Secure Configuration

vRealize Operations Manager 6.5

vmware®

VMware 웹 사이트 (https://docs.vmware.com/kr/) 에서 최신 기술 문서를 확인할 수 있습니다.
이 문서에 대한 의견이 있으면 docfeedback@vmware.com으로 사용자 의견을 보내주십시오.

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

목차

보안 구성 5

1 vRealize Operations Manager 보안 수준 6

2 vRealize Operations Manager 의 안전한 배포 7
- 설치 미디어의 무결성 확인 7
- 배포된 소프트웨어 인프라 강화 7
- 설치된 소프트웨어 및 지원되지 않는 소프트웨어 검토 8
- VMware 보안 권고 및 패치 9

3 vRealize Operations Manager 의 보안 구성 10
- vRealize Operations Manager 콘솔 보안 11
- 루트 비밀번호 변경 11
- 보안 셸, 관리 계정 및 콘솔 액세스 관리 12
- 부트 로더 인증 설정 17
- 단일 사용자 또는 유지 보수 모드 인증 18
- 필요한 최소 사용자 계정 모니터링 18
- 필요한 최소 그룹 모니터링 19
- vRealize Operations Manager 관리자 비밀번호 재설정(Linux) 20
- VMware 어플라이언스에서 NTP 구성 20
- Linux에서 TCP 타임스탬프 응답을 사용하지 않도록 설정 21
- FIPS 140-2 모드 활성화 21
- 전송 중인 데이터의 TLS 21
- 보호되어야 하는 애플리케이션 리소스 25
- PostgreSQL 클라이언트 인증 구성 26
- Apache 구성 27
- 구성 모드를 사용하지 않도록 설정 28
- 필요하지 않은 소프트웨어 구성 요소 관리 28
- Linux 설치 배포 32
- Endpoint Operations Management 에이전트 34
- 추가 보안 구성 작업 40

4 네트워크 보안 및 보안 통신 42
- 가상 애플리케이션 설치에 대한 네트워크 설정 구성 42
- 포트 및 프로토콜 구성 52

5 vRealize Operations Manager 시스템 감사 및 로깅 54
- 원격 로깅 서버 보안 유지 54

인증된 NTP 서버 사용 54
클라이언트 브라우저 고려 사항 55

보안 구성

보안 구성에 대한 설명서는 vRealize Operations Manager 배포의 보안 기준선 역할을 합니다. 시스템 모니터링 도구를 사용하여 보안 기준선 구성의 예기치 않은 변경을 지속적으로 모니터링하고 유지하려는 경우 이 문서를 참조하십시오.

기본적으로 아직 설정되지 않은 강화 작업은 수동으로 수행할 수 있습니다.

대상 사용자

이 정보를 vRealize Operations Manager 관리자를 대상으로 합니다.

VMware 기술 자료 용어집

VMware 기술 자료 사이트에서는 새로운 용어를 정리한 용어집을 제공하고 있습니다. VMware 기술 설명서에서 사용하는 용어의 정의에 대해 알아보려면 http://www.vmware.com/support/pubs로 이동하십시오.

vRealize Operations Manager 보안 수준

1

vRealize Operations Manager의 보안 수준은 시스템 및 네트워크 구성, 조직의 보안 정책 및 모범 사례를 기준으로 완벽하게 보안된 환경을 가정합니다. 조직의 보안 정책 및 모범 사례에 따라 강화 작업을 수행하는 것이 중요합니다.

이 문서는 다음 섹션으로 분류되어 있습니다.

- 보안 배포
- 보안 구성
- 네트워크 보안
- 통신

이 가이드에는 가상 애플리케이션의 설치에 대한 자세한 내용이 포함되어 있습니다. 그러나 다음 배포 유형에 대한 설명도 포함되어 있습니다.

- Linux 설치 배포

시스템을 안전하게 강화하려면 권장 사항을 검토하고 조직의 보안 정책 및 위험 노출 수준을 기준으로 해당 권장 사항을 평가하십시오.

vRealize Operations Manager 의 안전한 배포

2

제품을 설치하기 전에 설치 미디어의 무결성을 확인하여 다운로드된 파일의 신뢰성을 확인해야 합니다.

이 장에서는 다음 주제에 대해 설명합니다.

- 설치 미디어의 무결성 확인
- 배포된 소프트웨어 인프라 강화
- 설치된 소프트웨어 및 지원되지 않는 소프트웨어 검토
- VMware 보안 권고 및 패치

설치 미디어의 무결성 확인

미디어를 다운로드한 후에는 MD5/SHA1 합계 값을 사용하여 다운로드의 무결성을 확인하십시오. ISO, 오프라인 번들 또는 패치를 다운로드한 후에는 항상 SHA1 해시를 확인하여 다운로드한 파일의 무결성과 신뢰성을 확인하십시오. VMware에서 받은 물리적 미디어의 보안 실(seal)이 파손된 경우 소프트웨어를 VMware에 반환하여 교체받으십시오.

프로시저

- MD5/SHA1 합계 출력을 VMware 웹 사이트에 게시된 값과 비교합니다.

  SHA1 또는 MD5 해시가 일치해야 합니다.

  참고 vRealize Operations Manager 6.x-x.pak 파일은 VMware 소프트웨어 게시 인증서로 서명됩니다. vRealize Operations Manager는 설치 전에 PAK 파일의 서명을 검증합니다.

배포된 소프트웨어 인프라 강화

강화 프로세스의 일부로, VMware 시스템을 지원하는 배포된 소프트웨어 인프라를 강화해야 합니다.

VMware 시스템을 강화하기 전에 지원 소프트웨어 인프라의 보안 결함을 검토하고 해결하여 완전히 강화되고 보안이 유지되는 환경을 구축해야 합니다. 고려해야 하는 소프트웨어 인프라 요소로는 운영 체제 구성 요소, 지원 소프트웨어, 데이터베이스 소프트웨어 등이 있습니다. 제조업체 권장 사항과 기타 관련 보안 프로토콜에 따라 이러한 요소를 포함한 다른 구성 요소의 보안 문제를 해결합니다.

VMware vSphere 환경 강화

vRealize Operations Manager는 보안이 유지되는 VMware vSphere 환경을 통해 최상의 이점 및 보안이 유지되는 인프라를 실현합니다.

VMware vSphere 환경을 평가하고 적합한 수준의 vSphere 강화 지침이 적용되고 유지되는지 확인합니다.

강화에 대한 자세한 지침은 http://www.vmware.com/security/hardening-guides.html 항목을 참조하십시오.

Linux 설치 강화

해당 Linux 강화 및 보안 Best Practice 지침에 규정된 권장 사항을 검토하고 Linux 호스트가 올바르게 강화되었는지 확인합니다. 강화 권장 사항을 따르지 않을 경우 시스템이 Linux 릴리스에서 보안이 유지되지 않는 구성 요소의 알려진 보안 취약점에 노출될 수 있습니다.

vRealize Operations Manager는 버전 6.5부터 RHEL(Red Hat Enterprise Linux) 6에 설치가 가능합니다.

설치된 소프트웨어 및 지원되지 않는 소프트웨어 검토

사용하지 않는 소프트웨어의 취약성으로 인해 무단 시스템 액세스 및 사용 중단의 위험이 증가할 수 있습니다. VMware 호스트 시스템에 설치된 소프트웨어를 검토하고 사용 여부를 평가하십시오.

시스템의 안전한 작동에 필요하지 않은 소프트웨어를 vRealize Operations Manager 노드 호스트에 설치하지 마십시오. 사용하지 않거나 필요하지 않은 소프트웨어를 제거하십시오.

지원되지 않거나, 테스트되지 않았거나, 승인되지 않은 소프트웨어를
vRealize Operations Manager와 같은 인프라 제품에 설치하는 것은 인프라에 위협이 됩니다.

인프라에 대한 위협을 최소화하려면 VMware가 VMware 제공 호스트에서 지원하지 않는 타사 소프트웨어를 설치하거나 사용하지 마십시오.

vRealize Operations Manager 배포 및 설치된 제품 인벤토리를 평가하여 지원되지 않는 소프트웨어가 설치되지 않았는지 확인합니다.

타사 제품의 지원 정책에 대한 자세한 내용은
http://www.vmware.com/security/hardening-guides.html의 VMware 지원을 참조하십시오.

타사 소프트웨어 확인

VMware가 지원하지 않는 타사 소프트웨어를 사용하지 마십시오. 모든 타사 소프트웨어가 타사 벤더 지침에 따라 안전하게 구성되고 패치가 적용되었는지 확인합니다.

신뢰할 수 없거나 안전하지 않거나 패치가 적용되지 않은 타사 소프트웨어를 VMware 호스트 시스템에 설치하여 발생하는 취약성은 시스템 무단 액세스 및 사용 중단 위험의 원인이 될 수 있습니다. VMware가 제공하지 않는 모든 소프트웨어는 적절하게 보호되고 패치가 적용되어야 합니다.

VMware가 지원하지 않는 타사 소프트웨어를 사용해야 하는 경우 타사 벤더에 보안 구성 및 패치 요구 사항을 문의하십시오.

VMware 보안 권고 및 패치

VMware에서는 때때로 제품에 대한 보안 권고를 릴리스합니다. 이러한 권고를 숙지하면 기반 제품을 안전하게 유지하고 제품이 알려진 위협에 취약하지 않은지 확인할 수 있습니다.

vRealize Operations Manager 설치, 패치 및 업그레이드 기록을 평가하고 릴리스된 VMware 보안 권고가 준수 및 시행되었는지 확인하십시오.

최신 보안 픽스가 포함되는 vRealize Operations Manager 최신 릴리스를 유지하는 것이 좋습니다.

최신 VMware 보안 권고에 대한 자세한 내용은
http://www.vmware.com/kr/security/advisories/를 참조하십시오.

vRealize Operations Manager 의 보안 구성

3

보안 모범 사례로, vRealize Operations Manager 콘솔을 보호하고 SSH(보안 셸), 관리 계정 및 콘솔 액세스를 관리해야 합니다. 시스템이 보안 전송 채널로 배포되는지 확인하십시오.

또한 Endpoint Operations Management 에이전트 실행에 대한 특정 보안 모범 사례를 따라야 합니다.

이 장에서는 다음 주제에 대해 설명합니다.

- vRealize Operations Manager 콘솔 보안
- 루트 비밀번호 변경
- 보안 셸, 관리 계정 및 콘솔 액세스 관리
- 부트 로더 인증 설정
- 단일 사용자 또는 유지 보수 모드 인증
- 필요한 최소 사용자 계정 모니터링
- 필요한 최소 그룹 모니터링
- vRealize Operations Manager 관리자 비밀번호 재설정(Linux)
- VMware 어플라이언스에서 NTP 구성
- Linux에서 TCP 타임스탬프 응답을 사용하지 않도록 설정
- FIPS 140-2 모드 활성화
- 전송 중인 데이터의 TLS
- 보호되어야 하는 애플리케이션 리소스
- PostgreSQL 클라이언트 인증 구성
- Apache 구성
- 구성 모드를 사용하지 않도록 설정
- 필요하지 않은 소프트웨어 구성 요소 관리
- Linux 설치 배포
- Endpoint Operations Management 에이전트
- 추가 보안 구성 작업

vRealize Operations Manager 콘솔 보안

vRealize Operations Manager를 설치한 후 클러스터의 각 노드의 콘솔에 처음으로 로그인하고 콘솔에 보안을 적용해야 합니다.]

필수 조건

vRealize Operations Manager를 설치합니다.

프로시저

1 vCenter에서 또는 직접 액세스를 통해 노드 콘솔을 찾습니다.

vCenter에서 Alt+F1을 눌러 로그인 메시지에 액세스합니다. 보안상의 이유로 vRealize Operations Manager 원격 터미널 세션은 기본적으로 사용하지 않도록 설정되어 있습니다.

2 root로 로그인합니다.

vRealize Operations Manager에서는 루트 비밀번호를 생성해야 명령 프롬프트에 액세스할 수 있습니다.

3 비밀번호를 입력하라는 메시지가 표시되면 **Enter** 키를 누릅니다.

4 이전 비밀번호를 입력하라는 메시지가 표시되면 **Enter** 키를 누릅니다.

5 새 비밀번호를 입력하라는 메시지가 표시되면 원하는 루트 비밀번호를 입력하고 나중에 참조할 수 있도록 적어 둡니다.

6 루트 비밀번호를 다시 입력합니다.

7 콘솔에서 로그아웃합니다.

루트 비밀번호 변경

콘솔에서 vRealize Operations Manager 마스터 또는 데이터 노드의 루트 비밀번호를 언제든지 변경할 수 있습니다.

루트 사용자는 pam_cracklib 모듈 비밀번호 복잡성 검사(etc/pam.d/common-password에 위치)를 생략합니다. 강화된 모든 어플라이언스에서는 enforce_for_root가 pw_history 모듈(etc/pam.d/common-password 파일에 위치)에 대해 사용하도록 설정됩니다. 기본적으로 시스템은 마지막 5개 비밀번호를 기억합니다. 이전 비밀번호는 각 사용자에 대해 /etc/security/opasswd 파일에 저장됩니다.

필수 조건

어플라이언스의 루트 비밀번호가 조직의 기업 비밀번호 복잡성 요구 사항을 충족하는지 확인합니다. 계정 비밀번호가 6로 시작하는 경우 sha512 해시가 사용됩니다. 이는 강화된 모든 어플라이언스에 대한 표준 해시입니다.

프로시저

1 어플라이언스의 루트 셸에서 # passwd 명령을 실행합니다.

2 루트 비밀번호의 해시를 확인하려면 루트로 로그인하고 # more /etc/shadow 명령을 실행합니다.

   해시 정보가 나타납니다.

3 루트 비밀번호에 sha512 해시가 포함되지 않은 경우 passwd 명령을 실행하여 변경합니다.

비밀번호 만료 기간 관리

모든 계정 비밀번호 만료 기간은 조직의 보안 정책에 따라 구성합니다.

기본적으로 강화된 모든 VMware 어플라이언스는 60일의 비밀번호 만료 기간을 사용합니다. 대부분의 강화된 어플라이언스에서 루트 계정은 365일의 비밀번호 만료 기간으로 설정됩니다. 모범 사례로, 모든 계정의 만료 기간이 보안 및 운영 요구 사항 표준을 준수하는지 확인하십시오.

루트 비밀번호가 만료되면 복구할 수 없습니다. 사이트별 정책을 구현하여 관리 및 루트 비밀번호가 만료되는 것을 방지해야 합니다.

프로시저

1 가상 어플라이언스 시스템에 루트로 로그인하고 # more /etc/shadow 명령을 실행하여 모든 계정의 비밀번호 만료 기간을 확인합니다.

2 루트 계정의 만료 기간을 수정하려면 # passwd -x 365 root 명령을 실행합니다.

   이 명령에서 365는 비밀번호 만료까지 남은 일 수를 나타냅니다. 동일한 명령을 사용하여 root에 대한 특정 계정을 대체하고 조직의 만료 표준에 맞게 남은 일 수를 바꿔 사용자를 수정합니다.

   기본적으로 루트 비밀번호는 365일로 설정됩니다.

