VMware Telco Cloud Automation Security Configuration Guide

VMware Telco Cloud Automation 3.1

vmware by Broadcom

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

https://docs.vmware.com/

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

Contents

About the Telco Cloud Automation Security Configuration Guide

1

This VMware Telco Cloud Automation Security Configuration Guide contains verification and configuration procedures, and best practices for securely deploying VMware Telco Cloud Automation. This guide also helps you evaluate and optimize the secure configuration of Telco Cloud Automation deployments.

Intended Audience

This guide is intended for VMware Telco Cloud Automation administrators and other users who are responsible for system security maintenance and configuration.

Secure Deployment of Telco Cloud Automation

2

This section outlines the procedures for secure deployment of VMware Telco Cloud Automation (TCA) to prevent any potential security risks.

Read the following topics next:

- Verify the Integrity of Installation Media
- Harden the Deployed Software Infrastructure
- Review Installed and Unsupported Software
- VMware Security Advisories and Patches
- OS Package Updates

Verify the Integrity of Installation Media

Before installing VMware Telco Cloud Automation, you must verify the integrity of the installation media to ensure authenticity of the downloaded files.

Procedure

1. Verify the checksum of the TCA OVA bundle:
   - Linux

     ```
     sha256sum VMware-Telco-Cloud-Automation-<version>-<build>.ova
     ```

   - Windows

     ```
     certutil -hashfile VMware-Telco-Cloud-Automation-<version>-<build>.ova SHA256
     ```

   - MacOS

     ```
     shasum -a 256 VMware-Telco-Cloud-Automation-<version>-<build>.ova
     ```

   The command output displays sha256 hash of the TCA OVA bundle.
2. Compare the checksum sha256 hash value with the sha256 hash published for the TCA version on VMware Customer Connect.

3 If the hash values do not match, the TCA OVA is either corrupted or modified and you must re-download the OVA from VMware Customer Connect.

Harden the Deployed Software Infrastructure

To ensure a completely hardened and secure environment, you must harden the deployed software infrastructure that supports the VMware system. Software infrastructure components include operating system components, supporting software, and database software.

Before you harden the VMware system, review and address security concerns in these components according to the manufacturer's recommendations and other relevant security protocols.

Harden the VMware vSphere Environment

VMware Telco Cloud Automation relies on a secure VMware vSphere environment for optimal benefits and a secured infrastructure.

Verify that the appropriate level of vSphere hardening guidance is enforced and maintained in the vSphere environment.

For more guidance about hardening, see VMware Security Hardening Guides.

Review Installed and Unsupported Software

Vulnerabilities in unused software might increase the risk of unauthorized system access and disruption of availability.

To minimize the threat to the infrastructure,

- Evaluate the use of software that is installed on VMware host machines.
- Do not install software that is not required for the secure operation of the system on any of the Telco Cloud Automation node hosts.
- Do not install or use any third-party software that is not supported by VMware on VMware-supplied hosts.
- Verify that no unsupported software is installed in the TCA deployment and in the inventory of installed products.
- Uninstall unused or nonessential software.

For more information about the support policies for third-party products, contact VMware Support.

Verify Third-Party Software

Inauthentic, insecure, or unpatched third-party software on VMware host machines might contain vulnerabilities and put the system at risk of unauthorized access and disruption of availability.

If you are using third-party software in VMware host machines,

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

  Caution 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.

To ensure that the underlying product is secure and not vulnerable to known threats, you must:

- Be aware of these VMware Security Advisories
- Assess the VMware Telco Cloud Automation installation, patching, and upgrade history, and verify that the released advisories are enforced.
- Always use the most recent TCA release as it includes the most recent security fixes.

For more information, see the latest VMware security advisories.

OS Package Updates

Telco Cloud Automation updates related Linux OS packages every release. Installing new versions of the TCA appliance ensures uptaking Photon OS updates. We recommend that you update your TCA deployment to the latest version or the latest Long-Term Support (LTS) release.

Secure Configuration of Telco Cloud Automation

3

This section includes security considerations and configurations for managing VMware Telco Cloud Automation deployments.

