vCenter Server 구성

업데이트 3

VMware vSphere 7.0
VMware ESXi 7.0
vCenter Server 7.0

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

https://docs.vmware.com/kr/

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

VMware 코리아
서울시 강남구
영동대로 517
아셈타워 13층
(우) 06164
전화:+82 2 3016 6500
팩스: +82 2 3016 6501
www.vmware.com/kr

Copyright © 2019-2021 VMware, Inc. All rights reserved. 저작권 및 상표 정보

목차

vCenter Server 구성 정보 6

1 vCenter Server 구성 개요 7
Platform Services Controller 변경 사항 8

2 vCenter Server 관리 인터페이스를 사용하여 vCenter Server 구성 10
vCenter Server 관리 인터페이스에 로그인 11
vCenter Server 상태 보기 11
vCenter Server 재부팅 또는 종료 12
지원 번들 생성 12
CPU 및 메모리 활용률 모니터링 13
디스크 사용 모니터링 13
네트워크 사용 모니터링 13
데이터베이스 사용 모니터링 14
SSH 및 Bash 셸 액세스 사용 또는 사용 안 함 14
DNS, IP 주소 및 프록시 설정 구성 15
기본 네트워크 식별자 재구성 17
방화벽 설정 편집 18
시스템 표준 시간대 및 시간 동기화 설정 구성 19
서비스 시작, 중지 및 다시 시작 20
업데이트 설정 구성 20
루트 사용자의 암호 및 암호 만료 설정 변경 21
vCenter Server 로그 파일을 원격 Syslog 서버 22
백업 구성 및 스케줄링 23

3 vSphere Client를 사용하여 vCenter Server 구성 24
vCenter Server 구성 24
vCenter Server의 라이센스 설정 구성 24
통계 설정 구성 25
vCenter Server에 대한 런타임 설정 구성 27
사용자 디렉토리 설정 구성 28
메일 보낸 사람 설정 구성 29
SNMP 설정 구성 31
포트 설정 보기 31
시간 초과 설정 구성 32
로깅 옵션 구성 32

데이터베이스 설정 구성 33
레거시 호스트의 SSL 인증서 확인 34
고급 설정 구성 35
로그인된 다른 사용자에게 메시지 보내기 35
Active Directory 도메인 가입 또는 탈퇴 36
SystemConfiguration.BashShellAdministrators 그룹에 사용자 추가 38
노드 재부팅 39
노드의 상태 보기 39
지원 번들 내보내기 40

4 장치 셸을 사용하여 vCenter Server 구성 42
장치 셸에 액세스 42
장치 셸에서 Bash 셸 액세스를 사용하도록 설정 43
명령을 편집하기 위한 바로 가기 키 43
장치의 플러그인 및 API 명령에 대한 도움말 요청 44
vCenter Server 셸의 플러그인 45
showlog 플러그인을 사용하여 로그 파일 탐색 46
장치 셸의 API 명령 47
vCenter Server에 대한 SNMP 구성 52
폴링이 가능하도록 SNMP 에이전트 구성 52
SNMP v1 및 v2c용 vCenter Server 구성 53
SNMP v3용 vCenter Server 구성 55
알림을 필터링하도록 SNMP 에이전트 구성 58
SNMP 관리 클라이언트 소프트웨어 구성 59
SNMP 설정을 공장 기본값으로 재설정 59
vCenter Server에서 시간 동기화 설정 구성 60
VMware Tools 시간 동기화 사용 60
vCenter Server 구성에서 NTP 서버 추가 또는 바꾸기 61
NTP 서버와 vCenter Server의 시간 동기화 62
vCenter Server에서 로컬 사용자 계정 관리 62
vCenter Server의 사용자 역할 62
vCenter Server의 로컬 사용자 계정 목록 얻기 63
vCenter Server에서 로컬 사용자 계정 생성 63
vCenter Server의 로컬 사용자 암호 업데이트 64
vCenter Server의 로컬 사용자 계정 업데이트 64
vCenter Server에서 로컬 사용자 계정 삭제 65
vCenter Server의 상태 및 통계 모니터링 65
vimtop 플러그인을 사용하여 서비스의 리소스 사용 모니터링 66
대화형 모드에서 vimtop을 사용하여 서비스 모니터링 66
대화형 모드 명령줄 옵션 67

vimtop의 대화형 모드 단일 키 명령 67

5 DCUI(Direct Console User Interface)를 사용하여 vCenter Server 구성 69

DCUI(Direct Console User Interface)에 로그인 69

루트 사용자의 암호 변경 70

vCenter Server의 관리 네트워크 구성 70

vCenter Server의 관리 네트워크 다시 시작 71

Bash 셸에 액세스할 수 있도록 설정 72

문제 해결을 위해 Bash 셸에 액세스 72

문제 해결을 위해 vCenter Server 지원 번들 내보내기 72

vCenter Server 구성 정보

"vCenter Server 구성" 에서는 VMware vCenter® Server™를 구성하는 데 대한 정보를 제공합니다.

대상 사용자

이 정보는 VMware vCenter Server®를 구성하려는 모든 사용자를 대상으로 합니다. 이 정보는 가상 시스템 기술과 데이터 센터 운영에 대해 잘 알고 있는 숙련된 시스템 관리자를 대상으로 작성되었습니다.

VMware는 포용성을 중요하게 생각합니다. 고객, 파트너 및 내부 커뮤니티 안에서 이러한 원칙을 강화하기 위해 포용성 있는 언어를 사용하여 컨텐츠를 만듭니다.

vSphere Client 및 vCenter Server 관리 인터페이스

이 가이드의 지침은 vSphere Client, HTML5 기반 GUI 및 vCenter Server 관리 인터페이스를 반영합니다. vCenter Server 장치 셸 및 DCUI(Direct Console User Interface)를 사용하여 일부 추가적인 기능을 수행할 수 있습니다.

vCenter Server 구성 개요

1

vCenter Server는 VMware vCenter Server® 및 관련 서비스를 실행하도록 최적화된 사전 구성 가상 시스템을 사용하여 배포됩니다.

vCenter Server를 배포하는 동안 VMware vCenter® Single Sign-On™ 도메인을 생성하거나 기존 도메인에 가입할 수 있습니다. vCenter Server 배포에 대한 자세한 내용은 "vCenter Server 설치 및 설정" 항목을 참조하십시오.

vCenter Server는 VMware ESXi™ 6.0 이상에서 지원됩니다. 패키지에는 다음과 같은 소프트웨어가 포함되어 있습니다.

- Project Photon OS® 3.0
- PostgreSQL 데이터베이스
- vCenter Server 7.0 및 vCenter Server 7.0 구성 요소
- vCenter Single Sign-On, 라이센스 서비스, VMware Certificate Authority 등 vCenter Server를 실행하는 데 필요한 서비스

  인증에 대한 자세한 내용은 "vSphere 인증" 을 참조하십시오.

메모리, CPU 및 디스크 공간 추가를 제외하고는 사전 구성된 가상 시스템의 사용자 지정이 지원되지 않습니다.

vCenter Server에는 다음과 같은 기본 사용자 이름이 있습니다.

- 가상 장치를 배포하는 중에 설정하는 암호를 사용하는 루트 사용자. 루트 사용자를 사용하여 vCenter Server 관리 인터페이스 및 사전 구성된 가상 시스템 운영 체제에 로그인합니다.

  중요 기본적으로 vCenter Server 루트 계정의 암호는 365일 후 만료됩니다. 루트 암호를 변경하고 암호 만료 설정을 구성하는 방법에 대한 자세한 내용은 루트 사용자의 암호 및 암호 만료 설정 변경을 참조하십시오.

- 장치를 배포하는 중에 설정하는 암호와 도메인 이름을 사용하는 vCenter Single Sign-On 사용자인 administrator@*your_domain_name*.

  vCenter Server를 설치할 때 vSphere 도메인을 변경할 수 있습니다. Microsoft Active Directory의 도메인 이름 또는 OpenLDAP 도메인 이름으로 동일한 도메인 이름을 사용하지 마십시오.

처음에는 administrator@*your_domain_name* 사용자만 vCenter Server 시스템에 로그인할 수 있습니다. 기본적으로 administrator@*your_domain_name* 사용자는 SystemConfiguration.Administrators 그룹의 멤버이며 추가 사용자 및 그룹이 정의된 ID 소스를 vCenter Single Sign-On에 추가하거나, 사용자 및 그룹에게 사용 권한을 부여할 수 있습니다. 자세한 내용은 "vSphere 보안" 의 내용을 참조하십시오.

다음 네 가지 방법으로 vCenter Server 설정을 구성할 수 있습니다.

- vCenter Server 관리 인터페이스를 사용합니다.

  액세스, 네트워크, 시간 동기화 및 루트 암호 설정 등의 시스템 설정을 편집할 수 있습니다. 이는 vCenter Server를 구성하는 기본 방법입니다.

- vSphere Client를 사용합니다.

  vCenter Server의 시스템 구성 설정으로 이동하여 배포를 Active Directory 도메인에 가입시킵니다. vCenter Server에서 실행 중인 서비스를 관리하고, 액세스, 네트워크, 방화벽 설정 등의 다양한 설정을 수정할 수 있습니다.

- Bash 셸을 사용합니다.

  TTY1을 사용하여 콘솔에 로그인하거나 SSH를 사용하여 vCenter Server에서 구성, 모니터링 및 문제 해결 명령을 실행할 수 있습니다.

- DCUI(Direct Console User Interface)를 사용합니다.

  TTY2를 사용하여 vCenter Server DCUI(Direct Console User Interface)에 로그인하여 루트 사용자의 암호를 변경하거나, 네트워크 설정을 구성하거나, Bash 셸 또는 SSH에 액세스할 수 있도록 설정할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- Platform Services Controller 변경 사항

Platform Services Controller 변경 사항

vSphere 7.0에서는 모든 Platform Services Controller서비스가 vCenter Server에 통합됩니다.

vSphere 7.0부터는 vSphere 7.0에서 vCenter Server를 배포하거나 업그레이드하려면 vCenter Server 실행을 위해 최적화된 미리 구성된 가상 시스템인 vCenter Server Appliance를 사용해야 합니다. 새 vCenter Server에는 인증, 인증서 관리 및 라이센싱을 포함하여 기능 및 워크플로를 보존하는 모든 Platform Services Controller 서비스가 포함되어 있습니다. 더 이상 외부 Platform Services Controller를 배포할 필요가 없으며 배포할 수도 없습니다. 모든 Platform Services Controller 서비스가 vCenter Server에 통합되고 배포 및 관리가 간소화됩니다.

이제 이러한 서비스는 vCenter Server의 일부이며 더 이상 Platform Services Controller의 일부로 설명되지 않습니다. vSphere 7.0에서 "vSphere 인증" 자료는 "Platform Services Controller 관리" 자료를 대체합니다. 새 자료에는 인증 및 인증서 관리에 대한 모든 정보가 포함되어 있습니다. 기존 외부 Platform Services Controller를 사용하는 vSphere 6.5 및 6.7 배포를 vCenter Server Appliance를 사용하여 vSphere 7.0으로 업그레이드하거나 마이그레이션하는 데 대한 자세한 내용은 "vSphere 업그레이드" 설명서를 참조하십시오.

vCenter Server 관리 인터페이스를 사용하여 vCenter Server 구성

2

vCenter Server를 배포한 후 vCenter Server 관리 인터페이스에 로그인하여 설정을 편집할 수 있습니다.

vCenter Server에 패치를 적용하고 vCenter Server 패치에 대한 자동 확인을 설정하는 데 대한 자세한 내용은 "vSphere 업그레이드" 설명서를 참조하십시오.

vCenter Server 백업 및 복원에 대한 자세한 내용은 "vCenter Server 설치 및 설정" 항목을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- vCenter Server 관리 인터페이스에 로그인
- vCenter Server 상태 보기
- vCenter Server 재부팅 또는 종료
- 지원 번들 생성
- CPU 및 메모리 활용률 모니터링
- 디스크 사용 모니터링
- 네트워크 사용 모니터링
- 데이터베이스 사용 모니터링
- SSH 및 Bash 셸 액세스 사용 또는 사용 안 함
- DNS, IP 주소 및 프록시 설정 구성
- 기본 네트워크 식별자 재구성
- 방화벽 설정 편집
- 시스템 표준 시간대 및 시간 동기화 설정 구성
- 서비스 시작, 중지 및 다시 시작
- 업데이트 설정 구성
- 루트 사용자의 암호 및 암호 만료 설정 변경
- vCenter Server 로그 파일을 원격 Syslog 서버
- 백업 구성 및 스케줄링

vCenter Server 관리 인터페이스에 로그인

vCenter Server 관리 인터페이스에 로그인하여 vCenter Server 구성 설정에 액세스합니다.

참고 vCenter Server 관리 인터페이스를 10분간 유휴 상태로 두면 로그인 세션이 만료됩니다.

사전 요구 사항

vCenter Server가 배포되고 실행 중인지 확인합니다.

절차

1 웹 브라우저에서 vCenter Server 관리 인터페이스, https://*appliance-IP-address-or-FQDN*:5480으로 이동합니다.

2 root로 로그인합니다.

기본 루트 암호는 vCenter Server를 배포할 때 설정하는 암호입니다.

vCenter Server 상태 보기

vCenter Server 관리 인터페이스를 사용하여 vCenter Server의 전반적인 상태 및 상태 메시지를 볼 수 있습니다.

vCenter Server의 전반적인 상태는 CPU, 메모리, 데이터베이스, 스토리지 등 하드웨어 구성 요소의 상태에 따라 달라집니다. 업데이트 구성 요소의 상태를 기반으로 하며, 사용 가능한 패치에 대한 마지막 확인에 따라 소프트웨어 패키지가 최신 상태인지 표시합니다.

중요 사용 가능한 패치에 대한 정기적인 확인을 수행하지 않으면 업데이트 구성 요소의 상태가 최신 상태가 아니게 될 수 있습니다. vCenter Server 패치를 확인하고 vCenter Server 패치에 대한 자동 확인을 사용하도록 설정하는 방법에 대한 자세한 내용은 "vSphere 업그레이드" 을(를) 참조하십시오.

사전 요구 사항

vCenter Server 관리 인터페이스에 루트로 로그인합니다.

절차

1 vCenter Server 관리 인터페이스에서 **요약**을 클릭합니다.

2 상태 창에서 전반적인 상태 배지를 봅니다.

표 2-1. 상태

배지 아이콘	설명
	정상. 모든 구성 요소가 정상입니다.
	주의. 구성 요소 하나 이상이 곧 오버로드될 수 있습니다. 상태 메시지 창에서 세부 정보를 봅니다.

표 2-1. 상태 (계속)

배지 아이콘	설명
	경고. 구성 요소 하나 이상의 성능이 저하될 수 있습니다. 비보안 패치가 제공될 수 있습니다. 상태 메시지 창에서 세부 정보를 봅니다.
	위험. 구성 요소 하나 이상이 사용할 수 없는 상태일 수 있으며, vCenter Server가 곧 응답할 수 없는 상태가 될 수 있습니다. 보안 패치가 제공될 수 있습니다. 상태 메시지 창에서 세부 정보를 봅니다.
	알 수 없습니다. 사용할 수 있는 데이터가 없습니다.

vCenter Server 재부팅 또는 종료

vCenter Server 관리 인터페이스를 사용하여 실행 중인 가상 시스템을 다시 시작하거나 전원을 끌 수 있습니다.

사전 요구 사항

vCenter Server 관리 인터페이스에 루트로 로그인합니다.

절차

1 vCenter Server 관리 인터페이스에서 **요약**을 클릭합니다.

2 맨 위 메뉴 창에서 **작업** 드롭다운 메뉴를 클릭합니다.

3 **재부팅** 또는 **종료**를 클릭하여 가상 시스템을 다시 시작하거나 전원을 끌 수 있습니다.

4 확인 대화상자에서 **예**를 클릭하여 작업을 확인합니다.

지원 번들 생성

장치에서 실행되는 vCenter Server 인스턴스에 대한 로그 파일이 포함된 지원 번들을 생성할 수 있습니다. 시스템에서 로컬로 로그를 분석하고 VMware 지원팀에 번들을 보낼 수 있습니다.

사전 요구 사항

vCenter Server 관리 인터페이스에 루트로 로그인합니다.

절차

1 vCenter Server 관리 인터페이스에서 **요약**을 클릭합니다.

2 맨 위 메뉴 창에서 **작업** 드롭다운 메뉴를 클릭합니다.

3 **지원 번들 생성**을 클릭하고 번들을 로컬 시스템에 저장합니다.

결과

지원 번들은 로컬 시스템에서 `.tgz` 파일로 다운로드됩니다.

CPU 및 메모리 활용률 모니터링

vCenter Server 관리 인터페이스를 사용하여 vCenter Server의 전체 CPU 활용률과 메모리 활용률을 모니터링할 수 있습니다.

사전 요구 사항

vCenter Server 관리 인터페이스에 루트로 로그인합니다.

절차

1. vCenter Server 관리 인터페이스에서 **모니터**를 클릭합니다.
2. [모니터] 페이지에서 **CPU 및 메모리** 탭을 클릭합니다.
3. **날짜 범위** 드롭다운 메뉴에서 CPU 활용률 추세 그래프를 및 메모리 활용률 추세 그래프를 생성할 기간을 선택합니다.
4. 그래프를 가리켜서 특정 날짜와 시간의 CPU 및 메모리 사용량을 확인합니다.

디스크 사용 모니터링

vCenter Server 관리 인터페이스를 사용하여 vCenter Server의 전체 디스크 사용을 모니터링할 수 있습니다.

사전 요구 사항

vCenter Server 관리 인터페이스에 루트로 로그인합니다.

절차

1. vCenter Server 관리 인터페이스에서 **모니터**를 클릭합니다.
2. [모니터] 페이지에서 **디스크** 탭을 클릭합니다.

결과

[디스크 모니터링] 창에 디스크가 표시되며, 이름, 파티션 또는 활용률을 기준으로 디스크를 정렬할 수 있습니다.

네트워크 사용 모니터링

vCenter Server 관리 인터페이스를 사용하여 어제, 지난주, 지난달 또는 지난 분기에 해당하는 vCenter Server의 네트워크 사용을 모니터링할 수 있습니다.

사전 요구 사항

vCenter Server 관리 인터페이스에 루트로 로그인합니다.

절차

1 vCenter Server 관리 인터페이스에서 **모니터**를 클릭합니다.

2 [모니터] 페이지에서 **네트워크** 탭을 클릭합니다.

3 **데이터 범위** 드롭다운 메뉴에서 네트워크 활용률 그래프를 생성할 기간을 선택합니다.

4 그래프 그리드 아래쪽의 테이블에서 모니터링할 패킷 또는 전송 바이트 속도를 선택합니다.

옵션은 네트워크 설정에 따라 다릅니다.

선택한 항목의 활용률을 표시하도록 네트워크 활용률 그래프가 새로 고쳐집니다.

5 네트워크 활용률 그래프를 가리켜서 특정 날짜와 시간에 대한 네트워크 사용 데이터를 확인합니다.

데이터베이스 사용 모니터링

vCenter Server 관리 인터페이스를 사용하여 vCenter Server의 내장된 데이터베이스의 사용을 데이터 유형별로 모니터링할 수 있습니다. 또한 공간 사용 추세 그래프를 모니터링하고 가장 많은 데이터 유형을 필터링할 수 있습니다.

