



VMware vSphere 환경을 위한 Virtual Storage Console을 구성합니다

VSC, VASA Provider, and SRA 9.7

NetApp
March 21, 2024

This PDF was generated from <https://docs.netapp.com/ko-kr/vsc-vasa-provider-sra-97/deploy/reference-esx-host-values-set-by-vsc-for-vmware-vsphere.html> on March 21, 2024. Always check docs.netapp.com for the latest.

목차

VMware vSphere 환경을 위한 Virtual Storage Console을 구성합니다	1
ESXi 서버 경로 다중화 및 시간 초과 설정을 구성합니다	1
Virtual Storage Console에 대한 SSL 인증서를 다시 생성합니다	7
여러 vCenter Server 환경에 VSC를 등록하는 데 필요한 요구 사항	7
VSC 기본 설정 파일을 구성합니다	8
서로 다른 서버넷에 데이터 저장소 마운트를 설정합니다	9
VSC, VASA Provider, SRA를 위한 가상 어플라이언스의 유지보수 콘솔 옵션에 액세스합니다	10
관리자 암호를 변경합니다	12
VSC, VASA Provider, SRA를 위해 가상 어플라이언스에 대한 고가용성을 구성합니다	12
VSC, VASA 공급자, SRA를 위한 가상 어플라이언스가 지원하는 MetroCluster 구성	14

VMware vSphere 환경을 위한 Virtual Storage Console을 구성합니다

VSC는 다양한 환경을 지원합니다. 이러한 환경에서 일부 기능을 사용하려면 추가 구성이 필요할 수 있습니다.

ESXi 호스트, 게스트 운영 체제 및 VSC를 구성하려면 다음 작업 중 일부를 수행해야 할 수 있습니다.

- UNMAP 설정을 비롯한 ESXi 호스트 설정 확인
- 게스트 운영 체제에 대한 시간 초과 값을 추가하는 중입니다
- VSC SSL 인증서를 재생성하는 중입니다
- 스토리지 용량 프로파일 및 임계값 알람 생성
- 서로 다른 서브넷에서 데이터 저장소를 마운트할 수 있도록 기본 설정 파일을 수정합니다

ESXi 서버 경로 다중화 및 시간 초과 설정을 구성합니다

VMware vSphere용 Virtual Storage Console은 스토리지 시스템에 가장 적합한 ESXi 호스트 경로 다중화 설정 및 HBA 시간 초과 설정을 확인하고 설정합니다.

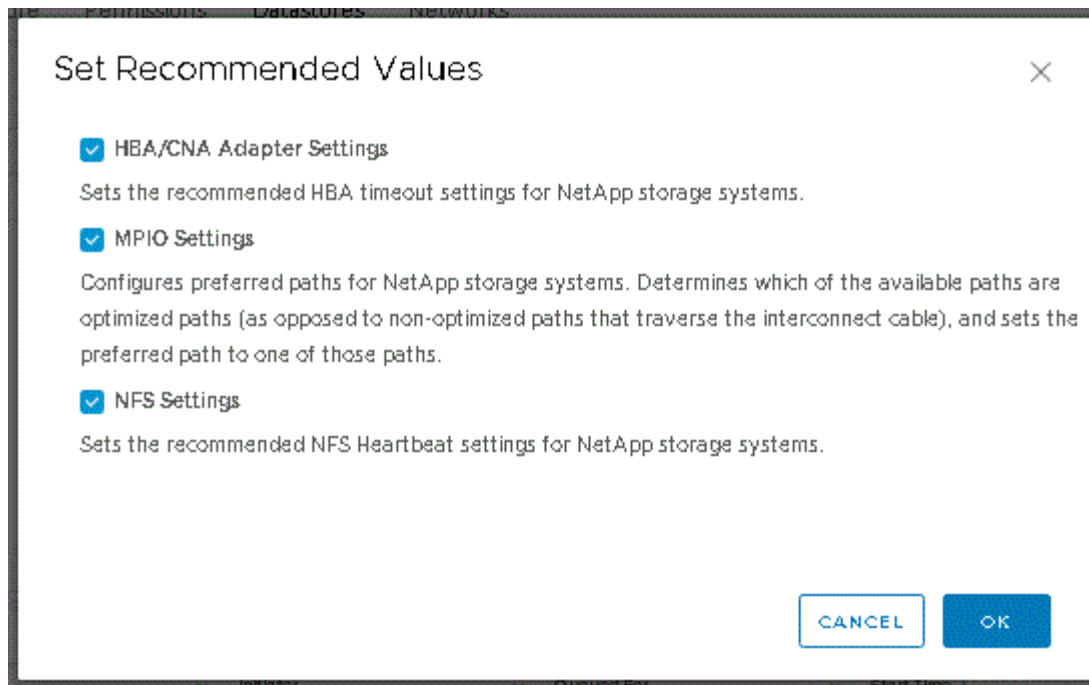
이 작업에 대해

이 프로세스는 구성 및 시스템 로드에서 따라 시간이 오래 걸릴 수 있습니다. 작업 진행률이 * Recent Tasks * (최근 작업) 패널에 표시됩니다. 작업이 완료되면 호스트 상태 경고 아이콘이 일반 아이콘 또는 재부팅 보류 중 아이콘으로 바뀝니다.

