리 포털에서 **SSO**로 로그인할 수 있도록 자동으로 **Grafana**를 구성하지만 사용자를 자동으로 생성하지는 않습니다. 새 사용자(**Grafana UI**에서 **Invite**)를 만들고 새 사용자를 확인한 다음 로그인할 수 있습니다.

1.

Manager에서 아직 정의되지 않은 경우 사용자의 이메일 주소를 설정합니다.

2.

기존 **admin** 사용자로 **Grafana**에 로그인합니다(처음에 구성된 **admin**).

3.

Configuration(구성) **Users**(사용자) 로 이동하여 **Invite** (인벤토리)를 선택합니다.

4.

이메일 주소와 이름을 입력하고 **Role**(역할)을 선택합니다.

5.

다음 옵션 중 하나를 사용하여 초대를 보냅니다.

- **Send invite mail**을 선택하고 **Submit(제출)**을 클릭합니다. 이 옵션에는 **Grafana** 시스템에 구성된 운영 로컬 메일 서버가 필요합니다.

또는

- **보류 중인 초대**를 선택합니다
 - 원하는 항목을 찾습니다
 - 복사 초대선택
 - 이 링크를 복사하여 브라우저 주소 표시줄에 직접 붙여넣거나 다른 사용자에게 전송하여 계정을 만듭니다.

보류 중인 초대 옵션을 사용하면 이메일이 전송되지 않으며 이메일 주소가 실제로 존재할 필요는 없습니다. **Manager** 사용자의 이메일 주소로 구성된 한 유효한 주소를 찾을 수 있습니다.

이 계정으로 로그인하려면 다음을 수행합니다.

1. 이 이메일 주소가 있는 계정을 사용하여 **Red Hat Virtualization** 웹 관리 시작 페이지에 로그인합니다.
2. **Monitoring Portal (모니터링 포털)**을 선택하여 **Grafana** 대시보드를 엽니다.
3. **Sign in with oVirt Engine Auth** 를 선택합니다.

4.1.1.3. 기본 제공 Grafana 대시보드

다음 대시보드는 초기 **Grafana** 설정에서 데이터 센터, 클러스터, 호스트 및 가상 머신 데이터를 보고할 수 있습니다.

표 4.1. 기본 제공 Grafana 대시보드

대시보드 유형	콘텐츠
주요 대시보드	● 시스템 대시보드 - 최신 구성에 따라 시스템의 호스트 및 스토리지 도메인에 대한 리소스 사용량 및 가동 시간. ● 데이터 센터 대시보드 - 최신 구성에 따라 선택한 데이터 센터의 클러스터, 호스트 및 스토리지 도메인에 대한 리소스 사용량, 피크 및 가동 시간. ● 클러스터 대시보드 - 최신 구성에 따라 선택한 클러스터의 호스트 및 가상 시스템에 대한 리소스 사용량, 피크, 과다 할당, 가동 시간. ● 호스트 대시보드 - 선택한 기간 동안 선택한 호스트의 최신 및 기록 구성 세부 정보 및 리소스 사용 지표입니다. ● 가상 시스템 대시보드 - 선택한 기간 동안 선택한 가상 시스템의 최신 구성 세부 정보 및 리소스 사용 지표입니다. ● 핵심 대시보드 - 선택한 기간 동안 선택한 클러스터에서 호스트 및 가상 시스템의 사용자 리소스 사용량 및 운영 체제 수.
인벤토리 대시보드	● 최신 구성에 따라 인벤토리 대시보드 - 선택한 데이터 센터에 대한 호스트, 가상 시스템, 실행 중인 가상 시스템, 리소스 사용 및 과다 할당 비율입니다. ● Host Inventory dashboard - FQDN, VDSM 버전, 운영 체제, CPU 모델, CPU 코어, 메모리 크기, 날짜 생성, 삭제 날짜, 선택한 호스트에 대한 하드웨어 세부 정보 최신 구성에 따라. ● Storage Domains Inventory dashboard - 도메인 유형, 스토리지 유형, 사용 가능한 디스크 크기, 사용된 디스크 크기, 총 디스크 크기, 생성 날짜, 선택한 스토리지 도메인의 날짜. ● 가상 시스템 인벤토리 대시보드 - 최신 구성에 따라 템플릿 이름, 운영 체제, CPU 코어, 메모리 크기, 선택한 가상 시스템의 날짜 및 삭제 날짜.

대시보드 유형	콘텐츠
서비스 수준 대시보드	● 가동 시간 대시보드 - 선택한 기간에 호스트, 고가용성 가상 시스템 및 모든 가상 시스템의 계획된 가동 중지 시간, 계획되지 않은 다운타임 및 총 시간. ● 호스트 가동 시간 대시보드 - 선택한 기간 내에 선택한 호스트에 대한 가동 시간, 계획되지 않은 가동 중지 시간 및 계획되지 않은 가동 중지 시간. ● Virtual Machines Uptime 대시보드 - 선택한 기간 내에 선택한 가상 머신의 가동 시간, 계획된 가동 중지 시간 및 계획되지 않은 가동 중지 시간. ● 클러스터 서비스 품질 ○ 호스트 대시보드 - 선택한 호스트는 선택한 기간 중 CPU 및 메모리 임계값 이상 및 그 아래로 수행되었습니다. ○ 가상 시스템 대시보드 - 선택한 가상 시스템이 선택한 기간 중 CPU 및 메모리 임계값 이상 및 아래에 수행된 시간입니다.
추세 대시보드	● 추세 대시보드 - 선택한 기간 동안 선택한 클러스터의 메모리 및 CPU별로 가장 적게 사용되는 가상 시스템 및 호스트의 사용량 비율입니다. ● Host Trend dashboard(호스트 추세 대시보드) - 선택한 기간 동안 선택한 호스트의 리소스 사용량(가상 시스템, CPU, 메모리 및 네트워크 Tx/Rx 수)입니다. ● 가상 시스템 추세 대시보드 - 선택한 기간 동안 선택한 가상 시스템의 CPU, 메모리, 네트워크 Tx/Rx, 디스크 I/O(CPU, 메모리, 네트워크 Tx/Rx, 디스크 I/O) 사용. ● Host Resource Usage dashboard - 선택한 기간에 선택한 호스트에 대한 일일 및 매시간 리소스 사용량(가상 시스템, CPU, 메모리, 네트워크 Tx/Rx 수)입니다. ● 가상 시스템 리소스 사용 대시보드 - 선택한 기간에 선택한 가상 시스템의 일일 및 매시간 리소스 사용량(CPU, 메모리, 네트워크 Tx/Rx, 디스크 I/O)입니다.



참고

Grafana 대시보드에는 **Red Hat Virtualization** 관리 포털에 대한 직접 링크가 포함되어 있으므로 클러스터, 호스트 및 가상 시스템에 대한 추가 세부 정보를 빠르게 볼 수 있습니다.

4.1.1.4. 사용자 정의된 **Grafana** 대시보드

사용자 지정 대시보드를 만들거나 보고 요구 사항에 따라 기존 대시보드를 복사 및 수정할 수 있습니다.



참고

대시보드는 사용자 정의할 수 없습니다.

4.1.2. **Elasticsearch**의 원격 인스턴스에 지표 및 로그 전송



참고

Red Hat은 **Elasticsearch**를 소유하거나 유지 관리하지 않습니다. 이 옵션을 배포하려면 **Elasticsearch** 설정 및 유지 관리를 잘 알고 있어야 합니다.

메트릭 데이터와 로그를 기존 **Elasticsearch** 인스턴스에 보내도록 **Red Hat Virtualization Manager** 및 호스트를 구성할 수 있습니다.

이렇게 하려면 **Manager** 및 모든 호스트에서 **collectd** 및 **rsyslog** 를 구성하여 **engine.log**, **vdsm.log** 및 **collectd** 지표를 수집하고 **Elasticsearch** 인스턴스로 전송하는 **Ansible** 역할을 실행합니다.

사용 가능한 지표 스키마에 대한 설명이 포함된 전체 목록을 포함하여 자세한 내용은 [원격 Elasticsearch 인스턴스에 RHV 모니터링 데이터 전송을 참조하십시오](#).

4.1.2.1. **collectd** 및 **rsyslog** 설치

호스트에 **collectd** 및 **rsyslog** 를 배포하여 로그 및 지표를 수집합니다.



참고

새 호스트에 대해 이 절차를 반복할 필요가 없습니다. 추가되는 모든 새 호스트는 **host-deploy** 중에 **Elasticsearch**에 데이터를 전송하도록 관리자가 자동으로 구성합니다.

절차

1.

SSH를 사용하여 **Manager** 시스템에 로그인합니다.

2.

/etc/ovirt-engine-metrics/config.yml.example 을 복사하여 **/etc/ovirt-engine-metrics/config.yml.d/config.yml** 을 만듭니다.

```
# cp /etc/ovirt-engine-metrics/config.yml.example /etc/ovirt-engine-
metrics/config.yml.d/config.yml
```

3.

config.yml 에서 **ovirt_env_name** 및 **elasticsearch_host** 매개 변수를 편집하고 파일을 저장합니다. 다음 추가 매개 변수를 파일에 추가할 수 있습니다.

```
use_omasticsearch_cert: false
rsyslog_elasticsearch_usehttps_metrics: !!str off
rsyslog_elasticsearch_usehttps_logs: !!str off
```

•

인증서를 사용하는 경우 **use_omasticsearch_cert** 를 **true**로 설정합니다.

•

로그 또는 지표를 비활성화하려면 **rsyslog_elasticsearch_usehttps_metrics** 및/또는 **rsyslog_elasticsearch_usehttps_logs** 매개변수를 사용합니다.

4.

호스트에 **collectd** 및 **rsyslog** 를 배포합니다.

```
# /usr/share/ovirt-engine-
metrics/setup/ansible/configure_ovirt_machines_for_metrics.sh
```

configure_ovirt_machines_for_metrics.sh 스크립트는 **linux-system-roles** (**RHEL**의 시스템 역할을 사용하여 관리 및 구성 작업 참조)를 포함하는 **Ansible** 역할을 실행하고 호스트에 **rsyslog** 를 배포하고 구성하는 데 사용합니다. **rsyslog** 는 **collectd** 에서 지표를 수집하여 **Elasticsearch**로 보냅니다.

4.1.2.2. 로깅 스키마 및 로그 분석

Discover(검색) 페이지를 사용하여 **RHV**에서 수집한 데이터를 대화형으로 살펴봅니다. 수집된 각 결과 세트를 문서라고 합니다. 문서는 다음 로그 파일에서 수집됩니다.

- **engine.log** - 모든 **oVirt Engine UI** 충돌, **Active Directory** 조화, 데이터베이스 문제 및 기타 이벤트를 포함합니다.
- **VDSM.log** - 가상화 호스트의 관리자 에이전트인 **VDSM**의 로그 파일이며 호스트 관련 이벤트를 포함합니다.

다음 필드를 사용할 수 있습니다.

매개 변수	description
_id	문서의 고유 ID
_index	문서가 속한 인덱스의 ID입니다. project.ovirt-logs 접두사가 있는 인덱스는 검색 페이지에 있는 유일한 관련 인덱스입니다.
호스트 이름	engine.log의 경우 Manager의 호스트 이름입니다. vdsml.log의 경우 호스트의 호스트 이름입니다.
level	로그 레코드 심각도: TRACE, DEBUG, INFO, WARN, ERROR, FATAL.
message	문서 메시지의 본문입니다.
ovirt.class	이 로그를 생성한 Java 클래스의 이름입니다.
ovirt.correlationid	engine.log에만 해당. 이 ID는 관리자가 수행하는 단일 작업의 여러 부분을 서로 연결하는 데 사용됩니다.
ovirt.thread	로그 레코드가 생성된 Java 스레드의 이름입니다.
tag	데이터를 필터링하는 데 사용할 수 있는 사전 정의된 메타데이터 세트입니다.
@timestamp	레코드가 발행된 [time](Troubleshooting#information-is-missing-from-kibana).
_score	해당 없음
_type	해당 없음

매개 변수	description
ipaddr4	시스템의 IP 주소입니다.
ovirt.cluster_name	vdsm.log의 경우, 호스트가 속한 클러스터의 이름입니다.
ovirt.engine_fqdn	관리자의 FQDN.
ovirt.module_lineno	ovirt.class 에 정의된 명령을 실행한 파일 내의 파일 및 행 번호입니다.

4.1.3. Insights 배포

Red Hat Virtualization Manager가 설치된 기존 RHEL(Red Hat Enterprise Linux) 시스템에 Red Hat Insights를 배포하려면 다음 작업을 완료합니다.

- 시스템을 **Red Hat Insights** 애플리케이션에 등록합니다.
- **Red Hat Virtualization** 환경에서 데이터 수집을 활성화합니다.

4.1.3.1. 시스템을 Red Hat Insights에 등록

시스템을 등록하여 **Red Hat Insights** 서비스와 통신하고 **Red Hat Insights** 콘솔에 표시된 결과를 확인합니다.

```
[root@server ~]# insights-client --register
```

4.1.3.2. Red Hat Virtualization 환경에서 데이터 수집 활성화

다음 행을 포함하도록 **/etc/ovirt-engine/rhv-log-collector-analyzer/rhv-log-collector-analyzer.conf** 파일을 수정합니다.

```
upload-json=True
```

4.1.3.3. Insights 콘솔에서 Insights 결과 보기

시스템 및 인프라 결과는 **Insights 콘솔에서 볼 수 있습니다**. **Overview(개요)** 탭은 인프라에 대한 현재 위험 요소에 대한 대시보드 보기를 제공합니다. 이 시작 지점에서 특정 규칙이 시스템에 미치는 영향을

조사하거나 시스템 기반 접근 방식을 사용하여 시스템이 위험을 초래하는 모든 규칙 일치를 볼 수 있습니다.

절차

1. **Rule hits by severity**(심각도별 규칙 조회수)를 선택하여 인프라에 미치는 총 위험 (심각,중요,보통 또는 낮음)에 따라 규칙을 확인합니다.

