Secure Configuration

29 FEB 2024

VMware Aria Operations for Logs 8.16

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

https://docs.vmware.com/

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

Contents

Secure Configuration

The documentation for *Secure Configuration* is intended to serve as a secure baseline for the deployment of VMware Aria Operations for Logs. 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 VMware Aria Operations for Logs.

VMware Aria Operations for Logs Security Posture

1

The security posture of VMware Aria Operations for Logs 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.

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 VMware Aria Operations for Logs 2

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

After you download the media, use the MD5/SHA1/SHA256 sum value to verify the integrity of the download. Always verify the MD5/SHA1/ SHA256 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/ SHA256 hash output with the value posted on the VMware website.

  SHA1, MD5 or SHA256 hash should match.

  Note The VMware Aria Operations for Logs installation files are signed by the VMware software publishing certificate. VMware Aria Operations for Logs validates the signature of the files 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

VMware Aria Operations for Logs relies on a secure VMware vSphere environment to achieve the greatest benefits and a secure infrastructure.

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

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

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 VMware Aria Operations for Logs 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 VMware Aria Operations for Logs release, as this will include the most recent security fixes also.

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

Secure Configuration of VMware Aria Operations for Logs

3

As a security best practice, you must secure the VMware Aria Operations for Logs 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 Log Insight.

This chapter includes the following topics:

Secure the VMware Aria Operations for Logs Console

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

Prerequisites

Install VMware Aria Operations for Logs.

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, VMware Aria Operations for Logs remote terminal sessions are deactivated by default.

2. Log in as root.

   VMware Aria Operations for Logs does not allow you to access the command prompt until you create a root password.

3. At the prompt for a new password, enter the root password that you want and note it for future reference.
4. Reenter the root password.
5. Log out of the console.

Enabling FIPS 140-2

FIPS 140-2 accreditation validates that an encryption solution meets a specific set of requirements designed to protect the cryptographic module from being cracked, altered, or otherwise tampered with. When FIPS 140-2 mode is activated, any secure communication to or from VMware Aria Operations for Logs 8.3 uses cryptographic algorithms or protocols that are allowed by the United States Federal Information Processing Standards (FIPS). FIPS mode turns on the cipher suites that comply with FIPS 140-2. Security related libraries that are shipped with VMware Aria Operations for Logs 8.16 are FIPS 140-2 certified. However, the FIPS 140-2 mode is not activated by default. FIPS 140-2 mode can be activated if there is a security compliance requirement to use FIPS certified cryptographic algorithms with the FIPS mode activated.

Note Enabling FIPS is a one-way action and cannot be deactivated after it is activated.

Activate FIPS during the initial cluster deployment

- Ensure a new deployment of a VMware Aria Operations for Logs cluster.
- Ensure that the Activate FIPS flag is appropriately used during the deployment of cluster nodes (OVF/OVA).

Activate FIPS on a working cluster

1. Navigate to `https://<Log Insight IP>/admin/general`
2. Login as an admin user.
3. Take the cluster offline to activate the Activate FIPS button in the **General Configuration** page.

4 Open the **Configuration General** tab in the left panel.

5 Click Activate FIPS Mode under the **FIPS MODE** section. (Cluster will be automatically rebooted)

6 Bring the cluster online.

API to activate FIPS mode on a working cluster

Using the API to activate FIPS produces the same result as using the UI to activate FIPS mode.

- FIPS mode status

```
GET /api/v1/fips
```

```
1. Response Body: '{"enabled": false}'
2. Response code: 200
```

Verify that FIPS mode is activated from the admin user interface

1 Navigate to `https://<Log Insight IP>/admin/general`

2 Login as the admin user.

3 Open the **Configuration General** tab from the left panel.

4 A **FIPS 140-2 Status** message appears.

By using REST API:

```
POST /api/v1/fips
```

```
1. Request Body: '{"enabled": true}'
2. Response code: 200
```

Change the Root Password

You can change the root password for any VMware Aria Operations for Logs nodes 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/system-password`. All hardened appliances activate `enforce_for_root` for the `pw_history` module, found in the `/etc/pam.d/system-password` file. The system remembers the last five passwords by default. Old passwords are stored for each user in the `/etc/security/opasswd` file.