단계

1. VMware vSphere Web Client * Home * 페이지에서 vCenter [Hosts] 메뉴를 클릭합니다.
2. 호스트를 마우스 오른쪽 버튼으로 클릭하고 Actions[NetApp VSC > Set Recommended Values] 메뉴를 선택합니다.
3. NetApp 권장 설정 * 대화 상자에서 시스템에 가장 적합한 값을 선택합니다.

표준 권장 값은 기본적으로 설정됩니다.



4. 확인 * 을 클릭합니다.

VMware vSphere용 Virtual Storage Console을 사용하여 설정된 ESXi 호스트 값

최상의 성능과 성공적인 페일오버를 보장하기 위해 VMware vSphere용 Virtual Storage Console을 사용하여 ESXi 호스트에서 시간 초과 및 기타 값을 설정할 수 있습니다. VSC(Virtual Storage Console) 세트는 내부 테스트를 기반으로 합니다.

ESXi 호스트에서 다음 값을 설정할 수 있습니다.

ESXi 고급 구성

- * VMFS3.HardwareAcceleratedLocking *

이 값을 1로 설정해야 합니다.

- * VMFS3.EnableBlockDelete *

이 값을 0으로 설정해야 합니다.

NFS 설정

- * Net.TcpipHeapSize *

vSphere 6.0 이상을 사용하는 경우 이 값을 32로 설정해야 합니다.

- * Net.TcpipHeapMax *

vSphere 6.0 이상을 사용하는 경우 이 값을 1536으로 설정해야 합니다.

- * NFS.MaxVolumes *

vSphere 6.0 이상을 사용하는 경우 이 값을 256으로 설정해야 합니다.

- * NFS41.MaxVolumes *

vSphere 6.0 이상을 사용하는 경우 이 값을 256으로 설정해야 합니다.

- NFS.MaxQueueDepth *

vSphere 6.0 이상 버전의 ESXi 호스트를 사용하는 경우 큐 병목 현상을 방지하려면 이 값을 128 이상으로 설정해야 합니다.

vSphere 6.0 이전 버전의 경우 이 값을 64로 설정해야 합니다.

- * nfs.HeartbeatMaxFailures *

모든 NFS 구성에 대해 이 값을 10으로 설정해야 합니다.

- * nfs.HeartbeatFrequency * 를 선택합니다

모든 NFS 구성에 대해 이 값을 12로 설정해야 합니다.

- * nfs.HeartbeatTimeout *

모든 NFS 구성에 대해 이 값을 5로 설정해야 합니다.

FC/FCoE 설정

- * 경로 선택 정책 *

ALUA를 사용하는 FC 경로를 사용할 때는 이 값을 ""RR"(라운드 로빈)으로 설정해야 합니다.

다른 모든 설정에 대해 이 값을 ""고정""으로 설정해야 합니다.

이 값을 ""rr""로 설정하면 모든 활성/최적화 경로에 대한 로드 밸런싱을 제공하는 데 도움이 됩니다. 값 ""FIXED""는 이전 비 ALUA 구성에 사용되며 프록시 I/O를 방지하는 데 도움이 됩니다

- * Disk.QFullSampleSize *

모든 설정에 대해 이 값을 32로 설정해야 합니다. 이 값을 설정하면 I/O 오류가 발생하지 않습니다.

- * Disk.QFullThreshold *

모든 설정에 대해 이 값을 8로 설정해야 합니다. 이 값을 설정하면 I/O 오류가 방지됩니다.

- * Emulex FC HBA 시간 초과 *

기본값을 사용합니다.

- * QLogic FC HBA 시간 초과 *

기본값을 사용합니다.

iSCSI 설정

- * 경로 선택 정책 *

모든 iSCSI 경로에 대해 이 값을 ""rr""로 설정해야 합니다.

이 값을 ""rr""로 설정하면 모든 활성/최적화 경로에 대한 로드 밸런싱을 제공하는 데 도움이 됩니다.

- * Disk.QFullSampleSize *

모든 설정에 대해 이 값을 32로 설정해야 합니다. 이 값을 설정하면 I/O 오류가 발생하지 않습니다.

- * Disk.QFullThreshold *

모든 설정에 대해 이 값을 8로 설정해야 합니다. 이 값을 설정하면 I/O 오류가 방지됩니다.