사전 요구 사항

vCenter Server 관리 인터페이스에 루트로 로그인합니다.

절차

1 vCenter Server 관리 인터페이스에서 **모니터**를 클릭합니다.

2 vCenter Server 데이터베이스의 사용된 공간과 사용 가능한 공간을 모니터링하려면 [모니터] 페이지에서 **데이터베이스** 탭을 클릭합니다.

3 **날짜 범위** 드롭다운 메뉴에서 공간 활용률 추세 그래프를 생성할 기간을 선택합니다.

4 기본 그래프에서 특정 데이터베이스 구성 요소를 포함하거나 제외하려면 해당 구성 요소의 제목을 클릭합니다.

옵션	설명
사용자 공간 활용률 추세 그래프	경보, 이벤트, 작업 및 통계 추세선을 선택하고 볼 수 있습니다.
전체 공간 활용률 추세 그래프	사용자, DB 로그 및 핵심 추세선을 선택하고 볼 수 있습니다.

5 공간 활용률 그래프를 가리켜서 특정 날짜와 시간에 대한 데이터베이스 사용 값을 확인합니다.

SSH 및 Bash 셸 액세스 사용 또는 사용 안 함

vCenter Server 관리 인터페이스를 사용하여 장치에 대한 액세스 설정을 편집할 수 있습니다.

장치에 대한 SSH 관리자 로그인을 사용하거나 사용하지 않도록 설정할 수 있습니다. 또한 특정 시간 간격 동안 vCenter Server Bash 셸에 대한 액세스를 사용하도록 설정할 수 있습니다.

사전 요구 사항

vCenter Server 관리 인터페이스에 루트로 로그인합니다.

절차

1 vCenter Server 관리 인터페이스에서 **액세스**를 클릭하고 **편집**을 클릭합니다.

2 vCenter Server에 대한 액세스 설정을 편집합니다.

옵션	설명
SSH 로그인 사용	SSH를 통해 vCenter Server에 액세스할 수 있도록 설정합니다.
DCUI 사용	DCUI를 통해 vCenter Server에 액세스할 수 있도록 설정합니다.
콘솔 CLI 사용	콘솔 CLI를 통해 vCenter Server에 액세스할 수 있도록 설정합니다.
Bash 셸 사용	입력한 시간 동안 Bash 셸을 통해 vCenter Server에 액세스하도록 설정합니다.

3 **확인**을 클릭하여 설정을 저장합니다.

DNS, IP 주소 및 프록시 설정 구성

고정 및 DHCP, IPv4 및 IPv6 주소 조합을 설정하고, DNS 설정을 편집하고, vCenter Server에 대한 프록시 설정을 정의할 수 있습니다.

사전 요구 사항

- 장치의 IP 주소를 변경하려면 장치의 시스템 이름이 FQDN인지 확인합니다. 시스템 이름은 기본 네트워크 식별자로 사용됩니다. 장치를 배포하는 동안 시스템 이름으로 IP 주소를 설정한 경우에는 나중에 PNID를 FQDN으로 변경할 수 있습니다.

  참고 IPv4 IP 주소만 시스템 이름으로 설정할 수 있습니다. 이렇게 설정하기 전에 IPv4 IP 주소를 사용하도록 설정해야 합니다.

- 이중 스택 VC를 복원하려면 1단계 배포 후 기본 VC를 다음과 같이 구성해야 합니다.
  - 백업된 VC의 PNID가 IPv4로 확인되고 IPv4가 고정으로 구성된 경우에는 1단계 중 기본 VC에 고정 또는 DHCP IPv4가 구성되어 있어야 합니다.
  - 백업된 VC의 PNID가 IPv4로 확인되고 IPv4가 DHCP로 구성된 경우에는 1단계 중 기본 VC에 DHCP IPv4가 구성되어 있어야 합니다.
  - 백업된 VC의 PNID가 IPv6로 확인되고 IPv6가 고정으로 구성된 경우에는 1단계 중 기본 VC에 고정 또는 DHCP IPv6가 구성되어 있어야 합니다.
  - 백업된 VC의 PNID가 IPv6로 확인되고 IPv6가 DHCP로 구성된 경우에는 1단계 중 기본 VC에 DHCP IPv6가 구성되어 있어야 합니다.

- vCenter Server 관리 인터페이스에 루트로 로그인합니다.

절차

1 vCenter Server 관리 인터페이스에서 **네트워킹**을 클릭합니다.

2 [네트워크 설정] 페이지에서 **편집**을 클릭합니다.

3 [호스트 이름 및 DNS] 섹션을 확장하여 DNS 설정을 구성합니다.

참고 호스트 이름으로 유효한 값은 사용하도록 설정된 IP 주소 또는 IPv4 IP 주소로 확인되는 FQDN입니다.

옵션	설명
자동으로 DNS 설정 가져오기	네트워크에서 DNS 설정을 자동으로 가져옵니다.
DNS 설정 수동 입력	DNS 주소 설정을 수동으로 설정할 수 있습니다. 이 옵션을 선택하면 다음 정보를 반드시 제공해야 합니다. ■ 기본 DNS 서버의 IP 주소 ■ (선택 사항) 대체 DNS 서버의 IP 주소

4 [네트워크 설정] 페이지에서 **편집**을 클릭합니다.

5 NIC0 섹션을 확장하여 게이트웨이 설정을 구성합니다.

참고 PNID 및 네트워크 API는 NIC0만 기본 NIC로 지원합니다.

6 IPv4 주소 설정을 편집합니다.

옵션	설명
IPv4 설정 사용 또는 사용 안 함	전환 스위치 옵션을 기반으로 IPv4 주소를 사용하거나 사용하지 않도록 설정합니다.
자동으로 IPv4 설정 가져오기	네트워크에서 장치의 IPv4 주소를 자동으로 가져옵니다.
IPv4 설정 수동 입력	수동으로 설정한 IPv4 주소를 사용합니다. IP 주소, 서브넷 접두사 길이 및 기본 게이트웨이를 입력해야 합니다. **참고** 고정 IPv4 또는 IPv6 주소의 경우 DNS 서버를 수동으로 설정해야 합니다.

참고 IPv4 및 IPv6 IP 주소가 변경되면 세컨드 파티 및 타사 솔루션을 다시 등록해야 합니다.

7 IPv6 주소 설정을 편집합니다.

옵션	설명
IPv6 설정 사용 또는 사용 안 함	전환 스위치 옵션을 기반으로 IPv6 주소를 사용하거나 사용하지 않도록 설정합니다.
DHCP를 통해 자동으로 IPv6 설정 가져오기	DHCP를 사용하여 네트워크에서 장치에 IPv6 주소를 자동으로 할당합니다.

옵션	설명
라우터 알림을 통해 자동으로 IPv6 설정 가져오기	라우터 알림을 사용하여 네트워크에서 장치에 IPv6 주소를 자동으로 할당합니다.
정적 IPv6 주소 사용	수동으로 설정한 정적 IPv6 주소를 사용합니다. 1 확인란을 클릭합니다. 2 IPv6 주소 및 서브넷 접두사 길이를 입력합니다. 3 **추가**를 클릭하여 추가 IPv6 주소를 입력합니다. 4 **저장**을 클릭합니다. **참고** 고정 IPv4 또는 IPv6 주소의 경우 DNS 서버를 수동으로 설정해야 합니다.

DHCP 및 라우터 알림을 통해 IPv6 설정을 자동으로 가져오도록 장치를 구성할 수 있습니다. 동시에 정적 IPv6 주소를 할당할 수 있습니다.

참고 IPv4 및 IPv6 IP 주소가 변경되면 세컨드 파티 및 타사 솔루션을 다시 등록해야 합니다.

8 프록시 서버를 구성하려면 [프록시 설정] 섹션에서 **편집**을 클릭합니다.

9 사용하도록 설정할 프록시 설정 선택

옵션	설명
HTTPS	HTTPS 프록시 설정을 구성하려면 사용하도록 설정합니다.
FTP	FTP 프록시 설정을 구성하려면 사용하도록 설정합니다. **참고** 프록시 서버에서 ICMP가 사용되도록 설정되어 있는지 확인합니다.
HTTP	HTTP 프록시 설정을 구성하려면 사용하도록 설정합니다.

10 서버 호스트 이름 또는 IP 주소를 입력합니다.

11 포트를 입력합니다.

12 사용자 이름을 입력합니다(선택 사항).

13 암호를 입력합니다(선택 사항).

14 **저장**을 클릭합니다.

기본 네트워크 식별자 재구성

vCenter Server 관리 네트워크의 FQDN, IP 또는 PNID를 변경할 수 있습니다.

사전 요구 사항

시스템 이름은 기본 네트워크 식별자로 사용됩니다. 장치를 배포하는 동안 시스템 이름으로 IP 주소를 설정한 경우에는 나중에 PNID를 FQDN으로 변경할 수 있습니다.

vCenter HA(고가용성)가 사용되도록 설정된 경우에는 PNID를 재구성하기 전에 vCenter HA 설정을 사용하지 않도록 설정해야 합니다.

절차

1. 관리자 SSO 자격 증명을 사용하여 vCenter Server 관리 인터페이스에 로그인합니다.
2. vCenter Server 관리 인터페이스에서 **네트워킹** 페이지로 이동하여 **편집**을 클릭합니다.
3. 수정할 NIC를 선택하고 **다음**을 클릭합니다.
4. **설정 편집** 창에서 호스트 이름을 변경하고 새 IP 주소를 입력합니다. **다음**을 클릭합니다.
5. **SSO 자격 증명** 창에서 관리자 SSO 자격 증명을 입력합니다. **administrator@<domain_name>** 자격 증명을 사용해야 합니다.
6. **완료 준비** 창에서 새 설정을 검토하고 백업 승인 상자를 선택합니다. **마침**을 클릭합니다.

   작업 표시줄에 네트워크 업데이트의 상태가 표시됩니다. 업데이트를 취소하려면 **네트워크 업데이트 취소**를 클릭합니다. 네트워크 재구성이 완료되면 UI가 새 IP 주소로 리디렉션됩니다.
7. 재구성 프로세스를 완료하고 서비스를 다시 시작하려면 관리자 SSO 자격 증명을 사용하여 로그인합니다.
8. **네트워킹** 페이지에서 새 호스트 이름 및 IP 주소를 확인합니다.

다음에 수행할 작업

- 배포되어 있는 모든 플러그인을 다시 등록합니다.
- 모든 사용자 지정 인증서를 재생성합니다.
- vCenter HA가 사용되도록 설정된 경우, vCenter HA를 재구성합니다.
- 활성 도메인이 사용되도록 설정된 경우 활성 도메인을 재구성합니다.
- 하이브리드 연결 모드가 사용되도록 설정된 경우 클라우드 vCenter Server를 사용하여 하이브리드 연결 하이브리드 연결을 재구성합니다.

방화벽 설정 편집

vCenter Server를 배포한 후 해당 방화벽 설정을 편집하고 관리 인터페이스를 사용하여 방화벽 규칙을 생성할 수 있습니다.

방화벽 규칙을 설정하여 vCenter Server와 특정 서버, 호스트 또는 가상 시스템 간의 트래픽을 허용하거나 차단할 수 있습니다. 특정 포트를 차단할 수 없고 모든 트래픽을 차단합니다.

사전 요구 사항

vCenter Server 인스턴스에 로그인하는 사용자가 vCenter Single Sign-On에서 SystemConfiguration.Administrators 그룹의 멤버인지 확인합니다.

절차

1. vCenter Server 관리 인터페이스에서 **방화벽**을 클릭합니다.

2 방화벽 설정을 편집합니다.

명령	작업
추가	a 방화벽 규칙을 생성하려면 **추가**를 클릭합니다. b 가상 시스템의 네트워크 인터페이스를 선택합니다. c 이 규칙을 적용할 네트워크의 IP 주소를 입력합니다. IP 주소는 IPv4 및 IPv6 주소가 될 수 있습니다. d 서브넷 접두사 길이를 입력합니다. e **작업** 드롭다운 메뉴에서 vCenter Server와 입력한 네트워크 간의 연결을 **허용**, **무시**, **거부** 또는 **반환**할지 선택합니다. f **저장**을 클릭합니다.
편집	a 규칙을 선택하고 **편집**을 클릭합니다. b 규칙 설정을 편집합니다. c **저장**을 클릭합니다.
삭제	a 규칙을 선택하고 **삭제**를 클릭합니다. b 메시지가 표시되면 **삭제**를 다시 클릭합니다.
순서 변경	a 규칙을 선택하고 **순서 변경**을 클릭합니다. b [순서 변경] 창에서 이동할 규칙을 선택합니다. c **위로 이동** 또는 **아래로 이동**을 클릭합니다. d **저장**을 클릭합니다.

시스템 표준 시간대 및 시간 동기화 설정 구성

vCenter Server를 배포한 후 vCenter Server 관리 인터페이스에서 시스템 표준 시간대 및 시간 동기화 설정을 변경할 수 있습니다.

vCenter Server를 배포하는 경우 vCenter Server가 실행되고 있는 ESXi 호스트의 시간 설정을 사용하거나 NTP 서버를 기반으로 시간 동기화를 구성합니다. vSphere 네트워크의 시간 설정이 변경될 경우 장치의 표준 시간대 및 시간 동기화 설정을 편집할 수 있습니다.

사전 요구 사항

vCenter Server 관리 인터페이스에 루트로 로그인합니다.

절차

1 vCenter Server 관리 인터페이스에서 **시간**을 클릭합니다.

2 시스템 표준 시간대 설정을 구성합니다.

a 표준 시간대 창에서 **편집**을 클릭합니다.

b **표준 시간대** 드롭다운 메뉴에서 위치나 표준 시간대를 선택하고 **저장**을 클릭합니다.

3 시간 동기화 설정을 구성합니다.

a [시간 동기화] 창에서 **편집**을 클릭합니다.

b **모드** 드롭다운 메뉴에서 시간 동기화 방법을 구성합니다.

옵션	설명
사용 안 함	시간이 동기화되지 않습니다. 시스템 표준 시간대 설정을 사용합니다.
호스트	VMware Tools 시간 동기화를 사용하도록 설정합니다. VMware Tools를 사용하여 장치의 시간을 ESXi 호스트의 시간과 동기화합니다.
NTP	NTP 동기화를 사용하도록 설정합니다. NTP 서버 하나 이상의 IP 주소 또는 FQDN을 입력해야 합니다.

c **저장**을 클릭합니다.

서비스 시작, 중지 및 다시 시작

vCenter Server 관리 인터페이스를 사용하여 vCenter Server 구성 요소의 상태를 보고 서비스를 시작, 중지 및 다시 시작할 수 있습니다.

사전 요구 사항

vCenter Server 관리 인터페이스에 루트로 로그인합니다.

절차

1 vCenter Server 관리 인터페이스에서 **서비스**를 클릭합니다.

서비스 페이지에는 설치된 서비스의 테이블이 표시되며, 이러한 서비스를 이름, 시작 유형 및 상태를 기준으로 정렬할 수 있습니다.

2 서비스를 선택하고 **시작 유형 설정**을 클릭하여 서비스의 수동 또는 자동 시작을 구성합니다.

3 서비스를 선택하고 **시작**을 클릭하여 서비스를 시작합니다.

4 서비스를 선택하고 **중지**를 클릭하여 중지하거나 **다시 시작**을 클릭하여 서비스를 다시 시작한 다음 **확인**을 클릭합니다.

경고 일부 서비스를 중지하거나 다시 시작하면 기능을 일시적으로 사용하지 못하게 될 수 있습니다.

업데이트 설정 구성

vCenter Server 관리 인터페이스를 사용하여 업데이트 설정을 구성하고 새 업데이트를 확인할 수 있습니다.

사전 요구 사항

vCenter Server 관리 인터페이스에 루트로 로그인합니다.

절차

1 vCenter Server 관리 인터페이스에서 **업데이트**를 클릭합니다.

2 업데이트 설정을 구성하려면 **설정**을 클릭합니다.

   a 자동으로 업데이트를 확인하려면 확인란을 선택합니다.

   b 기본 또는 사용자 지정 저장소를 사용하려면 선택합니다.

   c 사용자 지정 저장소를 선택한 경우 저장소 URL, 사용자 이름(선택 사항) 및 암호(선택 사항)를 입력합니다. **저장**을 클릭합니다.

   URL에는 HTTPS 및 FTPS 프로토콜이 지원됩니다.

3 업데이트를 수동으로 확인하려면 **업데이트 확인** 드롭다운 메뉴를 클릭합니다.

   a **CD-ROM** 또는 **CD-ROM + URL**에서 업데이트를 확인하려면 선택합니다.

결과

[사용 가능한 업데이트] 테이블에 사용 가능한 업데이트가 표시되며, 이를 버전, 유형, 릴리스 날짜, 재부팅 요구 사항 및 심각도를 기준으로 정렬할 수 있습니다.

루트 사용자의 암호 및 암호 만료 설정 변경

vCenter Server를 배포할 때, 루트 사용자의 초기 암호를 설정합니다. 이 암호는 기본적으로 90일 후 만료됩니다. vCenter Server 관리 인터페이스에서 루트 암호 및 암호 만료 설정을 변경할 수 있습니다.

사전 요구 사항

vCenter Server 관리 인터페이스에 루트로 로그인합니다.

절차

1 vCenter Server 관리 인터페이스에서 **관리**를 클릭합니다.

2 [암호] 섹션에서 **변경**을 클릭합니다.

3 현재 암호와 새 암호를 입력하고 **저장**을 클릭합니다.

4 루트 사용자에 대한 암호 만료 설정을 구성합니다.

a [암호 만료 설정] 섹션에서 **편집**을 클릭하고 암호 만료 정책을 선택합니다.

옵션	설명
예	루트 사용자의 암호가 지정된 기간(일) 후 만료됩니다. 다음 정보를 제공해야 합니다. ■ **루트 암호 유효성(일)** 암호가 만료되는 일수입니다. ■ **만료 주의용 이메일** vCenter Server가 만료 날짜 전에 주의 메시지를 보내는 이메일 주소입니다.
아니요	루트 사용자 암호가 만료되지 않습니다.

b [암호 만료 설정] 창에서 **저장**을 클릭하여 새 암호 만료 설정을 적용합니다.

[암호 만료 설정] 섹션에 새 만료 날짜가 표시됩니다.

vCenter Server 로그 파일을 원격 Syslog 서버

vCenter Server 로그 파일을 원격 syslog 서버에 전달하여 로그 분석을 수행할 수 있습니다.

참고 로그 파일을 로컬 디스크에 저장하지 않고 vCenter Server로 전송하도록 ESXi를 구성할 수 있습니다. 로그 수집을 위해 지원되는 최대 권장 호스트 수는 30입니다. ESXi 로그 전달을 구성하는 방법에 대한 자세한 내용은 http://kb.vmware.com/s/article/2003322를 참조하십시오. 이 기능은 상태 비저장 ESXi 호스트가 있는 소규모 환경을 위한 것이며, 다른 모든 경우에는 전용 로그 서버를 사용해야 합니다. vCenter Server를 사용하여 ESXi 로그 파일을 받으면 vCenter Server 성능에 영향을 미칠 수 있습니다.

사전 요구 사항

vCenter Server 관리 인터페이스에 루트로 로그인합니다.

절차

1 vCenter Server 관리 인터페이스에서 **Syslog**를 선택합니다.