또는
2. **Rule hits by category**(범주별 규칙 조회수)를 선택하여 인프라에 야기되는 위험 유형을 확인합니다(가용성,안정성,성능 또는 보안).
3. 이름별로 특정 규칙을 검색하거나 규칙 목록을 스크롤하여 해결을 자동화하는 **Ansible** 플레이북의 위험, 시스템 노출 및 가용성에 대한 높은 수준의 정보를 확인합니다.
4. 규칙을 클릭하여 규칙 설명을 확인하고 관련 기술 자료 문서에 대해 자세히 알아보고 영향을 받는 시스템 목록을 확인합니다.
5. 시스템을 클릭하여 탐지된 문제 및 문제 해결 단계에 대한 특정 정보를 확인합니다.

4.2. 로그 파일

4.2.1. Manager 설치 로그 파일

표 4.2. 설치

로그 파일	설명
/var/log/ovirt-engine/engine-cleanup-yyyy_mm_dd_hh_mm_ss.log	engine-cleanup 명령에서 로그합니다. Red Hat Virtualization Manager 설치를 재설정하는 데 사용되는 명령입니다. 명령을 실행할 때마다 로그가 생성됩니다. 실행 날짜와 시간은 파일 이름에 사용하여 여러 로그가 존재할 수 있습니다.
/var/log/ovirt-engine/engine-db-install-yyyy_mm_dd_hh_mm_ss.log	engine-setup 명령의 로그에서 엔진 데이터베이스의 생성 및 구성을 자세히 설명합니다.

로그 파일	설명
/var/log/ovirt-engine/ovirt-engine-dwh-setup-yyyy_mm_dd_hh_mm_ss.log	ovirt-engine-dwh-setup 명령의 로그. 이는 보고를 위한 ovirt_engine_history 데이터베이스를 만드는 데 사용되는 명령입니다. 명령을 실행할 때마다 로그가 생성됩니다. 실행 날짜와 시간은 파일 이름에 사용하여 여러 로그를 동시에 만들 수 있습니다.
/var/log/ovirt-engine/setup/ovirt-engine-setup-yyyymmddhhmmss.log	engine-setup 명령의 로그. 명령을 실행할 때마다 로그가 생성됩니다. 실행 날짜와 시간은 파일 이름에 사용하여 여러 로그를 동시에 만들 수 있습니다.

4.2.2. Red Hat Virtualization Manager 로그 파일

표 4.3. 서비스 활동

로그 파일	설명
/var/log/ovirt-engine/engine.log	모든 Red Hat Virtualization Manager GUI 충돌, Active Directory 조회, 데이터베이스 문제 및 기타 이벤트를 반영합니다.
/var/log/ovirt-engine/host-deploy	Red Hat Virtualization Manager에서 배포된 호스트의 로그 파일입니다.
/var/lib/ovirt-engine/setup-history.txt	Red Hat Virtualization Manager와 관련된 패키지 설치 및 업그레이드를 추적합니다.
/var/log/httpd/ovirt-requests-log	HTTPS를 통해 Red Hat Virtualization Manager에 수행된 요청에서 각 요청이 걸리는 시간을 포함하여 파일을 기록합니다. 로그 파일을 /var/log/ovirt-engine/engine.log와 비교할 때 요청을 비교할 수 있도록 Correlation-Id 헤더가 포함되어 있습니다.
/var/log/ovn-provider/ovirt-provider-ovn.log	OVN 프로바이더의 활동을 기록합니다. Open vSwitch 로그에 대한 자세한 내용은 Open vSwitch 설명서 를 참조하십시오.

4.2.3. SPICE 로그 파일

SPICE 로그 파일은 **SPICE** 연결 문제를 해결할 때 유용합니다. **SPICE** 디버깅을 시작하려면 로그 수준을 디버깅으로 변경합니다. 그런 다음 로그 위치를 식별합니다.

게스트 시스템에 액세스하는 데 사용되는 클라이언트와 게스트 시스템에는 **SPICE** 로그 파일이 있습니다. 클라이언트측 로그의 경우 네이티브 클라이언트에서 **console.vv** 파일을 다운로드한 **SPICE** 클라이

언트를 시작한 경우 **remote-viewer** 명령을 사용하여 디버깅을 활성화하고 로그 출력을 생성합니다.

4.2.3.1. 하이퍼바이저 SPICE 서버용 SPICE 로그

표 4.4. 하이퍼바이저 SPICE 서버용 SPICE 로그

로그 유형	로그 위치	로그 수준을 변경하려면 다음을 수행합니다.
호스트/하이퍼바이저 SPICE 서버	/var/log/libvirt/qemu/(guest_name).log	게스트를 시작하기 전에 호스트/하이퍼바이저에서 내보내기 SPICE_DEBUG_LEVEL=5 를 실행합니다. 이 변수는 QEMU에서 구문 분석하며, system-wide를 실행하는 경우 시스템의 모든 가상 시스템의 디버깅 정보를 출력합니다. 이 명령은 클러스터의 각 호스트에서 실행해야 합니다. 이 명령은 클러스터별 기준이 아닌 호스트/하이퍼바이저 기반으로만 작동합니다.

4.2.3.2. 게스트 머신 용 SPICE 로그

표 4.5. 게스트 시스템용 spice-vdagent 로그

로그 유형	로그 위치	로그 수준을 변경하려면 다음을 수행합니다.
Windows 게스트	C:\Windows\Temp\vdagent.log C:\Windows\Temp\vdservice.log	해당 없음
Red Hat Enterprise Linux 게스트	journalctl 을 root 사용자로 사용합니다.	root 사용자가 이 항목으로 /etc/sysconfig/spice-vdagentd 파일을 만들므로 디버그 모드에서 spice-vdagentd 서비스를 실행하려면 다음을 실행합니다. SPICE_VDAGENTD_EXTRA_ARGS="-d -d" 디버그 모드에서 spice-vdagent를 실행하려면 명령줄에서 다음을 수행합니다. <pre>\$ killall -u \$USER spice-vdagent \$ spice-vdagent -x -d [-d] [& tee spice-vdagent.log]</pre>

4.2.3.3. console.vv 파일을 사용하여 시작되는 SPICE 클라이언트를 위한 SPICE 로그

Linux 클라이언트 시스템의 경우:

1. **remote-viewer** 명령을 **--spice-debug** 옵션으로 실행하여 **SPICE 디버깅을 활성화합니다.** 메시지가 표시되면 연결 **URL**을 입력합니다(예: **spice://virtual_machine_IP:포트**).

```
# remote-viewer --spice-debug
```

2. **debug** 매개 변수를 사용하여 **SPICE 클라이언트를 실행하고 .vv 파일을 전달하려면 console.vv 파일을 다운로드하고 --spice-debug 옵션을 사용하여 remote-viewer 명령을 실행하고 console.vv 파일의 전체 경로를 지정합니다.**

```
# remote-viewer --spice-debug /path/to/console.vv
```

Windows 클라이언트 머신의 경우:

1. **virt-viewer 2.0-11.el7ev 이상 버전에서 virt-viewer.msi 는 virt-viewer 및 debug-viewer.exe 를 설치합니다.**
2. **spice-debug** 인수와 함께 **remote-viewer** 명령을 실행하고 콘솔 경로에 있는 명령을 지시합니다.

```
remote-viewer --spice-debug path\to\console.vv
```

3. **로그를 보려면 가상 시스템에 연결하면 원격 뷰어의 표준 출력 및 표준 오류를 출력하는 GDB를 실행하는 명령 프롬프트가 표시됩니다.**

4.2.4. 호스트 로그 파일

로그 파일	설명
/var/log/messages	libvirt 에서 사용하는 로그 파일입니다. journalctl 을 사용하여 로그를 봅니다. 로그를 보려면 adm , systemd-journal 또는 wheel 그룹의 멤버여야 합니다.
/var/log/vdsm/spm-lock.log	스토리지 풀 관리자 역할에 대한 리스를 가져오는 호스트의 기능을 자세히 설명하는 로그 파일입니다. 호스트가 리스를 구입, 릴리스, 갱신 또는 갱신하지 못한 경우 로그 세부 정보입니다.

로그 파일	설명
/var/log/vdsm/vdsm.log	호스트의 관리자 에이전트인 VDSM에 대한 로그 파일입니다.
/tmp/ovirt-host-deploy-Date.log	호스트가 성공적으로 배포된 후 관리자에게 /var/log/ovirt-engine/host-deploy/ovirt-Date-Host-Correlation_ID.log 로 복사되는 호스트 배포 로그입니다.
/var/log/vdsm/import/import-UUID-Date.log	실패 정보 가져오기를 포함하여 KVM 호스트, VMWare 공급자 또는 RHEL 5 Xen 호스트에서 가상 시스템 가져오기를 설명하는 로그 파일입니다. <i>UUID</i> 는 가져온 가상 시스템의 UUID 이며 날짜는 가져오기를 시작한 날짜와 시간입니다.
/var/log/vdsm/supervdsm.log	수퍼유저 권한으로 실행된 VDSM 작업을 기록합니다.
/var/log/vdsm/upgrade.log	VDSM은 호스트 업그레이드 중에 이 로그 파일을 사용하여 구성 변경을 기록합니다.
/var/log/vdsm/mom.log	VDSM 메모리 과다 할당 관리자의 활동을 기록합니다.

4.2.5. Red Hat Virtualization 서비스에 대한 디버그 수준 로깅 설정

각 서비스의 **sysconfig** 파일을 수정하여 다음 **RHV(Red Hat Virtualization)** 서비스의 로그를 디버그 수준으로 설정할 수 있습니다.

표 4.6. RHV 서비스 및 **sysconfig** 파일 경로

Service	파일 경로
ovirt-engine.service	/etc/sysconfig/ovirt-engine
ovirt-engine-dwhd.service	/etc/sysconfig/ovirt-engine-dwhd
ovirt-fence-kdump-listener.service	/etc/sysconfig/ovirt-fence-kdump-listener
ovirt-websocket-proxy.service	/etc/sysconfig/ovirt-websocket-proxy

이 수정은 기본 서비스 프로세스가 아닌 **Python** 래퍼에서 수행한 로깅에 영향을 미칩니다.

로깅을 디버그 수준으로 설정하는 것은 시작과 관련된 문제를 디버깅하는 데 유용합니다(예: 누락되거나 잘못된 **Java** 런타임 또는 라이브러리로 인해 기본 프로세스가 시작되지 않는 경우).

사전 요구 사항

- 수정할 **sysconfig** 파일이 있는지 확인합니다. 필요한 경우 생성합니다.

절차

1. 서비스의 **sysconfig** 파일에 다음을 추가합니다.

```
OVIRT_SERVICE_DEBUG=1
```

2. 서비스를 다시 시작하십시오.

```
# systemctl restart <service>
```

서비스의 **sysconfig** 로그 파일이 이제 **debug-level**으로 설정됩니다.

이 설정으로 인한 로깅은 시스템 로그에 전송되므로 생성되는 로그는 서비스별 로그 파일이 아닌 **/var/log/messages**에 있거나 **journalctl** 명령을 사용하여 확인할 수 있습니다.

4.2.6. Red Hat Virtualization 서비스의 기본 설정 파일

sysconfig 파일 외에도 이러한 각 **RHV**(Red Hat Virtualization) 서비스에는 더 자주 사용되는 또 다른 구성 파일이 있습니다.

표 4.7. RHV 서비스 및 구성 파일

Service	sysconfig 파일 경로	기본 설정 파일
ovirt-engine.service	/etc/sysconfig/ovirt-engine	/etc/ovirt-engine/engine.conf.d/*.conf
ovirt-engine-dwhd.service	/etc/sysconfig/ovirt-engine-dwhd	/etc/ovirt-engine-dwhd/ovirt-engine-dwhd.conf.d/*.conf
ovirt-fence-kdump-listener.service	/etc/sysconfig/ovirt-fence-kdump-listener	/etc/ovirt-engine/ovirt-fence-kdump-listener.conf.d/*.conf

Service	sysconfig 파일 경로	기본 설정 파일
ovirt-websocket-proxy.service	/etc/sysconfig/ovirt-websocket-proxy	/etc/ovirt-engine/ovirt-websocket-proxy.conf.d/*.conf

4.2.7. 호스트 로깅 서버 설정

호스트는 로그 파일을 생성하고 업데이트하여 작업 및 문제를 기록합니다. 이러한 로그 파일을 수집하면 중앙에서 디버깅이 간소화됩니다.

이 절차는 중앙 집중식 로그 서버에서 사용해야 합니다. 별도의 로깅 서버를 사용하거나 다음 절차를 사용하여 **Red Hat Virtualization Manager**에서 호스트 로깅을 활성화할 수 있습니다.

절차

1.

방화벽이 **UDP 514** 포트에서 트래픽을 허용하는지 확인하고 **syslog** 서비스 트래픽에 열려 있는지 확인합니다.

```
# firewall-cmd --query-service=syslog
```

출력이 **no** 이면 다음을 사용하여 **UDP 514** 포트의 트래픽을 허용합니다.

```
# firewall-cmd --add-service=syslog --permanent
# firewall-cmd --reload
```

2.

syslog 서버에 새 **.conf** 파일을 생성합니다(예: **/etc/rsyslog.d/from_remote.conf**).

```
template(name="DynFile" type="string"
string="/var/log/%HOSTNAME%/%PROGRAMNAME%.log")
RuleSet(name="RemoteMachine"){ action(type="omfile" dynaFile="DynFile") }
Module(load="imudp")
Input(type="imudp" port="514" ruleset="RemoteMachine")
```

3.

rsyslog 서비스를 다시 시작하십시오.

```
# systemctl restart rsyslog.service
```

4.

하이퍼바이저에 로그인하고 `/etc/rsyslog.conf` 에 다음 행을 추가합니다.

```
*.info;mail.none;authpriv.none;cron.none @<syslog-FQDN>:514
```

5.

하이퍼바이저에서 **rsyslog** 서비스를 다시 시작합니다.

```
# systemctl restart rsyslog.service
```

이제 가상화 호스트에서 메시지 와 보안 로그를 수신하고 저장하도록 중앙 집중식 로그 서버가 구성되어 있습니다.

4.2.8. SyslogHandler를 활성화하여 RHV Manager 로그를 원격 syslog 서버에 전달

이 구현에서는 **JBoss EAP SyslogHandler** 로그 관리자를 사용하며 `engine.log` 및 `server.log` 에서 **syslog** 서버로 로그 레코드를 전달할 수 있습니다.