게스트 운영 체제 스크립트를 구성합니다

게스트 운영 체제(OS) 스크립트의 ISO 이미지는 VMware vSphere 서버용 가상 스토리지 콘솔에 마운트됩니다. 게스트 OS 스크립트를 사용하여 가상 머신에 대한 스토리지 시간 초과를 설정하려면 vSphere Client에서 스크립트를 마운트해야 합니다.

운영 체제 유형입니다	60초 제한 시간 설정	190초 제한 시간 설정
리눅스	"https://<appliance_ip>: 8143/vsc/public/writable/linux_gos_ timeout-install.iso.	'https://<appliance_ip>: 8143/vsc/public/writable/linux_gos_ timeout_190 - install.iso
Windows	"https://<appliance_ip>: 8143/vsc/public/writable/windows_ gos_timeout.iso"	"https://<appliance_ip>: 8143/vsc/public/writable/windows_ gos_timeout_190.iso.
Solaris	"https://<appliance_ip>: 8143/vsc/public/writable/Solaris_go s_timeout-install.iso.	'https://<appliance_ip>: 8143/vsc/public/writable/Solaris_go s_timeout_190 - install.iso

가상 머신을 관리하는 vCenter Server에 등록된 VSC 인스턴스 복사본에서 스크립트를 설치해야 합니다. 환경에 vCenter Server가 여러 개 포함된 경우 스토리지 시간 초과 값을 설정할 가상 머신이 포함된 서버를 선택해야 합니다.

가상 머신에 로그인한 다음 스크립트를 실행하여 스토리지 시간 초과 값을 설정해야 합니다.

Windows 게스트 운영 체제에 대한 시간 초과 값을 설정합니다

게스트 운영 체제(OS) 시간 초과 스크립트는 Windows 게스트 운영 체제에 대한 SCSI 입출력 시간 초과 설정을 설정합니다. 60초 제한 시간 또는 190초 제한 시간을 지정할 수 있습니다. 설정을 적용하려면 Windows 게스트 OS를 재부팅해야 합니다.

시작하기 전에

Windows 스크립트를 포함하는 ISO 이미지를 마운트해야 합니다.

단계

1. Windows 가상 머신의 콘솔에 액세스하고 관리자 권한이 있는 계정으로 로그인합니다.
2. 스크립트가 자동으로 시작되지 않으면 CD 드라이브를 연 다음 "windows_gos_timeout.reg" 스크립트를 실행합니다.

레지스트리 편집기 대화 상자가 표시됩니다.

3. 계속하려면 * 예 * 를 클릭하십시오.

"D:\WINDOWS_Gos_TIMEOUT.reg에 포함된 키와 값이 레지스트리에 추가되었습니다."라는 메시지가 표시됩니다

4. Windows 게스트 OS를 재부팅합니다.

5. ISO 이미지를 마운트 해제합니다.

Solaris 게스트 운영 체제에 대한 시간 초과 값을 설정합니다

게스트 운영 체제(OS) 시간 초과 스크립트는 Solaris 10에 대한 SCSI I/O 시간 초과 설정을 지정합니다. 60초 제한 시간 또는 190초 제한 시간을 지정할 수 있습니다.

시작하기 전에

Solaris 스크립트를 포함하는 ISO 이미지를 마운트해야 합니다.

단계

1. Solaris 가상 머신의 콘솔에 액세스하고 루트 권한이 있는 계정으로 로그인합니다.
2. 'olaris_gos_timeout-install.sh' 스크립트를 실행합니다.

Solaris 10의 경우 다음과 유사한 메시지가 표시됩니다.

```
Setting I/O Timeout for /dev/s-a - SUCCESS!
```

3. ISO 이미지를 마운트 해제합니다.

Linux 게스트 운영 체제에 대한 시간 제한 값을 설정합니다

게스트 운영 체제(OS) 시간 제한 스크립트는 Red Hat Enterprise Linux 버전 4, 5, 6, 7과 SUSE Linux Enterprise Server 버전 9, 10 및 11에 대한 SCSI I/O 시간 초과 설정을 설정합니다. 60초 제한 시간 또는 190초 제한 시간을 지정할 수 있습니다. 새 버전의 Linux로 업그레이드할 때마다 스크립트를 실행해야 합니다.

시작하기 전에

Linux 스크립트를 포함하는 ISO 이미지를 마운트해야 합니다.

