

vSphere 단일 호스트 관리 - VMware Host Client

업데이트 3

VMware vSphere 8.0

VMware ESXi 8.0

VMware Host Client 2.18.0

VMware by Broadcom 웹 사이트

<https://docs.vmware.com/kr>에서 최신 기술 문서를 찾을 수 있습니다.

VMware by Broadcom

3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2015-2024 Broadcom. All Rights Reserved. “Broadcom”은 Broadcom Inc. 및/또는 해당 자회사를 뜻합니다. 자세한 내용은 <https://www.broadcom.com> 페이지를 참조하십시오. 여기에서 언급된 모든 상표, 상호, 서비스 마크 및 로고는 해당 회사의 소유입니다.

목차

vSphere 단일 호스트 관리 - VMware Host Client 정보 9

1 VMware Host Client는 무엇입니까? 10

- VMware Host Client를 사용합니다. 11
 - VMware Host Client 시작 및 로그인 11
 - VMware Host Client에서 로그아웃 11
 - VMware Host Client UI 테마를 사용자 지정하는 방법 11
 - VMware Host Client의 UI 로그인 화면에 대한 로그인 배너 구성 13
 - VMware Host Client에서 고객 환경 향상 프로그램에 재가입 또는 탈퇴 18

2 VMware Host Client로 호스트 관리 19

- VMware Host Client에서 시스템 설정 관리 19
 - VMware Host Client에서 고급 설정 관리 20
 - DCUI(Direct Console User Interface) 및 VMware Host Client에 대한 초기 시작 메시지 생성 20
 - VMware Host Client 사용자 인터페이스 세션 시간 초과 구성 21
 - VMware Host Client에서 SOAP 세션 시간 초과 구성 22
 - VMware Host Client에서 암호 및 계정 잠금 정책 구성 23
 - VMware Host Client에서 Syslog 구성 26
 - 고급 TLS/SSL 키 옵션 구성 27
 - Userworld 메모리 비우기 구성 28
 - VMware Host Client에서 자동 시작 구성 변경 29
 - VMware Host Client에서 ESXi 호스트의 시간 구성 편집 30
- VMware Host Client를 사용하여 ESXi 호스트에 대한 하드웨어 관리 31
 - ESXi 호스트 전원 관리 정책 31
 - VMware Host Client에서 전원 관리 정책 변경 32
 - VMware Host Client에서 하드웨어 레이블 변경 32
- ESXi 호스트에 대한 라이선싱 33
 - VMware Host Client 환경에 대한 라이선싱 정보 보기 35
 - VMware Host Client에서 ESXi 호스트에 라이선스 키 할당 35
 - VMware Host Client에서 ESXi 호스트로부터 라이선스 제거 35
- VMware Host Client에서 서비스 관리 36
- VMware Host Client를 사용하여 ESXi에 대한 보안 및 사용자 관리 36
 - VMware Host Client를 사용하여 호스트 인증 관리 36
 - VMware Host Client를 사용하여 호스트 인증서 관리 38
 - VMware Host Client를 사용하여 사용자 관리 39
 - VMware Host Client에서 ESXi 역할 관리 41

- vCenter Server에서 호스트 관리 43
 - VMware Host Client 환경을 최신 버전으로 업데이트 43
 - 최신 버전의 ESXi로 업그레이드한 후 VMware Host Client에서 ESXi 호스트로 연결할 수 없음 44
 - vSphere Client로 전환 45
 - VMware Host Client를 사용하여 vCenter Server와 ESXi 연결 끊기 45
- VMware Host Client에서 ESXi 호스트 재부팅 또는 종료 46
- ESXi Shell 사용 46
 - VMware Host Client에서 SSH(Secure Shell) 사용 47
 - VMware Host Client에서 ESXi 콘솔 셸 사용 47
 - VMware Host Client에서 ESXi Shell 가용성에 대한 시간 초과 생성 48
 - VMware Host Client에서 유휴 ESXi Shell 세션에 대한 시간 초과 생성 48
- VMware Host Client에서 ESXi 호스트를 유지 보수 모드로 설정 49
- VMware Host Client에서 사용 권한 관리 50
 - 사용 권한 유효성 검사 50
 - VMware Host Client에서 ESXi 호스트에 대해 사용자에게 사용 권한 할당 50
 - VMware Host Client에서 사용자에게 대한 사용 권한 제거 51
 - VMware Host Client에서 가상 시스템에 대한 사용자 사용 권한 할당 51
 - VMware Host Client에서 가상 시스템에 대한 사용 권한 제거 52
- VMware Host Client에서 지원 번들 생성 52
- VMware Host Client의 잠금 모드 53
 - VMware Host Client를 사용하여 ESXi 호스트를 정상 잠금 모드로 전환 54
 - VMware Host Client를 사용하여 ESXi 호스트를 엄격 잠금 모드로 전환 54
 - VMware Host Client를 사용하여 잠금 모드 종료 55
 - VMware Host Client에서 잠금 모드 예외 사용자 지정 55
- VMware Host Client를 사용하여 CPU 리소스 관리 55
 - VMware Host Client를 사용하여 프로세서 정보 보기 55
 - VMware Host Client에서 특정 프로세서에 가상 시스템 할당 56
- VMware Host Client에서 ESXi 호스트 모니터링 56
 - VMware Host Client에서 차트 보기 56
 - VMware Host Client에서 하드웨어 상태 모니터링 57
 - VMware Host Client에서 이벤트 보기 57
 - VMware Host Client에서 태스크 보기 57
 - VMware Host Client에서 시스템 로그 보기 58
 - VMware Host Client에서 알림 보기 58
- 3 VMware Host Client로 가상 시스템 관리 59**
 - VMware Host Client에서 가상 시스템 생성 59
 - VMware Host Client에서 기존 가상 시스템 등록 63
 - VMware Host Client에서 콘솔 사용 64
 - VMware Host Client에서 VMware Remote Console 애플리케이션 설치 65

- VMware Host Client에서 가상 시스템에 대한 원격 콘솔 시작 65
- VMware Host Client에서 가상 시스템 콘솔 열기 66
- VMware Host Client에서 게스트 운영 체제 관리 66
 - VMware Host Client를 사용하여 게스트 운영 체제 종료 및 다시 시작 66
 - VMware Host Client에서 게스트 운영 체제 변경 66
- VMware Tools 소개 67
 - VMware Tools 설치 68
 - VMware Host Client에서 VMware Tools 설치 68
 - VMware Tools 업그레이드 68
 - VMware Host Client에서 VMware Tools 업그레이드 70
- VMware Host Client에서 가상 시스템 구성 70
 - VMware Host Client에서 가상 시스템 호환성 확인 71
 - VMware Host Client에서 가상 시스템의 이름 변경 71
 - VMware Host Client에서 가상 시스템 구성 파일 위치 보기 71
 - VMware Host Client에서 가상 시스템 전원 상태 구성 72
 - VMware Host Client에서 구성 파일 매개 변수 편집 73
 - VMware Host Client에서 가상 시스템의 자동 시작 옵션 구성 74
 - VMware Host Client를 사용하여 가상 시스템 호환성 업그레이드 75
- VMware Host Client에서 가상 시스템 관리 76
 - VMware Host Client에서 가상 시스템 액세스 76
 - VMware Host Client에서 가상 시스템의 전원 상태 76
 - VMware Host Client에서 가상 시스템 열 구성 사용 77
 - VMware Host Client에서 호스트로부터 가상 시스템 제거 77
 - VMware Host Client에서 데이터스토어의 가상 시스템 제거 78
 - VMware Host Client에서 가상 시스템 등록 78
- 스냅샷으로 가상 시스템 관리 78
 - 스냅샷 파일 및 제한 사항 80
 - 스냅샷 제한 사항 82
 - VMware Host Client에서 가상 시스템의 스냅샷 생성 83
 - VMware Host Client에서 최신 스냅샷으로 복구 84
 - VMware Host Client에서 스냅샷 삭제 86
 - VMware Host Client에서 스냅샷 관리자를 사용하는 이유 87
- VMware Host Client에서 가상 시스템 모니터링 87
 - VMware Host Client에서 가상 시스템 성능 차트 보기 87
 - VMware Host Client에서 가상 시스템 이벤트 보기 88
 - VMware Host Client에서 가상 시스템 태스크 보기 88
 - VMware Host Client에서 가상 시스템 로그 브라우저 보기 89
 - VMware Host Client에서 가상 시스템 알림 보기 89

4 VMware Host Client에서 가상 시스템 하드웨어 구성 90

- 가상 CPU 구성 및 제한 사항 90
 - 가상 CPU 제한 92
 - 다중 코어 가상 CPU 구성 93
 - 가상 CPU 수 변경 93
 - VMware Host Client에서 CPU 리소스 할당 94
- 가상 메모리 구성 95
 - 메모리 구성 변경 95
 - 메모리 리소스 할당 96
 - Hot Add 메모리 설정 변경 97
 - VMware Host Client에서 VM에 NVDIMM 디바이스 추가 98
- 네트워크 가상 시스템 구성 99
 - 네트워크 어댑터 기본 99
 - 네트워크 어댑터와 레거시 가상 시스템 101
 - VMware Host Client에서 가상 네트워크 어댑터 구성 변경 101
 - VMware Host Client에서 가상 시스템에 네트워크 어댑터 추가 102
- 가상 디스크 구성 102
 - 가상 디스크 프로비저닝 정책 정보 103
 - VMware Host Client에서 가상 디스크 구성 변경 104
 - VMware Host Client에서 가상 시스템에 새로운 표준 하드 디스크 추가 105
 - VMware Host Client에서 가상 시스템에 기존 하드 디스크 추가 107
 - Host Client에서 영구 메모리 디스크 추가 107
 - 디스크 공유를 사용하여 VMware Host Client에서 가상 시스템에 우선 순위 부여 108
- VMware Host Client에서 가상 시스템 컨트롤러 구성 109
 - USB 컨트롤러를 가상 시스템에 추가 109
 - VMware Host Client에서 SCSI 컨트롤러 추가 111
 - VMware Host Client에서 SCSI 버스 공유 구성 변경 111
 - VMware Host Client에서 SCSI 컨트롤러 유형 변경 112
 - VMware 반가상화 SCSI 컨트롤러 정보 113
 - VMware Host Client에서 반가상화 SCSI 컨트롤러 추가 113
 - VMware Host Client에서 가상 시스템에 SATA 컨트롤러 추가 114
 - VMware Host Client에서 NVMe 컨트롤러 추가 114
- VMware Host Client에서 기타 가상 시스템 디바이스 구성 115
 - VMware Host Client에서 가상 시스템에 CD 또는 DVD 드라이브 추가 115
 - 플로피 드라이브를 VMware Host Client 내 가상 시스템에 추가 116
 - VMware Host Client에서 가상 시스템에 USB 디바이스 추가 117
 - VMware Host Client에서 가상 시스템에 사운드 컨트롤러 추가 117
 - VMware Host Client에서 병렬 및 직렬 포트 구성 118
 - 가상 시스템에 가상 감시 타이머 디바이스를 추가하는 방법 120
 - VMware Host Client에서 가상 시스템에 정밀 클럭 디바이스 추가 120
 - VMware Host Client에서 가상 시스템에 PCI 디바이스 추가 121

- VMware Host Client에서 가상 시스템 보호 122
 - VMware Host Client의 가상 시스템에서 vSGX 활성화 122
 - VMware Host Client의 가상 시스템에서 vSGX 비활성화 124
 - VMware Host Client를 사용하여 VM에서 vTPM 디바이스 제거 124
 - VMware Host Client에서 기존 VM에 가상화 기반 보안 활성화 또는 비활성화 125

5 VMware Host Client에서 스토리지 관리 127

- VMware Host Client의 데이터스토어 127
 - VMware Host Client에서 데이터스토어 정보 보기 128
 - VMware Host Client에서 VMFS 데이터스토어 생성 128
 - VMFS 데이터스토어 용량 증가 129
 - VMware Host Client에서 네트워크 파일 시스템 데이터스토어 마운트 130
 - VMware Host Client에서 데이터스토어 마운트 해제 131
 - VMware Host Client에서 데이터스토어 파일 브라우저 사용 133
 - VMware Host Client에서 데이터스토어 이름 바꾸기 136
 - VMware Host Client에서 VMFS 데이터스토어 삭제 136
 - VMware Host Client에서 스토리지 썸 프로비저닝 136
- VMware Host Client에서 스토리지 어댑터 관리 138
 - VMware Host Client에서 스토리지 어댑터 보기 138
 - VMware Host Client에서 소프트웨어 iSCSI 어댑터 구성 138
- VMware Host Client에서 스토리지 디바이스 관리 148
 - VMware Host Client에서 스토리지 어댑터 보기 148
 - VMware Host Client에서 디바이스 파티션 테이블 지우기 149
 - VMware Host Client에서 개별 디바이스 파티션 편집 149
- 영구 메모리 관리 149
 - 호스트의 영구 메모리 리소스 소비 모드 150
 - PMem 데이터스토어 구조 151
- VMware Host Client에서 스토리지 모니터링 153
 - VMware Host Client에서 데이터스토어 모니터링 153
 - VMware Host Client에서 vSAN 모니터링 153
- VMware Host Client에서 스토리지 새로 고침 및 다시 검색 작업 수행 158
 - VMware Host Client에서 어댑터 다시 검색 수행 159
 - VMware Host Client에서 디바이스 다시 검색 수행 159
 - VMware Host Client에서 검색되는 스토리지 디바이스 수 변경 159

6 VMware Host Client의 네트워킹 160

- VMware Host Client에서 포트 그룹 관리 160
 - VMware Host Client에서 포트 그룹 정보 보기 160
 - VMware Host Client에서 가상 스위치 포트 그룹 추가 161
 - VMware Host Client에서 포트 그룹 설정 편집 161

VMware Host Client에서 가상 스위치 포트 그룹 제거	164
VMware Host Client에서 가상 스위치 관리	165
VMware Host Client에서 가상 스위치 정보 보기	165
VMware Host Client에서 표준 가상 스위치 추가	165
VMware Host Client에서 표준 가상 스위치 제거	166
VMware Host Client에서 가상 스위치에 물리적 업링크 추가	166
VMware Host Client에서 가상 스위치 설정 편집	167
VMware Host Client에서 물리적 네트워크 어댑터 관리	170
VMware Host Client에서 물리적 네트워크 어댑터 정보 보기	170
VMware Host Client에서 물리적 NIC 편집	170
VMware Host Client에서 VMkernel 네트워크 어댑터 관리	170
VMware Host Client에서 VMkernel 네트워크 어댑터 정보 보기	170
VMware Host Client에서 VMkernel 네트워크 어댑터 추가	170
VMware Host Client에서 VMkernel 네트워크 어댑터 설정 편집	172
VMware Host Client에서 VMkernel 네트워크 어댑터 제거	173
VMware Host Client에서 호스트의 TCP/IP 스택 구성 보기	173
VMware Host Client에서 호스트에 있는 TCP/IP 스택의 구성 변경	173
VMware Host Client에서 ESXi 방화벽 구성	174
VMware Host Client를 사용하여 ESXi 방화벽 설정 관리	174
VMware Host Client를 사용하여 ESXi에 대해 허용되는 IP 주소 추가	175
VMware Host Client에서 네트워킹 이벤트 및 작업 모니터링	175
VMware Host Client에서 포트 그룹 모니터링	175
VMware Host Client에서 가상 스위치 모니터링	176
VMware Host Client에서 물리적 네트워크 어댑터 모니터링	176
VMware Host Client에서 VMkernel 네트워크 어댑터 모니터링	176
VMware Host Client에서 TCP/IP 스택 모니터링	177

vSphere 단일 호스트 관리 - VMware Host Client 정보

"vSphere 단일 호스트 관리 - VMware Host Client" 는 VMware Host Client를 통한 단일 호스트 관리에 대한 정보를 제공합니다.

VMware Host Client는 vCenter Server를 사용할 수 없을 때 긴급 관리를 수행하는 데 사용할 수 있습니다. VMware Host Client를 사용하여 관리 작업, 기본 문제 해결 작업 및 고급 관리 작업도 수행할 수 있습니다.

VMware는 포용성을 중요하게 생각합니다. 고객, 파트너 및 내부 커뮤니티 안에서 이러한 원칙을 강화하여 포용성이 없는 언어 인스턴스를 제거하기 위해 이 가이드를 업데이트했습니다.

대상 사용자

이 정보는 VMware Host Client를 사용하여 단일 ESXi 호스트를 관리하려는 모든 사용자를 위한 것입니다. 이 정보는 가상 시스템 기술과 데이터 센터 운영에 대해 잘 알고 있는 숙련된 Windows 또는 Linux 시스템 관리자를 대상으로 작성되었습니다.

VMware Host Client는 무엇입니까?

1

VMware Host Client는 단일 ESXi 호스트에 연결하고 관리하는 HTML5 기반 클라이언트입니다.

VMware Host Client를 사용하여 다음을 수행할 수 있습니다.

- 대상 ESXi 호스트에서 관리 및 기본 문제 해결 작업과 고급 관리 작업을 수행합니다.
- vCenter Server를 사용할 수 없을 때 긴급 관리를 수행합니다.

VMware Host Client는 vSphere Client와 다르다는 점을 알고 있는 것이 중요합니다. vSphere Client는 vCenter Server에 연결하고 여러 ESXi 호스트를 관리하는 데 사용하지만 VMware Host Client는 단일 ESXi 호스트를 관리하는 데 사용됩니다.

VMware Host Client 기능에는 다음 작업이 포함되지만 이에 국한되지는 않습니다.

- 기본 가상화 작업(예: 다양한 복잡도의 가상 시스템 배포 및 구성)
- 네트워킹 및 데이터스토어 생성 및 관리
- 성능 향상을 위한 호스트 수준 옵션 고급 조정

VMware Host Client 시스템 요구 사항

브라우저가 VMware Host Client를 지원하는지 확인합니다.

VMware Host Client는 다음과 같은 게스트 운영 체제 및 웹 브라우저 버전을 지원합니다.

지원되는 브라우저	Mac OS	Windows 32비트 및 64비트	Linux
Google Chrome	89+	89+	75+
Mozilla Firefox	80+	80+	60+
Microsoft Edge	90+	90+	해당 없음
Safari	9.0+	해당 없음	해당 없음

다음으로 아래 항목을 읽으십시오.

- [VMware Host Client를 사용합니다.](#)

VMware Host Client를 사용합니다.

vCenter Server를 일시적으로 사용할 수 없을 때 VMware Host Client를 사용하여 긴급 관리를 수행할 수 있습니다.

VMware Host Client 시작 및 로그인

VMware Host Client를 사용하여 가상 시스템에서 단일 ESXi 호스트를 관리하고 다양한 관리 및 문제 해결 태스크를 수행할 수 있습니다.

ESXi 호스트에 로그인하려면 다음 단계를 수행합니다.

절차

- 1 웹 브라우저에서 `https://host-name/ui` 또는 `https://host-IP-address/ui` 형식을 사용하여 대상 호스트 이름 또는 IP 주소를 입력합니다.
로그인 화면이 나타납니다.
- 2 사용자 이름 및 암호를 입력합니다.
- 3 계속하려면 **로그인**을 클릭합니다.
- 4 [VMware CEIP(고객 환경 향상 프로그램)] 페이지를 검토하고 프로그램에 가입할지 선택합니다.
프로그램에 대해 자세히 살펴보고 언제든지 구성하는 방법을 알아보려면 [VMware Host Client에서 고객 환경 향상 프로그램에 재가입 또는 탈퇴 항목을 참조하십시오.](#)
- 5 **확인**을 클릭합니다.

VMware Host Client에서 로그아웃

대상 ESXi 호스트를 더 이상 보거나 관리할 필요가 없는 경우 VMware Host Client에서 로그아웃합니다.

참고 VMware Host Client 세션을 닫아도 호스트는 중지되지 않습니다.

절차

- ◆ ESXi 호스트에서 로그아웃하려면 VMware Host Client 창 상단의 사용자 이름을 클릭하고 드롭다운 메뉴에서 **로그아웃**을 선택합니다.
VMware Host Client에서 로그아웃되었습니다. 대상 ESXi 호스트는 모든 정상 작업을 계속 실행합니다.

VMware Host Client UI 테마를 사용자 지정하는 방법

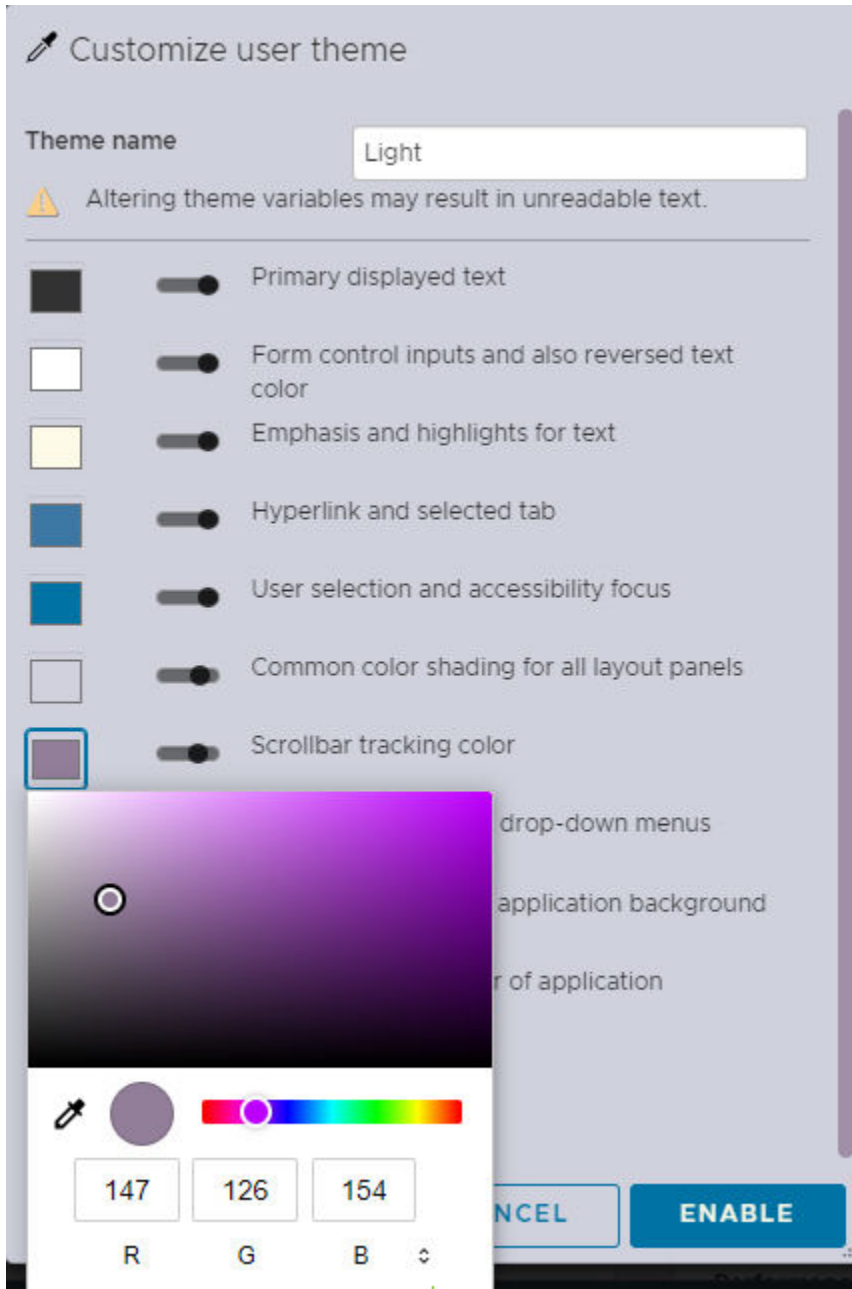
vSphere 8.0을 사용하면 VMware Host Client UI의 브랜딩과 콘텐츠가 표시되는 방식과 모양을 사용자 지정할 수 있습니다.

미리 설정된 세 가지 테마(밝은 테마, 어두운 테마 및 클래식 테마)를 선택하고 기본 설정에 따라 VMware Host Client에 테마를 적용할 수 있습니다.

절차

- 1 VMware Host Client 도구 모음에서 **도움말**을 클릭하고 **정보**를 클릭합니다.
정보 창이 나타납니다.
- 2 **UI 기본 설정 테마** 드롭다운 메뉴에서 적용할 테마를 선택합니다.

- 3 테마 이름을 변경하고 선택한 테마의 최대 10개 매개 변수를 수정하려면 **사용자 지정** 버튼을 클릭합니다.



- a **테마 이름** 필드에 테마의 사용자 지정 이름을 입력합니다.
- b 각 매개 변수에 대해 사용자 지정 색을 선택하려면 각 매개 변수 앞에 있는 색상 상자를 클릭하고 색을 선택한 다음 **사용**을 클릭합니다.
- a 기본 팔레트로 되돌리려면 **재설정** 버튼을 클릭합니다.

VMware Host Client의 UI 로그인 화면에 대한 로그인 배너 구성

법적 주의 메시지나 공식 발표 내용을 표시하려면 제한된 형식의 마크다운 구문을 사용하여 로그인 페이지 배너를 구성하면 됩니다.

호스트에서 직접 텍스트 파일 `/etc/vmware/welcome`을 수정하여 사용자 이름 및 암호 로그인 필드 오른쪽에 나타나는 로그인 배너 콘텐츠를 변경할 수 있습니다.

참고 마크다운 파서가 콘텐츠 블록에 적용되고 `#`, ```, `*` 등의 특정 문자 시퀀스가 의도치 않게 마크다운 형식 규칙을 트리거할 수도 있습니다.

`welcome` 파일에서 다음과 같은 제한된 집합의 마크다운 지시문을 적용할 수 있습니다.

레이아웃 개념	마크다운 코드 구문	출력
머리글 레이블	<ul style="list-style-type: none"> 새 줄에서 시작하여 1~6개의 해시 표시 기호를 입력합니다. <p>예</p> <pre># My Title.</pre>	<p>"내 제목"에 대해 큰 HTML <code><h1></code> 태그를 생성합니다.</p> <p>My Title</p>
가로 규칙	<ul style="list-style-type: none"> 새 줄에서 시작하여 일련의 대시 문자를 3개 이상 입력합니다. <p>예</p> <pre>-----.</pre>	<p>HTML에서 <code><hr /></code> 규칙 태그를 생성합니다.</p> <hr/>
리터럴 또는 코드 블록	<ul style="list-style-type: none"> 새 줄에서 시작하여 역음 악센트 기호 3개만 입력합니다. 이후 줄에 소스 자료를 추가합니다. 소스를 종결하려면 새 줄에 역음 악센트 기호 3개를 입력합니다. <p>예</p> <pre>``` My content - - - *Login Secure* >_ Read the policy ```</pre>	<p>역음 악센트 기호 줄 사이의 텍스트 블록을 서식이나 해석 없이 고정 폭 글꼴로 표시합니다.</p> <pre>My content - - - *Login Secure* >_ Read the policy</pre> <p>참고 콘텐츠가 마크다운 파서에 의해 실수로 형식이 지정되면 한 쌍의 백틱 문자 행으로 콘텐츠를 감쌌니다. 공백 문자가 유지되므로 고정 폭 글꼴을 사용하듯이 ASCII 아트를 사용할 수 있습니다.</p>
굵게 텍스트	<p>텍스트 문자열 양쪽에 이중 별표 문자로 묶습니다.</p> <p>예</p> <pre>**important message**.</pre> <p>참고 마크다운 이중 밑줄 문자 구문은 URL과의 충돌을 방지하기 위해 생략됩니다.</p>	<p>중요 메시지</p>

레이아웃 개념	마크다운 코드 구문	출력
기울임꼴 텍스트	<p>텍스트 문자열 양쪽에 하나의 별표 문자로 묶습니다.</p> <p>예</p> <pre>*A named document*.</pre> <p>참고 마크다운 밑줄 문자 구문은 URL과의 충돌을 방지하기 위해 생략됩니다.</p>	<pre><i> "명명된 문서" </i></pre>
하이퍼링크	<p>절대 URL을 연결하려면 링크 텍스트를 대괄호로 묶고 그 뒤에 URL을 괄호로 묶는 마크다운 구문을 사용합니다.</p> <p>예</p> <pre>[My link] (https://www.example.com?search=virtual)</pre>	<p>클릭 가능한 텍스트가 있는 일반 하이퍼링크 앵커 태그를 생성합니다. My link</p>

지원되는 변수

텍스트 파일의 아무 위치에도 다음 변수를 삽입할 수 있습니다.

변수 개념	메타 태그 변수 코드	출력
현재 호스트 또는 IP 주소의 FQDN(정규화된 도메인 이름)	{hostname}	현재 호스트의 전체 이름을 표시합니다. 예를 들어 sample.host.com입니다.
ESXi 버전을 점 숫자 형식으로 지정	{esxversion}	예를 들어, 7.0.0 형식으로 표시합니다.
ESXi 전체 제품 이름, 버전 및 빌드 번호	{esxproduct}	예를 들어, VMware ESXi 7.0.0 build-16324942 형식으로 표시합니다.
사용자 시스템의 현재 날짜	{client-current-date}	예를 들어, Tuesday, August 30, 2022 형식으로 표시합니다. 참고 이는 로케일별로 다릅니다.
사용자 시스템의 현재 시간	{client-current-time}	예를 들어, 08:00 AM 형식으로 표시합니다. 참고 이는 로케일별로 다릅니다.

고급 태그

고급 태그를 사용하면 로그인 페이지에 적용하는 규칙에 따라 시각적 변화 및 동작 변화를 줄 수 있습니다. 텍스트 파일의 맨 끝에 이러한 태그를 삽입합니다.

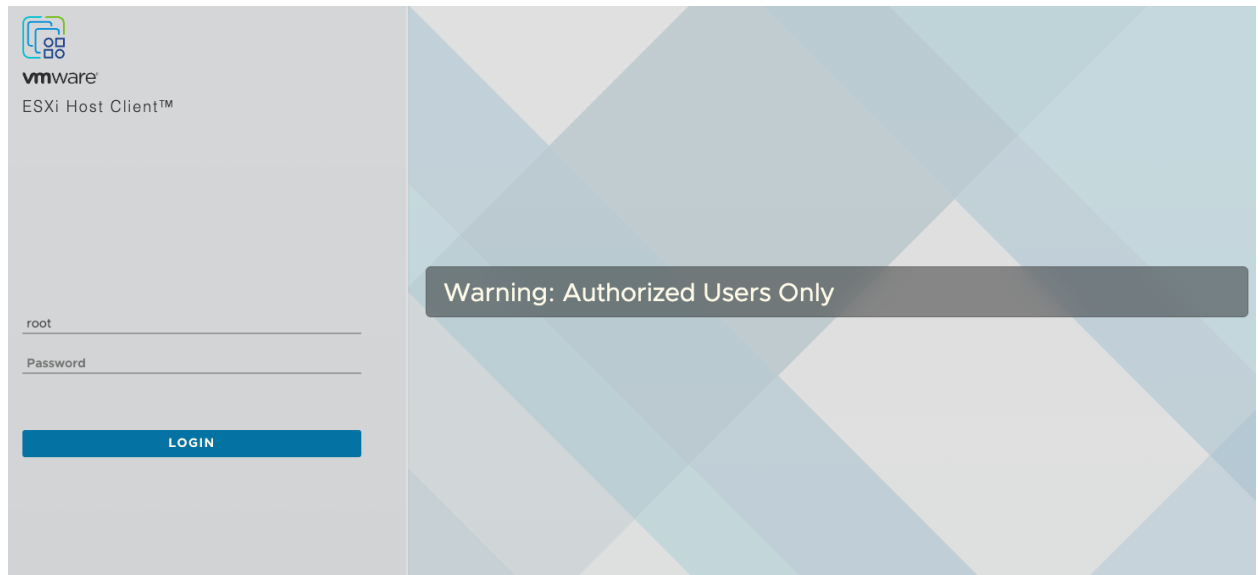
UI 개념	메타 태그 변수 코드	출력
사용자 지정 이미지	<pre>{logo src="https://site/logo.png" width="100" height="100" align="center"}My Secured ESXi Server Tooltip{/logo}</pre>	메시지 블록 위에 가로 방향으로 중앙에 100x100 픽셀 이미지 logo.png를 표시합니다. My Secured ESXi Server Tooltip의 액세스 가능한 도구 설명 제목이 이미지에 추가됩니다. 참고 width, height 및 align 특성은 선택 사항이지만 사용해야 합니다. 모든 웹 이미지 형식이 지원됩니다.
사용자 계약 확인란	<pre>{accept}Please accept the terms{/accept}</pre>	메시지 콘텐츠 하단에 [약관 동의] 레이블이 있는 확인란을 표시합니다.
강제 동의 오류 메시지	<pre>{mustaccept}You must agree before logging into the system{/mustaccept}</pre>	사용자가 로그인하기 전에 확인란을 선택하도록 요구하는 양식 검증을 추가합니다. 사용자가 확인란을 선택하지 않으면 로그인 버튼 위에 "시스템에 로그인하기 전에 동의해야 합니다."라는 메시지가 나타납니다.

예

단순 마크다운

간단한 텍스트 전용 메시지를 위한 한 줄 마크다운

```
## Warning: Authorized Users Only
```



고급 마크다운

양식에 로고, 링크 및 필수 동의 확인란이 있는 가상 클라우드 스토리지 회사인 Vaulted의 고급 마크다운 샘플입니다.

```
## Warning: Authorized Users Only

The information on this host is the property of "Vaulted Storage" *(sample organization)*
and is protected under sovereign intellectual property rights.

You must be assigned an account on this computer to access information and are only allowed
to access information defined by the system administrators.

All activities are monitored and trespassing violators will be reported to a federal
law enforcement agency.

### Policy bulletins
*Please refer to the helpful links* below on end user protection guidelines.

* [Privacy addendum] (https://en.wikipedia.org/wiki/Computer\_security)
* [Terms of Use] (https://en.wikipedia.org/wiki/Terms\_of\_service#:~:text=Terms%20of%20service%20\(also%20known,to%20use%20the%20offered%20service.\))
...

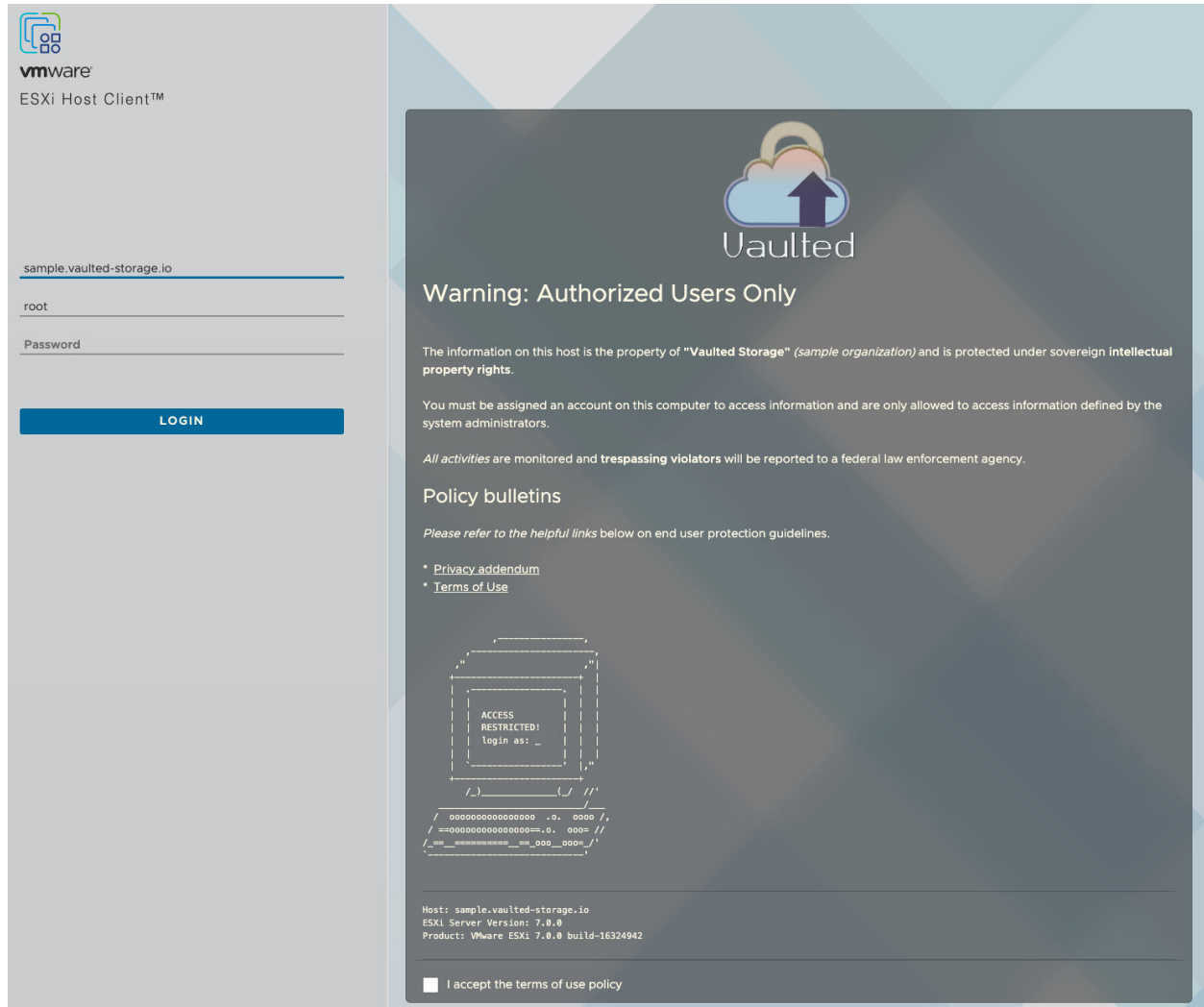
      ,-----,
    ,-----,
  ,-----,
,-----,
+-----+
| .----- . |
| |         | |
| | ACCESS  | |
| | RESTRICTED! | |
| | login as: _ | |
| |         | |
| | `-----' | |
+-----+
  /_)_____(_/ //'
    _____/
  / ooooooooooooo .o. oooo /,
 / ==ooooooooooooo==.o. ooo= //
/_==_=====___==_ooo_ooo=/'
 `-----'

-----
Host: {hostname}
ESXi Server Version: {esxversion}
Product: {esxproduct}
-----
...

{logo align="center" width="200" height="200" src="https://i.postimg.cc/y6wZXPm/vaulted-logo-white-text.png"}Vaulted Enterprise Storage{/logo}

{accept}I accept the terms of use policy{/accept}

{mustaccept}User must check terms of use to login. LOG OFF immediately if you do not agree to
the conditions stated in the warning.{/mustaccept}
```



VMware Host Client에서 고객 환경 향상 프로그램에 재가입 또는 탈퇴

CEIP(고객 환경 향상 프로그램)에 참여하여 VMware 제품 및 서비스의 품질, 안정성 및 기능 향상을 위해 VMware에 익명의 피드백이나 정보를 제공할 수 있습니다.

CEIP(고객 환경 향상 프로그램)에서 탈퇴하거나 언제든지 CEIP에 재가입할 수 있습니다.

CEIP를 통해 수집되는 데이터에 대한 세부 정보와 VMware에서 해당 정보를 사용하는 목적은 신뢰 및 보증 센터 (<http://www.vmware.com/trustvmware/ceip.html>)에 명시되어 있습니다.

절차

- 1 CEIP에 재가입하거나 탈퇴하려면 VMware Host Client 페이지의 맨 위에서 사용자 이름을 클릭합니다.
- 2 **설정 > 사용량 통계 보내기**를 선택하여 CEIP에서 탈퇴하거나 재가입합니다.

VMware Host Client로 호스트 관리

2

VMware Host Client로 vCenter Server를 업그레이드하는 동안 또는 vCenter Server가 응답을 중지하거나 사용할 수 없게 되는 경우 단일 ESXi 호스트를 관리할 수 있습니다.

VMware Host Client에는 vCenter Server를 사용할 수 없는 경우 로그인한 ESXi 호스트에서 태스크를 수행할 수 있는 중요 문제 해결 기능 집합이 있습니다. 이러한 기능에는 고급 호스트 설정 구성, 라이선싱, 인증서 관리, ESXi Shell 사용, 잠금 모드 사용 등의 기능이 포함되며 이에 제한되지 않습니다.

다음으로 아래 항목을 읽으십시오.

- VMware Host Client에서 시스템 설정 관리
- VMware Host Client를 사용하여 ESXi 호스트에 대한 하드웨어 관리
- ESXi 호스트에 대한 라이선싱
- VMware Host Client에서 서비스 관리
- VMware Host Client를 사용하여 ESXi에 대한 보안 및 사용자 관리
- vCenter Server에서 호스트 관리
- VMware Host Client에서 ESXi 호스트 재부팅 또는 종료
- ESXi Shell 사용
- VMware Host Client에서 ESXi 호스트를 유지 보수 모드로 설정
- VMware Host Client에서 사용 권한 관리
- VMware Host Client에서 지원 번들 생성
- VMware Host Client의 잠금 모드
- VMware Host Client를 사용하여 CPU 리소스 관리
- VMware Host Client에서 ESXi 호스트 모니터링

VMware Host Client에서 시스템 설정 관리

VMware Host Client로 고급 호스트 설정을 관리하고 호스트에 라이선스를 할당하거나 제거하고 호스트 서비스의 시작 및 중지 정책을 구성하고 호스트의 시간 및 날짜 구성을 관리할 수 있습니다.

VMware Host Client에서 고급 설정 관리

VMware Host Client를 사용하여 호스트의 설정을 변경할 수 있습니다.

경고 VMware 기술 지원 또는 KB 지침 문서에 명시되지 않는 한 고급 옵션 변경은 지원되지 않습니다. 다른 모든 경우, 이러한 옵션 변경은 지원되지 않습니다. 대부분의 경우 기본 설정으로 최적의 결과를 얻을 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **시스템**을 클릭합니다.
- 2 **고급 설정**을 클릭합니다.
- 3 목록에서 적절한 항목을 마우스 오른쪽 버튼으로 클릭하고 드롭다운 메뉴에서 **옵션 편집**을 선택합니다.
옵션 편집 대화상자가 표시됩니다.
- 4 값을 편집하고 **저장**을 클릭하여 변경 내용을 적용합니다.
- 5 (선택 사항) 목록에서 적절한 항목을 마우스 오른쪽 버튼으로 클릭하고 **기본값으로 재설정**을 선택하여 항목의 원래 설정으로 돌아갑니다.

DCUI(Direct Console User Interface) 및 VMware Host Client에 대한 초기 시작 메시지 생성

VMware Host Client를 사용하여 DCUI(Direct Console User Interface)의 초기 화면과 VMware Host Client의 로그인 창에 표시되는 시작 메시지를 생성할 수 있습니다. 사용자가 VMware Host Client에 로그인한 후에 표시되는 시작 메시지를 생성하고 시작 메시지를 표시할지 여부를 결정할 수도 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **고급 설정**을 클릭합니다.

옵션	작업
DCUI 및 VMware Host Client에 로그인 하기 전에 표시되는 시작 메시지 생성	<ol style="list-style-type: none"> a 검색 텍스트 상자에 <code>Annotations.WelcomeMessage</code>를 입력하고 검색 아이콘을 클릭합니다. b <code>Annotations.WelcomeMessage</code>을 마우스 오른쪽 버튼으로 클릭하고 드롭다운 메뉴에서 옵션 편집을 선택합니다. 옵션 편집 대화상자가 열립니다. c 새 값 텍스트 상자에 시작 메시지를 입력합니다. 기본 메시지를 설정하려면 새 값 텍스트 상자를 비워둡니다.
VMware Host Client에 로그인한 후 표시 되는 시작 메시지 생성	<ol style="list-style-type: none"> a 검색 텍스트 상자에 <code>UserVars.HostClientWelcomeMessage</code>를 입력하고 검색 아이콘을 클릭합니다. b <code>UserVars.HostClientWelcomeMessage</code>을 마우스 오른쪽 버튼으로 클릭하고 드롭다운 메뉴에서 옵션 편집을 선택합니다. 옵션 편집 대화상자가 열립니다. c 새 값 텍스트 상자에 시작 메시지를 입력합니다. 기본 메시지를 설정하려면 새 값 텍스트 상자를 비워둡니다.
VMware Host Client에 로그인한 후 시작 메시지 표시를 활성화 또는 비활성화합니다.	<ol style="list-style-type: none"> a 검색 텍스트 상자에 <code>UserVars.HostClientEnableMOTDNotification</code>을 입력하고 검색 아이콘을 클릭합니다. b <code>UserVars.HostClientEnableMOTDNotification</code>을 마우스 오른쪽 버튼으로 클릭하고 드롭다운 메뉴에서 옵션 편집을 선택합니다. 옵션 편집 대화상자가 열립니다. c 새 값 텍스트 상자에 새 값을 입력합니다. 값이 0이면 시작 메시지 표시가 비활성화됩니다. 값이 1이면 시작 메시지 표시가 활성화됩니다.

- 2 **저장**을 클릭합니다.
- 3 (선택 사항) 키 설정을 기본값으로 재설정하려면 목록에서 해당 키를 마우스 오른쪽 버튼으로 클릭하고 **기본값으로 재설정**을 선택합니다.

VMware Host Client 사용자 인터페이스 세션 시간 초과 구성

VMware Host Client에서 사용자 인터페이스 세션은 15분마다 자동으로 시간 초과되며 그렇게 되면 VMware Host Client에 다시 로그인해야 합니다.

기본 비활성 시간 초과 값은 고급 구성 매개 변수를 변경하여 늘릴 수 있습니다. 기본값은 900초입니다.

절차

- ◆ 사용자 인터페이스 세션 시간 초과를 구성합니다.

옵션	작업
VMware Host Client 고급 설정에서	<p>a VMware Host Client 인벤토리에서 관리를 클릭하고 고급 설정을 클릭합니다.</p> <p>b 검색 텍스트 상자에 <code>UserVars.HostClientSessionTimeout</code>을 입력하고 검색 아이콘을 클릭합니다.</p> <p>c <code>UserVars.HostClientSessionTimeout</code>을 마우스 오른쪽 버튼으로 클릭하고 드롭다운 메뉴에서 옵션 편집을 선택합니다.</p> <p>옵션 편집 대화상자가 열립니다.</p> <p>d 새 값 텍스트 상자에 시간 초과 설정을 초 단위로 입력합니다.</p> <hr/> <p>참고 값이 0이면 시간 초과가 비활성화됩니다.</p> <hr/> <p>e 저장을 클릭합니다.</p> <p>f (선택 사항) 키 설정을 기본값으로 재설정하려면 목록에서 해당 키를 마우스 오른쪽 버튼으로 클릭하고 기본값으로 재설정을 선택합니다.</p>
사용자 설정 드롭다운 메뉴에서	<p>a VMware Host Client 창의 위쪽에서 사용자 이름을 클릭하고 설정 > 애플리케이션 시간 초과 >를 선택합니다.</p> <p>b 비활성 시간 초과를 지정하려면 시간을 선택합니다.</p> <p>c 비활성 시간 초과를 비활성화하려면 <code>off</code>를 선택합니다.</p>

VMware Host Client에서 SOAP 세션 시간 초과 구성

VMware Host Client에서 SOAP 세션 시간 초과를 구성할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **고급 설정**을 클릭합니다.
- 2 **검색** 텍스트 상자에 `Config.HostAgent.vmacore.soap.sessionTimeout`을 입력하고 **검색** 아이콘을 클릭합니다.
- 3 `Config.HostAgent.vmacore.soap.sessionTimeout`을 마우스 오른쪽 버튼으로 클릭하고 드롭다운 메뉴에서 **옵션 편집**을 선택합니다.
- 옵션 편집** 대화상자가 열립니다.
- 4 **새 값** 텍스트 상자에 시간 초과 설정을 초 단위로 입력합니다.
- 값이 0이면 시간 초과가 비활성화됩니다.
- 5 **저장**을 클릭합니다.
- 6 (선택 사항) 키 설정을 기본값으로 재설정하려면 목록에서 해당 키를 마우스 오른쪽 버튼으로 클릭하고 **기본값으로 재설정**을 선택합니다.

VMware Host Client에서 암호 및 계정 잠금 정책 구성

ESXi 호스트에 대해 미리 정의된 요구 사항이 있는 암호를 사용해야 합니다.

`Security.PasswordQualityControl` 고급 옵션을 사용하여 필요한 암호 길이 및 문자 클래스 요구 사항을 변경하거나 암호 문구를 허용할 수 있습니다. `Security.PasswordHistory` 고급 옵션을 사용하여 각 사용자에 대해 기억할 암호 수도 설정할 수 있습니다. 이 설정은 중복되거나 유사한 암호를 방지합니다.

`Security.PasswordMaxDays` 고급 옵션을 사용하면 암호 변경 간격의 최대 일수를 설정할 수 있습니다.

참고 기본 암호 설정을 변경한 후에는 항상 추가 테스트를 수행하십시오.

잘못된 자격 증명으로 로그인을 시도하는 경우 계정 잠금 정책에 따라 시스템이 계정을 잠그는 시기와 기간이 지정됩니다.

ESXi 암호

ESXi는 액세스에 대한 암호 요구 사항을 적용합니다.

- 기본적으로 암호를 생성할 때는 소문자, 대문자, 숫자, 특수 문자(예: 밑줄 또는 대시)의 네 가지 문자 클래스 중 세 가지의 문자를 혼합하여 포함해야 합니다.
- 기본적으로 암호의 길이는 최소 7자, 최대 40자여야 합니다.
- 암호에는 사전에 나오는 단어 또는 사전에 나오는 단어의 일부를 포함하면 안 됩니다.
- 암호에는 사용자 이름이나 사용자 이름의 일부가 포함되어서는 안 됩니다.

참고 암호를 시작할 때의 대문자는 사용된 문자 클래스 수에 포함되지 않습니다. 암호가 끝날 때의 숫자도 사용된 문자 클래스 수에 포함되지 않습니다.

ESXi 암호 예

다음 암호 후보는 옵션이 다음과 같이 설정되었을 때 설정 가능한 암호를 보여줍니다.

```
retry=3 min=disabled,disabled,disabled,7,7
```

이 설정을 사용하면 암호가 충분히 강력하지 않거나 암호가 올바르게 두 번 입력되지 않은 경우 새 암호를 입력하라는 메시지가 사용자에게 최대 세 번(retry=3) 표시됩니다. 처음 3개 항목이 비활성화되기 때문에 1개 또는 2개의 문자 클래스 및 암호 문구가 있는 암호는 허용되지 않습니다. 3개 및 4개의 문자 클래스의 암호에는 7개의 문자가 필요합니다.

다음 암호 후보는 암호 요구 사항을 충족합니다.

- xQaTEhb!: 세 가지 문자 클래스의 문자 8개를 포함합니다.
- xQaT3#A: 네 가지 문자 클래스의 문자 7개를 포함합니다.

다음 암호 후보는 암호 요구 사항을 충족하지 않습니다.

- Xqat3hi: 대문자로 시작되기 때문에 유효한 문자 클래스 수가 2개로 줄어듭니다. 필수 문자 클래스의 수는 최소 3개입니다.

- xQaTEh2: 숫자로 끝나기 때문에 유효한 문자 클래스가 2개로 줄어듭니다. 필수 문자 클래스의 수는 최소 3개입니다.

비밀번호 품질 제어

Security.PasswordQualityControl 고급 옵션 사용하여 암호의 품질을 제어할 수 있습니다.

Security.PasswordQualityControl은 패턴을 따르는 몇 가지 설정으로 구성됩니다.

```
retry=N min=N0,N1,N2,N3,N4 max=N passphrase=N similar=permit|deny
```

비밀번호 품질 제어 설정	설명	기본값
retry=N	암호가 올바르지 않거나 충분히 강력하지 않은 경우 사용자가 새 암호를 제공해야 하는 횟수입니다.	retry=3
min=N0,N1,N2,N3,N4	문자 클래스 및 암호 최소 길이 요구 사항입니다. <ul style="list-style-type: none"> ■ N0은 단일 문자 클래스에 대한 최소 암호 길이입니다. ■ N1은 두 가지 문자 클래스에 대한 최소 암호 길이입니다. ■ N2는 암호의 최소 길이입니다. ■ N3은 세 가지 문자 클래스에 대한 최소 길이입니다. ■ N4는 네 가지 문자 클래스에 대한 최소 길이입니다. disabled를 사용하면 지정된 수의 문자 클래스가 있는 암호를 허용하지 않을 수 있습니다.	min=disabled,disabled,disabled,7,7
max=N	허용되는 최대 암호 길이입니다.	max=40
passphrase=N	암호에 필요한 단어 수입니다. passphrase가 인식되도록 하려면 min 설정에서 N2를 disabled로 설정하지 마십시오.	passphrase=3
similar=permit deny	암호가 이전 암호와 유사해도 되는지 여부를 나타냅니다. 이 설정을 사용하려면 Security.PasswordHistory 옵션을 0이 아닌 값으로 설정해야 합니다. vSphere 8.0 업데이트 1부터 기본값은 5입니다.	similar=deny

ESXi 암호 문구

암호 대신 암호 문구를 사용할 수 있습니다. 암호 문구는 기본적으로 비활성화됩니다.

Security.PasswordQualityControl 고급 옵션을 사용하여 기본 설정을 변경할 수 있습니다.

예를 들어 옵션을 다음으로 변경할 수 있습니다.

```
retry=3 min=disabled,disabled,16,7,7
```

이 예에서는 16자 이상의 암호 문구를 허용합니다. 암호 문구는 공백으로 구분된 3개 이상의 단어로 구성되어 야 합니다.

암호 기록 및 순환 정책 예

암호 기록을 6개 기억하려면 `Security.PasswordHistory` 옵션을 6으로 설정합니다.

90일 암호 순환 정책을 적용하려면 `Security.PasswordMaxDays` 옵션을 90으로 설정합니다.

ESXi 계정 잠금 정책

사용자는 미리 설정된 수의 연속 시도 실패 후에 잠깁니다. 기본적으로 3분 내에 시도가 5회 연속 실패하면 사용자가 잠기고 잠긴 계정은 기본적으로 15분 후에 자동으로 잠금이 해제됩니다. 최대로 허용되는 실패 시도 횟수와 사용자 계정이 잠기는 기간은 `Security.AccountLockFailures` 및 `Security.AccountUnlockTime` 고급 옵션을 사용하여 변경할 수 있습니다.

관리자 암호 및 계정 잠금 동작을 구성하려면 다음 단계를 수행합니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **고급 설정**을 클릭합니다.

옵션	작업
필요한 암호 길이, 문자 클래스 요구 사항 또는 허용 암호 구성	<ol style="list-style-type: none"> 검색 텍스트 상자에 <code>Security.PasswordQualityControl</code>을 입력하고 검색 아이콘을 클릭합니다. <code>Security.PasswordQualityControl</code>을 마우스 오른쪽 버튼으로 클릭하고 드롭다운 메뉴에서 옵션 편집을 선택합니다.
각 사용자에게 기억할 암호 수 구성	<ol style="list-style-type: none"> 검색 텍스트 상자에 <code>Security.PasswordHistory</code>를 입력하고 검색 아이콘을 클릭합니다. <code>Security.PasswordHistory</code>을 마우스 오른쪽 버튼으로 클릭하고 드롭다운 메뉴에서 옵션 편집을 선택합니다. <p>참고 영(0)은 암호 기록을 비활성화합니다.</p>
암호 변경 간격의 최대 일수 구성	<ol style="list-style-type: none"> 검색 텍스트 상자에 <code>Security.PasswordMaxDays</code>를 입력하고 검색 아이콘을 클릭합니다. <code>Security.PasswordMaxDays</code>을 마우스 오른쪽 버튼으로 클릭하고 드롭다운 메뉴에서 옵션 편집을 선택합니다.

옵션	작업
잠길 때까지 허용되는 로그인 시도 실패 횟수 구성	<p>a 검색 텍스트 상자에 <code>Security.AccountLockFailures</code>를 입력하고 검색 아이콘을 클릭합니다.</p> <p>b <code>Security.AccountLockFailures</code>을 마우스 오른쪽 버튼으로 클릭하고 드롭다운 메뉴에서 옵션 편집을 선택합니다.</p> <p>참고 0은 계정 잠금을 비활성화합니다.</p>
사용자 계정이 잠기는 기간 구성	<p>a 검색 텍스트 상자에 <code>Security.AccountUnlockTime</code>를 입력하고 검색 아이콘을 클릭합니다.</p> <p>b <code>Security.AccountUnlockTime</code>을 마우스 오른쪽 버튼으로 클릭하고 드롭다운 메뉴에서 옵션 편집을 선택합니다.</p>

옵션 편집 대화상자가 열립니다.

- 2 **새 값** 텍스트 상자에 새 설정을 입력합니다.
- 3 **저장**을 클릭합니다.
- 4 (선택 사항) 키 설정을 기본값으로 재설정하려면 목록에서 해당 키를 마우스 오른쪽 버튼으로 클릭하고 **기본값으로 재설정**을 선택합니다.

VMware Host Client에서 Syslog 구성

Syslog 서비스를 구성하려면 VMware Host Client를 사용하면 됩니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **고급 설정**을 클릭합니다.
- 2 **검색** 텍스트 상자에 변경할 설정의 이름을 입력하고 **검색** 아이콘을 클릭합니다.

옵션	설명
<code>Syslog.global.LogHost</code>	<p>Syslog 메시지가 전달되는 원격 호스트 및 원격 호스트가 Syslog 메시지를 수신하는 포트입니다. 프로토콜과 포트를 포함할 수 있습니다(예: <code>protocol://hostName1:port</code>, 여기서 <code>protocol</code>은 <code>udp</code>, <code>tcp</code> 또는 <code>ssl</code>일 수 있음). UDP에는 포트 514만 사용할 수 있습니다. SSL 프로토콜은 TLS 1.2를 사용합니다. 예: <code>ssl://hostName1:1514</code>. <code>port</code> 값은 1에서 65535 사이의 십진수일 수 있습니다.</p> <p>syslog 메시지를 수신할 원격 호스트 수에 대한 고정 제한은 없지만 원격 호스트 수는 5개 이하로 유지하는 것이 좋습니다.</p>
<code>Syslog.global.logCheckSSLCerts</code>	원격 호스트에 로그인할 때 SSL 인증서 확인을 적용합니다.
<code>Syslog.global.defaultRotate</code>	유지할 아카이브의 최대 수입니다. 이 숫자는 전체적으로 설정할 수 있으며 개별 하위 로그에 대해 설정할 수도 있습니다.
<code>Syslog.global.defaultSize</code>	시스템에서 로그를 회전할 때까지의 기본 로그 크기(KB)입니다. 이 숫자는 전체적으로 설정할 수 있으며 개별 하위 로그에 대해 설정할 수도 있습니다.

