MOP: Cisco XR Device Audit

Objective:

The purpose of this MOP is to outline the steps for conducting an audit on a Cisco XR device to assess its configuration, security, and compliance with best practices and organizational standards.

Prerequisites:

1. Ensure you have the necessary access credentials to log in to the Cisco XR device.

2. Have a secure network connection to the device.

3. Obtain approval from the relevant stakeholders and notify them of the audit schedule.

Step 1: Establish a Secure Connection

1.1. Use a secure protocol like SSH to establish a connection to the Cisco XR device.

1.2. Log in using the provided access credentials.

Step 2: Gather Device Information

2.1. Retrieve the device's hostname, model, and software version using the following commands:

- show hostname

- show version

2.2. Document the retrieved information for reference.

Step 3: Review Running Configuration

3.1. Use the command "show running-config" to display the device's current running configuration.

3.2. Analyze the configuration for any discrepancies, misconfigurations, or deviations from best practices and organizational standards.

3.3. Take note of any issues or areas that require further investigation.

Step 4: Check Interface Configuration

4.1. Use the command "show interfaces" to display information about the device's interfaces.

4.2. Review the interface configurations, including IP addresses, VLANs, and status.

4.3. Verify that the interfaces are properly configured and in the expected state.

Step 5: Assess Security Configuration

5.1. Check the device's access control lists (ACLs) using the command "show access-lists".

5.2. Review the ACLs to ensure they are properly configured and align with security best practices.

5.3. Verify that unnecessary or insecure protocols and services are disabled.

Step 6: Examine Routing Configuration

6.1. Use the command "show ip route" to display the device's routing table.

6.2. Review the routing configuration to ensure proper routing protocols are in place and routes are correctly configured.

6.3. Check for any unusual or unauthorized routes.

Step 7: Analyze System Logs

7.1. Use the command "show logging" to view the device's system logs.

7.2. Examine the logs for any error messages, warnings, or suspicious activities.

7.3. Investigate and document any issues found in the logs.

Step 8: Generate Audit Report

8.1. Compile all the findings and observations from the previous steps into a comprehensive audit report.

8.2. Include recommendations for addressing any identified issues or areas of improvement.

8.3. Distribute the audit report to the relevant stakeholders for review and action.

Step 9: Close the Connection

9.1. Gracefully exit the SSH session using the "exit" command.

9.2. Ensure the connection is properly terminated.

Post-Audit Actions:

1. Schedule a meeting with the relevant stakeholders to discuss the audit findings and recommendations.

2. Develop an action plan to address any identified issues and implement necessary changes.

3. Perform follow-up audits to ensure the implemented changes are effective and the device remains compliant.

Note: The specific commands and steps may vary depending on the Cisco XR software version and device model. Always refer to the official Cisco documentation for the most accurate and up-to-date information.