# U.S. Air Force
# Base Information Transport Infrastructure (BITI)
# Base Area Network (BAN)
# Network Management Systems (NMS)

## NMS Fundamentals Lecture

# Communications Check

- Microsoft Teams
  - How we will communicate via voice and video
- Government Azure Portal
  - Turn off Pop-Up Blocker
  - Restart Browser
- Student VM Access
  - Open VM in new window

# Lesson Scope

This training course will provide operational knowledge of the Network Monitoring System (NMS) base platform and the SolarWinds modules:

- Orion Platform
- Network Performance Monitoring (NPM)
- Network Traffic Analyzer (NTA)
- Network Configuration Manager (NCM)
- User Device Tracker (UDT)
- Enterprise Operations Console (EOC)
- USAF BITI BAN NMS Architecture

# Classroom Expectations

- Professionalism always
- Live & follow military and academic ethics
- Collaborate with others/be respectful of their opinions
- Challenge yourself academically (See, Do, Teach)
- Prefer a dialogue instead of a monologue

# Classroom Expectations

- All questions are helpful
- Use time management skills
- Be prepared for each lesson
- Be Neighborly

# Course Administration

- Student Roster and Accounting
  - Please sign in on-time
  - Prepare for questions
- Student Evaluation
  - Please fill out on Friday
- Certificate of Completion
  - Will be sent to Govt. Email listed on Registration Course Worksheet

# Virtual Classroom Expectations

- Be on time for Class
- Be prepared to be on Camera
- Casual Dress or Uniform of the Day
- Mute your Microphone when not speaking

# About the Author

- Enterprise Solutions Architect for Nisga'a Data Systems
- Subject Matter Expert on SolarWinds and Network Compliance
- SolarWinds Thwack MVP - @CourtesyIT
- Helping the SolarWinds Community one IP Address at a time
- SolarWinds Thwack MVP since 2015
- SolarWinds Thwack #1 since April 2017
- Favorite Concert - U2 Joshua Tree Tour 1989

solarwinds CERTIFIED PROFESSIONAL

NPM NCM SAM

USER LEADERBOARD

| | | |
|---|---|---|
| 1st | CourtesyIT | 677,188 Points |
| 2nd | wluther | 642,974 Points |
| 3rd | rschroeder | 615,602 Points |
| 4th | jeremymayfield | 566,102 Points |
| 5th | aLTeReGo | 554,245 Points |
| 6th | Peter Monagh... | 525,494 Points |
| 7th | byrona | 517,842 Points |
| 8th | ecklerwr1 | 480,074 Points |
| 9th | zackm | 476,981 Points |
| 10th | tomiannelli | 468,707 Points |

# Introductions

- Student Name
- Years of Service/Civilian/Contractor
- IT Experience
- Student Ice Breaker
  - Favorite Concert/Band
  - Favorite Restaurant

# Course Agenda

- Introductions
- SolarWinds Orion Platform
- SolarWinds Network Performance Monitor (NPM)
- SolarWinds Network Configuration Manager (NCM)
- SolarWinds NetFlow Traffic Analyzer (NTA)
- SolarWinds User Device Tracker (UDT)
- SolarWinds Enterprise Operations Console (EOC)
- Additional Resources

# Course Agenda

- The USAF BITI BAN NMS
  - Local and Regional Differences
  - Maintaining the BITI BAN NMS
  - BAN NMS Overview
  - BAN NMS Architecture Overview
  - NMS Host
  - NMS Hypervisor/Host OS
  - NMS VMs/Guest OS

# How this Course is Designed

- First Part – Lecture
  - Instructor led discussions and material
- Second Part – Demo
  - Instructor led walkthrough to familiarize the students with the interface and lab tasks
- Third Part – Lab
  - Students will perform the lab individually & independently
- Quiz
  - End of Course Quiz
- Questions and Answers - Encouraged
  - Please feel free to speak up and ask questions, You may not be the only one with that question

# Agenda: 4 Day Class

| TP Sec. # | Course Name | Class Time | Lab Time | Day-1 | Day-2 | Day-3 | Day-4 | Totals |
|---|---|---|---|---|---|---|---|---|
| | Introductions and Housekeeping | 0.5 | | 0.5 | | | | |
| 6.2.2.a | Orion Platform | 5 | 3 | 8 | | | | |
| 6.2.2.b | Network Performance Monitor (NPM) | 4 | 2 | 1.5 | 4.5 | | | |
| 6.2.2.c | Network Configuration Manager (NCM) | 5 | 4 | | 5 | 4 | | |
| 6.2.2.d | NetFlow Traffic Analyzer (NTA) | 2 | 1 | | | 3 | | |
| 6.2.2.e | User Device Tracker (UDT) | 3 | 1 | | | 3 | 1 | |
| 6.2.2.f | Enterprise Operations Console (EOC) | 3 | 1 | | | | 4 | |
| 6.2.2.g | BITI BAN NMS Architecture and Solution Design | 5 | | | | | 5 | |
| | Daily Hr. Subtotals | 27.5 | 12 | 10 | 9.5 | 10 | 10 | 39.5 |

# Agenda: 5 Day Class

| TP Sec. # | Course Name | Class Time | Lab Time | Day-1 | Day-2 | Day-3 | Day-4 | Day-5 | Totals |
|---|---|---|---|---|---|---|---|---|---|
| | Introductions and Housekeeping | 0.5 | | 0.5 | | | | | |
| 6.2.2.a | Orion Platform | 5 | 3 | 8 | | | | | |
| 6.2.2.b | Network Performance Monitor (NPM) | 4 | 2 | | 6 | | | | |
| 6.2.2.c | Network Configuration Manager (NCM) | 5 | 4 | | | 7 | 2 | | |
| 6.2.2.d | NetFlow Traffic Analyzer (NTA) | 2 | 1 | | 2 | 1 | | | |
| 6.2.2.e | User Device Tracker (UDT) | 3 | 1 | | | | 4 | | |
| 6.2.2.f | Enterprise Operations Console (EOC) | 3 | 1 | | | | | 4 | |
| 6.2.2.g | BITI BAN NMS Architecture and Solution Design | 5 | | | | | | 5 | |
| | Daily Hr. Subtotals | 27.5 | 12 | 8.5 | 8 | 8 | 6 | 9 | 39.5 |

- 15 Minutes

# Break

# SolarWinds Orion Network Management System

# Today's Agenda

- This section's topics include:
  - Introduction to the Orion Platform
  - Orion Installer, SQL, and Configuration Wizard
  - Network Discovery Wizard
  - Custom Properties
  - Groups
  - Views & Dashboards
  - Managing Users
  - Managing Node Database
  - Maps & Network Atlas

# Orion Architecture



**Orion Platform Features**

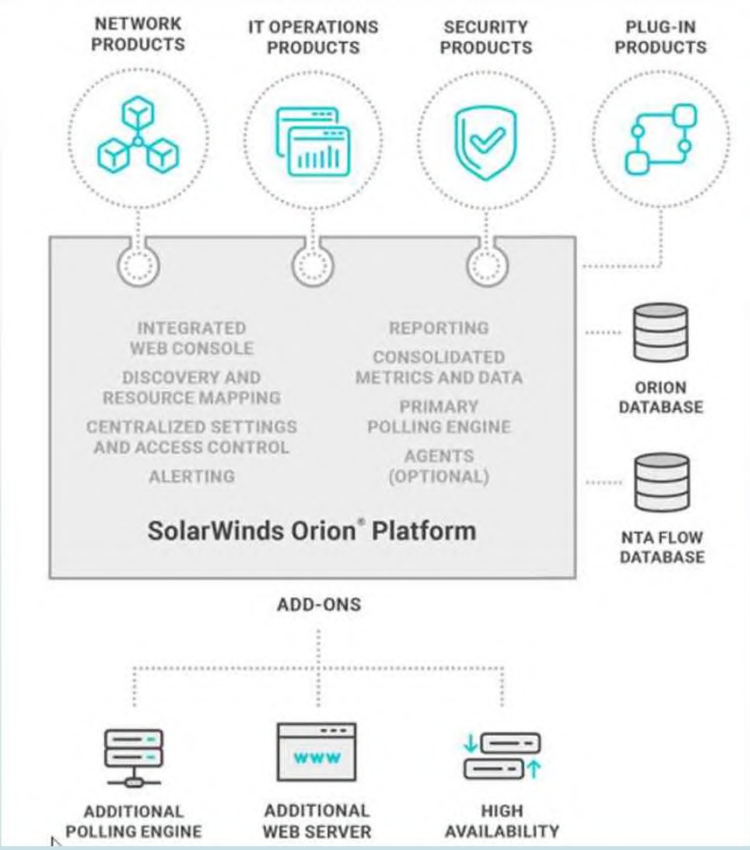
- Integrated Web Console
- Discovery and Resource Mapping
- Centralized Settings and Access Control
- Alerting
- Reporting
- Consolidated Metric and Data
- Primary Polling Engine

**Basic Requirements**

- Windows Server 2016/2019
- SQL Server 2016/2019

**Sizing Depends**

- How many Nodes, Interfaces and Volumes
- How many Platform Products
- How many Sites, Subnets and Security

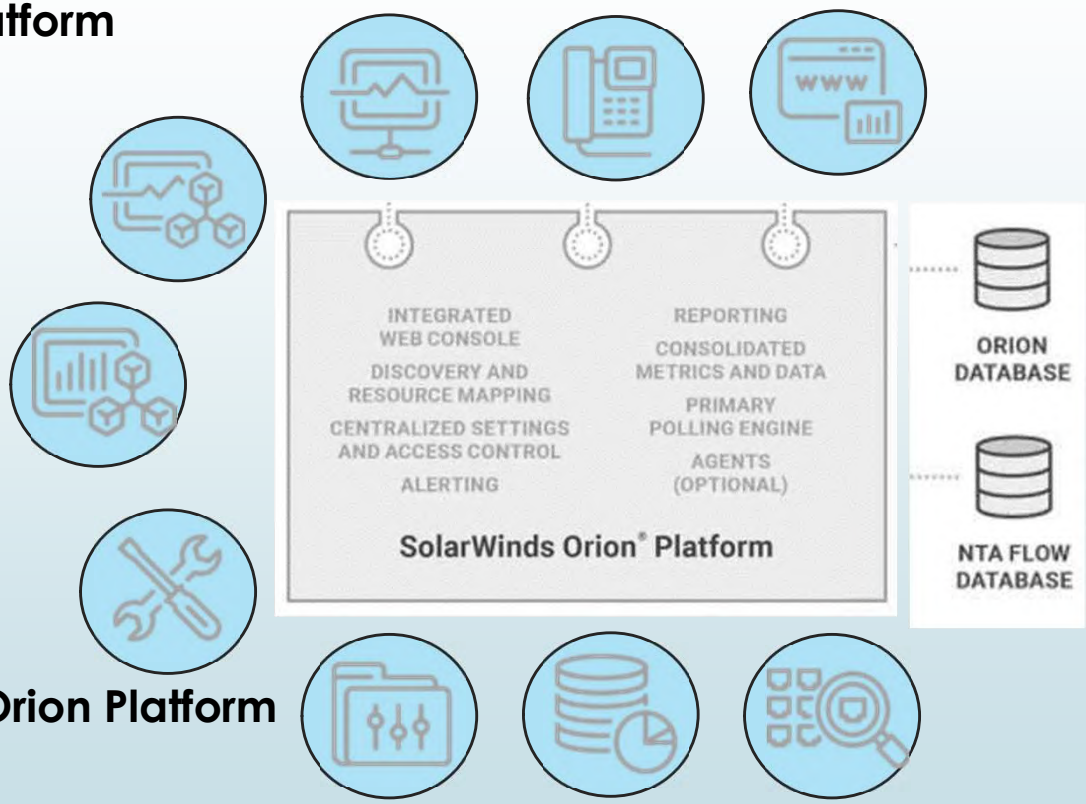


# Orion Architecture



**Products built on the Orion Platform**

- Network Performance Monitor
- NetFlow Traffic Analyzer
- Network Configuration Manager
- IP Address Manager
- VoIP & Network Quality Manager
- User Device Tracker
- Log Analyzer
- Web Performance Monitor
- Server & Application Monitor
- Server Configuration Monitor
- Virtualization Manager
- Storage Resource Monitor




**Products integrated with the Orion Platform**

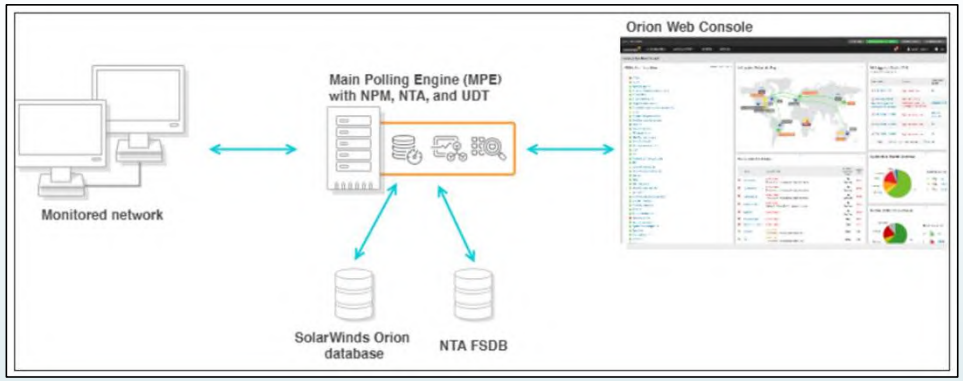
- Database Performance Analyzer
- Application Monitor
- Patch Manager
- Engineers Toolset

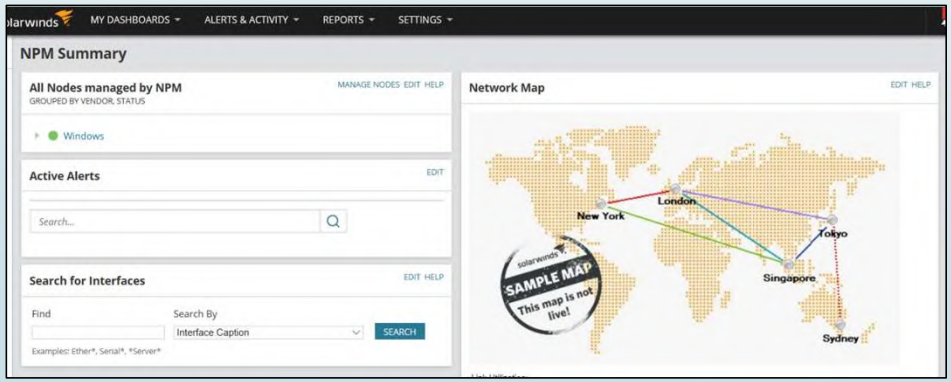
# SolarWinds Orion



Orion Common Terms

- Orion Platform: The backbone on which many products reside and are integrated with each other
- Orion Web Console: Web interface to View, Configure and manage all your monitored objects
- View: Dashboard to view status of your monitored objects
- Widget: The informational blocks that make up your view



# BITI BAN NMS SolarWinds Products



- Network Performance Monitor (NPM):
  - Monitors the health and performance of network devices and interfaces.
- NetFlow Traffic Analyzer (NTA):
  - Analyzes flow data for the details of traffic impacting bandwidth on the network.
- Network Configuration Manager (NCM):
  - Monitors, manages, and backs up configuration files for network devices. Provide Regulatory Compliance Auditing for DISA STIGs, NIST, PCI, and others
- User Device Tracker (UDT):
  - Tracks both current and historical switch and port connections for network users.
- Enterprise Operations Console (EOC):
  - Aggregates NMS data from multiple BAN NMS systems for simultaneous view.

# SolarWinds Software Installer



- Orion Installer
  - Evaluation Version
    - Standalone with SQL Express
  - Production Version
    - Orion Server and a separate SQL Server
  - Scalability Version
    - For use Additional Polling Engines and Additional Webservers
- Contains Hot Fixes, Patches, and Updates
- There are two different types of installers
  - Online – for those systems connected to the internet with access to SolarWinds.com
  - Offline – Downloaded from SolarWinds and moved from internet connected network to air-gapped or standalone networks (i.e., NIPRNET, SIPRNET)

# SolarWinds Software Installer



- Orion Installer
  - Lightweight Installation
    - Evaluation Version
    - Standalone with SQL Express
  - Standard Installation
    - Production Version
    - Orion Server and a separate SQL Server
  - Add a Scalability Engine
    - For use Additional Polling Engines and Additional Webservers

- Contains Hot Fixes, Patches, and Updates

# Installing SQL

- How does SolarWinds write data? How does it affect I/O operations of the Database.
  - Constant and persistent, small amounts of Data. No large data dumps.

# SQL Best Practices

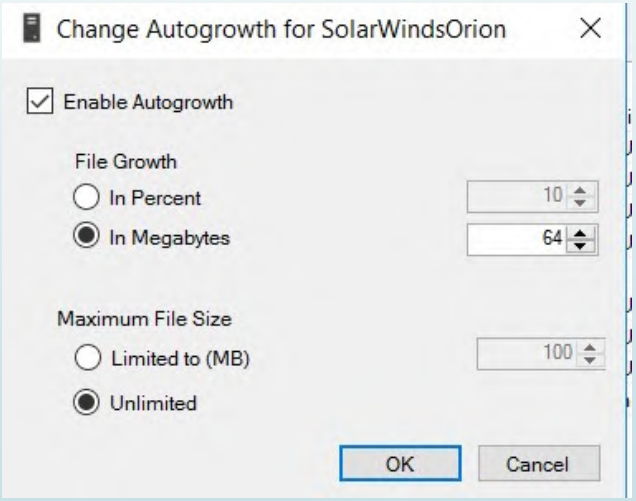


- SolarWinds supports Windows© authentication to SQL Databases
  - Encrypts the Username and Password in transmission but not database data
  - SQL Authentication is also supported with the following configurations:
    - Mixed-Mode authentication and strong passwords
    - DB_Creator role for new databases
    - DB_Owner role will work for existing databases
    - Security_Admin role for SQL User account

# SQL Best Practices



- Before you install
  - Use SQL, not SQL Express
  - SQL Server and Orion Server on same LAN
  - SQL Mgt Studio > Database > Your database right-click Properties > scroll to the right and select primary Autogrowth.
  - RAID 10 is the recommended disk configuration for the best DB I/O with SolarWinds Products

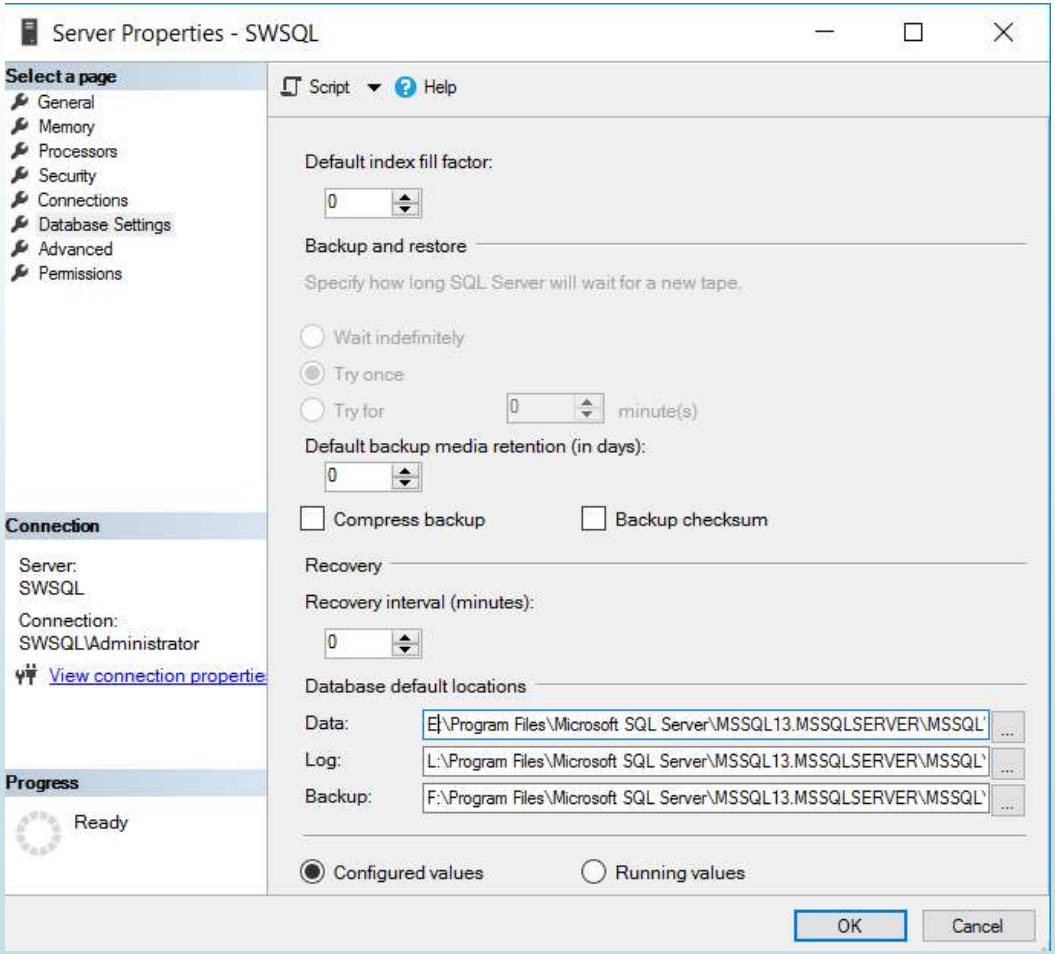



- Review Installation Guide and Administrators Guide
- RAM, RAM, RAM! Did you Reserve RAM for your OS?

# SQL for use with SolarWinds



- Database Recommendations
  - SQL data files and log files on separate logical drives
    - E:\Data
    - F:\Logs
    - G:\Backups
  - Set Auto-growth to (X)MB or 10%
    - Do not set file growth limits
  - Reserve 10% of System RAM for Operating System



# Installing Orion Platform Products



- Two Dedicated Servers: SolarWinds Orion Server and SolarWinds SQL Server
- Do not install on Domain Controllers.
- Systems check will automatically stop.
- Install the defaults, then go back and make changes.
- Disable UAC Slider prior to installation of software, updates, patches and running the Configuration Wizard.
- Installer will install MSMQ, .NET, and IIS

# Configuration Wizard

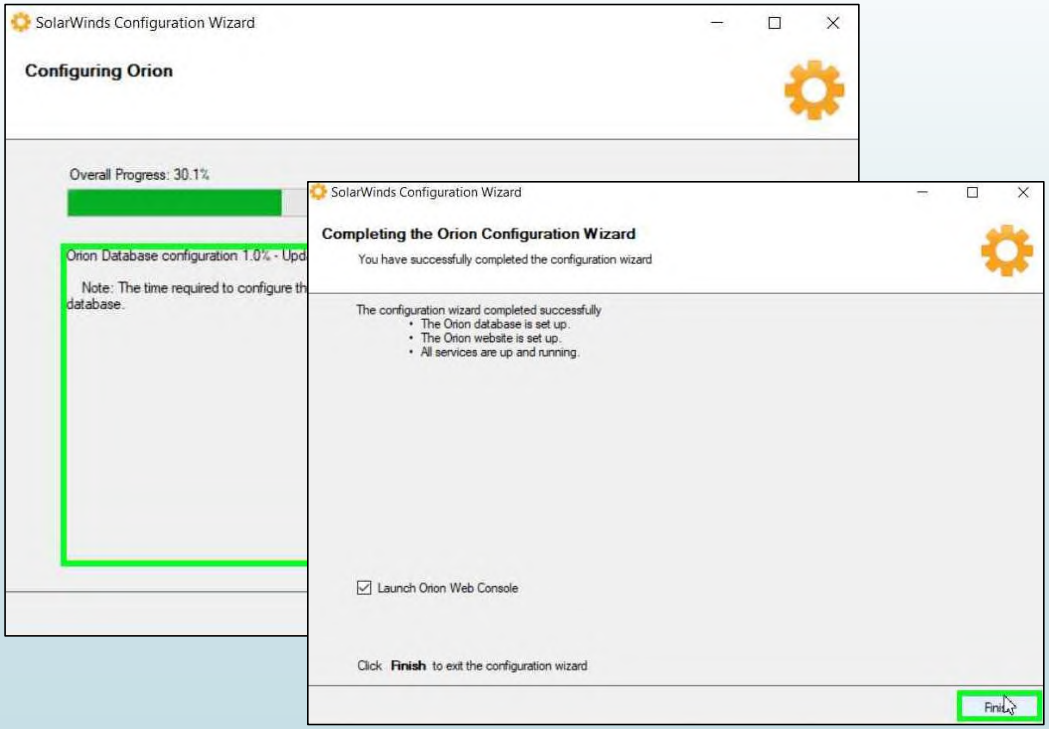


- What is the Configuration Wizard?
  - Configures Installed SolarWinds Software
  - Builds, initializes, and synchronizes database
- When do I use the Configuration Wizard?
  - Communication issues between Orion Server and SQL Server
  - Microsoft .NET Framework Patches
  - Microsoft SQL Server Patches

# Configuration Wizard



- 15-60 Minutes
- Will take down services
- Fix Issues
  - Database
  - Web
  - Services



- Installing SolarWinds 2020.2.1 HF2 Software
- Running the Configuration Wizard

# Break

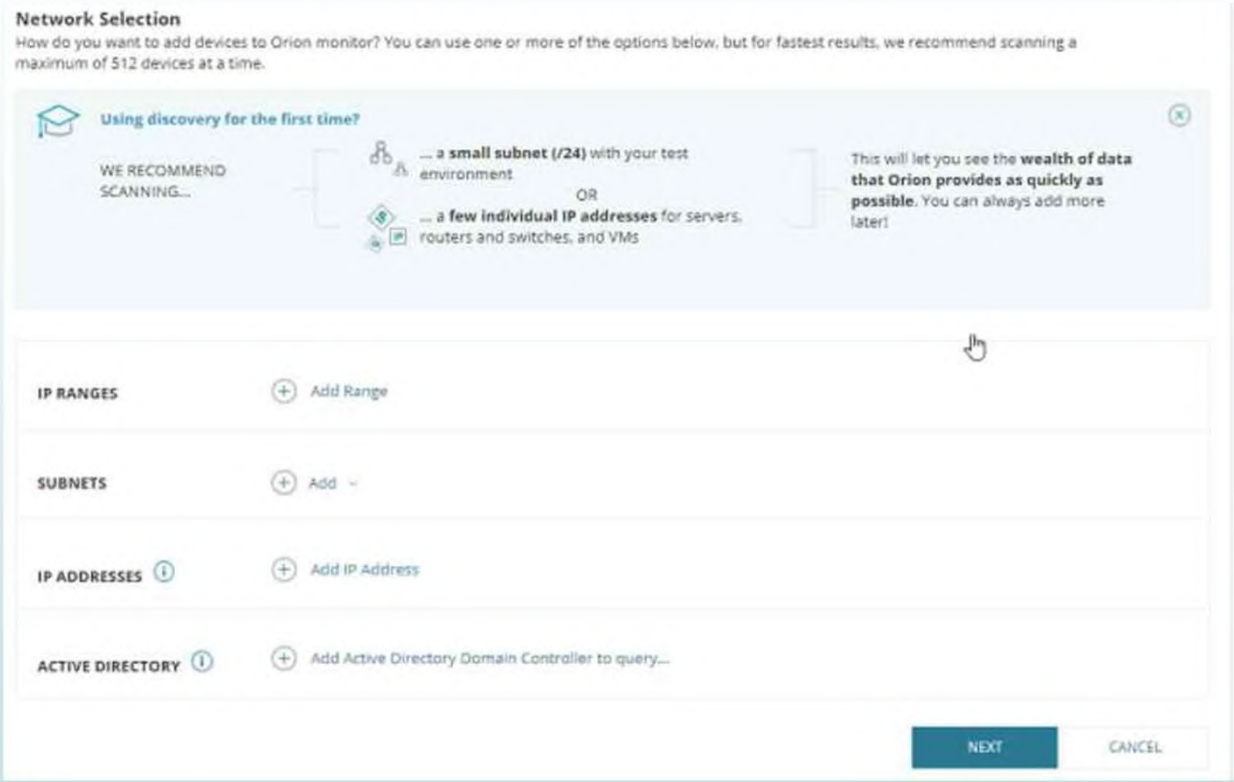
# DEMO & LAB 01

# Network Discovery Wizard

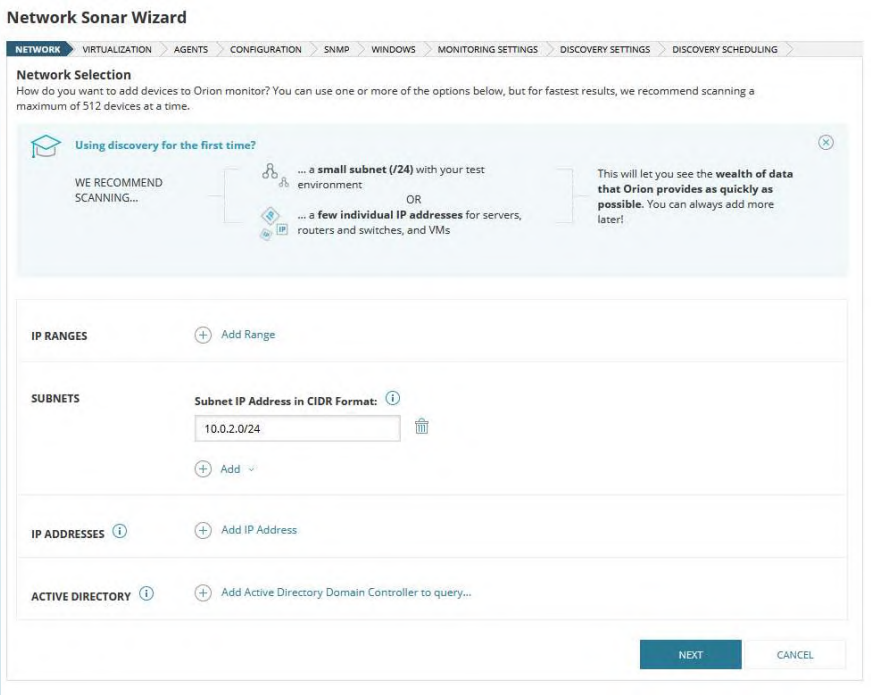
- IP Ranges
- Subnets and Seed Router
- IP Address or Hostname
- Active Directory

# Network Discovery Wizard





# Network Discovery Wizard

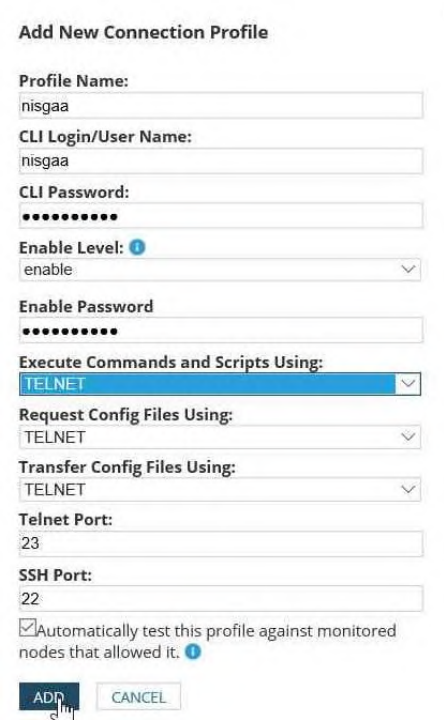



- Adding a single subnet or multiple
- Best Practice is to keep it within a CIDR /22

# Network Discovery Wizard



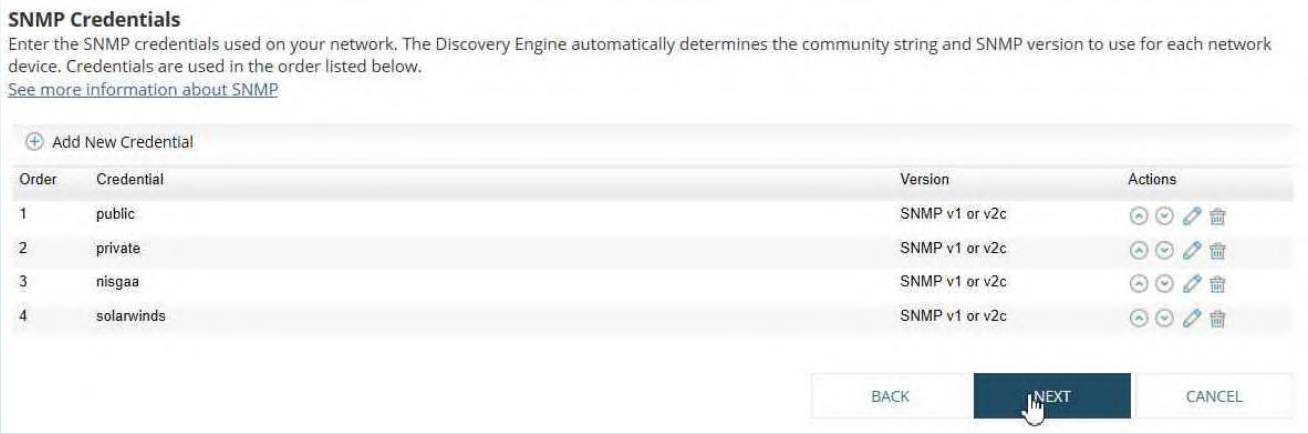
- Configuration tab will be discovering all networking devices using a set of credentials allowed access from the device
- This will be from the SolarWinds Server to the target device



# Network Discovery Wizard



- The SNMP tab will be used to search the discovery objects for valid SNMP credentials
- Some Vendor may have case-sensitivity and character restricts on SNMP credentials

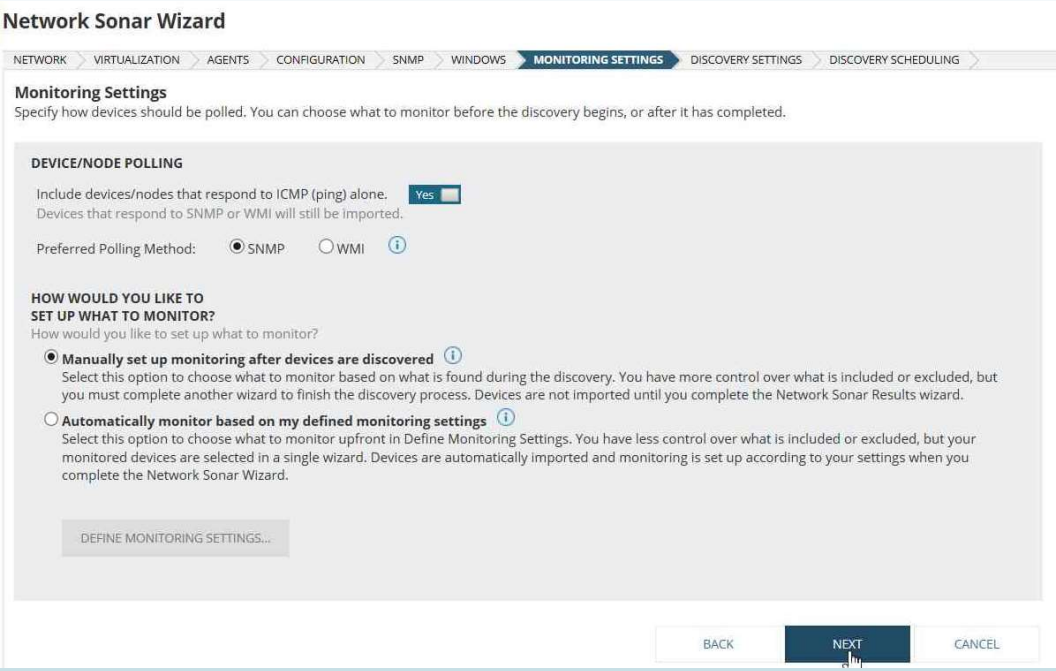


# Network Discovery Wizard



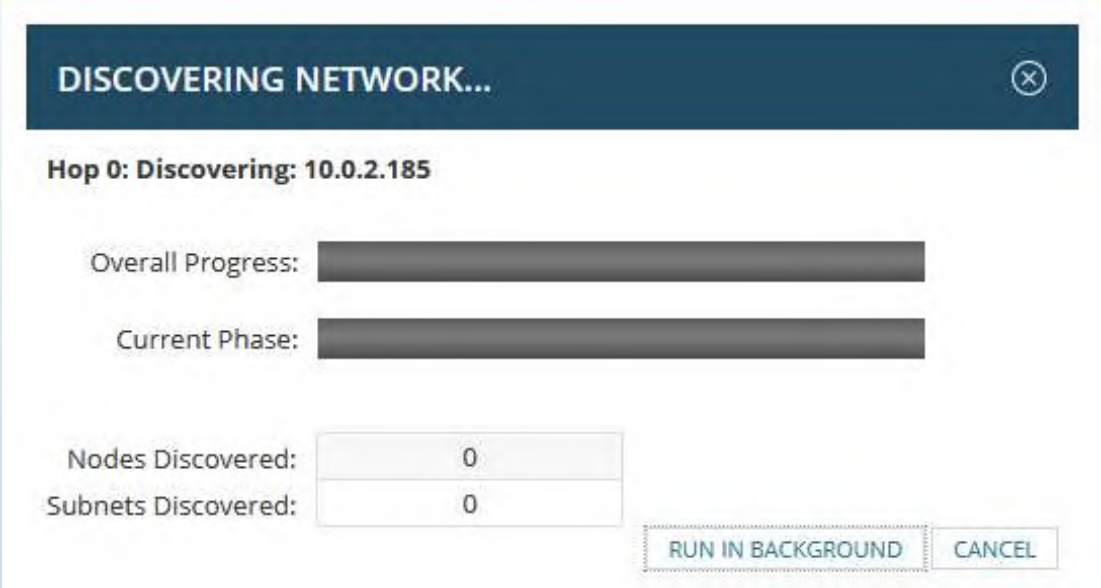
- Use directed discoveries
  - Network Devices
  - Servers
  - Workstations
  - Printers
  - Appliances

- Each discovery will define Polling method



# Network Discovery Wizard

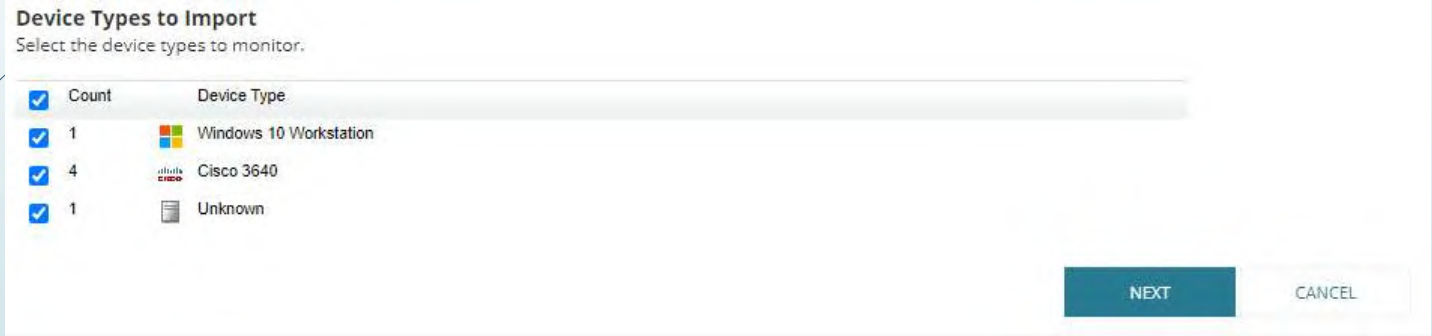
- Progress of a discovery



# Network Discovery Wizard

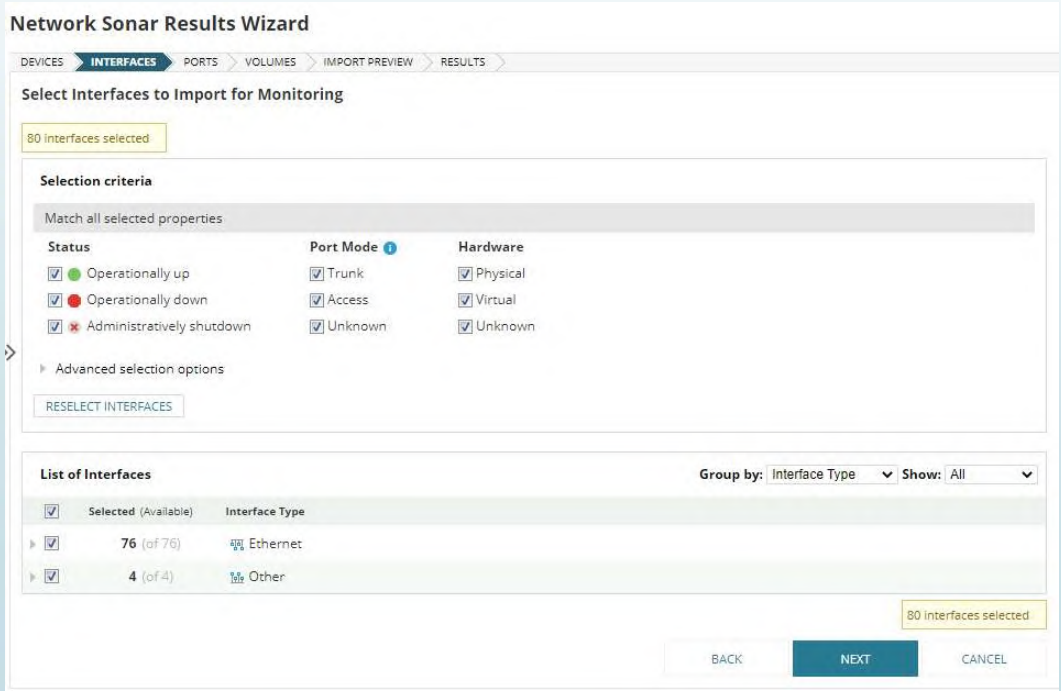


- Results of a discovery with the credentials and methods defined



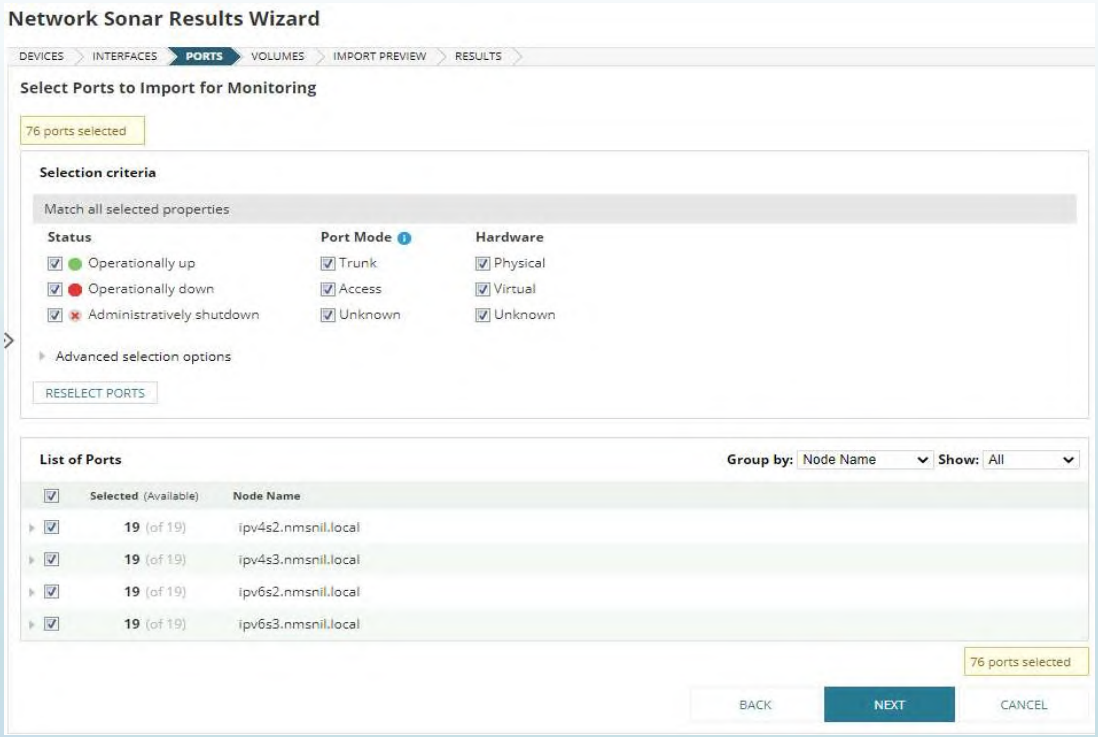
# Network Discovery Wizard

- Importing Interfaces can be tricky
  - Beware of Juniper devices! A single Juniper Device may import up to 8,000 interfaces/volumes per device.



# Network Discovery Wizard

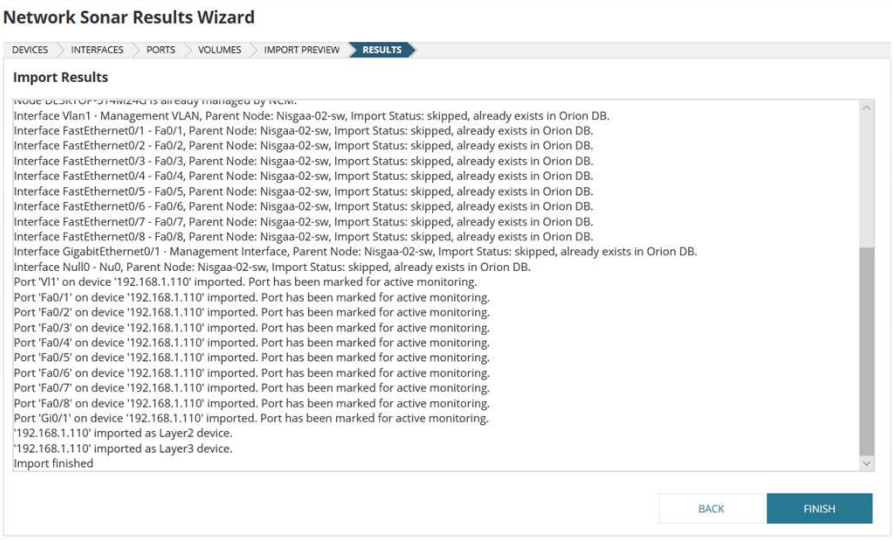
- List of interfaces, volumes and nodes to import into your SolarWinds database



# Network Discovery Wizard



- The wizard will import elements selection on the previous screens
- If there is a duplicate in the database, the Wizard will skip the duplicate

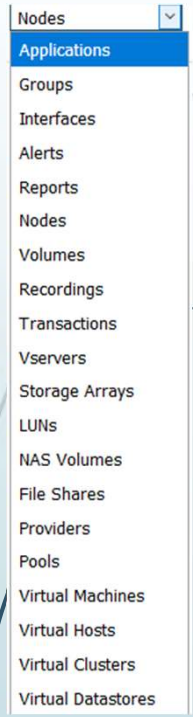


- Network Sonar Wizard Tabs
  - Network
  - Virtualization
  - Configuration
  - Agents
  - SNMP
  - Windows
  - Monitoring Settings
  - Discovery Settings
  - Discovery Schedule

# Break

# DEMO & LAB 02

# Custom Properties (CP)



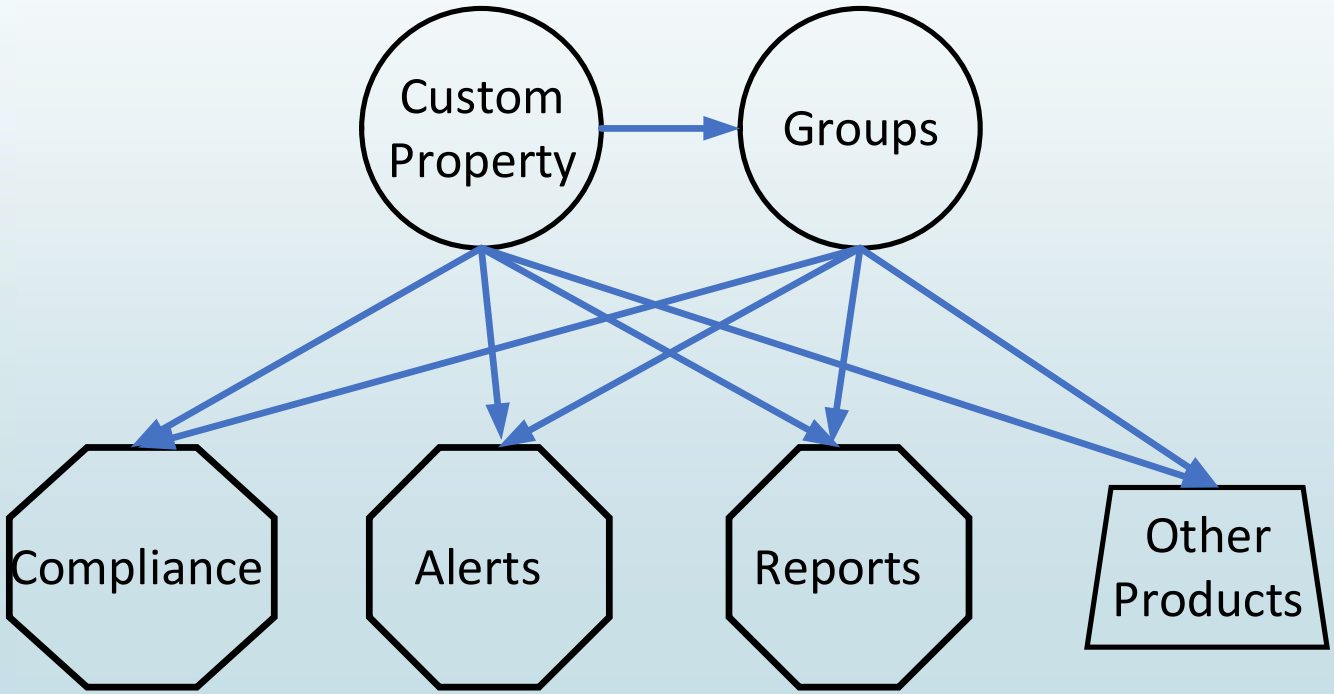

- Basic Building blocks for automation features in SolarWinds
- Types
- Usage
  - Assist in identify nodes on location, environment, Scorecard Reporting, etc.
  - Grouping like CPs together to find in drop down menus throughout the system
- BITI BAN NMS Standards
  - (1) Digit Alpha & (1) Numeric nomenclature for all custom properties
  - Examples:

| | | | |
|---|---|---|---|
| L1_Base | C1_DeviceType | M1_Polling Method | P1_Unit |
| L2_Building | C2_OS | M2_CredentialSet | P2_Name |
| L3_Room | C3_Function | M3_Polling Engine | P3_Phone |
| L4_Rack | C4_Application | | P4_Email |

# Custom Properties

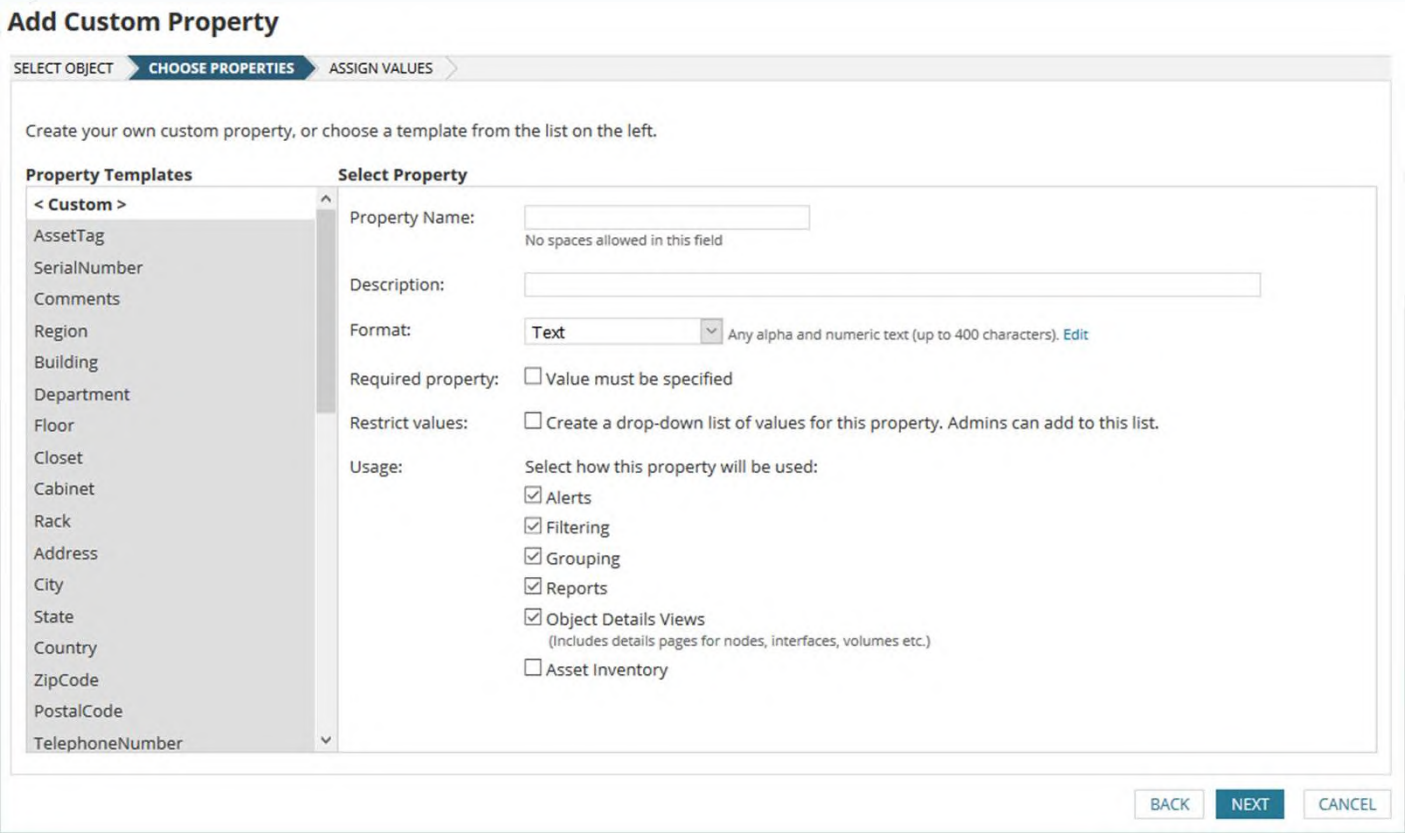


- The importance of well-defined custom properties



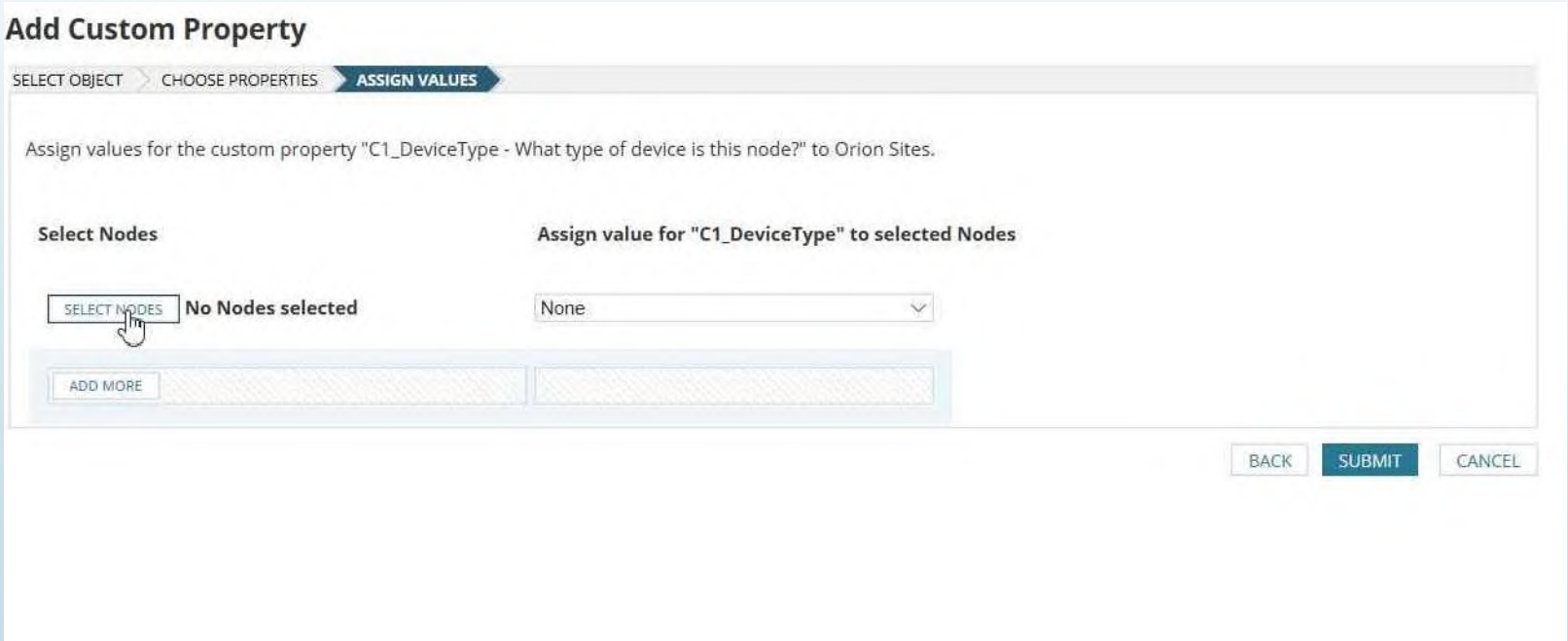
# Custom Properties





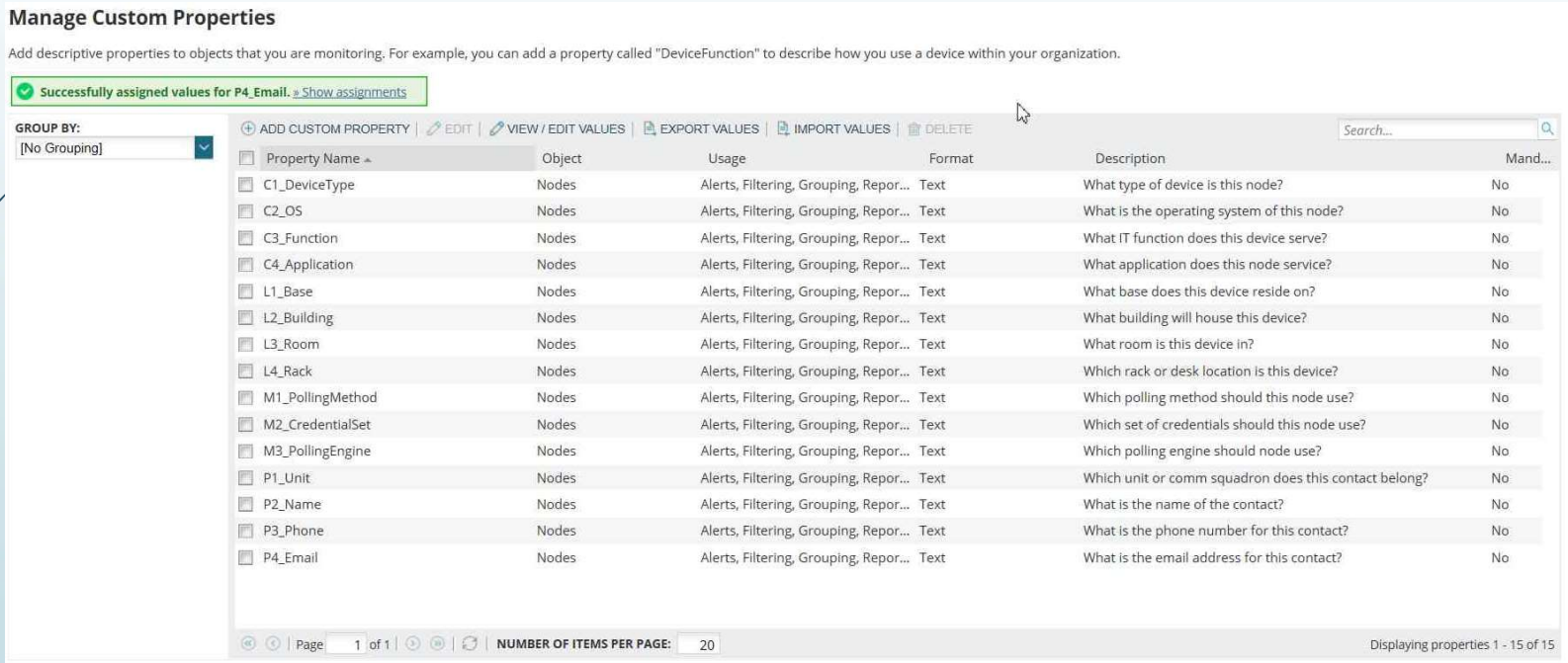
# Custom Properties

- Selection of nodes to configure with this customer property



# Custom Properties

- Each Custom Property has a well-defined description for others that come behind us to know what the Custom Property is to be used for.



**Manage Custom Properties**

Add descriptive properties to objects that you are monitoring. For example, you can add a property called "DeviceFunction" to describe how you use a device within your organization.