옵션	설명
Syslog.global.LogDir	로그가 저장된 디렉토리입니다. 디렉토리는 마운트된 NFS 또는 VMFS 볼륨에 있을 수 있습니다. 로컬 파일 시스템의 /scratch 디렉토리만 여러 번 재부팅해도 영구적으로 유지됩니다. 디렉토리는 [datastorename] path_to_file로 지정해야 하며, 여기서 경로는 데이터스토어 백업 볼륨의 루트에 상대적입니다. 예를 들어 경로 [storage1] / systemlogs는 경로 /vmfs/volumes/storage1/systemlogs에 매핑됩니다.
Syslog.global.logDirUnique	이 옵션을 선택하면 Syslog.global.LogDir에서 지정한 디렉토리 아래에 ESXi 호스트의 이름을 가진 하위 디렉토리가 생성됩니다. 여러 ESXi 호스트에서 동일한 NFS 디렉토리를 사용하는 경우에는 고유한 디렉토리를 사용하는 것이 유용합니다.

3 설정 이름을 마우스 오른쪽 버튼으로 클릭하고 드롭다운 메뉴에서 **옵션 편집**을 선택합니다.

옵션 편집 대화상자가 열립니다.

4 원격 호스트에 로그인할 때 SSL 인증서 검사를 수행하려면 **새 값**에서 **True**를 클릭합니다.

5 **저장**을 클릭합니다.

6 (선택 사항) 키 설정을 기본값으로 재설정하려면 목록에서 해당 키를 마우스 오른쪽 버튼으로 클릭하고 **기본값으로 재설정**을 선택합니다.

고급 TLS/SSL 키 옵션 구성

ESXi 호스트와의 통신을 암호화하는 데 사용되는 보안 프로토콜 및 암호화 알고리즘을 구성할 수 있습니다.

자세한 내용은 VMware KB 문서(<https://kb.vmware.com/s/article/79476>)를 참조하십시오.

TLS(Transport Layer Security) 키는 TLS 프로토콜을 사용하여 호스트와의 통신을 보호합니다. 처음 부팅할 때 ESXi 호스트는 TLS 키를 2048비트 RSA 키로 생성합니다. 현재 ESXi는 TLS에 대한 ECDSA 키의 자동 생성을 구현하지 않습니다. TLS 개인 키는 관리자가 서비스하기 위한 것이 아닙니다.

SSH 키는 SSH 프로토콜을 사용하여 ESXi 호스트와의 통신을 보호합니다. 처음 부팅할 때 시스템은 SSH 키를 2048비트 RSA 키로 생성합니다. SSH 서버는 기본적으로 비활성화되어 있습니다. SSH 액세스는 주로 문제 해결을 위한 것입니다. SSH 키는 관리자가 서비스하기 위한 것이 아닙니다. SSH를 통해 로그인하려면 전체 호스트 제어와 동등한 관리 권한이 필요합니다. SSH 액세스를 사용하도록 설정하려면 [VMware Host Client에서 SSH\(Secure Shell\) 사용](#) 항목을 참조하십시오.

다음 ESXi 호스트 보안 키 설정을 구성할 수 있습니다.

참고 UserVars.ESXiVPsAllowedCiphers 보안 키 설정은 I/O 필터에만 영향을 줍니다.

키	기본값	설명
UserVars.ESXiVPsAllowedCiphers	! aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES: ECDH+AES:RSA+AES	기본 암호 제어 문자열입니다.
Config.HostAgent.ssl.keyStore.allowAny	False	ESXi CA 신뢰 저장소에 인증서를 추가할 수 있습니다.

키	기본값	설명
Config.HostAgent.ssl.keyStore.allowSelfSigned	False	CA가 아닌 자체 서명 인증서를 ESXi CA 신뢰 저장소에 추가할 수 있습니다(즉, CA 비트가 설정되지 않은 인증서).
Config.HostAgent.ssl.keyStore.discardLeaf	True	ESXi CA 신뢰 저장소에 추가된 리프 인증서를 삭제합니다.

ESXi 보안 키 설정을 구성하려면 다음을 수행합니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **고급 설정**을 클릭합니다.
- 2 **검색** 텍스트 상자에 보안 키를 입력하고 **검색** 아이콘을 클릭합니다.
- 3 보안 키를 마우스 오른쪽 버튼으로 클릭하고 드롭다운 메뉴에서 **옵션 편집**을 선택합니다.
옵션 편집 대화상자가 열립니다.
- 4 **새 값** 필드에 새 값을 입력하고 **저장**을 클릭합니다.
- 5 (선택 사항) 키 설정을 기본값으로 재설정하려면 목록에서 해당 키를 마우스 오른쪽 버튼으로 클릭하고 **기본값으로 재설정**을 선택합니다.

Userworld 메모리 비우기 구성

VMware Host Client에서는 고급 옵션인 `Mem.MemEagerZero`를 사용하여 가상 시스템 및 사용자 공간 애플리케이션에 대해 페이지를 비우는 방식을 결정할 수 있습니다.

모든 페이지가 가상 시스템 및 사용자 공간 애플리케이션에 할당될 때 해당 페이지를 비우려면 `Mem.MemEagerZero`를 1로 설정합니다. 메모리가 재사용되지 않는 경우 이 설정을 통해 메모리에 이전 콘텐츠를 유지하면서 가상 시스템 또는 사용자 공간 애플리케이션의 정보가 다른 클라이언트에 노출되지 못하게 방지할 수 있습니다.

`Mem.MemEagerZero`를 1로 설정하면 사용자 공간 애플리케이션이 종료될 때 페이지가 비워집니다. 가상 시스템은 다음과 같은 경우 해당 페이지가 비워집니다.

- 가상 시스템의 전원이 꺼져 있습니다.
- 가상 시스템 페이지가 마이그레이션됩니다.
- ESXi 호스트가 가상 시스템 메모리를 회수합니다.

참고 가상 시스템의 경우 `sched.mem.eagerZero` 고급 옵션을 **TRUE**로 설정하여 이러한 동작을 가져올 수 있습니다.

고급 가상 시스템 옵션 설정에 대한 자세한 내용은 "vSphere 리소스 관리" 설명서를 참조하십시오.

userworld 메모리 비우기를 구성하려면 다음 단계를 수행합니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **고급 설정**을 클릭합니다.
- 2 **검색** 텍스트 상자에 **Mem.MemEagerZero**를 입력하고 **검색** 아이콘을 클릭합니다.
- 3 Mem.MemEagerZero을 마우스 오른쪽 버튼으로 클릭하고 드롭다운 메뉴에서 **옵션 편집**을 선택합니다.
옵션 편집 대화상자가 열립니다.
- 4 **새 값** 텍스트 상자에 새 값을 입력합니다.
기본값은 0입니다.
- 5 **저장**을 클릭합니다.
- 6 (선택 사항) 키 설정을 기본값으로 재설정하려면 목록에서 해당 키를 마우스 오른쪽 버튼으로 클릭하고 **기본값으로 재설정**을 선택합니다.

VMware Host Client에서 자동 시작 구성 변경

호스트가 시작되고 중지될 때 ESXi 호스트가 설정할 자동 시작 옵션을 구성합니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **시스템**을 클릭합니다.
- 2 **자동 시작**을 클릭합니다.
- 3 **설정 편집**을 클릭합니다.
- 4 **예**를 선택하여 자동 시작 구성 변경 내용을 설정합니다.

옵션	설명
시작 지연	ESXi 호스트를 시작하면 이 호스트는 자동 시작되도록 구성된 가상 시스템의 전원을 켜기 시작합니다. ESXi 호스트는 첫 번째 가상 시스템의 전원을 켜 후 지정된 지연 시간 동안 기다렸다가 다음 가상 시스템의 전원을 켭니다.
중지 지연	중지 지연은 종료 명령이 완료될 때까지 ESXi 호스트가 대기하는 최대 시간입니다. 가상 시스템은 시작 순서와 반대로 종료됩니다. ESXi 호스트에서 지정한 시간 내에 첫 번째 가상 시스템이 종료되면 호스트는 다음 가상 시스템을 종료합니다. 지정된 지연 시간 내에 가상 시스템이 종료되지 않으면 호스트는 전원 끄기 명령을 실행한 후 다음 가상 시스템 종료를 시작합니다. ESXi 호스트는 모든 가상 시스템이 종료된 후에만 종료됩니다.

옵션	설명
작업 중지	호스트가 종료될 때 해당 호스트의 가상 시스템에 적용할 수 있는 종료 작업을 선택합니다. <ul style="list-style-type: none"> ■ 시스템 기본값 ■ 전원 끄기 ■ 일시 중단 ■ 종료
하트비트 대기	예를 선택하여 하트비트 대기 옵션을 사용하도록 설정합니다. 가상 시스템의 게스트 운영 체제에 VMware Tools가 설치된 경우 이 옵션을 사용할 수 있습니다. ESXi 호스트가 첫 번째 가상 시스템의 전원을 켜면 호스트는 즉시 다음 가상 시스템의 전원을 켭니다. 가상 시스템의 전원이 켜지는 시작 순서는 가상 시스템이 첫 번째 하트비트를 수신한 후에도 계속됩니다.

지연 옵션을 -1로 설정하면 시스템에서 기본 옵션을 사용합니다.

5 **저장**을 클릭합니다.

VMware Host Client에서 ESXi 호스트의 시간 구성 편집

VMware Host Client를 사용하여 호스트의 시간 설정을 수동으로 구성하거나 호스트의 시간 및 날짜를 NTP 또는 PTP 서버와 동기화할 수 있습니다. NTP는 밀리초 타이밍 정확도를 제공하고 PTP는 마이크로초 타이밍 정확도를 유지합니다.

호스트의 NTP 서비스는 NTP 서버의 시간 및 날짜를 정기적으로 가져옵니다. **시작**, **중지** 또는 **다시 시작** 버튼을 사용하여 NTP 서비스에 대해 선택된 시작 정책에 상관없이 언제든지 호스트의 NTP 서비스 상태를 변경할 수 있습니다.

PTP는 네트워크 내 가상 시스템에 정확한 시간 동기화를 프로비저닝합니다. 호스트에서 언제든지 PTP 서비스를 변경하려면 **시작**, **중지** 또는 **다시 시작** 버튼을 사용하면 됩니다. PTP 서비스를 시작하거나 중지하면 PTP가 자동으로 활성화 또는 비활성화됩니다. PTP를 수동으로 활성화 또는 비활성화할 때 변경 내용을 적용하려면 PTP 서비스를 시작하거나 중지합니다.

서비스에 대한 자세한 내용은 [VMware Host Client에서 서비스 관리](#)에서 참조하십시오.

참고 NTP와 PTP 서비스는 동시에 실행할 수 없습니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭합니다.
- 2 **시스템** 탭에서 **시간 및 날짜**를 클릭합니다.

3 호스트의 시간 및 날짜를 설정합니다.

옵션	작업
이 호스트에서 날짜 및 시간 수동 구성	a NTP 설정 편집 을 클릭합니다. NTP 설정 편집 대화 상자가 나타납니다. b 호스트의 시간 및 날짜를 수동으로 설정합니다. c 저장 을 클릭합니다.
네트워크 시간 프로토콜 사용(NTP 클라이언트 사용)	a NTP 설정 편집 을 클릭합니다. NTP 설정 편집 대화 상자가 나타납니다. b 네트워크 시간 프로토콜 사용 라디오 버튼을 선택합니다. c NTP 서버 텍스트 상자에 사용할 NTP 서버의 IP 주소나 호스트 이름을 입력합니다. d NTP 서비스 시작 정책 드롭다운 메뉴에서 호스트의 NTP 서비스를 시작 및 중지하기 위한 옵션을 선택합니다. <ul style="list-style-type: none"> ■ 포트의 사용 현황에 따라 시작 및 중지합니다. 호스트의 보안 프로파일에 액세스하기 위해 NTP 클라이언트 포트가 활성화되거나 비활성화될 때 NTP 서비스를 시작하거나 중지합니다. ■ 호스트와 함께 시작 및 중지. 호스트의 전원을 켜거나 호스트를 종료할 때 NTP 서비스를 시작 또는 중지합니다. ■ 수동으로 시작 및 중지. NTP 서비스를 수동으로 시작하고 중지할 수 있습니다. 수동으로 시작 및 중지 정책을 선택하면 UI 제어를 사용할 때만 NTP 서비스의 상태가 변경됩니다. e 저장 을 클릭합니다.
정밀 시간 프로토콜 사용(PTP 클라이언트 사용)	a PTP 설정 편집 을 클릭합니다. b 사용 확인란 을 선택합니다. c 네트워크 인터페이스 드롭다운 메뉴에서 네트워크 인터페이스를 선택합니다. IPv4 및 서브넷 마스크가 나타납니다. d 저장 을 클릭합니다.

VMware Host Client를 사용하여 ESXi 호스트에 대한 하드웨어 관리

VMware Host Client를 사용하여 ESXi 호스트에 로그인하면 PCI 디바이스를 관리하고 전원 관리 설정을 구성할 수 있습니다.

ESXi 호스트 전원 관리 정책

호스트 하드웨어에서 제공하는 ESXi의 여러 전원 관리 기능을 적용하여 성능과 전원 간의 균형을 조정할 수 있습니다. ESXi에서 이러한 기능을 사용하는 방법은 전원 관리 정책을 선택하여 제어할 수 있습니다.

고성능 정책을 선택하면 보다 강력한 성능을 얻을 수 있지만 효율성 및 와트당 성능은 낮아집니다. 저전력 정책을 선택하면 절대 성능은 줄어들지만 효율성이 높아집니다.

VMware Host Client를 사용하면 관리하는 호스트에 대한 정책을 선택할 수 있습니다. 정책을 선택하지 않으면 ESXi에서는 기본적으로 균형 조정을 사용합니다.

표 2-1. CPU 전원 관리 정책

전원 관리 정책	설명
고성능	전원 관리 기능을 사용하지 않습니다.
균형 조정(기본값)	성능 손실을 최소화하면서 에너지 소비 줄임
저전력	성능 저하의 위험을 감수하고 에너지 소비 줄임
사용자 지정	사용자 정의 전원 관리 정책입니다. 고급 구성을 사용할 수 있게 됩니다.

CPU가 낮은 주파수로 실행되면 낮은 전압으로 실행되어 전력을 절감할 수 있습니다. 이러한 유형의 전원 관리를 일반적으로 DVFS(Dynamic Voltage and Frequency Scaling)라 합니다. ESXi에서는 가상 시스템 성능이 저하되지 않도록 CPU 주파수를 조정하려고 합니다.

CPU가 유휴 상태이면 ESXi는 깊은 중지 상태(C-상태라고도 함)를 적용할 수 있습니다. C-상태가 깊어질수록 CPU에서 더 적은 전력을 사용하지만 CPU가 실행을 재개하는 데 걸리는 시간도 늘어납니다. CPU가 유휴 상태가 되면 ESXi에서는 유휴 상태 기간을 예측하는 알고리즘을 적용해 전환할 적절한 C-상태를 선택합니다. 깊은 C-상태를 사용하지 않는 전원 관리 정책의 경우 ESXi는 유휴 상태의 CPU에 가장 얕은 중지 상태인 C1만 사용합니다.

VMware Host Client에서 전원 관리 정책 변경

관리하는 호스트의 전원 관리 정책을 변경하여 호스트의 에너지 소비를 제어합니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **하드웨어**를 클릭합니다.
- 2 **전원 관리**를 클릭하고 **정책 변경**을 클릭합니다.
사용할 수 있는 전원 관리 정책이 표시됩니다.
- 3 적용할 정책을 선택하고 **확인**을 클릭합니다.

VMware Host Client에서 하드웨어 레이블 변경

VMware Host Client에서는 가상 시스템에서 사용 가능한 모든 PCI 패스스루 디바이스의 하드웨어 레이블을 변경할 수 있습니다. 하드웨어 레이블을 사용하여 가상 시스템 배치를 특정 하드웨어 인스턴스로 제한합니다. 동일한 하드웨어 레이블 또는 빈 하드웨어 레이블이 있는 사용 가능한 모든 디바이스를 가상 시스템에 추가할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭합니다.
- 2 **하드웨어** 탭에서 **PCI 디바이스**를 클릭합니다.
- 3 목록에서 사용 가능한 디바이스를 선택하고 **하드웨어 레이블**을 클릭합니다.
선택한 디바이스에 대해 패스스루 전환이 활성화 상태여야 합니다.
하드웨어 레이블 편집 대화 상자가 나타납니다.

4 하드웨어 레이블을 편집하고 **저장**을 클릭하여 변경 내용을 적용합니다.

결과

새 하드웨어 레이블이 하드웨어 레이블 열에 나타납니다.

ESXi 호스트에 대한 라이선싱

ESXi 호스트는 vSphere 라이선스를 통해 라이선스가 할당됩니다. 각각의 vSphere 라이선스에는 ESXi 호스트의 여러 물리적 CPU에 라이선스를 부여하는 데 사용할 수 있는 특정 용량이 있습니다.

vSphere에 대한 세 가지 주요 라이선싱 모델이 있습니다.

- 최대 32개 코어가 있는 하나의 CPU를 포함하는 CPU별 라이선싱.
- 가상 시스템별 라이선싱.
- 구독 기반 라이선싱.

ESXi 호스트에 라이선스를 부여하려면 다음과 같은 사전 요구 사항을 충족하는 vSphere 라이선스를 호스트에 할당해야 합니다.

- 라이선싱 모델에 따라 라이선스에 충분한 용량이 있어야 합니다.
- 라이선스는 호스트가 사용하는 모든 기능을 지원해야 합니다. 예를 들어 호스트가 vSphere Distributed Switch와 연결된 경우 할당하는 라이선스는 vSphere Distributed Switch 기능을 지원해야 합니다.

용량이 충분하지 않거나 호스트가 사용하는 기능을 지원하지 않는 라이선스를 할당하려고 시도하면 라이선스 할당이 실패합니다.

vSphere의 CPU별 라이선싱 모델

vSphere 7.0부터는 CPU 라이선스 하나가 최대 32개의 코어가 포함된 CPU 하나에 적용됩니다. CPU 하나의 코어 수가 32를 초과하면 CPU 라이선스가 추가로 필요합니다.

CPU 수	CPU당 코어 수	CPU 라이선스 수
1	1-32	1
2	1-32	2
1	33-64	2
2	33-64	4

vSphere 라이선스를 호스트에 할당할 때 사용되는 용량은 호스트의 물리적 CPU 수와 각 물리적 CPU의 코어 수에 따라 결정됩니다.

최대 32코어의 라이선싱 모델을 사용하는 경우 32코어 CPU 10개에 대한 vSphere 라이선스를 다음과 같은 호스트 조합 중 하나에 할당할 수 있습니다.

- CPU당 코어 수가 32인 2중 CPU 호스트 5개
- CPU당 코어 수가 64인 1중 CPU 호스트 5개

- CPU당 코어 수가 48인 2중 CPU 호스트 2개 및 CPU당 코어 수가 20인 단일 CPU 호스트 2개

2개 또는 4개의 독립적 CPU를 단일 칩에 결합하는 Intel CPU 같은 듀얼 코어 및 쿼드 코어 CPU는 1개의 CPU로 간주됩니다.

vSphere의 가상 시스템별 라이선싱 모델

일부 VMware 제품은 가상 시스템별로 라이선스가 부여됩니다.

예를 들어 Horizon View와 같은 VDI 환경을 위한 vSphere Desktop이 있습니다. vSphere Desktop에 대한 라이선스 사용은 vSphere Desktop 라이선스가 할당된 호스트에서 실행 중인 전원이 켜진 데스크톱 가상 시스템의 총 수와 같습니다.

vSphere의 구독 기반 라이선싱 모델

vSphere+ 워크로드 플랫폼을 사용하면 vSphere의 라이선스 기반 관리에서 종량제 구독 모델로 전환할 수 있습니다. 자세한 내용은 "vCenter Server 및 호스트 관리" 설명서에서 **vSphere+ 및 vSAN+ 구독**을 참조하십시오.

ESXi 호스트에 대한 평가 모드 라이선스

ESXi를 설치하면 최대 60일(연속) 동안 평가 모드로 작동합니다. 평가 모드 라이선스는 최신 vSphere 제품 버전의 모든 기능을 제공합니다.

ESXi 호스트에 라이선스를 할당한 후 평가 기간이 만료되기 전에 언제든지 호스트를 다시 평가 모드로 설정하면 남은 평가 기간 동안 사용할 수 있는 전체 기능 집합을 탐색할 수 있습니다.

예를 들어 ESXi 호스트를 평가 모드로 20일 동안 사용한 다음, 호스트에 vSphere Standard 라이선스를 할당하고 5일 후에 호스트를 다시 평가 모드로 설정하면 남은 평가 기간인 35일 동안 호스트에서 사용할 수 있는 전체 기능 집합을 탐색할 수 있습니다.

ESXi 호스트의 라이선스 및 평가 기간 만료

ESXi 호스트의 경우 라이선스 또는 평가 기간이 만료되면 vCenter Server에서 연결이 끊깁니다. 전원이 켜진 모든 가상 시스템은 계속 작동하지만 전원이 꺼진 후 가상 시스템의 전원을 켤 수는 없습니다. 이미 사용 중인 기능의 현재 구성은 변경할 수 없습니다. 라이선스 만료 전에 사용하지 않은 상태로 남아있는 기능은 사용할 수 없습니다.

참고 만료되는 라이선스가 있으면 라이선스 만료 90일 전에 알림이 표시됩니다.

업그레이드 후 ESXi 호스트 라이선싱

ESXi 호스트를 동일한 숫자로 시작되는 버전으로 업그레이드하는 경우 기존 라이선스를 새 라이선스로 교체하지 않아도 됩니다. 예를 들어 호스트를 ESXi 8.0에서 8.1로 업그레이드하는 경우 호스트에 동일한 라이선스를 사용할 수 있습니다.

ESXi 호스트를 버전 번호가 다른 주 버전으로 업그레이드하는 경우 평가 기간이 다시 시작되고 새 라이선스를 할당해야 합니다. 예를 들어, ESXi 호스트를 7.x에서 8.x로 업그레이드할 때는 해당 호스트에 vSphere 8 라이선스를 할당해야 합니다.

VMware Host Client 환경에 대한 라이선싱 정보 보기

VMware Host Client에서 사용할 수 있는 라이선스와 함께 만료 날짜, 라이선스 키 및 다양한 기능을 볼 수 있습니다. 사용 가능한 제품과 자산을 볼 수도 있습니다.

절차

- ◆ VMware Host Client 인벤토리에서 **관리**를 클릭하고 **라이선싱**을 클릭합니다.
라이선스 키, 만료 날짜 및 모든 사용 가능한 기능 및 자산을 볼 수 있습니다.

VMware Host Client에서 ESXi 호스트에 라이선스 키 할당

VMware Host Client를 사용하여 기존 또는 새 라이선스 키를 ESXi 호스트에 할당할 수 있습니다.

사전 요구 사항

글로벌 라이선스 권한이 있는지 확인합니다.

참고 vCenter Server를 사용하여 ESXi 호스트를 관리하는 경우에는 vSphere Client에서만 라이선스를 변경할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **라이선싱**을 클릭합니다.
- 2 **라이선스 할당**을 클릭하고 **xxxxxx-xxxxxx-xxxxxx-xxxxxx-xxxxxx** 형식으로 라이선스 키를 입력한 다음 **라이선스 확인**을 클릭합니다.
- 3 **라이선스 할당**을 클릭하여 변경 내용을 저장합니다.

VMware Host Client에서 ESXi 호스트로부터 라이선스 제거

vSphere와 함께 사용하는 제품의 라이선싱 모델 규정을 계속 준수하려면 할당되지 않은 모든 라이선스를 인벤토리에서 제거해야 합니다.

Customer Connect에서 라이선스를 분할, 결합 또는 업그레이드한 경우에는 이전 라이선스를 제거해야 합니다.

예를 들어 Customer Connect에서 vSphere 라이선스를 6.5에서 6.7로 업그레이드했다고 가정해 보십시오. 이 라이선스를 ESXi 6.7 호스트에 할당합니다. 새로운 vSphere 6.7 라이선스를 할당한 후에는 이전 vSphere 6.5 라이선스를 인벤토리에서 제거해야 합니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **라이선싱**을 클릭합니다.
- 2 **라이선스 제거**를 클릭하고 **확인**을 클릭합니다.

VMware Host Client에서 서비스 관리

VMware Host Client에서 로그인한 호스트에서 실행 중인 서비스를 시작, 중지 및 다시 시작할 수 있고 호스트 서비스 정책을 구성할 수 있습니다.

호스트 구성을 변경하거나 의심되는 기능 또는 성능 문제가 있는 경우 서비스를 다시 시작할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **서비스**를 클릭합니다.
- 2 **서비스** 목록에서 서비스를 선택합니다.
- 3 **작업** 드롭다운 메뉴에서 작업을 선택합니다.
 - **다시 시작**
 - **시작**
 - **중지**
- 4 (선택 사항) **작업** 드롭다운 메뉴에서 **정책**을 선택하고 메뉴에서 서비스에 대한 옵션을 선택합니다.
 - **방화벽 포트와 함께 시작 및 중지**
 - **호스트와 함께 시작 및 중지**
 - **수동으로 시작 및 중지**

VMware Host Client를 사용하여 ESXi에 대한 보안 및 사용자 관리

ESXi 하이퍼바이저 아키텍처에는 보안을 강화하기 위해 구성할 수 있는 많은 기본 제공 보안 기능이 있습니다.

VMware Host Client를 사용하여 액티브 디렉토리와 같은 기능을 구성하고 인증서를 관리할 수도 있습니다.

VMware Host Client를 사용하여 호스트 인증 관리

VMware Host Client를 사용하여 ESXi 호스트에 로그인하면 액티브 디렉토리 및 스마트 카드 인증을 사용하도록 설정했는지 여부를 확인하고 디렉토리 서비스 도메인에 호스트를 가입시킬 수도 있습니다.

VMware Host Client를 사용하여 디렉토리 서비스 도메인에 ESXi 호스트 가입

호스트에 대해 디렉토리 서비스를 사용하려면 호스트를 디렉토리 서비스 도메인에 가입시켜야 합니다.

두 가지 방법 중 하나로 도메인 이름을 입력할 수 있습니다.

- **name.tld**(예: **domain.com**): 계정이 기본 컨테이너 아래에 생성됩니다.
- **name.tld/container/path**(예: **domain.com/OU1/OU2**): 계정이 특정 OU(조직 구성 단위) 아래에 생성됩니다.

vSphere Authentication Proxy 서비스를 사용하려면 "vSphere 보안" 항목을 참조하십시오.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **보안 및 사용자**를 클릭합니다.
- 2 **인증**을 클릭하고 **도메인 가입**을 클릭합니다.
- 3 도메인 이름을 입력합니다.
name.tld 또는 **name.tld/container/path** 형식을 사용합니다.
- 4 도메인에 호스트를 가입시킬 수 있는 사용 권한이 있는 디렉토리 서비스 사용자 계정의 사용자 이름 및 암호를 입력하고 **도메인 가입**을 클릭합니다.
- 5 (선택 사항) 인증 프록시를 사용하려면 프록시 서버 IP 주소를 입력하고 **도메인 가입**을 클릭합니다.

Active Directory를 통해 ESXi 사용자 관리

Active Directory와 같은 디렉토리 서비스를 사용하여 사용자를 관리하도록 ESXi를 구성할 수 있습니다.

각 호스트에서 로컬 사용자 계정을 생성하면 여러 호스트에서 계정 이름과 암호를 동기화해야 하는 번거로움이 있습니다. ESXi 호스트를 Active Directory 도메인에 가입하면 로컬 사용자 계정을 생성하고 유지할 필요가 없습니다. Active Directory를 사용하여 사용자를 인증하면 ESXi 호스트 구성이 간소화되고 무단 액세스가 발생할 수 있는 구성 문제의 위험이 줄어듭니다.

Active Directory를 사용할 경우 사용자는 도메인에 호스트를 추가할 때 자신의 Active Directory 자격 증명과 Active Directory 서버의 도메인 이름을 제공합니다.

vSphere Authentication Proxy 사용

명시적으로 Active Directory 도메인에 ESXi 호스트를 추가하는 대신 vSphere Authentication Proxy를 사용하여 Active Directory 도메인에 호스트를 추가할 수 있습니다.

Active Directory 서버의 도메인 이름과 vSphere Authentication Proxy의 IP 주소만 지정하여 호스트를 설정하면 됩니다. vSphere Authentication Proxy가 사용하도록 설정된 경우 이를 통해 Auto Deploy를 사용하여 프로비저닝되는 호스트가 Active Directory 도메인에 자동으로 추가됩니다. 또한 Auto Deploy를 사용하여 프로비저닝되지 않는 호스트에도 vSphere Authentication Proxy를 사용할 수 있습니다.

vSphere Authentication Proxy를 사용하도록 설정하는 방법 및 vSphere Authentication Proxy에 필요한 vCenter Server 포트에 대한 자세한 내용은 "vSphere 보안" 설명서를 참조하십시오.

Auto Deploy

Auto Deploy를 사용하여 호스트를 프로비저닝하는 경우 Authentication Proxy를 가리키는 참조 호스트를 설정할 수 있습니다. 그런 다음 Auto Deploy를 사용하여 프로비저닝된 모든 ESXi 호스트에 참조 호스트의 프로파일을 적용하는 규칙을 설정합니다. vSphere Authentication Proxy는 Auto Deploy가 PXE를 사용하여 프로비저닝하는 모든 호스트의 IP 주소를 해당 액세스 제어 목록에 저장합니다. 호스트가 부팅될 때 호스트에서 vSphere Authentication Proxy에 연결하며 vSphere Authentication Proxy가 해당 액세스 제어 목록에 이미 있는 호스트를 Active Directory 도메인에 가입시킵니다.

VMCA 또는 타사 인증서로 프로비저닝된 인증서를 사용하는 환경에서 vSphere Authentication Proxy를 사용하더라도 Auto Deploy를 사용한 사용자 지정 인증서 사용에 대한 지침을 따르는 한 프로세스가 원활하게 작동합니다.

다른 ESXi 호스트

다른 호스트가 Active Directory 자격 증명을 사용하지 않고 도메인에 가입할 수 있도록 하려는 경우 해당 호스트가 vSphere Authentication Proxy를 사용하도록 설정할 수 있습니다. 즉, 해당 호스트에 Active Directory 자격 증명을 전송할 필요가 없고 호스트 프로파일에 Active Directory 자격 증명이 저장되지 않습니다.

이 경우 호스트의 IP 주소가 vSphere Authentication Proxy 액세스 제어 목록에 추가되고 vSphere Authentication Proxy에서 기본적으로 IP 주소를 기반으로 호스트를 인증합니다. 클라이언트 인증을 사용하도록 설정하여 vSphere Authentication Proxy에서 호스트의 인증서를 확인하게 할 수 있습니다.

참고 IPv6만 지원하는 환경에서는 vSphere Authentication Proxy를 사용할 수 없습니다.

VMware Host Client를 사용하여 호스트 인증서 관리

VMware Host Client를 사용하여 ESXi 호스트에 로그인하면 발급자 및 유효 기간과 같은 호스트의 인증서 세부 정보를 보고 새 인증서를 가져올 수도 있습니다.

VMware Host Client에서 ESXi 호스트에 대한 인증서 세부 정보 보기

인증서 정보를 디버깅에 사용할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **보안 및 사용자**를 클릭합니다.
- 2 **인증서**를 클릭합니다.

다음 인증서 세부 정보를 볼 수 있습니다.

필드	설명
발급자	인증서의 발급자입니다.
다음 날짜까지 유효:	인증서가 만료되는 날짜입니다.
다음 날짜부터 유효	인증서가 생성된 날짜입니다.
제목	인증서 생성 동안 사용되는 제목입니다.

VMware Host Client에서 ESXi 호스트에 대한 새 인증서 가져오기

VMware Host Client로 ESXi 호스트에 로그인한 경우 신뢰할 수 있는 CA(인증 기관)로부터 인증서를 가져올 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **보안 및 사용자**를 클릭합니다.

- 2 **인증서를 클릭하고 새 인증서 가져오기**를 클릭합니다.
- 3 인증서 서명 요청을 생성합니다.

옵션	설명
FQDN 서명 요청 생성	<ul style="list-style-type: none"> ■ FQDN 서명 요청 생성을 클릭하고 클립보드에 복사 버튼을 클릭한 후 닫기를 클릭합니다. ■ 서명된 인증서를 생성하려면 CA(인증 기관)에 인증서 서명 요청을 전달합니다. ■ 인증서 텍스트 상자에 생성된 서명된 인증서를 PEM 형식으로 붙여넣고 가져오기를 클릭합니다.
IP 서명 요청 생성	<ul style="list-style-type: none"> ■ IP 서명 요청 생성을 클릭하고 클립보드에 복사 버튼을 클릭한 후 닫기를 클릭합니다. ■ 서명된 인증서를 생성하려면 CA에 인증서 서명 요청을 전달합니다. ■ 인증서 텍스트 상자에 생성된 서명된 인증서를 PEM 형식으로 붙여넣고 가져오기를 클릭합니다.

인증서를 즉시 가져올 필요는 없습니다. 서명된 인증서를 사용할 수 있으려면 인증서 서명 요청을 생성하고 인증서를 가져오는 사이에 호스트를 다시 시작하지 마십시오.

그러면 공식 인증서를 생성하기 위해 인증서 서명 요청이 CA(인증 기관)로 전달됩니다.

FQDN 요청에는 인증서의 공통 이름 필드 결과에 호스트의 정규화된 호스트 이름이 있습니다. IP 서명 요청에는 공통 이름 필드에 호스트의 현재 IP 주소가 있습니다.

VMware Host Client를 사용하여 사용자 관리

사용자 관리를 통해 ESXi에 로그인할 수 있는 권한을 지닌 사용자를 제어할 수 있습니다.

사용자 및 역할은 ESXi 호스트 구성 요소에 액세스할 수 있는 사용자와 각 사용자가 수행할 수 있는 작업을 제어합니다.

vSphere 5.1 이상에서 ESXi 사용자 관리 기능을 사용할 때 주의할 사항은 다음과 같습니다.

- ESXi 호스트에 직접 연결할 때 생성된 사용자는 vCenter Server 사용자와 동일하지 않습니다. 호스트가 vCenter Server에 의해 관리되는 경우 vCenter Server는 호스트에 직접 생성된 사용자를 무시합니다.
- ESXi 사용자는 vSphere Client를 사용하여 생성할 수 없습니다. ESXi 사용자를 생성하려면 VMware Host Client를 통해 호스트에 직접 로그인해야 합니다.
- ESXi 5.1 이상은 로컬 그룹을 지원하지 않습니다. 그러나 Active Directory 그룹은 지원됩니다.

루트와 같은 익명 사용자가 DCUI(Direct Console User Interface) 또는 ESXi Shell을 사용하여 호스트에 액세스하는 것을 방지하려면 호스트의 루트 폴더에 대한 사용자의 관리자 권한을 제거합니다. 이것은 로컬 사용자와 Active Directory 사용자 및 그룹 모두에 적용됩니다.

VMware Host Client에서 ESXi 사용자 추가

사용자 표에 사용자를 추가하면 호스트에서 유지 관리하는 내부 사용자 목록이 업데이트됩니다.

사전 요구 사항

암호 요구 사항에 대한 자세한 내용은 [VMware Host Client에서 암호 및 계정 잠금 정책 구성](#) 또는 "vSphere 보안" 설명서를 참조하십시오.

절차

- 1 VMware Host Client로 ESXi에 로그인합니다.
vSphere Client에서는 ESXi 사용자를 생성할 수 없습니다. ESXi 사용자를 생성하려면 VMware Host Client를 통해 호스트에 직접 로그인해야 합니다.
- 2 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **보안 및 사용자**를 클릭합니다.
- 3 **사용자**를 클릭합니다.
- 4 **사용자 추가**를 클릭합니다.
- 5 사용자 이름 및 암호를 입력합니다.

참고 이름이 **ALL**인 사용자는 생성하지 마십시오. 경우에 따라 일부 사용자는 이름 **ALL**과 관련된 권한을 사용하지 못할 수도 있습니다. 예를 들어, 이름이 **ALL**인 사용자가 관리자 권한을 가지고 있는 경우 **ReadOnly** 권한이 있는 사용자가 원격으로 호스트에 로그인할 수 있습니다. 이러한 동작은 적절하지 않습니다.

- 사용자 이름에 공백을 포함하지 마십시오.
 - 사용자 이름에 ASCII가 아닌 문자를 포함하지 마십시오.
 - 길이 및 복잡성 요구 사항을 충족하는 암호를 생성합니다. 호스트는 기본 인증 플러그인인 `pam_passwdqc.so`를 사용하여 암호 규정 준수 여부를 확인합니다. 암호가 규정을 준수하지 않으면 암호 요구 사항을 나타내는 오류 메시지가 표시됩니다.
- 6 ESXi Shell에 대한 로컬 액세스를 활성화하려면 **셸 액세스 사용** 확인란을 선택합니다.
 - 7 **추가**를 클릭합니다.

VMware Host Client에서 ESXi 사용자 업데이트

VMware Host Client에서 ESXi 사용자에 대한 설명과 암호를 변경할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **보안 및 사용자**를 클릭합니다.
- 2 **사용자**를 클릭합니다.
- 3 목록에서 사용자를 선택하고 **사용자 편집**을 클릭합니다.
- 4 사용자 세부 정보를 업데이트하고 **저장**을 클릭합니다.

VMware Host Client에서 호스트로부터 로컬 ESXi 사용자 제거

호스트에서 로컬 ESXi 사용자를 제거할 수 있습니다.

경고 루트 사용자는 제거하지 마십시오.

호스트에서 사용자를 제거하면 해당 사용자는 호스트의 모든 개체에 대한 사용 권한을 잃게 되므로 다시 로그인할 수 없습니다.

참고 로그인한 사용자를 도메인에서 제거하면 호스트를 다시 시작할 때까지 해당 사용자는 호스트 권한을 유지합니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **보안 및 사용자**를 클릭합니다.
- 2 **사용자**를 클릭합니다.
- 3 목록에서 제거할 사용자를 선택하고 **사용자 제거**를 클릭한 다음 **예**를 클릭합니다.
어떤 경우에도 루트 사용자는 제거하지 마십시오.

VMware Host Client에서 ESXi 역할 관리

ESXi에서는 개체에 대한 사용 권한이 할당된 사용자에게만 개체에 대한 액세스 권한을 부여합니다. 개체에 대한 사용 권한을 사용자에게 할당할 때는 사용자와 역할을 쌍으로 연결합니다.

역할이란 미리 정의된 권한의 집합입니다. 권한에 대한 자세한 내용은 "vSphere 보안" 설명서를 참조하십시오.

ESXi 호스트에는 세 가지 기본 역할이 있는데 기본 역할과 연관된 권한은 변경할 수 없습니다. 각각의 기본 하위 역할에는 이전 역할의 권한이 포함됩니다. 예를 들어 관리자 역할은 읽기 전용 역할의 권한을 상속합니다. 사용자가 생성하는 역할은 기본 역할의 권한을 상속하지 않습니다.

VMware Host Client에서 역할 편집 기능을 사용하여 사용자 지정 역할을 생성하면 사용자 필요에 맞는 권한 집합을 생성할 수 있습니다. 또한 호스트에서 직접 생성한 역할은 vCenter Server에서 액세스할 수 없습니다. 이러한 역할에 대한 작업은 VMware Host Client에서 호스트에 직접 로그인한 경우에만 가능합니다.

참고 사용자 지정 역할을 추가할 때 역할에 권한을 할당하지 않으면 이 역할은 **System.Anonymous**, **System.View** 및 **System.Read** 시스템 정의 권한을 갖는 읽기 전용 역할로 생성됩니다.

vCenter Server를 통해 ESXi 호스트를 관리하는 경우에 호스트와 vCenter Server에서 사용자 지정 역할을 동시에 유지 보수하면 혼란이 발생하고 역할이 잘못 사용될 수 있습니다. 이와 같은 유형의 구성에서는 사용자 지정 역할을 vCenter Server에서만 유지 보수해야 합니다.

VMware Host Client를 사용하여 ESXi 호스트에 대한 직접 연결을 통해 호스트 역할을 생성하고 사용 권한을 설정할 수 있습니다.

VMware Host Client에서 역할 추가

환경의 액세스 제어 요구에 맞게 역할을 생성할 수 있습니다.

사전 요구 사항

루트 또는 vpxuser 같은 관리자 권한이 있는 사용자로 로그인했는지 확인합니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **보안 및 사용자**를 클릭합니다.
- 2 **역할**을 클릭합니다.
- 3 **역할 추가**를 클릭합니다.
- 4 새 역할의 이름을 입력합니다.
- 5 새 역할에 연결할 권한을 목록에서 선택한 다음 **추가**를 클릭합니다.

VMware Host Client에서 역할 업데이트

역할을 편집할 때 이 역할에 선택된 권한을 변경할 수 있습니다. 작업이 완료되면 편집된 역할이 할당된 사용자 또는 그룹에 이러한 권한이 적용됩니다.

사전 요구 사항

루트 또는 vpxuser 같은 관리자 권한이 있는 사용자로 로그인했는지 확인합니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **보안 및 사용자**를 클릭합니다.
- 2 **역할**을 클릭합니다.
- 3 목록에서 역할을 선택하고 **역할 편집**을 클릭합니다.
- 4 역할 세부 정보를 업데이트하고 **저장**을 클릭합니다.

VMware Host Client에서 역할 제거

어떠한 사용자 또는 그룹에도 할당되지 않은 역할을 제거하면 정의가 역할 목록에서 제거됩니다. 사용자 또는 그룹에 할당된 역할을 제거하는 경우 할당을 제거하거나 이러한 할당을 다른 역할에 대한 할당으로 바꿀 수 있습니다.

경고 모든 할당을 제거하거나 교체하기 전에 사용자가 어떤 영향을 받을지 알고 있어야 합니다. 사용 권한을 부여 받지 않은 사용자는 로그인할 수 없습니다.

사전 요구 사항

루트 또는 vpxuser 같은 관리자 권한이 있는 사용자로 로그인했는지 확인합니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **보안 및 사용자**를 클릭합니다.
- 2 **역할**을 클릭합니다.
- 3 목록에서 제거할 역할의 이름을 선택합니다.

4 역할 제거를 클릭하고 사용되지 않는 경우에만 제거를 선택한 다음 예를 클릭합니다.

vCenter Server에서 호스트 관리

호스트를 vCenter Server 시스템에 연결하면 vSphere 환경의 모든 호스트를 한 곳에서 모니터링하고 호스트 구성을 간소화할 수 있습니다.

ESXi 호스트의 구성 관리에 대한 자세한 내용은 "vSphere 네트워킹" 설명서, "vSphere 스토리지" 설명서 및 "vSphere 보안" 설명서를 참조하십시오.

VMware Host Client 환경을 최신 버전으로 업데이트

VMware Host Client의 최신 버전을 사용하는지 여부를 평가하려면 환경에 설치되어 있는 VIB를 확인하여 VIB 버전 정보를 검사합니다. ESXi 오프라인 번들 패키지의 `metadata.zip` 파일 또는 VIB에 대한 데이터스토어 경로 또는 URL을 입력하여 VMware Host Client 환경을 업데이트할 수 있습니다.

VIB 파일을 제공하는 경우 VMware Host Client 환경에 설치되어 있는 기존 VIB가 새 VIB로 업데이트됩니다.

오프라인 번들을 제공하는 경우 전체 ESXi 호스트를 번들에 있는 `metadata.zip` 파일에 설명된 버전으로 업데이트합니다. URL을 통해 전체 오프라인 번들을 사용할 수 있는지 또는 데이터스토어에 업로드되었는지 확인합니다.

절차

- ◆ 환경을 최신 버전으로 업데이트하려면 다음 작업을 수행합니다.

작업	단계
데이터스토어에 VIB 업로드	a VMware Host Client 환경에서 스토리지 를 클릭합니다. b 목록에서 데이터스토어를 선택하고 데이터스토어 브라우저 를 클릭합니다. c VIB를 저장하려면 디렉토리를 선택하고 업로드 를 클릭합니다. d 파일을 찾아서 두 번 클릭합니다.
데이터스토어에 오프라인 번들 업로드	a ESXi 오프라인 번들 패키지를 다운로드합니다. b ESXi 오프라인 번들 패키지를 ESXi 호스트에 업로드합니다. 오프라인 번들 패키지는 데이터스토어 브라우저 를 사용하거나 SCP 또는 WinSCP를 사용하여 업로드할 수 있습니다. c ESXi 호스트에서 오프라인 번들의 콘텐츠를 추출합니다. 예를 들어 SSH를 사용하여 호스트에 로그인합니다. d 오프라인 번들을 업로드한 디렉토리로 이동합니다. e 다음을 사용하여 콘텐츠를 추출합니다. <pre>unzip</pre> 명령.
환경 업데이트	a VMware Host Client에서 관리 를 클릭하고 패키지 를 클릭합니다. b 업데이트 설치 를 클릭하고 오프라인 번들의 <code>metadata.zip</code> 파일 또는 VIB에 대한 데이터스토어 경로 또는 URL을 입력합니다. c 업데이트 를 클릭합니다. <p>경고 vSphere Lifecycle Manager에 의해 관리되는 ESXi 호스트를 업데이트하면 호스트가 비준수 상태가 될 수 있습니다.</p> d 새로 고침 을 클릭하여 업데이트가 성공했는지 확인합니다.

최신 버전의 ESXi로 업그레이드한 후 VMware Host Client에서 ESXi 호스트로 연결할 수 없음

ESXi 호스트를 새 버전으로 업그레이드한 후 VMware Host Client를 사용하여 ESXi 호스트에 액세스하려고 하면 브라우저 콘솔에 오류 메시지가 표시될 수 있으며 연결이 실패할 수 있습니다.

문제

ESXi 호스트를 최신 버전으로 업그레이드한 후 `https://host-fqdn/ui` 또는 `https://1.2.3.4/ui`로 이동하려고 하면 다음과 같은 오류가 발생할 수 있습니다.

```
503 서비스 사용 불가(끝점에 연결하지 못함: [N7Vmacore4Http16LocalServiceSpecE:0xffa014e8]
_serverNamespace = /ui _isRedirect = false _port = 8308)
```

원인

`/etc/vmware/rhttpproxy/endpoints.conf`에 대한 변경 내용이 업그레이드 후 남아 있으며 이로 인해 `/ui` 끝점이 VMware Host Client를 재정의합니다.

/ticket이 6.0 이상 ESXi 호스트의 endpoint.conf 파일에서 누락되면 브라우저 내 가상 시스템 콘솔에 연결하지 못함 오류 메시지가 표시되지만 VMware Remote Console이 계속해서 작동합니다.

해결책

- 1 SSH 또는 ESXi Shell을 사용하여 ESXi 호스트에 로그인합니다.

SSH를 사용하는 경우 먼저 SSH를 사용하도록 설정해야 할 수 있습니다. DCUI를 사용하여 SSH를 사용하도록 설정할 수 있습니다.

- 2 endpoints.conf 파일을 백업합니다.

```
cp /etc/vmware/rhttpproxy/endpoints.conf /tmp
```

- 3 편집기에서 /etc/vmware/rhttpproxy/endpoints.conf 파일을 열고 다음 줄을 제거합니다.

```
/ui local 8308 redirect allow
```

- 4 rhttpproxy 구성 관리 서버를 다시 시작합니다.

```
/etc/init.d/rhttpproxy restart
```

- 5 유효한 숫자 IP 주소 **https://1.2.3.4/ui** 또는 **https://host-fqdn/ui**가 있는 보안 URL에서 호스트의 지정된 전체 이름을 사용하여 VMware Host Client에 액세스합니다.

vSphere Client로 전환

ESXi 호스트의 전체 기능 집합, 고급 관리 및 문제 해결 기능에 액세스하려면 ESXi 호스트를 vCenter Server에 연결합니다.

절차

- 1 VMware Host Client 인벤토리에서 **호스트**를 마우스 오른쪽 버튼으로 클릭하고 드롭다운 메뉴에서 **vCenter Server**를 사용하여 관리를 선택합니다.

새 창에 vCenter Server 로그인 페이지가 열립니다.

- 2 자격 증명을 입력하고 **로그인**을 클릭합니다.

VMware Host Client를 사용하여 vCenter Server와 ESXi 연결 끊기

vCenter Server를 통해 호스트 관리에 사용할 수 있는 기능의 고급 집합을 더 이상 사용하지 않으려는 경우 또는 vCenter Server가 실패했고 호스트에서 긴급 작업을 수행해야 하는 경우 vCenter Server와 ESXi 호스트의 연결을 끊을 수 있습니다.

ESXi 호스트의 연결을 끊는 데 몇 분이 걸릴 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **호스트**를 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **vCenter Server와 연결 끊기**를 선택합니다.

참고 이 호스트가 응답하지 않는 호스트 신호 vCenter Server 연결을 끊습니다.

- 2 vCenter Server와 **연결 끊기**를 클릭합니다.

VMware Host Client에서 ESXi 호스트 재부팅 또는 종료

VMware Host Client를 사용하여 ESXi 호스트를 다시 시작하거나 전원을 끌 수 있습니다. 관리 호스트의 전원을 끄면 vCenter Server와의 연결이 끊어지지만 해당 호스트가 인벤토리에서 제거되지는 않습니다.

사전 요구 사항

호스트를 재부팅하거나 종료하려면 이러한 권한이 필요합니다.

- **호스트.구성.유지 보수**
- **글로벌.이벤트 기록**

호스트를 재부팅하거나 종료하기 전에 항상 다음 태스크를 수행합니다.

- 호스트의 가상 시스템 전원을 모두 끕니다.
- 호스트를 유지 보수 모드에 설정합니다.

절차

- 1 호스트를 마우스 오른쪽 버튼으로 클릭하고 **호스트 종료** 또는 **호스트 재부팅**을 선택합니다.

참고 호스트가 유지 보수 모드가 아닌 경우 종료하거나 재부팅하면 이 호스트에서 실행 중인 가상 시스템은 안전하게 중지되지 않으며 저장하지 않은 데이터가 손실될 수 있습니다. 호스트가 vSAN 클러스터의 일부인 경우 호스트에서 vSAN 데이터에 대한 액세스가 손실될 수 있습니다.

- 2 **종료** 또는 **재부팅**을 클릭하여 절차를 완료합니다.

ESXi Shell 사용

ESXi Shell는 필수 유지 보수 명령을 제공하며 ESXi호스트에서 기본적으로 비활성화됩니다. 필요한 경우 셸에 대한 로컬 및 원격 액세스를 활성화할 수 있습니다. 무단 액세스 위험을 줄이기 위해 문제 해결용으로만 ESXi Shell을 활성화하십시오.

ESXi Shell은 잠금 모드와 상관이 없습니다. 호스트가 잠금 모드에서 실행되더라도 활성화되어 있으면 ESXi Shell에 로그인할 수 있습니다.

"vSphere 보안"의 내용을 참조하십시오.

해당 서비스는 다음과 같습니다.

ESXi Shell

ESXi Shell에 로컬로 액세스하려면 이 서비스를 활성화합니다.

SSH

SSH를 사용하여 ESXi Shell에 원격으로 액세스하려면 이 서비스를 활성화합니다.

DCUI(Direct Console User Interface)

잠금 모드에서 실행 중일 때 이 서비스를 활성화하면 로컬 위치에서 Direct Console User Interface에 루트 사용자로 로그인하고 잠금 모드를 비활성화할 수 있습니다. 그런 다음 VMware Host Client에 대한 직접 연결을 사용하거나 ESXi Shell을 활성화하여 호스트에 액세스할 수 있습니다.

루트 사용자와 관리자 역할이 할당된 사용자가 ESXi Shell에 액세스할 수 있습니다. Active Directory의 ESX Admins 그룹에 속한 사용자에게는 관리자 역할이 자동으로 할당됩니다. 기본적으로 루트 사용자만 ESXi Shell을 사용하여 시스템 명령(예: `vmware -v`)을 실행할 수 있습니다.

참고 실제로 액세스가 필요한 경우가 아니면 ESXi Shell을 활성화하지 마십시오.

VMware Host Client에서 SSH(Secure Shell) 사용

SSH(Secure Shell)를 사용하도록 설정하고 SSH를 사용하여 원격으로 ESXi Shell에 액세스합니다.

절차

- 1 SSH(보안 셸)를 활성화 또는 비활성화하려면 VMware Host Client 인벤토리에서 **호스트**를 마우스 오른쪽 버튼으로 클릭합니다.
- 2 드롭다운 메뉴에서 **서비스**를 선택합니다.
- 3 SSH(보안 셸)를 사용하도록 설정하려면 **SSH(Secure Shell) 사용**을 선택합니다.
- 4 ESXi Shell을 사용하도록 설정하려면 **ESXi Shell 사용**을 선택합니다.

VMware Host Client에서 ESXi 콘솔 셸 사용

잠금 모드에서 실행 중일 때 이 서비스를 사용하도록 설정하면 로컬 위치에서 Direct Console User Interface에 루트 사용자로 로그인하고 잠금 모드를 비활성화할 수 있습니다. 그런 다음 VMware Host Client에 대한 직접 연결을 사용하거나 ESXi Shell을 사용하도록 설정하여 호스트에 액세스할 수 있습니다.

절차

- 1 콘솔 셸을 활성화 또는 비활성화하려면 VMware Host Client 인벤토리에서 **호스트**를 마우스 오른쪽 버튼으로 클릭합니다.
- 2 드롭다운 메뉴에서 **서비스**를 선택하고 **콘솔 셸**을 선택합니다.
- 3 수행할 태스크를 선택합니다.
 - 콘솔 셸이 활성화된 경우 **사용 안 함**을 클릭하여 비활성화합니다.

- 콘솔 셸이 비활성화된 경우 **사용**을 클릭하여 활성화합니다.

VMware Host Client에서 ESXi Shell 가용성에 대한 시간 초과 생성

ESXi Shell은 기본적으로 비활성화되어 있습니다. 셸을 사용하도록 설정할 때 보안을 강화하기 위해 ESXi Shell에 대한 가용성 시간 초과를 설정할 수 있습니다.

가용성 시간 초과는 셸을 통한 로그인 기능이 비활성화되기 전까지 로컬 및 원격 셸 로그인이 모두 허용되는 지속 시간을 정의합니다. 가용성 시간 초과가 만료되면 기존 셸 세션은 유지되지만 새 셸 세션은 허용되지 않습니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭합니다.
- 2 **시스템** 탭에서 **고급 설정**을 선택합니다.
- 3 **검색** 텍스트 상자에 `UserVars.ESXiShellTimeOut`을 입력하고 **검색** 아이콘을 클릭합니다.
- 4 `UserVars.ESXiShellTimeOut`을 선택하고 **옵션 편집**을 클릭합니다.
옵션 편집 대화상자가 열립니다.
- 5 **새 값** 텍스트 상자에 시간 초과 설정을 입력합니다.
값이 0이면 시간 초과가 비활성화됩니다.
- 6 **저장**을 클릭합니다.
시간 초과를 적용하려면 SSH 서비스 및 ESXi Shell 서비스를 다시 시작해야 합니다.
- 7 (선택 사항) 키 설정을 기본값으로 재설정하려면 목록에서 해당 키를 마우스 오른쪽 버튼으로 클릭하고 **기본값으로 재설정**을 선택합니다.

VMware Host Client에서 유휴 ESXi Shell 세션에 대한 시간 초과 생성

호스트에서 ESXi Shell을 사용하도록 설정했지만 세션에서 로그아웃하는 것을 잊어버린 경우 유휴 세션이 무기한 연결된 상태로 유지됩니다. 연결이 열려 있으면 누군가가 ESXi 호스트에 대해 권한 있는 액세스 권한을 얻을 가능성이 높아집니다. 유휴 세션에 대한 시간 초과를 설정하여 이 문제를 방지합니다.

유휴 시간 초과는 유휴 대화형 세션에서 로그아웃될 때까지 경과할 수 있는 시간입니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭합니다.
- 2 **시스템** 탭에서 **고급 설정**을 클릭합니다.
- 3 **검색** 텍스트 상자에 `UserVars.ESXiShellInteractiveTimeOut`을 입력하고 **검색** 아이콘을 클릭합니다.
- 4 `UserVars.ESXiShellInteractiveTimeOut`을 선택하고 **옵션 편집**을 클릭합니다.
옵션 편집 대화상자가 열립니다.

5 **새 값** 텍스트 상자에 시간 초과 설정을 입력합니다.

값이 0이면 시간 초과가 비활성화됩니다.

6 **저장**을 클릭합니다.

시간 초과는 새로 로그인한 세션에만 적용됩니다.

7 (선택 사항) 키 설정을 기본값으로 재설정하려면 목록에서 해당 키를 마우스 오른쪽 버튼으로 클릭하고 **기본값으로 재설정**을 선택합니다.

결과

세션이 유효 상태일 때 시간 초과 기간이 경과하면 사용자가 로그아웃됩니다.

VMware Host Client에서 ESXi 호스트를 유지 보수 모드로 설정

예를 들어 추가 메모리를 설치하기 위해 업그레이드해야 하는 경우 ESXi 호스트를 유지 보수 모드로 전환합니다. 호스트는 사용자 요청에 의해서만 유지 보수 모드로 전환하거나 유지 보수 모드를 마칩니다.

호스트는 실행 중인 모든 가상 시스템의 전원이 꺼지거나 다른 호스트로 마이그레이션될 때까지 **유지 보수 모드로 전환 중** 상태에 있습니다. 가상 시스템의 전원을 끄거나 유지 보수 모드로 전환 중이거나 유지 보수 모드인 호스트로 가상 시스템을 마이그레이션할 수 없습니다.

호스트를 유지 보수 모드로 설정하려면 호스트에서 실행 중인 모든 가상 시스템의 전원을 끄거나 다른 호스트로 마이그레이션해야 합니다. 가상 시스템이 실행 중인 호스트를 유지 보수 모드로 설정하도록 시도하는 경우 태스크를 완료하려면 DRS의 전원을 끄거나 실행 중인 가상 시스템을 마이그레이션해야 합니다. 가상 시스템의 전원이 꺼지거나 마이그레이션되기 전에 시간 초과가 발생하는 경우 오류 메시지가 나타납니다.

호스트의 모든 가상 시스템이 비활성화 상태인 경우 호스트의 아이콘이 **유지 보수 중**으로 표시되고 호스트의 요약 패널에 새 상태가 나타납니다. 유지 보수 모드인 호스트에서는 가상 시스템을 배포하거나 가상 시스템의 전원을 켤 수 없습니다.

사전 요구 사항

호스트를 유지 보수 모드로 설정하기 전에 해당 호스트에서 실행 중인 모든 가상 시스템의 전원을 끄거나 수동 또는 DRS를 사용하여 자동으로 다른 호스트로 마이그레이션합니다.

절차

1 호스트를 마우스 오른쪽 버튼으로 클릭하고 **유지 보수 모드로 전환**을 클릭합니다.

유지 보수 모드 변경 확인 창이 나타납니다.

2 **예**를 클릭합니다.

결과

유지 보수 모드 종료를 선택하기 전까지 호스트는 유지 보수 모드에 있습니다.