2 원격 Syslog 호스트를 구성하지 않은 경우 [전달 구성] 섹션에서 **구성**을 클릭합니다. 호스트를 이미 구성한 경우 **편집**을 클릭합니다.

3 [전달 구성 생성] 창에서 대상 호스트의 서버 주소를 입력합니다. 지원되는 대상 호스트의 최대 수는 3개입니다.

4 **프로토콜** 드롭다운 메뉴에서 사용할 프로토콜을 선택합니다.

메뉴 항목	설명
TLS	전송 계층 보안(Transport Layer Security)
TCP	전송 제어 프로토콜(Transmission Control Protocol)

메뉴 항목	설명
RELP	Reliable Event Logging Protocol
UDP	사용자 데이터그램 프로토콜(User Datagram Protocol)

5 **포트** 텍스트 상자에 대상 호스트와 통신하는 데 사용할 포트 번호를 입력합니다.

6 [전달 구성 생성] 창에서 **추가**를 클릭하여 다른 원격 syslog 서버를 입력합니다.

7 **저장**을 클릭합니다.

8 원격 Syslog 서버가 메시지를 수신하는지 확인합니다.

9 [전달 구성] 섹션에서 **테스트 메시지 전송**을 클릭합니다.

10 원격 Syslog 서버에서 테스트 메시지가 수신되었는지 확인합니다.

새 구성 설정이 [전달 구성] 섹션에 표시됩니다.

백업 구성 및 스케줄링

vCenter Server 관리 인터페이스를 사용하여 백업 위치를 설정하고 백업 스케줄을 생성하며 백업 작업을 모니터링할 수 있습니다.

사전 요구 사항

vCenter Server 관리 인터페이스에 루트로 로그인합니다.

절차

1 vCenter Server 관리 인터페이스에서 **백업**을 클릭합니다.

2 백업 스케줄을 생성하려면 **구성**을 클릭합니다. 기존 백업 스케줄을 편집하려면 **편집**을 클릭합니다.

   a **백업 스케줄** 창에서 **`protocol://server-address<:port-number>/folder/subfolder`** 형식을 사용하여 백업 위치를 입력합니다.

      백업에 지원되는 프로토콜은 FTPS, HTTPS, SFTP, FTP, NFS, SMB 및 HTTP입니다.

   b 백업 서버의 사용자 이름과 암호를 입력합니다.

   c 백업이 발생하는 시간과 빈도를 입력합니다.

   d (선택 사항) 백업의 암호화 암호를 입력합니다.

   e 보존할 백업 수를 나타냅니다.

   f 백업할 데이터 유형을 나타냅니다.

3 수동 백업을 시작하려면 **지금 백업**을 클릭합니다.

결과

스케줄링된 백업 및 수동 백업에 대한 정보가 **작업** 테이블에 표시됩니다.

vSphere Client를 사용하여 vCenter Server 구성

3

Active Directory 도메인에 장치를 가입시키거나, 네트워킹 또는 기타 설정을 구성하는 등 vSphere Client에서 일부 구성 작업을 수행할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- vCenter Server 구성
- Active Directory 도메인 가입 또는 탈퇴
- SystemConfiguration.BashShellAdministrators 그룹에 사용자 추가
- 노드 재부팅
- 노드의 상태 보기
- 지원 번들 내보내기

vCenter Server 구성

vSphere Client 및 vCenter Server 관리 인터페이스에서 vCenter Server를 구성할 수 있습니다.

수행할 수 있는 작업은 배포에 따라 달라집니다.

온-프레미스 vCenter Server

라이센싱, 통계 수집, 로깅 및 기타 설정을 포함한 다수의 vCenter Server 설정을 변경할 수 있습니다.

VMware Cloud on AWS의 vCenter Server

SDDC를 생성할 때 vCenter Server 인스턴스가 미리 구성됩니다. 구성 설정 및 고급 설정을 보고 오늘의 메시지를 설정할 수 있습니다.

vCenter Server를 구성하는 방법에 대한 자세한 내용은 "vCenter Server 구성" 가이드를 참조하십시오.

vCenter Server의 라이센스 설정 구성

평가 기간이 만료되거나 현재 할당된 라이센스가 만료되기 전에 vCenter Server 시스템에 라이센스를 할당해야 합니다. Customer Connect에서 vCenter Server 라이센스를 업그레이드, 결합 또는 분할하는 경우에는 vCenter Server 시스템에 새 라이센스를 할당하고 이전 라이센스를 제거해야 합니다.

사전 요구 사항

- vSphere 환경에서 라이센스를 보고 관리하려면 vSphere Client가 실행되고 있는 vCenter Server 시스템에 대한 **글로벌.라이센스** 권한이 있어야 합니다.

절차

1. vSphere Client에서 vCenter Server 인스턴스로 이동합니다.
2. **구성** 탭을 선택합니다.
3. **설정**에서 **라이센싱**을 선택합니다.
4. **라이센스 할당**을 클릭합니다.
5. **라이센스 할당** 대화상자에서 수행하려는 작업을 선택합니다.
   - vSphere Client에서 기존 라이센스를 선택하거나 새로 생성된 라이센스를 선택합니다.

작업	단계
기존 라이센스 선택	목록에서 기존 라이센스를 선택하고 **확인**을 클릭합니다.
새로 생성된 라이센스 선택	a **새 라이센스** 탭을 클릭합니다. b **라이센스 할당** 대화상자에서 라이센스 키를 입력하거나 복사하여 붙여넣고 **확인**을 클릭합니다. c 새 라이센스 이름을 입력하고 **확인**을 클릭합니다. 제품, 제품 기능, 용량 및 만료 기간에 대한 세부 정보가 페이지에 나타납니다. d **확인**을 클릭합니다. e **라이센스 할당** 대화상자에서 새로 생성된 라이센스를 선택하고 **확인**을 클릭합니다.

결과

라이센스가 vCenter Server 시스템에 할당되고 라이센스 용량의 인스턴스 하나가 vCenter Server 시스템에 할당됩니다.

통계 설정 구성

통계 데이터 기록 방법을 설정하려면 통계 수집 간격을 구성합니다. 명령줄 모니터링 유틸리티나 vSphere Client의 성능 차트를 통해 저장된 통계 정보에 액세스할 수 있습니다.

vSphere Client에서 통계 수집 간격 구성

통계 수집 간격은 통계 쿼리의 발생 빈도, 통계 데이터가 데이터베이스에 저장되는 기간, 그리고 수집되는 통계 데이터의 유형을 결정합니다. 수집된 통계는 vSphere Client의 성능 차트나 명령줄 모니터링 유틸리티를 통해 볼 수 있습니다.

참고 일부 간격 특성은 구성할 수 없습니다.

사전 요구 사항

필요한 권한: **성능.ModifyIntervals**

절차

1 vSphere Client에서 vCenter Server 인스턴스로 이동합니다.

2 **구성** 탭을 선택합니다.

3 **설정**에서 **일반**을 선택합니다.

4 **편집**을 클릭합니다.

5 통계 간격을 사용하거나 사용하지 않도록 설정하려면 해당 간격에 대한 확인란을 선택합니다.

6 통계 간격 특성 값을 변경하려면 드롭다운 메뉴에서 값을 선택합니다.

   a **간격**에서 통계 데이터가 수집되는 시간 간격을 선택합니다.

   b **저장 기간**에서 아카이브된 통계가 데이터베이스에 보관되는 기간을 선택합니다.

   c **통계 수준**에서 새 통계 수집 수준을 선택합니다.

      수준이 낮을수록 적은 수의 통계 카운터가 사용됩니다. 수준 4에서는 모든 통계 카운터가 사용됩니다. 디버깅 목적으로만 사용합니다.

      통계 수준은 이전 통계 간격에 대해 설정된 통계 수준보다 낮거나 같아야 합니다. 이 요구 사항은 vCenter Server에 종속됩니다.

7 (선택 사항) 데이터베이스 크기에서는 데이터베이스에 대한 통계 설정의 영향을 예측합니다.

   a **물리적 호스트** 수를 입력합니다.

   b **가상 시스템** 수를 입력합니다.

      필요한 예상 공간과 필요한 데이터베이스 행 개수가 계산되어 표시됩니다.

   c 필요할 경우 통계 수집 설정을 변경합니다.

8 **저장**을 클릭합니다.

예제: 통계 간격에 대한 기본 설정 간의 관계

- 5분마다 수집되는 샘플은 1일 동안 저장됩니다.
- 30분마다 수집되는 샘플은 1주 동안 저장됩니다.
- 2시간마다 수집되는 샘플은 1개월 동안 저장됩니다.
- 1일간 수집되는 샘플은 1년 동안 저장됩니다.

모든 통계 간격에서 기본 수준은 1입니다. 이 수준에서는 클러스터 서비스, CPU, 디스크, 메모리, 네트워크, 시스템 및 가상 시스템 작업 카운터가 사용됩니다.

데이터 수집 수준

각 수집 간격마다 수집된 데이터의 양과 차트 표시용으로 사용 가능한 카운터를 결정하는 기본 수집 수준이 있습니다. 수집 수준을 통계 수준이라고도 합니다.

표 3-1. 통계 수준

수준	메트릭	모범 사례
수준 1	■ 클러스터 서비스(VMware DRS(Distributed Resource Scheduler)) - 모든 메트릭 ■ CPU – CPU 사용 권한, totalmhz, 사용량(평균), usagemhz ■ 디스크 – 용량, maxTotalLatency, 프로비저닝, 공유하지 않음, 사용량(평균), 사용됨 ■ 메모리 – 소요됨, 메모리 사용 권한, 오버헤드, swapinRate, swapoutRate, swapused, totalmb, 사용량(평균), vmmemctl(벌룬) ■ 네트워크 – 사용량(평균), IPv6 ■ 시스템 – 하트비트, 작동 시간 ■ 가상 시스템 작업 – numChangeDS, numChangeHost, numChangeHostDS	장기간 성능 모니터링(디바이스 통계가 필요하지 않은 경우)에 사용합니다. 수준 1은 모든 수집 간격 동안 기본 수집 수준입니다.
수준 2	■ 수준 1 메트릭 ■ CPU – 유휴 상태, reservedCapacity ■ 디스크 – umberRead 및 numberWrite를 제외한 모든 메트릭 ■ 메모리 – memUsed와 최대 및 최소 롤업 값을 제외한 모든 메트릭 ■ 가상 시스템 작업 – 모든 메트릭	장기간 성능 모니터링(디바이스 통계가 필요하지 않지만 기본 통계 이상을 모니터링하려는 경우)에 사용합니다.
수준 3	■ 수준 1과 수준 2 메트릭 ■ 최대 및 최소 롤업 값을 제외한 모든 카운터의 메트릭 ■ 디바이스 메트릭	단기 성능 모니터링(문제가 발생한 이후 또는 디바이스 통계가 필요할 때)에 사용합니다.
수준 4	최대 및 최소 롤업 값을 포함하여 vCenter Server로 지원된 모든 메트릭	단기 성능 모니터링(문제가 발생한 이후 또는 디바이스 통계가 필요할 때)에 사용합니다.

참고 통계 수준, 수준 3 또는 수준 4가 기본값을 초과하여 사용되면, 데이터베이스에 통계 정보를 필요한 만큼 빠르게 저장할 수 없는 경우 한 가지 특정 프로세스 vpxd가 메모리 증가를 견딜 수 있습니다. 통계 수준의 사용량 제한을 면밀하게 모니터링하지 않으면 vpxd의 메모리가 부족해져서 결국 충돌이 발생할 수 있습니다.

따라서 관리자가 이러한 수준을 높이기로 결정한 경우에는 관리자가 vpxd 프로세스의 크기를 모니터링하여 변경 후 무한정 증가하지 않는지 확인해야 합니다.

vCenter Server에 대한 런타임 설정 구성

vCenter Server ID, 관리 주소 및 이름을 변경할 수 있습니다. 동일한 환경에서 여러 vCenter Server 시스템을 실행하려면 변경을 수행해야 할 수 있습니다.

사전 요구 사항

필요한 권한: **글로벌.설정**

절차

1 vSphere Client에서 vCenter Server 인스턴스로 이동합니다.

2 **구성** 탭을 선택합니다.

3 **설정**에서 **일반**을 선택합니다.

4 **편집**을 클릭합니다.

5 [vCenter Server 설정 편집] 대화상자에서 **런타임 설정**을 선택합니다.

6 **vCenter Server 고유 ID**에 고유 ID를 입력합니다.

이 값을 공통 환경에서 실행되는 각각의 vCenter Server 시스템을 고유하게 식별할 0 ~ 63의 숫자로 변경할 수 있습니다. 기본적으로 ID 값은 임의로 생성됩니다.

7 **vCenter Server 관리 주소**에 vCenter Server 시스템 주소를 입력합니다.

주소는 IPv4, IPv6, 정규화된 도메인 이름, IP 주소 또는 다른 주소 형식일 수 있습니다.

8 **vCenter Server 이름**에 vCenter Server 시스템의 이름을 입력합니다.

vCenter Server의 DNS 이름을 변경할 경우 이 텍스트 상자를 사용하여 그에 맞게 vCenter Server 이름을 수정합니다.

9 **저장**을 클릭합니다.

다음에 수행할 작업

vCenter Server 시스템 고유 ID를 변경한 경우 변경 내용을 적용하려면 vCenter Server 시스템을 다시 시작해야 합니다.

사용자 디렉토리 설정 구성

vCenter Server가 ID 소스로 구성된 사용자 디렉토리 서버와 상호 작용하는 일부 방식을 구성할 수 있습니다.

vCenter Server 5.0 이전 vCenter Server 버전의 경우 이러한 설정이 vCenter Server와 연결된 Active Directory에 적용됩니다. vCenter Server 5.0 이상의 경우 이러한 설정이 vCenter Single Sign-On ID 소스에 적용됩니다.

사전 요구 사항

필요한 권한: **글로벌.설정**

절차

1 vSphere Client에서 vCenter Server 인스턴스로 이동합니다.

2 **구성** 탭을 선택합니다.

3 **설정**에서 **일반**을 선택합니다.

4 **편집**을 클릭합니다.

5 [vCenter 일반 설정 편집] 창에서 **사용자 디렉토리**를 선택합니다.

6 **사용자 디렉토리 시간 초과**에 디렉토리 서버 연결에 대한 시간 초과 간격(초)을 입력합니다.

7 **쿼리 제한** 확인란을 사용하도록 설정하여 쿼리 제한 크기를 설정합니다.

8 **쿼리 제한 크기**에 vCenter Server 시스템의 하위 인벤토리 개체에 대한 사용 권한을 연결할 수 있는 사용자 및 그룹의 수를 입력합니다.

참고 vSphere 인벤토리 개체에 대해 **관리 > 사용 권한**에서 **사용 권한 추가**를 클릭할 때 표시되는 [사용 권한 추가] 대화상자에서 사용 권한을 사용자 및 그룹과 연결할 수 있습니다.

9 **저장**을 클릭합니다.

메일 보낸 사람 설정 구성

이메일 알림을 경보 작업으로 설정하는 등의 vCenter Server 작업을 설정하려면 보낸 사람 계정의 이메일 주소를 구성해야 합니다. 익명 또는 인증 모드를 사용하여 이메일 경고 및 경보를 보낼 수 있습니다.

사전 요구 사항

필요한 권한: **글로벌.설정**

SMTP 인증을 사용할 수 있는 경우:

- vSphere 7.0 업데이트 1 이상 버전에서만 사용할 수 있습니다.
- Office 365 사서함 사용자만 사용할 수 있습니다.
- SMTP 메일 발신자는 Microsoft 문서 SMTP AUTH 클라이언트 전송 요구 사항에 명시된 대로 SMTP 인증에 대한 기본 요구 사항을 충족해야 합니다.

절차

1 vSphere Client에서 vCenter Server 인스턴스로 이동합니다.

2 **구성** 탭을 선택합니다.

3 **설정**에서 **일반**을 선택합니다.

4 **편집**을 클릭합니다.

5 **메일**을 선택하고 vCenter Server가 이메일 경고를 보내는 데 사용하는 설정을 입력하십시오.

6 **메일 서버** 텍스트 상자에 SMTP 서버 정보를 입력합니다.

SMTP 서버는 이메일 메시지를 보내는 데 사용할 SMTP 게이트웨이의 IP 주소 또는 DNS 이름입니다.

- 메일을 익명으로 보내려면 SMTP 서버 정보를 메일 서버 이름으로 입력할 수 있습니다.

- SMTP 인증의 경우, 사용자 지정된 구성이 없으면 메일 서버 이름을 `smtp.office365.com`으로 입력해야 합니다. IP 주소를 메일 서버로 사용하지 마십시오. SMTP 인증에는 IP 주소가 지원되지 않기 때문입니다.

7 **메일 발신자** 텍스트 상자에 발신자 계정 정보를 입력합니다.

보낸 사람 계정은 보낸 사람의 이메일 주소입니다.

SMTP 인증의 경우 **메일 발신자** 텍스트 상자에 유효한 SMTP 계정 이름을 입력해야 합니다.

참고 도메인 이름을 포함한 전체 이메일 주소를 입력해야 합니다.

예: ***mail_server@example.com***

8 **저장**을 클릭합니다.

9 이 단계는 SMTP 인증에만 적용됩니다.

SMTP 사용자 설정은 다음과 같이 구성해야 합니다.

a **구성** 탭을 선택합니다.

b **고급 설정**을 선택합니다.

c **설정 편집**을 클릭하고 구성 매개 변수에 대해 다음 값을 입력합니다.

이름	값
`mail.smtp.username`	유효한 SMTP 계정 이름입니다. **참고** 이 계정 이름은 7단계에서 SMTP 인증을 사용하여 메일을 보내기 위해 **메일 발신자** 텍스트 상자에 제공한 계정 이름과 동일해야 합니다.
`mail.smtp.password`	유효한 SMTP 계정 암호입니다. **참고** 현재는 계정 암호가 마스킹되지 않고 표시됩니다. 향후 릴리스에서 마스킹을 사용할 수 있을 때까지 전용 SMTP 메일 사용자를 사용해야 합니다.
`mail.smtp.port`	587

d **저장**을 클릭합니다.

다음에 수행할 작업

다음 단계를 수행하여 메일 설정을 테스트할 수 있습니다.

1 사용자 작업을 통해 트리거되는 경보를 생성합니다.

예를 들어 사용자 작업을 통해 가상 시스템의 전원을 끌 수 있습니다.

2 경보가 트리거될 때 이메일이 수신되는지 확인합니다.

SNMP 설정 구성

vCenter Server에서 SNMP 트랩을 수신할 최대 4개의 수신기를 구성할 수 있습니다. 각 수신기마다 호스트 이름, 포트 및 커뮤니티를 지정합니다.

사전 요구 사항

필요한 권한: **글로벌.설정**

절차

1. vSphere Client에서 vCenter Server 인스턴스로 이동합니다.
2. **구성** 탭을 선택합니다.
3. **설정**에서 **일반**을 선택합니다.
4. **편집**을 클릭합니다.
5. **SNMP 수신기**를 선택합니다.
6. **수신기 1 사용** 확인란을 선택합니다.
7. **기본 수신기 URL**에서 SNMP 수신기의 호스트 이름이나 IP 주소를 입력합니다.
8. **수신기 포트**에 수신기의 포트 번호를 입력합니다.