Successfully assigned values for P4_Email. » Show assignments

GROUP BY: [No Grouping]

ADD CUSTOM PROPERTY | EDIT | VIEW / EDIT VALUES | EXPORT VALUES | IMPORT VALUES | DELETE

Search...

| Property Name | Object | Usage | Format | Description | Mand... |
|---|---|---|---|---|---|
| C1_DeviceType | Nodes | Alerts, Filtering, Grouping, Repor... | Text | What type of device is this node? | No |
| C2_OS | Nodes | Alerts, Filtering, Grouping, Repor... | Text | What is the operating system of this node? | No |
| C3_Function | Nodes | Alerts, Filtering, Grouping, Repor... | Text | What IT function does this device serve? | No |
| C4_Application | Nodes | Alerts, Filtering, Grouping, Repor... | Text | What application does this node service? | No |
| L1_Base | Nodes | Alerts, Filtering, Grouping, Repor... | Text | What base does this device reside on? | No |
| L2_Building | Nodes | Alerts, Filtering, Grouping, Repor... | Text | What building will house this device? | No |
| L3_Room | Nodes | Alerts, Filtering, Grouping, Repor... | Text | What room is this device in? | No |
| L4_Rack | Nodes | Alerts, Filtering, Grouping, Repor... | Text | Which rack or desk location is this device? | No |
| M1_PollingMethod | Nodes | Alerts, Filtering, Grouping, Repor... | Text | Which polling method should this node use? | No |
| M2_CredentialSet | Nodes | Alerts, Filtering, Grouping, Repor... | Text | Which set of credentials should this node use? | No |
| M3_PollingEngine | Nodes | Alerts, Filtering, Grouping, Repor... | Text | Which polling engine should node use? | No |
| P1_Unit | Nodes | Alerts, Filtering, Grouping, Repor... | Text | Which unit or comm squadron does this contact belong? | No |
| P2_Name | Nodes | Alerts, Filtering, Grouping, Repor... | Text | What is the name of the contact? | No |
| P3_Phone | Nodes | Alerts, Filtering, Grouping, Repor... | Text | What is the phone number for this contact? | No |
| P4_Email | Nodes | Alerts, Filtering, Grouping, Repor... | Text | What is the email address for this contact? | No |

Page 1 of 1 | NUMBER OF ITEMS PER PAGE: 20 | Displaying properties 1 - 15 of 15

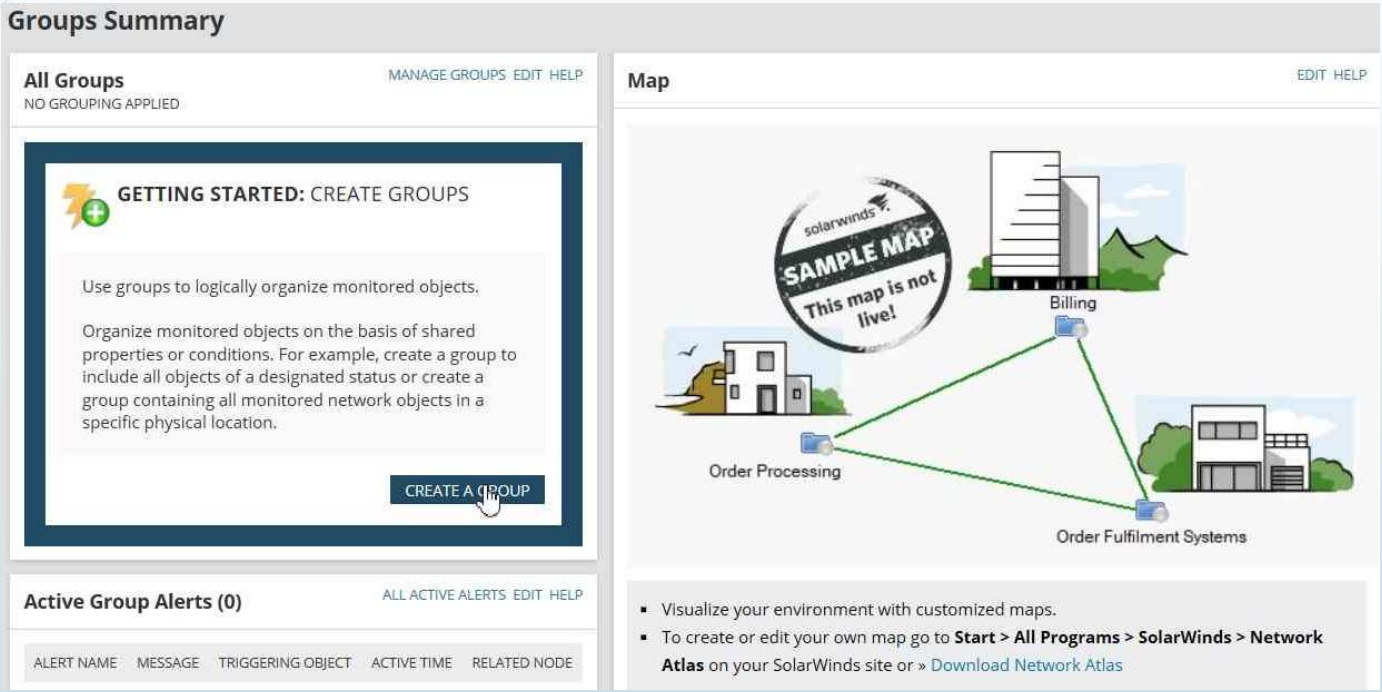
- Custom Properties
  - Refer to Custom Proper -ties worksheet for list of Custom Properties to configure

# Break

# DEMO & LAB 03

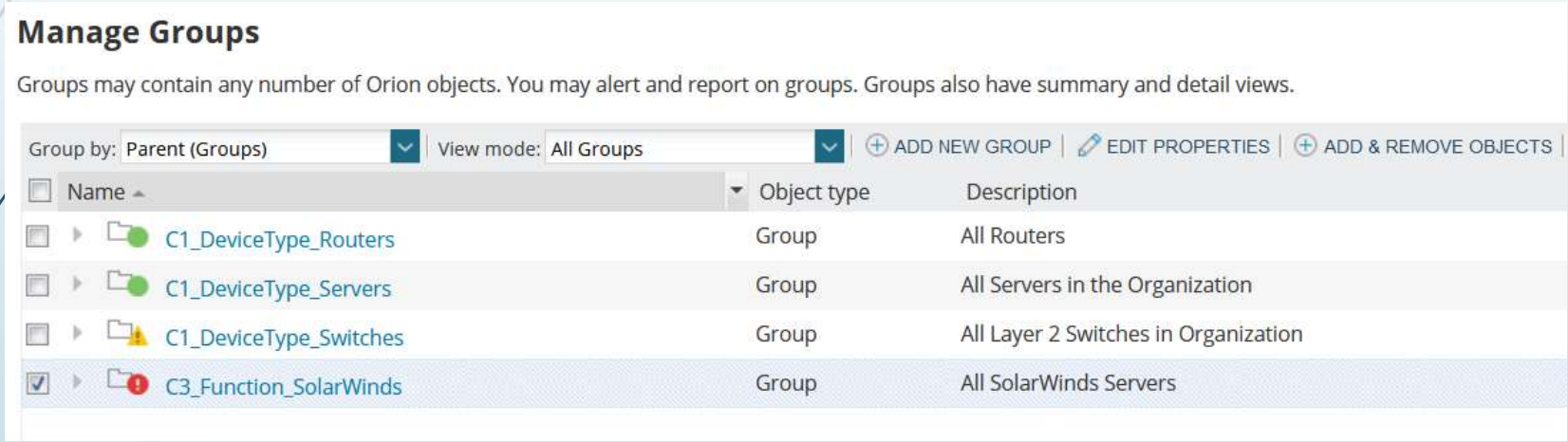
# Getting Started with Groups





# Groups

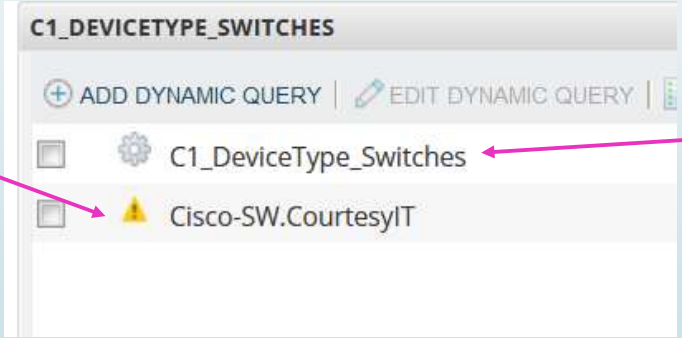
- What are they?
- How do I use them?



# Groups

- There are two different ways to populate groups
  - Manual Selection – Requires ongoing maintenance and Management
  - Dynamic Query – Automated way of populating groups based on Custom Property

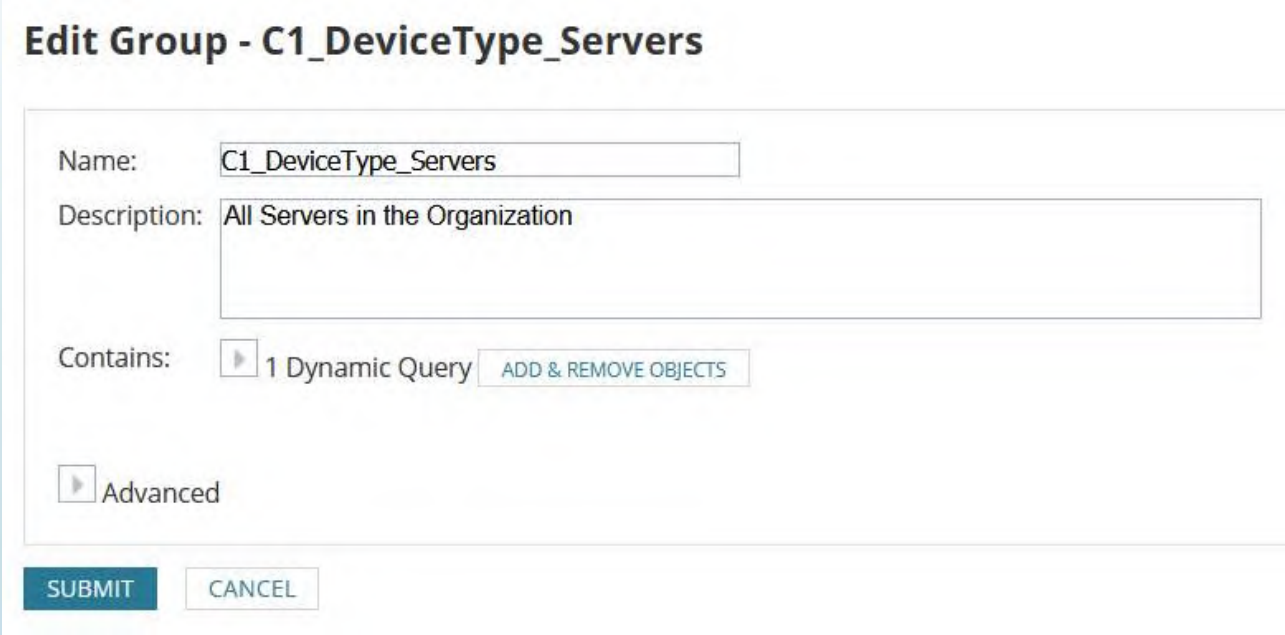
Manual Selection




Dynamic Selection
(Recommended)

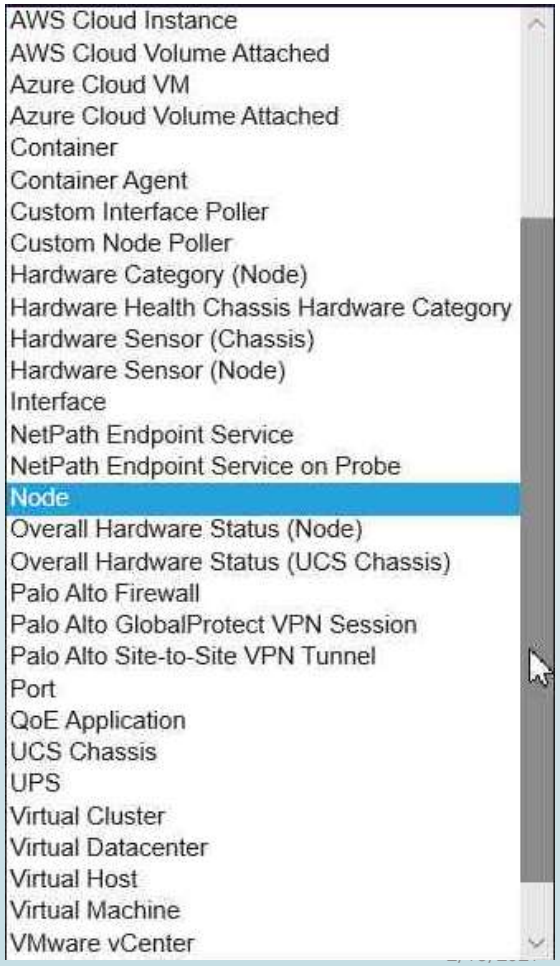
# Groups

- When adding groups use a naming nomenclature that makes sense then standardize the rest of your groups on that standard



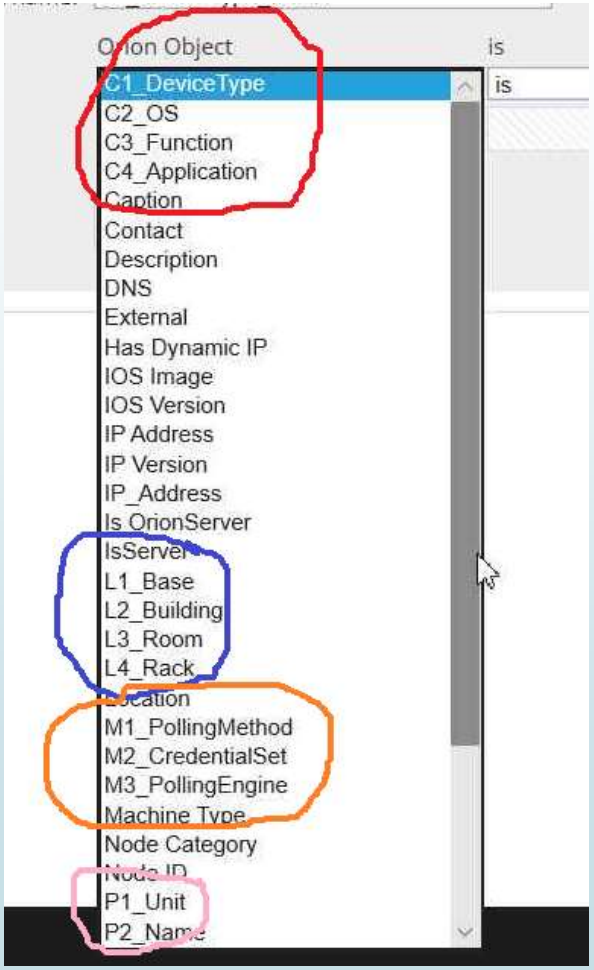
# Groups

- Majority of groups are created based on Nodes or interfaces
- Creating a group can be based or sourced from a plethora of items as shown here



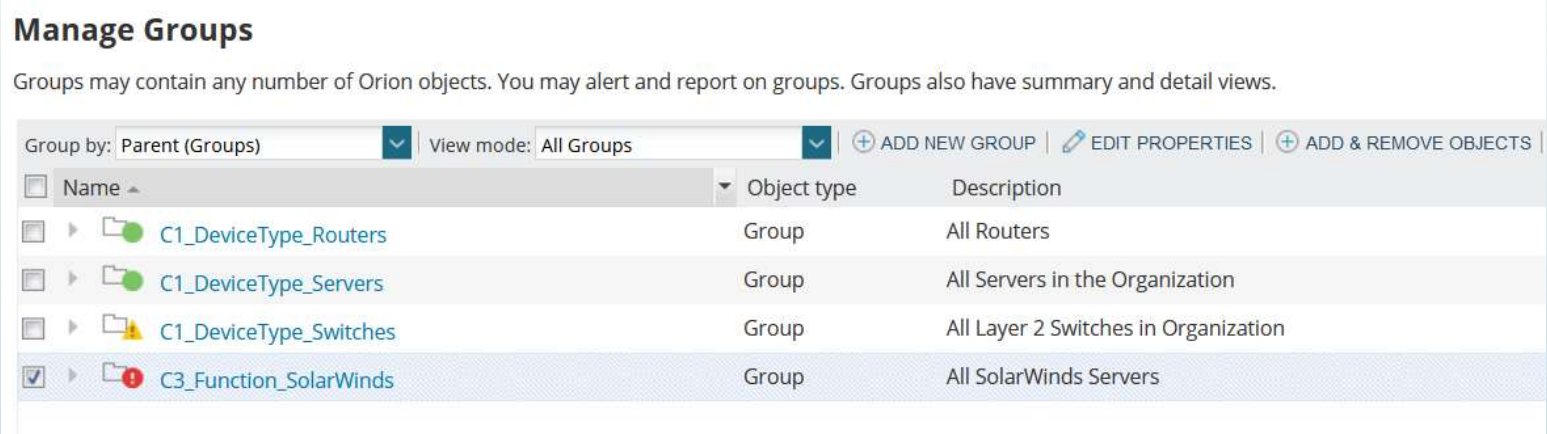
# Groups

- Notice the Custom Properties that were built!
- Select a Custom Property for the purpose of the Group



# Groups

- Keeping a standard naming convention will reduce clutter, confusion, and misconfiguration
- Always provide a description so those around you know why the group was created and the purpose of the group



- Groups
  - All Layer 2 Switches
  - All Infrastructure Layer 3 Switches
  - All Infrastructure Routers
  - All Windows Workstation
  - All SolarWinds Servers

# Break

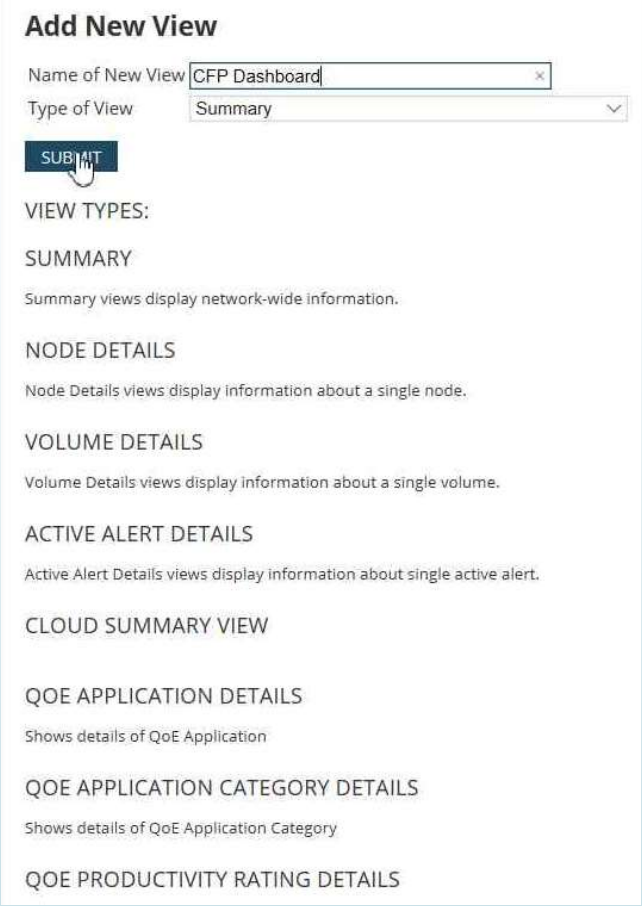
# DEMO & LAB 04

# Views

- Web Console Views
  - Each Product, some with ready-to-use, preconfigured views
  - Views can be used "as is," customized, or user-developed
  - View permissions can be configured using account limitations

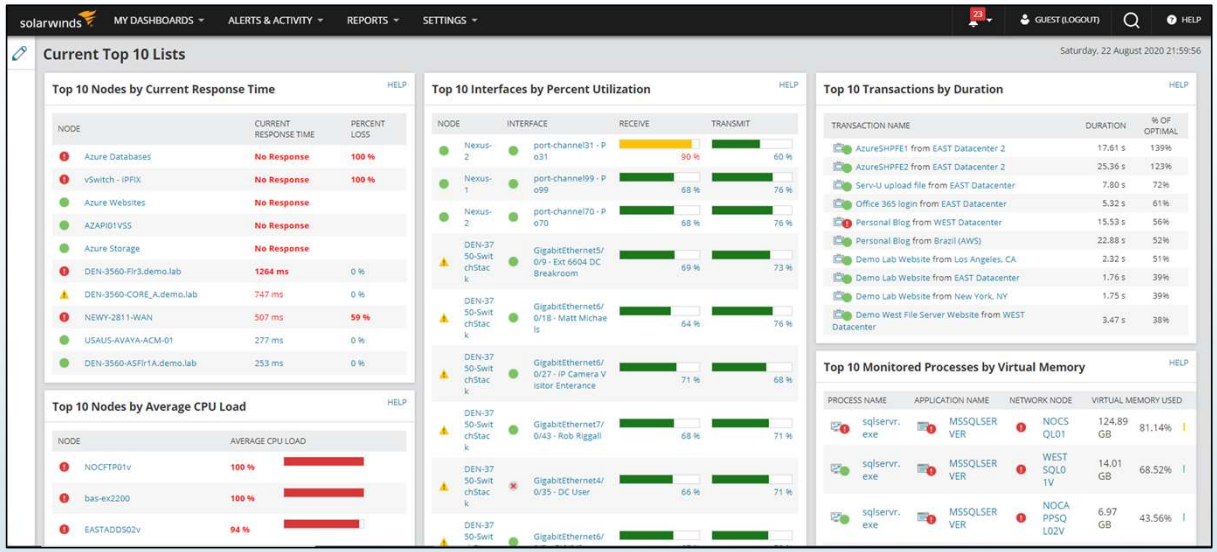
# Views

- Two Main Types of Web Console Views
  - Summary Views
  - Detailed Views



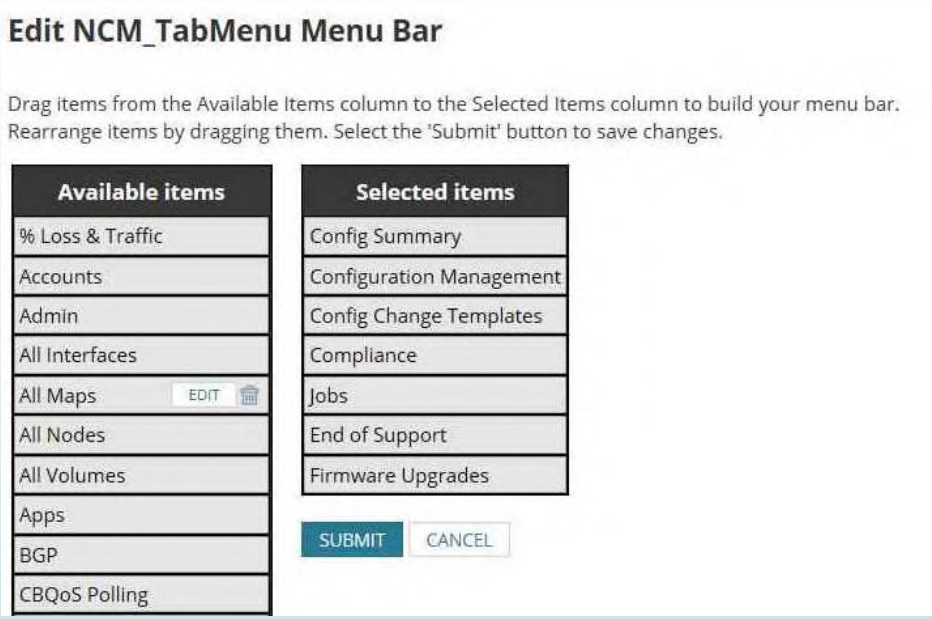
# Views

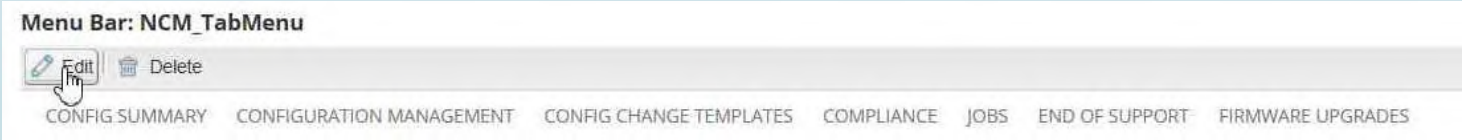
- Things to remember when building Views
  - Build views for role groups
  - Don't share views between Groups
  - Make copies of views and assign them
  - Think about naming conventions and nomenclatures



# Views

- Menu Bars provide the navigation points for users to operate the software and provide different product views

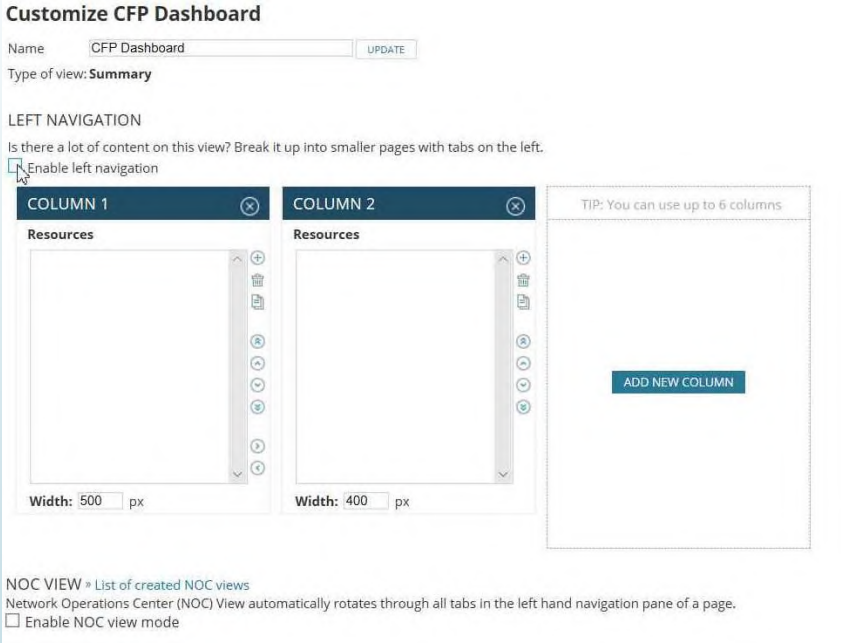


# Views

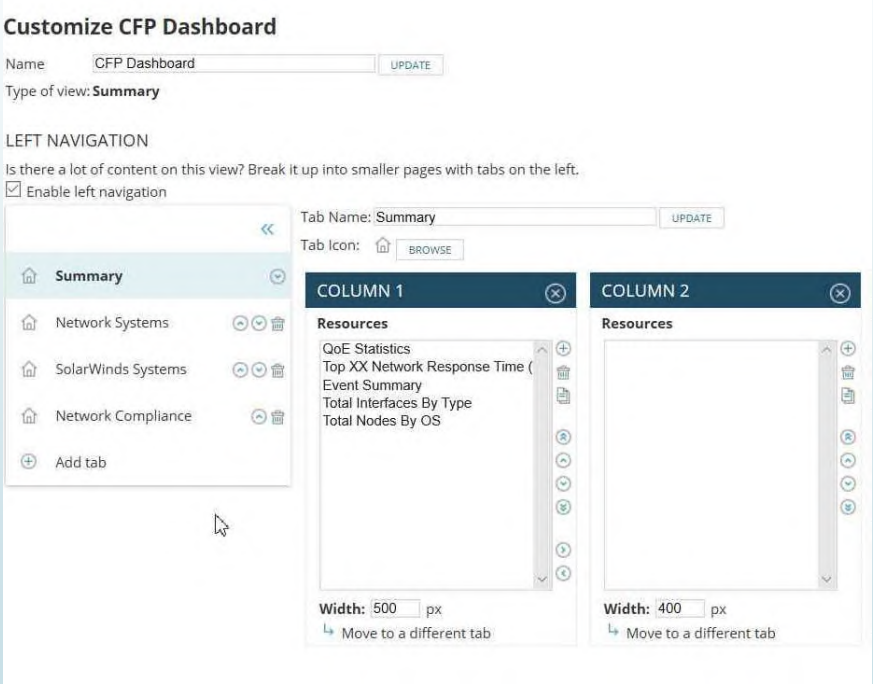


- Adding Widgets to specific columns
- Adding Columns
- Setting up Framework



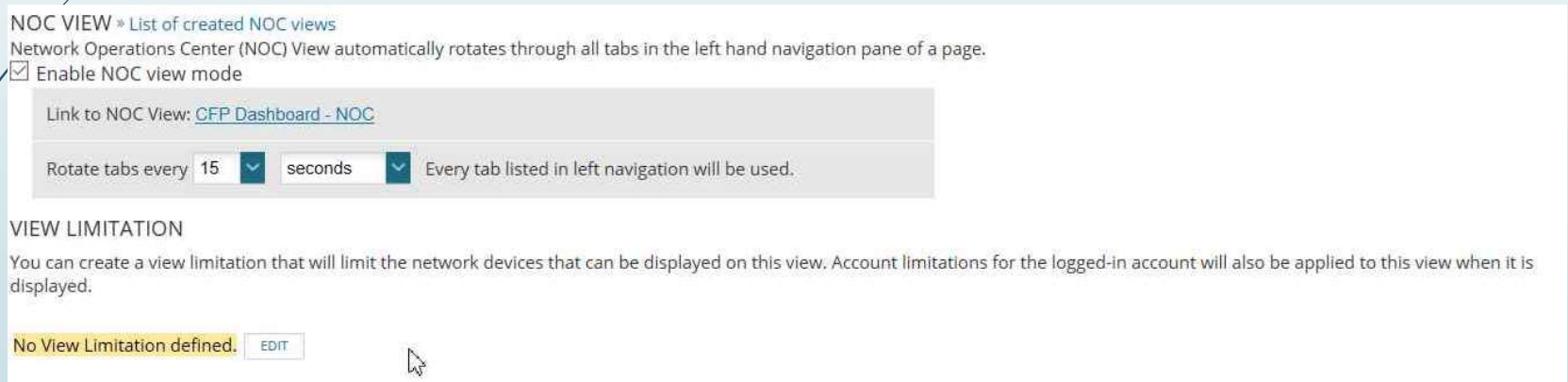
# Views

- Left Navigation
  - Ability to add additional tabs to a view
  - Categorizing various datapoints and metrics for an operations center



# Views

- NOC View
  - Provides rotating screens based on tabs created at a frequency which meets the needs of the user



# Views

- Define the limitation based on object, user, group parameters
- Ability to define who can see what and how they can view it

**Select Limitation Type For View "CFP Dashboard - Summary"**

Select a Limitation Type for this View. A Limitation can be used to limit the Network Devices that can be displayed on this view. For example, you could create a Limitation for a View that allows only Windows Servers. Or, you could limit this View to only show a specific Region or Country.

| | |
|---|---|
| **System Name Pattern** | Limit the Account to a group of Nodes with similar System Names |
| **Group of Machine Types** | Limit the Account to specific Types of Devices |
| **Machine Type Pattern** | Limit the Account to specific types of devices based on a Device Type pattern |
| **Hardware Manufacturer** | Limit the Account to specific Hardware Manufacturers |
| **Device Status** | Limit the Account based on the Node's Status ( Up, Down, Warning ) |
| **System Location** | Limit the Account to a specific list of device Locations. The Node's System Location is discovered and used. |
| **System Location Pattern** | Limit the Account based on a Location pattern. The Node's System Location is discovered and used. |
| **System Contact** | Limit the Account to a specific list of device Contacts. Each Node's System Contact is discovered and used. |
| **System Contact Pattern** | Limit the Account based on a Contact pattern. Each Node's System Contact is discovered and used. |
| **Single Machine Type** | Limit the Account to a single Machine Type |
| **Single Hardware Manufacturer** | Limit the Account to a single Hardware Manufacturer |
| **IP Address Pattern** | Limit the Account to Nodes within a specific Subnet or Network |
| **Node Category** | Limit nodes by category (Network device, Server, Other) |
| **Group of Volumes** | Limit the Account to a selected Group of Volumes |
| **Single Group** | Limit the Account to a Single Group |
| **Group of Groups** | Limit the Account to a group of selected Groups |
| **Group Name Pattern** | Limit the Account to a group of Groups with similar Group Names |
| **Single Report** | Limit the Account to a single Report |

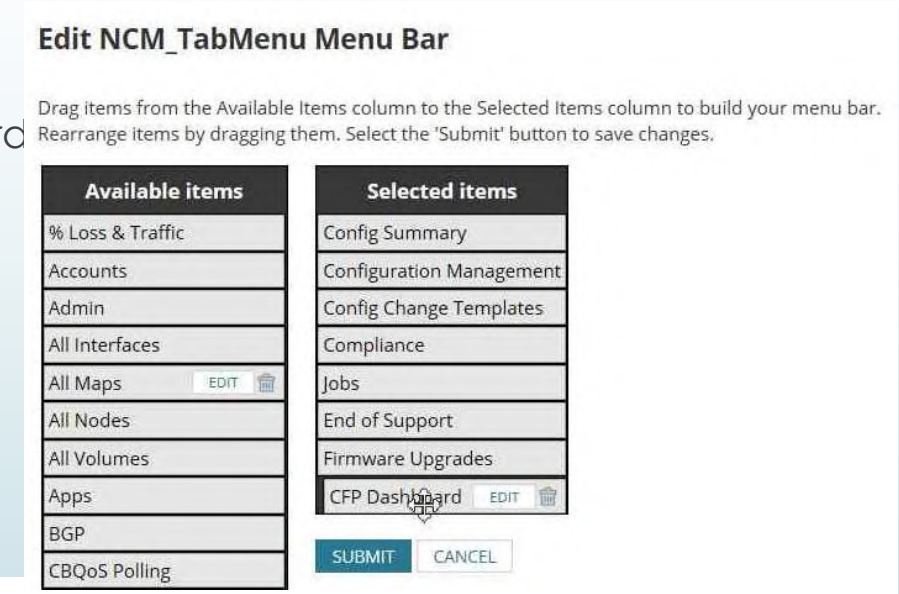
VIEW LIMITATION

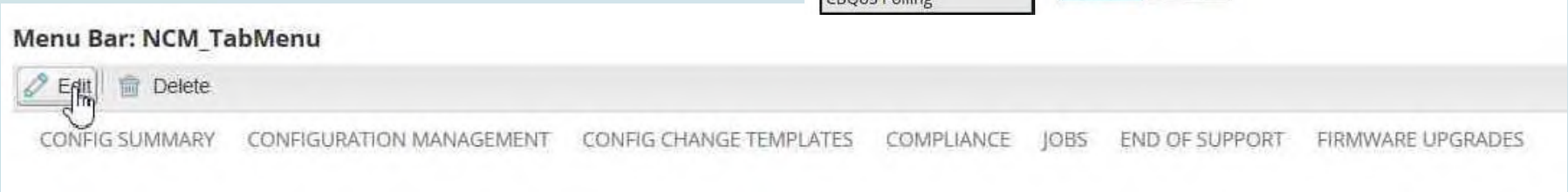
You can create a view limitation that will limit the network devices that can be displayed on this view. Account limitations for the logged-in account will also be applied to this view when it is displayed.

No View Limitation defined. EDIT

# Views

- Adding views to Orion Dashboard to create individual or group Dashboards



- Creating a Dashboard
  - Widgets
  - Views
  - Menu Bars
  - Expansion
  - Viewing Custom Properties
  - Editing Views & Menu Bars

***Break***

# DEMO & LAB 05

- 1 hour

# Lunch

# User Accounts



- Accounts
  - Five Types
    - Orion Individual Accounts
    - Windows® Individual User Accounts
    - Windows® Group User Accounts
    - SAML Individual user accounts
    - SAML Group user account
- User Account Permissions
  - Default Settings
    - Web Console Logon
    - See Information in views, resources, and reports
    - Extra permissions and restrictions can be configured
  - View Assignments
    - Specific Homepage for users
    - Views and allow or deny usage
  - Application specific settings

# User Accounts



- SAML User Account Integration
  - Provides for logons to the Orion Web Console using third-party single sign-on solutions
  - Supports Okta© and ADFS©
  - Allows for multi-factor authentication
  - Other user account types (Orion Platform user, AD user/groups still supported
  - Supported by both the primary and additional web servers
  - Set up in User Accounts – SAML Configuration

# User Accounts

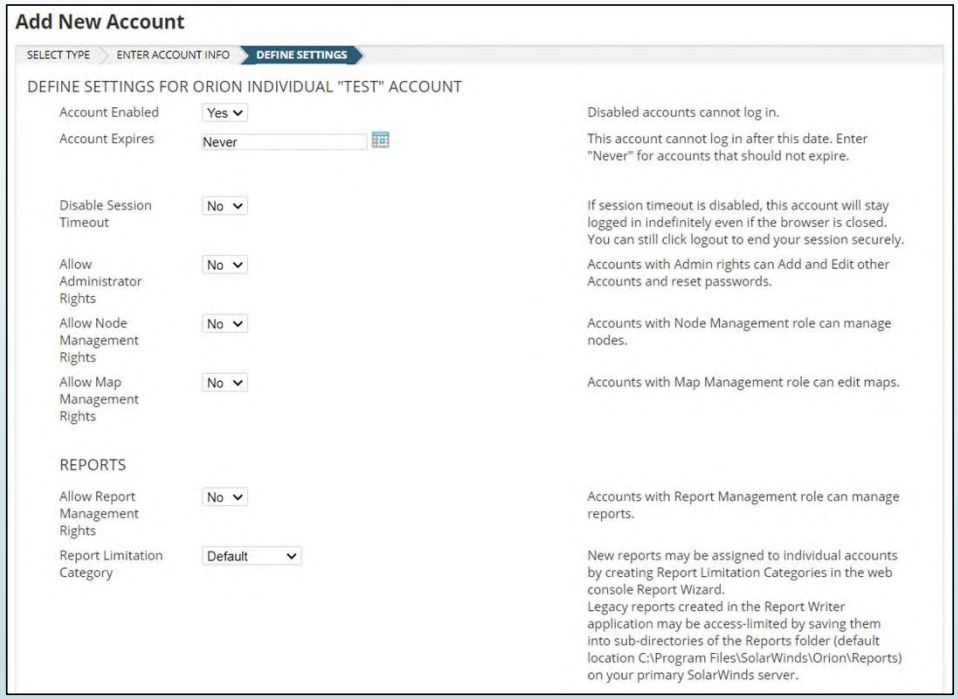


- Non-Web-Based applications unsupported
  - Cannot use SAML Accounts for the following:
    - Network Atlas
    - Orion SDK
    - Desktop notifications
    - WPM Recorders
    - Agent registrations

# User Accounts

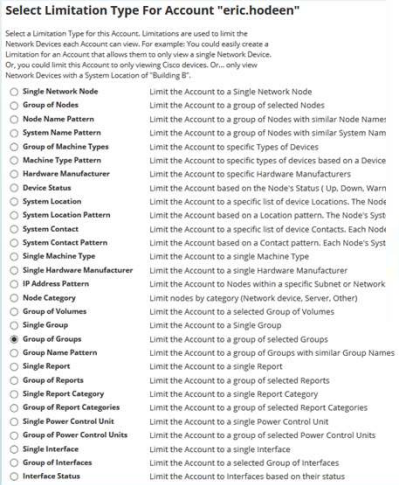


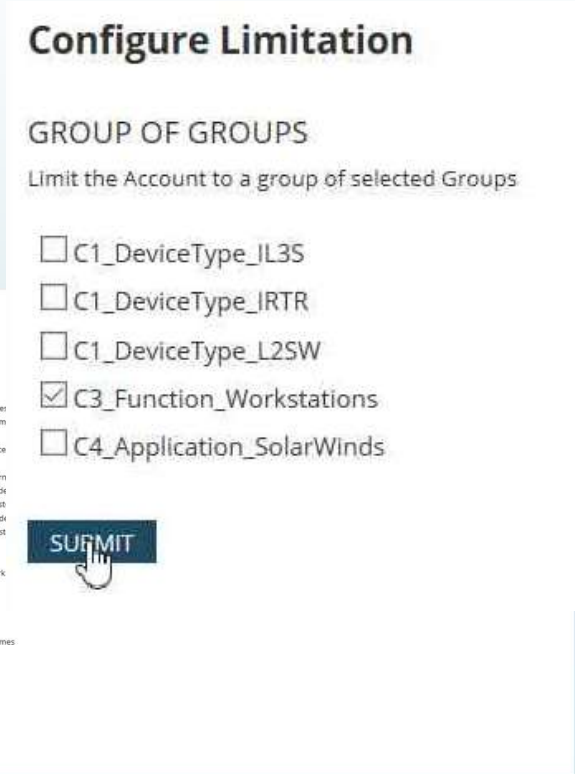
- User Account Permissions
  - Default Settings
    - Web Console Logon
    - See Information in views, resources, and reports
    - Extra permissions and restrictions can be configured
  - View Assignments
    - Specific Homepage for users
    - Views and allow or deny usage
  - Application specific settings



# Account Limitations

- Limit what users can view in the web console
- Limitations can be configured to limit views:
  - To specific network nodes
  - By department or function
  - By device type or role
  - By geographical location



- Account Management
  - Build an Orion Account
  - Create User Account
    - No SSH
    - No Admin
    - NCM Download only

# Break

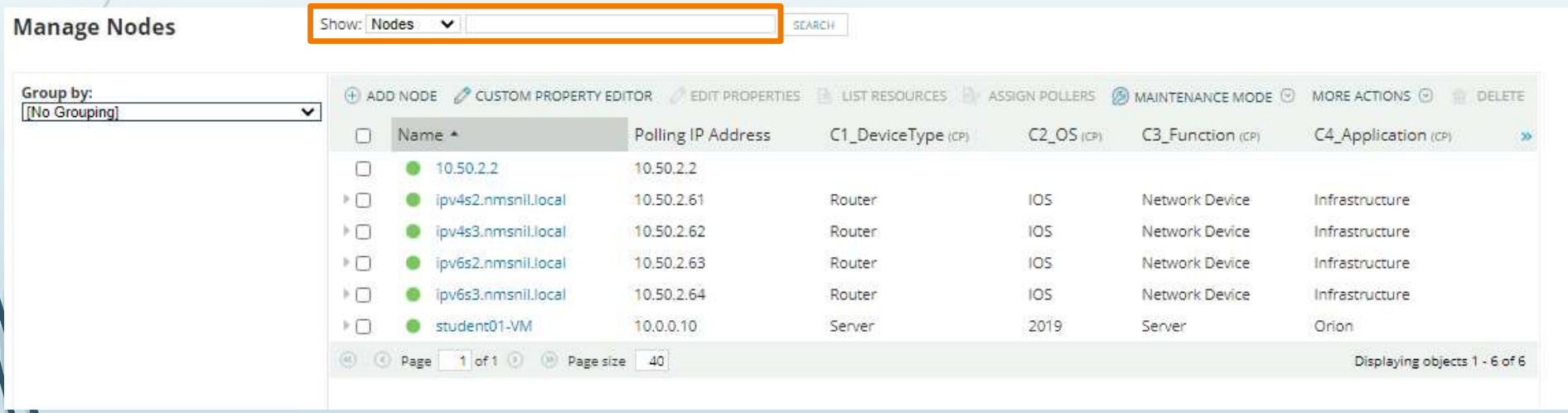
# DEMO & LAB 06

# Manage Nodes

- Location to locate nodes under management
  - Searchable criteria
  - Group by Option
  - Node Properties
  - Maintenance Options
  - Interface and Element Elections
  - Screen Modification

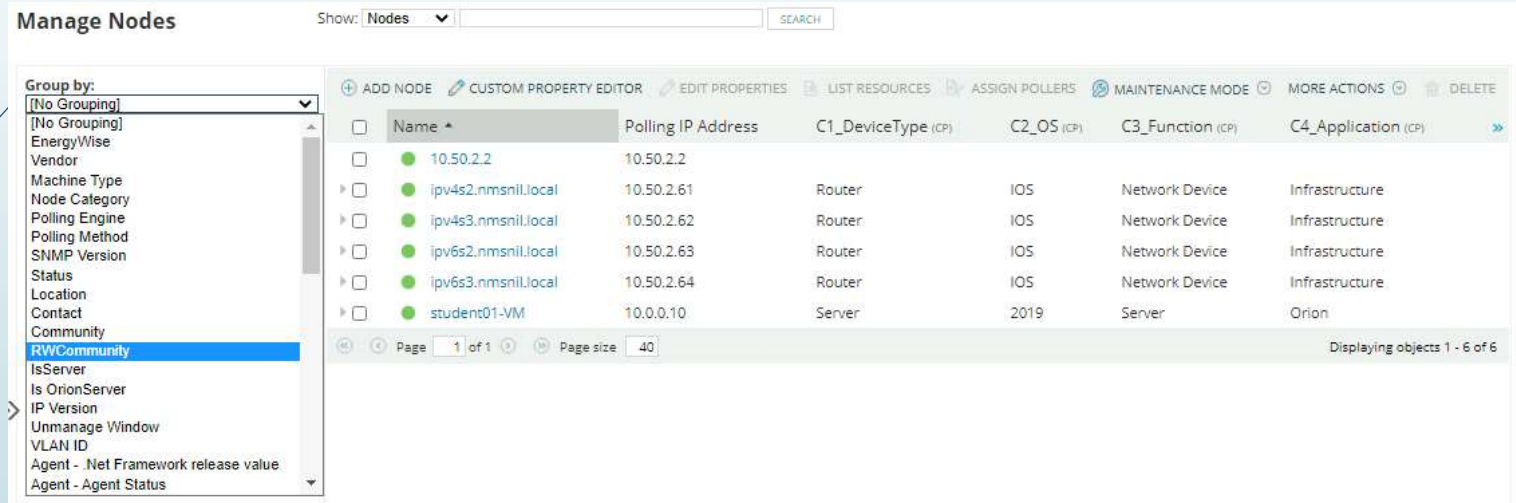
# Manage Nodes – Searchable Criteria

- Search by just a few characters, octet of an IP address, parts of a name, or even a Custom Property



# Manage Nodes – Group By

- Drop down menu will provide a list of native options to group nodes by
- Custom Properties are located at the bottom in Alphabetical Order

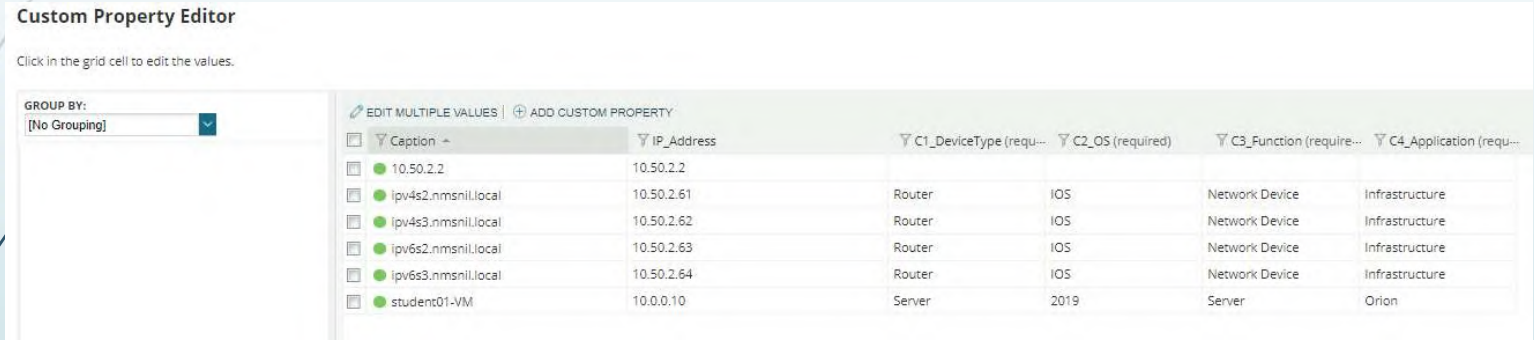


# Manage Nodes – Adding a Node

- Adding a single node or launching a Network Discovery Wizard

# Manage Nodes – Custom Property Editor

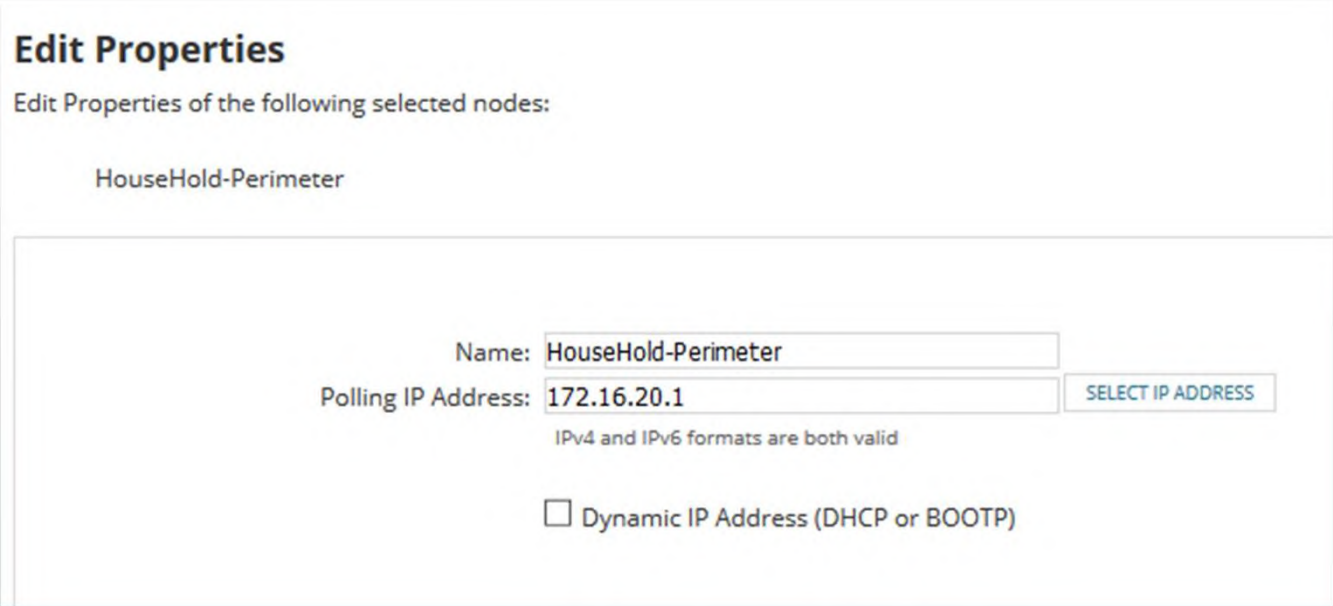
- Edit single / multiple values for Custom Properties




| Caption | IP_Address | C1_DeviceType (requ... | C2_OS (required) | C3_Function (require... | C4_Application (requ... |
|---|---|---|---|---|---|
| 10.50.2.2 | 10.50.2.2 | | | | |
| ipv4s2.nmsnil.local | 10.50.2.61 | Router | IOS | Network Device | Infrastructure |
| ipv4s3.nmsnil.local | 10.50.2.62 | Router | IOS | Network Device | Infrastructure |
| ipv6s2.nmsnil.local | 10.50.2.63 | Router | IOS | Network Device | Infrastructure |
| ipv6s3.nmsnil.local | 10.50.2.64 | Router | IOS | Network Device | Infrastructure |
| student01-VM | 10.0.0.10 | Server | 2019 | Server | Orion |

# Manage Nodes – Edit Properties

- Node identification



# Manage Nodes – Edit Properties

- Polling Method Election

Polling Method:

Help me choose a polling method

**External Node:** No Status
No data is collected for this node. Useful for monitoring a hosted application or other element on the node but not the node itself.

**Status Only:** ICMP
Limited data (status, response time, and packet loss) is collected using ICMP (ping). Useful for devices which do not support SNMP or WMI.

**Most Devices:** SNMP and ICMP
Standard polling method for network devices such as switches and routers, as well as Unix/Linux servers.

SNMP Version: SNMPv2c
SNMPv2c is used, by default, when SNMPv3 is neither required nor supported.
SNMP Port: 161
Allow 64 bit counters

Community String: beer4me Press down arrow to view all
Read/Write Community String:

TEST

**Windows Servers:** WMI and ICMP
Recommended agentless polling method for Windows servers.

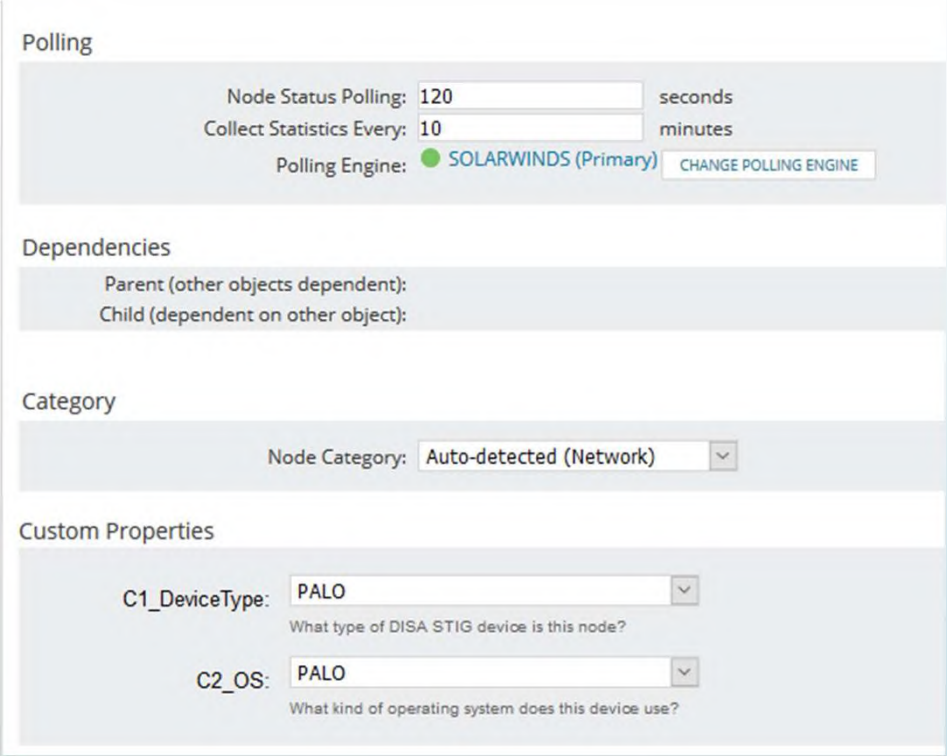
**Windows & Unix/Linux Servers:** Agent
Optional agent useful for monitoring Windows & Unix/Linux hosts in remote or distributed environments, such as the cloud. Credentials are needed only for installing the agent. The agent does not need to be installed on the server already. »What is an agent?

**VMware vCenter or Hyper-V devices:**
Use to monitor VMware vCenters or standalone ESX or Hyper-V hosts.

**Meraki Wireless:** API
API based polling for Meraki wireless gear.

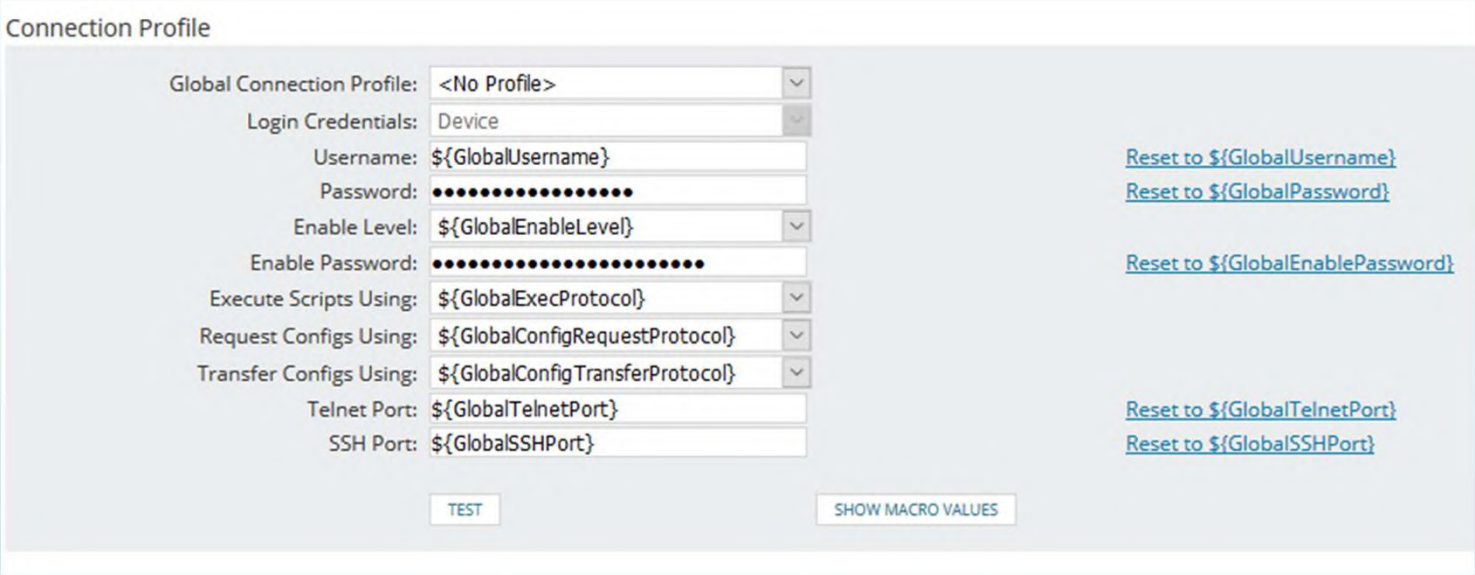
# Manage Nodes – Edit Properties

- Polling Intervals
  - Critical Nodes
  - Normal Nodes
  - Test and Eval Nodes
  - Workstations
- Dependencies
  - CDP or LLDP
  - Not built for nodes using ICMP
- Custom Properties



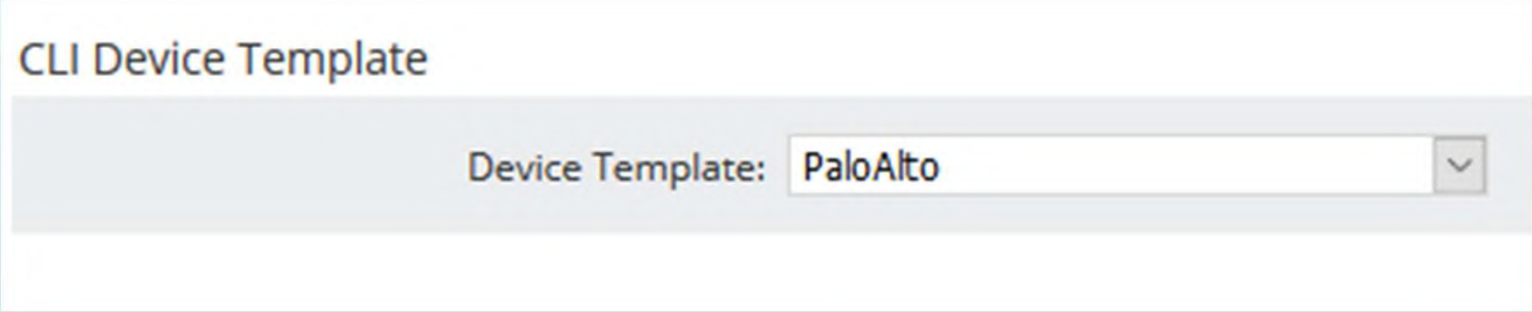
# Manage Nodes – Edit Properties

- NCM Specific Setting
  - Identification of Account to Access Routers, Switches, and other network gear



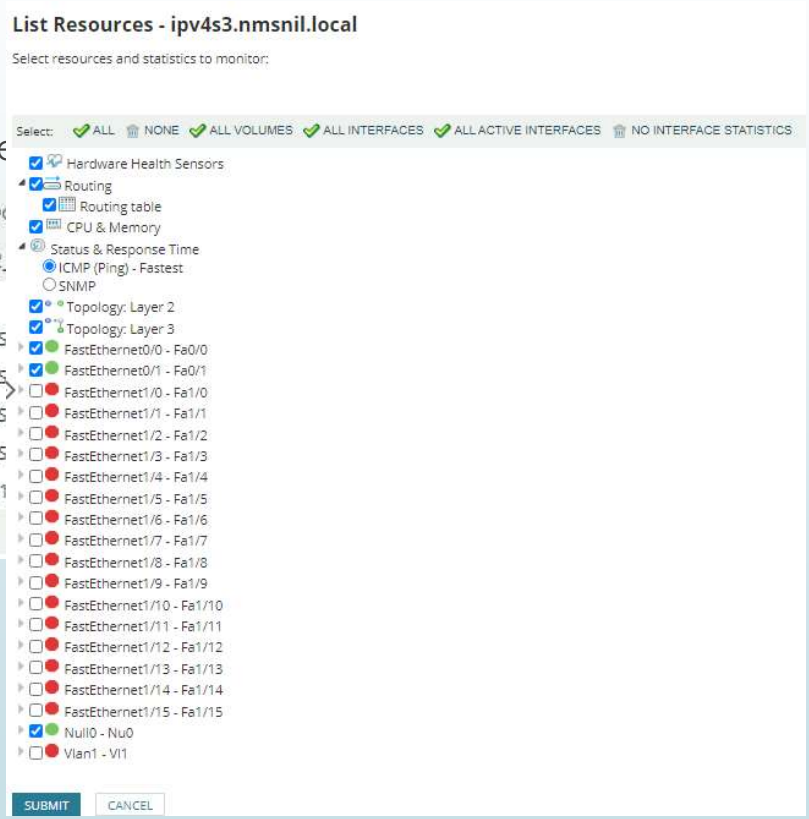
# Manage Nodes – Edit Properties

- Device Template Settings
  - NCM Specific Setting
  - Auto-Determine is Default
  - Use an organization defined custom property
    - Covered in the NCM Section of this Course



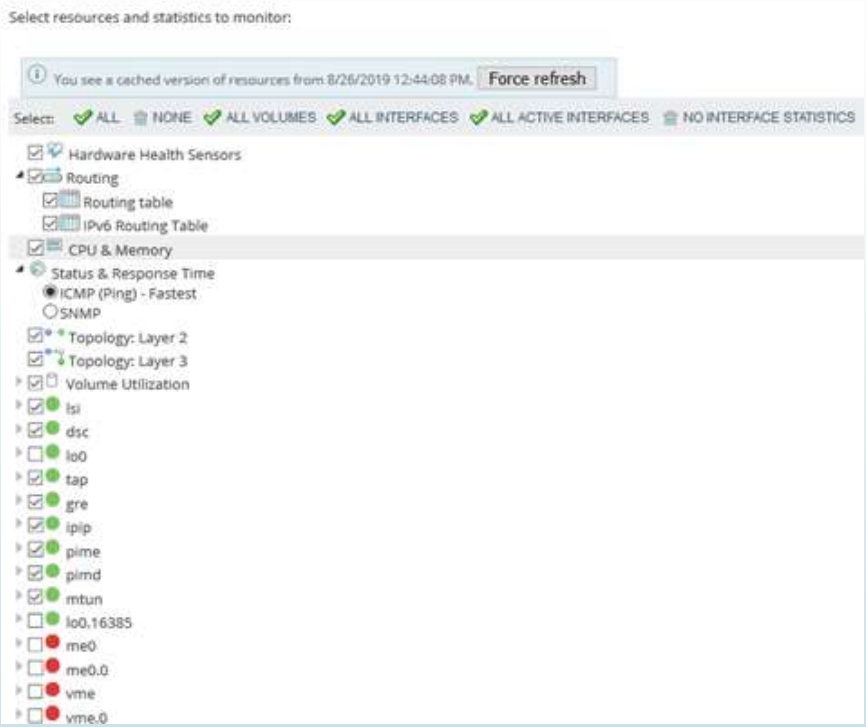
# Manage Nodes – List Resources

- List Resources
  - Provides the ability to add volumes, ele



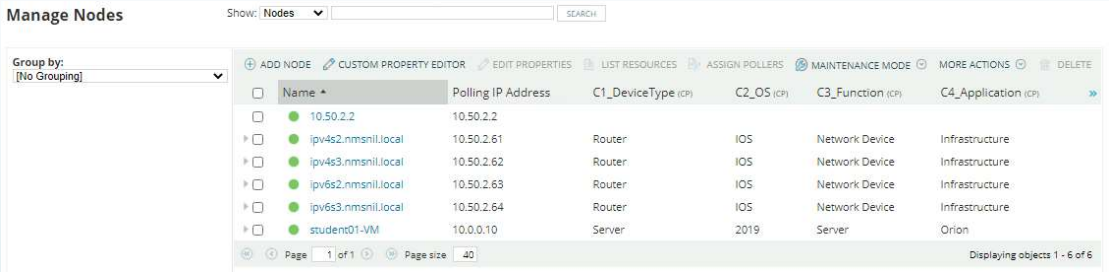
# Manage Nodes – List Resources

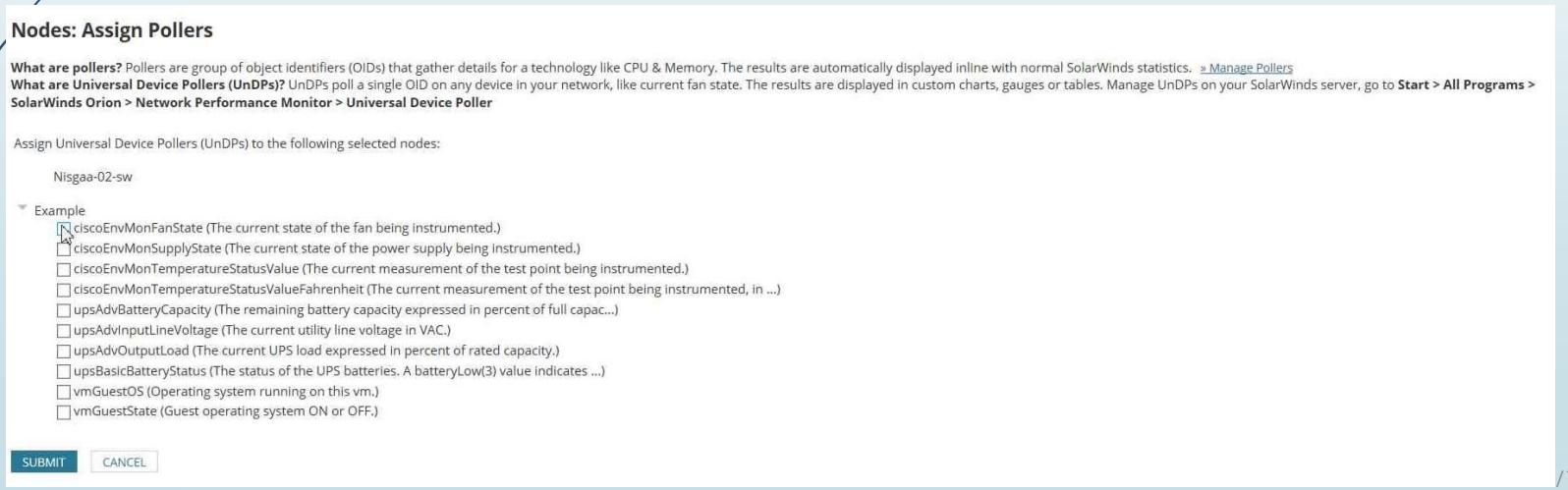
- Hardware Health
- Volumes
- CPU and Memory
- Status Response
- Topologies
- All Types of Interfaces
  - Start with only Infrastructure Ports then add others as licensing allows
- Management Considerations
  - Refresh every Tech Refresh
  - More Elections the more Element usage against license



