Secure Configuration

vRealize Operations Manager 6.5
You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

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

docfeedback@vmware.com
Contents

Secure Configuration  6

1 vRealize Operations Manager Security Posture  7

2 Secure Deployment of vRealize Operations Manager  8
   Verify the Integrity of Installation Media  8
   Hardening the Deployed Software Infrastructure  8
      Hardening the VMware vSphere Environment  9
   Reviewing Installed and Unsupported Software  9
      Verify Third-Party Software  9
   VMware Security Advisories and Patches  10

3 Secure Configuration of vRealize Operations Manager  11
   Secure the vRealize Operations Manager Console  12
   Change the Root Password  12
      Manage Password Expiry  13
   Managing Secure Shell, Administrative Accounts, and Console Access  13
      Enable or Disable Secure Shell on a vRealize Operations Manager node  14
      Create a Local Administrative Account for Secure Shell  14
      Restrict Secure Shell Access  15
      Maintain Secure Shell Key File Permissions  16
      Harden the Secure Shell Server Configuration  16
      Harden the Secure Shell Client Configuration  17
      Disable Direct Logins as Root  17
      Disable SSH Access for the Admin User Account  18
   Set Boot Loader Authentication  18
   Single-User or Maintenance Mode Authentication  19
   Monitor Minimal Necessary User Accounts  19
   Monitor Minimal Necessary Groups  19
   Resetting the vRealize Operations Manager Administrator Password (Linux)  20
   Configure NTP on VMware Appliances  21
   Disable the TCP Timestamp Response on Linux  21
   Enable FIPS 140-2 Mode  21
   TLS for Data in Transit  22
      Configure Strong Protocols for vRealize Operations Manager  22
      Configure vRealize Operations Manager to Use Strong Ciphers  24
   Application Resources That Must be Protected  26
   Configure PostgreSQL Client Authentication  27
Apache Configuration  27
  Disable Web Directory Browsing  27
  Remove the Sample Code for the Apache2 Server  28
  Verify Server Tokens for the Apache2 Server  28
  Disable the Trace Method for the Apache2 Server  28

Disable Configuration Modes  29

Managing Nonessential Software Components  29
  Secure the USB Mass Storage Handler  29
  Secure the Bluetooth Protocol Handler  29
  Secure the Stream Control Transmission Protocol  30
  Secure the Datagram Congestion Control Protocol  30
  Secure Reliable Datagram Sockets Protocol  30
  Secure the Transparent Inter-Process Communication Protocol  31
  Secure Internet Packet Exchange Protocol  31
  Secure Appletalk Protocol  31
  Secure DECnet Protocol  32
  Secure Firewire Module  32
  Kernel Message Logging  32

Linux Installed Deployment  33
  Enabling NTP Service  33
  TLS for Data in Transit  33

Endpoint Operations Management Agent  35
  Minimum Required Permissions for Agent Functionality  35
  Open Ports on Agent Host  38
  Revoking an Agent  39
  Agent Certificate Revocation and Update of Certificates  40
  Patching and Updating the Endpoint Operations Management Agent  41

Additional Secure Configuration Activities  41
  Verify Server User Account Settings  41
  Delete and Disable Unnecessary Applications  41
  Disabling Unnecessary Ports and Services  41

Network Security and Secure Communication  42

Configuring Network Settings for Virtual Application Installation  42
  Prevent User Control of Network Interfaces  42
  Set the Queue Size for TCP Backlog  42
  Deny ICMPv4 Echoes to Broadcast Address  43
  Configure the Host System to Disable IPv4 Proxy ARP  43
  Configure the Host System to Ignore IPv4 ICMP Redirect Messages  44
  Configure the Host System to Ignore IPv6 ICMP Redirect Messages  44
Configure the Host System to Deny IPv4 ICMP Redirects 45
Configure the Host System to Log IPv4 Martian Packets 45
Configure the Host System to use IPv4 Reverse Path Filtering 45
Configure the Host System to Deny IPv4 Forwarding 46
Configure the Host System to Deny Forwarding of IPv4 Source Routed Packets 46
Configure the Host System to Deny IPv4 Forwarding 47
Configure the Host System to Use IPv4 TCP Syncookies 47
Configure the Host System to Deny IPv6 Router Advertisements 48
Configure the Host System to Deny IPv6 Router Solicitations 48
Configure the Host System to Deny IPv6 Router Preference in Router Solicitations 49
Configure the Host System to Deny IPv6 Router Prefix 49
Configure the Host System to Deny IPv6 Router Advertisement Hop Limit Settings 50
Configure the Host System to Deny IPv6 Router Advertisement Autoconf Settings 50
Configure the Host System to Deny IPv6 Neighbor Solicitations 51
Configure the Host System to Restrict IPv6 Maximum Addresses 51
Configuring Ports and Protocols 52
Minimum Default Incoming Ports 52

5 Auditing and Logging on your vRealize Operations Manager System 54
Securing the Remote Logging Server 54
Use an Authorized NTP Server 54
Client Browser Considerations 55
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.