VMware Host Client에서 사용 권한 관리

VMware Host Client에서 사용 권한은 가상 시스템 또는 ESXi 호스트와 같은 다양한 개체에 대해 사용자에게 할당된 액세스 역할을 나타냅니다. 역할을 통해 사용자는 할당된 개체에 대해 다양한 작업을 수행할 수 있습니다.

예를 들어 호스트의 메모리를 구성하려면 사용자에게 **호스트.구성.메모리 구성** 권한이 포함된 역할이 부여되어야 합니다. 서로 다른 개체에 대해 서로 다른 역할을 사용자에게 할당함으로써 VMware Host Client를 사용하여 해당 사용자가 수행할 수 있는 작업을 제어할 수 있습니다.

VMware Host Client를 사용하여 호스트에 직접 연결할 경우 루트 및 vpxuser 사용자 계정은 모든 개체에 대해 관리자 역할이 할당된 사용자와 동일한 액세스 권한을 갖습니다.

다른 모든 사용자는 처음에 어떤 개체에 대해서도 사용 권한이 없으므로 이러한 개체를 보거나 개체에 대한 작업을 수행할 수 없습니다. 이러한 사용자는 관리자 권한을 가진 사용자가 사용 권한을 할당해야만 작업을 수행할 수 있습니다.

많은 작업에서 하나 이상의 개체에 대한 권한이 필요합니다. 다음 규칙은 특정 작업을 수행할 수 있도록 사용자에게 어떤 역할을 할당할지 결정하는 데 도움이 될 수 있습니다.

- 가상 디스크를 생성하거나 스냅샷을 생성하는 것처럼 하드 디스크 공간을 사용하는 모든 작업에는 대상 데이터스토어에 대한 **데이터스토어.공간 할당** 권한과 작업 자체를 수행할 수 있는 권한이 필요합니다.
- 각 호스트와 개체에는 해당 호스트 또는 클러스터의 모든 리소스가 들어 있는 고유한 암시적 리소스 풀이 있습니다. 가상 시스템을 호스트나 클러스터에 직접 배포하려면 **리소스.리소스 풀에 가상 시스템 할당** 권한이 필요합니다.

권한 목록은 ESXi 및 vCenter Server 모두에 대해 동일합니다.

ESXi 호스트에 대한 직접 연결을 통해 역할을 생성하고 사용 권한을 설정할 수 있습니다.

사용 권한 유효성 검사

Active Directory를 정기적으로 사용하는 vCenter Server 및 ESXi 호스트는 Windows Active Directory 도메인에 대해 사용자 및 그룹의 유효성을 검사합니다. 호스트 시스템이 시작될 때마다 그리고 vCenter Server 설정에 지정된 간격마다 정기적으로 유효성 검사가 이루어집니다.

예를 들어, 사용자 Smith에게 사용 권한이 할당되었는데 도메인에서 이 사용자의 이름이 Smith2로 변경된 경우 호스트는 Smith가 더 이상 존재하지 않는다고 단정하고 다음에 유효성 검사가 수행될 때 해당 사용자의 사용 권한을 제거합니다.

이와 마찬가지로 사용자 Smith가 도메인에서 제거되면 다음에 유효성 검사가 수행될 때 모든 사용 권한이 제거됩니다. 다음에 유효성 검사가 수행되기 전에 새로운 사용자 Smith가 도메인에 추가되면 새로운 사용자 Smith는 이전 사용자 Smith에게 할당되었던 모든 사용 권한을 받게 됩니다.

VMware Host Client에서 ESXi 호스트에 대해 사용자에게 사용 권한 할당

ESXi 호스트에 대해 특정 작업을 수행하려면 사용자에게 특정 역할과 연결된 사용 권한이 있어야 합니다.

VMware Host Client에서 사용자에게 역할을 할당하고 호스트에 대해 다양한 작업을 수행하는 데 필요한 사용 권한을 제공할 수 있습니다.

절차

1 VMware Host Client 인벤토리에서 **호스트**를 마우스 오른쪽 버튼으로 클릭하고 **사용 권한**을 클릭합니다.
사용 권한 관리 창이 나타납니다.

2 **사용자 추가**를 클릭합니다.

3 **사용자 선택** 텍스트 상자에서 역할을 할당할 사용자를 선택합니다.

4 **역할 선택** 텍스트 상자 옆의 화살표를 클릭하고 목록에서 역할을 선택합니다.

5 (선택 사항) **모든 하위 항목으로 전파** 또는 **그룹으로 추가**를 선택합니다.

vCenter Server 수준에서 사용 권한을 설정하고 하위 개체로 전파하는 경우 이 사용 권한은 데이터 센터, 폴더, 클러스터, 호스트, 가상 시스템 및 vCenter Server 인스턴스의 기타 개체에 적용됩니다.

6 **사용자 추가**를 클릭하고 **닫기**를 클릭합니다.

VMware Host Client에서 사용자에 대한 사용 권한 제거

사용자에 대한 사용 권한을 제거해도 사용 가능한 사용자 목록에서 사용자가 제거되지 않습니다. 또한 사용할 수 있는 항목 목록에서 해당 역할도 제거되지 않습니다. 선택한 인벤토리 개체에서 사용자 및 역할 쌍이 제거됩니다.

절차

1 VMware Host Client 인벤토리에서 **호스트**를 마우스 오른쪽 버튼으로 클릭하고 **사용 권한**을 클릭합니다.
사용 권한 관리 창이 나타납니다.

2 목록에서 사용자를 선택하고 **사용자 제거**를 클릭합니다.

3 **닫기**를 클릭합니다.

VMware Host Client에서 가상 시스템에 대한 사용자 사용 권한 할당

가상 시스템에 대해 특정 작업을 수행할 수 있도록 사용 권한을 제공하려면 특정 사용자에게 역할을 할당하십시오.

절차

1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.

2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **사용 권한**을 선택합니다.

사용 권한 관리 창이 나타납니다.

3 **사용자 추가**를 클릭합니다.

4 **사용자 선택** 텍스트 상자 옆의 화살표를 클릭하고 역할을 할당할 사용자를 선택합니다.

5 **역할 선택** 텍스트 상자 옆의 화살표를 클릭하고 목록에서 역할을 선택합니다.

6 (선택 사항) **모든 하위 항목으로 전파**를 선택합니다.

vCenter Server 수준에서 사용 권한을 설정하고 하위 개체로 전파하는 경우 이 사용 권한은 데이터 센터, 폴더, 클러스터, 호스트, 가상 시스템 및 vCenter Server 인스턴스의 유사 개체에 적용됩니다.

7 사용자 추가를 클릭하고 닫기를 클릭합니다.

VMware Host Client에서 가상 시스템에 대한 사용 권한 제거

사용자가 특정 가상 시스템에서 작업을 수행할 수 없도록 하려면 가상 시스템에 대한 해당 사용자의 사용 권한을 제거하십시오.

사용자에 대한 사용 권한을 제거해도 사용 가능한 사용자 목록에서 사용자가 제거되지 않습니다. 또한 사용할 수 있는 항목 목록에서 해당 역할도 제거되지 않습니다. 선택한 인벤토리 개체에서 사용자 및 역할 쌍이 제거됩니다.

절차

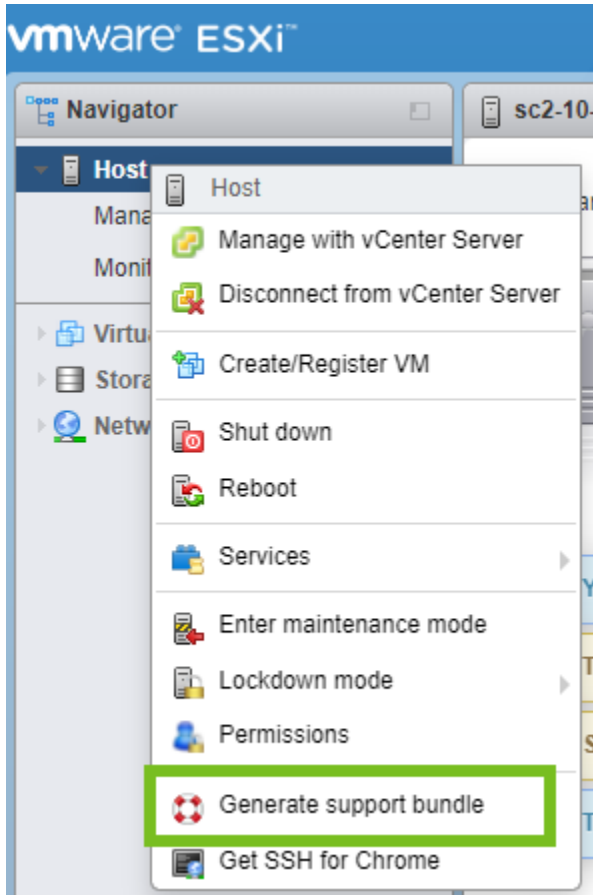
- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **사용 권한**을 선택합니다.
사용 권한 관리 창이 나타납니다.
- 3 목록에서 사용자를 선택하고 **사용자 제거**를 클릭합니다.
- 4 **닫기**를 클릭합니다.

VMware Host Client에서 지원 번들 생성

로그인한 ESXi 호스트에 대한 지원 번들을 생성할 수 있습니다. 지원 번들에는 문제를 진단하고 해결하는 데 사용할 수 있는 로그 파일 및 시스템 정보가 포함되어 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **호스트**를 마우스 오른쪽 버튼으로 클릭하고 드롭다운 메뉴에서 **지원 번들 생성**을 선택합니다.



지원 번들이 생성되면 번들 다운로드 링크가 포함된 대화상자가 팝업됩니다.

- 2 (선택 사항) VMware Host Client 인벤토리에서 **모니터**를 클릭하고 **작업**을 클릭한 다음 목록에서 로그 번들을 클릭합니다.

테이블 아래에서 로그 번들에 대한 링크를 볼 수 있습니다.

VMware Host Client의 잠금 모드

ESXi 호스트의 보안 수준을 높이려면 호스트를 잠금 모드로 설정합니다. 잠금 모드에서는 기본적으로 작업을 vCenter Server를 통해 수행해야 합니다.

정상 잠금 모드 및 엄격 잠금 모드

vSphere 6.0 이상에서는 정상 잠금 모드 또는 엄격 잠금 모드를 선택할 수 있습니다.

정상 잠금 모드

정상 잠금 모드에서는 DCUI 서비스가 활성 상태로 유지됩니다. vCenter Server 시스템에 대한 연결이 끊기고 vSphere Client를 통한 액세스를 사용할 수 없는 경우 권한이 있는 계정은 ESXi 호스트의 직접 콘솔 인터

페이지에 로그인하여 잠금 모드를 종료할 수 있습니다. 다음 계정만 DCUI(Direct Console User Interface)에 액세스할 수 있습니다.

- 호스트에 대한 관리 권한이 있는, 잠금 모드의 예외 사용자 목록 계정. 예외 사용자 목록은 특정 태스크를 수행하는 서비스 계정을 위한 것입니다. ESXi 관리자를 이 목록에 추가하면 잠금 모드의 목적이 무효화됩니다.
- 호스트에 대해 DCUI.Access 고급 옵션에서 정의된 사용자. 이 옵션은 vCenter Server에 대한 연결이 끊긴 경우 직접 콘솔 인터페이스에 긴급하게 액세스하기 위한 것입니다. 이러한 사용자는 호스트에 대한 관리 권한이 필요하지 않습니다.

엄격 잠금 모드

엄격 잠금 모드에서는 DCUI 서비스가 중지됩니다. vCenter Server에 대한 연결이 끊기고 vSphere Client를 더 이상 사용할 수 없는 경우 ESXi Shell 및 SSH 서비스가 사용하도록 설정되어 있고 예외 사용자가 정의되어 있지 않는 한 ESXi 호스트가 사용할 수 없게 됩니다. vCenter Server 시스템에 대한 연결을 복원할 수 없는 경우 호스트를 다시 설치해야 합니다.

잠금 모드와 ESXi Shell 및 SSH 서비스

엄격 잠금 모드는 DCUI 서비스를 중지합니다. 그러나 ESXi Shell 및 SSH 서비스는 잠금 모드와 상관이 없습니다. 잠금 모드가 효율적인 보안 대책이 되려면 ESXi Shell 및 SSH 서비스도 비활성화해야 합니다. 이러한 서비스는 기본적으로 비활성화되어 있습니다.

호스트가 잠금 모드에 있을 때 예외 사용자 목록의 사용자에게 호스트에 대한 관리자 역할이 있는 경우 해당 사용자는 ESXi Shell 및 SSH를 통해 호스트에 액세스할 수 있습니다. 이 액세스는 엄격 잠금 모드에서도 가능합니다. ESXi Shell 서비스 및 SSH 서비스를 비활성화한 상태로 유지하는 것이 가장 안전한 옵션입니다.

참고 예외 사용자 목록은 호스트 백업과 같은 한정된 작업을 수행하는 서비스 계정을 위한 것으로 관리자용이 아닙니다. 예외 사용자 목록에 관리자 사용자를 추가하면 잠금 모드의 존재 목적이 무효화됩니다.

VMware Host Client를 사용하여 ESXi 호스트를 정상 잠금 모드로 전환

VMware Host Client를 사용하여 정상 잠금 모드를 시작할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **호스트**를 마우스 오른쪽 버튼으로 클릭하고 드롭다운 메뉴에서 **잠금 모드**를 선택하고 **정상 잠금 시작**을 선택합니다.

주의 메시지가 나타납니다.

- 2 **정상 잠금 시작**을 클릭합니다.

VMware Host Client를 사용하여 ESXi 호스트를 엄격 잠금 모드로 전환

VMware Host Client를 사용하여 엄격 잠금 모드를 시작할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **호스트**를 마우스 오른쪽 버튼으로 클릭하고 드롭다운 메뉴에서 **잠금 모드**를 선택하고 **엄격 잠금 시작**을 선택합니다.

주의 메시지가 나타납니다.

- 2 **엄격 잠금 시작**을 클릭합니다.

VMware Host Client를 사용하여 잠금 모드 종료

ESXi 호스트에서 정상 잠금 또는 엄격 잠금 모드를 시작한 경우 VMware Host Client를 사용하여 잠금 모드를 종료할 수 있습니다.

절차

- ◆ VMware Host Client 인벤토리에서 **호스트**를 마우스 오른쪽 버튼으로 클릭하고 드롭다운 메뉴에서 **잠금 모드**를 선택하고 **잠금 종료**를 선택합니다.

VMware Host Client에서 잠금 모드 예외 사용자 지정

vSphere 6.0 이상에서는 VMware Host Client를 사용하여 예외 사용자 목록에 사용자를 추가할 수 있습니다. 이러한 사용자는 호스트가 잠금 모드에 들어갈 때 권한을 잃지 않습니다. 예외 사용자 목록에 백업 에이전트와 같은 서비스 계정을 추가할 수 있습니다.

예외 사용자는 ESXi 호스트에 대해 로컬로 정의된 권한을 가진 Active Directory 사용자 또는 호스트 로컬 사용자로서 Active Directory 그룹의 멤버가 아니며 vCenter Server 사용자가 아닙니다. 이러한 사용자는 해당 권한을 기반으로 호스트에서 작업을 수행할 수 있습니다. 이것은 예를 들어 읽기 전용 사용자가 호스트에서 잠금 모드를 비활성화할 수 없음을 의미합니다.

참고 예외 사용자 목록은 호스트 백업과 같은 한정된 태스크를 수행하는 서비스 계정에 유용하며 관리자가 아닙니다. 예외 사용자 목록에 관리자 사용자를 추가하면 잠금 모드의 존재 목적이 무효화됩니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **보안 및 사용자**를 클릭합니다.
- 2 **잠금 모드**를 클릭합니다.
- 3 **사용자 예외 추가**를 클릭하고 사용자의 이름을 입력하고 **예외 추가**를 클릭합니다.
- 4 (선택 사항) 예외 사용자 목록에서 이름을 선택하고 **사용자 예외 제거**를 클릭하고 **확인**을 클릭합니다.

VMware Host Client를 사용하여 CPU 리소스 관리

VMware Host Client로 ESXi 호스트에 연결하는 경우 제한된 수의 리소스 관리 설정에 액세스할 수 있습니다.

VMware Host Client를 사용하여 프로세서 정보 보기

VMware Host Client에서 로그인한 ESXi 호스트의 현재 CPU 구성에 대한 정보에 액세스할 수 있습니다.

절차

1 VMware Host Client 인벤토리에서 **호스트**를 클릭합니다.

2 **하드웨어**를 확장하고 **CPU**를 확장합니다.

물리적 프로세서의 개수와 유형 및 논리 프로세서의 개수에 대한 정보를 볼 수 있습니다.

VMware Host Client에서 특정 프로세서에 가상 시스템 할당

CPU 선호도를 사용하여 특정 프로세서에 가상 시스템을 할당할 수 있습니다. 이러한 방식으로 다중 프로세서 시스템에서 사용할 수 있는 특정 프로세서에만 가상 시스템을 할당할 수 있습니다.

사전 요구 사항

가상 시스템의 전원을 끕니다.

절차

1 VMware Host Client 인벤토리에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.

2 **가상 하드웨어** 아래에서 **CPU**를 확장합니다.

3 **스케줄링 선호도** 아래에서 가상 시스템의 물리적 프로세서 선호도를 선택합니다.

하이픈을 사용하여 범위를 나타내고 심표를 사용하여 값을 구분합니다.

예를 들어 0, 2, 4-7은 프로세서 0, 2, 4, 5, 6 및 7을 나타냅니다.

4 **저장**을 클릭하여 변경 내용을 적용합니다.

VMware Host Client에서 ESXi 호스트 모니터링

VMware Host Client를 사용하여 호스트에 연결하면 호스트 상태를 모니터링하고 성능 차트, 이벤트, 태스크, 시스템 로그 및 알림을 볼 수 있습니다.

VMware Host Client에서 차트 보기

VMware Host Client에 로그인하면 관리하는 ESXi 호스트의 리소스 사용량에 관한 정보를 선형 차트 형식으로 볼 수 있습니다.

메모리 소비를 줄이려면 지난 한 시간에 대한 통계만 VMware Host Client에 포함되어야 합니다.

절차

1 VMware Host Client에서 **모니터링**을 클릭하고 **성능**을 클릭합니다.

2 (선택 사항) 지난 한 시간에 대한 호스트 사용량을 보려면 드롭다운 메뉴에서 옵션을 선택합니다.

- 지난 한 시간 동안 호스트에서 사용한 CPU 백분율을 보려면 **CPU**를 선택합니다.

- 지난 한 시간 동안 호스트에서 소비한 메모리 백분율을 보려면 **메모리**를 선택합니다.
- ◆ 지난 한 시간 동안 호스트에서 소비한 네트워크 백분율을 보려면 **네트워크**를 선택합니다.
- ◆ 지난 한 시간 동안 호스트에서 소비한 디스크 사용량을 보려면 **디스크**를 선택합니다.

VMware Host Client에서 하드웨어 상태 모니터링

VMware Host Client에 로그인하면 ESXi 호스트 하드웨어의 상태를 모니터링할 수 있습니다.

참고 기본 하드웨어가 지원할 때만 하드웨어 상태를 사용할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **모니터링**을 클릭하고 **하드웨어**를 클릭합니다.
- 2 표시할 정보의 유형을 선택합니다.
- 3 (선택 사항) 목록 위의 필터 컨트롤을 사용하여 목록을 필터링합니다.
- 4 (선택 사항) 열 머리글을 클릭하여 목록을 정렬합니다.

VMware Host Client에서 이벤트 보기

이벤트는 ESXi 호스트에서 발생하는 사용자 작업이나 시스템 작업을 기록한 것입니다. VMware Host Client에 로그인하면 관리하는 호스트와 연결된 모든 이벤트를 볼 수 있습니다.

사전 요구 사항

필요한 권한: **읽기 전용**.

절차

- ◆ VMware Host Client 인벤토리에서 **모니터링**을 클릭하고 **이벤트**를 클릭합니다.
 - a (선택 사항) 이벤트 세부 정보를 볼 이벤트를 선택합니다.
 - b (선택 사항) 목록 위의 필터 컨트롤을 사용하여 목록을 필터링합니다.



- c (선택 사항) 열 머리글을 클릭하여 목록을 정렬합니다.

VMware Host Client에서 태스크 보기

VMware Host Client에 로그인하면 ESXi 호스트와 관련된 태스크를 볼 수 있습니다. 태스크 이니시에이터, 태스크 상태, 태스크 결과, 태스크 설명 등에 대한 정보를 볼 수 있습니다.

절차

- ◆ VMware Host Client 인벤토리에서 **모니터링**을 클릭하고 **태스크**를 클릭합니다.
 - a (선택 사항) 태스크 세부 정보를 볼 태스크를 선택합니다.
 - b (선택 사항) 목록 위의 필터 컨트롤을 사용하여 목록을 필터링합니다.
 - c (선택 사항) 열 머리글을 클릭하여 목록을 정렬합니다.

VMware Host Client에서 시스템 로그 보기

VMware Host Client로 ESXi 호스트에 로그인하면 로그 항목을 보고 이벤트를 생성한 사용자, 이벤트가 생성된 시간 및 이벤트 유형 등의 정보를 얻을 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **모니터링**을 클릭하고 **로그**를 클릭합니다.
로그 목록이 표시됩니다.
- 2 (선택 사항) 로그 세부 정보를 볼 로그를 클릭합니다.
- 3 (선택 사항) 로그를 마우스 오른쪽 버튼으로 클릭하고 다음 옵션 중 하나를 선택합니다.
 - 새 창에서 열기
 - 지원 번들 생성

VMware Host Client에서 알림 보기

VMware Host Client에 로그인하면 수행해야 하는 관련 태스크에 대한 호스트 알림 및 권장 사항을 볼 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **모니터링**을 클릭하고 **알림**을 클릭합니다.
- 2 목록에서 권장 작업을 볼 알림을 선택합니다.
알림 목록 아래에 권장 작업 및 설명이 포함된 메시지가 표시됩니다.

VMware Host Client로 가상 시스템 관리

3

물리적 컴퓨터와 동일한 작업을 수행하도록 가상 시스템을 구성할 수 있습니다. 물리적 컴퓨터와 달리 가상 시스템은 특수 기능을 지원합니다.

VMware Host Client를 사용하여 가상 시스템을 생성하고 등록하고 관리할 수 있으며 일별 관리 및 문제 해결 태스크를 수행할 수 있습니다.

다음으로 아래 항목을 읽으십시오.

- VMware Host Client에서 가상 시스템 생성
- VMware Host Client에서 기존 가상 시스템 등록
- VMware Host Client에서 콘솔 사용
- VMware Host Client에서 게스트 운영 체제 관리
- VMware Tools 소개
- VMware Host Client에서 가상 시스템 구성
- VMware Host Client에서 가상 시스템 관리
- 스냅샷으로 가상 시스템 관리
- VMware Host Client에서 가상 시스템 모니터링

VMware Host Client에서 가상 시스템 생성

가상 시스템은 가상 인프라의 핵심 구성 요소입니다. 가상 시스템을 생성할 때 가상 시스템을 호스트 인벤토리에 추가하고, 특정 데이터스토어와 연결하고, 운영 체제 및 가상 하드웨어 옵션을 선택할 수 있습니다.

전원을 켜면 가상 시스템은 워크로드가 증가함에 따라 리소스를 동적으로 사용하거나, 워크로드가 감소함에 따라 리소스를 동적으로 반환합니다.

모든 가상 시스템에는 물리적 하드웨어와 동일한 기능을 제공하는 가상 디바이스가 있습니다. 가상 시스템은 해당 가상 시스템이 실행되는 호스트로부터 CPU와 메모리, 스토리지에 대한 액세스 권한 및 네트워크 연결을 얻습니다.

사전 요구 사항

가상 시스템.인벤토리.생성 권한이 있는지 확인합니다.

생성하려는 가상 시스템의 속성에 따라 다음 추가 권한이 필요할 수 있습니다.

- **가상 시스템.구성.기존 디스크 추가** - 기존 가상 디스크 파일(RDM 아님)을 참조하는 가상 디스크 디바이스를 포함하는 경우.
- **가상 시스템.구성.새 디스크 추가** - 새 가상 디스크 파일(RDM 아님)을 생성하는 가상 디스크 디바이스를 포함하는 경우.
- **가상 시스템.구성.원시 디바이스** - RDM(원시 디바이스 매핑) 또는 SCSI 패스스루 디바이스를 포함하는 경우.
- **가상 시스템.구성.호스트 USB 디바이스** - 호스트 USB 디바이스를 사용하여 백업되는 가상 USB 디바이스를 포함하는 경우.
- **가상 시스템.구성.고급 구성** - `ConfigSpec.extraConfig` 값을 설정하는 경우.
- **가상 시스템.구성.스왑 배치** - 스왑 배치를 설정하는 경우.
- **데이터스토어.공간 할당** - 가상 시스템 및 가상 시스템의 가상 디스크가 생성되는 모든 데이터스토어에 필요.
- **네트워크.할당** - 생성되는 새 가상 시스템에 할당된 네트워크에 필요.

절차

- 1 VMware Host Client 인벤토리에서 **호스트**를 마우스 오른쪽 버튼으로 클릭하고 **VM 생성/등록**을 선택합니다.
- 새 가상 시스템 마법사가 열립니다.
- 2 새 가상 시스템 생성을 선택하고 다음을 클릭합니다.
- 3 **이름 및 게스트 운영 체제 선택** 페이지에서 가상 시스템의 고유한 이름을 입력하고 게스트 운영 체제를 구성합니다.
 - a **이름** 텍스트 상자에 가상 시스템의 이름을 입력합니다.
 - b **호환성** 드롭다운 메뉴에서 가상 시스템 호환성을 선택합니다.
 - c **게스트 운영 체제 제품군** 드롭다운 메뉴에서 게스트 운영 체제를 선택합니다.
 - d **게스트 운영 체제 버전** 드롭다운 메뉴에서 게스트 운영 체제 버전을 선택합니다.
 - e 가상 시스템에서 VBS를 사용하도록 설정하려면 **Windows 가상화 기반 보안 사용** 확인란을 선택하고 다음을 클릭합니다.

참고 Windows 가상화 기반 보안 사용 옵션은 Windows OS 버전이 최신(예: Windows 10 및 Windows Server 2016)이고 가상 시스템 호환성이 ESXi 6.7 이상인 경우에만 나타납니다.

이 옵션을 사용하도록 설정하면 게스트 운영 체제에서 하드웨어 가상화, IOMMU, EFI 및 보안 부팅을 사용할 수 있게 됩니다. 또한 이 가상 시스템의 게스트 운영 체제 내에서 **가상화 기반 보안**을 사용하도록 설정해야 합니다.

- 4 다음을 클릭합니다.

- 5 **스토리지 선택** 페이지에서 가상 시스템의 스토리지 유형과 가상 시스템 파일을 저장할 데이터스토어를 선택합니다.
- a 모든 가상 시스템 디스크 및 구성 파일을 표준 데이터스토어에 저장하려면 **표준** 버튼을 클릭합니다.
 - b 호스트-로컬 PMem 데이터스토어에 가상 시스템 하드 디스크를 저장하려면 **영구 메모리** 버튼을 클릭합니다.
 - c 목록에서 데이터스토어를 선택하고 **다음**을 클릭합니다.

참고 PMem 데이터스토어에는 구성 파일을 저장할 수 없습니다. PMem을 사용하기로 선택한 경우 가상 시스템 구성 파일에 일반 데이터스토어를 선택해야 합니다.

6 설정 사용자 지정 페이지에서 가상 시스템 하드웨어 및 옵션을 구성하고 다음을 클릭합니다.

다른 유형의 디바이스 추가 지침을 비롯하여 가상 시스템 옵션 및 가상 디스크 구성에 대한 자세한 내용은 "vSphere 가상 시스템 관리" 항목을 참조하십시오.

a 설정 사용자 지정 페이지에서 가상 하드웨어를 클릭하고 새 가상 하드웨어 디바이스를 추가합니다.

- 새 가상 하드 디스크를 추가하려면 **하드 디스크 추가** 아이콘을 클릭합니다.

참고 표준 또는 영구 메모리 하드 디스크를 가상 시스템에 추가할 수 있습니다. 영구 메모리 하드 디스크는 호스트-로컬 PMem 데이터스토어에 저장됩니다.

- 가상 시스템에 NIC를 추가하려면 **네트워크 어댑터 추가** 아이콘을 클릭합니다.
- 가상 시스템에 추가할 다른 유형의 디바이스를 선택하려면 **기타 디바이스 추가** 아이콘을 클릭합니다.

참고 가상 시스템이 PMem 스토리지를 사용하는 경우 PMem 데이터스토어에 저장되는 하드 디스크와 가상 시스템에 추가하는 NVDIMM 디바이스가 모두 동일한 PMem 리소스를 공유합니다. 따라서 호스트에서 사용 가능한 PMem 양에 따라 새로 추가되는 디바이스의 크기를 조정해야 합니다. 구성 과정에서 주의가 필요한 경우 마법사에 경고 메시지가 나타납니다.

b (선택 사항) 디바이스 설정을 보고 구성하려면 디바이스를 확장합니다.

옵션	설명
CPU	CPU나 프로세서는 컴퓨터 프로그램 명령을 수행하는 컴퓨터 시스템의 일부분이며 컴퓨터 기능을 수행하는 제1의 구성 요소입니다. CPU에는 코어가 포함되어 있습니다. 가상 시스템에 사용할 수 있는 가상 CPU의 수는 호스트에서 라이선스가 부여된 CPU의 수와 게스트 운영 체제에서 지원되는 CPU 수에 따라 다릅니다. VMware 다중 코어 가상 CPU 기능을 사용하려면 게스트 운영 체제 EULA 요구 사항을 준수해야 합니다.
메모리	가상 시스템 메모리 리소스 또는 옵션을 추가, 변경 또는 구성하여 가상 시스템 성능을 향상시킬 수 있습니다. 가상 시스템 생성 도중 또는 게스트 운영 체제가 설치된 이후에는 메모리 매개 변수 중 대부분을 설정할 수 있습니다. 가상 시스템의 메모리 리소스 설정은 가상 시스템에 할당되는 호스트 메모리의 양을 결정합니다. 가상 하드웨어 메모리 크기는 가상 시스템에서 실행되는 애플리케이션에 사용할 수 있는 메모리 양을 결정합니다.
하드 디스크	가상 시스템이 실행 중일 때도 가상 시스템에 대용량 가상 디스크를 추가하거나 기존 디스크에 더 많은 공간을 추가할 수 있습니다. 가상 시스템이 만들어지는 동안에 또는 게스트 운영 체제를 설치한 후에 대부분의 가상 디스크 매개 변수를 설정할 수 있습니다.
SCSI 컨트롤러	스토리지 컨트롤러는 가상 시스템에 BusLogic 병렬, LSI Logic 병렬, LSI Logic SAS, VMware 반가상화 SCSI 등의 여러 가지 SCSI 컨트롤러 유형으로 나타납니다. 가상 시스템의 SCSI 버스 공유 유형을 설정하고 SCSI 버스가 공유되어 있는지 여부를 표시할 수 있습니다. 공유 유형에 따라서 가상 시스템은 동일한 서버나 임의 서버의 동일한 가상 디스크에 동시에 액세스할 수 있습니다. 가상 시스템의 SCSI 컨트롤러 구성은 ESXi 호스트에서만 변경할 수 있습니다.

옵션	설명
SATA 컨트롤러	가상 시스템에 여러 개의 하드 디스크나 CD/DVD-ROM 디바이스가 있는 경우 최대 세 개의 SATA 컨트롤러를 추가하여 디바이스를 할당할 수 있습니다. 디바이스를 여러 컨트롤러에 분산하면 성능을 향상시키고 데이터 트래픽 정체를 방지할 수 있습니다. 또한 디바이스가 한 컨트롤러에 사용할 수 있는 한도인 30개를 초과할 경우 컨트롤러를 추가할 수도 있습니다. 대용량 가상 하드 디스크를 사용하려는 경우 SATA 컨트롤러에서 가상 시스템을 부팅하여 사용할 수 있습니다.
네트워크 어댑터	가상 시스템을 구성하는 경우 NIC(네트워크 어댑터)를 추가하고 어댑터 유형을 지정할 수 있습니다. 사용할 수 있는 네트워크 어댑터의 유형은 다음 요인에 따라 달라집니다. <ul style="list-style-type: none"> ■ 가상 시스템 호환성. 생성하거나 최근에 업데이트한 호스트에 따라 다릅니다. ■ 가상 시스템 호환성을 현재 호스트의 최신 버전으로 업데이트했는지 여부 ■ 게스트 운영 체제
CD/DVD 드라이브	DVD 또는 CD 디바이스를 구성하여 클라이언트 디바이스, 호스트 디바이스 또는 데이터스토어 ISO 파일에 연결할 수 있습니다.
비디오 카드	기본 설정을 선택하거나 사용자 지정 설정을 지정할 수 있습니다. 디스플레이 수, 총 비디오 메모리를 지정하고 VMware가 3D를 지원하는 게스트 운영 체제에 대해 3D 지원을 사용하도록 설정할 수 있습니다.
PCI 디바이스	ESXi 호스트에서 PCI 디바이스를 패스스루에 사용할 수 있도록 구성할 수 있습니다. 가상 시스템 배치를 특정 하드웨어 인스턴스로 제한하도록 하드웨어 레이블을 변경할 수도 있습니다.
동적 PCI 디바이스	PCI 패스스루 디바이스는 벤더 및 모델 이름별로 자동으로 그룹화됩니다. 하드웨어 주소로 물리적 PCI 디바이스를 선택하는 대신, 벤더 및 모델 이름을 기준으로 원하는 디바이스를 구성할 수 있습니다. 동일한 하드웨어 레이블 또는 빈 하드웨어 레이블이 있는 사용 가능한 모든 디바이스를 가상 시스템에 추가할 수 있습니다. 가상 시스템의 전원을 켜면 벤더 및 모델 이름이 일치하는 특정 물리적 PCI 패스스루 디바이스가 가상 시스템에 연결됩니다.
보안 디바이스	가상 시스템에 대해 vSGX(Virtual Intel® Software Guard Extensions)를 구성하고 워크로드에 추가적인 보안을 제공할 수 있습니다. 가상 시스템을 생성하거나 기존 가상 시스템을 편집할 때 vSGX를 활성화 또는 비활성화할 수 있습니다.

c (선택 사항) 디바이스를 제거하려면 디바이스 옆에 있는 삭제(✖) 아이콘을 클릭합니다.

안전하게 제거할 수 있는 가상 하드웨어에만 이 옵션이 나타납니다.

d (선택 사항) 가상 시스템 옵션을 사용자 지정하려면 **VM 옵션** 버튼을 클릭합니다.

7 **완료 준비** 페이지에서 세부 정보를 검토하고 **마침**을 클릭합니다.

VMware Host Client에서 기존 가상 시스템 등록

호스트에서 가상 시스템을 등록 취소하지만 데이터스토어에서 해당 가상 시스템을 삭제하지는 않는 경우 VMware Host Client를 사용하여 가상 시스템을 등록 취소할 수 있습니다. 가상 시스템을 다시 등록하면 인벤토리에 가상 시스템이 나타납니다.

데이터스토어 브라우저를 사용하여 등록하려는 가상 시스템 목록에 추가할 데이터스토어, 디렉토리 또는 .vmx 파일을 선택합니다. 데이터스토어 또는 디렉토리를 선택하여 해당 위치에서 모든 .vmx 파일을 검색합니다. 여러 번 검색하여 목록에 가상 시스템을 추가할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **호스트**를 마우스 오른쪽 버튼으로 클릭하고 **VM 생성/등록**을 선택합니다.
- 새 가상 시스템** 마법사가 열립니다.
- 2 **생성 유형 선택** 페이지에서 **기존 가상 시스템 등록**을 선택하고 **다음**을 클릭합니다.
- 3 **등록할 VM 선택** 페이지에서 **하나 이상의 가상 시스템, 데이터스토어 또는 디렉토리를 선택합니다.**를 클릭하고 등록할 가상 시스템을 찾은 다음 **선택**을 클릭합니다.
- 4 목록에서 가상 시스템을 제거하려면 파일 이름을 선택하고 **선택 항목 제거**를 클릭합니다.
- 5 선택 항목을 해제하고 다시 시작하려면 **모두 제거**를 클릭합니다.
- 6 **다음**을 클릭합니다.
- 7 **완료 준비** 페이지에서 세부 정보를 검토하고 **마침**을 클릭합니다.

VMware Host Client에서 콘솔 사용

VMware Host Client에서 브라우저 콘솔 또는 VMRC(VMware Remote Console)를 통해 가상 시스템에 액세스하고 가상 시스템에 대해 여러 태스크를 수행할 수 있습니다.

브라우저 콘솔 사용

참고 브라우저 콘솔은 6.0 이전 버전의 ESXi에 대해 지원됩니다. 브라우저 콘솔에 액세스하려면 VMRC를 사용해야 합니다.

브라우저 콘솔을 사용하여 추가 소프트웨어를 설치하지 않고 게스트 운영 체제에 액세스할 수 있습니다. 로컬 하드웨어 연결과 같은 추가 콘솔 기능을 사용하려면 VMware Remote Console을 설치하십시오.

참고 브라우저 콘솔은 현재 영어, 일본어 및 독일어 키보드 레이아웃만 지원합니다. 콘솔을 열기 전에 원하는 키보드 레이아웃을 선택해야 합니다.

VMware Remote Console 사용

VMware Remote Console은 원격 호스트의 가상 시스템에 대한 액세스를 제공하고 운영 체제 설정 구성 및 "VMware vSphere"에 대한 가상 시스템 콘솔 모니터링과 같은 콘솔 및 디바이스 작업을 수행합니다. 가상 시스템 게스트 운영 체제 다시 시작 및 종료, 가상 시스템 재개 및 일시 중단, VMware Tools 업데이트 구성, 가상 시스템 및 다른 디바이스 구성 및 관리 등과 같은 가상 시스템에 대한 다양한 태스크를 수행할 수 있습니다. VMRC는 RAM, CPU 코어 및 디스크와 같은 가상 시스템 설정을 수정할 수도 있습니다. VMware Workstation™, VMware Fusion™ 또는 VMware Player™는 세 개 항목 중 하나라도 시스템에 설치되어 있는 경우 VMRC를 다운로드하고 설치할 필요가 없도록 VMRC로 작동합니다.

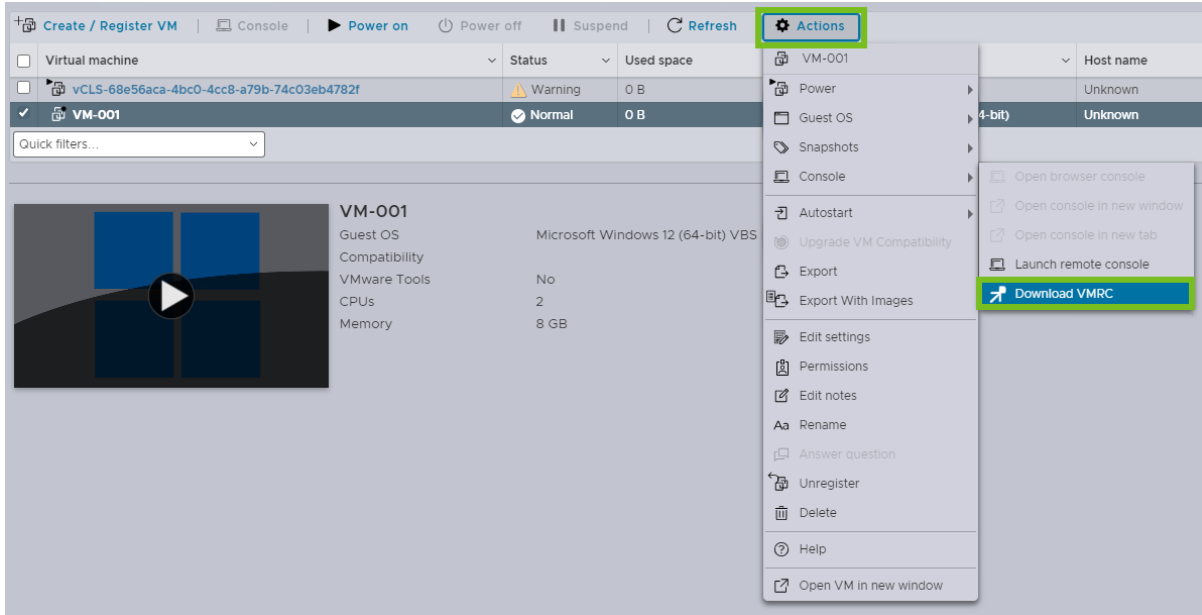
모든 콘솔 기능을 사용하려면 VMRC를 다운로드하여 설치합니다.

VMware Host Client에서 VMware Remote Console 애플리케이션 설치

VMRC(VMware Remote Console)는 원격 호스트에서 클라이언트 디바이스에 연결하고 가상 시스템 콘솔을 시작할 수 있는 독립형 콘솔 애플리케이션입니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
호스트에서 사용할 수 있는 가상 시스템 목록이 표시됩니다.
- 2 목록에서 가상 시스템을 선택하고 **작업** 메뉴에서 **콘솔 > VMRC 다운로드**를 선택합니다.



VMware Customer Connect 웹 사이트가 열립니다.

- 3 [Broadcom Support](#)에서 VMRC 설치 관리자를 다운로드합니다.

참고 VMRC 설치 관리자를 다운로드하려면 [Broadcom Support](#)에 프로파일이 있어야 합니다.

VMware Host Client에서 가상 시스템에 대한 원격 콘솔 시작

VMware Remote Console을 사용하여 VMware Host Client에서 가상 시스템에 액세스할 수 있습니다. 둘 이상의 콘솔을 시작하여 동시에 여러 원격 가상 시스템에 액세스할 수 있습니다.

사전 요구 사항

로컬 시스템에 VMware Remote Console이 설치되어 있는지 확인합니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭하고 목록에서 가상 시스템을 선택합니다.
- 2 **작업** 메뉴에서 **Console > 원격 콘솔 시작**을 선택합니다.

VMware Remote Console이 선택한 가상 시스템에 대한 독립형 애플리케이션으로 열립니다.

VMware Host Client에서 가상 시스템 콘솔 열기

VMware Host Client로 가상 시스템에 대한 콘솔을 시작하여 가상 시스템의 데스크톱에 액세스할 수 있습니다. 콘솔을 통해 가상 시스템에서 운영 체제 설정 구성, 애플리케이션 실행 및 성능 모니터링 등의 태스크를 수행할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 전원이 켜진 가상 시스템을 선택합니다.
- 3 **작업** 메뉴에서 **콘솔**을 선택하고 콘솔을 팝업 창, 새 창, 새 탭 중 어디에서 열 것인지 선택합니다.

VMware Host Client에서 게스트 운영 체제 관리

VMware Host Client로 가상 시스템의 게스트 운영 체제를 관리할 수 있습니다. VMware Tools를 설치 및 업그레이드하고, 종료하고, 재부팅하고, 구성된 게스트 운영 체제를 변경할 수 있습니다.

VMware Host Client를 사용하여 게스트 운영 체제 종료 및 다시 시작

VMware Tools를 가상 시스템에 설치하여 해당 가상 시스템에서 게스트 운영 체제를 종료하고 다시 시작할 수 있도록 합니다.

절차

- ◆ VMware Host Client 인벤토리에서 **가상 시스템**을 클릭하고 가상 시스템을 선택한 후 작업을 선택합니다.
 - 가상 시스템을 종료하려면 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **게스트 운영 체제 > 종료**를 선택합니다.
 - 가상 시스템을 다시 시작하려면 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **게스트 운영 체제 > 다시 시작**을 선택합니다.

VMware Host Client에서 게스트 운영 체제 변경

가상 시스템 설정에서 게스트 운영 체제 유형을 변경할 때에는 가상 시스템 구성 파일에서 게스트 운영 체제의 설정을 변경합니다. 게스트 운영 체제 자체를 변경하려면 가상 시스템에 반드시 새로운 운영 체제를 설치해야 합니다.

새로운 가상 시스템의 게스트 운영 체제 유형을 설정하면 vCenter Server가 게스트 운영 체제 유형에 따라 구성 기본값을 적용합니다. 게스트 운영 체제 유형 설정을 변경하면 가상 시스템 설정의 사용할 수 있는 범위 및 권장 사항에 영향을 줍니다.

사전 요구 사항

가상 시스템의 전원을 끕니다.

절차

1 VMware Host Client 인벤토리에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.

2 **VM 옵션** 탭을 클릭하고 **일반 옵션**을 확장합니다.

3 게스트 운영 체제 유형 및 버전을 선택합니다.

VBS를 지원하는 Windows 운영 체제 버전을 선택하고 가상 시스템 호환성이 ESXi 6.7 이상인 경우 VBS 행이 **VM 옵션** 탭에 나타납니다.

4 (선택 사항) VBS를 사용하도록 설정하려면 **가상화 기반 보안 사용**을 클릭합니다.

중요 VBS를 사용하도록 설정하려면 EFI를 사용하여 가상 시스템을 부팅해야 합니다. 펌웨어를 변경하면 게스트 운영 체제를 부팅하지 못하게 될 수 있습니다.

5 **저장**을 클릭하여 변경 내용을 적용합니다.

결과

게스트 운영 체제의 가상 시스템 구성 매개 변수가 변경됩니다. 이제 게스트 운영 체제를 설치할 수 있습니다.

VMware Tools 소개

VMware Tools는 게스트 운영 체제에 대한 더 나은 관리 및 원활한 사용자 상호 작용을 위해 VMware 제품의 일부 기능을 사용하도록 설정하는 서비스 및 모듈 집합입니다.

VMware Tools에는 다음과 같은 기능이 있습니다.

- 호스트 운영 체제에서 게스트 운영 체제로 메시지를 전달합니다.
- 게스트 운영 체제를 vCenter Server 및 기타 VMware 제품의 일부로 사용자 지정합니다.
- 게스트 운영 체제 작업을 자동화할 수 있도록 하는 스크립트를 실행합니다. 스크립트는 가상 시스템의 전원 상태가 변경될 때 실행됩니다.
- 게스트 운영 체제의 시간을 호스트 운영 체제의 시간과 동기화합니다.

VMware Tools 수명 주기 관리는 VMware Tools의 설치 및 업그레이드를 위한 간편하고 확장 가능한 접근 방법을 제공합니다. 여기에는 다양한 기능 향상, 드라이버 관련 기능 향상 및 새 게스트 운영 체제에 대한 지원이 포함됩니다.

최신 버전의 VMware Tools를 실행하거나 Linux OS 배포를 통해 배포된 open-vm-tools를 사용해야 합니다. 게스트 운영 체제는 VMware Tools 없이 실행할 수 있지만 최신 기능 및 업데이트에 액세스하려면 게스트 운영 체제에서 항상 최신 버전의 VMware Tools를 실행해야 합니다.

가상 시스템의 전원을 켤 때마다 자동으로 VMware Tools의 업그레이드를 적용하고 검사하도록 가상 시스템을 구성할 수 있습니다.

상 시스템에서 VMware Tools의 자동 업그레이드를 사용하도록 설정하는 방법에 대한 자세한 내용은 "vSphere 가상 시스템 관리 가이드" 를 참조하십시오.

VMware Tools 설치

VMware Tools 없이도 게스트 운영 체제를 사용할 수 있지만 VMware Tools를 설치해야만 사용할 수 있는 VMware 기능이 많이 있습니다. VMware Tools는 가상 시스템의 게스트 운영 체제 성능을 향상시킵니다.

VMware Tools 설치하는 새로운 가상 시스템 생성 프로세스의 일부입니다. 업데이트를 사용하려면 VMware Tools를 업그레이드하는 것이 중요합니다. 가상 시스템 생성에 대한 자세한 내용은 "VMware Tools 사용자 가이드" 를 참조하십시오.

VMware Tools용 설치 관리자는 ISO 이미지 파일입니다. 게스트 운영 체제에는 ISO 이미지 파일이 CD-ROM처럼 표시됩니다. Windows, Linux, Solaris, FreeBSD 및 NetWare를 비롯한 각 게스트 운영 체제 유형에는 ISO 이미지 파일이 있습니다. VMware Tools를 설치하거나 업그레이드할 경우 가상 시스템의 첫 번째 가상 CD-ROM 디스크 드라이브가 게스트 운영 체제의 VMware Tools ISO 파일에 일시적으로 연결됩니다.

Windows 가상 시스템, Linux 가상 시스템, Mac OS X 가상 시스템, Solaris 가상 시스템, NetWare 가상 시스템 또는 FreeBSD 가상 시스템에서 VMware Tools 설치 또는 업그레이드에 대한 자세한 내용은 "VMware Tools 사용자 가이드" 를 참조하십시오.

VMware Host Client에서 VMware Tools 설치

VMware Tools는 가상 시스템의 운영 체제에 설치하는 유틸리티 모음입니다. VMware Tools는 가상 시스템의 성능 및 관리를 향상시킵니다.

하나 이상의 가상 시스템에서 VMware Host Client를 사용하여 VMware Tools를 설치할 수 있습니다.

절차

1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.

2 목록에서 가상 시스템을 선택합니다.

VMware Tools를 설치하려면 가상 시스템 전원을 켜야 합니다.

3 **작업**을 클릭하고 드롭다운 메뉴에서 **게스트 OS**를 선택하고 **VMware Tools 설치**를 선택합니다.

VMware Tools 업그레이드

VMware Tools를 수동으로 업그레이드하거나 새로운 버전의 VMware Tools를 확인한 후 설치하도록 가상 시스템을 구성할 수 있습니다.

가상 시스템 전원을 켜면 게스트 운영 체제가 VMware Tools 버전을 확인합니다. 새 버전이 확인되면 가상 시스템의 상태 표시줄에 메시지가 표시됩니다.

vSphere 가상 시스템의 경우 설치된 VMware Tools 버전이 이전 버전인 경우 상태 표시줄에 다음 메시지가 표시됩니다.

최신 버전의 Tools를 이 VM에 사용할 수 있으며

Windows 가상 시스템에서 사용 가능한 업그레이드가 있을 때 알림을 표시하도록 VMware Tools를 설정할 수 있습니다. 이 알림 옵션을 설정하면 VMware Tools 업그레이드가 있을 때 Windows 작업 표시줄의 VMware Tools 아이콘에 노란색 주의 아이콘이 표시됩니다.

VMware Tools 업그레이드는 VMware Tools를 처음 설치할 때와 동일한 방법으로 설치할 수 있습니다. VMware Tools 업그레이드는 새 버전을 설치하는 것을 의미합니다.

Windows 및 Linux 게스트 운영 체제에서는 VMware Tools 업그레이드를 자동으로 수행하도록 가상 시스템을 구성할 수 있습니다. 버전 확인 작업은 가상 시스템의 전원을 켜 때 수행되지만 Windows 게스트 운영 체제에서는 자동 업그레이드는 가상 시스템의 전원을 끄거나 가상 시스템을 다시 시작할 때 수행됩니다. 업그레이드가 진행 중이면 상태 표시줄에 VMware Tools 설치 중...이라는 메시지가 표시됩니다. 해당 절차는 아래에 설명되어 있습니다.

참고 Windows 게스트 운영 체제에서 VMware Tools를 업그레이드하면 SVGA 그래픽 드라이버가 자동으로 설치됩니다. SVGA 그래픽 드라이버는 게스트 OS 전원 설정에서 절전 모드를 사용할 수 있게 하여 절전 옵션을 조정할 수 있습니다. 예를 들어 절전 모드 설정 **컴퓨터가 절전 상태일 때 변경**을 사용하여 일정 시간 후 게스트 OS가 자동으로 절전 모드로 전환되도록 구성하거나 일정 시간 동안 유휴 상태를 유지한 후 절전 모드로 전환되는 것을 방지합니다.

vSphere 가상 시스템의 경우 다음 프로세스 중 하나를 사용하여 여러 가상 시스템을 동시에 업그레이드할 수 있습니다.

다음 프로세스 중 하나를 사용하여 여러 가상 시스템을 동시에 업그레이드할 수 있습니다.

- vCenter Server에 로그인하여 호스트나 클러스터를 선택한 후 **가상 시스템** 탭에서 VMware Tools 업그레이드를 수행할 가상 시스템을 지정합니다.
- vSphere Lifecycle Manager를 사용하여 폴더 또는 데이터 센터 수준에서 가상 시스템의 오케스트레이션된 업그레이드를 수행합니다.

특정 릴리스의 VMware 제품에 있는 일부 기능은 해당 릴리스에 포함된 VMware Tools 버전으로 업그레이드하는지 아니면 해당 버전을 설치하는지에 따라 달라질 수 있습니다. 항상 최신 버전의 VMware Tools로 업그레이드할 필요는 없지만 VMware에서는 VMware Tools의 가장 최신 버전으로 업그레이드할 것을 권장합니다. 하지만 VMware Tools 버전이 더 최신일수록 여러 ESXi 호스트 버전과 호환됩니다. 불필요한 업그레이드를 방지하려면 추가된 특성과 기능이 현재 환경에 필요한지 여부를 평가하십시오. **가상 시스템 호환성 설정에 사용 가능한 하드웨어 기능**을 참조하십시오. 그러나 VMware에서는 최신 버전의 VMware Tools를 설치하고 사용하는 것을 권장합니다.

특정 릴리스의 VMware 제품에 있는 일부 기능은 해당 릴리스에 포함된 VMware Tools 버전으로 업그레이드하는지 아니면 해당 버전을 설치하는지에 따라 달라질 수 있습니다. 항상 최신 버전의 VMware Tools로 업그레이드해야 하는 것은 아닙니다. 하지만 VMware Tools 버전이 더 최신일수록 여러 호스트 버전과 호환됩니다. 불필요한 업그레이드를 방지하려면 추가된 특성과 기능이 현재 환경에 필요한지 여부를 평가하십시오.

표 3-1. 가상 시스템 호환성 옵션

호환성	설명
ESXi 8.0 업데이트 3	이 가상 시스템(하드웨어 버전 21)은 ESXi 8.0 업데이트 3 이상과 호환됩니다.
ESXi 8.0 업데이트 2	이 가상 시스템(하드웨어 버전 21)은 ESXi 8.0 업데이트 2 이상과 호환됩니다.
ESXi 8.0 업데이트 1	이 가상 시스템(하드웨어 버전 20)은 ESXi 8.0 업데이트 1, ESXi 8.0 업데이트 2 및 ESXi 8.0 업데이트 3과 호환됩니다.

표 3-1. 가상 시스템 호환성 옵션 (계속)

호환성	설명
ESXi 8.0	이 가상 시스템(하드웨어 버전 20)은 ESXi 8.0, ESXi 8.0 업데이트 1, ESXi 8.0 업데이트 2 및 ESXi 8.0 업데이트 3과 호환됩니다.
ESXi 7.0 업데이트 3	이 가상 시스템(하드웨어 버전 19)은 ESXi 7.0 업데이트 3, ESXi 8.0, ESXi 8.0 업데이트 1, ESXi 8.0 업데이트 2 및 ESXi 8.0 업데이트 3과 호환됩니다.
ESXi 7.0 업데이트 2	이 가상 시스템(하드웨어 버전 19)은 ESXi 7.0 업데이트 2, ESXi 7.0 업데이트 3, ESXi 8.0, ESXi 8.0 업데이트 1, ESXi 8.0 업데이트 2 및 ESXi 8.0 업데이트 3과 호환됩니다.
ESXi 7.0 업데이트 1 이상	이 가상 시스템(하드웨어 버전 18)은 ESXi 7.0 업데이트 1, ESXi 7.0 업데이트 2, ESXi 7.0 업데이트 3, ESXi 8.0, ESXi 8.0 업데이트 1, ESXi 8.0 업데이트 2 및 ESXi 8.0 업데이트 3과 호환됩니다.
ESXi 7.0	이 가상 시스템(하드웨어 버전 17)은 ESXi 7.0, ESXi 7.0 업데이트 1, ESXi 7.0 업데이트 2, ESXi 7.0 업데이트 3, ESXi 8.0, ESXi 8.0 업데이트 1, ESXi 8.0 업데이트 2 및 ESXi 8.0 업데이트 3과 호환됩니다.
ESXi 6.7 업데이트 2	이 가상 시스템(하드웨어 버전 15)은 ESXi 6.7 업데이트 2, ESXi 6.7 업데이트 3, ESXi 7.0, ESXi 7.0 업데이트 1, ESXi 7.0 업데이트 2, ESXi 7.0 업데이트 3, ESXi 8.0, ESXi 8.0 업데이트 1, ESXi 8.0 업데이트 2 및 ESXi 8.0 업데이트 3과 호환됩니다.
ESXi 6.7	이 가상 시스템(하드웨어 버전 14)은 ESXi 6.7, ESXi 6.7 업데이트 2, ESXi 6.7 업데이트 3, ESXi 7.0, ESXi 7.0 업데이트 1, ESXi 7.0 업데이트 2, ESXi 7.0 업데이트 3, ESXi 8.0, ESXi 8.0 업데이트 1, ESXi 8.0 업데이트 2, 및 ESXi 8.0 업데이트 3과 호환됩니다.
ESXi 6.5	이 가상 시스템(하드웨어 버전 13)은 ESXi 6.5, ESXi 6.7, ESXi 6.7 업데이트 2, ESXi 6.7 업데이트 3, ESXi 7.0, ESXi 7.0 업데이트 1, ESXi 7.0 업데이트 2, ESXi 7.0 업데이트 3, ESXi 8.0, ESXi 8.0 업데이트 1, ESXi 8.0 업데이트 2 및 ESXi 8.0 업데이트 3과 호환됩니다.

자세한 내용은 <http://www.vmware.com/resources/compatibility>에 있는 VMware 호환성 가이드를 참조하십시오.

VMware Host Client에서 VMware Tools 업그레이드

VMware Host Client를 사용하여 가상 시스템에서 VMware Tools를 업그레이드할 수 있습니다.

사전 요구 사항

가상 시스템 전원 켜기.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 선택합니다.
- 3 **작업**을 클릭하고 드롭다운 메뉴에서 **게스트 OS**를 선택하고 **VMware Tools 업그레이드**를 선택합니다.

VMware Host Client에서 가상 시스템 구성

대부분의 가상 시스템 속성은 가상 시스템을 생성하는 동안 또는 가상 시스템을 생성하고 게스트 운영 체제를 설치한 이후에 추가하거나 구성할 수 있습니다.

다음과 같은 세 가지 유형의 가상 시스템 속성을 구성할 수 있습니다.

하드웨어

기존 하드웨어 구성을 보고 하드웨어를 추가하거나 제거합니다.

옵션

게스트 운영 체제와 가상 시스템 간의 전원 관리 상호 작용 및 VMware Tools 설정과 같은 몇 가지 가상 시스템 속성을 보고 구성합니다.

리소스

CPU, CPU 하이퍼스레딩 소스, 메모리 및 디스크를 구성합니다.