참고

RHV 4.4.10 미만의 **RHV** 버전에서는 `ovirt-engine-extension-logger-log4j` 에서 제공하는 유사한 기능이 추가되었습니다. 해당 패키지는 **RHV 4.4.10**에서 제거되었으며 **JBoss EAP SyslogHandler** 로그 관리자를 사용하여 새 구현으로 교체되었습니다. 이전 **RHV** 버전에서 `ovirt-engine-extension-logger-log4j` 를 사용하는 경우 **RHV 4.4.10**으로 업그레이드한 후 다음 단계를 수행합니다.

- 이 장에 제공된 지침을 사용하여 로그 레코드 전송을 원격 **syslog** 서버로 수동으로 구성합니다.
- `ovirt-engine-extension-logger-log4j` 구성 파일(`/etc/ovirt-engine/extensions.d/Log4j.properties` 구성 파일 제거)을 수동으로 제거합니다.

중앙 **syslog** 서버에서 다음 절차를 사용하십시오. 별도의 로깅 서버를 사용하거나 이 절차를 사용하여 **Manager**에서 **syslog** 서버로 `engine.log` 및 `server.log` 파일을 전달할 수 있습니다. [호스트 로깅 서버 설정도](#) 참조하십시오.

SyslogHandler 구현 구성

1.

`/etc/ovirt-engine/engine.conf.d` 디렉터리에 구성 파일 `90-syslog.conf.d`를 생성하고 다음

콘텐츠를 추가합니다.

```
SYSLOG_HANDLER_ENABLED=true
SYSLOG_HANDLER_SERVER_HOSTNAME=localhost
SYSLOG_HANDLER_FACILITY=USER_LEVEL
```

2.

rsyslog 를 설치하고 구성합니다.

```
# dnf install rsyslog
```

3.

rsyslog 트래픽을 허용하도록 **SELinux**를 구성합니다.

```
# semanage port -a -t syslogd_port_t -p udp 514
```

4.

구성 파일 **/etc/octets.d/rhvm.conf** 를 생성하고 다음 콘텐츠를 추가합니다.

```
user.* /var/log/jboss.log
module(load="imudp") # needs to be done just once
input(type="imudp" port="514")
```

5.

rsyslog 서비스를 다시 시작합니다.

```
# systemctl restart rsyslog.service
```

6.

방화벽이 활성화되어 활성 상태인 경우 다음 명령을 실행하여 방화벽에서 **rsyslog** 포트를 여는 데 필요한 규칙을 추가합니다.

```
# firewall-cmd --permanent --add-port=514/udp
# firewall-cmd --reload
```

7.

Red Hat Virtualization Manager를 다시 시작합니다.

```
# systemctl restart ovirt-engine
```

syslog 서버는 이제 **engine.log** 파일을 수신하고 저장할 수 있습니다.

부록 A. VDSM 서비스 및 후크

VDSM 서비스는 Red Hat Virtualization Manager에서 RHVH(Red Hat Virtualization Hosts) 및 Red Hat Enterprise Linux 호스트를 관리하는 데 사용됩니다. VDSM에서는 호스트의 스토리지, 메모리 및 네트워크 리소스를 관리하고 모니터링합니다. 또한 가상 머신 생성, 통계 수집, 로그 컬렉션 및 기타 호스트 관리 작업을 조정합니다. VDSM은 Red Hat Virtualization Manager에서 관리하는 각 호스트에서 데몬으로 실행됩니다. 클라이언트의 XML-RPC 호출에 응답합니다. Red Hat Virtualization Manager는 VDSM 클라이언트로 작동합니다.

VDSM은 후크를 통해 확장할 수 있습니다. 후크는 키 이벤트가 발생할 때 호스트에서 실행되는 스크립트입니다. 지원되는 이벤트 발생 시 VDSM이 호스트의 `/usr/libexec/vdsm/hooks/nn_event-name/`에서 실행 가능한 후크 스크립트를 영숫자순으로 실행합니다. 일반적으로 각 후크 스크립트에는 파일 이름 앞에 포함된 두 자리 숫자가 할당되어 에서 스크립트를 실행할 순서가 명확합니다. 후크 스크립트는 모든 프로그래밍 언어로 만들 수 있지만, Python은 이 장에 포함된 예제에 사용됩니다.

이벤트의 호스트에서 정의된 모든 스크립트가 실행됩니다. 호스트에서 실행되는 가상 머신의 하위 집합에 대해서만 지정된 후크를 실행해야 하는 경우, 가상 머신과 연결된 사용자 정의 속성을 평가하여 후크 스크립트 자체에서 이 요구 사항을 처리해야 합니다.



주의

VDSM 후크는 Red Hat Virtualization의 운영을 방해할 수 있습니다. VDSM 후크의 버그로 인해 가상 시스템이 충돌하고 데이터가 손실될 수 있습니다. VDSM 후크는 신중하게 구현하고 엄격한 테스트를 거쳐야 합니다. 후크 API는 새로운 기능이며 향후 상당한 변경이 발생할 수 있습니다.

이벤트 중심 후크를 사용하여 VDSM을 확장할 수 있습니다. 후크를 사용하여 VDSM 확장은 실험적 기술이며 이 장은 숙련된 개발자를 대상으로 합니다.

가상 시스템에서 사용자 지정 속성을 설정하면 지정된 가상 시스템에 고유한 추가 매개 변수를 후크 스크립트에 전달할 수 있습니다.

A.1. VDSM 후크 설치

기본적으로 VDSM 후크는 설치되지 않습니다. 특정 후크가 필요한 경우 수동으로 설치해야 합니다.

사전 요구 사항

- **호스트 리포지토리를 활성화해야 합니다.**
- **root 권한을 사용하여 호스트에 로그인되어 있습니다.**

절차

1. **사용 가능한 후크 목록을 가져옵니다.**

```
# dnf list vdsm\*hook\*
```

2. **원하는 **VDSM** 후크 패키지를 호스트에 설치합니다.**

```
# dnf install <vdsm-hook-name>
```

예를 들어 호스트에 **vdsm-hook-vhostmd** 패키지를 설치하려면 다음을 입력합니다.

```
# dnf install vdsm-hook-vhostmd
```

추가 리소스

- [Red Hat Virtualization Host Repository 활성화](#)
- [Red Hat Enterprise Linux 호스트 리포지토리 활성화](#)

A.2. 지원되는 VDSM 이벤트

표 A.1. 지원되는 VDSM 이벤트

이름	설명
before_vm_start	가상 시스템이 시작되기 전.
after_vm_start	가상 시스템이 시작된 후.
before_vm_cont	가상 시스템이 계속되기 전에.

이름	설명
after_vm_cont	가상 시스템이 계속되면.
before_vm_pause	가상 머신을 일시 중지하기 전에.
after_vm_pause	가상 머신이 일시 중지된 후.
before_vm_hibernate	가상 시스템 최대화 전.
after_vm_hibernate	가상 시스템 최대 절전 후.
before_vm_dehibernate	가상 시스템이 손상되기 전.
after_vm_dehibernate	가상 시스템이 손상된 후.
before_vm_migrate_source	가상 시스템을 마이그레이션하기 전에 마이그레이션이 진행되는 소스 호스트에서 를 실행합니다.
after_vm_migrate_source	가상 시스템을 마이그레이션한 후 마이그레이션이 진행되는 소스 호스트에서 를 실행합니다.
before_vm_migrate_destination	가상 시스템을 마이그레이션하기 전에 마이그레이션이 진행되는 대상 호스트에서 를 실행합니다.
after_vm_migrate_destination	가상 시스템을 마이그레이션한 후 마이그레이션이 진행되는 대상 호스트에서 를 실행합니다.
after_vm_destroy	가상 머신이 제거된 후.
before_vdsm_start	VDSM을 호스트에서 시작하기 전에. before_vdsm_start 후크를 사용자 root로 실행하고 VDSM 프로세스의 환경을 상속하지 마십시오.
after_vdsm_stop	VDSM이 호스트에서 중지된 후 after_vdsm_stop 후크가 사용자 root로 실행되며 VDSM 프로세스의 환경을 상속하지 않습니다.
before_nic_hotplug	NIC가 핫플러그되기 전에 가상 머신에 연결하기 전에.
after_nic_hotplug	NIC가 핫플러그된 후 가상 머신에 연결합니다.
before_nic_hotunplug	NIC가 핫 플러그 해제되기 전에 가상 머신에서 NIC를 핫 플러그 해제합니다
after_nic_hotunplug	NIC가 핫 플러그 해제된 후 가상 머신에서 연결을 해제합니다.

이름	설명
after_nic_hotplug_fail	NIC를 가상 머신에 핫 플러그로 연결하면 실패합니다.
after_nic_hotunplug_fail	가상 머신에서 NIC를 핫플러그 해제하면 실패합니다.
before_disk_hotplug	디스크가 핫플러그되기 전에 가상 머신에 연결하기 전에.
after_disk_hotplug	디스크를 핫플러그한 후 가상 머신에 연결합니다.
before_disk_hotunplug	디스크가 핫플러그되기 전에 가상 머신에서 연결을 해제합니다
after_disk_hotunplug	디스크가 핫플러그되면 가상 시스템에서 연결을 해제합니다.
after_disk_hotplug_fail	디스크를 가상 머신에 핫 플러그로 연결하면 실패합니다.
after_disk_hotunplug_fail	가상 시스템에서 디스크를 핫플러그 해제하면 실패합니다.
before_device_create	사용자 지정 속성을 지원하는 장치를 만들기 전에.
after_device_create	사용자 지정 속성을 지원하는 장치를 생성한 후.
before_update_device	사용자 지정 속성을 지원하는 장치를 업데이트하기 전에.
after_update_device	사용자 지정 속성을 지원하는 장치를 업데이트한 후.
before_device_destroy	사용자 지정 속성을 지원하는 장치를 제거하기 전에 다음을 수행합니다.
after_device_destroy	사용자 지정 속성을 지원하는 장치를 삭제한 후.
before_device_migrate_destination	장치 마이그레이션 전에 마이그레이션이 수행 중인 대상 호스트에서 를 실행합니다.
after_device_migrate_destination	장치 마이그레이션 후 마이그레이션이 발생하는 대상 호스트에서 를 실행합니다.
before_device_migrate_source	장치 마이그레이션 전에 마이그레이션이 진행되는 소스 호스트에서 를 실행합니다.
after_device_migrate_source	장치 마이그레이션 후 마이그레이션이 진행되는 소스 호스트에서 를 실행합니다.

이름	설명
after_network_setup	호스트 시스템을 시작할 때 네트워크를 설정한 후.
before_network_setup	호스트 시스템을 시작할 때 네트워크를 설정하기 전에.

A.3. VDSM 후크 환경

대부분의 후크 스크립트는 **vds**m 사용자로 실행되며 **VDSM** 프로세스의 환경을 상속받습니다. 예외는 **before_vds**m_start 및 **after_vds**m_stop 이벤트에서 트리거하는 후크 스크립트입니다. 이러한 이벤트에서 트리거한 후크 스크립트는 **root** 사용자로 실행되며 **VDSM** 프로세스의 환경을 상속하지 않습니다.

A.4. VDSM 후크 도메인 XML 객체

VDSM에서는 **libvirt** 도메인 XML 형식을 사용하여 가상 머신을 정의합니다. 가상 시스템의 **UUID**는 도메인 XML에서 추론할 수 있지만 환경 변수 **vmld**로도 사용할 수 있습니다.

후크 스크립트가 시작되면 **_hook_domxml** 변수가 환경에 추가됩니다. 이 변수에는 관련 가상 머신의 **libvirt** 도메인 XML 표현 경로가 포함되어 있습니다.

일부 후크는 이 규칙의 예외입니다. 다음 후크에는 가상 머신이 아닌 **NIC**의 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 도메인 XML을 수신합니다. 대상의 도메인 XML은 다릅니다.

A.5. 사용자 정의 속성 정의

Red Hat Virtualization Manager에서 수락하고 사용자 지정 후크로 전달되는 사용자 정의 속성은 **engine-config** 명령을 사용하여 정의됩니다. **Red Hat Virtualization Manager**가 설치된 호스트에서 **root** 사용자로 이 명령을 실행합니다.

UserDefinedVMProperties 및 **CustomDeviceProperties** 구성 키는 지원되는 사용자 정의 속성의 이름을 저장하는 데 사용됩니다. 명명된 각 사용자 지정 속성에 유효한 값을 정의하는 정규 표현식도 이러한 구성 키에 포함됩니다.

여러 사용자 지정 속성은 세미콜론으로 구분됩니다. 구성 키를 설정할 때 포함된 기존 값을 덮어씁니다. 새 속성과 기존 사용자 지정 속성을 결합할 때 키 값을 설정하는 데 사용되는 명령에 있는 모든 사용자 지정 속성을 포함해야 합니다.

구성 키가 업데이트되면 새 값을 적용하려면 **ovirt-engine** 서비스를 다시 시작해야 합니다.

예 A.1. 가상 머신 속성 - 스마트 카드 사용자 정의 속성 정의

1.

다음 명령을 사용하여 **UserDefinedVMProperties** 구성 키로 정의된 기존 사용자 정의 속성을 확인합니다.

```
# engine-config -g UserDefinedVMProperties
```

아래 출력에 표시된 대로 사용자 지정 속성 메모리는 이미 정의되어 있습니다. 정규 표현식 **^[0-9]+\$**은 사용자 지정 속성에 숫자만 포함하도록 합니다.

```
# engine-config -g UserDefinedVMProperties
UserDefinedVMProperties: version: 4.3
UserDefinedVMProperties: version: 4.4
UserDefinedVMProperties : memory=^[0-9]+$ version: 4.4
```

2.

메모리 사용자 지정 속성은 이미 **UserDefinedVMProperties** 구성 키에 정의되어 있으므로 새 사용자 지정 속성을 추가해야 합니다. 추가 사용자 지정 속성인 **Smartcard**가 구성 키의 값에 추가됩니다. 새 사용자 지정 속성은 **true** 또는 **false** 값을 보유할 수 있습니다.

```
# engine-config -s UserDefinedVMProperties='memory=[0-9]+$;smartcard=^(true|false)$'
--cver=4.4
```

3.