Read the following topics next:

- Managing Password for User Accounts
- Manage Session Duration
- Manage Secure Shell
- Configure SSH
- Replace TCA Self-Signed Certificates with Signed-Certificates
- Secure External Connection to Telco Cloud Automation
- Manage Backup and Restore

Managing Password for User Accounts

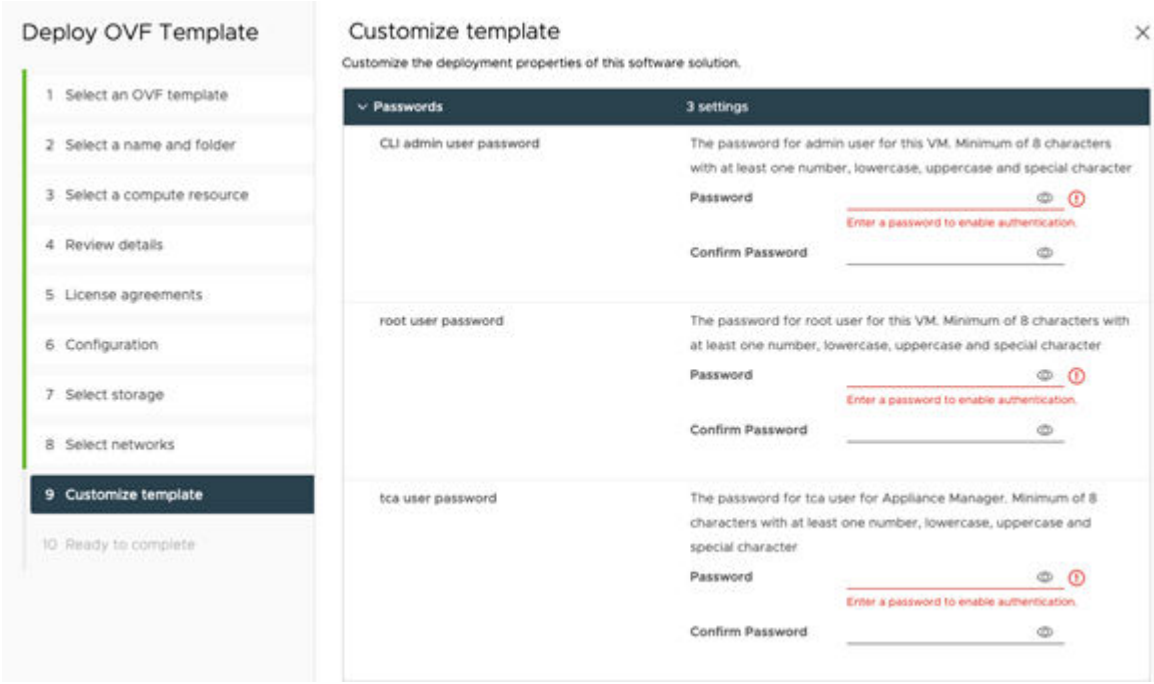
This section provides guidelines for managing password complexity and expiration for user accounts in Telco Cloud Automation.

Manage Password Complexity for User Accounts

Ensure that the following user accounts are configured during the deployment of TCA Manager or TCA Control Plane appliance:

- **admin** user (local user): Used to perform troubleshooting (command line only) on a TCA Manager or TCA Control Plane appliance used for
- **root** user: Used to perform troubleshooting (command line only) on a TCA Manager or TCA Control Plane appliance
- **tca** user: Used to log in to the Appliance Manager UI in TCA Manager or TCA Control Plane appliance and perform configuration and administration tasks

Note SSH root access is denied. The admin user account can connect using SSH by default.



For security purposes, TCA does not have default passwords for these user accounts. You must use different passwords for these accounts and ensure that the passwords comply with the suggested password complexity rule for the account.

Note Password complexity verification is not enforced during the TCA OVA deployment.

Recover Lost Password for TCA Appliance Manager UI

To log in to the TCA Appliance Manager UI, a separate tca user account is used. If the tca user password is lost, use the following procedure to reset the password.