Prerequisites

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

Procedure

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

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

   The hash information appears.

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

Manage Password Expiry

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

By default, the root account is set to a 365-day password expiry.

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

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

As a simple test to determine whether SSH is activated on a machine, try to open a connection by using SSH. If the connection opens and requests credentials, then SSH is activated 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. Deactivate 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 activated 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 activates 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.

Activate or Deactivate Secure Shell on a VMware Aria Operations for Logs Node

You can activate Secure Shell (SSH) on a VMware Aria Operations for Logs node for troubleshooting. For example, to troubleshoot a server, you might require console access to the server through SSH. Deactivate SSH on a VMware Aria Operations for Logs node for normal operation.

Procedure

1. Access the console of the VMware Aria Operations for Logs node from vCenter.
2. Press Alt + F1 to access the login prompt then log in.
3. Run the `#systemctl is-enabled sshd` command.
4. If the sshd service is deactivated, run the `#systemctl enable sshd` command.
5. Run the `# systemctl start sshd` command to start the sshd service.
6. Run the `# systemctl stop sshd` command to stop the sshd service.

   You can also activate or deactivate Secure Shell from the **SSH Status** column of the VMware Aria Operations for Logs administration interface.

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 deactivate 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/vrliuser -g users -G wheel –m
vrliuser # 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

Deactivate 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`), deactivate 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.

Setting	Status
Server Daemon Protocol	Protocol 2
Ciphers	aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
TCP Forwarding	AllowTCPForwarding no
Server Gateway Ports	Gateway Ports no
X11 Forwarding	X11Forwarding no
SSH Service	Use the AllowGroups field and specify a group permitted to access and add members to the secondary group for users permitted to use the service.
Tunnel Configuration	PermitTunnel no
Network Sessions	MaxSessions 1

Strict Mode Checking	Strict Modes yes
Compression	Compression no
Message Authentication code	hmac-sha2-512,hmac-sha2-256
User Access Restriction	PermitUserEnvironment no
KexAlgorithms	ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521

2 Save your changes and close the file.

Harden the Secure Shell Client Configuration

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

Procedure

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

Setting	Status
Client Protocol	Protocol 2
Client Gateway Ports	Gateway Ports no

Setting	Status
Local Variables (SendEnv global option)	Provide only LC_* or LANG variables
CBC Ciphers	aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
Message Authentication Codes	Used in the `MACs hmac-sha1` entry only
KexAlgorithms	ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521

2 Save your changes and close the file.

Deactivate 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 deactivate 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 deactivate 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`.

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.

Upgraded from 4.8

Step on how to set encrypted password for editing mode of boot loader for upgraded setups from 4.8 LI to 8.x. Following steps should be done for each node:

1. Reboot the VM and follow the console screen. When available operating systems are listed, select the second one - 'SUSE Linux Enterprise Server 11 SP4 - 3.0.101-108.21' . Press enter to boot sles.

2. When SLES is booted, run `grub-md5-crypt` command to encrypt desired password.

3. In /boot/grub/menu.lst file add the following line in the first section:

   password --md5 <encrypted password>

4. Reboot the VM and follow console to make sure the last entry 'Photon' is booted.

Freshly Deployed 8.x

Step on how to set encrypted password for boot loader for NEWLY deployed Log Insights of version 8.x:

1. Run `tdnf install grub2.x86_64` command and type `y` when asked

2. Run `grub2-mkpasswd-pbkdf2` which will ask for password. Set password

3. Add following lines at the end of /etc/grub.d/40_custom

   set superusers="root"

   password_pbkdf2 root <hash of password, which is the output of previous command including beginning 'grub.pbkdf2' >

4. grub2-mkconfig -o /boot/grub/grub.cfg

Those are almost the same steps as in vROps KB, only necessary lib is installed, and file path is corrected.