보안 셸, 관리 계정 및 콘솔 액세스 관리

원격 연결을 사용하려면 강화된 모든 어플라이언스에 SSH(보안 셸) 프로토콜이 포함되어야 합니다. 강화된 어플라이언스에서 SSH는 기본적으로 사용하지 않도록 설정됩니다.

SSH는 vRealize Operations Manager 노드에 대한 원격 연결을 지원하는 대화형 명령줄 환경입니다. SSH를 사용하려면 높은 수준의 권한이 있는 사용자 계정 자격 증명이 필요합니다. SSH 작업은 일반적으로 vRealize Operations Manager 노드의 RBAC(역할 기반 액세스 제어) 및 감사 제어를 생략합니다.

모범 사례로, 운영 환경에서 SSH를 사용하지 않도록 설정하고 문제를 진단하거나 다른 방법으로 해결할 수 없는 문제를 해결할 때만 사용하도록 설정하십시오. 특정 목적에 필요한 동안에만 조직의 보안 정책에 따라 사용하도록 설정합니다. SSH를 사용하도록 설정한 경우 공격으로부터 안전한지 확인하고 필요한 동안만 사용하도록 설정해야 합니다. vSphere 구성에 따라 OVF(Open Virtualization Format) 템플릿을 배포할 때 SSH를 사용하거나 사용하지 않도록 설정할 수 있습니다.

시스템에서 SSH가 사용하도록 설정되었는지 여부를 간단히 테스트하려면 SSH를 사용하여 연결을 열어 보십시오. 연결이 열리고 자격 증명이 요청되면 SSH가 사용하도록 설정된 것이고 연결 시 SSH를 사용할 수 있습니다.

보안 셸 루트 사용자

VMware 어플라이언스에는 사전 구성된 기본 사용자 계정이 포함되지 않으므로 기본적으로 루트 계정으로 SSH를 사용하여 직접 로그인할 수 있습니다. 가능한 빨리 루트로 SSH를 사용하지 않도록 설정하십시오.

부인 방지에 대한 규정 준수 표준을 준수하기 위해 강화된 모든 어플라이언스의 SSH 서버는 SSH 액세스를 보조 그룹 휠로 제한하는 AllowGroups 휠 항목으로 사전 구성됩니다. 직무 분리를 위해 /etc/ssh/sshd_config 파일의 AllowGroups 휠 항목을 sshd와 같은 다른 그룹을 사용하도록 수정할 수 있습니다.

이 휠 그룹은 수퍼유저 액세스를 위해 pam_wheel 모듈을 통해 사용하도록 설정되므로 휠 그룹 구성원이 su-root 명령을 사용할 수 있습니다. 이 명령을 사용하려면 루트 비밀번호가 필요합니다. 그룹을 분리하면 사용자가 SSH를 사용하여 어플라이언스에 연결할 수 있지만 su 명령을 사용하여 루트로 로그인할 수는 없습니다. AllowGroups 필드의 다른 항목은 제거하거나 수정하지 마십시오. 어플라이언스가 제대로 기능하지 않을 수 있습니다. 변경이 완료되면 # service sshd restart 명령을 실행하여 SSH 대몬을 다시 시작합니다.

vRealize Operations Manager 노드에서 보안 셸을 사용하거나 사용하지 않도록 설정

문제 해결을 위해 vRealize Operations Manager 노드에서 SSH(보안 셸)를 사용하도록 설정할 수 있습니다. 예를 들어, 서버 문제를 해결하려면 서버에 대한 콘솔 액세스가 필요할 수 있습니다. 콘솔 액세스는 SSH를 통과합니다. 정상적인 작업을 위해 vRealize Operations Manager 노드에서 SSH를 사용하지 않도록 설정합니다.

프로시저

1. vCenter에서 vRealize Operations Manager 노드의 콘솔에 액세스합니다.
2. Alt + F1을 눌러 로그인 프롬프트에 액세스한 후 로그인합니다.
3. #chkconfig 명령을 실행합니다.
4. sshd 서비스가 해제된 경우 #chkconfig sshd on 명령을 실행합니다.
5. #service sshd start 명령을 실행하여 sshd 서비스를 시작합니다.
6. #service sshd stop 명령을 실행하여 sshd 서비스를 중지합니다.

보안 셸을 위한 로컬 관리자 계정 생성

루트 SSH 액세스를 제거하기 전에 SSH(보안 셸)로 사용할 수 있거나 보조 휠 그룹의 구성원인, 또는 이 둘 모두에 해당하는 로컬 관리자 계정을 생성해야 합니다.

직접 루트 액세스를 사용하지 않도록 설정하기 전에 권한 있는 관리자가 AllowGroups를 사용하여 SSH에 액세스할 수 있는지와 휠 그룹과 su 명령을 사용하여 루트로 로그인할 수 있는지를 테스트해야 합니다.

프로시저

1 루트로 로그인하고 다음 명령을 실행합니다.

```
# useradd -d /home/vropsuser -g users -G wheel -m
# passwd username
```

휠은 AllowGroups에서 SSH 액세스가 가능하도록 지정된 그룹입니다. 보조 그룹을 여러 개 추가하려면 -G wheel,sshd를 사용하십시오.

2 해당 사용자로 전환하고 암호 복잡성 검사를 통과하는 새 암호를 제공합니다.

```
# su - username
username@hostname:~>passwd
```

암호 복잡성이 충족되는 경우 암호가 업데이트됩니다. 암호 복잡성이 충족되지 않으면 암호가 원래 암호로 되돌려지고, 이 경우 암호 명령을 다시 실행해야 합니다.

SSH 원격 액세스를 허용하는 로그인 계정을 생성하고 su 명령을 사용하여 휠 액세스를 사용하는 루트로 로그인한 후에는 SSH 직접 로그인에서 루트 계정을 제거할 수 있습니다.

3 (#)PermitRootLogin yes를 PermitRootLogin no로 대체하는 방식으로 /etc/ssh/sshd_config 파일을 수정하여 SSH에 대한 직접 로그인을 제거합니다.

후속 작업

루트로 직접 로그인을 사용하지 않도록 설정합니다. 기본적으로, 강화된 어플라이언스에서는 콘솔을 통해 루트에 직접 로그인할 수 있습니다. 부인 방지를 위한 관리자 계정을 생성하고 휠 액세스가 가능한지에 대해 이러한 계정을 테스트(su-root)한 후에는 루트로 /etc/securetty 파일을 편집하고 tty1 항목을 console로 대체하여 직접 루트 로그인을 사용하지 않도록 설정합니다.

보안 셸 액세스 제한

시스템 강화 프로세스의 일부로 모든 VMware 가상 어플라이언스 호스트 시스템에 tcp_wrappers 패키지를 적절히 구성하여 SSH(보안 셸) 액세스를 제한합니다. 또한 필요한 SSH 키 파일 사용 권한을 이러한 어플라이언스에 유지합니다.

모든 VMware 가상 어플라이언스에는 libwrapped 대몬에 액세스할 수 있는 네트워크 서브넷을 tcp-supported 대몬을 통해 제어할 수 있도록 하는 tcp_wrappers 패키지가 포함됩니다. 기본적으로 /etc/hosts.allow 파일에는 보안 셸에 대한 모든 액세스를 허용하는 일반 항목인 sshd: ALL : ALLOW가 포함됩니다. 이 액세스를 조직의 요구 사항에 적절하게 제한하십시오.

프로시저

1 텍스트 편집기에서 가상 어플라이언스 호스트 시스템의 /etc/hosts.allow 파일을 엽니다.

2 운영 환경의 일반 항목을 로컬 호스트 항목 및 관리 네트워크 서브넷만 포함하도록 변경하여 작업을 보호합니다.

```
sshd:127.0.0.1 : ALLOW
sshd: [::1] : ALLOW
sshd: 10.0.0.0 :ALLOW
```

이 예에서는 모든 로컬 호스트 연결 및 클라이언트가 10.0.0.0 서브넷에서 수행하는 연결이 허용됩니다.

3 호스트 이름, IP 주소, FQDN(정규화된 도메인 이름) 및 루프백 등 해당하는 모든 시스템 ID를 추가합니다.

4 파일을 저장하고 닫습니다.

보안 셸 키 파일 사용 권한 유지

적절한 보안 수준을 유지하려면 SSH(보안 셸) 키 파일 사용 권한을 구성합니다.

프로시저

1 /etc/ssh/*key.pub에 위치한 공용 호스트 키 파일을 봅니다.

2 파일의 소유자가 루트인지, 그룹의 소유자가 루트인지, 파일의 사용 권한이 0644로 설정되었는지 확인합니다.

사용 권한은 (-rw-r--r--)입니다.

3 모든 파일을 닫습니다.

4 /etc/ssh/*key에 위치한 개인 호스트 키 파일을 봅니다.

5 파일 및 그룹의 소유자가 루트인지와 파일의 사용 권한이 0600으로 설정되었는지 확인합니다.

사용 권한은 (-rw-------)입니다.

6 모든 파일을 닫습니다.

보안 셸 서버 구성 강화

가능한 경우, 가상 애플리케이션 설치(OVF)에는 기본적으로 강화된 구성이 포함됩니다. 사용자는 구성 파일의 글로벌 옵션 섹션에서 서버 및 클라이언트 서비스를 검토하여 구성이 올바르게 강화되었는지 확인할 수 있습니다.

가능한 경우, /etc/hosts.allow 파일에서 SSH 서버 사용을 관리 서브넷으로 제한합니다.

프로시저

1 /etc/ssh/sshd_config 서버 구성 파일을 열고 설정이 올바른지 확인합니다.

설정	실행 상태
서버 대몬 프로토콜	Protocol 2
암호	Ciphers aes256-ctr,aes128-ctr

설정	실행 상태
TCP 전달	AllowTCPForwarding no
서버 게이트웨이 포트	Gateway Ports no
X11 전달	X11Forwarding no
SSH 서비스	AllowGroups 필드를 사용하여 액세스가 허용되는 그룹을 지정하고 서비스 사용이 허용되는 사용자의 보조 그룹에 구성원을 추가합니다.
GSSAPI 인증	GSSAPIAuthentication no(사용하지 않는 경우)
Kerberos 인증	KerberosAuthentication no(사용하지 않는 경우)
로컬 변수(AcceptEnv 글로벌 옵션)	disabled by commenting out 또는 enabled for only LC_* or LANG variables로 설정
터널 구성	PermitTunnel no
네트워크 세션	MaxSessions 1
엄격한 모드 검사	Strict Modes yes
권한 분리	UsePrivilegeSeparation yes
rhosts RSA 인증	RhostsRSAAuthentication no
압축	Compression delayed 또는 Compression no
메시지 인증 코드	MACs hmac-sha1
사용자 액세스 제한	PermitUserEnvironment no

2 변경 사항을 저장하고 파일을 닫습니다.

보안 셸 클라이언트 구성 강화

시스템 강화 모니터링 프로세스의 일부로, 가상 어플라이언스 호스트 시스템의 SSH 클라이언트 구성 파일을 검토하는 방식으로 SSH 클라이언트 강화를 확인하여 VMware 지침에 따라 구성되었는지 확인해야 합니다.

프로시저

1 SSH 클라이언트 구성 파일 /etc/ssh/ssh_config를 열고 글로벌 옵션 섹션의 설정이 올바른지 확인합니다.

설정	실행 상태
클라이언트 프로토콜	Protocol 2
클라이언트 게이트웨이 포트	Gateway Ports no
GSSAPI 인증	GSSAPIAuthentication no
로컬 변수(SendEnv 글로벌 옵션)	LC_* 또는 LANG 변수만 제공
CBC 암호	Ciphers aes256-ctr,aes128-ctr
메시지 인증 코드	MACs hmac-sha1 항목에서만 사용됨

2 변경 사항을 저장하고 파일을 닫습니다.

루트로 직접 로그인을 사용하지 않도록 설정

기본적으로, 강화된 어플라이언스에서는 콘솔을 사용하여 루트로 직접 로그인할 수 있습니다. 보안 Best Practice로, 부정 방지를 위한 관리자 계정을 생성하고 su-root 명령을 사용하여 휠 액세스가 가능한지에 대해 이 계정을 테스트한 후에는 직접 로그인을 사용하지 않도록 설정할 수 있습니다.

필수 조건

- 보안 셸을 위한 로컬 관리자 계정 생성 항목에 있는 단계를 따릅니다.
- 직접 루트 로그인을 사용하지 않도록 설정하기 전에 시스템에 관리자로 액세스할 수 있는지 테스트해 보아야 합니다.

프로시저

1 루트로 로그인하고 /etc/securetty 파일을 찾습니다.

명령 프롬프트에서 이 파일에 액세스할 수 있습니다.

2 tty1 항목을 console로 대체합니다.

관리자 계정에 대해 SSH 액세스를 사용하지 않도록 설정

보안 모범 사례에 따라 관리자 계정에 대해 SSH를 사용하지 않도록 설정할 수 있습니다. vRealize Operations Manager admin 계정과 Linux admin 계정은 동일한 암호를 사용합니다. 관리자가 SSH 액세스를 사용하지 못하도록 설정하면 모든 SSH 사용자가 vRealize Operations Manager admin 계정과 다른 암호를 사용하고 권한도 보다 낮은 서비스 계정에 일단 로그인한 다음, admin이나 루트 등 권한이 높은 사용자로 전환되므로 보안이 강화됩니다.

프로시저

1 /etc/ssh/sshd_config 파일을 편집합니다.

명령 프롬프트에서 이 파일에 액세스할 수 있습니다.

2 파일의 아무 곳에나 DenyUsers admin 항목을 추가하고 파일을 저장합니다.

3 sshd 서버를 다시 시작하려면 service sshd restart 명령을 실행합니다.

부트 로더 인증 설정

적절한 수준의 보안을 제공하려면 VMware 가상 어플라이언스에 부트 로더 인증을 구성합니다. 시스템 부트 로더에 인증을 필요로 하지 않는 경우 콘솔에서 시스템에 액세스하는 사용자가 시스템 부팅 구성을 조작하거나 단일 사용자 또는 유지 보수 모드로 부팅하여 서비스 거부 또는 무단 시스템 액세스를 유발할 수 있습니다.

부트 로더 인증은 VMware 가상 어플라이언스에 기본적으로 설정되지 않으므로 GRUB 비밀번호를 생성하여 부트 로더 인증을 구성해야 합니다.

프로시저

1 가상 어플라이언스의 /boot/grub/menu.lst 파일에서 password --md5 <password-hash> 줄을 찾아 부팅 비밀번호가 있는지 확인합니다.

2 비밀번호가 없는 경우 가상 어플라이언스에서 # /usr/sbin/grub-md5-crypt 명령을 실행합니다.

MD5 비밀번호가 생성되고 명령이 md5 해시 출력을 제공합니다.

3 # password --md5 <hash from grub-md5-crypt> 명령을 실행하여 비밀번호를 menu.lst 파일에 추가합니다.

단일 사용자 또는 유지 보수 모드 인증

시스템에서 유효한 루트 인증 없이 단일 사용자 또는 유지 보수 모드로 부팅할 수 있는 경우 단일 사용자 또는 유지 보수 모드를 호출하는 모든 사용자에게 시스템의 모든 파일에 액세스할 수 있는 권한이 부여됩니다.