Procedure

1 SSH into the TCA virtual appliance as an admin user:

```
ssh admin@<tca-address>
```

2 Run the following in the appliance manager container:

```
kubectl exec -it $(kubectl get pod -A | grep platform-manager | awk '{print $2}') -n
$(kubectl get pod -A | grep platform-manager | awk '{print $1}') -- bash
```

3 Navigate to the scripts directory:

```
cd /opt/vmware/scripts/
```

4 Set executable permissions on the resetTcaUserPassword.sh script:

```
chmod +x ./resetTcaUserPassword.sh
```

5 Set the new password for tca user:

```
./resetTcaUserPassword.sh <base64-encoded-password>
```

6 Log in to the TCA Appliance Manager UI (9943) with the new password.

Configure Password Expiration for User Accounts

Ensure that password expirations for all user accounts of the TCA virtual appliance are configured in accordance with your organization's security policies. By default, admin user accounts use a 90-day password expiration. The root user account password never expires.

As a best practice, verify that the password expiration on all accounts meets your organization's security and operation standards.

Procedure

1 SSH into the TCA virtual appliance using the admin account, elevate privileges with "su" to connect to the root user account, and run the command: `chage -l <username>`

```
root@tca-m-01 [ ~ ]# chage -l root
Last password change                                    : Jan 29, 2024
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7
root@tca-m-01 [ ~ ]# chage -l admin
Last password change                                    : Jan 29, 2024
Password expires                                        : Apr 28, 2024
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 1
Maximum number of days between password change          : 90
Number of days of warning before password expires       : 7
root@tca-m-01 [ ~ ]#
```

2 Change the password expiration duration:

```
chage m <number of days> <username>
```

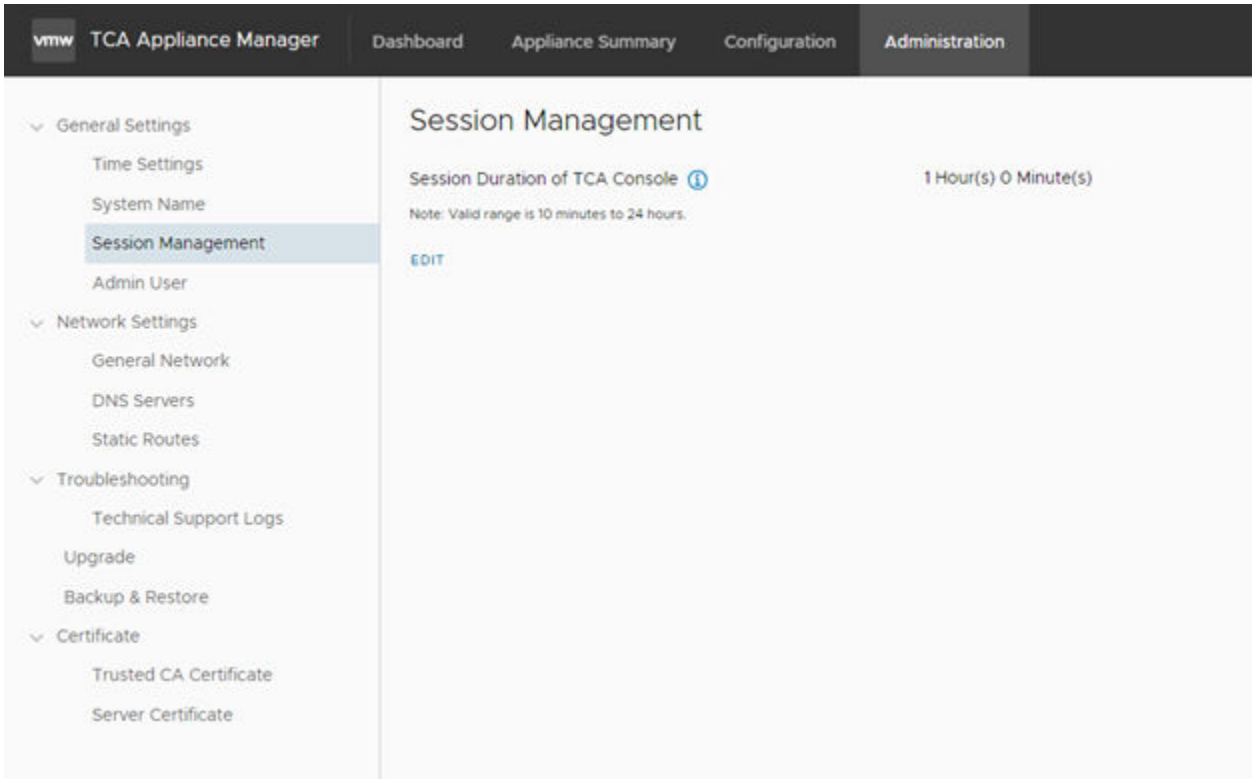
Manage Session Duration

Using Session Management in the TCA Appliance Manager UI, you can configure the session duration limits in the range of 10 minutes to 24 hours.

