Secure Configuration

vRealize Operations Manager 6.1

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001961-00

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

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

Contents

Secure Configuration

The documentation for *Secure Configuration* is intended to serve as a secure baseline for the deployment of vRealize Operations Manager. Refer to this document when you are using system-monitoring tools to ensure that the secure baseline configuration is monitored and maintained for any unexpected changes on an ongoing basis.

Hardening activities that are not already set by default can be carried out manually, or in some cases, automatically by using the vRealize Hardening Tool. For more information about the vRealize Hardening Tool, see Chapter 2, "vRealize Hardening Tool," on page 9.

Intended Audience

This information is intended for administrators of vRealize Operations Manager.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

vRealize Operations Manager Security Posture

1

The security posture of vRealize Operations Manager assumes a complete secure environment based on system and network configuration, organizational security policies, and best practices. It is important that you perform the hardening activities according to your organization's security policies and best practices.

The document is broken down into the following sections:

- Secure Deployment
- Secure Configuration
- Network Security
- Communication

The guide details the installation of the Virtual Application. However, the following deployment types are also discussed:

- "Linux Installed Deployment," on page 36
- "Windows Installed Deployment," on page 35

To ensure that your system is securely hardened, review the recommendations and assess them against your organization's security policies and risk exposure.

vRealize Hardening Tool 2

You can use the vRealize Hardening Tool to ensure that the secure baseline is reached and maintained. Because many of the hardening requirements that are set by the vRealize Hardening Tool are already in their default-hardened state, you can use the hardening tool to bring the installation back to the default-hardened state if changes are made.

The vRealize Hardening Tool is available on the VMware vRealize Automation Drivers and Tools download page.

This chapter includes the following topics:

Install Ansible

The vRealize Hardening Tool is based on Ansible, which is an open-source software platform for configuring and managing computers. Before you can use the vRealize Hardening Tool, you must install the Ansible software.

Procedure

1 Install the Ansible software by downloading it and following the instructions on the Ansible Web site at http://docs.ansible.com/intro_installation.html.

2 Verify the Ansible installation.

   a Run the `ansible --version` command.

   b If errors appear, see the `vrhtool/Readme.txt` file for instructions about how to install missing modules required to run Ansible.

Set Up the vRealize Hardening Tool

You can set up the vRealize Hardening Tool and modify the list of vRealize Operations Manager nodes on which the configuration changes are to occur.

Procedure

1 Run the `tar -zxvf vrhtool.tar.gz` command to install the hardening tool.

2 Modify the list of vRealize Operations Manager nodes on which the configuration changes are to occur.

The list is in the *inventory.yaml* file located in `vrhtool/baseline/`.

a Replace *abc1.xyxz.com* with the fully qualified domain name (FQDN) of your vRealize Operations Manager node.

b Replace *username* and *password* with the SSH credentials enable the vRealize Hardening Tool to modify the vRealize Operations Manager appliance.

You can include multiple vRealize Operations Manager appliances.

Run the vRealize Hardening Tool from the User Interface

You can run the vRealize Hardening Tool from the user interface (UI) rather than from the command line to complete some hardening activities.

Procedure

1 Change to the directory where the tool resides.

```
cd vrhtool
```

2 Run the `python script/vRHT.py` command.

The vRealize Hardening Tool UI appears.

3 In Categories, select the hardening activities to run.

4 Select **Dry Run**, and click **Execute** to verify the changes before they are made to the system.

5 Click **Execute** to run the vRealize Hardening Tool based on the selections you made.

Run the vRealize Hardening Tool from the Command Line

You can run the following commands from the command-line interface (CLI) to use the vRealize Hardening Tool.

Procedure

1 Change to the directory where the vRealize Hardening Tool resides.

```
cd vrhtool
```

2 Verify that the vRealize Hardening Tool was installed without making changes.

```
ansible-playbook -i baseline/inventory.yaml baseline/vROps.yaml --check
```

No changes are made to the system.

3 Run the vRealize Hardening Tool and make changes to the system.

```
ansible-playbook -i baseline/inventory.yaml baseline/vROps.yaml --tags
web,ssh,pwd_expiry,network_cfg,softwarecomponents,postgres,create_admin_user,tcptimestamp,sin
gleuserauth,ntp,apache2
```

Each comma-separated tag is associated with a hardening activity that is supported by the vRealize Hardening Tool. If you do not want to run a hardening activity, you can omit it from the command.

vRealize Hardening Tool Categories

The following table correlates the hardening activity with the user interface and command line options.

Table 2-1. vRealize Hardening Tool Categories

Hardening Activity	UI Option	Command Line Tag
Apache Server Response Header	Apache2 Configuration	apache2
Configure NTP	Network Time Protocol	ntp
Single-user or maintenance mode authentication	Single User Authentication	singleuserauth
TCP Timestamp response	TCP Timestamp Settings	tcptimestamp
Create Local Administrative Account For SSH	Linux Admin User	create_admin_user
PostgreSQL (Client Authentication Configuration)	PostgreSQL Settings	postgres
Unrequired Software Components	Software Components	softwarecomponents
Network Settings for Virtual Application Installation (OVF)	Network Settings	network_cfg
Modify root password expiry	Root Password Expiry	pwd_expiry
Maintain SSH Key File Permissions	Secure Shell	ssh
Harden the SSH Server Configuration	Secure Shell	ssh
Harden the SSH Client Configuration	Secure Shell	ssh
Disable Web Directory Browsing	Web Directory Settings	web

Secure Deployment of vRealize Operations Manager 3

You must verify the integrity of the installation media before you install the product to ensure authenticity of the downloaded files.

This chapter includes the following topics:

Verifying the Integrity of Installation Media

After you download the media, use the MD5/SHA1 sum value to verify the integrity of the download. Always verify the SHA1 hash after you download an ISO, offline bundle, or patch to ensure integrity and authenticity of the downloaded files. If you obtain physical media from VMware and the security seal is broken, return the software to VMware for a replacement.

Procedure

- Compare the MD5/SHA1 hash output with the value posted on the VMware Web site. SHA1 or MD5 hash should match.

NOTE The vRealize Operations Manager 6.1 - x .pak files are signed by the VMware software publishing certificate. vRealize Operations Manager validates the signature of the pak file before installation.

Hardening the Deployed Software Infrastructure

As part of your hardening process, you must harden the deployed software infrastructure that supports your VMware system.

Before you harden your VMware system, review and address security deficiencies in your supporting software infrastructure to create a completely hardened and secure environment. Software infrastructure elements to consider include operating system components, supporting software, and database software. Address security concerns in these and other components according to the manufacturer's recommendations and other relevant security protocols.

Hardening the VMware vSphere Environment

vRealize Operations Manager relies on a secure VMware vSphere environment to achieve the greatest benefits and a secured infrastructure.

Assess the VMware vSphere environment and verify that the appropriate level of vSphere hardening guidance is enforced and maintained.

For more guidance about hardening, see http://www.vmware.com/security/hardening-guides.html.

Hardening for Linux Installation

Review the recommendations set out in the appropriate Linux hardening and secure best practice guidelines, and ensure that your Linux hosts are appropriately hardened. If you do not follow the hardening recommendations, the system might be exposed to known security vulnerabilities from insecure components on Linux releases.

vRealize Operations Manager is supported for installation on Red Hat Enterprise Linux (RHEL) 6, starting with version 6.5.

Hardening for Windows Installation

Review the recommendations set out in the appropriate Windows hardening and secure best practice guidelines, and ensure that your Windows Server host is appropriately hardened. If you do not follow the hardening recommendations, the system might be exposed to known security vulnerabilities from insecure components on Windows releases.

Contact your Microsoft vendor for hardening practices of Microsoft products.

Reviewing Installed and Unsupported Software

Vulnerabilities in unused software might increase the risk of unauthorized system access and disruption of availability. Review the software that is installed on VMware host machines and evaluate its use.

Do not install software that is not required for the secure operation of the system on any of the vRealize Operations Manager node hosts. Uninstall unused or nonessential software.

Installing unsupported, untested, or unapproved software on infrastructure products such as vRealize Operations Manager is a threat to the infrastructure.

To minimize the threat to the infrastructure, do not install or use any third-party software that is not supported by VMware on VMware supplied hosts.

Assess your vRealize Operations Manager deployment and inventory of installed products to verify that no unsupported software is installed.

For more information about the support policies for third-party products, see the VMware support at https://www.vmware.com/support/policies/thirdparty.html.

Verify Third-Party Software

Do not use third-party software that VMware does not support. Verify that all third-party software is securely configured and patched in accordance with third-party vendor guidance.

Inauthentic, insecure, or unpatched vulnerabilities of third-party software installed on VMware host machines might put the system at risk of unauthorized access and disruption of availability. All software that VMware does not supply must be appropriately secured and patched.

If you must use third-party software that VMware does not support, consult the third-party vendor for secure configuration and patching requirements.

VMware Security Advisories and Patches

VMware occasionally releases security advisories for products. Being aware of these advisories can ensure that you have the safest underlying product and that the product is not vulnerable to known threats.

Assess the vRealize Operations Manager installation, patching, and upgrade history and verify that the released VMware Security Advisories are followed and enforced.

It is recommended that you always remain on the most recent vRealize Operations Manager release, as this will include the most recent security fixes also.

For more information about the current VMware security advisories, see http://www.vmware.com/security/advisories/.

Secure Configuration of vRealize Operations Manager

4

As a security best practice, you must secure the vRealize Operations Manager console and manage Secure Shell (SSH), administrative accounts, and console access. Ensure that your system is deployed with secure transmission channels.