프로시저

- /etc/inittab 파일을 검토하고 ls:S:wait:/etc/init.d/rc S 및 ~~:S:respawn:/sbin/sulogin의 2개 줄이 나타나는지 확인합니다.

필요한 최소 사용자 계정 모니터링

기존 사용자 계정을 모니터링하여 불필요한 사용자 계정이 제거되었는지 확인해야 합니다.

프로시저

- *host*:~ # cat /etc/passwd 명령을 실행하고 필요한 최소 사용자 계정을 확인합니다.

```
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
haldaemon:x:101:102:User for haldaemon:/var/run/hald:/bin/false
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
messagebus:x:100:101:User for D-Bus:/var/run/dbus:/bin/false
nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
ntp:x:74:106:NTP daemon:/var/lib/ntp:/bin/false
polkituser:x:103:104:PolicyKit:/var/run/PolicyKit:/bin/false
postfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/false
root:x:0:0:root:/root:/bin/bash
sshd:x:71:65:SSH daemon:/var/lib/sshd:/bin/false
suse-ncc:x:104:107:Novell Customer Center User:/var/lib/YaST2/suse-ncc-fakehome:/bin/bash
uuidd:x:102:103:User for uuidd:/var/run/uuidd:/bin/false
wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false
nginx:x:105:108:user for nginx:/var/lib/nginx:/bin/false
admin:x:1000:1003::/home/admin:/bin/bash
tcserver:x:1001:1004:tc Server User:/home/tcserver:/bin/bash
postgres:x:1002:100::/var/vmware/vpostgres/9.3:/bin/bash
```

필요한 최소 그룹 모니터링

기존 그룹 및 구성원을 모니터링하여 불필요한 그룹이나 그룹 액세스가 제거되었는지 확인해야 합니다.

프로시저

- <host>:~ # cat /etc/group 명령을 실행하여 필요한 최소 그룹 및 그룹 구성원 자격을 확인합니다.

```
audio:x:17:
bin:x:1:daemon
cdrom:x:20:
console:x:21:
daemon:x:2:
dialout:x:16:u1,tcserver,postgres
disk:x:6:
floppy:x:19:
haldaemon:!:102:
kmem:x:9:
mail:x:12:
man:x:62:
messagebus:!:101:
modem:x:43:
nobody:x:65533:
nogroup:x:65534:nobody
ntp:!:106:
polkituser:!:105:
public:x:32:
root:x:0:admin
shadow:x:15:
sshd:!:65:
suse-ncc:!:107:
sys:x:3:
tape:!:103:
trusted:x:42:
tty:x:5:
utmp:x:22:
uuidd:!:104:
video:x:33:u1,tcserver,postgres
wheel:x:10:root,admin
www:x:8:
xok:x:41:
maildrop:!:1001:
postfix:!:51:
users:x:100:
vami:!:1002:root
nginx:!:108:
admin:!:1003:
vfabric:!:1004:admin,wwwrun
```

vRealize Operations Manager 관리자 비밀번호 재설정 (Linux)

보안 모범 사례로, vApp 또는 Linux 설치에 대한 Linux 클러스터의 vRealize Operations Manager 비밀번호를 재설정할 수 있습니다.

프로시저

1 마스터 노드의 원격 콘솔에 루트로 로그인합니다.

2 $VMWARE_PYTHON_BIN $VCOPS_BASE/../vmware-vcopssuite/utilities/sliceConfiguration/bin/vcopsSetAdminPassword.py --reset 명령을 입력하고 프롬프트의 메시지를 따릅니다.

VMware 어플라이언스에서 NTP 구성

시간 소싱이 중요한 경우 VMware 어플라이언스에서 호스트 시간 동기화를 사용하지 않도록 설정하고 NTP(Network Time Protocol)를 사용하십시오. 시간 동기화에 신뢰할 수 있는 원격 NTP 서버를 구성해야 합니다. NTP 서버는 신뢰할 수 있는 시간 서버이거나, 최소한 신뢰할 수 있는 시간 서버와 동기화되어야 합니다.

VMware 가상 어플라이언스에 구축된 NTP 대몬은 동기화된 시간 서비스를 제공합니다. NTP는 기본적으로 사용하지 않도록 설정되어 있으므로 수동으로 구성해야 합니다. 가능한 경우, 프로덕션 환경에서 NTP를 사용하여 정확한 감사 및 로그 유지 기능을 통해 사용자 작업을 추적하고 잠재적으로 악의적인 공격 및 침입을 감지합니다. NTP 보안 알림에 대한 자세한 내용은 NTP 웹 사이트를 참조하십시오.

NTP 구성 파일의 위치는 각 어플라이언스에서 /etc/ntp.conf 파일입니다.

프로시저

1 가상 어플라이언스 호스트 시스템에서 /etc/ntp.conf 구성 파일을 찾습니다.

2 파일 소유권을 root:root로 설정합니다.

3 권한을 0640으로 설정합니다.

4 NTP 서비스에 대한 DOS(서비스 거부 공격) 증폭 공격의 위험을 완화하기 위해 /etc/ntp.conf 파일을 열고 restrict 줄이 파일에 나타나는지 확인합니다.

```
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1
```

5 변경 사항을 저장하고 파일을 닫습니다.

NTP 보안 알림에 대한 자세한 내용은 http://support.ntp.org/bin/view/Main/SecurityNotice 항목을 참조하십시오.

Linux에서 TCP 타임스탬프 응답을 사용하지 않도록 설정

TCP 타임스탬프 응답을 사용하면 원격 호스트 가동 시간의 근사치를 계산하고 향후 공격 시 도움을 줄 수 있습니다. 또한, 일부 운영 체제의 경우 해당 TCP 타임스탬프의 동작을 바탕으로 핑거프린팅될 수 있습니다.

프로시저

- Linux에서 TCP 타임스탬프 응답을 사용하지 않도록 설정합니다.
  a. sysctl -w net.ipv4.tcp_timestamps=0 명령을 실행하여 net.ipv4.tcp_timestamps의 값을 0으로 설정합니다.
  b. 기본 sysctl.conf 파일에 ipv4.tcp_timestamps=0 값을 추가합니다.

FIPS 140-2 모드 활성화

vRealize Operations Manager 6.3 이상 릴리스가 탑재되어 있는 OpenSSL 버전은 FIPS 140-2 인증을 받았습니다. 단, FIPS 모드는 기본적으로 활성화되어 있지 않습니다.

FIPS 모드가 활성화된 FIPS 인증 암호 알고리즘을 사용해야 하는 보안 준수 요구 사항이 있는 경우 FIPS 모드를 활성화할 수 있습니다.

프로시저

1. mod_ssl.so 파일을 대체하려면 다음 명령을 실행합니다.

```
cd /usr/lib64/apache2-prefork/
cp mod_ssl.so mod_ssl.so.old
cp mod_ssl.so.FIPSON.openssl1.0.2 mod_ssl.so
```

2. /etc/apache2/ssl-global.conf 파일을 편집하여 Apache2 구성을 수정합니다.
3. <IfModule mod_ssl.c> 줄을 검색하고 아래줄에 SSLFIPS on 지침을 추가합니다.
4. Apache 구성을 재설정하려면 service apache2 restart 명령을 실행합니다.

전송 중인 데이터의 TLS

보안 모범 사례로, 시스템이 보안 전송 채널을 통해 배포되는지 확인합니다.

vRealize Operations Manager 에 대한 강력한 프로토콜 구성

SSLv2 및 SSLv3와 같은 프로토콜은 더 이상 안전한 것으로 간주되지 않습니다. TLS 1.0도 사용하지 않도록 설정하는 것이 좋습니다. TLS 1.1 및 TLS 1.2만 사용하도록 설정하십시오.

Apache HTTPD에 있는 프로토콜의 올바른 사용 확인

vRealize Operations Manager에서는 기본적으로 SSLv2 및 SSLv3가 사용하지 않도록 설정됩니다. 시스템을 운영에 배치하기 전에 모든 로드 밸런서에서 약한 프로토콜을 사용하지 않도록 설정해야 합니다.

프로시저

1 명령 프롬프트에서 grep SSLProtocol /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf | grep -v '#' 명령을 실행하여 SSLv2 및 SSLv3가 사용하지 않도록 설정되었는지 확인합니다.

프로토콜이 사용하지 않도록 설정되어 있으면 명령에서 SSLProtocol All -SSLv2 -SSLv3 출력을 반환합니다.

2 TLS 1.0 프로토콜도 사용하지 않도록 설정하려면 명령 프롬프트에서 sed -i "/^[^#]*SSLProtocol/ c₩SSLProtocol All -SSLv2 -SSLv3 -TLSv1" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf 명령을 실행합니다.

3 Apache2 서버를 다시 시작하려면 명령 프롬프트에서 /etc/init.d/apache2 restart 명령을 실행합니다.

GemFire TLS 핸들러에 있는 프로토콜의 올바른 사용 확인

vRealize Operations Manager에서는 기본적으로 SSLv3를 사용하지 않도록 설정되어 있습니다. 시스템을 운영에 배치하기 전에 모든 로드 밸런서에서 약한 프로토콜을 사용하지 않도록 설정해야 합니다.

프로시저

1 프로토콜이 사용하도록 설정되었는지 확인합니다. 프로토콜이 사용하도록 설정되었는지 확인하려면 각 노드에서 다음 명령을 실행합니다.

```
grep cluster-ssl-protocol /usr/lib/vmware-vcops/user/conf/gemfire.properties | grep -v '#'
```

예상 결과:

```
cluster-ssl-protocols=TLSv1.2 TLSv1.1 TLSv1
grep cluster-ssl-protocol /usr/lib/vmware-vcops/user/conf/gemfire.native.properties | grep -v '#'
```

예상 결과:

```
cluster-ssl-protocols=TLSv1.2 TLSv1.1 TLSv1
grep cluster-ssl-protocol /usr/lib/vmware-vcops/user/conf/gemfire.locator.properties | grep -v '#'
```

예상 결과:

```
cluster-ssl-protocols=TLSv1.2 TLSv1.1 TLSv1
```

2 TLS 1.0을 사용하지 않도록 설정합니다.

a url/admin에서 관리자 사용자 인터페이스로 이동합니다.

b **오프라인으로 전환**을 클릭합니다.

c SSLv3 및 TLS 1.0을 사용하지 않도록 설정하려면 다음 명령을 실행합니다.

```
sed -i "/^[^#]*cluster-ssl-protocol/ c₩cluster-ssl-protocols=TLSv1.2
TLSv1.1" /usr/lib/vmware-vcops/user/conf/gemfire.properties
sed -i "/^[^#]*cluster-ssl-protocol/ c₩cluster-ssl-protocols=TLSv1.2
TLSv1.1" /usr/lib/vmware-vcops/user/conf/gemfire.native.properties
sed -i "/^[^#]*cluster-ssl-protocol/ c₩cluster-ssl-protocols=TLSv1.2
TLSv1.1" /usr/lib/vmware-vcops/user/conf/gemfire.locator.properties
```

각 노드에 대해 이 단계를 반복합니다.

d 관리자 사용자 인터페이스로 이동합니다.

e **온라인으로 전환**을 클릭합니다.

3 TLS 1.0을 다시 사용하도록 설정합니다.

a 관리자 사용자 인터페이스로 이동하여 클러스터를 오프라인으로 전환합니다. url/admin

b **오프라인으로 전환**을 클릭합니다.

c SSLv3 및 TLS 1.0이 사용하지 않도록 설정되었는지 확인하려면 다음 명령을 실행합니다.

```
sed -i "/^[^#]*cluster-ssl-protocol/ c₩cluster-ssl-protocols=TLSv1.2 TLSv1.1
TLSv1" /usr/lib/vmware-vcops/user/conf/gemfire.properties
sed -i "/^[^#]*cluster-ssl-protocol/ c₩cluster-ssl-protocols=TLSv1.2 TLSv1.1
TLSv1" /usr/lib/vmware-vcops/user/conf/gemfire.native.properties
sed -i "/^[^#]*cluster-ssl-protocol/ c₩cluster-ssl-protocols=TLSv1.2 TLSv1.1
TLSv1" /usr/lib/vmware-vcops/user/conf/gemfire.locator.properties
```

각 노드에 대해 이 단계를 반복합니다.

d 관리자 사용자 인터페이스로 이동하여 클러스터를 온라인으로 전환합니다.

e **온라인으로 전환**을 클릭합니다.

강력한 암호를 사용하도록 vRealize Operations Manager 구성

최상의 보안을 위해 강력한 암호를 사용하도록 vRealize Operations Manager 구성 요소를 구성해야 합니다. 강력한 암호만 선택되도록 하려면 취약한 암호 사용을 비활성화하십시오. 서버가 강력한 암호만 지원하고 충분히 큰 키 크기를 사용하도록 구성합니다. 또한, 적합한 순서로 암호를 구성합니다.

기본적으로 vRealize Operations Manager가 DHE 키 교환을 사용하여 암호 그룹을 사용하지 않도록 설정합니다. 시스템을 프로덕션 환경에 배치하기 전에 모든 로드 밸런서에서 동일한 취약한 암호 그룹을 사용하지 않도록 설정해야 합니다.

강력한 암호 사용

서버와 브라우저 사이에 협상되는 암호화 암호에 따라 TLS 세션에 사용되는 암호화 강도와 키 교환 방법이 결정됩니다.

Apache HTTPD에 있는 암호 그룹의 올바른 사용 확인

보안을 최대화하기 위해 Apache httpd에 있는 암호 그룹의 올바른 사용을 확인하십시오.

프로시저

1 Apache httpd에 있는 암호 그룹의 올바른 사용을 확인하려면 명령 프롬프트에서 grep SSLCipherSuite /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf | grep -v '#' 명령을 실행합니다.

Apache httpd에서 올바른 암호 그룹이 사용되고 있으면 명령이 다음 출력을 반환합니다. SSLCipherSuite kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH

2 암호 그룹의 올바른 사용을 구성하려면 명령 프롬프트에서 sed -i "/^[^#]*SSLCipherSuite/c₩SSLCipherSuite kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:₩!aNULL₩!ADH:₩!EXP:₩!MD5:₩!3DES:₩!CAMELLIA:₩!PSK:₩!SRP:₩!DH" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf 명령을 실행합니다.

1단계에서 예상대로 출력되지 않으면 이 명령을 실행합니다.

이 명령은 DH 및 DHE 키 교환 메서드를 사용하는 모든 암호 교환을 사용하지 않도록 설정합니다.

3 명령 프롬프트에서 /etc/init.d/apache2 restart 명령을 실행하여 Apache2 서버를 다시 시작합니다.

4 DH를 다시 사용하도록 설정하려면 명령 프롬프트에서 sed -i "/^[^#]*SSLCipherSuite/c₩SSLCipherSuite kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES:₩!aNULL₩!ADH:₩!EXP:₩!MD5:₩!3DES:₩!CAMELLIA:₩!PSK:₩!SRP" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf 명령을 실행하여 암호 그룹에서 !DH를 제거합니다.

5 명령 프롬프트에서 /etc/init.d/apache2 restart 명령을 실행하여 Apache2 서버를 다시 시작합니다.