   포트 번호는 1 ~ 65535의 값이어야 합니다.
9. **커뮤니티 문자열**에 커뮤니티 식별자를 입력합니다.
10. 여러 수신기에 경보를 전송하려면 추가 **수신기 사용** 확인란을 선택하고 이러한 수신기의 호스트 이름, 포트 번호 및 커뮤니티 식별자를 입력합니다.
11. **저장**을 클릭합니다.

포트 설정 보기

웹 서비스에서 다른 애플리케이션과 통신하는 데 사용하는 포트를 볼 수 있습니다. 이러한 포트 설정은 구성할 수 없습니다.

웹 서비스는 VMware vCenter Server 설치의 일부로 설치됩니다. 웹 서비스는 VMware SDK API(애플리케이션 프로그래밍 인터페이스)를 사용하는 타사 애플리케이션의 필수 구성 요소입니다. 웹 서비스 설치에 대한 자세한 내용은 "vCenter Server 설치 및 설정" 설명서를 참조하십시오.

절차

1. vSphere Client에서 vCenter Server 인스턴스로 이동합니다.
2. **구성** 탭을 선택합니다.
3. **설정**에서 **일반**을 선택합니다.
4. **편집**을 클릭합니다.

5 **포트**를 선택합니다.

웹 서비스에서 사용하는 포트가 표시됩니다.

6 **저장**을 클릭합니다.

시간 초과 설정 구성

vCenter Server 작업에 대한 시간 초과 간격을 구성할 수 있습니다. 지정한 이 시간 초과 간격이 지나면 vSphere Client가 시간 초과됩니다.

사전 요구 사항

필요한 권한: **글로벌.설정**

절차

1 vSphere Client에서 vCenter Server 인스턴스로 이동합니다.

2 **구성** 탭을 선택합니다.

3 **설정**에서 **일반**을 선택합니다.

4 **편집**을 클릭합니다.

5 **시간 초과 설정**을 선택합니다.

6 **일반**에 일반 작업의 시간 초과 간격(초)을 입력합니다.

값을 0으로 설정하지 마십시오.

7 **긴 작업**에 긴 작업의 시간 초과 간격(분)을 입력합니다.

값을 0으로 설정하지 마십시오.

8 **저장**을 클릭합니다.

9 vCenter Server 시스템을 재시작하여 변경 내용을 적용합니다.

로깅 옵션 구성

vCenter Server에서 로그 파일에 수집하는 세부 정보의 양을 구성할 수 있습니다.

사전 요구 사항

필요한 권한: **글로벌.설정**

절차

1 vSphere Client에서 vCenter Server 인스턴스로 이동합니다.

2 **구성** 탭을 선택합니다.

3 **설정**에서 **일반**을 선택합니다.

4 **편집**을 클릭합니다.

5 **로깅 설정**을 선택합니다.

6 로깅 옵션을 선택합니다.

옵션	설명
없음	로깅 끄기
Error	오류 로그 항목만 표시
주의	경고 및 오류 로그 항목 표시
정보	정보, 오류 및 경고 로그 항목 표시
세부 정보 표시	정보, 오류, 경고 및 세부 로그 항목 표시
기타 정보	정보, 오류, 경고, 세부 로그 항목 및 기타 로그 항목 표시

7 **저장**을 클릭합니다.

결과

로깅 설정을 변경하면 즉시 적용됩니다. vCenter Server 시스템을 다시 시작할 필요가 없습니다.

데이터베이스 설정 구성

동시에 발생할 수 있는 최대 데이터베이스 연결 수를 구성할 수 있습니다. vCenter Server 데이터베이스의 확장을 제한하고 스토리지 공간을 절약하기 위해 작업이나 이벤트에 대한 정보를 정기적으로 삭제하도록 데이터베이스를 구성할 수 있습니다.

참고 vCenter Server에 대한 전체 작업 및 이벤트 기록을 보존하려면 데이터베이스 보존 옵션을 사용하지 마십시오.

절차

1 vSphere Client에서 vCenter Server 인스턴스로 이동합니다.

2 **구성** 탭을 선택합니다.

3 **설정**에서 **일반**을 선택합니다.

4 **편집**을 클릭합니다.

5 [vCenter 일반 설정 편집] 창에서 **데이터베이스**를 클릭합니다.

6 **최대 연결 수** 필드에 필요한 연결 수를 입력합니다.

참고 이러한 문제 중 하나가 시스템에 있는 경우가 아니면 이 값을 변경하지 마십시오.

- vCenter Server 시스템이 많은 작업을 자주 수행하며 성능이 중요한 경우에는 연결 수를 늘립니다.
- 데이터베이스가 공유되며 데이터베이스 연결에 비용이 많이 드는 경우에는 연결 수를 줄입니다.

7 보존된 작업을 주기적으로 삭제하려면 vCenter Server에 대한 **작업 정리** 옵션을 사용하도록 설정합니다.

8 (선택 사항) **작업 보존(일)** 필드에 값을 일 단위로 입력합니다.

지정한 일수가 지나면 이 vCenter Server 시스템에서 수행된 작업에 대한 정보가 삭제됩니다.

9 보존된 이벤트를 주기적으로 정리하려면 vCenter Server에 대한 **이벤트 정리** 옵션을 사용하도록 설정합니다.

10 (선택 사항) **이벤트 보존(일)** 필드에 값을 일 단위로 입력합니다.

지정한 일수가 지나면 이 vCenter Server 시스템 관련 이벤트에 대한 정보가 삭제됩니다.

참고 vCenter Server 관리 인터페이스에서 vCenter Server 데이터베이스 사용 및 디스크 파티션을 모니터링합니다.

경고 이벤트 보존 기간이 30일을 초과하도록 늘리면 vCenter 데이터베이스 크기가 현저히 증가하고 vCenter Server가 종료될 수 있습니다. 이 점을 고려하여 vCenter 데이터베이스를 늘려야 합니다.

11 vCenter Server를 다시 시작하여 변경 내용을 수동으로 적용합니다.

12 **저장**을 클릭합니다.

레거시 호스트의 SSL 인증서 확인

연결되는 호스트의 SSL 인증서를 확인하도록 vCenter Server를 구성할 수 있습니다. 이 설정을 구성하는 경우 vCenter Server 및 vSphere Client가 호스트를 추가하거나 가상 시스템에 원격 콘솔을 연결하는 등의 작업을 수행하기 위해 호스트에 연결하기 전에 먼저 유효한 SSL 인증서를 확인합니다.

vCenter Server 5.1 및 vCenter Server 5.5는 항상 SSL 지문 인증서를 사용하여 ESXi 호스트에 연결합니다. vCenter Server 6.0부터 SSL 인증서는 기본적으로 VMware 인증 기관에서 서명됩니다. 대신 타사 CA의 인증서를 사용할 수 있습니다. 지문 모드는 레거시 호스트에만 지원됩니다.

절차

1 vSphere Client에서 vCenter Server 인스턴스로 이동합니다.

2 **구성** 탭을 선택합니다.

3 **설정**에서 **일반**을 선택합니다.

4 **편집**을 클릭합니다.

5 **SSL 설정**을 선택합니다.

6 검증이 필요한 각 레거시 호스트에 대해 호스트 지문을 확인합니다.

a 직접 콘솔에 로그인합니다.

b **시스템 사용자 지정** 메뉴에서 **지원 정보 보기**를 선택합니다.

지문이 오른쪽 열에 표시됩니다.

7 호스트에서 얻은 지문과 vCenter Server SSL 설정 대화상자에 나열된 지문을 비교합니다.

8 지문이 일치하면 호스트의 확인란을 선택합니다.

선택되지 않은 호스트는 **저장**을 클릭한 후 연결 해제됩니다.

9 **저장**을 클릭합니다.

고급 설정 구성

고급 설정에서 vCenter Server 구성 파일 `vpxd.cfg`를 수정할 수 있습니다.

고급 설정을 사용하여 `vpxd.cfg` 파일에 항목을 추가할 수 있지만 이러한 항목을 편집하거나 삭제할 수는 없습니다. 이러한 설정은 VMware 기술 지원 센터에서 변경할 것을 지시했거나 VMware 설명서의 특정 지침을 따르는 경우에만 변경하는 것이 좋습니다.

사전 요구 사항

필요한 권한: **글로벌.설정**

절차

1 vSphere Client에서 vCenter Server 인스턴스로 이동합니다.

2 **구성** 탭을 선택합니다.

3 **고급 설정**을 선택합니다.

4 **설정 편집**을 클릭합니다.

5 **이름** 필드에 설정 이름을 입력합니다. 이름은 'config'로 시작되어야 합니다. 예: **`config.log`**

6 **값** 필드에 지정된 설정의 값을 입력합니다.

7 **추가**를 클릭합니다.

8 **저장**을 클릭합니다.

결과

새로 추가된 고급 설정으로 `vpxd.cfg` 파일에서 설정 키에 `config.`이 추가됩니다. 예:

```
config.example.setting = exampleValue
```

다음에 수행할 작업

고급 설정을 변경하려면 많은 경우 vCenter Server 시스템을 다시 시작해야 합니다. VMware 기술 지원 센터에 문의하여 다시 시작해야만 변경 내용이 적용되는지 여부를 확인하십시오.

로그인된 다른 사용자에게 메시지 보내기

관리자는 vCenter Server 시스템에 현재 로그인되어 있는 사용자에게 메시지를 보낼 수 있습니다. 메시지를 사용하여 유지 보수를 알리거나 사용자에게 임시 로그아웃을 요청할 수 있습니다.

절차

1 vSphere Client에서 vCenter Server 인스턴스로 이동합니다.

2 **구성**을 클릭합니다.

3 **설정 > 오늘의 메시지**를 선택하고 **편집**을 클릭합니다.

4 메시지를 입력하고 **확인**을 클릭합니다.

결과

각 활성 사용자 세션에서 vSphere Client의 맨 위에 메시지가 표시됩니다.

Active Directory 도메인 가입 또는 탈퇴

vCenter Server를 Active Directory 도메인에 가입시킬 수 있습니다. 이 Active Directory 도메인에서 vCenter Single Sign-On 도메인으로 사용자 및 그룹을 연결할 수 있습니다. Active Directory 도메인을 탈퇴할 수 있습니다.

중요 RODC(읽기 전용 도메인 컨트롤러)가 있는 Active Directory 도메인에 vCenter Server를 가입시키는 것은 지원되지 않습니다. 쓰기 가능 도메인 컨트롤러가 있는 Active Directory에만 vCenter Server를 가입시킬 수 있습니다.

Active Directory 사용자 및 그룹이 vCenter Server 구성 요소에 액세스할 수 있도록 사용 권한을 구성하려면 Active Directory 도메인에 vCenter Server 인스턴스를 가입시켜야 합니다.

예를 들어 Active Directory 사용자가 vSphere Client를 사용하여 vCenter Server 인스턴스에 로그인할 수 있게 하려면 vCenter Server 인스턴스를 Active Directory 도메인에 가입시키고 이 사용자에게 관리자 역할을 할당해야 합니다.

사전 요구 사항

- vCenter Server 인스턴스에 로그인하는 사용자가 vCenter Single Sign-On에서 SystemConfiguration.Administrators 그룹의 멤버인지 확인합니다.
- 장치의 시스템 이름이 FQDN인지 확인합니다. 장치 배포 과정에서 시스템 이름으로 IP 주소를 설정한 경우 vCenter Server를 Active Directory 도메인에 가입할 수 없습니다.

절차

1 vSphere Client를 사용하여 vCenter Server 인스턴스에 administrator@*your_domain_name*으로 로그인합니다.

2 vSphere Client 메뉴에서 **관리**를 선택합니다.

3 **Single Sign On > 구성**을 선택합니다.

4 **ID 제공자** 탭을 클릭하고 **Active Directory 도메인**을 ID 제공자 유형으로 선택합니다.

5 **AD 가입**을 클릭합니다.

6 [Active Directory 도메인 가입] 창에서 다음 세부 정보를 제공합니다.

옵션	설명
도메인	Active Directory 도메인 이름(예: mydomain.com)입니다. 이 텍스트 상자에 IP 주소를 입력하지 마십시오.
조직 구성 단위(선택 사항)	예를 들어 전체 OU(조직 구성 단위) LDAP FQDN은 OU=Engineering,DC=mydomain,DC=com입니다. **중요** LDAP에 익숙한 경우에만 이 텍스트 상자를 사용합니다.
사용자 이름	UPN(사용자 계정 이름) 형식의 사용자 이름입니다(예: jchin@mydomain.com). **중요** 다운 레벨 로그인 이름 형식(예: DOMAIN\UserName)은 지원되지 않습니다.
암호	사용자의 암호입니다.

참고 변경 내용을 적용하려면 노드를 재부팅하십시오.

7 **가입**을 클릭하여 vCenter Server를 Active Directory 도메인에 가입합니다.

작업이 자동으로 성공하고 [AD 가입] 옵션이 [AD 탈퇴]로 전환되는 것을 볼 수 있습니다.

8 (선택 사항) Active Directory 도메인을 탈퇴하려면 **AD 탈퇴**를 클릭합니다.

9 vCenter Server를 다시 시작하여 변경 내용을 적용합니다.

중요 vCenter Server를 다시 시작하지 않을 경우 vSphere Client를 사용할 때 문제가 발생할 수 있습니다.

10 **ID 소스** 탭을 선택하고 **추가**를 클릭합니다.

a [ID 소스 추가] 창에서 ID 소스 유형으로 **Active Directory(통합 Windows 인증)**를 선택합니다.

b 가입된 Active Directory 도메인의 ID 소스 설정을 입력하고 **추가**를 클릭합니다.

표 3-2. ID 소스 추가 설정

텍스트 상자	설명
도메인 이름	도메인의 FQDN입니다. 이 텍스트 상자에 IP 주소를 입력하지 마십시오.
시스템 계정 사용	로컬 시스템 계정을 SPN으로 사용하려면 이 옵션을 선택합니다. 이 옵션을 선택하는 경우 도메인 이름만 지정하십시오. 이 시스템의 이름을 변경해야 할 경우에는 이 옵션을 선택하지 마십시오.
SPN(서비스 사용자 이름) 사용:	로컬 시스템의 이름을 변경해야 할 경우 이 옵션을 선택합니다. SPN, ID 소스를 사용하여 인증할 수 있는 사용자 및 사용자 암호를 지정해야 합니다.

표 3-2. ID 소스 추가 설정 (계속)

텍스트 상자	설명
서비스 사용자 이름	Kerberos가 Active Directory 서비스를 식별하는 데 도움이 되는 SPN입니다. 이름에 도메인을 포함합니다(예: STS/example.com). `setspn -S`를 실행하여 사용할 사용자를 추가해야 할 수도 있습니다. `setspn`에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오. SPN은 전체 도메인에서 고유해야 합니다. `setspn -S`를 실행하면 중복 SPN이 생성되지 않았는지 확인할 수 있습니다.
사용자 이름	이 ID 소스를 사용하여 인증할 수 있는 사용자의 이름입니다. 이메일 주소 형식(예: jchin@mydomain.com)을 사용합니다. Active Directory 서비스 인터페이스 편집기(ADSI 편집)를 사용하여 사용자 계정 이름을 확인할 수 있습니다.
암호	이 ID 소스를 사용하여 인증하는 데 사용되는 사용자(사용자 계정 이름에 지정된 사용자)의 암호입니다. 도메인 이름을 포함합니다(예: jdoe@example.com).

결과

ID 소스 탭에서 가입된 Active Directory 도메인을 볼 수 있습니다.

다음에 수행할 작업

가입된 Active Directory 도메인의 사용자 및 그룹이 vCenter Server 구성 요소에 액세스하기 위한 사용 권한을 구성할 수 있습니다. 사용 권한 관리에 대한 자세한 내용은 "vSphere 보안" 설명서를 참조하십시오.

SystemConfiguration.BashShellAdministrators 그룹에 사용자 추가

vSphere Client를 사용하여 장치 Bash 셸에 액세스할 수 있도록 설정하려면 로그인하는 데 사용하는 사용자가 SystemConfiguration.BashShellAdministrators 그룹의 멤버여야 합니다. 기본적으로 이 그룹은 비어 있으며 수동으로 사용자를 그룹에 추가해야 합니다.

사전 요구 사항

vCenter Server 인스턴스에 로그인할 때 사용하는 사용자가 vCenter Single Sign-On 도메인에서 SystemConfiguration.Administrators 그룹의 멤버인지 확인하십시오.

절차

1 vSphere Client를 사용하여 vCenter Server 인스턴스에 administrator@*your_domain_name*으로 로그인합니다.

주소의 유형은 http://*appliance-IP-address-or-FQDN*/ui입니다.

2 vSphere Client 메뉴에서 **관리**를 선택합니다.

3 **Single Sign-On > 사용자 및 그룹**을 선택합니다.

4 **그룹** 탭을 클릭하고 그룹 이름 열에 있는 옵션에서 **SystemConfiguration.BashShellAdministrators**를 선택합니다.

5 **편집**을 클릭합니다.

6 **그룹 편집** 창에서 멤버를 추가하려면 드롭다운 메뉴에서 도메인을 선택한 후 필요한 사용자를 검색합니다.

7 **저장**을 클릭합니다.

노드 재부팅

vSphere Client에서 vCenter Server의 노드를 재부팅할 수 있습니다.

사전 요구 사항

vCenter Server 인스턴스에 로그인할 때 사용하는 사용자가 vCenter Single Sign-On 도메인에서 SystemConfiguration.Administrators 그룹의 멤버인지 확인하십시오.

절차

1 vSphere Client를 사용하여 vCenter Server 인스턴스에 administrator@*your_domain_name*으로 로그인합니다.

2 vSphere Client 기본 페이지에서 **관리 > 배포 > 시스템 구성**을 클릭합니다.

3 [시스템 구성] 아래의 목록에서 노드를 선택합니다.

4 **노드 재부팅**을 클릭합니다.

노드의 상태 보기

vSphere Client에서 vCenter Server 노드의 상태를 볼 수 있습니다.

vCenter Server 서비스를 실행하는 vCenter Server 인스턴스 및 시스템은 노드로 간주됩니다. 그래픽 배지는 노드의 상태를 나타냅니다.

사전 요구 사항

vCenter Server 인스턴스에 로그인할 때 사용하는 사용자가 vCenter Single Sign-On 도메인에서 SystemConfiguration.Administrators 그룹의 멤버인지 확인하십시오.

절차

1 vSphere Client를 사용하여 vCenter Server 인스턴스에 administrator@*your_domain_name*으로 로그인합니다.

주소의 유형은 http://*appliance-IP-address-or-FQDN*/ui입니다.

2 vSphere Client 메뉴에서 **관리**를 선택합니다.

3 **배포 > 시스템 구성**을 선택합니다.

4 상태를 볼 노드를 선택합니다.

표 3-3. 상태

배지 아이콘	설명
	정상. 개체의 상태가 정상입니다.
	주의. 개체에 일부 문제가 발생하고 있습니다.
	위험. 개체가 올바르게 작동하지 않거나 곧 작동이 중지됩니다.
	알 수 없습니다. 이 개체에 사용할 수 있는 데이터가 없습니다.

지원 번들 내보내기

vCenter Server에 포함된 특정 제품의 로그 파일이 포함되어 있는 지원 번들을 내보낼 수 있습니다.

사전 요구 사항

vCenter Server 인스턴스에 로그인하는 사용자가 vCenter Single Sign-On에서 SystemConfiguration.Administrators 그룹의 멤버인지 확인합니다.