ONLY PLEASE NOTE that by applying these steps you will need to enter username and password even during simple boot.

if only edit mode requires authentication, then there will be need to add '--unrestricted' to all 'menuentries' so that any user shall be able to boot.

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:

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/dev/null:/bin/false
daemon:x:6:6:Daemon User:/dev/null:/bin/false
messagebus:x:18:18:D-Bus Message Daemon User:/var/run/dbus:/bin/false
systemd-bus-proxy:x:72:72:systemd Bus Proxy:/:/bin/false
systemd-journal-gateway:x:73:73:systemd Journal Gateway:/:/bin/false
systemd-journal-remote:x:74:74:systemd Journal Remote:/:/bin/false
systemd-journal-upload:x:75:75:systemd Journal Upload:/:/bin/false
systemd-network:x:76:76:systemd Network Management:/:/bin/false
systemd-resolve:x:77:77:systemd Resolver:/:/bin/false
systemd-timesync:x:78:78:systemd Time Synchronization:/:/bin/false
nobody:x:65534:65533:Unprivileged User:/dev/null:/bin/false
sshd:x:50:50:sshd PrivSep:/var/lib/sshd:/bin/false

named:x:999:999::/var/lib/bind:/bin/false
smmsp:x:26:26:Sendmail Daemon:/dev/null:/bin/false
ntp:x:87:87:Network Time Protocol:/var/lib/ntp:/bin/false
rpc:x:31:31::/var/lib/rpcbind:/bin/false

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.

```
root:x:0:
bin:x:1:daemon
sys:x:2:
kmem:x:3:
tape:x:4:
tty:x:5:
daemon:x:6:
floppy:x:7:
disk:x:8:
lp:x:9:
dialout:x:10:
audio:x:11:
video:x:12:
utmp:x:13:
usb:x:14:
cdrom:x:15:
adm:x:16:
messagebus:x:18:
systemd-journal:x:23:
input:x:24:
mail:x:34:
lock:x:54:
dip:x:30:
systemd-bus-proxy:x:72:
systemd-journal-gateway:x:73:
systemd-journal-remote:x:74:
systemd-journal-upload:x:75:
systemd-network:x:76:
systemd-resolve:x:77:
systemd-timesync:x:78:
nogroup:x:65533:
users:x:100:
sudo:x:27:
wheel:x:28:root
docker:x:999:
rpc:x:31:
sshd:x:50:
named:x:998:
nobody:x:997:
smmsp:x:26:
ntp:x:87:
salt:x:996:
```

Configure NTP on VMware Appliances

For critical time sourcing, deactivate 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 deactivated 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.

1. Configure NTP from internal config UI by visiting /internal/config webpage.

   Find the following configuration:

   <ntp>

   <mode value="ntp" />

   <ntp-servers value="0.vmware.pool.ntp.org, 1.vmware.pool.ntp.org, 2.vmware.pool.ntp.org" />

   </ntp>

2. The NTP configuration file is 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 -4 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.

Deactivate 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

- Deactivate 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.

TLS for Data in Transit

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

Configure Strong Protocols for VMware Aria Operations for Logs

Protocols such as SSLv2 and SSLv3 are no longer considered secure. In addition, TLS 1.0 and TLS 1.1 have also been deactivated and only TLS 1.2 is activated by default.

Note When you upgrade your VMware Aria Operations for Logs instance from 8.2, both TLS 1.0 and TLS 1.1 are deactivated on all the VMware Aria Operations for Logs nodes. TLS 1.2 is the only protocol that is supported by default.