GemFire TLS 핸들러에 있는 암호 그룹의 올바른 사용 확인

보안을 최대화하기 위해 GemFire TLS 핸들러에 있는 암호 그룹의 올바른 사용을 확인하십시오.

프로시저

1 암호 그룹이 사용하도록 설정되었는지 확인하려면 각 노드에서 다음 명령을 실행하여 프로토콜이 사용하도록 설정되었는지 확인합니다.

grep cluster-ssl-ciphers /usr/lib/vmware-vcops/user/conf/gemfire.properties | grep -v '#'

grep cluster-ssl-ciphers /usr/lib/vmware-vcops/user/conf/gemfire.native.properties | grep -v '#'

grep cluster-ssl-ciphers /usr/lib/vmware-vcops/user/conf/gemfire.locator.properties | grep -v '#'

2 올바른 암호 그룹을 구성합니다.

a *URL*/admin에서 관리자 사용자 인터페이스로 이동합니다.

b 클러스터를 오프라인으로 전환하려면 **오프라인으로 전환**을 클릭합니다.

c 올바른 암호 그룹을 구성하려면 다음 명령을 실행합니다.

```
sed -i "/^[^#]*cluster-ssl-ciphers/ c₩cluster-ssl-
ciphers=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256" /usr/lib/vmware-
vcops/user/conf/gemfire.properties

sed -i "/^[^#]*cluster-ssl-ciphers/ c₩cluster-ssl-
ciphers=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256" /usr/lib/vmware-
vcops/user/conf/gemfire.native.properties

sed -i "/^[^#]*cluster-ssl-ciphers/ c₩cluster-ssl-
ciphers=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256" /usr/lib/vmware-
vcops/user/conf/gemfire.locator.properties
```

각 노드에 대해 이 단계를 반복합니다.

d *URL*/admin에서 관리자 사용자 인터페이스로 이동합니다.

e **온라인으로 전환**을 클릭합니다.

보호되어야 하는 애플리케이션 리소스

보안 모범 사례로, 애플리케이션 리소스가 보호되는지 확인합니다.

아래의 단계에 따라 애플리케이션 리소스가 보호되는지 확인합니다.

프로시저

1 Find / -path /proc -prune -o -type f -perm +6000 -ls 명령을 실행하여 파일에 올바르게 정의된 SUID 및 GUID 비트가 설정되어 있는지 확인합니다.

다음 목록이 나타납니다.

```
354131   24 -rwsr-xr-x   1 polkituser root 23176 /usr/lib/PolicyKit/polkit-set-default-helper
354126   20 -rwxr-sr-x   1 root     polkituser    19208 /usr/lib/PolicyKit/polkit-grant-helper
354125   20 -rwxr-sr-x   1 root     polkituser    19008 /usr/lib/PolicyKit/polkit-explicit-grant-helper
354130   24 -rwxr-sr-x   1 root     polkituser    23160 /usr/lib/PolicyKit/polkit-revoke-helper
354127   12 -rwsr-x---   1 root     polkituser    10744 /usr/lib/PolicyKit/polkit-grant-helper-pam
354128   16 -rwxr-sr-x   1 root     polkituser    14856 /usr/lib/PolicyKit/polkit-read-auth-helper
 73886   84 -rwsr-xr-x   1 root     shadow        77848 /usr/bin/chsh
 73888   88 -rwsr-xr-x   1 root     shadow        85952 /usr/bin/gpasswd
 73887   20 -rwsr-xr-x   1 root     shadow        19320 /usr/bin/expiry
 73890   84 -rwsr-xr-x   1 root     root          81856 /usr/bin/passwd
 73799  240 -rwsr-xr-x   1 root     root         238488 /usr/bin/sudo
 73889   20 -rwsr-xr-x   1 root     root          19416 /usr/bin/newgrp
 73884   92 -rwsr-xr-x   1 root     shadow        86200 /usr/bin/chage
 73885   88 -rwsr-xr-x   1 root     shadow        82472 /usr/bin/chfn
 73916   40 -rwsr-x---   1 root     trusted       40432 /usr/bin/crontab
296275   28 -rwsr-xr-x   1 root     root          26945 /usr/lib64/pt_chown
```

```
353804  816 -r-xr-sr-x   1 root     mail        829672 /usr/sbin/sendmail
278545   36 -rwsr-xr-x   1 root     root         35792 /bin/ping6
278585   40 -rwsr-xr-x   1 root     root         40016 /bin/su
278544   40 -rwsr-xr-x   1 root     root         40048 /bin/ping
278638   72 -rwsr-xr-x   1 root     root         69240 /bin/umount
278637  100 -rwsr-xr-x   1 root     root         94808 /bin/mount
475333   48 -rwsr-x---   1 root     messagebus      47912 /lib64/dbus-1/dbus-daemon-launch-helper
 41001   36 -rwsr-xr-x   1 root     shadow       35688 /sbin/unix_chkpwd
 41118   12 -rwsr-xr-x   1 root     shadow       10736 /sbin/unix2_chkpwd
```

2 find / -path */proc -prune -o -nouser -o -nogroup 명령을 실행하여 vApp의 모든 파일에 소유자가 있는지 확인합니다.

   결과가 표시되지 않으면 모든 파일에 소유자가 있는 것입니다.

3 find / -name "*.*" -type f -perm -a+w | xargs ls -ldb 명령을 실행하고 vApp의 모든 파일에 대한 사용 권한을 검토하여 모든 파일이 모두 쓰기 가능한(world writable) 파일이 아닌지 확인합니다.

   어떠한 파일에도 xx2 사용 권한이 포함되어서는 안 됩니다.

4 find / -path */proc -prune -o ! -user root -o -user admin -print 명령을 실행하여 올바른 사용자가 파일을 소유하고 있는지 확인합니다.

   결과가 표시되지 않으면 모든 파일이 root 또는 admin에 속하는 것입니다.

5 find /usr/lib/vmware-casa/ -type f -perm -o=w 명령을 실행하여 /usr/lib/vmware-casa/ 디렉토리의 파일이 모두 쓰기 가능한(world writable) 파일이 아닌지 확인합니다.

   결과가 표시되지 않아야 합니다.

6 find /usr/lib/vmware-vcops/ -type f -perm -o=w 명령을 실행하여 /usr/lib/vmware-vcops/ 디렉토리의 파일이 모두 쓰기 가능한(world writable) 파일이 아닌지 확인합니다.

   결과가 표시되지 않아야 합니다.

7 find /usr/lib/vmware-vcopssuite/ -type f -perm -o=w 명령을 실행하여 /usr/lib/vmware-vcopssuite/ 디렉토리의 파일이 모두 쓰기 가능한(world writable) 파일이 아닌지 확인합니다.

   결과가 표시되지 않아야 합니다.

PostgreSQL 클라이언트 인증 구성

클라이언트 인증을 사용하도록 시스템을 구성할 수 있습니다. 로컬 신뢰 인증을 사용하도록 시스템을 구성할 수 있습니다. 이렇게 하면 데이터베이스 수퍼유저를 포함한 모든 로컬 사용자가 비밀번호 없이 PostgreSQL 사용자로 연결할 수 있습니다. 강력한 방어를 구축하려는 경우와 모든 로컬 사용자 계정에 대한 높은 신뢰가 없는 경우에는 다른 인증 방법을 사용하십시오. 기본적으로는 md5 방법이 설정됩니다. 모든 로컬 및 호스트 연결에 md5가 설정되어 있는지 확인하십시오.

postgres 서비스 인스턴스에 대한 클라이언트 인증 구성 설정
은 /storage/db/vcops/vpostgres/data/pg_hba.conf에서 찾을 수 있습니다. 모든 로컬 및 호스트 연결에 md5가 설정되어 있는지 확인하십시오.

postgres-repl 서비스 인스턴스에 대한 클라이언트 인증 구성 설정은 /storage/db/vcops/vpostgres/repl/pg_hba.conf에서 찾을 수 있습니다. 모든 로컬 및 호스트 연결에 md5가 설정되어 있는지 확인하십시오.

참고 postgres 사용자 계정에 대한 클라이언트 구성 설정은 수정하지 마십시오.

Apache 구성

웹 디렉토리 찾아보기를 사용하지 않도록 설정

보안 모범 사례로, 사용자가 디렉토리를 찾아볼 수 없는지 확인합니다. 디렉토리 찾아보기가 가능한 경우 디렉토리 통과 공격에 노출될 위험이 커질 수 있습니다.

프로시저

- 모든 디렉토리에 대해 웹 디렉토리 찾아보기가 사용하지 않도록 설정되었는지 확인합니다.
  a 텍스트 편집기에서 /etc/apache2/default-server.conf 및 /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf 파일을 엽니다.
  b 각 <Directory> 목록에서 해당하는 태그에 대한 Indexes 옵션이 Options 줄에서 생략되어 있는지 확인합니다.

Apache2 서버의 샘플 코드 제거

Apache에는 두 개의 샘플 Common Gateway Interface(CGI) 스크립트인 printenv 및 test-cgi가 들어 있습니다. 운영 웹 서버에는 운영상 필요한 구성 요소만 포함되어야 합니다. 이러한 구성 요소로 공격자에게 시스템에 대한 중요한 정보가 노출될 수 있습니다.

보안 모범 사례로 cgi-bin 디렉토리에서 CGI 스크립트를 삭제합니다.

프로시저

- test-cgi 및 prinenv 스크립트를 제거하려면 rm /usr/share/doc/packages/apache2/test-cgi 및 rm /usr/share/doc/packages/apache2/printenv 명령을 실행합니다.

Apache2 서버의 서버 토큰 확인

시스템 강화 프로세스의 일환으로 Apache2 서버의 서버 토큰을 확인하십시오. HTTP 응답의 웹 서버 응답 머리글에는 여러 정보 필드를 포함할 수 있습니다. 정보에는 요청된 HTML 페이지, 웹 서버 유형 및 버전, 운영 체제 및 버전, 웹 서버와 연결된 포트가 포함됩니다. 이 정보는 악의적인 사용자에게 확장 도구의 사용 없이 중요한 정보를 제공합니다.

지시문 ServerTokens는 Prod로 설정해야 합니다. 예를 들면 ServerTokens Prod입니다. 이 지시문은 클라이언트에 다시 전송되는 서버의 응답 머리글 필드에 운영 체제 설명 및 컴파일된 모듈 정보를 포함할지 여부를 제어합니다.

프로시저

1. 서버 토큰을 확인하려면 cat /etc/apache2/sysconfig.d/global.conf | grep ServerTokens 명령을 실행합니다.
2. ServerTokens OS를 ServerTokens Prod로 수정하려면 sed -i 's/₩(ServerTokens₩s₩+₩)OS/₩1Prod/g' /etc/apache2/sysconfig.d/global.conf 명령을 실행합니다.

Apache2 서버의 Trace 메서드 사용 안 함

표준 운영 작업에서 진단을 사용하면 발견되지 않은 취약점이 나타나 데이터가 손상될 수 있습니다. 데이터가 잘못된 사용을 방지하기 위해 HTTP Trace 메서드를 사용하지 않도록 설정하십시오.

프로시저

1. Apache2 서버의 Trace 메서드를 확인하려면 grep TraceEnable /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf 명령을 실행합니다.
2. Apache2 서버의 Trace 메서드를 사용하지 않도록 설정하려면 sed -i "/^[^#]*TraceEnable/c₩TraceEnable off" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf 명령을 실행합니다.

구성 모드를 사용하지 않도록 설정

Best Practice로 vRealize Operations Manager를 설치, 구성 또는 유지 관리할 때 구성 또는 설정을 수정하여 설치 관련 문제 해결 및 디버깅을 사용하도록 설정할 수 있습니다.

변경한 사항이 제대로 보호되는지 확인하기 위해 이러한 변경 사항 각각에 대해 카탈로그를 작성하고 감사합니다. 구성 변경 사항이 제대로 보호되는지 확실치 않은 경우 변경 사항을 프로덕션 환경에 적용하지 마십시오.

필요하지 않은 소프트웨어 구성 요소 관리

보안 위험을 줄이려면 vRealize Operations Manager 호스트 시스템에서 필요하지 않은 소프트웨어를 제거하거나 구성하십시오.

제거하지 않은 모든 소프트웨어는 제조업체의 권장 사항 및 보안 모범 사례에 따라 구성하여 보안 침해가 발생할 가능성을 최소화하십시오.

USB 대량 스토리지 처리기 보안

USB 대량 스토리지 처리기에 보안을 적용하여 기본적으로 vRealize 어플라이언스에 로드되지 않도록 하고 vRealize 어플라이언스에서 USB 디바이스 처리기로 사용하는 일이 없도록 하십시오. 잠재적 공격자가 이 처리기를 악용하여 악성 소프트웨어를 설치할 수 있습니다.

프로시저

1. 텍스트 편집기에서 /etc/modprobe.conf.local 파일을 엽니다.
2. install usb-storage /bin/true 줄이 파일에 나타나는지 확인합니다.

3 파일을 저장하고 닫습니다.

Bluetooth 프로토콜 처리기 보안

vRealize 어플라이언스의 Bluetooth 프로토콜 처리기에 보안을 적용하여 잠재적 공격자가 악용할 수 없도록 하십시오.

Bluetooth 프로토콜을 네트워크 스택에 바인딩하는 작업은 불필요하며 호스트의 공격 취약성이 증가할 수 있습니다. Bluetooth 프로토콜 처리기 모듈이 기본적으로 vRealize 어플라이언스에 로드되지 않도록 하십시오.

프로시저

1 텍스트 편집기에서 /etc/modprobe.conf.local 파일을 엽니다.

2 install bluetooth /bin/true 줄이 이 파일에 나타나는지 확인합니다.

3 파일을 저장하고 닫습니다.

SCTP(Stream Control Transmission Protocol) 보안

SCTP(Stream Control Transmission Protocol) 모듈이 기본적으로 vRealize 어플라이언스에 로드되지 않도록 하십시오. 잠재적 공격자가 이 프로토콜을 악용하여 시스템을 손상시킬 수 있습니다.

절대적으로 필요하지 않은 한 SCTP 모듈을 로드하지 않도록 시스템을 구성합니다. SCTP는 사용되지 않는 IETF 표준 전송 계층 프로토콜입니다. 이 프로토콜을 네트워크 스택에 바인딩하면 호스트의 공격 취약성이 증가합니다. 권한이 없는 로컬 프로세스가 이 프로토콜을 사용하여 소켓을 열면 커널이 프로토콜 처리기를 동적으로 로드할 수 있습니다.

프로시저

1 텍스트 편집기에서 /etc/modprobe.conf.local 파일을 엽니다.

2 다음 줄이 이 파일에 나타나는지 확인합니다.

```
install sctp /bin/true
```

3 파일을 저장하고 닫습니다.

DCCP(Datagram Congestion Control Protocol) 보안

시스템 강화 작업의 일부로, DCCP(Datagram Congestion Control Protocol) 모듈이 기본적으로 vRealize 어플라이언스에 로드되지 않도록 하십시오. 잠재적 공격자가 이 프로토콜을 악용하여 시스템을 손상시킬 수 있습니다.

