SolarWinds Certified Professional NCM Exam Preparation Guide

Study Resources

Each category in this guide includes links to topics with information. The intention of the resources in this guide are to supplement your years of experience and hands-on training with SolarWinds' products. The included resources are not all-inclusive and should only aid as a starting place for your studies.

Use the available documentation to learn more about NCM.

- NCM Getting Started Guide
- NCM Administrator Guide

For additional study resources, visit THWACK.

Category: Installation

Use the SolarWinds Orion Installer to install or upgrade NCM. Know the system requirements needed to install NCM and how to add nodes.

NCM Licensing

Know the seven types of licenses available for NCM.

Install NCM

Use the SolarWinds Orion Installer to install or upgrade Orion Platform products.

NCM system requirements

Know the system requirements needed for NCM—including ports, server, and database requirements.

Getting Started with Network Configuration Manager – Video

Learn how to use NCM, such as navigating the web console, how to backup devices, how to check & compare configuration changes, how to set up the change approval process and run and customize reports.

Use the SolarWinds Orion Installer

Know how to install or upgrade Orion Platform products and scalability engines.

NCM port requirements

Know the NCM port requirements.

Supported software

Know which NCM versions are supported and which are end-of-life, end-of-engineering, or end-of-announcement.

[Manage NCM nodes](#)

After you discover devices and add them to the Orion Platform for monitoring, you also need to add the devices to NCM.

Sample Questions

1. Which column can you view in Orion's Manage Nodes to verify you successfully added a router?
    A. Status column
    B. NCM Licensed column
    C. Resource column
    D. Node name column
	2. NCM can download and upload both XML and binary configs for Palo Alto devices.
	    A. True
	    B. False

Category: Configuration Management

Edit configs to streamline complex configuration changes and make bulk changes to multiple nodes. To edit a config, you can manually run a script against a node or use a config change template. Know how to download configs and execute scripts. Know how to run config comparison and check config file statuses.

[The basics of config change templates](#)

Use a change config template to accomplish a specific device configuration task for a set of NCM-managed nodes.

[Create a config change template](#)

How to create a config change template.

[Schedule a recurring network config change report](#)

Know how to create or schedule a report that would display configuration changes made based on a specified criteria.

[Download an NCM configuration to a file](#)

How to download a configuration to a file.

[Download configuration files in NCM](#)

Download configuration files to view the current configuration of your managed devices, compare current and previous configurations, or archive configuration files for backup.

[Enable a new config type](#)

If you have devices that use other config types, you can define custom config types to be used with NCM operations.

[Edit a config using a script in NCM](#)

Know how to add and edit a config change script.

[Upload a network config](#)

Use this resource to upload a configuration file you have previously downloaded from this node to NCM.

[Search network config files or node properties](#)

Know how to find a specific node or config, or all nodes or configs that share a common characteristic.

[Establish baselines as a comparison point for network config changes](#)

Information about creating and managing baselines.

[Schedule daily backups of config files](#)

Install an example job that downloads the configuration files nightly for all nodes in the database.

[SolarWinds Information Service Data Entities](#)

View the SWIS entities and properties that you can use in developing config change templates.

[Troubleshoot issues with configuration files](#)

Resolve issues with downloading and managing config files and viewing config file information.

[Issue caused by a network config change](#)

Troubleshoot a network issue caused by a network config change

Sample Questions

1. What part of the NCM Policy Report are nodes specified? A. Report B. Policy C. Rule D. Compliance page	2. When are policy reports updated and cached to the Web for review? Select all that apply. A. At the time specified in NCM Settings > Advanced Settings > Cache Settings B. Every 7 days C. After you select Update all/Update Selected on the Compliance Policy Reports page

Category: Features

NCM features help you manage critical changes and repetitive tasks across complex, multi-vendor networks. Use NCM to make sure your network is compliant and secure. Learn more about the different features NCM offers and uses.

[Approval system for device configuration changes](#)

Know how to define a semi-automated approval process for making configuration changes on network devices.

[Set up config change approval in NCM](#)

Specify an email server for notifications, addresses of change approvers, and accounts of team members who manage device configurations.

[Create a device template](#)

Create or edit device templates in NCM.

[NCM command template commands and attributes](#)

An overview of device command templates and how to implement them in your NCM deployment.

[How NCM assigns device templates to nodes](#)

Assign a device template to a node manually or allow NCM to assign templates to nodes automatically.

[Best practices for device command templates](#)

Review the best practices before modifying device command templates.

[Assign a device template manually](#)

Manually assign device templates to nodes to allow back up of the device configs.

[Uses of NCM inventory reports](#)

Use NCM inventory reports to access up-to-date device information and to manage the inventory of your network infrastructure.

[NCM inventory report](#)

View a list of NCM Inventory reports.

[Run an inventory scan on a node](#)

An inventory scan queries a node and gathers device information including the model and serial numbers, the operating system version, the number of NIC or interface cards, routing protocols, IP addresses, active ports, and much more.