You must also follow certain security best practices for running Endpoint Operations Management agents.

This chapter includes the following topics:

Secure the vRealize Operations Manager Console

After you install vRealize Operations Manager, you must log in for the first time and secure the console of each node in the cluster.

Prerequisites

Install vRealize Operations Manager.

Procedure

1 Locate the node console in vCenter or by direct access.

In vCenter, press Alt+F1 to access the login prompt. For security reasons, vRealize Operations Manager remote terminal sessions are disabled by default.

2 Log in as root.

vRealize Operations Manager does not allow you to access the command prompt until you create a root password.

3 At the password prompt, press **Enter**.

4 At the old password prompt, press **Enter**.

5 At the prompt for a new password, enter the root password that you want and note it for future reference.

6 Reenter the root password.

7 Log out of the console.

Change the Root Password

You can change the root password for any vRealize Operations Manager master or data node at any time by using the console.

The root user bypasses the `pam_cracklib` module password complexity check, which is found in `etc/pam.d/common-password`. All hardened appliances enable `enforce_for_root` for the `pw_history` module, found in the `etc/pam.d/common-password` file. The system remembers the last five passwords by default. Old passwords are stored for each user in the `/etc/security/opasswd` file.

Prerequisites

Verify that the root password for the appliance meets your organization's corporate password complexity requirements. If the account password starts with `$6$`, it uses a sha512 hash. This is the standard hash for all hardened appliances.

Procedure

1 Run the `# passwd` command at the root shell of the appliance.

2 To verify the hash of the root password, log in as root and run the `# more /etc/shadow` command.

The hash information appears.

3 If the root password does not contain a sha512 hash, run the `passwd` command to change it.

Manage Password Expiry

Configure all account password expirations in accordance with your organization's security policies.

By default, all hardened VMware appliances use a 60-day password expiry. On most hardened appliances, the root account is set to a 365-day password expiry. As a best practice, verify that the expiry on all accounts meets security and operation requirements standards.

If the root password expires, you cannot reinstate it. You must implement site-specific policies to prevent administrative and root passwords from expiring.

Procedure

1 Log in to your virtual appliance machines as root and run the `# more /etc/shadow` command to verify the password expiry on all accounts.

2 To modify the expiry of the root account, run the `# passwd –x 365 root` command.

In this command, 365 specifies the number of days until password expiry. Use the same command to modify any user, substituting the specific account for `root` and replacing the number of days to meet the expiry standards of the organization.

By default, the root password is set for 365 days. You can use the **Root Password Expiry** option in the vRealize Hardening Tool to set the root password to the secure baseline default of 365 days.

Managing Secure Shell, Administrative Accounts, and Console Access

For remote connections, all hardened appliances include the Secure Shell (SSH) protocol. SSH is disabled by default on the hardened appliance.

SSH is an interactive command-line environment that supports remote connections to a vRealize Operations Manager node. SSH requires high-privileged user account credentials. SSH activities generally bypass the role-based access control (RBAC) and audit controls of the vRealize Operations Manager node.

As a best practice, disable SSH in a production environment and enable it only to diagnose or troubleshoot problems that you cannot resolve by other means. Leave it enabled only while needed for a specific purpose and in accordance with your organization's security policies. If you enable SSH, ensure that it is protected against attack and that you enable it only for as long as required. Depending on your vSphere configuration, you can enable or disable SSH when you deploy your Open Virtualization Format (OVF) template.

As a simple test to determine whether SSH is enabled on a machine, try to open a connection by using SSH. If the connection opens and requests credentials, then SSH is enabled and is available for making connections.

Secure Shell Root User

Because VMware appliances do not include preconfigured default user accounts, the root account can use SSH to directly log in by default. Disable SSH as root as soon as possible.

To meet the compliance standards for nonrepudiation, the SSH server on all hardened appliances is preconfigured with the AllowGroups wheel entry to restrict SSH access to the secondary group wheel. For separation of duties, you can modify the AllowGroups wheel entry in the `/etc/ssh/sshd_config` file to use another group such as sshd.

The wheel group is enabled with the `pam_wheel` module for superuser access, so members of the wheel group can use the su-root command, where the root password is required. Group separation enables users to use SSH to the appliance, but not to use the su command to log in as root. Do not remove or modify other entries in the AllowGroups field, which ensures proper appliance function. After making a change, restart the SSH daemon by running the `# service sshd restart` command.

Enable or Disable Secure Shell on a vRealize Operations Manager node

You can enable Secure Shell (SSH) on a vRealize Operations Manager node for troubleshooting. For example, to troubleshoot a server, you might require console access to the server. This is through SSH. Disable SSH on a vRealize Operations Manager node for normal operation.

Procedure

1 Access the console of the vRealize Operations Manager node from vCenter.

2 Press Alt + F1 to access the login prompt then log in.

3 Run the `#chkconfig` command.

4 If the sshd service is off, run the `#chkconfig sshd on` command.

5 Run the `#service sshd start` command to start the sshd service.

6 Run the `#service sshd stop` command to stop the sshd service.

Create a Local Administrative Account for Secure Shell

You must create local administrative accounts that can be used as Secure Shell (SSH) and that are members of the secondary wheel group, or both before you remove the root SSH access.

Before you disable direct root access, test that authorized administrators can access SSH by using AllowGroups, and that they can use the wheel group and the `su` command to log in as root.

The vRealize Hardening Tool supports the creation of the user by using the **Linux Admin User** option. You must set the password manually.

Procedure

1 Log in as root and run the following commands.

```
# useradd –d /home/vcacuser –g users –G wheel -m
```

```
# passwd username
```

Wheel is the group specified in AllowGroups for SSH access. To add multiple secondary groups, use `–G wheel,sshd`

2 Switch to the user and provide a new password to ensure password complexity checking.

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

If the password complexity is met, the password updates. If the password complexity is not met, the password reverts to the original password, and you must rerun the password command.

After you create the login accounts to allow SSH remote access and use the `su` command to log in as root using the wheel access, you can remove the root account from the SSH direct login.

3 To remove direct login to SSH, modify the `/etc/ssh/sshd_config` file by replacing `(#)PermitRootLogin yes` with `PermitRootLogin no`.

Alternatively, you can enable or disable SSH in the Web Management Console (VAMI).

a Log in as root on thevRealize Operations Manager node.

b Navigate to the VAMI.

c Click the **Admin** tab, and select or deselect the **Administrator SSH** login enabled check box.

What to do next

Disable direct logins as root. By default, the hardened appliances allow direct login to root through the console. After you create administrative accounts for nonrepudiation and test them for wheel access (su-root), disable direct root logins by editing the`/etc/security` file as root and replacing the **`tty1`** entry with **`console`**.

Restrict Secure Shell Access

As part of your system hardening process, restrict Secure Shell (SSH) access by configuring the tcp_wrappers package appropriately on all VMware virtual appliance host machines. Also maintain required SSH key file permissions on these appliances.

All VMware virtual appliances include the tcp_wrappers package to allow tcp-supported daemons to control the network subnets that can access the libwrapped daemons. By default, the `/etc/hosts.allow` file contains a generic entry, `sshd: ALL : ALLOW`, that allows all access to the secure shell. Restrict this access as appropriate for your organization.

Procedure

1 Open the `/etc/hosts.allow` file on your virtual appliance host machine in a text editor.

2 Change the generic entry in your production environment to include only the local host entries and the management network subnet for secure operations.

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

In this example, all local host connections and connections that the clients make on the 10.0.0.0 subnet are allowed.

3 Add all appropriate machine identification, for example, host name, IP address, fully qualified domain name (FQDN), and loopback.

4 Save the file and close it.

Maintain Secure Shell Key File Permissions

To maintain an appropriate level of security, configure Secure Shell (SSH) key file permissions.

Procedure

1 View the public host key files, located in `/etc/ssh/*key.pub`.

2 Verify that these files are owned by root, that the group is owned by root, and that the files have permissions set to 0644.

The permissions are (-rw-r--r--).

3 Close all files.

4 View the private host key files, located in `/etc/ssh/*key`.

5 Verify that root owns these files and the group, and that the files have permissions set to 0600.

The permissions are (-rw-------).

6 Close all files.

Configure Secure Shell Port

By default, the SSHD service listens on port 22. Consider changing this port assignment, because potential attackers often target the most commonly used ports, such as 22.

Changing the port number considerably reduces the number of automated attacks performed by systematic attackers or zombie computers. Conversely, changing the port number forces the configuration of this alternative port for all clients that connect to the system.

Procedure

1 Log in to your virtual appliance as root and edit the `/etc/ssh/sshd_config` file.

2 Change # Port 22 to Port *preferred port number*.

3 Restart the SSHD service by running the `# service sshd restart` command.

What to do next

Update your firewall settings accordingly to support the new port.

Harden the Secure Shell Server Configuration

Where possible, the Virtual Application Installation (OVF) has a default hardened configuration. Users can verify that their configuration is appropriately hardened by examining the server and client service in the global options section of the configuration file.

If possible, restrict use of the SSH server to a management subnet in the `/etc/hosts.allow` file.