VMware Host Client에서 가상 시스템 호환성 확인

가상 시스템 요약 페이지를 확인하여 가상 시스템 호환성을 확인할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 클릭합니다.

가상 시스템 이름 아래에 가상 시스템 호환성이 나타납니다.

VMware Host Client에서 가상 시스템의 이름 변경

생성 프로세스를 마친 후 가상 시스템의 이름을 변경할 수 있습니다. 이름을 변경해도 가상 시스템 파일의 이름이 나 이 파일이 들어 있는 디렉토리의 이름은 변경되지 않습니다.

사전 요구 사항

가상 시스템의 전원을 끕니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **VM 옵션**을 클릭합니다.
- 4 **VM 이름** 텍스트 상자에서 가상 시스템의 새 이름을 입력합니다.
- 5 **저장**을 클릭합니다.

VMware Host Client에서 가상 시스템 구성 파일 위치 보기

VMware Host Client를 사용하여 가상 시스템의 구성 파일 및 작업 파일의 위치를 볼 수 있습니다.

백업 시스템을 구성할 때 이 정보가 유용합니다.

사전 요구 사항

가상 시스템의 전원을 끕니다.

절차


- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 가상 시스템을 마우스 오른쪽 버튼으로 클릭한 후 **설정 편집**을 클릭합니다.
- 3 **VM 옵션** 탭을 클릭하고 **일반 옵션**을 확장합니다.
- 4 구성 파일 및 작업 파일의 위치를 기록합니다.
- 5 **취소**를 클릭하여 화면을 종료합니다.

VMware Host Client에서 가상 시스템 전원 상태 구성

호스트를 유지 보수할 경우 가상 시스템 전원 상태를 변경하는 것이 유용합니다. 가상 시스템 전원 컨트롤에 시스템 기본 설정을 사용하거나, 컨트롤이 게스트 운영 체제와 상호 작용하도록 구성할 수 있습니다.

예를 들어 **전원 끄기** 컨트롤이 가상 시스템의 전원을 끄거나 게스트 운영 체제를 종료하도록 구성할 수 있습니다.

가상 시스템이 실행 중인 동안 여러 가지 가상 시스템 구성을 수정할 수 있지만 일부 구성의 경우에는 가상 시스템 전원 상태를 변경해야 할 수 있습니다.


전원 켜기() 작업을 구성할 수 없습니다. 이 작업은 중지된 가상 시스템의 전원을 켜거나 가상 시스템이 일시 중단되어 있고 VMware Tools가 설치되어 있으며 사용할 수 있는 경우 가상 시스템을 시작하고 스크립트를 실행합니다. VMware Tools가 설치되어 있지 않은 경우에는 일시 중단된 가상 시스템을 시작하고 스크립트는 실행하지 않습니다.

사전 요구 사항

- 가상 시스템에 대해 원하는 전원 작업을 수행할 수 있는 권한을 가지고 있는지 확인합니다.
- 전원 기능 선택 사항을 설정하려면 가상 시스템에 VMware Tools를 설치합니다.
- VMware Tools 옵션을 변경하기 전에 먼저 가상 시스템의 전원을 끕니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 드롭다운 목록에서 **설정 편집**을 선택합니다.
- 3 **VM 옵션** 탭에서 **VMware Tools**를 확장합니다.

- 4 드롭다운 메뉴에서 가상 시스템 **전원 끄기**() 제어에 대한 옵션을 선택합니다.

옵션	설명
전원 끄기	가상 시스템을 즉시 중지합니다. 전원 끄기 작업은 게스트 운영 체제를 종료하거나 가상 시스템의 전원을 끕니다. 메시지는 게스트 운영 체제가 올바르게 종료되지 않을 수 있다는 것을 나타냅니다. 이 전원 끄기 옵션은 꼭 필요한 경우에만 사용하십시오.
게스트 종료	VMware Tools를 사용하여 가상 시스템의 순차적인 종료를 시작합니다. 소프트웨어 전원 작업은 도구가 게스트 운영 체제에 설치되어 있는 경우에만 사용할 수 있습니다.
시스템 기본값	시스템 설정을 따릅니다. 시스템 설정의 현재 값은 괄호 안에 표시됩니다.

- 5 드롭다운 메뉴에서 **일시 중단**() 제어에 대한 옵션을 선택합니다.

옵션	설명
일시 중단	모든 가상 시스템 작업을 일시 중지합니다. VMware Tools가 설치되어 있고 사용 가능한 경우 일시 중단 작업은 스크립트를 실행하고 가상 시스템을 일시 중단합니다. VMware Tools가 설치되어 있지 않은 경우 일시 중단 작업은 스크립트를 실행하지 않고 가상 시스템을 일시 중단합니다.
대기 모드로 게스트 전환	게스트 운영 체제를 대기 모드로 전환합니다. 이 옵션을 선택하면 모든 프로세스가 중지되지만 모든 가상 디바이스가 가상 시스템에 연결된 상태로 유지됩니다.
시스템 기본값	시스템 설정을 따릅니다. 시스템 설정의 현재 값은 괄호 안에 표시됩니다.

- 6 드롭다운 메뉴에서 **재설정**() 제어에 대한 옵션을 선택합니다.

옵션	설명
재설정	가상 시스템의 전원을 끄지 않고 게스트 운영 체제를 종료한 후 다시 시작합니다. VMware Tools가 설치되어 있지 않은 경우 재설정 작업은 가상 시스템을 재설정합니다.
게스트 다시 시작	VMware Tools를 사용하여 다시 시작을 순차적으로 시작합니다. 소프트웨어 전원 작업은 도구가 게스트 운영 체제에 설치되어 있는 경우에만 사용할 수 있습니다.
기본값	시스템 설정을 따릅니다. 시스템 설정의 현재 값은 괄호 안에 표시됩니다.

- 7 **저장**을 클릭합니다.

VMware Host Client에서 구성 파일 매개 변수 편집

시스템의 특정 문제를 수정하기 위해 VMware 설명서 또는 VMware 기술 지원 담당자가 가상 시스템 구성 매개 변수를 변경하거나 추가하도록 지침을 줄 수 있습니다.

중요 시스템에 문제가 없을 때 매개 변수를 변경하거나 추가하면 시스템 성능이나 안정성이 낮아질 수 있습니다.

다음 조건이 적용됩니다.

- 매개 변수를 변경하려는 경우 키워드/값 쌍에 대한 기존 값을 변경해야 합니다. 예를 들어 키워드/값인 기존 쌍을 키워드/값2로 변경하는 경우 새 키워드는 값2입니다.

- 구성 매개 변수 항목은 삭제할 수 없습니다.

경고 구성 매개 변수 키워드에 값을 할당해야 합니다. 값을 할당하지 않으면 키워드가 값 0 또는 false를 수신해 가상 시스템의 전원을 켤 수 없습니다.

사전 요구 사항

가상 시스템의 전원을 끕니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **VM 옵션** 탭에서 **고급**을 확장합니다.
- 4 [구성 매개 변수] 행에서 **구성 편집**을 클릭합니다.
구성 매개 변수 대화상자가 열립니다.
- 5 (선택 사항) 매개 변수를 추가하려면 **매개 변수 추가**를 클릭하고 매개 변수의 이름과 값을 입력합니다.
- 6 (선택 사항) 매개 변수를 변경하려면 해당 매개 변수의 **값** 텍스트 상자에 새로운 값을 입력합니다.
- 7 **확인**을 클릭하여 변경 내용을 저장하고 **구성 매개 변수** 대화상자를 종료합니다.
- 8 **저장**을 클릭합니다.

VMware Host Client에서 가상 시스템의 자동 시작 옵션 구성

가상 시스템의 자동 시작 옵션을 구성하여 호스트의 다른 가상 시스템 이전이나 이후에 가상 시스템이 시작하도록 설정할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭합니다.
- 3 자동 시작 옵션을 구성하려면 **자동 시작 > 구성**을 선택합니다.
- 4 가상 시스템에 대한 기본 타이밍 및 시작 순서를 설정하려면 팝업 메뉴에서 옵션을 선택합니다.

옵션	설명
시작 지연	시간(초)을 선택합니다. ESXi 호스트는 첫 번째 가상 시스템의 전원을 켜 후 지정된 지연 시간 동안 기다렸다가 다음 가상 시스템의 전원을 켭니다.
중지 지연	시간(초)을 선택합니다. 중지 지연은 종료 명령이 완료될 때까지 ESXi 호스트가 대기하는 최대 시간입니다. 가상 시스템은 시작 순서와 반대로 종료됩니다. ESXi 호스트에서 지정한 시간 내에 첫 번째 가상 시스템이 종료되면 호스트는 다음 가상 시스템을 종료합니다.

옵션	설명
작업 중지	<p>중지 작업 드롭다운 메뉴에서 호스트가 종료될 때 해당 호스트의 가상 시스템에 적용할 수 있는 종료 작업을 선택합니다.</p> <ul style="list-style-type: none"> ■ 시스템 기본값 ■ 전원 끄기 ■ 일시 중단 ■ 종료
하트비트 대기	<ul style="list-style-type: none"> ■ 예를 선택하여 하트비트 대기 옵션을 사용하도록 설정합니다. 가상 시스템에 VMware Tools가 설치된 경우 이 옵션을 사용할 수 있습니다. ESXi 호스트가 첫 번째 가상 시스템의 전원을 켜면 호스트는 즉시 다음 가상 시스템의 전원을 켭니다. 가상 시스템의 전원이 켜지는 시작 순서는 가상 시스템이 첫 번째 하트비트를 수신한 후에도 계속됩니다.

5 **저장**을 클릭합니다.

VMware Host Client를 사용하여 가상 시스템 호환성 업그레이드

가상 시스템 호환성에 따라 가상 시스템에서 사용할 수 있는 가상 하드웨어가 결정되며, 이는 호스트 시스템에서 사용 가능한 물리적 하드웨어에 해당됩니다.

호환성 수준을 업그레이드하여 가상 시스템이 호스트에서 실행 중인 ESXi의 최신 버전과 호환되도록 할 수 있습니다.

가상 시스템 하드웨어 버전 및 호환성에 대한 자세한 내용은 "vSphere 가상 시스템 관리"의 내용을 참조하십시오.

사전 요구 사항

- 가상 시스템의 백업 또는 스냅샷을 생성합니다. [스냅샷으로 가상 시스템 관리](#)의 내용을 참조하십시오.
- VMware Tools를 업그레이드합니다. Microsoft Windows를 실행하는 가상 시스템에서 VMware Tools를 업그레이드하기 전에 호환성을 업그레이드할 경우 가상 시스템의 네트워크 설정이 손실될 수 있습니다.
- VMFS3, VMFS5 또는 NFS 데이터스토어의 ESXi 호스트에서 모든 .vmdk 파일을 사용할 수 있는지 확인합니다.
- 가상 시스템이 VMFS3, VMFS5 또는 NFS 데이터스토어에 저장되어 있는지 확인합니다.
- 가상 시스템의 호환성 설정이 지원되는 최신 버전으로 설정되어 있지 않은지 확인합니다.
- 가상 시스템과 호환되도록 할 ESXi 버전을 결정합니다. "vSphere 가상 시스템 관리"의 내용을 참조하십시오.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **VM 호환성 업그레이드**를 선택합니다.
- 3 지원되는 최신 버전을 선택하고 **업그레이드**를 클릭합니다.

VMware Host Client에서 가상 시스템 관리

VMware Host Client에서 가상 시스템을 생성한 후 가상 시스템에서 다양한 관리 작업을 수행할 수 있습니다.

호스트에서 가상 시스템을 삭제하고, 데이터스토어에서 가상 시스템을 제거하고, 데이터스토어에 다시 등록하는 등의 작업을 수행할 수 있습니다. 가상 시스템을 호스트로 이동할 수도 있습니다.

VMware Host Client에서 가상 시스템 액세스

로그인한 호스트에서 가상 시스템에 액세스하여 가상 시스템 하드웨어 및 옵션을 구성하고 관리 작업 및 기본 문제 해결 작업을 수행할 수 있습니다.

VMware Host Client 인벤토리에서 가상 시스템을 표시하려면 가상 시스템의 전원을 켭니다.

절차

- ◆ 로그인한 호스트에서 사용할 수 있는 가상 시스템에 액세스하려면 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.

결과

사용할 수 있는 가상 시스템 목록은 **가상 시스템**에 표시됩니다.

이제 목록의 가상 시스템에서 가상 시스템 설정을 편집하고 여러 관리 및 문제 해결 작업을 수행할 수 있습니다.

VMware Host Client에서 가상 시스템의 전원 상태

가상 시스템의 기본 전원 작업에는 전원 켜기, 전원 끄기, 일시 중단 및 리셋이 포함됩니다.

가상 시스템 전원 상태를 변경하는 방법에 대한 자세한 내용은 [VMware Host Client에서 가상 시스템 전원 상태 구성](#)에서 참조하십시오.





사전 요구 사항

- **VirtualMachine.상호 작용.전원 켜기** 권한이 있는지 확인합니다.
- **VirtualMachine.상호 작용.전원 끄기** 권한이 있는지 확인합니다.
- **VirtualMachine.상호 작용.일시 중단** 권한이 있는지 확인합니다.
- **VirtualMachine.상호 작용.리셋** 권한이 있는지 확인합니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.

- 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 전원 작업을 선택합니다.

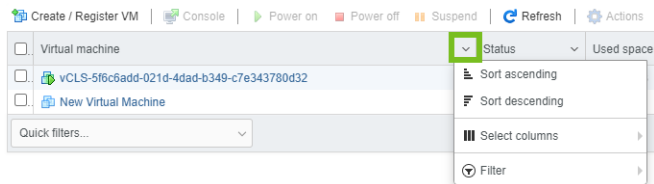
옵션	설명
전원 켜기()	가상 시스템이 중지되면 가상 시스템의 전원을 켭니다.
전원 끄기()	가상 시스템의 전원을 끄고 게스트 운영 체제를 종료합니다. 가상 시스템의 전원을 끄면 데이터가 손실될 수 있습니다.
일시 중단()	실행 중인 가상 시스템을 일시 중단하고 네트워크에 연결된 상태로 둡니다. 일시 중단된 가상 시스템을 재개하면 가상 시스템이 일시 중단되었을 때와 동일한 지점에서 가상 시스템이 계속 작동합니다.
재설정()	가상 시스템의 전원을 끄지 않고 게스트 운영 체제를 종료한 후 다시 시작합니다.

VMware Host Client에서 가상 시스템 열 구성 사용

VMware Host Client의 가상 시스템 패널을 사용하여 표시할 정보를 구성할 수 있습니다. 상태, 사용된 공간, 호스트 이름, 호스트 CPU 등과 같이 다양한 열을 표시하거나 숨길 수 있습니다.

절차

- VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 가상 시스템 목록에서 열 제목 옆에 있는 아래쪽 화살표 아이콘을 클릭하고 **열 선택**을 선택합니다.



사용 가능한 모든 열이 포함된 목록이 표시됩니다.

- 가상 시스템 패널에서 표시할 정보를 선택합니다.

VMware Host Client에서 호스트로부터 가상 시스템 제거

가상 시스템을 데이터스토어에서는 유지하지만 VMware Host Client 인벤토리에서는 표시하지 않게 하려는 경우 가상 시스템을 등록 취소할 수 있습니다.

사전 요구 사항

가상 시스템의 전원을 끕니다.

절차

- VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **등록 취소**를 선택합니다.
- 인벤토리에서 가상 시스템을 제거하는 것을 확인하려면 **예**를 클릭합니다.

결과

호스트가 인벤토리에서 가상 시스템을 제거하고 해당 가상 시스템의 상태를 더 이상 추적하지 않습니다.

VMware Host Client에서 데이터스토어의 가상 시스템 제거

데이터스토어의 공간을 확보하기 위해 더 이상 필요하지 않은 가상 시스템을 제거할 수 있습니다. VMware Host Client 인벤토리에서 가상 시스템을 제거하면 데이터스토어에서 모든 가상 시스템 파일(구성 파일 및 가상 디스크 파일 포함)이 삭제됩니다. 여러 가상 시스템을 삭제할 수 있습니다.

사전 요구 사항

- 가상 시스템의 전원을 끕니다.
- 가상 시스템이 다른 가상 시스템과 디스크를 공유하지 않는지 확인합니다. 두 가상 시스템이 하나의 디스크를 공유하는 경우에는 디스크 파일이 삭제되지 않습니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 제거할 가상 시스템 옆에 있는 확인란을 하나 이상 선택하고 **작업 > 삭제**를 선택합니다.
VM 삭제 대화상자가 열립니다.
- 3 **삭제**를 클릭합니다.

VMware Host Client에서 가상 시스템 등록

가상 시스템 또는 템플릿을 호스트에서 제거했지만 호스트 데이터스토어에서는 제거하지 않은 경우 호스트의 인벤토리로 돌려보낼 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭합니다.
- 2 목록에서 데이터스토어를 마우스 오른쪽 버튼으로 클릭하고 **VM 등록**을 클릭합니다.
- 3 목록에서 등록하려는 가상 시스템을 선택하고 **등록**을 클릭합니다.

스냅샷으로 가상 시스템 관리

스냅샷은 스냅샷을 만드는 시점의 가상 시스템 상태 및 데이터를 보관합니다. 가상 시스템의 스냅샷을 생성하면 지정된 상태의 가상 시스템 이미지가 복사되고 저장됩니다.

반복적으로 특정 가상 시스템 상태로 되돌려야 하지만 가상 시스템을 여러 개 생성하지는 않으려는 경우 스냅샷을 사용하면 편리합니다.

선형 프로세스에서 여러 개의 가상 시스템 스냅샷을 만들어 여러 복원 지점을 만들 수 있습니다. 여러 스냅샷을 사용하면 여러 위치를 저장하여 다양한 종류의 작업 프로세스를 지원할 수 있습니다. 스냅샷은 개별 가상 시스템에서 작동합니다. 예를 들어 여러 가상 시스템의 스냅샷을 만들어 팀의 각 멤버를 위한 VM의 스냅샷을 만들려면 각 팀 멤버의 가상 시스템마다 개별 스냅샷을 만들어야 합니다.

스냅샷은 알려지지 않거나 유해한 영향이 있을 수 있는 소프트웨어를 테스트하기 위한 단기 솔루션으로 유용합니다. 예를 들어 업데이트 패키지 설치와 같은 선형 또는 반복 프로세스나 다른 버전의 프로그램 설치와 같은 분기 프로세스 중에 스냅샷을 복원 지점으로 사용할 수 있습니다. 스냅샷을 사용하면 동일한 기준선에서 각각의 설치가 시작될 수 있습니다.

스냅샷으로 가상 시스템을 변경하기 전에 기준선을 보존할 수도 있습니다.

vSphere Client에서 가상 시스템 스냅샷 및 스냅샷 트리의 생성 및 관리에 대한 다양한 작업을 사용할 수 있습니다. 이러한 작업을 통해 스냅샷을 생성하고, 스냅샷 계층의 스냅샷을 되돌리고, 스냅샷을 삭제하는 등의 작업을 수행할 수 있습니다. 나중에 특정 가상 시스템 상태를 되돌릴 수 있도록 특정 시점에 가상 시스템 상태를 저장하는 스냅샷 트리를 생성할 수 있습니다. 스냅샷 트리의 각 분기에는 최대 32개의 스냅샷이 포함될 수 있습니다.

스냅샷에서 보존하는 정보는 다음과 같습니다.

- 가상 시스템 설정 스냅샷을 생성한 후 추가되거나 변경된 디스크가 포함된 가상 시스템 디렉토리입니다.
- 전원 상태 가상 시스템은 전원 켜짐, 전원 꺼짐 또는 일시 중단 상태일 수 있습니다.
- 디스크 상태 모든 가상 시스템의 가상 디스크의 상태입니다.
- (선택 사항) 메모리 상태입니다. 가상 시스템 메모리의 내용입니다.

스냅샷 계층

vSphere Client는 스냅샷 계층을 하나 이상의 분기가 있는 트리로 표시합니다. 계층의 스냅샷에는 상위-하위 관계가 있습니다. 선형 프로세스에서는 각 스냅샷(마지막 스냅샷 제외)마다 상위 스냅샷 하나와 하위 스냅샷 하나가 있습니다. 마지막 스냅샷에는 하위 스냅샷이 없습니다. 각 상위 스냅샷에는 하위 스냅샷이 둘 이상 있을 수 있습니다. 현재 상위 스냅샷으로 되돌리거나 스냅샷 트리의 상위 또는 하위 스냅샷으로 되돌리고 해당 스냅샷에서 더 많은 스냅샷을 만들 수 있습니다. 스냅샷을 되돌리고 다른 스냅샷을 생성할 때마다 분기(하위 스냅샷)가 생성됩니다.

상위 스냅샷

처음으로 만드는 가상 시스템 스냅샷은 기본 상위 스냅샷이 됩니다. 상위 스냅샷은 가상 시스템의 현재 상태에 대한 최근에 저장된 버전입니다. 스냅샷을 만들면 해당 가상 시스템에 연결된 각 디스크에 대해 델타 디스크 파일이 만들어지고 선택적으로 메모리 파일도 만들어집니다. 델타 디스크 파일과 메모리 파일은 기본 .vmdk 파일과 함께 저장됩니다. 상위 스냅샷은 스냅샷 관리자에서 항상 **현재 위치** 아이콘 위에 즉시 나타나는 스냅샷입니다. 스냅샷을 되돌리면 해당 스냅샷이 **현재 위치** 상태의 상위 스냅샷이 됩니다.

참고 경우에 따라 상위 스냅샷이 최근에 생성한 스냅샷이 아닐 수도 있습니다.

하위 스냅샷

상위 스냅샷 이후에 생성된 가상 시스템의 스냅샷입니다. 각 하위 스냅샷은 연결된 각 가상 디스크에 대한 델타 파일을 포함하고, 필요할 경우 가상 디스크의 현재 상태(현재 위치)에서 가리키는 메모리 파일도 생성합니다. 각 하위 스냅샷의 델타 파일은 상위 디스크에 도달할 때까지 이전의 각 하위 스냅샷과 병합됩니다. 하위 디스크는 나중에 후속 하위 디스크의 상위 디스크가 될 수 있습니다.

스냅샷 트리에 여러 개의 분기가 있는 경우에는 상위 스냅샷과 하위 스냅샷의 관계가 변경될 수 있습니다. 상위 스냅샷에는 하위 스냅샷이 둘 이상 있을 수 있습니다. 많은 스냅샷에 하위가 없습니다.

경고 개별 하위 디스크나 스냅샷 구성 파일을 수동으로 저작하면 스냅샷 트리가 손상되고 데이터가 손실될 수 있으므로 수동으로 조작하지 마십시오. 이 제한에는 `vmkfstools` 명령을 사용하여 기본 상위 디스크에 대해 디스크 크기를 조정하고 디스크를 수정하는 작업이 포함됩니다.

스냅샷 동작

스냅샷을 만들면 연결된 각 가상 디스크나 가상 RDM에 대한 일련의 델타 디스크가 만들어져 특정 시점의 디스크 상태가 보존되며, 필요할 경우 메모리 파일이 만들어져 메모리 및 전원 상태도 보존됩니다. 스냅샷을 만들면 스냅샷 관리자에 가상 시스템 상태 및 설정을 나타내는 스냅샷 개체가 만들어집니다.

각 스냅샷마다 추가 델타 `.vmdk` 디스크 파일이 만들어집니다. 스냅샷을 만들 때 스냅샷 메커니즘은 게스트 운영 체제가 기본 `.vmdk` 파일에 쓰지 못하도록 하고 대신 모든 쓰기 작업을 델타 디스크 파일에 연결합니다. 델타 디스크는 가상 디스크의 현재 상태와 이전 스냅샷을 만든 시점의 상태 간의 차이를 나타냅니다. 스냅샷이 둘 이상 있는 경우 델타 디스크는 각 스냅샷 간의 차이를 나타낼 수 있습니다. 델타 디스크 파일은 급속히 커질 수 있으며, 게스트 운영 체제에서 가상 디스크의 모든 블록에 쓰는 경우 전체 가상 디스크만큼 커질 수도 있습니다.

스냅샷 파일 및 제한 사항

스냅샷을 만들면 가상 시스템 설정 및 가상 디스크의 상태가 캡처됩니다. 메모리 스냅샷을 만드는 경우에는 가상 시스템의 메모리 상태도 캡처됩니다. 이러한 상태는 가상 시스템의 기본 파일과 함께 상주하는 파일에 저장됩니다.

스냅샷 파일

스냅샷은 지원되는 스토리지 디바이스에 저장되는 여러 파일로 구성됩니다. 스냅샷 생성 작업은 `.vmdk`, `-delta.vmdk` 또는 `-sesparse.vmdk`, `.vmsd` 및 `.vmsn` 파일을 생성합니다. 기본적으로 첫 번째 및 모든 델타 디스크가 기본 `.vmdk` 파일에 저장됩니다. `.vmsd` 및 `.vmsn` 파일은 가상 시스템 디렉토리에 저장됩니다.

SEsparse는 VMFS6 데이터스토어에 있는 모든 델타 디스크의 기본 형식입니다.

델타 디스크 파일

게스트 운영 체제에서 쓸 수 있는 `.vmdk` 파일입니다. 델타 디스크는 가상 디스크의 현재 상태와 이전 스냅샷을 만든 시점의 상태 간의 차이를 나타냅니다. 스냅샷을 만들면 가상 디스크의 상태가 보관되고, 게스트 운영 체제가 이 가상 디스크에 쓰기를 중지하며, 델타 또는 하위 디스크가 생성됩니다.

델타 디스크에는 두 개의 파일에 있습니다. 하나는 기하 도형 및 하위-상위 관계 정보와 같은 가상 디스크에 대한 정보가 포함된 작은 설명자 파일입니다. 다른 하나는 원시 데이터가 포함된 해당 파일입니다.

델타 디스크를 구성하는 파일을 하위 디스크 또는 redo 로그라고 합니다.

플랫 파일

기본 디스크를 구성하는 두 개의 파일 중 하나인 `-flat.vmdk` 파일입니다. 플랫 디스크에는 기본 디스크의 원시 데이터가 포함됩니다. 이 파일은 데이터스토어 브라우저에서 별도의 파일로 표시되지 않습니다.

데이터베이스 파일

가상 시스템의 스냅샷 정보가 포함되며 스냅샷 관리자의 기본 정보 소스인 `.vmsd` 파일입니다. 이 파일에는 스냅샷 간의 관계와 각 스냅샷의 하위 디스크 간의 관계를 정의하는 줄 항목이 포함됩니다.

메모리 파일

가상 시스템의 활성 상태를 포함하는 `.vmsn` 파일입니다. 가상 시스템의 메모리 상태를 캡처하면 전원이 켜진 가상 시스템 상태로 복귀할 수 있습니다. 메모리 스냅샷이 아닌 스냅샷을 사용할 경우에는 전원이 꺼진 가상 시스템 상태로만 복귀할 수 있습니다. 메모리 스냅샷은 메모리 스냅샷이 아닌 스냅샷보다 만드는 데 오랜 시간이 걸립니다. ESXi 호스트에서 디스크에 메모리를 쓰는 데 걸리는 시간은 가상 시스템에서 사용하도록 구성된 메모리의 양에 따라 달라집니다.

스냅샷 생성 작업은 `.vmdk`, `-delta.vmdk`, `vmsd` 또는 `-sesparse.vmdk` 및 `vmsn` 파일을 생성합니다.

파일	설명
<code>vmname-number.vmdk</code> 및 <code>vmname-number-delta.vmdk</code>	가상 디스크의 현재 상태와 이전 스냅샷이 생성될 때 존재했던 상태 간의 차이를 나타내는 스냅샷 파일입니다. 파일 이름에는 <code>s1vm-000001.vmdk</code> 구문을 사용합니다. 여기에서 <code>s1vm</code> 은 가상 시스템의 이름이고, 여섯 자리 숫자인 <code>000001</code> 은 디렉토리에 이미 있는 파일을 기반으로 합니다. 이 숫자에서 가상 시스템에 연결된 디스크의 수는 고려되지 않습니다.
<code>vmname.vmsd</code>	가상 시스템 스냅샷 정보의 데이터베이스이자 스냅샷 관리자 관련 정보의 기본 소스입니다.
<code>vmname.Snapshotnumber.vmsn</code>	스냅샷을 생성하는 시점의 가상 시스템 메모리 상태입니다. 파일 이름에는 <code>s1vm.snapshot1.vmsn</code> 구문을 사용합니다. 여기에서 <code>s1vm</code> 은 가상 시스템 이름이고, <code>snapshot1</code> 은 첫 번째 스냅샷을 나타냅니다. 참고 <code>.vmsn</code> 파일은 메모리 선택에 관계없이 스냅샷을 만들 때마다 만들어집니다. 메모리가 없는 <code>.vmsn</code> 파일은 메모리가 있는 파일보다 훨씬 작습니다.

스냅샷 제한 사항

스냅샷은 가상 시스템 성능에 영향을 줄 수 있으며, 버스 공유를 사용하여 구성된 일부 디스크 유형 또는 가상 시스템은 지원하지 않습니다. 스냅샷은 특정 시점의 가상 시스템 상태를 캡처하는 데 유용한 단기 솔루션으로, 장기적 가상 시스템 백업에는 적절하지 않습니다.

- VMware에서는 게스트에서 iSCSI 이니시에이터를 사용하는 게스트 운영 체제, RDM 물리적 모드 디스크 또는 원시 디스크의 스냅샷을 지원하지 않습니다.
- 독립 디스크가 있는 가상 시스템은 스냅샷을 만들기 전에 전원을 꺼야 합니다.
- 독립 디스크가 있는 가상 시스템의 메모리 스냅샷은 가상 시스템의 게스트 운영 체제 동작을 분석하기 위한 용도로만 생성할 수 있습니다. 가상 시스템 백업에는 이러한 스냅샷을 사용할 수 없습니다. 이런 유형의 스냅샷 복원은 지원되지 않기 때문입니다.
- 중지된 스냅샷에는 VMware Tools 설치와 게스트 운영 체제 지원이 필요합니다.
- PCI vSphere DirectPath I/O 디바이스에서는 스냅샷이 지원되지 않습니다.

- VMware에서는 버스 공유를 사용하여 구성된 가상 시스템의 스냅샷은 지원하지 않습니다. 버스 공유가 필요한 경우 대체 솔루션으로 게스트 운영 체제에서 백업 소프트웨어를 실행하는 것이 좋습니다. 가상 시스템에 버스 공유의 구성을 방해하는 스냅샷이 현재 있는 경우 스냅샷을 삭제(통합)합니다.
- 스냅샷은 백업 솔루션에서 사용할 수 있는 특정 시점의 디스크 이미지를 제공하지만 스냅샷은 강력한 백업 및 복구 방법이 아닙니다. 가상 시스템이 들어 있는 파일이 손실되면 스냅샷 파일도 손실됩니다. 또한 여러 개의 스냅샷을 사용하면 관리하기가 어렵고 디스크 공간이 많이 소모되며 하드웨어 장애 발생 시 스냅샷이 보호되지 않습니다.
- 스냅샷은 가상 시스템의 성능에 부정적인 영향을 줄 수 있습니다. 성능 저하 정도는 스냅샷 또는 스냅샷 트리의 저장 기간, 트리 깊이 및 스냅샷을 만든 후 가상 시스템과 게스트 운영 체제가 변경된 횟수에 따라 달라집니다. 또한 가상 시스템의 전원을 켜는 데 걸리는 시간이 지연될 수 있습니다. 프로덕션 가상 시스템을 영구 기반의 스냅샷에서 실행하면 안 됩니다.
- 가상 시스템에 2TB보다 큰 가상 하드 디스크가 있는 경우 스냅샷 작업을 마치는 데 상당한 시간이 걸릴 수 있습니다.

스냅샷 제한 사항

스냅샷은 가상 시스템 성능에 영향을 줄 수 있으며, 버스 공유를 사용하여 구성된 일부 디스크 유형 또는 가상 시스템은 지원하지 않습니다. 스냅샷은 특정 시점의 가상 시스템 상태를 캡처하는 데 유용한 단기 솔루션으로, 장기적 가상 시스템 백업에는 적절하지 않습니다.

- VMware에서는 게스트에서 iSCSI 이니시에이터를 사용하는 게스트 운영 체제, RDM 물리적 모드 디스크 또는 원시 디스크의 스냅샷을 지원하지 않습니다.
- 독립 디스크가 있는 가상 시스템은 스냅샷을 만들기 전에 전원을 꺼야 합니다.
- ESXi 7.0 업데이트 3i부터, 독립 디스크가 있는 가상 시스템의 메모리 스냅샷은 가상 시스템의 게스트 운영 체제 동작을 분석하기 위한 용도로만 생성할 수 있습니다. 가상 시스템 백업에는 이러한 스냅샷을 사용할 수 없습니다. 이런 유형의 스냅샷 복원은 지원되지 않기 때문입니다.
- 중지된 스냅샷에는 VMware Tools 설치와 게스트 운영 체제 지원이 필요합니다.
- PCI vSphere DirectPath I/O 디바이스에서는 스냅샷이 지원되지 않습니다.
- VMware에서는 버스 공유를 사용하여 구성된 가상 시스템의 스냅샷은 지원하지 않습니다. 버스 공유가 필요한 경우 대체 솔루션으로 게스트 운영 체제에서 백업 소프트웨어를 실행하는 것이 좋습니다. 가상 시스템에 버스 공유의 구성을 방해하는 스냅샷이 현재 있는 경우 스냅샷을 삭제(통합)합니다.
- 스냅샷은 백업 솔루션에서 사용할 수 있는 특정 시점의 디스크 이미지를 제공하지만 백업 및 복구에는 강력한 방법이 아닙니다. 가상 시스템이 들어 있는 파일이 손실되면 스냅샷 파일도 손실됩니다. 또한 여러 개의 스냅샷을 사용하면 관리하기가 어렵고 디스크 공간이 많이 소모되며 하드웨어 장애 발생 시 스냅샷이 보호되지 않습니다.
- 스냅샷은 가상 시스템의 성능에 부정적인 영향을 줄 수 있습니다. 성능 저하 정도는 스냅샷 또는 스냅샷 트리의 저장 기간, 트리 깊이 및 스냅샷을 만든 후 가상 시스템과 게스트 운영 체제가 변경된 횟수에 따라 달라집니다. 또한 가상 시스템의 전원을 켜는 데 걸리는 시간이 지연될 수 있습니다. 프로덕션 가상 시스템을 영구 기반의 스냅샷에서 실행하면 안 됩니다.

- 가상 시스템에 2TB보다 큰 가상 하드 디스크가 있는 경우 스냅샷 작업을 마치는 데 상당한 시간이 걸릴 수 있습니다.

VMware Host Client에서 가상 시스템의 스냅샷 생성

가상 시스템의 스냅샷을 하나 이상 생성하여 스냅샷 생성 시 설정 상태, 디스크 상태 및 메모리 상태를 캡처할 수 있습니다. 스냅샷을 만들 때 가상 시스템 파일을 중지하고 가상 시스템 디스크를 스냅샷에서 제외할 수도 있습니다. 가상 시스템의 전원이 켜져 있거나 꺼져 있거나 또는 일시 중단되면 스냅샷을 생성할 수 있습니다. 일시 중단한 가상 시스템의 스냅샷을 생성하려면 스냅샷을 생성하기 전에 일시 중단 작업이 완료될 때까지 기다립니다.

스냅샷을 만들 때 가상 시스템에서 수행 중인 다른 작업이 있으면 해당 스냅샷으로 되돌릴 때 스냅샷 프로세스에 영향이 있을 수 있습니다. 스토리지 관점에서는 대량 I/O 로드가 발생하지 않는 때 스냅샷을 만드는 것이 가장 좋습니다. 서비스 관점에서는 가상 시스템에 다른 컴퓨터와 통신하는 애플리케이션이 없을 때 스냅샷을 만드는 것이 가장 좋습니다. 가상 시스템이 다른 컴퓨터와 통신 중인 경우, 특히 프로덕션 환경에서는 문제가 발생할 가능성이 가장 큼니다. 예를 들어 가상 시스템이 네트워크에서 서버의 파일을 다운로드하고 있을 때 스냅샷을 만들면 가상 시스템이 계속해서 파일을 다운로드하고 진행률을 서버에 전달하게 됩니다. 스냅샷으로 복구할 경우 가상 시스템과 서버 간 통신이 뒤엉켜서 파일 전송이 실패합니다. 수행하는 작업에 따라 메모리 스냅샷을 생성할 수도 있고 가상 시스템의 파일 시스템을 중지할 수도 있습니다.

메모리 스냅샷

스냅샷을 생성하는 기본 옵션입니다. 가상 시스템 메모리 상태를 캡처할 경우 스냅샷에는 가상 시스템의 라이브 상태가 보관됩니다. 메모리 스냅샷은 정확한 시간에 스냅샷을 생성합니다. 예를 들어 계속 작동 중인 소프트웨어를 업그레이드할 때 스냅샷을 생성합니다. 메모리 스냅샷을 생성하면 업그레이드가 예상대로 완료되지 않거나 소프트웨어가 원하는 대로 작동하지 않는 경우 가상 시스템을 이전 상태로 되돌릴 수 있습니다.

메모리 상태를 캡처할 때 가상 시스템 파일을 중지할 필요가 없습니다. 메모리 상태를 캡처하지 않을 경우 스냅샷에는 가상 시스템의 라이브 상태가 저장되지 않으며, 사용자가 디스크를 중지하지 않는 한 디스크는 충돌 일치 상태가 됩니다.

가상 시스템의 메모리 상태를 캡처하는 스냅샷은 완료하는 데 시간이 오래 걸립니다. 네트워크를 통해 응답할 때 약간의 시간이 걸릴 수도 있습니다.

중지된 스냅샷

가상 시스템을 중지하면 VMware Tools에서는 가상 시스템의 파일 시스템을 중지합니다. 중지 작업은 스냅샷 디스크가 게스트 파일 시스템의 일관된 상태를 나타내도록 합니다. 중지 작업은 가상 시스템에서 실행 중인 프로세스(특히, 복원 작업 중 디스크에 저장하는 정보를 수정할 수 있는 프로세스)의 상태를 일시 중지하거나 변경합니다. 중지된 스냅샷은 자동 또는 정기 백업에 적절합니다. 예를 들어 가상 시스템 작업을 알지 못하는 상황에서 복구할 최신 백업을 여러 개 확보하려면 파일을 중지하면 됩니다.

가상 시스템의 전원이 꺼져 있거나 VMware Tools를 사용할 수 없는 경우에는 Quiesce 매개 변수를 사용할 수 없습니다. 대용량 디스크가 있는 가상 시스템은 중지할 수 없습니다.

IDE 또는 SATA 디스크가 있는 가상 시스템에서는 애플리케이션 일관성이 보장되는 중지 작업이 지원되지 않습니다.

중요 스냅샷을 유일한 백업 솔루션 또는 장기 백업 솔루션으로 사용하지 마십시오.

참고 동적 디스크(Microsoft 특정 디스크 유형)의 스냅샷을 생성하는 경우 해당 스냅샷 기술은 파일 시스템의 중지 상태를 유지하지만 애플리케이션의 중지 상태는 유지하지 않습니다.

사전 요구 사항

- 디스크 모드가 각기 다른 여러 개의 디스크를 사용하는 가상 시스템의 메모리 스냅샷을 만드는 경우 가상 시스템의 전원이 꺼져 있는지 확인합니다. 예를 들어 개별 디스크를 사용해야 하는 특수한 용도의 구성이 있는 경우 스냅샷을 생성하기 전에 먼저 가상 시스템의 전원을 꺼야 합니다.
- 가상 시스템의 메모리 상태를 캡처하려면 가상 시스템의 전원이 켜져 있는지 확인합니다.
- 가상 시스템 파일을 중지하려면 가상 시스템의 전원이 켜져 있고 VMware Tools가 설치되어 있는지 확인합니다.
- 가상 시스템에 대한 **가상 시스템.스냅샷 관리.스냅샷 생성** 권한이 있는지 확인합니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록의 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **스냅샷 > 스냅샷 생성**을 선택합니다.
- 3 스냅샷의 이름을 입력합니다.
- 4 (선택 사항) 스냅샷에 대한 설명을 입력합니다.
- 5 (선택 사항) **가상 시스템 메모리 스냅샷 생성** 확인란을 선택하여 가상 시스템의 메모리를 캡처합니다.
- 6 (선택 사항) 스냅샷을 생성할 때 파일 시스템 내용이 알려진 일관된 상태가 되도록 **가상 시스템 메모리 스냅샷 생성**을 선택 취소하고 **게스트 파일 시스템 일시 정지(VMware Tools가 설치되어 있어야 함)** 확인란을 선택하여 게스트 운영 체제에서 실행 중인 프로세스를 일시 중지합니다.

가상 시스템의 전원이 켜져 있는 상태에서 가상 시스템의 메모리를 캡처하지 않으려는 경우에만 가상 시스템 파일을 중지합니다.

- 7 **스냅샷 생성**을 클릭합니다.

VMware Host Client에서 최신 스냅샷으로 복구

가상 시스템을 원래 상태로 되돌리거나 스냅샷 계층의 다른 스냅샷으로 되돌리려면 스냅샷을 복원합니다.

스냅샷을 복원하면 가상 시스템 메모리, 설정 및 가상 시스템 디스크의 상태가 해당 스냅샷을 만든 시점의 상태로 돌아갑니다. 시작 시 가상 시스템이 일시 중단, 전원 켜짐 또는 전원 꺼짐 상태가 되게 하려면 스냅샷을 만들 때 가상 시스템이 올바른 상태에 있도록 해야 합니다.

다음과 같은 방법으로 스냅샷을 복원할 수 있습니다.

최신 스냅샷으로 복구

현재 위치 위치에서 계층 내 한 레벨 위, 상위 스냅샷을 복원합니다. **최신 스냅샷으로 복구**는 가상 시스템의 현재 상태에 대한 상위 스냅샷을 활성화합니다.

다음으로 복구

스냅샷 트리의 스냅샷을 복원하고 해당 스냅샷을 가상 시스템의 현재 상태에 대한 상위 스냅샷으로 만들 수 있습니다. 이후부터는 후속 스냅샷을 만들면 스냅샷 트리의 새 분기가 만들어집니다.

스냅샷 복원의 효과는 다음과 같습니다.

- 현재 디스크 및 메모리 상태는 무시되고 가상 시스템이 상위 스냅샷의 디스크 및 메모리 상태로 돌아갑니다.
- 기존 스냅샷이 제거되지 않았습니다. 언제라도 그러한 스냅샷을 복원할 수 있습니다.
- 스냅샷에 메모리 상태가 포함되면, 가상 시스템은 스냅샷을 생성했을 때와 같은 전원 상태가 됩니다.

표 3-2. 스냅샷을 복원한 후의 가상 시스템 전원 상태

상위 스냅샷을 만들 때의 가상 시스템 상태	복원 후 가상 시스템 상태
전원 켜짐(메모리 포함)	상위 스냅샷으로 돌아가고 가상 시스템의 전원이 켜진 상태로 실행됩니다.
전원 켜짐(메모리 포함 안 함)	상위 스냅샷으로 돌아가고 가상 시스템의 전원이 꺼집니다.
전원 꺼짐(메모리 포함 안 함)	상위 스냅샷으로 돌아가고 가상 시스템의 전원이 꺼집니다.

특정 유형의 워크로드를 실행하는 가상 시스템은 스냅샷에서 복구한 후 응답을 재개하는 데 몇 분이 걸릴 수 있습니다.

참고 vApp 내의 가상 시스템에 대한 vApp 메타데이터는 가상 시스템 구성의 스냅샷 의미 체계를 따르지 않습니다. 따라서 스냅샷이 만들어진 후 삭제, 수정 또는 정의된 vApp 속성은 가상 시스템이 해당 스냅샷이나 이전 스냅샷으로 돌아간 후에도 그대로 유지됩니다(삭제, 수정 또는 정의된 상태).

사전 요구 사항

가상 시스템에 대한 **가상 시스템.스냅샷 관리.스냅샷으로 복구** 권한이 있는지 확인합니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록의 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **스냅샷 > 스냅샷 복원**을 선택합니다.

참고 스냅샷에 저장하지 않으면 가상 시스템의 현재 상태가 손실됩니다.

- 3 **복원**을 클릭하여 최신 스냅샷으로 가상 시스템을 되돌립니다.

VMware Host Client에서 스냅샷 삭제

스냅샷 관리자를 사용하여 단일 스냅샷 또는 스냅샷 트리의 모든 스냅샷을 삭제할 수 있습니다. 스냅샷을 삭제하면 스냅샷 관리자에서 해당 스냅샷이 제거됩니다. 스냅샷 파일은 상위 스냅샷 디스크에 통합되어 기록되며 가상 시스템 기본 디스크와 병합됩니다.

스냅샷을 삭제해도 가상 시스템 또는 다른 스냅샷이 변경되지 않습니다. 스냅샷을 삭제하면 스냅샷과 이전 디스크 상태 간의 변경 내용이 통합되고 삭제된 스냅샷에 대한 정보가 포함된 델타 디스크의 모든 데이터가 상위 디스크에 기록됩니다. 기본 상위 스냅샷을 삭제할 경우에는 모든 변경 내용이 기본 가상 시스템 디스크와 병합됩니다.

스냅샷을 삭제하려면 많은 양의 정보를 디스크에서 읽거나 디스크에 써야 합니다. 이 프로세스로 인해 통합이 완료되기 전까지 가상 시스템 성능이 낮아질 수 있습니다. 스냅샷을 통합하면 중복된 디스크가 제거되므로 가상 시스템 성능이 개선되고 스토리지 공간이 절약됩니다. 스냅샷을 삭제하고 스냅샷 파일을 통합하는 데 소요되는 시간은 마지막 스냅샷을 만든 후 게스트 운영 체제에서 가상 디스크에 쓰는 데이터의 양에 따라 달라집니다. 필요한 시간은 가상 시스템의 전원이 켜져 있는 경우 통합 과정에서 가상 시스템이 쓰는 데이터의 양에 비례합니다.

디스크 통합이 실패하면 가상 시스템의 성능이 낮아질 수 있습니다. 목록을 보고 별도의 통합 작업이 필요한 가상 시스템이 있는지 확인할 수 있습니다. 여러 가상 시스템의 통합 상태를 찾아서 보는 방법과 별도의 통합 작업을 실행하는 방법에 대한 자세한 내용은 "vSphere 가상 시스템 관리" 항목을 참조하십시오.

삭제

스냅샷 트리에서 상위 또는 하위 스냅샷 하나를 제거하려면 **삭제** 옵션을 사용합니다. **삭제** 옵션을 사용하면 스냅샷의 상태 및 이전 디스크 상태 간에 발생하는 디스크 변경 내용을 상위 스냅샷에 씁니다.

참고 단일 스냅샷을 삭제하면 가상 시스템의 현재 상태가 유지되고 다른 스냅샷에는 영향을 미치지 않습니다.

삭제 옵션을 사용하여 스냅샷 트리의 중단된 분기에서 손상된 스냅샷 및 해당 파일을 상위 스냅샷과 병합하지 않고 제거할 수도 있습니다.

모두 삭제

스냅샷 관리자에서 모든 스냅샷을 삭제하려면 **모두 삭제** 옵션을 사용합니다. **모두 삭제** 옵션을 사용하면 스냅샷과 이전 델타 디스크 상태 간에 발생하는 변경 내용을 기본 상위 디스크에 쓰고 기본 가상 시스템 디스크와 병합됩니다.

예를 들어 업데이트나 설치에 실패한 경우 스냅샷 파일을 상위 스냅샷과 병합하지 않으려면 먼저 **복원** 명령을 사용하여 이전 스냅샷으로 복원합니다. 이 작업은 스냅샷 델타 디스크를 무효화하고 메모리 파일을 삭제합니다. 그런 다음 **삭제** 옵션을 사용하여 스냅샷 및 관련 파일을 제거할 수 있습니다.

필요한 스냅샷을 실수로 삭제하지 않도록 주의하십시오. 삭제된 스냅샷은 복원할 수 없습니다. 예를 들어 브라우저 a, b 및 c를 설치하면서 각 브라우저가 설치된 후의 가상 시스템 상태를 캡처하려고 할 수 있습니다. 첫 번째 또는 기본 스냅샷은 브라우저 a가 설치된 가상 시스템을 캡처하고 두 번째 스냅샷은 브라우저 b를 캡처합니다. 이때 브라우저 a가 포함된 기본 스냅샷을 복원하고 브라우저 c를 캡처하는 세 번째 스냅샷을 만든 다음 브라우저 b가 포함된 스냅샷을 삭제하면 브라우저 b가 포함된 가상 시스템 상태로 돌아갈 수 없게 됩니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록의 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **스냅샷 > 스냅샷 관리**를 선택합니다.
- 3 삭제할 스냅샷을 선택하고 **스냅샷 삭제**를 클릭합니다.
- 4 (선택 사항) 선택한 스냅샷과 함께 모든 하위 스냅샷을 삭제하려면 **스냅샷 삭제** 대화상자에서 **모든 하위 스냅샷을 제거합니다** 확인란을 선택합니다.
- 5 **제거**를 클릭하여 삭제를 확인합니다.
- 6 **닫기**를 클릭하여 스냅샷 관리자에서 나갑니다.

VMware Host Client에서 스냅샷 관리자를 사용하는 이유

가상 시스템의 모든 스냅샷을 검토하고 스냅샷 관리자를 사용하여 스냅샷을 관리할 수 있습니다.

스냅샷을 생성한 후 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **스냅샷으로 되돌리기**를 클릭하여 언제든지 스냅샷 상태로 가상 시스템을 복원할 수 있습니다.

일련의 스냅샷이 있는 경우 스냅샷 관리자를 사용하여 상위 또는 하위 스냅샷을 복원할 수 있습니다. 복원된 스냅샷으로 만드는 후속 하위 스냅샷은 스냅샷 트리에 분기를 만듭니다. 스냅샷 관리자를 사용하여 트리에서 스냅샷을 삭제합니다.

표 3-3. 스냅샷 관리자

옵션	설명
스냅샷 트리	가상 시스템의 모든 스냅샷이 표시됩니다.
현재 위치 아이콘	현재 위치 아이콘은 가상 시스템의 현재 및 활성 상태를 나타냅니다. 복원, 삭제 및 편집 작업은 현재 위치 상태에 대해 비활성화되어 있습니다.
생성, 복원, 삭제, 편집	스냅샷 옵션입니다.
세부 정보	스냅샷 이름과 설명, 스냅샷을 생성한 날짜가 표시됩니다. 콘솔에는 스냅샷 생성 시 가상 시스템의 전원 상태가 표시됩니다. 스냅샷을 선택하지 않은 경우 이름, 설명 및 생성일 텍스트 상자는 비어 있습니다.

VMware Host Client에서 가상 시스템 모니터링

VMware Host Client에서 생성한 가상 시스템에서 수행되는 작업을 추적하고 다양한 성능 측면을 모니터링할 수 있습니다.

VMware Host Client에서 가상 시스템 성능 차트 보기

VMware Host Client에서 생성하는 가상 시스템의 리소스 사용량에 대한 정보가 있는 선형 차트를 볼 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.

- 2 목록에서 가상 시스템을 클릭합니다.
- 3 VMware Host Client 인벤토리에서 가상 시스템을 확장하고 **모니터**를 클릭합니다.
- 4 **성능**을 클릭합니다.
- 5 지난 한 시간에 대한 가상 시스템 리소스 사용량을 보려면 드롭다운 메뉴에서 옵션을 선택합니다.
 - 지난 한 시간 동안 가상 시스템에서 사용한 CPU 백분율을 보려면 **CPU 사용량**을 선택합니다.
 - 지난 한 시간 동안 호스트에서 소비한 메모리를 보려면 **메모리 사용량**을 선택합니다.

VMware Host Client에서 가상 시스템 이벤트 보기

이벤트는 사용자가 가상 시스템에서 수행하는 작업의 기록입니다. VMware Host Client에서 가상 시스템을 생성하면 가상 시스템과 연결된 이벤트를 볼 수 있습니다.

사전 요구 사항

필요한 권한: **읽기 전용**.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 클릭합니다.
- 3 VMware Host Client 인벤토리에서 가상 시스템을 확장하고 **모니터**를 클릭합니다.
- 4 **이벤트**를 클릭합니다.

모든 가상 시스템 이벤트 목록이 표시됩니다.
- 5 (선택 사항) 목록에서 이벤트 세부 정보를 볼 이벤트를 클릭합니다.
- 6 (선택 사항) 목록 위의 필터 컨트롤을 사용하여 목록을 필터링합니다.
- 7 (선택 사항) 열 머리글을 클릭하여 목록을 정렬합니다.

VMware Host Client에서 가상 시스템 태스크 보기

VMware Host Client에서 가상 시스템을 생성하면 모든 가상 시스템 태스크 및 태스크 대상, 이니시에이터, 대기 열 시간, 시작 시간, 결과 및 완료 시간에 대한 정보를 볼 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 클릭합니다.
- 3 VMware Host Client 인벤토리에서 가상 시스템을 확장하고 **모니터**를 클릭합니다.
- 4 **태스크**를 클릭합니다.
- 5 (선택 사항) 목록에서 태스크 세부 정보를 볼 태스크를 클릭합니다.

- 6 (선택 사항) 목록 위의 필터 컨트롤을 사용하여 목록을 필터링합니다.
- 7 (선택 사항) 열 머리글을 클릭하여 목록을 정렬합니다.

VMware Host Client에서 가상 시스템 로그 브라우저 보기

VMware Host Client를 사용하여 관리하는 호스트에 대한 로그를 생성하고 모니터링합니다. 로그를 사용하여 호스트 환경의 다양한 문제를 진단하고 해결합니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 클릭합니다.
- 3 VMware Host Client 인벤토리에서 가상 시스템을 확장하고 **모니터**를 클릭합니다.
- 4 **로그**를 클릭합니다.
- 5 (선택 사항) **지원 번들 생성**을 클릭하여 문제 해결을 위한 모든 로그를 통합합니다.
- 6 목록에서 로그를 마우스 오른쪽 버튼으로 클릭하고 **새 창에서 열기**를 선택하여 로그를 봅니다.

VMware Host Client에서 가상 시스템 알림 보기

VMware Host Client에서 생성하는 가상 시스템의 가상 시스템 알림 및 수행할 수 있는 관련 태스크에 대한 정보를 볼 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 클릭합니다.
- 3 VMware Host Client 인벤토리에서 가상 시스템을 확장하고 **모니터**를 클릭합니다.
- 4 **알림**을 클릭합니다.
모든 가상 시스템 알림이 있는 목록이 표시됩니다.
- 5 (선택 사항) 세부 정보를 볼 알림을 클릭합니다.
- 6 (선택 사항) 알림을 클릭하고 **작업**을 클릭하여 제안된 작업을 봅니다.

VMware Host Client에서 가상 시스템 하드웨어 구성

4

가상 시스템을 생성할 때 또는 가상 시스템을 생성하고 게스트 운영 체제를 설치한 후에 대부분의 가상 시스템 하드웨어 설정을 구성할 수 있습니다.

다음으로 아래 항목을 읽으십시오.

- 가상 CPU 구성 및 제한 사항
- 가상 메모리 구성
- 네트워크 가상 시스템 구성
- 가상 디스크 구성
- VMware Host Client에서 가상 시스템 컨트롤러 구성
- VMware Host Client에서 기타 가상 시스템 디바이스 구성
- VMware Host Client에서 가상 시스템 보호

가상 CPU 구성 및 제한 사항

가상 시스템을 생성할 때 또는 게스트 운영 체제를 설치한 이후에는 CPU 매개 변수 중 대부분을 설정할 수 있습니다. 일부 작업의 경우에는 설정을 변경하기 전에 가상 시스템의 전원을 꺼야 할 수도 있습니다.

VMware에서는 다음 용어를 사용합니다. 이러한 용어를 이해하면 CPU 리소스 할당에 대한 전략을 계획하는 데 도움이 될 수 있습니다.

CPU

CPU 또는 프로세서는 컴퓨터 애플리케이션의 실행에 필요한 작업을 수행하는 컴퓨터 시스템 구성 요소입니다. CPU는 컴퓨터 기능을 수행하는 기본 요소입니다. CPU에는 코어가 포함되어 있습니다.

CPU 소켓

CPU 소켓은 컴퓨터 마더보드에서 물리적 CPU 한 개를 연결할 수 있는 물리적 커넥터입니다. 일부 마더보드에는 여러 소켓이 있으며 여러 다중 코어 CPU(프로세서)를 연결할 수 있습니다.

코어

코어에는 L1 캐시를 포함하는 유닛과 애플리케이션을 실행하는 데 필요한 기능 유닛이 포함됩니다. 코어는 애플리케이션이나 스레드를 독립적으로 실행할 수 있습니다. 하나의 CPU에 하나 이상의 코어가 있을 수 있습니다.

리소스 공유

지분은 가상 시스템이나 리소스 풀의 중요도나 상대적 우선 순위를 지정합니다. 가상 시스템이 다른 가상 시스템 리소스 지분의 두 배를 가지고 있는 경우 두 개의 가상 시스템이 리소스 확보를 위해 경쟁한다면 이 리소스의 두 배를 소비할 수 있는 자격이 주어집니다.

리소스 할당

사용 가능한 리소스 용량이 수요를 충족하지 못할 경우 지분, 예약 및 제한 등의 CPU 리소스 할당 설정을 변경할 수 있습니다. 예를 들어 연말에 회계 관련 작업의 부하가 증가할 경우 회계 리소스 풀 예약을 늘릴 수 있습니다.

vSphere Virtual SMP(Virtual Symmetric Multiprocessing)

가상 SMP 또는 vSphere Virtual Symmetric Multiprocessing은 하나의 가상 시스템에 여러 프로세서를 포함할 수 있도록 해주는 기능입니다.

가상 CPU 제한

가상 시스템에 할당할 수 있는 가상 CPU의 최대 개수는 768개입니다. 가상 CPU의 개수는 호스트의 논리적 CPU 수 및 가상 시스템에 설치된 게스트 운영 체제 유형에 따라 달라집니다.

다음 제한 사항을 알아 두어야 합니다.

- 가상 시스템에는 호스트의 논리적 코어 수보다 많은 가상 CPU가 있지 않아야 합니다. 하이퍼스레딩이 비활성화되어 있으면 논리적 코어 수와 물리적 코어 수가 같고 하이퍼스레딩이 활성화되어 있으면 논리적 코어 수가 물리적 코어 수의 두 배입니다.
- 실행 중인 가상 시스템에 128개 이하의 가상 CPU가 있는 경우 무중단 추가를 사용하여 가상 CPU 수를 더 늘릴 수 없습니다. 이러한 제한을 초과하여 가상 CPU의 수를 변경하려면, 먼저 가상 시스템의 전원을 꺼야 합니다. 반면에 실행 중인 가상 시스템에 128개가 넘는 가상 CPU가 이미 있으면 무중단 추가를 사용하여 가상 CPU 수를 최대 768개까지 늘릴 수 있습니다.
- 가상 시스템에 구성할 수 있는 가상 CPU 소켓의 최대 수는 128개입니다. 128개가 넘는 가상 CPU로 가상 시스템을 구성하려면 다중 코어 가상 CPU를 사용해야 합니다.
- 일부 게스트 운영 체제는 Virtual SMP를 지원하지 않으며 이 기능을 지원하는 게스트 운영 체제는 호스트에서 사용할 수 있는 것보다 적은 수의 프로세서를 지원할 수도 있습니다. Virtual SMP 지원에 대한 자세한 내용은 "VMware 호환성 가이드" (<http://www.vmware.com/resources/compatibility>)를 참조하십시오.