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.
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 type is also discussed:

- Linux Installed Deployment

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

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:

- Verify the Integrity of Installation Media
- Hardening the Deployed Software Infrastructure
- Reviewing Installed and Unsupported Software
- VMware Security Advisories and Patches

Verify 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 the 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. x-. 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.


**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.

**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 [http://www.vmware.com/security/hardening-guides.html](http://www.vmware.com/security/hardening-guides.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/](http://www.vmware.com/security/advisories/).
Secure Configuration of vRealize Operations Manager

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
- Change the Root Password
- Managing Secure Shell, Administrative Accounts, and Console Access
- Set Boot Loader Authentication
- Single-User or Maintenance Mode Authentication
- Monitor Minimal Necessary User Accounts
- Monitor Minimal Necessary Groups
- Resetting the vRealize Operations Manager Administrator Password (Linux)
- Configure NTP on VMware Appliances
- Disable the TCP Timestamp Response on Linux
- Enable FIPS 140-2 Mode
- TLS for Data in Transit
- Application Resources That Must be Protected
- Configure PostgreSQL Client Authentication
- Apache Configuration
- Disable Configuration Modes
- Managing Nonessential Software Components
- Linux Installed Deployment
- Endpoint Operations Management Agent
- Additional Secure Configuration Activities
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.
To verify the hash of the root password, log in as root and run the `# more /etc/shadow` command. The hash information appears.

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.

**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.

Procedure

1. Log in as root and run the following commands.

```
# useradd -d /home/vropsuser -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
```

**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/securetty 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.

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Daemon Protocol</td>
<td>Protocol 2</td>
</tr>
<tr>
<td>Ciphers</td>
<td>Ciphers aes256-ctr,aes128-ctr</td>
</tr>
<tr>
<td>TCP Forwarding</td>
<td>AllowTCPForwarding no</td>
</tr>
<tr>
<td>Server Gateway Ports</td>
<td>Gateway Ports no</td>
</tr>
<tr>
<td>X11 Forwarding</td>
<td>X11Forwarding no</td>
</tr>
<tr>
<td>SSH Service</td>
<td>Use the AllowGroups field and specify a group permitted to access and add members to the secondary group for users permitted to use the service.</td>
</tr>
<tr>
<td>GSSAPI Authentication</td>
<td>GSSAPIAuthentication no, if unused</td>
</tr>
<tr>
<td>Kerberos Authentication</td>
<td>KerberosAuthentication no, if unused</td>
</tr>
<tr>
<td>Local Variables (AcceptEnv global option)</td>
<td>Set to disabled by commenting out or enabled for only LC_* or LANG variables</td>
</tr>
<tr>
<td>Tunnel Configuration</td>
<td>PermitTunnel no</td>
</tr>
</tbody>
</table>
Secure Configuration

<table>
<thead>
<tr>
<th>Setting</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Sessions</td>
<td>MaxSessions 1</td>
</tr>
<tr>
<td>Strict Mode Checking</td>
<td>Strict Modes yes</td>
</tr>
<tr>
<td>Privilege Separation</td>
<td>UsePrivilegeSeparation yes</td>
</tr>
<tr>
<td>rhosts RSA Authentication</td>
<td>RhostsRSAAuthentication no</td>
</tr>
<tr>
<td>Compression</td>
<td>Compression delayed or Compression no</td>
</tr>
<tr>
<td>Message Authentication code</td>
<td>MACs hmac-sha1</td>
</tr>
<tr>
<td>User Access Restriction</td>
<td>PermitUserEnvironment no</td>
</tr>
</tbody>
</table>

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.

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

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.

Prerequisites

- Complete the steps in the topic called Create a Local Administrative Account for Secure Shell.
- Verify that you have tested accessing the system as an administrator before you disable direct root logins.
Procedure
1. Log in as root and navigate to the /etc/securetty file.
   You can access this file from the command prompt.
2. Replace the tty1 entry with console.