절차

1 vSphere Client를 사용하여 vCenter Server 인스턴스에 administrator@*your_domain_name*으로 로그인합니다.

주소의 유형은 http://*appliance-IP-address-or-FQDN*/ui입니다.

2 vSphere Client 홈 페이지에서 **관리 > 배포 > 시스템 구성**을 클릭합니다.

3 목록에서 노드를 선택하고 **지원 번들 내보내기**를 클릭합니다.

4 **지원 번들 내보내기** 창에서 트리를 확장하여 장치에서 실행 중인 서비스를 확인하고 로그 파일을 내보낼 서비스의 선택을 취소합니다.

   기본적으로 모든 서비스가 선택되어 있습니다. 지원 번들을 내보내고 VMware 지원팀에 보내려면 모든 확인란을 선택된 상태로 둡니다. 서비스는 장치의 특정 제품의 서비스를 포함하는 클라우드 인프라 범주 및 장치와 vCenter Server 제품에 특정된 서비스를 포함하는 가상 장치 범주의 두 범주로 구분되어 있습니다.

5 **지원 번들 내보내기**를 클릭하고 번들을 로컬 시스템에 저장합니다.

결과

시스템에 지원 번들을 저장하였으며 탐색할 수 있습니다.

장치 셸을 사용하여 vCenter Server 구성

4

장치를 모니터링하고, 구성하고, 장치 문제를 해결하는 데 사용할 수 있는 모든 vCenter Server API 명령 및 플러그인은 장치 셸을 사용하여 액세스할 수 있습니다.

`pi` 키워드를 사용하거나 사용하지 않고 장치 셸에서 모든 명령을 실행할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 장치 셸에 액세스
- 장치 셸에서 Bash 셸 액세스를 사용하도록 설정
- 명령을 편집하기 위한 바로 가기 키
- 장치의 플러그인 및 API 명령에 대한 도움말 요청
- vCenter Server 셸의 플러그인
- showlog 플러그인을 사용하여 로그 파일 탐색
- 장치 셸의 API 명령
- vCenter Server에 대한 SNMP 구성
- vCenter Server에서 시간 동기화 설정 구성
- vCenter Server에서 로컬 사용자 계정 관리
- vCenter Server의 상태 및 통계 모니터링
- vimtop 플러그인을 사용하여 서비스의 리소스 사용 모니터링

장치 셸에 액세스

장치 셸에 포함된 플러그인에 액세스하고 API 명령을 보고 사용하려면 먼저 장치 셸에 액세스하십시오.

절차

1 장치 셸에 액세스합니다.
   - 장치 콘솔에 직접 액세스할 수 있으면 Alt+F1을 누릅니다.
   - 원격으로 연결하려면 SSH 또는 다른 원격 콘솔 연결을 사용하여 장치의 세션을 시작합니다.
2 장치에서 인식하는 사용자 이름 및 암호를 입력합니다.

결과

장치 셸에 로그인되고 시작 메시지가 표시됩니다.

장치 셸에서 Bash 셸 액세스를 사용하도록 설정

슈퍼 관리자 역할이 있는 사용자로서 장치 셸에 로그인하는 경우 다른 사용자가 장치의 Bash 셸에 액세스 가능하도록 설정할 수 있습니다. 루트 사용자는 기본적으로 장치 Bash 셸에 액세스할 수 있습니다.

장치 Bash 셸은 기본적으로 루트에 사용하도록 설정됩니다.

절차

1 장치 셸에 액세스하고 수퍼 관리자 역할을 가진 사용자로 로그인합니다.

수퍼 관리자 역할이 있는 기본 사용자는 루트입니다.

2 다른 사용자가 Bash 셸에 액세스 가능하도록 설정하려면 다음 명령을 실행합니다.

```
shell.set --enabled true
```

3 Bash 셸에 액세스하려면 `shell` 또는 `pi shell`을 실행합니다.

명령을 편집하기 위한 바로 가기 키

다양한 바로 가기 키를 사용하여 장치 Bash 셸에서 명령을 입력하고 편집할 수 있습니다.

표 4-1. 바로 가기 키 및 기능

바로 가기 키	세부 정보
탭	현재 명령을 완성합니다. 명령 이름의 일부를 입력하고 Tab 키를 누르면 시스템에서 명령 이름을 완성합니다. 입력한 문자 집합과 일치하는 명령을 보려면 문자를 입력하고 Tab 키를 누르십시오.
Enter(명령줄에서)	입력한 명령을 실행합니다.
Enter(**자세히** 프롬프트에서)	출력의 다음 페이지를 표시합니다.
Delete 또는 백스페이스	커서 왼쪽에 있는 문자를 삭제합니다.
왼쪽 화살표 또는 Ctrl+B	커서를 왼쪽으로 한 문자 이동합니다. 여러 줄에 걸쳐서 명령을 입력할 때는 왼쪽 화살표 또는 Ctrl-B 키를 눌러서 명령의 처음으로 돌아갈 수 있습니다.
오른쪽 화살표 또는 Ctrl+F	커서를 오른쪽으로 한 문자 이동합니다.
Esc, B	커서를 한 단어 뒤로 이동합니다.
Esc, F	커서를 한 단어 앞으로 이동합니다.
Ctrl+A	커서를 명령줄의 처음으로 이동합니다.
Ctrl+E	커서를 명령줄의 끝으로 이동합니다.

표 4-1. 바로 가기 키 및 기능 (계속)

바로 가기 키	세부 정보
Ctrl+D	커서에 의해 선택된 문자를 삭제합니다.
Ctrl+W	커서 옆의 단어를 삭제합니다.
Ctrl+K	줄의 뒷부분을 삭제합니다. Ctrl+K를 누르면 커서 위치부터 명령줄의 끝까지 입력한 모든 내용이 삭제됩니다.
Ctrl+U 또는 Ctrl+X	줄의 앞부분을 삭제합니다. Ctrl+U를 누르면 명령줄의 시작에서 커서 위치까지 입력한 모든 내용이 삭제됩니다.
Ctrl+T	커서 왼쪽에 있는 문자와 커서에 의해 선택된 문자의 위치를 바꿉니다.
Ctrl+R 또는 Ctrl+L	시스템 프롬프트와 명령줄을 표시합니다.
Ctrl+V 또는 Esc, Q	다음 키 입력을 편집 키가 아니라 명령 입력으로 취급해야 한다는 것을 시스템에 알리는 코드를 삽입합니다.
위쪽 화살표 또는 Ctrl+P	가장 최근의 명령부터 시작하여 기록 버퍼에 있는 명령을 리콜합니다.
아래쪽 화살표 또는 Ctrl+N	위쪽 화살표 또는 Ctrl+P를 사용하여 명령을 리콜한 후에 기록 버퍼에 있는 좀 더 최근의 명령으로 돌아갑니다.
Ctrl+Y	삭제 버퍼에서 가장 최근의 항목을 리콜합니다. 삭제 버퍼는 잘라내거나 삭제한 마지막 10개 항목을 포함하고 있습니다.
Esc, Y	삭제 버퍼에서 다음 항목을 리콜합니다. 삭제 버퍼는 잘라내거나 삭제한 마지막 10개 항목을 포함하고 있습니다. 먼저 Ctrl+Y를 눌러서 가장 최근의 항목을 리콜한 후에 Esc, Y를 최대 9번까지 눌러서 버퍼에 있는 나머지 항목을 리콜합니다.
Esc, C	커서에 의해 선택된 문자를 대문자로 표시합니다.
Esc, U	다음 공백에 도달할 때까지 커서에 의해 선택된 단어의 모든 문자를 대문자로 변경합니다.
Esc, L	커서에 의해 선택된 문자부터 해당 단어의 끝까지 단어의 대문자를 소문자로 변경합니다.

장치의 플러그인 및 API 명령에 대한 도움말 요청

장치 셸에서 vCenter Server 플러그인 및 API 명령에 액세스할 수 있습니다. 장치를 모니터링하고, 구성하고, 장치 문제를 해결하는 데 플러그인 및 명령을 사용할 수 있습니다.

Tab 키를 사용하여 API 명령, 플러그인 이름 및 API 매개 변수를 자동 완성할 수 있습니다. 플러그인 매개 변수는 자동 완성을 지원하지 않습니다.

절차

1 장치 셸에 액세스하고 로그인합니다.

2 플러그인에 대한 도움말을 보려면 `help pi list` 또는 `? pi list` 명령을 실행합니다.

장치의 모든 플러그인 목록이 수신됩니다.

3 API 명령에 대한 도움말을 보려면 `help api list` 또는 `? api list` 명령을 실행합니다.

장치의 모든 API 명령 목록이 수신됩니다.

4 특정 API 명령에 대한 도움말을 보려면 `help api api_name` 또는 `? api api_name` 명령을 실행합니다.

예를 들어 `com.vmware.appliance.version1.timesync.set` 명령에 대한 도움말을 보려면 `help api timesync.set` 또는 `? api timesync.set`를 실행합니다.

vCenter Server 셸의 플러그인

vCenter Server의 플러그인을 사용하면 다양한 관리 도구에 액세스할 수 있습니다. 플러그인은 CLI에 내장되어 있습니다. 플러그인은 독립형 Linux 또는 VMware 유틸리티이며 VMware 서비스에 의존하지 않습니다.

표 4-2. vCenter Server에서 사용 가능한 플러그인

플러그인	설명
com.vmware.clear	터미널 화면을 지우는 데 사용할 수 있는 플러그인입니다.
com.vmware.cmsso-util	PNID, 시스템 인증서에 대한 변경 사항을 오케스트레이션하고, Component Manager, vCenter Single Sign-On에서 노드의 등록을 취소하고, vCenter Server를 재구성하는 데 사용하는 플러그인입니다.
com.vmware.dcli	vAPI 기반 CLI 클라이언트입니다.
com.vmware.nslookup	DNS(도메인 이름 시스템)를 쿼리하여 도메인 이름 또는 IP 주소 매핑을 가져오는 데 사용하거나 기타 특정 DNS 레코드에 대해 사용할 수 있는 플러그인입니다.
com.vmware.pgrep	모든 명명된 프로세스를 검색하는 데 사용할 수 있는 플러그인입니다.
com.vmware.pgtop	PostgreSQL 데이터베이스를 모니터링하는 데 사용할 수 있는 플러그인입니다.
com.vmware.ping	원격 호스트를 ping하는 데 사용할 수 있는 플러그인입니다. bin/ping과 동일한 인수를 허용합니다.
com.vmware.ping6	원격 호스트를 ping하는 데 사용할 수 있는 플러그인입니다. bin/ping6과 동일한 인수를 허용합니다.
com.vmware.portaccess	호스트의 포트 액세스 문제를 해결하는 데 사용할 수 있는 플러그인입니다.
com.vmware.ps	실행 중인 프로세스에 대한 통계를 보는 데 사용할 수 있는 플러그인입니다.
com.vmware.rvc	Ruby vSphere 콘솔입니다.
com.vmware.service-control	VMware 서비스를 관리하는 데 사용할 수 있는 플러그인입니다.
com.vmware.shell	장치 Bash 셸에 대한 액세스를 허용하는 플러그인입니다.

표 4-2. vCenter Server에서 사용 가능한 플러그인 (계속)

플러그인	설명
com.vmware.showlog	로그 파일을 탐색하는 데 사용할 수 있는 플러그인입니다.
com.vmware.shutdown	장치를 다시 시작하거나 끄는 데 사용할 수 있는 플러그인입니다.
com.vmware.software-packages	장치에서 소프트웨어 패키지를 업데이트하는 데 사용할 수 있는 플러그인입니다.
com.vmware.support-bundle	로컬 파일 시스템에 번들을 생성하고 원격 Linux 시스템으로 내보내는 데 사용할 수 있는 플러그인입니다. 이 플러그인을 stream 명령과 함께 사용하면 지원 번들을 로컬 파일 시스템에서 생성하지 않고 원격 Linux 시스템으로 바로 내보냅니다.
com.vmware.top	프로세스 정보를 표시하는 플러그인입니다. /usr/bin/top/과 동일한 인수를 허용합니다.
com.vmware.tracepath	네트워크 호스트의 경로를 추적하는 플러그인입니다. sbin/tracepath와 동일한 인수를 허용합니다.
com.vmware.tracepath6	네트워크 호스트의 경로를 추적하는 플러그인입니다. /sbin/tracepath6과 동일한 인수를 허용합니다.
com.vmware.updatemgr-util	VMware Update Manager를 구성하는 데 사용할 수 있는 플러그인입니다.
com.vmware.vcenter-restore	vCenter Server를 복원하는 데 사용할 수 있는 플러그인입니다.
com.vmware.vimtop	vSphere 서비스 및 해당 리소스 사용량의 목록을 보는 데 사용할 수 있는 플러그인입니다.

showlog 플러그인을 사용하여 로그 파일 탐색

vCenter Server에서 로그 파일을 탐색하여 오류가 있는지 검사할 수 있습니다.

절차

1 장치 셸에 액세스하고 로그인합니다.

2 showlog 명령을 입력하고, 공백을 추가하고, Tab 키를 눌러 /var/log 폴더의 모든 컨텐츠를 봅니다.

3 firstboot 로그 파일을 보기 위한 명령을 실행합니다.

```
showlog /var/log/firstboot/cloudvm.log
```

장치 셸의 API 명령

vCenter Server의 API 명령을 사용하여 다양한 관리 작업을 수행할 수 있습니다. API 명령은 장치 관리 서비스에 의해 제공됩니다. 시간 동기화 설정을 편집하고, 프로세스 및 서비스를 모니터링하고, SNMP 설정을 지정하는 등의 작업을 수행할 수 있습니다.

표 4-3. vCenter Server에서 사용할 수 있는 API 명령

API 명령	설명
com.vmware.appliance.health.applmgmt.get	applmgmt 서비스 상태를 가져옵니다.
com.vmware.appliance.health.databasestorage.get	데이터베이스 스토리지 상태를 가져옵니다.
com.vmware.appliance.health.load.get	CPU 로드 상태를 가져옵니다.
com.vmware.appliance.health.mem.get	메모리 상태를 가져옵니다.
com.vmware.appliance.health.softwarepackages.get	시스템 업데이트 상태를 가져옵니다.
com.vmware.appliance.health.storage.get	전반적인 스토리지 상태를 가져옵니다.
com.vmware.appliance.health.swap.get	스왑 상태를 가져옵니다.
com.vmware.appliance.health.system.get	시스템 상태를 가져옵니다.
com.vmware.appliance.health.system.lastcheck	상태를 마지막으로 확인한 시간을 가져옵니다.
com.vmware.appliance.monitoring.list	모니터링되는 항목 목록을 가져옵니다.
com.vmware.appliance.monitoring.get	모니터링되는 항목 정보를 가져옵니다.
com.vmware.appliance.monitoring.query	모니터링되는 항목의 값 범위를 쿼리합니다.
com.vmware.appliance.recovery.backup.job.cancel	ID로 백업 작업을 취소합니다.
com.vmware.appliance.recovery.backup.job.create	백업 작업을 시작합니다.
com.vmware.appliance.recovery.backup.job.get	ID로 백업 작업의 상태를 가져옵니다.
com.vmware.appliance.recovery.backup.job.list	백업 작업 목록을 가져옵니다.
com.vmware.appliance.recovery.backup.parts.list	백업 작업에 포함될 수 있는 vCenter Server 구성 요소의 목록을 가져옵니다.
com.vmware.appliance.recovery.backup.parts.get	백업의 일부에 대한 세부 정보를 가져옵니다.
com.vmware.appliance.recovery.backup.validate	작업을 시작하지 않고 백업 작업에 대한 매개 변수를 검증합니다.
com.vmware.appliance.recovery.restore.job.cancel	복원 작업을 취소합니다.
com.vmware.appliance.recovery.restore.job.create	복원 작업을 시작합니다.
com.vmware.appliance.recovery.restore.job.get	복원 작업의 상태를 가져옵니다.

표 4-3. vCenter Server에서 사용할 수 있는 API 명령 (계속)

API 명령	설명
com.vmware.appliance.recovery.restore.validate	작업을 시작하지 않고 복원 작업에 대한 복원 매개 변수를 검증합니다.
com.vmware.appliance.system.uptime.get	시스템 가동 시간을 가져옵니다.
com.vmware.appliance.version1.access.consolecli.get	콘솔 기반 제어 CLI(TTY1)의 상태에 대한 정보를 가져옵니다.
com.vmware.appliance.version1.access.consolecli.set	콘솔 기반 제어 CLI(TTY1)의 사용 상태를 설정합니다.
com.vmware.appliance.version1.access.dcui.get	DCUI(Direct Console User Interface) TTY2의 상태에 대한 정보를 가져옵니다.
com.vmware.appliance.version1.access.dcui.set	DCUI(Direct Console User Interface) TTY2의 사용 상태를 설정합니다.
com.vmware.appliance.version1.access.shell.get	Bash 셸의 상태에 대한 정보를 가져옵니다. 즉, 제어된 CLI 내에서 Bash 셸에 액세스합니다.
com.vmware.appliance.version1.access.shell.set	Bash 셸의 사용 상태를 설정합니다. 즉, 제어된 CLI 내에서 Bash 셸에 액세스합니다.
com.vmware.appliance.version1.access.ssh.get	SSH 기반 제어 CLI의 사용 상태를 가져옵니다.
com.vmware.appliance.version1.access.ssh.set	SSH 기반 제어 CLI의 사용 상태를 설정합니다.
com.vmware.appliance.version1.localaccounts.user.add	새 로컬 사용자 계정을 생성합니다.
com.vmware.appliance.version1.localaccounts.user.delete	로컬 사용자 계정을 삭제합니다.
com.vmware.appliance.version1.localaccounts.user.get	로컬 사용자 계정 정보를 가져옵니다.
com.vmware.appliance.version1.localaccounts.user.list	로컬 사용자 계정을 나열합니다.
com.vmware.appliance.version1.localaccounts.user.password.update	로그인된 사용자 또는 username 매개 변수에서 지정된 사용자의 암호를 업데이트합니다.
com.vmware.appliance.version1.localaccounts.user.set	역할, 전체 이름, 사용 상태, 암호 등의 로컬 사용자 계정 속성을 업데이트합니다.
com.vmware.appliance.version1.monitoring.snmp.disable	사용하도록 설정된 SNMP 에이전트를 중지합니다.
com.vmware.appliance.version1.monitoring.snmp.enable	사용하지 않도록 설정된 SNMP 에이전트를 시작합니다.
com.vmware.appliance.version1.monitoring.snmp.get	SNMP 에이전트 구성을 반환합니다.
com.vmware.appliance.version1.monitoring.snmp.hash	안전한 SNMPv3 통신을 위한 지역화된 키를 생성합니다.