다중 코어 가상 CPU 구성

VMware 다중 코어 가상 CPU 지원을 사용하면 가상 시스템에서 가상 소켓당 코어 수를 제어할 수 있습니다. 이 기능을 사용하면 소켓 제한이 있는 운영 체제가 호스트 CPU의 코어를 더 많이 사용할 수 있으므로 전체적인 성능이 향상됩니다.

중요 다중 코어 가상 CPU 설정에 맞게 가상 시스템을 구성하는 경우 해당 구성은 게스트 운영 체제 EULA 요구 사항을 반드시 준수해야 합니다.

다중 코어 가상 CPU를 사용하면 제한된 수의 CPU 소켓만 사용할 수 있는 운영 체제나 애플리케이션을 실행할 때 유용할 수 있습니다.

ESXi 7.0 업데이트 1 이상과 호환되는 가상 시스템은 가상 CPU를 최대 768까지 구성할 수 있습니다. 가상 시스템은 호스트의 실제 논리적 CPU 수보다 더 많은 가상 CPU를 가질 수 없습니다. 논리적 CPU 수는 물리적 프로세서 코어 수와 같거나 하이퍼스레딩을 사용하는 경우 물리적 프로세서 코어 수의 두 배입니다. 예를 들어서 호스트에 128개의 논리적 CPU가 있으면 128개의 가상 CPU에 대해 가상 시스템을 구성할 수 있습니다.

코어 수 및 소켓당 코어 수와 관련지어 가상 CPU의 할당 방법을 구성합니다. 가상 시스템에서 필요한 CPU 코어 수를 결정할 다음, 단일 코어 CPU, 듀얼 코어 CPU, 트라이 코어 CPU 등 어떤 CPU가 필요한지에 따라 각 소켓에서 원하는 코어 수를 선택합니다. 선택에 따라 가상 시스템에서 사용하는 소켓 수가 결정됩니다.

가상 시스템에 구성할 수 있는 가상 CPU 소켓의 최대 수는 128개입니다. 128개가 넘는 가상 CPU로 가상 시스템을 구성하려면 다중 코어 가상 CPU를 사용해야 합니다.

다중 코어 CPU에 대한 자세한 내용은 "vSphere 리소스 관리" 설명서를 참조하십시오.

가상 CPU 제한

가상 시스템에 할당할 수 있는 가상 CPU의 최대 개수는 768개입니다. 가상 CPU의 개수는 호스트의 논리적 CPU 수 및 가상 시스템에 설치된 게스트 운영 체제 유형에 따라 달라집니다.

다음 제한 사항을 알아 두어야 합니다.

- 가상 시스템에는 호스트의 논리적 코어 수보다 많은 가상 CPU가 있지 않아야 합니다. 하이퍼스레딩이 비활성화되어 있으면 논리적 코어 수와 물리적 코어 수가 같고 하이퍼스레딩이 활성화되어 있으면 논리적 코어 수가 물리적 코어 수의 두 배입니다.
- 실행 중인 가상 시스템에 128개 이하의 가상 CPU가 있는 경우 무중단 추가를 사용하여 가상 CPU 수를 더 늘릴 수 없습니다. 이러한 제한을 초과하여 가상 CPU의 수를 변경하려면, 먼저 가상 시스템의 전원을 꺼야 합니다. 반면에 실행 중인 가상 시스템에 128개가 넘는 가상 CPU가 이미 있으면 무중단 추가를 사용하여 가상 CPU 수를 최대 768개까지 늘릴 수 있습니다.
- 가상 시스템에 구성할 수 있는 가상 CPU 소켓의 최대 수는 128개입니다. 128개가 넘는 가상 CPU로 가상 시스템을 구성하려면 다중 코어 가상 CPU를 사용해야 합니다.
- 일부 게스트 운영 체제는 Virtual SMP를 지원하지 않으며 이 기능을 지원하는 게스트 운영 체제는 호스트에서 사용할 수 있는 것보다 적은 수의 프로세서를 지원할 수도 있습니다. Virtual SMP 지원에 대한 자세한 내용은 "VMware 호환성 가이드" (<http://www.vmware.com/resources/compatibility>)를 참조하십시오.

다중 코어 가상 CPU 구성

VMware 다중 코어 가상 CPU 지원을 사용하면 가상 시스템에서 가상 소켓당 코어 수를 제어할 수 있습니다. 이 기능을 사용하면 소켓 제한이 있는 운영 체제가 호스트 CPU의 코어를 더 많이 사용할 수 있으므로 전체적인 성능이 향상됩니다.

중요 다중 코어 가상 CPU 설정에 맞게 가상 시스템을 구성하는 경우 해당 구성은 게스트 운영 체제 EULA 요구 사항을 반드시 준수해야 합니다.

다중 코어 가상 CPU를 사용하면 제한된 수의 CPU 소켓만 사용할 수 있는 운영 체제나 애플리케이션을 실행할 때 유용할 수 있습니다.

ESXi 7.0 업데이트 1 이상과 호환되는 가상 시스템은 가상 CPU를 최대 768까지 구성할 수 있습니다. 가상 시스템은 호스트의 실제 논리적 CPU 수보다 더 많은 가상 CPU를 가질 수 없습니다. 논리적 CPU 수는 물리적 프로세서 코어 수와 같거나 하이퍼스레딩을 사용하는 경우 물리적 프로세서 코어 수의 두 배입니다. 예를 들어서 호스트에 128개의 논리적 CPU가 있으면 128개의 가상 CPU에 대해 가상 시스템을 구성할 수 있습니다.

코어 수 및 소켓당 코어 수와 관련지어 가상 CPU의 할당 방법을 구성합니다. 가상 시스템에서 필요한 CPU 코어 수를 결정할 다음, 단일 코어 CPU, 듀얼 코어 CPU, 트라이 코어 CPU 등 어떤 CPU가 필요한지에 따라 각 소켓에서 원하는 코어 수를 선택합니다. 선택에 따라 가상 시스템에서 사용하는 소켓 수가 결정됩니다.

가상 시스템에 구성할 수 있는 가상 CPU 소켓의 최대 수는 128개입니다. 128개가 넘는 가상 CPU로 가상 시스템을 구성하려면 다중 코어 가상 CPU를 사용해야 합니다.

다중 코어 CPU에 대한 자세한 내용은 "vSphere 리소스 관리" 설명서를 참조하십시오.

가상 CPU 수 변경

ESXi 7.0 업데이트 1 이상과 호환되는 가상 시스템은 가상 CPU를 최대 768까지 구성할 수 있습니다. 가상 시스템의 전원이 꺼진 상태에서도 가상 CPU의 수를 변경할 수 있습니다. 가상 CPU 무중단 추가를 사용하도록 설정하면 가상 시스템이 실행되는 동안 가상 CPU의 수를 늘릴 수 있습니다.

가상 CPU 핫 추가는 다중 코어 CPU가 지원되고 호환성이 ESXi 5.0 이상인 가상 시스템의 경우에 지원됩니다. 가상 시스템의 전원이 켜져 있고 CPU 무중단 추가를 사용하도록 설정한 경우 실행 중인 가상 시스템에 가상 CPU를 무중단 추가할 수 있습니다. 소켓당 코어 수의 배수 단위로만 추가할 수 있습니다.

가상 시스템에 128개 이하의 가상 CPU가 있는 경우 무중단 추가를 사용하여 가상 CPU 수를 더 늘릴 수 없습니다. 이러한 제한을 초과하여 가상 CPU의 수를 변경하려면, 먼저 가상 시스템의 전원을 꺼야 합니다. 반면에 가상 시스템에 128개가 넘는 가상 CPU가 이미 있으면 무중단 추가를 사용하여 가상 CPU 수를 최대 768개까지 늘릴 수 있습니다.

가상 시스템에 구성할 수 있는 가상 CPU 소켓의 최대 수는 128개입니다. 128개가 넘는 가상 CPU로 가상 시스템을 구성하려면 다중 코어 가상 CPU를 사용해야 합니다.

중요 다중 코어 가상 CPU 설정에 맞게 가상 시스템을 구성하는 경우 해당 구성은 게스트 운영 체제 EULA 요구 사항을 반드시 준수해야 합니다.

사전 요구 사항

- CPU 무중단 추가가 사용되도록 설정되지 않은 경우 가상 CPU를 추가하기 전에 가상 시스템의 전원을 끕니다.
- 다중 코어 CPU를 무중단 추가하려면 가상 시스템이 ESXi 5.0 이상과 호환되는지 확인합니다.
- **가상 시스템.구성.CPU 수 변경** 권한이 있는지 확인합니다.

절차

- 1 인벤토리의 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
- 2 **가상 하드웨어** 탭에서 **CPU**를 확장합니다.
- 3 **CPU** 드롭다운 메뉴에서 코어 수를 선택합니다.
- 4 **소켓 당 코어 수** 드롭다운 메뉴에서 소켓당 코어 수를 선택하고 **확인**을 클릭합니다.

VMware Host Client에서 CPU 리소스 할당

작업 부하 요구를 관리하기 위해 공유, 예약 및 제한 설정을 사용하여 가상 시스템에 할당된 CPU 리소스의 양을 변경할 수 있습니다.

가상 시스템에는 CPU 리소스 할당에 영향을 미치는 다음과 같은 사용자 정의 설정이 있습니다.

제한

가상 시스템의 CPU 시간 소비량에 제한을 설정합니다. 이 값은 MHz 또는 GHz 단위로 표시합니다.

예약

가상 시스템에 보장된 최소 할당량을 지정합니다. 예약은 MHz 또는 GHz 단위로 표시합니다.

공유

각각의 가상 시스템에는 CPU 공유가 부여됩니다. 가상 시스템이 더 많이 공유될수록 CPU 유휴 시간이 없을 때 가상 시스템은 더 빈번한 CPU의 시간 조각을 받게 됩니다. 공유는 CPU 용량 할당을 위한 상대적인 메트릭을 나타냅니다.

사전 요구 사항

가상 시스템의 전원을 끕니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.

3 가상 하드웨어 탭에서 CPU를 확장하고 가상 시스템의 CPU 용량을 할당합니다.

옵션	설명
예약	이 가상 시스템에 보장된 CPU 할당량입니다.
제한	이 가상 시스템의 CPU 할당 상한 값입니다. 상한 값을 지정하지 않으려면 무제한 을 선택합니다.
공유	상위 총합을 기준으로 한 이 가상 시스템의 CPU 공유를 나타냅니다. 형제 가상 시스템은 예약과 제한에 의해 바인딩된 상대 공유 값에 따라 리소스를 공유합니다. 낮음 , 보통 또는 높음 을 선택합니다. 이 설정은 각각 1:2:4 비율의 공유 값을 지정합니다. 비례로 표시되는 특정 숫자의 공유를 각 가상 시스템에 제공하려면 사용자 지정 을 선택합니다.

4 저장을 클릭합니다.

가상 메모리 구성

가상 시스템 메모리 리소스 또는 옵션을 추가, 변경 또는 구성하여 가상 시스템 성능을 향상시킬 수 있습니다. 가상 시스템 생성 도중 또는 게스트 운영 체제가 설치된 이후에는 메모리 매개 변수 중 대부분을 설정할 수 있습니다.

일부 작업의 경우에는 설정을 변경하려면 가상 시스템의 전원을 꺼야 할 수도 있습니다.

가상 시스템의 메모리 리소스 설정은 가상 시스템에 할당되는 호스트 메모리의 양을 결정합니다. 가상 하드웨어 메모리 크기는 가상 시스템에서 실행되는 애플리케이션에 사용할 수 있는 메모리 양을 결정합니다. 가상 시스템은 구성된 가상 하드웨어 메모리 크기 이상의 메모리 리소스를 활용할 수 없습니다. ESXi 호스트가 메모리 리소스 사용을 가상 시스템에 사용할 수 있는 최대값으로 제한하므로 메모리 리소스를 기본값인 무제한으로 설정해도 좋습니다.

메모리 구성 변경

가상 시스템에 할당된 메모리 양을 재구성하여 성능을 향상시킬 수 있습니다.

BIOS 펌웨어를 사용하는 가상 시스템의 최소 메모리 크기는 4MB입니다. EFI 펌웨어를 사용하는 가상 시스템은 최소 96MB의 RAM이 필요하며, 이 용량보다 부족하면 전원이 켜지지 않습니다.

BIOS 펌웨어를 사용하는 가상 시스템의 최대 메모리 크기는 24560GB입니다. 메모리 크기가 6128GB 보다 큰 가상 시스템에는 EFI 펌웨어를 사용해야 합니다.

가상 시스템의 최대 메모리 크기는 ESXi 호스트의 물리적 메모리 및 가상 시스템의 호환성 설정에 따라 다릅니다.

가상 시스템 메모리가 호스트 메모리 크기보다 크면 가상 시스템 성능에 심각한 영향을 미칠 수 있는 스와핑이 발생합니다. 최상의 성능을 위한 최대값은 가상 시스템을 최고 속도로 실행하기 위해 ESXi 호스트의 물리적 메모리가 초과하지 않아야 하는 임계값을 나타냅니다. 이 값은 호스트의 상태가 변경됨(예: 가상 시스템 전원 켜짐 또는 꺼짐)에 따라 달라집니다.

메모리 크기는 4MB의 배수여야 합니다.

표 4-1. 최대 가상 시스템 메모리

호스트 버전에서 소개	가상 시스템 호환성	최대 메모리 크기
ESXi 8.0 업데이트 3	ESXi 8.0 업데이트 3 이상	24560 GB
ESXi 8.0 업데이트 2	ESXi 8.0 업데이트 2 이상	24560 GB
ESXi 8.0 업데이트 1	ESXi 8.0 업데이트 1 이상	24560 GB
ESXi 8.0	ESXi 8.0 이상	24560 GB
ESXi 7.0 업데이트 3	ESXi 7.0 업데이트 3 이상	24560 GB
ESXi 7.0 업데이트 2	ESXi 7.0 업데이트 2 이상	24560 GB
ESXi 7.0 업데이트 1	ESXi 7.0 업데이트 1 이상	24560 GB
ESXi 7.0	ESXi 7.0 이상	6128GB
ESXi 6.7 업데이트 2	ESXi 6.7 업데이트 2 이상	6128GB
ESXi 6.7	ESXi 6.7 이상	6128GB
ESXi 6.5	ESXi 6.5 이상	6128GB
ESXi 6.0	ESXi 6.0 이상	4080GB

ESXi 호스트 버전은 증가된 메모리 크기에 대한 지원이 시작된 시기를 나타냅니다. 예를 들어 ESXi 6.5에서 실행되며 ESXi 6.0 이상과 호환되는 가상 시스템의 메모리 크기는 4080GB로 제한됩니다.

사전 요구 사항

가상 시스템에 대한 **가상 시스템.구성.메모리 변경** 권한이 있는지 확인합니다.

절차

- 인벤토리의 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
- 가상 하드웨어** 탭에서 **메모리**를 확장하고 메모리 구성을 변경합니다.
 - 메모리** 텍스트 상자에 가상 시스템에 할당할 RAM 크기를 입력합니다.
 - MB, GB 또는 TB 중 어느 단위로 메모리를 지정할지 선택합니다.
- 확인**을 클릭합니다.

메모리 리소스 할당

공유, 예약 및 제한 설정을 이용하여 가상 시스템에 할당된 메모리 리소스의 양을 변경할 수 있습니다. 호스트는 이러한 설정에 따라 가상 시스템에 할당할 물리적 RAM의 적절한 양을 결정합니다. 부하와 상태에 따라 가상 시스템에 공유 값을 높거나 낮게 할당할 수 있습니다.

다음 사용자 정의 설정에 따라 가상 시스템의 메모리 리소스 할당이 달라집니다.

제한

가상 시스템의 메모리 소비량에 제한을 설정합니다. 이 값은 메가바이트 단위로 표시합니다.

예약

가상 시스템에 보장된 최소 할당량을 지정합니다. 예약은 메가바이트 단위로 표시합니다. 예약이 충족되지 않으면 가상 시스템이 켜지지 않습니다.

공유

각각의 가상 시스템에는 많은 메모리 공유가 부여됩니다. 가상 시스템에 더 많은 메모리 공유량이 부여될수록 해당 호스트가 받는 메모리 공유량도 더 커집니다. 공유는 메모리 용량 할당을 위한 상대적인 메트릭을 나타냅니다. 공유량 값에 대한 자세한 내용은 "vSphere 리소스 관리" 설명서를 참조하십시오.

구성된 메모리보다 더 큰 예약을 가상 시스템에 할당할 수는 없습니다. 가상 시스템에 큰 예약 용량을 지정하고 구성된 메모리 크기를 줄이면 예약 용량이 새로 구성된 메모리 크기에 맞게 감소됩니다.

사전 요구 사항

가상 시스템의 전원이 꺼져 있는지 확인합니다.

절차

- 1 인벤토리의 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
- 2 **가상 하드웨어** 탭에서 메모리를 확장하고 가상 시스템의 메모리 용량을 할당합니다.

옵션	설명
예약	이 가상 시스템에 보장된 메모리 할당량입니다.
제한	이 가상 시스템의 메모리 할당 상한 값입니다. 상한 값을 지정하지 않으려면 무제한 을 선택합니다.
공유	낮음, 일반, 높음 및 사용자 지정 값은 서버의 가상 시스템 공유 합계와 비교됩니다.

- 3 **확인**을 클릭합니다.

Hot Add 메모리 설정 변경

메모리 무중단 추가를 사용하면 가상 시스템의 전원이 켜져 있는 동안 가상 시스템의 메모리 리소스를 추가할 수 있습니다.

메모리 무중단 추가를 사용하도록 설정하면 가상 시스템의 ESXi 호스트에 일부 메모리 오버헤드가 발생합니다.

참고 ESXi 호스트가 버전 7.0 업데이트 2 이하인 경우 NVIDIA vGPU를 사용하는 가상 시스템에 메모리를 무중단 추가하려면 ESXi 호스트에 사용 가능한 vGPU 슬롯이 있어야 합니다. vSphere 7.0 업데이트 3부터는 소스 호스트에 사용 가능한 vGPU 슬롯이 필요하지 않습니다.

사전 요구 사항

- 가상 시스템의 전원을 끕니다.
- 가상 시스템에 메모리 무중단 추가 기능을 지원하는 게스트 운영 체제가 있는지 확인합니다.

- 가상 시스템 호환성이 ESXi 4.x 이상인지 확인합니다.
- VMware Tools가 설치되어 있는지 확인합니다.

절차

- 1 인벤토리의 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
- 2 **가상 하드웨어** 탭에서 **메모리**를 확장하고 **사용**을 선택하여 가상 시스템의 전원이 켜져 있을 때 가상 시스템에 메모리를 추가할 수 있도록 합니다.
- 3 **확인**을 클릭합니다.

결과

이제 가상 시스템이 켜져 있어도 가상 시스템에 메모리를 추가할 수 있습니다.

VMware Host Client에서 VM에 NVDIMM 디바이스 추가

비휘발성 또는 영구 컴퓨터 메모리를 사용할 수 있도록 하려면 가상 시스템에 가상 NVDIMM 디바이스를 추가합니다. NVM(비휘발성 메모리) 또는 PMem(영구 메모리)은 휘발성 메모리의 높은 데이터 전송 속도와 기존 스토리지의 지속성 및 복원력을 결합합니다. 가상 NVDIMM 디바이스는 재부팅 또는 전원 장애 시에도 저장된 데이터를 유지할 수 있는 가상 NVM 디바이스입니다.

가상 시스템은 호스트의 PMem 리소스를 가상 NVDIMM(비휘발성 듀얼 인라인 메모리 모듈) 또는 가상 영구 메모리 디스크를 통해 사용합니다.

영구 메모리에 대한 자세한 내용은 [영구 메모리 관리](#) 항목을 참조하십시오.

사전 요구 사항

- 가상 시스템의 게스트 운영 체제가 PMem을 지원하는지 확인합니다.
- 가상 하드웨어 버전이 14 이상인지 확인합니다.
- **데이터스토어.공간 할당** 권한이 있는지 확인합니다.
- 가상 시스템이 상주하는 호스트 또는 클러스터에 사용 가능한 PMem 리소스가 있는지 확인합니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭에서 **기타 디바이스 추가**를 클릭하고 드롭다운 메뉴에서 **NVDIMM**을 선택합니다.

NVDIMM 디바이스가 가상 하드웨어 디바이스 목록에 나타납니다. 각 가상 시스템에는 최대 64개의 NVDIMM 디바이스가 있을 수 있습니다.

- 4 새로 추가된 NVDIMM 디바이스를 구성합니다.
 - a 가상 하드웨어 디바이스 목록에서 **새 NVDIMM**을 확장합니다.
 - b 새 NVDIMM 디바이스의 크기를 입력합니다.

참고 나중에 NVDIMM 디바이스의 크기를 변경할 수 있습니다. 가상 시스템의 전원을 꺼야 합니다.

- c NVDIMM 컨트롤러 위치를 선택하거나 기본 위치를 그대로 둡니다.

- 5 **저장**을 클릭하여 마법사를 닫습니다.

네트워크 가상 시스템 구성

ESXi 네트워킹 기능은 동일한 호스트 또는 서로 다른 호스트에 있는 가상 시스템 간의 통신이나 다른 가상 시스템과 물리적 시스템 간의 통신을 사용하도록 설정합니다.

네트워킹 기능을 사용하면 ESXi 호스트를 관리할 수 있으며 NFS, iSCSI 또는 vSphere vMotion과 같은 VMkernel 서비스와 물리적 네트워크 간에 통신할 수 있습니다. 가상 시스템에 대한 네트워킹을 구성할 경우 어댑터 유형, 네트워크 연결 및 가상 시스템의 전원이 켜질 때 네트워크를 연결할지 여부를 선택하거나 변경합니다.

네트워크 어댑터 기본

가상 시스템을 구성하는 경우 NIC(네트워크 어댑터)를 추가하고 어댑터 유형을 지정할 수 있습니다.

네트워크 어댑터 유형

사용할 수 있는 네트워크 어댑터의 유형은 다음 요인에 따라 달라집니다.

- 가상 시스템 호환성. 생성하거나 최근에 업데이트한 호스트에 따라 다릅니다.
- 가상 시스템 호환성을 현재 호스트의 최신 버전으로 업데이트했는지 여부
- 게스트 운영 체제

현재 온-프레미스 환경과 VMware Cloud on AWS 간에서 지원되는 NIC가 다릅니다. 온-프레미스 배포에서는 다음과 같은 NIC 유형이 지원됩니다.

E1000E

Intel 82574 기가비트 이더넷 NIC의 에뮬레이트 버전입니다. E1000E는 Windows 8 및 Windows Server 2012의 기본 어댑터입니다.

E1000

Intel 82545EM 기가비트 이더넷 NIC의 에뮬레이트 버전입니다. Windows XP 이상과 Linux 버전 2.4.19 이상을 비롯하여 최신 게스트 운영 체제에서 사용할 수 있는 드라이버를 함께 제공합니다.

유동적

가상 시스템이 부팅될 때 자체가 Vlance 어댑터로 식별되지만, 가상 시스템을 초기화하는 드라이버에 따라 자체적으로 초기화되고 Vlance 또는 VMXNET 어댑터로 작동합니다. VMware Tools를 설치한 경우 VMXNET 드라이버가 Vlance 어댑터를 더 나은 성능의 VMXNET 어댑터로 변경합니다.

Vlance

구형 10Mbps NIC인 AMD 79C970 PCnet32 LANCE NIC의 에뮬레이트 버전으로, 32비트 레거시 게스트 운영 체제에서 사용할 수 있는 드라이버를 함께 제공합니다. 이 네트워크 어댑터로 구성된 가상 시스템은 네트워크를 즉시 사용할 수 있습니다.

VMXNET

가상 시스템의 성능에 맞게 최적화되었으며 상응하는 물리적 디바이스는 없습니다. 운영 체제 벤더는 이 카드의 드라이버를 기본으로 제공하지 않으므로 VMXNET 네트워크 어댑터용 드라이버를 사용하려면 VMware Tools를 설치해야 합니다.

VMXNET 2(고급)

VMXNET 어댑터를 기반으로 하지만, 점보 프레임 및 하드웨어 오프로드 등 최신 네트워크에 일반적으로 사용되는 고성능 기능을 제공합니다. VMXNET 2(고급)는 ESX/ESXi 3.5 이상에서 일부 게스트 운영 체제에만 사용할 수 있습니다.

VMXNET 3

성능 위주로 설계된 반가상화 NIC. VMXNET 3은 VMXNET2에서 사용할 수 있는 모든 기능을 제공하며 다중 대기열 지원(Windows의 수신측 배율), IPv6 오프로드 및 MSI/MSI-X 인터럽트 전달 등 몇 가지 새로운 기능을 추가합니다. VMXNET 3은 VMXNET 또는 VMXNET 2와 관련이 없습니다.

PVRDMA

OFED 동사 API를 통해 가상 시스템 간의 RDMA(원격 직접 메모리 액세스)를 지원하는 반가상화 NIC. 모든 가상 시스템에는 PVRDMA 디바이스가 있어야 하며 모든 가상 시스템은 Distributed Switch에 연결되어야 합니다. PVRDMA는 VMware vSphere vMotion 및 스냅샷 기술을 지원합니다. PVRDMA는 하드웨어 버전 13 및 게스트 운영 체제 Linux 커널 4.6 이상이 포함된 가상 시스템에서 사용할 수 있습니다.

가상 시스템에 PVRDMA 네트워크 어댑터를 할당하는 방법에 대한 자세한 내용은 "vSphere 네트워킹" 설명서를 참조하십시오.

SR-IOV 패스스루

SR-IOV가 지원되는 물리적 NIC의 VF(가상 기능)에 대한 표현. 가상 시스템과 물리적 어댑터는 VMkernel을 중재자로 사용하지 않고 데이터를 교환합니다. 이 어댑터 유형은 지연 시간으로 인해 장애가 발생할 수 있거나 더 많은 CPU 리소스가 필요한 가상 시스템에 적절합니다.

SR-IOV 패스스루는 게스트 운영 체제 Red Hat Enterprise Linux 6 이상과 Windows Server 2008 R2 SP2의 ESXi 6.0 이상에서 사용할 수 있습니다. 운영 체제 릴리스에는 일부 NIC의 기본 VF 드라이버가 포함되어 있을 수 있지만 나머지 NIC의 경우 해당 NIC 또는 호스트 벤더가 제공하는 위치에서 드라이버를 다운로드하여 설치해야 합니다.

가상 시스템에 SR-IOV 패스스루 네트워크 어댑터를 할당하는 방법에 대한 자세한 내용은 "vSphere 네트워킹" 설명서를 참조하십시오.

네트워크 어댑터 호환성 고려 사항은 "VMware 호환성 가이드" (<http://www.vmware.com/resources/compatibility>)를 참조하십시오.

레거시 네트워크 어댑터 및 ESXi 가상 하드웨어 버전

모든 레거시 가상 시스템의 기본 네트워크 어댑터는 게스트 운영 체제에서 사용할 수 있는 호환 어댑터와 가상 시스템이 생성된 가상 하드웨어의 버전에 따라 달라집니다.

가상 하드웨어 버전을 사용하도록 가상 시스템을 업그레이드하지 않으면 어댑터 설정이 변경되지 않습니다. 가상 시스템을 업그레이드하여 최신 가상 하드웨어를 활용할 경우 기본 어댑터 설정이 게스트 운영 체제 및 업그레이드 호스트 하드웨어와 호환되도록 변경될 가능성이 높습니다.

vSphere ESXi의 특정 버전에 대해 지원되는 게스트 운영 체제에 사용할 수 있는 네트워크 어댑터를 확인하려면 "VMware 호환성 가이드" (<http://www.vmware.com/resources/compatibility>)를 참조하십시오.

네트워크 어댑터와 레거시 가상 시스템

레거시 가상 시스템이란 사용 중인 제품에서 지원되지만 해당 제품의 최신 버전이 아닌 가상 시스템을 말합니다.

모든 레거시 가상 시스템의 기본 네트워크 어댑터는 게스트 운영 체제에서 사용할 수 있는 호환 어댑터와 가상 시스템이 생성된 가상 하드웨어의 버전에 따라 달라집니다.

ESXi 호스트의 최신 버전으로 업그레이드하여 가상 시스템을 최신 버전으로 업그레이드하지 않을 경우 어댑터 설정이 변경되지 않은 상태로 유지됩니다. 가상 시스템을 업그레이드하여 최신 가상 하드웨어를 활용할 경우 기본 어댑터 설정이 게스트 운영 체제 및 업그레이드 호스트 하드웨어와 호환되도록 변경될 가능성이 높습니다.

vSphere ESXi의 특정 버전에 대해 지원되는 게스트 운영 체제에 사용할 수 있는 네트워크 어댑터를 확인하려면 "VMware 호환성 가이드" (<http://www.vmware.com/resources/compatibility>)를 참조하십시오.

VMware Host Client에서 가상 네트워크 어댑터 구성 변경

가상 시스템의 가상 네트워크 어댑터에 대한 전원을 켜 때 연결 설정, MAC 주소 및 네트워크 연결을 구성할 수 있습니다.

사전 요구 사항

필요한 권한:

- MAC 주소 및 네트워크 편집을 위한 **가상 시스템.구성.디바이스 설정 수정.**
- **연결 및 전원을 켜 때 연결** 변경을 위한 **가상 시스템.상호 작용.디바이스 연결.**
- **네트워크.네트워크 할당**

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.

- 3 가상 하드웨어 탭을 클릭하고 하드웨어 목록에서 적절한 NIC(네트워크 어댑터)를 선택합니다.
- 4 (선택 사항) 가상 시스템의 전원을 켤 때 가상 NIC를 연결하려면 **전원을 켤 때 연결**을 선택합니다.
- 5 (선택 사항) **어댑터 유형** 드롭다운 메뉴에서 어댑터 유형을 선택합니다.
- 6 MAC 주소 구성에 대한 옵션을 선택합니다.

옵션	설명
자동	vSphere에서 MAC 주소를 자동으로 할당합니다.
수동	사용할 MAC 주소를 입력합니다.

- 7 **저장**을 클릭합니다.

VMware Host Client에서 가상 시스템에 네트워크 어댑터 추가

가상 시스템에 네트워크 어댑터(NIC)를 추가할 경우 어댑터 유형, 네트워크 연결을 선택하고 가상 시스템의 전원이 켜져 있을 때 디바이스를 연결할지 여부를 선택해야 합니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭을 클릭하고 **네트워크 어댑터 추가**를 클릭합니다.
- 4 네트워크 연결 패널에서 특정 레이블인 네트워크 또는 기존 네트워크를 선택합니다.
- 5 (선택 사항) 가상 시스템의 전원이 켜져 있을 때 가상 NIC를 연결하도록 구성하려면 **전원을 켤 때 연결**을 선택합니다.
- 6 **저장**을 클릭합니다.

가상 디스크 구성

가상 시스템이 실행 중일 때도 가상 시스템에 대용량 가상 디스크를 추가하거나 기존 디스크에 더 많은 공간을 추가할 수 있습니다.

가상 시스템이 만들어지는 동안에 또는 게스트 운영 체제를 설치한 후에 대부분의 가상 디스크 매개 변수를 설정할 수 있습니다.

새로운 가상 디스크, 기존 가상 디스크 또는 매핑된 SAN LUN에 가상 시스템 데이터를 저장할 수 있습니다. 가상 디스크는 게스트 운영 체제에 하나의 하드 디스크로 표시됩니다. 가상 디스크는 호스트 파일 시스템의 파일 하나 이상으로 구성됩니다. 가상 디스크는 동일한 호스트에서 또는 여러 호스트 간에 복사하거나 이동할 수 있습니다.

ESXi 호스트에서 실행되는 가상 시스템의 경우 가상 디스크 파일을 사용하는 대신 SAN LUN에 직접 가상 시스템 데이터를 저장할 수 있습니다. 이 옵션은 가상 시스템에서 스토리지 디바이스의 물리적 특성을 감지해야 하는 애플리케이션을 실행하는 경우에 유용합니다. 또한 SAN LUN을 매핑하면 기존 SAN 명령을 사용하여 디스크 스토리지를 관리할 수 있습니다.

LUN을 VMFS 볼륨에 매핑하면 vCenter Server 또는 ESXi 호스트에서 원시 LUN을 가리키는 RDM(원시 디바이스 매핑) 파일을 생성합니다. 디스크 정보를 파일로 캡슐화하면 vCenter Server 또는 ESXi 호스트에서 LUN을 잠글 수 있으므로 하나의 가상 시스템만 해당 LUN에 쓰기 작업을 수행할 수 있습니다. 이 파일은 .vmdk 확장명을 가지고 있지만 ESXi 시스템에 있는 LUN으로의 매핑을 나타내는 디스크 정보만 포함합니다. 실제 데이터는 LUN에 저장됩니다. 템플릿에서 가상 시스템을 배포할 수 없고 해당 데이터를 LUN에 저장할 수 없습니다. 이 데이터는 가상 디스크 파일에만 저장할 수 있습니다.

사용 가능한 데이터스토어 공간의 크기는 항상 변경됩니다. 가상 시스템 생성 작업과 스파스 파일, 스냅샷 등의 증가와 같은 다른 가상 시스템 작업에 필요한 공간이 충분히 남아 있는지 확인하십시오. 데이터스토어의 파일 형식별 공간 사용률을 검토하려면 "vSphere 모니터링 및 성능" 설명서를 참조하십시오.

씬 프로비저닝을 사용할 경우 처음 액세스할 때 할당되는 블록으로 스파스 파일을 생성할 수 있습니다. 이 경우 데이터스토어가 과다 프로비저닝될 수 있습니다. 스파스 파일은 계속해서 증가하여 데이터스토어를 가득 채우게 될 수 있습니다. 가상 시스템이 실행 중일 때 데이터스토어의 디스크 공간이 부족하게 되면 가상 시스템의 작동이 중지될 수 있습니다.

가상 디스크 프로비저닝 정책 정보

특정 가상 시스템 관리 작업을 수행할 때는 가상 디스크 파일에 대해 프로비저닝 정책을 지정할 수 있습니다. 가상 시스템 관리 작업에는 가상 디스크를 생성하거나, 가상 시스템을 템플릿으로 복제하거나, 가상 시스템을 마이그레이션하는 작업이 포함됩니다.

하드웨어 가속이 적용된 NFS 데이터스토어와 VMFS 데이터스토어는 다음 디스크 프로비저닝 정책을 지원합니다. 하드웨어 가속을 지원하지 않는 NFS 데이터스토어에서는 씬 형식만 사용할 수 있습니다.

Storage vMotion 또는 크로스 호스트 Storage vMotion을 사용하여 가상 디스크를 한 형식에서 다른 형식으로 변환할 수 있습니다.

느리게 비워지는 씬 프로비저닝

기본 씬 형식의 가상 디스크를 생성합니다. 가상 디스크에 필요한 공간은 해당 디스크를 생성할 때 할당됩니다. 물리적 디바이스에 남아 있는 데이터는 생성 시 지워지지 않지만, 나중에 가상 시스템에서 처음 쓸 때 필요시 비워집니다. 가상 시스템은 물리적 디바이스에서 오래된 데이터를 읽지 않습니다.

빠르게 비워지는 씬 프로비저닝

Fault Tolerance와 같은 클러스터 기능을 지원하는 씬 가상 디스크 유형입니다. 가상 디스크에 필요한 공간은 디스크 생성 시에 할당됩니다. 느리게 비워지는 씬 프로비저닝 형식과 다르게 물리적 디바이스에 남아 있는 데이터는 가상 디스크를 생성하는 동안 비워집니다. 다른 유형의 디스크보다 이 형식의 가상 디스크를 생성하는 것이 더 오래 걸릴 수도 있습니다. 빠르게 비워지는 씬 가상 디스크의 크기를 늘리면 가상 시스템에서 상당한 스텐 시간이 발생합니다.

씬 프로비저닝

스토리지 공간을 저장하려면 이 형식을 사용합니다. 씬 디스크의 경우 입력하는 가상 디스크 크기 값에 따라 디스크에 필요한 만큼의 데이터스토어 공간을 프로비저닝합니다. 그러나 씬 디스크는 먼저 작은 크기부터 시작합니다. 초기 작업을 위해 이 디스크에 필요한 데이터스토어 공간 만큼의 크기만 사용합니다. 씬 디스크가 나중에 더 많은 공간이 필요하면 최대 용량으로 커질 수 있으며 디스크를 해당 디스크에 프로비저닝된 전체 데이터스토어 공간을 차지할 수 있습니다.

씬 프로비저닝은 헤더 정보만을 사용하여 디스크를 생성하므로 가상 디스크를 생성하는 가장 빠른 방법입니다. 스토리지 블록을 할당하거나 비우지 않습니다. 처음 액세스할 때 스토리지 블록이 할당되고 비워집니다.

참고 가상 디스크가 Fault Tolerance와 같은 클러스터링 솔루션을 지원하는 경우, 씬 디스크로 만들지 마십시오.

VMware Host Client에서 가상 디스크 구성 변경

디스크 공간이 부족한 경우 디스크 크기를 늘릴 수 있습니다. 가상 시스템의 가상 디바이스에 대한 가상 디바이스 노드 및 지속성 모드를 변경할 수 있습니다.

사전 요구 사항

가상 시스템의 전원을 끕니다.

다음 권한이 있는지 확인합니다.

- 가상 시스템에 대한 **가상 시스템.구성.디바이스 설정 수정**.
- 가상 시스템에 대한 **가상 시스템.구성.가상 디스크 확장**.
- 데이터스토어에 대한 **데이터스토어.공간 할당**.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭에서 하드 디스크를 확장하여 모든 디스크 옵션을 표시합니다.
- 4 (선택 사항) 디스크 크기를 변경하려면 텍스트 상자에 새 값을 입력하고 드롭다운 메뉴에서 단위를 선택합니다.

- 5 (선택 사항) 디스크가 스냅샷의 영향을 받는 방식을 변경하려면 **디스크 모드** 드롭다운 메뉴에서 디스크 모드를 선택합니다.

옵션	설명
종속	종속 디스크는 스냅샷에 포함되어 있습니다.
독립-영구	지속성 모드의 디스크는 물리적 컴퓨터의 기존 디스크처럼 작동합니다. 지속성 모드의 디스크에 기록된 모든 데이터가 디스크에 영구적으로 기록됩니다.
독립-비영구	가상 시스템의 전원을 끄거나 가상 시스템을 재설정할 경우 비지속성 모드의 디스크에 대한 변경 내용이 무시됩니다. 비지속성 모드를 사용하면 언제나 동일한 상태의 가상 디스크로 가상 시스템을 다시 시작할 수 있습니다. 디스크에 대한 변경 내용은 가상 시스템의 전원을 끄거나 재설정할 때 삭제되는 재실행 로그 파일에 기록되거나 이 파일에서 읽어옵니다.

- 6 **저장**을 클릭합니다.

VMware Host Client에서 가상 시스템에 새로운 표준 하드 디스크 추가

가상 하드 디스크를 기존 가상 시스템에 추가하거나 가상 시스템 생성 프로세스 중 가상 시스템 하드웨어를 사용자 지정할 때 하드 디스크를 추가할 수 있습니다. 예를 들어 작업 로드가 많은 기존 가상 시스템에 추가 디스크 공간을 제공해야 할 수 있습니다. 가상 시스템이 생성되는 동안 부팅 디스크로 사전 구성된 하드 디스크를 추가할 수 있습니다.

사전 요구 사항

- 가상 하드 디스크를 추가하기 위한 구성 옵션 및 주의 사항을 숙지하고 있는지 확인합니다. [가상 디스크 구성](#)의 내용을 참조하십시오.
- 가상 시스템에 2TB보다 큰 용량의 디스크를 추가하려면 먼저 "vSphere 가상 시스템 관리" 항목을 참조하십시오.
- 대상 폴더 또는 데이터스토어에 대한 **가상 시스템.구성.새 디스크 추가** 권한이 있는지 확인합니다.

가상 시스템의 전원을 끕니다.

절차

- VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- (선택 사항) 기존 하드 디스크를 삭제하려면 디스크 위에 포인터를 놓고 **제거** 아이콘(X)을 클릭합니다. 디스크가 가상 시스템에서 제거됩니다. 다른 가상 시스템이 디스크를 공유하는 경우에는 디스크 파일이 삭제되지 않습니다.
- 가상 하드웨어** 탭에서 **하드 디스크 추가**를 선택하고 드롭다운 메뉴에서 **새 표준 하드 디스크**를 선택합니다. 하드 디스크가 가상 하드웨어 디바이스 목록에 나타납니다.
- 새 하드 디스크**를 확장합니다.

- 6 (선택 사항) 하드 디스크의 크기 값을 입력하고 드롭다운 메뉴에서 단위를 선택합니다.
- 7 가상 시스템 파일을 저장할 데이터스토어 위치를 선택합니다.
- 8 가상 시스템 디스크의 형식을 선택합니다.

옵션	설명
느리게 비워지는 싹 프로비저닝	기본 싹 형식인 가상 디스크를 만듭니다. 가상 디스크에 필요한 공간은 생성 중에 할당됩니다. 물리적 디바이스에 남아 있는 데이터는 생성 동안에 지워지지 않지만 나중에 가상 시스템에서 처음으로 쓰는 경우, 해당 데이터는 요구대로 비워집니다.
빠르게 비워지는 싹 프로비저닝	Fault Tolerance와 같은 클러스터링 기능을 지원하는 싹 디스크를 생성합니다. 가상 디스크에 필요한 공간은 디스크 생성 시에 할당됩니다. 플랫폼 형식과 대조하여 물리적 디바이스에 남아 있는 데이터는 생성하는 동안에 비워집니다. 다른 유형의 디스크를 만드는 것보다 이 포맷의 디스크를 만드는 것이 더 오래 걸릴 수도 있습니다.
씬 프로비저닝	씬 프로비저닝된 형식을 사용합니다. 맨 먼저 씬 프로비저닝된 디스크는 초기에 디스크가 필요한 데이터스토어 공간 만큼만 사용합니다. 씬 디스크가 나중에 더 많은 공간이 필요하면 할당할 수 있는 최대 용량으로 증가될 수 있습니다.

- 9 **공유** 드롭다운 메뉴에서 가상 디스크에 할당할 공유량의 값을 선택합니다.

공유량은 디스크 대역폭을 제어하기 위한 상대적인 메트릭을 나타내는 값입니다. 해당 값인 낮음, 보통, 높음 및 사용자 지정은 호스트의 모든 가상 시스템에 대한 모든 공유량의 합계와 비교됩니다.

- 10 **사용자 지정**을 선택한 경우 텍스트 상자에서 공유 숫자를 입력합니다.

- 11 **IOP 제한** 상자에서 가상 시스템에 할당되는 스토리지 리소스의 상한 값을 입력하거나 **제한 없음**을 선택합니다.

이 값은 가상 디스크에 할당된 초당 I/O 작업 수의 상한입니다.

- 12 기본값을 승인하거나 다른 가상 디바이스 노드를 선택합니다.

대부분의 경우에는 기본 디바이스 노드를 승인할 수 있습니다. 하드 디스크의 경우 기본 설정되지 않은 디바이스 노드를 사용하면 부팅 순서를 제어하거나 다른 SCSI 컨트롤러 유형을 갖는 것이 쉬워집니다. 예를 들어 LSI Logic 컨트롤러에서 부팅하여 버스 공유가 설정되어 있는 Buslogic 컨트롤러를 사용하는 다른 가상 시스템과 데이터 디스크를 공유하고자 할 수 있습니다.

- 13 (선택 사항) 디스크 모드를 선택합니다.

옵션	설명
종속	종속 디스크는 스냅샷에 포함되어 있습니다.
독립-영구	영구 모드의 디스크는 기존 물리적 컴퓨터 디스크처럼 작동합니다. 지속성 모드의 디스크에 기록된 모든 데이터가 디스크에 영구적으로 기록됩니다.
독립-비영구	가상 시스템의 전원을 끄거나 가상 시스템을 재설정할 경우 비지속성 모드의 디스크에 대한 변경 내용이 무시됩니다. 가상 시스템을 다시 시작할 때마다 가상 디스크가 동일한 상태로 되돌아갑니다. 디스크에 대한 변경 내용은 전원을 끄거나 재설정할 때 삭제되는 재실행 로그 파일에 기록되거나 읽혀집니다.

- 14 **저장**을 클릭합니다.

VMware Host Client에서 가상 시스템에 기존 하드 디스크 추가

가상 시스템 생성 프로세스 동안 또는 가상 시스템이 생성된 후 가상 시스템 하드웨어를 사용자 지정할 때 가상 시스템에 기존 가상 하드 디스크를 추가할 수 있습니다. 예를 들어 부팅 디스크로 사전 구성된 기존 하드 디스크를 추가할 수 있습니다.

가상 시스템을 생성하는 동안 기본적으로 사용자가 선택한 게스트 운영 체제를 기반으로 하드 디스크와 SCSI 또는 SATA 컨트롤러가 가상 시스템에 추가됩니다. 이 디스크가 사용자 요구 사항을 충족하지 않을 경우 생성 프로세스가 끝난 후에 디스크를 제거하고 기존 하드 디스크를 추가할 수 있습니다.

사전 요구 사항

- 컨트롤러 및 다른 가상 하드 디스크 구성에 대한 가상 디바이스 노드 동작을 숙지하고 있는지 확인합니다.
- 대상 폴더 또는 데이터스토어에 대한 **가상 시스템.구성.기존 디스크 추가** 권한이 있는지 확인합니다.

가상 시스템의 전원을 끕니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭에서 **하드 디스크 추가**를 선택하고 드롭다운 메뉴에서 **기존 하드 디스크**를 선택합니다.
- 4 (선택 사항) 기존 하드 디스크를 삭제하려면 디스크 위에 포인터를 놓고 **제거** 아이콘(X)을 클릭합니다.
디스크가 가상 시스템에서 제거됩니다. 다른 가상 시스템이 디스크를 공유하는 경우에는 디스크 파일이 삭제되지 않습니다.
- 5 데이터스토어 열에서 데이터스토어를 확장하고 가상 시스템 폴더를 선택하고 추가할 디스크를 선택합니다.
디스크 파일이 내용 열에 나타납니다. **파일 형식** 메뉴에는 이 디스크에 대한 호환 파일 형식이 표시됩니다.
- 6 **선택**을 클릭하고 **저장**을 클릭하여 기존 하드 디스크를 추가합니다.

Host Client에서 영구 메모리 디스크 추가

가상 하드 디스크를 기존 가상 시스템에 추가하거나 가상 시스템 생성 프로세스 중 가상 시스템 하드웨어를 사용자 지정할 때 하드 디스크를 추가할 수 있습니다. 예를 들어 작업 로드가 많은 기존 가상 시스템에 추가 디스크 공간을 제공해야 할 수 있습니다. 가상 시스템이 생성되는 동안 부팅 디스크로 사전 구성된 하드 디스크를 추가할 수 있습니다.

가상 시스템을 생성하는 동안 기본적으로 사용자가 선택한 게스트 운영 체제를 기반으로 하드 디스크와 SCSI 또는 SATA 컨트롤러가 가상 시스템에 추가됩니다. 이 디스크가 사용자 요구 사항을 충족하지 않을 경우 생성 프로세스가 끝난 후에 디스크를 제거하고 기존 하드 디스크를 추가할 수 있습니다.

사전 요구 사항

- 가상 하드 디스크를 추가하기 위한 구성 옵션 및 주의 사항을 숙지하고 있는지 확인합니다. [가상 디스크 구성](#)의 내용을 참조하십시오.

- 가상 시스템에 2TB보다 큰 용량의 디스크를 추가하려면 먼저 "vSphere 가상 시스템 관리" 항목을 참조하십시오.
- 대상 폴더 또는 데이터스토어에 대한 **가상 시스템.구성.새 디스크 추가** 권한이 있는지 확인합니다.

가상 시스템의 전원을 끕니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭에서 **하드 디스크 추가**를 선택하고 드롭다운 메뉴에서 **새 영구 메모리 디스크**를 선택합니다.
하드 디스크가 가상 하드웨어 디바이스 목록에 나타납니다. 기본적으로 디스크는 호스트-로컬 PMem 데이터스토어에 저장되며 데이터스토어를 변경할 수 없습니다.
- 4 (선택 사항) 새 하드 디스크에 대한 설정을 구성하고 **저장**을 클릭하여 마법사를 닫습니다.
 - a **새 하드 디스크**를 확장합니다.
 - b 하드 디스크의 크기 값을 입력하고 드롭다운 메뉴에서 단위를 선택합니다.

참고 가상 시스템에 추가된 모든 영구 메모리 하드 디스크와 NVDIMM 모듈은 동일한 PMem 리소스를 공유합니다. 따라서 호스트에서 사용 가능한 PMem 양에 따라 새로 추가되는 영구 메모리 디바이스의 크기를 조정해야 합니다. 구성 과정에서 주의가 필요한 경우 마법사에 경고 메시지가 나타납니다.

- c **공유** 드롭다운 메뉴에서 가상 디스크에 할당할 공유량의 값을 선택합니다.
공유량은 디스크 대역폭을 제어하기 위한 상대적인 메트릭을 나타내는 값입니다. 해당 값인 낮음, 보통, 높음 및 사용자 지정은 호스트의 모든 가상 시스템에 대한 모든 공유량의 합계와 비교됩니다.
- d **컨트롤러 위치** 드롭다운 메뉴에서 새 하드 디스크가 사용하는 컨트롤러의 위치를 선택합니다.
- e 디스크 모드를 선택합니다.

옵션	설명
종속	종속 디스크는 스냅샷에 포함되어 있습니다.
독립-영구	영구 모드의 디스크는 기존 물리적 컴퓨터 디스크처럼 작동합니다. 지속성 모드의 디스크에 기록된 모든 데이터가 디스크에 영구적으로 기록됩니다.
독립-비영구	가상 시스템의 전원을 끄거나 가상 시스템을 재설정할 경우 비지속성 모드의 디스크에 대한 변경 내용이 무시됩니다. 가상 시스템을 다시 시작할 때마다 가상 디스크가 동일한 상태로 되돌아갑니다. 디스크에 대한 변경 내용은 전원을 끄거나 재설정할 때 삭제되는 재실행 로그 파일에 기록되거나 잊혀집니다.

디스크 공유를 사용하여 VMware Host Client에서 가상 시스템에 우선 순위 부여

가상 시스템에 대한 디스크 리소스를 변경할 수 있습니다. 여러 가상 시스템이 동일한 VMFS 데이터스토어 및 동일한 LUN(논리 유닛 번호)에 액세스하는 경우 디스크 공유를 사용하여 리소스에 대한 가상 시스템의 액세스 우선

순위를 부여할 수 있습니다. 디스크 공유는 우선 순위가 높은 가상 시스템과 우선 순위가 낮은 가상 시스템을 구분합니다.

호스트의 I/O 대역폭을 가상 시스템의 가상 하드 디스크에 할당할 수 있습니다. 클러스터에서 디스크 I/O를 풀링할 수 없습니다.

공유 값은 모든 가상 시스템에 대한 디스크 대역폭을 제어하기 위한 상대적 메트릭을 나타냅니다.

디스크 공유는 지정된 호스트 내에서만 적용됩니다. 즉, 한 호스트의 가상 시스템에 할당된 공유는 다른 호스트의 가상 시스템에 적용되지 않습니다.

가상 시스템에 할당되는 스토리지 리소스에 대한 상한을 설정하는 IOP 제한을 선택할 수 있습니다. IOPS는 초당 I/O 작업 수입입니다.

사전 요구 사항

가상 시스템의 전원을 끕니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭에서 하드 디스크를 확장하여 디스크 옵션을 표시합니다.
- 4 **공유** 드롭다운 메뉴에서 가상 시스템에 할당하는 공유 값을 선택합니다.
- 5 **사용자 지정**을 선택한 경우 텍스트 상자에서 공유 숫자를 입력합니다.
- 6 **제한- IOPS** 텍스트 상자에서 가상 시스템에 할당되는 스토리지 리소스의 상한을 입력하거나 **제한 없음**을 선택합니다.
- 7 **저장**을 클릭합니다.

VMware Host Client에서 가상 시스템 컨트롤러 구성

VMware Host Client에서 USB 컨트롤러, SCSI 컨트롤러, 반가상화 SCSI 컨트롤러 및 SATA 컨트롤러와 같은 다양한 컨트롤러를 가상 시스템에 추가할 수 있습니다. 또한 SCSI 버스 공유 구성 및 SCSI 컨트롤러 유형을 변경할 수 있습니다.

USB 컨트롤러를 가상 시스템에 추가

가상 시스템에 USB 컨트롤러를 추가하여 ESXi호스트 또는 클라이언트 컴퓨터에서 가상 시스템으로의 USB 패스 스루를 지원할 수 있습니다.

vSphere Client에서 xHCI 컨트롤러 하나와 EHCI+UHCI 컨트롤러 하나를 추가할 수 있습니다.

- 하드웨어 버전 11에서 하드웨어 버전 16까지는 xHCI 컨트롤러마다 지원되는 루트 허브 포트의 수는 8개입니다(로컬 USB 3.1 SuperSpeed 포트 4개와 논리적 USB 2.0 포트 4개).

- 하드웨어 버전 17부터 하드웨어 버전 20까지 xHCI 컨트롤러당 지원되는 루트 허브 포트의 수는 8개입니다 (로컬 USB 3.1 SuperSpeedPlus 포트 4개와 논리적 USB 2.0 포트 4개).
- 하드웨어 버전 21의 경우 xHCI 컨트롤러당 지원되는 루트 허브 포트의 수는 8개입니다(로컬 USB 3.2 Gen 2x2 포트 4개와 논리적 USB 2.0 포트 4개).

컨트롤러 추가 조건은 디바이스 버전, 패스루 유형(호스트 또는 클라이언트 컴퓨터) 및 게스트 운영 체제에 따라 달라집니다.

표 4-2. USB 컨트롤러 지원

컨트롤러 유형	지원되는 USB 디바이스 버전	ESXi 호스트에서 VM으로의 패스루를 위해 지원됨	클라이언트 컴퓨터에서 VM으로의 패스루를 위해 지원됨
EHCI+UHCI	2.0	예	예
xHCI	3.2, 3.1, 2.0	예 USB 3.2, 3.1 및 2.0	예 Windows 8 이상, Windows Server 2012 이상 또는 2.6.35 이상의 커널이 있는 Linux 게스트 운영 체제가 있어야 합니다.

Mac OS X 시스템의 경우 EHCI+UHCI 컨트롤러가 기본적으로 사용되며 이 컨트롤러는 USB 마우스와 키보드에 액세스하는 데 필요합니다.

Windows 또는 Linux 게스트 운영 체제를 사용하는 가상 시스템에서는 서로 다른 유형의 컨트롤러를 한 개 또는 두 개 추가할 수 있습니다. 동일한 유형의 두 컨트롤러를 추가할 수는 없습니다.

ESXi 호스트에서 가상 시스템으로의 USB 패스루의 경우 USB 중재자가 최대 15개의 USB 컨트롤러를 모니터링할 수 있습니다. 시스템에 있는 컨트롤러가 15개를 초과하는 경우 여기에 USB 디바이스를 연결하면 가상 시스템에서 해당 디바이스를 사용할 수 없습니다.

사전 요구 사항

- ESXi 호스트에 USB 3.1, 2.0 및 1.1 디바이스를 지원하는 USB 컨트롤러 하드웨어와 모듈이 있는지 확인합니다.
- 클라이언트 컴퓨터에 USB 3.2, 2.0 및 3.1 디바이스를 지원하는 USB 컨트롤러 하드웨어 및 모듈이 있는지 확인합니다.
- Linux 게스트 운영 체제에서 xHCI 컨트롤러를 사용하려면 Linux 커널 버전이 2.6.35 이상인지 확인합니다.
- 가상 시스템의 전원이 켜졌는지 확인합니다.
- 필요한 권한(ESXi 호스트 패스루): **가상 시스템.구성.디바이스 추가 또는 제거**.

절차

- 1 vSphere 인벤토리에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
- 2 **가상 하드웨어** 탭에서 **새 디바이스 추가**를 클릭하고 드롭다운 메뉴에서 **USB 컨트롤러**를 선택합니다.
해당 컨트롤러가 **가상 하드웨어** 디바이스 목록에 나타납니다.

3 USB 컨트롤러 유형을 변경하려면 **새 USB 컨트롤러**를 확장합니다.

호환성 오류가 나타날 경우 컨트롤러를 추가하기 전에 먼저 오류를 수정해야 합니다.

4 **확인**을 클릭합니다.

다음에 수행할 작업

하나 이상의 USB 디바이스를 가상 시스템에 추가합니다.

VMware Host Client에서 SCSI 컨트롤러 추가

사용되지 않는 SCSI 버스 번호에 하드 디스크를 추가하여 기존 가상 시스템에 SCSI 컨트롤러를 추가할 수 있습니다.

사용되지 않는 SCSI 버스 번호에 새 하드 디스크를 추가하면 새 SCSI 컨트롤러가 생성됩니다.

사전 요구 사항

가상 시스템의 전원을 끕니다.

절차

1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.

2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.

3 **가상 하드웨어** 탭에서 **하드 디스크 추가**를 선택하고 드롭다운 메뉴에서 **새 하드 디스크**를 선택합니다.

4 하드 디스크를 확장하여 모든 옵션을 표시합니다.

5 **컨트롤러 위치** 섹션의 드롭다운 메뉴에서 사용되지 않는 SCSI 버스 번호를 선택합니다.

예를 들어, 버스 및 디바이스 번호 0:0 - 0:15는 초기 SCSI 컨트롤러에서 사용됩니다. 두 번째 SCSI 컨트롤러는 버스 및 디바이스 번호 1:0 - 1:15를 사용합니다.

6 **저장**을 클릭합니다.

결과

새 하드 디스크와 새 SCSI 컨트롤러가 동시에 생성됩니다.

VMware Host Client에서 SCSI 버스 공유 구성 변경

가상 시스템의 SCSI 버스 공유 유형을 설정하고 SCSI 버스를 공유할지 여부를 나타낼 수 있습니다. 공유 유형에 따라서 가상 시스템은 동일한 서버나 임의 서버의 동일한 가상 디스크에 동시에 액세스할 수 있습니다.

가상 시스템이 ESXi 호스트에 있는 경우에만 가상 시스템의 SCSI 컨트롤러 구성을 변경할 수 있습니다.