Procedure

1 Open the `/etc/ssh/sshd_config` server configuration file and verify that the settings are correct.

Setting	Status
Server Daemon Protocol	Protocol 2
Ciphers	Ciphers aes256-ctr,aes128-ctr
TCP Forwarding	AllowTCPForwarding no
Server Gateway Ports	Gateway Ports no
X11 Forwarding	X11Forwarding no
SSH Service	Use the AllowGroups field and specify a group permitted to access and add members to the secondary group for users permitted to ue the service.
GSSAPI Authentication	GSSAPIAuthentication no, if unused
Kerberos Authentication	KerberosAuthentication no, if unused
Local Variables (AcceptEnv global option)	Set to `disabled by commenting out` or `enabled for only LC_* or LANG variables`
Tunnel Configuration	PermitTunnel no
Network Sessions	MaxSessions 1
Strict Mode Checking	Strict Modes yes
Privilege Separation	UsePrivilegeSeparation yes

Setting	Status
rhosts RSA Authentication	RhostsRSAAuthentication no
Compression	Compression delayed or Compression no
Message Authentication code	MACs hmac-sha1
User Access Restriction	PermitUserEnvironment no

2 Save your changes and close the file.

Harden the Secure Shell Client Configuration

As part of your system hardening monitoring process, verify hardening of the SSH client by examining the SSH client configuration file on virtual appliance host machines to ensure that it is configured according to VMware guidelines.

Procedure

1 Open the SSH client configuration file, `/etc/ssh/ssh_config`, and verify that the settings in the global options section are correct.

Setting	Status
Client Protocol	Protocol 2
Client Gateway Ports	Gateway Ports no
GSSAPI Authentication	GSSAPIAuthentication no
Local Variables (SendEnv global option)	Provide only LC_* or LANG variables
CBC Ciphers	Ciphers aes256-ctr,aes128-ctr
Message Authentication Codes	Used in the `MACs hmac-sha1` entry only

2 Save your changes and close the file.

Disable Direct Logins as root

By default, the hardened appliances allow you to use the console to log in directly as root. As a security best practice, you can disable direct logins after you create an administrative account for nonrepudiation and test it for wheel access by using the `su-root` command.

Procedure

- Disable direct root logins.
  a Log in as root and navigate to the `/etc/security` file.
  b Replace the `tty1` entry with `console`.

Set Boot Loader Authentication

To provide an appropriate level of security, configure boot loader authentication on your VMware virtual appliances. If the system boot loader requires no authentication, users with console access to the system might be able to alter the system boot configuration or boot the system to single user or maintenance mode, which can result in denial of service or unauthorized system access.

Because boot loader authentication is not set by default on the VMware virtual appliances, you must create a GRUB password to configure it.

Procedure

1 Verify whether a boot password exists by locating the `password --md5 <password-hash>` line in the `/boot/grub/menu.lst` file on your virtual appliances.

2 If no password exists, run the `# /usr/sbin/grub-md5-crypt` command on your virtual appliance.

An MD5 password is generated, and the command supplies the md5 hash output.

3 Append the password to the `menu.lst` file by running the `# password --md5 <hash from grub-md5-crypt>` command.

Single-User or Maintenance Mode Authentication

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system.

Review the/`etc/inittab` file and ensure that the following two lines appear: `ls:S:wait:/etc/init.d/rc S` and `~~:S:respawn:/sbin/sulogin`.

Monitor Minimal Necessary User Accounts

You must monitor existing user accounts and ensure that any unnecessary user accounts are removed.

Procedure

- Run the `<host>:~ # cat /etc/passwd` command and verify the minimal necessary user accounts:

```
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
```

Monitor Minimal Necessary Groups

You must monitor existing groups and members to ensure that any unnecessary groups or group access is removed.

Procedure

- Run the `<host>:~ # cat /etc/group` command to verify the minimal necessary groups and group membership.

```
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
```

Resetting the vRealize Operations Manager Administrator Password (Linux)

As a security best practice, you can reset the vRealize Operations Manager password on Linux clusters for vAppp or Linux installations.

Procedure

1 Log in to the remote console of the master node as root.

2 Enter the `$VMWARE_PYTHON_BIN $VCOPS_BASE/../vmware-vcopssuite/utilities/sliceConfiguration/bin/vcopsSetAdminPassword.py --reset` command and follow the prompts.

Configure NTP on VMware Appliances

For critical time sourcing, disable host time synchronization and use the Network Time Protocol (NTP) on VMware appliances.

The NTP daemon on VMware virtual appliances provides synchronized time services. NTP is disabled by default, so you need to configure it manually. If possible, use NTP in production environments to track user actions and to detect potential malicious attacks and intrusions through accurate audit and log keeping. For information about NTP security notices, see the NTP Web site.

The NTP configuration file is located in the `/etc/ntp.conf` file on each appliance.

As an alternative to manually editing the NTP configuration files, the vRealize Hardening Tool supports this hardening activity with the Network Time Protocol option.

Procedure

1 Navigate to the `/etc/ntp.conf` configuration file on your virtual appliance host machine.

2 Set the file ownership to **`root:root`**.

3 Set the permissions to **`0640`**.

4 To mitigate the risk of a denial-of-service amplification attack on the NTP service, open the `/etc/ntp.conf` file and ensure that the restrict lines appear in the file.

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

5 Save any changes and close the files.

For information on NTP security notices, see http://support.ntp.org/bin/view/Main/SecurityNotice .

Disable the TCP Timestamp Response

The TCP timestamp response can be used to approximate the remote host's uptime and aid in further attacks. Additionally, some operating systems can be fingerprinted based on the behavior of their TCP time stamps.

Procedure

- Disable the TCP timestamp response on Linux.
  a. Set the value of `net.ipv4.tcp_timestamps` to `0` by running the `sysctl –w net.ipv4.tcp_timestamps=0` command.
  b. Add the `ipv4.tcp_timestamps=0` value in the default `sysctl.conf` file.

SSL and TLS

As a security best practice, ensure that the system is deployed with secure transmission channels.

Configure Strong Protocols for vRealize Operations Manager

Protocols such as SSLv2 and SSLv3 are no longer considered secure. As a best security practice for transport layer protection, provide support for only the TLS protocols such as TLS1.0, TLS 1.1, and TLS 1.2.

Verify that SSLv2 and SSLv3 are disabled in Apache Httpd.

Prerequisites

vRealize Operations Manager disables SSLv2 and SSLv3 by default. Ensure that you disable insecure protocols such as SSLv2 and SSLv3 on all load balancers before you put the system into production.

Procedure

- Open the `/usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` file and verify that the `SSLProtocol All -SSLv2 -SSLv3` entry appears.

  There are various Tomcat https handlers. It is important to note that all https traffic is routed through port 443 and all internal Tomcat ports are blocked by firewall and are not externally exposed.

Configure vRealize Operations Manager to Use Strong Ciphers

For maximum security, you must configure vRealize Operations Manager components to use strong ciphers.

To ensure that only strong ciphers are selected, disable the use of weak ciphers. Configure the server to support only strong ciphers and to use sufficiently large key sizes. Also, configure the ciphers in a suitable order.

Using Strong Ciphers

The encryption cipher negotiated between the server and the browser determines the encryption strength that is used in a TLS session.

vRealize Operations Manager

The following TLS ciphers are acceptable and enabled by default on vRealize Operations Manager vApp.

- TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA

The preferred server cipher is TLS_RSA_WITH_AES_256_CBC_SHA.

Disable Weak Ciphers

Disable cipher suites that do not offer authentication such as NULL cipher suites, NULL, or eNULL. No authentication makes them vulnerable to man-in-the-middle attacks.

You must also disable the anonymous Diffie-Hellman key exchange (ADH), export level ciphers (EXP, ciphers containing DES), key sizes smaller than 128 bits for encrypting payload traffic, the use of MD5 as a hashing mechanism for payload traffic, IDEA Cipher Suites, and RC4 cipher suites because they are all vulnerable to attacks.

Disable Weak Ciphers in Apache HTTPD Handler

Disable the weak ciphers and enable strong ciphers that are used in the Apache HTTPD handler.

Prerequisites

For maximum security, review the Apache HTTPD handler ciphers on vRealize Operations Manager against the list of acceptable ciphers and disable all of the ciphers that are considered weak. This will help to prevent man-in-the middle attacks.

Procedure

1 Open the `/usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` file in a text editor.

2 Verify that the file contains the line `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH:@STRENGTH`.

3 Save the changes you made and close the file.

Diffie-Hellman Key Exchange

Diffie-Hellman key exchange has weaknesses. You are advised to disable all cipher suites that contain DH, DHE, and EDH.

These cipher suites are now disabled by default. These can be enabled if you need to use these cipher suites.

Procedure

- Enable the Diffie-Hellman key exchange.
  a Open the `/usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` file.
  b Find the `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH:@STRENGTH` line.
  c Remove `!DH:` so that the line now reads `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:@STRENGTH`.
  d Save and close the file.

Application Resources that must be Protected

As a security best practice, ensure that the application resources are protected.

Follow the steps to ensure that the application resources are protected.

Procedure

1 Run the `Find / -path /proc -prune -o -type f -perm +6000 -ls` command to verify that the files have a well defined SUID AND GUID bits set.