표 4-3. vCenter Server에서 사용할 수 있는 API 명령 (계속)

API 명령	설명
com.vmware.appliance.version1.monitoring.snmp.limits	SNMP 한계 정보를 가져옵니다.
com.vmware.appliance.version1.monitoring.snmp.reset	설정을 공장 기본값으로 복원합니다.
com.vmware.appliance.version1.monitoring.snmp.set	SNMP 구성을 설정합니다.
com.vmware.appliance.version1.monitoring.snmp.stats	SNMP 에이전트에 대한 진단 보고서를 생성합니다.
com.vmware.appliance.version1.networking.dns.domains.add	DNS 검색 도메인에 도메인을 추가합니다.
com.vmware.appliance.version1.networking.dns.domains.list	DNS 검색 도메인의 목록을 가져옵니다.
com.vmware.appliance.version1.networking.dns.domains.set	DNS 검색 도메인을 설정합니다.
com.vmware.appliance.version1.networking.dns.hostname.get	정규화된 도메인 이름을 가져옵니다.
com.vmware.appliance.version1.networking.dns.hostname.set	정규화된 도메인 이름을 설정합니다.
com.vmware.appliance.version1.networking.dns.servers.add	DNS 서버를 추가합니다. 이 방법은 DHCP를 사용하는 경우에 실패합니다.
com.vmware.appliance.version1.networking.dns.servers.get	DNS 서버 구성을 가져옵니다.
com.vmware.appliance.version1.networking.dns.servers.set	DNS 서버 구성을 설정합니다. 호스트가 DHCP를 사용하여 DNS 서버 및 호스트 이름을 획득하도록 구성된 경우에는 DHCP를 강제로 새로 고칩니다.
com.vmware.appliance.version1.networking.firewall.addr.inbound.add	수신 IP 주소로부터 액세스를 허용하거나 거부하기 위한 방화벽 규칙을 추가합니다.
com.vmware.appliance.version1.networking.firewall.addr.inbound.delete	해당 위치에서 특정 규칙을 삭제하거나 모든 규칙을 삭제합니다.
com.vmware.appliance.version1.networking.firewall.addr.inbound.list	방화벽 규칙에 의해 허용되거나 거부되는 수신 IP 주소의 순서 지정 목록을 가져옵니다.
com.vmware.appliance.version1.networking.interfaces.get	특정 네트워크 인터페이스에 대한 정보를 가져옵니다.
com.vmware.appliance.version1.networking.interfaces.list	아직 구성되지 않은 네트워크 인터페이스를 비롯하여 사용 가능한 네트워크 인터페이스의 목록을 가져옵니다.
com.vmware.appliance.version1.networking.ipv4.get	인터페이스에 대한 IPv4 네트워크 구성을 가져옵니다.
com.vmware.appliance.version1.networking.ipv4.list	구성된 모든 인터페이스에 대한 IPv4 네트워크 구성을 가져옵니다.

표 4-3. vCenter Server에서 사용할 수 있는 API 명령 (계속)

API 명령	설명
com.vmware.appliance.version1.networking.ipv4.renew	인터페이스에서 IPv4 네트워크 구성을 갱신합니다. 인터페이스가 DHCP를 사용하여 IP 주소를 할당하도록 구성된 경우에는 인터페이스 리스가 갱신됩니다.
com.vmware.appliance.version1.networking.ipv4.set	인터페이스에 대한 IPv4 네트워크 구성을 설정합니다.
com.vmware.appliance.version1.networking.ipv6.get	인터페이스에 대한 IPv6 네트워크 구성을 가져옵니다.
com.vmware.appliance.version1.networking.ipv6.list	구성된 모든 인터페이스에 대한 IPv6 네트워크 구성을 가져옵니다.
com.vmware.appliance.version1.networking.ipv6.set	인터페이스에 대한 IPv6 네트워크 구성을 설정합니다.
com.vmware.appliance.version1.networking.routes.add	정적 라우팅 규칙을 추가합니다. 0.0.0.0/0(IPv4의 경우) 또는 ::/0(IPv6의 경우) 유형의 대상/접두사는 기본 게이트웨이를 나타냅니다.
com.vmware.appliance.version1.networking.routes.delete	정적 라우팅 규칙을 삭제합니다.
com.vmware.appliance.version1.networking.routes.list	라우팅 테이블을 가져옵니다. 0.0.0.0/0(IPv4의 경우) 또는 ::/0(IPv6의 경우) 유형의 대상/접두사는 기본 게이트웨이를 나타냅니다.
com.vmware.appliance.version1.ntp.get	NTP 구성 설정을 가져옵니다. tymesync.get 명령을 실행하면 현재 시간 동기화 방법을 검색할 수 있습니다(NTP 또는 VMware Tools를 사용하여). 시간 동기화 방법이 NTP로 설정되지 않았더라도 ntp.get 명령은 항상 NTP 서버 정보를 반환합니다. NTP를 사용하여 시간 동기화 방법을 설정하지 않으면 NTP 상태가 아래와 같이 표시됩니다.
com.vmware.appliance.version1.ntp.server.add	NTP 서버를 추가합니다. 이 명령은 NTP 서버를 구성에 추가합니다. 시간 동기화가 NTP를 기반으로 하는 경우에는 새 NTP 서버를 다시 불러오기 위해 NTP 데몬이 다시 시작됩니다. 그 외의 경우 이 명령은 단지 서버를 NTP 구성에 추가합니다.

표 4-3. vCenter Server에서 사용할 수 있는 API 명령 (계속)

API 명령	설명
com.vmware.appliance.version1.ntp.server.delete	NTP 서버를 삭제합니다. 이 명령은 구성에서 NTP 서버를 삭제합니다. 시간 동기화 모드가 NTP를 기반으로 하는 경우에는 새 NTP 구성을 다시 불러오기 위해 NTP 데몬이 다시 시작됩니다. 그 외의 경우 이 명령은 단지 서버를 NTP 구성에서 삭제합니다.
com.vmware.appliance.version1.ntp.server.set	NTP 서버를 설정합니다. 이 명령은 이전 NTP 서버를 구성에서 삭제하고 입력 NTP 서버를 구성에 설정합니다. 시간 동기화가 NTP를 사용하여 설정된 경우에는 새 NTP 구성을 다시 불러오기 위해 NTP 데몬이 다시 시작됩니다. 그 외의 경우 이 명령은 단지 NTP 구성에 있는 NTP 서버를 입력된 서버로 바꿉니다.
com.vmware.appliance.version1.resources.cpu.stats.get	CPU 통계를 가져옵니다.
com.vmware.appliance.version1.resources.load.health.get	로드 상태를 가져옵니다.
com.vmware.appliance.version1.resources.load.stats.get	로드 평균을 가져옵니다(1분, 5분 및 15분 간격으로).
com.vmware.appliance.version1.resources.mem.health.get	메모리 상태를 가져옵니다.
com.vmware.appliance.version1.resources.mem.stats.get	메모리 통계를 가져옵니다.
com.vmware.appliance.version1.resources.net.stats.get	네트워크 상태를 가져옵니다.
com.vmware.appliance.version1.resources.net.stats.list	가동되어 실행 중인 모든 인터페이스의 네트워크 통계를 가져옵니다.
com.vmware.appliance.version1.resources.processes.stats.list	모든 프로세스의 통계를 가져옵니다.
com.vmware.appliance.version1.resources.softwarepackages.health.get	업데이트 구성 요소의 상태를 가져옵니다.
com.vmware.appliance.version1.resources.storage.health.get	스토리지 상태 통계를 가져옵니다.
com.vmware.appliance.version1.resources.storage.stats.list	각 논리 디스크의 스토리지 통계를 가져옵니다.
com.vmware.appliance.version1.resources.swap.health.get	스왑 상태를 가져옵니다.
com.vmware.appliance.version1.resources.swap.stats.get	스왑 통계를 가져옵니다.
com.vmware.appliance.version1.resources.system.health.get	시스템의 전체 상태를 가져옵니다.
com.vmware.appliance.version1.resources.system.stats.get	시스템 상태를 가져옵니다.
com.vmware.appliance.version1.services.list	알려진 모든 서비스의 목록을 가져옵니다.
com.vmware.appliance.version1.services.restart	서비스를 다시 시작합니다.

표 4-3. vCenter Server에서 사용할 수 있는 API 명령 (계속)

API 명령	설명
com.vmware.appliance.version1.services.status.get	서비스의 상태를 가져옵니다.
com.vmware.appliance.version1.services.stop	서비스를 중지합니다.
com.vmware.appliance.version1.system.storage.list	디스크에서 파티션으로의 매핑을 가져옵니다.
com.vmware.appliance.version1.system.storage.resize	모든 파티션의 크기를 디스크 크기의 100%로 조정합니다.
com.vmware.appliance.version1.system.time.get	시스템 시간을 가져옵니다.
com.vmware.appliance.version1.system.update.get	URL 기반 패치 구성을 가져옵니다.
com.vmware.appliance.version1.system.update.set	URL 기반 패치 구성을 설정합니다.
com.vmware.appliance.version1.system.version.get	장치의 버전을 가져옵니다.
com.vmware.appliance.version1.timesync.get	시간 동기화 구성을 가져옵니다.
com.vmware.appliance.version1.timesync.set	시간 동기화 구성을 설정합니다.

vCenter Server에 대한 SNMP 구성

vCenter Server에는 트랩 알림을 전송하고 GET, GETBULK 및 GETNEXT 요청을 수신할 수 있는 SNMP 에이전트가 포함되어 있습니다.

장치 셸 API 명령을 사용하여 vCenter Server SNMP 에이전트를 사용하도록 설정하고 구성할 수 있습니다. SNMP v1/v2c를 사용할지 SNMP v3을 사용할지에 따라 에이전트를 다르게 구성합니다.

SNMP v3 알림은 지원되지 않습니다. vCenter Server는 v1/v2c 트랩 및 v3 트랩 같은 알림만 모든 보안 수준에서 지원합니다.

폴링이 가능하도록 SNMP 에이전트 구성

vCenter Server SNMP 에이전트를 폴링에 대해 구성한 경우에는 GET, GETNEXT 및 GETBULK 요청과 같은 SNMP 관리 클라이언트 시스템의 요청을 수신하고 응답할 수 있습니다.

기본적으로, 포함된 SNMP 에이전트는 관리 시스템에서 보내는 폴링 요청을 UDP 포트 161에서 수신합니다. `snmp.set --port` 명령을 사용하여 대체 포트를 구성할 수 있습니다. SNMP 에이전트의 포트와 다른 서비스의 포트가 충돌하는 것을 방지하려면 `/etc/services`에 정의되어 있지 않은 UDP 포트를 사용하십시오.

절차

1 장치 셸에 액세스하고 관리자 또는 수퍼 관리자 역할을 가진 사용자로 로그인합니다.

수퍼 관리자 역할의 기본 사용자는 루트입니다.

2 `snmp.set --port` 명령을 실행하여 포트를 구성합니다.

예를 들어 다음 명령을 실행합니다.

```
snmp.set --port port
```

여기서 *port*는 SNMP 에이전트가 폴링 요청을 수신하는 데 사용할 포트입니다.

중요 지정한 포트가 다른 서비스에서 이미 사용 중이어서는 안 됩니다. 동적 범위, 포트 49152 이상의 IP 주소를 사용하십시오.

3 (선택 사항) SNMP 에이전트를 사용하도록 설정하지 않은 경우 `snmp.enable` 명령을 실행하여 사용하도록 설정합니다.

SNMP v1 및 v2c용 vCenter Server 구성

SNMP v1 및 v2c용 vCenter Server SNMP 에이전트를 구성하면 에이전트에서는 알림 보내기와 `GET` 요청 받기를 지원합니다.

SNMP v1 및 v2c에서 커뮤니티 문자열은 하나 이상의 관리되는 개체가 포함된 네임스페이스입니다. 네임스페이스가 인증을 위한 하나의 형식 역할을 할 수 있지만 통신을 보호하지는 않습니다. 통신을 보호하려면 SNMP v3을 사용합니다.

절차

1 SNMP 커뮤니티 구성

vCenter Server SNMP 에이전트에서 SNMP v1 및 v2c 메시지를 보내고 받을 수 있도록 하려면 에이전트에 대해 하나 이상의 커뮤니티를 구성해야 합니다.

2 v1 또는 v2c 알림을 보내도록 SNMP 에이전트 구성

vCenter Server SNMP 에이전트를 사용하여 가상 시스템 및 환경 알림을 관리 시스템에 보낼 수 있습니다.

SNMP 커뮤니티 구성

vCenter Server SNMP 에이전트에서 SNMP v1 및 v2c 메시지를 보내고 받을 수 있도록 하려면 에이전트에 대해 하나 이상의 커뮤니티를 구성해야 합니다.

SNMP 커뮤니티는 디바이스 및 관리 시스템의 그룹을 정의합니다. 동일한 커뮤니티의 멤버인 디바이스와 관리 시스템만 SNMP 메시지를 교환할 수 있습니다. 하나의 디바이스 또는 관리 시스템이 여러 커뮤니티의 멤버일 수 있습니다.

절차

1 장치 셸에 액세스하고 관리자 또는 수퍼 관리자 역할을 가진 사용자로 로그인합니다.

수퍼 관리자 역할의 기본 사용자는 루트입니다.

2 `snmp.set --communities` 명령을 실행하여 SNMP 커뮤니티를 구성합니다.

예를 들어 public, east 및 west 네트워크 작업 센터 커뮤니티를 구성하려면 다음 명령을 실행합니다.

```
snmp.set --communities public,eastnoc,westnoc
```

이 명령을 사용하여 커뮤니티를 지정할 때마다 해당 설정이 이전 구성을 덮어씁니다.

커뮤니티를 여러 개 지정하려면 커뮤니티 이름을 쉼표로 구분합니다.

v1 또는 v2c 알림을 보내도록 SNMP 에이전트 구성

vCenter Server SNMP 에이전트를 사용하여 가상 시스템 및 환경 알림을 관리 시스템에 보낼 수 있습니다.

SNMP 에이전트를 사용하여 SNMP v1 및 v2c 알림을 보내려면 대상(수신기), 유니캐스트 주소, 커뮤니티 및 선택적 포트를 구성해야 합니다. 포트를 지정하지 않을 경우 SNMP 에이전트는 기본적으로 대상 관리 시스템의 UDP 포트 162에 알림을 보냅니다.

절차

1 장치 셸에 액세스하고 관리자 또는 수퍼 관리자 역할을 가진 사용자로 로그인합니다.

수퍼 관리자 역할의 기본 사용자는 루트입니다.

2 `snmp.set --targets` 명령을 실행합니다.

```
snmp.set --targets target_address@port/community
```

여기서 *target_address*, *port* 및 *community*는 각각 대상 시스템의 주소, 트랩을 보낼 대상 포트 번호, 커뮤니티 이름입니다. 포트 값은 선택 사항입니다. 포트를 지정하지 않으면 기본 포트인 161이 사용됩니다.

이 명령을 사용하여 대상을 지정할 때마다 해당 설정이 이전에 지정한 설정을 덮어씁니다. 대상을 여러 개 지정하려면 각 대상을 쉼표로 구분합니다.

예를 들어 대상 192.0.2.1@678/targetcommunity 및 2001:db8::1/anothercom을 구성하기 위한 다음 명령을 실행합니다.

```
snmp.set --targets 192.0.2.1@678/targetcommunity,2001:db8::1/anothercom
```

3 (선택 사항) SNMP 에이전트를 사용하도록 설정하지 않은 경우 `snmp.enable` 명령을 실행하여 사용하도록 설정합니다.

4 (선택 사항) 에이전트가 올바르게 구성되었는지 확인하기 위해 테스트 트랩을 보내려면 `snmp.test` 명령을 실행합니다.

에이전트가 `warmStart` 트랩을 구성된 대상에 보냅니다.

SNMP v3용 vCenter Server 구성

SNMP v3용 SNMP 에이전트를 구성하면 에이전트에서 트랩 보내기를 지원합니다. 또한 SNMP v3에서는 암호화 인증 및 암호화를 포함하여 v1 또는 v2c보다 강력한 보안을 제공합니다.

SNMP v3 알림은 지원되지 않습니다. vCenter Server는 v1/v2c 트랩 및 v3 트랩 같은 알림만 모든 보안 수준에서 지원합니다.

절차

1 SNMP 엔진 ID 구성

   모든 SNMP v3 에이전트에는 에이전트의 고유 식별자 역할을 하는 엔진 ID가 있습니다. 엔진 ID는 해싱 함수와 함께 SNMP v3 메시지의 인증 및 암호화를 위한 지역화된 키를 생성하는 데 사용됩니다.

2 SNMP 인증 및 프라이버시 프로토콜 구성

   SNMP v3에서는 선택적으로 인증 및 개인 정보 프로토콜을 지원합니다.

3 SNMP 사용자 구성

   SNMP v3 정보에 액세스할 수 있는 사용자를 다섯 명까지 구성할 수 있습니다. 사용자 이름은 32자를 넘지 않아야 합니다.

4 SNMP v3 대상 구성

   SNMP 에이전트가 SNMP v3 트랩을 보낼 수 있도록 SNMP v3 대상을 구성합니다.

SNMP 엔진 ID 구성

모든 SNMP v3 에이전트에는 에이전트의 고유 식별자 역할을 하는 엔진 ID가 있습니다. 엔진 ID는 해싱 함수와 함께 SNMP v3 메시지의 인증 및 암호화를 위한 지역화된 키를 생성하는 데 사용됩니다.

SNMP 에이전트를 사용하도록 설정하기 전에 엔진 ID를 지정하지 않으면 독립형 SNMP 에이전트를 사용하도록 설정할 때 엔진 ID가 생성됩니다.

절차

1 장치 셸에 액세스하고 관리자 또는 수퍼 관리자 역할을 가진 사용자로 로그인합니다.

   수퍼 관리자 역할의 기본 사용자는 루트입니다.

2 `snmp.set --engineid` 명령을 실행하여 대상을 구성합니다.

   예를 들어 다음 명령을 실행합니다.

```
snmp.set --engineid 80001adc802417e202b8613f5400000000
```

   여기서 80001adc802417e202b8613f5400000000은 ID로서, 5~32자 길이의 16진수 문자열이어야 합니다.

SNMP 인증 및 프라이버시 프로토콜 구성

SNMP v3에서는 선택적으로 인증 및 개인 정보 프로토콜을 지원합니다.

인증은 사용자의 ID를 확인하는 데 사용됩니다. 개인 정보 보호는 SNMP v3 메시지를 암호화할 수 있도록 하여 데이터의 기밀성을 보장합니다. 개인 정보 프로토콜은 보안에 커뮤니티 문자열을 사용하는 SNMP v1 및 v2c에서 사용할 수 있는 보안보다 높은 수준의 보안을 제공합니다.

인증 및 개인 정보 보호는 모두 선택 사항입니다. 그러나 개인 정보 보호를 사용할 계획이면 인증도 사용해야 합니다.

SNMP v3 인증 및 개인 정보 프로토콜은 라이센스가 부여된 vSphere 기능으로, 일부 vSphere 버전에서는 사용할 수 없습니다.

절차

1 장치 셸에 액세스하고 관리자 또는 수퍼 관리자 역할을 가진 사용자로 로그인합니다.

수퍼 관리자 역할의 기본 사용자는 루트입니다.

2 (선택 사항) `snmp.set --authentication` 명령을 실행하여 인증을 구성합니다.

예를 들어 다음 명령을 실행합니다.

```
snmp.set --authentication protocol
```

여기서 *protocol*은 **none**(인증을 사용하지 않을 경우), **SHA1** 또는 **MD5**여야 합니다.

3 (선택 사항) `snmp.set --privacy` 명령을 실행하여 개인 정보 프로토콜을 구성합니다.

예를 들어 다음 명령을 실행합니다.

```
snmp.set --privacy protocol
```

여기서 *protocol*은 **none**(개인 정보를 사용하지 않을 경우) 또는 **AES128**이어야 합니다.