절대적으로 필요하지 않은 한 DCCP(Datagram Congestion Control Protocol) 모듈이 로드되지 않도록 해야 합니다. DCCP는 제안된 전송 계층 프로토콜이며 사용되지 않습니다. 이 프로토콜을 네트워크 스택에 바인딩하면 호스트의 공격 취약성이 증가합니다. 권한이 없는 로컬 프로세스가 이 프로토콜을 사용하여 소켓을 열면 커널이 프로토콜 처리기를 동적으로 로드할 수 있습니다.

프로시저

1 텍스트 편집기에서 /etc/modprobe.conf.local 파일을 엽니다.

2 DCCP 줄이 파일에 나타나는지 확인합니다.

```
install dccp /bin/true
install dccp_ipv4 /bin/true
install dccp_ipv6 /bin/true
```

3 파일을 저장하고 닫습니다.

RDS(Reliable Datagram Sockets) 프로토콜 보안

시스템 강화 작업의 일부로, RDS(Reliable Datagram Sockets) 프로토콜이 기본적으로 vRealize 어플라이언스에 로드되지 않도록 하십시오. 잠재적 공격자가 이 프로토콜을 악용하여 시스템을 손상시킬 수 있습니다.

RDS 프로토콜을 네트워크 스택에 바인딩하면 호스트의 공격 취약성이 증가합니다. 권한이 없는 로컬 프로세스가 이 프로토콜을 사용하여 소켓을 열면 커널이 프로토콜 처리기를 동적으로 로드할 수 있습니다.

프로시저

1 텍스트 편집기에서 /etc/modprobe.conf.local 파일을 엽니다.

2 install rds /bin/true 줄이 이 파일에 나타나는지 확인합니다.

3 파일을 저장하고 닫습니다.

TIPC(Transparent Inter-Process Communication) 프로토콜 보안

시스템 강화 작업의 일부로, TIPC(Transparent Inter-Process Communication) 프로토콜이 기본적으로 가상 어플라이언스 호스트 시스템에 로드되지 않도록 하십시오. 잠재적 공격자가 이 프로토콜을 악용하여 시스템을 손상시킬 수 있습니다.

TIPC프로토콜을 네트워크 스택에 바인딩하면 호스트의 공격 취약성이 증가합니다. 권한이 없는 로컬 프로세스가 이 프로토콜을 사용하여 소켓을 열면 커널이 프로토콜 처리기를 동적으로 로드할 수 있습니다.

프로시저

1 텍스트 편집기에서 /etc/modprobe.conf.local 파일을 엽니다.

2 install tipc /bin/true 줄이 이 파일에 나타나는지 확인합니다.

3 파일을 저장하고 닫습니다.

IPX(Internet Packet Exchange) 프로토콜 보안

IPX(Internet Packet Exchange) 프로토콜이 기본적으로 vRealize 어플라이언스에 로드되지 않도록 하십시오. 잠재적 공격자가 이 프로토콜을 악용하여 시스템을 손상시킬 수 있습니다.

절대적으로 필요하지 않은 한 IPX 프로토콜 모듈이 로드되지 않도록 해야 합니다. IPX 프로토콜은 더 이상 사용되지 않는 네트워크 계층 프로토콜입니다. 이 프로토콜을 네트워크 스택에 바인딩하면 호스트의 공격 취약성이 증가합니다. 권한이 없는 로컬 프로세스가 이 프로토콜을 사용하여 소켓을 열면 시스템이 프로토콜 처리기를 동적으로 로드할 수 있습니다.

프로시저

1 텍스트 편집기에서 /etc/modprobe.conf.local 파일을 엽니다.

2 install ipx /bin/true 줄이 이 파일에 나타나는지 확인합니다.

3 파일을 저장하고 닫습니다.

Appletalk 프로토콜 보안

Appletalk 프로토콜이 기본적으로 vRealize 어플라이언스에 로드되지 않도록 하십시오. 잠재적 공격자가 이 프로토콜을 악용하여 시스템을 손상시킬 수 있습니다.

절대적으로 필요하지 않은 한 Appletalk 프로토콜 모듈이 로드되지 않도록 해야 합니다. 이 프로토콜을 네트워크 스택에 바인딩하면 호스트의 공격 취약성이 증가합니다. 권한이 없는 로컬 프로세스가 이 프로토콜을 사용하여 소켓을 열면 시스템이 프로토콜 처리기를 동적으로 로드할 수 있습니다.

프로시저

1 텍스트 편집기에서 /etc/modprobe.conf.local 파일을 엽니다.

2 install appletalk /bin/true 줄이 이 파일에 나타나는지 확인합니다.

3 파일을 저장하고 닫습니다.

DECnet 프로토콜 보안

DECnet 프로토콜이 기본적으로 시스템에 로드되지 않도록 하십시오. 잠재적 공격자가 이 프로토콜을 악용하여 시스템을 손상시킬 수 있습니다.

절대적으로 필요하지 않은 한 DECnet 프로토콜 모듈이 로드되지 않도록 해야 합니다. 이 프로토콜을 네트워크 스택에 바인딩하면 호스트의 공격 취약성이 증가합니다. 권한이 없는 로컬 프로세스가 이 프로토콜을 사용하여 소켓을 열면 시스템이 프로토콜 처리기를 동적으로 로드할 수 있습니다.

프로시저

1 텍스트 편집기에서 DECnet 프로토콜 /etc/modprobe.conf.local 파일을 엽니다.

2 install decnet /bin/true 줄이 이 파일에 나타나는지 확인합니다.

3 파일을 저장하고 닫습니다.

방화벽 모듈 보안

방화벽 모듈이 기본적으로 vRealize 어플라이언스에 로드되지 않도록 하십시오. 잠재적 공격자가 이 프로토콜을 악용하여 시스템을 손상시킬 수 있습니다.

절대적으로 필요하지 않은 한 방화벽 모듈이 로드되지 않도록 해야 합니다.

프로시저

1 텍스트 편집기에서 /etc/modprobe.conf.local 파일을 엽니다.

2 install ieee1394 /bin/true 줄이 이 파일에 나타나는지 확인합니다.

3 파일을 저장하고 닫습니다.

커널 메시지 로깅

/etc/sysctl.conf 파일에서 kernel.printk 규격은 커널 인쇄 로깅 규격을 지정합니다.

다음 4개의 값이 지정됩니다.

- console loglevel. 콘솔에 인쇄되는 가장 낮은 우선 순위의 메시지입니다.
- default loglevel. 특정 로그 수준이 없는 가장 낮은 수준의 메시지입니다.
- 콘솔 로그 수준에서 가장 낮은 수준입니다.
- 콘솔 로그 수준의 기본값입니다.

값당 가능한 항목은 8개입니다.

- define KERN_EMERG "<0>" /* system is unusable */
- define KERN_ALERT "<1>" /* action must be taken immediately */
- define KERN_CRIT "<2>" /* critical conditions */
- define KERN_ERR "<3>" /* error conditions */
- define KERN_WARNING "<4>" /* warning conditions */
- define KERN_NOTICE "<5>" /* normal but significant condition */
- define KERN_INFO "<6>" /* informational */
- define KERN_DEBUG "<7>" /* debug-level messages */

kernel.printk 값을 **3 4 1 7**로 설정하고 kernel.printk=3 4 1 7 줄이 /etc/sysctl.conf 파일에 있는지 확인합니다.

Linux 설치 배포

NTP(Network Time Protocol) 서비스를 사용하도록 설정하고 시스템이 안전한 전송 채널을 통해 배포되도록 할 수 있습니다.

NTP 서비스를 사용하도록 설정

시간 소스가 중요한 경우 호스트 시간 동기화를 사용하지 않도록 설정하고 NTP(네트워크 시간 프로토콜)을 사용할 수 있습니다. 운영 환경에서 NTP를 사용하면 사용자 작업을 정확하게 추적하고 감사 및 로그 기록을 정확하게 유지하여 잠재적인 악의적 공격 및 침입을 인지할 수 있습니다.

NTP 대몬은 어플라이언스에 포함되며 동기화된 시간 서비스를 제공하는 데 사용됩니다. NTP 구성 파일은 /etc/ntp.conf에서 찾을 수 있습니다.

전송 중인 데이터의 TLS

보안 모범 사례로, 시스템이 보안 전송 채널을 통해 배포되는지 확인합니다.

vRealize Operations Manager에 대한 강력한 프로토콜 구성

SSLv2 및 SSLv3과 같은 프로토콜은 SSLv2 및 SSLv3을 포함하여 더 이상 안전한 것으로 간주되지 않습니다. 전송 계층 보호를 위한 보안 모범 사례로, TLS 프로토콜에 대한 지원만 제공합니다.

운영 전에 SSLv2 및 SSLv3이 사용하지 않도록 설정되었는지 확인해야 합니다.

강력한 암호를 사용하도록 vRealize Operations Manager 구성

TLS 세션에 사용되는 암호화 강도는 서버와 브라우저 사이에 협상되는 암호화 암호에 따라 결정됩니다. 강력한 암호만 선택되도록 하려면 서버가 취약한 암호를 사용하지 않도록 수정해야 합니다. 또한, 적합한 순서로 암호를 구성해야 합니다. 서버가 강력한 암호만 지원하고 충분히 큰 키 크기를 사용하도록 구성해야 합니다.

취약한 암호를 사용하지 않도록 설정

NULL 암호 모음, NULL 또는 eNULL과 같은 인증을 제공하지 않는 암호 모음을 사용하지 않도록 설정합니다. 암호 모음을 메시지 가로채기(man-in-the-middle) 공격에 취약하도록 만드는 인증은 없습니다.

익명 Diffie-Hellman 키 교환(ADH), 내보내기 수준 암호(EXP, DES를 포함하는 암호), 128비트보다 작은 키 크기(페이로드 트래픽 암호화용), 페이로드 트래픽에 대한 해싱으로 MD5 사용, IDEA 암호 모음 및 RC4 암호 모음도 모두 공격에 취약하므로 사용하지 않도록 설정해야 합니다.

Apache HTTPD 핸들러에서 취약한 암호를 사용하지 않도록 설정

취약한 암호를 사용하지 않도록 설정하고 Apache HTTPD 핸들러에 사용된 강력한 암호를 사용하도록 설정합니다. 메시지 가로채기(man-in-the-middle) 공격을 방지하려면 vRealize Operations Manager의 Apache HTTPD 핸들러 암호를 허용 가능한 암호 목록과 비교하여 검토하고 취약한 것으로 간주되는 모든 암호를 사용하지 않도록 설정합니다.

프로시저

1. 텍스트 편집기에서 /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf 파일을 엽니다.
2. 파일에 SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH:@STRENGTH 줄이 포함되어 있는지 확인합니다.
3. 파일을 저장한 후 닫습니다.

Diffie-Hellman 키 교환을 사용하도록 설정

Diffie-Hellman 키 교환에는 여러 약점이 있습니다. DH, DHE 및 EDH를 포함하는 모든 암호 모음을 사용하지 않도록 설정해야 합니다. 이러한 암호 모음은 기본적으로 사용하지 않도록 설정됩니다. 이들 암호 모음은 사용해야 할 경우 사용하도록 설정할 수 있습니다.

프로시저

1. /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf 파일을 엽니다.
2. SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH:@STRENGTH 줄을 찾습니다.
3. 줄이 SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:@STRENGTH가 되도록 !DH:를 제거합니다.
4. 파일을 저장한 후 닫습니다.

구성 모드를 사용하지 않도록 설정

Best Practice로 vRealize Operations Manager를 설치, 구성 또는 유지 관리할 때 구성 또는 설정을 수정하여 설치 관련 문제 해결 및 디버깅을 사용하도록 설정할 수 있습니다.

변경한 사항이 제대로 보호되는지 확인하기 위해 이러한 변경 사항 각각에 대해 카탈로그를 작성하고 감사합니다. 구성 변경 사항이 제대로 보호되는지 확실치 않은 경우 변경 사항을 프로덕션 환경에 적용하지 마십시오.

호스트 서버의 보안 구성 확인

vRealize Operations Manager가 안전하게 작동하려면 강화 작업을 보호하고 확인해야 합니다.

자세한 내용은 조직의 보안 정책에 따라 Red Hat Enterprise Linux 6 강화 지침을 참조하십시오.

Endpoint Operations Management 에이전트

Endpoint Operations Management 에이전트를 설치하면 에이전트 기반 검색 및 모니터링 기능이 vRealize Operations Manager에 추가됩니다.

Endpoint Operations Management 에이전트는 호스트에 직접 설치되고 Endpoint Operations Management 서버와 동일한 신뢰 수준이거나 그렇지 않을 수 있습니다. 따라서, 에이전트가 안전하게 설치되었는지 확인해야 합니다.

Endpoint Operations Management 에이전트 실행에 대한 보안 모범 사례

사용자 계정을 사용할 때는 특정 보안 모범 사례를 따라야 합니다.

- 자동 설치의 경우 AGENT_HOME/conf/agent.properties 파일에 저장된 자격 증명 및 서버 인증서 지문을 제거합니다.
- Endpoint Operations Management 에이전트 등록을 위해 예약된 vRealize Operations Manager 사용자 계정을 사용합니다. 자세한 내용은 vRealize Operations Manager 도움말에서 vRealize Operations Manager의 "역할 및 권한" 항목을 참조하십시오.

- 설치가 완료되면 에이전트 등록에 사용한 vRealize Operations Manager 사용자 계정을 사용하지 않도록 설정합니다. 에이전트 관리 작업을 수행하려면 사용자 액세스를 사용하도록 설정해야 합니다. 자세한 내용은 vRealize Operations Manager 도움말에서 vRealize Operations Manager의 사용자 및 그룹 구성 항목을 참조하십시오.
- 에이전트를 실행하는 시스템이 손상된 경우 vRealize Operations Manager 사용자 인터페이스에서 에이전트 리소스를 제거하여 에이전트 인증서를 해지할 수 있습니다. 자세한 내용은 에이전트 해지 관련 섹션을 참조하십시오.

에이전트 기능에 필요한 최소 사용 권한

서비스를 설치하고 수정할 수 있는 사용 권한이 필요합니다. 실행 중인 프로세스를 검색하려면 에이전트를 실행할 때 사용한 사용자 계정에 프로세스 및 프로그램에 액세스하는 데 필요한 권한도 있어야 합니다. Windows 운영 체제 설치의 경우 서비스를 설치하고 수정할 수 있는 사용 권한이 필요합니다. Linux 설치에서 RPM 설치 프로그램을 사용하여 에이전트를 설치하는 경우 에이전트를 서비스로 설치할 수 있는 사용 권한이 필요합니다.

vRealize Operations Manager 서버에 에이전트를 등록하려면 최소한 에이전트 관리자 역할이 부여된 사용자의 자격 증명이 필요하며, 이때 시스템 내 개체에 대해 어떠한 권한도 할당할 필요는 없습니다.

Linux 기반 플랫폼 파일 및 사용 권한

Endpoint Operations Management 에이전트를 설치한 후 소유자는 에이전트를 설치한 사용자입니다.

Endpoint Operations Management 에이전트를 설치한 사용자가 TAR 파일을 추출하거나 RPM을 설치하면 설치 디렉토리 및 파일 사용 권한(예: 600 및 700)이 소유자로 설정됩니다.