UserDefinedVMProperties 구성 키로 정의된 사용자 지정 속성이 올바르게 업데이트되었는지 확인합니다.

```
# engine-config -g UserDefinedVMProperties
UserDefinedVMProperties: version: 4.3
UserDefinedVMProperties: version: 4.4
UserDefinedVMProperties : memory=[0-9]+$;smartcard=^(true|false)$ version: 4.4
```

4.

마지막으로 구성 변경 사항을 적용하려면 **ovirt-engine** 서비스를 다시 시작해야 합니다.

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

예 A.2. 장치 속성 - 인터페이스 사용자 정의 속성 정의

1.

다음 명령을 사용하여 **CustomDeviceProperties** 구성 키로 정의된 기존 사용자 정의 속성을 확인합니다.

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

아래 출력에 표시된 대로 사용자 지정 속성이 아직 정의되지 않았습니다.

```
# engine-config -g CustomDeviceProperties
CustomDeviceProperties: version: 4.3
CustomDeviceProperties: version: 4.4
```

2.

인터페이스 사용자 지정 속성이 아직 존재하지 않으므로 그대로 추가할 수 있습니다. 이 예에서 속도 하위 속성의 값은 0에서 99999까지의 범위로 설정되고 이중 하위 속성의 값은 **full** 또는 **half**의 선택으로 설정됩니다.

```
# engine-config -s CustomDeviceProperties="{type=interface;prop={speed=[0-9]{1,5}}$;duplex=^(full|half)$}" --cver=4.4
```

3.

CustomDeviceProperties 구성 키로 정의된 사용자 지정 속성이 올바르게 업데이트되었는지 확인합니다.

```
# engine-config -g CustomDeviceProperties
UserDefinedVMProperties: version: 4.3
```

```
UserDefinedVMProperties: version: 4.4
UserDefinedVMProperties : {type=interface;prop={speed=^[0-9]{1,5}}$;duplex=^(full|half)$}} version: 4.4
```

4.

마지막으로 구성 변경 사항을 적용하려면 **ovirt-engine** 서비스를 다시 시작해야 합니다.

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

A.6. 가상 머신 사용자 정의 속성 설정

Red Hat Virtualization Manager에 사용자 지정 속성을 정의하면 가상 머신에서 설정을 시작할 수 있습니다. 사용자 지정 속성은 관리 포털에서 **New Virtual Machine**(새 가상 시스템) 및 **Edit Virtual Machine** (가상 시스템 편집) 창의 **Custom Properties**(사용자 지정 속성) 탭에 설정됩니다.

Run Virtual Machine(s)(가상 시스템 실행) 대화 상자에서 사용자 지정 속성을 설정할 수도 있습니다. **Run Virtual Machine(s)**(가상 시스템 실행) 대화 상자에서 설정한 사용자 지정 속성은 다음 종료 시점까지 가상 시스템에만 적용됩니다.

Custom Properties(사용자 정의 속성) 탭은 정의된 사용자 정의 속성 목록에서 선택할 수 있는 기능을 제공합니다. 사용자 정의 속성 키를 선택하면 추가 필드가 표시되어 해당 키의 값을 입력할 수 있습니다. + 버튼을 클릭하고 - 버튼을 클릭하여 키/값 쌍을 추가로 추가합니다.

A.7. VDSM 후크에서 가상 머신 사용자 정의 속성 평가

후크 스크립트를 호출할 때 가상 시스템의 **Custom Properties**(사용자 정의 속성) 필드에 설정된 각 키가 환경 변수로 추가됩니다. **Custom Properties**(사용자 지정 속성) 필드의 유효성을 검사하는 데 사용되는 정규 표현식이 일부 보호 기능을 제공하지만 스크립트가 제공된 입력이 예상과 일치하는지 확인해야 합니다.

예 A.3. 사용자 정의 속성 평가

이 짧은 **Python** 예제에서는 사용자 지정 속성 **key1**이 있는지 확인합니다. 사용자 지정 속성이 설정되면 값이 표준 오류로 출력됩니다. 사용자 지정 속성이 설정되지 않으면 작업이 수행되지 않습니다.

```
#!/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.8. VDSM 후크 모듈 사용

VDSM은 Python 후크 모듈과 함께 제공되어 VDSM 후크 스크립트의 도우미 기능을 제공합니다. 이 모듈은 예제로 제공되며 Python으로 작성된 VDSM 후크에만 관련이 있습니다.

hooking 모듈은 가상 머신의 libvirt XML을 Track 오브젝트로 읽는 기능을 지원합니다. 그런 다음 후크 스크립트는 Python의 기본 제공 [xml.dom 라이브러리](#)를 사용하여 오브젝트를 조작할 수 있습니다.

그런 다음 수정된 오브젝트를 hooking 모듈을 사용하여 libvirt XML로 다시 저장할 수 있습니다. 후크 모듈은 후크 개발을 지원하는 다음 기능을 제공합니다.

표 A.2. 모듈 기능 후크

이름	인수	설명
tobool	string	"true" 또는 "false" 문자열을 부울 값으로 변환합니다.
read_domxml	-	가상 머신의 libvirt XML을 RAW 객체로 읽습니다.
write_domxml	PART 개체	DEV 객체에서 가상 머신의 libvirt XML 작성

A.9. VDSM 후크 실행

before_vm_start 스크립트는 libvirt에 도달하기 전에 가상 시스템의 VDSM 정의를 변경하기 위해 도메인 XML을 편집할 수 있습니다. 이 작업을 수행하려면 반드시 주의해야 합니다. 후크 스크립트는 VDSM의 작동을 중단할 수 있으며 버그 스크립트로 인해 Red Hat Virtualization 환경이 중단될 수 있습니다. 특히 도메인의 UUID를 변경하지 않고 충분한 배경 지식 없이 도메인에서 장치를 제거하지 않도록 합니다.

before_vdsm_start 및 after_vdsm_stop 후크 스크립트는 모두 root 사용자로 실행됩니다. 시스템에 대한 루트 액세스 권한이 필요한 기타 후크 스크립트는 권한 에스컬레이션에 sudo 명령을 사용하도록 작성해야 합니다. 이를 지원하려면 vdsm 사용자가 암호를 다시 입력하지 않고 sudo를 사용할 수 있도록 /etc/sudoers를 업데이트해야 합니다. 후크 스크립트가 비대화식으로 실행되므로 이 작업이 필요합니다.

예 A.4. VDSM 후크에 대한 sudo 구성

이 예제에서는 **vds**m 사용자가 **/bin/chown** 명령을 **root** 로 실행할 수 있도록 **sudo** 명령을 구성합니다.

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 **vds**m 사용자에게 **/bin/chown** 명령을 **root** 사용자로 실행할 수 있음을 지정합니다. **NOPASSWD** 매개 변수는 **sudo** 를 호출할 때 사용자에게 암호를 입력하라는 메시지가 표시되지 않음을 나타냅니다.

이 구성을 변경하면 **VDSM** 후크가 **sudo** 명령을 사용하여 **/bin/chown** 을 **root** 로 실행할 수 있습니다. 이 **Python** 코드는 **sudo** 를 사용하여 **/bin/chown** 을 **/my_file** 파일에서 **root** 로 실행합니다.

```
retcode = subprocess.call(["/usr/bin/sudo", "/bin/chown", "root", "/my_file"])
```

후크 스크립트의 표준 오류 스트림은 **VDSM**의 로그에 수집됩니다. 이 정보는 후크 스크립트를 디버깅하는 데 사용됩니다.

A.10. VDSM 후크 반환 코드

후크 스크립트는 후크 반환 코드에 표시된 반환 코드 중 하나를 반환해야 합니다. 반환 코드는 **VDSM**에서 추가 후크 스크립트를 처리할지 여부를 결정합니다.

표 A.3. 후크 반환 코드

코드	설명
0	후크 스크립트가 성공적으로 종료되었습니다

코드	설명
1	후크 스크립트가 실패했습니다. 다른 후크를 처리해야 합니다.
2	후크 스크립트가 실패했습니다. 더 이상 후크를 처리하지 않아야 합니다.
>2	예약됨

A.11. VDSM 후크 예

이 섹션에서 제공하는 예제 후크 스크립트는 **Red Hat**에서 엄격하게 지원하지 않습니다. 소스와 관계없이 시스템에 설치하는 모든 후크 스크립트가 환경에 맞게 철저하게 테스트되었는지 확인해야 합니다.

예 A.5. NUMA 노드 튜닝

목적:

이 후크 스크립트를 사용하면 **numaset** 사용자 지정 속성을 기반으로 **NUMA** 호스트에서 메모리 할당을 조정할 수 있습니다. 사용자 지정 속성이 설정되지 않은 위치입니다.

구성 문자열:

```
numaset=^(interleave|strict|preferred):[^\?]\d+(-\d+)?(,[^\?]\d+(-\d+)?)*$
```

사용된 정규 표현식을 사용하면 지정된 가상 시스템의 **numaset** 사용자 지정 속성에서 할당 모드(인터리브, 엄격한, 기본 설정)와 사용할 노드 모두를 지정할 수 있습니다. 두 값은 콜론(:)으로 구분됩니다. 정규 표현식을 사용하면 다음과 같이 노드 세트를 지정할 수 있습니다.

- 특정 노드(**numaset=strict:1**) 가 노드 1만 사용됨을 지정합니다.
- 사용 가능한 노드 범위(**numaset=strict:1-4**, 노드가 1-4로 사용됨) 또는
- (**numaset=strict:~3**) 특정 노드가 사용되지 않는 경우 노드 3을 사용하지 않도록 지정합니다.

- 위의 쉘표로 구분된 조합(*numaset=strict:1-4,6*)은 노드를 1에서 4로, 6을 사용하도록 지정합니다.

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 매개변수 설명

표 B.1. bridge_opts parameters

매개변수	설명
forward_delay	브릿지가 수신 대기 및 학습 상태에 소비하는 시간을 디시초 단위로 설정합니다. 이번에는 전환 루프가 발견되지 않으면 브릿지가 전달 상태가 됩니다. 이렇게 하면 일반적인 네트워크 작업 전에 네트워크의 트래픽과 레이아웃을 검사할 수 있습니다.
group_addr	일반 쿼리를 보내려면 이 값을 0으로 설정합니다. 그룹별 그룹별 및 소스별 쿼리를 보내려면 이 값을 IP 주소가 아닌 6바이트 MAC 주소로 설정합니다. 허용되는 값은 01:80:C2:00:00 :01 , 01:80:C2:C2:00:00 :02 및 01:80:C2:00:00 :03 을 제외한 01:80:C2:00:00:0x 입니다.
group_fwd_mask	브리지를 활성화하여 링크 로컬 그룹 주소를 전달합니다. 이 값을 기본값에서 변경하면 비표준 브리징 동작이 허용됩니다.
hash_max	해시 테이블의 최대 버킷 양입니다. 이는 즉시 적용되며 현재 멀티캐스트 그룹 항목 수보다 작은 값으로 설정할 수 없습니다. 값은 2의 거듭제곱이어야 합니다.
hello_time	네트워크 토폴로지에서 브리지 위치를 발표하는 동안 'hello' 메시지 보내기 사이의 시간 간격을 설정합니다. 이 브릿지가 스페닝 트리 루트 브리지인 경우에만 적용됩니다.
max_age	브릿지가 종료된 것으로 간주되고 인수가 시작되기 전에 다른 루트 브리지에서 'hello' 메시지를 받을 수 있도록 최대 시간(디시초)을 설정합니다.
multicast_last_member_count	호스트에서 '리프 그룹' 메시지를 수신한 후 멀티캐스트 그룹으로 전송된 '마지막 멤버' 쿼리 수를 설정합니다.
multicast_last_member_interval	'마지막 멤버' 쿼리 간에 시간을 디시초 단위로 설정합니다.
multicast_membership_interval	멀티캐스트 트래픽 전송을 호스트로 중지하기 전에 브릿지가 멀티캐스트 그룹의 구성원으로부터 수신 대기하는 시간을 디시초 단위로 설정합니다.

매개변수	설명
multicast_querier	브리지가 멀티 캐스트 쿼리를 실행하는지 여부를 설정합니다. 브리지가 다른 네트워크 호스트에서 'multicast 호스트 멤버십' 쿼리를 수신하면 쿼리가 수신된 시간과 멀티캐스트 쿼리 간격 시간을 기준으로 해당 호스트를 추적합니다. 나중에 브리지가 해당 멀티캐스트 멤버십에 대한 트래픽을 전달하거나 쿼리 멀티캐스트 라우터와 통신하려는 경우 이 타이머는 쿼리의 유효성을 확인합니다. 유효한 경우 멀티 캐스트 트래픽은 브리지의 기존 멀티 캐스트 멤버십 테이블을 통해 전달됩니다. 더 이상 유효하지 않으면 트래픽이 모든 브리지 포트를 통해 전송됩니다. 성능을 향상시키기 위해 멀티 캐스트 멤버십을 하나 이상 실행해야 합니다.
multicast_querier_interval	호스트에서 수신한 마지막 'multicast 호스트 멤버십' 쿼리 간에 최대 시간(분)을 설정하여 계속 유효한지 확인합니다.
multicast_query_use_ifaddr	부울. 기본값은 '0'이며, 이 경우 쿼리에서 IPv4 메시지의 소스 주소로 0.0.0.0을 사용합니다. 이렇게 변경하면 브리지 IP가 소스 주소로 설정됩니다.
multicast_query_interval	멀티캐스트 멤버십의 유효성을 보장하기 위해 브리지에서 보낸 메시지를 쿼리하는 간 시간(디시초)을 설정합니다. 현재 또는 브리지가 해당 멤버십에 대한 멀티캐스트 쿼리를 보내야 하는 경우 브리지는 점점이 요청된 시간에 multicast_query_interval이 요청된 시간을 기준으로 자체 멀티캐스트 쿼리 상태를 확인합니다. 마지막 multicast_query_interval 내에 이 멤버십에 대한 멀티캐스트 쿼리가 전송된 경우 다시 전송되지 않습니다.
multicast_query_response_interval	길이(deciseconds)는 전송되면 호스트가 쿼리에 응답할 수 있습니다. multicast_query_interval 값보다 작거나 같아야 합니다.
multicast_router	멀티캐스트 라우터가 연결되어 있어 포트를 활성화하거나 비활성화할 수 있습니다. 하나 이상의 멀티캐스트 라우터가 있는 포트는 모든 멀티캐스트 트래픽을 수신합니다. 값 0은 완전히 비활성화되고, 값 1을 사용하면 쿼리를 기반으로 라우터의 존재를 자동으로 감지하고, 2 값을 사용하면 포트에서 항상 모든 멀티캐스트 트래픽을 수신할 수 있습니다.
multicast_snooping	스누핑이 활성화되었는지 여부를 토글합니다. 스누핑을 사용하면 브리지가 라우터와 호스트 간의 네트워크 트래픽을 수신 대기하여 적절한 링크에 대한 멀티캐스트 트래픽을 필터링하는 맵을 유지할 수 있습니다. 이 옵션을 사용하면 해시 충돌로 인해 자동으로 비활성화된 경우 스누핑을 다시 활성화할 수 있지만 해시 충돌이 해결되지 않은 경우 스누핑이 다시 활성화되지 않습니다.

매개변수	설명
multicast_startup_query_count	시작 시 전송된 쿼리 수를 설정하여 멤버십 정보를 확인합니다.
multicast_startup_query_interval	시작 시 전송된 쿼리 간 시간(디시초)을 설정하여 멤버십 정보를 결정합니다.

B.2. ETHTOOL을 사용하도록 RED HAT VIRTUALIZATION MANAGER 설정 방법

관리 포털에서 호스트 네트워크 인터페이스 카드의 **ethtool** 속성을 구성할 수 있습니다. **ethtool_opts** 키는 기본적으로 사용할 수 없으며 엔진 구성 도구를 사용하여 **Manager**에 추가해야 합니다. 호스트에 필요한 **VDSM** 후크 패키지도 설치해야 합니다.

관리자에 **ethtool_opts** 키 추가

1. **Manager**에서 다음 명령을 실행하여 키를 추가합니다.