The following list should appear:

```
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 Run the `find / -path */proc -prune -o -nouser -o -nogroup` command to verify that all the files in the vApp have an owner.

If there are no results, then all the files have an owner.

3 Run the `find / -name "*.*" -type f -perm -a+w | xargs ls -ldb` command to verify that none of the files are world writable files by reviewing permissions of all the files on the vApp.

None of the files should include the permission `xx2`.

4 Run the `find / -path */proc -prune -o ! -user root -o -user admin -print` command to verify that the files are owned by the correct user.

There should be no results as all the files belong to either `root` or `admin`.

5 Ensure that files in the `/usr/lib/vmware-casa/` directory are not world readable.

a Run the `find /usr/lib/vmware-casa/ -type f -perm -o=r` command.

By default, some files in the `/usr/lib/vmware-casa/` directory are world readable. Depending on your level of trust with the user accounts on the vApp, you can ensure that these files are not world readable by running the `chmod -R a=--- /usr/lib/vmware-casa/` file.

6 Ensure that files in the `/usr/lib/vmware-vcops/` directory are read-only by the owner and group.

   a Run the `find /usr/lib/vmware-casa/ -type f -perm -o=r` command.

   By default, some files in the `/usr/lib/vmware-vcops/` directory are world readable. Depending on your level of trust with the user accounts on the vApp, you can ensure that the files are read-only by the owner and group.

7 Ensure that files in the `/usr/lib/vmware-vcopssuite/` directory are world readable.

   a Run the `find /usr/lib/vmware-casa/ -type f -perm -o=r` command.

   By default, some files in the `/usr/lib/vmware-vcopssuite/` directory are world readable. Depending on your level of trust with the user accounts on the vApp, you can ensure that the files are read-only by the owner and group.

8 Ensure that files in the `/usr/lib/vmware-casa/` directory are not world writable.

   a Run the `find /usr/lib/vmware-casa/ -type f -perm -o=w` command.

   There must be no results.

9 Ensure that files in the `/usr/lib/vmware-vcops/` directory are not world writable.

   a Run the `find /usr/lib/vmware-vcops/ -type f -perm -o=w` command.

   There must be no results.

10 Ensure that files in the `/usr/lib/vmware-vcopssuite/` directory are not world writable.

   a Run the `find /usr/lib/vmware-vcopssuite/ -type f -perm -o=w` command.

   There must be no results.

11 Ensure that files in the `/usr/lib/vmware-casa/` directory are world executable.

   a Run the `find /usr/lib/vmware-casa/ -type f -perm -o=x` command.

   There must be no results.

12 Ensure that files in the `/usr/lib/vmware-vcops/` directory are world executable.

   a Run the `find /usr/lib/vmware-vcops/ -type f -perm -o=x` command.

   By default, some files in the `/usr/lib/vmware-vcops/` directory are world executable. Depending on your level of trust with the user accounts on the vApp, you can ensure that the files are world executable by the owner and group by running the `chmod -R a=--- /usr/lib/vmware-vcops/` command.

13 Ensure that files in the `/usr/lib/vmware-vcopssuite/` directory are world executable.

   a Run the `find /usr/lib/vmware-vcopssuite/ -type f -perm -o=x` command.

   There must be no results.

PostgreSQL Client Authentication Configuration

You can configure the system for local `trust` authentication. This allows any local user to connect as a PostgreSQL user, including the database super user without a password.

To provide a strong defense and if you do not have significant trust in all local user accounts, use another authentication method. The md5 method is recommended and set by default. Verify that md5 is set for all local and host connections.

The client authentication configuration settings for the postgres service instance can be found in `/storage/db/vcops/vpostgres/data/pg_hba.conf`. Verify that md5 is set for all local and host connections.

The client authentication configuration settings for the postgres-repl service instance can be found in `/storage/db/vcops/vpostgres/repl/pg_hba.conf`. Verify that md5 is set for all local and host connections.

Disable Web Directory Browsing

As a security best practice, ensure that a user cannot bowse through a directory because it can increase the risk of exposure to directory traversal attacks.

Procedure

- Verify that web directory browsing is disabled for all directories.
  a. Open the `/etc/apache2/default-server.conf` and `/usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` files in a text editor.
  b. Verify that for each `<Directory>` listing, the option called `Indexes` for the relevant tag is omitted from the `Options` line.

Disable Configuration Modes

As a best practice, when you install, configure, or maintain vRealize Operations Manager, you can modify the configuration or settings to enable troubleshooting and debugging of your installation.

Catalog and audit each of the changes you make to ensure that they are properly secured. Do not put the changes into production if you are not sure that your configuration changes are correctly secured.

Managing Nonessential Software Components

To minimize security risks, remove or configure nonessential software from your vRealize Operations Manager host machines.

Configure all software that you do not remove in accordance with manufacturer recommendations and security best practices to minimize its potential to create security breaches.

Secure the USB Mass Storage Handler

Secure the USB mass storage handler to prevent it from loading by default on vRealize appliances and to prevent its use as the USB device handler with the vRealize appliances. Potential attackers can exploit this handler to install malicious software.

Procedure

1. Open the`/etc/modprobe.conf.local` file in a text editor.
2. Ensure that the `install usb-storage /bin/true` line appears in the file.
3. Save the file and close it.

Secure the Bluetooth Protocol Handler

Secure the Bluetooth protocol handler on your vRealize Appliances to prevent potential attackers from exploiting it.

Binding the Bluetooth protocol to the network stack is unnecessary and can increase the attack surface of the host. Prevent the Bluetooth protocol handler module from loading by default on vRealize Appliances.

Procedure

1. Open the `/etc/modprobe.conf.local` file in a text editor.
2. Ensure that the line `install bluetooth /bin/true` appears in this file.

3 Save the file and close it.

Secure the Stream Control Transmission Protocol

Prevent the Stream Control Transmission Protocol (SCTP) module from loading on vRealize appliances by default. Potential attackers could exploit this protocol to compromise your system.

Configure your system to prevent the SCTP module from loading unless it is absolutely necessary. SCTP is an unused IETF-standardized transport layer protocol. Binding this protocol to the network stack increases the attack surface of the host. Unprivileged local processes might cause the kernel to dynamically load a protocol handler by using the protocol to open a socket.

Procedure

1 Open the `/etc/modprobe.conf.local` file in a text editor.

2 Ensure that the following line appears in this file.

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

3 Save the file and close it.

Secure the Datagram Congestion Control Protocol

As part of your system hardening activities, prevent the Datagram Congestion Control Protocol (DCCP) module from loading on vRealize appliances by default. Potential attackers can exploit this protocol to compromise your system.

Avoid loading the DCCP module, unless it is absolutely necessary. DCCP is a proposed transport layer protocol, which is not used. Binding this protocol to the network stack increases the attack surface of the host. Unprivileged local processes can cause the kernel to dynamically load a protocol handler by using the protocol to open a socket.

Procedure

1 Open the `/etc/modprobe.conf.local` file in a text editor.

2 Ensure that the DCCP lines appear in the file.

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

3 Save the file and close it.

Secure Reliable Datagram Sockets Protocol

As part of your system hardening activities, prevent the Reliable Datagram Sockets (RDS) protocol from loading on your vRealize appliances by default. Potential attackers can exploit this protocol to compromise your system.

Binding the RDS protocol to the network stack increases the attack surface of the host. Unprivileged local processes might cause the kernel to dynamically load a protocol handler by using the protocol to open a socket.

Procedure

1 Open the `/etc/modprobe.conf.local` file in a text editor.

2 Ensure that the `install rds /bin/true` line appears in this file.

3 Save the file and close it.

Secure the Transparent Inter-Process Communication Protocol

As part of your system hardening activities, prevent the Transparent Inter-Process Communication protocol (TIPC) from loading on your virtual appliance host machines by default. Potential attackers can exploit this protocol to compromise your system.

Binding the TIPC protocol to the network stack increases the attack surface of the host. Unprivileged local processes can cause the kernel to dynamically load a protocol handler by using the protocol to open a socket.

Procedure

1 Open the `/etc/modprobe.conf.local` file in a text editor.

2 Ensure that the `install tipc /bin/true` line appears in this file.

3 Save the file and close it.

Secure Internet Packet Exchange Protocol

Prevent the Internetwork Packet Exchange (IPX) protocol from loading vRealize appliances by default. Potential attackers could exploit this protocol to compromise your system.

Avoid loading the IPX protocol module unless it is absolutely necessary. IPX protocol is an obsolete network-layer protocol. Binding this protocol to the network stack increases the attack surface of the host. Unprivileged local processes might cause the system to dynamically load a protocol handler by using the protocol to open a socket.

Procedure

1 Open the `/etc/modprobe.conf.local` file in a text editor.

2 Ensure that the line `install ipx /bin/true` appears in this file.

3 Save the file and close it.

Secure Appletalk Protocol

Prevent the Appletalk protocol from loading on vRealize appliances by default. Potential attackers might exploit this protocol to compromise your system.

Avoid loading the Appletalk Protocol module unless it is absolutely necessary. Binding this protocol to the network stack increases the attack surface of the host. Unprivileged local processes might cause the system to dynamically load a protocol handler by using the protocol to open a socket.

Procedure

1 Open the `/etc/modprobe.conf.local` file in a text editor.

2 Ensure that the line `install appletalk /bin/true` appears in this file.

3 Save the file and close it.

Secure DECnet Protocol

Prevent the DECnet protocol from loading on your system by default. Potential attackers might exploit this protocol to compromise your system.

Avoid loading the DECnet Protocol module unless it is absolutely necessary. Binding this protocol to the network stack increases the attack surface of the host. Unprivileged local processes could cause the system to dynamically load a protocol handler by using the protocol to open a socket.

Procedure

1 Open the DECnet Protocol `/etc/modprobe.conf.local` file in a text editor.

2 Ensure that the line `install decnet /bin/true` appears in this file.

3 Save the file and close it.

Secure Firewire Module

Prevent the Firewire module from loading on vRealize appliances by default. Potential attackers might exploit this protocol to compromise your system.

Avoid loading the Firewire module unless it is absolutely necessary.

Procedure

1 Open the `/etc/modprobe.conf.local` file in a text editor.

2 Ensure that the line `install ieee1394 /bin/true` appears in this file.

3 Save the file and close it.

Kernel Message Logging

You can view the kernel print logging specification in the `kernel.printk` specification in the `/etc/sysctl.conf` file.

Ensure that the `kernel.printk` values in the `/etc/sysctl.conf` file is set to `3 4 1 7`.

There are four values specified.

Value	Description
console loglevel	The lowest priority of messages printed to the console.
default loglevel	The lowest level for messages without a specific log level.
-	The lowest possible level for the console log level
-	The default value for console log level.

There are eight possible entries per value.