참고 ZIP 파일을 추출할 경우 사용 권한이 올바르게 적용되지 않을 수 있습니다. 사용 권한이 올바른지 확인하십시오.

에이전트에서 생성하고 기록하는 모든 파일에는 700 사용 권한이 할당되고 소유자는 에이전트를 실행하는 사용자가 됩니다.

표 3-1. Linux 파일 및 사용 권한

디렉토리 또는 파일	사용 권한	그룹 또는 사용자	읽기	쓰기	실행
agent directory/bin	700	소유자	예	예	예
		그룹	아니요	아니요	아니요
		모두	아니요	아니요	아니요
agent directory/conf	700	소유자	예	예	예
		그룹	아니요	아니요	아니요
		모두	아니요	아니요	아니요
agent directory/log	700	소유자	예	예	아니요
		그룹	아니요	아니요	아니요
		모두	아니요	아니요	아니요

표 3-1. Linux 파일 및 사용 권한 (계속)

디렉토리 또는 파일	사용 권한	그룹 또는 사용자	읽기	쓰기	실행
agent directory/data	700	소유자	예	예	예
		그룹	아니요	아니요	아니요
		모두	아니요	아니요	아니요
agent directory/bin/ep-agent.bat	600	소유자	예	예	아니요
		그룹	아니요	아니요	아니요
		모두	아니요	아니요	아니요
agent directory/bin/ep-agent.sh	700	소유자	예	예	예
		그룹	아니요	아니요	아니요
		모두	아니요	아니요	아니요
agent directory/conf/* (conf 디렉토리의 모든 파일)	600	소유자	예	예	예
		그룹	아니요	아니요	아니요
		모두	아니요	아니요	아니요
agent directory/log/* (log 디렉토리의 모든 파일)	600	소유자	예	예	아니요
		그룹	아니요	아니요	아니요
		모두	아니요	아니요	아니요
agent directory/data/* (data 디렉토리의 모든 파일)	600	소유자	예	예	아니요
		그룹	아니요	아니요	아니요
		모두	아니요	아니요	아니요

Windows 기반 플랫폼 파일 및 사용 권한

Windows 기반 Endpoint Operations Management 에이전트 설치 시 에이전트를 설치하려면 사용자에게 서비스를 설치하고 수정할 수 있는 사용 권한이 있어야 합니다.

Endpoint Operations Management 에이전트를 설치한 후 모든 하위 디렉토리 및 파일이 포함된 설치 폴더에는 SYSTEM, 관리자 그룹 및 설치 사용자만 액세스할 수 있어야 합니다. ep-agent.bat를 사용하여 Endpoint Operations Management 에이전트를 설치하는 경우 강화 프로세스가 성공하는지 확인해야 합니다. 에이전트를 설치하는 사용자는 모든 오류 메시지를 기록하는 것이 좋습니다. 강화 프로세스가 실패할 경우 사용자는 이러한 사용 권한을 수동으로 적용할 수 있습니다.

표 3-2. Windows 파일 및 사용 권한

디렉토리 또는 파일	그룹 또는 사용자	모든 권한	수정	읽기 및 실행	읽기	쓰기
<agent directory>/bin	SYSTEM	예	-	-	-	-
	관리자	예	-	-	-	-
	설치 사용자	예	-	-	-	-
	사용자		-	-	-	-

표 3-2. Windows 파일 및 사용 권한 (계속)

디렉토리 또는 파일	그룹 또는 사용자	모든 권한	수정	읽기 및 실행	읽기	쓰기
<agent directory>/conf	SYSTEM	예	–	–	–	–
	관리자	예	–	–	–	–
	설치 사용자	예	–	–	–	–
	사용자		–	–	–	–
<agent directory>/log	SYSTEM	예	–	–	–	–
	관리자	예	–	–	–	–
	설치 사용자	예	–	–	–	–
	사용자		–	–	–	–
<agent directory>/data	SYSTEM	예	–	–	–	–
	관리자	예	–	–	–	–
	설치 사용자	예	–	–	–	–
	사용자		–	–	–	–
<agent directory>/bin/hq-agent.bat	SYSTEM	예	–	–	–	–
	관리자	예	–	–	–	–
	설치 사용자	예	–	–	–	–
	사용자		–	–	–	–
<agent directory>/bin/hq-agent.sh	SYSTEM	예	–	–	–	–
	관리자	예	–	–	–	–
	설치 사용자	예	–	–	–	–
	사용자		–	–	–	–
<agent directory>/conf/* (conf 디렉토리의 모든 파일)	SYSTEM	예	–	–	–	–
	관리자	예	–	–	–	–
	설치 사용자	예	–	–	–	–
	사용자		–	–	–	–
<agent directory>/log/* (log 디렉토리의 모든 파일)	SYSTEM	예	–	–	–	–
	관리자	예	–	–	–	–
	설치 사용자	예	–	–	–	–
	사용자		–	–	–	–
<agent directory>/data/* (data 디렉토리의 모든 파일)	SYSTEM	예	–	–	–	–
	관리자	예	–	–	–	–
	설치 사용자	예	–	–	–	–
	사용자		–	–	–	–

에이전트 호스트의 열린 포트

에이전트 프로세스는 127.0.0.1:2144 및 127.0.0.1:32000의 구성 가능한 2개 포트에서 명령을 수신합니다. 이러한 포트는 임의로 할당될 수 있으므로 정확한 포트 번호를 다를 수 있습니다. 에이전트는 외부 인터페이스에 포트를 열지 않습니다.

표 3-3. 필요한 최소 포트

포트	프로토콜	방향	주석
443	TCP	송신	에이전트에서 HTTP, TCP 또는 ICMP를 통한 송신 연결에 사용됩니다.
2144	TCP	수신	내부 전용입니다. 구성 가능합니다. 에이전트와 에이전트를 로드하고 구성하는 명령줄 사이의 프로세스 간 통신에 사용됩니다. 에이전트 프로세스는 이 포트를 통해 수신합니다. **참고** 포트 번호는 임의로 할당되므로 다를 수 있습니다.
32000	TCP	수신	내부 전용입니다. 구성 가능합니다. 에이전트와 에이전트를 로드하고 구성하는 명령줄 사이의 프로세스 간 통신에 사용됩니다. 에이전트 프로세스는 이 포트를 통해 수신합니다. **참고** 포트 번호는 임의로 할당되므로 다를 수 있습니다.

에이전트 해지

실행 중인 에이전트가 있는 시스템이 손상된 경우와 같이 어떤 이유로든 에이전트를 해지해야 하는 경우 시스템에서 에이전트 리소스를 삭제할 수 있습니다. 후속 요청은 검증에 실패하게 됩니다.

vRealize Operations Manager 사용자 인터페이스에서 에이전트 리소스를 제거하여 에이전트 인증서를 해지합니다. 자세한 내용은 에이전트 리소스 제거 항목을 참조하십시오.

시스템이 다시 안전해지면 에이전트를 복구할 수 있습니다. 자세한 내용은 에이전트 리소스 복구 항목을 참조하십시오.

에이전트 리소스 제거

vRealize Operations Manager에서 에이전트 리소스를 제거하여 에이전트 인증서를 해지할 수 있습니다.

필수 조건

이전에 기록된 메트릭 데이터와 리소스의 연속성을 보존하려면 리소스 세부 정보에 표시된 Endpoint Operations Management 에이전트 토큰을 기록합니다.

프로시저

1. vRealize Operations Manager 사용자 인터페이스에서 Inventory Explorer로 이동합니다.
2. 어댑터 유형 트리를 엽니다.
3. EP Ops 어댑터 목록을 엽니다.
4. **EP Ops 에이전트 – *HOST_DNS_NAME***을 선택합니다.

5 **개체 편집**을 클릭합니다.

6 에이전트 ID(에이전트 토큰 문자열)를 기록합니다.

7 [개체 편집] 대화 상자를 닫습니다.

8 **EP Ops 에이전트 - *HOST_DNS_NAME***을 선택하고 **개체 삭제**를 클릭합니다.

에이전트 리소스 복구

시스템의 보안 상태가 회복되면 해지한 에이전트를 복구할 수 있습니다. 복구된 에이전트는 기간별 데이터의 손실 없이 동일한 리소스를 계속해서 보고합니다. 에이전트를 복구하려면 에이전트 리소스를 제거하기 전에 기록한 동일한 토큰을 사용하여 새 Endpoint Operations Management 토큰 파일을 생성해야 합니다. 에이전트 리소스 제거 섹션을 참조하십시오.

필수 조건

- Endpoint Operations Management 토큰 문자열을 기록했는지 확인합니다.
- vRealize Operations Manager 서버에서 에이전트 리소스를 제거하기 전에 기록한 리소스 토큰을 사용합니다.
- 에이전트 관리 권한이 있는지 확인하십시오.

프로시저

1 에이전트를 실행한 사용자가 포함된 에이전트 토큰 파일을 생성합니다.

예를 들어 명령을 실행하여 123-456-789 토큰이 포함된 토큰이 포함된 토큰 파일을 생성합니다.

- Linux의 경우

  ```
  echo 123-456-789 > /etc/epops/epops-token
  ```

- Windows의 경우

  ```
  echo 123-456-789 > %PROGRAMDATA%₩VMware₩Ep Ops Agent₩epops-token
  ```

이 예에서 토큰 파일은 해당 플랫폼의 기본 토큰 위치에 기록됩니다.

2 새 에이전트를 설치하고 vRealize Operations Manager 서버에 등록합니다. 토큰 파일에 삽입한 토큰을 에이전트가 로드하는지 확인합니다.

이 작업을 수행하려면 에이전트 관리 권한이 있어야 합니다.

에이전트 인증서 해지 및 인증서 업데이트

재발급 흐름은 에이전트에서 setup 명령줄 인수를 사용하여 시작됩니다. 이미 등록된 에이전트에서 setup 명령줄 인수 ep-agent.sh setup을 사용하여 필요한 자격 증명을 입력하면 새 registerAgent 명령이 서버로 전송됩니다.

서버가 이미 등록된 에이전트를 감지하여 다른 에이전트 리소스를 생성하지 않고 새 클라이언트 인증서를 에이전트에 전송합니다. 에이전트 측에서는 새 클라이언트 인증서가 이전 인증서를 대체합니다. 서버 인증서가 수정된 경우 ep-agent.sh setup 명령을 실행하면 새 인증서를 신뢰할지를 묻는 메시지가 표시됩니다. 프로세스가 자동으로 실행되도록 하려면 ep-agent.sh setup 명령을 실행하기 전에 agent.properties 파일에 새 서버 인증서 지문을 입력하면 됩니다.

필수 조건

에이전트 권한을 관리하여 인증서를 해지하고 업데이트합니다.

프로시저

- Linux 기반 운영 체제에서는 에이전트 호스트에서 ep-agent.sh setup 명령을 실행합니다. Windows 기반 운영 체제에서는 ep-agent.bat setup 명령을 실행합니다.

  에이전트가 서버 인증서가 수정된 것을 감지한 경우 메시지가 표시됩니다. 새 인증서를 신뢰하고 해당 인증서가 유효한 경우 인증서를 수락합니다.

Endpoint Operations Management 에이전트 패치 적용 및 업데이트

필요한 경우, 새로운 Endpoint Operations Management 에이전트 번들을 vRealize Operations Manager 릴리스와 별개로 사용할 수 있습니다.

Endpoint Operations Management 에이전트에 대해서는 패치 또는 업데이트가 제공되지 않습니다. 최신 보안 프로그램을 포함하는 에이전트의 사용 가능한 최신 버전을 설치해야 합니다. 중요 보안 프로그램은 VMware 보안 공지 지침에 따라 전달될 예정입니다. 보안 공지의 항목을 참조하십시오.

추가 보안 구성 작업

서버 사용자 계정을 확인하고 호스트 서버에서 불필요한 애플리케이션을 삭제합니다. 불필요한 포트를 차단하고 호스트 서버에서 실행 중인 불필요한 서비스를 사용하지 않도록 설정합니다.

서버 사용자 계정 설정 확인

로컬 및 도메인 사용자 계정 및 설정에 불필요한 사용자 계정이 없는지 확인하는 것이 좋습니다.

애플리케이션의 기능과 관련되지 않은 모든 사용자 계정을 관리, 유지 보수 및 문제 해결에 필요한 계정으로 제한합니다. 도메인 사용자 계정의 원격 액세스를 서버를 유지하는 데 필요한 최소한의 액세스로 제한합니다. 이러한 계정을 엄격하게 제어하고 감사합니다.

불필요한 애플리케이션 삭제 및 사용하지 않도록 설정

호스트 서버에서 불필요한 애플리케이션을 삭제합니다. 각각의 부가적이며 불필요한 애플리케이션은 취약점이 알려지지 않았거나 취약점에 대한 패치가 없으므로 노출 위험이 증가합니다.

불필요한 포트 및 서비스를 사용하지 않도록 설정

호스트 서버의 방화벽에서 트래픽을 허용하는 열려 있는 포트 목록을 확인합니다.

이 문서의 포트 및 프로토콜 구성 섹션에서 vRealize Operations Manager에 대한 최소 요구 사항으로 나와 있지 않거나 불필요한 모든 포트를 차단합니다. 또한, 호스트 서버에서 실행 중인 서비스를 감사하고 불필요한 서비스를 사용하지 않도록 설정합니다.

4 네트워크 보안 및 보안 통신

보안 모범 사례로, VMware 가상 어플라이언스 및 호스트 시스템의 네트워크 통신 설정을 검토하고 편집합니다. 또한 vRealize Operations Manager의 최소 수신 및 송신 포트 수도 구성해야 합니다.

이 장에서는 다음 주제에 대해 설명합니다.

- 가상 애플리케이션 설치에 대한 네트워크 설정 구성
- 포트 및 프로토콜 구성

가상 애플리케이션 설치에 대한 네트워크 설정 구성

VMware 가상 어플라이언스 및 호스트 시스템이 안전한 필수 통신만 허용하도록 하려면 해당 네트워크 통신 설정을 검토하고 편집해야 합니다.

네트워크 인터페이스의 사용자 제어 방지

보안 모범 사례로, 권한이 있는 사용자만 네트워크 인터페이스 설정을 변경할 수 있도록 합니다. 사용자가 네트워크 인터페이스를 조작하면 네트워크 보안 메커니즘의 생략 또는 서비스 거부가 발생할 수 있습니다. 사용자가 네트워크 인터페이스를 제어할 수 있도록 구성되지 않았는지 확인하십시오.

프로시저

1. 사용자 제어 설정을 확인하려면 `#grep -i '^USERCONTROL=' /etc/sysconfig/network/ifcfg*` 명령을 실행합니다.
2. 각 인터페이스가 NO로 설정되어 있는지 확인합니다.

TCP 백로그의 대기열 크기 설정

보안 모범 사례로, VMware 어플라이언스 호스트 시스템에 기본 TCP 백로그 대기열 크기를 구성합니다. TCP 서비스 거부 공격을 방지하려면 TCP 백로그 대기열 크기에 해당하는 기본 크기를 설정합니다. 권장되는 기본 설정은 1280입니다.

프로시저

1. 각 VMware 어플라이언스 호스트 시스템에서 `# cat /proc/sys/net/ipv4/tcp_max_syn_backlog` 명령을 실행합니다.