```
# engine-config -s UserDefinedNetworkCustomProperties=ethtool_opts=. * --cver=4.4
```

2. **ovirt-engine** 서비스를 다시 시작하십시오.

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

3. **ethtool** 속성을 구성할 호스트에 **VDSM** 후크 패키지를 설치합니다. 패키지는 기본적으로 **Red Hat Virtualization Host**에서 사용할 수 있지만 **Red Hat Enterprise Linux** 호스트에 설치해야 합니다.

```
# dnf install vds-hook-ethtool-options
```

이제 관리 포털에서 **ethtool_opts** 키를 사용할 수 있습니다. [호스트 네트워크 인터페이스 편집 및 호스트에 논리적 네트워크 할당에서](#) **ethtool** 속성을 논리 네트워크에 적용합니다.

B.3. FCOE 사용을 위해 RED HAT VIRTUALIZATION MANAGER 설정 방법

관리 포털에서 호스트 네트워크 인터페이스 카드의 **FCoE(Fibre Channel over Ethernet)** 속성을 구성할 수 있습니다. **fcoe** 키는 기본적으로 사용할 수 없으며 엔진 구성 도구를 사용하여 **Manager**에 추가해야

합니다. 다음 명령을 실행하여 **fcoe** 가 이미 활성화되어 있는지 확인할 수 있습니다.

```
# engine-config -g UserDefinedNetworkCustomProperties
```

호스트에 필요한 **VDSM** 후크 패키지도 설치해야 합니다. 호스트의 **FCoE** 카드에 따라 특수 구성도 필요할 수 있습니다. **Red Hat Enterprise Linux**에서 스토리지 장치 관리에서 **Fibre Channel over Ethernet** 구성을 참조하십시오.

절차

1. **Manager**에서 다음 명령을 실행하여 키를 추가합니다.

```
# engine-config -s
UserDefinedNetworkCustomProperties='fcoe=^((enable|dcb/auto_vlan)=(yes/no),?)*$'
```

2. **ovirt-engine** 서비스를 다시 시작하십시오.

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

3. **FCoE** 속성을 구성할 각 **Red Hat Enterprise Linux** 호스트에 **VDSM** 후크 패키지를 설치합니다. 패키지는 **RHVH(Red Hat Virtualization Host)**에서 기본적으로 사용할 수 있습니다.

```
# dnf install vdsmd-hook-fcoe
```

이제 관리 포털에서 **fcoe** 키를 사용할 수 있습니다. **호스트 네트워크 인터페이스 편집** 및 **호스트에 논리 네트워크 할당**을 참조하여 **FCoE** 속성을 논리 네트워크에 적용합니다.

부록 C. RED HAT VIRTUALIZATION 사용자 인터페이스 플러그인

C.1. RED HAT VIRTUALIZATION 사용자 인터페이스 플러그인 정보

Red Hat Virtualization은 비표준 기능을 제공하는 플러그인을 지원합니다. 따라서 **Red Hat Virtualization** 관리 포털을 사용하여 다른 시스템과 쉽게 통합할 수 있습니다. 각 인터페이스 플러그인은 **Red Hat Virtualization**과 함께 사용할 수 있도록 패키징 및 배포할 수 있는 일련의 사용자 인터페이스 확장을 나타냅니다.

Red Hat Virtualization의 사용자 인터페이스 플러그인은 **JavaScript** 프로그래밍 언어를 사용하여 클라이언트에서 직접 관리 포털과 통합됩니다. 플러그인은 관리 포털에서 호출하고 웹 브라우저의 **JavaScript** 런타임에서 실행됩니다. 사용자 인터페이스 플러그인은 **JavaScript** 언어 및 해당 라이브러리를 사용할 수 있습니다.

런타임 중 주요 이벤트에서 관리 포털은 **Administration-Portal-to-plugin-in** 통신을 나타내는 이벤트 핸들러 기능을 통해 개별 플러그인을 호출합니다. 관리 포털에서 여러 이벤트 핸들러 기능을 지원하더라도 플러그인은 해당 구현에만 관심이 있는 함수를 선언합니다. 각 플러그인은 관리 포털에서 플러그인을 사용하도록 배치하기 전에 관련 이벤트 핸들러 기능을 플러그인 부트스트랩 시퀀스의 일부로 등록해야 합니다.

사용자 인터페이스 확장을 구동하는 플러그인-관리-포털 통신을 용이하게 하기 위해 관리 포털은 플러그인 **API**를 글로벌(최상위) **pluginApi JavaScript** 오브젝트로 노출하여 개별 플러그인에서 사용할 수 있습니다. 각 플러그인은 별도의 **pluginApi** 인스턴스를 가져와 관리 포털에서 플러그인의 라이프사이클과 관련하여 각 플러그인에 대한 플러그인 **API** 기능 호출을 제어할 수 있도록 합니다.

C.2. RED HAT VIRTUALIZATION 사용자 인터페이스 플러그인 라이프 사이클

사용자 인터페이스 플러그인의 기본 라이프 사이클은 세 단계로 나뉩니다.

- 플러그인 검색.
- 플러그인 로드.
- 플러그인 부트스트랩.

C.2.1. Red Hat Virtualization 사용자 인터페이스 플러그인 검색

플러그인 설명자 생성은 플러그인 검색 프로세스의 첫 번째 단계입니다. 플러그인 설명자에는 중요한 플러그인 메타데이터 및 선택적 기본 플러그인별 구성이 포함되어 있습니다.

관리 포털 **HTML** 페이지 요청(**HTTP GET**)을 처리하는 과정의 일환으로 사용자 인터페이스 플러그인 인프라는 로컬 파일 시스템에서 플러그인 설명자를 검색하고 로드하려고 합니다. 각 플러그인 설명자에 대해 인프라는 기본 플러그인별 구성(있는 경우)을 재정의하고 플러그인 런타임 동작을 수정하는 데 사용되는 해당 플러그인 사용자 구성을 로드하려고 합니다. 플러그인 사용자 구성은 선택 사항입니다. 설명자와 해당 사용자 구성 파일을 로드한 후 **oVirt Engine**은 사용자 인터페이스 플러그인 데이터를 집계하여 런타임 평가를 위해 관리 포털 **HTML** 페이지에 포함합니다.

기본적으로 플러그인 설명자는 **\$ENGINE_USR/ui-plug-ins**에 상주하며, 기본 매핑은 **oVirt Engine** 로컬 구성에 정의된 **ENGINE_USR=/usr/share/ovirt-engine**입니다. 플러그인 설명자는 **JSON** 형식 사양을 준수할 것으로 예상되지만 플러그인 설명자는 **JSON** 형식 사양 외에도 **Java/C++** 스타일 주석(**/*** 및 **MiB** 모두)을 허용합니다.

기본적으로 플러그인 사용자 구성 파일은 **\$ENGINE_ETC/ui-plug-ins**에 상주하며 **oVirt Engine** 로컬 구성에서 정의한 대로 기본 매핑 **ENGINE_ETC=/etc/ovirt-engine**이 있습니다. 플러그인 사용자 구성 파일은 플러그인 설명자와 동일한 콘텐츠 형식 규칙을 준수해야 합니다.



참고

플러그인 사용자 구성 파일은 일반적으로 **<descriptorFileName>-config.json** 명명 규칙을 따릅니다.

C.2.2. Red Hat Virtualization 사용자 인터페이스 플러그인 로딩

플러그인이 검색되고 해당 데이터가 관리 포털 **HTML** 페이지에 포함되면 관리 포털은 애플리케이션 시작의 일부로 플러그인을 로드하려고 합니다(애플리케이션 시작의 일부로 로드하지 않은 경우).

검색된 각 플러그인에 대해 관리 포털은 호스트 페이지를 로드하는 데 사용되는 **HTML iframe** 요소를 생성합니다. 플러그인 호스트 페이지는 플러그인의 **iframe** 요소 컨텍스트에서 플러그인 코드를 평가하는 데 사용되는 플러그인 부트스트랩 프로세스를 시작하는 데 필요합니다. 사용자 인터페이스 플러그인 인프라는 로컬 파일 시스템에서 플러그인 리소스 파일(예: 플러그인 호스트 페이지) 제공 기능을 지원합니다. 플러그인 호스트 페이지가 **iframe** 요소에 로드되고 플러그인 코드가 평가됩니다. 플러그인 코드를 평가한 후 플러그인은 플러그인 **API**를 통해 관리 포털과 통신합니다.

C.2.3. Red Hat Virtualization 사용자 인터페이스 플러그인 부트스트래핑

일반적인 플러그인 부트스트랩 시퀀스는 다음 단계로 구성됩니다.

플러그인 부트스트랩 순서

1. 주어진 플러그인에 대한 **pluginApi** 인스턴스 가져오기
2. 런타임 플러그인 구성 오브젝트 가져오기 (선택 사항)
3. 관련 이벤트 처리기 기능 등록
4. 플러그인 초기화를 진행하도록 **UI** 플러그인 인프라에 알립니다

다음 코드 조각은 연습에서 위에서 언급한 단계를 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({
  // Uilnit event handler function.
  Uilnit: function() {
    // Handle Uilnit 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 해당 위치

파일	위치	비고
플러그인 설명자 파일 (meta-data)	/usr/share/ovirt-engine/ui-plugins/my-plugin.json	
플러그인 사용자 구성 파일	/etc/ovirt-engine/ui-plugins/my-plugin-config.json	
플러그인 리소스 파일	/usr/share/ovirt-engine/ui-plugins/<resourcePath>/PluginHostPage.html	<resourcePath>는 플러그인 설명자의 해당 특성으로 정의됩니다.

C.4. 사용자 인터페이스 플러그인 배포 예

다음 지침에 따라 Red Hat Virtualization Manager 관리 포털에 로그인할 때 **Hello World!** 프로그램을 실행하는 사용자 인터페이스 플러그인을 생성합니다.

Hello World 배포! 플러그인

1.

Manager에 /usr/share/ovirt-engine/ui-plugins/helloWorld.json에 다음 파일을 생성하여 플러그인 설명자를 생성합니다.

```
{
  "name": "HelloWorld",
  "url": "/ovirt-engine/webadmin/plugin/HelloWorld/start.html",
  "resourcePath": "hello-files"
}
```

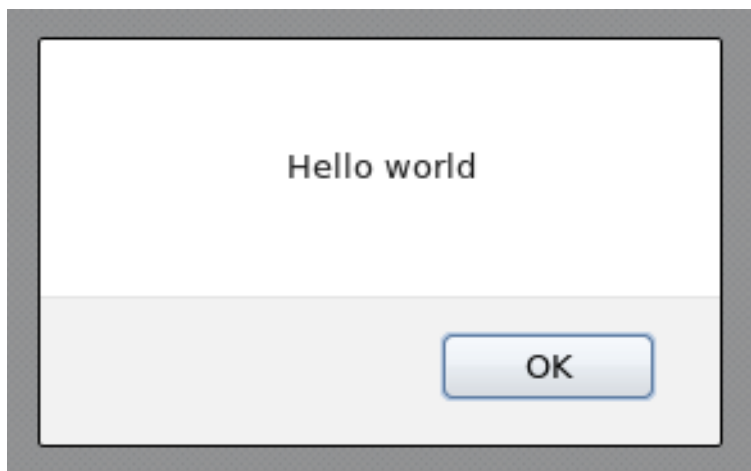
2.

Manager에 /usr/share/ovirt-engine/ui-plugins/hello-files/start.html에 다음 파일을 생성하여 플러그인 호스트 페이지를 생성합니다.