Disable SSH Access for the Admin User Account

As a security best practice, you can disable SSH access for the admin user account. The vRealize Operations Manager admin account and the Linux admin account share the same password. Disabling SSH access to the admin user enforces defense in depth by ensuring all users of SSH first login to a lesser privileged service account with a password that differs from the vRealize Operations Manager admin account and then switch user to a higher privilege such as the admin or root.

Procedure
1. Edit the /etc/ssh/sshd_config file.
   You can access this file from the command prompt.
2. Add the DenyUsers admin entry anywhere in the file and save the file.
3. To restart the sshd server, run the service sshd restart command.

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.

Procedure

- Review the `/etc/inittab` file and ensure that the following two lines appear:

  ```
  ls:S:wait:/etc/init.d/rc S
  ~~: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
  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 minimum necessary groups and group membership.

  ```
  audio:x:17:
  bin:x:1:daemon
  ```
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 vApp 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. You must configure a trusted remote NTP server for time synchronization. The NTP server must be an authoritative time server or at least synchronized with an authoritative time server.

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.

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 on Linux

Use the TCP timestamp response 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. To set the value of net.ipv4.tcp_timestamps to 0, run the `sysctl -w net.ipv4.tcp_timestamps=0` command.
  b. Add the `ipv4.tcp_timestamps=0` value in the default `sysctl.conf` file.

Enable FIPS 140-2 Mode

The version of OpenSSL that is shipped with vRealize Operations Manager 6.3 and later releases is FIPS 140-2 certified. However, the FIPS mode is not enabled by default.
You can enable the FIPS mode if there is a security compliance requirement to use FIPS certified cryptographic algorithms with the FIPS mode enabled.

**Procedure**

1. To replace the `mod_ssl.so` file run the following command:

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

2. Modify your Apache2 configuration by editing the `/etc/apache2/ssl-global.conf` file.

3. Search for the `<IfModule mod_ssl.c>` line and add the `SSLFIPS on` directive below it.

4. To reset the Apache configuration, run the `service apache2 restart` command.

**TLS for Data in Transit**

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. In addition, it is recommended that you disable TLS 1.0. Enable only TLS 1.1 and TLS 1.2.

**Verify the Correct Use of Protocols in Apache HTTPD**

vRealize Operations Manager disables SSLv2 and SSLv3 by default. You must disable weak protocols on all load balancers before you put the system into production.

**Procedure**

1. Run the `grep SSLProtocol /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf | grep -v '#'` command from the command prompt to verify that SSLv2 and SSLv3 are disabled.

   If the protocols are disabled, the command returns the following output: `SSLProtocol All -SSLv2 -SSLv3`

2. To also disable the TLS 1.0 protocol, run the `sed -i "/^[^#]*SSLProtocol/ c\SSLProtocol All -SSLv2 -SSLv3 -TLSv1" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` command from the command prompt.

3. To restart the Apache2 server, run the `/etc/init.d/apache2 restart` command from the command prompt.

**Verify the Correct Use of Protocols in the GemFire TLS Handler**

vRealize Operations Manager disables SSLv3 by default. You must disable weak protocols on all load balancers before you put the system into production.
Procedure

1 Verify that the protocols are enabled. To verify that the protocols are enabled, run the following commands on each node:

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

The following result is expected:

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

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

The following result is expected:

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

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

The following result is expected:

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

2 Disable TLS 1.0.
   a Navigate to the administrator user interface at url/admin.
   b Click Bring Offline.
   c To disable SSLv3 and TLS 1.0, run the following commands:

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

Repeat this step for each node
   d Navigate to the administrator user interface.
   e Click Bring Online.

3 Reenable TLS 1.0.