2 TCP 백로그의 대기열 크기를 설정합니다.

a 텍스트 편집기에서 /etc/sysctl.conf 파일을 엽니다.

b 다음 항목을 파일에 추가하여 기본 TCP 백로그 대기열 크기를 설정합니다.

```
net.ipv4.tcp_max_syn_backlog=1280
```

c 변경 사항을 저장하고 파일을 닫습니다.

브로드캐스트 주소에 대한 ICMPv4 에코 거부

브로드캐스트 ICMP(Internet Control Message Protocol) 에코에 대한 응답은 증폭 공격에 대한 공격 벡터를 제공하며 악의적인 에이전트에 의한 네트워크 매핑을 가능하게 할 수 있습니다. ICMPv4 에코를 무시하도록 시스템을 구성하면 이러한 공격으로부터 보호할 수 있습니다.

프로시저

1 # cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts 명령을 실행하여 시스템이 ICMP 브로드캐스트 주소 에코 요청에 대한 응답을 전송하지 않는지 확인합니다.

2 ICMPv4 브로드캐스트 주소 에코 요청을 거부하도록 호스트 시스템을 구성합니다.

a 텍스트 편집기에서 /etc/sysctl.conf 파일을 엽니다.

b 이 항목에 대한 값이 1로 설정되어 있지 않은 경우 net.ipv4.icmp_echo_ignore_broadcasts=1 항목을 추가합니다.

c 변경 사항을 저장하고 파일을 닫습니다.

IPv4 프록시 ARP를 사용하지 않도록 호스트 시스템 구성

IPv4 프록시 ARP를 사용하면 시스템이 다른 인터페이스에 연결된 호스트를 대신하여 특정 인터페이스에서 ARP 요청에 대한 응답을 전송할 수 있습니다. 무단 정보 공유를 방지하려면 IPv4 프록시 ARP를 사용하지 않도록 설정해야 합니다. 연결된 네트워크 세그먼트 사이에 주소 정보가 누출되지 않도록 하려면 이 설정을 사용하지 않도록 지정하십시오.

프로시저

1 # grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp|egrep "default|all" 명령을 실행하여 프록시 ARP가 사용되지 않도록 설정되었는지 여부를 확인합니다.

2 IPv4 프록시 ARP를 사용하지 않도록 호스트 시스템을 구성합니다.

a 텍스트 편집기에서 /etc/sysctl.conf 파일을 엽니다.

b 값이 0으로 설정되어 있지 않은 경우 항목을 추가하거나 기존 항목을 이에 맞게 업데이트합니다. 값을 0로 설정합니다.

```
net.ipv4.conf.all.proxy_arp=0
net.ipv4.conf.default.proxy_arp=0
```

c 변경 사항을 저장하고 파일을 닫습니다.

IPv4 ICMP 리디렉션 메시지를 무시하도록 호스트 시스템 구성

보안 Best Practice로, 호스트 시스템이 IPv4 ICMP(Internet Control Message Protocol) 리디렉션 메시지를 무시하는지 확인합니다. 악의적인 ICMP 리디렉션 메시지는 메시지 가로채기(man-in-the-middle) 공격이 발생하도록 허용할 수 있습니다. 라우터는 ICMP 리디렉션 메시지를 사용하여 더욱 직접적인 경로가 특정 대상에 대해 존재함을 호스트에 알립니다. 이러한 메시지는 인증되지 않은 것이며, 호스트의 경로 테이블을 수정합니다.

프로시저

1 호스트 시스템에서 # grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects|egrep "default|all" 명령을 실행하여 호스트 시스템이 IPv4 리디렉션 메시지를 무시하는지 여부를 확인합니다.

2 IPv4 ICMP 리디렉션 메시지를 무시하도록 호스트 시스템을 구성합니다.

   a /etc/sysctl.conf 파일을 엽니다.

   b 값이 0로 설정되어 있지 않은 경우 다음 항목을 파일에 추가하거나 기존 항목을 이에 맞게 업데이트합니다. 값을 0로 설정합니다.

```
net.ipv4.conf.all.accept_redirects=0
net.ipv4.conf.default.accept_redirects=0
```

   c 변경 사항을 저장하고 파일을 닫습니다.

IPv6 ICMP 리디렉션 메시지를 무시하도록 호스트 시스템 구성

보안 Best Practice로, 호스트 시스템이 IPv6 ICMP(Internet Control Message Protocol) 리디렉션 메시지를 무시하는지 확인합니다. 악의적인 ICMP 리디렉션 메시지는 메시지 가로채기(man-in-the-middle) 공격이 발생하도록 허용할 수 있습니다. 라우터는 ICMP 리디렉션 메시지를 사용하여 더욱 직접적인 경로가 특정 대상에 대해 존재함을 호스트에 알립니다. 이러한 메시지는 인증되지 않은 것이며, 호스트의 경로 테이블을 수정합니다.

프로시저

1 호스트 시스템에서 # grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects|egrep "default|all" 명령을 실행하여 호스트 시스템이 IPv6 리디렉션 메시지를 무시하는지 여부를 확인합니다.

2 IPv6 ICMP 리디렉션 메시지를 무시하도록 호스트 시스템을 구성합니다.

   a /etc/sysctl.conf를 열어 IPv6 리디렉션 메시지를 무시하도록 호스트 시스템을 구성합니다.

   b 값이 0로 설정되어 있지 않은 경우 다음 항목을 파일에 추가하거나 기존 항목을 이에 맞게 업데이트합니다. 값을 0로 설정합니다.

```
net.ipv6.conf.all.accept_redirects=0
net.ipv6.conf.default.accept_redirects=0
```

   c 변경 사항을 저장하고 파일을 닫습니다.

IPv4 ICMP 리디렉션을 거부하도록 호스트 시스템 구성

보안 Best Practice로, 호스트 시스템이 IPv4 ICMP(Internet Control Message Protocol) 리디렉션을 거부하는지 확인합니다. 라우터는 ICMP 리디렉션 메시지를 사용하여 직접 경로가 특정 대상에 대해 존재함을 서버에 알립니다. 이러한 메시지에는 네트워크 토폴로지의 여러 부분을 나타낼 수 있는 시스템 경로 테이블의 정보가 포함됩니다.

프로시저

1. 호스트 시스템에서 # grep [01] /proc/sys/net/ipv4/conf/*/send_redirects|egrep "default|all"을 실행하여 호스트 시스템이 IPv4 ICMP 리디렉션을 거부하는지 여부를 확인합니다.
2. IPv4 ICMP 리디렉션을 거부하도록 호스트 시스템을 구성합니다.
   a. /etc/sysctl.conf 파일을 열어 호스트 시스템을 구성합니다.
   b. 값이 0로 설정되어 있지 않은 경우 다음 항목을 파일에 추가하거나 기존 항목을 이에 맞게 업데이트합니다. 값을 0로 설정합니다.

```
net.ipv4.conf.all.send_redirects=0
net.ipv4.conf.default.send_redirects=0
```

   c. 변경 사항을 저장하고 파일을 닫습니다.

IPv4 Martian 패킷을 기록하도록 호스트 시스템 구성

보안 모범 사례로, 호스트 시스템이 IPv4 Martian 패킷을 기록하는지 확인합니다. Martian 패킷에는 유효하지 않은 것으로 시스템에 알려진 주소가 포함됩니다. 메시지를 기록하도록 호스트 시스템을 구성하여 진행 중인 구성 오류 또는 공격을 식별할 수 있도록 하십시오.

프로시저

1. # grep [01] /proc/sys/net/ipv4/conf/*/log_martians|egrep "default|all" 명령을 실행하여 호스트가 IPv4 Martian 패킷을 기록하는지 확인합니다.
2. IPv4 Martian 패킷을 기록하도록 호스트 시스템을 구성합니다.
   a. /etc/sysctl.conf 파일을 열어 호스트 시스템을 구성합니다.
   b. 값이 1로 설정되어 있지 않은 경우 다음 항목을 파일에 추가하거나 기존 항목을 이에 맞게 업데이트합니다. 값을 1로 설정합니다.

```
net.ipv4.conf.all.log_martians=1
net.ipv4.conf.default.log_martians=1
```

   c. 변경 사항을 저장하고 파일을 닫습니다.

IPv4 역방향 경로 필터링을 사용하도록 호스트 시스템 구성

보안 Best Practice로, IPv4 역방향 경로 필터링을 사용하도록 호스트 시스템을 구성합니다. 역방향 경로 필터링은 소스 주소에 경로가 없거나 경로가 원래 인터페이스를 가리키지 않을 경우 시스템이 해당 패킷을 삭제하도록 하여 스푸핑된 소스 주소로부터 보호합니다.

가능한 경우 항상 역방향 경로 필터링을 사용하도록 시스템을 구성합니다. 시스템 역할에 따라 역방향 경로 필터링으로 인해 적합한 트래픽이 삭제될 수 있습니다. 이러한 경우, 더욱 허용되는 모드를 사용하거나 역방향 경로 필터링을 모두 사용하지 않도록 설정해야 할 수 있습니다.

프로시저

1. 호스트 시스템에서 # grep [01] /proc/sys/net/ipv4/conf/*/rp_filter|egrep "default|all" 명령을 실행하여 시스템이 IPv4 역방향 경로 필터링을 사용하는지 여부를 확인합니다.
2. IPv4 역방향 경로 필터링을 사용하도록 호스트 시스템을 구성합니다.
   a. /etc/sysctl.conf 파일을 열어 호스트 시스템을 구성합니다.
   b. 값이 1로 설정되어 있지 않은 경우 다음 항목을 파일에 추가하거나 기존 항목을 이에 맞게 업데이트합니다. 값을 1로 설정합니다.

```
net.ipv4.conf.all.rp_filter=1
net.ipv4.conf.default.rp_filter=1
```

   c. 변경 사항을 저장하고 파일을 닫습니다.

IPv4 전달을 거부하도록 호스트 시스템 구성

보안 Best Practice로, 호스트 시스템이 IPv4 전달을 거부하는지 확인합니다. 시스템이 IP 전달이 가능하도록 구성되어 있고 지정된 라우터가 아닌 경우, 네트워크 장치에서 필터링되지 않는 통신 경로를 제공함으로써 네트워크 보안을 우회하는 데 사용될 수 있습니다.

프로시저

1. # cat /proc/sys/net/ipv4/ip_forward 명령을 실행하여 호스트가 IPv4 전달을 거부하는지 여부를 확인합니다.
2. IPv4 전달을 거부하도록 호스트 시스템을 구성합니다.
   a. /etc/sysctl.conf를 열어 호스트 시스템을 구성합니다.
   b. 값이 0으로 설정되어 있지 않은 경우 다음 항목을 파일에 추가하거나 기존 항목을 이에 맞게 업데이트합니다. 값을 0로 설정합니다.

```
net.ipv4.ip_forward=0
```

   c. 변경 사항을 저장하고 파일을 닫습니다.

IPv4 소스에서 라우팅된 패킷에 대한 전달을 거부하도록 호스트 시스템 구성

소스에서 라우팅된 패킷을 통해 패킷의 소스는 라우터가 라우터에 구성된 경로가 아닌 다른 경로를 따라 패킷을 전달하는지 나타낼 수 있습니다. 이러한 경로는 네트워크 보안 조치를 우회하는 데 사용될 수 있습니다.

이 요구 사항은 IPv4 전달이 사용하도록 설정되어 있고 시스템이 라우터로 작동하는 경우와 같이 소스에서 라우팅된 트래픽의 전달에 대해서만 적용됩니다.

프로시저

1 # grep [01] /proc/sys/net/ipv4/conf/*/accept_source_route|egrep "default|all" 명령을 실행하여 시스템이 IPv4 소스에서 라우팅된 패킷을 사용하지 않는지 여부를 확인합니다.

2 IPv4 소스에서 라우팅된 패킷에 대한 전달을 거부하도록 호스트 시스템을 구성합니다.

   a 텍스트 편집기에서 /etc/sysctl.conf 파일을 엽니다.

   b 값이 0으로 설정되어 있지 않은 경우 net.ipv4.conf.all.accept_source_route=0 및 et.ipv4.conf.default.accept_source_route=0이 0으로 설정되어 있는지 확인합니다.

   c 파일을 저장한 후 닫습니다.

IPv6 전달을 거부하도록 호스트 시스템 구성

보안 Best Practice로, 호스트 시스템이 IPv6 전달을 거부하는지 확인합니다. 시스템이 IP 전달이 가능하도록 구성되어 있고 지정된 라우터가 아닌 경우, 네트워크 장치에서 필터링되지 않는 통신 경로를 제공함으로써 네트워크 보안을 우회하는 데 사용될 수 있습니다.

프로시저

1 # grep [01] /proc/sys/net/ipv6/conf/*/forwarding|egrep "default|all" 명령을 실행하여 호스트가 IPv6 전달을 거부하는지 여부를 확인합니다.

2 IPv6 전달을 거부하도록 호스트 시스템을 구성합니다.

   a /etc/sysctl.conf를 열어 호스트 시스템을 구성합니다.

   b 값이 0로 설정되어 있지 않은 경우 다음 항목을 파일에 추가하거나 기존 항목을 이에 맞게 업데이트합니다. 값을 0로 설정합니다.

```
net.ipv6.conf.all.forwarding=0
net.ipv6.conf.default.forwarding=0
```

   c 변경 사항을 저장하고 파일을 닫습니다.

IPv4 TCP SYN 쿠키를 사용하도록 호스트 시스템 구성

보안 모범 사례로, 호스트 시스템이 IPv4 TCP(Transmission Control Protocol) SYN 쿠키를 사용하는지 확인합니다. TCP SYN 서비스 장애 공격이 시스템의 TCP 연결 테이블을 SYN_RCVD 상태의 연결로 채우면 서비스 거부가 발생할 수 있습니다. SYN 쿠키는 이니시에이터가 유효한 연결을 시도하고 서비스 장애 공격의 소스가 아닌지 확인하여 후속 ACK가 수신되기 전까지 연결을 추적하지 않도록 하는 데 사용됩니다.

이 기술은 완벽하게 표준을 준수하는 방식으로 작동하지 않지만 서비스 장애 조건이 감지될 때만 활성화되므로 유효한 요청에 대한 서비스를 계속 제공하면서 시스템을 방어할 수 있습니다.

프로시저

1. # cat /proc/sys/net/ipv4/tcp_syncookies 명령을 실행하여 호스트 시스템이 IPv4 TCP SYN 쿠키를 사용하는지 여부를 확인합니다.
2. IPv4 TCP SYN 쿠키를 사용하도록 호스트 시스템을 구성합니다.
   a. /etc/sysctl.conf를 열어 호스트 시스템을 구성합니다.
   b. 값이 1으로 설정되어 있지 않은 경우 다음 항목을 파일에 추가하거나 기존 항목을 이에 맞게 업데이트합니다. 값을 1로 설정합니다.

      ```
      net.ipv4.tcp_syncookies=1
      ```

   c. 변경 사항을 저장하고 파일을 닫습니다.