```
<!DOCTYPE html><html><head>
<script>
  var api = parent.pluginApi('HelloWorld');
  api.register({
    Uilnit: function() { window.alert('Hello world'); }
  });
  api.ready();
</script>
</head><body></body></html>
```

Hello World! 플러그인을 성공적으로 구현한 경우 관리 포털에 로그인하면 이 화면이 표시됩니다.

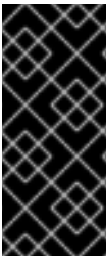
그림 C.1. Hello World의 성공적인 구현! 플러그인



부록 D. RED HAT VIRTUALIZATION에서 FIPS 활성화

Red Hat Virtualization을 **FIPS(Federal Information Processing Standard)**, 특히 **FIPS 140-2**에 맞게 설정할 수 있습니다. 조직의 **FIPS** 준수 요구 사항에 따라 특정 가상 머신, 베어 메탈 머신 또는 전체 환경에서 **FIPS** 모드를 선택적으로 활성화할 수 있습니다.

FIPS 모드에서 운영 체제를 설치하거나 운영 체제를 설치한 후 시스템을 **FIPS** 모드로 전환하여 **RHV 4.4**에서 **FIPS** 지원 베어 메탈 시스템을 생성할 수 있습니다. 그러나 시스템 충돌이 발생하지 않도록 **Red Hat Virtualization**을 설치하고 구성하기 전에 **FIPS** 모드로 전환해야 합니다.



중요

Red Hat은 나중에 **FIPS** 모드를 활성화하는 것과 달리 **FIPS** 모드가 활성화된 **RHEL 8**을 설치하는 것이 좋습니다. 설치 중에 **FIPS** 모드를 활성화하면 시스템이 **FIPS** 승인 알고리즘 및 지속적인 모니터링 테스트로 모든 키를 생성합니다.

각 베어 메탈 머신에서 먼저 **FIPS**를 활성화한 다음 **Manager**에서 **FIPS**를 활성화합니다.

- 자체 호스팅 엔진에서 **FIPS** 활성화
- **RHEL** 호스트에서 **FIPS** 활성화 및 독립 실행형 관리자

D.1. 자체 호스팅 엔진에서 FIPS 활성화

명령줄을 사용할 때 배포 중에 자체 호스팅 엔진에서 **FIPS**를 활성화할 수 있습니다.

절차

1. 셀프 호스팅 엔진 배포 스크립트를 시작합니다. 명령줄을 사용하여 자체 호스팅 엔진으로 **Red Hat Virtualization** 설치를 참조하십시오.
2. **FIPS**를 활성화하려면 배포 스크립트에 프롬프트가 표시되면 **Yes**를 입력합니다.

검증

호스트에 **fips-mode-setup --check** 명령을 입력하여 **FIPS**가 활성화되었는지 확인합니다. 이 명령은 **FIPS** 모드가 활성화되었습니다:

```
# fips-mode-setup --check
FIPS mode is enabled.
```

D.2. RHV 호스트 및 독립 실행형 관리자에서 **FIPS** 활성화

RHEL(Red Hat Enterprise Linux) 호스트 또는 **RHVV**(Red Hat Virtualization Host)를 설치할 때 **FIPS** 모드를 활성화할 수 있습니다. 자세한 내용은 [Red Hat Enterprise Linux 8의 보안 강화 가이드에서 **FIPS** 모드가 활성화된 **RHEL 8** 시스템 설치를 참조하십시오.](#) Red Hat은 프로비저닝된 호스트 또는 관리자 머신을 **FIPS** 모드로 전환할 수 없습니다

검증

호스트에 **fips-mode-setup --check** 명령을 입력하여 **FIPS**가 활성화되었는지 확인합니다. 이 명령은 **FIPS** 모드가 활성화되었습니다:

```
# fips-mode-setup --check
FIPS mode is enabled.
```

D.3. 추가 리소스

- [Red Hat Virtualization 호스트 설치](#)
- [설치 중 **SCAP** 정책 구성 및 적용](#)
- [Red Hat Virtualization Manager용 설치 프로그램 및 이미지\(v. 4.4 for x86_64\)](#)
- [SCAP 보안 가이드에서 사용 가능한 보안 정책](#)
- [Red Hat Enterprise Linux 8용 **Security Hardening**](#)

부록 E. RED HAT VIRTUALIZATION 및 암호화된 통신

E.1. RED HAT VIRTUALIZATION MANAGER CA 인증서 교체

조직의 타사 CA 인증서를 구성하여 HTTPS를 통해 Red Hat Virtualization Manager에 연결하는 사용자를 인증할 수 있습니다.

HTTPS 연결에 타사 CA 인증서를 사용하는 경우 관리자와 호스트 간의 인증에 사용되는 인증서에는 영향을 미치지 않습니다. 해당 인증서는 Manager에서 생성한 자체 서명 인증서를 계속 사용합니다.

P12 파일에서 CA에서 개인 키 및 인증서를 받은 경우 다음 절차를 사용하여 추출합니다. 다른 파일 형식은 CA에 문의하십시오. 개인 키와 인증서를 추출한 후 [Red Hat Virtualization Manager Apache CA 인증서 교체](#)를 진행합니다.

E.1.1. P12 번들에서 인증서 및 개인 키 추출

내부 CA는 내부적으로 생성된 키와 인증서를 P12 파일인 `/etc/pki/ovirt-engine/keys/apache.p12`에 저장합니다. 새 파일을 동일한 위치에 저장합니다. 다음 절차에서는 새 P12 파일이 `/tmp/apache.p12`에 있다고 가정합니다.



주의

`/etc/pki` 디렉토리 또는 하위 디렉토리에 대한 권한 및 소유권은 변경하지 마십시오. `/etc/pki` 및 `/etc/pki/ovirt-engine` 디렉토리에 대한 권한은 기본값인 755로 유지되어야 합니다.

절차

1. 현재 `apache.p12` 파일을 백업하십시오.

```
# cp -p /etc/pki/ovirt-engine/keys/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12.bck
```

2. 현재 파일을 새 파일로 바꿉니다.

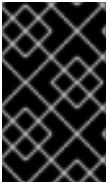
```
# cp /tmp/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12
```

3.

개인 키와 인증서를 필요한 위치에 추출합니다.

```
# openssl pkcs12 -in /etc/pki/ovirt-engine/keys/apache.p12 -nocerts -nodes > /tmp/apache.key
# openssl pkcs12 -in /etc/pki/ovirt-engine/keys/apache.p12 -nokeys > /tmp/apache.cer
```

파일이 암호로 보호되는 경우 명령에 **-passin pass:** 암호를 추가하고 암호를 필요한 암호로 바꿉니다.



중요

새로운 Red Hat Virtualization 설치의 경우 이 절차의 모든 단계를 완료해야 합니다.

E.1.2. Red Hat Virtualization Manager Apache CA 인증서 교체

조직의 타사 CA 인증서를 구성하여 사용자가 관리 포털과 HTTPS를 통해 VM 포털에 연결하는 사용자를 인증합니다.



주의

/etc/pki 디렉토리 또는 하위 디렉토리에 대한 권한 및 소유권은 변경하지 마십시오. **/etc/pki** 및 **/etc/pki/ovirt-engine** 디렉토리에 대한 권한은 기본값인 **755**로 유지되어야 합니다.

사전 요구 사항

•

타사 CA(인증 기관) 인증서. PEM 파일로 제공됩니다. 인증서 체인을 루트 인증서까지 완료해야 합니다. 체인의 순서는 매우 중요하며 마지막 중간 인증서부터 루트 인증서까지이어야 합니다. 이 절차에서는 타사 CA 인증서가 **/tmp/3rd-ca-cert.pem**에 제공된 것으로 가정합니다.

•

Apache httpd에 사용하려는 개인 키입니다. 암호가 없어야 합니다. 이 절차에서는 해당 파일이 **/tmp/apache.key**에 있다고 가정합니다.

•

CA에서 발급한 인증서입니다. 이 절차에서는 해당 파일이 **/tmp/apache.cer**에 있다고 가정

합니다.

절차

1. **셀프 호스트 엔진을 사용하는 경우 환경을 전역 유지 관리 모드로 설정합니다.**

```
# hosted-engine --set-maintenance --mode=global
```

자세한 내용은 [셀프 호스트 엔진 유지 관리](#)를 참조하십시오.

2. **호스트 전체 신뢰 저장소에 CA 인증서를 추가합니다.**

```
# cp /tmp/3rd-party-ca-cert.pem /etc/pki/ca-trust/source/anchors
# update-ca-trust
```

3. **Manager는 /etc/pki/ovirt-engine/apache-ca.pem 을 사용하도록 구성되었으며, 이 기능은 /etc/pki/ovirt-engine/ca.pem 에 심볼릭으로 연결됩니다. 심볼릭 링크를 제거합니다.**

```
# rm /etc/pki/ovirt-engine/apache-ca.pem
```

4. **CA 인증서를 /etc/pki/ovirt-engine/apache-ca.pem으로 저장합니다.**

```
# cp /tmp/3rd-party-ca-cert.pem /etc/pki/ovirt-engine/apache-ca.pem
```

5. **기존 개인 키 및 인증서를 백업합니다.**

```
# cp /etc/pki/ovirt-engine/keys/apache.key.nopass /etc/pki/ovirt-engine/keys/apache.key.nopass.bck
# cp /etc/pki/ovirt-engine/certs/apache.cer /etc/pki/ovirt-engine/certs/apache.cer.bck
```

6. **개인 키를 필요한 위치에 복사합니다.**

```
# cp /tmp/apache.key /etc/pki/ovirt-engine/keys/apache.key.nopass
```

7. **개인 키 소유자를 root로 설정하고 권한을 0640으로 설정합니다.**

```
# chown root:ovirt /etc/pki/ovirt-engine/keys/apache.key.nopass
# chmod 640 /etc/pki/ovirt-engine/keys/apache.key.nopass
```

8.

필요한 위치에 인증서를 복사합니다.

```
# cp /tmp/apache.cer /etc/pki/ovirt-engine/certs/apache.cer
```

9.

인증서 소유자를 **root**로 설정하고 권한을 **0644**로 설정합니다.

```
# chown root:ovirt /etc/pki/ovirt-engine/certs/apache.cer
# chmod 644 /etc/pki/ovirt-engine/certs/apache.cer
```

10.

Apache 서버를 다시 시작하십시오.

```
# systemctl restart httpd.service
```

11.

다음 매개 변수를 사용하여 새 신뢰 저장소 구성 파일 `/etc/ovirt-engine/engine.conf.d/99-custom-truststore.conf` 를 생성합니다.

```
ENGINE_HTTPS_PKI_TRUST_STORE="/etc/pki/java/cacerts"
ENGINE_HTTPS_PKI_TRUST_STORE_PASSWORD=""
```

12.

`/etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf` 파일을 복사하고 **10**보다 큰 인덱스 번호로 이름을 바꿉니다(예: `99-setup.conf`). 새 파일에 다음 매개변수를 추가합니다.

```
SSL_CERTIFICATE=/etc/pki/ovirt-engine/certs/apache.cer
SSL_KEY=/etc/pki/ovirt-engine/keys/apache.key.nopass
```

13.

websocket-proxy 서비스를 다시 시작합니다.

```
# systemctl restart ovirt-websocket-proxy.service
```

14.

`/etc/ovirt-provider-ovn/conf.d/10-setup-ovirt-provider-ovn.conf` 파일을 수동으로 변경하거나 이전 설치의 구성 파일을 사용하는 경우 **Manager**가 계속 `/etc/pki/ovirt-engine/apache-ca.pem` 을 인증서 소스로 사용하도록 구성되었는지 확인합니다.

15.

`/etc/ovirt-engine-backup/engine-backup-config.d` 디렉토리를 만듭니다.

```
# mkdir -p /etc/ovirt-engine-backup/engine-backup-config.d
```

16.

ovirt-engine-backup /engine-backup /engine-backup-config.d/update-system-wide-pki.sh 파일을 생성하여 복원 시 시스템을 업데이트합니다.

```
BACKUP_PATHS="${BACKUP_PATHS}
/etc/ovirt-engine-backup"
cp -f /etc/pki/ovirt-engine/apache-ca.pem \
/etc/pki/ca-trust/source/anchors/3rd-party-ca-cert.pem
update-ca-trust
```

17.

ovirt-provider-ovn 서비스를 다시 시작합니다.

```
# systemctl restart ovirt-provider-ovn.service
```

18.

ovirt-imageio 서비스를 다시 시작하십시오.

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

19.

ovirt-engine 서비스를 다시 시작하십시오.

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

20.

자체 호스팅 엔진을 사용하는 경우 글로벌 유지 관리 모드를 비활성화합니다.

```
# hosted-engine --set-maintenance --mode=none
```

이제 사용자가 인증서 경고가 표시되지 않고 관리 포털 및 VM 포털에 연결할 수 있습니다.

E.2. 관리자와 LDAP 서버 간의 암호화된 통신 설정

Red Hat Virtualization Manager와 LDAP 서버 간에 암호화된 통신을 설정하려면 LDAP 서버의 루트 CA 인증서를 가져오고 Manager에 루트 CA 인증서를 복사하고 PEM 인코딩 CA 인증서를 생성합니다. 키 저장소 유형은 모든 Java 지원 유형일 수 있습니다. 다음 절차에서는 Java KeyStore(JKS) 형식을 사용합니다.



참고

PEM 인코딩 CA 인증서 생성 및 인증서 가져오기에 대한 자세한 내용은 `/usr/share/doc/ovirt-engine-extension-aaa-ldap-<버전> README` 파일의 **X.509RTIFICATE TRUST STORE** 섹션을 참조하십시오.



참고

ovirt-engine-extension-aaa-ldap 는 더 이상 사용되지 않습니다. 새로 설치하는 경우 **Red Hat Single Sign On**을 사용하십시오. 자세한 내용은 관리 가이드의 [Red Hat Single Sign-On 설치 및 구성](#)을 참조하십시오.

절차

1.

Red Hat Virtualization Manager에서 **LDAP** 서버의 루트 **CA** 인증서를 `/tmp` 디렉터리에 복사하고 **keytool** 을 사용하여 루트 **CA** 인증서를 가져와 **PEM** 인코딩 **CA** 인증서를 생성합니다. 다음 명령은 `/tmp/myrootca.pem` 에 루트 **CA** 인증서를 가져오고 `/etc/ovirt-engine/aaa/` 에 **PEM** 인코딩 **CA** 인증서 `myrootca.jks` 를 만듭니다. 인증서의 위치와 암호를 기록해 둡니다. 대화식 설정 도구를 사용하는 경우 필요한 모든 정보입니다. **LDAP** 서버를 수동으로 구성하는 경우 나머지 절차에 따라 구성 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

`${local:_basedir}` 는 **LDAP** 속성 구성 파일이 상주하고 `/etc/ovirt-engine/aaa` 디렉터리를 가리키는 디렉터리입니다. 다른 디렉터리에 **PEM** 인코딩 **CA** 인증서를 생성한 경우 `${local:_basedir}` 을 인증서의 전체 경로로 바꿉니다.

•

startTLS(권장 사항)를 사용하려면 다음을 수행합니다.