사전 요구 사항

가상 시스템의 전원을 끕니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭에서 편집하려는 SCSI 컨트롤러를 확장합니다.
- 4 **SCSI 버스 공유** 목록에서 공유 유형을 선택합니다.

옵션	설명
없음	가상 디스크는 다른 가상 시스템에서 공유할 수 없습니다.
가상	가상 디스크는 동일한 서버의 가상 시스템에서 공유할 수 있습니다.
물리적	가상 디스크는 임의 서버의 가상 시스템에서 공유할 수 있습니다.

- 5 **저장**을 클릭합니다.

VMware Host Client에서 SCSI 컨트롤러 유형 변경

가상 시스템에서 가상 SCSI 컨트롤러를 구성하여 가상 디스크 및 RDM을 가상 시스템에 연결할 수 있습니다.

SCSI 컨트롤러 선택은 가상 디스크가 IDE인지 SCSI 디스크인지 여부에 영향을 받지 않습니다. IDE 어댑터는 항상 ATAPI입니다. 게스트 운영 체제의 기본값은 이미 선택되어 있습니다. 구형 게스트 운영 체제의 기본 컨트롤러는 BusLogic 어댑터입니다.

LSI Logic 가상 시스템을 만들고 BusLogic 어댑터를 사용하는 가상 디스크를 추가하는 경우에는 가상 시스템이 BusLogic 어댑터 디스크에서 부팅됩니다. LSI Logic SAS는 하드웨어 버전 7 이상을 사용하는 가상 시스템에만 사용할 수 있습니다. 스냅샷이 있는 디스크는 LSI Logic SAS, VMware 반가상화 및 LSI Logic 병렬 어댑터를 사용하는 경우 성능 향상 효과를 보지 못할 수 있습니다.

경고 SCSI 컨트롤러 유형을 변경하면 가상 시스템을 부팅할 때 오류가 생길 수 있습니다.

사전 요구 사항

가상 시스템의 전원을 끕니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭을 클릭하고 SCSI 컨트롤러를 확장합니다.
- 4 드롭다운 메뉴에서 SCSI 컨트롤러 유형을 선택합니다.
- 5 **저장**을 클릭합니다.

VMware 반가상화 SCSI 컨트롤러 정보

VMware 반가상화 SCSI 컨트롤러는 처리량을 높이고 CPU 사용량은 낮출 수 있는 고성능 스토리지 컨트롤러입니다. 이러한 컨트롤러는 고성능 스토리지 환경에 적합합니다.

VMware 반가상화 SCSI 컨트롤러는 ESXi 4.x 이상의 가상 시스템과 호환됩니다. 이러한 컨트롤러의 디스크에 스냅샷이 있거나 ESXi 호스트의 메모리가 오버 커밋된 경우 이 디스크는 최적의 성능을 얻지 못할 수 있습니다. 이러한 동작으로 인해 기타 SCSI 컨트롤러 옵션에 비해 VMware 반가상화 SCSI 컨트롤러를 사용하여 얻는 전체적인 성능 향상 효과가 완화되지는 않습니다.

VMware 반가상화 SCSI 컨트롤러의 플랫폼 지원에 대해서는 "VMware 호환성 가이드" (<http://www.vmware.com/resources/compatibility>)를 참조하십시오.

VMware Host Client에서 반가상화 SCSI 컨트롤러 추가

처리량을 높이고 CPU 활용도를 낮출 수 있도록 VMware 반가상화 SCSI 고성능 스토리지 컨트롤러를 추가할 수 있습니다.

VMware 반가상화 SCSI 컨트롤러는 특히 I/O를 많이 사용하는 애플리케이션을 실행하는 SAN 환경에 적합합니다.

사전 요구 사항

- 가상 시스템이 게스트 운영 체제를 가지고 있고 VMware Tools가 설치되었는지 확인합니다.
- 가상 시스템이 하드웨어 버전 7 이상을 사용하고 있는지 확인합니다.
- VMware 반가상화 SCSI 제한 사항을 숙지합니다. "vSphere 가상 시스템 관리"의 내용을 참조하십시오.
- VMware 반가상화 SCSI 컨트롤러에 연결되어 있는 부팅 디스크 디바이스에 액세스하려면 가상 시스템이 Windows 2003 또는 Windows 2008 게스트 운영 체제를 사용하고 있는지 확인합니다.
- 일부 운영 체제에서는 컨트롤러 유형을 변경하기 전에 LSI Logic 컨트롤러가 있는 가상 시스템을 생성하고 VMware Tools를 설치해야 합니다.

가상 시스템의 전원을 끕니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭에서 **기타 디바이스 추가**를 클릭하고 드롭다운 메뉴에서 **SCSI 컨트롤러**를 선택합니다.
하드웨어 목록에 새 SCSI 컨트롤러가 나타납니다.
- 4 **새 SCSI 컨트롤러**를 클릭하고 드롭다운 메뉴에서 **VMware 반가상화**를 선택합니다.
- 5 **저장**을 클릭합니다.

VMware Host Client에서 가상 시스템에 SATA 컨트롤러 추가

가상 시스템에 여러 개의 하드 디스크나 CD/DVD-ROM 디바이스가 있는 경우 최대 세 개의 SATA 컨트롤러를 추가하여 디바이스를 할당할 수 있습니다. 디바이스를 여러 컨트롤러에 할당하면 성능을 향상시키고 데이터 트래픽 정체를 방지할 수 있습니다. 또한 디바이스가 한 컨트롤러에 사용할 수 있는 한도인 30개를 초과해야 하는 경우 컨트롤러를 추가할 수도 있습니다.

대용량 가상 하드 디스크를 사용하려는 경우 SATA 컨트롤러에서 가상 시스템을 부팅하여 사용할 수 있습니다.

일부 게스트 운영 체제에서는 AHCI SATA 컨트롤러를 지원하지 않습니다. 일반적으로 ESXi 5.5 이상과 호환되며 Mac OS X 게스트 운영 체제를 사용하는 가상 시스템을 생성할 때는 기본적으로 가상 하드 디스크 및 CD/DVD-ROM 디바이스에 대한 SATA 컨트롤러가 추가됩니다. Windows Vista 이상을 비롯한 대부분의 게스트 운영 체제에는 CD/DVD-ROM 디바이스용 기본 SATA 컨트롤러가 있습니다. 확인하려면 <http://www.vmware.com/resources/compatibility>에서 적절한 "VMware 호환성 가이드" 를 참조하십시오.

사전 요구 사항

- 가상 시스템이 ESXi 5.5 이상과 호환되는지 확인합니다.
- 스토리지 컨트롤러의 동작 및 제한 사항을 숙지하고 있는지 확인합니다. "vSphere 가상 시스템 관리" 를 참조하십시오.
- 가상 시스템에 대한 **가상 시스템.구성.디바이스 추가 또는 제거** 권한이 있는지 확인합니다.
- 가상 시스템의 전원을 끕니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭에서 **기타 디바이스 추가**를 선택하고 드롭다운 메뉴에서 **SATA 컨트롤러**를 선택합니다.
하드웨어 목록에 SATA 컨트롤러가 나타납니다.
- 4 **저장**을 클릭합니다.

VMware Host Client에서 NVMe 컨트롤러 추가

가상 시스템에 여러 하드 디스크가 있는 경우 디스크를 할당할 최대 네 개의 가상 NVMe 컨트롤러를 추가할 수 있습니다. NVMe 컨트롤러를 사용하면 AHCI SATA 또는 SCSI 컨트롤러와 비교하여 게스트 운영 체제 I/O 처리에 대한 소프트웨어 오버헤드가 상당히 줄어듭니다.

NVMe 컨트롤러는 플래시 전용 디스크 어레이, 로컬 NVMe SSD 및 PMem 스토리지의 가상 디스크에서 최상의 성능을 제공합니다.

사전 요구 사항

- 가상 시스템에 NVMe를 지원하는 게스트 운영 체제가 있는지 확인합니다.
- 가상 시스템 호환성이 ESXi 6.5 이상인지 확인합니다.

- 스토리지 컨트롤러의 동작 및 제한 사항을 숙지하고 있는지 확인합니다. 자세한 내용은 "가상 시스템 관리" 가이드를 참조하십시오.
- 가상 시스템에 대한 **가상 시스템.구성.새 디스크 추가** 권한이 있는지 확인합니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭에서 **기타 디바이스 추가** 아이콘을 클릭하고 드롭다운 메뉴에서 **NVMe 컨트롤러**를 선택합니다.

결과

새 NVMe 컨트롤러가 가상 시스템에 추가됩니다.

다음에 수행할 작업

가상 시스템에 하드 디스크를 추가하고 이를 NVMe 컨트롤러에 할당할 수 있습니다.

VMware Host Client에서 기타 가상 시스템 디바이스 구성

가상 시스템 CPU 및 메모리를 구성하고 하드 디스크 및 가상 네트워크 어댑터를 추가하는 것 외에도 DVD/CD-ROM 드라이브, 플로피 드라이브 및 SCSI 디바이스 등 가상 하드웨어를 추가 및 구성할 수도 있습니다. VVDT(가상 감시 타이머) 디바이스, 정밀 클럭 디바이스 및 PCI 디바이스를 추가할 수도 있습니다.

VMware Host Client에서 가상 시스템에 CD 또는 DVD 드라이브 추가

클라이언트 또는 호스트에서 물리적 드라이브를 사용하거나 ISO 이미지를 사용하여 CD/DVD 드라이브를 가상 시스템에 추가할 수 있습니다.

호스트의 USB CD/DVD 드라이브를 사용하여 백업되는 CD/DVD 드라이브를 추가하려는 경우에는 해당 드라이브를 SCSI 디바이스로 추가해야 합니다. ESXi 호스트에서 SCSI 디바이스를 무중단 추가 또는 제거하는 기능은 지원되지 않습니다.

사전 요구 사항

가상 시스템의 전원을 끕니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭에서 **기타 디바이스 추가**를 선택하고 드롭다운 메뉴에서 **CD/DVD 드라이브**를 선택합니다.

4 CD/DVD 드라이브를 확장하고 옵션을 선택합니다.

옵션	설명
물리적 드라이브 사용	a 위치로 클라이언트 디바이스 를 선택합니다. b 디바이스 모드 드롭다운 메뉴에서 CD-ROM 에뮬레이션 또는 CD-ROM 패스스루 를 선택합니다.
ISO 이미지 사용	a 위치로 데이터스토어 ISO 파일 을 선택합니다. b 이미지 파일의 경로와 파일 이름을 입력하거나 찾아보기 를 클릭하여 파일을 찾습니다.

5 가상 시스템을 시작할 때 CD-ROM 드라이브를 연결하지 않으려면 **전원을 켤 때 연결**의 선택을 취소합니다.

6 가상 시스템에서 드라이브가 사용하는 가상 디바이스 노드를 선택합니다.

7 **저장**을 클릭합니다.

플로피 드라이브를 VMware Host Client 내 가상 시스템에 추가

플로피 드라이브를 가상 시스템에 추가하려면 물리적 플로피 드라이브나 플로피 이미지를 사용합니다.

ESXi는 호스트의 물리적 플로피 드라이브를 사용하여 백업되는 플로피 드라이브를 지원하지 않습니다.

사전 요구 사항

- 가상 시스템의 전원을 끕니다.
- 가상 시스템에 대한 **가상 시스템.구성.디바이스 추가 또는 제거** 권한이 있는지 확인합니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭에서 **기타 디바이스 추가**를 선택하고 드롭다운 메뉴에서 **플로피 드라이브**를 선택합니다.
하드웨어 목록에 플로피 드라이브가 나타납니다.
- 4 **플로피 드라이브**를 확장하고 사용하려는 디바이스 유형을 선택합니다.

옵션	설명
클라이언트 디바이스	이 옵션을 선택하여 플로피 디바이스를 VMware Host Client에 액세스하는 시스템의 물리적 플로피 디바이스 또는 .flp 플로피 이미지에 연결합니다.
기존 플로피 이미지 사용	a 이 옵션을 선택하여 가상 디바이스를 호스트에 액세스할 수 있는 데이터스토어의 기존 플로피 드라이브 이미지에 연결합니다. b 찾아보기 를 클릭하고 플로피 이미지를 선택합니다.

5 (선택 사항) 가상 시스템의 전원이 켜질 때 디바이스를 연결하도록 구성하려면 **전원을 켤 때 연결**을 선택합니다.

6 **저장**을 클릭합니다.

VMware Host Client에서 가상 시스템에 USB 디바이스 추가

VMware Host Client를 사용하여 가상 시스템에 USB 디바이스를 추가할 수 있습니다.

사전 요구 사항

- USB 컨트롤러가 있는지 확인합니다. [USB 컨트롤러를 가상 시스템에 추가](#)의 내용을 참조하십시오.
- USB 디바이스를 가상 시스템이 위치한 ESXi 호스트에 꽂아 해당 호스트에 물리적 USB 디바이스를 추가합니다.

참고 ESXi 호스트에 사용 가능한 USB 디바이스가 없으면 USB 디바이스를 가상 시스템에 추가할 수 없습니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭에서 **기타 디바이스 추가**를 선택하고 드롭다운 메뉴에서 **USB 디바이스**를 선택합니다.
USB 디바이스가 가상 시스템에 사용 가능한 하드웨어 디바이스의 하드웨어 목록에 나타납니다.
- 4 **USB 디바이스** 드롭다운에서 가상 시스템에 추가할 USB 디바이스를 선택합니다.
- 5 **저장**을 클릭합니다.

VMware Host Client에서 가상 시스템에 사운드 컨트롤러 추가

VMware Host Client를 사용하여 가상 시스템에 사운드 컨트롤러를 추가할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭에서 **기타 디바이스 추가**를 선택하고 드롭다운 메뉴에서 **사운드 컨트롤러**를 선택합니다.



사운드 컨트롤러가 가상 시스템에 사용할 수 있는 하드웨어 디바이스 목록에 나타납니다.

- 4 **사운드 카드** 드롭다운 메뉴에서 가상 시스템에 연결할 사운드 컨트롤러를 선택합니다.
- 5 **저장**을 클릭합니다.

VMware Host Client에서 병렬 및 직렬 포트 구성

병렬 및 직렬 포트는 주변 디바이스를 가상 시스템에 연결하기 위한 인터페이스입니다. 가상 직렬 포트는 물리적 직렬 포트 또는 호스트 컴퓨터의 파일에 연결할 수 있습니다.

또한 가상 직렬 포트를 사용하여 두 가상 시스템 간에 직접 연결을 설정하거나 호스트 컴퓨터의 애플리케이션과 가상 시스템 간 연결을 설정할 수도 있습니다. 병렬 및 직렬 포트를 추가하고 직렬 포트 구성을 변경할 수 있습니다.

VMware Host Client에서 가상 시스템에 직렬 포트 추가

가상 시스템에서는 최대 4개의 가상 직렬 포트를 사용할 수 있습니다. 가상 직렬 포트는 호스트 컴퓨터의 파일 또는 물리적 직렬 포트에 연결할 수 있습니다. 호스트 측 명명된 파이프를 사용하여 두 가상 시스템 간 직접 연결을 설정하거나 가상 시스템과 호스트 컴퓨터의 애플리케이션 간 연결을 설정할 수도 있습니다. 또한 포트나 vSPC(가상 직렬 포트 집중 장치) URI를 사용하여 네트워크를 통해 직렬 포트에 연결할 수 있습니다.

사전 요구 사항

- 포트가 액세스할 수 있는 여러 미디어 유형, vSPC 연결 및 적용될 수 있는 조건을 숙지합니다. "vSphere 가상 시스템 관리" 를 참조하십시오.
- 네트워크를 통해 직렬 포트를 연결하려면, 방화벽 규칙 집합을 추가하십시오. "vSphere 가상 시스템 관리" 를 참조하십시오.

- 필요한 권한: **가상 시스템.구성.디바이스 추가 또는 제거**

가상 시스템의 전원을 끕니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭에서 **기타 디바이스 추가**를 선택하고 **직렬 포트**를 선택합니다.
하드웨어 목록에 직렬 포트가 나타납니다.
- 4 하드웨어 목록에서 직렬 포트를 확장하고 액세스할 미디어 포트 유형을 선택합니다.

옵션	설명
출력 파일 사용	호스트에서 가상 직렬 포트의 출력을 저장할 파일 위치를 찾아봅니다.
물리적 직렬 포트 사용	드롭다운 메뉴에서 포트를 선택합니다.
이름이 지정된 파이프 사용	<ol style="list-style-type: none"> a 파이프 이름 필드에 파이프 이름을 입력합니다. b 드롭다운 메뉴에서 파이프의 근단 및 원단을 선택합니다.
네트워크 사용	<ol style="list-style-type: none"> a 방향 드롭다운 메뉴에서 서버 또는 클라이언트를 선택합니다. b 포트 URI를 입력합니다. 이 URI는 가상 시스템의 직렬 포트를 연결해야 하는 직렬 포트의 원단입니다. c vSPC가 단일 IP 주소를 통해 모든 가상 시스템을 액세스하는 중간 단계로 사용되면 가상 직렬 포트 집중 장치 사용을 선택하고 vSPC URI 위치를 입력합니다.

- 5 (선택 사항) 가상 시스템의 전원을 켜 때 병렬 포트 디바이스를 연결하지 않으려면 **전원을 켜 때 연결**의 선택을 취소합니다.
- 6 **저장**을 클릭합니다.

예제: 인증 매개 변수 없이 클라이언트 또는 서버에 대한 직렬 포트 네트워크 연결 설정

vSPC를 사용하지 않고 가상 시스템을 telnet://:12345 URI를 사용하는 서버로 연결된 직렬 포트 구성할 경우 Linux 또는 Windows 운영 체제에서 가상 시스템의 직렬 포트에 연결할 수 있습니다.

```
telnet yourESXiServerIPAddress 12345
```

마찬가지로, 포트 23(telnet://yourLinuxBox:23)을 통해 Linux 시스템에서 텔넷 서버를 실행하는 경우에는 가상 시스템을 클라이언트 URI로 구성할 수 있습니다.

```
telnet://yourLinuxBox:23
```

가상 시스템이 포트 23에서 Linux 시스템에 대한 연결을 시작합니다.

VMware Host Client에서 가상 시스템에 병렬 포트 추가

가상 시스템에 프린터 및 스캐너 같은 주변 디바이스를 연결하려면 병렬 포트를 사용할 수 있습니다. 이러한 디바이스의 출력은 호스트 컴퓨터의 파일로 보내게 됩니다.

참고 ESXi 4.1 이하의 호스트에서 실행되는 가상 시스템에 병렬 포트를 추가하려면 출력을 호스트의 물리적 병렬 포트에 보내도록 선택할 수도 있습니다. ESXi 5.0 이상의 호스트 버전에서는 이 옵션을 사용할 수 없습니다.

사전 요구 사항

- 가상 시스템의 전원을 끕니다.
- 가상 시스템에 대한 **가상 시스템.구성.디바이스 추가 또는 제거** 권한이 있는지 확인합니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭에서 **기타 디바이스 추가**를 선택하고 **병렬 포트**를 선택합니다.
하드웨어 목록에 병렬 포트가 나타납니다.
- 4 병렬 포트를 확장하고 [연결] 필드에서 파일을 생성할 폴더를 찾습니다.
파일 경로가 **연결** 텍스트 상자에 나타납니다.
- 5 (선택 사항) 가상 시스템의 전원이 켜질 때 디바이스를 연결하도록 구성하려면 **전원을 켜 때 연결**을 선택합니다.
- 6 **저장**을 클릭합니다.

가상 시스템에 가상 감시 타이머 디바이스를 추가하는 방법

가상 시스템 내에서 시스템 성능과 관련된 자체 의존도를 보장하기 위해 VWDT(가상 감시 타이머) 디바이스를 추가할 수 있습니다.

게스트 운영 체제가 응답을 중지하고 소프트웨어 결함이나 오류로 인해 자체적으로 복구할 수 없는 경우, VWDT가 미리 정의된 시간 동안 대기한 후 시스템을 다시 시작합니다.

게스트 운영 체제 또는 BIOS나 EFI 펌웨어에서 시작하도록 VWDT를 설정할 수 있습니다. BIOS 또는 EFI 펌웨어에서 VWDT를 시작하도록 선택할 경우 VWDT는 게스트 운영 체제가 부팅되기 전에 시작됩니다.

VWDT는 각 가상 시스템이 실패할 경우 자체 복구가 가능한 게스트 기반 클러스터링 솔루션에서 중요한 역할을 합니다.

VMware Host Client에서 가상 시스템에 가상 감시 타이머 디바이스 추가

가상 시스템에 가상 감시 타이머 디바이스를 추가하여 가상 시스템에서 긴 시간 동안 게스트 운영 체제 장애가 발생하는 것을 방지할 수 있습니다.

사전 요구 사항

- 가상 시스템의 전원을 끕니다.
- 가상 시스템에 대해 **가상 시스템.구성.디바이스 추가 또는 제거** 권한이 있는지 확인합니다.
- 가상 시스템의 게스트 운영 체제가 VWDT 디바이스를 지원하는지 확인합니다.
- 가상 하드웨어가 버전 17인지 확인합니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭에서 **기타 디바이스 추가**를 선택하고 **감시 타이머**를 클릭합니다.
감시 타이머 디바이스가 하드웨어 목록에 나타납니다.
- 4 (선택 사항) BIOS 또는 EFI 펌웨어를 사용하여 감시 타이머를 시작하려면 **BIOS/EFI 부팅으로 시작**을 선택합니다.
이 옵션을 선택하면 VWDT 디바이스가 게스트 운영 체제보다 먼저 시작됩니다. 게스트 운영 체제 부팅이 너무 오래 걸리거나 감시 타이머가 지원되지 않는 경우, 디바이스가 가상 시스템을 계속 다시 시작할 수 있습니다.
- 5 **저장**을 클릭합니다.

VMware Host Client에서 가상 시스템에 정밀 클럭 디바이스 추가

정밀 클럭은 가상 시스템에서 실행되고 호스트의 시스템 시간에 액세스하는 가상 디바이스입니다. 가상 시스템에 정밀 클럭을 추가하면 시간 동기화 및 고정밀 타임스탬프가 보장됩니다.

사전 요구 사항

- 가상 시스템의 전원을 끕니다.
- 가상 하드웨어가 버전 17인지 확인합니다.
- 가상 시스템에 대해 **가상 시스템.구성.디바이스 추가 또는 제거** 권한이 있는지 확인합니다.
- 가상 시스템에 대해 **가상 시스템.구성.디바이스 설정 수정** 권한이 있는지 확인합니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭에서 **기타 디바이스 추가**를 클릭하고 **정밀 클릭**을 선택합니다.
정밀 클릭 디바이스가 하드웨어 목록에 나타납니다.
- 4 (선택 사항) 시간 동기화 프로토콜을 선택합니다.
- 5 **저장**을 클릭합니다.

VMware Host Client에서 가상 시스템에 PCI 디바이스 추가

DirectPath I/O를 사용하면 가상 시스템의 게스트 운영 체제가 호스트에 직접 연결된 물리적 PCI 및 PCIe 디바이스에 액세스할 수 있습니다. 이 기술을 사용하면 각 가상 시스템을 최대 16개의 물리적 PCI 디바이스에 연결할 수 있습니다.

동적 DirectPath I/O를 사용하여 가상 시스템에 여러 개의 PCI 패스스루 디바이스를 할당할 수 있습니다. vSphere 7.0부터는 벤더 및 모델 이름으로 PCI 패스스루 디바이스를 식별할 수 있습니다.

참고 가상 시스템에 PCI 또는 PCIe 패스스루 디바이스를 추가하면 일부 가상 시스템 작업을 사용할 수 없게 됩니다.

하드웨어 레이블 구성에 대한 자세한 내용은 [VMware Host Client에서 하드웨어 레이블 변경](#)에서 참조하십시오.

사전 요구 사항

- 가상 시스템의 전원을 끕니다.
- 가상 시스템에 대해 **가상 시스템.구성.디바이스 추가 또는 제거** 권한이 있는지 확인합니다.
- PCI 디바이스가 호스트에 연결되어 있고 사용 가능한 패스스루 연결로 표시되어 있는지 확인합니다.
- 가상 시스템에 동적 PCI 디바이스를 추가하려면 가상 하드웨어 버전이 17인지 확인합니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.

3 가상 하드웨어 탭에서 기타 디바이스 추가를 클릭하고 디바이스를 선택합니다.

옵션	작업
PCI 디바이스	<p>a PCI 디바이스를 클릭합니다.</p> <p>새 디바이스가 하드웨어 목록에 나타납니다.</p> <p>b 드롭다운 메뉴에서 가상 시스템에 연결할 PCI 디바이스를 선택합니다.</p>
동적 PCI 디바이스	<p>a 동적 PCI 디바이스를 클릭합니다.</p> <p>새 디바이스가 하드웨어 목록에 나타납니다.</p> <p>b 새 PCI 디바이스를 확장하고 드롭다운 메뉴에서 가상 시스템에 연결할 PCI 패스스루 디바이스를 선택합니다.</p> <p>PCI 패스스루 디바이스는 벤더, 모델 이름 및 하드웨어 레이블로 식별할 수 있습니다. 하드웨어 레이블이 있으면 괄호 안에 표시됩니다.</p> <p>참고 가상 시스템에 PCI 디바이스를 추가하면 가상 시스템의 전체 메모리 크기가 자동으로 예약됩니다.</p>

4 저장을 클릭합니다.

VMware Host Client에서 가상 시스템 보호

가상 시스템에서 실행되는 게스트 운영 체제에는 물리적 시스템과 동일한 보안 위험이 따릅니다.

가상 환경의 보안을 향상시키기 위해 ESXi 호스트에 vTPM(신뢰할 수 있는 가상 플랫폼 모듈)을 추가할 수 있습니다. 또한 최신 Windows 10 및 Windows Server 2016 운영 체제를 실행하는 가상 시스템에 VBS(가상화 기반 보안)를 사용하도록 설정할 수 있습니다. 가상 시스템에 대해 vSGX(Virtual Intel® Software Guard Extensions)를 사용하여 워크로드에 추가적인 보안을 제공할 수 있습니다.

VMware Host Client의 가상 시스템에서 vSGX 활성화

Enclave 콘텐츠가 공개 및 수정되는 것을 방지하려면 VMware Host Client의 가상 시스템에서 vSGX를 활성화하면 됩니다.

vSGX를 사용하여 가상 시스템 보호

vSphere에서 가상 시스템에 대해 vSGX를 구성할 수 있습니다. 일부 최신 Intel CPU는 Intel® SGX(Intel® Software Guard Extension)라고 하는 보안 확장을 구현합니다. Intel SGX를 사용하면 사용자 수준 코드에서 Enclave라고 하는 메모리의 개인 영역을 정의할 수 있습니다. Intel SGX는 공개 또는 수정으로부터 Enclave 콘텐츠를 보호하여 Enclave 외부에서 실행되는 코드가 Enclave 콘텐츠에 액세스할 수 없도록 합니다.

가상 시스템은 하드웨어에서 사용할 수 있는 경우 vSGX를 통해 Intel SGX 기술을 사용할 수 있습니다. vSGX를 사용하려면 SGX 지원 CPU에 ESXi 호스트를 설치해야 하며 ESXi 호스트의 BIOS에서 SGX를 사용하도록 설정해야 합니다. vSphere Client를 사용하여 가상 시스템에 대해 SGX를 사용하도록 설정할 수 있습니다. 자세한 내용은 "vSphere 보안" 설명서를 참조하십시오.

일부 작업 및 기능은 SGX와 호환되지 않습니다.

- Storage vMotion을 사용한 마이그레이션
- 가상 시스템 일시 중단 또는 재개
- 가상 시스템의 스냅샷 생성
- Fault Tolerance
- GI(게스트 무결성, VMware AppDefense 1.0의 플랫폼 기반) 사용

사전 요구 사항

- 가상 시스템의 전원을 끕니다.
- 가상 시스템에서 EFI 펌웨어를 사용하는지 확인합니다.
- ESXi 호스트가 버전 7.0 이상인지 확인합니다.
- 가상 시스템의 게스트 운영 체제가 Linux, Windows 10(64비트) 이상 또는 Windows Server 2016(64비트) 이상인지 확인합니다.
- 가상 시스템에 대해 **가상 시스템.구성.디바이스 설정 수정** 권한이 있는지 확인합니다.
- ESXi 호스트가 SGX 지원 CPU에 설치되어 있고 ESXi 호스트의 BIOS에서 SGX를 사용하도록 설정되어 있는지 확인합니다. 지원되는 CPU에 대한 자세한 내용은 <https://kb.vmware.com/s/article/71367>에서 참조하십시오.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭에서 **보안 디바이스**를 확장합니다.
- 4 **사용** 확인란을 선택합니다.
- 5 **Enclave 페이지 캐시 크기**에서 텍스트 상자에 새 값을 입력하고 드롭다운 메뉴에서 크기를 MB 또는 GB 단위로 선택합니다.

참고 Enclave 페이지 캐시 크기는 2의 배수여야 합니다.

6 제어 구성 시작 드롭다운 메뉴에서 적절한 모드를 선택합니다.

옵션	작업
잠김	Enclave 시작 구성을 활성화합니다. Enclave 공용 키 해시 시작 아래에 유효한 SHA256 해시를 입력합니다. SHA256 해시 키는 64자를 포함해야 합니다.
잠금 해제됨	게스트 운영 체제의 Enclave 시작 구성을 활성화합니다.

7 저장을 클릭합니다.

VMware Host Client의 가상 시스템에서 vSGX 비활성화

가상 시스템에서 vSGX를 비활성화하려면 VMware Host Client를 사용하면 됩니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭에서 **보안 디바이스**를 확장합니다.
- 4 **사용** 확인란의 선택을 취소하고 **저장**을 클릭합니다.

결과

vSGX가 가상 시스템에서 비활성화되어 있습니다.

VMware Host Client를 사용하여 VM에서 vTPM 디바이스 제거

TPM(신뢰할 수 있는 플랫폼 모듈)은 호스트 관련 중요 정보(예: 개인 키 및 운영 체제 암호)를 저장하는 특수한 칩입니다. 또한 TPM 칩은 암호화 작업을 수행하고 플랫폼의 무결성을 증명하는 데에도 사용됩니다. VMware Host Client에서는 가상 시스템에서 vTPM 디바이스를 제거할 수만 있습니다.

가상 TPM 디바이스는 TPM 기능의 소프트웨어 에뮬레이션입니다. 환경 내 가상 시스템에 vTPM(가상 TPM) 디바이스를 추가할 수 있습니다. vTPM을 구현하기 위해 호스트에 물리적 TPM 칩이 필요하지 않습니다. ESXi는 vTPM 디바이스를 사용하여 vSphere 환경에 TPM 기능을 적용합니다.

vTPM은 Windows 10 및 Windows Server 2016 운영 체제가 있는 가상 시스템에 사용할 수 있습니다. 가상 시스템은 하드웨어 버전 14 이상이어야 합니다.

vCenter Server 인스턴스에서만 가상 TPM 디바이스를 가상 시스템에 추가할 수 있습니다. 자세한 내용은 "vSphere 보안" 설명서를 참조하십시오.

VMware Host Client에서는 가상 시스템에서 가상 TPM 디바이스를 제거할 수만 있습니다.

사전 요구 사항

- 가상 시스템은 하드웨어 버전 14 이상이어야 합니다.
- 게스트 운영 체제가 Windows 10 또는 Windows Server 2016 이상이어야 합니다.

- 가상 시스템의 전원을 꺼야 합니다.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **가상 하드웨어** 탭에서 TPM 디바이스를 찾아서 **제거** 아이콘을 클릭합니다.
가상 TPM 디바이스가 가상 시스템에서 제거됩니다.
- 4 **저장**을 클릭하여 마법사를 닫습니다.

VMware Host Client에서 기존 VM에 가상화 기반 보안 활성화 또는 비활성화

VBS(가상화 기반 보안)는 Microsoft Hyper-V 기반 가상화 기술을 사용하여 별도의 가상화된 환경에서 핵심 Windows OS 서비스를 분리합니다. 이렇게 분리하면 환경 내 키 서비스를 조작할 수 없기 때문에 보호가 한층 강화됩니다.

지원되는 Windows 게스트 운영 체제에 대해 기존 가상 시스템에서 Microsoft VBS(가상화 기반 보안)를 사용하거나 사용하지 않도록 설정하여 가상 시스템의 보안 수준을 변경할 수 있습니다.

가상 시스템에서 VBS를 활성화하면 VBS 기능을 위해 Windows에 필요한 가상 하드웨어가 자동으로 활성화됩니다. VBS를 사용하도록 설정하면 가상 시스템에서 Hyper-V 변형이 시작되고 Hyper-V 루트 파티션 내에서 Windows가 실행됩니다.

VBS는 최신 Windows 운영 체제 버전(예: Windows 10 및 Windows Server 2016)에서 사용할 수 있습니다. 가상 시스템에서 VBS를 사용하려면 가상 시스템 호환성이 ESXi 6.7 이상이어야 합니다.

VMware Host Client에서는 가상 시스템을 생성하는 동안 VBS를 활성화할 수 있습니다. 또는 기존 가상 시스템에 대해 VBS를 활성화 또는 비활성화할 수 있습니다.

사전 요구 사항

VBS를 구성하려면 먼저 가상 시스템에서 VBS를 활성화한 후에 게스트 운영 체제에서 VBS를 활성화해야 합니다.

참고 버전 14 이전의 하드웨어 버전에서 Windows 10, Windows Server 2016 및 Windows Server 2019을 사용하도록 구성된 새 가상 시스템은 기본적으로 레거시 BIOS를 사용하여 생성됩니다. 가상 시스템의 펌웨어 유형을 레거시 BIOS에서 UEFI로 변경하는 경우 게스트 운영 체제를 다시 설치해야 합니다.

호스트의 TPM 검증이 성공하는 경우에만 가상 시스템에서 VBS를 활성화할 수 있습니다.

VBS에 Intel CPU를 사용하려면 vSphere 6.7 이상이 필요합니다. 하드웨어 버전 14 이상 및 지원되는 다음 게스트 운영 체제 중 하나를 사용하여 가상 시스템이 생성되어 있어야 합니다.

- Windows 10(64비트) 이상 릴리스
- Windows Server 2016(64비트) 이상 릴리스

VBS에 AMD CPU를 사용하려면 vSphere 7.0 업데이트 2 이상이 필요합니다. 하드웨어 버전 19 이상 및 지원되는 다음 게스트 운영 체제 중 하나를 사용하여 가상 시스템이 생성되어 있어야 합니다.

- Windows 10(64비트), 버전 1809 이상 릴리스
- Windows Server 2019(64비트) 이상 릴리스

VBS를 사용하도록 설정하기 전에 Windows 10, 버전 1809 및 Windows Server 2019에 대한 최신 패치를 설치해야 합니다.

AMD 플랫폼의 가상 시스템에서 VBS를 활성화하는 방법에 대한 자세한 내용은 VMware KB 문서 <https://kb.vmware.com/s/article/89880>을 참조하십시오.

절차

- 1 VMware Host Client 인벤토리에서 **가상 시스템**을 클릭합니다.
- 2 목록에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **설정 편집**을 선택합니다.
- 3 **VM 옵션** 탭에서 가상 시스템에 VBS를 활성화 또는 비활성화합니다.
 - 가상 시스템에 VBS를 활성화하려면 **가상화 기반 보안 사용** 확인란을 선택합니다.
 - 가상 시스템에 VBS를 비활성화하려면 **가상화 기반 보안 사용** 확인란을 선택 취소합니다.

VBS를 활성화하면 마법사에서 몇 가지 옵션이 자동으로 선택되고 흐리게 표시됩니다.

- 4 **저장**을 클릭하여 마법사를 닫습니다.

VMware Host Client에서 스토리지 관리

5

VMware Host Client를 사용하여 ESXi 호스트에 연결하면 어댑터 구성, 데이터스토어 생성 및 스토리지 디바이스 정보 보기를 비롯하여 ESXi 호스트에 대한 여러 스토리지 관리 태스크를 수행할 수 있습니다.

다음으로 아래 항목을 읽으십시오.

- VMware Host Client의 데이터스토어
- VMware Host Client에서 스토리지 어댑터 관리
- VMware Host Client에서 스토리지 디바이스 관리
- 영구 메모리 관리
- VMware Host Client에서 스토리지 모니터링
- VMware Host Client에서 스토리지 새로 고침 및 다시 검색 작업 수행

VMware Host Client의 데이터스토어

데이터스토어는 파일 시스템과 유사한 논리적 컨테이너로, 각 스토리지 디바이스의 특정 정보를 포함하고 가상 시스템 파일 저장을 위한 통일된 모델을 제공합니다.

데이터스토어를 사용하여 ISO 이미지, 가상 시스템 템플릿 및 플로피 이미지를 저장할 수 있습니다.

사용하는 스토리지의 유형에 따라 데이터스토어는 다음과 같은 유형 중 하나일 수 있습니다.

- 가상 시스템 파일 시스템(VMFS)
- 네트워크 파일 시스템(NFS)

데이터스토어를 생성한 후 데이터스토어 용량을 늘릴 수 있지만 VMFS 데이터스토어인 경우에만 가능합니다.

블록 스토리지 디바이스, Fibre Channel 및 iSCSI, NAS 디바이스는 하드웨어 가속을 지원합니다.

하드웨어 가속 기능을 통해 ESXi 호스트를 호환되는 스토리지 시스템과 통합할 수 있습니다. 호스트는 특정 가상 시스템 및 스토리지 관리 작업을 스토리지 시스템에 오프로드할 수 있습니다. 호스트는 스토리지 하드웨어의 도움을 받아 이러한 작업을 보다 빠르게 처리하고 CPU, 메모리 및 스토리지 패브릭 대역폭의 사용량을 줄일 수 있습니다.

자세한 내용은 <http://kb.vmware.com/kb/1021976>에서 VMware 기술 자료 문서를 참조하십시오.

VMware Host Client에서 데이터스토어 정보 보기

VMware Host Client를 사용하여 호스트에서 사용할 수 있는 데이터스토어를 표시하고 해당 속성을 분석할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **데이터스토어**를 클릭합니다.
- 2 특정 데이터스토어의 세부 정보를 보려면 목록에서 데이터스토어를 선택합니다.

VMware Host Client에서 VMFS 데이터스토어 생성

가상 시스템의 저장소로서 VMFS 데이터스토어를 처리합니다. 파이버 채널, iSCSI 및 로컬 스토리지 디바이스를 포함하여 호스트가 감지하는 SCSI 기반의 스토리지 디바이스에 VMFS 데이터스토어를 설정할 수 있습니다.

VMware Host Client에서 데이터스토어를 생성하려면 **새 데이터스토어** 마법사를 사용할 수 있습니다.

사전 요구 사항

스토리지에 필요한 어댑터를 설치하고 구성합니다. 새롭게 추가된 스토리지 디바이스를 검색하려면 어댑터를 재검색합니다.

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **데이터스토어**를 클릭합니다.
- 2 **새 데이터스토어**를 클릭합니다.
새 데이터스토어 마법사가 열립니다.
- 3 [생성 유형 선택] 페이지에서 **새 VMFS 데이터스토어 생성**을 선택하고 **다음**을 클릭합니다.

옵션	설명
새 VMFS 데이터스토어 생성	로컬 디스크 디바이스에 새 VMFS 데이터스토어를 생성합니다.
기존 VMFS 데이터스토어에 익스텐트 추가	다른 디스크에 새 익스텐트를 추가하여 기존 데이터스토어의 크기를 늘립니다.
기존 VMFS 데이터스토어 익스텐트 확장	기존 데이터스토어 익스텐트의 크기를 늘립니다.
NFS 데이터스토어 마운트	원격 NFS 볼륨을 마운트하여 새 데이터스토어를 생성합니다.

- 4 [디바이스 선택] 페이지에서 새 VMFS 파티션을 생성할 디바이스를 선택합니다.
 - a 새 데이터스토어의 이름을 입력합니다.
 - b 데이터스토어를 추가할 디바이스를 선택합니다.
목록에는 사용할 수 있는 공간이 충분한 디바이스만 포함됩니다.
 - c **다음**을 클릭합니다.

- 5 [파티셔닝 옵션 선택] 페이지에서 디바이스를 파티셔닝하는 방법을 선택하고 **다음**을 클릭합니다.

옵션	설명
전체 디스크 사용	디바이스에서 사용할 수 있는 전체 여유 공간을 표시합니다.
사용자 지정	사용 가능한 공간 막대를 클릭하고 가로 스크롤러를 사용하여 디바이스를 파티션합니다.

- 6 [완료 준비] 페이지에서 구성 세부 정보를 검토하고 **마침**을 클릭합니다.

VMFS 데이터스토어 용량 증가

VMFS 데이터스토어에 추가 공간이 필요한 경우 데이터스토어 용량을 늘릴 수 있습니다. 데이터스토어 익스텐트를 확장하거나 .익스텐트를 추가하여 용량을 동적으로 늘릴 수 있습니다.

다음 방법 중 하나를 사용하여 데이터스토어 용량을 늘립니다.

- 확장 가능한 데이터스토어 익스텐트를 동적으로 확장하여 사용 가능한 인접 용량을 채웁니다. 익스텐트는 기본 스토리지 디바이스에서 익스텐트 바로 뒤에 여유 공간이 있을 때 확장 가능한 것으로 간주됩니다.
- 익스텐트를 동적으로 추가합니다. 데이터스토어는 각각 크기가 2TB 이상인 최대 32개의 익스텐트에 분산될 수 있지만 단일 볼륨으로 나타납니다. 확장된 VMFS 데이터스토어는 익스텐트의 일부 또는 전체를 언제든지 사용할 수 있습니다. 특정 익스텐트가 반드시 다 차야만 다음 익스텐트를 사용할 수 있는 것은 아닙니다.

참고 ATS(원자성 테스트 및 세트) 메커니즘이라고도 하는 하드웨어 지원 잠금만 지원하는 데이터스토어는 ATS가 아닌 디바이스에 확장될 수 없습니다. 자세한 내용은 "vSphere 스토리지" 의 내용을 참조하십시오.

VMware Host Client에서 기존 VMFS 데이터스토어 늘리기

데이터스토어에 가상 시스템을 추가해야 하는 경우 또는 데이터스토어에서 실행 중인 가상 시스템에 더 많은 공간이 필요한 경우 VMFS 데이터스토어의 용량을 동적으로 늘릴 수 있습니다.

공유 데이터스토어에 전원이 켜져 있는 가상 시스템이 있고 공간이 100% 다 찬 경우 전원이 켜진 가상 시스템이 등록된 호스트에서만 데이터스토어의 용량을 늘릴 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **데이터스토어**를 클릭합니다.
- 2 **새 데이터스토어**를 클릭합니다.
- 3 [생성 유형 선택] 페이지에서 **기존 VMFS 데이터스토어에 익스텐트 추가**를 클릭하고 **다음**을 클릭합니다.
- 4 [데이터스토어 선택] 페이지에서 확장할 데이터스토어를 선택하고 **다음**을 클릭합니다.
- 5 [디바이스 선택] 페이지에서 새 VMFS 파티션을 생성할 디바이스를 선택하고 **다음**을 클릭합니다.

- 6 [파티셔닝 옵션 선택] 페이지에서 디바이스를 파티셔닝하는 방법을 선택하고 **다음**을 클릭합니다.

옵션	설명
전체 디스크 사용	디바이스에서 사용할 수 있는 전체 여유 공간을 표시합니다.
사용자 지정	사용 가능한 공간 막대를 클릭하고 가로 스크롤러를 사용하여 디바이스를 파티션합니다.

- 7 [완료 준비] 페이지에서 구성 세부 정보를 검토하고 **마침**을 클릭합니다.

VMware Host Client에서 네트워크 파일 시스템 데이터스토어 마운트

VMware Host Client로 NFS(네트워크 파일 시스템)를 생성하여 가상 디스크를 저장하고 ISO 이미지, 가상 시스템 템플릿 등에 대한 중앙 저장소로 사용할 수 있습니다.

ESXi에 기본 제공된 NFS 클라이언트는 TCP/IP를 통한 NFS(네트워크 파일 시스템) 프로토콜을 사용하여 NAS 서버에 있는 지정된 NFS 볼륨에 액세스합니다. vSphere는 NFS 프로토콜 버전 3 및 4.1을 지원합니다.

ESXi 호스트는 NFS 볼륨을 마운트하고 스토리지 요구 사항에 맞춰 사용할 수 있습니다.

일반적으로 NFS 볼륨 또는 디렉토리는 스토리지 관리자가 생성하며 NFS 서버에서 내보냅니다. NFS 볼륨은 VMFS 같은 로컬 파일 시스템을 사용하여 포맷하지 않아도 됩니다. 대신 볼륨을 ESXi 호스트에 직접 마운트하고, VMFS 데이터스토어를 사용하는 것과 동일한 방식으로 해당 볼륨을 사용하여 가상 시스템을 저장하고 부팅할 수 있습니다.

가상 디스크를 NFS 데이터스토어에 저장할 수 있을 뿐만 아니라 NFS를 ISO 이미지, 가상 시스템 템플릿 등의 중앙 저장소로 사용할 수 있습니다. ISO 이미지에 대해 데이터스토어를 사용하는 경우에는 가상 시스템의 CD-ROM 디바이스를 데이터스토어에 있는 ISO 파일에 연결할 수 있습니다. 그런 후 ISO 파일에서 게스트 운영 체제를 설치할 수 있습니다.

NFS 스토리지를 사용하는 경우에는 NFS 서버 구성, 네트워킹, NFS 데이터스토어 등과 관련된 특정 지침을 따라야 합니다.

다음으로 읽을 항목

절차

1 VMware Host Client에서 NFS 데이터스토어 마운트

새 데이터스토어 마법사를 사용하여 VMware Host Client에서 NFS(네트워크 파일 시스템) 데이터스토어를 마운트합니다.

VMware Host Client에서 NFS 데이터스토어 마운트

새 데이터스토어 마법사를 사용하여 VMware Host Client에서 NFS(네트워크 파일 시스템) 데이터스토어를 마운트합니다.

사전 요구 사항

NFS가 원격 서버의 데이터에 액세스하려면 네트워크 연결이 필요하므로 NFS를 구성하기 전에 먼저 VMkernel 네트워킹을 구성해야 합니다.

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **데이터스토어**를 클릭합니다.
- 2 **새 데이터스토어**를 클릭합니다.
새 데이터스토어 마법사가 열립니다.
- 3 [생성 유형 선택] 페이지에서 **NFS 데이터스토어 마운트**를 클릭하고 **다음**을 클릭합니다.
- 4 [NFS 마운트 세부 정보 제공] 페이지에서 마운트하는 NFS에 대한 자세한 정보를 입력합니다.

- a NFS 데이터스토어의 이름을 입력합니다.
- b NFS 서버 이름을 입력합니다.

서버 이름의 경우 IP 주소, DNS 이름 또는 NFS UUID를 입력할 수 있습니다.

참고 다른 호스트에 동일한 NFS 볼륨을 마운트할 때에는 서버와 폴더 이름이 호스트에서 동일해야 합니다. 이름이 일치하지 않으면 호스트에서는 다른 두 개의 데이터스토어와 동일한 NFS 볼륨을 검색합니다. 이 경우 vMotion 같은 기능에서 실패가 발생할 수 있습니다. 예를 들어 서버 이름을 한 호스트에는 **filer**로 입력하고 다른 호스트에는 **filer.domain.com**으로 입력하는 경우에 이러한 불일치가 발생할 수 있습니다.

- c NFS 공유를 지정합니다.
 - d NFS 버전을 지정합니다.
 - e **다음**을 클릭합니다.
- 5 [완료 준비] 페이지에서 NFS 데이터스토어에 대한 구성 설정을 검토한 후 **마침**을 클릭합니다.

VMware Host Client에서 데이터스토어 마운트 해제

VMware Host Client에서 데이터스토어를 마운트 해제하면 데이터스토어가 그대로 유지되지만 관리하는 호스트의 인벤토리에서 더 이상 볼 수 없습니다. 이 데이터스토어는 마운트된 상태를 유지하는 다른 호스트에서 계속 나타납니다.

마운트 해제를 진행하고 있는 동안 데이터스토어에 I/O가 이루어지는 작업 구성을 실행하지 마십시오.

사전 요구 사항

참고 데이터스토어가 vSphere HA 하트비트에 사용되지 않는지 확인합니다. vSphere HA 하트비트를 사용해도 데이터스토어를 마운트 해제할 수는 있습니다. 그러나 데이터스토어가 하트비트에 사용된 경우 데이터스토어를 마운트 해제하면 호스트에 장애가 발생하고 모든 활성 가상 시스템이 다시 시작될 수 있습니다.

데이터스토어를 마운트 해제하기 전에 다음 필수 구성 요소를 충족하는지도 확인해야 합니다.

- 가상 시스템이 이 데이터스토어에 없습니다.
- Storage DRS는 데이터스토어를 관리하지 않습니다.
- 이 데이터스토어에는 Storage I/O Control이 비활성화되었습니다.

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **데이터스토어**를 클릭합니다.
- 2 목록에서 마운트 해제하려는 데이터스토어를 마우스 오른쪽 버튼으로 클릭하고 **마운트 해제**를 클릭합니다.
- 3 마운트 해제하려는 데이터스토어를 확인합니다.

데이터스토어 마운트 해제 또는 제거 실패

데이터스토어를 마운트 해제하거나 제거하려고 할 때 작업이 실패합니다.

문제

데이터스토어에 열려 있는 파일이 있으면 데이터스토어 마운트 해제 또는 제거 작업이 실패합니다. 이러한 사용자 작업을 위해 vSphere HA 에이전트는 하트비트 파일처럼 열려 있는 모든 파일을 닫습니다. vCenter Server에서 에이전트에 연결할 수 없거나 에이전트가 파일을 닫기 위해 보류 중인 I/O를 풀러시킬 수 없는 경우 호스트 '{hostName}'의 vSphere HA 에이전트가 데이터스토어 '{dsName}'의 파일 작업을 중지하지 못했습니다. 오류가 트리거됩니다.

원인

마운트 해제 또는 제거할 데이터스토어가 하트비트에 사용되는 경우 vCenter Server에서는 이를 하트비트에서 제외하고 새 데이터스토어를 선택합니다. 하지만 에이전트가 연결되지 않는 경우, 즉 호스트가 분리되었거나 네트워크 파티션에 있는 경우에는 업데이트된 하트비트 데이터스토어가 에이전트에 수신되지 않습니다. 이 경우 하트비트 파일이 닫히지 않고 사용자 작업이 실패합니다. 모든 경로가 다운된 경우와 같은 스토리지 장애로 인해 데이터스토어에 액세스할 수 없는 경우에도 작업이 실패할 수 있습니다.

참고 VMFS 데이터스토어를 제거하면 데이터스토어가 인벤토리의 모든 호스트에서 제거됩니다. 따라서 vSphere HA 클러스터에 연결할 수 없거나 데이터스토어에 액세스할 수 없는 호스트가 있으면 작업이 실패합니다.

해결책

데이터스토어에 액세스할 수 있으며 영향을 받는 호스트에 연결할 수 있는지 확인하십시오.

VMware Host Client에서 데이터스토어 파일 브라우저 사용

데이터스토어 파일 브라우저를 사용하여 데이터스토어의 콘텐츠를 관리합니다. 데이터스토어에 파일 업로드, 시스템에 데이터스토어 파일 다운로드, 데이터스토어 폴더 또는 파일 이동 및 복사 또는 새 데이터 디렉토리 생성을 포함하는 많은 작업을 수행할 수 있습니다.

VMware Host Client에서 데이터스토어에 파일 업로드

데이터스토어 파일 브라우저를 사용하여 호스트에서 데이터스토어에 파일을 업로드합니다.

참고 Virtual Volumes는 가상 데이터스토어에 파일을 직접 업로드하는 것을 지원하지 않습니다. 먼저 가상 데이터스토어에 폴더를 생성한 다음 파일을 폴더에 업로드해야 합니다.

데이터스토어는 가상 시스템 파일의 스토리지로 일반적으로 사용될 뿐 아니라 가상 시스템과 관련된 데이터 또는 파일을 저장하는 역할도 담당할 수 있습니다. 예를 들어 로컬 컴퓨터에서 호스트의 데이터스토어로 운영 체제의 ISO 이미지를 업로드할 수 있습니다. 그런 다음 이 이미지를 사용하여 새 가상 시스템에서 게스트 운영 체제를 설치할 수 있습니다.

사전 요구 사항

필요한 권한: [데이터스토어.데이터스토어 찾아보기](#)

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **데이터스토어**를 클릭합니다.
- 2 **데이터스토어 브라우저**를 클릭합니다.
- 3 파일을 저장할 데이터스토어를 선택합니다.
- 4 (선택 사항) **디렉토리 생성**을 클릭하여 파일을 저장할 새 데이터스토어 디렉토리를 생성합니다.
- 5 대상 폴더를 선택하고 **업로드**를 클릭합니다.
- 6 로컬 컴퓨터에서 업로드하려는 항목을 찾고 **열기**를 클릭합니다.
선택한 데이터스토어로 파일이 업로드됩니다.
- 7 (선택 사항) 데이터스토어 파일 브라우저를 새로 고쳐 목록에서 업로드된 파일을 확인합니다.
- 8 **닫기**를 클릭하여 파일 브라우저를 종료합니다.

VMware Host Client에서 데이터스토어로부터 시스템으로 파일 다운로드

데이터스토어 파일 브라우저를 사용하여 관리하는 호스트에서 사용할 수 있는 데이터스토어로부터 로컬 시스템으로 파일을 다운로드합니다.

사전 요구 사항

필요한 권한: [데이터스토어.데이터스토어 찾아보기](#)

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **데이터스토어**를 클릭합니다.
- 2 **데이터스토어 브라우저**를 클릭합니다.
- 3 대상 데이터스토어를 선택합니다.
- 4 다운로드하려는 파일이 포함된 폴더를 클릭합니다.
폴더에서 사용할 수 있는 파일이 표시됩니다.
- 5 다운로드하려는 파일을 클릭합니다.
- 6 **다운로드**를 클릭합니다.
파일이 시스템으로 다운로드됩니다.
- 7 **닫기**를 클릭하여 파일 브라우저를 종료합니다.

VMware Host Client에서 데이터스토어의 파일 삭제

데이터스토어에서 더 이상 사용하지 않는 파일을 영구적으로 제거할 수 있습니다.

사전 요구 사항

필요한 권한: **데이터스토어.데이터스토어 찾아보기**

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **데이터스토어**를 클릭합니다.
- 2 **데이터스토어 브라우저**를 클릭합니다.
- 3 대상 데이터스토어를 선택합니다.
- 4 제거하려는 파일이 포함된 폴더를 선택합니다.
폴더에서 사용할 수 있는 파일이 표시됩니다.
- 5 데이터스토어에서 제거하려는 파일을 클릭하고 **삭제**를 클릭하고 **삭제**를 다시 클릭합니다.
- 6 **닫기**를 클릭하여 파일 브라우저를 종료합니다.

VMware Host Client에서 데이터스토어 폴더 또는 파일 이동

데이터스토어 파일 브라우저를 사용하여 동일한 데이터스토어 또는 다른 데이터스토어에서 파일 또는 폴더를 새로운 위치로 이동합니다.

참고 가상 디스크 파일은 포맷 변환없이 이동 및 복사됩니다. 소스 호스트 유형과 다른 호스트 유형의 데이터스토어로 가상 디스크를 이동하는 경우 가상 디스크를 사용하려면 변환해야 할 수 있습니다.

사전 요구 사항

필요한 권한: **데이터스토어.데이터스토어 찾아보기**

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **데이터스토어**를 클릭합니다.
- 2 **데이터스토어 브라우저**를 클릭합니다.
- 3 대상 데이터스토어를 선택합니다.
- 4 다른 위치로 이동하려는 파일 또는 폴더를 선택하고 **이동**을 클릭합니다.
- 5 대상을 선택하고 **이동**을 클릭합니다.
- 6 **닫기**를 클릭하여 파일 브라우저를 종료합니다.

VMware Host Client에서 데이터스토어 폴더 또는 파일 복사

데이터스토어 파일 브라우저를 사용하여 동일한 데이터스토어 또는 다른 데이터스토어에서 폴더 또는 파일을 새로운 위치로 복사합니다.

참고 가상 디스크 파일은 포맷 변환없이 이동 및 복사됩니다. 소스 호스트 유형과 다른 호스트 유형의 데이터스토어로 가상 디스크를 이동하는 경우 가상 디스크를 변환해야 할 수 있습니다.

사전 요구 사항

필요한 권한: [데이터스토어.데이터스토어 찾아보기](#)

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **데이터스토어**를 클릭합니다.
- 2 **데이터스토어 브라우저**를 클릭합니다.
- 3 대상 데이터스토어를 선택합니다.
- 4 다른 위치로 이동하려는 파일 또는 폴더를 선택하고 **복사**를 클릭합니다.
- 5 대상을 선택하고 **복사**를 클릭합니다.
- 6 **닫기**를 클릭하여 파일 브라우저를 종료합니다.

VMware Host Client에서 새 데이터스토어 디렉토리 생성

특정 위치에 파일을 저장하려는 경우 새 데이터스토어 디렉토리를 생성할 수 있습니다.

사전 요구 사항

필요한 권한: [데이터스토어.데이터스토어 찾아보기](#)

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **데이터스토어**를 클릭합니다.
- 2 **데이터스토어 브라우저**를 클릭합니다.
- 3 **디렉토리 생성**을 클릭합니다.

- 4 대상 데이터스토어를 선택합니다.
- 5 (선택 사항) 새 디렉토리의 이름을 입력합니다.
- 6 **디렉토리 생성**을 클릭합니다.
- 7 **닫기**를 클릭하여 파일 브라우저를 종료합니다.

VMware Host Client에서 데이터스토어 이름 바꾸기

VMware Host Client에서 데이터스토어의 표시 이름을 변경할 수 있습니다.

참고 호스트가 vCenter Server에서 관리되는 경우 VMware Host Client에서 데이터스토어 이름을 변경할 수 없습니다. 호스트를 관리하는 vCenter Server 인스턴스에서만 작업을 수행할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **데이터스토어**를 클릭합니다.
- 2 목록에서 데이터스토어를 마우스 오른쪽 버튼으로 클릭하고 드롭다운 메뉴에서 **이름 바꾸기**를 선택합니다.
- 3 데이터스토어의 새 이름을 입력하고 **저장**을 클릭하여 변경 내용을 적용합니다.
- 4 (선택 사항) **새로 고침**을 클릭하여 사용할 수 있는 데이터스토어 목록에서 데이터스토어의 새 이름을 확인합니다.

VMware Host Client에서 VMFS 데이터스토어 삭제

다시 서명 없이 마운트된 복사본을 포함하여 VMFS 데이터스토어의 유형을 삭제할 수 있습니다. 데이터스토어를 삭제하면 호스트에서 데이터스토어 및 데이터스토어에 연결된 모든 파일이 제거됩니다.