For enhanced security and to prevent long user sessions in the system, set the session duration to a lower time limit.

Note

- By default, the session duration limit is set to 60 minutes. This session duration is also applied for API.



Manage Secure Shell

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

SSH is an interactive command-line environment that supports remote connections to VMware virtual appliances. For remote connections, all TCA appliances include the SSH protocol.

Use SSH only when necessary and manage it appropriately to preserve system security.

Note By default, SSH access requires high-privileged user account credentials.

- Root user SSH activities generally bypass the role-based access control (RBAC) and audit controls of the virtual appliances.
- By default, only admin users can connect by SSH. Root access is denied.

Unlock an Admin User Account

TCA appliance is pre-configured to not allow more than three consecutive failed authentication attempts per user during the 15-minute interval. TCA does not display any lockout message even when you enter the correct password into a locked account.

Note Root access is required to check a user's locked status or unlock a user.

Procedure

1 Log in to the TCA appliance console as a root user. For instructions, see Open the Web Console.

2 List the users and the number of failed login attempts by running the `faillock` command:

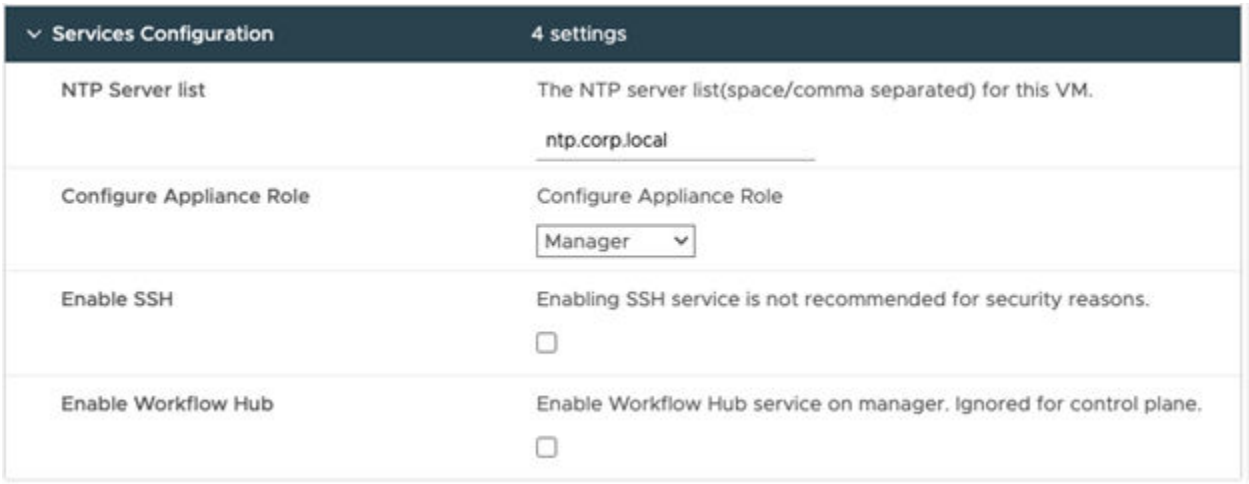
```
root@tca-m-01 [ ~ ]# faillock
Login           Failures    Latest failure         From
admin                3      2024-02-07 21:02:34    10.32.25.24
root                 0
root@tca-m-01 [ ~ ]# _
```

3 Unlock the locked admin user account by running the `faillock -user admin -reset` command:

```
root@tca-m-01 [ ~ ]# faillock --user admin --reset
root@tca-m-01 [ ~ ]# faillock
Login           Failures    Latest failure         From
admin                0
root                 0
root@tca-m-01 [ ~ ]#
```

Configure SSH

For best security, do not enable SSH access to TCA Manager or TCA Control Plane appliances during the installation of appliances. Enable SSH only when required for troubleshooting purposes.



To enable SSH access, follow these steps:

Procedure

1 Launch the Web Console for the TCA Manager or TCA Control Plave virtual appliance from vCenter and log in as a root user. For instructions, see Open the Web Console.