단계

1. Linux 가상 머신의 콘솔에 액세스하고 루트 권한이 있는 계정으로 로그인합니다.
2. Linux_gos_timeout-install.sh 스크립트를 실행합니다.

Red Hat Enterprise Linux 4 또는 SUSE Linux Enterprise Server 9의 경우 다음과 유사한 메시지가 표시됩니다.

```
Restarting udev... this may take a few seconds.
```

```
Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
```

Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6 및 Red Hat Enterprise Linux 7의 경우 다음과 유사한 메시지가 표시됩니다.

```
patching file /etc/udev/rules.d/50-udev.rules
```

```
Hunk #1 succeeded at 333 (offset 13 lines).
```

```
Restarting udev... this may take a few seconds.
```

```
Starting udev: [ OK ]
```

```
Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
```

SUSE Linux Enterprise Server 10 또는 SUSE Linux Enterprise Server 11의 경우 다음과 유사한 메시지가 표시됩니다.

```
patching file /etc/udev/rules.d/50-udev-default.rules
```

```
Hunk #1 succeeded at 114 (offset 1 line).
```

```
Restarting udev ...this may take a few seconds.
```

```
Updating all available device nodes in /dev: done
```

3. ISO 이미지를 마운트 해제합니다.

Virtual Storage Console에 대한 SSL 인증서를 다시 생성합니다

SSL 인증서는 VSC(VSC)를 설치할 때 생성됩니다. SSL 인증서에 대해 생성된 DN(고유 이름)은 클라이언트 컴퓨터에서 인식하는 CN(일반 이름)이 아닐 수 있습니다. 키 저장소 및 개인 키 암호를 변경하여 인증서를 다시 생성하고 사이트별 인증서를 만들 수 있습니다.

이 작업에 대해

유지보수 콘솔을 사용하여 원격 진단을 활성화하고 사이트별 인증서를 생성할 수 있습니다.

"NetApp 기술 자료 답변 1075654: 가상 스토리지 콘솔 7.x: CA 서명 인증서 구현"

단계

1. 유지보수 콘솔에 로그인합니다.
2. Application Configuration 메뉴에 액세스하려면 1을 입력하십시오.
3. Application Configuration 메뉴에서 3을 입력하여 VSC 서비스를 중단한다.
4. SSL 인증서를 다시 생성하려면 7을 입력하십시오.

여러 vCenter Server 환경에 VSC를 등록하는 데 필요한 요구 사항

단일 VMware vSphere HTML5 클라이언트가 있는 환경에서 VMware vSphere용 Virtual Storage Console을 사용하는 경우 여러 vCenter Server 인스턴스를 관리하는 경우 VSC와 vCenter Server 간에 1:1 페어링이 있을 수 있도록 각 vCenter Server에 VSC 인스턴스 하나를 등록해야 합니다. 이렇게 하면 단일 vSphere HTML5 클라이언트에서 연결된 모드와 연결되지 않은 모드 모두에서 vCenter 6.0 이상을 실행하는 모든 서버를 관리할 수 있습니다.



vCenter Server에서 VSC를 사용하려면 관리할 모든 vCenter Server 인스턴스에 대해 VSC 인스턴스를 하나 이상 설정하거나 등록해야 합니다. 등록된 각 VSC 인스턴스의 버전은 동일해야 합니다.

연결된 모드는 vCenter Server 구축 중에 자동으로 설치됩니다. 연결 모드는 Microsoft ADAM(Active Directory Application Mode)을 사용하여 여러 vCenter Server 시스템에 데이터를 저장하고 동기화합니다.

vSphere HTML5 클라이언트를 사용하여 여러 vCenter Server에서 VSC 작업을 수행하려면 다음이 필요합니다.

- 관리하려는 VMware 인벤토리의 각 vCenter Server에는 고유한 1:1 페어링에 단일 VSC 서버가 등록되어 있어야 합니다.

예를 들어, VSC 서버 A에 등록된 VSC 서버 A, vCenter Server B에 등록된 VSC 서버 B, vCenter Server C에 등록된 VSC 서버 C 등의 작업을 수행할 수 있습니다.

vCenter Server A와 vCenter Server B 모두에 VSC 서버 A를 등록할 수 없습니다

VMware 인벤토리에 VSC 서버가 등록되지 않은 vCenter Server가 포함되어 있지만 VSC에 등록된 vCenter Server가 하나 이상 있는 경우, 그런 다음 VSC의 인스턴스를 확인하고 VSC를 등록한 vCenter Server에 대해 VSC 작업을 수행할 수 있습니다.

- SSO(Single Sign-On)에 등록된 각 vCenter Server에 대한 VSC별 View 권한이 있어야 합니다.

또한 올바른 RBAC 권한도 있어야 합니다.

vCenter Server를 지정해야 하는 작업을 수행하는 경우 * vCenter Server * 드롭다운 상자에 사용 가능한 vCenter Server가 영숫자 순서로 표시됩니다. 기본 vCenter Server는 항상 드롭다운 목록의 첫 번째 서버입니다.

스토리지의 위치를 알고 있는 경우(예: * Provisioning * 마법사를 사용하고 데이터 저장소가 특정 vCenter Server에서 관리하는 호스트에 있는 경우) vCenter Server 목록이 읽기 전용 옵션으로 표시됩니다. 이 문제는 vSphere Web Client에서 마우스 오른쪽 버튼 클릭 옵션을 사용하여 항목을 선택하는 경우에만 발생합니다.