IPv6 라우터 알림을 거부하도록 호스트 시스템 구성

보안 Best Practice로, 호스트 시스템이 필요하지 않은 경우 라우터 알림 및 ICMP(Internet Control Message Protocol) 리디렉션 수락을 거부하는지 확인합니다. IPv6의 기능은 시스템이 네트워크의 정보를 자동으로 사용하여 네트워킹 장치를 구성할 수 있는 방식입니다. 보안 측면에서 인증되지 않은 방법으로 네트워크로부터 중요한 구성 정보를 받는 대신 이러한 정보를 수동으로 설정하는 것이 좋습니다.

프로시저

1. 호스트 시스템에서 # grep [01] /proc/sys/net/ipv6/conf/*/accept_ra|egrep "default|all" 명령을 실행하여 시스템이 필요하지 않은 경우 라우터 알림 및 ICMP 리디렉션의 수락을 거부하는지 여부를 확인합니다.

2 IPv6 라우터 알림을 거부하도록 호스트 시스템을 구성합니다.

a /etc/sysctl.conf 파일을 엽니다.

b 값이 0로 설정되어 있지 않은 경우 다음 항목을 파일에 추가하거나 기존 항목을 이에 맞게 업데이트합니다. 값을 0로 설정합니다.

```
net.ipv6.conf.all.accept_ra=0
net.ipv6.conf.default.accept_ra=0
```

c 변경 사항을 저장하고 파일을 닫습니다.

IPv6 라우터 요청을 거부하도록 호스트 시스템 구성

보안 Best Practice로, 호스트 시스템이 필요하지 않은 경우 IPv6 라우터 요청을 거부하는지 확인합니다. 라우터 요청 설정에 따라 인터페이스를 작동할 때 전송되는 라우터 요청의 수가 결정됩니다. 주소가 정적으로 할당된 경우 요청을 전송할 필요가 없습니다.

프로시저

1 # grep [01] /proc/sys/net/ipv6/conf/*/router_solicitations|egrep "default|all" 명령을 실행하여 호스트 시스템이 필요하지 않은 경우 IPv6 라우터 요청을 거부하는지 여부를 확인합니다.

2 IPv6 라우터 요청을 거부하도록 호스트 시스템을 구성합니다.

a /etc/sysctl.conf를 엽니다.

b 값이 0로 설정되어 있지 않은 경우 다음 항목을 파일에 추가하거나 기존 항목을 이에 맞게 업데이트합니다. 값을 0로 설정합니다.

```
net.ipv6.conf.all.router_solicitations=0
net.ipv6.conf.default.router_solicitations=0
```

c 변경 사항을 저장하고 파일을 닫습니다.

라우터 요청에서 IPv6 라우터 기본 설정을 거부하도록 호스트 시스템 구성

보안 Best Practice로, 호스트 시스템이 필요하지 않은 경우 IPv6 라우터 요청을 거부하는지 확인합니다. 요청 설정의 라우터 기본 설정에 따라 라우터 기본 설정이 결정됩니다. 주소가 정적으로 할당된 경우 요청에 대해 라우터 기본 설정을 수신할 필요가 없습니다.

프로시저

1 호스트 시스템에서 # grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref|egrep "default|all"을 실행하여 호스트 시스템이 IPv6 라우터 요청을 거부하는지 여부를 확인합니다.

2 라우터 요청에서 IPv6 라우터 기본 설정을 거부하도록 호스트 시스템을 구성합니다.

a /etc/sysctl.conf 파일을 엽니다.

b 값이 0로 설정되어 있지 않은 경우 다음 항목을 파일에 추가하거나 기존 항목을 이에 맞게 업데이트합니다. 값을 0로 설정합니다.

```
net.ipv6.conf.all.accept_ra_rtr_pref=0
net.ipv6.conf.default.accept_ra_rtr_pref=0
```

c 변경 사항을 저장하고 파일을 닫습니다.

IPv6 라우터 접두사를 거부하도록 호스트 시스템 구성

보안 Best Practice로, 호스트 시스템이 필요하지 않은 경우 IPv6 라우터 접두사 정보를 거부하는지 확인합니다. accept ra pinfo 설정은 시스템이 라우터에서 접두사 정보를 받는지 여부를 제어합니다. 주소가 정적으로 할당된 경우 시스템이 라우터 접두사 정보를 수신하지 않습니다.

프로시저

1 # grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo|egrep "default|all"을 실행하여 시스템이 IPv6 라우터 접두사 정보를 거부하는지 확인합니다.

2 IPv6 라우터 접두사를 거부하도록 호스트 시스템을 구성합니다.

a /etc/sysctl.conf 파일을 엽니다.

b 값이 0로 설정되어 있지 않은 경우 다음 항목을 파일에 추가하거나 기존 항목을 이에 맞게 업데이트합니다. 값을 0로 설정합니다.

```
net.ipv6.conf.all.accept_ra_pinfo=0
net.ipv6.conf.default.accept_ra_pinfo=0
```

c 변경 사항을 저장하고 파일을 닫습니다.

IPv6 라우터 알림 홉 제한 설정을 거부하도록 호스트 시스템 구성

보안 모범 사례로, 호스트 시스템이 필요한 경우를 제외하고 라우터 알림의 IPv6 라우터 알림 홉 제한 설정을 거부하는지 확인합니다. accept_ra_defrtr 설정은 라우터 알림의 홉 제한 설정에 대한 시스템의 수락 여부를 제어합니다. 0으로 설정하면 라우터가 송신 패킷에 대한 기본 IPv6 홉 제한을 변경하지 못합니다.

프로시저

1 # grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr|egrep "default|all" 명령을 실행하여 호스트 시스템이 IPv6 라우터 홉 제한 설정을 거부하는지 확인합니다.

2 값이 0으로 설정되어 있지 않은 경우 IPv6 라우터 알림 홉 제한 설정을 거부하도록 호스트 시스템을 구성합니다.

a /etc/sysctl.conf 파일을 엽니다.

b 값이 0로 설정되어 있지 않은 경우 다음 항목을 파일에 추가하거나 기존 항목을 이에 맞게 업데이트합니다. 값을 0로 설정합니다.

```
net.ipv6.conf.all.accept_ra_defrtr=0
net.ipv6.conf.default.accept_ra_defrtr=0
```

c 변경 사항을 저장하고 파일을 닫습니다.

IPv6 라우터 알림 Autoconf 설정을 거부하도록 호스트 시스템 구성

보안 Best Practice로, 호스트 시스템이 IPv6 라우터 알림 autoconf 설정을 거부하는지 확인합니다. autoconf 설정은 라우터 알림으로 인해 시스템이 글로벌 유니캐스트 주소를 인터페이스에 할당할 수 있는지 여부를 제어합니다.

프로시저

1 # grep [01] /proc/sys/net/ipv6/conf/*/autoconf|egrep "default|all" 명령을 실행하여 호스트 시스템이 IPv6 라우터 알림 autoconf 설정을 거부하는지 여부를 확인합니다.

2 값이 0으로 설정되어 있지 않은 경우 IPv6 라우터 알림 autoconf 설정을 거부하도록 호스트 시스템을 구성합니다.

a /etc/sysctl.conf 파일을 엽니다.

b 값이 0로 설정되어 있지 않은 경우 다음 항목을 파일에 추가하거나 기존 항목을 이에 맞게 업데이트합니다. 값을 0로 설정합니다.

```
net.ipv6.conf.all.autoconf=0
net.ipv6.conf.default.autoconf=0
```

c 변경 사항을 저장하고 파일을 닫습니다.

IPv6 인접 라우터 요청을 거부하도록 호스트 시스템 구성

보안 Best Practice로, 호스트 시스템이 필요하지 않은 경우 IPv6 인접 라우터 요청을 거부하는지 확인합니다. 인터페이스를 작동하여 원하는 주소가 네트워크에서 고유한지를 확인할 때 dad_transmits 설정에 따라 글로벌 및 링크-로컬을 비롯한 주소당 전송되는 인접 라우터 요청 수가 결정됩니다.

프로시저

1 # grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits|egrep "default|all" 명령을 실행하여 호스트 시스템이 IPv6 인접 라우터 요청을 거부하는지 여부를 확인합니다.

2 값이 0으로 설정되어 있지 않은 경우 IPv6 인접 라우터 요청을 거부하도록 호스트 시스템을 구성합니다.

   a /etc/sysctl.conf 파일을 엽니다.

   b 값이 0로 설정되어 있지 않은 경우 다음 항목을 파일에 추가하거나 기존 항목을 이에 맞게 업데이트합니다. 값을 0로 설정합니다.

```
net.ipv6.conf.all.dad_transmits=0
net.ipv6.conf.default.dad_transmits=0
```

   c 변경 사항을 저장하고 파일을 닫습니다.

IPv6 최대 주소 수를 제한하도록 호스트 시스템 구성

보안 모범 사례로, 호스트가 할당 가능한 IPv6 주소의 최대 수를 제한하는지 확인합니다. 최대 주소 수 설정은 각 인터페이스에 할당할 수 있는 글로벌 유니캐스트 IPv6 주소의 수를 결정합니다. 기본값은 16이지만 이 수를 정적으로 구성된 필요한 글로벌 주소의 수로 설정해야 합니다.

프로시저

1 # grep [1] /proc/sys/net/ipv6/conf/*/max_addresses|egrep "default|all" 명령을 실행하여 호스트 시스템이 할당 가능한 IPv6 주소의 최대 수를 제한하는지 확인합니다.

2 값을 1로 설정하지 않은 경우 할당 가능한 IPv6 주소의 최대 수를 제한하도록 호스트 시스템을 구성합니다.

   a /etc/sysctl.conf 파일을 엽니다.

   b 다음 항목을 파일에 추가하거나 그에 따라 기존 항목을 업데이트합니다. 값을 1로 설정합니다.

```
net.ipv6.conf.all.max_addresses=1
net.ipv6.conf.default.max_addresses=1
```

   c 변경 사항을 저장하고 파일을 닫습니다.

포트 및 프로토콜 구성

보안 Best Practice로, 불필요한 포트 및 프로토콜을 모두 사용하지 않도록 설정합니다.

중요한 시스템 구성 요소가 프로덕션 환경에서 작동하는 데 필요한 만큼
vRealize Operations Manager 구성 요소에 대해 최소한의 송수신 포트만 구성합니다.

최소 기본 수신 포트

보안 모범 사례로, vRealize Operations Manager를 운영 환경에서 작동하는 데 필요한 수신 포트를 구성합니다.

표 4-1. 필요한 최소 수신 포트

포트	프로토콜	주석
443	TCP	vRealize Operations Manager 사용자 인터페이스 및 vRealize Operations Manager 관리자 인터페이스에 액세스하는 데 사용됩니다.
123	UDP	vRealize Operations Manager에서 마스터 노드로 NTP(네트워크 시간 프로토콜)를 동기화할 경우 사용됩니다.
5433	TCP	고가용성을 사용하도록 설정한 경우 마스터 및 복제본 노드에서 글로벌 데이터베이스(vPostgreSQL)를 복제하는 데 사용됩니다.
7001	TCP	Cassandra의 노드 클러스터 간 보안 통신에 사용됩니다. 이 포트는 인터넷에 노출시키지 마십시오. 이 포트를 방화벽에 추가하십시오.
9042	TCP	Cassandra에서 노드 간 클라이언트 관련 통신의 보안에 사용됩니다. 이 포트는 인터넷에 노출시키지 마십시오. 이 포트를 방화벽에 추가하십시오.
6061	TCP	분산 시스템의 서버에 대한 연결 정보를 가져오기 위해 클라이언트에서 GemFire Locator에 연결하는 데 사용됩니다. 또한 서버 로드를 모니터링하여 클라이언트를 로드가 가장 적은 서버로 보냅니다.
10000-10010	TCP 및 UDP	피어 투 피어(peer-to-peer) 분산 시스템에서 유니캐스트 UDP 메시징 및 TCP 실패 감지 시 사용되는 GemFire 서버 사용 후 삭제 포트 범위입니다.
20000-20010	TCP 및 UDP	피어 투 피어(peer-to-peer) 분산 시스템에서 유니캐스트 UDP 메시징 및 TCP 실패 감지 시 사용되는 GemFire 로케이터 사용 후 삭제 포트 범위입니다.

표 4-2. 선택적 수신 포트

포트	프로토콜	주석
22	TCP	선택 사항입니다. SSH(보안 셸)입니다. 포트 22 또는 다른 포트를 통해 수신하는 SSH 서비스는 운영 환경에서 사용하지 않도록 설정되어야 하며 포트 22는 닫아야 합니다.
80	TCP	선택 사항입니다. 443으로 리디렉션됩니다.
3091-3101	TCP	Horizon View를 설치한 경우 Horizon View에서 vRealize Operations Manager의 데이터에 액세스하는 데 사용됩니다.

vRealize Operations Manager 시스템 감사 및 로깅

5

보안 Best Practice로, vRealize Operations Manager 시스템에 대한 감사 및 로깅을 설정합니다.

감사 및 로깅에 대한 자세한 구현 정보는 이 문서 범위에 포함되지 않습니다.

중앙 로그 호스트로의 원격 로깅은 로그를 저장할 수 있는 안전한 저장소를 제공합니다. 로그 파일을 중앙 호스트에 수집하면 단일 도구를 사용하여 환경을 손쉽게 모니터링할 수 있습니다. 또한 분석 정보를 집계하고 인프라 내에 포함된 여러 엔티티에 대한 연계 공격을 검색할 수 있습니다. 안전한 중앙 로그 서버에 로깅하면 로그 변조를 방지하는 데 도움이 될 뿐만 아니라 장기적인 감사 레코드도 확보할 수 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

- 원격 로깅 서버 보안 유지
- 인증된 NTP 서버 사용
- 클라이언트 브라우저 고려 사항

원격 로깅 서버 보안 유지

보안 Best Practice로, 원격 로깅 서버가 권한 있는 사용자만 구성할 수 있으며 보안이 유지되는지 확인합니다.

호스트 시스템의 보안을 위반하는 공격자는 로그 파일을 찾고, 검색 없이 해당 추적을 처리하고 제어를 유지하도록 로그 파일의 변조를 시도할 수 있습니다.

인증된 NTP 서버 사용

모든 호스트 시스템이 동일한 상대적 시간 소스(관련 지역화 오프셋 포함)를 사용하는지 확인합니다. 상대적 시간 소스를 합의된 시간 표준(예: 협정 세계시-UTC)에 연관시킬 수 있습니다.

관련 로그 파일을 검토할 때 침입자의 작업을 쉽게 추적하고 연관할 수 있습니다. 시간 설정이 잘못되면 로그 파일을 검사하고 연관하여 공격을 감지하기가 힘들 뿐 아니라 정확하지 않은 감사로 이어질 수 있습니다. 시간 소스 외부에서 최소 3개의 NTP 서버를 사용하거나 최소 3개의 외부 시간 소스에서 시간을 가져오는 소수의 로컬 NTP 서버를 신뢰할 수 있는 네트워크에 구성할 수 있습니다.

클라이언트 브라우저 고려 사항

보안 모범 사례로, 신뢰할 수 없거나 패치가 적용되지 않은 클라이언트 또는 브라우저 확장을 사용하는 클라이언트에서 vRealize Operations Manager를 사용하지 마십시오.