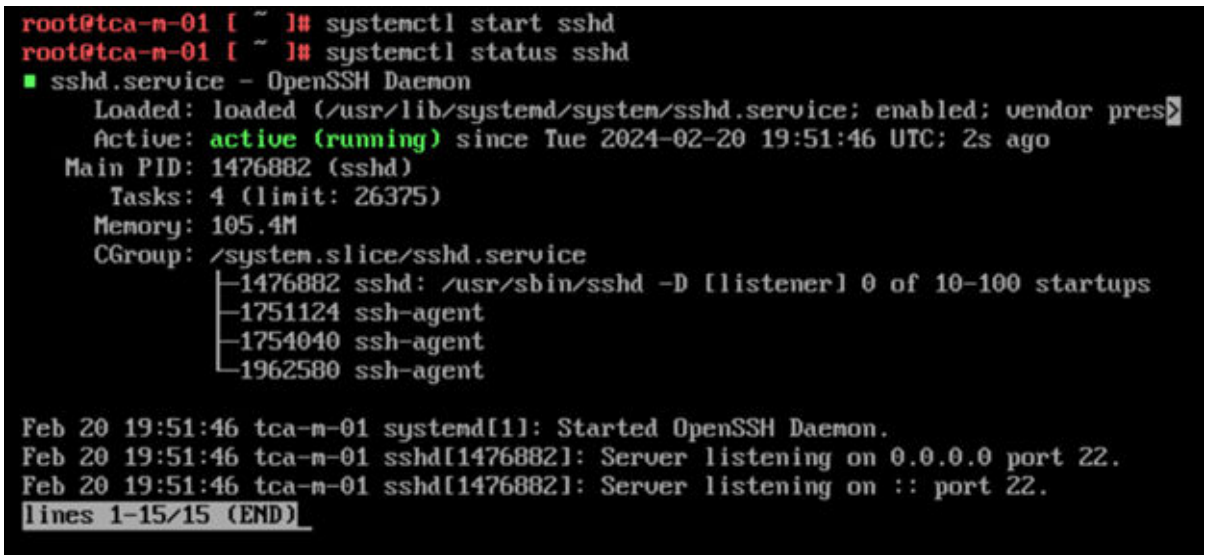
2 Start the sshd service.

```
systemctl start sshd
```

Note This command does not produce any output.

3 Verify the status of the sshd service.

```
systemctl status sshd
```



What to do next

1. If the sshd service is successfully started, you can use SSH to log in to the appliance as an admin user for troubleshooting.
2. After troubleshooting is completed, stop the sshd service.

```
systemctl stop sshd
```

Replace TCA Self-Signed Certificates with Signed-Certificates

TCA Manager and TCA Control Plane appliances are deployed with self-signed certificates. These certificates are generated at the deployment time and applied on both ports 443 and 9443. As a security practice, replace these self-signed certificates with your own certificates signed by a Certificate Authority.

For instructions to update your server certificate, see Update Server Certificate in the VMware Telco Cloud Automation Deployment Guide.

Secure External Connection to Telco Cloud Automation

To secure a VMware Telco Cloud Automation server from external attackers, you must implement defensive measures common to all web-based services. Such measures include securing HTTPS endpoints with signed certificates.

Example of endpoints to be secured: Harbor, Airgap, Active Directory, vCenter, NSX, Cloud Director, and so on.