VSC는 관리하지 않는 개체를 선택하려고 할 때 경고합니다.

VSC 요약 페이지에서 특정 vCenter Server를 기반으로 스토리지 시스템을 필터링할 수 있습니다. vCenter Server에 등록된 모든 VSC 인스턴스에 대한 요약 페이지가 나타납니다. 특정 VSC 인스턴스 및 vCenter Server와 연관된 스토리지 시스템을 관리할 수 있지만, VSC의 여러 인스턴스를 실행하는 경우 각 스토리지 시스템의 등록 정보를 별도로 유지해야 합니다.

VSC 기본 설정 파일을 구성합니다

기본 설정 파일에는 VMware vSphere 작업을 위한 Virtual Storage Console을 제어하는 설정이 포함되어 있습니다. 대부분의 경우 이러한 파일의 설정을 수정할 필요가 없습니다. 기본 설정 파일(VSC)에서 사용하는 파일을 알면 도움이 됩니다.

VSC에는 몇 가지 기본 설정 파일이 있습니다. 이러한 파일에는 VSC에서 다양한 작업을 수행하는 방법을 결정하는 항목 키와 값이 포함되어 있습니다. 다음은 VSC에서 사용하는 몇 가지 기본 설정 파일입니다.

`/opt/netapp/vscserver/etc/kaminoprefs.xml`

`/opt/netapp/vscserver/etc/vsc/vscPreferences.xml`

특정 상황에서 기본 설정 파일을 수정해야 할 수 있습니다. 예를 들어 iSCSI 또는 NFS를 사용하고 서브넷이 ESXi 호스트와 스토리지 시스템 간에 다른 경우 기본 설정 파일을 수정해야 합니다. 기본 설정 파일에서 설정을 수정하지 않으면 VSC에서 데이터 저장소를 마운트할 수 없기 때문에 데이터 저장소 프로비저닝이 실패합니다.

IPv4 또는 IPv6를 설정합니다

VSC에 추가된 모든 스토리지 시스템에서 IPv4 또는 IPv6를 지원하도록 설정할 수 있는 기본 설정 파일 'kaminoprefs.xml'에 새로운 옵션이 추가되었습니다.

- `default.override.option.provision.mount.datastore.address.family` 매개 변수가 데이터 저장소 프로비저닝을 위해 선호되는 데이터 LIF 프로토콜을 설정하기 위해 "kaminoprefs.xml" 기본 설정 파일에 추가되었습니다.

이 기본 설정은 VSC에 추가된 모든 스토리지 시스템에 적용됩니다.

- 새 옵션의 값은 IPv4 IPv6 없음.
- 기본적으로 이 값은 "없음"으로 설정됩니다.

값	설명
없음	<ul style="list-style-type: none"> 프로비저닝은 스토리지 추가에 사용되는 클러스터 또는 관리 LIF의 유형과 동일한 IPv6 또는 IPv4 주소 유형의 데이터 LIF를 사용하여 수행됩니다. 동일한 IPv6 또는 IPv4 주소 유형의 데이터 LIF가 없으면 다른 유형의 데이터 LIF를 통해 프로비저닝이 수행됩니다(가능한 경우).
IPv4	<ul style="list-style-type: none"> 프로비저닝은 선택된 IPv4 데이터 LIF를 사용하여 이루어집니다. 에 IPv4 데이터 LIF가 없으면 에서 사용할 수 있는 경우 IPv6 데이터 LIF를 통해 프로비저닝이 수행됩니다.
IPv6	<ul style="list-style-type: none"> 프로비저닝은 선택된 IPv6 데이터 LIF를 사용하여 이루어집니다. 에 IPv6 데이터 LIF가 없으면 에서 사용할 수 있는 경우 IPv4 데이터 LIF를 통해 프로비저닝이 수행됩니다.

서로 다른 서브넷에 데이터 저장소 마운트를 설정합니다

iSCSI 또는 NFS를 사용하고 서브넷이 ESXi 호스트와 스토리지 시스템 간에 다른 경우 VMware vSphere 기본 설정 파일용 Virtual Storage Console을 수정해야 합니다. 기본 설정 파일을 수정하지 않으면 (VSC)에서 데이터 저장소를 마운트할 수 없기 때문에 데이터 저장소 프로비저닝이 실패합니다.

이 작업에 대해

데이터 저장소 프로비저닝이 실패하면 VSC에서 다음 오류 메시지를 기록합니다.