   a Navigate to the administrator user interface to bring the cluster offline: url/admin.
   b Click Bring Offline.
To ensure that SSLv3 and TLS 1.0 are disabled, run the following commands:

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

Repeat this step for each node.

d Navigate to the administrator user interface to bring the cluster online.

e Click **Bring Online**.

**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.

vRealize Operations Manager disables the use of cipher suites using the DHE key exchange by default. Ensure that you disable the same weak cipher suites on all load balancers before you put the system into production.

**Using Strong Ciphers**

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

**Verify the Correct Use of Cipher Suites in Apache HTTPD**

For maximum security, verify the correct use of cipher suites in Apache httpd.

**Procedure**

1. To verify the correct use of cipher suites in Apache httpd, run the `grep SSLCipherSuite /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf | grep -v '#'` command from the command prompt.

   If Apache httpd uses the correct cipher suites, the command returns the following output:
   ```bash
   SSLCipherSuite kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES::ECDH+AESGCM:kECDH+AES::RSA+AES::
aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH
   ```

2. To configure the correct use of cipher suites, run the `sed -i "/^\[^#\]*SSLCipherSuite/ c \SSLCipherSuite kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES::ECDH+AES::RSA+AES::
aNULL\!ADH\:!EXP\:!MD5\:!3DES\:!CAMELLIA\:!PSK\:!SRP\:!DH" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` command from the command prompt.

   Run this command if the output in Step 1 is not as expected.
This command disables all cipher suites that use DH and DHE key exchange methods.

3 Run the `/etc/init.d/apache2 restart` command from the command prompt to restart the Apache2 server.

4 To reenable DH, remove `!DH` from the cipher suites by running the `sed -i "/^[^#]*SSLCipherSuite/ c\SSLCipherSuite kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AESGCM:RSA+AES:ECDH+AESGCM:!null:!adH:!exp:!MD5:!3DES:!camellia:!PSK:!SRP" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf` command from the command prompt.

5 Run the `/etc/init.d/apache2 restart` command from the command prompt to restart the Apache2 server.

Verify the Correct Use of Cipher Suites in GemFire TLS Handler

For maximum security, verify the correct use of cipher suites in GemFire TLS Handler.

Procedure

1 To verify that the cipher suites are enabled, run the following commands on each node to verify that the protocols are enabled:

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

2 Configure the correct cipher suites.
   a Navigate to the administrator user interface at `URL/admin`
   b To bring the cluster offline, click **Bring Offline**.
   c To configure the correct cipher suites, run the following commands:

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

   Repeat this step for each node.
d Navigate to the administrator user interface at URL/admin.

e Click Bring Online.

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 appears:

<table>
<thead>
<tr>
<th>Owner</th>
<th>Type</th>
<th>Permissions</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>polkituser</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>/usr/lib/PolicyKit/polkit-set-default-helper</td>
</tr>
<tr>
<td>root</td>
<td>polkituser</td>
<td>rwxr-sr-x</td>
<td>/usr/lib/PolicyKit/polkit-grant-helper</td>
</tr>
<tr>
<td>root</td>
<td>polkituser</td>
<td>rwxr-sr-x</td>
<td>/usr/lib/PolicyKit/polkit-explicit-grant-helper</td>
</tr>
<tr>
<td>root</td>
<td>polkituser</td>
<td>rwxr-sr-x</td>
<td>/usr/lib/PolicyKit/polkit-revoke-helper</td>
</tr>
<tr>
<td>root</td>
<td>polkituser</td>
<td>rwsr-x---</td>
<td>/usr/lib/PolicyKit/polkit-grant-helper-pam</td>
</tr>
<tr>
<td>root</td>
<td>polkituser</td>
<td>rwxr-sr-x</td>
<td>/usr/lib/PolicyKit/polkit-read-auth-helper</td>
</tr>
<tr>
<td>root</td>
<td>shadow</td>
<td>rwsr-xr-x</td>
<td>/usr/bin/chsh</td>
</tr>
<tr>
<td>root</td>
<td>shadow</td>
<td>rwsr-xr-x</td>
<td>/usr/bin/gpasswd</td>
</tr>
<tr>
<td>root</td>
<td>shadow</td>
<td>rwsr-xr-x</td>
<td>/usr/bin/expiry</td>
</tr>
<tr>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>/usr/bin/sudo</td>
</tr>
<tr>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>/usr/bin/newgrp</td>
</tr>
<tr>
<td>root</td>
<td>shadow</td>
<td>rwsr-xr-x</td>
<td>/usr/bin/chage</td>
</tr>
<tr>
<td>root</td>
<td>shadow</td>
<td>rwsr-xr-x</td>
<td>/usr/bin/chfn</td>
</tr>
<tr>
<td>root</td>
<td>trusted</td>
<td>rwsr-xr-x</td>
<td>/usr/bin/crontab</td>
</tr>
<tr>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>/usr/lib64/pt_chown</td>