```
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 */
```

Windows Installed Deployment

Using Windows Time Service

For critical time sourcing, you must disable host time synchronization and use authorized time servers.

You can use authorized time servers in a production environment as a way to track user actions and to identify potential malicious attacks and intrusion through accurate auditing and logging.

SSL and TLS

As a security best practice, ensure that the system is deployed with secure transmission channels.

Configure vRealize Operations Manager to Use Strong Ciphers

The encryption strength that is used in a TLS session is determined by the encryption cipher negotiated between the server and the browser. To ensure that only strong ciphers are selected, you must modify the server to disable the use of weak ciphers. In addition, the ciphers should be configured in a suitable order. You should configure the server to support only strong ciphers and to use sufficiently large key sizes.

Configure Strong Protocols for vRealize Operations Manager

Protocols such as SSLv2 and SSLv3 are no longer considered secure. including SSLv2 and SSLv3. As a best security practice for transport layer protection, provide support for only the TLS protocols.

Prior to production, you must verify that SSLv2 and SSLv3 are disabled.

Disable Weak Ciphers

Disable cipher suites that do not offer authentication such as NULL cipher suites, NULL, or eNULL. No authentication makes them vulnerable to man-in-the-middle attacks.

You must also disable the anonymous Diffie-Hellman key exchange (ADH), export level ciphers (EXP, ciphers containing DES), key sizes smaller than 128 bits for encrypting payload traffic, the use of MD5 as a hashing mechanism for payload traffic, IDEA Cipher Suites, and RC4 cipher suites because they are all vulnerable to attacks.

Disable Weak Ciphers in Apache HTTPD Handler

Disable the weak ciphers and enable strong ciphers that are used in the Apache HTTPD handler.

Prerequisites

For maximum security, review the Apache HTTPD handler ciphers on the vRealize Operations Manager against the list of acceptable ciphers and disable all of the ciphers that are considered weak. This will help to prevent man-in-the middle attacks.

Procedure

1 Open the `C:\vmware\vrealize-operations\vmware-vcopssuite\utilities\conf` file in a text editor.

2 Verify that the file contains the line `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH:@STRENGTH`.

3 Save the changes you made and close the file.

Diffie-Hellman Key Exchange

Diffie-Hellman key exchange has weaknesses. You are advised to disable all cipher suites that contain DH, DHE, and EDH.

These cipher suites are now disabled by default. These can be enabled if you need to use these cipher suites.

Procedure

- Enable the Diffie-Hellman key exchange.
  a. Open the `C:\vmware\vrealize-operations\vmware-vcopssuite\utilities\conf` file.
  b. Find the `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH:@STRENGTH` line.
  c. Remove `!DH:` so that the line now reads `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:@STRENGTH`.
  d. Save and close the file.

Disable Configuration Modes

As a best practice, when you install, configure, or maintain vRealize Operations Manager, you can modify the configuration or settings to enable troubleshooting and debugging of your installation.

Catalog and audit each of the changes you make to ensure that they are properly secured. Do not put the changes into production if you are not sure that your configuration changes are correctly secured.

Verify the Host Server's Secure Baseline

You can use the Microsoft Baseline Security Analyzer (MBSA) to quickly identify that your server has the latest updates or hot fixes. You can use MBSA to install any missing security patches from Microsoft to keep your server up-to-date with Microsoft security recommendations. You can download this tool from Microsoft.

The latest tool, at the time this document was published, can be found here: http://www.microsoft.com/en-us/download/details.aspx?id=7558.

NOTE Contact your Microsoft vendor for guidance on the most appropriate use of this tool.

Verify that the Host Server is Securely Configured

You can use the Windows Security Configuration Wizard (SCW) and the Microsoft Security Compliance Manager toolkit to verify that the host server is securely configured.

Start the SCW from the administrative tools of your Windows server. This tool can identify the roles of your server and the installed features including networking, Windows firewalls, and registry settings. Compare the report with the latest hardening guidance from the relevant Microsoft Security Compliance Manager (SCM) for your Windows server. Based on the results, you can configure the security settings for each feature such as network services, account settings, and Windows firewalls, and apply the settings to your server.

For more information on the SCW tool refer to: http://technet.microsoft.com/en-us/library/cc754997.aspx

NOTE: Contact your Microsoft vendor for guidance on the most appropriate use of these tools.

Linux Installed Deployment

NTP Service

For critical time sourcing, you can disable the host time synchronization and use the Network Time Protocol (NTP). NTP is recommended in production as a means to accurately track user actions and to realize potential malicious attacks and intrusion through accurate audit and log keeping.

The ntp daemon is included on the appliance and is used to provide synchronized time services. You can find the configuration file for NTP in `/etc/ntp.conf`.

SSL and TLS

As a security best practice, ensure that the system is deployed with secure transmission channels.

Configure Strong Protocols for vRealize Operations Manager

Protocols such as SSLv2 and SSLv3 are no longer considered secure. including SSLv2 and SSLv3. As a best security practice for transport layer protection, provide support for only the TLS protocols.

Prior to production, you must verify that SSLv2 and SSLv3 are disabled.

Configure vRealize Operations Manager to Use Strong Ciphers

The encryption strength that is used in a TLS session is determined by the encryption cipher negotiated between the server and the browser. To ensure that only strong ciphers are selected, you must modify the server to disable the use of weak ciphers. In addition, the ciphers should be configured in a suitable order. You should configure the server to support only strong ciphers and to use sufficiently large key sizes.

Disable Weak Ciphers

Disable cipher suites that do not offer authentication such as NULL cipher suites, NULL, or eNULL. No authentication makes them vulnerable to man-in-the-middle attacks.

You must also disable the anonymous Diffie-Hellman key exchange (ADH), export level ciphers (EXP, ciphers containing DES), key sizes smaller than 128 bits for encrypting payload traffic, the use of MD5 as a hashing mechanism for payload traffic, IDEA Cipher Suites, and RC4 cipher suites because they are all vulnerable to attacks.

Disable Weak Ciphers in Apache HTTPD Handler

Disable the weak ciphers and enable strong ciphers that are used in the Apache HTTPD handler.

Prerequisites

For maximum security, review the Apache HTTPD handler ciphers on vRealize Operations Manager against the list of acceptable ciphers and disable all of the ciphers that are considered weak. This will help to prevent man-in-the middle attacks.

Procedure

1. Open the `/usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` file in a text editor.
2. Verify that the file contains the line `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH:@STRENGTH`.
3. Save the changes you made and close the file.

Diffie-Hellman Key Exchange

Diffie-Hellman key exchange has weaknesses. You are advised to disable all cipher suites that contain DH, DHE, and EDH.

These cipher suites are now disabled by default. These can be enabled if you need to use these cipher suites.

Procedure

- Enable the Diffie-Hellman key exchange.
  a. Open the `/usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` file.
  b. Find the `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH:@STRENGTH` line.
  c. Remove `!DH:` so that the line now reads `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:@STRENGTH`.
  d. Save and close the file.

Disable Configuration Modes

As a best practice, when you install, configure, or maintain vRealize Operations Manager, you can modify the configuration or settings to enable troubleshooting and debugging of your installation.

Catalog and audit each of the changes you make to ensure that they are properly secured. Do not put the changes into production if you are not sure that your configuration changes are correctly secured.

Verify the Host Server's Secure Configuration

For the secure operation of vRealize Operations Manager you must secure and verify the hardening activities.

For more information, refer to the Red Hat Enterprise Linux 6 hardening guidance in accordance with your organizations security policies.

Endpoint Operations Management Agent

The Endpoint Operations Management agent adds agent based discovery and monitoring capabilities to vRealize Operations Manager.

The Endpoint Operations Management agent is directly installed on the hosts and may or may not be at the same level of trust as the Endpoint Operations Management server. Therefore, you must verify that the agents are securely installed.

Security Best Practices for Running Endpoint Operations Management Agents

As a security best practice you can follow certain best practices while using user accounts.

- Remove any credentials and server certificate thumbprints that were stored in the `AGENT_HOME/conf/agent.properties` file for a silent installation.
- Use a vRealize Operations Manager user account reserved specifically for Endpoint Operations Management agent registration only. For more information, see the topic called Roles and Privileges in vRealize Operations Manager in the vRealize Operations Manager Help.
- Disable the vRealize Operations Manager user account that you use for agent registration after the installation is over. You must enable the user's access for agent administration activities. For more information, see the topic called Configuring Users and Groups in vRealize Operations Manager in the vRealize Operations Manager Help.
- If a system that runs an agent is compromised, you can revoke the agent certificate using the vRealize Operations Manager user interface by removing the agent resource. See the section called Revoking an Agent for more detail.

Minimum Required Permissions for Agent Functionality

You require permissions to install and modify a service. If you want to discover a running process, the user account you use to run the agent must also have privileges to access the processes and programs. For Windows operating system installations, you require permissions to install and modify a service. If you want to discover a running process, the user account you use to run the agent must also have privileges to access the processes and programs. For Linux installations, you require permission to install the agent as a service, if you install the agent using a RPM installer.

The minimal credentials that are required for the agent to register with the vRealize Operations Manager server are those for a user granted the Agent Manager role, without any assignment to objects within the system.

Linux based Platform Files and Permissions

After you install the Endpoint Operations Management agent, the owner is the user that installs the agent.