SNMP 사용자 구성

SNMP v3 정보에 액세스할 수 있는 사용자를 다섯 명까지 구성할 수 있습니다. 사용자 이름은 32자를 넘지 않아야 합니다.

사용자를 구성하는 중에 사용자의 인증 및 개인 정보 암호와 SNMP 에이전트의 엔진 ID를 기반으로 인증 및 개인 정보 해시 값을 생성합니다. 사용자를 구성한 후 엔진 ID, 인증 프로토콜 또는 개인 정보 프로토콜을 변경하면 해당 사용자는 더 이상 유효하지 않게 되므로 재구성해야 합니다.

사전 요구 사항

- 사용자를 구성하기 전에 인증 및 개인 정보 프로토콜을 구성했는지 확인합니다.
- 구성할 계획인 각 사용자에 대해 인증 및 개인 정보 암호를 알고 있는지 확인합니다. 암호는 8자 이상이어야 합니다. 이 암호를 호스트 시스템의 파일에 저장하십시오.

절차

1 장치 셸에 액세스하고 관리자 또는 수퍼 관리자 역할을 가진 사용자로 로그인합니다.

수퍼 관리자 역할의 기본 사용자는 루트입니다.

2 인증 또는 개인 정보를 사용하는 경우 `snmp.hash --auth_hash --priv_hash` 명령을 실행하여 사용자의 인증 및 개인 정보 해시 값을 가져옵니다.

예를 들어 다음 명령을 실행합니다.

```
snmp.hash  --auth_hash secret1 --priv_hash secret2
```

여기서 *secret1*은 사용자의 인증 암호가 들어 있는 파일에 대한 경로이고, *secret2*는 사용자의 개인 정보 암호가 들어 있는 파일에 대한 경로입니다. 또는 `--raw_secret` 플래그를 지정하고 부울 매개 변수를 *true*로 설정할 수 있습니다.

인증 및 개인 정보 해시 값이 표시됩니다.

3 `snmp.set --user`를 실행하여 사용자를 구성합니다.

예를 들어 다음 명령을 실행합니다.

```
snmp.set --user userid/authhash/privhash/security
```

명령의 매개 변수는 다음과 같습니다.

매개 변수	설명
userid	사용자 이름으로 바꿉니다.
authhash	인증 해시 값으로 바꿉니다.
privhash	개인 정보 해시 값으로 바꿉니다.
security	해당 사용자에 대해 설정된 보안 수준, 즉 **auth**(인증만 사용할 경우), **priv**(인증과 개인 정보 보호를 사용할 경우) 또는 **none**(인증 또는 개인 정보 보호를 사용하지 않을 경우)으로 바꿉니다.

SNMP v3 대상 구성

SNMP 에이전트가 SNMP v3 트랩을 보낼 수 있도록 SNMP v3 대상을 구성합니다.

최대 세 개의 SNMP v3 대상과 함께 최대 세 개의 SNMP v1 또는 v2c 대상을 구성할 수 있습니다.

대상을 구성하려면 트랩을 받는 시스템의 호스트 이름 또는 IP 주소, 사용자 이름, 보안 수준, 그리고 트랩을 보낼지 여부를 지정해야 합니다. 보안 수준은 **none**(보안을 사용하지 않을 경우), **auth**(인증만 사용할 경우) 또는 **priv**(인증과 개인 정보를 사용할 경우)일 수 있습니다.

절차

1 장치 셸에 액세스하고 관리자 또는 수퍼 관리자 역할을 가진 사용자로 로그인합니다.

수퍼 관리자 역할의 기본 사용자는 루트입니다.

2 `snmp.set --v3targets` 명령을 실행하여 SNMP v3 대상을 설정합니다.

예를 들어 다음 명령을 실행합니다.

```
snmp.set --v3targets hostname@port/userid/secLevel/trap
```

명령의 매개 변수는 다음과 같습니다.

매개 변수	설명
hostname	트랩을 받는 관리 시스템의 호스트 이름 또는 IP 주소로 바꿉니다.
port	관리 시스템에서 트랩을 받는 포트로 바꿉니다. 포트를 지정하지 않으면 기본 포트인 161이 사용됩니다.
userid	사용자 이름으로 바꿉니다.
secLevel	**none**, **auth** 또는 **priv** 중 하나로 바꿔 구성한 인증 및 개인 정보 보호 수준을 나타냅니다. 인증만 구성한 경우 **auth**, 인증과 개인 정보 보호를 모두 구성한 경우 **priv**, 아무 것도 구성하지 않은 경우 **none**을 사용합니다.

3 (선택 사항) SNMP 에이전트를 사용하도록 설정하지 않은 경우 `snmp.enable` 명령을 실행하여 사용하도록 설정합니다.

4 (선택 사항) 에이전트가 올바르게 구성되었는지 확인하기 위해 테스트 트랩을 보내려면 `snmp.test` 명령을 실행합니다.

에이전트가 `warmStart` 트랩을 구성된 대상에 보냅니다.

알림을 필터링하도록 SNMP 에이전트 구성

SNMP 관리 소프트웨어가 특정 알림을 받지 않도록 하려는 경우에는 해당 알림을 필터링하도록 vCenter Server SNMP 에이전트를 구성할 수 있습니다.

절차

1 장치 셸에 액세스하고 관리자 또는 수퍼 관리자 역할을 가진 사용자로 로그인합니다.

수퍼 관리자 역할의 기본 사용자는 루트입니다.

2 `snmp.set --notraps` 명령을 실행하여 트랩을 필터링합니다.

- 특정 트랩을 필터링하려면 다음 명령을 실행합니다.

```
snmp.set  --notraps oid_list
```

여기서 *oid_list*는 필터링한 트랩에 대한 개체 ID의 쉼표로 구분된 목록입니다. 이 목록은 이전에 이 명령을 사용하여 지정한 모든 개체 ID를 대체합니다.

- 모든 트랩 필터를 지우려면 다음 명령을 실행합니다.

```
snmp.set  --notraps reset
```

3 (선택 사항) SNMP 에이전트를 사용하도록 설정하지 않은 경우 `snmp.enable` 명령을 실행하여 사용하도록 설정합니다.

결과

지정한 개체 ID로 식별된 트랩은 SNMP 에이전트의 출력에서 필터링되며 SNMP 관리 소프트웨어로 전송되지 않습니다.

SNMP 관리 클라이언트 소프트웨어 구성

트랩을 보내도록 vCenter Server를 구성한 후에는 이러한 트랩을 수신하고 해석하도록 관리 클라이언트 소프트웨어를 구성해야 합니다.

관리 클라이언트 소프트웨어를 구성하려면 관리되는 디바이스의 커뮤니티를 지정하고, 포트 설정을 구성하고, VMware MIB 파일을 로드합니다. 이러한 단계에 대한 자세한 지침은 사용 중인 관리 시스템의 설명서를 참조하십시오.

사전 요구 사항

https://kb.vmware.com/s/article/1013445에서 VMware MIB 파일을 다운로드합니다.

절차

1 관리 소프트웨어에서 vCenter Server 인스턴스를 SNMP 기반의 관리되는 디바이스로 지정합니다.

2 SNMP v1 또는 v2c를 사용 중인 경우 관리 소프트웨어에서 적절한 커뮤니티 이름을 설정합니다.

   이러한 이름은 vCenter Server에 있는 SNMP 에이전트에 대해 설정한 커뮤니티에 대응되는 이름이어야 합니다.

3 SNMP v3을 사용 중인 경우 사용자와 인증 및 개인 정보 프로토콜을 vCenter Server에 구성된 프로토콜과 일치하도록 구성합니다.

4 SNMP 에이전트를 구성할 때 관리 시스템의 기본 UDP 포트 162가 아닌 다른 포트로 트랩을 보내도록 설정한 경우에는 구성한 해당 포트에서 수신하도록 관리 클라이언트 소프트웨어를 구성해야 합니다.

5 VMware MIB를 관리 소프트웨어에 로드하여 vCenter Server 변수의 심볼 이름을 봅니다.

   조회 오류를 방지하려면 다른 MIB 파일을 로드하기 전에 이러한 MIB 파일을 다음 순서대로 로드합니다.

   a `VMWARE-ROOT-MIB.mib`

   b `VMWARE-TC-MIB.mib`

   c `VMWARE-PRODUCTS-MIB.mib`

결과

이제 vCenter Server에서 보내는 트랩을 관리 소프트웨어가 수신하고 해석할 수 있습니다.

SNMP 설정을 공장 기본값으로 재설정

SNMP 설정을 공장 기본값으로 재설정할 수 있습니다. 또한 특정 인수의 값을 공장 기본값으로 재설정할 수도 있습니다.

커뮤니티 또는 대상과 같은 특정 인수를 재설정할 수 있습니다. 또한 SNMP 구성을 공장 기본값으로 재설정할 수도 있습니다.

절차

1 장치 셸에 액세스하고 관리자 또는 수퍼 관리자 역할을 가진 사용자로 로그인합니다.

수퍼 관리자 역할의 기본 사용자는 루트입니다.

2 특정 인수를 재설정하려면 `snmp.set --arguments reset` 명령을 실행합니다.

예를 들어 구성한 커뮤니티를 재설정하려면 다음 명령을 실행합니다.

```
snmp.set --communities reset
```

3 전체 SNMP 구성을 공장 기본값으로 재설정하려면 `snmp.reset` 명령을 실행합니다.

vCenter Server에서 시간 동기화 설정 구성

배포 후에 vCenter Server에서 시간 동기화 설정을 변경할 수 있습니다.

vCenter Server를 배포할 때 NTP 서버를 사용하거나 VMware Tools를 사용하는 것 중에 하나로 시간 동기화 방법을 선택할 수 있습니다. vSphere 네트워크의 시간 설정이 변경될 경우 장치 셸에 있는 명령을 사용하여 vCenter Server를 편집하고 시간 동기화 설정을 구성할 수 있습니다.

정기 시간 동기화 기능을 사용하도록 설정한 경우 VMware Tools는 게스트 운영 체제의 시간을 호스트의 시간과 동일하게 설정합니다.

시간을 동기화한 후 VMware Tools는 게스트 운영 체제와 호스트의 클럭이 일치하는지 1분 단위로 확인합니다. 시간이 일치하지 않으면 호스트의 클럭을 기준으로 게스트 운영 체제의 클럭을 동기화합니다.

일반적으로 NTP(Network Time Protocol)와 같은 기본적으로 제공되는 시간 동기화 소프트웨어가 VMware Tools의 정기 시간 동기화보다 정확하기 때문에 되도록이면 이러한 시간 동기화 소프트웨어를 사용하는 것이 좋습니다. vCenter Server에서 한 가지 형태의 정기 시간 동기화만 사용할 수 있습니다. 기본적으로 제공되는 시간 동기화 소프트웨어와 vCenter Server VMware Tools 정기 시간 동기화 중에서 하나를 사용하기로 결정하면 다른 하나는 해제됩니다.

VMware Tools 시간 동기화 사용

VMware Tools 시간 동기화를 사용하도록 vCenter Server를 설정할 수 있습니다.

절차

1 장치 셸에 액세스하고 관리자 또는 수퍼 관리자 역할을 가진 사용자로 로그인합니다.

수퍼 관리자 역할의 기본 사용자는 루트입니다.

2 명령을 실행하여 VMware Tools 시간 동기화를 사용하도록 설정합니다.

```
timesync.set --mode host
```

3 (선택 사항) 해당 명령을 실행하여 VMware Tools 시간 동기화를 적용했는지 확인합니다.

```
timesync.get
```

이 명령은 시간 동기화가 호스트 모드에 있다고 반환합니다.

결과

장치 시간이 ESXi 호스트 시간과 동기화됩니다.

vCenter Server 구성에서 NTP 서버 추가 또는 바꾸기

NTP 기반 시간 동기화를 사용하도록 vCenter Server를 설정하려면 NTP 서버를 vCenter Server 구성에 추가해야 합니다.

절차

1 장치 셸에 액세스하고 관리자 또는 수퍼 관리자 역할을 가진 사용자로 로그인합니다.

수퍼 관리자 역할의 기본 사용자는 루트입니다.

2 다음 `ntp.set` 명령을 사용하여 NTP 서버를 vCenter Server 구성에 추가합니다.

```
ntp.set --servers IP-addresses-or-host-names
```

명령에서 *IP-addresses-or-host-names*는 NTP 서버의 IP 주소 또는 호스트 이름을 쉼표로 구분한 목록입니다.

이 명령은 현재 NTP 서버(있는 경우)를 제거하고 새 NTP 서버를 구성에 추가합니다. 시간 동기화가 NTP 서버를 기반으로 하는 경우에는 새 NTP 서버를 다시 불러오기 위해 NTP 데몬이 다시 시작됩니다. 그렇지 않으면 이 명령은 NTP 구성의 현재 NTP 서버를 지정한 새 NTP 서버로 바꿉니다.

3 (선택 사항) 새로운 NTP 구성 설정이 적용되었는지 확인하려면 다음 명령을 실행합니다.

```
ntp.get
```

이 명령은 NTP 동기화에 대해 구성된 서버의 공백으로 구분된 목록을 반환합니다. NTP 동기화가 사용되는 경우 이 명령은 NTP 구성이 작동 상태에 있다고 반환합니다. NTP 동기화가 사용되지 않는 경우 이 명령은 NTP 구성이 중단 상태에 있다고 반환합니다.

4 (선택 사항) NTP 서버에 연결할 수 있는지 확인하려면 다음 명령을 실행합니다.

```
ntp.test --servers IP-addresses-or-host-names
```

이 명령은 NTP 서버의 상태를 반환합니다.

다음에 수행할 작업

NTP 동기화가 사용되지 않는 경우 vCenter Server에서 NTP 서버를 기반으로 하도록 시간 동기화 설정을 구성할 수 있습니다. NTP 서버와 vCenter Server의 시간 동기화의 내용을 참조하십시오.

NTP 서버와 vCenter Server의 시간 동기화

vCenter Server에서 NTP 서버를 기반으로 하도록 시간 동기화 설정을 구성할 수 있습니다.

사전 요구 사항

vCenter Server 구성에서 하나 이상의 NTP(네트워크 시간 프로토콜) 서버를 설정합니다. vCenter Server 구성에서 NTP 서버 추가 또는 바꾸기의 내용을 참조하십시오.

절차

1 장치 셸에 액세스하고 관리자 또는 수퍼 관리자 역할을 가진 사용자로 로그인합니다.

수퍼 관리자 역할의 기본 사용자는 루트입니다.

2 명령을 실행하여 NTP 기반 시간 동기화를 사용하도록 설정합니다.

```
timesync.set --mode NTP
```

3 (선택 사항) 해당 명령을 실행하여 NTP 동기화를 적용했는지 확인합니다.

```
timesync.get
```

이 명령은 시간 동기화가 NTP 모드에 있다고 반환합니다.

vCenter Server에서 로컬 사용자 계정 관리

수퍼 관리자로 장치 셸에 로그인하는 경우 장치 셸에서 명령을 실행하여 vCenter Server에서 로컬 사용자 계정을 관리할 수 있습니다. 수퍼 관리자 역할이 있는 기본 사용자는 루트입니다.

vCenter Server의 사용자 역할

vCenter Server에는 3가지 기본 사용자 역할이 있습니다.

vCenter Server의 로컬 사용자는 다양한 작업을 수행할 권한이 있습니다. vCenter Server에서 다음과 같은 3가지 사용자 역할을 사용할 수 있습니다.

연산자

연산자 사용자 역할이 있는 로컬 사용자는 vCenter Server 구성을 읽을 수 있습니다.

관리자

관리자 사용자 역할이 있는 로컬 사용자는 vCenter Server를 구성할 수 있습니다.

수퍼 관리자

수퍼 관리자 사용자 역할이 있는 로컬 사용자는 vCenter Server를 구성하고 로컬 계정을 관리하고 Bash 셸을 사용할 수 있습니다.

vCenter Server의 로컬 사용자 계정 목록 얻기

로컬 사용자 계정 목록을 확인하여 장치 셸에서 관리할 사용자 계정을 결정할 수 있습니다.

절차

1 장치 셸에 액세스하고 수퍼 관리자 역할을 가진 사용자로 로그인합니다.

수퍼 관리자 역할이 있는 기본 사용자는 루트입니다.

2 `localaccounts.user.list` 명령을 실행합니다.

로컬 사용자의 목록을 확인할 수 있습니다. 사용자에 대한 정보에는 사용자 이름, 상태, 역할, 암호 상태, 전체 이름 및 이메일이 포함됩니다.

참고 로컬 사용자 목록에는 장치 셸로 기본 셸이 있는 로컬 사용자만 들어 있습니다.

vCenter Server에서 로컬 사용자 계정 생성

새 로컬 사용자 계정을 생성할 수 있습니다.

사용자 역할에 대한 자세한 내용은 vCenter Server의 사용자 역할 항목을 참조하십시오.

절차

1 장치 셸에 액세스하고 수퍼 관리자 역할을 가진 사용자로 로그인합니다.

수퍼 관리자 역할이 있는 기본 사용자는 루트입니다.

2 `localaccounts.user.add --role --username --password` 명령을 실행합니다.

예를 들어 연산자 사용자 역할이 있는 로컬 사용자 계정 테스트를 추가하려면 다음 명령을 실행합니다.

```
localaccounts.user.add --role operator --username test --password
```

역할은 **operator**, **admin** 또는 **superAdmin**일 수 있습니다.
또한 새 로컬 사용자 계정을 설정하고 이메일 및 사용자의 전체 이름을 지정할 수도 있습니다. 예를 들어 연산자 사용자 역할이 있는 로컬 사용자 계정 test1, 전체 이름 TestName 및 이메일 주소 test1@mymail.com을 추가하려면 다음 명령을 실행합니다.

```
localaccounts.user.add --role operator --username test1 --password --fullname TestName --
email test1@mymail.com
```

전체 이름에 공백을 사용할 수 없습니다.

3 메시지가 표시되면 새 로컬 사용자의 암호를 입력 및 확인합니다.

결과

장치의 새 로컬 사용자를 생성했습니다.

vCenter Server의 로컬 사용자 암호 업데이트

보안상의 이유로 vCenter Server의 로컬 사용자 암호를 업데이트할 수 있습니다.

절차

1 장치 셸에 액세스하고 수퍼 관리자 역할을 가진 사용자로 로그인합니다.

수퍼 관리자 역할이 있는 기본 사용자는 루트입니다.

2 `localaccounts.user.password.update --username user name --password` 명령을 실행합니다.

예를 들어 사용자 이름 테스트로 사용자 암호를 변경하려면 다음 명령을 실행합니다.

```
localaccounts.user.password.update --username test --password
```

3 메시지가 표시되면 새 암호를 입력 및 확인합니다.

vCenter Server의 로컬 사용자 계정 업데이트

vCenter Server의 기존 로컬 사용자 계정을 업데이트할 수 있습니다.

사용자 역할에 대한 자세한 내용은 vCenter Server의 사용자 역할 항목을 참조하십시오.

절차

1 장치 셸에 액세스하고 수퍼 관리자 역할을 가진 사용자로 로그인합니다.

수퍼 관리자 역할이 있는 기본 사용자는 루트입니다.

2 `localaccounts.user.set --username` 명령을 실행하여 기존 로컬 사용자를 업데이트합니다.