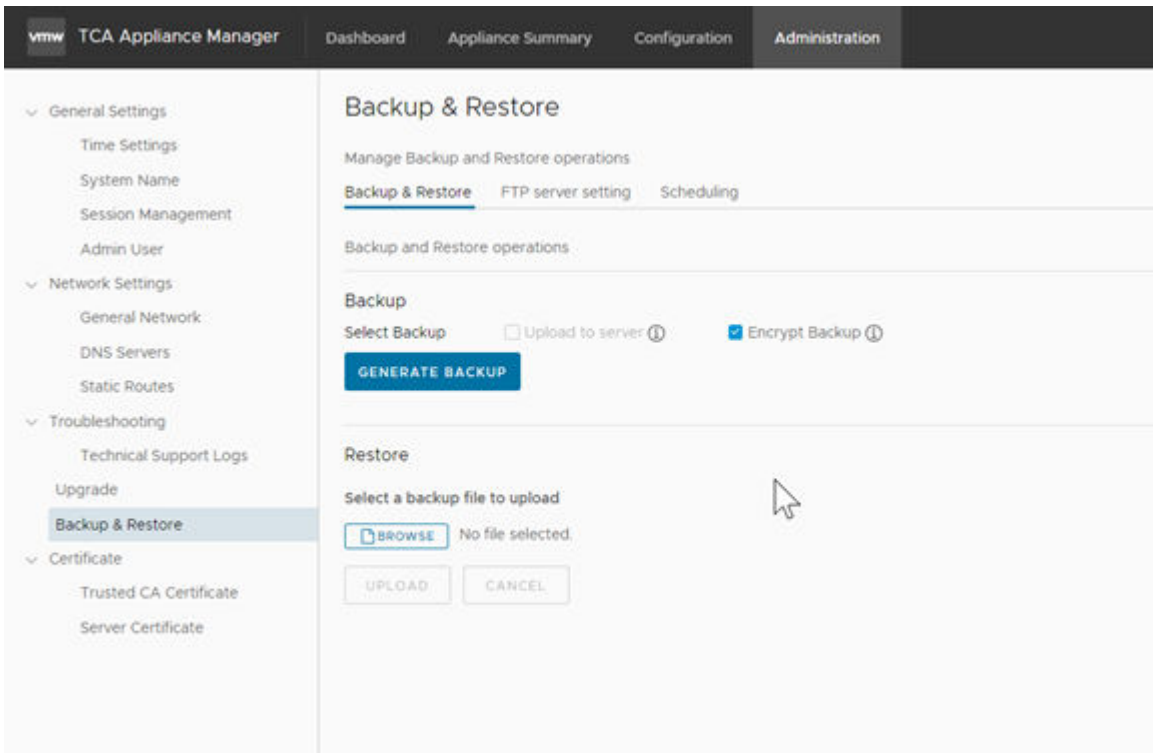
Note For Active Directory, we recommend that you use LDAPS connection instead of LDAP.

Manage Backup and Restore

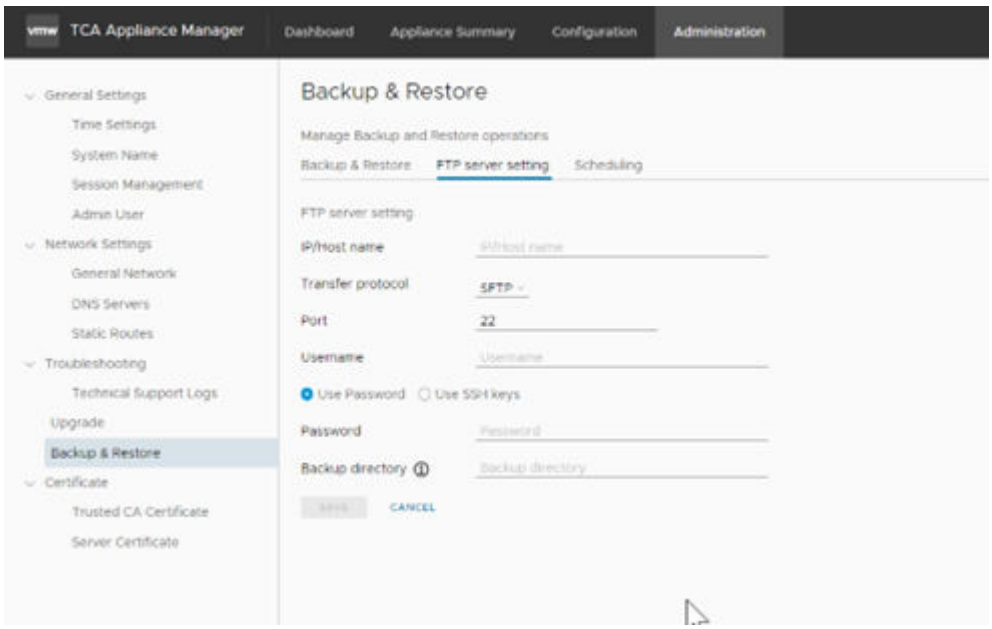
When you manage restore and backup bundles in the TCA Appliance Manager, follow these security best practices:

- Always encrypt the backup bundle.