</tr>
<tr>
<td>mail</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>/usr/sbin/sendmail</td>
</tr>
<tr>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>/bin/ping6</td>
</tr>
<tr>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>/bin/su</td>
</tr>
<tr>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>/bin/ping</td>
</tr>
<tr>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>/bin/umount</td>
</tr>
<tr>
<td>root</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>/bin/mount</td>
</tr>
<tr>
<td>messagebus</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>/lib64/dbus-1/dbus-daemon-launch-helper</td>
</tr>
<tr>
<td>shadow</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>/sbin/unix_chkpwd</td>
</tr>
<tr>
<td>shadow</td>
<td>root</td>
<td>rwsr-xr-x</td>
<td>/sbin/unix2_chkpwd</td>
</tr>
</tbody>
</table>

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

All the files have an owner if there are no results.

3 Run the `find / -name "*.k" -type f -perm -a+w | xargs ls -ld` 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 must 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.

All the files belong to either root or admin if there are no results.

5 Run the find /usr/lib/vmware-casa/ -type f -perm -o=w command to ensure that files in the /usr/lib/vmware-casa/ directory are not world writable.

There must be no results.

6 Run the find /usr/lib/vmware-vcops/ -type f -perm -o=w command to ensure that files in the /usr/lib/vmware-vcops/ directory are not world writable.

There must be no results.

7 Run the find /usr/lib/vmware-vcopssuite/ -type f -perm -o=w command to ensure that files in the /usr/lib/vmware-vcopssuite/ directory are not world writable.

There must be no results.

Configure PostgreSQL Client Authentication

You can configure the system for client authentication. You can configure the system for local trust authentication. This allows any local user, including the database super user to connect as a PostgreSQL user without a password. If you want 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 set by default. Verify that md5 is set for all local and host connections.

You can find the client authentication configuration settings for the postgres service instance 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.

Note  Do not modify client configuration settings for the postgres user account.

Apache Configuration

Disable Web Directory Browsing

As a security best practice, ensure that a user cannot browse 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.
  b. Verify that for each <Directory> listing, the option called Indexes for the relevant tag is omitted from the Options line.

Remove the Sample Code for the Apache2 Server

Apache includes two sample Common Gateway Interface (CGI) scripts, printenv and test-cgi. A production Web server must contain only components that are operationally necessary. These components have the potential to disclose critical information about the system to an attacker.

As a security best practice, delete the CGI scripts from the cgi-bin directory.

Procedure

- To remove test-cgi and printenv scripts, run the rm /usr/share/doc/packages/apache2/test-cgi and rm /usr/share/doc/packages/apache2/printenv commands.

Verify Server Tokens for the Apache2 Server

As part of your system hardening process, verify server tokens for the Apache2 server. The Web server response header of an HTTP response can contain several fields of information. Information includes the requested HTML page, the Web server type and version, the operating system and version, and ports associated with the Web server. This information provides malicious users important information without the use of extensive tools.

The directive ServerTokens must be set to Prod. For example, ServerTokens Prod. This directive controls whether the response header field of the server that is sent back to clients includes a description of the operating system and information about compiled-in modules.

Procedure

1. To verify server tokens, run the cat /etc/apache2/sysconfig.d/global.conf | grep ServerTokens command.
2. To modify ServerTokens OS to ServerTokens Prod, run the sed -i 's/\(ServerTokens\s+\)OS/\1Prod/g' /etc/apache2/sysconfig.d/global.conf command.

Disable the Trace Method for the Apache2 Server

In standard production operations, use of diagnostics can reveal undiscovered vulnerabilities that lead to compromised data. To prevent misuse of data, disable the HTTP Trace method.

Procedure

1. To verify the Trace method for the Apache2 server, run the following command grep TraceEnable /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf.
2 To disable the Trace method for the Apache2 server, run the following command:

```
sed -i "/^[^#]*TraceEnable/ c\TraceEnable off" /usr/lib/vmware-vcopssuite/utilities/conf/vcops-apache.conf.
```

**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.
Secure Configuration

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**

The `kernel.printk` specification in the `/etc/sysctl.conf` file specifies the kernel print logging specifications.

There are 4 values specified:

- `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 */

Set the kernel.printk values to 3 4 1 7 and ensure that the line kernel.printk=3 4 1 7 exists in the /etc/sysctl.conf file.

Linux Installed Deployment

You can enable the Network Time Protocol (NTP) service and ensure that the system is deployed with secure transmission channels.

Enabling NTP Service

For critical time sourcing, you can disable the host time synchronization and use the Network Time Protocol (NTP). NTP in production is 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.

TLS for Data in Transit

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, you must configure the ciphers in a suitable order. You must 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. To prevent man-in-the-middle attacks, 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.

Procedure

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

Enable Diffie-Hellman Key Exchange

Diffie-Hellman key exchange has weaknesses. You must disable all cipher suites that contain DH, DHE, and EDH. These cipher suites are disabled by default. These can be enabled if you need to use them.

Procedure

2. Find the line `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:!DH:@STRENGTH`.
3. Remove `!DH:` so that the line reads `SSLCipherSuite HIGH:!aNULL!ADH:!EXP:!MD5:!3DES:!CAMELLIA:!PSK:!SRP:@STRENGTH`.
4. 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.
Verifying 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, see the Red Hat Enterprise Linux 6 hardening guidance in accordance with your organization’s 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 installed on the hosts directly and might or might not be at the same level of trust as the Endpoint Operations Management server. Therefore, you must verify that the agents are securely installed.


You must follow certain security best practices while using user accounts.

- For a silent installation, remove any credentials and server certificate thumbprints that were stored in the AGENT_HOME/conf/agent.properties file.
- Use a vRealize Operations Manager user account reserved specifically for Endpoint Operations Management agent registration. 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. For Linux installations, you require permission to install the agent as a service, if you install the agent using a RPM installer.

The minimum 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 3-1. Linux Files and Permissions**

<table>
<thead>
<tr>
<th>Directory or File</th>
<th>Permissions</th>
<th>Groups or Users</th>
<th>Read</th>
<th>Write</th>
<th>Execute</th>
</tr>
</thead>
<tbody>
<tr>
<td>agent directory/bin</td>
<td>700</td>
<td>Owner</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>agent directory/conf</td>
<td>700</td>
<td>Owner</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>agent directory/log</td>
<td>700</td>
<td>Owner</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>agent directory/data</td>
<td>700</td>
<td>Owner</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>agent directory/bin/ep-agent.bat</td>
<td>600</td>
<td>Owner</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>agent directory/bin/ep-agent.sh</td>
<td>700</td>
<td>Owner</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>agent directory/conf/* (all files in the conf directory)</td>
<td>600</td>
<td>Owner</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>agent directory/log/* (all files in the log directory)</td>
<td>600</td>
<td>Owner</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
Windows Based Platform Files and Permissions

For a Windows based installation of the Endpoint Operations Management agent, the user installing the agent must 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, the administrators group, and the installation user. When you install the Endpoint Operations Management agent using `ep-agent.bat`, ensure that the hardening process succeeds. As the user installing the agent, it is advised that you take note of any error messages. If the hardening process fails, the user can apply these permissions manually.

Table 3-2. Windows Files and Permissions

<table>
<thead>
<tr>
<th>Directory or File</th>
<th>Groups or Users</th>
<th>Full Control</th>
<th>Modify</th>
<th>Read and Execute</th>
<th>Read</th>
<th>Write</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;agent directory&gt;/bin</code></td>
<td>SYSTEM</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Installation</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>User</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;agent directory&gt;/conf</td>
<td>SYSTEM</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Installation</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>User</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;agent directory&gt;/log</td>
<td>SYSTEM</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Installation</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>User</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;agent directory&gt;/data</td>
<td>SYSTEM</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Administrator</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Installation</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>User</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

VMware, Inc.
## Directory or File

<table>
<thead>
<tr>
<th>Groups or Users</th>
<th>Full Control</th>
<th>Modify</th>
<th>Read and Execute</th>
<th>Read</th>
<th>Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;agent directory&gt;/bin/hq-agent.bat</td>
<td>SYSTEM</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Administrator</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Installation User</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Users</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>&lt;agent directory&gt;/bin/hq-agent.sh</td>
<td>SYSTEM</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Administrator</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Installation User</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Users</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>&lt;agent directory&gt;/conf/* (all files in the conf directory)</td>
<td>SYSTEM</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Administrator</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Installation User</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Users</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>&lt;agent directory&gt;/log/* (all files in the log directory)</td>
<td>SYSTEM</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Administrator</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Installation User</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Users</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>&lt;agent directory&gt;/data/* (all files in the data directory)</td>
<td>SYSTEM</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Administrator</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Installation User</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Users</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

## 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, and so, the exact port number might vary. The agent does not open ports on external interfaces.
Table 3-3. Minimum Required Ports

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

Revoking an Agent

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

Use the vRealize Operations Manager user interface to revoke the agent certificate by removing the agent resource. For more information, see Removing the Agent Resource.

When the system is secured again, you can reinstate the agent. For more information, see Reinstate an Agent Resource.

Removing the Agent Resource

You can use the vRealize Operations Manager to revoke the agent certificate 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 **Edit Object**.
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 **Delete Object**.
Reinstate 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 removed the agent resource. See the section called Removing The Agent Resource.

Prerequisites

- Ensure that you have the recorded Endpoint Operations Management token string.
- Use the resource token recorded prior to removing the agent resource from the vRealize Operations Manager server.
- Ensure that you have the Manage Agent privilege.

Procedure

1. Create the agent token file with the user that runs the agent.
   
   For example, run the command to create a token file containing the 123-456-789 token.
   
   - On Linux:
     ```bash
     echo 123-456-789 > /etc/epops/epops-token
     ```
   
   - On Windows:
     ```cmd
     echo 123-456-789 > %PROGRAMDATA%\VMware\Ep Ops Agent\epops-token
     ```
   
   In the example, the token file is written to the default token location for that platform

2. Install a new agent and register it with the vRealize Operations Manager server. Ensure that the agent loads the token you inserted in the token file.
   
   You must have the Manage Agent privilege to perform this action.

Agent Certificate Revocation and Update of 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 detects 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

Manage agent privilege to revoke and update certificates.
Procedure

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

  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.

Patching and Updating the Endpoint Operations Management Agent

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

Patches or updates are not provided for the Endpoint Operations Management agent. You must install the latest available version of the agent that includes the latest security fixes. Critical security fixes will be communicated as per the VMware security advisory guidance. See the topic on Security Advisories.

Additional Secure Configuration Activities

Verify the server user accounts and delete unnecessary applications from the host servers. Block unnecessary ports and disable the services running on your host server that are not required.

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 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.
Network Security and Secure Communication

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
- Configuring Ports and Protocols

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 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.
Secure Configuration

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/sysct1.conf` file 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 `net.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.

   \[
   \text{net.ipv4.tcp_syncookies=1}
   \]
   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.

   \[
   \begin{align*}
   \text{net.ipv6.conf.all.accept_ra} &= 0 \\
   \text{net.ipv6.conf.default.accept_ra} &= 0
   \end{align*}
   \]
   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.