- 로컬 사용자의 역할을 업데이트하려면 다음 명령을 실행합니다.

  ```
  localaccounts.user.set --username user name --role new role
  ```

  여기서 *user name*은 편집할 사용자의 이름이고 *new role*은 새 역할입니다. 역할은 **operator**, **admin** 또는 **superAdmin**일 수 있습니다.

- 로컬 사용자의 이메일을 업데이트하려면 다음 명령을 실행합니다.

  ```
  localaccounts.user.set --username user name --email new email address
  ```

  여기서 *user name*은 편집할 사용자의 이름이고 *new email address*는 새 이메일 주소입니다.

- 로컬 사용자의 전체 이름을 업데이트하려면 다음 명령을 실행합니다.

  ```
  localaccounts.user.set --username user name --fullname new full name
  ```

  여기서 *user name*은 편집할 사용자의 이름이고 *new full name*은 사용자의 새 전체 이름입니다.

- 로컬 사용자의 상태를 업데이트하려면 다음 명령을 실행합니다.

  ```
  localaccounts.user.set --username user name --status new status
  ```

  여기서 *user name*은 편집할 사용자의 이름이고 *status*는 로컬 사용자의 새 상태입니다. 상태는 **disabled** 또는 **enabled**일 수 있습니다.

vCenter Server에서 로컬 사용자 계정 삭제

vCenter Server에서 로컬 사용자 계정을 삭제할 수 있습니다.

절차

1 장치 셸에 액세스하고 수퍼 관리자 역할을 가진 사용자로 로그인합니다.

수퍼 관리자 역할이 있는 기본 사용자는 루트입니다.

2 `localaccounts.user.delete --username` 명령을 실행합니다.

예를 들어 사용자 이름 테스트를 사용하여 사용자를 삭제하려면 다음 명령을 실행합니다.

```
localaccounts.user.delete --username test
```

사용자가 삭제됩니다.

vCenter Server의 상태 및 통계 모니터링

장치 셸에서 API 명령을 사용하여 vCenter Server의 하드웨어 상태를 모니터링할 수 있습니다. 업데이트 구성 요소의 상태를 모니터링하여 사용 가능한 패치에 대한 정보를 확인할 수 있습니다.

메모리, CPU, 스토리지 및 네트워크 등 하드웨어 구성 요소의 상태뿐만 아니라 사용 가능한 패치에 대한 마지막 확인에 따라 소프트웨어 패키지가 최신 상태인지 표시하는 업데이트 구성 요소의 상태를 볼 수 있습니다.

특정 상태는 녹색, 노란색, 주황색, 빨간색 또는 회색일 수 있습니다. 자세한 내용은 vCenter Server 상태 보기의 내용을 참조하십시오.

vCenter Server 시스템의 상태 및 통계를 모니터링하기 위해 사용할 수 있는 전체 API 명령 목록은 장치 셸의 API 명령을(를) 참조하십시오.

절차

1 장치 셸에 액세스하고 로그인합니다.

로그인하기 위해 사용하는 사용자 이름은 운영자, 관리자 또는 수퍼 관리자 사용자 역할이 있는 사용자면 됩니다.

2 특정 구성 요소의 상태를 봅니다.

- vCenter Server의 메모리 상태를 보려면 `mem.health.get` 명령을 실행합니다.
- vCenter Server의 스토리지 상태를 보려면 `storage.health.get` 명령을 실행합니다.

- vCenter Server의 스왑 상태를 보려면 `swap.health.get` 명령을 실행합니다.
- vCenter Server의 업데이트 구성 요소 상태를 보려면 `softwarepackages.health.get` 명령을 실행합니다.

  중요 사용 가능한 패치에 대한 정기적인 확인을 수행하지 않으면 업데이트 구성 요소의 상태가 최신 상태가 아니게 될 수 있습니다. vCenter Server 패치를 확인하고 vCenter Server 패치에 대한 자동 확인을 사용하도록 설정하는 방법은 "vSphere 업그레이드" 의 내용을 참조하십시오.

- vCenter Server 시스템의 전체 상태를 보려면 `health.system.get` 명령을 실행합니다.

3 특정 하드웨어 구성 요소에 대한 통계를 보려면 개별 명령을 실행합니다.

예를 들어 각 논리 디스크의 스토리지 통계를 보려면 `storage.stats.list` 명령을 실행합니다.

vimtop 플러그인을 사용하여 서비스의 리소스 사용 모니터링

`vimtop` 유틸리티 플러그인을 사용하여 vCenter Server에서 실행되는 vSphere 서비스를 모니터링할 수 있습니다.

`vimtop`은 vCenter Server 환경에서 실행되는 `esxtop`과 비슷한 도구입니다. 장치 셸에서 `vimtop`의 텍스트 기반 인터페이스를 사용하여 vCenter Server에 대한 전체 정보와 vSphere 서비스 목록 및 해당 리소스 사용을 볼 수 있습니다.

- 대화형 모드에서 vimtop을 사용하여 서비스 모니터링

  `vimtop` 플러그인을 사용하여 서비스를 실시간으로 모니터링할 수 있습니다.

- 대화형 모드 명령줄 옵션

  플러그인 대화형 모드로 전환하기 위해 `vimtop` 명령을 실행할 때 다양한 명령줄 옵션을 사용할 수 있습니다.

- vimtop의 대화형 모드 단일 키 명령

  대화형 모드에서 실행하는 경우 `vimtop`에서 몇 개의 단일 키 명령을 인식합니다.

대화형 모드에서 vimtop을 사용하여 서비스 모니터링

`vimtop` 플러그인을 사용하여 서비스를 실시간으로 모니터링할 수 있습니다.

`vimtop` 대화형 모드의 기본 보기는 개요 테이블 및 기본 테이블로 구성됩니다. 대화형 모드에서 단일 키 명령을 사용하여 보기를 프로세스에서 디스크 또는 네트워크로 전환할 수 있습니다.

절차

1 SSH 클라이언트 애플리케이션에서 vCenter Server 셸에 로그인합니다.

2 `vimtop` 명령을 사용하여 대화형 모드에서 플러그인에 액세스합니다.

대화형 모드 명령줄 옵션

플러그인 대화형 모드로 전환하기 위해 vimtop 명령을 실행할 때 다양한 명령줄 옵션을 사용할 수 있습니다.

표 4-4. 대화형 모드 명령줄 옵션

옵션	설명
-h	vimtop 명령줄 옵션의 도움말을 출력합니다.
-v	vimtop 버전 번호를 출력합니다.
-c *파일 이름*	사용자 정의 vimtop 구성 파일을 로드합니다. -c 옵션을 사용하지 않을 경우 기본 구성 파일은 /root/vimtop/vimtop.xml입니다. 사용자 고유의 구성 파일을 생성하고 W 단일 키 대화형 명령을 사용하여 다른 파일 이름 및 경로를 지정할 수 있습니다.
-n *숫자*	vimtop이 대화형 모드를 종료하기 전에 수행한 반복 횟수를 설정합니다. vimtop은 표시 *숫자* 횟수를 업데이트하고 종료됩니다. 기본값은 10000입니다.
-p / -d초	업데이트 기간(초)을 설정합니다.

vimtop의 대화형 모드 단일 키 명령

대화형 모드에서 실행하는 경우 vimtop에서 몇 개의 단일 키 명령을 인식합니다.

모든 대화형 모드 패널은 다음 표에 나열된 명령을 인식합니다.

표 4-5. 대화형 모드 단일 키 명령

키 이름	설명
시간	명령에 대한 간단한 요약과 보안 모드 상태를 제공하는 현재 패널에 대한 도움말 메뉴를 표시합니다.
i	vimtop 플러그인의 개요 패널의 윗줄 보기를 표시하거나 숨깁니다.
터	vCenter Server 인스턴스에서 실행되고 있는 작업에 대한 정보를 개요 패널에서 표시하는 작업 섹션을 표시하거나 숨깁니다.
m	개요 패널의 메모리 섹션을 표시하거나 숨깁니다.
f	모든 사용 가능한 CPU에 대한 정보를 개요 패널에서 표시하는 CPU 섹션을 표시하거나 숨깁니다.
g	상위 4개 물리적 CPU에 대한 정보를 개요 패널에서 표시하는 CPU 섹션을 표시하거나 숨깁니다.
스페이스바	현재 창을 즉시 새로 고칩니다.
p	현재 패널에 표시된 서비스 리소스 사용에 대한 정보를 일시 중지합니다.
r	현재 패널에 표시된 서비스 리소스 사용에 대한 정보를 새로 고칩니다.
초	새로 고침 기간을 설정합니다.
q	vimtop 플러그인의 대화형 모드를 종료합니다.
k	기본 패널의 디스크 보기를 표시합니다.

표 4-5. 대화형 모드 단일 키 명령 (계속)

키 이름	설명
니요	기본 패널을 네트워크 보기로 전환합니다.
Esc	선택 항목을 지우거나 기본 패널의 프로세스 보기로 돌아갑니다.
Enter	추가 세부 정보를 볼 서비스를 선택합니다.
n	기본 패널에서 헤더의 이름을 표시하거나 숨깁니다.
u	기본 패널에서 헤더의 측정 단위를 표시하거나 숨깁니다.
왼쪽, 오른쪽 화살표	열을 선택합니다.
위, 아래 화살표	행을 선택합니다.
<,>	선택한 열을 이동합니다.
삭제	선택한 열을 제거합니다.
c	기본 패널의 현재 보기에 열을 추가합니다. 스페이스바를 사용하여 표시된 목록에서 열을 추가하거나 제거합니다.
a	선택한 열을 오름차순으로 정렬합니다.
d	선택한 열을 내림차순으로 정렬합니다.
z	모든 열의 정렬 순서를 지웁니다.
l	선택한 열의 너비를 설정합니다.
x	열 너비를 기본값으로 되돌립니다.
+	선택한 항목을 확장합니다.
-	선택한 항목을 축소합니다.
w	현재 설정을 vimtop 구성 파일에 씁니다. 기본 파일 이름은 -c 옵션을 통해 지정된 이름이거나 -c 옵션을 사용하지 않을 경우 /root/vimtop/vimtop.xml입니다. 또한 w 명령을 통해 생성된 프롬프트에서 다른 파일 이름을 지정할 수도 있습니다.

DCUI(Direct Console User Interface)를 사용하여 vCenter Server 구성

5

vCenter Server를 배포한 후 네트워크 설정을 재구성하고 문제 해결을 위해 Bash 셸에 액세스할 수 있도록 설정할 수 있습니다. DCUI(Direct Console User Interface)에 액세스하려면 루트로 로그인해야 합니다.

DCUI(Direct Console User Interface)의 홈 페이지에는 vCenter Server 지원 번들에 대한 링크가 포함되어 있습니다. 지원 번들에 대한 링크의 유형은 https://*appliance-host-name*:443/appliance/support-bundle입니다.

본 장은 다음 항목을 포함합니다.

- DCUI(Direct Console User Interface)에 로그인
- 루트 사용자의 암호 변경
- vCenter Server의 관리 네트워크 구성
- vCenter Server의 관리 네트워크 다시 시작
- Bash 셸에 액세스할 수 있도록 설정
- 문제 해결을 위해 Bash 셸에 액세스
- 문제 해결을 위해 vCenter Server 지원 번들 내보내기

DCUI(Direct Console User Interface)에 로그인

DCUI(Direct Console User Interface)를 사용하면 텍스트 기반 메뉴를 사용하여 로컬에서 vCenter Server와 상호 작용할 수 있습니다.

절차

1. vSphere Client에서 호스트로 이동하고 **구성 > 서비스**를 클릭합니다. SSH 및 DCUI(Direct Console User Interface) 서비스가 실행 중인지 확인합니다.
2. SSH 클라이언트를 열고 vCenter Server에 연결합니다.
3. 루트 계정으로 로그인합니다.
4. **`DCUI`**를 입력하여 DCUI(Direct Console User Interface)를 시작합니다.
5. 콘솔 창 내부를 클릭한 다음 F2를 눌러 시스템을 사용자 지정합니다.

6 루트 사용자의 암호를 입력하고 Enter 키를 누릅니다.

중요 잘못된 자격 증명을 세 번 입력하면 루트 계정은 5분간 잠깁니다.

결과

DCUI(Direct Console User Interface)에 로그인하였습니다. 루트 사용자의 암호를 변경하고, 네트워크 설정을 편집하고, vCenter Server Appliance Bash 셸에 액세스할 수 있도록 설정할 수 있습니다.

루트 사용자의 암호 변경

vCenter Server DCUI(Direct Console User Interface)에 대한 무단 액세스를 방지하기 위해 루트 사용자의 암호를 변경할 수 있습니다.

vCenter Server 인스턴스의 기본 루트 암호는 배포 중에 입력한 암호입니다.

중요 vCenter Server 루트 계정의 암호는 90일 후 만료됩니다. vCenter Server Bash 셸에 루트로 로그인하고 `chage -M number_of_days -W warning_until_expiration user_name`을 실행하여 계정의 만료 시간을 변경할 수 있습니다. 루트 암호의 만료 시간을 무한대로 늘리려면 `chage -M -1 -E -1 root` 명령을 실행합니다.

절차

1 DCUI(Direct Console User Interface)에 로그인합니다.

2 **암호 구성**을 선택하고 Enter를 누릅니다.

3 루트 사용자의 이전 암호를 입력하고 Enter 키를 누릅니다.

4 새 암호를 설정하고 Enter 키를 누릅니다.

5 Direct Console User Interface의 기본 메뉴로 돌아갈 때까지 Esc 키를 누릅니다.

결과

장치의 루트 사용자 암호를 변경했습니다.

vCenter Server의 관리 네트워크 구성

vCenter Server 인스턴스는 DHCP 서버에서 네트워킹 설정을 가져오거나 정적 IP 주소를 사용할 수 있습니다. DCUI(Direct Console User Interface)에서 vCenter Server의 네트워킹 설정을 변경할 수 있습니다. IPv4, IPv6 및 DNS 구성을 변경할 수 있습니다.

사전 요구 사항

vCenter Server 인스턴스의 IP 주소를 변경하려면 시스템 이름이 FQDN인지 확인합니다. 배포 중에 IP 주소를 시스템 이름으로 설정하면 배포한 후에 IP 주소를 변경할 수 없습니다. 시스템 이름은 항상 기본 네트워크 식별자로 사용됩니다.

절차

1 vCenter Server의 DCUI(Direct Console User Interface)에 로그인

2 **관리 네트워크 구성**을 선택하고 Enter 키를 누릅니다.

3 **IP 구성**에서 IPv4 설정을 변경합니다.

옵션	설명
동적 IP 주소 및 네트워크 구성 사용	네트워크에 사용 가능한 DHCP 서버가 있는 경우 DHCP 서버에서 네트워킹 설정을 가져옵니다.
정적 IP 주소 및 네트워크 구성 설정	정적 네트워킹 구성을 설정합니다.

4 **IPv6 구성**에서 IPv6 설정을 변경합니다.

옵션	설명
IPv6 사용	IPv6을 사용하거나 사용하지 않도록 설정
DHCP 상태 저장 구성 사용	DHCP 서버를 사용하여 IPv6 주소 및 네트워킹 설정을 가져옵니다.
ICMP 상태 비저장 구성 사용	상태 비저장 주소 자동 구성(SLAAC)을 사용하여 IPv6 주소 및 네트워킹 설정을 가져옵니다.

5 **DNS 구성**에서 DNS 설정을 변경합니다.

옵션	설명
자동으로 DNS 서버 주소 및 호스트 이름 가져오기	DNS 서버 주소 및 호스트 이름을 자동으로 가져옵니다. DHCP 서버에서 IP 설정을 자동으로 가져오는 경우 이 옵션을 사용합니다.
다음 DNS 서버 주소 및 호스트 이름 사용	DNS 서버에 대한 정적 IP 주소 및 호스트 이름을 설정합니다.

6 **사용자 지정 DNS 접미사**에서 사용자 지정 DNS 접미사를 설정합니다.

접미사를 지정하지 않으면 기본 접미사 목록이 로컬 도메인 이름에서 파생됩니다.

7 Direct Console User Interface의 기본 메뉴로 돌아갈 때까지 Esc 키를 누릅니다.

vCenter Server의 관리 네트워크 다시 시작

vCenter Server의 관리 네트워크를 다시 시작하여 네트워크 연결을 복원합니다.

절차

1 vCenter Server의 DCUI(Direct Console User Interface)에 로그인합니다.

2 **관리 네트워크 다시 시작**을 선택하고 Enter 키를 누릅니다.

3 F11을 누릅니다.

Bash 셸에 액세스할 수 있도록 설정

DCUI(Direct Console User Interface)를 사용하여 Bash 셸에 대한 로컬 및 원격 액세스가 가능하도록 설정할 수 있습니다. DCUI(Direct Console User Interface)를 통해 설정된 Bash 셸 액세스는 3600초간 사용된 상태로 유지됩니다.

절차

1 vCenter Server의 DCUI(Direct Console User Interface)에 로그인합니다.

2 **문제 해결 옵션**을 선택하고 Enter를 누릅니다.

3 문제 해결 모드 옵션 메뉴에서 Bash 셸 또는 SSH를 사용하도록 선택합니다.

4 Enter 키를 눌러 서비스를 사용하도록 설정합니다.

5 Direct Console User Interface의 기본 메뉴로 돌아갈 때까지 Esc 키를 누릅니다.

다음에 수행할 작업

문제 해결을 위해 vCenter Server Bash 셸에 액세스합니다.

문제 해결을 위해 Bash 셸에 액세스

문제 해결 목적으로만 Bash 셸에 로그인합니다.

절차

1 다음 중 한 가지 방법을 사용하여 셸에 액세스합니다.

- vCenter Server 인스턴스에 직접 액세스할 수 있으면 Alt+F1을 누릅니다.
- 원격으로 연결하려면 SSH 또는 다른 원격 콘솔 연결을 사용하여 세션을 시작합니다.

2 사용자 이름 및 암호를 입력하십시오.

3 셸에서 `pi shell` 또는 `shell` 명령을 입력하여 Bash 셸에 액세스합니다.

문제 해결을 위해 vCenter Server 지원 번들 내보내기

문제 해결을 위해 DCUI 홈 화면에 표시되는 URL을 사용하여 장치에서 vCenter Server 인스턴스의 지원 번들을 내보낼 수 있습니다.

vCenter Server Appliance Bash 셸에서 `vc-support.sh` 스크립트를 실행하여 지원 번들을 수집할 수도 있습니다.

지원 번들을 `.tgz` 형식으로 내보냅니다.

절차

1 번들을 다운로드하려는 Windows 호스트 시스템에 로그인합니다.

2 웹 브라우저를 열고 DCUI에 표시되는 지원 번들에 대한 URL을 입력합니다.

https://*appliance-fully-qualified-domain-name*:443/appliance/support-bundle

3 루트 사용자에 대한 사용자 이름 및 암호를 입력합니다.

4 **Enter** 키를 클릭합니다.

지원 번들은 Windows 시스템에서 `.tgz` 파일로 다운로드됩니다.

5 (선택 사항) 실패한 firstboot 스크립트가 무엇인지 확인하려면 `firstbootStatus.json` 파일을 검사합니다.

vCenter Server Appliance Bash 셸에서 `vc-support.sh` 스크립트를 실행한 경우 `firstbootStatus.json` 파일을 검토하려면 다음을 실행합니다.

```
cat /var/log/firstboot/firstbootStatus.json
```