The installation directory and file permissions such as 600 and 700, are set to the owner when the user who installs the Endpoint Operations Management agent extracts the tar file or installs the rpm.

NOTE When you extract the zip file, the permissions might not be correctly applied. Verify and ensure that the permissions are correct.

All the files that are created and written to by the agent are given 700 permissions with the owner being the user who runs the agent.

Table 4-1. Linux Files and Permissions

Directory or File	Permissions	Groups or Users	Read	Write	Execute
<agent directory>/bin	700	Owner	r	w	x
		Group	-	-	-
		All	-	-	-
<agent directory>/conf	700	Owner	r	w	x
		Group	-	-	-
		All	-	-	-
<agent directory>/log	700	Owner	r	w	-
		Group	-	-	-
		All	-	-	-
<agent directory>/data	700	Owner	r	w	x
		Group	-	-	-
		All	-	-	-
<agent directory>/bin/ep-agent.bat	600	Owner	r	w	-
		Group	-	-	-
		All	-	-	-
<agent directory>/bin/ep-agent.sh	700	Owner	r	w	x
		Group	-	-	-
		All	-	-	-

Table 4-1. Linux Files and Permissions (Continued)

Directory or File	Permissions	Groups or Users	Read	Write	Execute
<agent directory>/conf/* (all files in the `conf` directory)	600	Owner	r	w	-
		Group	-	-	-
		All	-	-	-
<agent directory>/log/* (all files in the `log` directory)	600	Owner	r	w	-
		Group	-	-	-
		All	-	-	-
<agent directory>/data/* (all files in the `data` directory)	600	Owner	r	w	-
		Group	-	-	-
		All	-	-	-

Windows based Platform Files and Permissions

For a Windows based installation of the Endpoint Operations Management agent, the user installing the agent should have permissions to install and modify the service.

After you install the Endpoint Operations Management agent, the installation folder including all subdirectories and files should only be accessible by the SYSTEM, administrators group, and the installation user. When installing the Endpoint Operations Management agent using `ep-agent.bat`, ensure that the hardening process succeeds. It is advised that the user installing the agent takes note of any error messages. If the hardening process fails, the user can apply these permissions manually.

Table 4-2. Windows Files and Permissions

Directory or File	Groups or Users	Full Control	Modify	Read and Execute	Read	Write
<agent directory>/bin	SYSTEM	X	-	-	-	-
	Administrator	X	-	-	-	-
	Installation User	X	-	-	-	-
	Users		-	-	-	-
<agent directory>/conf	SYSTEM	X	-	-	-	-
	Administrator	X	-	-	-	-
	Installation User	X	-	-	-	-
	Users		-	-	-	-
<agent directory>/log	SYSTEM	X	-	-	-	-
	Administrator	X	-	-	-	-
	Installation User	X	-	-	-	-
	Users		-	-	-	-
<agent directory>/data	SYSTEM	X	-	-	-	-
	Administrator	X	-	-	-	-
	Installation User	X	-	-	-	-
	Users		-	-	-	-

Table 4-2. Windows Files and Permissions (Continued)

Directory or File	Groups or Users	Full Control	Modify	Read and Execute	Read	Write
<agent directory>/bin/hq-agent.bat	SYSTEM	X	-	-	-	-
	Administrator	X	-	-	-	-
	Installation User	X	-	-	-	-
	Users		-	-	-	-
<agent directory>/bin/hq-agent.sh	SYSTEM	X	-	-	-	-
	Administrator	X	-	-	-	-
	Installation User	X	-	-	-	-
	Users		-	-	-	-
<agent directory>/conf/* (all files in the `conf` directory)	SYSTEM	X	-	-	-	-
	Administrator	X	-	-	-	-
	Installation User	X	-	-	-	-
	Users		-	-	-	-
<agent directory>/log/* (all files in the `log` directory)	SYSTEM	X	-	-	-	-
	Administrator	X	-	-	-	-
	Installation User	X	-	-	-	-
	Users		-	-	-	-
<agent directory>/data/* (all files in `data` directory)	SYSTEM	X	-	-	-	-
	Administrator	X	-	-	-	-
	Installation User	X	-	-	-	-
	Users		-	-	-	-

Open Ports on Agent Host

The agent process listens for commands on two ports **127.0.0.1:2144** and **127.0.0.1:32000** that are configurable. These ports might be arbitrarily assigned so the exact port number may vary. The agent does not open ports on external interfaces.

Table 4-3. Minimum Required Ports

Port	Protocol	Direction	Comments
443	TCP	Outgoing	Used by the agent for outgoing connections over HTTP, TCP, or ICMP.
2144*	TCP	Listening	Internal Only. Configurable. The agent process listens on this port. Used for inter-process communication between the agent and the command line that loads and configures it. NOTE The port number is assigned arbitrarily and might differ.
32000*	TCP	Listening	Internal Only. Configurable. The agent process listens on this port. Used for inter-process communication between the agent and the command line that loads and configures it. NOTE The port number is assigned arbitrarily and might differ.

Revoking an Agent

If for any reason you need to revoke an agent, this might occur when a system with a running agent is compromised, you can delete the agent resource from the system. Any subsequent request will fail verification.

Revoke the agent certificate using the vRealize Operations Manager user interface by removing the agent resource. For more information see "Removing the Agent Resource," on page 42.

When a secure state of the system is restored you can reinstate the agent. For more information see "Reinstating an Agent Resource," on page 43.

Removing the Agent Resource

You can revoke the agent certificate using the vRealize Operations Manager user interface by removing the agent resource.

Prerequisites

To preserve the continuity of the resource with previously recorded metric data, take a record of the Endpoint Operations Management agent token that is displayed in the resource details.

Procedure

1 Navigate to the Inventory Explorer in the vRealize Operations Manager user interface.

2 Open the Adapter Types tree.

3 Open the EP Ops Adapter list.

4 Select `EP Ops Agent – *HOST_DNS_NAME*`.

5 Click on the **Edit Object** button.

6 Record the Agent ID, which is the agent token string.

7 Close the **Edit Object** dialog box.

8 Select `EP Ops Agent – *HOST_DNS_NAME*` and click the **Delete Object** button.

Reinstating an Agent Resource

When the secure state of a system is recovered, you can reinstate a revoked agent. This ensures that the agent continues to report on the same resources without losing historical data. To do this you must create a new Endpoint Operations Management token file by using the same token recorded before you remove the agent resource. See the section called Removing The Agent Resource.

Procedure

1 Ensure that you have the recorded Endpoint Operations Management token string.

2 Create the agent token file with the user that runs the agent. Use the resource token recorded prior to removing the agent resource from the vRealize Operations Manager server.

For example, run the command to create a token file containing the 123-456-789 token.

On Linux:

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

On Windows:

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

In the above example, the token file is written to the default token location for that platform.

3 Install a new agent and register it with the vRealize Operations Manager server. Ensure that the agent loaded the token you inserted in the aforementioned token file at the beginning of this setup process.

You must have the Manage Agent privilege to perform this action

Agent Certificate Revocation and Updating Certificates

The reissue flow is initiated from the agent using the `setup` command line argument. When an agent that is already registered uses the `setup` command line argument `ep-agent.sh setup` and fills in the required credentials, a new `registerAgent` command is sent to the server.

The server recognizes that the agent is already registered and sends the agent a new client certificate without creating another agent resource. On the agent side, the new client certificate replaces the old one. In cases where the server certificate is modified and you run the `ep-agent.sh setup` command, you will see a message that asks you to trust the new certificate. You can alternatively provide the new server certificate thumbprint in the `agent.properties` file prior to running the `ep-agent.sh setup` command, in order to make the process silent.

Prerequisites

You need the manage agent privilege to revoke and update certificates.

Procedure

1 On Linux based operating systems, run the `ep-agent.sh setup` command on the agent host.

2 On Windows based operating systems, run the `ep-agent.bat setup` command.

3 If the agent detects that the server certificate has been modified, a message is displayed. Accept the new certificate if you trust it and it is valid.

End Point Operations Management Agent Patching and Updates

If required, new Endpoint Operations Management agent bundles will be available independent of vRealize Operations Manager releases.

Patches or updates are not provided for the Endpoint Operations Management agent. It is recommended that you install the latest available version of the agent that includes the latest security fixes. Communication of critical security fixes will follow the VMware security advisory guidance. See the section on Security Advisories.

Additional Secure Configuration Activities

Verify Server User Account Settings

It is recommended that you verify that no unnecessary user accounts exist for local and domain user accounts and settings.

Restrict any user account not related to the functioning of the application to those accounts required for administration, maintenance, and troubleshooting. Restrict remote access from domain user accounts to the minimum required to maintain the server. Strictly control and audit these accounts.

Delete and Disable Unnecessary Applications

Delete the unnecessary applications from the host servers. Each additional and unnecessary application increases the risk of exposure because of their unknown or unpatched vulnerabilities.

Disabling Unnecessary Ports and Services

Verify the host server's firewall for the list of open ports that allow traffic.

Block all the ports that are not listed as a minimum requirement for vRealize Operations Manager in the "Configuring Ports and Protocols," on page 55 section of this document, or are not required. In addition, audit the services running on your host server and disable those that are not required.

Information Disclosure 5

As a security best practice, configure the vRealize Operations Manager system to limit information available to potential attackers.

As much as possible, minimize the amount of information that your system shares about its identity and version. Hackers and malicious actors can use this information to craft targeted attacks against your Web server or version.

Create the Apache Server Response Header and Omit the Version Information

The Apache HTTP server does not allow you to disable the sending of the response header, because the server header is considered a feature. You can suppress sending the software version, operating system, and so on.

You can create the Apache server response header and omit the version information when you use the companion hardening tool and the `Apache2 Configuration` option.

Procedure

1 Open the `/etc/sysconsfig/apache2` file in a text editor.

2 Verify that the `APACHE_SERVERTOKENS="ProductOnly"` line is set.

3 Run the `etc/init.d/apache2 stop` and `/etc/init.d/apache2 start` commands to restart the Apache server if a change is required.

Network Security and Secure Communication 6

As a security best practice, review and edit the network communication settings of your VMware virtual appliances and host machines. You must also configure the minimum incoming and outgoing ports for vRealize Operations Manager.

This chapter includes the following topics:

Configuring Network Settings for Virtual Application Installation