```plaintext
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.

```plaintext
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.
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>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>Used to access the vRealize Operations Manager user interface and the vRealize Operations Manager administrator interface.</td>
</tr>
<tr>
<td>123</td>
<td>UDP</td>
<td>Used by vRealize Operations Manager for Network Time Protocol (NTP) synchronization to the master node.</td>
</tr>
<tr>
<td>5433</td>
<td>TCP</td>
<td>Used by the master and replica nodes to replicate the global database (vPostgreSQL) when high availability is enabled.</td>
</tr>
<tr>
<td>7001</td>
<td>TCP</td>
<td>Used by Cassandra for secure inter-node cluster communication. Do not expose this port to the internet. Add this port to a firewall.</td>
</tr>
<tr>
<td>9042</td>
<td>TCP</td>
<td>Used by Cassandra for secure client-related communication among nodes. Do not expose this port to the internet. Add this port to a firewall.</td>
</tr>
<tr>
<td>6061</td>
<td>TCP</td>
<td>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.</td>
</tr>
<tr>
<td>Port</td>
<td>Protocol</td>
<td>Comments</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>10000-10010</td>
<td>TCP and UDP</td>
<td>GemFire Server ephemeral port range used for unicast UDP messaging and for TCP failure detection in a peer-to-peer distributed system.</td>
</tr>
<tr>
<td>20000-20010</td>
<td>TCP and UDP</td>
<td>GemFire Locator ephemeral port range used for unicast UDP messaging and for TCP failure detection in a peer-to-peer distributed system.</td>
</tr>
</tbody>
</table>

### Table 4-2. Optional Incoming Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>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.</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>Optional. Redirects to 443.</td>
</tr>
<tr>
<td>3091-3101</td>
<td>TCP</td>
<td>When Horizon View is installed, used to access data for vRealize Operations Manager from Horizon View.</td>
</tr>
</tbody>
</table>
Auditing and Logging on your vRealize Operations Manager System

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
- Use an Authorized NTP Server
- Client Browser Considerations

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 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.