"계속할 수 없습니다. 컨트롤러의 커널 IP 주소와 주소를 상호 참조할 때 IP 주소를 찾을 수 없습니다

이 호스트에 대한 NFS 마운트 볼륨과 일치하는 네트워크를 찾을 수 없습니다 ``이

단계

1. vCenter Server 인스턴스에 로그인합니다.
2. 통합 어플라이언스 가상 머신을 사용하여 유지보수 콘솔을 시작합니다.

["VSC, VASA Provider, SRA를 위한 가상 어플라이언스의 유지보수 콘솔 옵션에 액세스합니다"](#)

3. 지원 및 진단* 옵션에 액세스하려면 '4'를 입력하십시오.
4. Access Diagnostic Shell * 옵션에 액세스하려면 "2"를 입력하십시오.
5. kaminoprefs.xml을 업데이트하려면 vi/opt/netapp/vscserver/etc/kaminoprefs.xml을 입력하십시오.
6. kaminoprefs.xml 파일을 업데이트합니다.

사용하는 경우...	수행할 작업...
iSCSI	항목 키 ddefault.allow.iscsi.mount.networks` 값을 모두 에서 ESXi 호스트 네트워크 값으로 변경합니다.
NFS 를 참조하십시오	항목 키 ddefault.allow.nfs.mount.networks` 값을 모두 에서 ESXi 호스트 네트워크 값으로 변경합니다.

기본 설정 파일에는 이러한 입력 키에 대한 샘플 값이 포함되어 있습니다.



모든 네트워크가 의미하는 것은 아닙니다. ""모두" 값을 사용하면 호스트와 스토리지 시스템 간의 일치하는 모든 네트워크를 데이터 저장소를 마운트하는 데 사용할 수 있습니다. 호스트 네트워크를 지정할 때 지정된 서브넷에서만 마운트를 활성화할 수 있습니다.

7. kaminoprefs.xml 파일을 저장하고 닫습니다.

VSC, VASA Provider, SRA를 위한 가상 어플라이언스의 유지보수 콘솔 옵션에 액세스합니다

VSC(Virtual Storage Console), VASA Provider, SRA(Storage Replication Adapter)용 가상 어플라이언스의 유지보수 콘솔을 사용하여 애플리케이션, 시스템, 네트워크 구성을 관리할 수 있습니다. 관리자 암호 및 유지보수 암호를 변경할 수 있습니다. 또한 지원 번들을 생성하고, 다양한 로그 수준을 설정하고, TLS 구성을 확인 및 관리하고, 원격 진단을 시작할 수 있습니다.


시작하기 전에

VSC, VASA Provider, SRA를 위한 가상 어플라이언스를 구축한 후에는 VMware 툴을 설치해야 합니다.

이 작업에 대해

- VSC, VASA Provider, SRA를 위해 가상 어플라이언스의 유지보수 콘솔에 로그인하려면 구축 중에 구성한 사용자 이름과 암호로 "maint"를 사용해야 합니다.
- 원격 진단을 활성화하는 동안 "diag" 사용자의 암호를 설정해야 합니다.

단계

1. 구축된 가상 어플라이언스의 * 요약 * 탭에 액세스합니다.
2.  을 클릭합니다. 를 눌러 유지보수 콘솔을 시작합니다.

다음 유지보수 콘솔 옵션에 액세스할 수 있습니다.

◦ * 응용 프로그램 구성 *

다음 옵션을 사용할 수 있습니다.

- 서버 상태 요약을 표시합니다
- Virtual Storage Console 서비스를 시작합니다
- Virtual Storage Console 서비스를 중지합니다

- VASA Provider 및 SRA 서비스를 시작합니다
- VASA Provider 및 SRA 서비스를 중지합니다
- '관리자' 사용자 암호를 변경합니다
- 인증서를 다시 생성합니다
- 키 저장소 및 인증서를 하드 리셋합니다
- 데이터베이스를 하드 리셋합니다
- Virtual Storage Console 서비스의 로그 레벨을 변경합니다
- VASA Provider 및 SRA 서비스의 로그 레벨을 변경합니다
- TLS 구성을 표시합니다
- TLS 프로토콜을 활성화합니다
- TLS 프로토콜을 비활성화합니다

◦ * 시스템 구성 *

다음 옵션을 사용할 수 있습니다.

- 가상 머신을 재부팅합니다
- 가상 머신을 종료합니다
- '성자' 사용자 암호를 변경합니다
- 시간대를 변경합니다
- NTP 서버를 변경합니다

NTP 서버에 IPv6 주소를 제공할 수 있습니다.

- SSH 액세스를 설정/해제합니다
- jail 디스크 크기 증가(/jail)
- 업그레이드
- VMware Tools를 설치합니다

◦ * 네트워크 구성 *

다음 옵션을 사용할 수 있습니다.

- IP 주소 설정을 표시합니다
- IP 주소 설정을 변경합니다

이 옵션을 사용하여 IP 주소 사후 배포를 IPv6로 변경할 수 있습니다.