# Manage Nodes – Assign Pollers

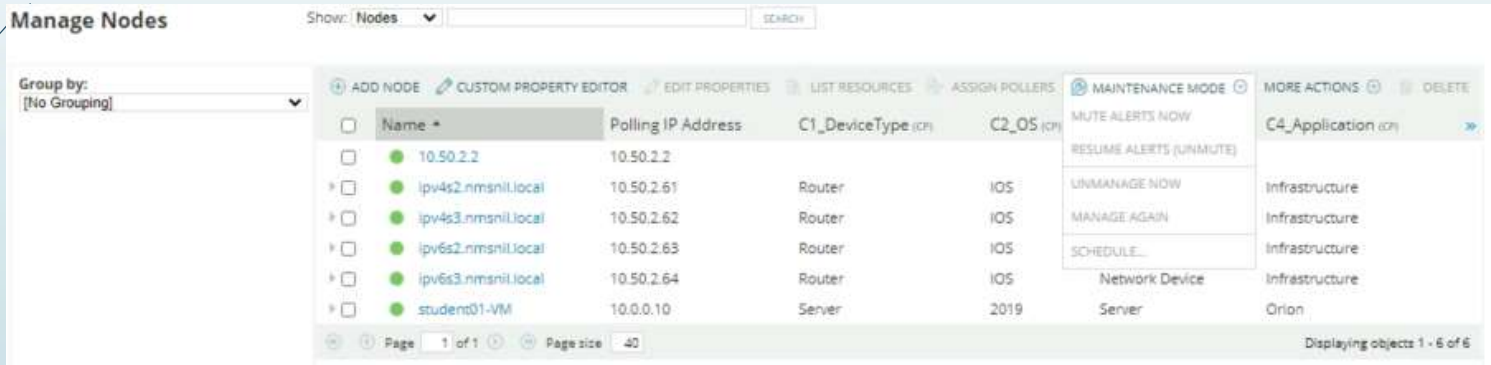
- Custom Pollers are specific MIB requests of a node, which may not be in the SolarWinds Database
  - New Vendor Device
  - New OS from Vendor



# Manage Nodes – Maintenance Options

- Ability to apply maintenance options to nodes during Authorized Service Interruptions

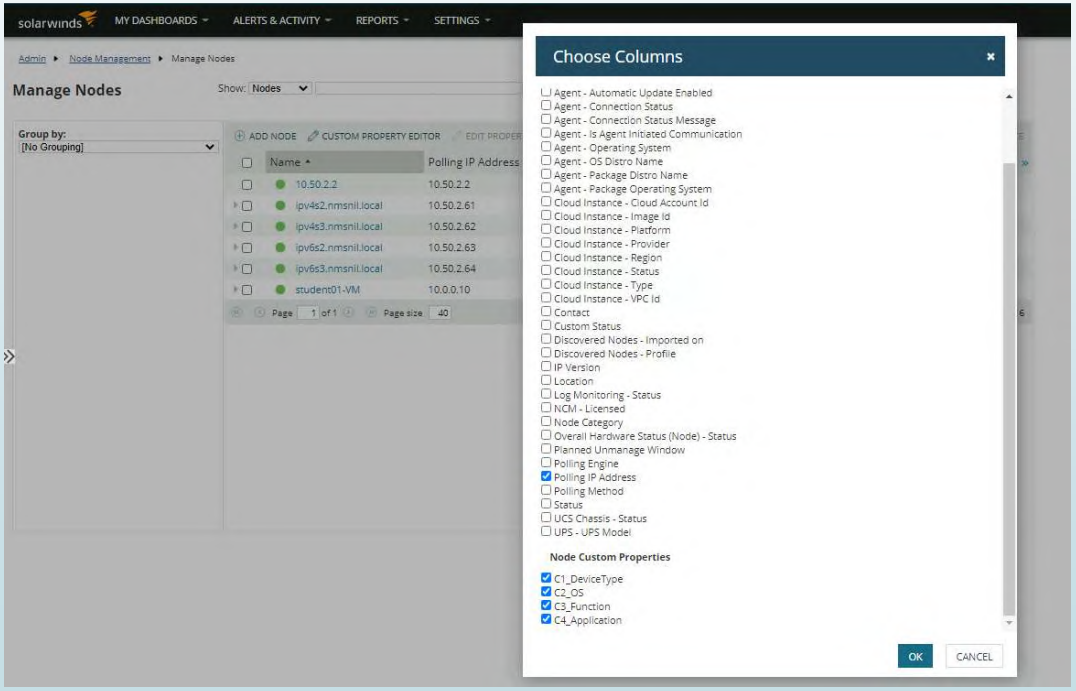


# Manage Nodes – More Actions

- Immediate Node Actions
  - Polling
  - Rediscovery
- Interface Actions
  - Shutdown
  - Enable
- Custom Property Actions
- NCM Node Assignments
- Log Monitoring Actions

# Manage Nodes – Screen Modification

- Blue Arrows allow user to election to view various system and custom properties of their nodes



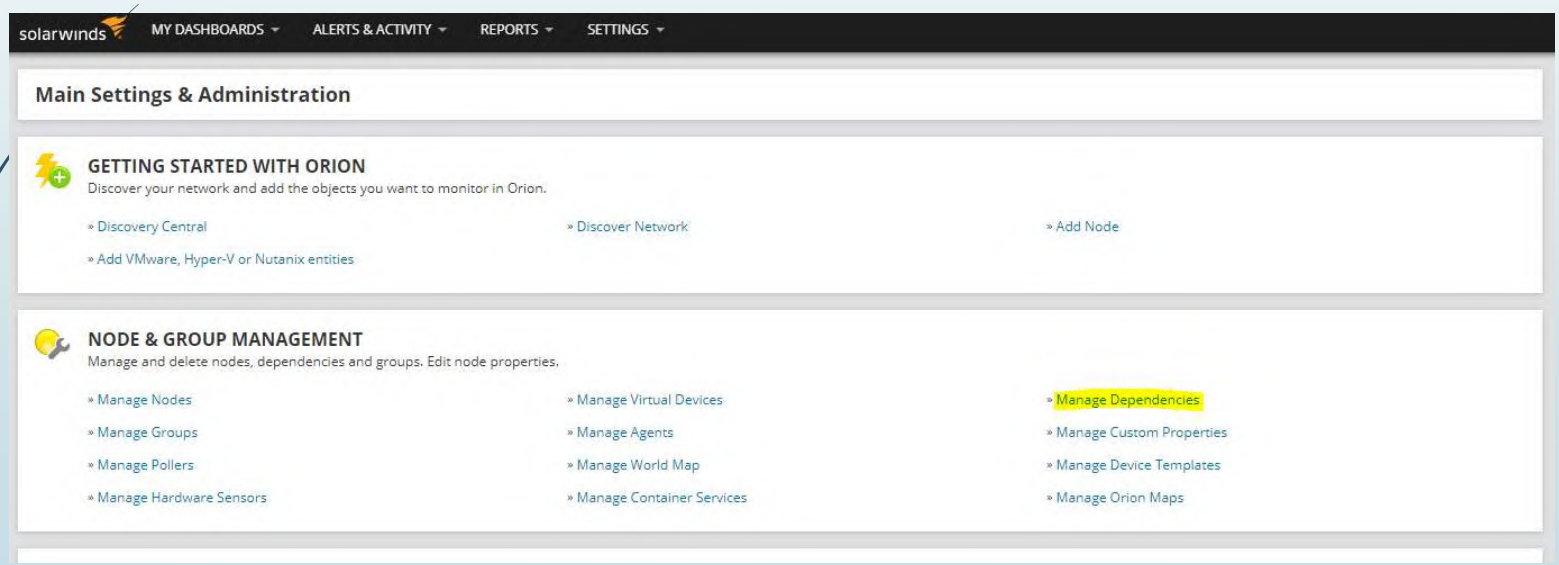
- Manage Nodes
  - Search for Nodes
  - Group By
  - Edit Properties
  - Maintenance Options
  - Interface Elections
  - Screen Modification

# DEMO & LAB 07

# *Break*

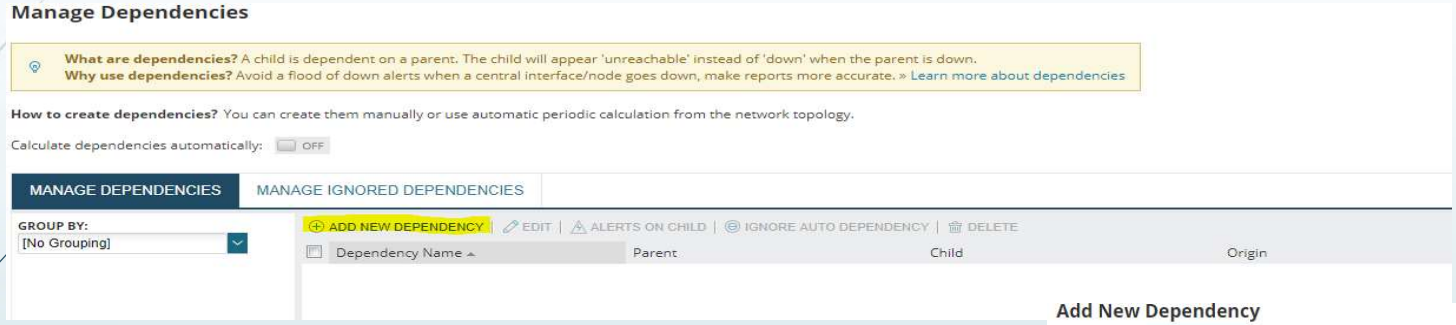
# Manage Dependencies

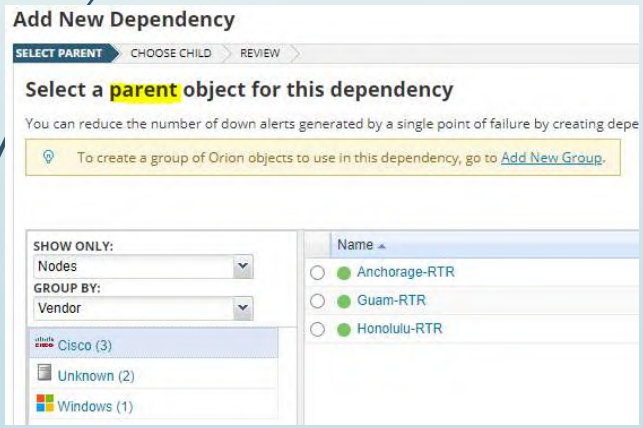
- What are dependencies? A child is a dependent on a parent. The child will appear unreachable instead of down when the parent is down
- Why use dependencies? Avoid a flood of down alerts when a central interface/node goes down, make reports more accurate, and save troubleshooting man hours
- Select Setting/All Settings/Manage Dependencies (highlighted)



# Manage Dependencies

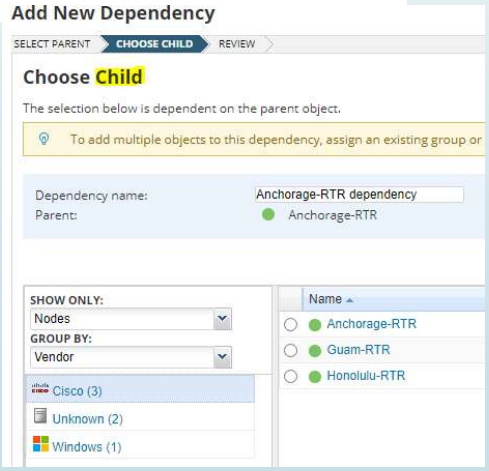
- Select + Add new dependencies



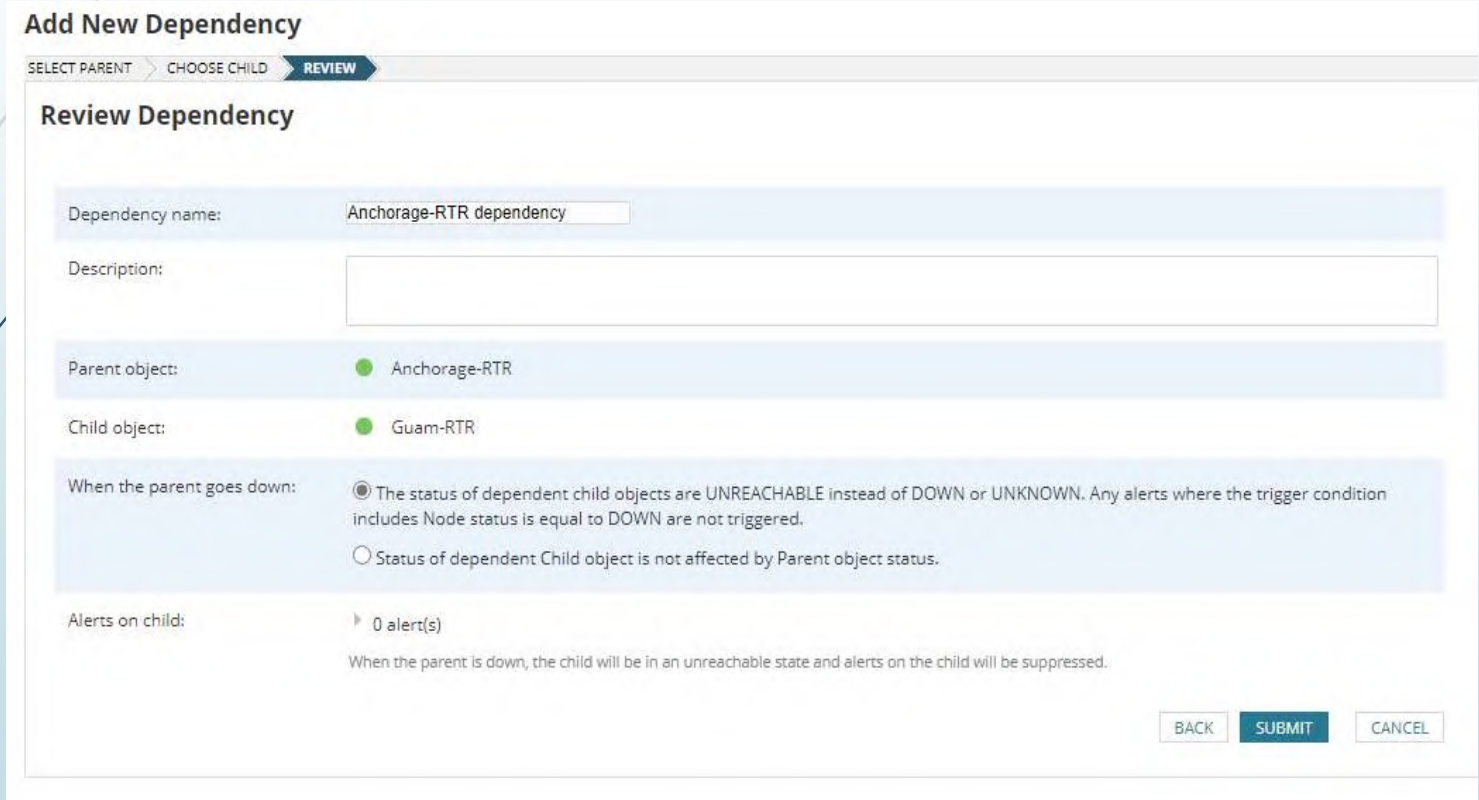

- Select Parent
- Click Next

- Select Child
- Click Next



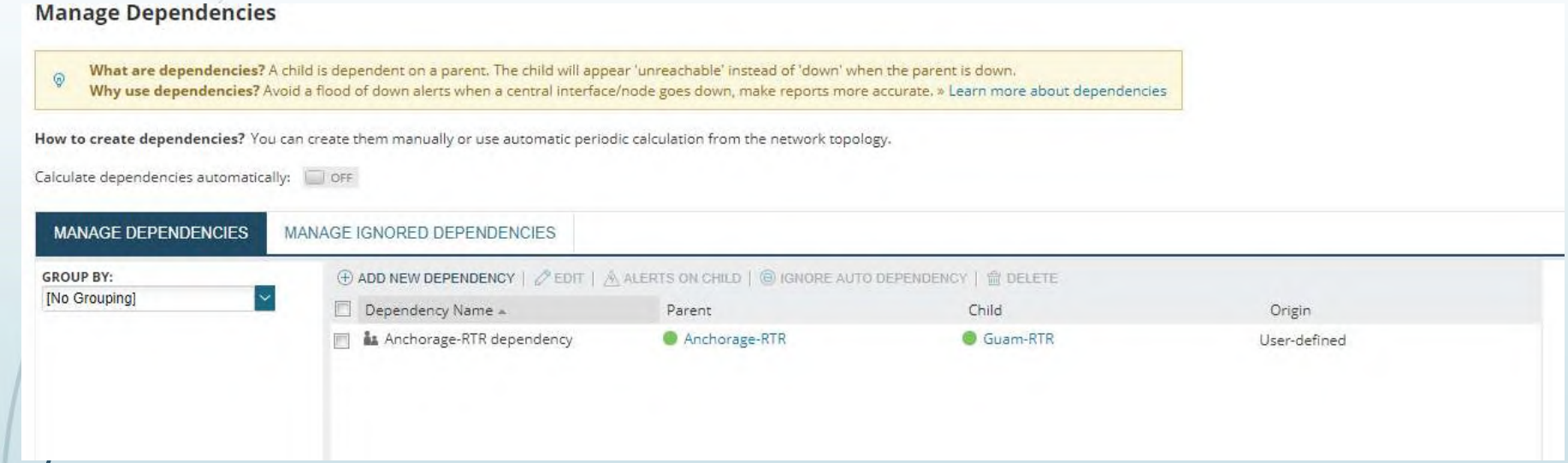
# Manage Dependencies

- Review and Submit



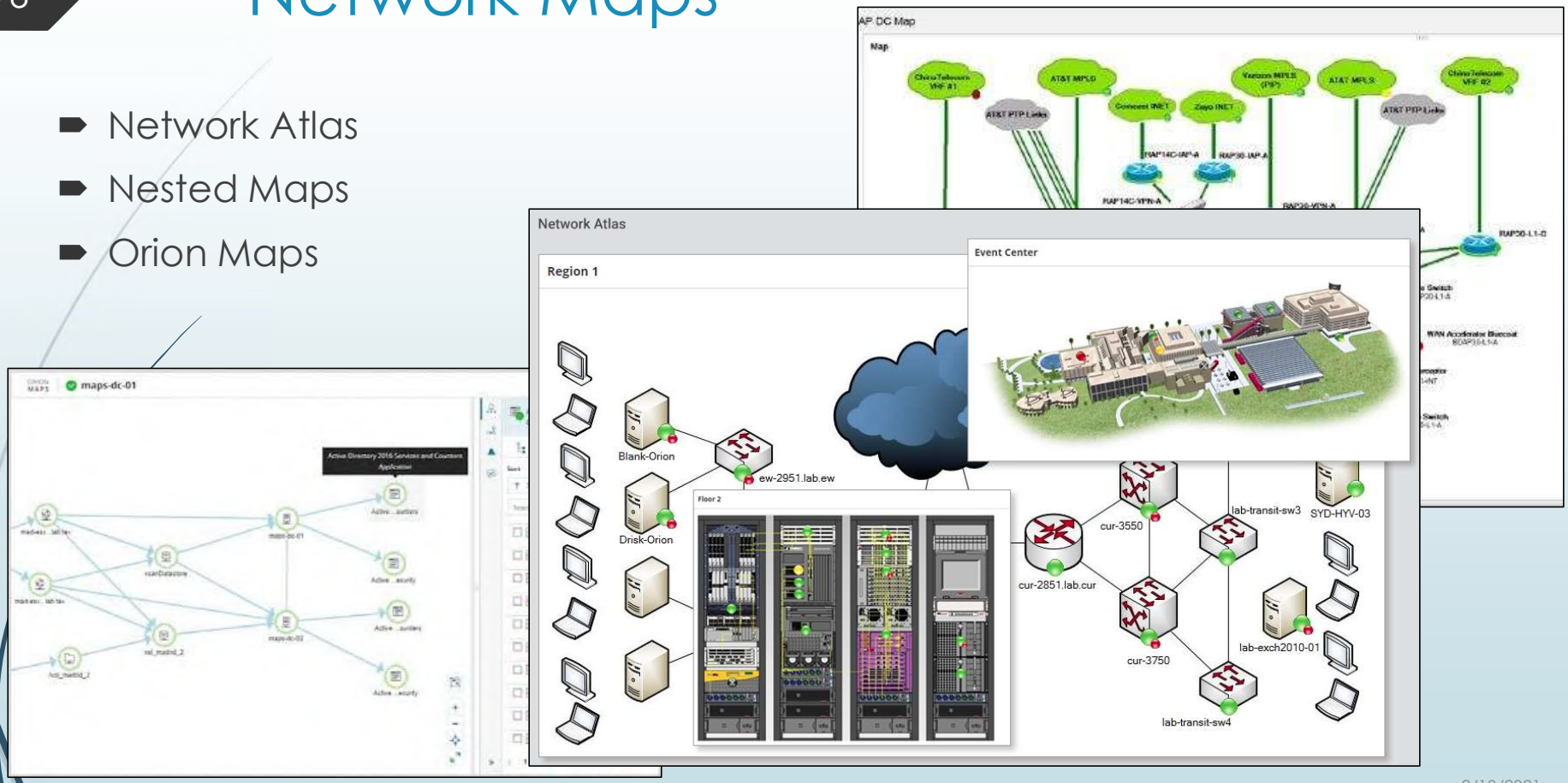
# Manage Dependencies

- Any questions?



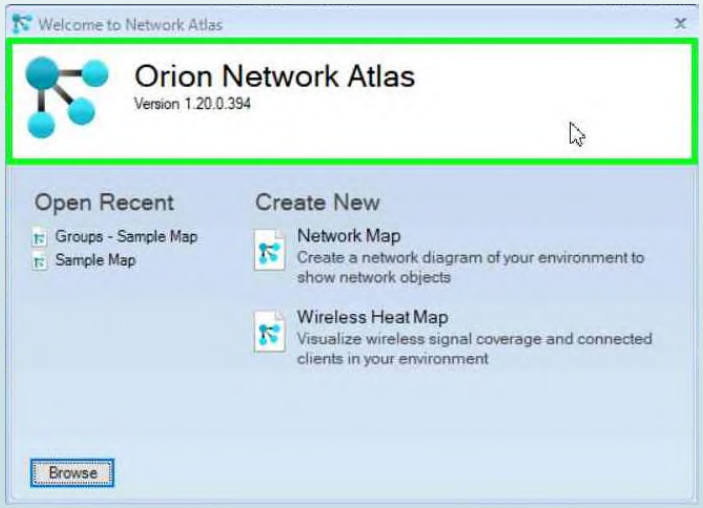
# Network Maps

- Network Atlas
- Nested Maps
- Orion Maps



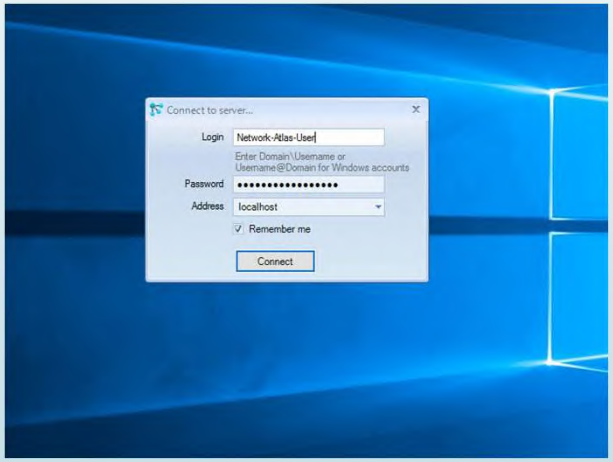
# Network Maps

- What is Network Atlas?
  - Application for creating customized diagrams of your environment or infrastructure
  - Used to create maps embedded in web console views



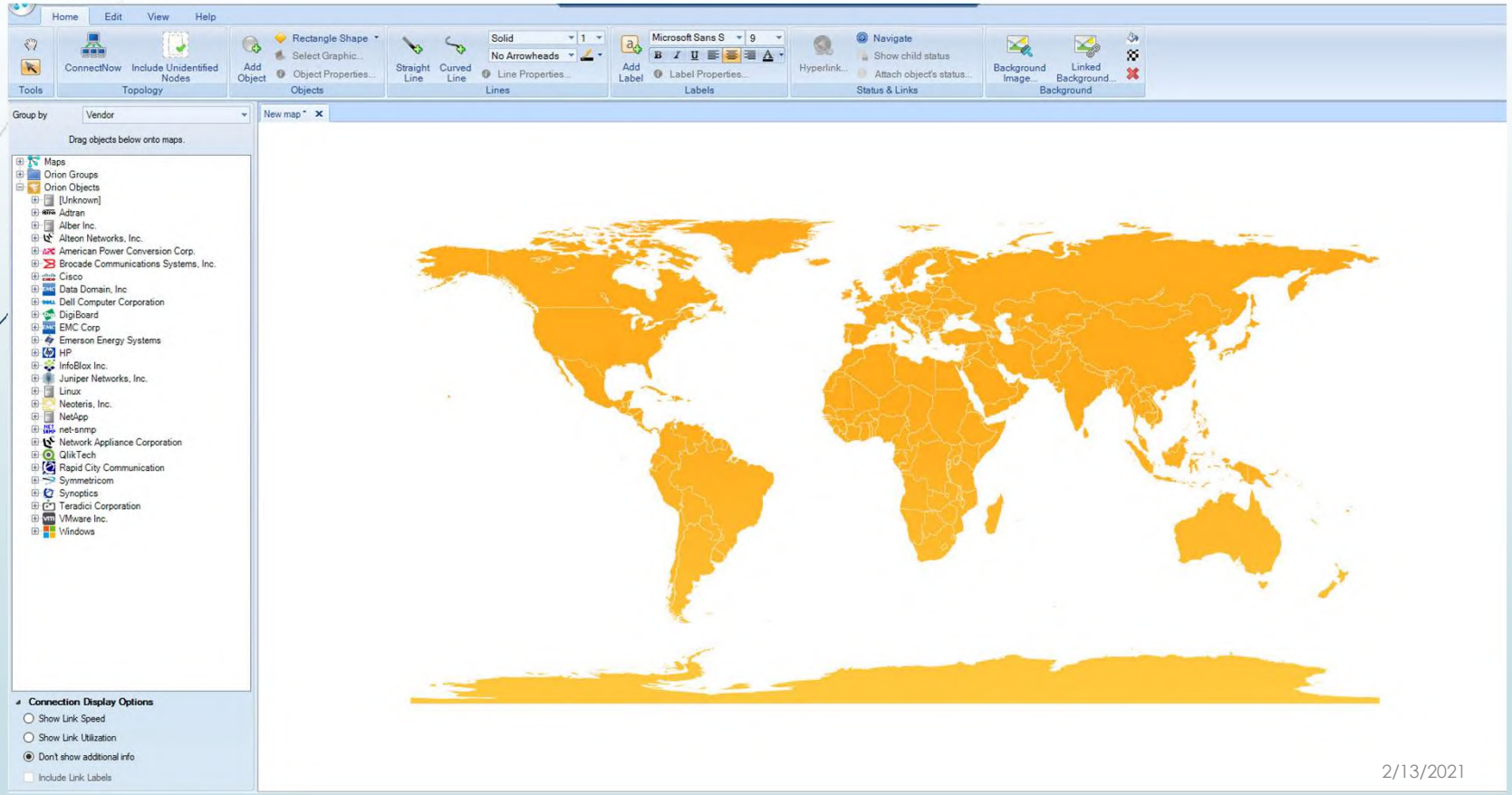
# Network Maps

- Network Atlas
  - Accessed through the SolarWinds Orion Program Group
    - Access Solarwinds Core Orion Server
    - Start – Solarwinds – Network Atlas
    - Run as Administrator (recommended)



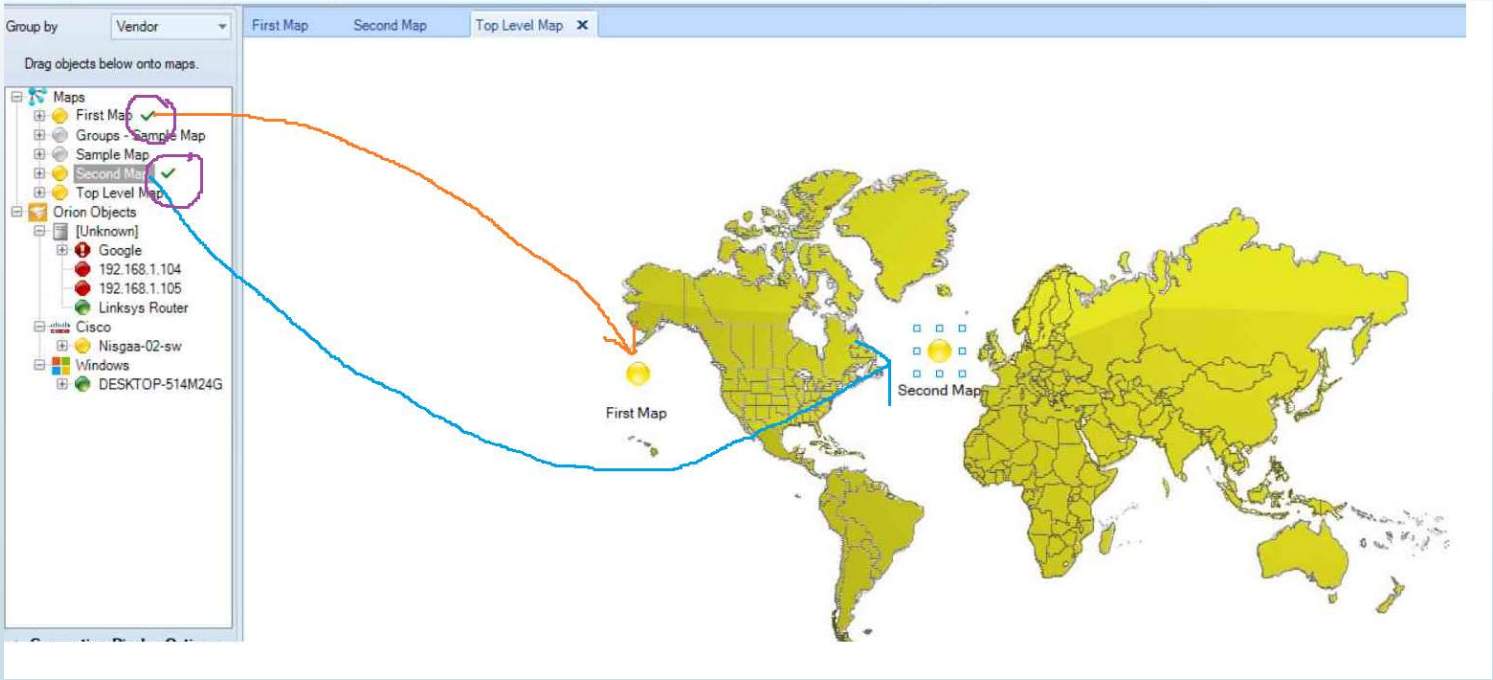

- Features
  - Connect Now
  - Icon Settings
  - Three Different Groups
    - Maps
    - Orion Groups
    - Orion Objects

# Network Atlas



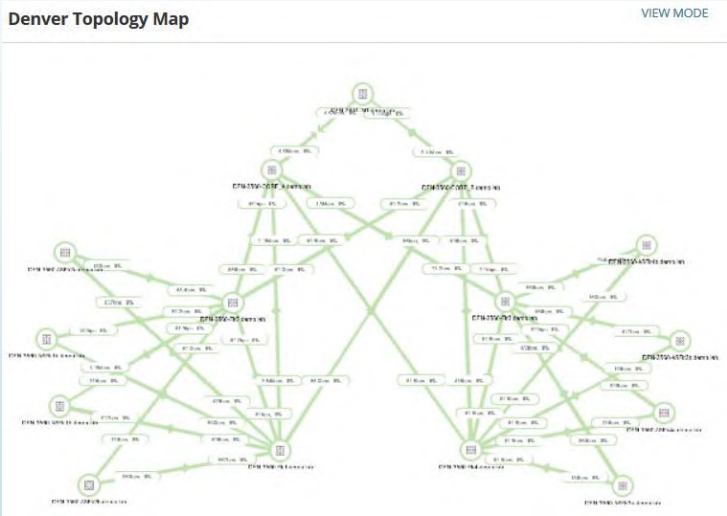
# Network Maps

- Nested Maps
  - Ability to place a previously development map inside a parent or master map.



# Network Maps

- Orion Maps
  - New mapping feature for SolarWinds
  - Replacing Network Atlas
  - Must manage in List Resources
    - Layer 2 Topology
    - Layer 3 Topology
  - Supports Nested maps
  - Dynamically linking networking devices
  - Providing greater insight to the connection between two devices



- Network Atlas
  - Create a Map
    - Used Nodes
    - Groups
    - Interfaces
- Create a Nested Map
- Create an Orion Map

***Break***

# DEMO & LAB 08

# NPM Identify Purpose

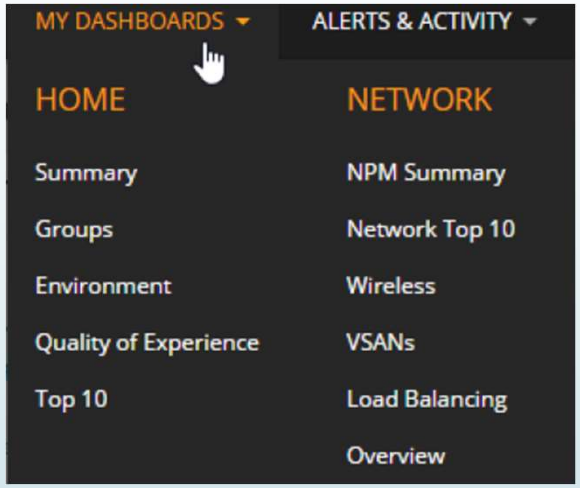
Before you begin monitoring your network, Identify the devices to monitor in your environment and the purpose of monitoring:

- Is monitoring the specific node important
- Who needs to know if the monitored node goes down
- Is the node Mission Critical or part of Core Services
- Are you adding the node for inventory purposes
- What kind of nodes can SolarWinds monitor
- Is there active monitoring (Network Operations Center)
- If a nodes goes down is there an Escalation Policy

# Navigate SolarWinds NPM

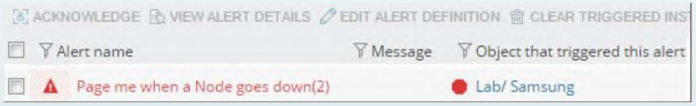
MY DASHBOARDS / NETWORK

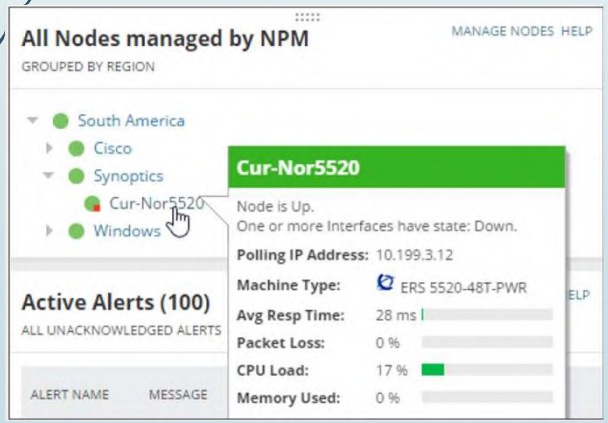
- NPM Summary
- Network Top 10
- Wireless
- VSANs
- Load Balancing
- OverView
- Custom View/Dashboards

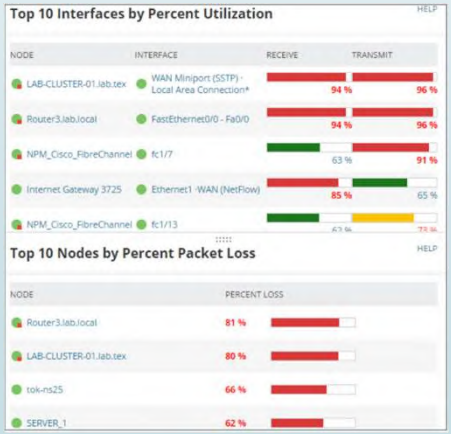


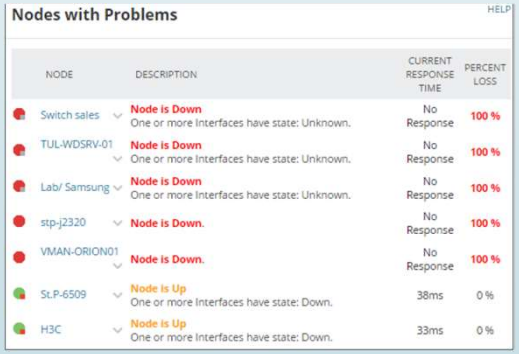
# Troubleshoot a node with NPM

- Node: More Details
- Active Alerts
- Node with Problems
- Top 10



# NPM WIDGET: Nodes with Problems

Node with Problems

Information about the Interface associate with each node

**Nodes with Problems** HELP

| NODE | DESCRIPTION | CURRENT RESPONSE TIME | PERCENT LOSS |
|---|---|---|---|
| Switch sales | **Node is Down** One or more Interfaces have state: Unknown. | No Response | 100 % |
| TUL-WDSRV-01 | **Node is Down** One or more Interfaces have state: Unknown. | No Response | 100 % |
| Lab/ Samsung | **Node is Down** One or more Interfaces have state: Unknown. | No Response | 100 % |
| stp-j2320 | **Node is Down.** | No Response | 100 % |
| VMAN-ORION01 | **Node is Down.** | No Response | 100 % |
| St.P-6509 | **Node is Up** One or more Interfaces have state: Down. | 38ms | 0 % |
| H3C | **Node is Up** One or more Interfaces have state: Down. | 33ms | 0 % |

# Navigate SolarWinds NPM

Top 10 Interfaces by Percentage Utilization

Shows interface transmit/receive Utilization

Green <70%, Yellow 70-90%, Red 90%-100%

**Top 10 Interfaces by Percent Utilization** HELP

| NODE | INTERFACE | RECEIVE | TRANSMIT |
|---|---|---|---|
| LAB-CLUSTER-01.lab.tex | WAN Miniport (SSTP) · Local Area Connection* | 94 % | 96 % |
| Router3.lab.local | FastEthernet0/0 - Fa0/0 | 94 % | 96 % |
| NPM_Cisco_FibreChannel | fc1/7 | 63 % | 91 % |
| Internet Gateway 3725 | Ethernet1 ·WAN (NetFlow) | 85 % | 65 % |
| NPM_Cisco_FibreChannel | fc1/13 | 62 % | 73 % |

# Navigate SolarWinds NPM

Top 10 Errors and Discards

Errors: A packet that was received but could not be processed because there was a problem with the packet

Discards: A packet that was received without errors but was dropped because of interface utilization near 100%

**Top 10 Errors & Discards Today** HELP

| NODE | INTERFACE | RECEIVE ERRORS | RECEIVE DISCARDS | TRANSMIT ERRORS | TRANSMIT DISCARDS |
|---|---|---|---|---|---|
| Perm_Tex-Mds9120-76-76 | fc1/5 | 0 errors | 0 discards | **5,582,170,112 errors** | **5,808,010 discards** |
| Perm_ap6511-E6C8C0 | fe4 | **64,088,776 errors** | **78,073,384 discards** | 0 errors | 0 discards |
| Perm_ap6511-E6C8C0 | fe2 | **100,061,432 errors** | 2,349 discards | 0 errors | 0 discards |
| Perm_Tex-Mds9120-76-76 | fc1/6 | 0 errors | 0 discards | **5,808,179 errors** | **10,024,648 discards** |

# End of Day

- Review
  - Installation, SQL, and Configuration Wizard
  - Discovery Methods
  - Custom Properties
  - Groups
  - Views
  - Accounts
  - Managing Nodes
  - Network Atlas

# Questions and Answers

# Welcome Back!

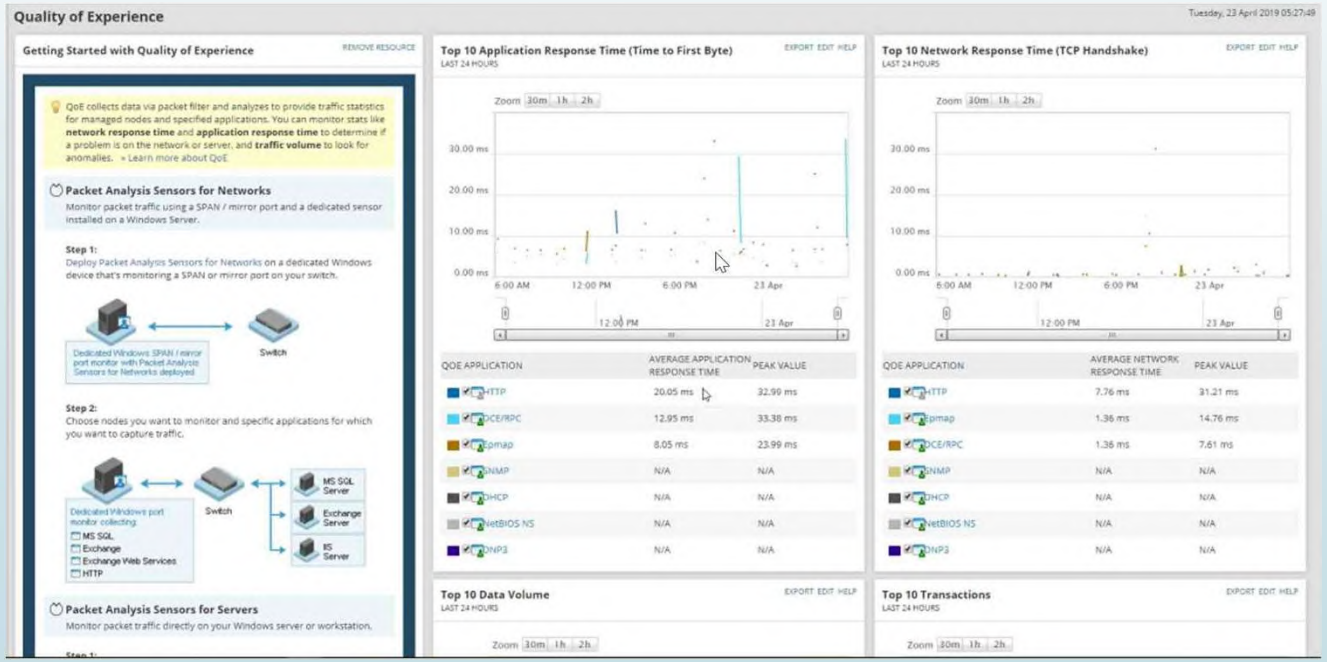
Let's Review

# Today's Agenda

- This sections topics include:
  - Quality of Experience
  - Alerts
  - Reports
  - NetPath Services
  - PerfStack

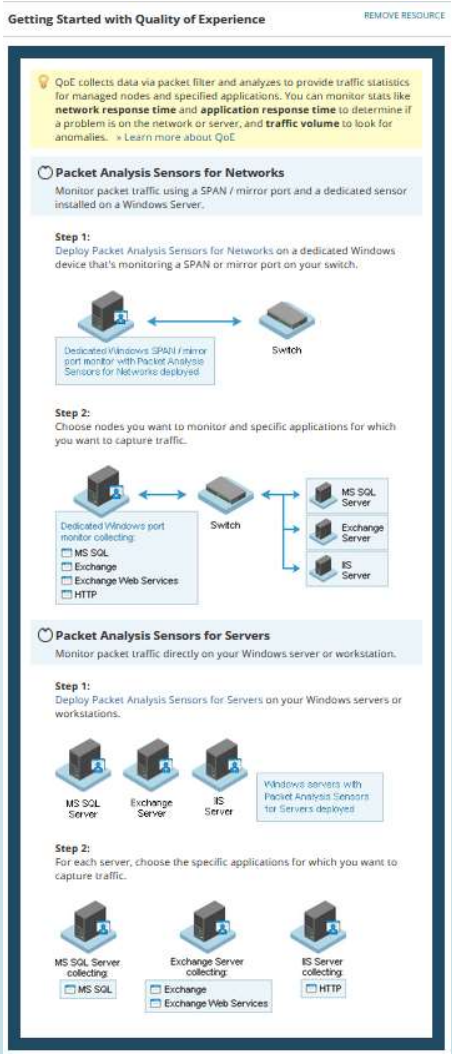
# Quality of Experience

- What is QoE?
- How will QoE help identify issues in my Environment?



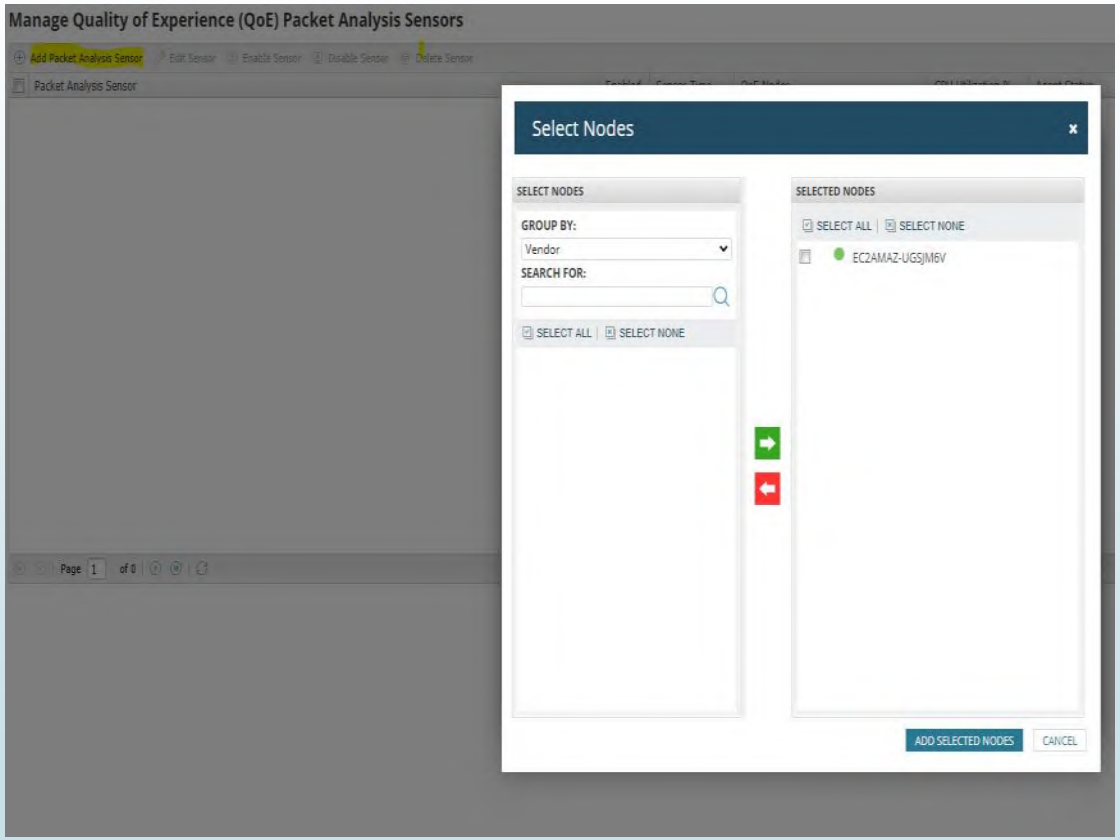
# Quality of Experience

- Sample of the type of information gathered for the Quality of Experience (QoE) in your Enterprise



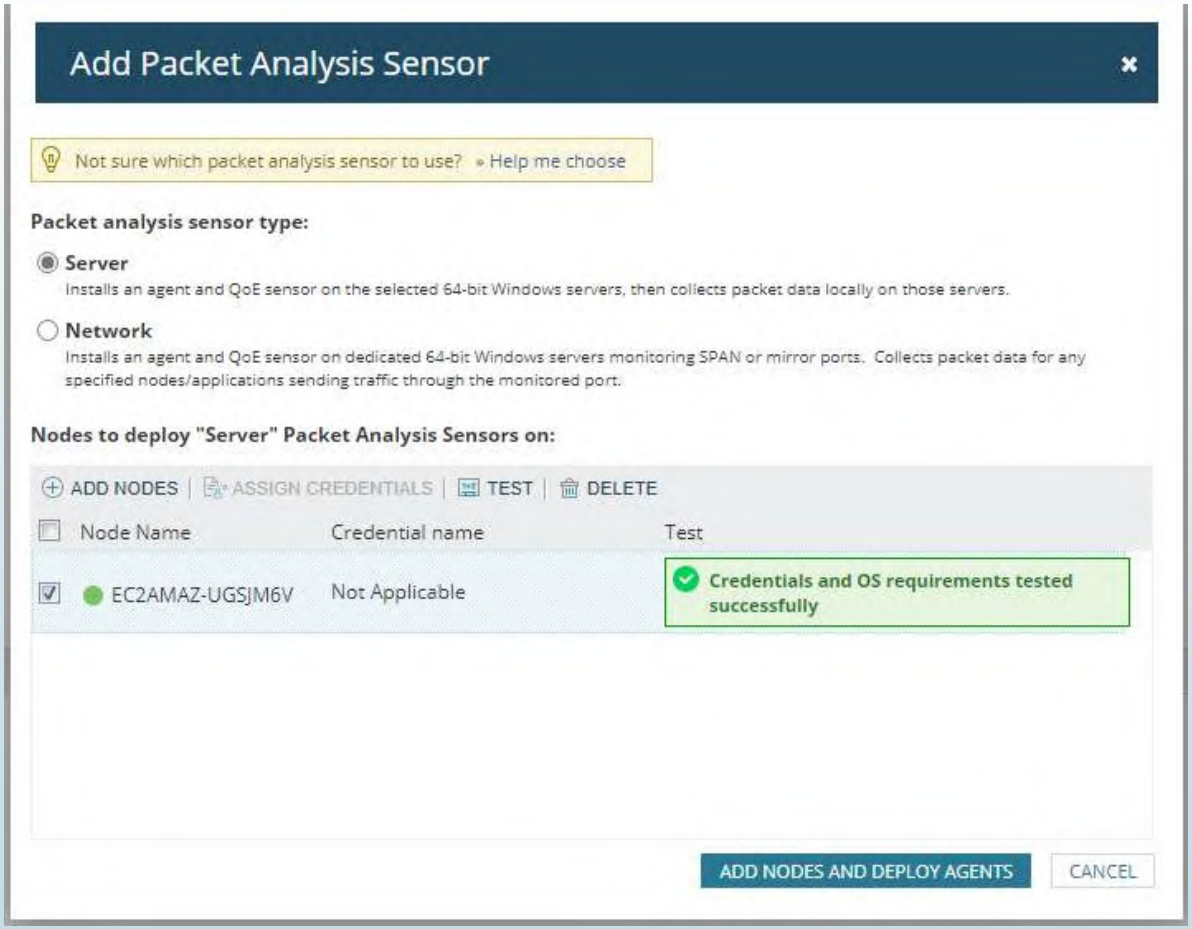
# Quality of Experience

- QoE of Severs/Network Devices
- Select the + Add Packet Analysis Sensor
- Select the server or servers that you would like to deploy a packet analysis sensor to and use the green right arrow to move them into the selected nodes field
- Select the blue Add Selected nodes icon



# Quality of Experience

- QoE for Servers/Network Devices
- Select either Server or Network depending on want device type you would like to deploy packet analysis sensor to
- Once added check the box to the left of the server and test Credentials and OS requirements by selecting test on the menu bar



# Quality of Experience

- Sample of the type of information gathered for the Quality of Experience in your Enterprise

**QoE Nodes Exceeding Thresholds**
LAST 24 HOURS

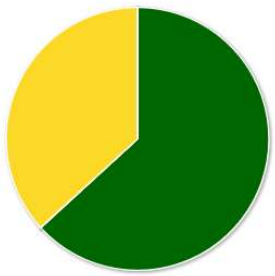
| NODE | QOE APPLICATION | AVG APPLICATION RESPONSE TIME | AVG NETWORK RESPONSE TIME |
|---|---|---|---|
| EASTAGENT01v | Doubleclick | 1.49 s | 12.83 ms |
| EASTAGENT01v | Google | 729.94 ms | 16.95 ms |
| EASTAGENT01v | Google APIs | 2.54 s | 15.19 ms |
| EASTEXMBX01v | HTTP - 10.1.40.61:... | 1.00 s | 2.56 ms |
| EASTEXMBX02v | HTTP - 10.1.40.62:... | 1.03 s | 3.36 ms |
| EASTAGENT01v | HTTP - ajax.aspnet... | 8.09 s | 20.37 ms |
| NEWYAGENT01v | HTTP - blog.kmsig... | 8.72 s | 37.07 ms |
| LOSAAGENT01v | HTTP - blog.kmsig... | 4.36 s | 26.88 ms |
| EASTEXMBX02v | SNPP | 6.99 s | 63.12 ms |
| NEWYAGENT01v | SSL | 877.89 ms | 27.91 ms |

Page 1 of 2 Items on page 10 Show all

Displaying objects 1 - 10 of 17

**Traffic by Risk Level**
LAST 24 HOURS

HELP



| | |
|---|---|
| Evades Detection / Bypasses Firewalls | 0 bytes |
| Data Leaks / Malware | 108.6 MB |
| Possible Misuse | 93.7 GB |
| Minimal Risk | 138.1 MB |
| No Risk | 161.3 GB |
| **Total Data Volume:** | **255.2 GB** |

- 15 Minutes

# Break

# Alerts

- How to use Alerts
  - Does it provide value?

- All Orion Platform products contain Alerts specific to that product

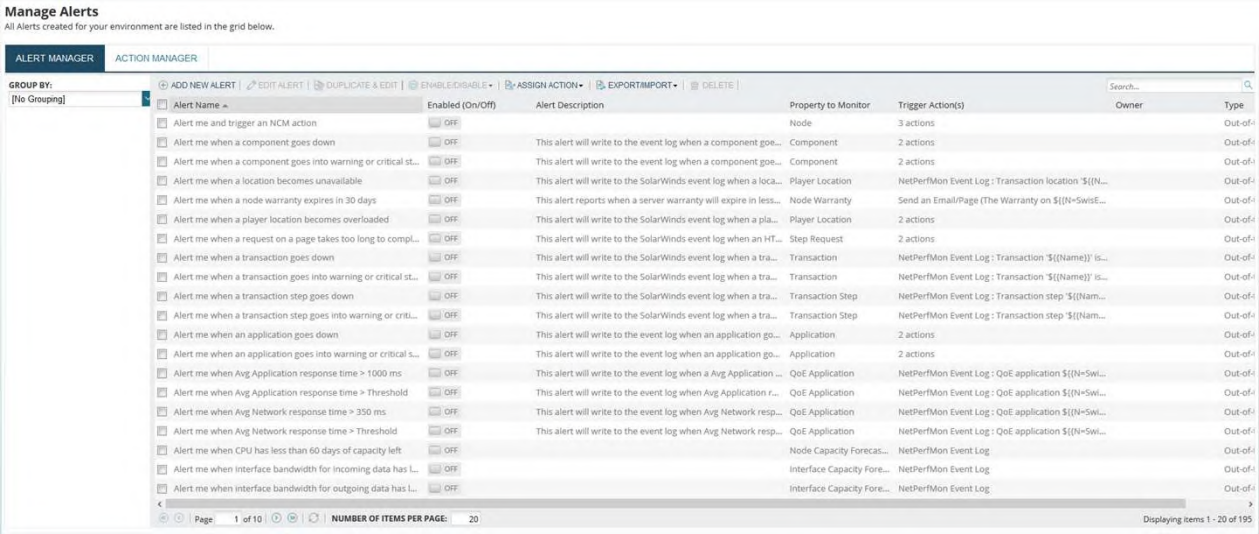
- Create/Edit Alerts
  - Employ Standard Naming Nomenclature

- Polling/Trigger and Performance impacts

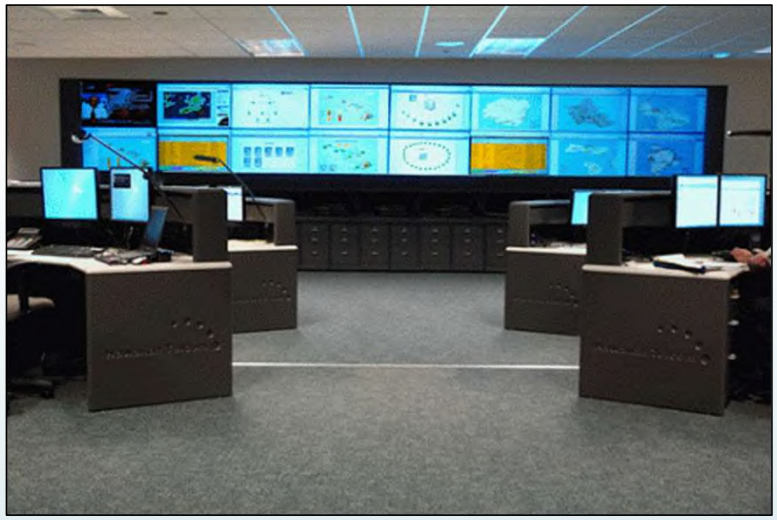
- Test, Test, Test!