To ensure that your VMware virtual appliance and host machines allow only safe and essential communication, review and edit their network communication settings.

Prevent User Control of Network Interfaces

As a security best practice, restrict the ability to change the network interface setting to privileged users. If users manipulate network interfaces, it might result in bypassing network security mechanisms or denial of service. Ensure that network interfaces are not configured for user control.

Procedure

1 To verify user control settings, run the `#grep –i '^USERCONTROL=' /etc/sysconfig/network/ifcfg*` command.

2 Make sure that each interface is set to `NO`.

Set the Queue Size for TCP Backlog

As a security best practice, configure a default TCP backlog queue size on VMware appliance host machines. To mitigate TCP denial or service attacks, set an appropriate default size for the TCP backlog queue size. The recommended default setting is 1280.

Procedure

1 Run the `# cat /proc/sys/net/ipv4/tcp_max_syn_backlog` command on each VMware appliance host machine.

2 Set the queue size for TCP backlog.

   a Open the `/etc/sysctl.conf` file in a text editor.

   b Set the default TCP backlog queue size by adding the following entry to the file.

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

   c Save your changes and close the file.

Deny ICMPv4 Echoes to Broadcast Address

Responses to broadcast Internet Control Message Protocol (ICMP) echoes provide an attack vector for amplification attacks and can facilitate network mapping by malicious agents. Configuring your system to ignore ICMPv4 echoes provides protection against such attacks.

Procedure

1 Run the `# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts` command to verify that the system is not sending responses to ICMP broadcast address echo requests.

2 Configure the host system to deny ICMPv4 broadcast address echo requests.

   a Open the `/etc/sysctl.conf` file on a Windows host machine in a text editor.

   b If the value for this entry is not set to `1`, add the `net.ipv4.icmp_echo_ignore_broadcasts=1` entry.

   c Save the changes and close the file.

Configure the Host System to Disable IPv4 Proxy ARP

IPv4 Proxy ARP allows a system to send responses to ARP requests on one interface on behalf of hosts connected to another interface. You must disable IPv4 Proxy ARP to prevent unauthorized information sharing. Disable the setting to prevent leakage of addressing information between the attached network segments.

Procedure

1 Run the `# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp|egrep "default|all"` command to verify whether the Proxy ARP is disabled.

2 Configure the host system to disable IPv4 Proxy ARP.

   a Open the `/etc/sysctl.conf` file in a text editor.

   b If the values are not set to `0`, add the entries or update the existing entries accordingly. Set the value to `0`.

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

   c Save any changes you made and close the file.

Configure the Host System to Ignore IPv4 ICMP Redirect Messages

As a security best practice, verify that the host system ignores IPv4 Internet Control Message Protocol (ICMP) redirect messages. A malicious ICMP redirect message can allow a man-in-the-middle attack to occur. Routers use ICMP redirect messages to notify hosts that a more direct route exists for a destination. These messages modify the host's route table and are unauthenticated.

Procedure

1 Run the `# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects|egrep "default|all"` command on the host system to check whether the host system ignores IPv4 redirect messages.

2 Configure the host system to ignore IPv4 ICMP redirect messages.

   a Open the `/etc/sysctl.conf` file.

   b If the values are not set to `0`, add the following entries to the file or update the existing entries accordingly. Set the value to `0`.

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

   c Save the changes and close the file.

Configure the Host System to Ignore IPv6 ICMP Redirect Messages

As a security best practice, verify that the host system ignores IPv6 Internet Control Message Protocol (ICMP) redirect messages. A malicious ICMP redirect message might allow a man-in-the-middle attack to occur. Routers use ICMP redirect messages to tell hosts that a more direct route exists for a destination. These messages modify the host's route table and are unauthenticated.

Procedure

1 Run the `# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects|egrep "default|all"` command on the host system and check whether it ignores IPv6 redirect messages.

2 Configure the host system to ignore IPv6 ICMP redirect messages.

   a Open the `/etc/sysctl.conf` to configure the host system to ignore the IPv6 redirect messages.

   b If the values are not set to `0`, add the following entries to the file or update the existing entries accordingly. Set the value to `0`.

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

   c Save the changes and close the file.

Configure the Host System to Deny IPv4 ICMP Redirects

As a security best practice, verify that the host system denies IPv4 Internet Control Message Protocol (ICMP) redirects. Routers use ICMP redirect messages to inform servers that a direct route exists for a particular destination. These messages contain information from the system's route table that might reveal portions of the network topology.

Procedure

1 Run the `# grep [01] /proc/sys/net/ipv4/conf/*/send_redirects|egrep "default|all"` on the host system to verify whether it denies IPv4 ICMP redirects.

2 Configure the host system to deny IPv4 ICMP redirects.

   a Open the `/etc/sysctl.conf` file to configure the host system.

   b If the values are not set to `0`, add the following entries to the file or update the existing entries accordingly. Set the value to `0`.

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

   c Save the changes and close the file.

Configure the Host System to Log IPv4 Martian Packets

As a security best practice, verify that the host system logs IPv4 Martian packets. Martian packets contain addresses that the system knows to be invalid. Configure the host system to log the messages so that you can identify misconfigurations or attacks in progress.

Procedure

1 Run the `# grep [01] /proc/sys/net/ipv4/conf/*/log_martians|egrep "default|all"` command to check whether the host logs IPv4 Martian packets.

2 Configure the host system to log IPv4 Martian packets.

   a Open the `/etc/sysctl.conf` file to configure the host system.

   b If the values are not set to `1`, add the following entries to the file or update the existing entries accordingly. Set the value to `1`.

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

   c Save the changes and close the file.

Configure the Host System to use IPv4 Reverse Path Filtering

As a security best practice, configure your host machines to use IPv4 reverse path filtering. Reverse path filtering protects against spoofed source addresses by causing the system to discard packets with source addresses that have no route or if the route does not point towards the originating interface.

Configure your system to use reverse-path filtering whenever possible. Depending on the system role, reverse-path filtering might cause legitimate traffic to be discarded. In such cases, you might need to use a more permissive mode or disable reverse-path filtering altogether.

Procedure

1 Run the `# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter|egrep "default|all"` command on the host system to check whether the system uses IPv4 reverse path filtering.

2 Configure the host system to use IPv4 reverse path filtering.

   a Open the `/etc/sysctl.conf` file to configure the host system.

   b If the values are not set to `1`, add the following entries to the file or update the existing entries accordingly. Set the value to `1`.

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

   c Save the changes and close the file.

Configure the Host System to Deny IPv4 Forwarding

As a security best practice, verify that the host system denies IPv4 forwarding. If the system is configured for IP forwarding and is not a designated router, it could be used to bypass network security by providing a path for communication that is not filtered by network devices.

Procedure

1 Run the `# cat /proc/sys/net/ipv4/ip_forward` command to verify whether the host denies IPv4 forwarding.

2 Configure the host system to deny IPv4 forwarding.

   a Open the `/etc/sysctl.conf` to configure the host system.

   b If the value is not set to `0`, add the following entry to the file or update the existing entry accordingly. Set the value to `0`.

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

   c Save the changes and close the file.

Configure the Host System to Deny Forwarding of IPv4 Source Routed Packets

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than what is configured on the router, which can be used to bypass network security measures.

This requirement applies only to the forwarding of source-routed traffic, such as when IPv4 forwarding is enabled and the system is functioning as a router.

Procedure

1 Run the `# grep [01] /proc/sys/net/ipv4/conf/*/accept_source_route|egrep "default|all"` command to verify whether the system does not use IPv4 source routed packets

2 Configure the host system to deny forwarding of IPv4 source routed packets.

   a Open the `/etc/sysctl.conf` file with a text editor.

   b If the values are not set to `0`, ensure that `net.ipv4.conf.all.accept_source_route=0` and the `et.ipv4.conf.default.accept_source_route=0` are set to `0`.

   c Save and close the file.

Configure the Host System to Deny IPv6 Forwarding

As a security best practice, verify that the host system denies IPv6 forwarding. If the system is configured for IP forwarding and is not a designated router, it can be used to bypass network security by providing a path for communication that is not filtered by network devices.

Procedure

1 Run the `# grep [01] /proc/sys/net/ipv6/conf/*/forwarding|egrep "default|all"` command to verify whether the host denies IPv6 forwarding.

2 Configure the host system to deny IPv6 forwarding.

   a Open the `/etc/sysctl.conf` to configure the host system.

   b If the values are not set to `0`, add the following entries to the file or update the existing entries accordingly. Set the value to `0`.

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

   c Save the changes and close the file.

Configure the Host System to Use IPv4 TCP Syncookies

As a security best practice, verify that the host system uses IPv4 Transmission Control Protocol (TCP) Syncookies. A TCP SYN flood attack might cause a denial of service by filling a system's TCP connection table with connections in the SYN_RCVD state. Syncookies are used so as not to track a connection until a subsequent ACK is received, verifying that the initiator is attempting a valid connection and is not a flood source.

This technique does not operate in a fully standards-compliant manner, but is only activated when a flood condition is detected, and allows defence of the system while continuing to service valid requests.

Procedure

1 Run the `# cat /proc/sys/net/ipv4/tcp_syncookies` command to verify whether the host system uses IPv4 TCP Syncookies.

2 Configure the host system to use IPv4 TCP syncookies.

   a Open the `/etc/sysctl.conf` to configure the host system.

   b If the value is not set to `1`, add the following entry to the file or update the existing entry accordingly. Set the value to `1`.