- 도메인 이름 검색 설정을 표시합니다
- 도메인 이름 검색 설정을 변경합니다
- 정적 경로를 표시합니다
- 정적 경로를 변경합니다

이 옵션을 사용하여 IPv6 경로를 추가할 수 있습니다.

- 변경 사항을 커밋합니다
- 호스트에 Ping을 보냅니다

이 옵션을 사용하여 IPv6 호스트에 ping을 수행할 수 있습니다.

- 기본 설정을 복원합니다
- * 지원 및 진단 *

다음 옵션을 사용할 수 있습니다.

- 지원 번들을 생성합니다
- 진단 셀에 액세스합니다
- 원격 진단 액세스를 활성화합니다
 - 관련 정보 *

VSC 및 VASA 공급자 로그 파일

관리자 암호를 변경합니다

유지보수 콘솔을 사용하여 VSC, VASA Provider, SRA 구축 후 가상 어플라이언스의 관리자 암호를 변경할 수 있습니다.

단계

1. vCenter Server에서 VSC, VASA Provider, SRA를 위한 콘솔을 엽니다.
2. 유지보수 사용자로 로그인합니다.
3. 유지보수 콘솔에 '1'을 입력하여 * 애플리케이션 구성 * 을 선택합니다.
4. '6'을 입력하여 '관리자' 사용자 암호 변경 * 을 선택합니다.
5. 최소 8자 및 최대 63자의 암호를 입력합니다.
6. 확인 대화 상자에 y를 입력합니다.

VSC, VASA Provider, SRA를 위해 가상 어플라이언스에 대한 고가용성을 구성합니다

VSC(Virtual Storage Console), VASA Provider, SRA(Storage Replication Adapter)용 가상 어플라이언스는 장애 시 VSC, VASA Provider, SRA의 무중단 기능을 제공할 수 있도록 HA(Virtual Storage Console) 구성을 지원합니다.

VSC, VASA Provider, SRA를 위한 가상 어플라이언스는 VMware vSphere(HA) 기능과 vSphere FT(Fault Tolerance) 기능을 사용하여 제공합니다. (HA) 솔루션을 사용하면 다음과 같은 원인으로 인한 운영 중단으로부터 신속하게 복구할 수 있습니다.

- 호스트 오류입니다

- 네트워크 오류입니다
- 가상 머신 장애(게스트 OS 장애)
- 애플리케이션(VSC, VASA Provider, SRA)이 충돌합니다

가상 어플라이언스의 경우 추가 구성이 필요하지 않습니다. 요구 사항에 따라 vCenter Server 및 ESXi 호스트만 VMware vSphere HA 기능 또는 vSphere FT 기능으로 구성해야 합니다. HA와 FT에는 모두 공유 스토리지와 함께 클러스터 호스트가 필요합니다. FT는 추가적인 요구 사항과 제한 사항이 있습니다.

가상 어플라이언스는 VMware vSphere HA 솔루션 및 vSphere FT 솔루션 외에도 VSC, VASA Provider 및 SRA 서비스를 항상 실행할 수 있도록 지원합니다. 가상 어플라이언스 감시 프로세스는 세 가지 서비스를 주기적으로 모니터링하여 어떤 종류의 장애가 감지되면 자동으로 다시 시작합니다. 이렇게 하면 응용 프로그램 오류를 방지할 수 있습니다.



vCenter HA는 VSC, VASA Provider, SRA용 가상 어플라이언스에서 지원되지 않습니다.

VMware vSphere HA

가상 스토리지 콘솔(VSC), VASA 공급자, SRA(Storage Replication Adapter)용 가상 어플라이언스가 구축된 vSphere 환경을 구성할 수 있습니다. VMware HA 기능은 가상 환경에서 하드웨어 장애 및 운영 체제 장애로부터 페일오버 보호 기능을 제공합니다.

VMware HA 기능은 가상 시스템을 모니터링하여 운영 체제 장애 및 하드웨어 장애를 감지합니다. 장애가 감지되면 VMware HA 기능은 리소스 풀의 다른 물리적 서버에서 가상 머신을 다시 시작합니다. 서버 오류가 감지되면 수동 개입이 필요하지 않습니다.

VMware HA 구성 절차는 vCenter Server 버전에 따라 다릅니다. 예를 들어 다음 참조 링크를 사용하여 필요한 vCenter Server 버전을 선택하여 VMware HA 구성 단계를 볼 수 있습니다.