# Alerts

- SolarWinds Alerts
  - Out-of-the-Box Alerts
  - Managing Alerts
    - Acknowledge
    - Alert Actions
    - Action Manager
  - Customizing Alerts
  - Message Center



# Alerts

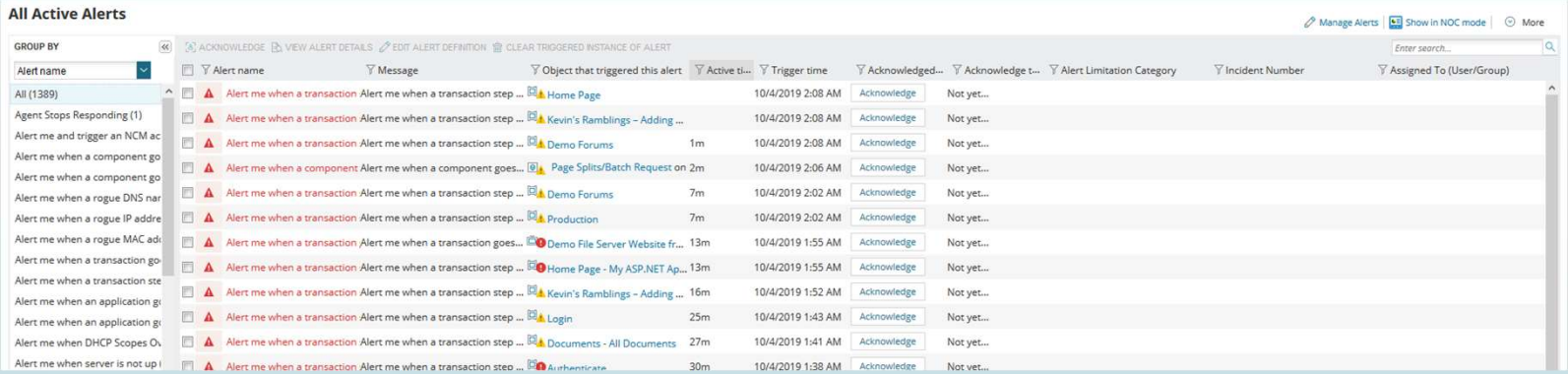


- What are Alerts?
  - Notification of a problem or issue on a monitored element
  - Can be very simple or complex depending on configuration and variables
  - Orion Platform comes with a native set of alerts
  - Other products come with their own set of alerts
  - Some alerts are enabled by default

* Recommendation is to disable all alerts until an architecture, design, and implementation plan can be devised for the organization

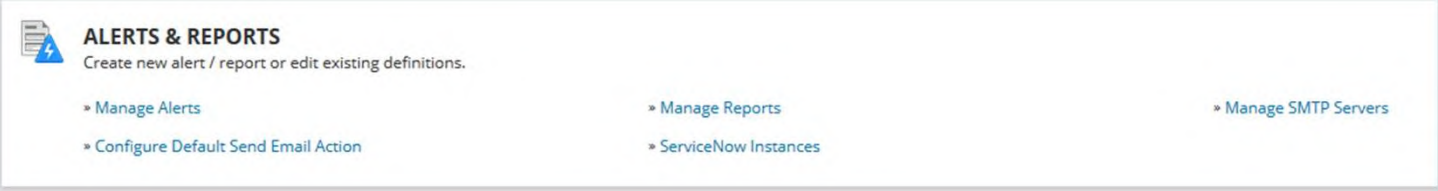
# Alerts

- Option settings for all alerts
- Acknowledge the alert has been viewed and is being worked on, NOT resolved
- Escalation is configurable for alerts that go without acknowledgement for set amount of time



# Alerts

- Managing Alerts
  - Manage alerts to see or edit all alerts, both enabled and disabled
  - Group by different parameters including installed product
  - Use duplicate and edit to make changes (Treat Native alerts as Master Copy)
  - Use Add Alert to create new alerts
  - Use Action Manager to manage actions and associated alerts

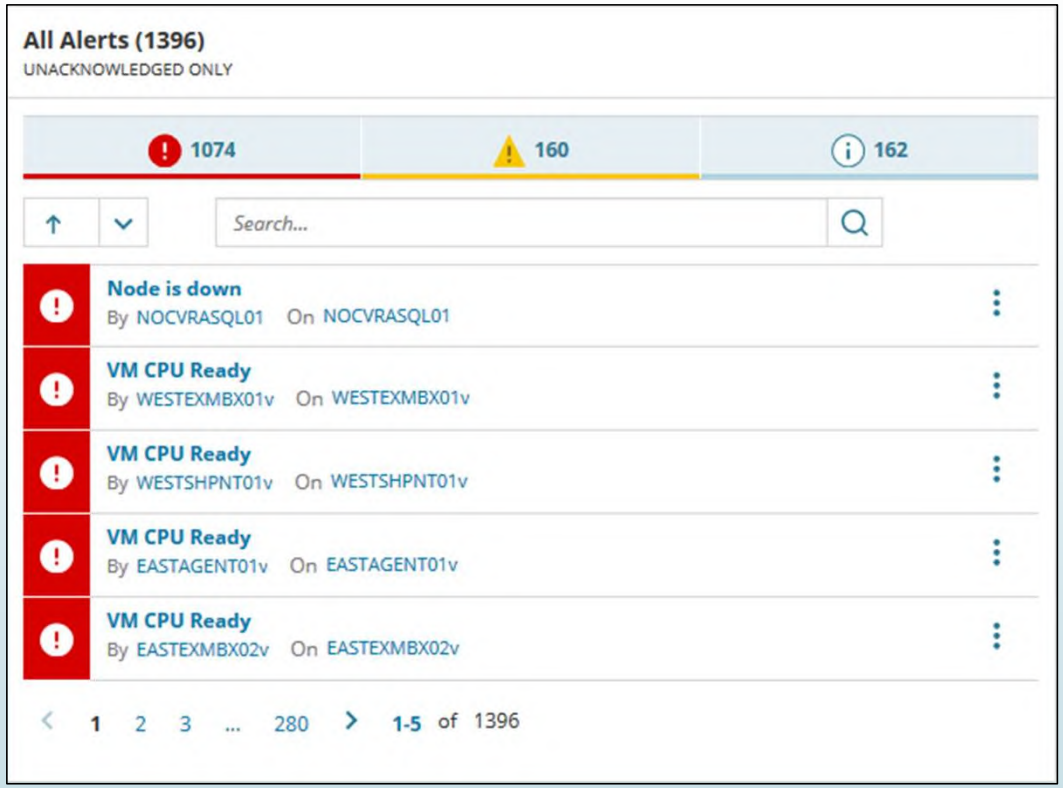


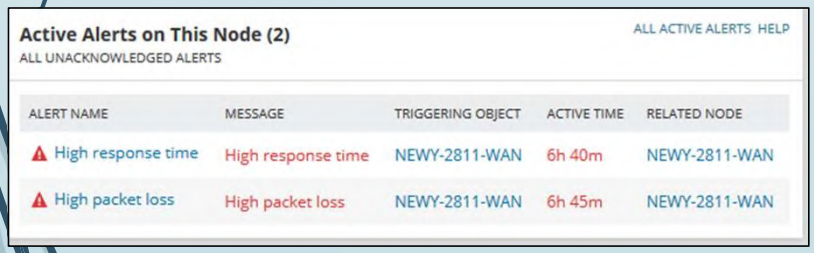
# Alerts

- Editing and Building New Alerts
  - Alerts are defined by trigger conditions
  - Trigger conditions are Boolean logic based
    - Allows for single lines of logic
    - Allows for and/or and groups of parameters
    - Can be very simple of extremely complex give properties of alert
  - Several parameters can be defined
    - Time of Day
    - Reset thresholds and times
    - Actions

# Alerts

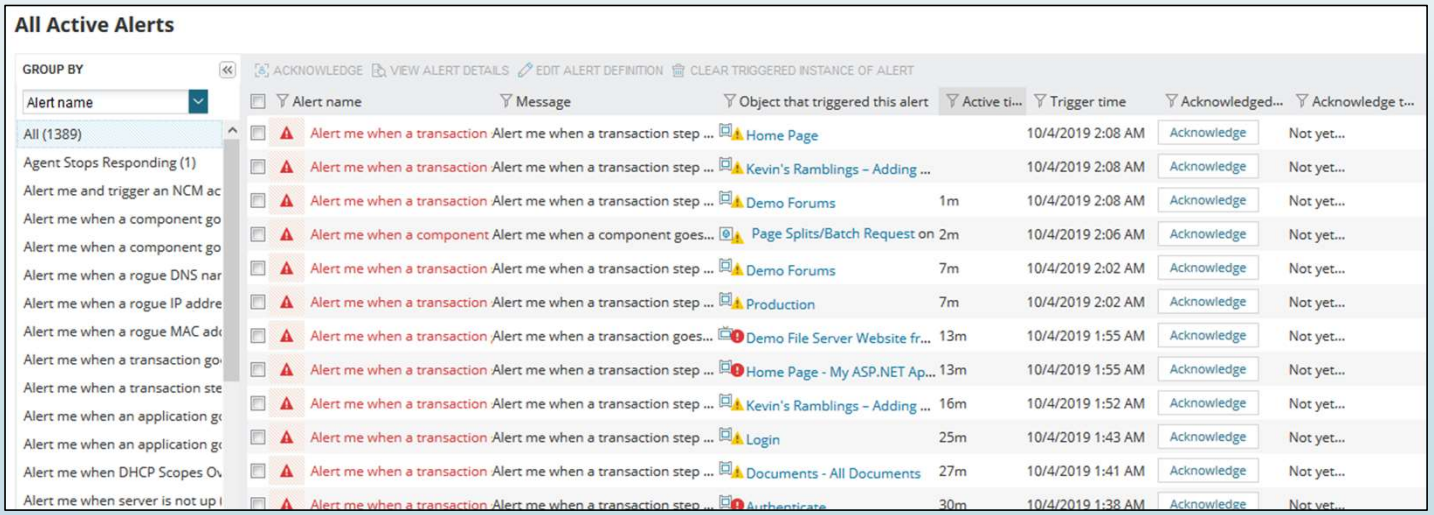
- Active alerts show in the web console at the global and node level
- Active alerts on product summary pages or node detail pages



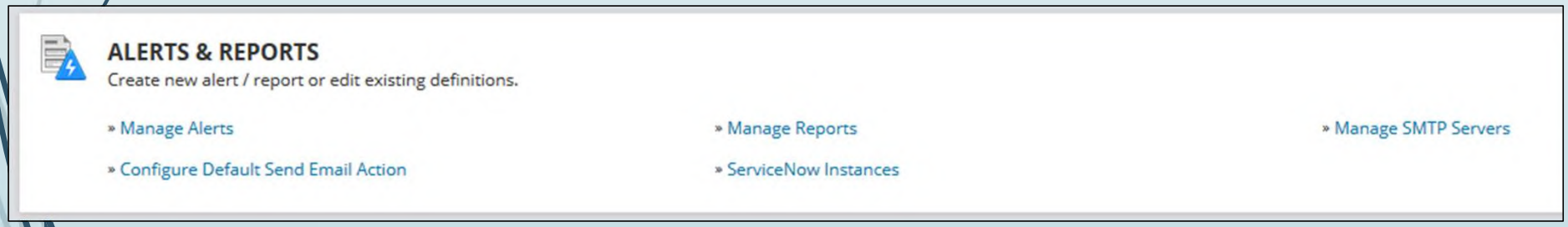
# Alerts

- Option settings for all alerts
- Acknowledge the alert has been viewed and is being worked on, NOT resolved
- Escalation is configurable for alerts that go without acknowledgement for set amount of time



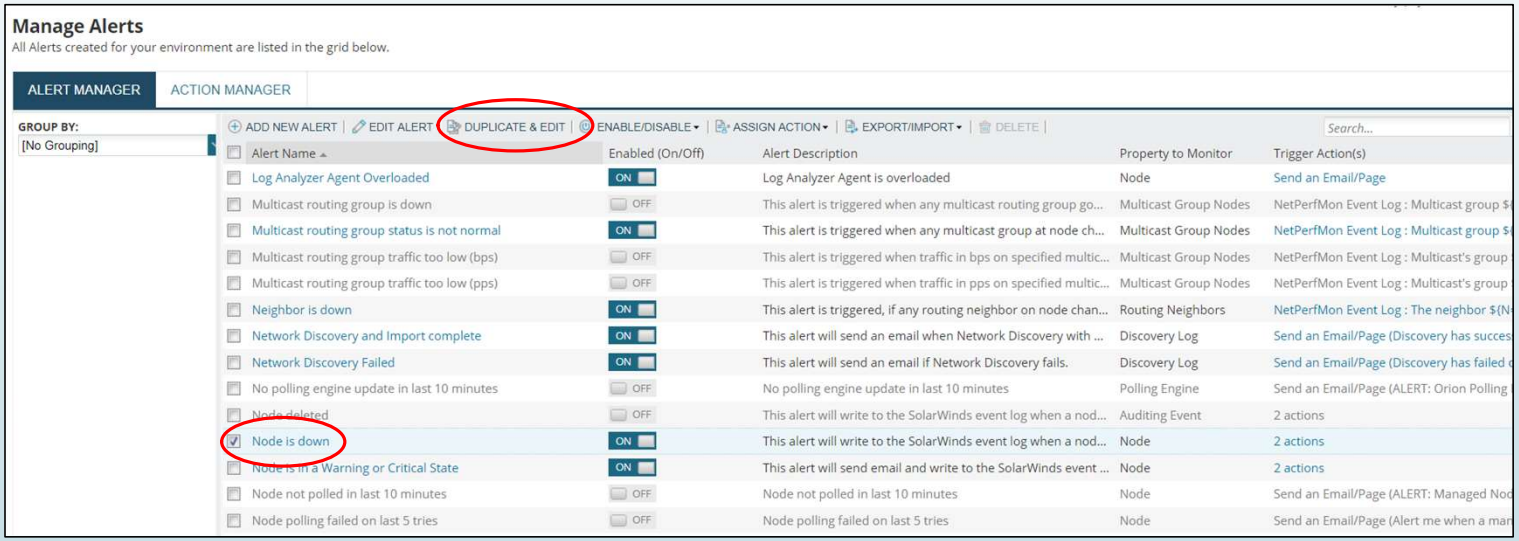
# Alerts

- Managing Alerts
  - Manage alerts to see or edit all alerts, both enabled and disabled
  - Group by different parameters including installed product
  - Use duplicate and edit to make changes (Treat Native alerts as Master Copy)
  - Use Add Alert to create new alerts
  - Use Action Manager to manage actions and associated alerts



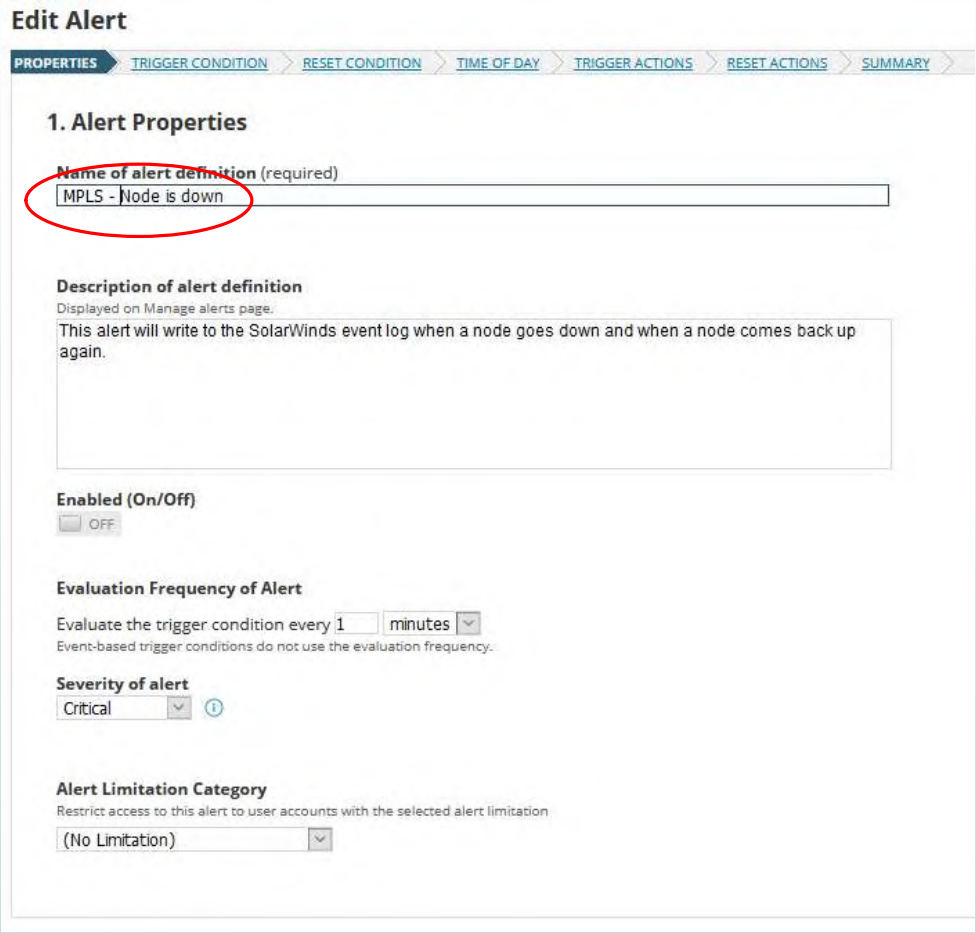
# Alerts - Managing Alerts

- Native Alerts from Installation will only allow for minor adjustments. Use duplicate and edit to make changes



# Editing Alerts

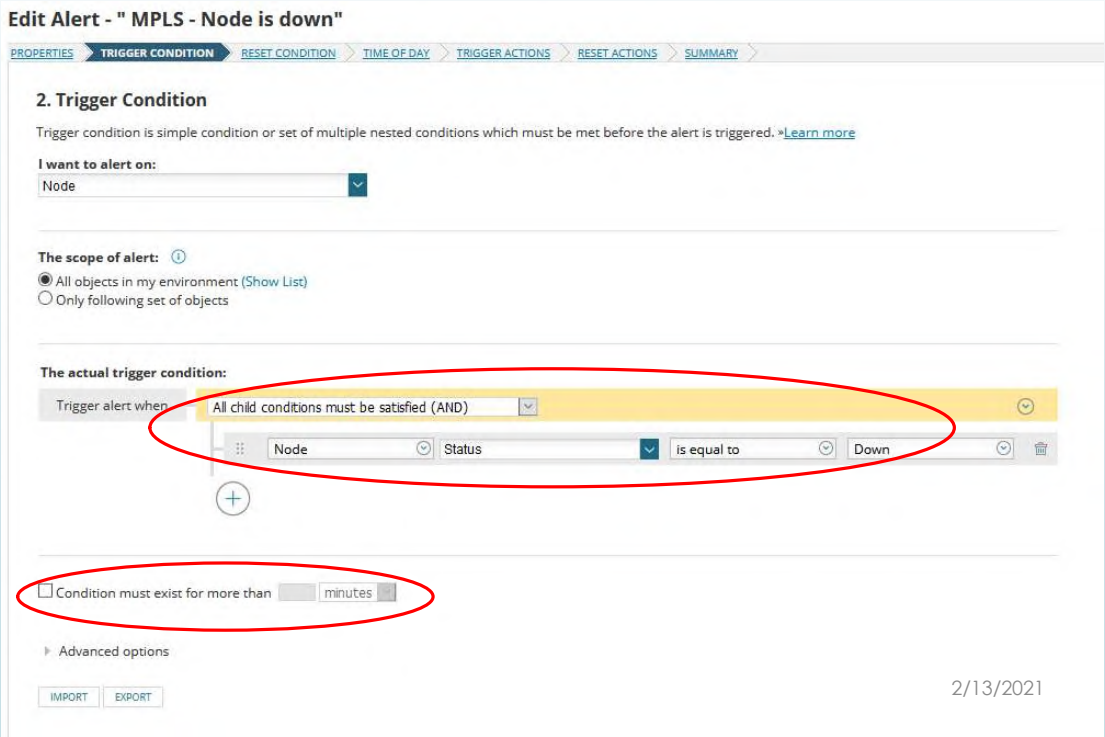
- Default name is "Copy of" Change name to something identifiable



# Alerts – Trigger Condition

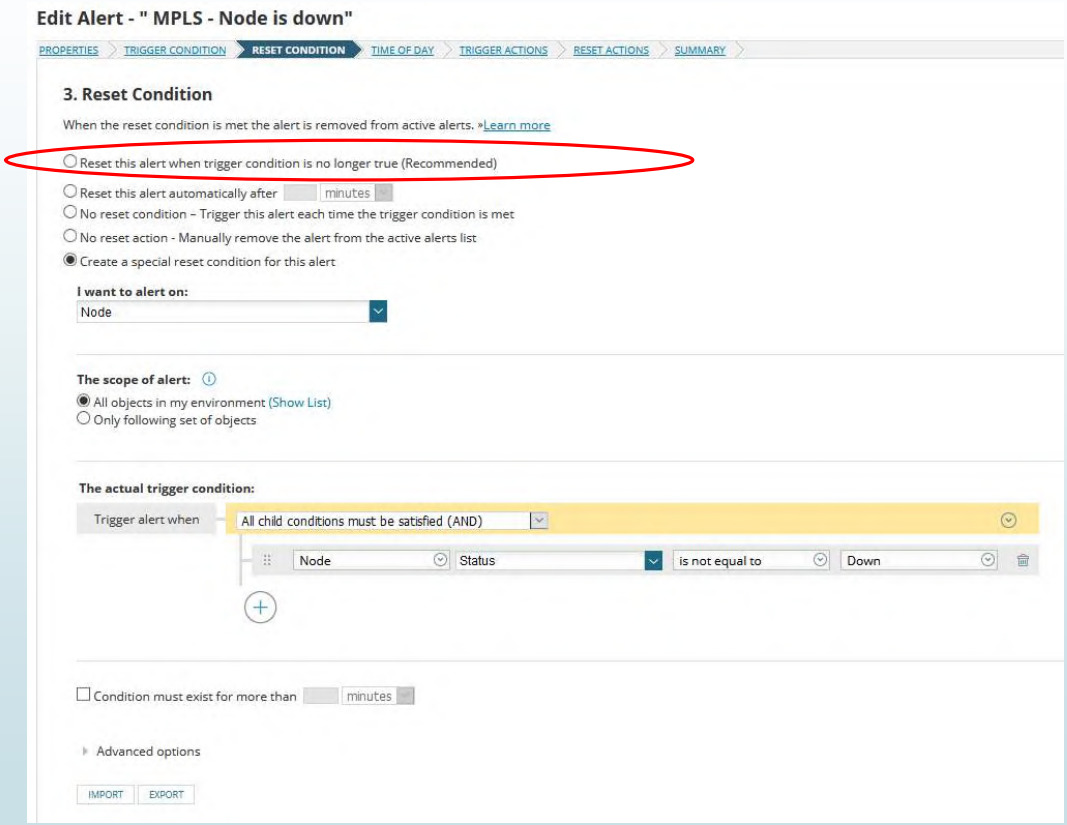
- Define parameters for alert, in this case parameters are "node = down"

- Condition settings can also be defined here



# Alerts – Reset Condition

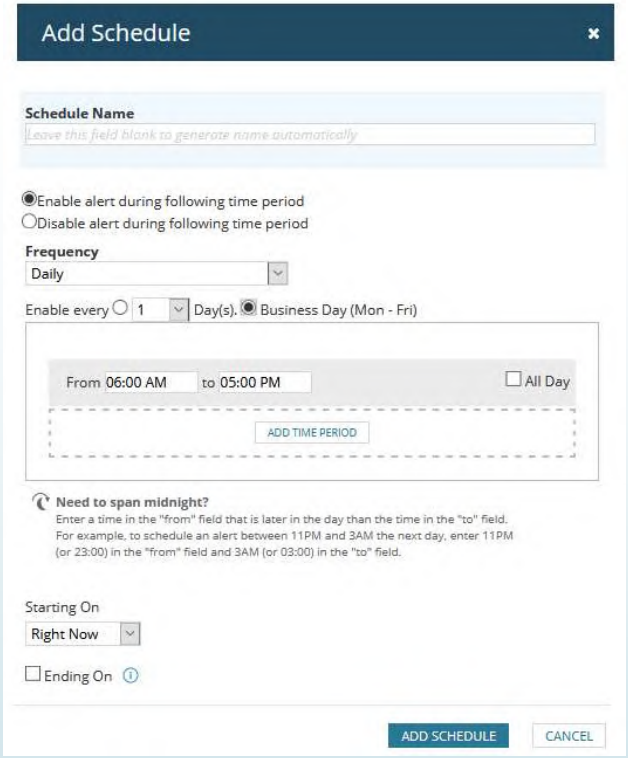
- Reset this alert when the trigger condition is no longer true

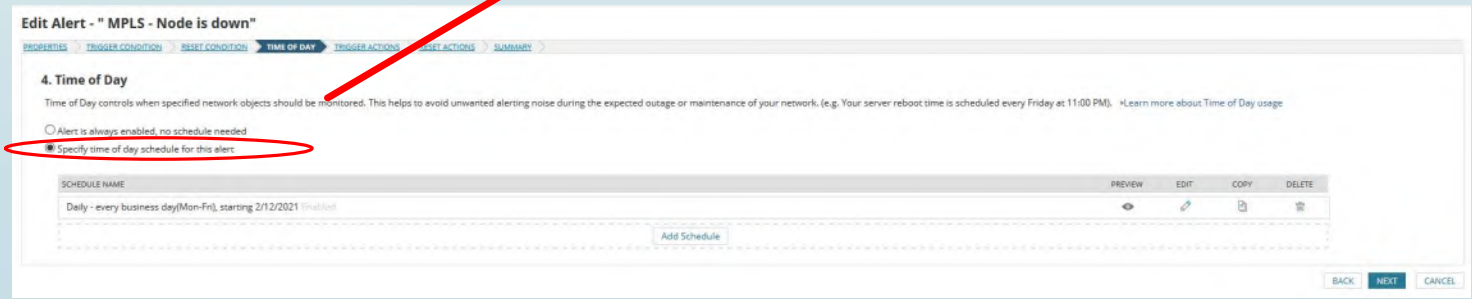


# Alerts – Time of Day

Time of day settings example:

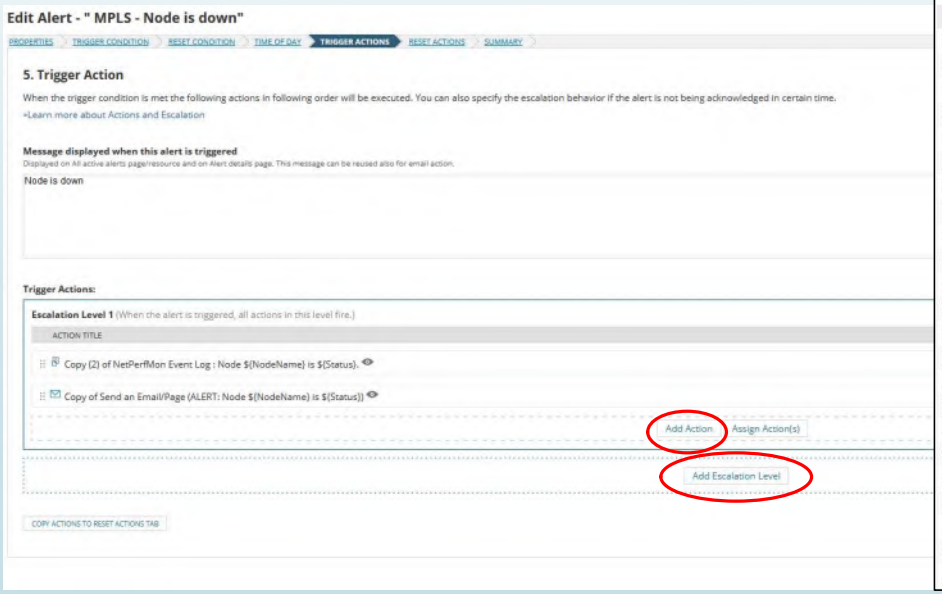
- Alert active Mon-Fri, 6AM-5PM

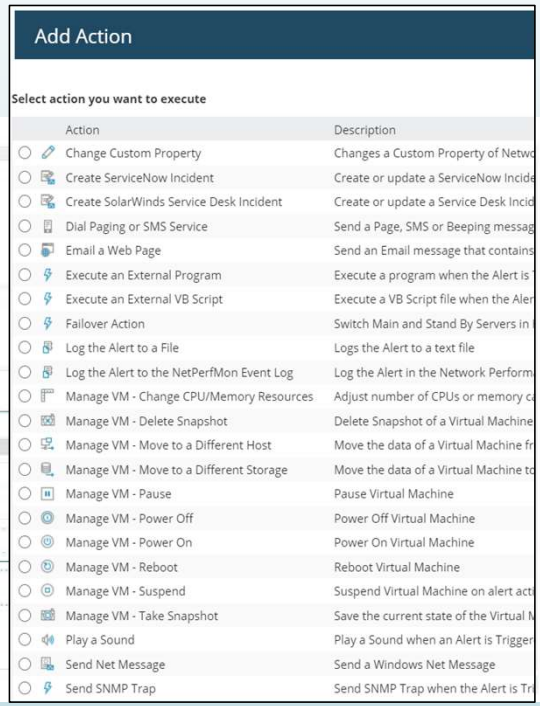


# Alerts – Triggered Action

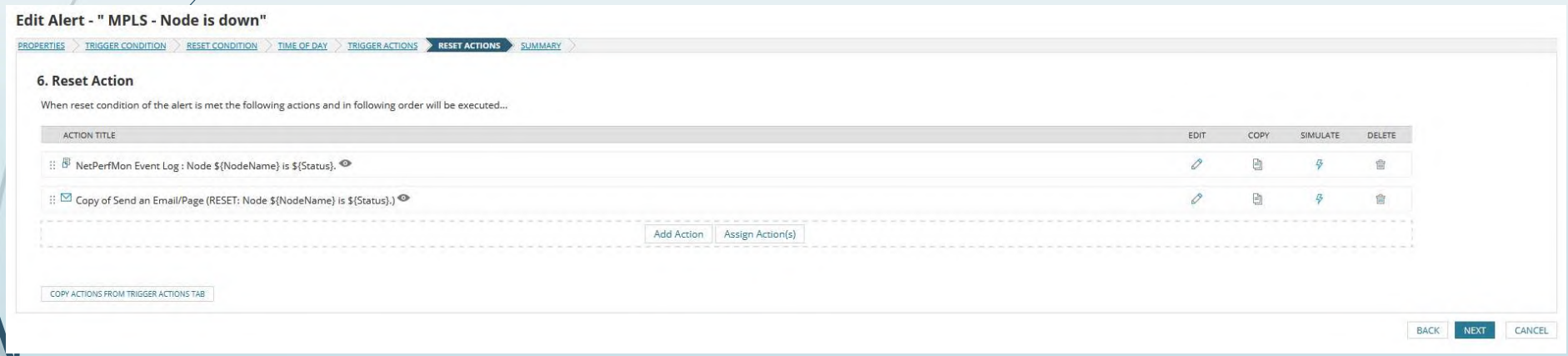
- Select what action is necessary when the alert is triggered
- Set escalation parameters



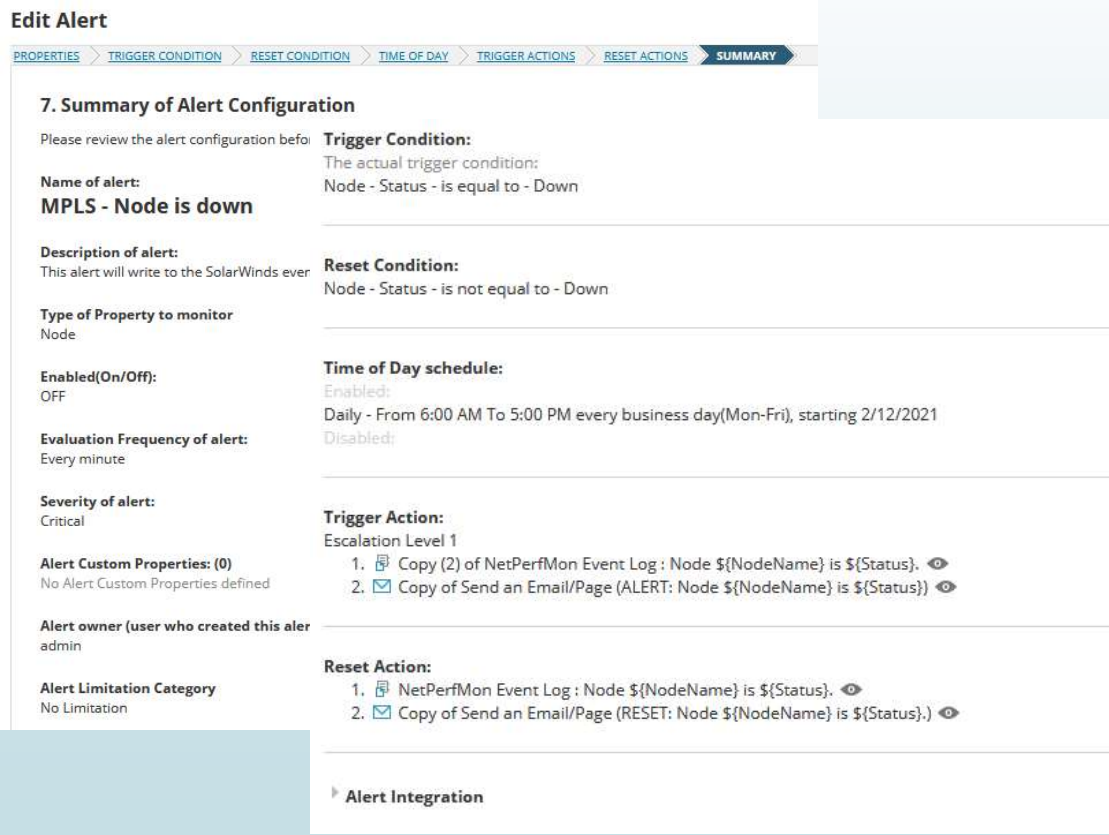
# Alerts – Reset Action

- Configure what action is needed when Node is back up

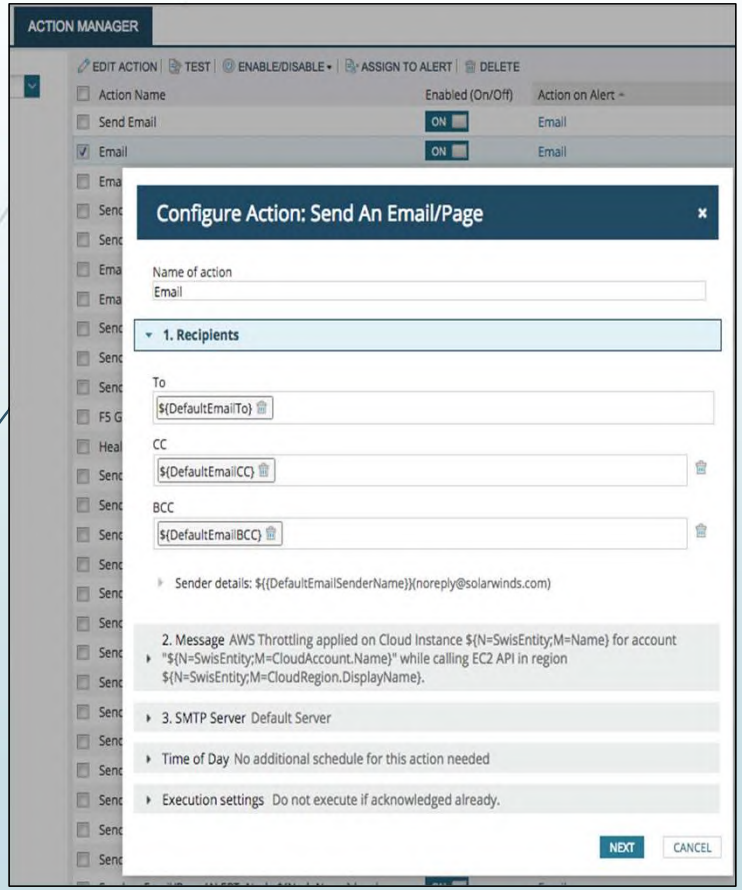


# Alerts - Summary

- Review parameters
- Review what alerts will be triggered once you hit submit



# Alerts - Email Action




- Action Manager
- E-mail is the most common form of notification.
- Excessive Email notification will translate to the recipient as junk and not valued

- Configuring and Editing Alerts
  - Enable/Disable Alerts
  - Duplicate and Edit Alert
- Create an Alert

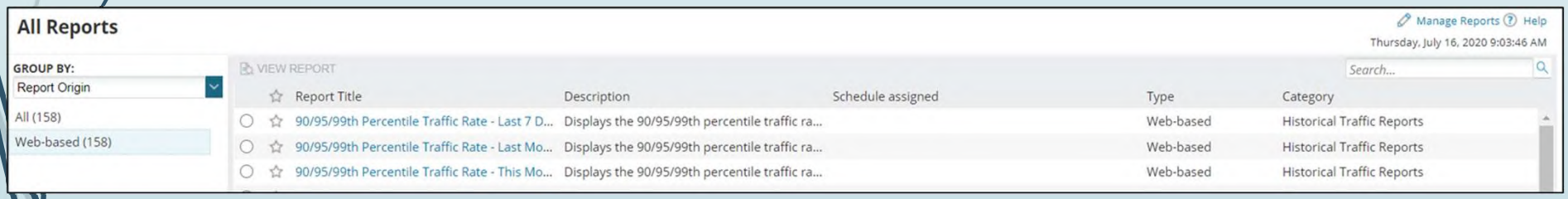
# DEMO & LAB 09

# *Break*

# Reports



- What are Reports?
  - Best way to access and pull data from database without tricky coding
  - Can show both historical and current data
  - Typically contains detailed information about selections parameters
- Default Reports
  - Come with each Orion product and available to use after install or product
  - Some reports will be enabled from the start
  - Report information gathered from nodes as a result of polling
  - Editable, configuration, and created



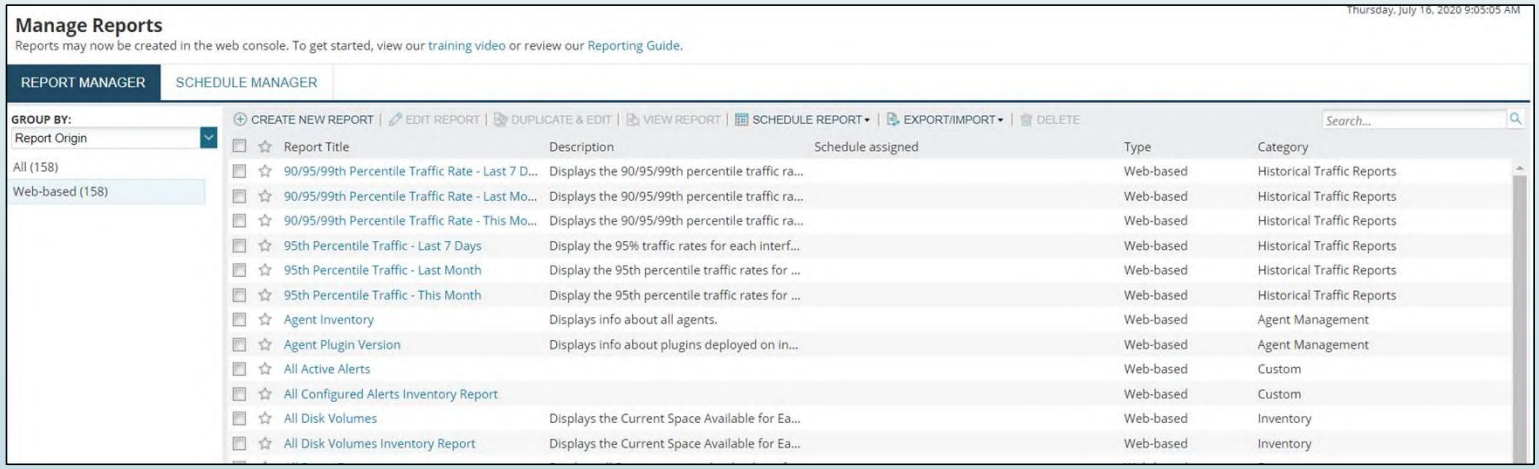
# Reports



- Creating Reports
  - Reports can be created for defined or perceived requirements
  - Edit an existing
  - Create a new
- Web Console Report
  - Create reports to show data, charts, and graphs
  - Uses drag-and-drop
  - Add Organizations graphic(s) to report if needed
- Scheduling Reports
  - Reports can be run and saved or sent on a defined schedule
  - Used for regular, management, or operational requirements
  - Exportable to PDF, Excel®, or HTML document for delivery via email

# Reports

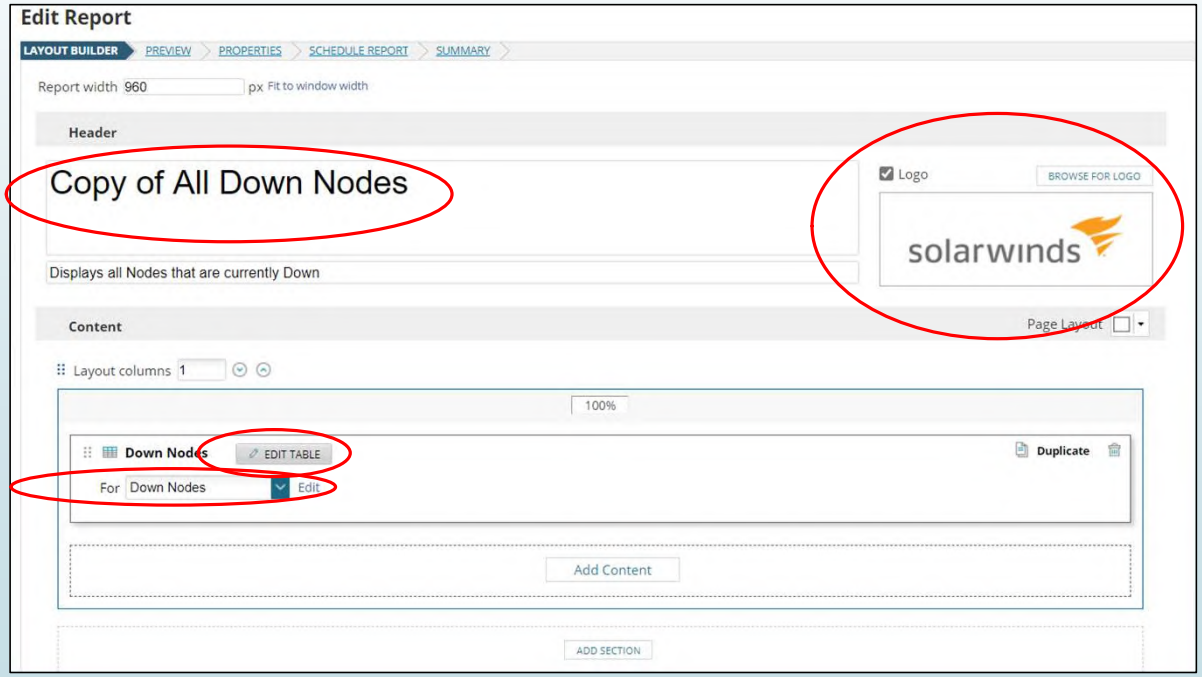
- Manage Reports: edit, duplicate, view, schedule, export/import created reports
- When learning how to create reports, best to pick and existing report that has data close to what you need, best to copy then edit the copy



# Reports



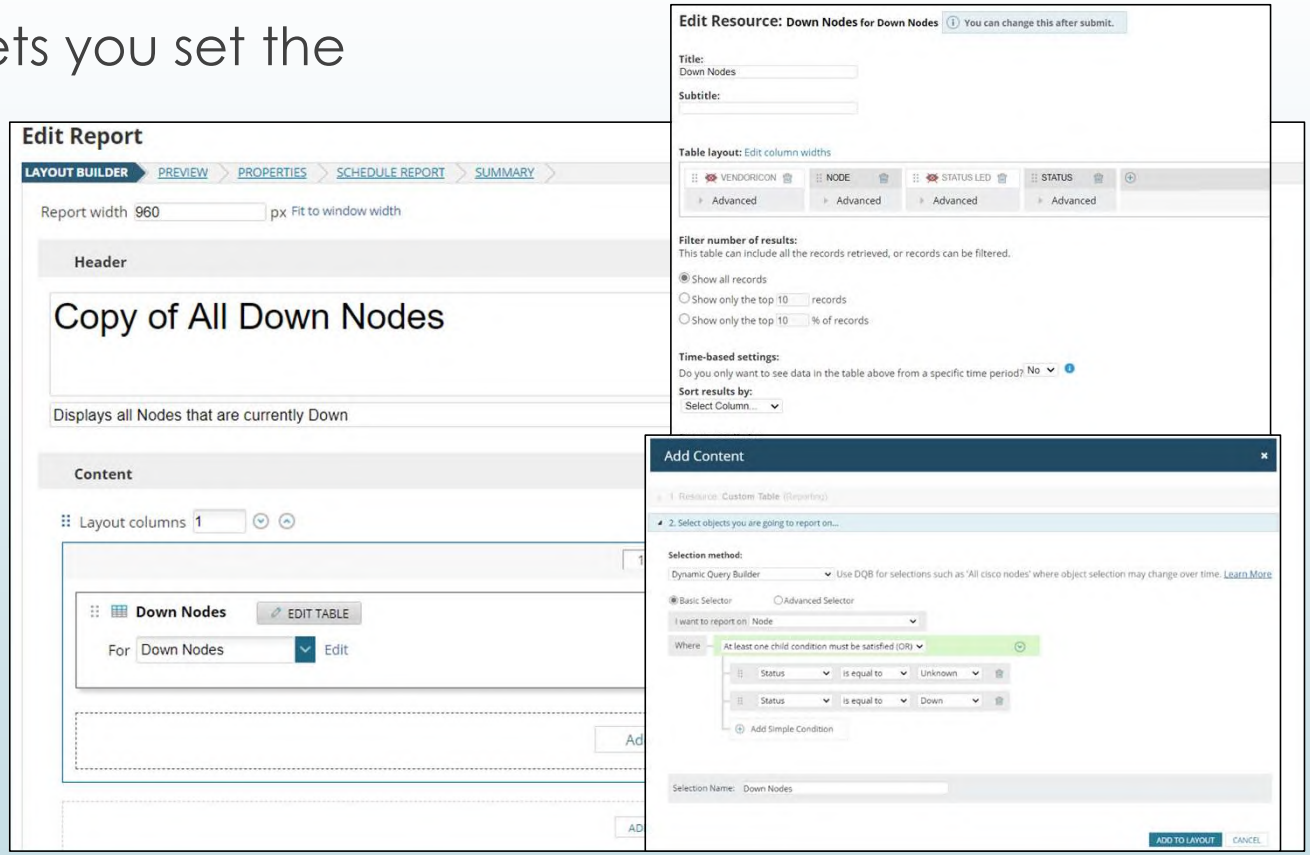
- Copy and edit an existing report
- Layout builder lets you change header, logo, layout and devices



# Reports



- Edit Resource lets you set the columns
- Edit Data Source lets you configure what to report on



# Reports



➨Preview the changes that were made

**Edit Report**

LAYOUT BUILDER | **PREVIEW** | PROPERTIES | SCHEDULE REPORT | SUMMARY

## All Nodes

solarwinds

Summary of Orion Objects: **All Nodes**

**All Nodes (Custom Table)** for **All Nodes**

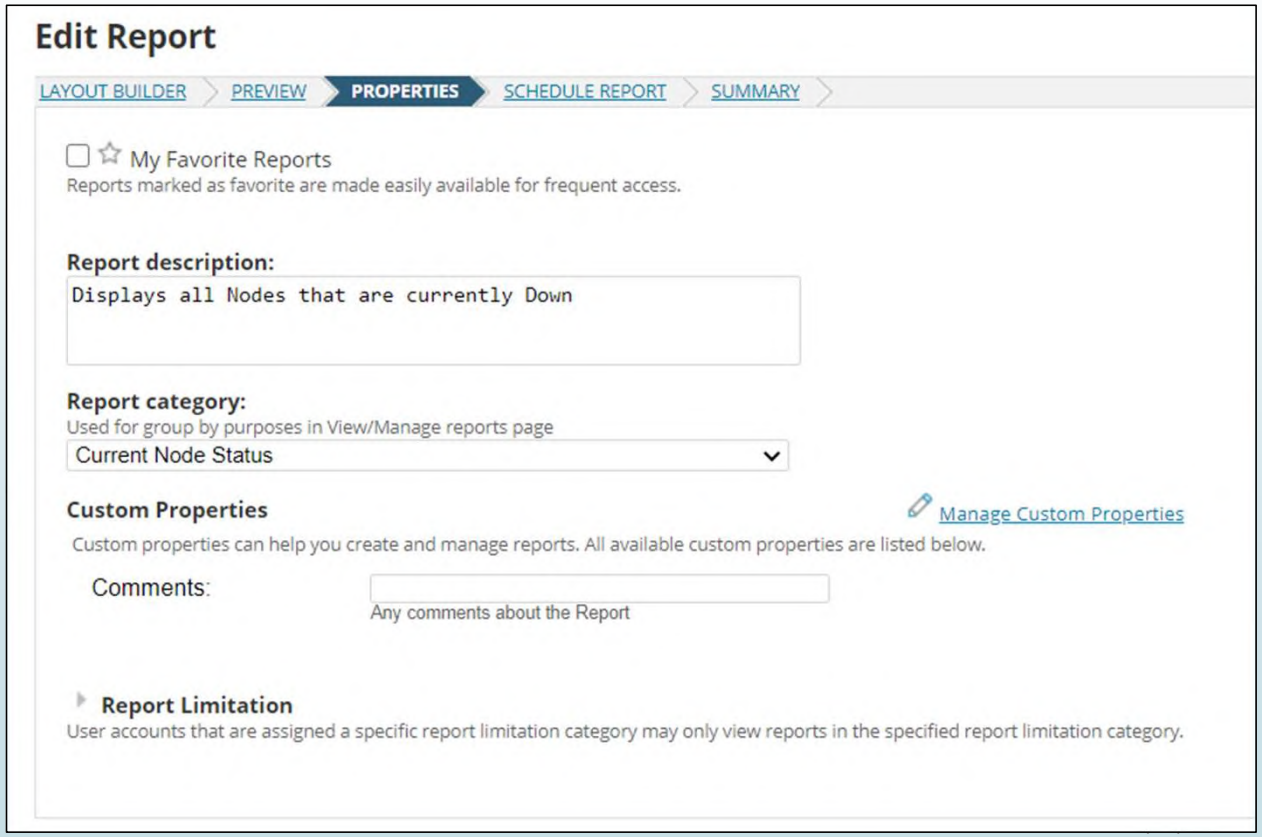
Ordered by:Caption - Ascending then by IP Address - Ascending

| CAPTION | IP ADDRESS | IP VERSION | VENDOR | MACHINE TYPE |
|---|---|---|---|---|
| | 192.168.248.159 | IPv4 | Juniper Networks, Inc. | Juniper EX4300 |
| | 192.168.248.152 | IPv4 | Juniper Networks, Inc. | Juniper EX4300 |
| | 192.168.247.16 | IPv4 | Unknown | Unknown |
| | 192.168.247.15 | IPv4 | Unknown | Unknown |
| | 192.168.248.41 | IPv4 | Juniper Networks, Inc. | Juniper EX4550 |
| | 192.168.248.153 | IPv4 | Juniper Networks, Inc. | Juniper EX4300 |
| | 192.168.248.154 | IPv4 | Juniper Networks, Inc. | Juniper EX4300 |

# Reports



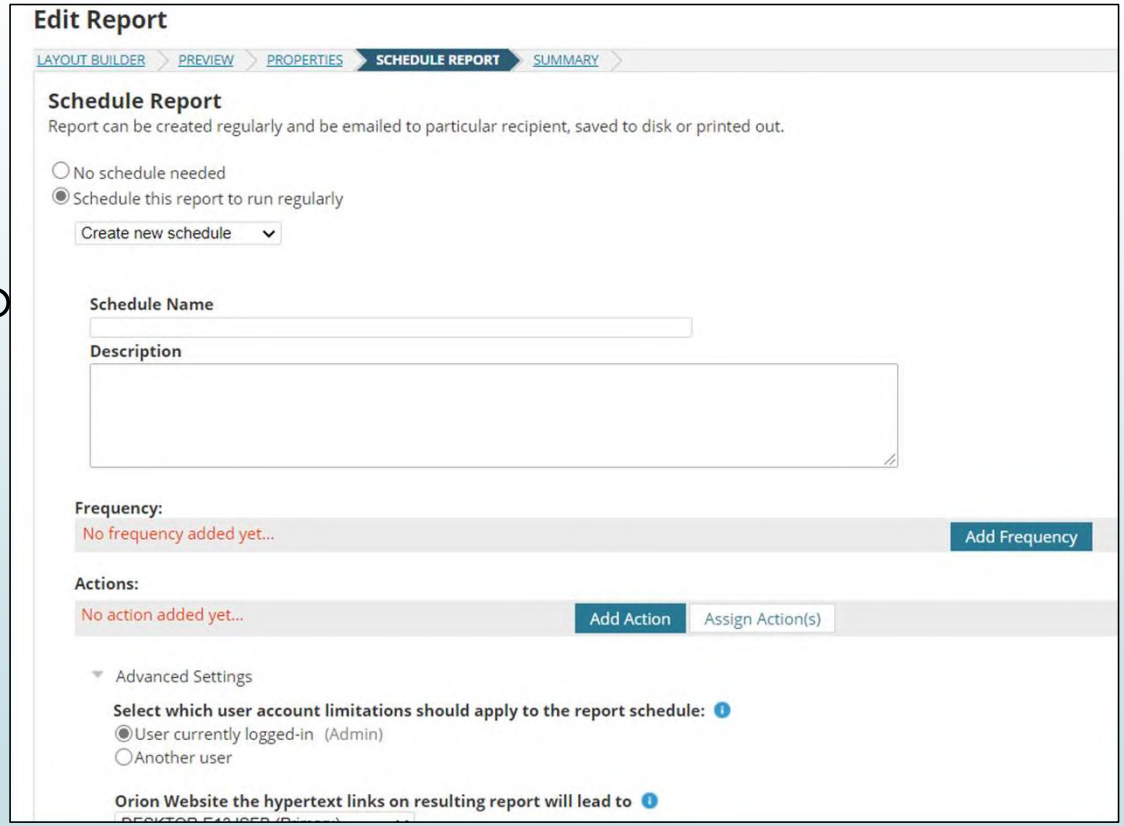
- Report properties allow you to set:
  - Favorites
  - Description
  - Category
  - Custom Properties
  - Limitations



# Reports



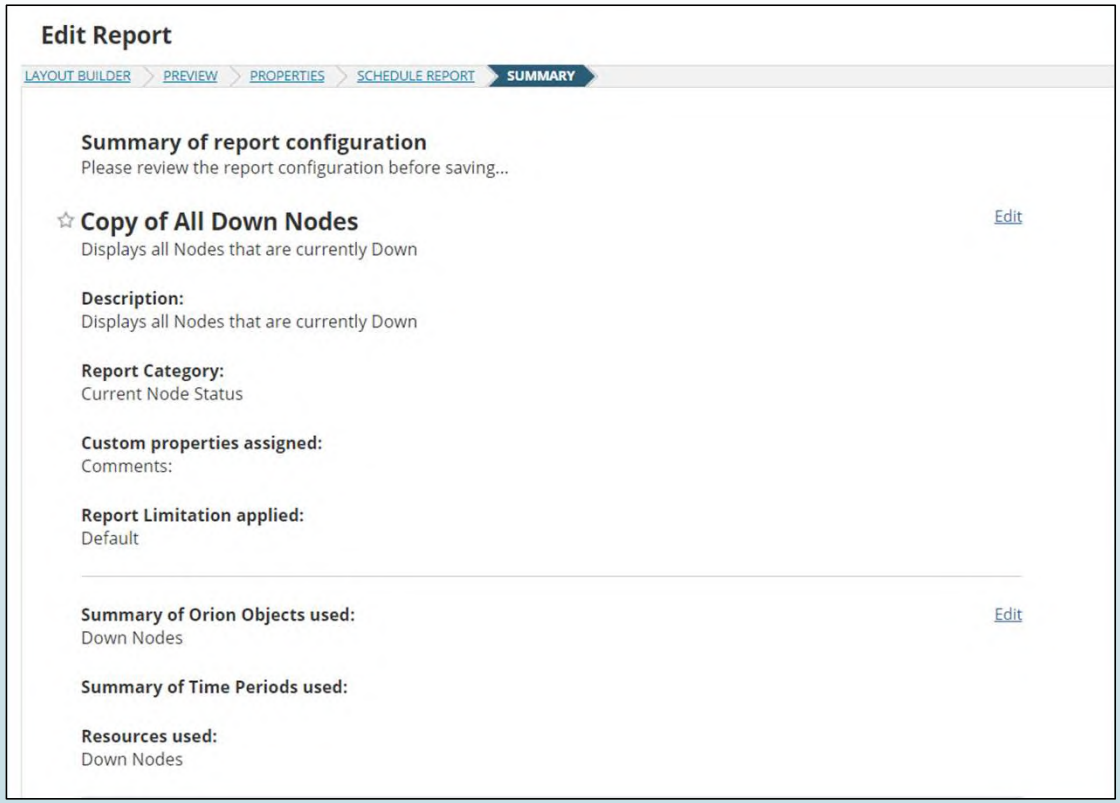
- Report schedule
- Frequency is how often does the report run
- Action is what to do after the report runs? Send in an email?