참고 데이터스토어 삭제 작업은 데이터스토어의 가상 시스템과 연결된 모든 파일을 영구적으로 삭제합니다. 마운트 해제 없이 데이터스토어를 삭제할 수 있지만 데이터스토어를 먼저 마운트 해제하는 것이 좋습니다.

사전 요구 사항

데이터스토어에서 모든 가상 시스템을 제거합니다.

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **데이터스토어**를 클릭합니다.
- 2 목록에서 데이터스토어를 마우스 오른쪽 버튼으로 클릭하고 드롭다운 메뉴에서 **삭제**를 선택합니다.
- 3 **확인**을 클릭하여 데이터스토어를 삭제합니다.

VMware Host Client에서 스토리지 씬 프로비저닝

ESXi로 어레이 수준과 가상 디스크 수준의 두 가지 씬 프로비저닝 모델을 사용할 수 있습니다.

씬 프로비저닝은 스토리지 공간을 필요할 때 유연하게 할당하여 스토리지 활용도를 최적화하는 방법입니다. 씬 프로비저닝은 씩 프로비저닝이라고 하는 기존 모델과는 대조적입니다. 씩 프로비저닝에서는 향후 스토리지 요구 사항에 대비하여 대량의 스토리지 공간을 미리 제공하지만 공간이 사용되지 않는 상태로 유지될 수 있기 때문에 스토리지 용량의 활용도가 저하되게 됩니다.

VMware 씬 프로비저닝 기능을 사용하면 데이터스토어 및 스토리지 어레이 수준에서 스토리지 활용도 저하 문제를 해결할 수 있습니다.

VMware Host Client에서 씬 프로비저닝된 가상 디스크 생성

스토리지 공간을 절약하기 위해 씬 프로비저닝된 디스크를 생성할 수 있습니다. 씬 프로비저닝된 가상 디스크는 작게 시작하며 필요한 디스크 공간이 늘어날수록 크기가 증가합니다. 씬 디스크는 디스크 수준 씬 프로비저닝을 지원하는 데이터스토어에만 생성할 수 있습니다.

다음 절차에서는 새 가상 시스템을 생성하는 것으로 가정합니다. 자세한 내용은 [VMware Host Client에서 가상 시스템 생성](#)의 내용을 참조하십시오.

절차

- 1 VMware Host Client 인벤토리에서 **호스트**를 마우스 오른쪽 버튼으로 클릭하고 **VM 생성/등록**을 선택합니다.
- 2 **새 가상 시스템** 마법사가 열립니다.
- 3 호스트에서 새 가상 시스템을 추가하는 방법을 선택하고 **다음**을 클릭합니다.
- 4 가상 시스템의 이름을 입력합니다.
- 5 **호환성** 드롭다운 메뉴에서 가상 시스템 호환성을 선택합니다.
- 6 **게스트 OS 버전** 드롭다운 메뉴에서 게스트 운영 체제 버전을 선택하고 **다음**을 클릭합니다.
- 7 **새 가상 시스템** 마법사의 스토리지 선택 페이지의 액세스할 수 있는 목록에서 가상 시스템 구성 파일 및 모든 가상 디스크에 대한 대상 데이터스토어를 선택합니다.
- 8 **가상 하드웨어** 탭에서 **하드 디스크**를 확장합니다.
- 9 **디스크 프로비저닝** 아래에서 **씬 프로비저닝** 라디오 버튼을 선택하고 **다음**을 클릭합니다.
- 10 **새 가상 시스템** 마법사의 완료 준비 페이지에서 가상 시스템의 구성 설정을 검토하고 **마침**을 클릭하여 설정을 저장합니다.

VMware Host Client에서 가상 시스템 스토리지 리소스 보기

VMware Host Client에서 가상 시스템에 데이터스토어 스토리지 공간이 할당되는 방법을 볼 수 있습니다.

리소스 사용은 구성 파일, 로그 파일, 스냅샷, 가상 디스크 등을 포함하여 가상 시스템 파일이 차지하고 있는 데이터스토어 공간을 보여 줍니다. 가상 시스템이 실행 중인 경우에는 사용된 스토리지 공간에 스왑 파일도 포함됩니다.

씬 디스크가 있는 가상 시스템의 경우 실제 스토리지 사용량 값이 가상 디스크 크기보다 작을 수도 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 가상 시스템을 클릭합니다.
- 2 가상 시스템 요약 페이지의 오른쪽 아래 영역에서 리소스 사용 정보를 검토합니다.

VMware Host Client에서 가상 시스템의 디스크 포맷 확인

가상 디스크가 씩 또는 썬 포맷으로 프로비저닝되었는지 여부를 확인할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
- 2 **가상 하드웨어** 탭에서 **하드 디스크**를 확장합니다.
유형 텍스트 상자는 가상 디스크의 형식을 표시합니다.

VMware Host Client에서 스토리지 어댑터 관리

VMware Host Client를 사용하여 호스트 또는 vCenter Server에 연결하면 다양한 iSCSI 구성 요소를 구성하는 것 같이 스토리지 어댑터에 대해 다양한 작업을 수행할 수 있습니다.

VMware Host Client 환경에서 관리하는 호스트에서 iSCSI를 사용하도록 설정하면 네트워크 포트 바인딩과 정적/동적 대상을 구성하거나 새로 추가할 수 있고, CHAP 인증을 관리할 수 있으며 호스트 스토리지에 다양한 고급 설정을 구성할 수 있습니다.

VMware Host Client에서 스토리지 어댑터 보기

호스트가 사용하는 스토리지 어댑터 및 관련 정보를 봅니다.

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **어댑터**를 클릭합니다.
호스트가 사용할 수 있는 모든 스토리지 어댑터가 **어댑터** 아래에 나열됩니다.
- 2 특정 어댑터의 세부 정보를 보려면 목록에서 어댑터를 선택합니다.

VMware Host Client에서 소프트웨어 iSCSI 어댑터 구성

소프트웨어 기반 iSCSI 구현에서는 표준 NIC를 사용하여 IP 네트워크상의 원격 iSCSI 대상에 호스트를 연결할 수 있습니다. ESXi에 기본 제공되는 소프트웨어 iSCSI 어댑터는 네트워크 스택을 통해 물리적 NIC와 통신합니다.

참고 소프트웨어 iSCSI 어댑터를 사용하려면 먼저 네트워킹을 설정하고 어댑터를 활성화한 후 CHAP 같은 매개 변수를 구성해야 합니다.

iSCSI 어댑터 구성 워크플로에는 다음과 같은 프로시저가 포함됩니다.

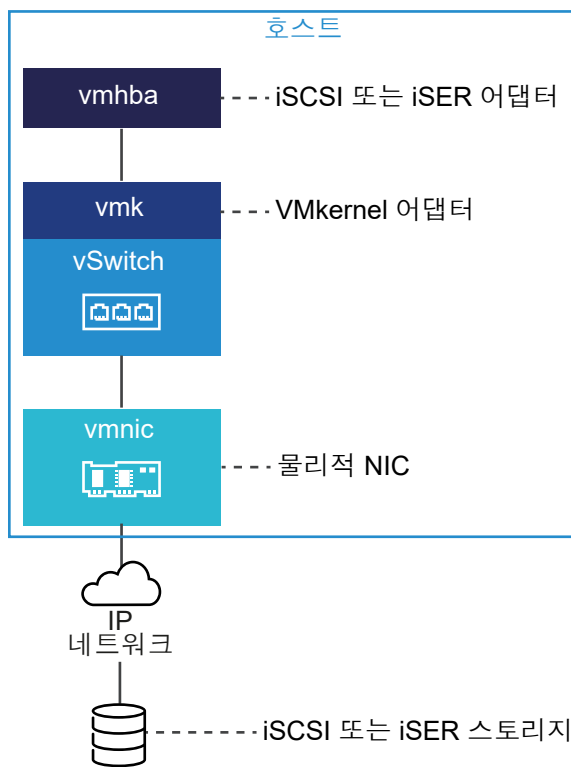
- 호스트에서 iSCSI를 사용하도록 설정. [VMware Host Client에서 ESXi 호스트에 대해 iSCSI를 사용하도록 설정](#) 항목을 참조하십시오.

- 포트 바인딩 추가. VMware Host Client에서 포트 바인딩 추가의 내용을 참조하십시오.
- 포트 바인딩 제거. VMware Host Client에서 포트 바인딩 제거의 내용을 참조하십시오.

ESXi를 사용하여 iSCSI 및 iSER에 대한 네트워크 설정

특정 유형의 iSCSI 어댑터는 VMkernel 네트워크에 따라 달라집니다. 이러한 어댑터에는 소프트웨어 또는 종속 하드웨어 iSCSI 어댑터와 RDMA(iSER) 기반 VMware iSCSI 어댑터가 포함됩니다. ESXi 환경에 이러한 어댑터 중 하나가 포함된 경우 iSCSI 또는 iSER 구성 요소와 물리적 네트워크 어댑터 간의 트래픽을 위한 연결을 구성해야 합니다.

네트워크 연결을 구성하려면 각각의 물리적 네트워크 어댑터마다 가상의 VMkernel 어댑터를 생성해야 합니다. 각 가상 네트워크 어댑터와 물리적 네트워크 어댑터 간에 일대일 매핑을 사용합니다. 그런 다음 이 VMkernel 어댑터를 적절한 iSCSI 또는 iSER 어댑터와 연결합니다. 이 프로세스를 포트 바인딩이라고 합니다.



포트 바인딩을 구성하는 경우 이러한 규칙을 따릅니다.

- 소프트웨어 iSCSI 어댑터는 호스트에서 사용할 수 있는 모든 물리적 NIC에 연결할 수 있습니다.
- 종속 iSCSI 어댑터는 고유한 물리적 NIC에만 연결해야 합니다.
- RDMA 지원 네트워크 어댑터에만 iSER 어댑터를 연결해야 합니다.

소프트웨어 iSCSI와의 네트워크 연결을 사용하는 시기 및 방법에 대한 특정 고려 사항을 보려면 VMware 기술 자료 문서(<http://kb.vmware.com/kb/2038869>)를 참조하십시오.

VMware Host Client에서 ESXi 호스트에 대해 iSCSI를 사용하도록 설정

VMware Host Client 환경에 있는 호스트에 대해 iSCSI를 사용하도록 설정하여 CHAP 인증, 네트워크 포트 바인딩, 정적/동적 대상 등의 스토리지 어댑터 매개 변수와 여러 가지 고급 설정을 구성할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **어댑터**를 클릭한 후 **iSCSI 구성**을 클릭합니다.
- 2 **사용** 라디오 버튼을 선택합니다.
- 3 (선택 사항) 변경하려는 매개 변수와 구성 요소를 구성합니다.
- 4 **구성 저장**을 클릭합니다.

소프트웨어 iSCSI를 사용하여 네트워킹을 구성하는 모범 사례

소프트웨어 iSCSI를 사용하여 네트워킹을 구성하는 경우, 몇 가지 모범 사례를 고려하십시오.

소프트웨어 iSCSI 포트 바인딩

ESXi 호스트의 소프트웨어 iSCSI 이니시에이터를 VMkernel 포트 하나 또는 여러 개에 바인딩하여 iSCSI 트래픽이 바인딩된 포트를 통해서만 이동하도록 할 수 있습니다. 바인딩되지 않은 포트는 iSCSI 트래픽에 사용되지 않습니다.

포트 바인딩이 구성되어 있으면 iSCSI 이니시에이터는 바인딩된 모든 포트에서 구성된 모든 대상 포털로 iSCSI 세션을 생성합니다.

다음 예제를 참조하십시오.

VMkernel 포트	대상 포털	iSCSI 세션
바인딩된 VMkernel 포트 2개	대상 포털 2개	세션 4개(2 x 2)
바인딩된 VMkernel 포트 4개	대상 포털 1개	세션 4개(4 x 1)
바인딩된 VMkernel 포트 2개	대상 포털 4개	세션 8개(2 x 4)

참고 포트 바인딩을 사용하는 경우에는 모든 VMkernel 포트에서 모든 대상 포털에 연결할 수 있는지 확인해야 합니다. 연결할 수 없으면 iSCSI 세션이 생성되지 않을 수 있습니다. 그 결과 다시 검색 작업이 예상보다 오래 걸릴 수 있습니다.

포트 바인딩 안 함

포트 바인딩을 사용하지 않으면 ESXi 네트워킹 계층이 해당 라우팅 테이블에 기반하여 가장 적합한 VMkernel 포트를 선택합니다. 호스트는 이 포트를 사용하여 대상 포털과의 iSCSI 세션을 생성합니다. 포트 바인딩을 사용하지 않으면 각 대상 포털마다 하나의 세션만 생성됩니다.

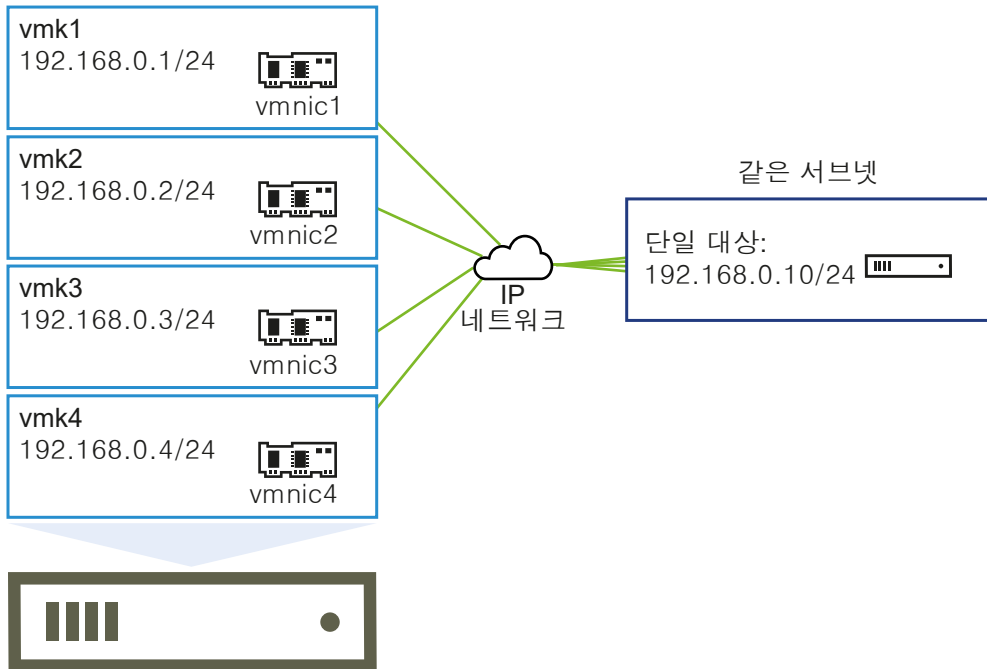
다음 예제를 참조하십시오.

VMkernel 포트	대상 포털	iSCSI 세션
바인딩되지 않은 VMkernel 포트 2개	대상 포털 2개	세션 2개
바인딩되지 않은 VMkernel 포트 4개	대상 포털 1개	세션 1개
바인딩되지 않은 VMkernel 포트 2개	대상 포털 4개	세션 4개

소프트웨어 iSCSI 다중 경로 지정

예제 1. 단일 네트워크 포털을 사용하는 iSCSI 대상에 대한 다중 경로

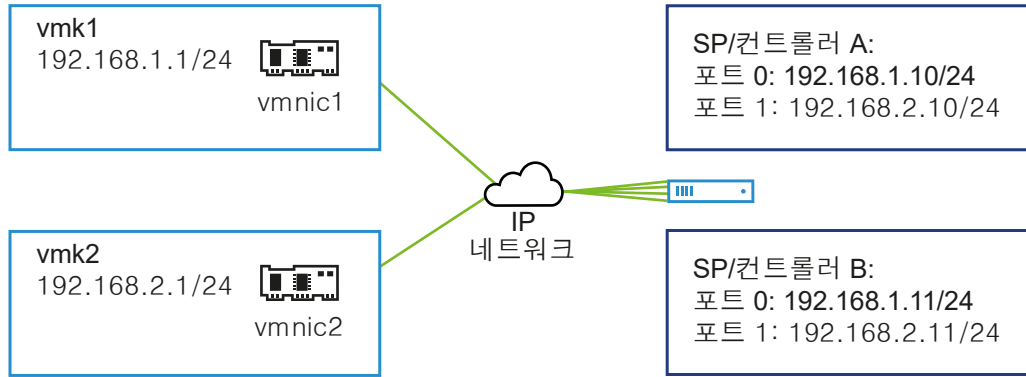
대상에 네트워크 포털이 하나뿐인 경우에는 ESXi 호스트에 VMkernel 포트를 여러 개 추가한 후 iSCSI 이니시에이터에 바인딩하여 대상에 대한 경로를 여러 개 생성할 수 있습니다.



이 예제에서는 모든 이니시에이터 포트와 대상 포털이 동일한 서브넷에 구성되어 있습니다. 바인딩된 모든 포트를 통해 대상에 연결할 수 있습니다. VMkernel 포트 4개와 대상 포털 하나가 있으므로 총 4개의 경로가 생성됩니다. 포트 바인딩을 사용하지 않으면 경로가 하나만 생성됩니다.

예제 2. 서로 다른 서브넷에 있는 VMkernel 포트를 사용하는 다중 경로

서로 다른 IP 서브넷에 있는 다중 포트 및 대상 포털을 구성하여 여러 경로를 생성할 수 있습니다. 이니시에이터와 대상 포트를 서로 다른 서브넷에 두면 ESXi가 특정 포트를 통해 경로를 생성하도록 할 수 있습니다. 포트를 바인딩하려면 모든 이니시에이터와 대상 포트가 같은 서브넷에 있어야 하기 때문에 이 구성에서는 포트 바인딩을 사용하지 않습니다.



컨트롤러 A와 컨트롤러 B의 포트 0에 연결하는 경우 ESXi는 vmk1을 선택합니다. 이는 세 포트 모두 동일한 서브넷에 있기 때문입니다. 마찬가지로 컨트롤러 A와 컨트롤러 B의 포트 1에 연결할 때는 vmk2가 선택됩니다. 이 구성에서는 NIC 팀 구성을 사용할 수 있습니다.

경로가 총 4개 생성됩니다.

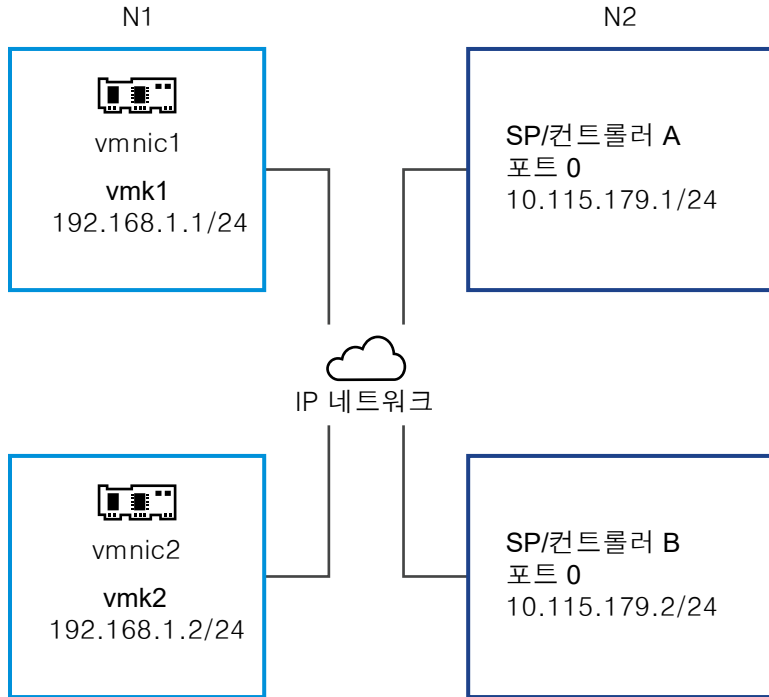
경로	설명
경로 1	vmk1 및 컨트롤러 A의 포트 0
경로 2	vmk1 및 컨트롤러 B의 포트 0
경로 3	vmk2 및 컨트롤러 A의 포트 1
경로 4	vmk2 및 컨트롤러 B의 포트 1

소프트웨어 iSCSI를 사용하는 라우팅

`esxcli` 명령을 사용하여 iSCSI 트래픽에 사용할 정적 경로를 추가할 수 있습니다. 정적 경로를 구성하면 서로 다른 서브넷에 있는 이니시에이터와 대상 포트가 서로 통신할 수 있습니다.

예제 1. 정적 경로와 포트 바인딩 사용

이 예제에서는 바인딩된 모든 VMkernel 포트를 서브넷 하나(N1)에 두고 모든 대상 포털을 다른 서브넷(N2)에 구성합니다. 그런 다음 대상 서브넷(N2)에 정적 경로를 추가할 수 있습니다.

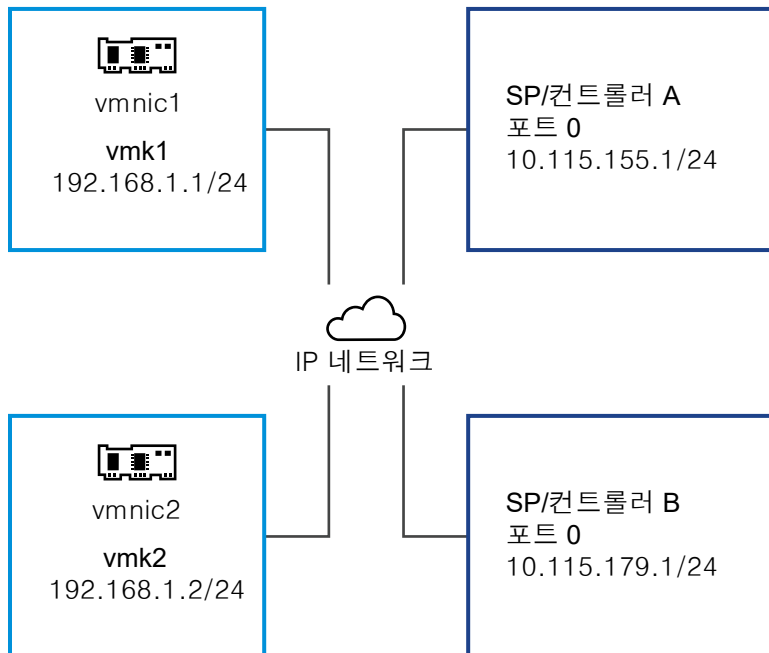


다음 명령을 사용합니다.

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network 10.115.179.0/24
```

예제 2. 정적 경로를 사용하여 다중 경로 생성

이 구성에서는 서로 다른 서브넷을 사용할 때 정적 라우팅을 사용합니다. 포트 바인딩은 이 구성에서 사용할 수 없습니다.



vmk1과 vmk2를 별도의 서브넷인 192.168.1.0과 192.168.2.0에 구성합니다. 대상 포털도 별도의 서브넷인 10.115.155.0과 10.115.179.0에 있습니다.

vmk1에서 10.115.155.0에 대한 정적 경로를 추가할 수 있습니다. vmk1에서 게이트웨이에 연결할 수 있어야 합니다.

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network 10.115.155.0/24
```

그런 다음 vmk2에서 10.115.179.0에 대한 정적 경로를 추가합니다. vmk2에서 게이트웨이에 연결할 수 있어야 합니다.

```
# esxcli network ip route ipv4 add -gateway 192.168.2.253 -network 10.115.179.0/24
```

컨트롤러 A의 포트 0을 사용하여 연결할 경우 vmk1이 사용됩니다.

컨트롤러 B의 포트 0을 사용하여 연결할 경우 vmk2가 사용됩니다.

예제 3. vmkernel 포트마다 별도의 게이트웨이를 사용하여 라우팅

vSphere 6.5부터는 VMkernel 포트마다 별도의 게이트웨이를 구성할 수 있습니다. DHCP를 사용하여 VMkernel 포트에 대한 IP 구성을 가져오는 경우, DHCP를 사용하여 게이트웨이 정보도 가져올 수 있습니다.

VMkernel 포트별 게이트웨이 정보를 보려면 다음 명령을 사용합니다.

```
# esxcli network ip interface ipv4 address list
```

Name	IPv4 Address	IPv4 Netmask	IPv4 Broadcast	Address Type	Gateway	DHCP	DNS
vmk0	10.115.155.122	255.255.252.0	10.115.155.255	DHCP	10.115.155.253	true	
vmk1	10.115.179.209	255.255.252.0	10.115.179.255	DHCP	10.115.179.253	true	
vmk2	10.115.179.146	255.255.252.0	10.115.179.255	DHCP	10.115.179.253	true	

VMkernel 포트마다 별도의 게이트웨이가 있는 경우에는 포트 바인딩을 사용하여 서로 다른 서브넷에 있는 대상에 연결할 수 있습니다.

VMware Host Client에서 포트 바인딩 추가

VMware Host Client를 사용하여 호스트에서 iSCSI 어댑터를 VMkernel 어댑터와 바인딩합니다.

사전 요구 사항

- 호스트에서 각각의 물리적 네트워크 어댑터마다 가상 VMkernel 어댑터를 만듭니다. 여러 VMkernel 어댑터를 사용하는 경우 올바른 네트워크 정책을 설정합니다.
- 필요한 권한: **호스트.구성.스토리지 파티션 구성**

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **어댑터**를 클릭한 후 **iSCSI 구성**을 클릭합니다.
- 2 **네트워크 포트 바인딩** 섹션에서 **포트 바인딩 추가**를 클릭합니다.

- 3 iSCSI 어댑터와 바인딩할 VMkernel 어댑터를 선택합니다.

참고 VMkernel 어댑터에 대한 네트워크 정책이 바인딩 요구 사항을 준수하는지 확인하십시오.

소프트웨어 iSCSI 어댑터를 하나 이상의 VMkernel 어댑터에 바인딩할 수 있습니다. 종속 하드웨어 iSCSI 어댑터의 경우 올바른 물리적 NIC에 연결된 VMkernel 어댑터 하나만 사용할 수 있습니다.

- 4 **선택**을 클릭합니다.
- 5 **구성 저장**을 클릭합니다.

VMware Host Client에서 포트 바인딩 제거

호스트에서 iSCSI 구성을 편집하여 포트 바인딩을 제거합니다.

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **어댑터**를 클릭한 후 **iSCSI 구성**을 클릭합니다.
- 2 **네트워크 포트 바인딩** 섹션의 목록에서 VMkernel NIC를 선택합니다.
- 3 **포트 바인딩 제거**를 클릭합니다.
- 4 **구성 저장**을 클릭합니다.

VMware Host Client에서 동적 대상 설정

iSCSI 어댑터가 네트워크에서 액세스할 수 있는 스토리지 리소스를 확인할 수 있도록 대상 검색 주소를 반드시 설정해야 합니다. ESXi 호스트는 동적 및 정적 검색 방법을 지원합니다. 동적 검색을 사용하면 이니시에이터가 특정 iSCSI 스토리지 시스템에 연결할 때마다 iSCSI 시스템에 SendTargets 요청을 전송합니다. iSCSI 시스템은 사용할 수 있는 대상 목록을 이니시에이터에 제공하는 방식으로 응답합니다.

SendTargets 탐색이라고도 합니다. 이니시에이터가 지정된 iSCSI 서버에 연결할 때마다 서버에 SendTarget 요청을 보냅니다. 서버는 사용할 수 있는 대상 목록을 이니시에이터에 제공함으로써 응답합니다. 이러한 대상의 이름과 IP 주소가 **정적 검색** 탭에 나타납니다. 동적 검색을 통해 추가된 정적 대상을 제거할 경우 다시 검색할 때마다 대상이 목록으로 반환될 수 있으며 iSCSI 어댑터가 재설정되거나 호스트가 재부팅됩니다.

참고 소프트웨어 및 종속 하드웨어 iSCSI를 사용하는 경우 ESXi는 지정된 iSCSI 서버 주소의 IP 패밀리를 기준으로 대상 주소를 필터링합니다. 주소가 IPv4인 경우 iSCSI 서버의 SendTargets 응답에서 발생할 수 있는 IPv6 주소가 필터링됩니다. DNS 이름이 iSCSI 서버를 지정하는 데 사용되거나 iSCSI 서버의 SendTargets 응답에 DNS 이름이 있는 경우 ESXi는 DNS 조회에서 처음 확인된 항목의 IP 패밀리를 사용합니다.

동적 검색을 설정할 때는 새 iSCSI 시스템만 추가할 수 있습니다. 기존 iSCSI 시스템의 IP 주소, DNS 이름 또는 포트 번호를 변경할 수는 없습니다. 이러한 매개 변수를 수정하려면 기존 시스템을 삭제한 후 새 시스템을 추가해야 합니다.

사전 요구 사항

필요한 권한: **호스트.구성.스토리지 파티션 구성**

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **어댑터**를 클릭한 후 **iSCSI 구성**을 클릭합니다.
- 2 **동적 대상 추가**를 클릭합니다.
새 동적 대상이 목록에 나타납니다.
- 3 새 동적 대상의 주소를 추가하려면 목록에서 대상을 클릭하고 주소를 입력합니다.
- 4 (선택 사항) 새 동적 대상의 포트 번호를 변경하려면 대상 **포트** 텍스트 상자를 클릭하고 새 포트 번호를 입력합니다.
- 5 (선택 사항) 동적 대상 설정을 편집하려면 사용 가능한 대상 목록에서 새 대상을 선택하고 **설정 편집**을 클릭하여 변경할 매개 변수를 구성한 후 **저장**을 클릭합니다.
- 6 (선택 사항) 특정 대상을 삭제하려면 대상을 선택하고 **동적 대상 삭제**를 클릭합니다.
대상이 기존 동적 대상 목록에 더 이상 표시되지 않습니다.
- 7 **구성 저장**을 클릭합니다.

VMware Host Client에서 정적 대상 설정

iSCSI 이니시에이터가 있으면 정적 검색을 사용하여 대상에 대한 정보를 수동으로 입력할 수 있습니다.

정적 검색을 설정할 때는 새 iSCSI 대상만 추가할 수 있습니다. 기존 대상의 IP 주소, DNS 이름, iSCSI 대상 이름 또는 포트 번호는 변경할 수 없습니다. 이러한 정보를 변경하려면 기존 대상을 제거한 후 새 대상을 추가해야 합니다.

동적 검색 기능 외에도 정적 검색을 사용하고 대상에 대한 정보를 수동으로 입력할 수 있습니다. iSCSI 어댑터는 제공된 대상 목록을 사용하여 iSCSI 서버와 연결 및 통신합니다.

사전 요구 사항

필요한 권한: **호스트.구성.스토리지 파티션 구성**

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **어댑터**를 클릭한 후 **iSCSI 구성**을 클릭합니다.
- 2 **정적 대상 추가**를 클릭합니다.
새 정적 대상이 목록에 나타납니다.
- 3 새 정적 대상의 이름을 추가하려면 목록에서 대상을 클릭하고 이름을 입력합니다.
- 4 새 정적 대상의 주소를 추가하려면 목록에서 대상을 클릭하고 주소를 입력합니다.
- 5 (선택 사항) 새 정적 대상의 포트 번호를 변경하려면 대상 **포트** 텍스트 상자를 클릭하고 새 포트 번호를 입력합니다.
- 6 (선택 사항) 정적 대상 설정을 편집하려면 사용 가능한 대상 목록에서 새 대상을 선택하고 **설정 편집**을 클릭하여 변경할 매개 변수를 구성한 후 **저장**을 클릭합니다.

7 (선택 사항) 특정 대상을 삭제하려면 대상을 선택하고 **정적 대상 삭제**를 클릭합니다.

대상이 기존 정적 대상 목록에 더 이상 표시되지 않습니다.

8 **구성 저장**을 클릭합니다.

VMware Host Client에서 iSCSI의 고급 설정 편집

고급 iSCSI 설정은 헤더와 데이터 다이제스트, ARP 리디렉션, 지연된 ACK 등의 매개 변수를 제어합니다. 일반적으로 호스트는 할당된 기본 제공 값으로 작동하므로 이러한 설정을 변경할 필요가 없습니다.

경고 VMware 지원 팀과 함께 작업하는 경우 또는 설정 수정을 위해 제공할 값에 대해 잘 알고 있는 경우가 아니면 고급 iSCSI 설정을 변경하지 마십시오.

사전 요구 사항

필요한 권한: **호스트.구성.스토리지 파티션 구성**

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **어댑터**를 클릭한 후 **iSCSI 구성**을 클릭합니다.
- 2 **고급 설정**을 클릭하여 전체 설정 목록을 표시합니다.
- 3 변경할 매개 변수를 편집한 후 **구성 저장**을 클릭합니다.

VMware Host Client에서 iSCSI 어댑터에 대한 CHAP 인증 설정

모든 대상이 이니시에이터 수준의 iSCSI 이니시에이터에서 동일한 CHAP 이름과 암호를 받도록 설정할 수 있습니다. 기본적으로 모든 검색 주소 또는 정적 대상은 이니시에이터 수준에서 설정하는 CHAP 매개 변수를 상속합니다.

CHAP 이름은 영숫자 511자 미만이어야 하며 CHAP 암호는 영숫자 255자 미만이어야 합니다. QLogic 어댑터와 같은 일부 어댑터의 경우 CHAP 이름의 하한 값이 255자이며 CHAP 암호의 하한 값이 100자입니다.

사전 요구 사항

- 소프트웨어 또는 종속 하드웨어 iSCSI의 CHAP 매개 변수를 설정하려면 단방향 CHAP(보통 CHAP라고도 함)를 구성할지 아니면 상호 CHAP를 구성할지 결정해야 합니다. 독립 하드웨어 iSCSI 어댑터는 상호 CHAP를 지원하지 않습니다.
 - 단방향 CHAP에서는 대상이 이니시에이터를 인증합니다.
 - 상호 CHAP에서는 대상과 이니시에이터 둘 다 서로를 인증합니다. CHAP와 상호 CHAP에 대해 서로 다른 암호를 사용하십시오.

CHAP 매개 변수를 구성할 때 이러한 매개 변수가 스토리지 쪽의 매개 변수와 일치하는지 확인합니다.

- 필요한 권한: **호스트.구성.스토리지 파티션 구성**

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **어댑터**를 클릭한 후 **iSCSI 구성**을 클릭합니다.

- 2 단방향 CHAP를 구성하려면 **CHAP 인증**을 확장하여 모든 매개 변수를 표시합니다.
 - a CHAP 보안 수준을 선택합니다.
 - b CHAP 이름을 입력합니다.
입력하는 이름은 스토리지 측에 구성된 이름과 일치해야 합니다.
 - c 인증에 사용할 단방향 CHAP 암호를 입력합니다. 스토리지 쪽에서 입력한 것과 동일한 암호를 사용합니다.
- 3 상호 CHAP를 구성하려면 단방향 CHAP의 옵션으로 **CHAP 사용**을 선택합니다. **상호 CHAP 인증**을 확장하여 모든 매개 변수를 표시합니다.
 - a **CHAP 사용**을 선택합니다.
 - b 상호 CHAP 이름을 입력합니다.
 - c 상호 CHAP 암호를 입력합니다.
단방향 CHAP와 상호 CHAP에 서로 다른 암호를 사용해야 합니다.
- 4 **구성 저장**을 클릭합니다.

결과

iSCSI 어댑터의 인증 설정을 변경한 경우 새 iSCSI 세션에 업데이트된 자격 증명만 사용합니다. 강제 재인증과 같은 다른 외부적인 요인에 의해 연결이 끊어지거나, 어댑터 iSCSI 대상을 제거했다가 추가하지 않는 한 기존 세션이 유지됩니다.

VMware Host Client에서 스토리지 디바이스 관리

VMware Host Client를 사용하여 관리하는 로컬 및 네트워크 디바이스가 액세스하는 ESXi 호스트를 관리할 수 있습니다.

VMware Host Client에서 스토리지 어댑터 보기

호스트가 사용할 수 있는 모든 스토리지 디바이스를 봅니다. 타사의 다중 경로 지정 플러그인을 사용할 경우, 해당 플러그인을 통해 사용 가능한 스토리지 디바이스도 목록에 표시됩니다.

스토리지 디바이스 보기에서는 호스트의 스토리지 디바이스를 나열하고, 해당 정보를 분석하고, 속성을 수정할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **디바이스**를 클릭합니다.
호스트가 사용할 수 있는 모든 스토리지 디바이스가 **디바이스** 아래에 나열됩니다.
- 2 특정 디바이스에 대한 세부 정보를 보려면 목록에서 디바이스를 선택합니다.

VMware Host Client에서 디바이스 파티션 테이블 지우기

VMware Host Client를 사용하여 ESXi 호스트에 로그인한 경우 호스트에서 액세스할 수 있는 디스크 디바이스의 파티션 테이블을 지울 수 있습니다.

사전 요구 사항

ESXi에서 디바이스를 부팅 디스크, VMFS 데이터스토어 또는 vSAN으로 사용하고 있지 않은지 확인합니다.

절차

- 1 VMware Host Client에서 **스토리지**를 클릭하고 **디바이스**를 클릭합니다.
- 2 목록에서 디바이스를 마우스 오른쪽 버튼으로 클릭하고 **파티션 테이블 지우기**를 클릭하고 **예**를 클릭합니다.
파티션 테이블을 지우면 데이터가 손실될 수 있습니다.

VMware Host Client에서 개별 디바이스 파티션 편집

VMware Host Client를 사용하여 ESXi에 로그인하면 파티션 편집기를 사용하여 디바이스의 개별 파티션을 제거할 수 있습니다.

사전 요구 사항

ESXi에서 디바이스를 부팅 디스크, VMFS 데이터스토어 또는 vSAN으로 사용하고 있지 않은지 확인합니다.

절차

- 1 VMware Host Client에서 **스토리지**를 클릭하고 **디바이스**를 클릭합니다.
- 2 목록에서 마우스 오른쪽 버튼으로 디바이스를 클릭하고 **파티션 편집**을 클릭합니다.
- 3 파티션을 선택하고 **파티션 삭제**를 클릭합니다.
- 4 (선택 사항) **재설정**을 클릭하여 원래 파티션을 복원합니다.
- 5 **파티션 저장**을 클릭합니다.
- 6 파티션 변경을 확인합니다.

영구 메모리 관리

ESXi 6.7 이상은 NVM(비휘발성 메모리) 또는 PMem(영구 메모리)이라고 하는 최신 컴퓨터 메모리 기술을 지원합니다.

PMem은 휘발성 컴퓨터 메모리의 높은 데이터 전송 속도와 기존 스토리지의 지속성 및 복원력을 모두 갖추고 있습니다. PMem 디바이스는 낮은 액세스 지연 시간을 가지며 재부팅 또는 정전 과정에서도 저장된 데이터를 유지할 수 있습니다.

호스트의 영구 메모리 리소스 소비 모드

물리적 PMem 디바이스를 호스트에 추가하면 ESXi가 PMem 리소스를 탐지하고 호스트에서 실행되는 가상 시스템에 호스트-로컬 PMem 데이터스토어로 제공합니다. 게스트 운영 체제에 따라 가상 시스템은 PMem 리소스에 직접 액세스할 수 있습니다.

각 호스트에는 호스트의 모든 PMem 리소스를 풀링하고 표현하는 로컬 PMem 데이터스토어 하나만 있을 수 있습니다.

영구 메모리는 메모리와 스토리지의 속성을 모두 가집니다. 따라서 가상 시스템은 ESXi 호스트의 PMem 리소스를 메모리(가상 NVDIMM 디바이스를 통해)로 사용하거나 스토리지(가상 PMem 하드 디스크를 통해)로 사용할 수 있습니다.

호스트-로컬 PMem 데이터스토어에는 직접 액세스되는 모든 NVDIMM 디바이스 및 가상 PMem 하드 디스크가 저장됩니다.

vPMem(가상 PMem)

이 모드에서 게스트 운영 체제가 PMem을 인식하는 경우 가상 시스템은 호스트의 물리적 PMem 리소스에 직접 액세스하여 표준 바이트 주소 지정 가능 메모리로 사용할 수 있습니다.

가상 시스템은 가상 NVDIMM(비휘발성 듀얼 인라인 메모리 모듈)을 사용하여 PMem에 직접 액세스합니다. NVDIMM은 일반 메모리 채널에 상주하지만 비휘발성 메모리를 포함하는 메모리 디바이스입니다. vSphere 6.7에서 가상 NVDIMM은 호스트의 물리적 PMem 영역을 나타내는 새로운 유형의 디바이스입니다. 단일 가상 시스템은 최대 64개의 가상 NVDIMM 디바이스를 가질 수 있습니다. 각 NVDIMM 디바이스는 호스트-로컬 PMem 데이터스토어에 저장됩니다.

참고 가상 시스템에 NVDIMM 디바이스를 추가하려면 가상 시스템이 하드웨어 버전 14여야 하며 게스트 운영 체제가 영구 메모리를 지원해야 합니다. 게스트 운영 체제가 PMem을 인식하지 못하면 PMem을 계속 사용할 수 있지만 NVDIMM 디바이스를 가상 시스템에 추가할 수 없습니다.

vPMemDisk(가상 PMem 디스크)

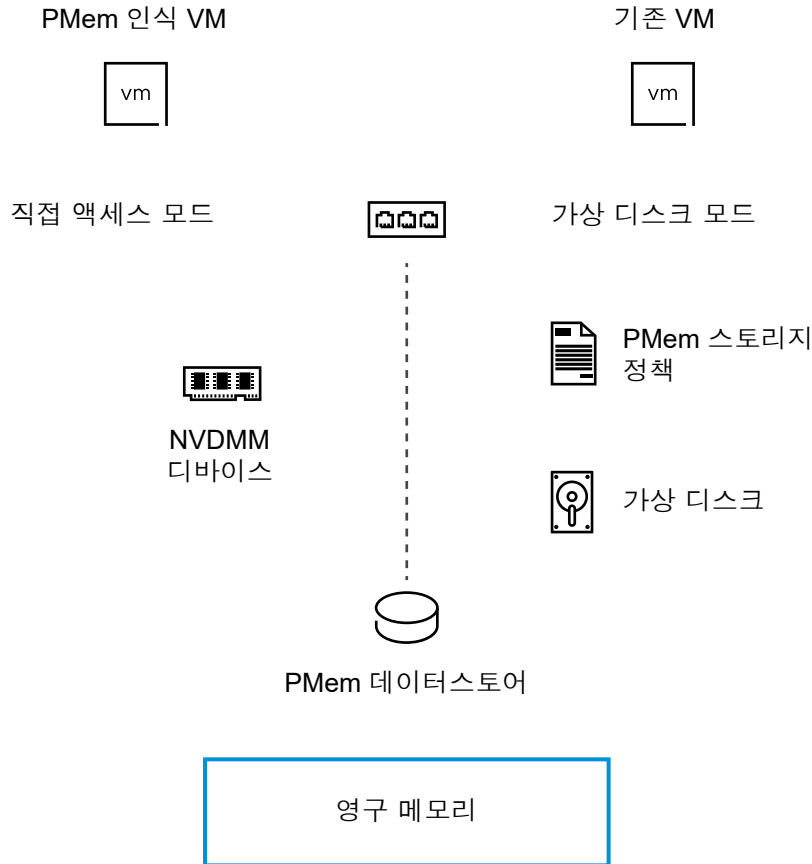
이 모드에서 가상 시스템은 호스트의 PMem 리소스에 직접 액세스할 수 없습니다.

가상 PMem 하드 디스크를 가상 시스템에 추가해야 합니다. 가상 PMem 하드 디스크는 PMem 스토리지 정책이 적용되는 전통적인 SCSI 디스크입니다. 이 정책은 하드 디스크를 자동으로 호스트-로컬 PMem 데이터스토어에 배치합니다.

이 사용 모드에서는 가상 시스템의 하드웨어 버전 및 게스트 운영 체제에 대한 요구 사항이 없습니다.

참고 게스트 운영 체제가 PMem을 인식하지 못하면 가상 시스템은 vPMemDisk를 통해서만 PMem을 사용할 수 있습니다.

다음 다이어그램은 영구 메모리 구성 요소가 상호 작용하는 방식을 보여줍니다.



NVDIMM 또는 가상 영구 메모리 디스크와 함께 VM을 구성하고 관리하는 방법에 대한 자세한 내용은 "vSphere 리소스 관리" 설명서를 참조하십시오.

PMem 데이터스토어 구조

VMware Host Client 사용자 인터페이스에서는 호스트-로컬 PMem 데이터스토어의 복잡한 구조에 대한 정보를 제공합니다. 이 정보를 분석하고 문제 해결 및 관리 목적으로 사용하려면 이러한 복잡한 구조와 관련된 개념을 숙지해야 합니다.

모듈

VMware Host Client 사용자 인터페이스에서 모듈은 호스트의 마더보드에 연결된 물리적 NVDIMM을 나타냅니다.

VMware Host Client에서 각 모듈의 상태를 확인하고 비정상 NVDIMM 모듈을 식별할 수 있습니다.

인터리빙 집합

인터리빙 집합은 하나 또는 여러 모듈의 논리적 그룹으로, 물리적 DIMM에 걸쳐 정보가 분산된 방식과 ESXi가 모듈에서 정보를 읽는 방식을 나타냅니다. ESXi는 각 인터리빙 집합에서 차례로 정보를 읽기 때문에 인터리빙 집합을 통해 메모리 처리량이 향상됩니다.

예를 들어 인터리빙 집합이 두 개의 모듈로 구성된 경우 ESXi는 두 개의 물리적 DIMM에서 병렬로 정보를 읽은 후 다음 인터리빙 집합을 처리합니다.

VMware Host Client 사용자 인터페이스에서는 NVDIMM이 인터리빙 집합으로 그룹화되는 방식에 대한 정보를 제공합니다.

네임스페이스

네임스페이스는 NVDIMM에서 연속적으로 주소가 지정된 메모리 범위 영역입니다. 네임스페이스는 전체 인터리빙 집합에 걸쳐 있을 수 있습니다. PMem 데이터스토어는 네임스페이스를 기반으로 구축됩니다.

VMware Host Client에서는 모든 네임스페이스의 용량, 상태 및 위치 ID를 볼 수 있습니다.

VMware Host Client에서 모듈, 인터리빙 집합 및 네임스페이스에 대한 정보 보기

VMware Host Client에서 호스트-로컬 PMem 데이터스토어의 모듈, 인터리빙 집합 및 네임스페이스에 대한 정보를 볼 수 있습니다. 따라서 비정상 모듈을 쉽게 식별하고 문제를 해결할 수 있습니다.

호스트-로컬 PMem 데이터스토어에서는 대부분의 기존 데이터스토어 관리 작업을 수행할 수 없습니다. 그러나 문제 해결을 위해 모듈, 인터리빙 집합 및 네임스페이스에 대한 정보를 사용할 수 있습니다.

사전 요구 사항

호스트에 하나 이상의 물리적 NVDIMM 디바이스가 있는지 확인합니다.

절차

- 1 **탐색기** 창에서 **스토리지**를 클릭합니다.
- 2 **영구 메모리** 탭에서 호스트-로컬 PMem 데이터스토어에 대한 정보를 봅니다.
 - PMem 데이터스토어를 구성하는 NVDIMM에 대한 정보를 보려면 **모듈**을 클릭합니다.
 - NVDIMM의 네임스페이스에 대한 정보를 보려면 **네임스페이스**를 클릭합니다.
 - 모듈 또는 물리적 NVDIMM이 인터리빙 집합으로 어떻게 그룹화되어 있는지 보려면 **인터리빙 집합**을 클릭합니다.

VMware Host Client에서 네임스페이스 삭제

ESXi가 아닌 이전에 호스트 시스템에 설치된 운영 체제를 통해 생성된 네임스페이스를 VMware Host Client에서 삭제할 수 있습니다.

사전 요구 사항

- 호스트를 유지 보수 모드로 전환합니다.
- 나중에 필요한 경우 네임스페이스의 콘텐츠를 백업합니다.

절차

- 1 VMware Host Client에서 **스토리지**를 클릭합니다.
- 2 **영구 메모리** 탭에서 **네임스페이스**를 클릭합니다.
- 3 (선택 사항) 네임스페이스 목록의 [상태] 열에서 ESXi가 현재 사용 중인 네임스페이스를 확인합니다.
공간을 확보하려면 [사용 중] 상태의 네임스페이스를 삭제해야 합니다.

- 네임스페이스를 선택하고 **삭제** 아이콘을 클릭합니다.

중요 네임스페이스를 삭제하면 데이터스토어의 공간이 확보되지만 호스트를 재부팅한 후에만 확보된 공간을 사용할 수 있습니다.

- 호스트 재부팅** 아이콘을 클릭하여 호스트를 재부팅합니다.

결과

선택된 네임스페이스가 PMem 데이터스토어에서 삭제됩니다. ESXi는 PMem 데이터스토어가 사용할 수 있는 새 네임스페이스를 자동으로 생성합니다. 새 네임스페이스는 삭제된 것과 동일한 용량, 유형 및 위치 ID를 갖습니다.

VMware Host Client에서 스토리지 모니터링

VMware Host Client에서는 ESXi 호스트의 스토리지 상태를 모니터링할 수 있습니다. 관리하는 호스트의 서로 다른 데이터스토어, 스토리지 어댑터 및 스토리지 디바이스와 연결된 이벤트 및 작업을 모니터링할 수도 있습니다.

VMware Host Client에서 데이터스토어 모니터링

VMware Host Client에서 데이터스토어의 상태 및 해당 데이터스토어와 연결된 이벤트와 작업도 모니터링할 수 있습니다.

vSphere 6.5 업데이트 1 이상부터는 vSphere Client에서 vSAN 서비스를 사용하도록 설정하며 vSAN 환경을 모니터링할 수도 있습니다.

절차

- VMware Host Client 인벤토리에서 **스토리지**를 클릭합니다.
- 데이터스토어**를 클릭합니다.
- 목록에서 데이터스토어를 클릭합니다.
VMware Host Client 인벤토리에서 데이터스토어가 확장됩니다.
- 데이터스토어 이름 아래에서 **모니터링**을 클릭합니다.
- (선택 사항) **이벤트**를 클릭하여 데이터스토어와 연결된 이벤트를 봅니다.
- (선택 사항) 호스트 vSAN 환경의 구성 매개 변수를 보려면 **vSAN**을 클릭합니다.
- (선택 사항) 이 데이터스토어에 있는 호스트를 보려면 **호스트**를 클릭합니다.
- (선택 사항) **성능 서비스, 네트워크, 물리적 디스크, 데이터, 클러스터 및 제한** 등의 다양한 매개 변수 상태에 대한 세부 정보를 보려면 **상태**를 클릭합니다.

VMware Host Client에서 vSAN 모니터링

VMware Host Client를 사용하여 ESXi 호스트의 vSAN 환경을 모니터링할 수 있습니다.

vSAN 개념

VMware vSAN은 소프트웨어 정의 방식을 사용하여 가상 시스템을 위한 공유 스토리지를 생성합니다.

VMware vSAN은 ESXi 호스트의 로컬 물리적 스토리지 리소스를 가상화한 후, 서비스 품질 요구 사항에 따라 분할하여 가상 시스템 및 애플리케이션에 할당할 수 있는 스토리지 풀로 변환합니다. vSAN은 ESXi 하이퍼바이저에 직접 구현됩니다.

vSAN은 하이브리드 또는 플래시 전용 클러스터로 작동하도록 구성할 수 있습니다. 하이브리드 클러스터에서는 플래시 디바이스를 캐시 계층에 사용하고 자화 디스크를 스토리지 용량 계층에 사용합니다. 플래시 전용 클러스터에서는 플래시 디바이스가 캐시 및 용량 모두에 사용됩니다.

vSAN은 기존 호스트 클러스터에 활성화하거나 새 클러스터를 생성할 때 활성화할 수 있습니다. vSAN은 모든 로컬 용량 디바이스를 vSAN 클러스터 내의 모든 호스트가 공유하는 단일 데이터스토어로 집계합니다. 클러스터에 용량 디바이스 또는 용량 디바이스가 포함된 호스트를 추가하여 데이터스토어를 확장할 수 있습니다. vSAN은 클러스터의 모든 ESXi 호스트가 비슷하거나 동일한 스토리지 구성을 포함하여 클러스터 멤버 전체에서 비슷하거나 동일한 구성을 공유할 때 가장 잘 작동합니다. 이 일관된 구성은 클러스터의 모든 디바이스 및 호스트 간에 가상 시스템 스토리지 구성 요소의 균형을 유지합니다. 로컬 디바이스가 없는 호스트도 vSAN 데이터스토어에 참여하고 해당 가상 시스템을 실행할 수 있습니다.

vSAN OSA(Original Storage Architecture)에서 스토리지 디바이스를 vSAN 데이터스토어에 기여하는 각 호스트는 하나 이상의 플래시 캐시용 디바이스와 하나 이상의 용량용 디바이스를 제공해야 합니다. 제공하는 호스트의 디바이스는 하나 이상의 디스크 그룹을 형성합니다. 각 디스크 그룹에는 플래시 캐시 디바이스 하나와 영구 스토리지를 위한 하나 또는 여러 개의 용량 디바이스가 포함됩니다. 각 호스트는 여러 디스크 그룹을 사용하도록 구성할 수 있습니다.

vSAN ESA(Express Storage Architecture)에서 vSAN에서 할당한 모든 스토리지 디바이스는 용량 및 성능에 기여합니다. vSAN에서 할당한 각 호스트의 스토리지 디바이스가 스토리지 풀을 구성합니다. 스토리지 풀은 호스트가 vSAN 데이터스토어에 제공하는 캐싱 및 용량을 나타냅니다.

vSAN 클러스터의 설계 및 크기 조정에 대한 모범 사례, 용량 고려 사항 및 일반 권장 사항은 "VMware vSAN 설계 및 크기 조정 가이드"를 참조하십시오.

vSAN의 특성

다음 특성은 vSAN, 해당 클러스터 및 데이터스토어에 적용됩니다.

vSAN에는 데이터 컴퓨팅 및 스토리지 환경에 복원력과 효율성을 추가하는 다양한 기능이 포함되어 있습니다.

표 5-1. vSAN 기능

지원되는 기능	설명
공유 스토리지 지원	vSAN은 공유 스토리지가 필요한 VMware 기능(예: HA, vMotion 및 DRS)을 지원합니다. 예를 들어 호스트가 오버로드되는 경우 DRS는 가상 시스템을 클러스터의 다른 호스트로 마이그레이션할 수 있습니다.
온디스크 형식	vSAN 온디스크 가상 파일 형식은 vSAN 클러스터당 고도로 확장 가능한 스냅샷 및 복제 관리 지원을 제공합니다. vSAN 클러스터당 지원되는 가상 시스템 스냅샷 및 복제 수에 대한 자세한 내용은 "구성 최대값" 설명서를 참조하십시오.

표 5-1. vSAN 기능 (계속)

지원되는 기능	설명
플래시 전용 및 하이브리드 구성	vSAN은 플래시 전용 또는 하이브리드 클러스터에 대해 구성할 수 있습니다.
장애 도메인	vSAN은 vSAN 클러스터가 데이터 센터의 여러 랙 또는 블레이드 서버 새시에 걸쳐 배포된 경우 랙 또는 새시 장애로부터 호스트를 보호하기 위한 장애 도메인의 구성을 지원합니다.
파일 서비스	vSAN 파일 서비스를 사용하여 클라이언트 워크스테이션이나 VM이 액세스할 수 있는 vSAN 데이터스토어에 파일 공유를 생성할 수 있습니다.
iSCSI 대상 서비스	vSAN iSCSI 대상 서비스를 통해 vSAN 클러스터 외부에 있는 호스트와 물리적 워크로드가 vSAN 데이터스토어에 액세스할 수 있습니다.
확장된 클러스터 및 2노드 클러스터	vSAN은 2개의 지리적 위치에 걸쳐 있는 확장된 클러스터를 지원합니다.
WSFC(Windows Server 장애 조치 클러스터) 지원	vSAN 6.7 Update 3 이상 릴리스에서는 노드 간 공유 디스크에 대한 액세스를 중재하기 위해 WSFC(Windows Server 장애 조치 클러스터)에 필요한 가상 디스크 수준 SCSI3-PR(SCSI-3 영구 예약)이 지원됩니다. SCSI-3 PR이 지원되면 기본적으로 vSAN 데이터스토어에서 VM 간에 공유되는 디스크 리소스로 WSFC를 구성할 수 있습니다. 현재 다음과 같은 구성이 지원됩니다. <ul style="list-style-type: none"> ■ 클러스터당 최대 6개의 애플리케이션 노드 ■ 노드당 최대 64개의 공유 가상 디스크 <p>참고 Microsoft Windows Server 2012 이상에서 실행되는 Microsoft SQL Server 2012 이상은 vSAN에서 검증되었습니다.</p>
vSAN Health Service	vSAN Health Service에는 클러스터 구성 요소 문제의 원인을 모니터링하고 문제를 해결 및 진단하며 잠재적인 위험을 식별하기 위한 미리 구성된 상태 점검 테스트가 포함됩니다.
vSAN 성능 서비스	vSAN 성능 서비스에는 IOPS, 처리량, 지연 시간 및 정체를 모니터링하는 데 사용되는 통계 차트가 포함됩니다. vSAN 클러스터, 호스트, 디스크 그룹, 디스크 및 VM의 성능을 모니터링할 수 있습니다.
vSphere 스토리지 기능과 통합	vSAN은 기존에 VMFS 및 NFS 스토리지와 함께 사용된 vSphere 데이터 관리 기능과 통합됩니다. 이러한 기능에는 스냅샷, 연결된 클론 및 vSphere Replication이 포함됩니다.
가상 시스템 스토리지 정책	vSAN은 VM 스토리지 정책과 함께 작동하여 VM 중심의 스토리지 관리 방식을 지원합니다. 배포 중에 가상 시스템에 스토리지 정책을 할당하지 않으면 vSAN 기본 스토리지 정책이 VM에 자동으로 할당됩니다.
빠른 프로비저닝	vSAN을 사용하면 가상 시스템 생성 및 배포 작업 도중 vCenter Server [®] 에서 스토리지를 빠르게 프로비저닝할 수 있습니다.
중복 제거 및 압축	vSAN은 블록 수준 중복 제거와 압축을 수행하여 스토리지 공간을 절약합니다. vSAN 플래시 전용 클러스터에서 중복 제거와 압축을 사용하도록 설정하면 각 디스크 그룹 내의 중복 데이터가 줄어듭니다. 중복 제거 및 압축은 클러스터 전체 설정이지만 이러한 기능은 디스크 그룹 단위로 적용됩니다. 압축 전용 vSAN은 디스크별로 적용됩니다.

표 5-1. vSAN 기능 (계속)

지원되는 기능	설명
저장된 데이터 암호화	vSAN에는 저장된 데이터 암호화가 제공됩니다. 데이터는 중복 제거 같은 다른 모든 처리가 수행된 이후에 암호화됩니다. 저장된 데이터 암호화 기능은 디바이스가 클러스터에서 제거되는 경우 스토리지 디바이스의 데이터를 보호합니다.
전송 중 데이터 암호화	vSAN은 클러스터의 호스트 간에 전송 중인 데이터를 암호화할 수 있습니다. 전송 중 데이터 암호화를 사용하도록 설정하면 vSAN은 호스트 간의 모든 데이터 및 메타데이터 트래픽을 암호화합니다.
SDK 지원	VMware vSAN SDK는 VMware vSphere Management SDK의 확장입니다. 여기에는 개발자가 vSAN의 설치, 구성, 모니터링 및 문제 해결을 자동화할 수 있도록 지원하는 설명서, 라이브러리 및 코드 예제가 포함되어 있습니다.