["VMware vSphere 설명서: vSphere HA 클러스터 생성 및 사용"](#)

VMware vSphere 내결함성

VMware vSphere FT(Fault Tolerance) 기능은 더 높은 수준에서 HA(Fault Tolerance)를 제공하며 데이터 또는 연결을 손실하지 않고 가상 머신을 보호할 수 있습니다. vCenter Server에서 VSC, VASA Provider 및 SRA를 위한 가상 어플라이언스에 대해 vSphere FT를 사용하거나 사용하지 않도록 설정해야 합니다.

vSphere 라이선스가 사용자 환경의 가상 어플라이언스에 필요한 vCPU 수로 FT를 지원하는지 확인합니다(대규모 환경의 경우 vCPU 2개 이상, vCPU 4개).

vSphere FT를 사용하면 서버 장애가 발생하더라도 가상 머신을 지속적으로 운영할 수 있습니다. 가상 머신에서 vSphere FT가 설정되면 DRS(Distributed Resource Scheduler)가 선택한 다른 호스트(보조 가상 머신)에 운영 가상 머신의 복제본이 자동으로 생성됩니다. DRS가 활성화되어 있지 않으면 사용 가능한 호스트에서 대상 호스트가 선택됩니다. vSphere FT는 운영 가상 머신과 보조 가상 머신을 잠금 단계 모드로 작동하여 각 가상 머신이 운영 가상 머신의 실행 상태를 보조 가상 머신에 미러링합니다.

운영 가상 시스템에 장애를 일으키는 하드웨어 장애가 있는 경우 보조 가상 머신이 운영 가상 머신이 중지된 위치를 즉시 감지합니다. 보조 가상 시스템은 네트워크 연결, 트랜잭션 또는 데이터의 손실 없이 계속 실행됩니다.

시스템은 vCenter Server 인스턴스에 대해 vSphere FT를 구성하기 위한 CPU 요구 사항, 가상 머신 제한 요구 사항 및 라이선스 요구 사항을 충족해야 합니다.

HA를 구성하는 절차는 vCenter Server 버전에 따라 다릅니다. 예를 들어 다음 참조 링크를 사용하여 필요한 vCenter Server 버전을 선택하여 HA 구성 단계를 볼 수 있습니다.

["VMware vSphere 설명서: 내결함성 요구 사항, 제한 사항 및 라이선스"](#)

VSC, VASA 공급자, SRA를 위한 가상 어플라이언스가 지원하는 MetroCluster 구성

VSC(가상 스토리지 콘솔), VASA 공급자, SRA(스토리지 복제 어댑터)용 가상 어플라이언스는 ONTAP용 MetroCluster IP 및 FC 구성을 사용하는 환경을 지원합니다. 대부분의 지원은 자동입니다. 하지만 MetroCluster 환경을 VSC 및 VASA 공급자와 함께 사용하면 몇 가지 차이점이 있을 수 있습니다.

MetroCluster 구성 및 VSC를 누릅니다

VSC는 운영 사이트와 2차 사이트에서 스토리지 시스템 컨트롤러를 검색하는지 확인해야 합니다. 일반적으로 VSC는 스토리지 컨트롤러를 자동으로 검색합니다. 클러스터 관리 LIF를 사용하는 경우, VSC가 두 사이트에서 클러스터를 검색했는지 확인하는 것이 좋습니다. 그렇지 않으면 스토리지 컨트롤러를 VSC에 수동으로 추가할 수 있습니다. VSC에서 스토리지 컨트롤러에 연결하는 데 사용하는 사용자 이름과 암호 쌍을 수정할 수도 있습니다.

전환이 발생하면 보조 사이트의 이(가) 대신 사용됩니다. 이들 이름에 "-mc" 접미사가 붙어 있습니다. 데이터 저장소 프로비저닝과 같은 작업을 수행하는 동안 전환 작업이 발생하면 데이터 저장소가 상주하는 의 이름이 ""-mc" 접미사를 포함하도록 변경됩니다. 스위치백 이 발생하고 기본 사이트 재시작 컨트롤에서 이 접미사가 삭제됩니다.



MetroCluster 구성을 VSC에 직접 추가한 경우 전환 후 SVM 이름의 변경("-mc" 접미사 추가)이 반영되지 않습니다. 다른 모든 스위치오버 작업은 정상적으로 계속 실행됩니다.

스위치오버 또는 스위치백을 수행할 때 VSC에서 클러스터를 자동으로 감지하여 검색하는 데 몇 분 정도 걸릴 수 있습니다. 데이터 저장소 프로비저닝과 같은 VSC 작업을 수행하는 동안 이 문제가 발생하면 지연이 발생할 수 있습니다.

MetroCluster 구성 및 VASA 공급자

VASA Provider는 MetroCluster 구성을 사용하는 환경을 자동으로 지원합니다. VASA Provider 환경에서는 전환이 투명합니다. VASA Provider에 직접 추가할 수 없습니다.



VASA Provider는 전환 후 보조 사이트의 이름에 ""-mc" 접미사를 추가하지 않습니다.

MetroCluster 구성 및 SRA

SRA는 MetroCluster 구성을 지원하지 않습니다.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.