# Reports



- Review the report
- If report is not correct changes can still be made
- Remember to change the report name from 'Copy of' to a friendly name



- Configuring and Editing Reports
  - Enable/Disable Reports
  - Duplicate and Edit Report

# DEMO & LAB 10

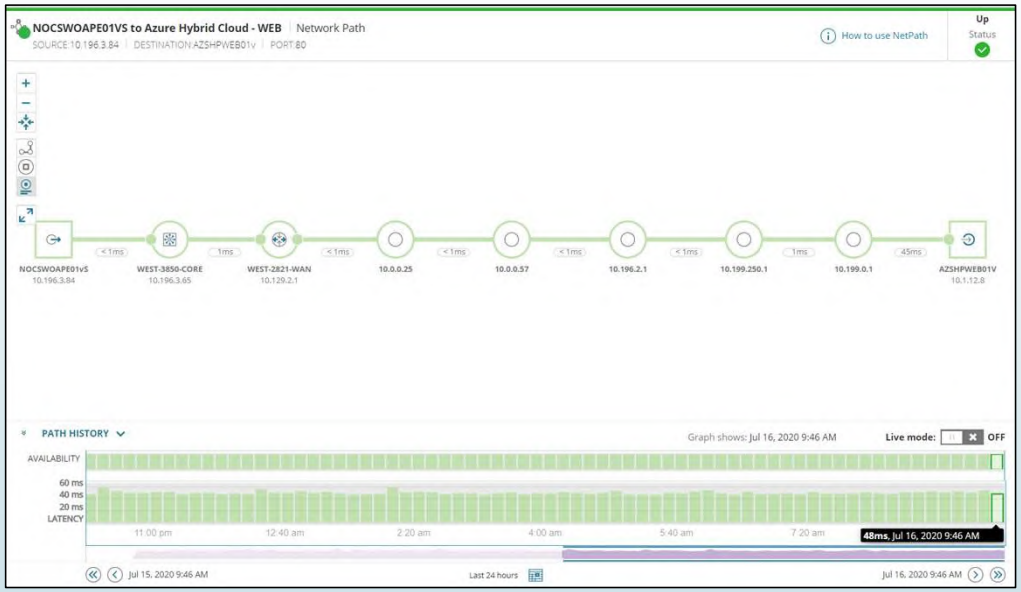
# *Break*

# NetPath Services

- So much more than just a Traceroute!
- Tracks results over time
- Choose port to test
- Multiple sources per Service

# NetPath Services

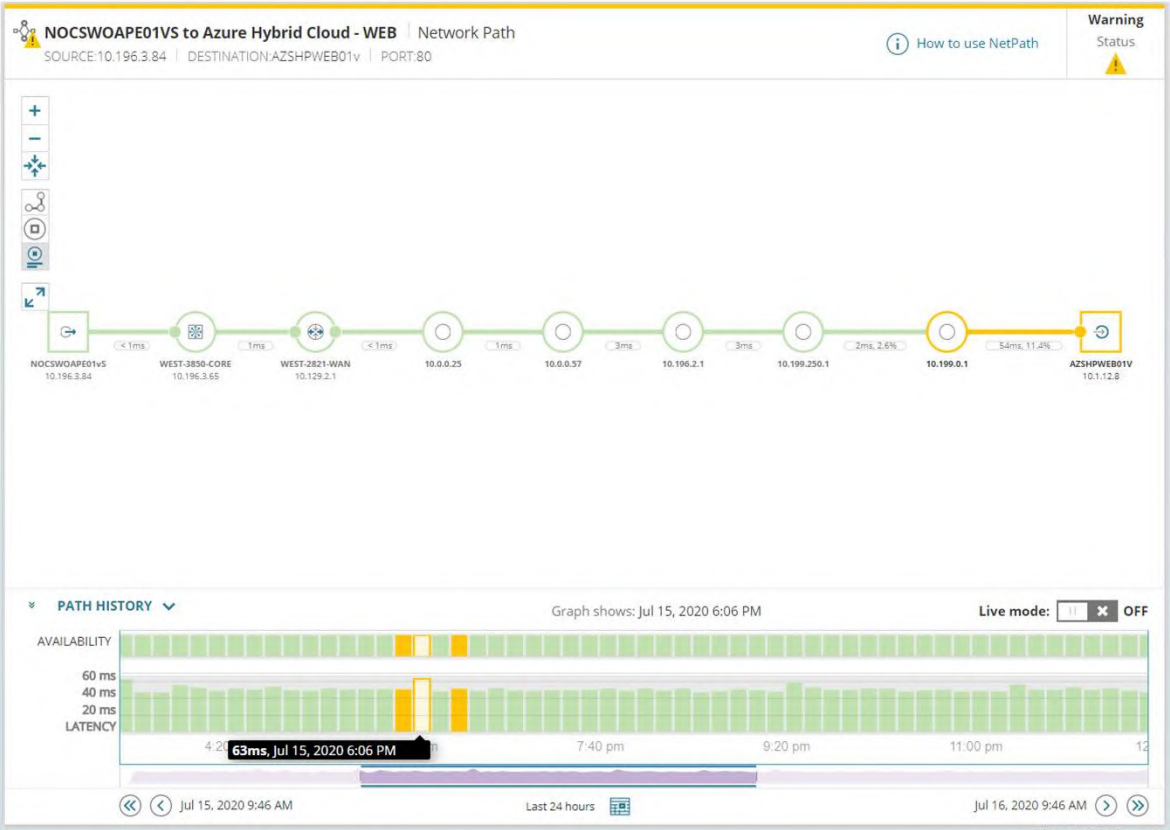
- Visibility of managed and unmanaged devices
- Able to trace path to a  service
- Integrate other SolarWinds Products (NPM, NTA)



# NetPath Services



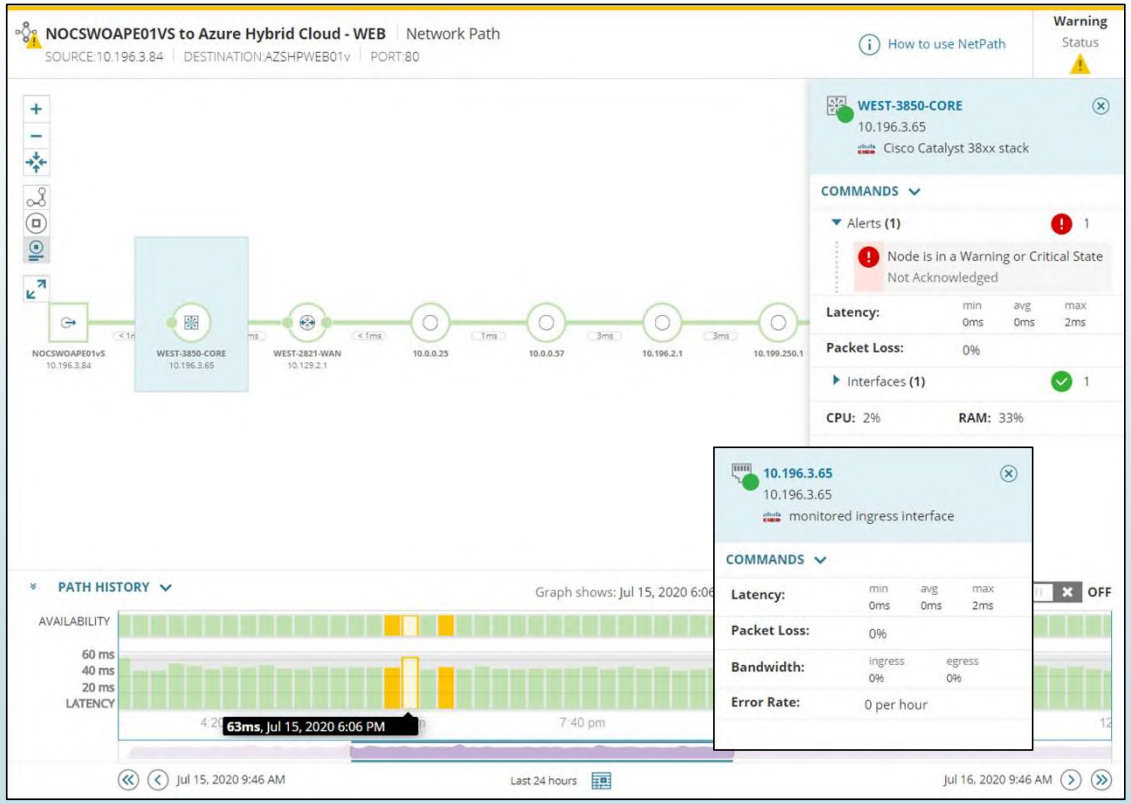
- Visually see where the path failed



# NetPath Services



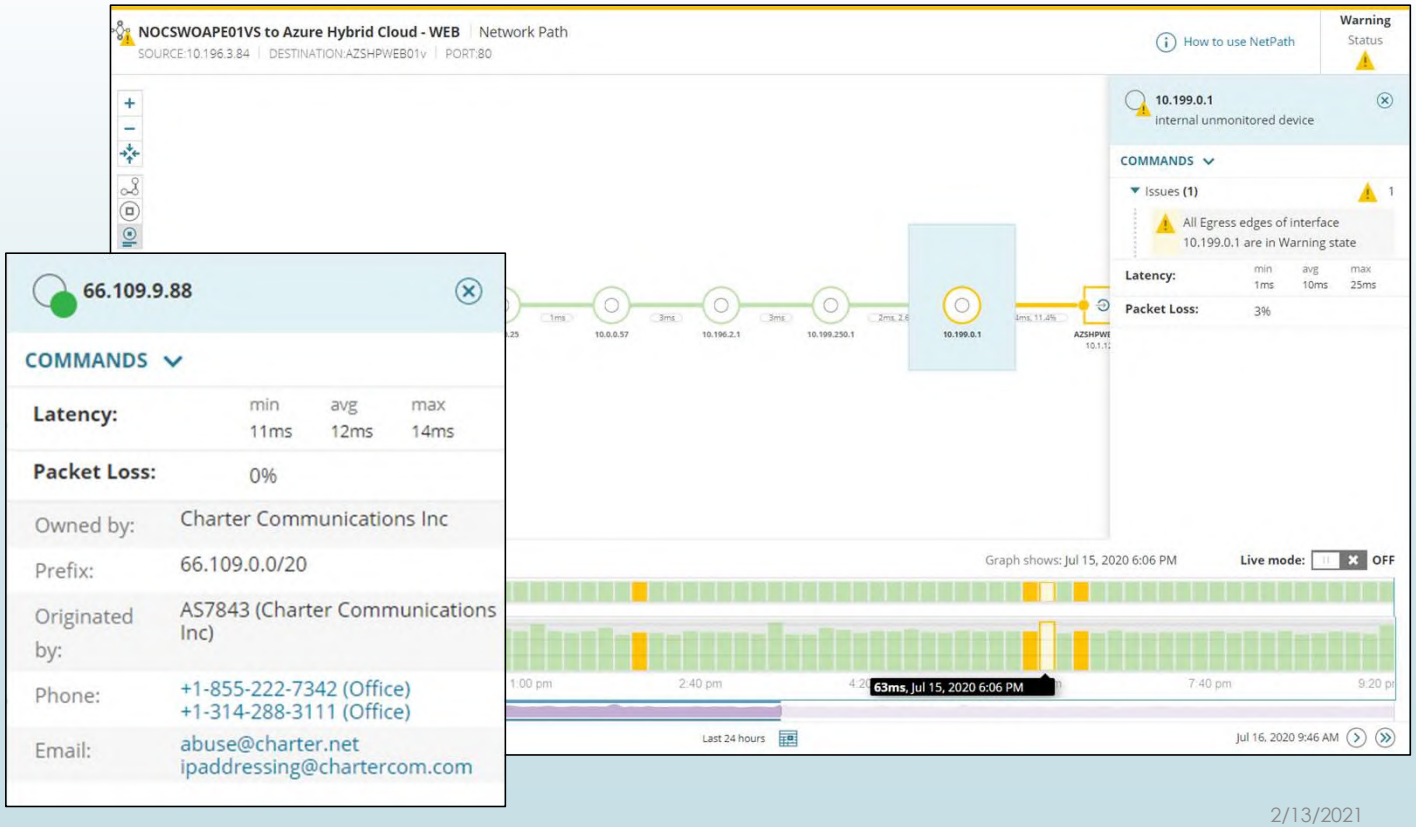
- View details about your SolarWinds Managed Devices



# NetPath Services



- View available statics on unmanaged WAN devices
- Ownership and contact information of unmanaged devices are sometimes available



# NetPath Services

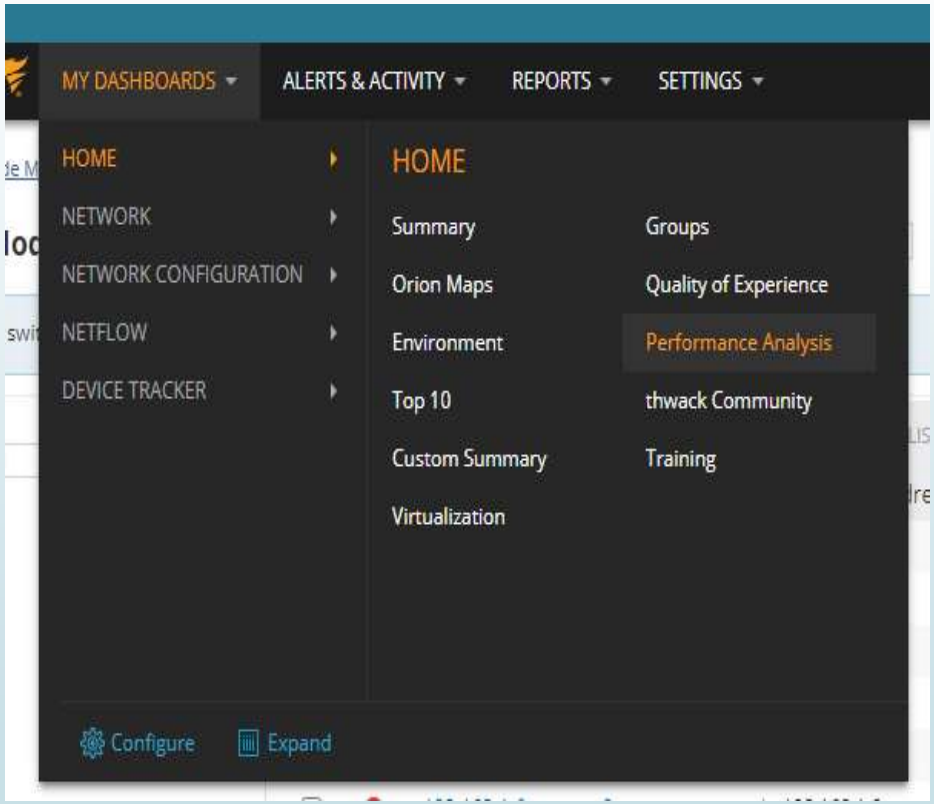


- View affects of the network slowdown
- In this case the server is not down but is experiencing 18% packet Loss
- Also notice the server CPU/Memory are not overloaded. This is an indication the server is operating correctly

# PerfStack



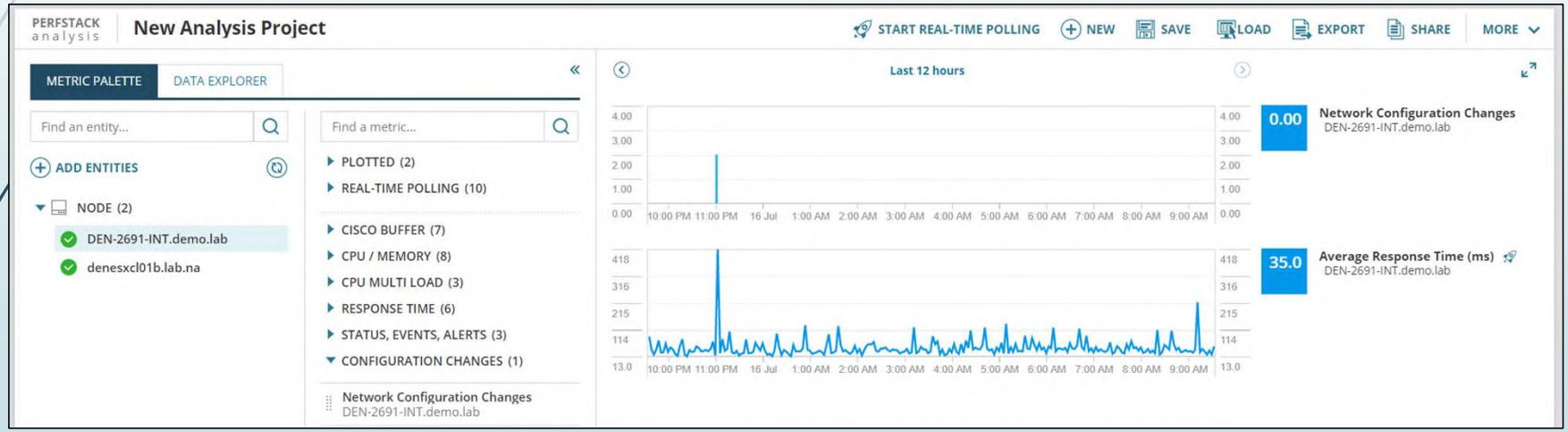
- PerfStack
  - What is PerfStack?
    - Feature of the Orion Platform designed for advanced troubleshooting for network issues
    - Drag-and-drop metrics to correlate data from different SolarWinds Products into a single graphical representation
    - Designed for multi-faceted, complex, intricate, troubleshooting scenarios
    - Allowing for both historic and real-time data analysis, monitoring, and collaboration between different functional groups through a single interface



# PerfStack



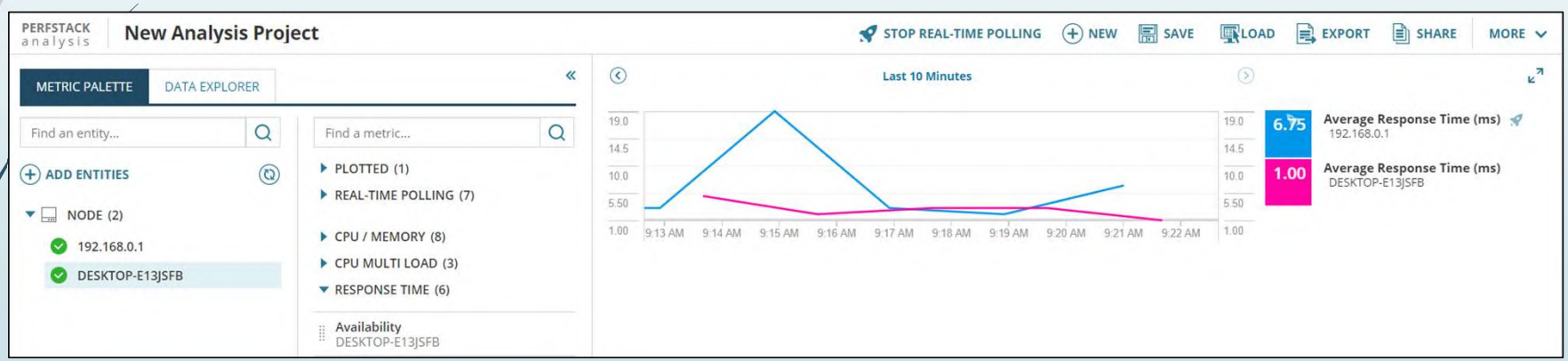
- New Project
  - Add network node
  - Chart Network Configuration and Response Time



# PerfStack



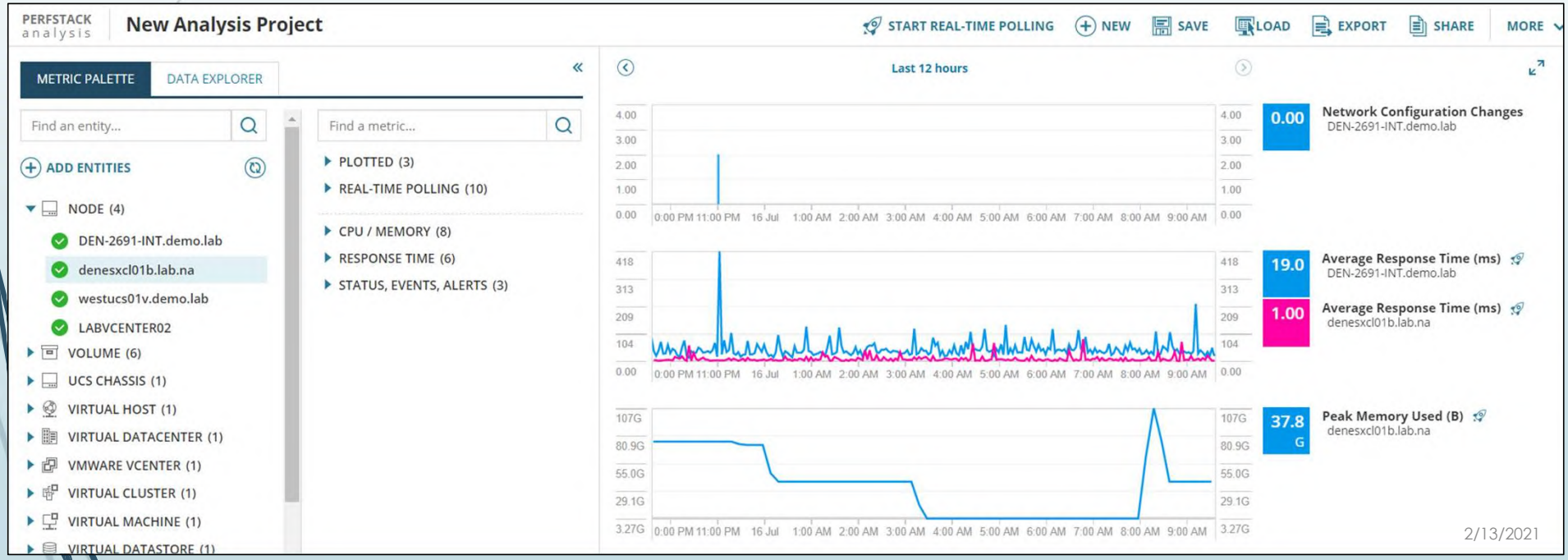
- New Project
  - Add server node
  - Add Server Response Time to Network Response Time Chart



# PerfStack



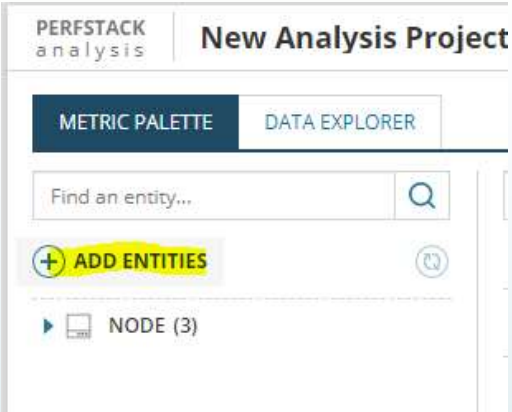
Added server Peak Memory to project
Now you can compare Network/Server statics to troubleshoot a problem



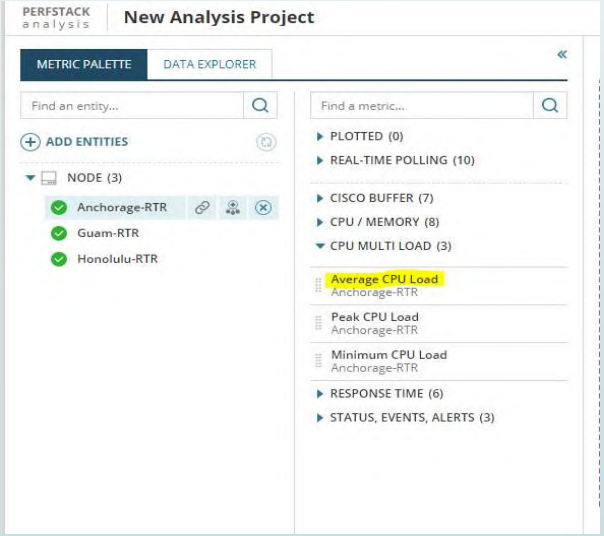
# PerfStack



- **NAVIGATION**
- (Right) select Add Entities



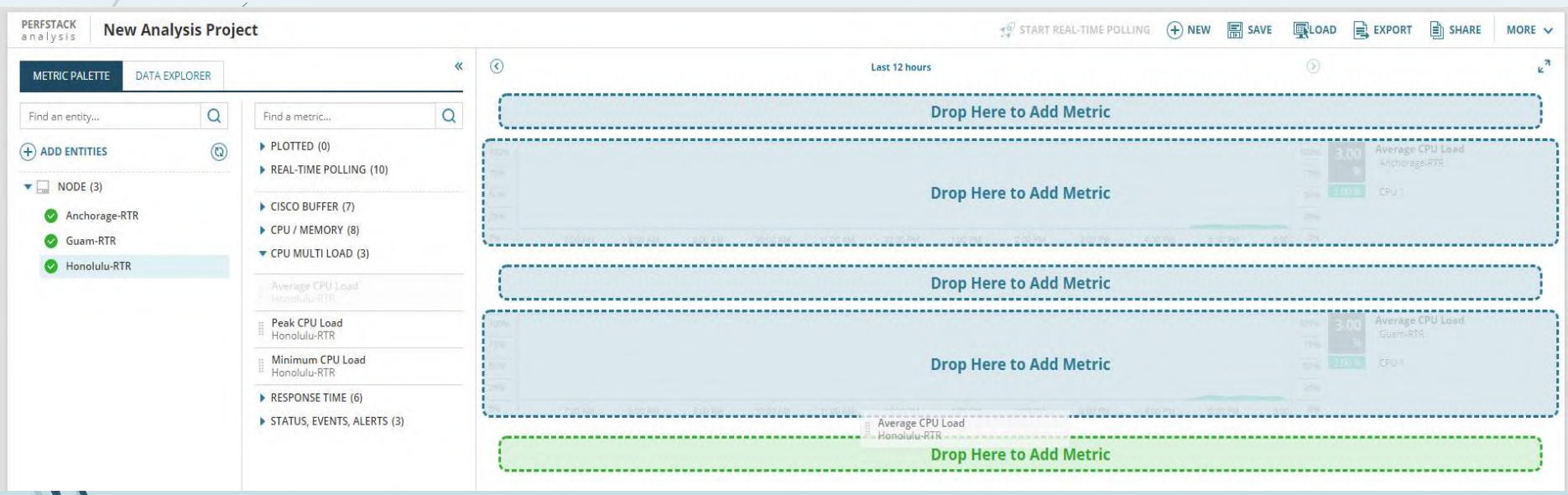

- (Right) click on device to expand a list of resources. Then select the resources you would like to compare (ex. Average CPU load) and repeat for other devices.



# PerfStack



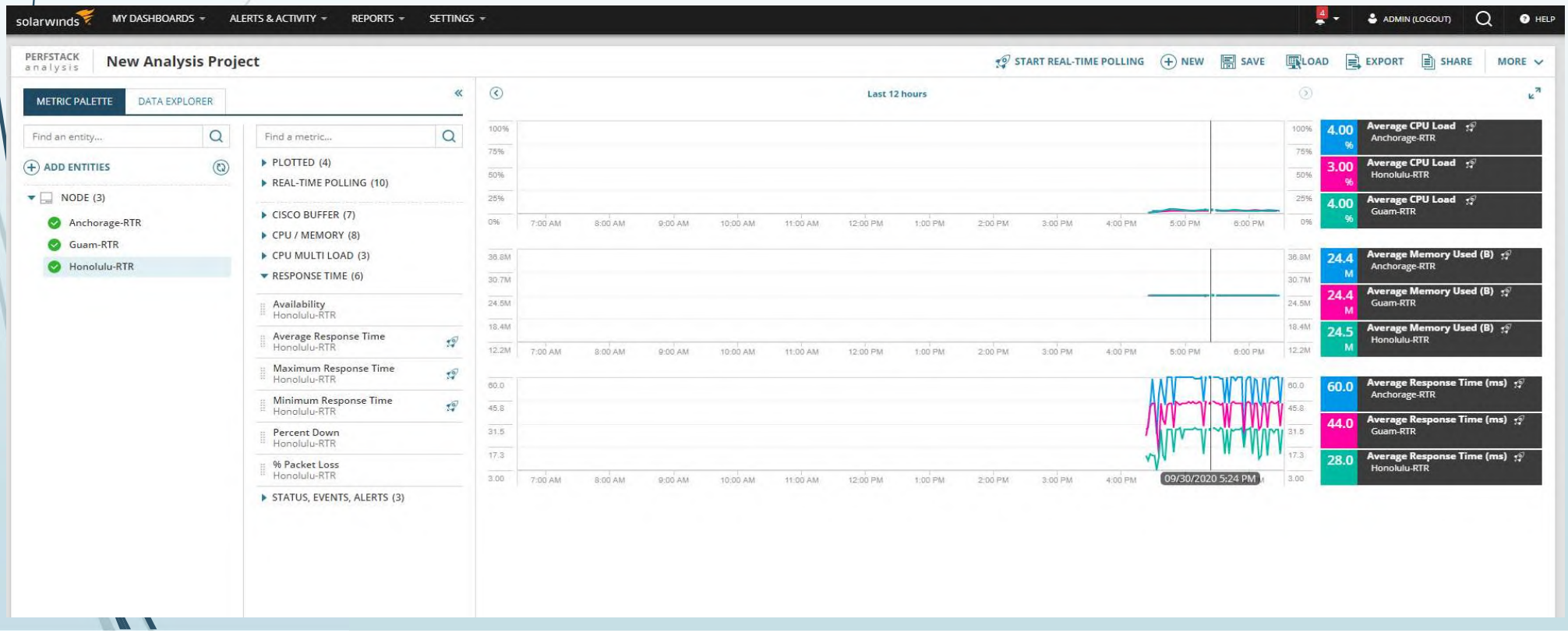
- To compare Average CPU Load of Honolulu/Guam/Anchorage select that resource under each device site and drag to the same <u>wide</u> Drop here to Add Metric
- To compare other resources repeat the process, however you will drop the resources above if you would like it displayed above or below if you would like to display it below



# PerfStack



- Top-Right Icons allow you to: start real-time polling, new (start new comparison), save, load (load existing projects), export (.csv), share, more (save as, delete, help.
- Additionally, you can display real-time polling on your dashboards.



# End of Day

- Review
  - Alerts
  - Reports
  - NetPath
  - Quality of Experience
  - PerfStack

# Questions and Answers

# Welcome Back!

Let's Review

# Today's Agenda

- This sections topics include:
  - Network Configuration Manager (NCM)
    - Adding NCM Nodes
    - Script Management
    - Device Templates
    - NCM Inventory
    - NCM Settings
    - Baseline Management
    - NCM Jobs
    - Compliance

# Network Configuration Manager (NCM)

- Product Information
  - What is NCM and who should use the product?
  - System and configuration requirements
- Installation and Configuration
  - Adding Nodes to NCM
  - Device Templates
  - Inventory
  - NCM Settings
- Configuration Management
  - Script Management
  - Baseline Management
  - Jobs
- NCM Compliance
  - STIGs

# What is NCM?
# Who should use NCM?

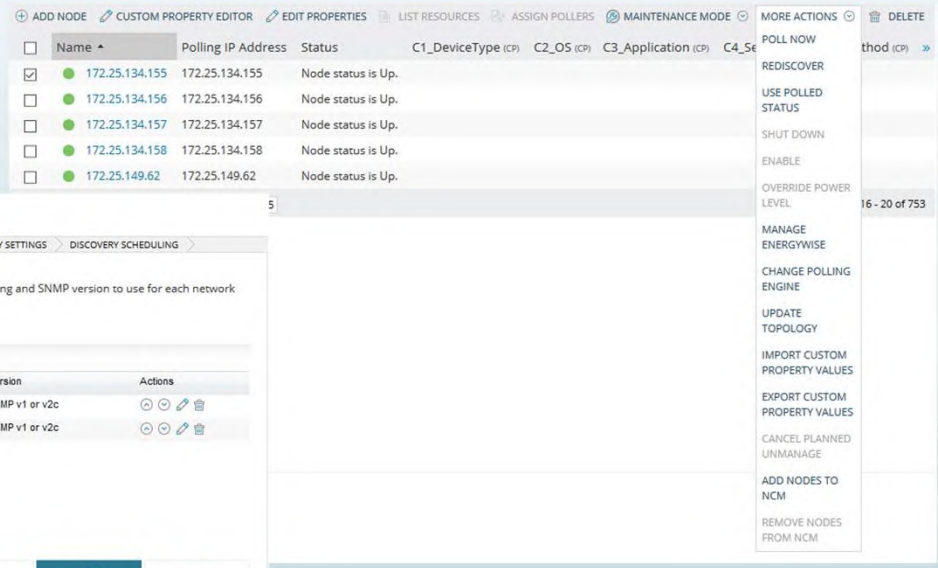
- NCM provides automated and consolidated management of network device configuration files for network management and compliant practices
  - Provides side-by-side configuration comparison
  - Real-time change detection
  - Scheduled backups
  - Integration with NPM's NetPath Services™
  - Bulk configuration changes

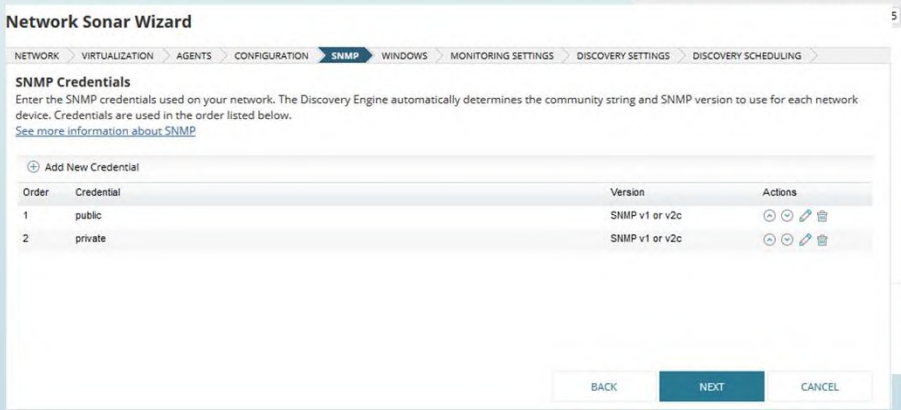
# NCM Product Requirements

- Port Requirements
  - 17777 (SWIS)
  - 80/443 (HTTP/HTTPS)
  - 22 (SSH)
  - UDP 161/162 (SNMP)
- Device Permissions and Requirements
  - CLI Credentials
    - Download/Upload
    - Change Configuration files
  - SSH Access
- NCM, NPM, and NTA are complementary to each other
  - Work together to provide data about the network
  - Solves problems with correlated data

# NCM Adding Nodes

- Three different ways
  - Through Discovery Process
  - Manage Nodes Menus
  - Edit Properties



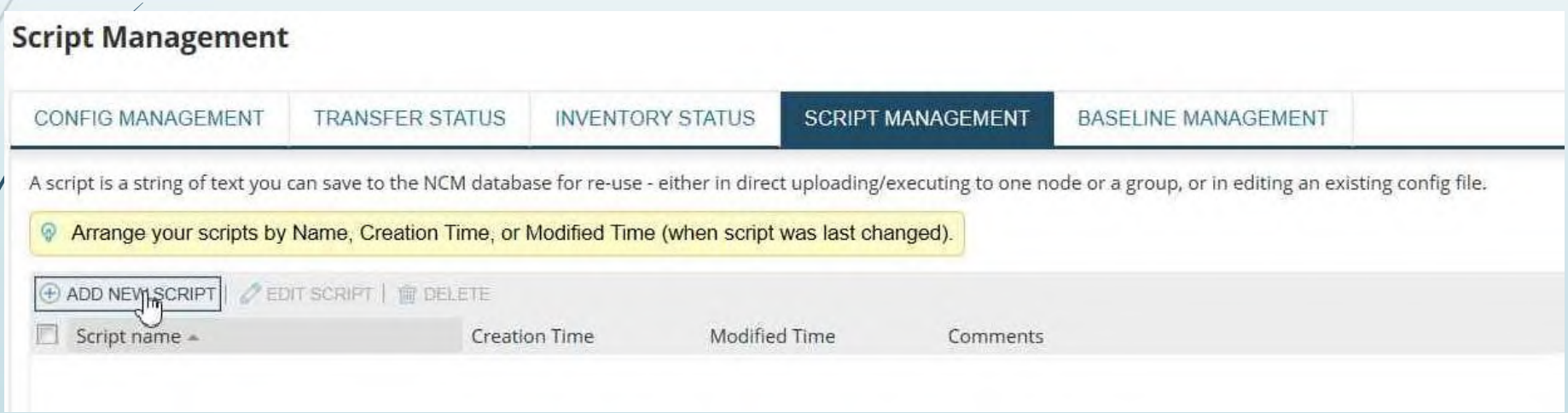



# NCM Script Management

- Push configuration snippets or full configs to devices
  - Compliance Requirements in minutes, not days

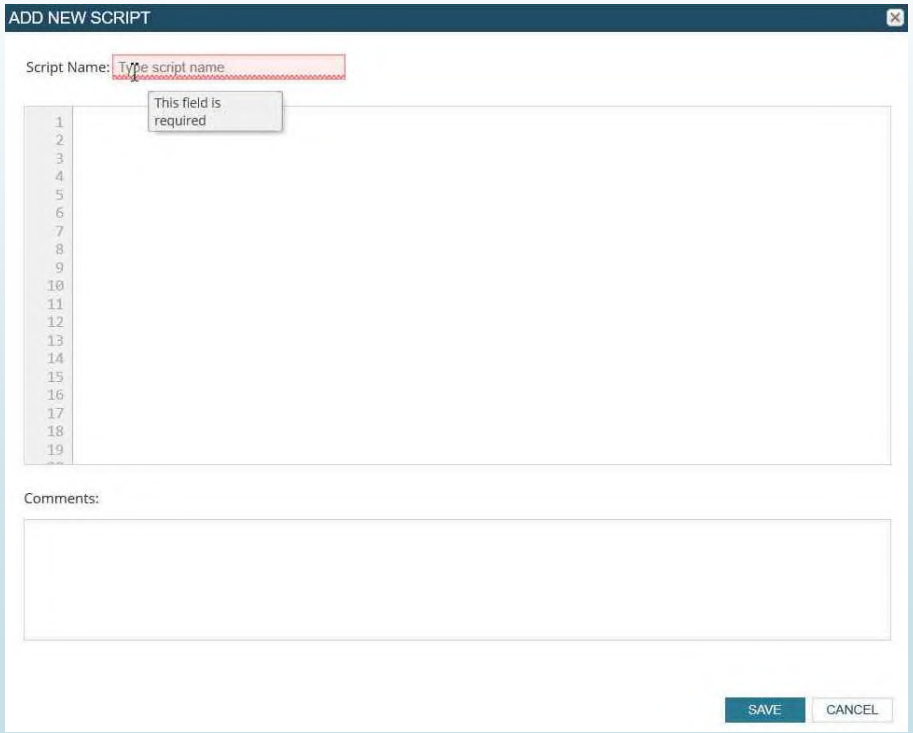
# Script Management

- Adding a new Script



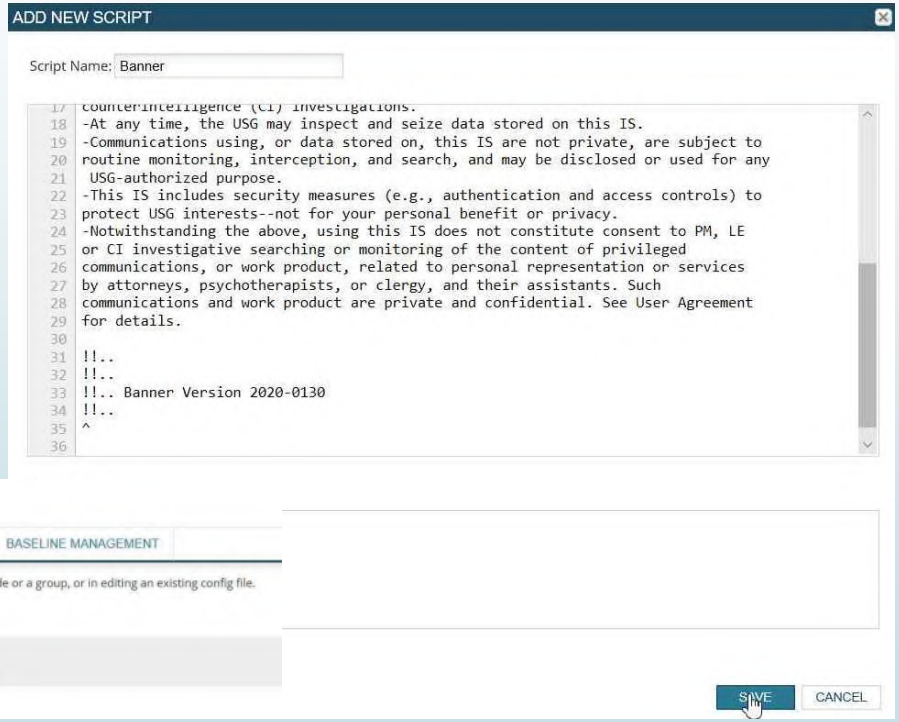
# Script Management

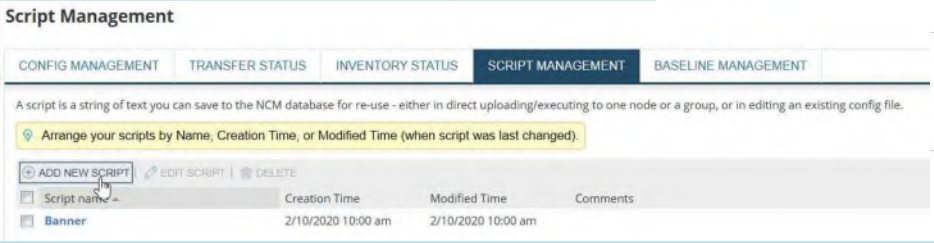
- New Script window operates like a text editor or a CLI for Cisco commands
- Provide Script Name which defines its operation
- Provide comments at the bottom to define which device set in which this script applies



# Script Management

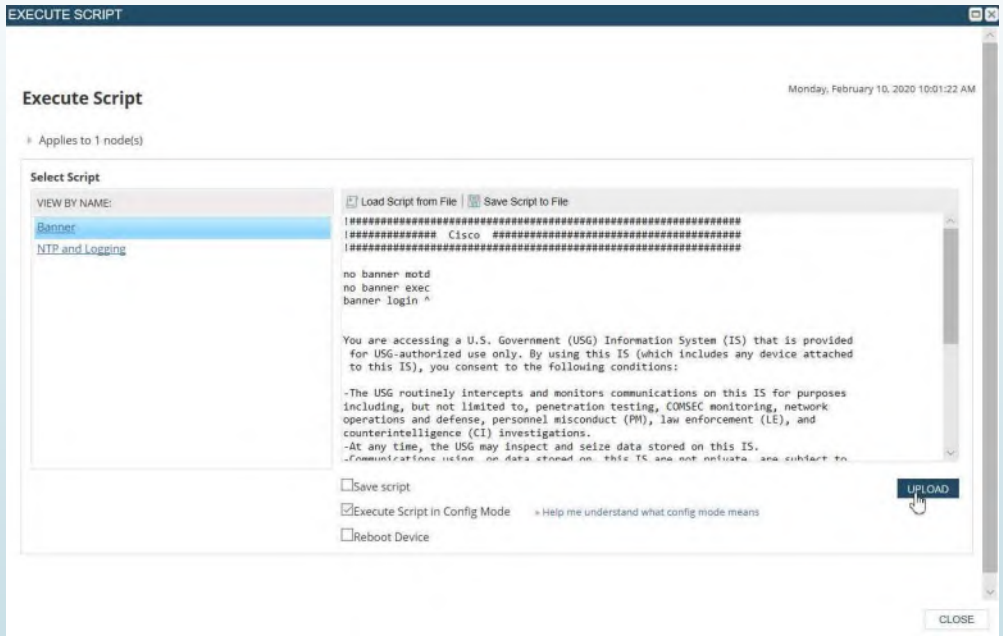
- Script to configure a banner for the devices



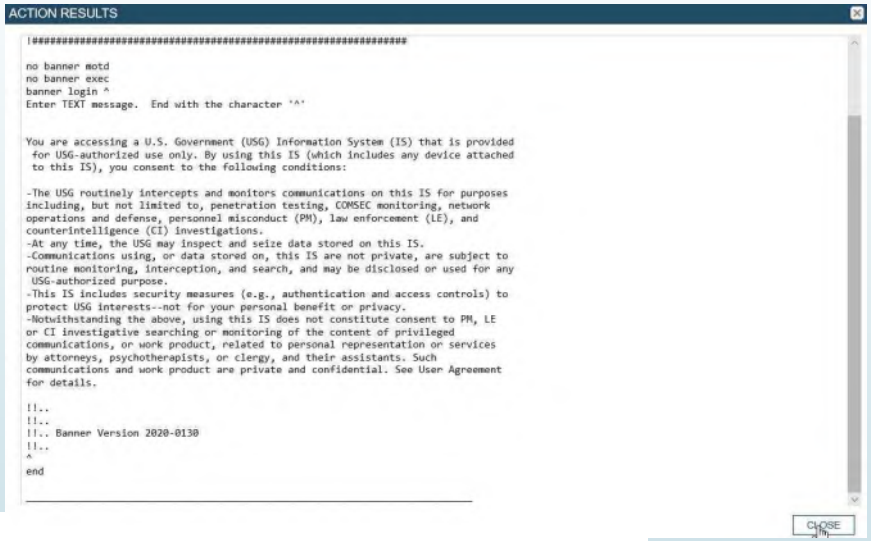
# Script Management

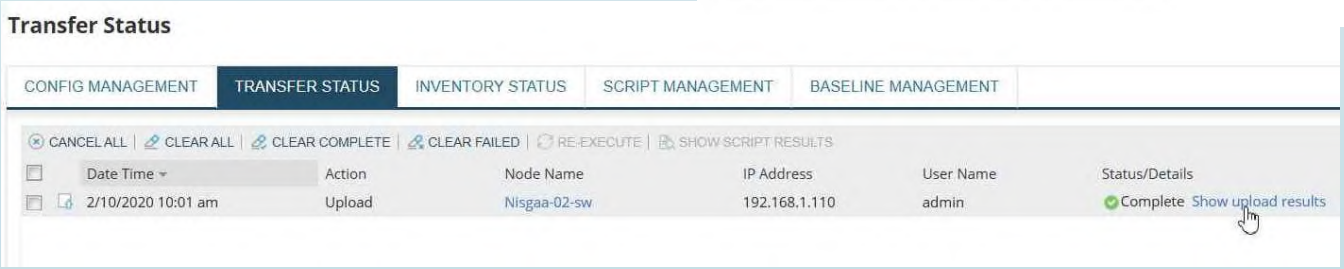
- Loading script
  - Be sure to execute in config mode if the command ***config t*** was not provided in the script



# Script Management

- View the results of your configuration upload
- Look for any errors in your CLI code
- Some configurations will take longer to upload than others



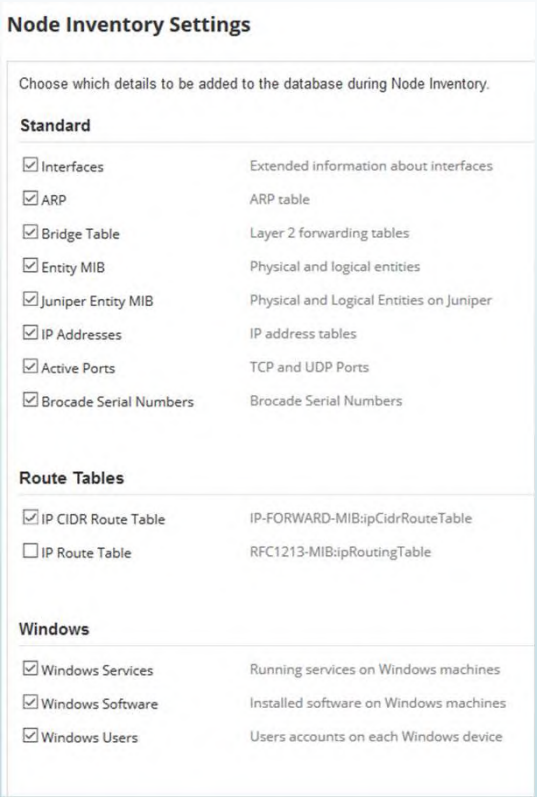



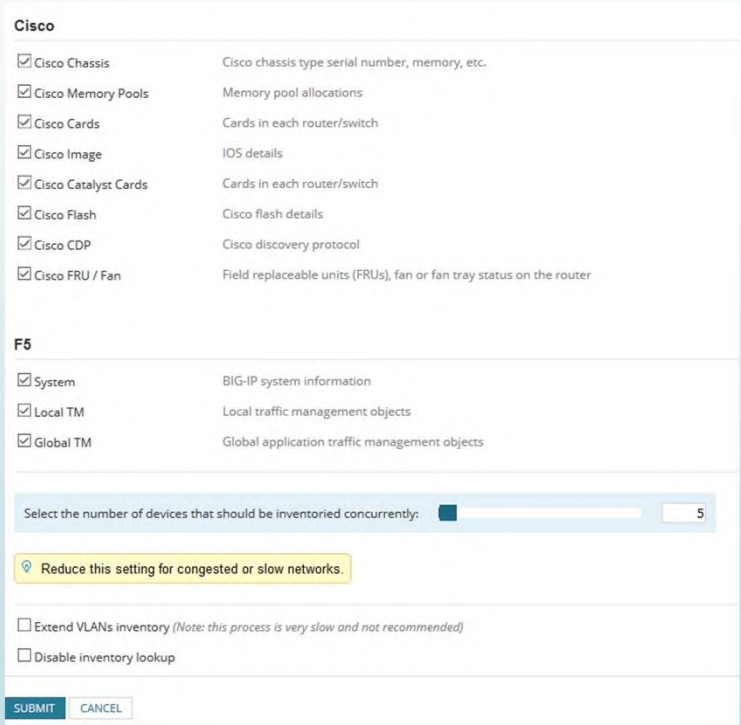
- Script Management
  - Develop NTP Script
  - Develop Services Script
  - Develop Logging Script
  - Develop Banner Script
  - Develop SNMPv3

# DEMO & LAB 11

# Inventory

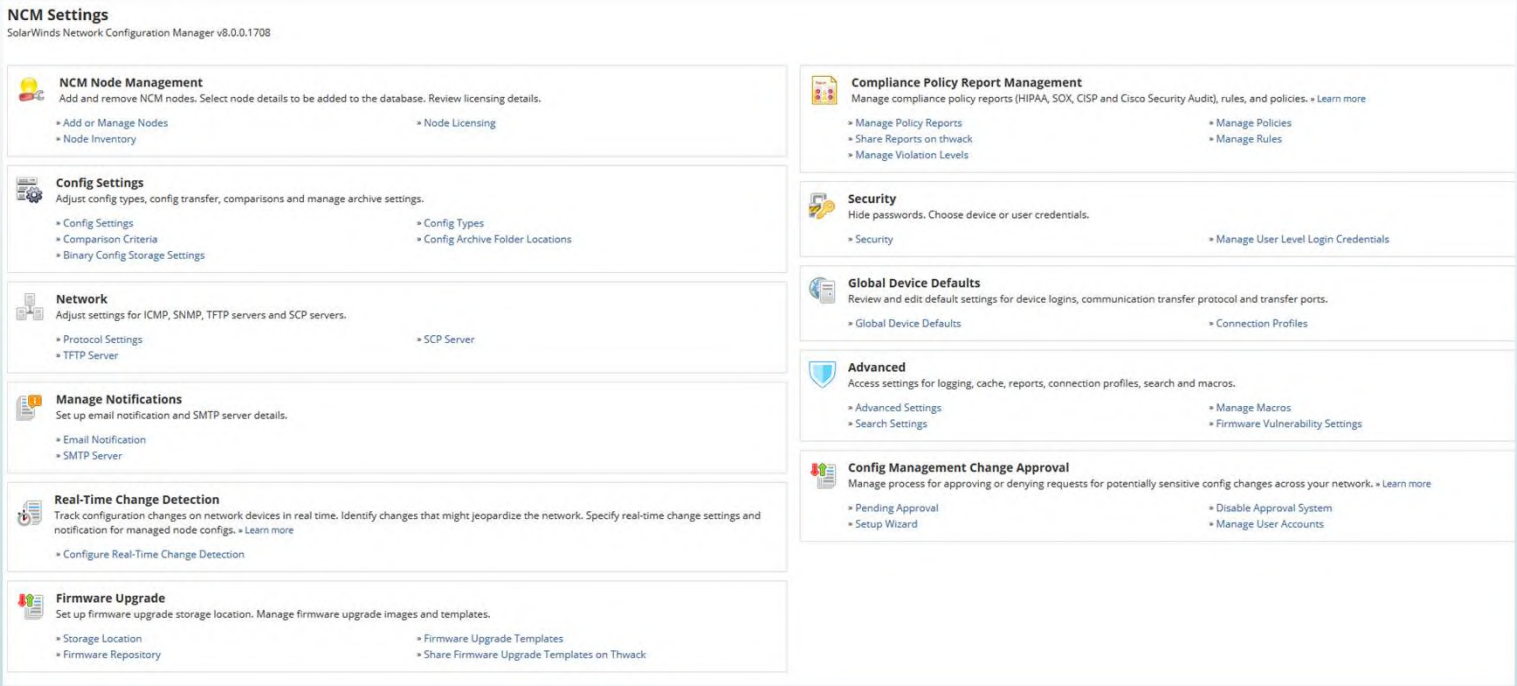
- Data is obtained through SNMP Polling
- Runs via On-Demand or Scheduled Job
- May take awhile to complete



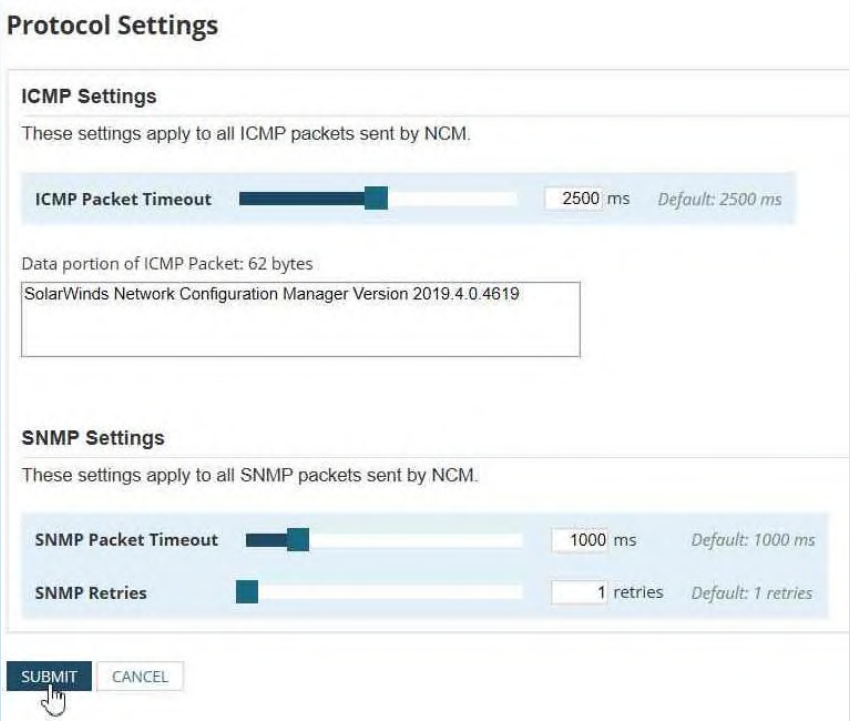
# NCM Settings

- Where to find NCM configurations?



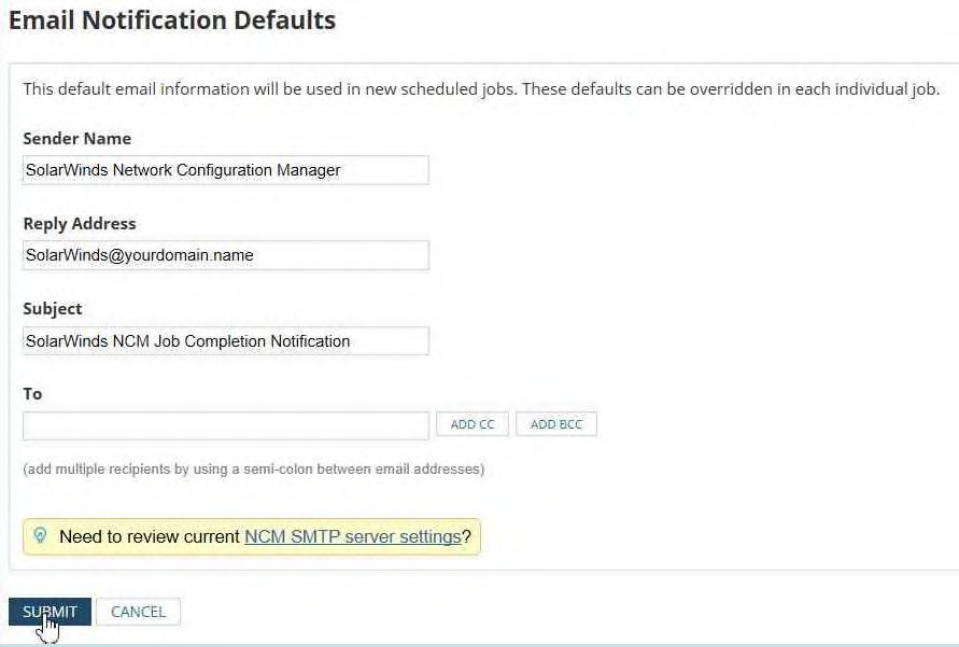
# NCM Settings

- Protocol Settings
  - If all devices are local to the base, consider reducing ICMP Timeout from 2500ms to 500ms for faster response
- SNMP Settings
  - If all devices are local to the base, consider reducing SNMP Timeout from 1000ms to 500ms for faster response



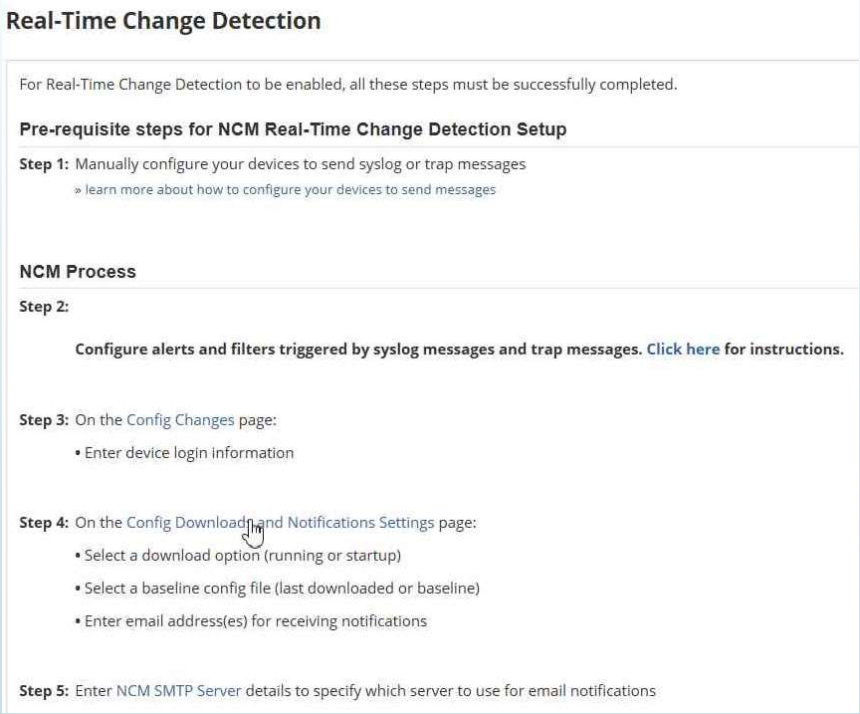
# NCM Settings

- Email configuration settings for alerts, reports, and other monitoring functions
- Consult local policy and AFNet policies for this option
- SolarWinds server will need to be able to send emails to other users



# NCM Settings

- Real-Time Change Detection for networking devices a possibility but will require the SolarWinds server to send emails and a job configured to accommodate feature

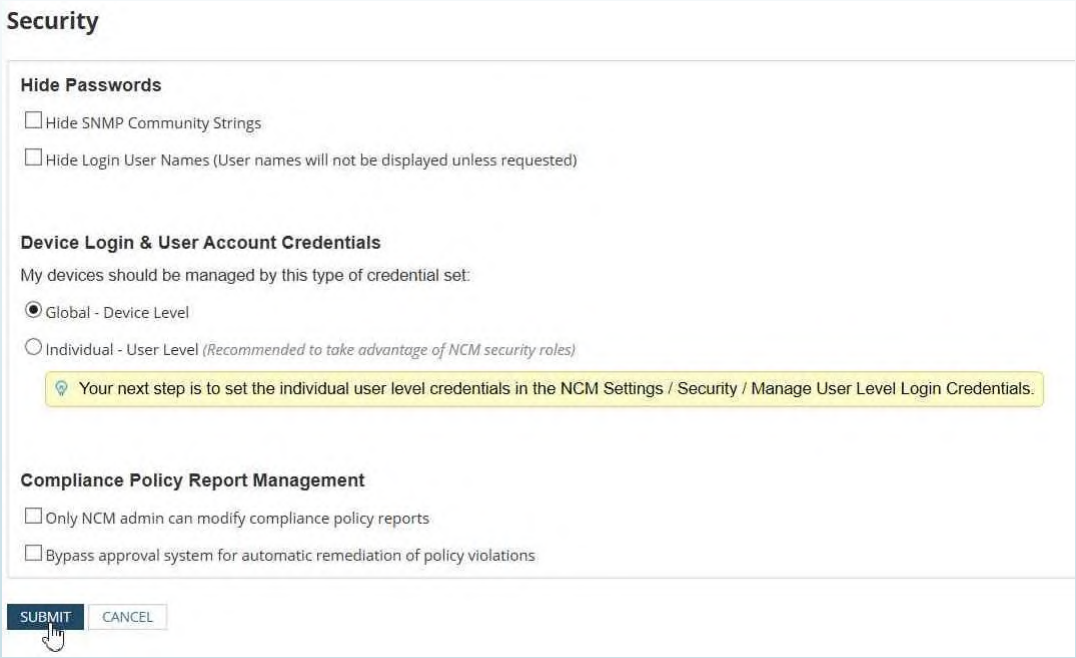


# NCM Settings

- Manage Violation Levels
  - Using this feature for STIG Compliance
  - Color coding of notification icons

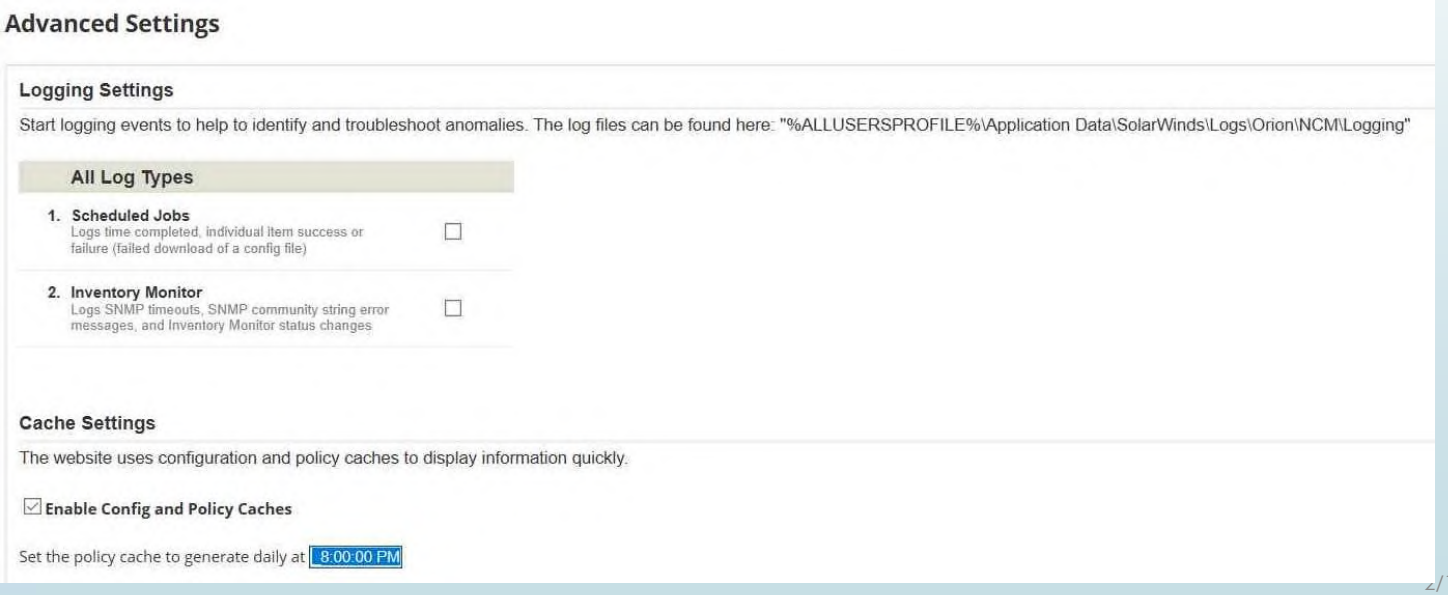
# NCM Settings

- Security Features
  - Hide Passwords
  - Credentials
  - Compliance Management



# NCM Settings

- Cache Settings – Here is where we can modify the time of the nightly audit. We will change this time from 11:55pm to 8:00pm



# NCM Settings

- EOS is not applicable in our environment; we are going to leave this timing as is.

**Reports Settings**

Inventory Reports use sorting settings to display information quickly. Choose which sorting to use, from the options below:

◉ All columns ○ A single column

**Connection Profile Settings**

☐ **Use auto-detect when assigned connection profile cannot be used for NCM operation**

**EOS Settings**

☑ **Enable EOS autorun**

Run EOS at 2:15:00 AM

- Inventory Walkthrough
- NCM Settings Modifications
  - Violation Levels
  - Connection Profiles

# DEMO & LAB 12

# NCM Device Templates

- Communicates to NCM which CLI command to run against devices
- Templates determined by System OID through SNMP Polling
  - NCM will apply exact or closest match to the OID

DEVICE TEMPLATES MANAGEMENT | SHARED TEMPLATES ON THWACK

ADD NEW | COPY | EDIT | DELETE | ENABLE/DISABLE AUTO-DETECT | IMPORT | EXPORT AS FILE | EXPORT TO THWACK

| Name | System OID | Use for auto-detect | Comments | Author |
|---|---|---|---|---|
| Cisco CSS 11501 | 1.3.6.1.4.1.9.9.368.4.7 | Yes | | SolarWinds |
| Cisco IOS | 1.3.6.1.4.1.9 | Yes | | SolarWinds |
| Cisco IOS2505 | 1.3.6.1.4.1.9.1.21 | Yes | | SolarWinds |
| Cisco IronPort | 1.3.6.1.4.1.15497.1.1.1 | Yes | | SolarWinds |
| Cisco Pix Firewall | 1.3.6.1.4.1.9.1.227 | Yes | | SolarWinds |
| Cisco Pix Firewall 501 | 1.3.6.1.4.1.9.1.417 | Yes | | SolarWinds |
| Cisco Pix Firewall 506 | 1.3.6.1.4.1.9.1.389 | Yes | | SolarWinds |
| Cisco Pix Firewall 506E | 1.3.6.1.4.1.9.1.450 | Yes | | SolarWinds |
| Cisco Pix Firewall 515 | 1.3.6.1.4.1.9.1.390 | Yes | | SolarWinds |
| Cisco Pix Firewall 515E | 1.3.6.1.4.1.9.1.451 | Yes | | SolarWinds |
| Cisco Pix Firewall 520 | 1.3.6.1.4.1.9.1.391 | Yes | | SolarWinds |
| Cisco Pix Firewall 525 | 1.3.6.1.4.1.9.1.392 | Yes | | SolarWinds |
| Cisco Pix Firewall 535 | 1.3.6.1.4.1.9.1.393 | Yes | | SolarWinds |
| Cisco VPN concentrator | 1.3.6.1.4.1.3076 | Yes | | SolarWinds |
| Cisco WLC | 1.3.6.1.4.1.14179 | Yes | | SolarWinds |
| Dell PowerConnect Switch | 1.3.6.1.4.1.674.10895.3 | Yes | | SolarWinds |
| Dell PowerConnect Switch | 1.3.6.1.4.1.674.10895.3006 | Yes | | SolarWinds |
| Dell PowerConnect Switch | 1.3.6.1.4.1.674.10895 | Yes | | SolarWinds |
| Enterasys Cabletron SmartSwitch Rout... | 1.3.6.1.4.1.52.3.9.20.1.4 | Yes | | SolarWinds |
| Enterasys Cabletron SmartSwitch Rout... | 1.3.6.1.4.1.52.3.9.20.1.5 | Yes | | SolarWinds |
| Enterasys Cabletron SmartSwitch Rout... | 1.3.6.1.4.1.52.3.9.20.1.3 | Yes | | SolarWinds |
| Extreme | 1.3.6.1.4.1.1916 | Yes | | SolarWinds |

Page 2 of 4 | Page size 25

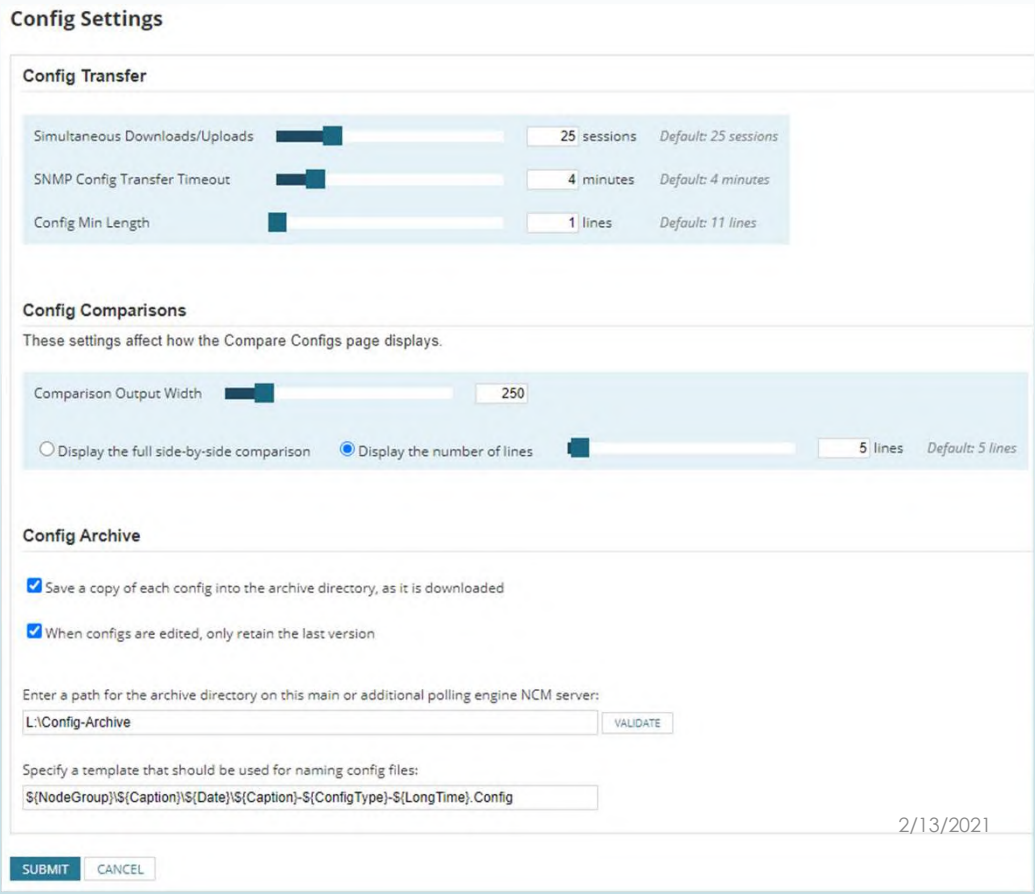
**NODE & GROUP MANAGEMENT**

Manage and delete nodes, dependencies and groups. Edit node properties.