VMware Host Client에서 vSAN 모니터링

VMware Host Client를 사용하여 ESXi 호스트의 vSAN 환경을 모니터링할 수 있습니다.

사전 요구 사항

데이터스토어에 대한 vSAN 관련 화면을 보려면 vSphere Client에서 vSAN 서비스를 사용하도록 설정해야 합니다.

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭합니다.
- 2 **데이터 스토어** 탭에서 **vSAN 데이터스토어**를 클릭합니다.
VMware Host Client 탐색기에서 vSAN 데이터스토어가 확장됩니다.
- 3 **모니터**를 클릭합니다.
UI에 **vSAN**, **호스트** 및 **상태** 탭이 표시됩니다.

옵션	설명
vSAN	<p>현재 호스트에 대한 구성을 표시합니다. 할당 모드와 중복 제거에 대한 설정을 편집할 수 있습니다. 또한 다음에 대한 설정을 볼 수 있습니다.</p> <ul style="list-style-type: none"> ■ 암호화 - vSAN은 전체 vSAN 데이터스토어에 대한 정보의 암호화를 지원합니다. ■ iSCSI 서비스 - iSCSI 서비스를 통한 추가 서비스입니다. ■ 성능 서비스 - 데이터스토어의 작동 방식에 대한 데이터를 수집합니다. 예를 들어 읽기/쓰기 작업의 속도를 수집합니다.
호스트	vSAN 서버에 있는 모든 호스트와 해당 IP 및 소속 장애 도메인의 목록을 표시합니다.
상태	<p>상태 탭에는 그룹으로 구성된 테스트가 포함되어 있습니다. 다음 그룹이 표시됩니다.</p> <ul style="list-style-type: none"> ■ 성능 서비스 ■ 네트워크 ■ 물리적 디스크 ■ 데이터 ■ 클러스터 ■ 제한 <p>각 그룹에는 오류, 주의, 알 수 없음 또는 정상 상태 아이콘이 표시됩니다. 그룹의 상태는 해당 그룹에 속한 테스트 중 가장 심각한 상태를 나타냅니다. 테스트와 해당 설명을 보려면 관심 있는 그룹의 오른쪽 상단에 있는 확장 아이콘을 클릭합니다. 확장된 카드에서 해당 그룹에 속한 모든 테스트와 테스트 실행 결과를 검토하고 각 테스트에서 시스템에 대해 조사한 사항에 대한 자세한 정보를 얻을 수 있습니다.</p>

4 모니터링할 vSAN 매개 변수를 선택합니다.

vSAN 데이터스토어에 대한 설정 편집

현재 호스트의 잘못 구성된 상태를 종료해야 하는 경우 vSAN 데이터스토어에 대한 설정을 편집할 수 있습니다.

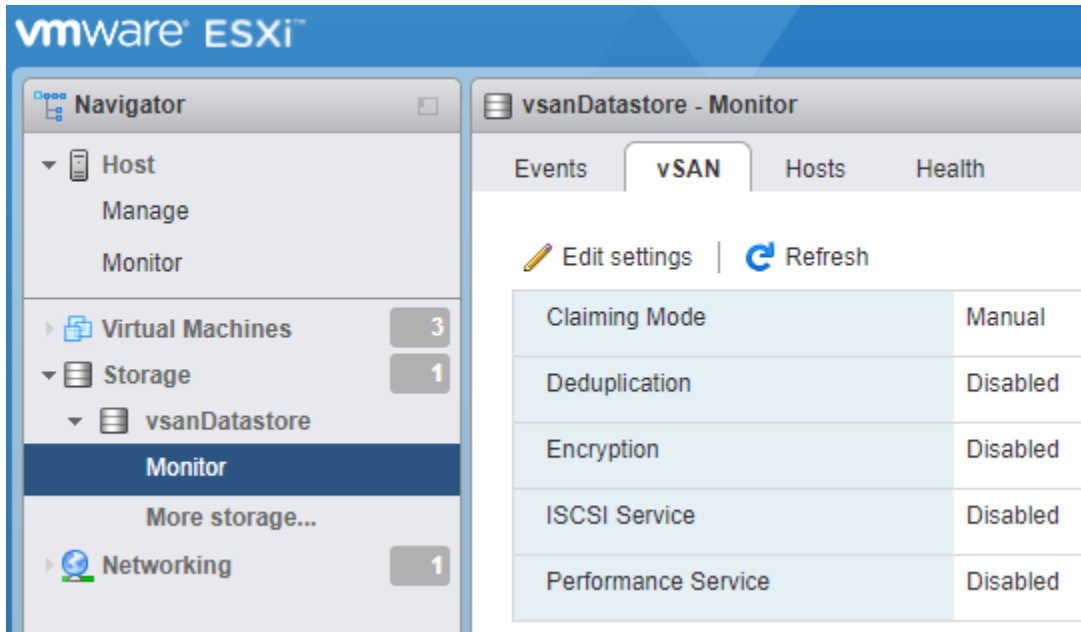
vSAN 데이터스토어에 대한 **할당 모드** 및 **중복 제거** 설정만 편집할 수 있습니다. 이러한 변경 내용은 현재 호스트에만 적용되며 vSAN 클러스터에 참여하는 다른 호스트에는 동기화되지 않습니다.

참고 문제 해결에만 이러한 설정을 사용하십시오.

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭합니다.
- 2 **데이터스토어** 탭의 테이블에서 vSAN 데이터스토어를 클릭합니다.

3 모니터를 클릭하고 vSAN 탭을 클릭합니다.



4 설정 편집을 클릭합니다.

설정 편집 대화상자가 열립니다.

5 설정을 변경합니다. 할당 모드에서 자동 또는 수동을 선택합니다.

옵션	작업
할당 모드	a 할당 모드에서 자동 또는 수동을 선택합니다. <ul style="list-style-type: none"> ■ 자동을 선택하는 경우 자동으로 모든 디스크가 사용되고 하나의 그룹 또는 같은 크기의 여러 그룹에 할당됩니다. <p>참고 자동 모드는 더 이상 지원되지 않습니다. 대부분의 vSAN 기능과 호환되지 않는 하이브리드 디스크 그룹만 할당할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 수동을 선택하는 경우 수동으로 디스크를 그룹으로 구성하고 vSphere Web Client를 사용하여 회수해야 합니다. 예를 들어 vCenter Server를 사용할 수 없을 때는 수동 할당 모드를 선택하는 것이 적절합니다.
중복 제거	a 중복 제거에 사용 또는 사용 안 함을 선택합니다.

6 저장을 클릭합니다.

VMware Host Client에서 스토리지 새로 고침 및 다시 검색 작업 수행

데이터스토어, 스토리지 디바이스 및 스토리지 어댑터를 새로 고치면 VMware Host Client에 표시되는 목록 및 스토리지 정보가 업데이트됩니다. 데이터스토어 용량과 같은 정보가 업데이트됩니다.

스토리지 관리 작업을 수행하거나 SAN 구성을 변경할 경우에는 스토리지를 다시 검색해야 할 수 있습니다.

VMware Host Client에서 어댑터 다시 검색 수행

SAN 구성을 변경하는 경우 해당 변경 사항이 특정 어댑터를 통해 액세스되는 스토리지로 국한되면 이 어댑터에 대해서만 다시 검색을 수행합니다. 어댑터를 다시 검색하면 해당 어댑터에서 사용할 수 있는 새 LUN을 검색할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **어댑터**를 클릭합니다.
- 2 **다시 검색**을 클릭합니다.

VMware Host Client에서 디바이스 다시 검색 수행

디바이스를 다시 검색하면 디바이스에서 사용할 수 있는 새 VMFS 볼륨을 검색할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **스토리지**를 클릭하고 **디바이스**를 클릭합니다.
- 2 **다시 검색**을 클릭합니다.

VMware Host Client에서 검색되는 스토리지 디바이스 수 변경

ESXi 호스트에 대해 검색되는 LUN ID의 범위는 0-16,383입니다. 16,383보다 큰 LUN ID는 ESXi에서 무시합니다. 구성 가능한 `Disk.MaxLUN` 매개 변수는 검색된 LUN ID의 범위를 제어합니다. 이 매개 변수의 기본값은 1024입니다.

`Disk.MaxLUN` 매개 변수는 SCSI 대상이 `REPORT_LUNS`를 사용한 직접 검색을 지원하지 않을 경우 SCSI 검색 코드가 개별 `INQUIRY` 명령을 사용하여 검색을 시도하는 LUN의 수도 결정합니다.

필요에 따라 `Disk.MaxLUN` 매개 변수를 수정할 수 있습니다. 예를 들어 환경에 LUN ID가 1에서 100까지인 적은 수의 스토리지 디바이스가 있는 경우에는 값을 101로 설정합니다. 따라서 `REPORT_LUNS`를 지원하지 않는 대상에서 디바이스 검색 속도를 높일 수 있습니다. 값을 낮추면 다시 검색 시간과 부팅 시간을 단축할 수 있습니다. 하지만 스토리지 디바이스를 다시 검색하는 시간은 스토리지 시스템 유형 및 스토리지 시스템의 로드와 같이 다른 요소에 따라 달라질 수도 있습니다.

반면에 해당 환경에서 1023보다 큰 LUN ID를 사용할 경우에는 값을 증가시켜야 할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **관리**를 클릭하고 **고급 설정**을 클릭합니다.
- 2 `Disk.MaxLUN`으로 스크롤합니다.
- 3 `Disk.MaxLUN`을 마우스 오른쪽 버튼으로 클릭하고 **옵션 편집**을 클릭합니다.
- 4 새 값을 입력하고 **저장**을 클릭합니다.

SCSI 검색 코드는 입력한 값보다 크거나 같은 ID인 LUN을 검색하지 않습니다.

예를 들어 LUN ID를 0부터 100까지 검색하려면 `Disk.MaxLUN`을 101로 설정합니다.

VMware Host Client의 네트워킹

6

VMware Host Client를 사용하여 ESXi 호스트에 연결하면 vSphere 표준 스위치, 포트 그룹, 물리적 NIC, VMkernel NIC 및 TCP/IP 스택을 보고 구성할 수 있습니다.

다음으로 아래 항목을 읽으십시오.

- VMware Host Client에서 포트 그룹 관리
- VMware Host Client에서 가상 스위치 관리
- VMware Host Client에서 물리적 네트워크 어댑터 관리
- VMware Host Client에서 VMkernel 네트워크 어댑터 관리
- VMware Host Client에서 호스트의 TCP/IP 스택 구성 보기
- VMware Host Client에서 호스트에 있는 TCP/IP 스택의 구성 변경
- VMware Host Client에서 ESXi 방화벽 구성
- VMware Host Client에서 네트워킹 이벤트 및 작업 모니터링

VMware Host Client에서 포트 그룹 관리

포트 그룹 설정을 관리하여 트래픽 관리를 구성하고, 네트워킹 보안을 강화하고, 성능을 향상시킬 수 있습니다.

VMware Host Client를 사용하여 포트 그룹을 추가하고 제거할 수 있습니다. 또한 포트 그룹 정보를 검사하고 NIC 팀 구성 및 트래픽 조절과 같은 포트 그룹 설정을 편집할 수 있습니다.

VMware Host Client에서 포트 그룹 정보 보기

VMware Host Client에서 포트 그룹 구성, 네트워크 세부 정보, 가상 스위치 토폴로지, NIC 팀 구성 정책, 오프로드 정책 및 보안 정책에 대한 정보를 볼 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **네트워킹**을 클릭하고 **포트 그룹**을 클릭합니다.
- 2 사용할 수 있는 포트 그룹 목록에서 항목을 클릭합니다.

네트워크 세부 정보, 가상 스위치 토폴로지, NIC 팀 구성 정책, 오프로드 정책 및 보안 정책에 대한 정보가 표시됩니다.

VMware Host Client에서 가상 스위치 포트 그룹 추가

VMware Host Client에서 가상 스위치에 포트 그룹을 추가할 수 있습니다. 포트 그룹은 가상 시스템을 위한 네트워크를 제공합니다.

절차

- 1 VMware Host Client 인벤토리에서 **네트워킹**을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **포트 그룹 추가**를 클릭합니다.
- 2 새 포트 그룹의 이름을 입력합니다.
- 3 VLAN ID를 설정하여 포트 그룹에서의 VLAN 처리를 구성합니다.

VLAN ID는 또한 포트 그룹의 VLAN 태깅 모드를 반영합니다.

VLAN 태그 지정 모드	VLAN ID	설명
EST(External Switch Tagging)	0	가상 스위치는 VLAN과 연결된 트래픽을 전달하지 않습니다.
VST(Virtual Switch Tagging)	1 ~ 4094	가상 스위치는 입력한 태그로 트래픽을 태그합니다.
VGT(Virtual Guest Tagging)	4095	가상 시스템은 VLAN을 처리합니다. 가상 스위치는 모든 VLAN의 트래픽을 허용합니다.

- 4 드롭다운 메뉴에서 가상 스위치를 선택합니다.
- 5 **보안**을 확장하고 비규칙 모드, MAC 주소 변경 및 위조 전송에 대해 사용하려는 옵션을 선택합니다.
- 6 **추가**를 클릭합니다.
포트 그룹이 생성됩니다.
- 7 (선택 사항) **새로 고침**을 클릭하여 목록에서 새 포트 그룹을 표시합니다.

VMware Host Client에서 포트 그룹 설정 편집

VMware Host Client에서 네트워크 보안을 개선하고 네트워크 성능을 높이기 위해서 포트 그룹 이름, VLAN ID, 가상 스위치 같은 다양한 포트 그룹 설정을 편집할 수 있습니다. 또한 보안, NIC 팀 구성 및 트래픽 조절 구성 요소를 구성할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **네트워킹**을 클릭하고 **포트 그룹**을 클릭합니다.
- 2 목록에서 편집하려는 포트 그룹을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
- 3 (선택 사항) 새 포트 그룹 이름을 입력합니다.
- 4 (선택 사항) VLAN ID의 새 값을 입력합니다.

VLAN ID는 포트 그룹의 VLAN 태깅 모드를 반영합니다.

VLAN 태그 지정 모드	VLAN ID	설명
EST(External Switch Tagging)	0	가상 스위치는 VLAN과 연결된 트래픽을 전달하지 않습니다.
VST(Virtual Switch Tagging)	1 ~ 4094	가상 스위치는 입력한 태그로 트래픽을 태그합니다.
VGT(Virtual Guest Tagging)	4095	가상 시스템은 VLAN을 처리합니다. 가상 스위치는 모든 VLAN의 트래픽을 허용합니다.

- 5 (선택 사항) 드롭다운 메뉴에서 가상 스위치를 선택합니다.
- 6 (선택 사항) **보안**을 확장하고 vSwitch에서 보안 정책 예외를 거부, 수락 또는 상속할지를 선택합니다.

옵션	설명
비규칙 모드	<ul style="list-style-type: none"> ■ 거부. 게스트 어댑터를 비규칙(Promiscuous) 모드로 설정해도 어댑터로 수신되는 프레임에 영향을 미치지 않습니다. ■ 동의. 게스트 어댑터를 무차별 모드로 설정하면 어댑터는 vSphere Distributed Switch를 통과하는 프레임 중 해당 어댑터가 연결되어 있는 포트 그룹의 VLAN 정책에서 허용하는 모든 프레임을 감지합니다. ■ vSwitch에서 상속. 게스트 어댑터를 비규칙 모드로 설정하면 어댑터는 연결된 가상 스위치에서 구성을 상속합니다.
MAC 주소 변경 사항	<ul style="list-style-type: none"> ■ 거부. MAC 주소 변경을 거부로 설정할 경우, 게스트 운영 체제에서 어댑터의 MAC 주소를 .vmx 구성 파일에 지정된 MAC 주소와 다르게 변경하면 모든 인바운드 프레임이 손실됩니다. 게스트 운영 체제가 .vmx 구성 파일에서 MAC 주소와 일치하도록 MAC 주소를 다시 변경하면 인바운드 프레임이 다시 통과합니다. ■ 동의. 게스트 운영 체제에서 MAC 주소를 변경하면 그대로 적용됩니다. 즉, 새 MAC 주소에 대한 프레임이 수신됩니다. ■ vSwitch에서 상속. MAC 주소 변경을 vSwitch에서 상속으로 설정하면 MAC 주소가 연결된 가상 스위치 중 하나의 주소로 변경됩니다.
위조 전송	<ul style="list-style-type: none"> ■ 거부. 어댑터에 설정된 주소와 다른 소스 MAC 주소를 사용하는 모든 아웃바운드 프레임이 삭제됩니다. ■ 동의. 필터링 없이 모든 아웃바운드 프레임이 통과합니다. ■ vSwitch에서 상속. 연결된 가상 스위치에서 아웃바운드 프레임 구성이 상속됩니다.

7 (선택 사항) NIC 팀 구성을 확장하고 다음 구성 요소를 구성합니다.

옵션	설명
로드 밸런싱	<p>업링크를 어떻게 선택하는지를 지정합니다.</p> <ul style="list-style-type: none"> ■ vSwitch에서 상속. 연결된 가상 스위치에 대해 선택된 업링크를 선택합니다. ■ IP 해시 기준 라우팅. 각 패킷의 소스 및 대상 IP 주소의 해시에 기반하여 업링크를 선택합니다. 비 IP 패킷에 대해서는 오프셋에 있는 어떤 것도 해시를 계산하기 위해 사용 됩니다. ■ 소스 MAC 해시 기준 라우팅. 소스 이더넷의 해시에 기반하여 업링크를 선택합니다. ■ 원시 포트 ID에 기반한 라우팅. 원시 포트 ID에 기반한 업링크를 선택합니다. ■ 명시적 페일오버 순서 사용. 페일오버 감지 기준을 통과한 활성 어댑터 목록에서 순서가 가장 높은 업링크를 항상 사용합니다. <p>참고 IP 기반의 팀 구성에서는 물리적 스위치를 EtherChannel로 구성해야 합니다. 다른 모든 옵션에서는 EtherChannel을 비활성화해야 합니다.</p>
네트워크 페일오버 감지	<p>페일오버 감지에 사용하는 방법을 지정합니다.</p> <ul style="list-style-type: none"> ■ ■ vSwitch에서 상속. 연결된 가상 스위치의 관련 구성을 상속합니다. ■ 링크 상태만. 네트워크 어댑터가 제공하는 링크 상태만 기준으로 합니다. 이 옵션은 케이블 당김, 물리적 스위치 전원 고장과 같은 고장을 감지하지만 스페닝 트리 (spanning tree)로 차단되는 물리적 스위치 포트 또는 물리적 스위치의 다른 측면에서 케이블 당김이나 잘못된 VLAN으로의 잘못된 구성과 같은 구성 오류는 감지하지 않습니다. ■ 비콘만. 팀의 모든 NIC에서 beacon probe를 보내고 수신하여 해당 정보를 연결 상태와 함께 사용하여 연결 장애를 판단합니다. 링크 상태만으로 감지할 수 없는 많은 장애를 감지합니다. <p>참고 IP-해시 로드 밸런싱과 함께 신호 검색을 사용하지 않습니다.</p>
스위치 알림	<p>예, 아니요 또는 vSwitch에서 상속을 선택하여 페일오버가 발생하는 경우 스위치에 알릴 지를 선택합니다.</p> <p>예를 선택한 경우, 가상 NIC가 Distributed Switch에 연결될 때 또는 가상 NIC의 트래픽이 페일오버 이벤트로 인해 팀의 다른 물리적 NIC로 라우팅될 때 물리적 스위치의 조회 표를 업데이트하기 위해 네트워크 전체에 알림이 전송됩니다. 페일오버 발생의 가장 낮은 지연 시간과 vMotion을 사용한 마이그레이션 때문에 거의 모든 경우에 이 프로세스가 선호 됩니다.</p> <p>참고 포트 그룹을 사용하는 가상 시스템이 유니캐스트 모드의 Microsoft 네트워크 로드 밸런싱을 이용할 때에는 이 옵션을 사용하지 않습니다. NLB가 멀티캐스트 모드에서 실행 되는 경우에는 이러한 문제가 존재하지 않습니다.</p>

옵션	설명
페일백	예, 아니요 또는 vSwitch에서 상속을 선택하여 페일백을 비활성화 또는 활성화합니다. 이 옵션은 물리적 어댑터가 고장을 복구한 후에 어떻게 실행 상태로 돌아가는가를 결정합니다. 페일백을 기본 설정인 예로 설정한 경우 인계받았던 대기 어댑터(있는 경우)를 대체함으로써 복구 시 어댑터가 즉시 실행 상태로 돌아갑니다. 페일오버가 아니요로 설정된 경우 고장난 어댑터는 복구되어도 현재의 다른 활성 어댑터가 고장나 교체가 필요할 때까지 비활성 상태로 둡니다.
페일오버 순서	업링크로 워크로드를 어떻게 분산하는가를 지정합니다. 사용 중인 업링크가 고장나는 긴급 상황을 고려하여 일부 업링크만 사용하고 나머지 업링크를 두려는 경우, 해당 업링크를 다른 그룹으로 이동하고 이 조건을 설정합니다. <ul style="list-style-type: none"> ■ 활성 업링크. 네트워크 어댑터 연결을 사용할 수 있고 활성 상태인 경우에 이 업링크를 계속 사용합니다. ■ 대기 업링크. 활성 어댑터의 연결 중 하나가 끊어져 있는 경우 이 업링크를 사용합니다. <p>참고 IP-해시 로드 밸런싱을 이용할 때에는 대기 업링크를 구성하지 않습니다. 포트 그룹 구성 요소 중 하나라도 연결된 가상 스위치에서 구성을 상속하도록 구성된 경우 페일오버 순서를 구성할 수 없습니다.</p>

- 8 (선택 사항) 트래픽 조절을 구성하려면 **트래픽 조절**을 확장하고 **사용**을 클릭한 후 다음 매개 변수를 지정합니다.

옵션	설명
평균 대역폭	포트 통과를 제한하는 시간 경과별 평균 초당 비트 수, 즉 허용되는 평균 로드를 설정합니다.
최대 대역폭	트래픽 버스트를 송신/수신할 때 포트 통과를 제한하는 초당 최대 비트 수입니다. 포트가 추가 버스트를 사용할 때마다 포트에서 사용하는 최대 대역폭입니다.
버스트 크기	버스트에 제한할 최대 바이트 수입니다. 이 매개 변수를 설정하면 할당된 대역폭의 일부만 사용될 때 포트에 추가 버스트가 제공될 수 있습니다. 추가 버스트를 사용할 수 있는 경우, 평균 대역폭 에서 지정한 것보다 더 많은 대역폭이 포트에 필요할 때 일시적으로 더 높은 속도로 데이터를 전송할 수 있습니다. 이 매개 변수는 추가 버스트에서 누적되어 더 높은 속도로 전송될 수 있는 최대 바이트 수를 나타냅니다.

트래픽 조절 정책은 가상 스위치에 연결된 각 가상 네트워크 어댑터의 트래픽에 적용됩니다.

- 9 **저장**을 클릭하여 변경 내용을 적용합니다.

VMware Host Client에서 가상 스위치 포트 그룹 제거

연결된 레이블 지정 네트워크가 더 이상 필요하지 않은 경우 가상 스위치에서 포트 그룹을 제거할 수 있습니다.

사전 요구 사항

제거하려는 포트 그룹에 VMkernel NIC 및 전원이 켜진 가상 시스템이 연결되어 있지 않은지 확인합니다.

절차

- 1 VMware Host Client 인벤토리에서 **네트워킹**을 클릭하고 **포트 그룹** 탭을 클릭합니다.

- 2 제거하려는 포트 그룹을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **제거**를 선택합니다.
- 3 포트 그룹을 제거하려면 **제거**를 클릭합니다.
- 4 (선택 사항) **새로 고침**을 클릭하여 포트 그룹을 제거했는지 확인합니다.

VMware Host Client에서 가상 스위치 관리

VMware Host Client에서 링크 검색, NIC 팀 구성, 트래픽 조절 같은 다양한 가상 스위치 설정을 구성할 수 있습니다.

VMware Host Client에서 가상 스위치 정보 보기

VMware Host Client에서 구성, 네트워크 세부 정보, 가상 스위치 토폴로지 등과 같은 가상 스위치에 대한 정보를 볼 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **네트워킹**을 클릭하고 **가상 스위치**를 클릭합니다.
- 2 사용할 수 있는 가상 스위치 목록에서 스위치를 클릭합니다.

가상 스위치 구성, 네트워크 세부 정보 및 가상 스위치 토폴로지에 대한 정보가 표시됩니다.

VMware Host Client에서 표준 가상 스위치 추가

VMware Host Client에서 표준 가상 스위치를 추가하여 관리하는 호스트 및 해당 호스트의 가상 시스템에 대한 네트워크 연결을 제공하고 VMkernel 트래픽을 처리할 수 있습니다. 생성하려는 연결 유형에 따라 VMkernel 어댑터를 포함하는 vSphere 표준 스위치를 생성하거나 기존 물리적 네트워크 어댑터를 새 스위치에 연결하거나 가상 시스템 포트 그룹을 포함하는 스위치를 생성할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **네트워킹**을 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 **표준 vSwitch 추가**를 선택합니다.
- 2 (선택 사항) **업링크 추가**를 클릭하여 가상 스위치에 새 물리적 업링크를 추가합니다.
- 3 가상 스위치 이름을 입력하고 **가상 스위치 생성**을 클릭합니다.
- 4 가상 스위치의 업링크를 선택합니다.
- 5 **링크 검색**을 확장하고 가상 스위치 모드에 대한 옵션을 선택합니다.

작업	설명
수신	ESXi에서 관련된 물리적 스위치 포트에 대한 정보를 감지 및 표시하지만 vSphere 표준 스위치에 대한 정보는 스위치 관리자가 사용할 수 없습니다.
알림	ESXi에서 vSphere 표준 스위치에 대한 정보를 스위치 관리자가 사용할 수 있도록 하지만 물리적 스위치에 대한 정보는 감지 및 표시하지 않습니다.

작업	설명
둘 다	ESXi에서 관련된 물리적 스위치에 대한 정보를 감지 및 표시하고 스위치 관리자가 vSphere 표준 스위치에 대한 정보를 사용할 수 있도록 합니다.
없음	ESXi에서 관련된 물리적 스위치 포트에 대한 정보를 감지하거나 표시하지 않으며 vSphere 표준 스위치에 대한 정보를 스위치 관리자가 사용할 수 없습니다.

- 6 프로토콜 섹션의 드롭다운 메뉴에서 **Cisco Discovery Protocol**을 선택합니다.
- 7 **보안**을 확장하고 표준 스위치에 연결된 가상 시스템의 비규칙 모드, MAC 주소 변경 및 위조 전송을 수락하거나 거부합니다.

옵션	설명
무차별 모드	<ul style="list-style-type: none"> ■ 거부. VM 네트워크 어댑터가 가상 시스템에 전송된 프레임만 수신합니다. ■ 동의. 가상 스위치가 VM 네트워크 어댑터가 연결된 포트에 대한 활성 VLAN 정책에 따라 모든 프레임을 가상 시스템에 전달합니다. <p>참고 무차별 모드는 안전하지 않은 작업 모드입니다. 방화벽, 포트 스캐너, 침입 감지 시스템이 무차별 모드로 실행되어야 합니다.</p>
MAC 주소 변경	<ul style="list-style-type: none"> ■ 거부. 게스트 운영 체제가 가상 시스템의 유효 MAC 주소를 VM 네트워크 어댑터의 MAC 주소(.vmx 구성 파일에서 설정)와 다른 값으로 변경하는 경우 스위치가 어댑터에 대한 모든 인바운드 프레임을 삭제합니다. <p>게스트 운영 체제가 가상 시스템의 유효 MAC 주소를 VM 네트워크 어댑터의 MAC 주소로 다시 변경하는 경우 가상 시스템이 프레임을 다시 수신합니다.</p> <ul style="list-style-type: none"> ■ 동의. 게스트 운영 체제가 가상 시스템의 유효 MAC 주소를 VM 네트워크 어댑터의 MAC 주소와 다른 값으로 변경하는 경우 스위치가 프레임을 새 주소에 전달할 수 있도록 허용합니다.
위조 전송	<ul style="list-style-type: none"> ■ 거부. 소스 MAC 주소가 .vmx 구성 파일에 있는 주소와 다를 경우 스위치가 가상 시스템 어댑터에서 모든 아웃바운드 프레임을 삭제합니다. ■ 동의. 스위치가 필터링을 수행하지 않고 모든 아웃바운드 프레임을 허용합니다.

- 8 **추가**를 클릭합니다.

VMware Host Client에서 표준 가상 스위치 제거

더 이상 필요 없는 가상 표준 스위치를 제거할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **네트워킹**을 클릭하고 **가상 스위치** 탭을 클릭합니다.
- 2 목록에서 제거하려는 가상 스위치를 마우스 오른쪽 버튼으로 클릭하고 **제거**를 클릭합니다.
- 3 **예**를 클릭합니다.

VMware Host Client에서 가상 스위치에 물리적 업링크 추가

여러 어댑터를 단일 vSphere 표준 스위치에 연결하여 NIC 팀 구성을 제공할 수 있습니다. 이 팀은 트래픽을 공유하고 페일오버를 제공할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **네트워킹**을 클릭하고 **가상 스위치**를 클릭합니다.
- 2 목록에서 가상 스위치를 클릭하고 **업링크 추가**를 클릭합니다.
- 3 사용 가능한 옵션에서 물리적 NIC를 선택합니다.
- 4 **저장**을 클릭합니다.

VMware Host Client에서 가상 스위치 설정 편집

VMware Host Client에서 가상 스위치 업링크 같은 가상 스위치 설정을 편집할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **네트워킹**을 클릭하고 **가상 스위치**를 클릭합니다.
- 2 편집하려는 가상 스위치를 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 클릭합니다.
- 3 (선택 사항) **업링크 추가**를 클릭하여 가상 스위치에 새 물리적 업링크를 추가합니다.
- 4 MTU(최대 전송 단위)를 변경합니다.

MTU는 점보 프레임 사용할 수 있도록 설정하여 단일 패킷으로 전송되는 페이로드 데이터의 양을 늘려 네트워크 효율성을 높입니다.

- 5 (선택 사항) **제거** 아이콘(✖)을 클릭하여 가상 스위치로부터 이전 업링크를 제거합니다.
- 6 **링크 검색**을 확장하고 가상 스위치 모드에 대한 옵션을 선택합니다.

작업	설명
수신	ESXi에서 관련된 물리적 스위치 포트에 대한 정보를 감지 및 표시하지만 vSphere 표준 스위치에 대한 정보는 스위치 관리자가 사용할 수 없습니다.
알림	ESXi에서 vSphere 표준 스위치에 대한 정보를 스위치 관리자가 사용할 수 있도록 하지만 물리적 스위치에 대한 정보는 감지 및 표시하지 않습니다.
둘 다	ESXi에서 관련된 물리적 스위치에 대한 정보를 감지 및 표시하고 스위치 관리자가 vSphere 표준 스위치에 대한 정보를 사용할 수 있도록 합니다.
없음	ESXi에서 관련된 물리적 스위치 포트에 대한 정보를 감지하거나 표시하지 않으며 vSphere 표준 스위치에 대한 정보를 스위치 관리자가 사용할 수 없습니다.

- 7 프로토콜 섹션의 드롭다운 메뉴에서 **Cisco Discovery Protocol**을 선택합니다.

8 보안을 확장하고 표준 스위치에 연결된 가상 시스템의 비규칙 모드, MAC 주소 변경 및 위조 전송을 수락하거나 거부합니다.

옵션	설명
무차별 모드	<ul style="list-style-type: none"> ■ 거부. VM 네트워크 어댑터가 가상 시스템에 전송된 프레임만 수신합니다. ■ 동의. 가상 스위치가 VM 네트워크 어댑터가 연결된 포트에 대한 활성 VLAN 정책에 따라 모든 프레임을 가상 시스템에 전달합니다. <p>참고 무차별 모드는 안전하지 않은 작업 모드입니다. 방화벽, 포트 스캐너, 침입 감지 시스템이 무차별 모드로 실행되어야 합니다.</p>
MAC 주소 변경	<ul style="list-style-type: none"> ■ 거부. 게스트 운영 체제가 가상 시스템의 유효 MAC 주소를 VM 네트워크 어댑터의 MAC 주소(.vmmx 구성 파일에서 설정)와 다른 값으로 변경하는 경우 스위치가 어댑터에 대한 모든 인바운드 프레임을 삭제합니다. <p>게스트 운영 체제가 가상 시스템의 유효 MAC 주소를 VM 네트워크 어댑터의 MAC 주소로 다시 변경하는 경우 가상 시스템이 프레임을 다시 수신합니다.</p> <ul style="list-style-type: none"> ■ 동의. 게스트 운영 체제가 가상 시스템의 유효 MAC 주소를 VM 네트워크 어댑터의 MAC 주소와 다른 값으로 변경하는 경우 스위치가 프레임을 새 주소에 전달할 수 있도록 허용합니다.
위조 전송	<ul style="list-style-type: none"> ■ 거부. 소스 MAC 주소가 .vmmx 구성 파일에 있는 주소와 다를 경우 스위치가 가상 시스템 어댑터에서 모든 아웃바운드 프레임을 삭제합니다. ■ 동의. 스위치가 필터링을 수행하지 않고 모든 아웃바운드 프레임을 허용합니다.

9 (선택 사항) NIC 팀 구성을 확장하고 다음 구성 요소를 구성합니다.

옵션	설명
로드 밸런싱	<p>업링크를 어떻게 선택하는지를 지정합니다.</p> <ul style="list-style-type: none"> ■ IP 해시 기준 라우팅. 각 패킷의 소스 및 대상 IP 주소의 해시에 기반하여 업링크를 선택합니다. 비 IP 패킷에 대해서는 오프셋에 있는 어떤 것도 해시를 계산하기 위해 사용 됩니다. ■ 소스 MAC 해시 기준 라우팅. 소스 이더넷의 해시에 기반하여 업링크를 선택합니다. ■ 원시 포트 ID에 기반한 라우팅. 원시 포트 ID에 기반한 업링크를 선택합니다. ■ 명시적 페일오버 순서 사용. 페일오버 검색 기준을 통과한 활성 어댑터 목록에서 순서가 가장 높은 업링크를 항상 사용합니다. <p>참고 IP 기반의 팀 구성에서는 물리적 스위치를 EtherChannel로 구성해야 합니다. 다른 모든 옵션에서는 EtherChannel을 비활성화해야 합니다.</p>
네트워크 페일오버 감지	<p>페일오버 감지에 사용하는 방법을 지정합니다.</p> <ul style="list-style-type: none"> ■ 링크 상태만. 네트워크 어댑터가 제공하는 링크 상태만 기준으로 합니다. 이 옵션은 케이블 당김, 물리적 스위치 전원 고장과 같은 고장을 감지하지만 스페닝 트리 (spanning tree)로 차단되는 물리적 스위치 포트 또는 물리적 스위치의 다른 측면에서 케이블 당김이나 잘못된 VLAN으로의 잘못된 구성과 같은 구성 오류는 감지하지 않습니다. ■ 비콘만. 팀의 모든 NIC에서 beacon probe을 보내고 수신하여 해당 정보를 연결 상태와 함께 연결 장애를 판단하는 데 사용합니다. 링크 상태만으로 검색할 수 없는 이전에 언급한 많은 장애를 검색합니다. <p>참고 IP-해시 로드 밸런싱과 함께 신호 검색을 사용하지 않습니다.</p>

옵션	설명
스위치 알림	<p>예, 아니요 또는 vSwitch에서 상속을 선택하여 페일오버 발생 시 스위치에 알릴지를 선택합니다.</p> <p>예를 선택한 경우, 가상 NIC가 Distributed Switch에 연결될 때마다 또는 가상 NIC의 트래픽이 페일오버 이벤트로 인해 팀의 다른 물리적 NIC로 라우팅될 때마다 네트워크를 통해 알림이 전송되어 물리적 스위치의 조회 테이블이 업데이트됩니다. 거의 모든 경우에서 이 프로세스는 페일오버 발생의 가장 낮은 지연 시간 그리고 vMotion을 사용하여 마이그레이션하는 데 바람직합니다.</p> <p>참고 포트 그룹을 사용하는 가상 시스템이 유니캐스트 모드의 Microsoft 네트워크 로드 밸런싱을 이용할 때에는 이 옵션을 사용하지 않습니다. NLB가 멀티캐스트 모드에서 실행되는 경우에는 이러한 문제가 존재하지 않습니다.</p>
페일백	<p>예, 아니요 또는 vSwitch에서 상속을 선택하여 페일백을 비활성화 또는 활성화합니다.</p> <p>이 옵션은 물리적 어댑터가 고장을 복구한 후에 어떻게 실행 상태로 돌아가는가를 결정합니다. 페일백을 예(기본값)로 설정한 경우 인계받았던 대기 어댑터(있는 경우)를 대체함으로써 복구 시 어댑터가 즉시 실행 상태로 돌아갑니다. 페일오버가 아니요로 설정된 경우 고장난 어댑터는 복구되어도 현재의 다른 활성 어댑터가 고장나 교체가 필요할 때까지 비활성 상태로 둡니다.</p>
페일오버 순서	<p>업링크로 작업 로드를 어떻게 분산하는가를 지정합니다. 사용 중인 업링크가 고장나는 긴급 상황을 고려하여 일부 업링크만 사용하고 나머지 업링크를 두려는 경우, 해당 업링크를 다른 그룹으로 이동하고 이 조건을 설정합니다.</p> <ul style="list-style-type: none"> ■ 활성 업링크. 네트워크 어댑터 연결을 사용할 수 있고 활성 상태인 경우에 이 업링크를 계속 사용합니다. ■ 대기 업링크. 활성 어댑터의 연결 중 하나가 끊어져 있는 경우 이 업링크를 사용합니다. <p>참고 IP-해시 로드 밸런싱을 이용할 때에는 대기 업링크를 구성하지 않습니다.</p>

10 (선택 사항) 트래픽 조절을 구성하려면 **트래픽 조절을 확장하고 사용**을 클릭한 후 다음 매개 변수를 지정합니다.

옵션	설명
평균 대역폭	포트를 통과할 수 있는 평균 초당 비트 수, 즉 허용되는 평균 로드를 설정합니다.
최대 대역폭	트래픽 버스트를 송신 또는 수신할 때 포트를 통과할 수 있는 초당 최대 비트 수입니다. 포트가 추가 버스트를 사용할 때마다 이 값은 포트에서 사용하는 대역폭보다 커집니다.
버스트 크기	버스트에 허용할 최대 바이트 수입니다. 이 매개 변수를 설정하면 할당되어 있는 대역폭의 일부만 사용될 때 포트에 추가 버스트가 제공될 수 있습니다. 추가 버스트를 사용할 수 있는 경우, 평균 대역폭 에서 지정한 것보다 더 많은 대역폭이 포트에 필요할 때 일시적으로 더 높은 속도로 데이터를 전송할 수 있습니다. 이 매개 변수는 추가 버스트에서 누적될 수 있는 바이트 수의 상한값을 지정하기 때문에 더 높은 속도로 전송됩니다.

트래픽 조절 정책은 가상 스위치에 연결된 각 가상 네트워크 어댑터의 트래픽에 적용됩니다.

11 **저장**을 클릭합니다.

VMware Host Client에서 물리적 네트워크 어댑터 관리

물리적 어댑터를 표준 스위치에 할당하여 관리하는 호스트의 가상 시스템 및 VMkernel 어댑터에 대한 연결을 제공합니다.

VMware Host Client에서 물리적 네트워크 어댑터 정보 보기

VMware Host Client에서 물리적 NIC(네트워크 어댑터) 구성 및 설정에 대한 다양한 정보를 볼 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **네트워킹**을 클릭하고 **물리적 NIC**를 클릭합니다.
- 2 정보를 보려는 네트워크 어댑터를 클릭합니다.

VMware Host Client에서 물리적 NIC 편집

VMware Host Client를 사용하여 물리적 NIC 속도를 편집할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **네트워킹**을 클릭하고 **물리적 NIC**를 클릭합니다.
- 2 테이블에서 편집하려는 NIC를 선택합니다.
- 3 **설정 편집**을 클릭하고 드롭다운 메뉴에서 속도를 선택합니다.
- 4 **저장**을 클릭합니다.

VMware Host Client에서 VMkernel 네트워크 어댑터 관리

VMware Host Client에서 VMkernel NIC(네트워크 어댑터)를 추가 및 제거할 수 있을 뿐만 아니라 VMkernel NIC 설정을 보고 수정할 수도 있습니다.

VMware Host Client에서 VMkernel 네트워크 어댑터 정보 보기

VMware Host Client에서 TCP/IP 구성, 네트워크 세부 정보, 가상 스위치 토폴로지 등과 같은 VMkernel NIC(네트워크 어댑터)에 대한 정보를 볼 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **네트워킹**을 클릭하고 **VMkernel NIC**를 클릭합니다.
- 2 목록에서 구성 및 토폴로지 세부 정보를 표시할 NIC를 클릭합니다.

VMware Host Client에서 VMkernel 네트워크 어댑터 추가

VMware vSphere® Standard Edition™ 스위치에서 VMkernel 네트워크 어댑터(NIC)를 추가하여 호스트에 대한 네트워크 연결을 제공할 수 있습니다. VMkernel NIC는 VMware vSphere® vMotion®, IP 스토리지, Fault Tolerance, 로깅, vSAN 등에 대한 시스템 트래픽도 처리합니다.

절차

- 1 VMware Host Client 인벤토리에서 **네트워킹**을 마우스 오른쪽 버튼으로 클릭하고 **VMkernel NIC 추가**를 클릭합니다.
- 2 **VMkernel NIC 추가** 대화상자에서 VMkernel 어댑터에 대한 설정을 구성합니다.

옵션	설명
새 포트 그룹 레이블	VMkernel NIC를 추가하면 포트 그룹도 추가됩니다. 해당 포트 그룹의 이름을 지정합니다.
VLAN ID	VMkernel 어댑터의 네트워크 트래픽이 사용할 VLAN을 확인하도록 VLAN ID를 입력합니다.
IP 버전	IPv4, IPv6 또는 둘 모두를 선택합니다. 참고 IPv6을 사용하도록 설정하지 않은 호스트에는 IPv6 옵션이 표시되지 않습니다.

- 3 드롭다운 메뉴에서 가상 스위치를 선택합니다.
- 4 (선택 사항) IPv4 설정 섹션을 확장하여 IP 주소를 가져오는 옵션을 선택합니다.

옵션	설명
DHCP를 사용하여 IP 설정 가져오기	IP 설정을 자동으로 가져옵니다. DHCP 서버가 네트워크에 표시되어야 합니다.
정적 IP 설정 사용	VMkernel 어댑터에 대한 IPv4 주소와 서브넷 마스크를 입력합니다. IPv4에 대한 VMkernel 기본 게이트웨이와 DNS 서버 주소는 선택한 TCP/IP 스택에서 가져옵니다.

- 5 (선택 사항) IPv6 설정 섹션을 확장하여 IPv6 주소를 가져오는 옵션을 선택합니다.

옵션	설명
DHCPv6	DHCP를 사용하여 IPv6 주소를 가져옵니다. DHCPv6 서버가 네트워크에 표시되어야 합니다.
자동 구성	라우터 알림을 사용하여 IPv6 주소를 가져옵니다.
정적 IPv6 주소	a 주소 추가를 클릭하여 새 IPv6 주소를 추가합니다. b IPv6 주소 및 서브넷 접두사 길이를 입력합니다.

- 6 드롭다운 메뉴에서 TCP/IP 스택을 선택합니다.

VMkernel 어댑터에 대한 TCP/IP 스택을 설정하고 나면 변경할 수 없습니다. vMotion 또는 프로비저닝 TCP/IP 스택을 선택하는 경우 이 스택만 사용하여 호스트의 vMotion 또는 프로비저닝 트래픽을 처리할 수 있습니다. 기본 TCP/IP 스택의 vMotion에 대한 모든 VMkernel 어댑터는 이후 vMotion 세션에 대해 비활성화되어 있습니다. 프로비저닝 TCP/IP 스택을 사용하는 경우 기본 TCP/IP 스택의 VMkernel 어댑터가 비활성화되며 일부 작업을 수행할 수 없습니다. 이러한 작업에는 가상 시스템 콜드 마이그레이션, 복제 및 스냅샷 마이그레이션과 같은 트래픽 프로비저닝이 포함됩니다.

- 7 (선택 사항) 호스트에서 기본 TCP/IP 스택에 대해 사용하도록 설정할 서비스를 선택합니다.

vMotion은 VMkernel 어댑터가 자신이 vMotion 트래픽이 전송되는 네트워크 연결임을 다른 호스트에 알리도록 설정합니다. vMotion 서비스가 기본 TCP/IP 스택의 모든 VMkernel 어댑터에 대해 사용하도록 설정되어 있지 않거나 vMotion TCP/IP 스택을 사용하는 어댑터가 없는 경우 vMotion을 사용하여 선택한 호스트로의 마이그레이션을 수행할 수 없습니다.

- 8 설정 선택 사항을 검토하고 **생성**을 클릭합니다.

VMware Host Client에서 VMkernel 네트워크 어댑터 설정 편집

VMkernel 네트워크 어댑터에 대해 지원되는 트래픽 유형을 변경하거나 IPv4 또는 IPv6 주소를 가져오는 방식을 변경해야 할 수도 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **네트워킹**을 클릭하고 **VMkernel NIC**를 클릭합니다.
- 2 대상 표준 스위치에 있는 VMkernel 어댑터를 선택하고 **작업**을 클릭하고 드롭다운 메뉴에서 **설정 편집**을 선택합니다.
- 3 (선택 사항) VLAN ID를 편집합니다.
VLAN ID는 VMkernel 어댑터의 네트워크 트래픽이 사용하는 VLAN을 확인합니다.
- 4 (선택 사항) IP 버전을 편집하려면 드롭다운 메뉴에서 IPv4, IPv6 또는 둘 모두를 선택합니다.

참고 IPv6을 사용하도록 설정하지 않은 호스트에는 IPv6 옵션이 표시되지 않습니다.

- 5 (선택 사항) IPv4 설정 섹션을 확장하여 IP 주소를 가져오는 옵션을 선택합니다.

옵션	설명
DHCP를 사용하여 IP 설정 가져오기	IP 설정을 자동으로 가져옵니다. DHCP 서버가 네트워크에 표시되어야 합니다.
정적 IP 설정 사용	VMkernel 어댑터에 대한 IPv4 주소와 서브넷 마스크를 입력합니다. IPv4에 대한 VMkernel 기본 게이트웨이와 DNS 서버 주소는 선택한 TCP/IP 스택에서 가져옵니다.

- 6 (선택 사항) IPv6 설정 섹션을 확장하여 IPv6 주소를 가져오는 옵션을 선택합니다.

옵션	설명
DHCPv6	DHCP를 사용하여 IPv6 주소를 가져옵니다. DHCPv6 서버가 네트워크에 표시되어야 합니다.
자동 구성	라우터 알림을 사용하여 IPv6 주소를 가져옵니다.
정적 IPv6 주소	a 주소 추가를 클릭하여 IPv6 주소를 추가합니다. b IPv6 주소 및 서브넷 접두사 길이를 입력합니다.

- 7 (선택 사항) 호스트에서 기본 TCP/IP 스택에 대해 활성화 또는 비활성화할 서비스를 선택합니다.

vMotion은 VMkernel 어댑터가 자신이 vMotion 트래픽이 전송되는 네트워크 연결임을 다른 호스트에 알리도록 설정합니다. vMotion 서비스가 기본 TCP/IP 스택의 VMkernel 어댑터에 대해 사용되도록 설정되어 있지 않거나 vMotion TCP/IP 스택을 사용하는 어댑터가 없는 경우 vMotion을 사용하여 선택한 호스트로의 마이그레이션을 수행할 수 없습니다.

- 8 설정 수정 내용을 검토하고 **저장**을 클릭하여 변경 내용을 적용합니다.

VMware Host Client에서 VMkernel 네트워크 어댑터 제거

VMware Host Client에서 VMkernel 네트워크 어댑터가 더 이상 필요 없는 경우 제거할 수 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **네트워킹**을 클릭하고 **VMkernel NIC**를 클릭합니다.
- 2 제거하려는 VMkernel 어댑터를 마우스 오른쪽 버튼으로 클릭하고 **제거**를 클릭합니다.
- 3 **확인**을 클릭하여 네트워크 어댑터를 제거합니다.

VMware Host Client에서 호스트의 TCP/IP 스택 구성 보기

호스트의 TCP/IP 스택에 대한 DNS 및 라우팅 구성을 볼 수 있습니다. 또한 IPv4 및 IPv6 라우팅 테이블, 정체 제어 알고리즘, 허용되는 최대 연결 수를 볼 수도 있습니다.

절차

- 1 호스트 인벤토리에서 **네트워킹**을 클릭하고 **TCP/IP 스택**을 클릭합니다.
- 2 목록에서 스택을 클릭합니다.
선택한 스택의 구성 설정이 표시됩니다.

VMware Host Client에서 호스트에 있는 TCP/IP 스택의 구성 변경

호스트의 TCP/IP 스택에 대한 DNS 및 기본 게이트웨이 구성을 변경할 수 있습니다. 또한 정체 제어 알고리즘, 최대 연결 수 및 사용자 지정 TCP/IP 스택의 이름을 변경할 수도 있습니다.

절차

- 1 VMware Host Client 인벤토리에서 **네트워킹**을 클릭하고 **TCP/IP 스택**을 클릭합니다.
- 2 목록에서 스택을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
TCP/IP 구성 편집 - 프로비저닝 스택 대화 상자가 나타납니다.
- 3 호스트가 이 TCP/IP 스택에 대한 설정을 가져오는 방법을 지정합니다.
 - **다음 어댑터의 DHCP 서비스 사용** 라디오 버튼을 선택하고 TCP/IP 스택에 대한 기본 설정 구성을 받을 어댑터를 선택합니다.

- 이 TCP/IP 스택에 대한 설정을 수동으로 구성을 선택하여 설정 구성을 변경합니다.

옵션	설명
기본 구성	호스트 이름 로컬 호스트의 이름을 편집합니다.
	도메인 이름 도메인 이름을 편집합니다.
	기본 DNS 서버 기본 DNS 서버 IP 주소를 입력합니다.
	보조 DNS 서버 대체 DNS 서버 IP 주소를 입력합니다.
	도메인 검색 정규화되지 않은 도메인 이름을 해결할 때 DNS 검색에서 사용할 DNS 접미사를 지정합니다.
라우팅	IPv4 및 IPv6 게이트웨이 정보를 편집합니다. 참고 기본 게이트웨이를 제거하면 호스트에 대한 연결이 손실될 수 있습니다.
고급 설정	정체 제어 알고리즘 및 최대 연결 수를 편집합니다.

- 4 저장을 클릭합니다.

VMware Host Client에서 ESXi 방화벽 구성

ESXi에는 기본적으로 활성화되는 방화벽이 포함됩니다. 설치 중에 ESXi 방화벽은 호스트 보안 프로파일에서 활성화된 서비스의 트래픽을 제어하고 들어오고 나가는 트래픽을 차단하도록 구성됩니다.

방화벽에서 포트를 열 때 ESXi 호스트에서 실행되는 서비스에 대한 제한되지 않은 액세스로 인해 외부 공격 및 인증되지 않은 액세스에 호스트가 노출될 수 있는지 고려하십시오. 인증된 네트워크에서만 액세스를 허용하도록 ESXi 방화벽을 구성하여 위험을 줄이십시오.

참고 방화벽을 사용하여 ICMP(Internet Control Message Protocol), ping과 DHCP 및 DNS(UDP만 해당) 클라이언트와의 통신을 허용할 수도 있습니다.

VMware Host Client를 사용하여 ESXi 방화벽 설정 관리

VMware Host Client로 ESXi 호스트에 로그인한 경우 서비스 또는 관리 에이전트에 대한 들어오는 방화벽 연결 및 나가는 방화벽 연결을 구성할 수 있습니다.

참고 서로 다른 서비스에 포트 규칙이 겹치는 경우, 특정 서비스를 사용하도록 설정했을 때 다른 서비스도 사용 가능하도록 암시적으로 설정될 수 있습니다. 이 문제를 방지하려면 호스트의 각 서비스에 액세스하도록 허용된 IP 주소를 지정하면 됩니다.

절차

1 VMware Host Client 인벤토리에서 **네트워킹**을 클릭합니다.

2 **방화벽 규칙**을 클릭합니다.

VMware Host Client에는 활성 상태의 들어오는 연결과 나가는 연결 및 해당 방화벽 포트의 목록이 표시됩니다.

3 일부 서비스의 경우 서비스 세부 정보를 관리할 수 있습니다. 서비스를 마우스 오른쪽 버튼으로 클릭하고 팝업 메뉴에서 옵션을 선택합니다.

- 시작, 중지 또는 다시 시작 버튼을 사용하여 서비스의 상태를 일시적으로 변경합니다.
- 시작 정책을 변경하여 서비스가 호스트, 방화벽 포트와 함께 또는 수동으로 시작하고 중지하도록 구성합니다.

VMware Host Client를 사용하여 ESXi에 대해 허용되는 IP 주소 추가

기본적으로 각 서비스의 방화벽은 모든 IP 주소에 대한 액세스를 허용합니다. 트래픽을 제한하려면 관리 서브넷에 서만 트래픽을 허용하도록 각 서비스를 구성합니다. 환경에서 사용하지 않는 경우 일부 서비스를 선택 취소할 수도 있습니다.

절차

1 VMware Host Client 인벤토리에서 **네트워킹**을 클릭하고 **방화벽 규칙**을 클릭합니다.

2 목록에서 서비스를 클릭하고 **설정 편집**을 클릭합니다.

3 허용된 IP 주소 섹션에서 **다음 네트워크의 연결만 허용**을 클릭하고 호스트에 연결하려는 네트워크의 IP 주소를 입력합니다.

여러 개의 IP 주소는 쉼표로 구분합니다. 다음과 같은 주소 형식을 사용할 수 있습니다.

- 192.168.0.0/24
- 192.168.1.2, 2001::1/64
- fd3e:29a6:0a81:e478::/64

4 **확인**을 클릭합니다.

VMware Host Client에서 네트워킹 이벤트 및 작업 모니터링

관리하는 ESXi 호스트의 포트 그룹, 가상 스위치, 물리적 네트워크 어댑터, VMkernel 네트워크 어댑터 및 TCP/IP 스택과 연결된 이벤트 및 태스크에 대한 세부 정보를 볼 수 있습니다.

VMware Host Client에서 포트 그룹 모니터링

VMware Host Client에서 호스트에 있는 포트 그룹의 이벤트 및 태스크를 보고 포트 그룹 성능을 모니터링할 수 있습니다.

절차

1 VMware Host Client 인벤토리에서 **네트워킹**을 클릭합니다.

2 **포트 그룹**을 클릭합니다.

3 목록에서 포트 그룹을 클릭합니다.

VMware Host Client 인벤토리에서 포트 그룹이 확장됩니다.

4 VMware Host Client 인벤토리의 포트 그룹 이름 아래에서 **모니터링**을 클릭합니다.

5 (선택 사항) **이벤트**를 클릭하여 포트 그룹과 연결된 이벤트를 봅니다.

VMware Host Client에서 가상 스위치 모니터링

VMware Host Client에서 호스트에 있는 가상 스위치의 이벤트 및 태스크를 보고 가상 스위치 성능을 모니터링할 수 있습니다.

절차

1 VMware Host Client 인벤토리에서 **네트워킹**을 클릭합니다.

2 **가상 스위치**를 클릭합니다.

3 목록에서 가상 스위치를 클릭합니다.

VMware Host Client 인벤토리에서 가상 스위치가 확장됩니다.

4 VMware Host Client 인벤토리의 가상 스위치 이름 아래에서 **모니터링**을 클릭합니다.

5 (선택 사항) **이벤트**를 클릭하여 가상 스위치와 연결된 이벤트를 봅니다.

VMware Host Client에서 물리적 네트워크 어댑터 모니터링

VMware Host Client에서 호스트에 있는 물리적 NIC의 이벤트 및 태스크를 보고 물리적 NIC(네트워크 어댑터) 성능을 모니터링할 수 있습니다.

절차

1 VMware Host Client 인벤토리에서 **네트워킹**을 클릭합니다.

2 **물리적 NIC**를 클릭합니다.

3 목록에서 물리적 네트워크 어댑터를 클릭합니다.

VMware Host Client 인벤토리에서 물리적 네트워크 어댑터가 확장됩니다.

4 VMware Host Client 인벤토리의 물리적 네트워크 어댑터 이름 아래에서 **모니터링**을 클릭합니다.

5 (선택 사항) **이벤트**를 클릭하여 물리적 네트워크 어댑터와 연결된 이벤트를 봅니다.

VMware Host Client에서 VMkernel 네트워크 어댑터 모니터링

VMware Host Client에서 호스트에 있는 VMkernel 네트워크 어댑터의 이벤트 및 태스크를 보고 VMkernel 네트워크 어댑터 성능을 모니터링할 수 있습니다.

절차

1 VMware Host Client 인벤토리에서 **네트워킹**을 클릭합니다.

2 **VMkernel NIC**를 클릭합니다.

3 목록에서 VMkernel 네트워크 어댑터를 클릭합니다.

VMware Host Client 인벤토리에서 VMkernel 네트워크 어댑터가 확장됩니다.

4 VMware Host Client 인벤토리의 VMkernel 네트워크 어댑터 이름 아래에서 **모니터링**을 클릭합니다.

5 (선택 사항) **이벤트**를 클릭하여 VMkernel 네트워크 어댑터와 연결된 이벤트를 봅니다.

VMware Host Client에서 TCP/IP 스택 모니터링

VMware Host Client에서 호스트에 있는 TCP/IP 스택의 이벤트 및 태스크를 보고 TCP/IP 스택 성능을 모니터링할 수 있습니다.

절차

1 VMware Host Client 인벤토리에서 **네트워킹**을 클릭합니다.

2 **TCP/IP 스택**을 클릭합니다.

3 목록에서 TCP/IP 스택을 클릭합니다.

VMware Host Client 인벤토리에서 TCP/IP 스택이 확장됩니다.

4 VMware Host Client 인벤토리의 TCP/IP 스택 이름 아래에서 **모니터링**을 클릭합니다.

5 (선택 사항) **이벤트**를 클릭하여 TCP/IP 스택과 연결된 이벤트를 봅니다.

6 (선택 사항) **태스크**를 클릭하여 TCP/IP 스택과 연결된 태스크를 봅니다.