```
# 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 수행합니다.

```
# 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 구성을 계속하려면 [외부 LDAP 공급자](#) 구성을 참조하십시오. Single Sign-on용 LDAP 및 Kerberos 구성을 계속하려면 [Single Sign-on 용 LDAP 및 Kerberos](#) 구성을 참조하십시오.

E.3. FIPS에 대해 암호화된 VNC 콘솔 활성화

RHV(Red Hat Virtualization) 관리자 및 FIPS가 활성화된 호스트에서 작동하도록 암호화된 VNC 콘솔을 설정할 수 있습니다.

암호화된 VNC 콘솔을 설정하려면 다음 절차를 완료합니다.

- [RHV에서 FIPS를 활성화합니다.](#)
- [VNC 암호화를 사용하도록 클러스터를 구성합니다.](#)
- [각 호스트에서 VNC SASL ansible 플레이북을 실행합니다.](#)
- [Manager의 CA 인증서를 신뢰하도록 Remote Viewer를 구성합니다.](#)

E.3.1. VNC 암호화를 활성화하도록 클러스터 구성

사전 요구 사항

- 클러스터에서 FIPS를 활성화해야 합니다.

절차

1. 관리 포털에서 **Compute(컴퓨팅) Clusters(클러스터)** 를 클릭합니다.
2. VNC 암호화를 활성화하려는 클러스터를 선택하고 편집을 클릭합니다. **Edit Cluster(클러스터)**

터 편집) 창이 열립니다.

3. **Console**(콘솔) 탭을 선택합니다.
4. **Enable VNC Encryption** 확인란을 선택하고 **OK**(확인)를 클릭합니다.

E.3.2. 각 호스트에 대해 VNC SASL Ansible 플레이북 실행

절차

1. 관리 포털에서 **FIPS** 지원 호스트를 유지 관리 모드로 설정합니다.
 - a. **Compute**(컴퓨팅) **Hosts**(호스트) 를 클릭합니다.
 - b. **Virtual Machines**(가상 시스템) 열에서 각 호스트에 0개의 가상 시스템이 있는지 확인합니다.

 필요한 경우 호스트에서 가상 시스템을 제거하려면 실시간 마이그레이션을 수행합니다. [호스트 간 가상 머신 마이그레이션](#) 을 참조하십시오.
 - c. 각 호스트를 선택하고 **Management** → **Maintenance** (관리 유지 관리) 및 **OK** (확인)를 클릭합니다.
2. **Manager**가 실행 중인 시스템의 명령줄에 연결합니다.
 - 독립 실행형 관리자:

```
# ssh root@rhvm
```
 - 셀프 호스트 엔진: **Compute** → **Virtual Machines** (가상 시스템)를 클릭하여 기본적으로 **HostedEngine** 이라는 자체 호스팅 엔진 가상 시스템을 선택한 다음 **Console** (콘솔)을 클릭합니다.
3. 각 호스트에 대해 **VNC SASL Ansible** 플레이북을 실행합니다.

```
# cd /usr/share/ovirt-engine/ansible-runner-service-project/project/
# ansible-playbook --ask-pass --inventory=<hostname> ovirt-vnc-sasl.yml <1>
```

Compute → 지정합니다.

4. 호스트를 선택하고 **Installation** → **Reinstall** (재설치)을 클릭합니다.
5. 재설치 후 호스트를 선택하고 **Management** → **Restart** (다시 시작)를 클릭합니다.
6. 재부팅 후 호스트를 선택하고 **Management** → **Activate** (활성화)를 클릭합니다.

VNC SASL Ansible Playbook 오류 메시지

VNC SASL Ansible 플레이북을 실행할 때 다음 오류 메시지와 함께 작업이 실패할 수 있습니다.

Using a SSH password instead of a key is not possible because Host Key checking is enabled and sshpass does not support this. Please add this host's fingerprint to your known_hosts file to manage this host.

이 문제를 해결하려면 다음 중 하나를 수행하여 호스트 키 검사를 비활성화합니다.

- `/etc/ansible/ansible.cfg`에서 다음 행의 주석을 제거하여 호스트 키 검사를 영구적으로 비활성화합니다.

```
#host_key_checking = False
```

- 다음 명령을 실행하여 호스트 키 검사를 일시적으로 비활성화합니다.

```
export ANSIBLE_HOST_KEY_CHECKING=False
```

추가 리소스

- [설치 중 SCAP 정책 구성 및 적용](#)
- [Red Hat Virtualization Manager용 설치 프로그램 및 이미지\(v. 4.3 for x86_64\)](#)

E.3.3. 관리자의 CA 인증서를 신뢰하도록 Remote Viewer 구성

RHV Manager의 CA(인증 기관)를 신뢰하도록 클라이언트 시스템, virt-viewer 또는 remote-viewer에서 Remote Viewer 콘솔을 구성합니다.

절차

1. **`https://<engine_address>/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA`로 이동합니다.**
2. **모든 신뢰 설정을 활성화합니다.**
3. **VNC 콘솔을 실행하려는 클라이언트 시스템에서 인증서 파일의 디렉토리를 생성합니다.**

```
$ mkdir ~/.pki/CA
```



주의

이 단계를 수행하면 **mkdir: 디렉토리 '/home/example_user/.pki/CA'를 생성할 수 없습니다: 파일이 exists, 다음 단계에서 ~/.pki/CA/cacert.pem을 덮어쓰지 않도록 예방합니다. 예를 들어, 파일 이름에 현재 날짜를 포함합니다.**

4. **인증서를 다운로드합니다.**

```
$ curl -k -o ~/.pki/CA/cacert-<today's date>.pem 'https://<engine_address>/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA'
```

5. **브라우저에서 인증 기관을 설치합니다.**



Firefox

- [Internet Explorer](#)
- [Google Chrome.](#)

6. 클라이언트 시스템에 **SASL SCRAM** 라이브러리를 설치합니다.

```
$ sudo dnf install cyrus-sasl-scam
```

검증 단계

1. 생성한 **FIPS** 지원 호스트 중 하나에서 가상 머신을 실행합니다.
2. **VNC** 콘솔을 사용하여 가상 머신에 연결합니다.

추가 리소스

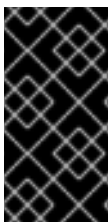
- [콘솔 구성 요소 설치](#)
- [Manager CA 인증서 교체](#)

부록 F. 프록시

F.1. SPICE 프록시

F.1.1. SPICE 프록시 개요

SPICE 프록시는 **SPICE** 클라이언트가 하이퍼바이저를 연결하는 네트워크 외부에 있을 때 **SPICE** 클라이언트를 가상 머신에 연결하는 데 사용되는 도구입니다. **SPICE** 프록시 설정은 시스템에 **Squid** 를 설치하고 프록시 트래픽을 허용하도록 방화벽을 구성하는 것입니다. **SPICE** 프록시 활성화는 **Manager**에서 **engine-config** 를 사용하여 **SpiceProxyDefault** 키를 프록시 이름과 포트로 구성된 값으로 설정하는 것입니다. **SPICE** 프록시를 끄는 작업은 **Manager**에서 **engine-config** 를 사용하여 **SpiceProxyDefault** 키가 설정된 값을 제거하는 것입니다.



중요

SPICE 프록시는 독립 실행형 **SPICE** 클라이언트와 함께 사용할 수 있으며 **noVNC**를 사용하여 가상 머신에 연결하는 데 사용할 수 없습니다.

F.1.2. SPICE 프록시 머신 설정

다음 절차에서는 시스템을 **SPICE** 프록시로 설정하는 방법을 설명합니다. **SPICE** 프록시를 사용하면 네트워크 외부에서 **Red Hat Virtualization** 네트워크에 연결할 수 있습니다. 이 프로세스에서 프록시 서비스를 제공하기 위해 **Squid** 를 사용합니다.

절차

1. 프록시 시스템에 **Squid** 를 설치합니다.

```
# dnf install squid
```

2. **/etc/squid/squid.conf** 를 엽니다. 변경:

```
http_access deny CONNECT !SSL_ports
```

다음으로 변경합니다.

```
http_access deny CONNECT !Safe_ports
```

3.

squid 서비스를 시작하고 재부팅 후 자동으로 실행되도록 설정합니다.

```
# systemctl enable squid.service --now
```

4.

기본 **firewalld** 영역에서 **squid** 서비스에 대한 들어오는 요청을 활성화합니다.

```
# firewall-cmd --permanent --add-service=squid
```

5.

런타임 구성에서 이 방화벽 규칙을 영구적으로 설정합니다.

```
# firewall-cmd --reload
```

6.

squid 서비스가 방화벽 서비스 목록에 표시되는지 확인합니다.

```
# firewall-cmd --list-services
ssh dhcpv6-client squid
```

이제 머신을 **SPICE** 프록시로 설정했습니다. 네트워크 외부에서 **Red Hat Virtualization** 네트워크에 연결하기 전에 **SPICE** 프록시를 활성화합니다.

F.1.3. SPICE 프록시 활성화

다음 절차에서는 **SPICE** 프록시를 활성화(또는 켜기)하는 방법을 설명합니다.

절차

1.

Manager에서 **engine-config** 도구를 사용하여 프록시를 설정합니다.

```
# engine-config -s SpiceProxyDefault=someProxy
```

2.

ovirt-engine 서비스를 다시 시작하십시오.

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

프록시에는 다음 형식이 있어야 합니다.

protocol://[host]:[port]



참고

Red Hat Enterprise Linux 6.7, Red Hat Enterprise Linux 7.2 이상과 함께 제공되는 SPICE 클라이언트만 HTTPS 프록시를 지원합니다. 이전 클라이언트는 HTTP만 지원합니다. HTTPS가 이전 클라이언트에 대해 지정된 경우 클라이언트는 프록시 설정을 무시하고 호스트에 대한 직접 연결을 시도합니다.

SPICE 프록시가 활성화되었습니다(위로 전환됨). 이제 **SPICE** 프록시를 통해 **Red Hat Virtualization** 네트워크에 연결할 수 있습니다.

F.1.4. SPICE 프록시 끄기

다음 절차에서는 **SPICE** 프록시를 비활성화(비활성화)하는 방법을 설명합니다.

절차

1. **Manager**에 로그인합니다.

```
$ ssh root@[IP of Manager]
```

2. 다음 명령을 실행하여 **SPICE** 프록시를 지웁니다.

```
# engine-config -s SpiceProxyDefault=""
```

3. 관리자를 다시 시작하십시오.

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

SPICE 프록시가 비활성화되었습니다(전원 해제됨). 더 이상 **SPICE** 프록시를 통해 **Red Hat Virtualization** 네트워크에 연결할 수 없습니다.

F.2. SQUID 프록시

F.2.1. Squid 프록시 설치 및 구성

이 섹션에서는 VM 포털에 대한 **Squid** 프록시를 설치하고 구성하는 방법을 설명합니다. **Squid** 프록시 서버는 콘텐츠 액셀러레이터로 사용됩니다. 자주 표시되는 콘텐츠를 캐시하고 대역폭을 줄이고 응답 시간을 개선합니다.

절차

1.

Squid 프록시 서버의 **HTTPS** 포트에 대한 키 쌍 및 인증서를 가져옵니다. 이 키 쌍을 다른 **SSL/TLS** 서비스의 키 쌍을 가져오는 것과 동일한 방식으로 가져올 수 있습니다. 키 쌍은 개인 키와 서명된 인증서를 포함하는 두 개의 **PEM** 파일의 형식입니다. 이 절차에서는 이름이 **proxy.key** 및 **proxy.cer** 라고 가정합니다.



참고

엔진의 인증 기관을 사용하여 키 쌍 및 인증서를 생성할 수도 있습니다. 프록시에 대한 개인 키와 인증서가 이미 있고 엔진 인증 기관을 사용하여 생성하지 않으려면 다음 단계로 건너뜁니다.

2.

프록시의 호스트 이름을 선택합니다. 그런 다음 프록시의 고유 이름인 다른 구성 요소를 선택합니다.



참고

엔진 자체에서 사용하는 동일한 국가와 동일한 조직 이름을 사용하는 것이 좋습니다. **Manager**가 설치된 시스템에 로그인하고 다음 명령을 실행하여 이 정보를 찾습니다.

```
openssl x509 -in /etc/pki/ovirt-engine/ca.pem -noout -text | grep DirName
```

이 명령은 다음과 같이 출력됩니다.

```
subject= /C=US/O=Example Inc./CN=engine.example.com.81108
```

여기에서 관련된 부분은 **/C=US/O=Example Inc.** 입니다. 이를 사용하여 프록시의 인증서에 대한 전체 고유 이름을 빌드합니다.

```
/C=US/O=Example Inc./CN=proxy.example.com
```

3.

프록시 머신에 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

인증서의 고유 이름 관련 따옴표를 포함해야 합니다. **nodes** 옵션은 개인 키가 암호화되지 않도록 합니다. 즉, 프록시 서버를 시작하기 위해 암호를 입력할 필요가 없습니다.

이 명령은 두 개의 파일을 생성합니다. **proxy.key** 및 **proxy.req**는 개인 키입니다. 이 파일을 안전하게 유지합니다. **proxy.req**는 인증서 서명 요청입니다. **proxy.req**는 특별한 보호가 필요하지 않습니다.

4.

서명된 인증서를 생성하려면 프록시 머신에서 **Manager** 시스템으로 인증서 서명 요청 파일을 복사합니다.

```
# scp proxy.req engine.example.com:/etc/pki/ovirt-engine/requests/.
```

5.

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'
```

이 인증서는 인증서에 서명하여 10년(3650일) 동안 유효합니다. 원하는 경우 이전에 만료되도록 인증서를 설정합니다.

6.

생성된 인증서 파일은 **/etc/pki/ovirt-engine/certs** 디렉토리에서 사용할 수 있으며 이름을 **proxy.cer**로 지정해야 합니다. 프록시 머신의 **Manager** 시스템에서 현재 디렉터리로 이 파일을 복사합니다.

```
# scp engine.example.com:/etc/pki/ovirt-engine/certs/proxy.cer .
```

7.

proxy.key 및 **proxy.cer**가 프록시 머신에 모두 있는지 확인합니다.

```
# ls -l proxy.key proxy.cer
```

8.