  In the following example, the backup bundle is encrypted using AES-GCM 256 from the Appliance Manager on port 9443.



- Transfer the backup and restore bundles using the SFTP protocol (from the Appliance Management on port 9443).



Secure Network and Communication for Telco Cloud Automation

4

This section outlines the best practices for ensuring secure network and communication in Telco Cloud Automation deployments.

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

For additional security, deploy TCA in an airgapped or Internet-restricted environment. These modes require the deployment of airgap server for the container images for TCA Containers as a Service (CaaS) system and the packages for Kubernetes cluster node customization.

For more information, see Deploy TCA Airgap Appliance OVA.

Read the following topics next:

- Configure Ports and Protocols
- Use an Authorized NTP Server
- Cipher Suites and Protocols

Configure Ports and Protocols

As a security best practice, deactivate all non-essential ports and protocols. Configuring the minimum incoming and outgoing ports is essential for the TCA components to operate in production.

Minimum Default Incoming Ports

The default incoming ports must be allowed or opened in the local network for TCA inter-node communication. For the latest list of open ports for TCA, see Ports and Protocols.

Use an Authorized NTP Server

Ensure that all 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 cause inaccurate auditing.

Use a minimum of three NTP servers from external time sources or configure a few local NTP servers on a trusted network that obtain their time from at least three external time sources.

For more information, see Updating the Time Settings.

Cipher Suites and Protocols

By default, TLS 1.2 and TLS 1.3 protocols are enabled on the TCA Manager and TCA Control Plane appliances.

Caution The following protocols are not used for TCA:

- TLS 1.0 and TLS 1.1 protocols are deactivated.
- SSLv2 and SSLv3 are no longer considered secure.

The following table lists the cipher suite configured in the TCA Manager and TCA Control Plane appliances:

Port	Protocol	Cipher
443	TLS 1.2	ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-CHACHA20-POLY1305
8500	TLS 1.2	ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-CHACHA20-POLY1305 ECDHE-RSA-AES256-CBC ECDHE-RSA-AES128-CBC ECDHE-RSA-AES256-GCM ECDHE-RSA-AES128-GCM
9092	TLS 1.2	ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-CHACHA20-POLY1305
9443	TLS 1.2	ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-CHACHA20-POLY1305
443	TLS 1.3	ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-CHACHA20-POLY1305
8500	TLS 1.3	ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-CHACHA20-POLY1305

9092	TLS 1.3	ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-CHACHA20-POLY1305
9443	TLS 1.3	ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-CHACHA20-POLY1305

Using Logs in Telco Cloud Automation

5

This section outlines the best practices for monitoring the TCA system activity and maintaining a secure TCA deployment.

As a best practice, ensure that you collect the full log bundle for troubleshooting purposes. For instructions, see Troubleshooting and Support.

Read the following topics next:

- Monitor Audit Logs for Suspicious Activity
- External Log Integration with Aria Operation for Logs

Monitor Audit Logs for Suspicious Activity

You can monitor your system for suspicious activity by using audit logs from the Telco Cloud Automation UI. The retention period for audit logs is two months.

For instructions to view audit logs in TCA, see Viewing Audit Logs.

The TCA platform runs as a containerized application within a virtual machine, capturing logging information for several deployments, pods, and services running in it.

Component	Service / Pods	Purpose
Audit Logging	audit-log-service	Contains all events related to Audit Logs for the TCA platform. Events include Authentication, NF Upload/Download, Instantiations of NF or CaaS clusters, and so on.
Keycloak	tca-keycloak-service	Contains detailed information regarding authentication attempts to login through Active Directory (successful and unsuccessful)

Within the logging framework, audit logs from TCA are prefixed with a k8s_app label set to ‘audit-log-service’. Thus, all TCA audit logs can be easily identified, searched, and reported upon.

External Log Integration with Aria Operation for Logs

VMware Telco Cloud Automation integrates with VMware Aria Operations for Logs to export the TCA application logs for long-term storage and retrieval.

- You can import the TCA content pack to Aria Operations for Logs. The content pack provides pre-defined filters that you can use to filter logs from specific TCA services.
- You can configure the Aria Operations for Logs details through the Appliance Management UI on TCA Manager and TCA-Control Plane.