Verify the Correct Use of Protocols in Tomcat

VMware Aria Operations for Logs deactivates SSLv2, SSLv3, TLSv1, and TLSv1.1 by default. You must deactivate weak protocols on all nodes before you put the system into production.

1. Run the `grep sslProtocol /usr/lib/loginsight/application/3rd_party/apache-tomcat/conf/server.xml | grep -v '#'`

   “clientAuth sslProtocol” attribute must be set to “TLS”.

2. Navigate to `/usr/java/jre-vmware/conf/security/java.security` file and search for `jdk.tls.disabledAlgorithms` value. Current value in vRLI 8.16 is:

   ```
   jdk.tls.disabledAlgorithms= SSLv3, TLSv1, TLSv1.1, RC4, DES, MD5withRSA,
   DH keySize < 1024, EC keySize < 224, 3DES_EDE_CBC, anon, NULL, RSA keySize
   < 512, DESede, TLS_RSA_WITH_AES_256_CBC_SHA,
   TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
   TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
   TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_RSA_WITH_AES_128_CBC_SHA,
   TLS_RSA_WITH_AES_128_CBC_SHA256, include jdk.disabled.namedCurves
   ```

3. To restart the Tomcat server, run the `systemctl restart tomcat` command from the command prompt.

Configure VMware Aria Operations for Logs to Use Strong Ciphers

For maximum security, you must configure VMware Aria Operations for Logs components to use strong ciphers. To ensure that only strong ciphers are selected, deactivate 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.

VMware Aria Operations for Logs deactivates the use of cipher suites using the DHE key exchange by default. Ensure that you deactivate 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 Tomcat

4 Open `/usr/lib/loginsight/application/3rd_party/apache-tomcat/conf/server.xml` Find “<Connector port=”443”” node and check ciphers attribute values.

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:

```
 301421    92 -rwsr-xr-x   1 root    root       86712 Dec 27 22:57 /usr/bin/gpasswd
 299699    64 -rwsr-xr-x   1 root    root       61192 May 10  2022 /usr/bin/mount
 301424    48 -rwsr-xr-x   1 root    root       46176 Dec 27 22:57 /usr/bin/newgrp
 303478    60 -rwsr-xr-x   1 root    root       53576 Feb 25  2021 /usr/bin/crontab
 301415    80 -rwsr-xr-x   1 root    root       73976 Dec 27 22:57 /usr/bin/chage
 299716    36 -rwsr-xr-x   1 root    root       36224 May 10  2022 /usr/bin/umount
 301423    60 -rwsr-xr-x   1 root    root       57008 Dec 27 22:57 /usr/bin/newgidmap
 301413    76 -rwsr-xr-x   1 root    root       70080 Dec 27 22:57 /usr/bin/passwd
 304228   116 -rwsr-sr-x   1 root    root      112144 Feb 24  2021 /usr/bin/procmail
 301418    32 -rwsr-xr-x   1 root    root       32376 Dec 27 22:57 /usr/bin/expiry
 303585    36 -rwsr-xr-x   1 root    root       36248 Feb 24  2021 /usr/bin/fusermount
 301425    60 -rwsr-xr-x   1 root    root       57000 Dec 27 22:57 /usr/bin/newuidmap
 301414    56 -rwsr-xr-x   1 root    root       50384 Dec 27 22:57 /usr/bin/su
 301416    64 -rwsr-xr-x   1 root    root       60280 Dec 27 22:57 /usr/bin/chfn
 304112   292 -rwsr-xr-x   1 root    root      294112 Jan  5 15:54 /usr/bin/sudo
 301417    60 -rwsr-xr-x   1 root    root       54472 Dec 27 22:57 /usr/bin/chsh
 304226    24 -rwxr-sr-x   1 root    root       23960 Feb 24  2021 /usr/bin/lockfile
 300285    40 -rwsr-xr-x   1 root    root       40376 May 31  2023 /usr/sbin/unix_chkpwd
 303905   832 -r-xr-sr-x   1 root    root      845696 May 16  2023 /usr/sbin/sendmail
 303702   140 -r-s--x--x   1 root    root      137328 Jul  5  2023 /usr/sbin/mount.nfs
 303992    16 -rwsr-xr-x   1 root    root       15408 Oct 28 03:10 /usr/sbin/usernetctl
 303036    72 -rwsr-x---   1 root    root       66128 Oct 13  2022 /usr/libexec/dbus-daemon-launch-
helper
 301126   516 -rwsr-xr-x   1 root    root      524176 Dec 27 22:58 /usr/libexec/ssh-keysign
```