[Create an NCM job to execute a command script on devices](#)

Learn how to create an NCM job to execute a command script on devices.

[Create and Manage NCM jobs](#)

NCM provides job scheduling to automate the management of network devices and configuration files.

[How to create an NCM Purge Old Configs from Database job](#)

Learn how to create an NCM Purge Old Configs from Database job.

[Set up a job that saves the results to a file](#)

Learn how to set up a job and save results to a file.

[NCM Compliance Policy Reports](#)

View information on the NCM Compliance Policy Reports and its features.

[Select nodes to include in a policy or compliance report](#)

Learn how to select nodes to include in a Policy or Compliance report in NCM.

[Create and manage policy rules](#)

Rules are used to ensure that device configurations comply with policies.

[Ensure compliance to policy rules](#)

Use policy reports to verify that device configurations comply with internal policies and external regulations.

[Find remediate policy violations](#)

You can use policy reports to find device configurations that do not comply with policies.

[Audit your Cisco routers](#)

Use the NCM compliance policy reports to verify and maintain compliance within your network.

[Set connection profiles as auto-detect](#)

Set a connection profile to Auto-Detect and set a node to connection profile to Auto-Determine which profile to use.

[Firmware upgrades](#)

Use NCM to upgrade the firmware on multiple devices.

[View firmware vulnerability data](#)

NCM helps identify risks to network security by detecting potential vulnerabilities in multiple device types.

[NCM Firmware Upgrade Guide](#)

View the commands and macros used by the Firmware Upgrade feature introduced in NCM 7.6.

[Ensure HA serves have complete firmware vulnerability data](#)

If you have implemented High Availability (HA) backup servers in your SolarWinds deployment, you must make sure that all servers have comprehensive firmware vulnerability data.

[Network Insight for F5 BIG-IP – Video](#)

Learn how to set up and use this feature of NPM with NCM.

[Network Insight for Cisco ASA Firewalls Getting Started Guide](#)

Learn about the network monitoring capabilities of NPM with the configuration capabilities with the configuration capabilities of NCM.

[NetPath – Video](#)

Learn how to configure and use NetPath.

[Orion integration with NetPath](#)

NetPath displays additional information about NCM nodes with backed-up config files.

Sample Questions

1. Policy reports verify that _____ comply with internal policies and external regulations.
   A. Jobs
   B. Inventory
   C. Network configurations
   D. Device configurations
	2. SolarWinds NCM helps identify risks to network security by detecting potential vulnerabilities for which device types? Select all that apply.
	   A. Palo Alto
	   B. Cisco IOS
	   C. Cisco Adaptive Security Appliance (ASA)
	   D. Cisco Nexus
	   E. Juniper

Category: Settings

Understand how to use real-time change detection and firmware update settings for NCM.

[About real-time change detection](#)

When you configure real-time change detection, SolarWinds NCM sends an email notification whenever a device configuration changes.

[Configure real-time change detection](#)

Learn how to configure real-time change detection.

[What is real-time change detection?](#)

Learn about the real-time change detection requirements.

[Troubleshooting NCM real time change detection](#)

Learn to configure network devices to send a syslog message or a trap message when the configuration on the device changes.

[Configure NCM for real-time change detection](#)

Learn how to configure SolarWinds NCM for real-time change detection after you configure a Cisco device to send syslog messages and configure alerts and filters triggered by syslog and trap messages.

[Set up real-time change detection based on syslog](#)

Know how to set up NCM real-time change detection.

[Examples of commands to send syslog or trap messages to the Orion server](#)

View examples of commands used for some device types.

Configure a Cisco device to send syslog messages

Real-time change detection provides instant notification through email whenever a change to any of your device configurations occurs.

Configure alerts and filters triggered by syslog and trap messages

NCM uses a built-in syslog server and SNMP trap receiver to notify you when it detects configuration changes to your monitored devices.

Access firmware vulnerability settings

NCM imports the firmware vulnerability warnings provided by National Institute of Standards and Technology (NIST) and correlates vulnerabilities with managed nodes.

Set up the storage location and firmware repository

Complete the initial setup before you perform a firmware upgrade operation.

Manage firmware upgrade templates

Each firmware upgrade template defines a set of device-specific commands and options that NCM uses to upgrade the firmware on a device of that type.

Perform a firmware upgrade operation

After you set up your storage location and firmware repository, and firmware upgrade templates, you can perform an upgrade operation.

Sample Questions

1. When you set up Real-Time Change Detection, you must configure your devices to send which type of messages to the Orion server? Select all that apply. A. TCP B. Trap C. DDS D. Syslog E. UDP	2. The firmware upgrade storage location cannot be the same as which root folders? Select all that apply. A. TFTP B. Serv-U C. SFTP/SCP D. ESX E. MFT

Sample Question Answer Key

Installation	1. B 2. B
Configuration Management	1. B 2. A, C
Features	1. D 2. B, C, D, E
Settings	1. B, D 2. A, C