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

   c Save the changes and close the file.

Configure the Host System to Deny IPv6 Router Advertisements

As a security best practice, verify that the host system denies the acceptance of router advertisements and Internet Control Message Protocol (ICMP) redirects unless necessary. A feature of IPv6 is how systems can configure their networking devices by automatically using information from the network. From a security perspective, it is preferable to manually set important configuration information rather than accepting it from the network in an unauthenticated way.

Procedure

1 Run the `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra|egrep "default|all"` command on the host system to verify whether the system denies the acceptance of router advertisements and ICMP redirects unless necessary.

2 Configure the host system to deny IPv6 router advertisements.

   a Open the `/etc/sysctl.conf` file.

   b If the values are not set to `0`, add the following entries to the file or update the existing entries accordingly. Set the value to `0`.

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

   c Save the changes and close the file.

Configure the Host System to Deny IPv6 Router Solicitations

As a security best practice, verify that host system denies IPv6 router solicitations unless necessary. The router solicitations setting determines how many router solicitations are sent when bringing up the interface. If addresses are assigned statically, there is no need to send any solicitations.

Procedure

1 Run the `# grep [01] /proc/sys/net/ipv6/conf/*/router_solicitations|egrep "default|all"` command to verify whether the host system denies IPv6 router solicitations unless necessary.

2 Configure the host system to deny IPv6 router solicitations.

   a Open the `/etc/sysctl.conf`.

   b If the values are not set to `0`, add the following entries to the file or update the existing entries accordingly. Set the value to `0`.

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

   c Save the changes and close the file.

Configure the Host System to Deny IPv6 Router Preference in Router Solicitations

As a security best practice, verify that your host system denies IPv6 router solicitations unless necessary. The router preference in the solicitations setting determines router preferences. If addresses are assigned statically, there is no need to receive any router preference for solicitations.

Procedure

1 Run the `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_rtr_pref|egrep "default|all"` on the host system to verify whether the host system denies IPv6 router solicitations.

2 Configure the host system to deny IPv6 router preference in router solicitations.

   a Open the `/etc/sysctl.conf` file.

   b If the values are not set to `0`, add the following entries to the file or update the existing entries accordingly. Set the value to `0`.

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

   c Save the changes and close the file.

Configure the Host System to Deny IPv6 Router Prefix

As a security best practice, verify that the host system denies IPv6 router prefix information unless necessary. The `accept ra pinfo` setting controls whether the system accepts prefix information from the router. If addresses are statically assigned, the system does not receive any router prefix information.

Procedure

1 Run the `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_pinfo|egrep "default|all"` to verify if that system denies IPv6 router prefix information.

2 Configure the host system to deny IPv6 router prefix.

   a Open the `/etc/sysctl.conf` file.

   b If the values are not set to `0`, add the following entries to the file or update the existing entries accordingly. Set the value to `0`.

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

   c Save the changes and close the file.

Configure the Host System to Deny IPv6 Router Advertisement Hop Limit Settings

As a security best practice, verify that the host system denies IPv6 router advertisement Hop Limit settings from a router advertisement unless necessary. The `accept_ra_defrtr` setting controls whether the system will accept Hop Limit settings from a router advertisement. Setting it to `0` prevents a router from changing your default IPv6 Hop Limit for outgoing packets.

Procedure

1 Run the `# grep [01] /proc/sys/net/ipv6/conf/*/accept_ra_defrtr|egrep "default|all"` command to verify that the host system denies IPv6 router Hop Limit settings.

2 If the values are not set to `0`, configure the host system to deny IPv6 router advertisement Hop Limit settings.

   a Open the `/etc/sysctl.conf` file.

   b If the values are not set to `0`, add the following entries to the file or update the existing entries accordingly. Set the value to `0`.

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

   c Save the changes and close the file.

Configure the Host System to Deny IPv6 Router Advertisement Autoconf Settings

As a security best practice, verify that the host system denies IPv6 router advertisement `autoconf` settings. The `autoconf` setting controls whether router advertisements can cause the system to assign a global unicast address to an interface.

Procedure

1 Run the `# grep [01] /proc/sys/net/ipv6/conf/*/autoconf|egrep "default|all"` command to verify whether the host system denies IPv6 router advertisement `autoconf` settings.

2 If the values are not set to `0`, configure the host system to deny IPv6 router advertisement autoconf settings.

   a Open the `/etc/sysctl.conf` file.

   b If the values are not set to `0`, add the following entries to the file or update the existing entries accordingly. Set the value to `0`.

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

   c Save the changes and close the file.

Configure the Host System to Deny IPv6 Neighbor Solicitations

As a security best practice, verify that the host system denies IPv6 neighbor solicitations unless necessary. The `dad_transmits` setting determines how many neighbor solicitations are to be sent out per address including global and link-local, when you bring up an interface to ensure the desired address is unique on the network.

Procedure

1 Run the `# grep [01] /proc/sys/net/ipv6/conf/*/dad_transmits|egrep "default|all"` command to verify whether the host system denies IPv6 neighbor solicitations.

2 If the values are not set to `0`, configure the host system to deny IPv6 neighbor solicitations.

   a Open the `/etc/sysctl.conf` file.

   b If the values are not set to `0`, add the following entries to the file or update the existing entries accordingly. Set the value to `0`.

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

   c Save the changes and close the file.

Configure the Host System to Restrict IPv6 Maximum Addresses

As a security best practice, verify that the host restricts the maximum number of IPv6 addresses that can be assigned. The maximum addresses setting determines how many global unicast IPv6 addresses can be assigned to each interface. The default is 16 but you must set the number to the statically configured global addresses required.

Procedure

1 Run the `# grep [1] /proc/sys/net/ipv6/conf/*/max_addresses|egrep "default|all"` command to verify whether the host system restricts the maximum number of IPv6 addresses that can be assigned.

2 If the values are not set to `1`, configure the host system to restrict the maximum number of IPv6 addresses that can be assigned.

   a Open the `/etc/sysctl.conf` file.

   b Add the following entries to the file or update the existing entries accordingly. Set the value to `1`.

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

   c Save the changes and close the file.

Configuring Ports and Protocols

As a security best practice, disable all non-essential ports and protocols.

Configure the minimum incoming and outgoing ports for vRealize Operations Manager components as required for important system components to operate in production.

Minimum Default Incoming Ports

As a security best practice, configure the incoming ports required for vRealize Operations Manager to operate in production.

Table 6-1. Minimum Required Incoming Ports

Port	Protocol	Comments
443	TCP	Used to access the vRealize Operations Manager user interface and the vRealize Operations Manager administrator interface.
123	UDP	Used by vRealize Operations Manager for Network Time Protocol (NTP) synchronization to the master node.
5433	TCP	Used by the master and replica nodes to replicate the global database (vPostgreSQL) when high availability is enabled .
7001	TCP	Used by Cassandra for secure inter-node cluster communication.
9042	TCP	Used by Cassandra for secure client-related communication among nodes.
6061	TCP	Used by clients to connect to the GemFire Locator to get connection information to servers in the distributed system. Also monitors server load to send clients to the least-loaded servers.
10000-10010	TCP and UDP	GemFire Server ephemeral port range used for unicast UDP messaging and for TCP failure detection in a peer-to-peer distributed system.
20000-20010	TCP and UDP	GemFire Locator ephemeral port range used for unicast UDP messaging and for TCP failure detection in a peer-to-peer distributed system.

Table 6-2. Optional Incoming Ports

Port	Protocol	Comments
22	TCP	Optional. Secure Shell (SSH). The SSH service listening on port 22, or any other port, must be disabled in a production environment, and port 22 must be closed.
80	TCP	Optional. Redirects to 443.
3091-3094	TCP	When Horizon View is installed, used to access data for vRealize Operations Manager from Horizon View.

Auditing and Logging on your vRealize Operations Manager System 7

As a security best practice, set up auditing and logging on your vRealize Operations Manager system.

The detailed implementation of auditing and logging is outside the scope of this document.

Remote logging to a central log host provides a secure store for logs. By collecting log files to a central host, you can easily monitor the environment with a single tool. You can also perform aggregate analysis and search for coordinated attacks on multiple entities within the infrastructure. Logging to a secure, centralized log server can help prevent log tampering and also provide a long-term audit record.

This chapter includes the following topics:

Securing the Remote Logging Server

As a security best practice, ensure that the remote logging server can be configured only by an authorized user and is secure.

Attackers who breach the security of your host machine might search for and attempt to tamper with log files to cover their tracks and maintain control without being discovered.

Use an Authorized NTP Server

Ensure that all the host systems use the same relative time source, including the relevant localization offset. You can correlate the relative time source to an agreed-upon time standard such as Coordinated Universal Time (UTC).

You can easily track and correlate an intruder's actions when you review the relevant log files. Incorrect time settings can make it difficult to inspect and correlate log files to detect attacks, and can make auditing inaccurate. You can use at the least three NTP servers from outside time sources or configure a few local NTP servers on a trusted network that obtain their time from at least three outside time sources.

Client Browser Considerations

As a security best practice, do not use vRealize Operations Manager from untrusted or unpatched clients or from clients that use browser extensions.

Index

W