프록시 머신에 **Squid** 프록시 서버 패키지를 설치합니다.

```
# dnf install squid
```

9.

개인 키와 서명된 인증서를 프록시가 액세스할 수 있는 위치로 이동합니다(예: `/etc/squid` 디렉토리).

```
# cp proxy.key proxy.cer /etc/squid/.
```

10.

squid 사용자가 다음 파일을 읽을 수 있도록 권한을 설정합니다.

```
# chgrp squid /etc/squid/proxy.*
# chmod 640 /etc/squid/proxy.*
```

11.

Squid 프록시는 엔진에서 사용하는 인증서를 확인해야 합니다. 관리자 인증서를 프록시 머신에 복사합니다. 이 예에서는 파일 경로 `/etc/squid`:

```
# scp engine.example.com:/etc/pki/ovirt-engine/ca.pem /etc/squid/.
```



참고

기본 **CA** 인증서는 **Manager** 시스템의 `/etc/pki/ovirt-engine/ca.pem`에 있습니다.

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 모드인 경우 **Squid**가 포트 **443**을 사용하도록 **semanage** 도구를 사용하여 포트 **443**의 컨텍스트를 변경합니다.

```
# dnf install polycoreutils-python
# semanage port -m -p tcp -t http_cache_port_t 443
```

14.

기존 **Squid** 구성 파일을 다음으로 바꿉니다.

■

```
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 login=PASSTHRU
cache_peer_access engine allow all
ssl_bump allow all
http_access allow all
```

15.

Squid 프록시 서버를 다시 시작하십시오.

```
# systemctl restart squid.service
```

참고

기본 구성에서 **squid** 프록시는 15분 후에 연결을 종료합니다. **Squid Proxy**가 유틸 연결을 종료하기 전의 시간을 늘리려면 **squid.conf** (예: **read_timeout 10** 시간)에서 **read_timeout** 옵션을 조정하십시오.

F.3. WEBSOCKET 프록시

F.3.1. WebSocket 프록시 개요

웹 소켓 프록시를 사용하면 **noVNC** 콘솔을 통해 가상 시스템에 연결할 수 있습니다.

초기 구성 중에 **Red Hat Virtualization Manager** 시스템에 웹 소켓 프록시를 설치하고 구성할 수 있습니다([Red Hat Virtualization Manager 구성 참조](#)).

부록 G. 브랜딩

G.1. 브랜딩

G.1.1. 관리자 재분산

및 에서 사용하는 아이콘과 팝업 창에 표시되는 텍스트 및 시작 페이지에 표시된 링크와 같이 **Red Hat Virtualization Manager**의 다양한 측면을 사용자 지정할 수 있습니다. 이를 통해 **Manager**를 다시 브랜딩할 수 있으며, 관리자와 사용자에게 제공되는 최종 모양과 느낌을 세부적으로 제어할 수 있습니다.

Manager를 사용자 지정하는 데 필요한 파일은 **Manager**가 설치된 시스템의 `/etc/ovirt-engine/Branding/` 디렉터리에 있습니다. 파일은 그래픽 사용자 인터페이스의 다양한 측면을 스타일링하는 데 사용되는 캐스케이딩 스타일 시트 파일 집합과 **Manager**의 다양한 구성 요소에 포함된 메시지 및 링크를 포함하는 속성 파일 집합으로 구성됩니다.

구성 요소를 사용자 지정하려면 해당 구성 요소의 파일을 편집하고 변경 사항을 저장합니다. 다음에 해당 구성 요소를 열거나 새로 고침하면 변경 사항이 적용됩니다.

G.1.2. 로그인 화면

로그인 화면은 관리 포털과 VM 포털 모두에서 사용하는 로그인 화면입니다. 사용자 지정할 수 있는 로그인 화면의 요소는 다음과 같습니다.

- 점두어
- 왼쪽에 헤더 이미지
- 오른쪽에 있는 헤더 이미지
- 헤더 텍스트

로그인 화면의 클래스는 **common.css**에 있습니다.

G.1.3. 관리 포털 화면

관리 포털 화면은 관리 포털에 로그인할 때 표시되는 기본 화면입니다. 사용자 지정할 수 있는 관리 포털 화면의 요소는 다음과 같습니다.

- 로고
- 왼쪽 배경 이미지
- 가운데 배경 이미지
- 오른쪽 배경 이미지
- 로고 오른쪽에 있는 텍스트

관리 포털 화면의 클래스는 `web_admin.css` 에 있습니다.

G.1.4. VM 포털 화면

VM Portal(VM 포털) 화면은 VM 포털에 로그인할 때 표시되는 화면입니다. 사용자 지정할 수 있는 VM 포털 화면의 요소는 다음과 같습니다.

- 로고
- 가운데 배경 이미지
- 오른쪽 배경 이미지
- 메인 그리드의 경계
- 사용자 레이블에서 기록된 텍스트

VM Portal(VM 포털) 화면의 클래스는 **user_portal.css**에 있습니다.

G.1.5. Windows 팝업

팝업 창은 **Manager**의 모든 창으로, 호스트 또는 가상 머신과 같은 엔터티를 생성, 편집 또는 업데이트 할 수 있습니다. 사용자 지정할 수 있는 팝업 창의 요소는 다음과 같습니다.

- 접두어
- 왼쪽에 헤더 이미지
- 헤더 센터 이미지(복사)

팝업 창에 대한 클래스는 **common.css**에 있습니다.

G.1.6. 탭

관리 포털의 여러 팝업 창에는 탭이 포함되어 있습니다. 사용자 지정할 수 있는 탭의 요소는 다음과 같습니다.

- 활성
- 비활성

탭의 클래스는 **common.css** 및 **user_portal.css**에 있습니다.

G.1.7. 시작 페이지

Welcome Page는 **Manager**의 홈페이지를 방문했을 때 처음 표시되는 페이지입니다. 전체 모양과 느낌을 사용자 지정하는 것 외에도 템플릿 파일을 편집하여 추가 문서 또는 내부 웹사이트에 대한 링크를 페이지에 추가하는 등의 다른 변경을 수행할 수도 있습니다. 사용자 지정할 수 있는 시작 페이지의 요소는 다음과 같습니다.

- 페이지 제목
- 머리글 (왼쪽, 중앙 및 오른쪽)
- 오류 메시지
- 전달할 링크 및 해당 링크의 관련 메시지
- 메시지 배너 또는 서문 추가

시작 페이지의 클래스는 **welcome_style.css** 에 있습니다.

템플릿 파일

Welcome Page의 템플릿 파일은 **HTML, HEAD** 또는 **BODY** 태그가 없는 **welcome_page.template** 이름의 일반 **HTML** 파일입니다. 이 파일은 시작 페이지 자체에 직접 삽입되며 시작 페이지에 표시되는 콘텐츠의 컨테이너 역할을 합니다. 따라서 새 링크를 추가하거나 콘텐츠 자체를 변경하려면 이 파일을 편집해야 합니다. 템플릿 파일의 또 다른 기능은 시작 페이지가 처리될 때 **messages.properties** 파일의 해당 텍스트로 대체되는 **{user_portal}** 과 같은 자리 표시자 텍스트가 포함되어 있다는 것입니다.

서문

배너 크기를 정의하는 **preamble.css** 파일과 **branding.properties** 파일에 연결하여 사용자 지정 메시지 배너를 시작 페이지에 추가할 수 있습니다. 샘플 파일은 [샘플 프리앰블 템플릿에서](#) 사용할 수 있습니다.



참고

엔진 업그레이드에서는 사용자 정의 메시지 배너가 그대로 유지되며 문제 없이 작동합니다. 엔진 백업 및 복원 후, 엔진 복원 중에 사용자 지정 메시지 배너를 수동으로 복원하고 확인해야 합니다.

G.1.8. 페이지를 찾을 수 없음

페이지를 찾을 수 없는 페이지는 **Red Hat Virtualization Manager**에서 찾을 수 없는 페이지에 대한 링크를 열 때 표시되는 페이지입니다. 사용자 지정할 수 있는 **Page Not Found** 페이지의 요소는 다음과 같습니다.

- 페이지 제목
- 머리글 (왼쪽, 중앙 및 오른쪽)
- 오류 메시지
- 전달할 링크 및 해당 링크의 관련 메시지

Page Not Found 페이지의 클래스는 `welcome_style.css`에 있습니다.

부록 H. 시스템 계정

H.1. RED HAT VIRTUALIZATION MANAGER 사용자 계정

rhevm 패키지를 설치할 때 **Red Hat Virtualization**을 지원하기 위해 많은 시스템 사용자 계정이 생성됩니다. 각 시스템 사용자에게는 기본 사용자 ID(**UID**)가 있습니다. 생성된 시스템 사용자 계정은 다음과 같습니다.

- **vds**m 사용자(**UID 36**). **NFS** 스토리지 도메인을 마운트하고 액세스하는 지원 툴에 필요합니다.
- **ovirt** 사용자(**UID 108**). **ovirt-engine Red Hat JBoss Enterprise Application Platform** 인스턴스 소유자.
- **ovirt-vmconsole** 사용자(**UID 498**). 게스트 직렬 콘솔에 필요합니다.

H.2. RED HAT VIRTUALIZATION MANAGER 그룹

rhevm 패키지를 설치할 때 **Red Hat Virtualization**을 지원하기 위해 다양한 시스템 사용자 그룹이 생성됩니다. 각 시스템 사용자 그룹에는 기본 그룹 ID(**GID**)가 있습니다. 생성된 시스템 사용자 그룹은 다음과 같습니다.

- **kvm** 그룹(**GID 36**). 그룹 멤버는 다음과 같습니다.
- **vds**m 사용자.
- **ovirt** 그룹(**GID 108**). 그룹 멤버는 다음과 같습니다.
- **ovirt** 사용자.
- **ovirt-vmconsole** 그룹(**GID 498**). 그룹 멤버는 다음과 같습니다.
- **ovirt-vmconsole** 사용자.

H.3. 가상화 호스트 사용자 계정

vdsm 및 **qemu-kvm-rhev** 패키지가 설치되면 여러 시스템 사용자 계정이 가상화 호스트에 생성됩니다. 각 시스템 사용자에게는 기본 사용자 ID(**UID**)가 있습니다. 생성된 시스템 사용자 계정은 다음과 같습니다.

- **vds**m 사용자(**UID 36**).
- **qemu** 사용자(**UID 107**).
- **sanlock** 사용자(**UID 179**).
- **ovirt-vmconsole** 사용자(**UID 498**).

중요

할당된 **UID**(사용자 식별자) 및 그룹 식별자(**GID**)는 시스템마다 다를 수 있습니다. **vds**m 사용자는 **36**의 **UID**로 수정되고 **kvm** 그룹은 **36**의 **GID**로 고정됩니다.

시스템의 다른 계정에서 **UID 36** 또는 **GID 36**을 이미 사용하는 경우 **vds**m 및 **qemu-kvm-rhev** 패키지를 설치하는 동안 충돌이 발생합니다.

H.4. 가상화 호스트 그룹

vdsm 및 **qemu-kvm-rhev** 패키지가 설치되면 여러 시스템 사용자 그룹이 가상화 호스트에 생성됩니다. 각 시스템 사용자 그룹에는 기본 그룹 ID(**GID**)가 있습니다. 생성된 시스템 사용자 그룹은 다음과 같습니다.

- **kvm** 그룹(**GID 36**). 그룹 멤버는 다음과 같습니다.
- **qemu** 사용자.
- **sanlock** 사용자.

- **qemu 그룹(GID 107).** 그룹 멤버는 다음과 같습니다.
- **vdsm 사용자.**
- **sanlock 사용자.**
- **ovirt-vmconsole 그룹(GID 498).** 그룹 멤버는 다음과 같습니다.
- **ovirt-vmconsole 사용자.**



중요

할당된 **UID**(사용자 식별자) 및 그룹 식별자(**GID**)는 시스템마다 다를 수 있습니다. **vdsm** 사용자는 **36**의 **UID**로 수정되고 **kvm** 그룹은 **36**의 **GID**로 고정됩니다.

시스템의 다른 계정에서 **UID 36** 또는 **GID 36**을 이미 사용하는 경우 **vdsm** 및 **qemu-kvm-rhev** 패키지를 설치하는 동안 충돌이 발생합니다.

부록 I. 법적 공지

Copyright © 2022 Red Hat, Inc.

(인용 [Commons Attribution-ShareAlike 4.0 International License](#))에 따라 라이선스가 부여됩니다.에 대한 설명서에서 파생됩니다([oVirt Project](#)). 이 문서 또는 수정 사항을 배포하는 경우 원래 버전의 URL을 제공해야 합니다.

수정된 버전에서는 모든 **Red Hat** 상표를 제거해야 합니다.

Red Hat, Red Hat Enterprise Linux, Red Hat 로고, **Shadowman** 로고, **JBoss, OpenShift, Fedora, Infinity** 로고 및 **RHCE**는 미국 및 기타 국가에서 등록된 **Red Hat, Inc.**의 상표입니다.

Linux®는 미국 및 기타 국가에서 **Linus Torvalds**의 등록 상표입니다.

Java®는 **Oracle** 및/또는 그 계열사의 등록 상표입니다.

XFS®는 미국 및/또는 기타 국가에 소재한 **orchestration graphics International Corp.** 또는 자회사의 상표입니다.

MySQL®은 미국, 유럽 연합 및 기타 국가에서 **MySQL AB**의 등록 상표입니다.

Node.js®는 **Joyent**의 공식 상표입니다. **Red Hat Software Collections**는 공식 **Joyent Node.js** 오픈 소스 또는 상용 프로젝트의 보증 대상이 아니며 공식적인 관계도 없습니다.

OpenStack® Word Mark 및 **OpenStack** 로고는 미국 및 기타 국가에서 **OpenStack Foundation**의 등록 상표/서비스 마크 또는 상표/서비스 마크이며 **OpenStack Foundation**의 허가 하에 사용됩니다. 당사는 **OpenStack Foundation** 또는 **OpenStack** 커뮤니티와 제휴 관계가 아니며 보증 또는 후원을 받지 않습니다.

다른 모든 상표는 해당 소유자의 자산입니다.