- » Manage Nodes
- » Manage Groups
- » Manage Pollers
- » Manage Hardware Sensors
- » Manage Virtual Devices
- » Manage Agents
- » Manage World Map
- » Manage Container Services
- » Manage Dependencies
- » Manage Custom Properties
- » Manage Device Templates
- » Manage Orion Maps

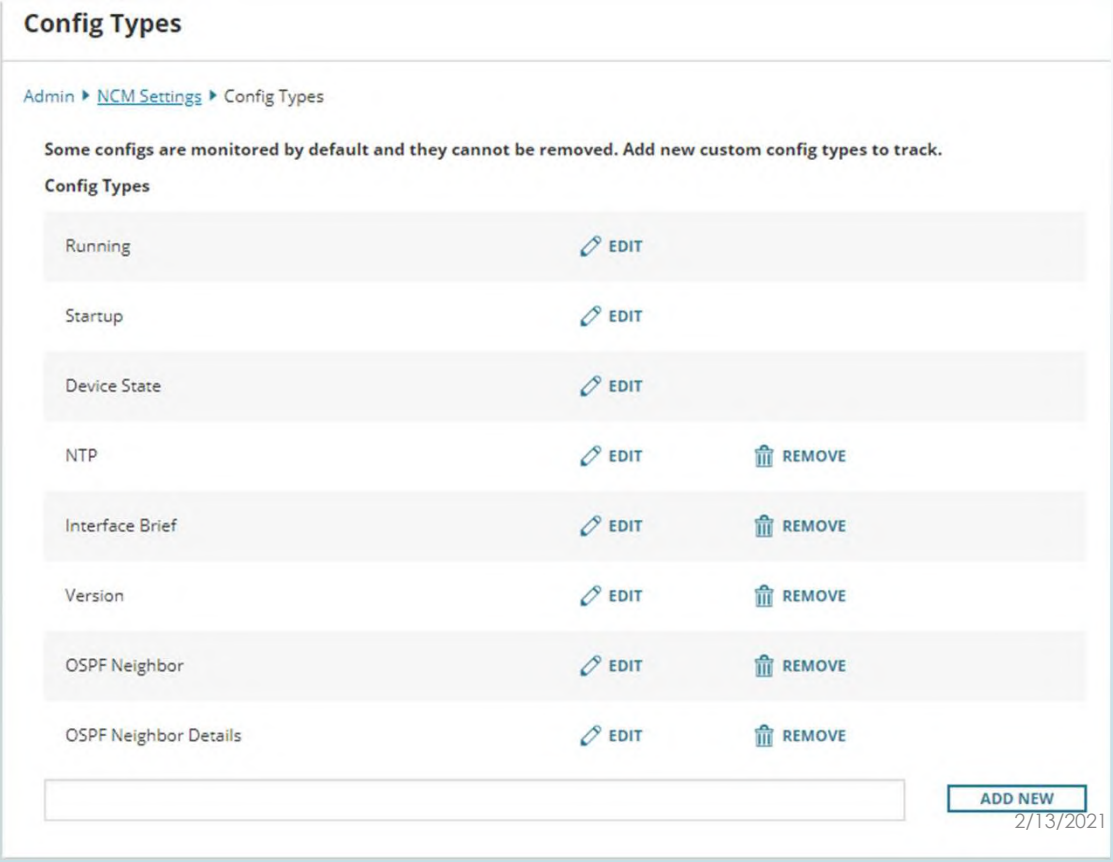
# Device Templates - Settings

- NCM Config Settings
  - Allows the changing of Config Transfers and Comparisons
  - Allows Config-Archive folder to be changed to a shared drive off of the Core (main) SolarWinds Server
  - Validates the archive directory folder to ensure reachability



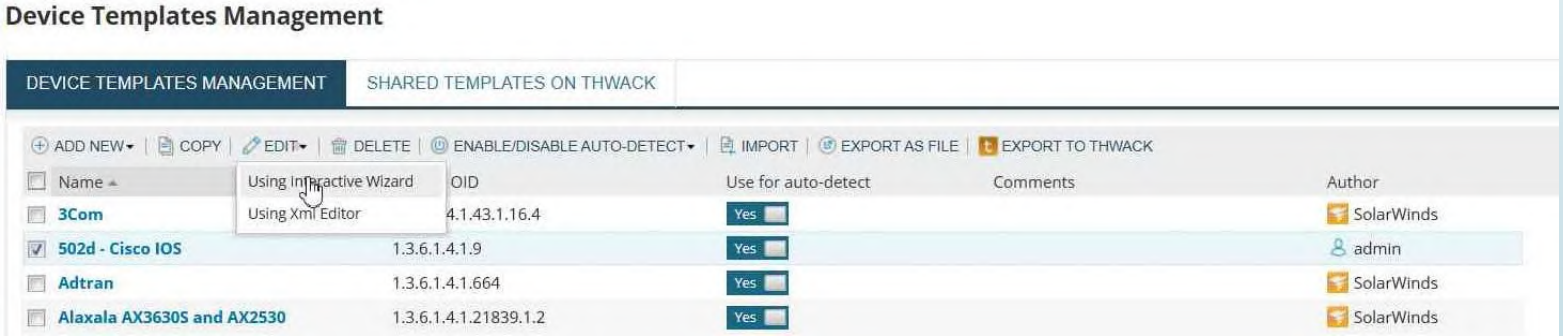
# Device Templates - Settings

- NCM Config Types
  - Allows the adding of custom config types
  - Config types can be used to add to the Device Templates



# Device Templates

- Always copy the Template provided
- Rename new Template with Unit #
- Two options for editing and modification of templates.
  - Using Interactive Wizard
  - Using XML Editor

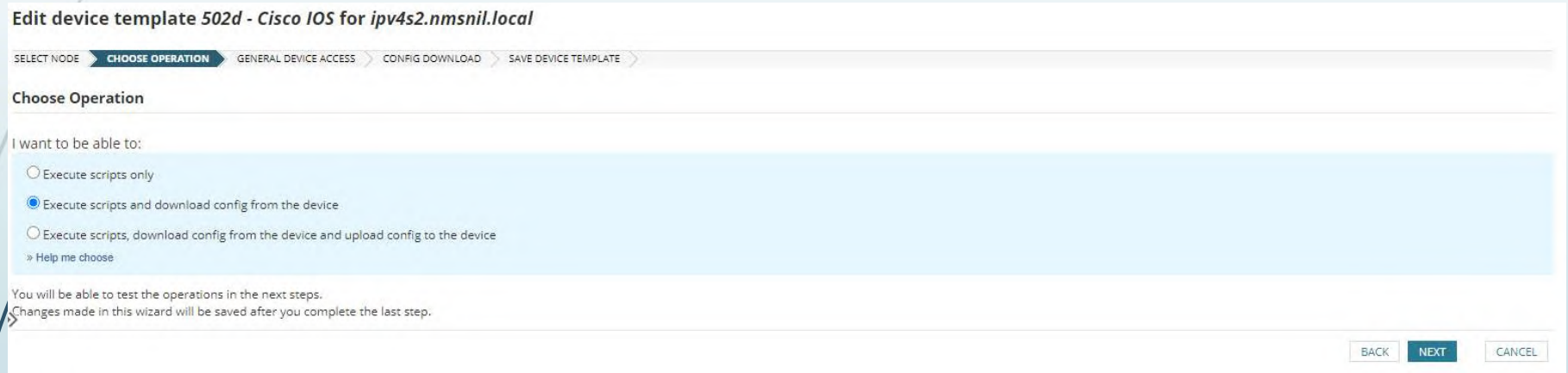


# Device Templates

- Interactive Wizard

# Device Templates

- Interactive Wizard



# Device Templates

- Interactive Wizard
  - Connection Profile

**Edit device template *502d - Cisco IOS* for *ipv4s2.nmsnil.local***

SELECT NODE > CHOOSE OPERATION > **GENERAL DEVICE ACCESS** > CONFIG DOWNLOAD > SAVE DEVICE TEMPLATE

**General Device Access**

Connection Profile

| | |
|---|---|
| Global Connection Profile: | Admin |
| Login Credentials: | Device |
| Username: | Admin |
| Password: | •••••••••• |
| Enable Level: | <No Enable Login> |
| Enable Password: | |
| Execute Scripts Using: | SSH2 |
| Request Configs Using: | SSH2 |
| Transfer Configs Using: | SSH2 |
| Telnet Port: | 23 |
| SSH Port: | 22 |

Device Template

| | |
|---|---|
| Reset Terminal Size Command | terminal width 0${CRLF}terminal length 0 |
| | *Enter command to turn off paging (more prompt) on device. Multiple commands can be separated by ${CRLF} macro* |
| Show Version Command: | show version |
| | *Multiple commands can be separated by ${CRLF} macro* |

Show advanced options

Test Device Access: TEST » What does this test validate?

Test Successful!

Show credential login details

# Device Templates

- Interactive Wizard
  - Config Downloads and Config Types

**Edit device template *502d - Cisco IOS* for *ipv4s2.nmsnil.local***

SELECT NODE > CHOOSE OPERATION > GENERAL DEVICE ACCESS > CONFIG DOWNLOAD > CONFIG UPLOAD > SAVE DEVICE TEMPLATE

**Config Download**

Download Command

Enter the command for downloading a config from this device.

Download Config Command: Show ${ConfigType}

SHOW MACRO VALUES

*For example: show ${ConfigType}*

**Available Macros:**
${ConfigType} - determine type of config to download

Config Types

Manage Config Types

Enter a name for each type of config file type than NCM should be able to download from this device.

| | | |
|---|---|---|
| Running Config File Name: | running | Is binary config |
| Startup Config File Name: | startup | Is binary config |
| NTP Status Config File Name: | ntp status | Is binary config |
| SNMP User Config File Name: | snmp user | Is binary config |
| Interface Brief Config File Name: | ip interface brief | Is binary config |

Download Test

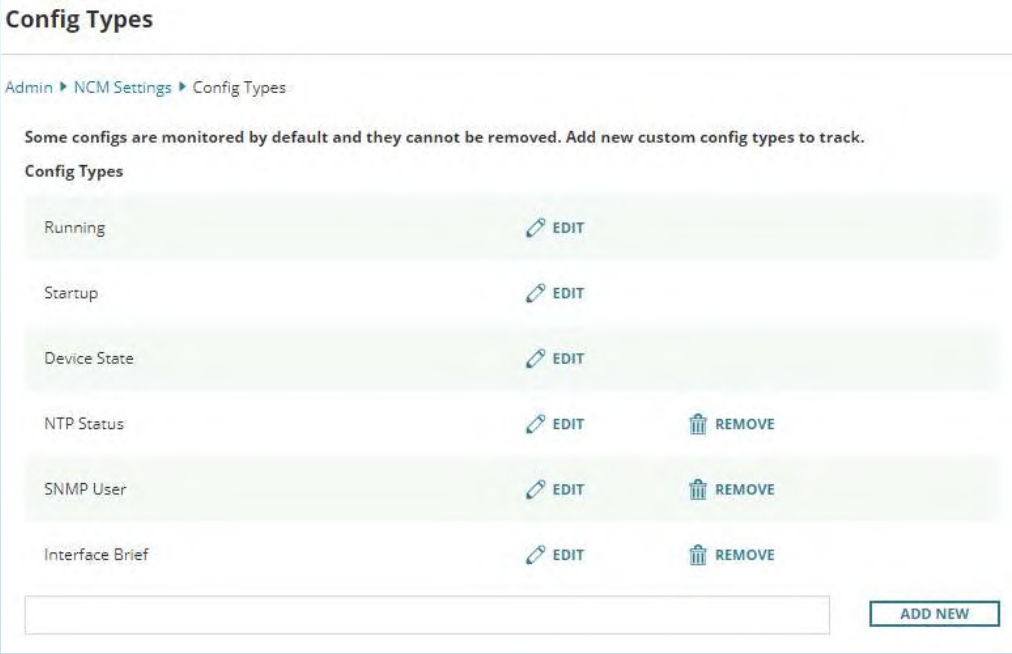
Download a config file to test the download config command. If the download is successful, the command is correct.

Select Config Type to Download: Running PERFORM DOWNLOAD TEST

BACK NEXT CANCEL

# Device Templates

- Adding NTP and Interface Brief to support added XML code



# Device Templates

- Interactive Wizard
  - Config Uploads

**Edit device template *502d - Cisco IOS* for *ipv4s2.nmsnil.local***

SELECT NODE > CHOOSE OPERATION > GENERAL DEVICE ACCESS > CONFIG DOWNLOAD > **CONFIG UPLOAD** > SAVE DEVICE TEMPLATE

**Config Upload**

Upload Options

| | |
|---|---|
| Enter Config Mode Command: | config terminal |
| Exit Config Mode Command: | end |
| Write to NVRAM Command: | write memory |
| Reboot Command: | reload${CRLF}y${CRLF}y |

Upload Command

| | |
|---|---|
| Upload Config Command: | ${EnterConfigMode}${CRLF}${ConfigText}${CRLF}${ExitConfigMode} |

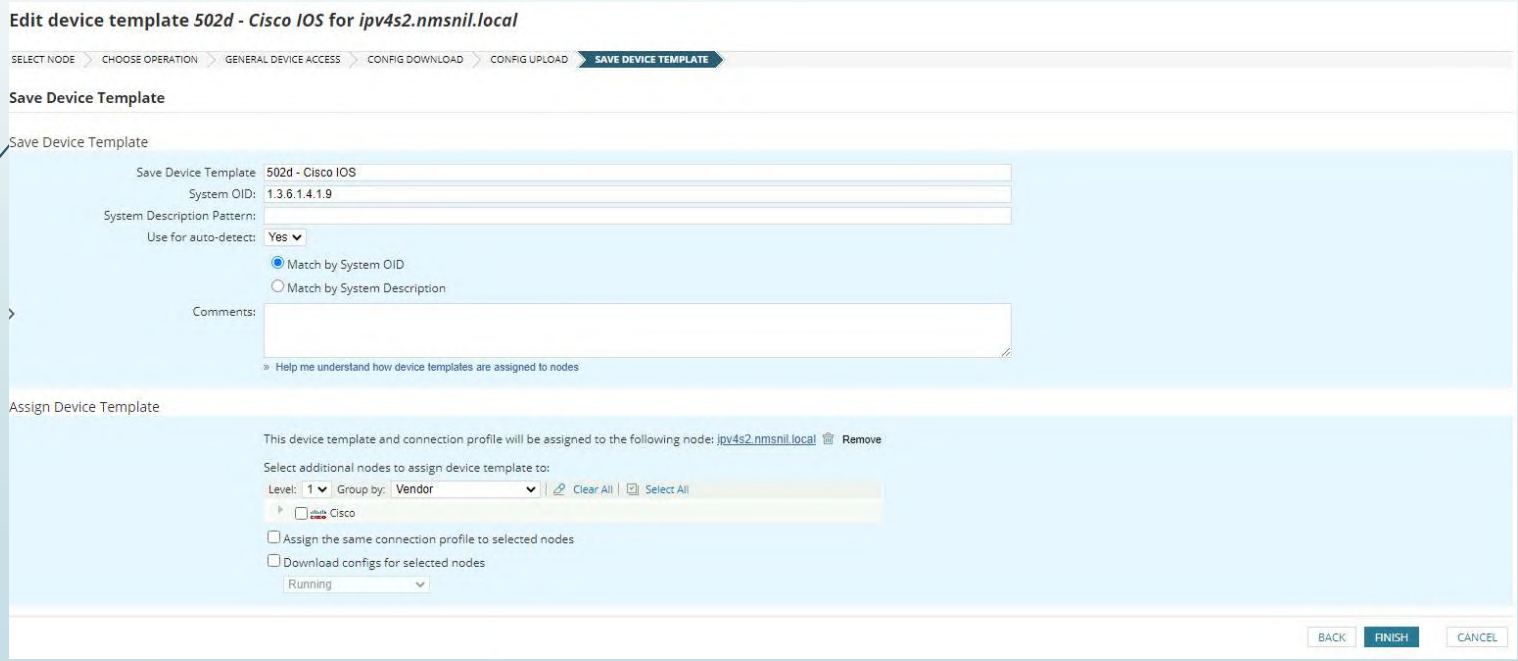
*For example: ${EnterConfigMode}${CRLF}${ConfigText}${CRLF}${ExitConfigMode}*

**Available Macros:**
${ConfigText} - text of config to upload
${EnterConfigMode} - command to enter into config mode
${ExitConfigMode} - command to exit from config mode
${CRLF} - use to separate multiple commands or simulate Enter key press

BACK NEXT CANCEL

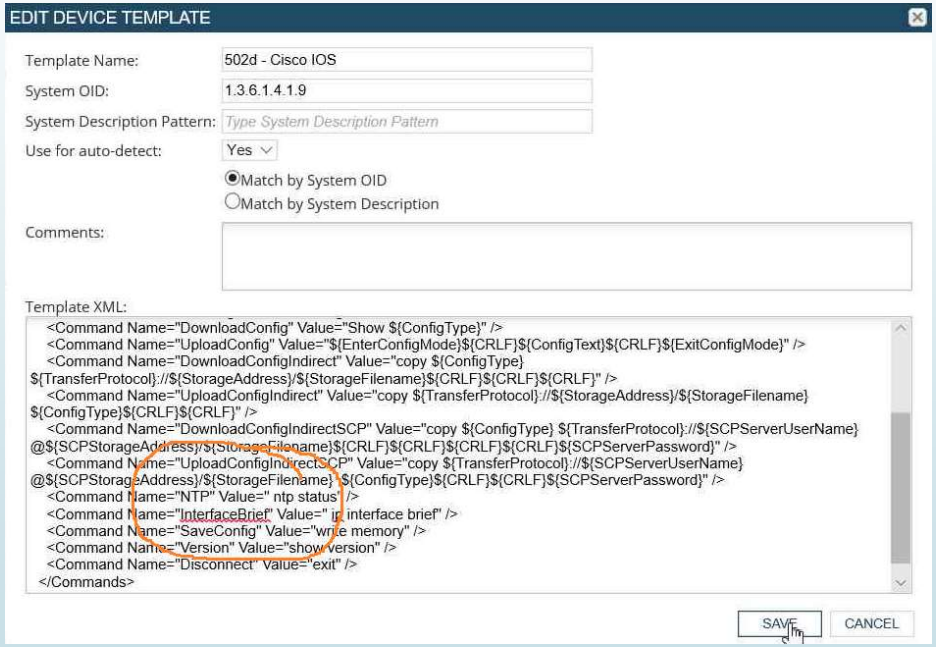
# Device Templates

- Interactive Wizard
  - Template Assignments



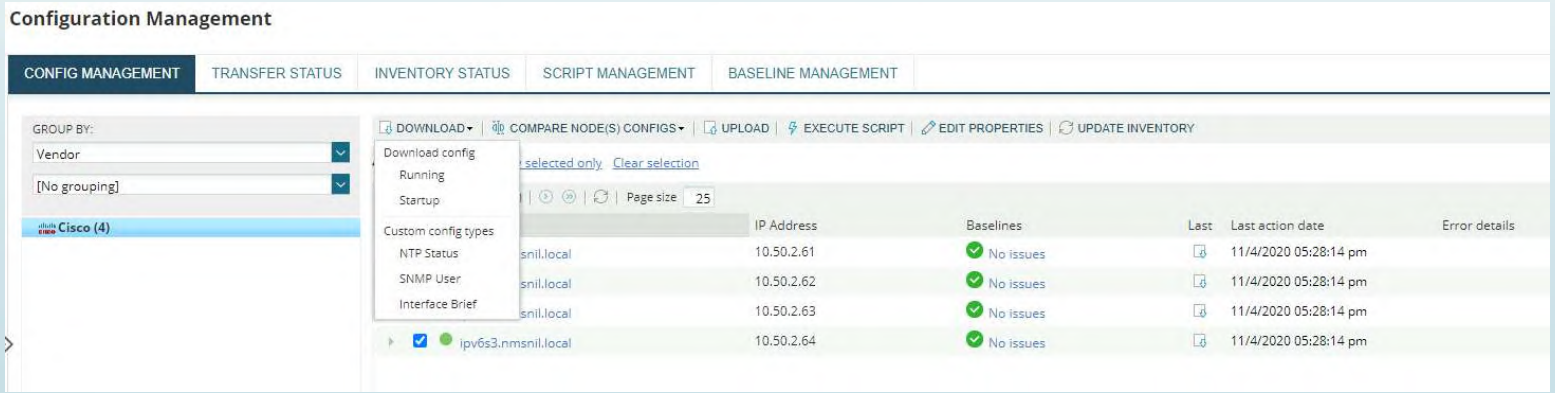
# Device Templates

- XML Editor
  - Modified Template Name
  - Adding xml code to the Template



# Device Templates

- XML Editor
  - Able to download results of ***show ntp status*** command
  - Able to download results of ***show ip interface brief*** command
  - Able to download results of ***show snmp user*** command

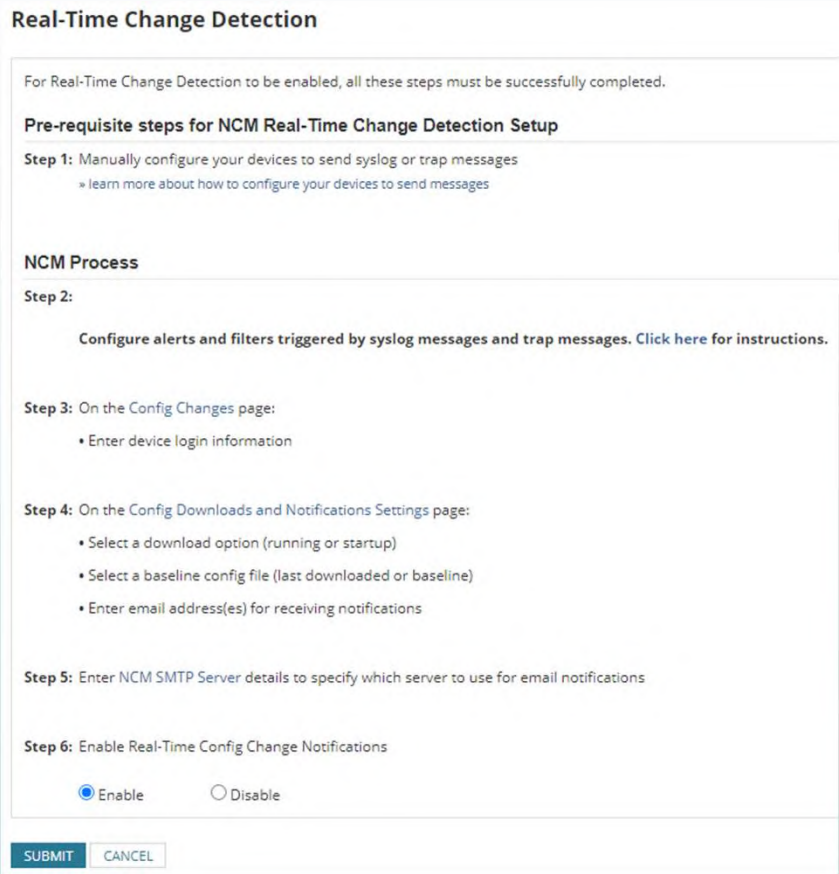


- Device Templates
  - Edit Cisco IOS template to make primary template for organization
  - Add ***show ntp status*** to the template
  - Add ***show ip interface brief*** to the template
  - Add ***show snmp user*** command to template
  - Add ***show logging*** command to template

# DEMO & LAB 13

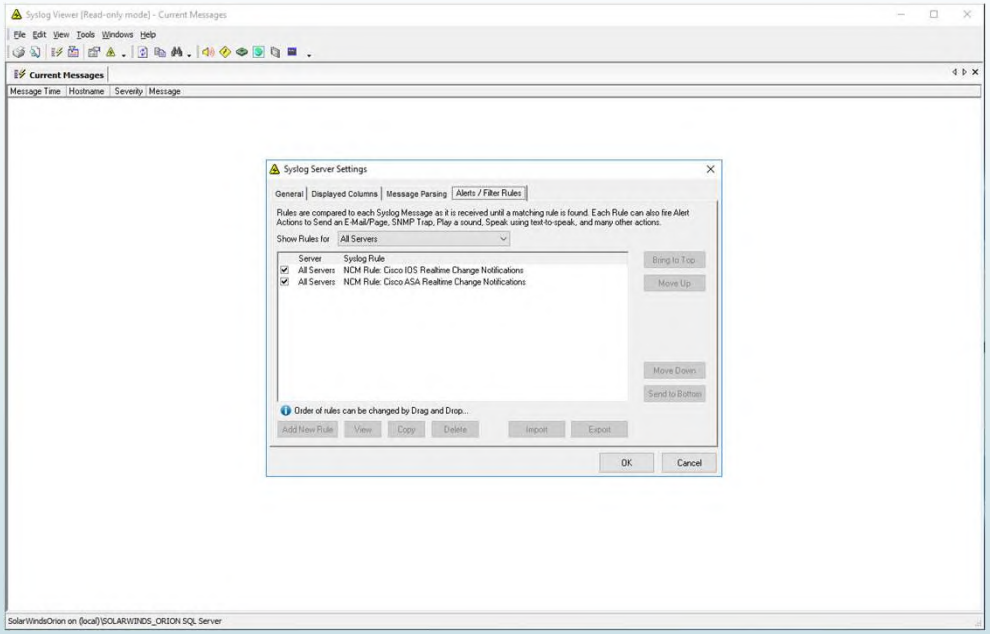
# Real-Time Change Detection

- Enables real-time detection of Config changes
- Assists in tracking down issues from misconfigurations within Network Devices
- Complements troubleshooting in NetPath Services



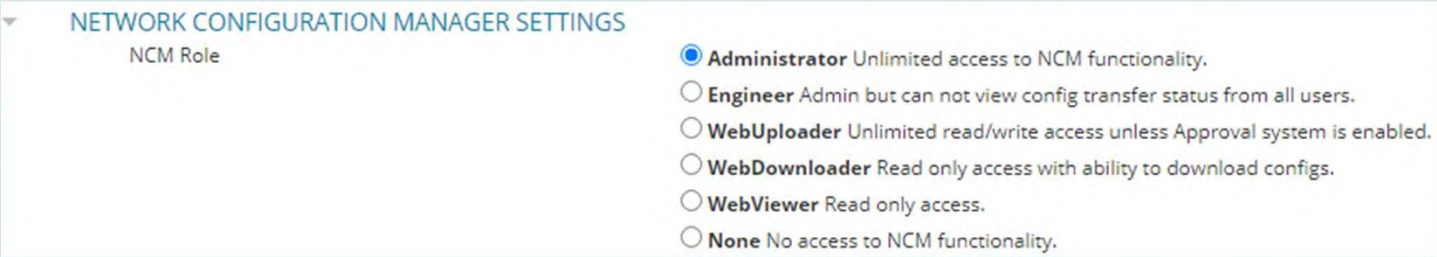
# Real-Time Change Detection

- Syslog Configuration
- Configure devices to send syslogs or traps to the SolarWinds Server
- SolarWinds Syslog Viewer comes with preconfigured rules for Cisco IOS/ASA
- Under View>Alerts/Filter Rules, select the two rules available to enable notifications



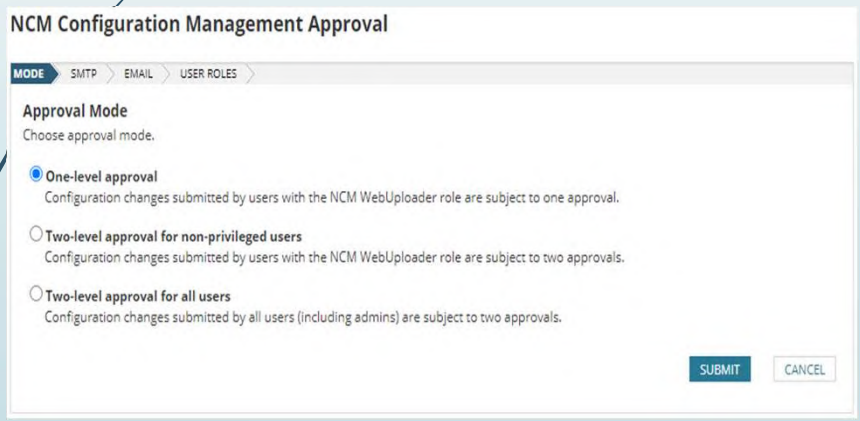
# Change Management Change Approval

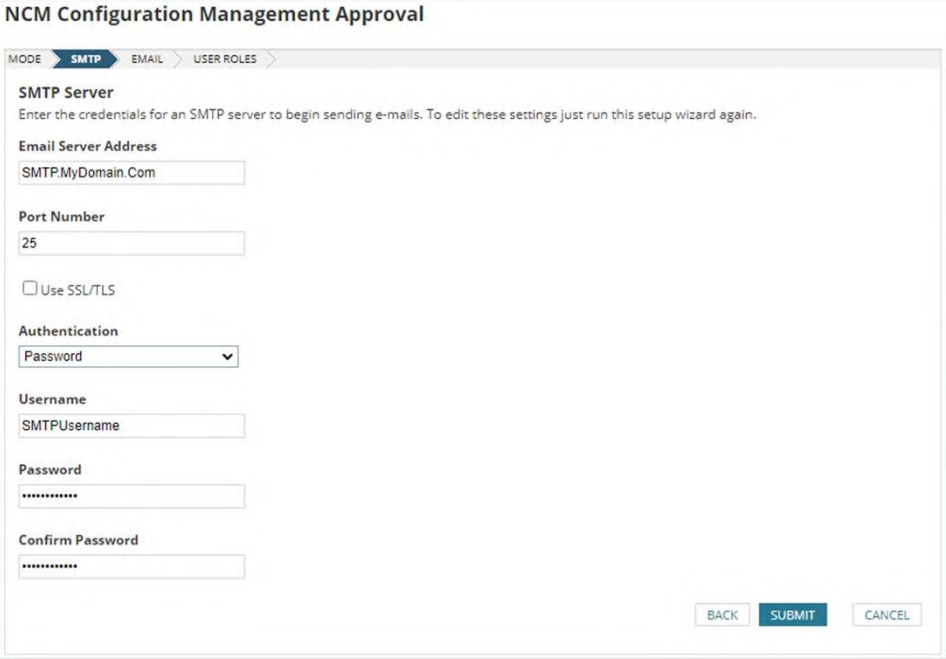
- Config Management Change Approval (CMCA)
  - NCM uses roles for the approval process
    - Administrator
    - Engineer
    - WebUploader
    - WebDownloader
    - WebViewer
    - None



# Change Management Change Approval

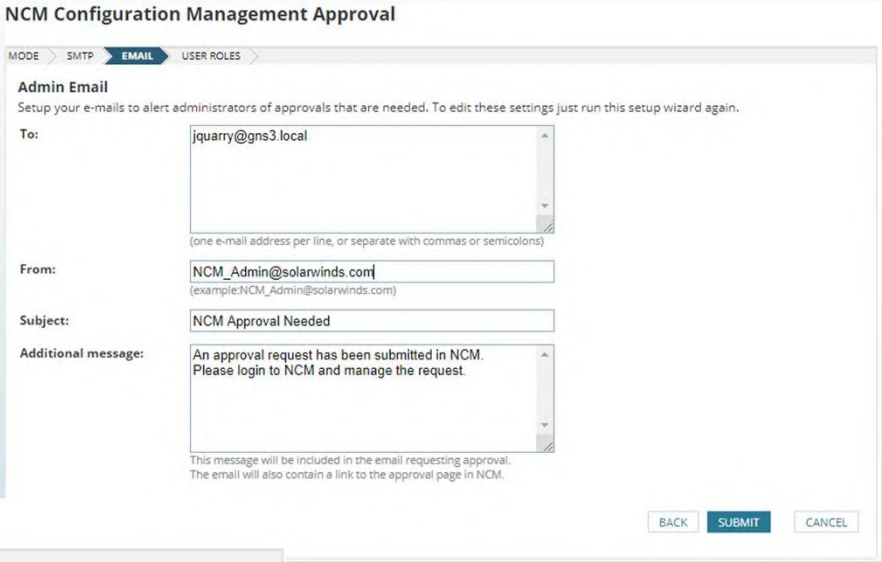
- Config Management Change Approval Setup

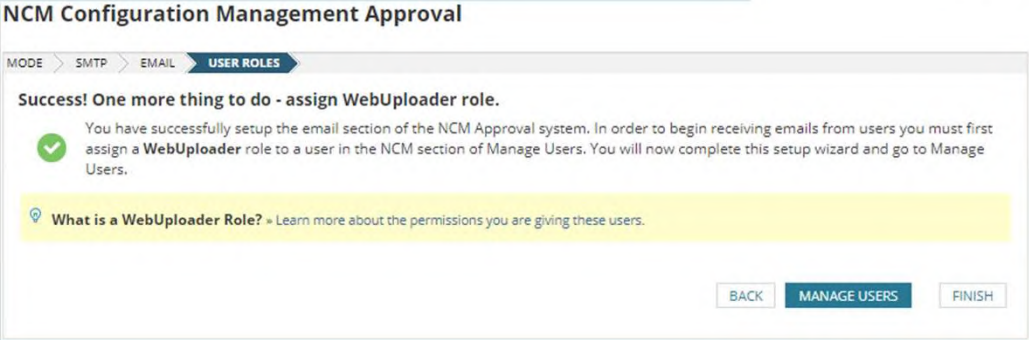


# Change Management Change Approval

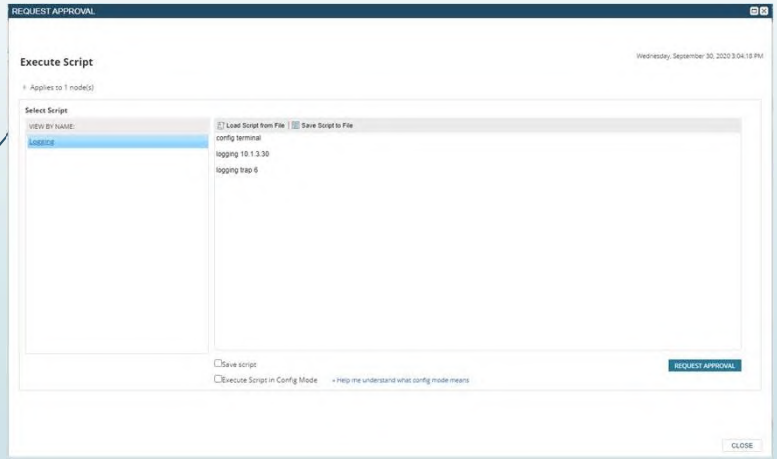
- Config Management Change Approval Setup

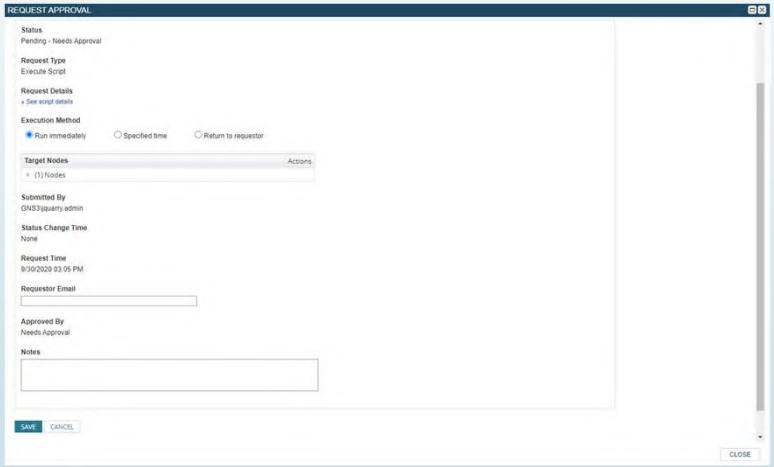


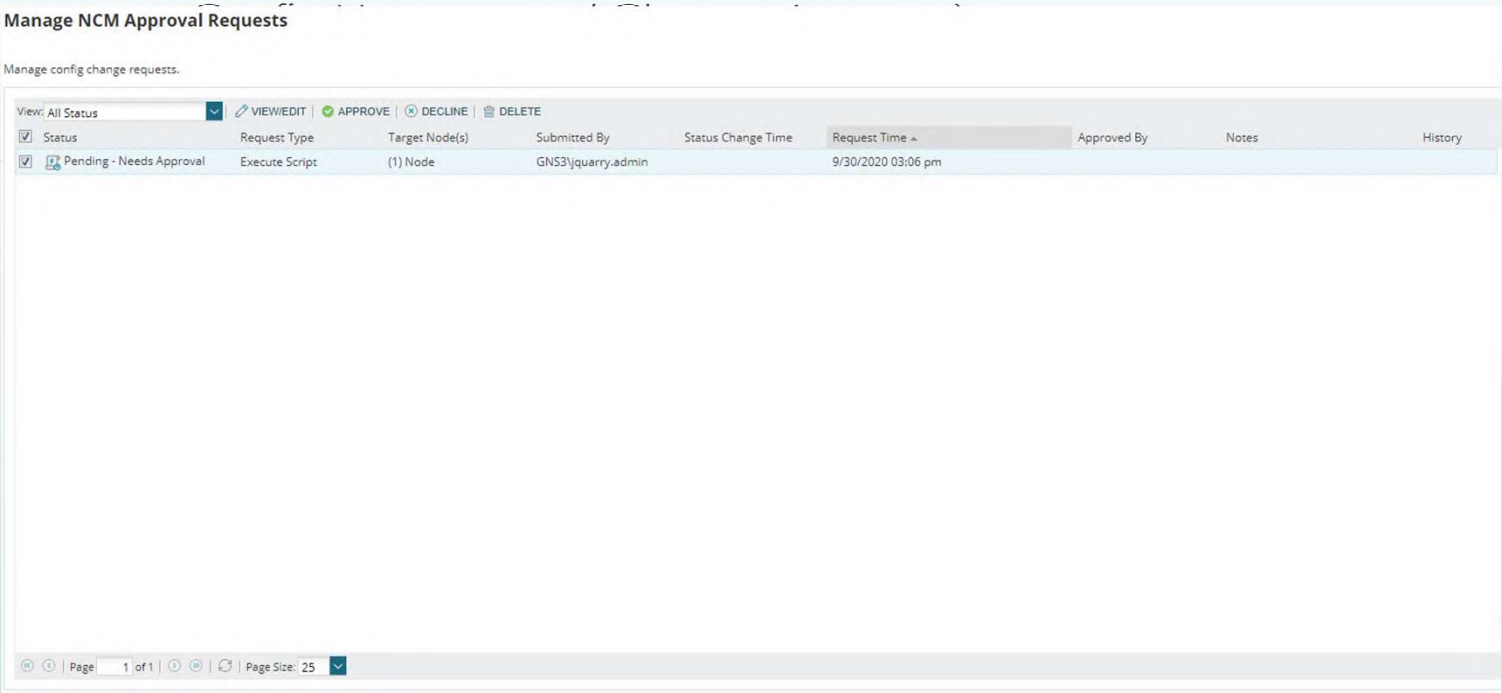
# Change Management Change Approval

- Config Management Change Approval Request



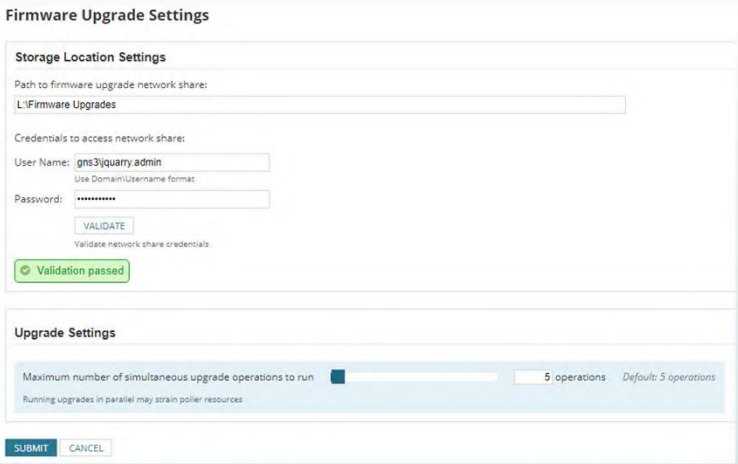



# Change Management Change Approval



# NCM Firmware Upgrade

- Firmware Upgrade
  - Use NCM to upgrade firmware on many devices at once
  - Helps Network Engineers/Administrators distribute security fixes to vulnerable devices
  - Can be configured to have access to the storage location of the firmware



# NCM Firmware Upgrade

- Use upgrade templates to make upgrade process easier
- Templates define device specific commands used to upgrade the firmware
- Default templates have been provided and the creation of new templates is available

**Firmware Upgrade Templates**

FIRMWARE UPGRADE TEMPLATES | SHARED FIRMWARE UPGRADE TEMPLATES ON THWACK

ADD | EDIT | IMPORT | EXPORT AS FILE | EXPORT TO THWACK | DELETE

| Name | Last Modified | Description | Author |
|---|---|---|---|
| Cisco ASA 5512 Multi Context Mode | 7/8/2020 02:23 pm | Upgrade template for Cisco ASA 5512 run in multiple contexts mode. | SolarWinds |
| Cisco ASA 5512 Single Context Mode | 7/8/2020 02:23 pm | Upgrade template for Cisco ASA 5512 run in single context mode. | SolarWinds |
| Cisco Catalyst 2960 | 7/8/2020 02:23 pm | Upgrade template for Cisco Catalyst 2960. | SolarWinds |
| Cisco Catalyst 3560 | 7/8/2020 02:23 pm | Upgrade template for Cisco Catalyst 3560. | SolarWinds |
| Cisco Catalyst 3750 | 7/8/2020 02:23 pm | Upgrade template for Cisco Catalyst 3750. This template does not support upgrade of ... | SolarWinds |
| Cisco Catalyst 3850 | 7/8/2020 02:23 pm | Upgrade template for Cisco Catalyst 3850. This template does not support upgrade of ... | SolarWinds |
| Cisco IOS Software 2800/2801 | 7/8/2020 02:23 pm | Upgrade template for Cisco 2800/2801 series. | SolarWinds |
| Cisco IOS Software 2921 | 7/8/2020 02:23 pm | Upgrade template for Cisco IOS Software 2921. | SolarWinds |
| Cisco Nexus 5548 | 7/8/2020 02:23 pm | Upgrade template for Nexus 5548 devices. Run disruptive firmware upgrade using ISSU. | SolarWinds |
| Cisco Nexus C7004 - ISSU | 7/8/2020 02:23 pm | Upgrade template for Nexus C7004 devices. Run disruptive firmware upgrade using IS... | SolarWinds |
| Cisco Nexus C7004 - Traditional | 7/8/2020 02:23 pm | Upgrade template for Nexus C7004. Run traditional firmware upgrade. | SolarWinds |
| EtherWAN | 7/8/2020 02:23 pm | Upgrade template for EtherWAN devices | SolarWinds |
| Juniper j2320 Junos | 7/8/2020 02:23 pm | Upgrade template for Juniper j2320 Junos devices | SolarWinds |
| Lenovo Campus NOS | 7/8/2020 02:23 pm | Upgrade template for Lenovo Campus NOS switches. | SolarWinds |
| Lenovo RackSwitch CNOS version 10.7 and new... | 7/8/2020 02:23 pm | Upgrade template for Lenovo RackSwitch devices with CNOS version 10.7 and newer. | SolarWinds |
| Lenovo RackSwitch CNOS versions before 10.7 | 7/8/2020 02:23 pm | Upgrade template for Lenovo RackSwitch devices with CNOS versions before 10.7. | SolarWinds |

# NCM Firmware Upgrade

- Firmware Upgrade Templates

**UPGRADE OPTIONS**

- [x] Save config to NVRAM before upgrade
- [x] Backup running and startup configs before upgrade
- [x] Verify backed up firmware image integrity
- [x] Verify uploaded firmware image integrity
- [x] Update boot variable
- [ ] Reboot device after upgrade
- [x] Backup running and startup configs after upgrade

SAVE CANCEL

**Edit Firmware upgrade template:** *Copy of Cisco Catalyst 3850*

Name: Copy of Cisco Catalyst 3850

Description: Upgrade template for Cisco Catalyst 3850

**COLLECT INFO COMMANDS**

- [x] Get current firmware image command
  - show ver | include System image
  - [x] Use capture results pattern: System image file is "${CaptureData}"
- [ ] Get info on config register command
- [ ] Collect Boot Variable Info
- [x] Get free space command
  - show file systems
- [x] Other commands
  - show version

**UPGRADE COMMANDS**

Firmware image(s): Firmware *Not defined* SELECT NEW IMAGE FROM REPOSITORY

Firmware Image Type ADD NEW

Upgrade firmware image command: copy ${TransferProtocol} //${StorageAddress}/${SubFolder}/${NewImageName} ${NewImageSlot}${CRLF}${CRLF}dir ${NewImageSlot} ${SuccessRegEx:${NewImageName}}

Transfer protocol: TFTP

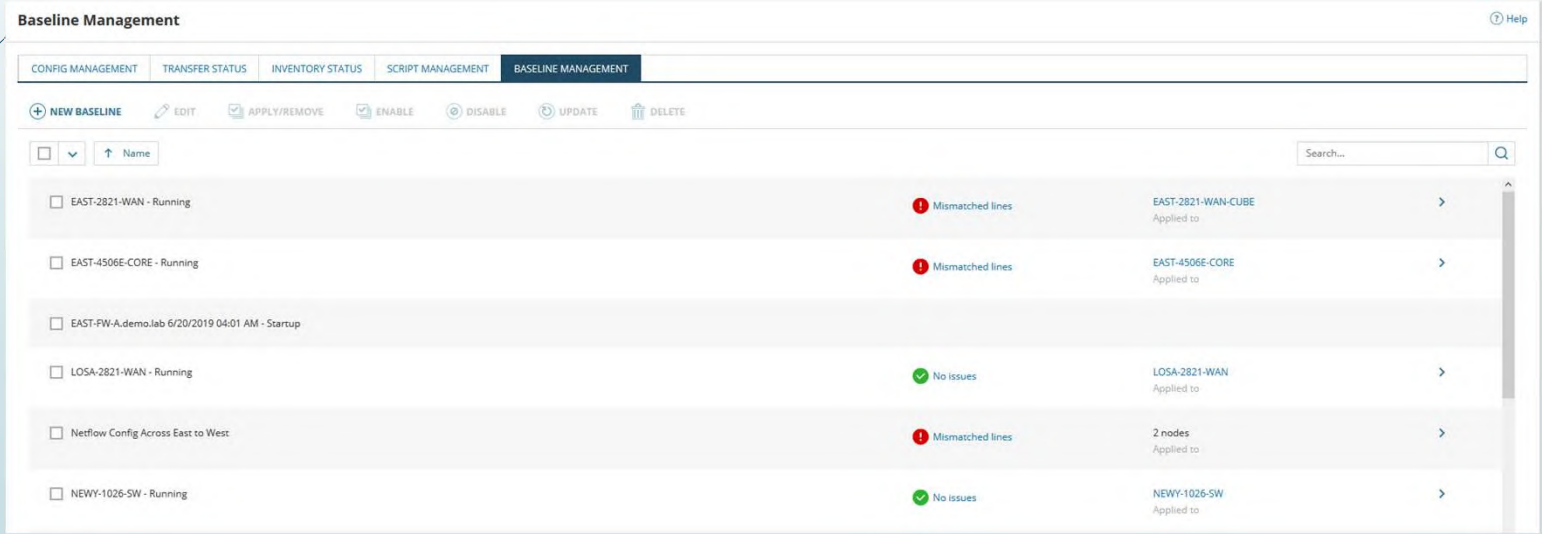
- [x] Delete firmware image command: delete ${ExistingImagePath}${CRLF}${CRLF}${CRLF}
- [x] Backup firmware image command: copy ${ExistingImagePath} ${TransferProtocol} //${StorageAddress}/${SubFolder}/${CRLF}${CRLF}${CRLF}
- [ ] Update config register command
- [x] Update boot variable command: config terminal${CRLF}no boot system${CRLF}boot system ${NewImageSlot}${NewImageName}${CRLF}end${CRLF}write memory${CRLF}${CRLF}${CRLF}show boot ${SuccessRegEx:${NewImageName}}
- [x] Reboot command: reload${CRLF}y${CRLF}y
- [x] Verify uploaded firmware image integrity command: verify /md5 ${NewImageSlot}${NewImageName} ${NewImageHash} ${SuccessRegEx:Verified}
- [x] Verify backed up firmware image integrity command: verify /md5 ${ExistingImagePath} ${BackupImageHash} ${SuccessRegEx:Verified}
- [ ] Verify Upgrade command

# NCM Firmware Upgrade

- Firmware Upgrade Templates
- Best Practices
  - Create copies of upgrade templates (NCM by default will not allow editing of original template)
  - Use naming convention that is easy to interpret
  - Cisco Nexus devices with multiple VDCs will be applied to all on the physical device. These cannot be upgraded individually
  - Cisco ASAs with multiple contexts, must be added as a node for each context in NCM. Adding the admin context by IP address will make the discovering of other contexts automatic. Then add each as a node

# NCM Baseline Management

- Develop Organizational standards based on device type, model, location
- Integrates with Compliance requirements



# NCM Jobs

- Used to schedule a variety of tasks
  - Config Backups
  - Downloads
  - Script Execution
  - Inventories

**Jobs List**

To keep the NCM database as efficiently accessible as possible, without unneeded config data, we recommend that you setup a "Purge Configs" Job.
» Learn more

CREATE NEW JOB | EDIT | DUPLICATE JOB | START JOB | STOP JOB | ENABLE | DISABLE | DELETE

| Job Name | Status | Job Type | Author | Last Date Run | Next Date Run | History |
|---|---|---|---|---|---|---|
| 47th - Configuration Saves | Scheduled | Execute Command Script on Devices | Admin | Never | 11/5/2020, 12:00:00 PM | |
| 47th - Default Database and Archive Maintena... | Scheduled | Perform Routine Database and Archive Maintenan... | Admin | Never | 11/8/2020, 7:00:00 AM | |
| 47th - Nightly Config Backup | Scheduled | Download Configs from Devices | Admin | 11/4/2020, 2:01:55 AM | 11/6/2020, 12:00:00 PM | |
| 47th - Nightly Network Inventory | Scheduled | Update Inventory | Admin | 11/4/2020, 3:41:46 PM | | |

# NCM Compliance

- Why use SolarWinds Compliance?
  - Used to ensure device meets organizational requirements
  - Used to ensure devices meet DISA STIG Compliance
- Non-Invasive, Offline Configuration File Scan
- Use CLI or Regular Expression

**Cisco Security Audit**

Last updated Friday, October 4, 2019 01:58:19 AM

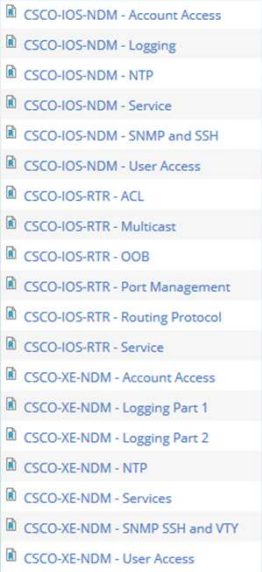
REPORT DETAILS

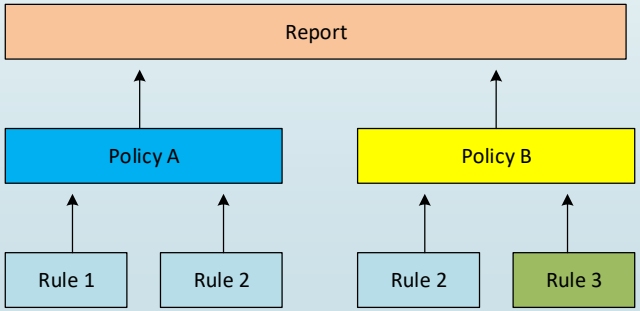
EXPORT

| | | Security Audit Flood (searched 160 configs) | | | | Security Audit IP Commands (searched 80 configs) | | | Security Audit Security (searched 200 configs) | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Node Name | IP Address | Disable IP Directed Broadcast (0 violations) | Disable IP Redirects & IP Unreachables (40 violations) | Set Authentication Failure Rate to less than 3 retries (40 violations) | Set TCP Synwait Time (40 violations) | Disable Proxy ARP (40 violations) | Discard IP Source-Route (40 violations) | Disable IP Gratuitous ARPs (0 violations) | Enable IP CEF (9 violations) | Enable NetFlow switching (40 violations) | Enable Secret (12 violations) | Set Minimum Password length (40 violations) |
| DEN-2691-INT.demo.lab | 10.91.0.6 | ✓ | ⚠ | ℹ | ℹ | ℹ | ⚠ | ✓ | ✓ | ℹ | ✓ | ℹ |
| DEN-3560-ASFlr1A.demo.lab | 10.95.5.2 | ✓ | ⚠ | ℹ | ℹ | ℹ | ⚠ | ✓ | ✓ | ℹ | ✓ | ℹ |
| DEN-3560-ASFlr1b.demo.lab | 10.96.5.2 | ✓ | ⚠ | ℹ | ℹ | ℹ | ⚠ | ✓ | ✓ | ℹ | ✓ | ℹ |
| DEN-3560-ASFlr2a.demo.lab | 10.97.5.2 | ✓ | ⚠ | ℹ | ℹ | ℹ | ⚠ | ✓ | ✓ | ℹ | ✓ | ℹ |
| DEN-3560-ASFlr2b.demo.lab | 10.98.5.2 | ✓ | ⚠ | ℹ | ℹ | ℹ | ⚠ | ✓ | ✓ | ℹ | ✓ | ℹ |
| DEN-3560-ASFlr3a.demo.lab | 10.99.5.2 | ✓ | ⚠ | ℹ | ℹ | ℹ | ⚠ | ✓ | ✓ | ℹ | ✓ | ℹ |
| DEN-3560-ASFlr3b.demo.lab | 10.100.5.2 | ✓ | ⚠ | ℹ | ℹ | ℹ | ⚠ | ✓ | ✓ | ℹ | ✓ | ℹ |
| DEN-3560-ASFlr4a.demo.lab | 10.101.5.2 | ✓ | ⚠ | ℹ | ℹ | ℹ | ⚠ | ✓ | ✓ | ℹ | ✓ | ℹ |
| DEN-3560-ASFlr4b.demo.lab | 10.102.5.2 | ✓ | ⚠ | ℹ | ℹ | ℹ | ⚠ | ✓ | ✓ | ℹ | ✓ | ℹ |
| DEN-3560-CORE_A.demo.lab | 10.92.0.2 | ✓ | ⚠ | ℹ | ℹ | ℹ | ⚠ | ✓ | ✓ | ℹ | ✓ | ℹ |

# Compliance

- Policy Reports
  - Group of policies to evaluate identified devices



# Compliance

- Rules
  - Define specific which must or must not be met
  - Can allow for auto remediation
- Best Practices
  - Keep a consistent naming convention throughout your configuration to make it easier to trace issues
  - Limit the use of Auto Remediation

**Edit CSCO-IOS-NDM-CISC-ND-001030 - NTP**

Rules describe what is to be found (or not found) in configuration files. If the rule is not met, the rule violation will appear with the error level set below in the policy report.

**IDENTIFY THIS RULE**

Rule name: CSCO-IOS-NDM-CISC-ND-001030 - NTP

Description: The Cisco router must be configured to synchronize its clock with the primary and secondary time sources using redundant authoritative time sources.

Alert level: CAT III CAT II CAT I

Save in folder: CSCO-IOS-NDM

**STRING MATCHING**

Alert on the rule below if String is found String is NOT found

**Advanced Config Search**(block search and/or search)

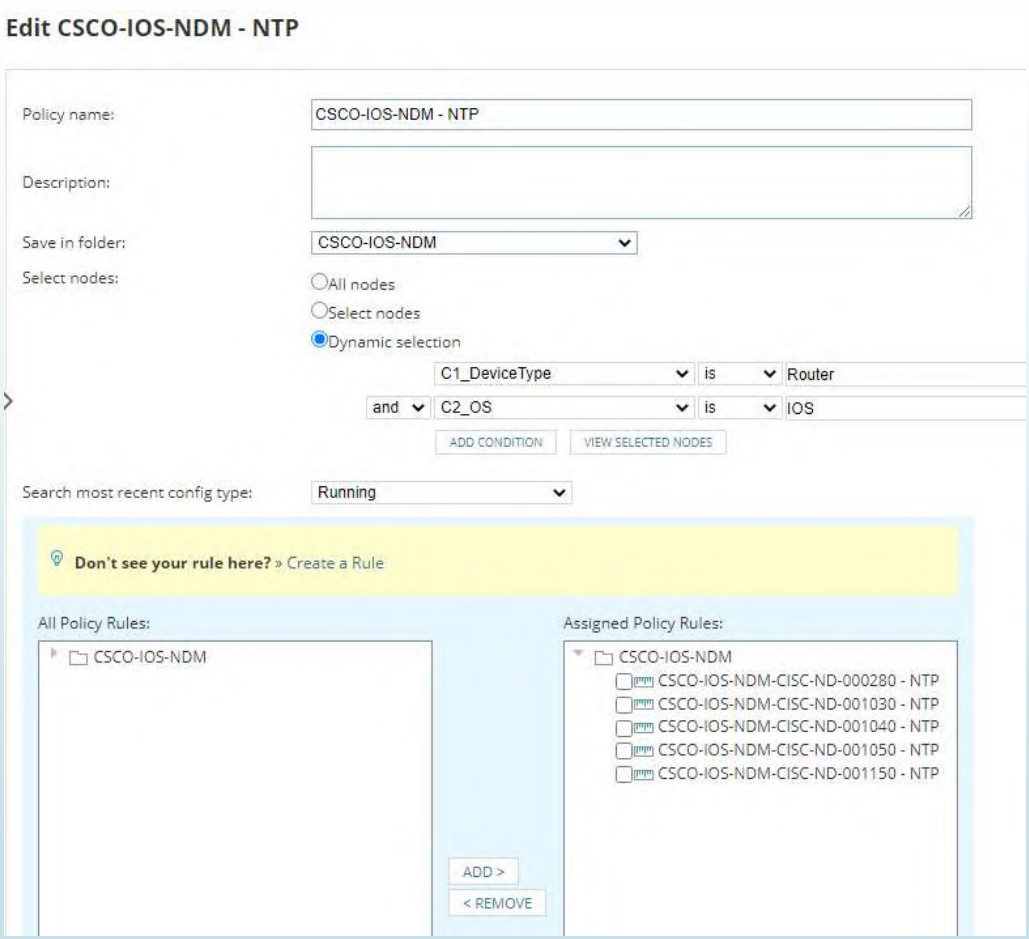
| AND/OR | PARENS (OPTIONAL) | | MUST/MUST NOT CONTAIN | STRING TYPE | STRING | PARENS (OPTIONAL) |
|---|---|---|---|---|---|---|
| | | Config File | must contain | Find string | ntp server 10.50.2.100 key 1 | |
| and | | Config File | must contain | Find string | ntp server 10.50.2.200 key 2 | |

ADD ANOTHER STRING

CHECK PARENTHESIS Check parenthesis in conditional statement. This does not check any parenthesis in a regular expression.