2 Run the **find / -path */proc -prune -o -nouser -print -o -nogroup -print** 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 "*.*" -type f -not -path "*/sys*" -not -path "*/proc*" -not -path "*/dev*" -perm -a+w | xargs ls -ldb** command to verify that none of the files are world writable files by

reviewing permissions of all the files on the vApp.

`Others` should not have written permission. The permissions on these files should be *##4* or *##5*, where *#* equals the default given set of permissions for the Owner and Group, such as *6* or *7*.

Tomcat Configuration

Deactivate 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 deactivated for all directories.
  a. Run `grep -A 1 “<param-name>listings” /usr/lib/loginsight/application/3rd_party/apache-tomcat-{X}/conf/web.xml` “X” value depends on Tomcat version.
  b. Verify that for `<param-value>` is set to `false` in the second line.

Deactivate Configuration Modes

As a best practice, when you install, configure, or maintain VMware Aria Operations for Logs, you can modify the configuration or settings to activate 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 VMware Aria Operations for Logs host machines.

Configure all software that you do not remove in accordance with manufacturer recommendations and security best practices to minimize the 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.d/modprobe.conf` file in a text editor.
2. Ensure that the `install usb-storage /bin/false` 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.d/modprobe.conf` file in a text editor.
2. Ensure that the line `install bluetooth /bin/false` 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 can 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.d/modprobe.conf` file in a text editor.
2. Ensure that the following line appears in this file.

   ```
   install sctp /bin/false
   ```
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.d/modprobe.conf` file in a text editor.
2. Ensure that the DCCP lines appear in the file.

```
install dccp /bin/false
install dccp_ipv4 /bin/false
install dccp_ipv6 /bin/false
```

3 Save the file and close it.

Secure Reliable Datagram Sockets Protocol

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

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

Procedure

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

2 Ensure that the `install rds /bin/false` 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.d/modprobe.conf` file in a text editor.

2 Ensure that the `install tipc /bin/false` 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 can 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.d/modprobe.conf` file in a text editor.
2. Ensure that the line `install ipx /bin/false` 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 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.d/modprobe.conf` file in a text editor.
2. Ensure that the line `install appletalk /bin/false` 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 can 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.d/modprobe.conf` file in a text editor.
2. Ensure that the line `install decnet /bin/false` 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 necessary.

Procedure

1. Open the `/etc/modprobe.d/modprobe.conf` file in a text editor.
2. Ensure that the line `install ieee1394 /bin/false` 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.

Open Ports on Log Insight Host

These ports might be arbitrarily assigned, and so, the exact port number might vary. The agent does not open ports on external interfaces.

You can find the most up-to-date technical documentation for open ports on the VMware website at: https://ports.vmware.com/home/vRealize-Log-Insight.

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 VMware Aria Operations for Logs user interface to revoke the agent certificate by removing the agent resource

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

Patching and updating the VMware Aria Operations for Logs Agent

If required, new agent bundles are available independent of VMware Aria Operations for Logs releases.

Patches or updates are not provided for the VMware Aria Operations for Logs 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.

Verify Server User Account Settings

It is recommended that you verify that no unnecessary user accounts exist for application.

Restrict any user account not related to the functioning of the application to those accounts required for administration, maintenance, and troubleshooting. Strictly control and audit these accounts.

Network Security and Secure Communication

4

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 VMware Aria Operations for Logs.

This chapter includes the following topics:

Configuring Network Settings for Virtual Application Installation

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

Deny ICMPv4 Echoes to Broadcast Address	`# cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts`	`1`

Configure the Host System to Deactivate IPv4 Proxy ARP	`# grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp|egrep "default|all"`	`net.ipv4.conf.all.proxy_arp=0`
		
		`net.ipv4.conf.default.proxy_arp=0`

Configure the Host System to Ignore IPv4 ICMP Redirect Messages	`# grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects|egrep "default|all"`	`net.ipv4.conf.all.accept_redirects=0`
		
		`net.ipv4.conf.default.accept_redirects=0`

Configure the Host System to Ignore IPv6 ICMP Redirect Messages	`# grep [01] /proc/sys/net/ipv6/conf/*/accept_redirects|egrep "default|all"`	`net.ipv6.conf.all.accept_redirects=0`
		
		`net.ipv6.conf.default.accept_redirects=0`

Configure the Host System to Deny IPv4 ICMP Redirects	`# grep [01] /proc/sys/net/ipv4/conf/*/send_redirects|egrep "default| all"`	`net.ipv4.conf.all.send_redirects=0`
		
		`net.ipv4.conf.default.send_redirects=0`

Configure the Host System to Log IPv4 Martian Packets	`# grep [01] /proc/sys/net/ipv4/conf/*/log_martians|egrep "default| all"`	`net.ipv4.conf.all.log_martians=1`
		
		`net.ipv4.conf.default.log_martians=1`

Configure the Host System to use IPv4 Reverse Path Filtering	`# grep [01] /proc/sys/net/ipv4/conf/*/rp_filter|egrep "default|all"`	`net.ipv4.conf.all.rp_filter=1`
		
		`net.ipv4.conf.default.rp_filter=1`

Configure the Host System to Deny IPv4 Forwarding	`# cat /proc/sys/net/ipv4/ip_forward`	`net.ipv4.ip_forward=0`

Configure the Host System to Deny Forwarding of IPv4 Source Routed Packets	`# grep [01] /proc/sys/net/ipv4/conf/*/accept_source_route|egrep "default|all"`	`net.ipv4.conf.all.accept_source_route=0`
		
		`net.ipv4.conf.default.accept_source_route=0`

Configure the Host System to Deny IPv6 Forwarding	`# grep [01] /proc/sys/net/ipv6/conf/*/forwarding|egrep "default|all"`	`net.ipv6.conf.all.forwarding=0`
		
		`net.ipv6.conf.default.forwarding=0`

Configure the Host System to Use IPv4 TCP SYN Cookies	`# cat /proc/sys/net/ipv4/tcp_syncookies`	`net.ipv4.tcp_syncookies=1`

Configure the Host System to Deny IPv6 Router Solicitations	`# grep [01] /proc/sys/net/ipv6/conf/*/router_solicitations|egrep "default|all"`	`net.ipv6.conf.all.router_solicitations=0`
		
		`net.ipv6.conf.default.router_solicitations=0`

Configuring Ports and Protocols

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

Configure the minimum incoming and outgoing ports for VMware Aria Operations for Logs 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 VMware Aria Operations for Logs to operate in production.

You can find the most up-to-date technical documentation for open ports on the VMware website at: https://ports.vmware.com/home/vRealize-Log-Insight

Auditing and Logging on your VMware Aria Operations for Logs System

5

As a security best practice, set up auditing and logging on your VMware Aria Operations for Logs system.

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

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

This chapter includes the following topics:

Securing the Remote Logging Server

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

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

Use an Authorized NTP Server

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

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

Client Browser Considerations

As a security best practice, do not use VMware Aria Operations for Logs from untrusted or unpatched clients or from clients that use browser extensions.