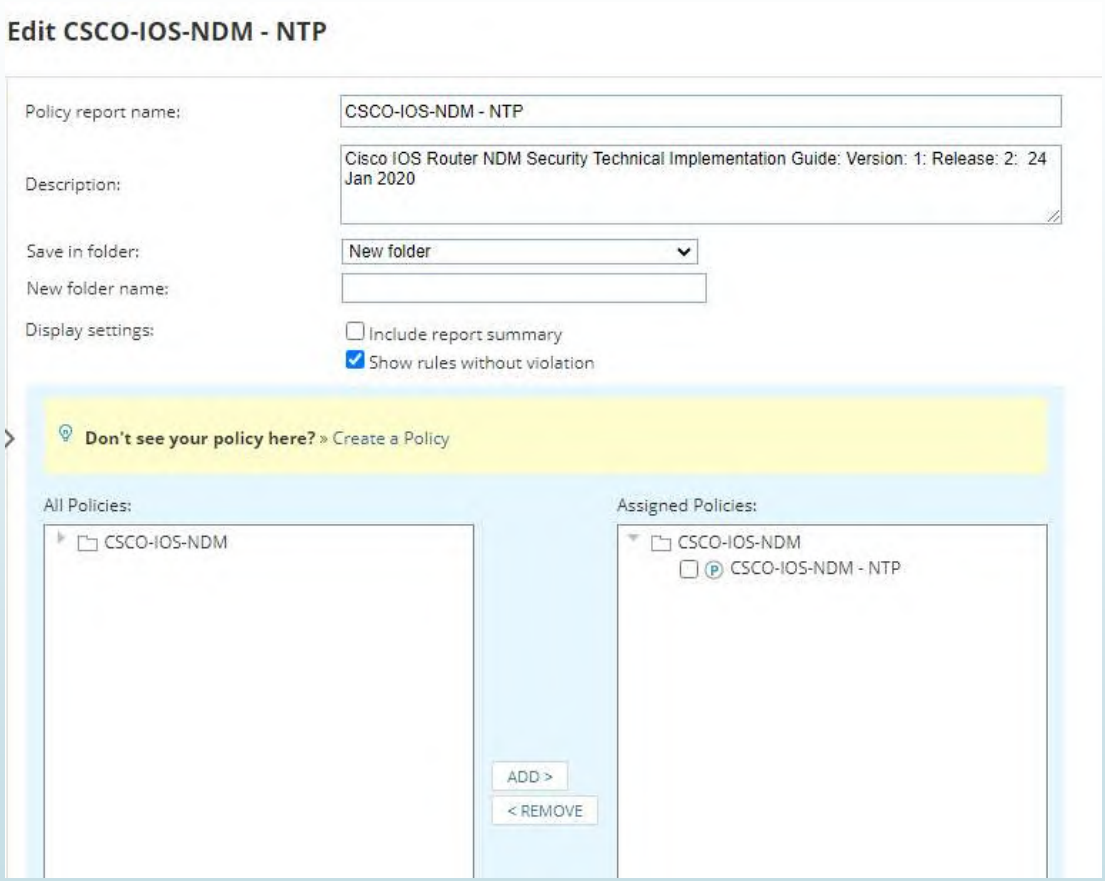
# Compliance

- Policy
  - Group of Rules
  - Specific nodes that meet
    - All nodes
    - Selected Nodes
    - Dynamic selection based on System or Custom Properties



# Compliance

- Reports
  - Compliance the latest downloaded configuration against the current policy or multiple policies for this report
  - Reports are shown in the dashboards



# Compliance

- During our Compliance Auditing we will be moving from insecure protocols to secure protocols
  - Insecure protocols
    - SNMPv2, TELNET, HTTP
  - Secure Protocols
    - SNMPv3
      - SHA Authentication
      - AES128 Privacy
    - SSH version 2
    - HTTPS

- Baseline Management
  - Review and Edit
- NCM Jobs
  - Review and Create
- Compliance
  - Create Reports and Policies by modifying Rules and device configuration

# DEMO & LAB 14, 15, 16

# End of Day

- Review NCM
  - Adding Nodes
  - Device Templates
  - Baselines
  - Jobs
  - Compliance

# Questions and Answers

# Welcome Back!

Let's Review

## Comprehensive Lab

# Today's Agenda

- This sections topics include:
  - Comprehensive Review
    - Deploy SolarWinds

# Comprehensive Lab

- Today you will perform all installation, implementation, and configuration activities of this course.
- If you have an issue, work with your classmate to troubleshoot.
- All configuration items must be configured and implemented.
- Refer to Lab Manual
- Duration:  8.0 hours

## End of Day

# Questions and Answers

# What is NetFlow Traffic Analyzer

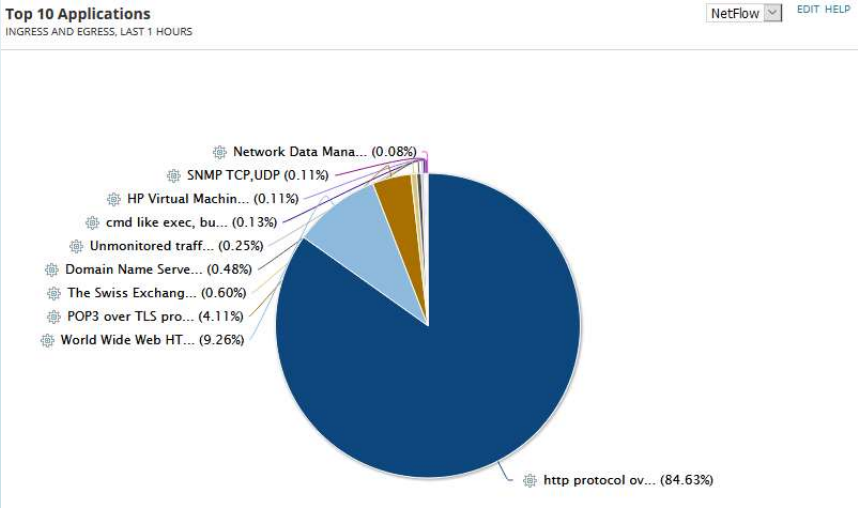
- NetFlow Traffic Analyzer (NTA) is a SolarWinds application to help the organization analyze the NetFlow type traffic in the Environment

- NTA and Network Performance Monitor (NPM) give you the ability to boost your network traffic analysis and assist with:

- Monitoring your Network
- Discover Traffic Patterns
- Avoid High Bandwidth Consumers

# What is NetFlow Traffic Analyzer

- Ability to analyze network traffic patterns over months, days, or minutes by drilling down into any network element
- Measure the effectiveness of pre- and post-policy traffic levels per class map to determine if QoS policies are working as planned
- Create, schedule, and deliver in-depth network traffic analysis and bandwidth reports



# NTA Terminology

- **NTA Flow Storage Database:** An independent database for storing flow data. The SolarWinds NTA Flow Storage Database must be installed before installing SolarWinds NTA

- **NetFlow collector:** A server responsible for receiving, storage, and processing of flow data

# Requirements

- System Requirements
  - SQL 2016 or Better
  - Try to stay in the same Operating System Family
    - Microsoft 2016 Server with SQL 2016, etc.
  - Unable to migrate from NTA 4.2.3 or earlier
- NTA must match the NPM licensing levels
  - SL100
  - SL250
  - SL500
  - SL2000
  - SLX

- Resource Requirements
  - 4-16 CPU and 3GHz or better
  - 16-128 GB RAM
  - 20-400GB on 7200RPM disk Quad/Dual Core
  - RAID 0 or 1+0
  - .NET Framework 4.6.2, but Orion server will auto-install if not present

| APPLICATION | INGRESS BYTES | EGRESS BYTES | INGRESS PACKETS | EGRESS PACKETS | PERCENT |
|---|---|---|---|---|---|
| http protocol over TLS/SSL (443) | 537.6 Mbytes | 537.6 Mbytes | 913.21 k | 913.21 k | 84.63% |
| World Wide Web HTTP (80) | 58.8 Mbytes | 58.8 Mbytes | 274.11 k | 274.11 k | 9.26% |
| POP3 over TLS protocol (995) | 26.1 Mbytes | 26.1 Mbytes | 37.36 k | 37.36 k | 4.11% |
| The Swiss Exchange (7351) | 3.8 Mbytes | 3.8 Mbytes | 10.73 k | 10.73 k | 0.6% |
| Domain Name Server (53) | 3.1 Mbytes | 3.1 Mbytes | 20.17 k | 20.17 k | 0.48% |
| Unmonitored traffic | 1.6 Mbytes | 1.6 Mbytes | 11.54 k | 11.54 k | 0.25% |
| cmd like exec, but automatic authentication is per (514) | 812.6 kbytes | 812.6 kbytes | 1.36 k | 1.36 k | 0.13% |
| HP Virtual Machine Group Management (5223) | 672.1 kbytes | 672.1 kbytes | 4.11 k | 4.11 k | 0.11% |
| SNMP (161) | 667.5 kbytes | 667.5 kbytes | 9.56 k | 9.56 k | 0.11% |
| Network Data Management Protocol (10000) | 519.8 kbytes | 519.8 kbytes | 720 | 720 | 0.08% |
| Remaining traffic | 1.6 Mbytes | 1.6 Mbytes | 14.43 k | 14.43 k | 0.25% |

# Other Software



- The Installation Wizard installs the following required x86 components if they are not found on your Orion database server:
  - SQL Server System Common Language Runtime (CLR) Types. Orion products use secure SQL CLR stored procedures for selected, non-business data operations to improve overall performance
  - Microsoft SQL Server Native Client
  - Microsoft SQL Server Management Objects

# TCP and UDP Port Assignments

Things go keep in mind:

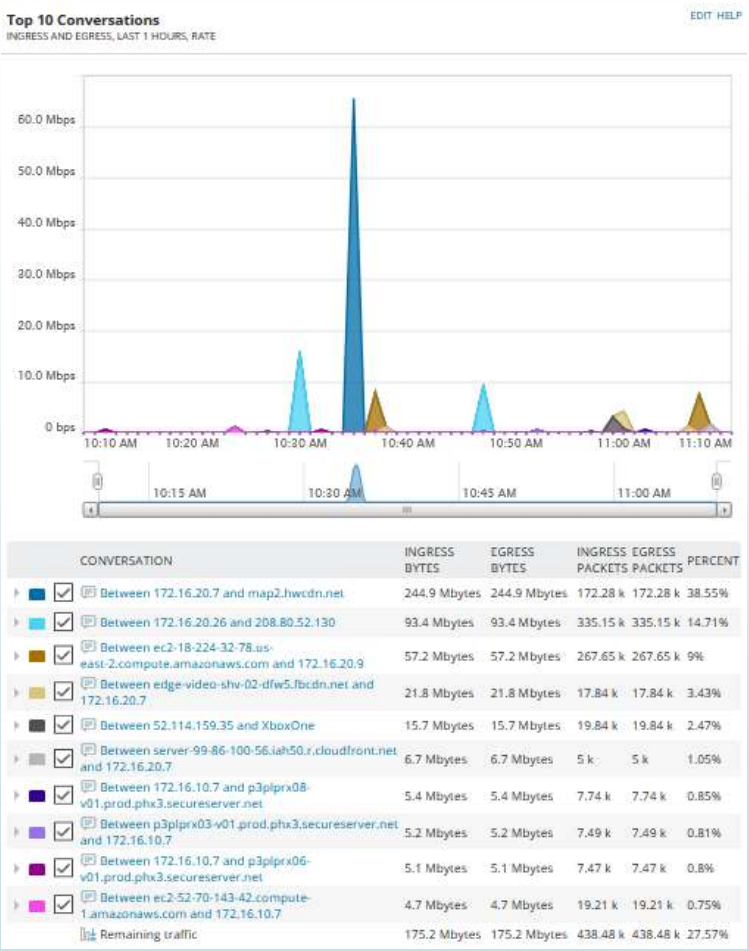
- Review Access-lists on your devices
- Review Control Plane Settings
- Ensure Routing is configured for Layer 3 Interfaces

| Port | Protocol | Service/Process | Direction |
|---|---|---|---|
| 80 | TCP | World Wide Web Publishing Service | Bidirectional |
| 137 | UDP | NetBIOS | Outbound |
| 161 | UDP<br><br>TCP | SolarWinds Job Engine v2 | Outbound |
| 1433 | TCP | SolarWinds NetFlow Service SolarWinds NetFlow Storage Service | Outbound |
| 1434 | UDP | SolarWinds NetFlow Service SolarWinds NetFlow Storage Service SQL Browse Service | Outbound |
| 2055 | UDP | SolarWinds NetFlow Service | Inbound |
| 5671 | TCP | RabbitMQ | Bidirectional |
| 17777 | TCP | SolarWinds Information Service | Bidirectional |
| 17778 | HTTPS and TCP | SolarWinds Information Service | Bidirectional |
| 17791 | TCP | SolarWinds Agent | Bidirectional |

# How NTA Works



- SolarWinds NTA collects CBQoS and flow data, processes it, and together with NPM performance data presents graphical displays of information to show results and bandwidth statistics



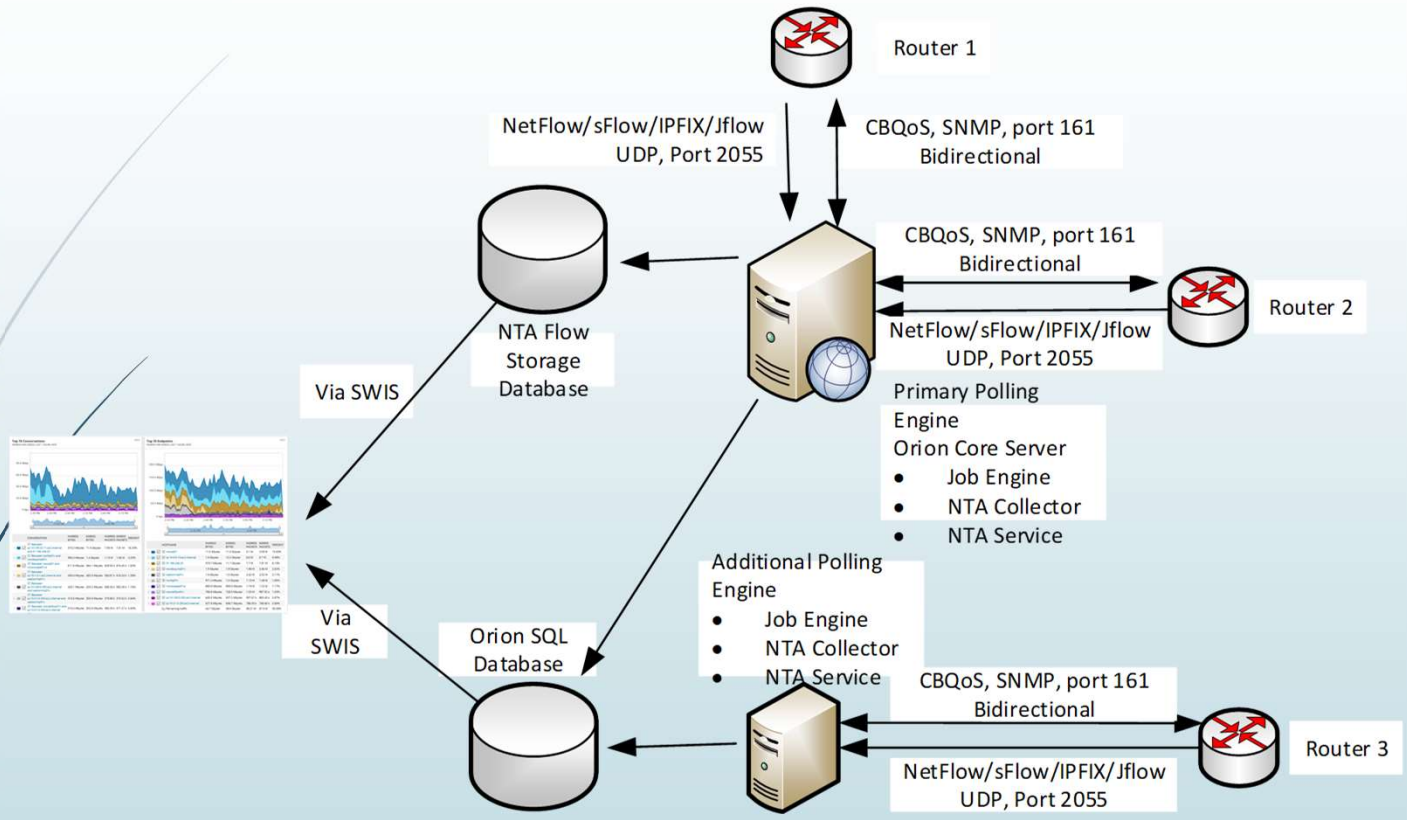

| CONVERSATION | INGRESS BYTES | EGRESS BYTES | INGRESS PACKETS | EGRESS PACKETS | PERCENT |
|---|---|---|---|---|---|
| Between 172.16.20.7 and map2.hwcdn.net | 244.9 Mbytes | 244.9 Mbytes | 172.28 k | 172.28 k | 38.55% |
| Between 172.16.20.26 and 208.80.52.130 | 93.4 Mbytes | 93.4 Mbytes | 335.15 k | 335.15 k | 14.71% |
| Between ec2-18-224-32-78.us-east-2.compute.amazonaws.com and 172.16.20.9 | 57.2 Mbytes | 57.2 Mbytes | 267.65 k | 267.65 k | 9% |
| Between edge-video-shv-02-dfw5.fbcdn.net and 172.16.20.7 | 21.8 Mbytes | 21.8 Mbytes | 17.84 k | 17.84 k | 3.43% |
| Between 52.114.159.35 and XboxOne | 15.7 Mbytes | 15.7 Mbytes | 19.84 k | 19.84 k | 2.47% |
| Between server-99-86-100-56.iah50.r.cloudfront.net and 172.16.20.7 | 6.7 Mbytes | 6.7 Mbytes | 5 k | 5 k | 1.05% |
| Between 172.16.10.7 and p3plprx08-v01.prod.phx3.secureserver.net | 5.4 Mbytes | 5.4 Mbytes | 7.74 k | 7.74 k | 0.85% |
| Between p3plprx03-v01.prod.phx3.secureserver.net and 172.16.10.7 | 5.2 Mbytes | 5.2 Mbytes | 7.49 k | 7.49 k | 0.81% |
| Between 172.16.10.7 and p3plprx06-v01.prod.phx3.secureserver.net | 5.1 Mbytes | 5.1 Mbytes | 7.47 k | 7.47 k | 0.8% |
| Between ec2-52-70-143-42.compute-1.amazonaws.com and 172.16.10.7 | 4.7 Mbytes | 4.7 Mbytes | 19.21 k | 19.21 k | 0.75% |
| Remaining traffic | 175.2 Mbytes | 175.2 Mbytes | 438.48 k | 438.48 k | 27.57% |

# NetFlow Traffic Analyzer

- NPM will show you the what and when
- NTA will show you the why
  - Why is my link slow?
    - What traffic is contributing to the issue?
    - Saturation?
    - What device(s) are using excessive bandwidth to cause this issue?

| APPLICATION | INGRESS BYTES | EGRESS BYTES | INGRESS PACKETS | EGRESS PACKETS | PERCENT |
|---|---|---|---|---|---|
| http protocol over TLS/SSL (443) | 14.2 Gbytes | 13.7 Gbytes | 93.91 M | 88.35 M | 37.05% |
| Port 0 | 4.6 Gbytes | 4.6 Gbytes | 872.27 k | 872.25 k | 12.25% |
| SolarWinds Backup (443 TCP) | 0 bytes | 5.2 Gbytes | 0 | 3.56 M | 6.92% |
| World Wide Web HTTP (80) | 2.6 Gbytes | 1.8 Gbytes | 15.55 M | 14.46 M | 5.82% |
| Microsoft-SQL-Server (1433) | 2.1 Gbytes | 2.0 Gbytes | 14.59 M | 14.52 M | 5.54% |
| MySQL (3306) | 1.2 Gbytes | 1.2 Gbytes | 13.58 M | 13.58 M | 3.24% |
| Oracle Database | 1.2 Gbytes | 1.2 Gbytes | 13.51 M | 13.51 M | 3.18% |
| SQL Services (118) | 1.2 Gbytes | 1.2 Gbytes | 13.51 M | 13.51 M | 3.18% |
| rpc (530) | 1.1 Gbytes | 1.1 Gbytes | 12.81 M | 12.81 M | 2.99% |
| SNMPTRAP (162) | 579.0 Mbytes | 575.1 Mbytes | 6.44 M | 6.43 M | 1.53% |
| Remaining traffic | 7.9 Gbytes | 5.9 Gbytes | 24.68 M | 24.15 M | 18.29% |

# NTA Integration



# Flow Monitoring Architecture



- The Orion Platform is used to run SolarWinds NTA. It provides centralized administration, access control, and alerting and reporting
- The Orion Web Console is the web interface used for navigating and managing SolarWinds NTA settings and features

**NetFlow Sources**
8 NODES

MANAGE FLOW SOURCES HELP

| SOURCE ENTITY | TRAFFIC IN | TRAFFIC OUT | LAST RECEIVED NETFLOW | LAST RECEIVED CBQOS |
|---|---|---|---|---|
| DEN-PA100VM-A | | | 7/22/20 3:51 PM | 7/22/20 3:51 PM |
| EAST-2821-WAN-CUBE | | | 7/22/20 3:51 PM | 7/22/20 3:51 PM |
| EASTESX01A | | | 7/22/20 3:51 PM | 7/22/20 3:51 PM |
| LOSA-2821-WAN | | | 7/22/20 3:51 PM | 7/22/20 3:51 PM |
| LOSA-MX64-FW | | | 7/22/20 3:51 PM | 7/22/20 3:51 PM |
| NEWY-2811-WAN | | | 7/22/20 3:51 PM | 7/22/20 3:51 PM |
| NEWY-EX2200-45thFl | | | 7/22/20 3:51 PM | 7/22/20 3:51 PM |
| WEST-2821-WAN | | | 7/22/20 3:51 PM | 7/22/20 3:51 PM |

# CBQoS Monitoring Architecture

- CBQoS implementations work much the same way as flow-enabled implementations, except that the NetFlow collector polls each device and the device returns data that meets the CBQoS policies you have defined

| Interface name | Node name | Last received CBQoS | CBQoS enabled |
|---|---|---|---|
| Adaptive Security Appliance 'CAPITA-DMZ' interface - CAPITA DMZ - LINK TO CAPITA NETWORK | EAST-FW-B | Never received | Disabled |
| Adaptive Security Appliance 'cplane' interface - cplane | EAST-FW-A | Never received | Disabled |
| Adaptive Security Appliance 'DMZ1' interface - DMZ1 | EAST-FW-B | Never received | Disabled |
| Adaptive Security Appliance 'GigabitEthernet0/4' interface - GigabitEthernet0/4 | EAST-FW-A | Never received | Disabled |
| Adaptive Security Appliance 'GigabitEthernet0/5' interface - GigabitEthernet0/5 | EAST-FW-A | Never received | Disabled |
| Adaptive Security Appliance 'INSIDE' interface - INSIDE | EAST-FW-B | Never received | Disabled |
| Adaptive Security Appliance 'mgmt_plane_int_tap' interface - mgmt_plane_int_tap | EAST-FW-A | Never received | Disabled |
| Adaptive Security Appliance 'OUTSIDE' interface - OUTSIDE | EAST-FW-B | Never received | Disabled |
| Adaptive Security Appliance 'Port-channel1' interface - Port-channel1 | EAST-FW-B | Never received | Disabled |
| Adaptive Security Appliance 'Port-channel2' interface - Port-channel2 | EAST-FW-B | Never received | Disabled |

# NTA Protocols



Sampled and Non-sampled Flow

Sampled Flow is collected data and provides only a sample. This will help prevent the network from congestion and overloading

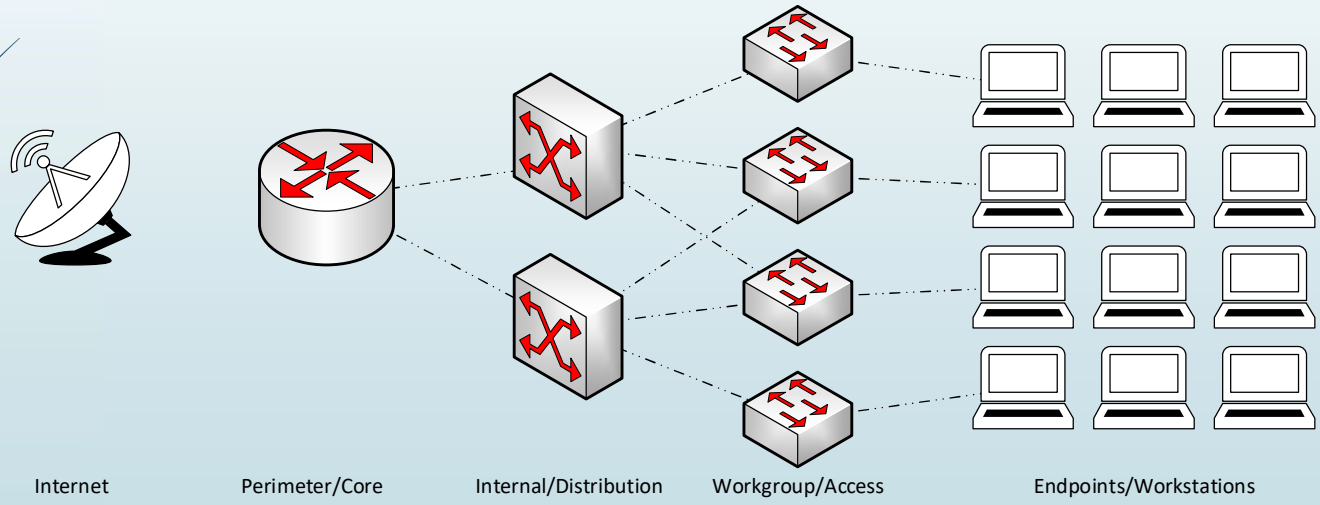
Non-Sampled Flow will collect all data. This may cause network congestion

| Flow | Supported Versions | Sampled Flow Support |
|---|---|---|
| NetFlow | v1, v5 and v9 | v5 and v9 |
| | | |
| | NetFlow version 9 is configured the same as NetFlow version 5, but uses a predefined template that is exported in separate flows. Flexible NetFlow is based on NetFlow version 9, but the fields are defined during configuration. | Some devices using IOS versions export flows without specifying that it is being sampled. SolarWinds NTA processes these flows as unsampled. |
| | | |
| | NetFlow v9 must have an appropriate template with all required fields. | |
| sFlow | v2, v4, and v5 | Supported |
| J-Flow | Supported | Supported |
| | | |
| | | Some devices using JunOS versions export flows without specifying that it is being sampled. SolarWinds NTA processes these flows as unsampled. |
| IPFIX | Supports IPFIX generated by ESX 5.1 and later, for IPv4 traffic. | Supported |

# NetFlow Best Practices



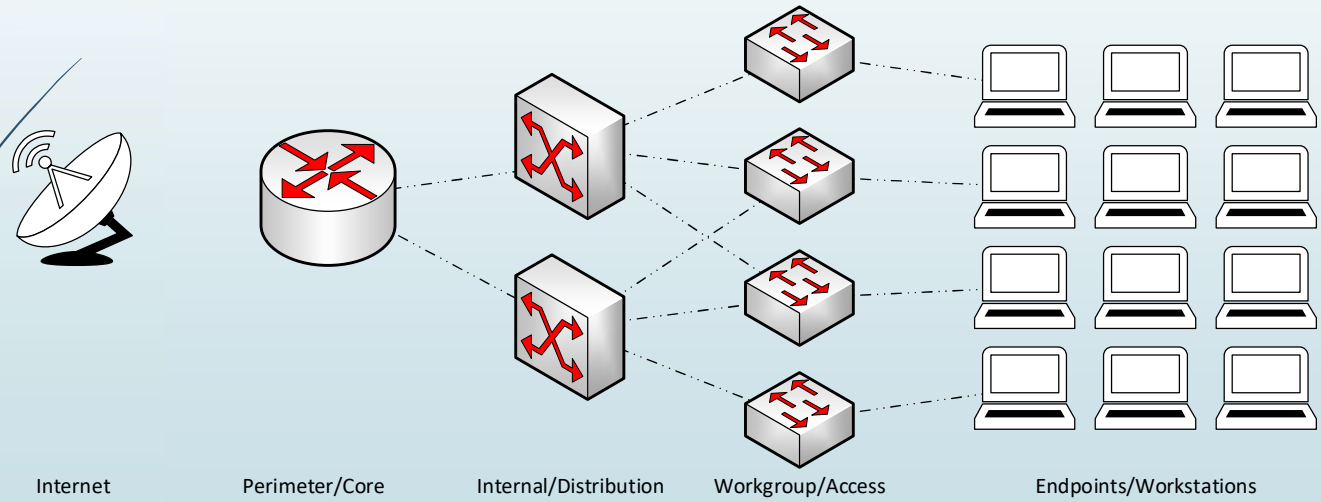
- Flows monitor Conversations on the network
  - The flow from the perspective of the interface on router, switch, firewall, etc.
    - Ingress – What is flowing into the device
    - Egress – What is flowing out of device



# NetFlow Best Practices



- Recommendation to configure both ingress and egress on WAN Interfaces at the highest of your infrastructure to start
- Otherwise on Ingress interfaces
- Start small work big!



# NTA Flow Requirements



- Minimum fields required:
  - Protocol Port UDP 2055 (default) should be open
  - Source & Destination IP Address
  - At least one interface
  - At least one byte group
  - Source & Destination Port
  - SQL Port open TCP 1433 (default)

# Troubleshooting the Flows



- If you are not seeing what you expect…
  - May require deeper Wireshark Analysis to ensure proper fields are configured
  - Check the configuration on your networking devices for completeness
    - Seeing the correct poller
    - Configuration?
  - Your Flow data isn't getting to where it should
    - Check port and protocol for network connectivity
    - Use Wireshark (if available)
      - Check with IA/IT Security prior to using Wireshark!

# One more thing…



- Unknown Traffic
  - Check Application Port Mapping
  - Check Device configuration, ports, or protocols
- What does this alert do?
  - Check the Customer Success Center
- Unmanageable Interfaces
  - OID may not be available
  - Update MIB Database
- Unmonitored/Not Defined Type Traffic
  - Not a defined application associated with this type traffic

# Beyond Getting Started

- SolarWinds Customer Support
- SolarWinds Customer Success Center
- NetFlow Traffic Analyzer Administrators Guide
- NTA on Thwack
- NTA Release Notes

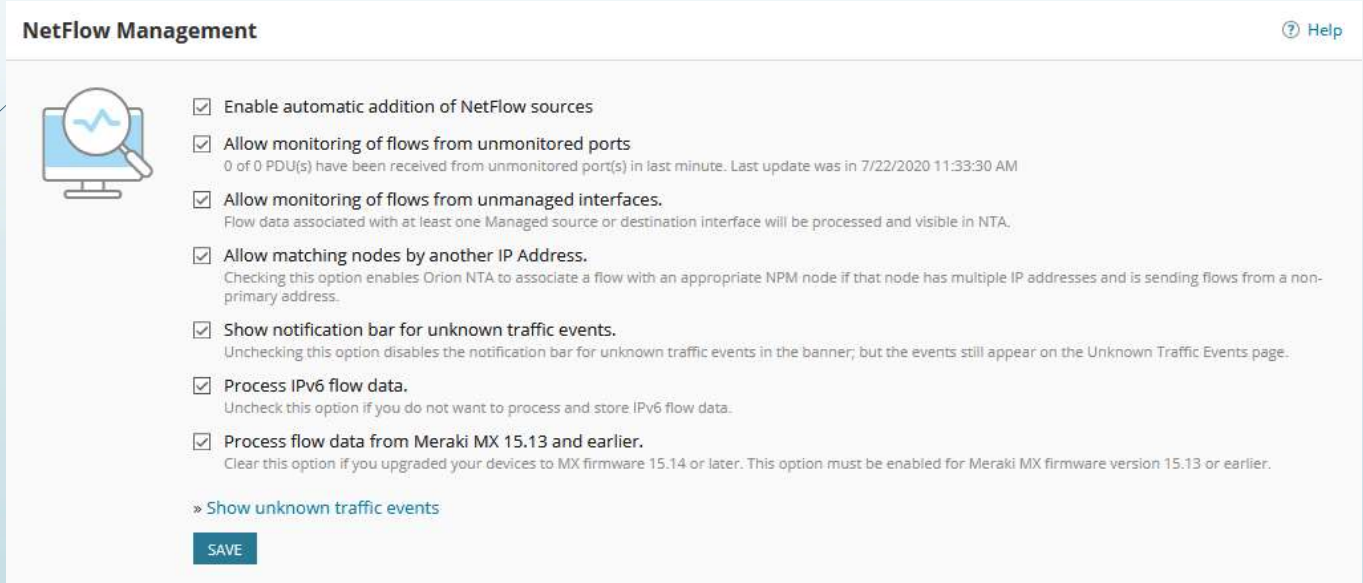
Documentation for
**NetFlow Traffic Analyzer**

RELEASE NOTES | INSTALL OR UPGRADE | GET STARTED | ADMINISTER

# NetFlow Management

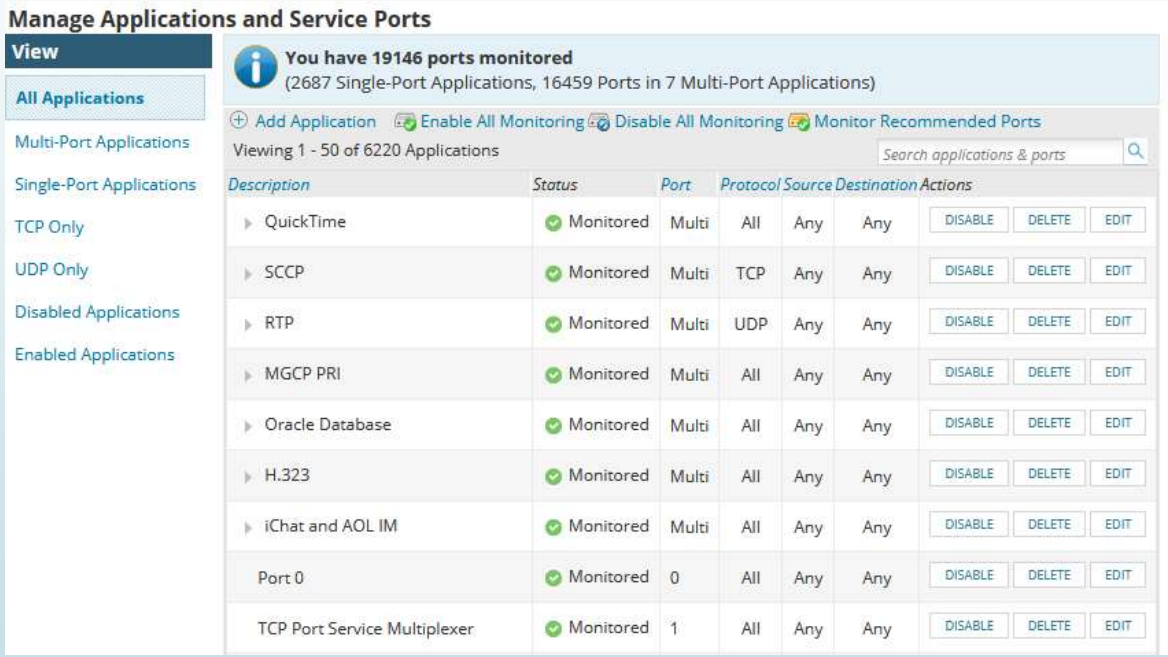


- Configures the default behavior when flows from SolarWinds NPM devices are received, towards data from ports not monitored in NTA, and unmanaged interfaces



# Application and Service Ports

- Using NTA to specify the applications to be monitored
- Using NTA to specify the protocol types by application thus providing the ability to monitor several applications on the same port



# Autonomous Systems



- The ability to manage BGP Autonomous Systems

**Manage Autonomous Systems**

Add Autonomous System

Viewing 1 - 50 of 96527 Autonomous Systems

Page 1 of 1931 | Search Name & ID | SEARCH

| Name | ID | Country | Organization | Registration Date | Last Updated | Actions |
|---|---|---|---|---|---|---|
| -Reserved AS- | 0 | ZZ | | | | DELETE EDIT |
| LVLT-1 - Level 3 Parent, LLC | 1 | United States (US) | | | | DELETE EDIT |
| UDEL-DCN - University of Delaware | 2 | United States (US) | | | | DELETE EDIT |
| MIT-GATEWAYS - Massachusetts Institute of Technology | 3 | United States (US) | | | | DELETE EDIT |
| ISI-AS - University of Southern California | 4 | United States (US) | | | | DELETE EDIT |
| SYMBOLICS - Symbolics, Inc. | 5 | United States (US) | | | | DELETE EDIT |
| BULL-HN - Bull HN Information Systems Inc. | 6 | United States (US) | | | | DELETE EDIT |
| DSTL | 7 | United Kingdom (GB) | | | | DELETE EDIT |
| RICE-AS - Rice University | 8 | United States (US) | | | | DELETE EDIT |
| CMU-ROUTER - Carnegie Mellon University | 9 | United States (US) | | | | DELETE EDIT |

# Monitored Protocols

- Ability to monitor specific protocols

**NetFlow Traffic Analyzer - Edit Transport Protocols to monitor**

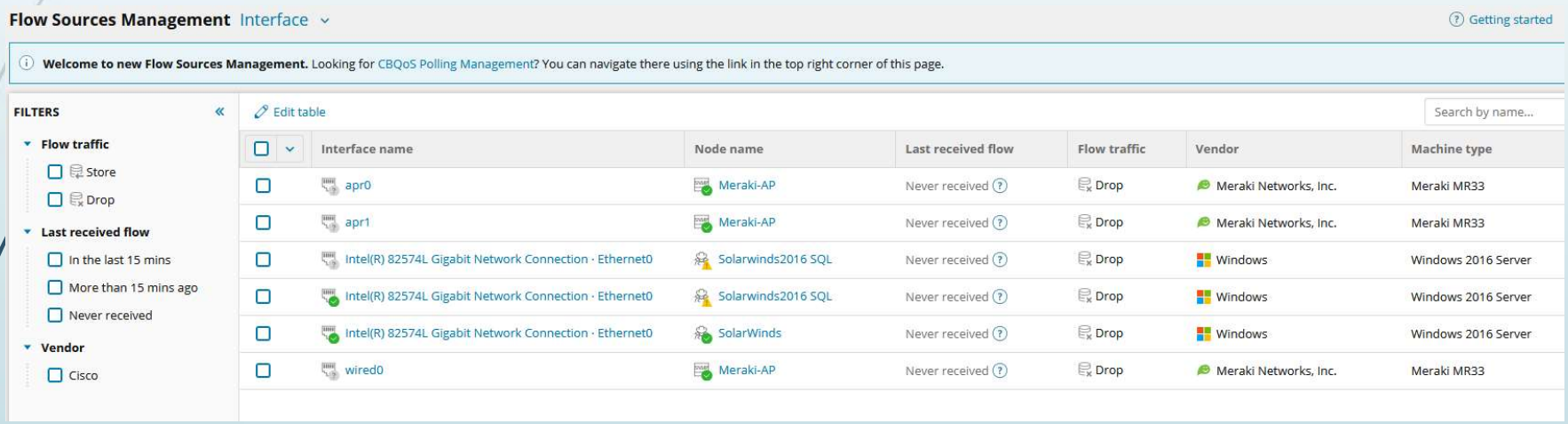
**Monitored Transport Protocols**
Check protocols to enable monitoring

**146 protocols selected**

| | PROTOCOL NAME | PROTOCOL DESCRIPTION |
|---|---|---|
| ☑ | -any 0-hop- | Any 0-hop protocol |
| ☑ | -any dfs- | Any distributed file system |
| ☑ | -any int host- | Any host internal protocol |
| ☑ | -any local net- | Any local network |
| ☑ | -any priv encrpt- | Any private encryption scheme |
| ☑ | -test 1- | Used for experimentation and testing |
| ☑ | -test 2- | Used for experimentation and testing |
| ☑ | 3PC | Third Party Connect Protocol |
| ☑ | A/N | Active Networks |
| ☑ | AH | Authentication Header |
| ☑ | ARGUS | ARGUS |
| ☑ | ARIS | ARIS |
| ☑ | AX.25 | AX.25 Frames |
| ☑ | BBN-RCC-MON | BBN RCC Monitoring |
| ☑ | BNA | BNA |
| ☑ | BR-SAT-MON | Backroom SATNET Monitoring |
| ☑ | CBT | CBT |

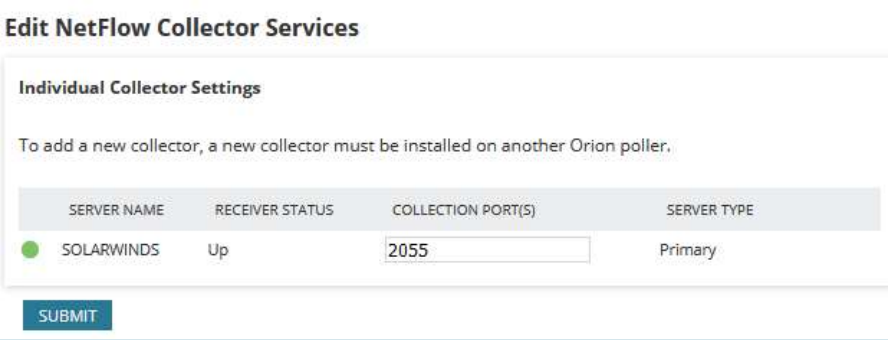
# Flow Sources Management

- Identifying the NetFlow sources on your network devices and appliances



# Collector Services

- NetFlow Collector Services will provide the status of the current flow collectors configure in NTA




- NTA will listen on port UDP 2055 by default, but able to be configured for a port of your choosing

# Type of Service



- SolarWinds NTA can recognize Differentiated Services model of packet delivery prioritization
- All flow-enabled devices can be configured to set a Type of Service byte, referred to as the Differentiated Service Code Point (DSCP)
- The DSCP prioritizes NetFlow packet delivery over the flow-enabled devices on your network by assigning each packet both a Differentiated Service class (1, 2, 3, or 4) and a packet-dropping precedence (low, medium, or high)

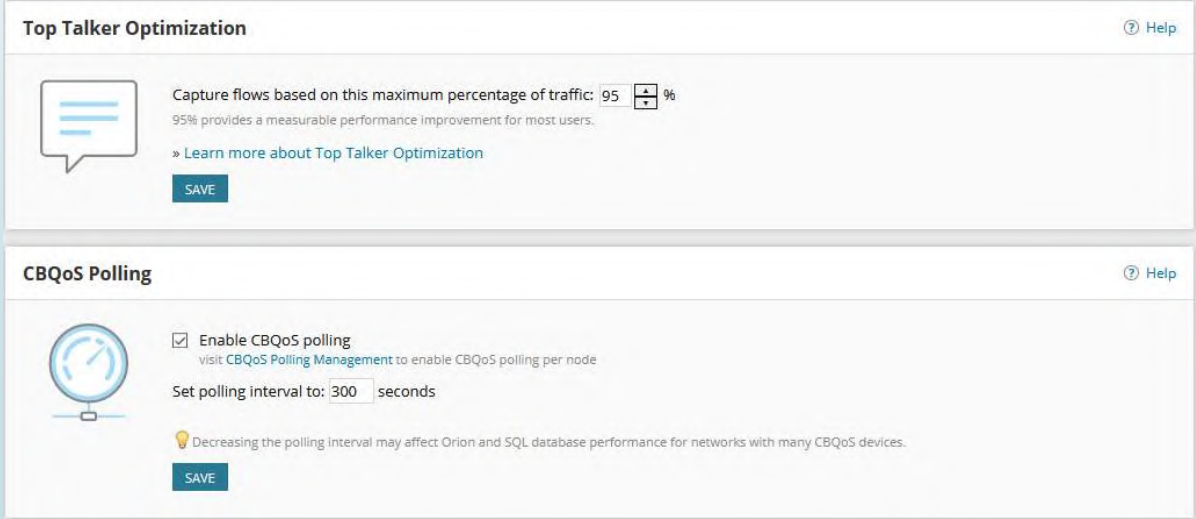
**NetFlow Types of Service - Configure labels for Types of Service**

| TYPE OF SERVICE NAME | DIFFSERV CODE POINT | |
|---|---|---|
| CS0 | 000000 | EDIT |
| CS1 | 001000 | EDIT |
| AF11 | 001010 | EDIT |
| AF12 | 001100 | EDIT |
| AF13 | 001110 | EDIT |
| CS2 | 010000 | EDIT |
| AF21 | 010010 | EDIT |
| AF22 | 010100 | EDIT |
| AF23 | 010110 | EDIT |
| CS3 | 011000 | EDIT |
| AF31 | 011010 | EDIT |
| AF32 | 011100 | EDIT |
| AF33 | 011110 | EDIT |
| CS4 | 100000 | EDIT |
| AF41 | 100010 | EDIT |
| AF42 | 100100 | EDIT |
| AF43 | 100110 | EDIT |
| CS5 | 101000 | EDIT |
| EF | 101110 | EDIT |
| CS6 | 110000 | EDIT |
| CS7 | 111000 | EDIT |

SUBMIT

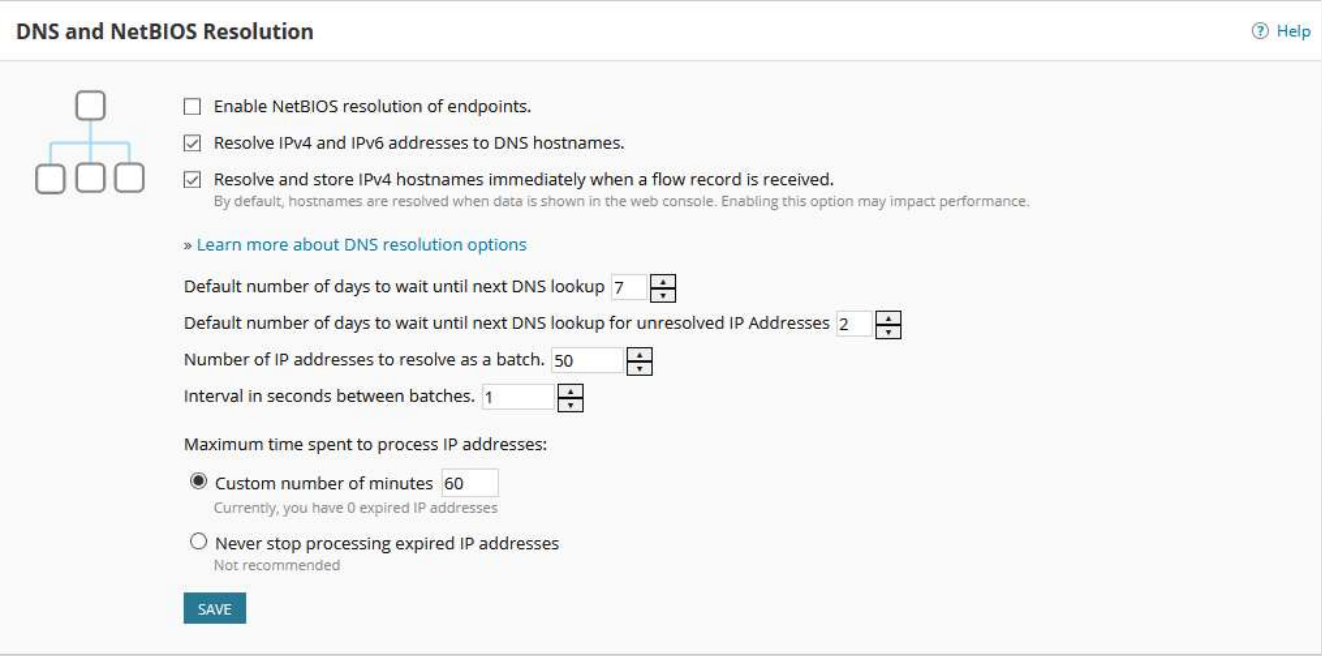
# Top Talkers and CBQoS Polling

- Top Talker configuration will allow you to only record those flows that represent the conversations requiring the most bandwidth in your organization
- Setting the Top Talker Optimization to 100% means 40 to 100 times higher storage space requirements and might affect resource rendering performance. Keeping 100% of flows is suitable only for small installations



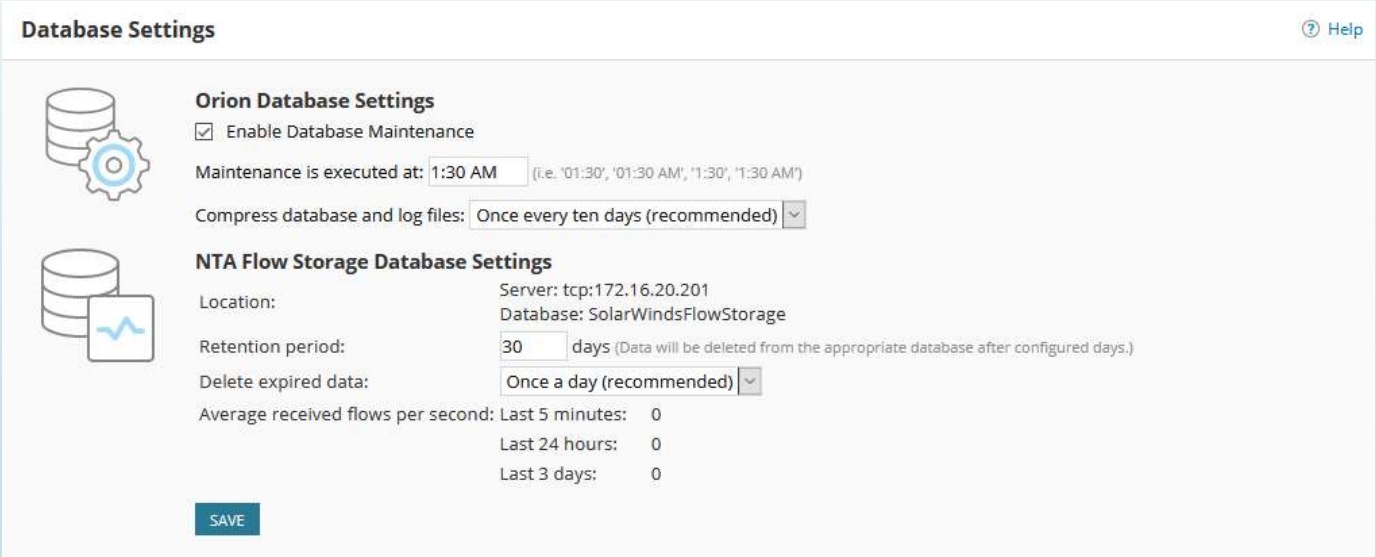
# DNS and NetBIOS Resolution

- NTA will continuously resolve domain names for devices involved in the flows



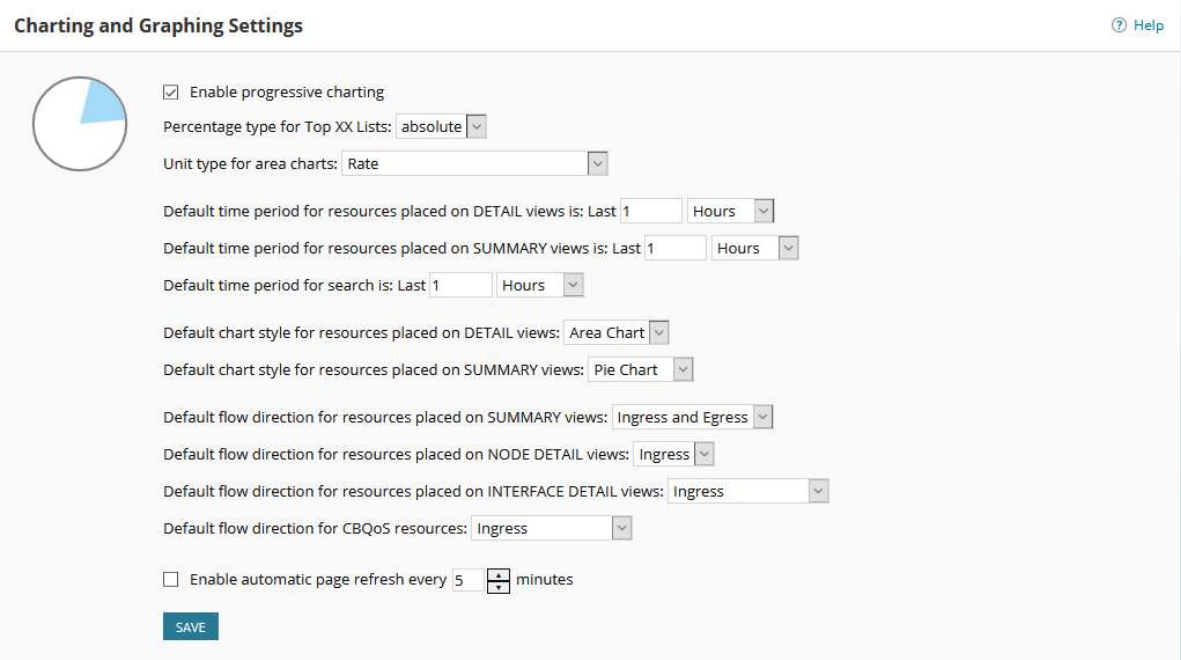
# Database Settings

- Orion Database will store the CBQoS data and node data relevant to NPM
- NTA SQL Flow Storage Database will store flows using column store indexes



# Charting and Graphing

- Ability to enhance your NTA performance by enabling progressive charting and to configure options



# Cisco Router



The following example is from a Cisco router of where to look to enable NetFlow traffic on a Cisco router

```
!
interface GigabitEthernet0/1
description link to PIX
ip address 10.3.1.2 255.255.255.252
ip route-cache flow
!
ip flow-export source GigabitEthernet0/1
ip flow-export version 5
ip flow-export destination 1.2.0.12 2055
ip flow-cache timeout active 1
ip flow-cache timeout inactive 15
snmp-server ifindex persist
!
```

# Cisco Flexible NetFlow



- Exporting flows on some Cisco devices (for example, the 4500 series, with Supervisor 7) requires using Flexible NetFlow

```
flow record ipv4
! match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match interface input
collect interface output
collect counter bytes
collect counter packets

flow exporter NetFlow-to-Orion
destination 10.10.10.10
source vlan254
transport udp 2055
export-protocol netflow-v5

flow monitor NetFlow-Monitor
description Original Netflow captures
record ipv4
exporter NetFlow-to-Orion
cache timeout inact 10
cache timeout act 5

vlan configuration 666
ip flow monitor NetFlow-Monitor input
```

# Juniper Flow

```
#show interfaces ge-0/0/0
unit 0 {
        family inet {
        sampling {
                input
                output;
        }
        address 1.1.1.1/30;
    }
}

#show forwarding-options
sampling {
        input {
        rate 100;
    }
    family inet {
        output {
                flow-server 2.2.2.2 {
                        port <JFlow port number e.g. 2055,2056>;

                        version 5;
                }
        }
    }
}
```

- Juniper sFlow is located to the right
- Juniper Jflow is located to the left

```
sflow {
    polling-interval 30;
    sample-rate 128;
    collector 10.1.2.5 {
    udp-port 2055;
    }
    interfaces ge-0/0/0.0;
    interfaces ge-0/0/1.0;
    interfaces ge-0/0/2.0;
    interfaces ge-0/0/3.0;
    interfaces ge-0/0/4.0;
    interfaces ge-0/0/5.0;
    interfaces ge-0/0/6.0;
    interfaces ge-0/0/7.0;
    interfaces ge-0/0/8.0;
    interfaces ge-0/0/9.0;
    interfaces ge-0/0/10.0;
    interfaces ge-0/0/11.0;
    interfaces ge-0/0/12.0;
    interfaces ge-0/0/13.0;
    interfaces ge-0/0/14.0;
    interfaces ge-0/0/15.0;
    interfaces ge-0/0/16.0;
    interfaces ge-0/0/17.0;
    interfaces ge-0/0/18.0;
    interfaces ge-0/0/19.0;
    interfaces ge-0/0/20.0;
    interfaces ge-0/0/21.0;
    interfaces ge-0/0/22.0;
    interfaces ge-0/0/23.0 {
        polling-interval 30;
        sample-rate 128;
    }
}
```

- NetFlow Traffic Analyzer
  - Web Console Walkthrough
  - Traffic Inspection
  - Traffic Investigation

# Break

# DEMO

# Welcome Back!

Let's Review

- User Device Tracker
- Enterprise Operations Console
- BITI BAN NMS
- Course Wrap Up

# User Device Tracker (UDT)

- What can UDT do for me?
  - Discover Endpoint devices
  - Where the devices have been connected
  - Port Capacity Planning
  - Port Capacity Analysis
  - Watchlist
  - Assistance with Network Topology Mapping
  - UDT specialized Alerts and Reports

# UDT Discovery and Requirements

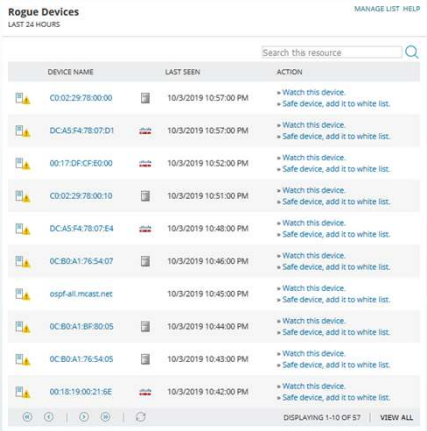
- Add Ports to UDT
  - Network Discovery, just like NPM and NCM
  - Managed Nodes View
    - Yes, there is a button to monitor node with UDT
- UDT will use SNMP to gather the information from a discovered device
- UDT will track activity by reading the Active Directory Event Log

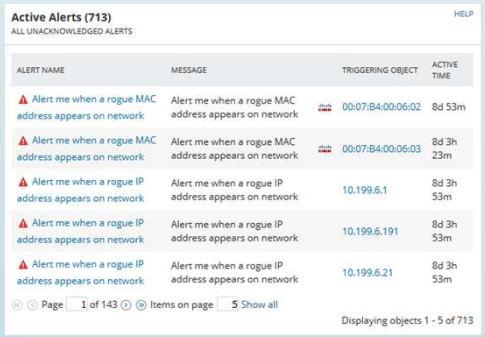
# UDT Special Devices and Lists

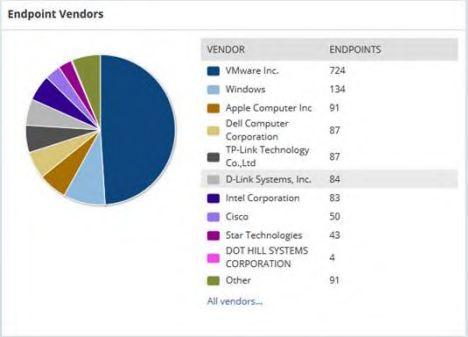
- Rogue Devices
  - Devices that are expected to be accessing your network. New nodes to the network and Solarwinds
- Watched Devices
  - Devices you want to monitor
- Safe Devices
  - Approved endpoint connections
- White List – two different types of lists
  - Included List – approved & safe devices
  - Ignored List – Forbidden Endpoints and their data
- Watch List
  - Current users or endpoints on the network and the connection details

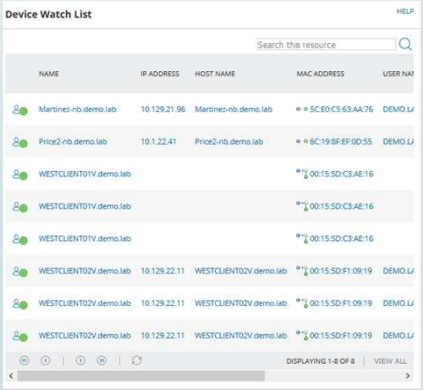
# UDT Drive-by

- UDT does not require extensive configuration
- Alerts and Reports available in Managed Alerts and Managed Reports Views

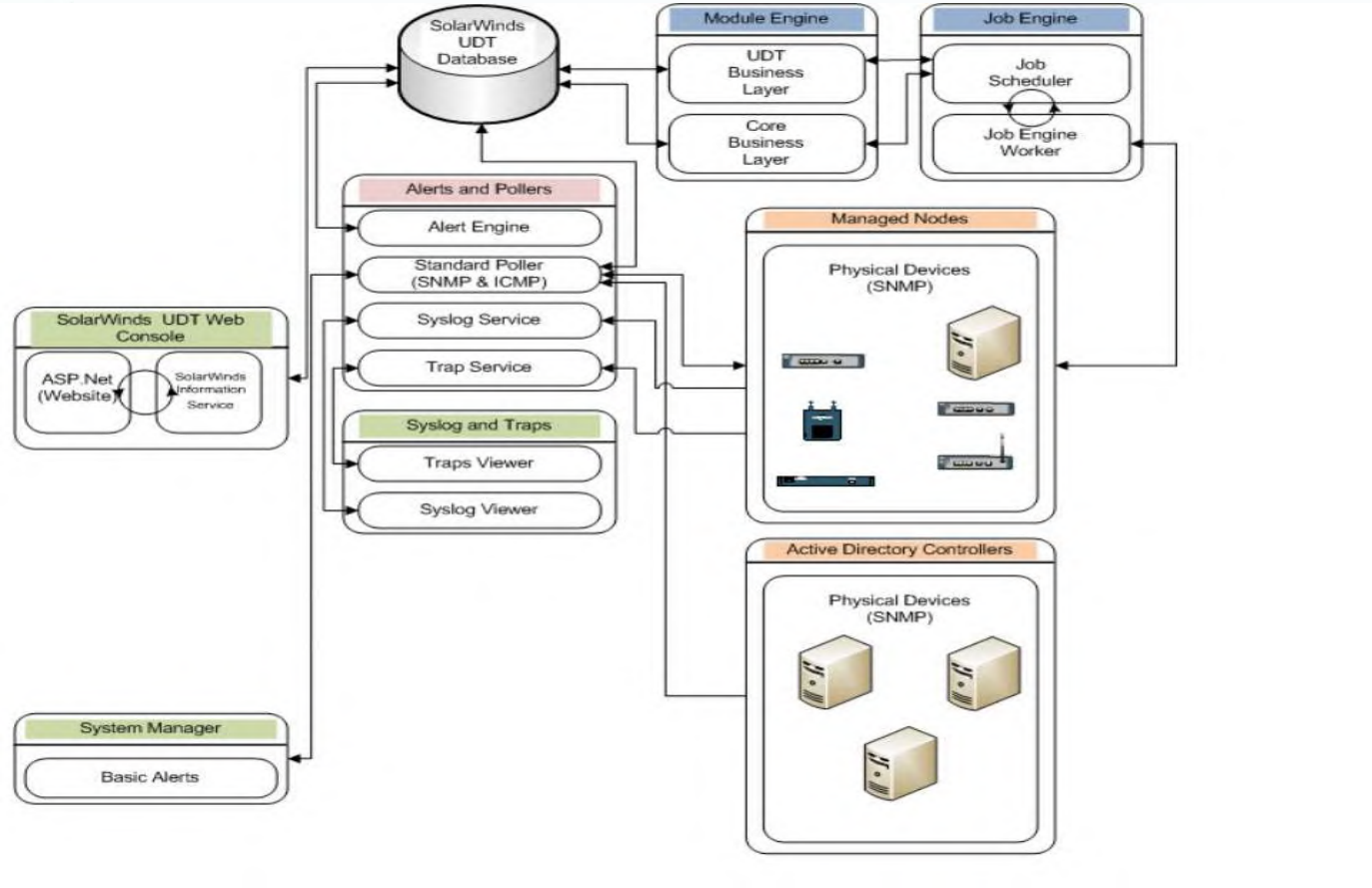


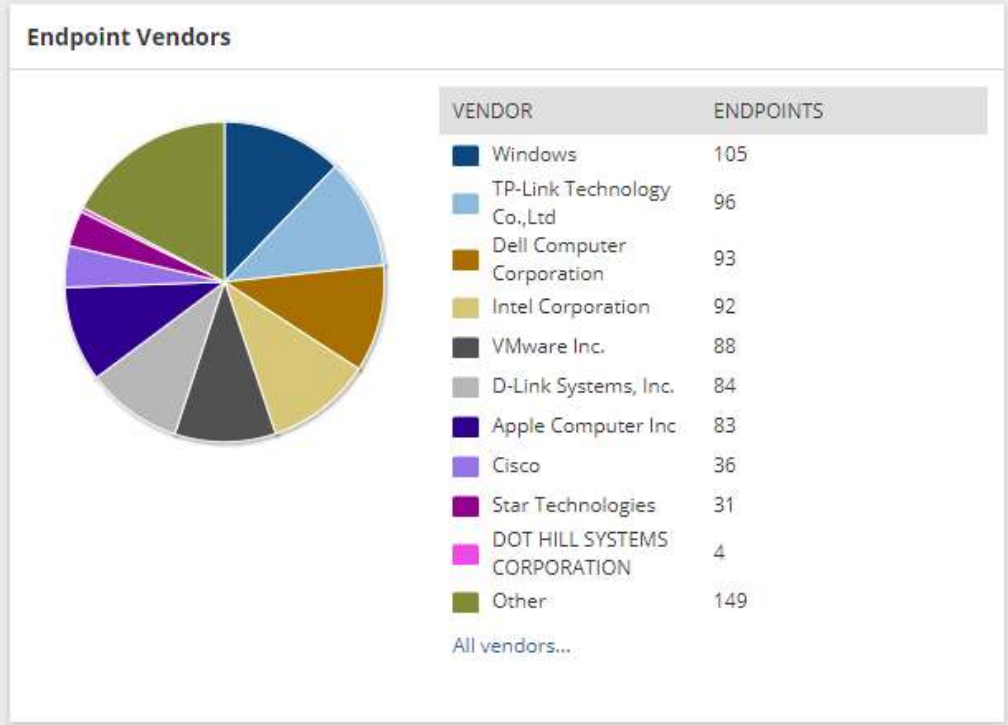



# UDT Architecture



# UDT Summary

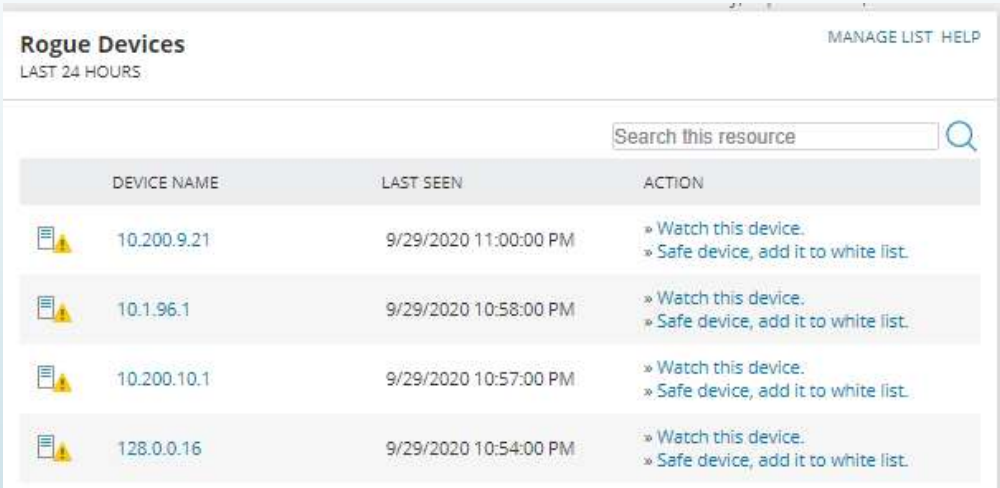
- Provides a list of UDT nodes, Endpoint vendors, Rogue Device and other widgets



# Views and Widgets in UDT

By default UDT has build it Widgets

- Device Inventory
- User Inventory
- Search
- Tracker port Details
- Access point details
- Tracker Endpoint Details



# Port Management

- Unmonitored Nodes
- Monitored Nodes
- Monitor and unmonitored ports

ADD NODE | EDIT PROPERTIES | UNMONITOR | MONITOR | SHUTDOWN | TURN ON | DELETE | Search

Page 1 of 1 | Page size 40 | Display

| Name | Node | MAC Address | Monitored |
|---|---|---|---|
| Fa0/0 | Anchorage-RTR | C2:02:03:D0:00:00 | Yes |
| Se2/0 | Anchorage-RTR | 00:00:00:00:00:00 | Yes |
| Se2/1 | Anchorage-RTR | 00:00:00:00:00:00 | Yes |
| Fa0/0 | Guam-RTR | C2:03:0D:C0:00:00 | Yes |
| Se2/0 | Guam-RTR | 00:00:00:00:00:00 | Yes |
| Se2/1 | Guam-RTR | 00:00:00:00:00:00 | Yes |
| Fa0/0 | Honolulu-RTR | C2:01:19:E0:00:00 | Yes |
| Se2/0 | Honolulu-RTR | 00:00:00:00:00:00 | Yes |
| Se2/1 | Honolulu-RTR | 00:00:00:00:00:00 | Yes |

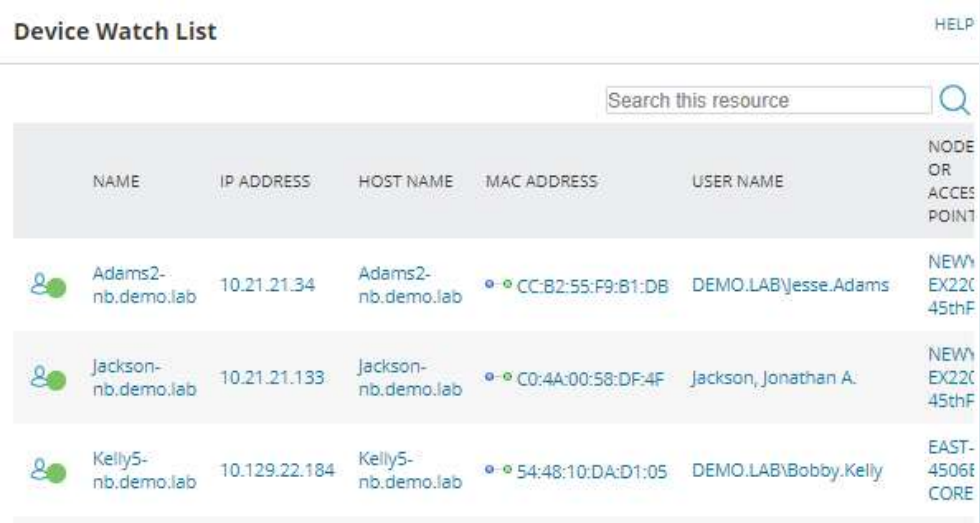
ADD NODE | EDIT PROPERTIES | UNMANAGE | REMANAGE | POLL NOW | DELETE | Search

Page 1 of 1 | Page size 40

| Name | Status |
|---|---|
| Anchorage-RTR | Node status is Down, Percent Packet Loss threshold is Critical, Hardware health monitoring is in Undefin |
| Se2/1 | Port is monitored. |
| Se2/0 | Port is monitored. |
| Fa0/0 | Port is monitored. |

# Manage Watch List

- Enables you to create a list devices and users. To see where they are located on your network



Device Watch List

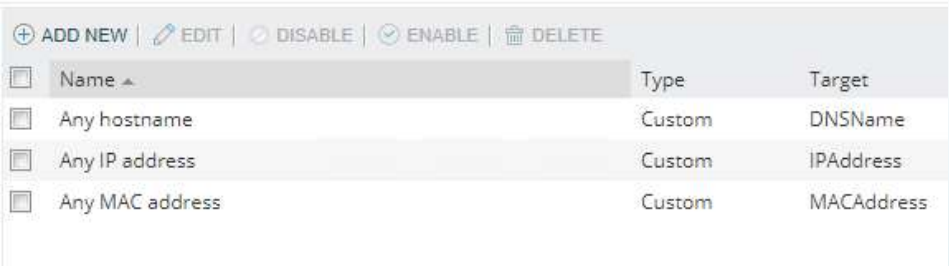
HELP

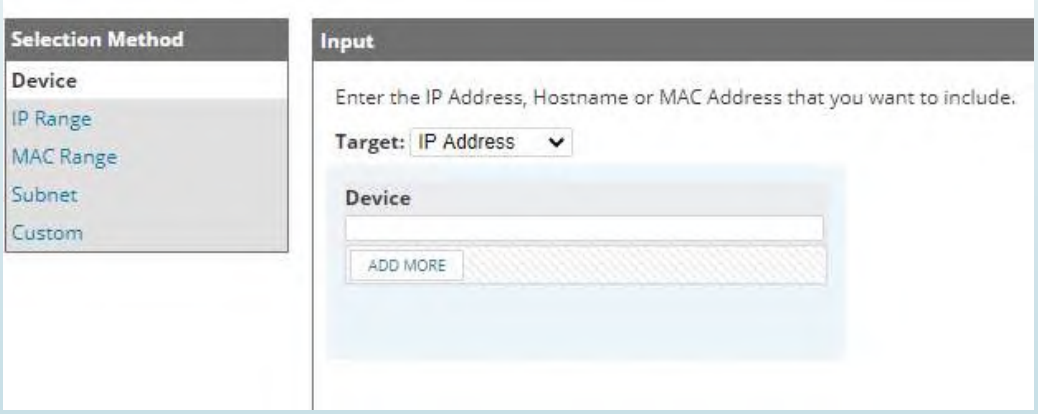
Search this resource

| NAME | IP ADDRESS | HOST NAME | MAC ADDRESS | USER NAME | NODE OR ACCES POINT |
|---|---|---|---|---|---|
| Adams2-nb.demo.lab | 10.21.21.34 | Adams2-nb.demo.lab | CC:B2:55:F9:B1:DB | DEMO.LAB\Jesse.Adams | NEW EX22 45thF |
| Jackson-nb.demo.lab | 10.21.21.133 | Jackson-nb.demo.lab | C0:4A:00:58:DF:4F | Jackson, Jonathan A. | NEW EX22 45thF |
| Kelly5-nb.demo.lab | 10.129.22.184 | Kelly5-nb.demo.lab | 54:48:10:DA:D1:05 | DEMO.LAB\Bobby.Kelly | EAST-4506 CORE |

# Manage White List

- Enables you to detect endpoints that are not considered safe, and displays these on the Rogue Device widget
- Enables which endpoints on your network to ignore

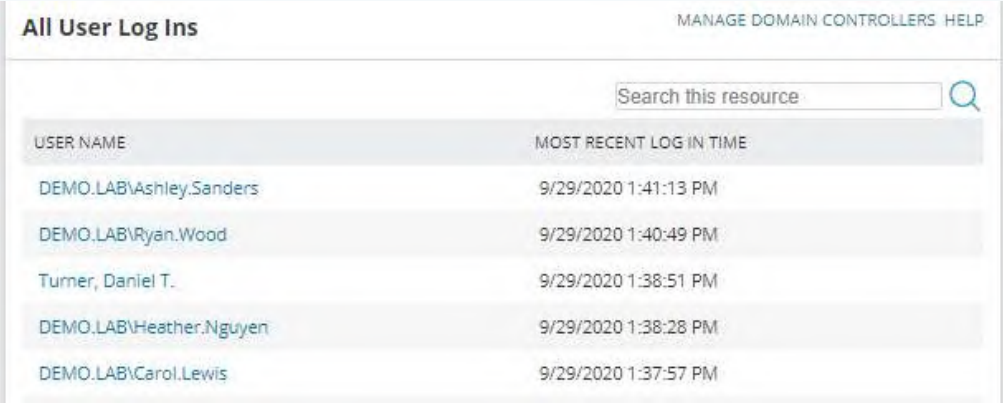


# Find a user's connection

The search bar allows you to track.

- Username
- Endpoint Hostname
- Endpoint IP Address
- Endpoint MAC Address
- Node name
- Node port
- Vendor

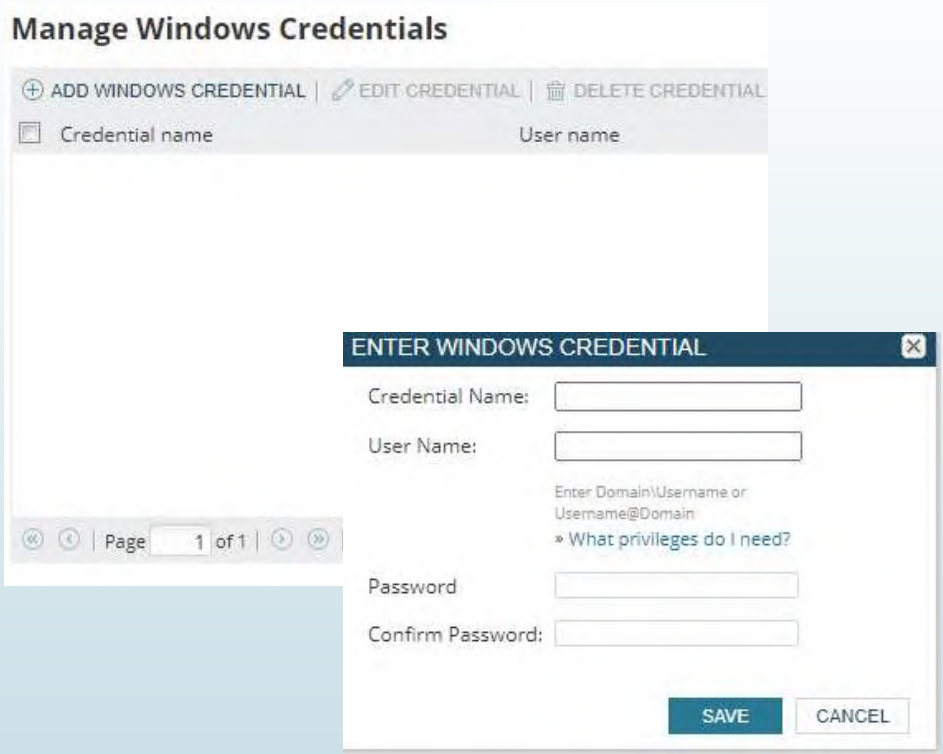


- User Device Tracker
- Walkthrough
  - Investigation
  - Identification

# DEMO

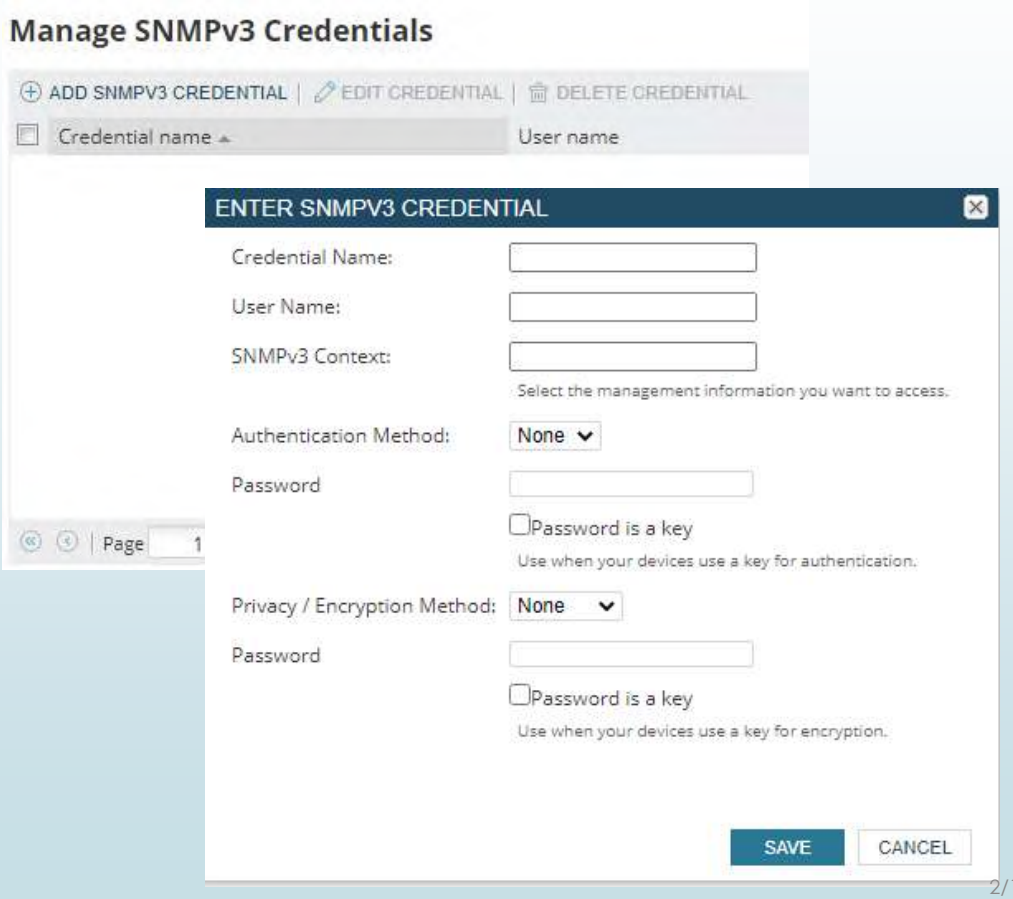
# Windows Credentials

- Is used for products such as (NPM, SAM, IPAM)
- Used to authenticate to servers
- Used to install SolarWinds Agent or WMI



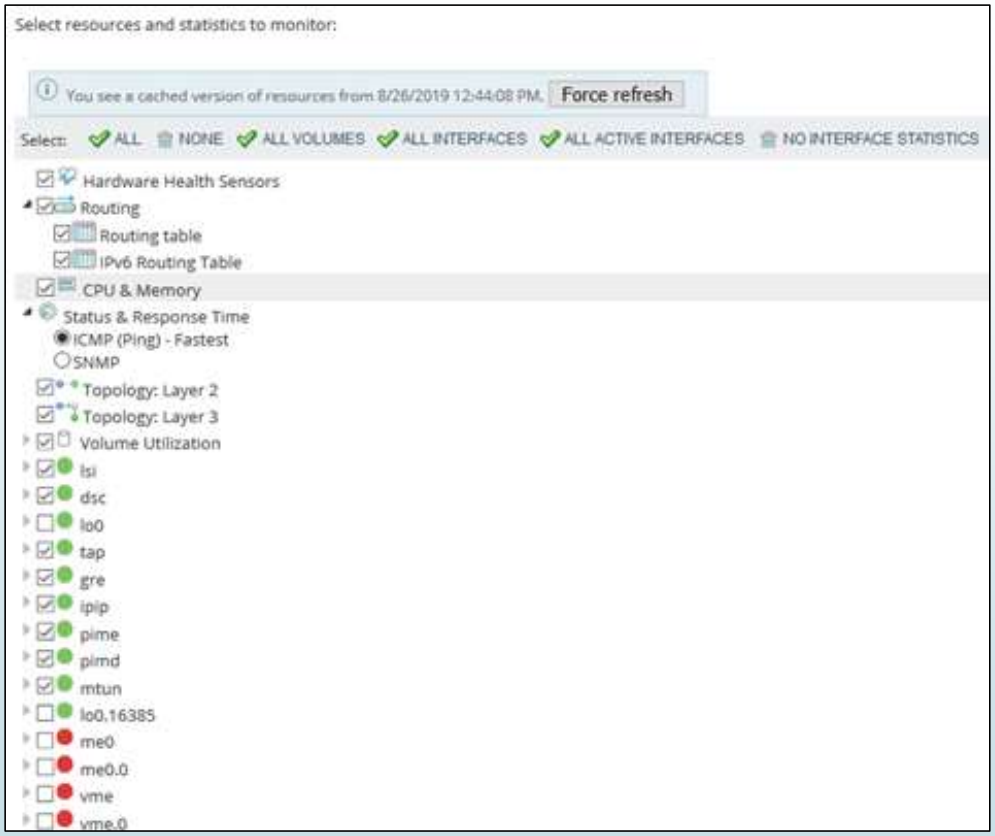
# Manage SNMPv3

- Create SNMP profile for Network devices
- Polls more than just up and down status
- Needs to be configured on Network devices as well



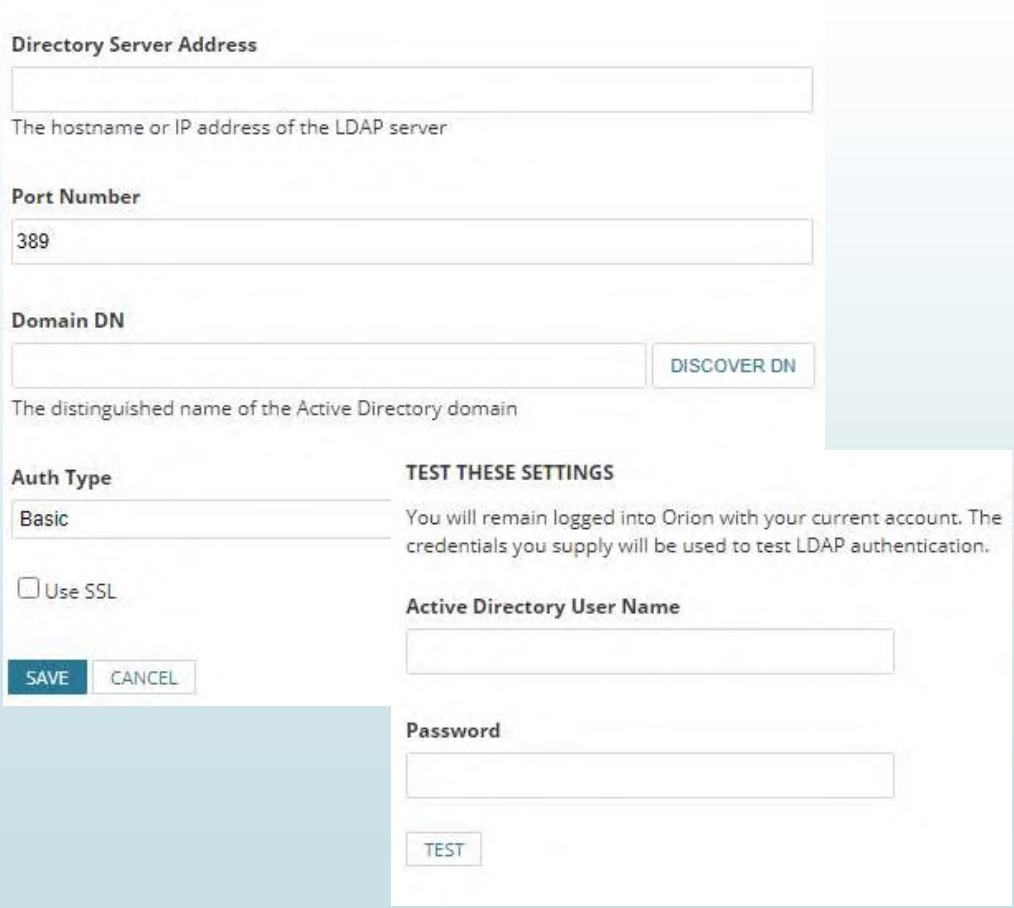
# Manage SNMPv3

- Provides list resources for the interfaces
- Provides routing tables and status & response time



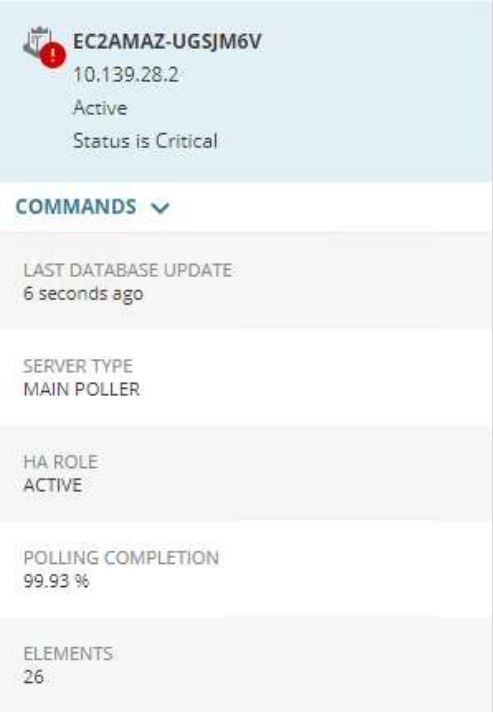
# Advanced AD Settings

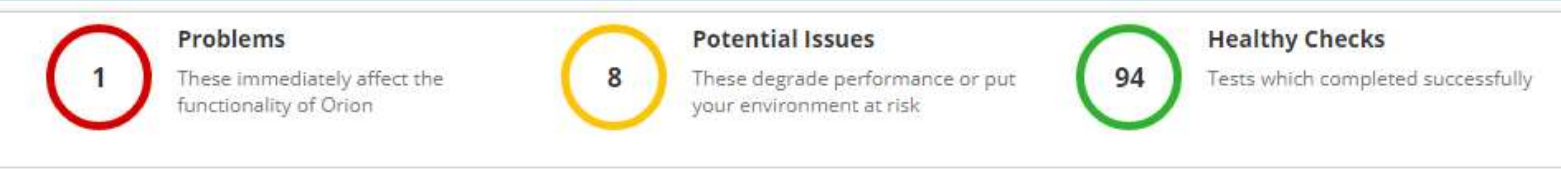
- SolarWinds can authenticate Active Directory via LDAP
- Enabling this feature will cause all SolarWinds AD accounts to authenticate with the LDAP settings



# My Orion Deployment

- Provides status update for servers
- Deployment Health
- Indications of pending issues with the Orion solution and monitoring of the IT Infrastructure



# My Orion Deployment

- Updates & Evaluations
- Diagnostics

**PRODUCT UPGRADES**

Click on the Servers tab at the top to see the status of your scalability engines and updates on all of

Updates are available for your environment. Let's get them installed. How does centralized upgrade wo

**Upgrade all products and evaluations to the latest version**

**Existing evaluations**

| | |
|---|---|
| User Device Tracker | Installed: 2019.4 HF 1 |
| NetFlow Traffic Analyzer | Installed: 2019.4 HF 1 |
| Network Performance Monitor | Installed: 2019.4 HF 1 |
| Network Configuration Manager | Installed: 2019.4 HF 1 |

**AVAILABLE EVALUATIONS**

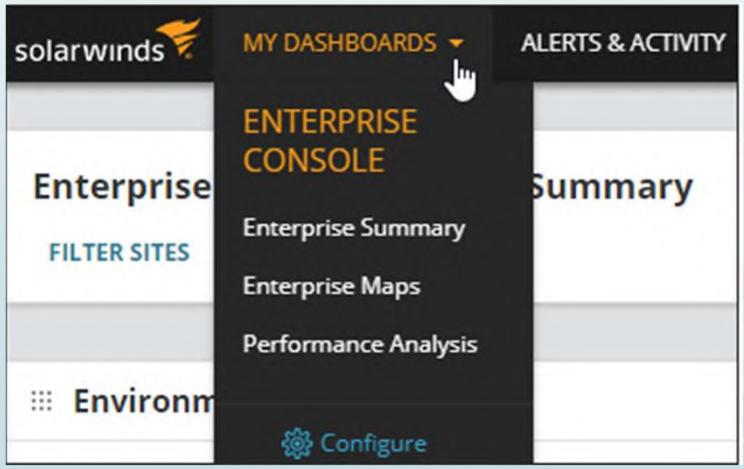
Based on the products you own, we think you might like these. If you'd like to try one, we can install while you upgrade.

☐ IP Address Manager
Simplify DHCP, DNS, and IP address provisioning and management

☐ Log Analyzer
Easily investigate log data to help identify the root cause of IT issues faster

# Enterprise Operations Console (EOC)

- What is Enterprise Operations Console?
- View Information from SolarWinds Sites
- Manage Reports in EOC



# Enterprise Operations Console

- What is EOC?

  EOC is an application which provides the ability to tie in other SolarWinds Orion Servers within the Air Force

- Why is EOC important?

  As each base develops their SolarWinds solution, it will provide rollup information to the higher-level Network Operations Security Centers

- How do I provide information for EOC to operate effectively?
  - Follow the standards set forth by this course
    - Example: Alerts and Reports written once
    - Example: If you move to another base the SolarWinds should be configured with the same baselines

# Enterprise Operations Console

- Manage other SolarWinds Sites
  - Ability to Manage data from the sites
- View Data from other SolarWinds Sites
  - Customization of Summary Widgets
  - Critical Status reviews
  - Alert Management from other Solarwinds Sites
  - Report Development from other SolarWinds Sites
  - Display Maps from other SolarWinds Sites

# Logging into EOC

- The first time you log in to SolarWinds EOC, the Discovery Central page opens. Click **Manage SolarWinds Sites** to begin adding sites or click **Go to Orion Home** to open the Enterprise Environment Summary view
- When you are logged in to the Web Console as an administrator, the Settings > All Settings option is available in the navigation bar. Use this option to manage user accounts and SolarWinds Sites, and to customize the Orion Web Console

# Adding/Managing a SolarWinds Site

- EOC can monitor SolarWinds Sites that meet the following requirements:
  - The SolarWinds Site must run on Orion Platform version 2016.1 or later
  - To determine the Orion Platform version, scroll to the bottom of the Orion Web Console window. All installed products are listed at the bottom of the window, as in the following image:

  - The UTC system time of the SolarWinds server must be within five minutes of the SolarWinds EOC server. For security reasons, SolarWinds EOC cannot communicate with SolarWinds servers that have a greater time difference

# Adding/Managing a SolarWinds Site

- Log in to EOC as an administrator
- Choose Settings > All Settings
- Under Getting Started with Orion, click **Manage SolarWinds Sites**
- Click **Add SolarWinds Site**
- Enter the IP address or host name of the SolarWinds server
  - SolarWinds EOC only supports SolarWinds servers with IPv4 addresses
  - SolarWinds EOC only recognizes host names that follow standard DNS naming conventions, which require that host names be composed of alphanumeric characters (A-Z, 0-9), the minus sign (-), periods (.), and underscore characters (_)
- Enter the URL of the SolarWinds Site's web console

# Enabling/Disabling a SolarWinds Site

- When you disable a SolarWinds Site, EOC does not display alerts, maps, status, or any other data from that site. The site remains in the list of monitored SolarWinds Sites, and you can enable it again to begin displaying site data
- Log in to the EOC Web Console as an administrator
- Choose Settings > All Settings
- Under Getting Started with Orion, click Manage SolarWinds Sites
- Select one or more SolarWinds Sites
- Click **Enable/Disable Site(s)** and choose an option from the drop-down menu
- The status column is updated with a status icon and description. For example:

# Administration of Credentials

- Accounts with administrator privileges are leveraged in order to add a site to EOC. This allows EOC to generate a least-privileged "system account" and establish a connection between EOC and the remote site. The system account is not visible from the remote site UI and its credentials are encrypted and stored in the EOC database
- Additional EOC user accounts configured for access to the new site will utilize this connection. If a user's account has custom credentials, the system account will impersonate the user in order to allow SWIS to apply settings and limitations according to the user's account access rights

- 15 Minutes

# Break

# Administration of Credentials

- User credentials:
  - Each EOC user or group account must be associated with the credentials of an account that can access the SolarWinds Site. The privileges granted to this account determine what site data the user or group members can access in EOC
  - The next slide shows how to associate SolarWinds Site user credentials with EOC accounts

# Administration of Credentials

- Create a default user account for the SolarWinds Site
- When you add or edit a SolarWinds Site, choose the Specify a default user account option to specify a default user account. This account is used by default for all EOC users with access to the site

**Default SolarWinds Site Account**

Select the following option to specify a default user account for this SolarWinds Site. specified in the EOC user account.

☑ Specify a default user account for this SolarWinds Site

**Username:**

Guest

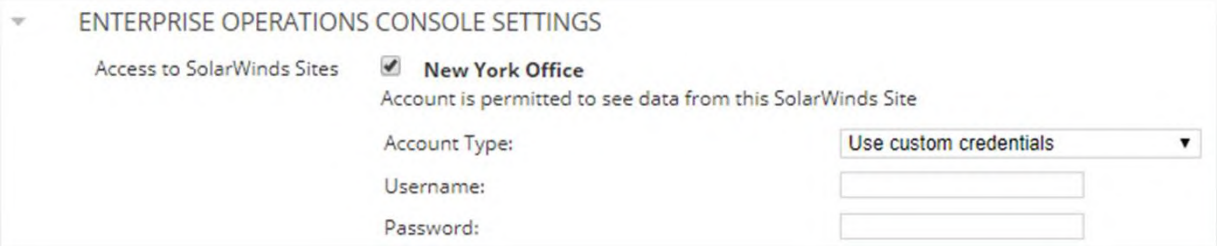
**Password:**

••••••••••••

- *Use this option if:*
  - *You did not establish a default user account for the site.*
  - *You want to associate this EOC account with an account that has different privileges than the default user account.*
  - *If an EOC account has access to a SolarWinds Site but is not associated with a SolarWinds Site user account, the Enterprise Summary view displays an error message and the user cannot access data from that site.*

# View and Filter of Consolidated Site Data

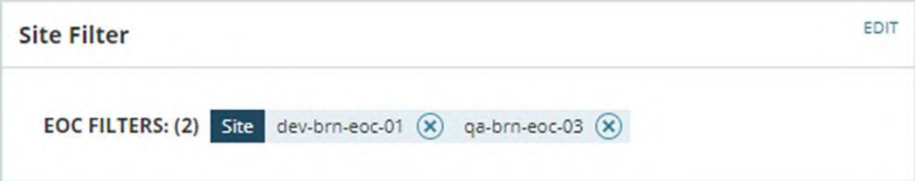
- Specify custom SolarWinds Site user credentials for an EOC account
- When you define which SolarWinds Sites a user can access, you can specify the SolarWinds Site user account used to determine what data this EOC user can access:




- Use this option if:
  - You did not establish a default user account for the site
  - You want to associate this EOC account with an account that has different privileges than the default user account
- If an EOC account has access to a SolarWinds Site but is not associated with a SolarWinds Site user account, the Enterprise Summary view displays an error message and the user cannot access data from that site

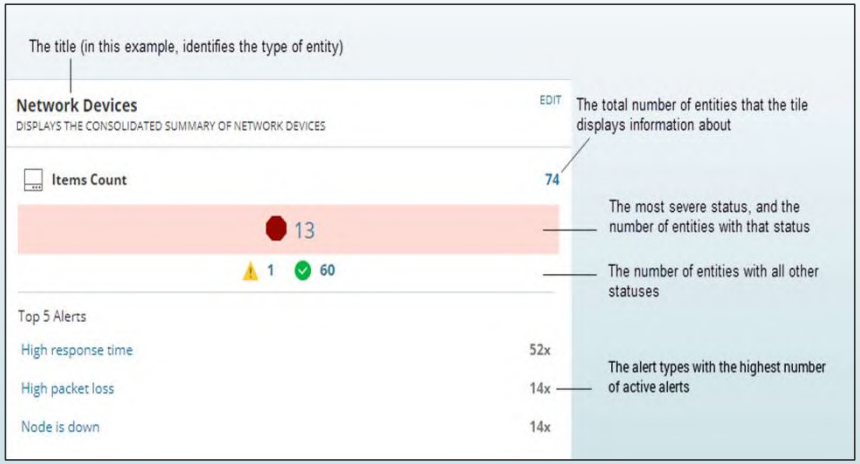
# View of Events/Messages/Alerts

- You can limit information on the Enterprise Environment Summary view to specific SolarWinds Sites:
  - At the top of the view, click **Filter Sites**
  - Select the SolarWinds Sites to include
  - If no sites are selected, all sites are included
  - Click **Apply Filters**
  - The sites whose data is being displayed are listed next to the Filter Sites option
  - To remove a filter, click the X next to it



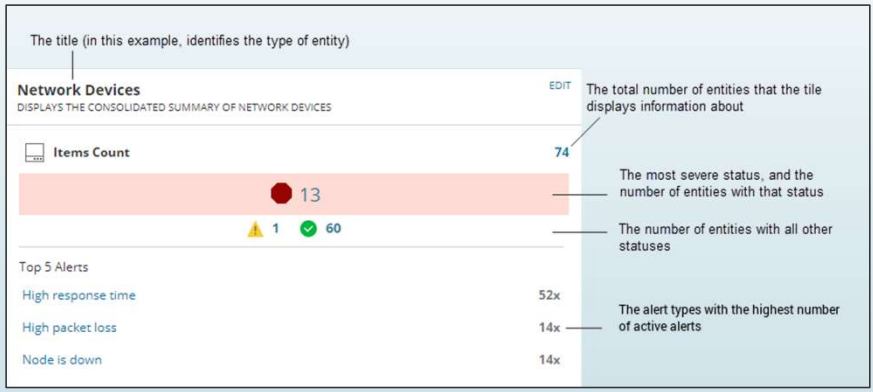
# View of Events/Messages/Alerts

- View summary data and drill through for details
- The Environment Summary widget aggregates information from your monitored sites. You can customize this widget to display the summary data that is most important to you
- By default, the Environment Summary widget displays one tile for each type of entity monitored at any active SolarWinds Site. An entity is any monitored item such as a node, a storage device, or an application. Each tile displays the following information aggregated from across all monitored sites. Use this information to identify critical issues and then drill through for more information



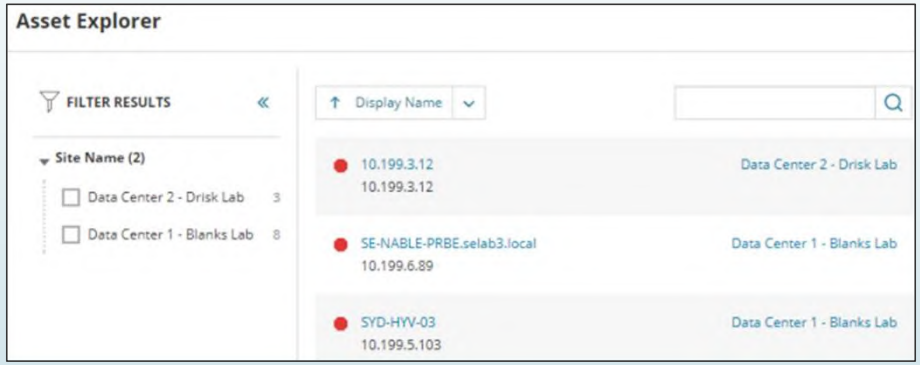
# View of Events/Messages/Alerts

- Click any link in the widget to display the associated list of entities or messages in the Asset Explorer
- Click the number in the upper-right corner to see a list of all entities represented by this tile
- Click the number next to a status symbol to see a list of entities in that status
- Click an alert to see a list of alerts of that type
- In this example, you can click the number next to the Down status symbol, and the Asset Explorer lists the network devices that are down



# View of Events/Messages/Alerts

- From the Asset Explorer, you can:
  - Filter or search to quickly find an entity
  - Click the entity name to open the SolarWinds Site and display information about that entity on the Details page
  - Click the SolarWinds Site name to open Home page for that site



# View of Events/Messages/Alerts

The All Alerts widget on the Enterprise Environment Summary view lists all active alerts ordered by the amount of time they have been active.

Display additional information:

- Click any link in the All Alerts widget to display additional information:
- Click the alert name to open the SolarWinds Site and display information about that alert on the All Alerts Details page
- Click the triggering object or related node name to open the SolarWinds Site and display information about that object or node on the Details page
- Click the SolarWinds Site name to open the Home page for that site
- You can acknowledge alerts from either the All Active Alerts widget or the All Active Alerts page

Show acknowledged alerts:

- To include acknowledged alerts in the list of alerts:
- Click the menu icon in the upper-right corner of the All Alerts widget
- On the drop-down menu, click **Configure**
- Select Show Acknowledged Alerts and click **OK**

# Acknowledge and Clear Events/Messages/Alerts

- Clearing an event removes it from the Message Center and the Events page. Clearing an alert removes it from the Message Center and marks it as Acknowledged on the Alerts page in EOC and on the SolarWinds Site:
  - To clear events or acknowledge alerts, users must have the Allow Account to Clear Events privilege
  - Choose Alerts & Activity > Message Center
  - The Message Center lists events, audit events, and alerts from all enabled SolarWinds Sites
  - Select individual events or alerts or click **Select All**
  - Click **Clear Selected Messages**
- Selected events are removed from the view. Selected alerts are removed from the Message Center view and identified as Acknowledged on the All Active Alerts page

# EOC Maps Display/Import/Add

- To import maps:
  - Log in to SolarWinds EOC as an administrator
  - Click **Settings > All Settings**
  - In the Product Specific Settings group, click **EOC Settings**
  - Click **Import maps**
  - The Import Maps From Remote Sites page lists the maps available on all SolarWinds Sites. By default, maps are listed alphabetically by map name
  - To filter the maps by SolarWinds Site, select the sites to include under Filter Results in the left pane
  - Select the maps you want to import and click **Next**
  - Review the list of selected maps and click **Next**
  - When the maps are imported, click **Done**
- You can now add the maps to views underneath the Enterprise Maps menu
- Imported map definitions are not automatically updated in EOC. If the map definition changes on the SolarWinds Site, reimport the map to view the updated version in EOC

# EOC Maps Display/Import/Add

- Add map widgets to the Enterprise Maps - Summary view, or to a custom subview created within this view. Then display imported maps within these resources. Users can view the maps by clicking **My Dashboards > Enterprise Maps**:
  - Log in to SolarWinds EOC as an administrator
  - Add the map widget:
    - Click **Settings > All Settings**
    - In the Views group, click **Manage Views**
    - In the list of views, select Enterprise Maps - Summary or a custom subview
    - Click **Edit**

# EOC Maps Display/Import/Add

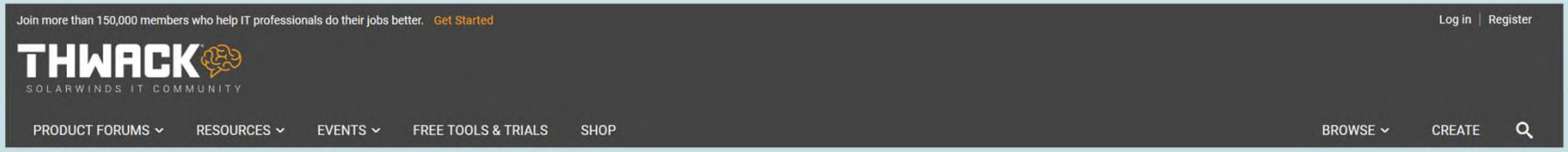
- The **Customize Enterprise Maps** page opens:
  - Click the **+** icon next to the column where you want to add the map widget
  - To list only map widgets, select **Type** under **Group By** and then select **Network Maps**
  - Select the widget type (for example, Map)
  - Click **Add Selected Resources**
  - Click **Done**
- Display the map in the widget:
  - Click **My Dashboards** > **Enterprise Maps**. If you added the map to a subview, select the subview
  - In the upper-right corner of the map widget, click **Edit**
  - In the Title field, enter a descriptive name
  - Select the map
  - Click **Submit**

- Demonstrations to be completed in class by connecting all users Orion Servers together from Instructors workstation

# DEMO

# Additional Resources

- Solarwinds Online Community – THWACK!
- Solarwinds Academy
- Success Center
- Other Bases
  - Other bases using the same system may have solved issues you are having
- Knowledge Base on Orion Platform Server
  - The Orion Platform Server will have a KB directory of all the documentation relating to this course
- Air Force ARC Helpdesk
  - Comm: 334-416-5771
  - DSN: 312-596-5771
  - Email: arc@us.af.mil



# SolarWinds Academy

**Additional Training Options**

- Instructor led classes are available in the Customer Portal
- How to webinars on popular topics
- Article and video based tips for getting started by product
- Visit the SolarWinds Lab on THWACK
- View popular panels from THWACKcamp 2018
- View Virtual Classroom calendar

**Smart Start Assisted Onboarding**

This program gives customers and partners one-on-one expert guidance, enabling them to quickly and effectively configure, customize and optimize their SolarWinds environments.

Learn more about Smart Start

SOLARWINDS ACADEMY

The SolarWinds Academy provides relevant and high quality education programs for IT Professionals. Our training curriculum promotes a comprehensive understanding of the SolarWinds portfolio of products through certifications, instructor-led classes, and eLearning videos.

**eLearning**

The online eLearning library contains training videos to help you learn about your product and setup, including key features and popular optimizations.

Access eLearning

**Classes**

The SolarWinds Academy offers both fundamental and intermediate level classes where you can learn about your products deployment, configuration, and more.

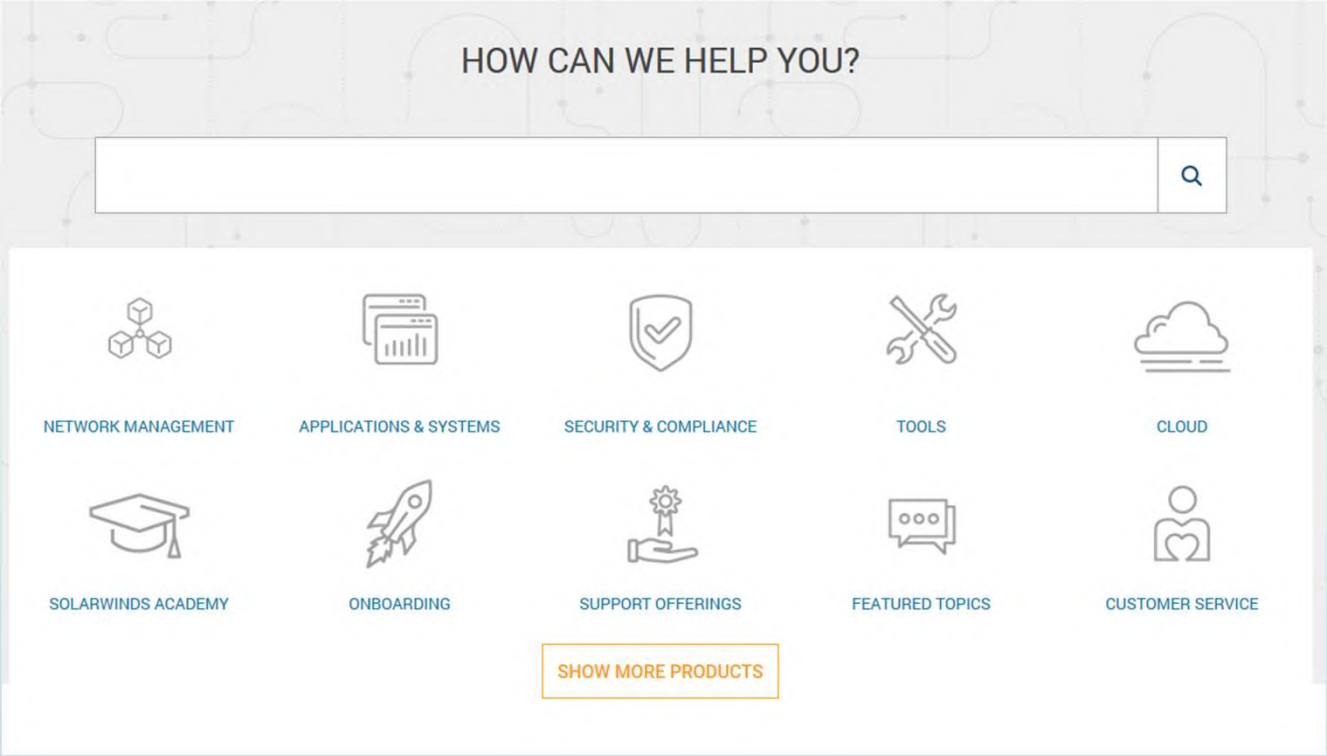
Access Classes

**Certification**

The SolarWinds Certified Professional program is a suite of product certifications that shows you have the knowledge and skills needed to manage and administer SolarWinds software.

Access Certification

# Success Center



300

- 1 Hour

# Lunch

# Welcome Back!

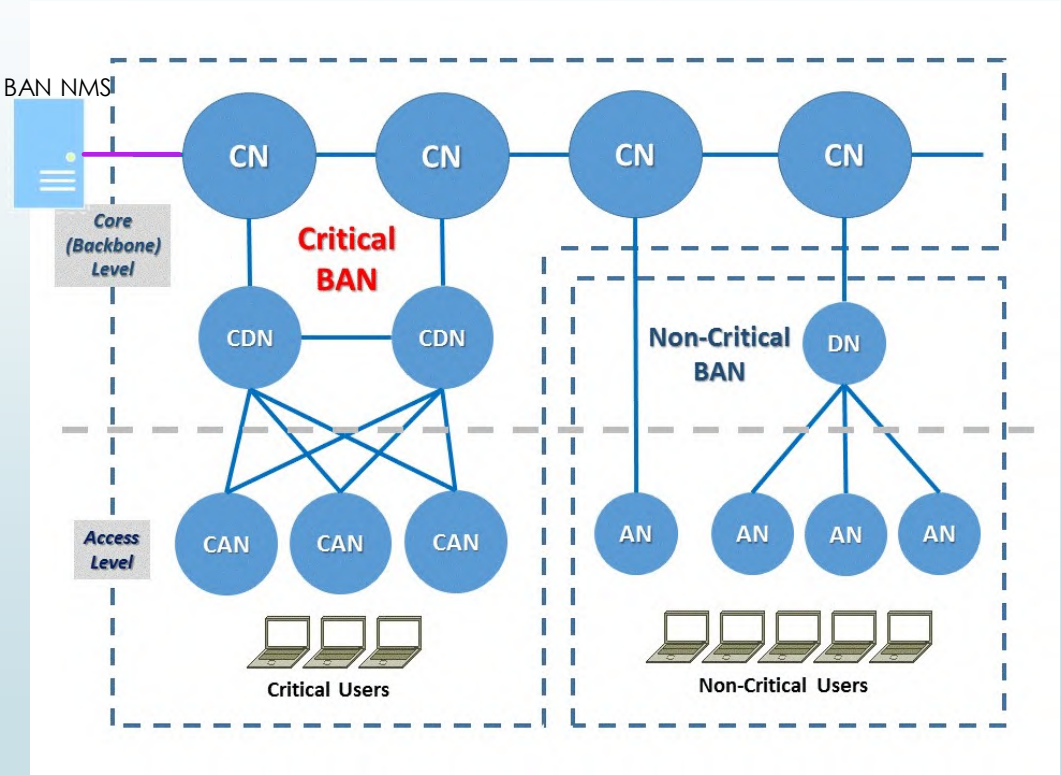
Before we continue with todays class there will be a short quiz to see what we have learned.

# BAN NMS

- Architecture as deployed
- Security as deployed
- Disaster Recovery

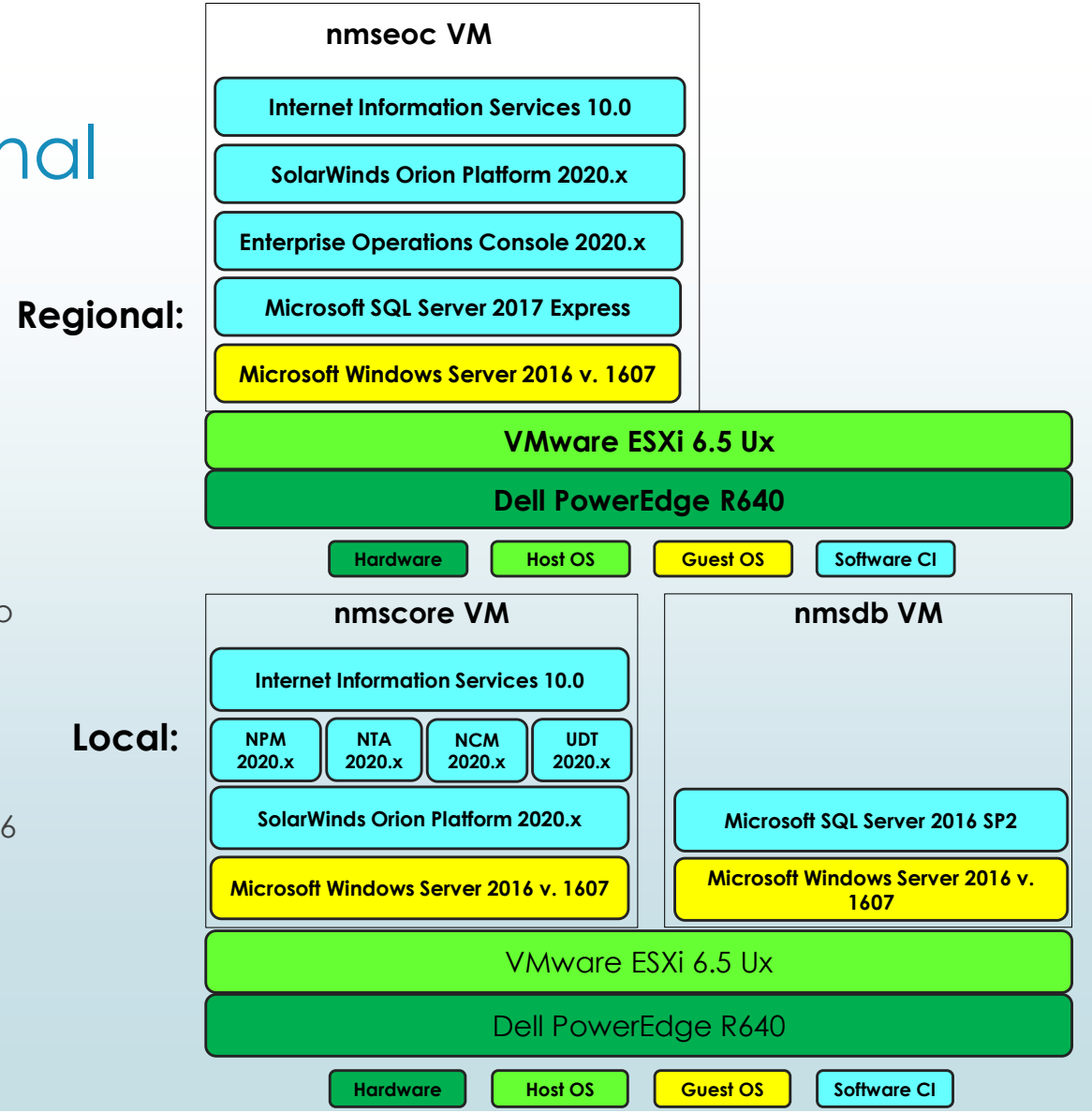
# Architecture - USAF BITI BAN

- BAN NMS
- Critical BAN Nodes:
  - Core Nodes
  - Critical Distribution Nodes
  - Critical Access Nodes
- Non-critical BAN:
  - Distribution Nodes
  - Access Nodes



# Local and Regional Differences

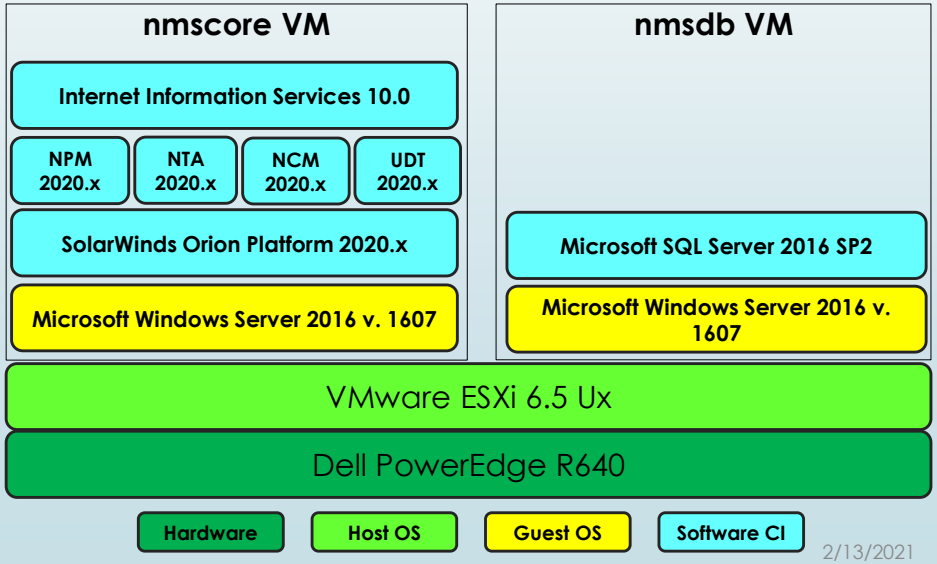
- REG NMS:
  - VM – nmseoc
  - EOC Module
- Local NMS:
  - VMs – nmscore, nmsdb
  - NPM, NTA, NCM, UDT Modules
- Guest OS:
  - REG NMS WIN SVR 2016
  - Local NMS WIN SVR 2016, MS SQL 2016



# BAN NMS Overview

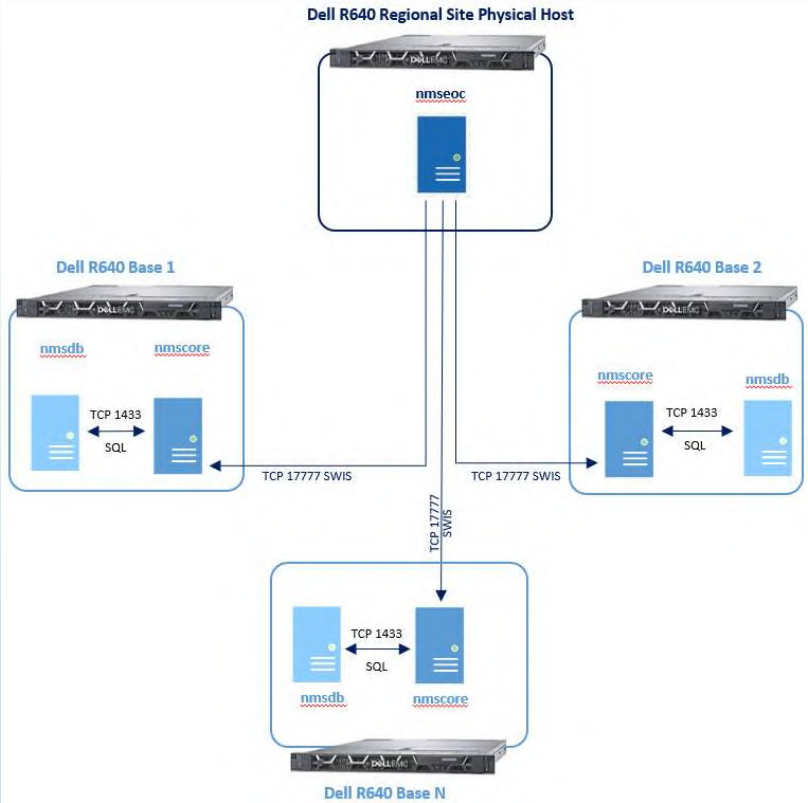
- System Overview of the BAN NMS Architecture:
  - Host
  - Hypervisor/Host OS
  - VMs/Guest OS

**Local:**



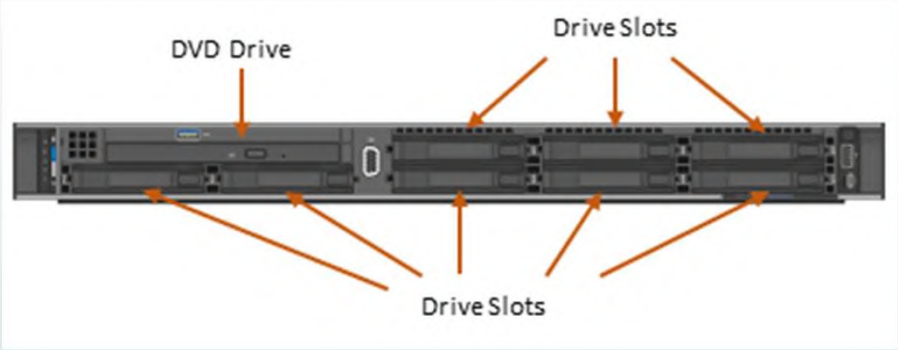
# BAN NMS Architecture Overview

- System Overview of the BAN NMS Architecture:
  - The Base BAN local instance of Solarwinds Orion Platform is to monitor the BITI Wired network.
  - The EOC at the regional NOSC location will connect to the base level instances and provide situational awareness to the AF management.

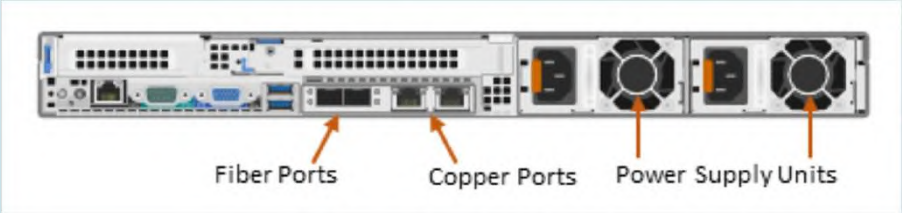


# NMS Host – Dell EMC PowerEdge R640

- Front View




- Rear View



# NMS Host

- Dell EMC PowerEdge R640 Installation and Service Manual

| Information Type | Supplemental Data |
|---|---|
| Front Panel Illustration, call-outs, descriptions | Pg. 10, Figure 2, Table 1. |
| Front Left control panel Illustration, call-outs, and button/ LED descriptions | Pg. 13-14, Figure 5, Table 4. |
| Front Status LED indicators and descriptions | Pg. 14-15, Table 5. |
| Front System health and system ID indicator codes. | Pg. 16, Table 6. |
| Front Right control panel. | Pg. 16, Figure 6, Table 8. |
| Back view of system. Port Identification. | Pg. 19-20, Figure 8, Table 11. |
| Back NIC indicator codes | Pg. 22, Figure 10, Table 13. |
| Power supply unit indicator codes | Pg. 22-24, Figure 11, Tables 14 and 15. |
| Back Drive Indicator Codes | Pg. 25, Figure 12, Table 16. |
| Back LCD Panel: Home Screen, Set Up, View Menu | Pg. 25-27, Figure 13, Table 17. |
| Locating the Service Tag of your system. | Pg. 27, Figure 14. |
| System information label | Pg. 28-29, Figure 15, Figure 16. |
| Ports and connectors specifications: USB, NIC, Serial, VGA | Pg. 35-38, Table 24 (Eight hard drive system) |

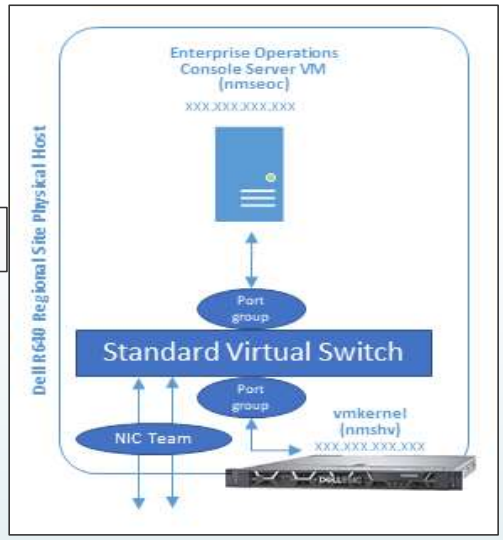
- 15 Minutes

# Break

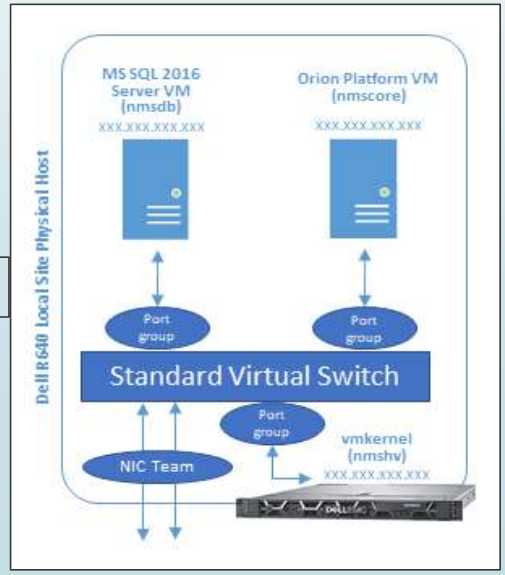
# NMS Hypervisor/Host OS

- VMWare ESXi 6.5 U2 (hypervisor)
- Microsoft Server 2016
- Microsoft SQL Server 2016 SP2 Standard

**Regional:**




**Local:**



# NMS VMs/Guest OS

- The BAN NMS resides on a Dell PowerEdge R640 (Dell R640) server and implements the VMWare ESXi 6.5 U2 hypervisor to create two virtual machines (VMs) for the Local site system. The Local solution will provide management tools for the Local site critical BAN nodes. The names of these machines and their contents are as follows:
  - nmscore – The Orion Platform, Web Server, and Main Poller.
  - nmsdb – The Orion database, a Microsoft SQL Server (utilizing Microsoft SQL Server 2016 SP2).
- The Regional site solution houses a single VM to monitor the Local solutions. The name of this machine and its contents are as follows:
  - nmseoc – The Enterprise Operations Console (for the regional system only).

# Security – BITI BAN NMS

- Common Access Card (CAC) Usage
  - Access to the Orion Web Console will be granted through the use of a CAC
- Limitations using CAC/tokens
  - Network Atlas
    - Recommend an Orion Individual Account for map usage only
  - Deployment Health
    - Questionable at this time
  - Report Scheduler
    - Manual interaction required
    - Visit for option: https://support.SolarWinds.com/SuccessCenter/s/article/Create-a-dedicated-report-scheduler-website-for-use-in-a-CAC-card-environment

# Disaster Recovery

- Configuring the Network
- Configure NTP
- Configure Server Certificates
- Activate Image
- Joining the Domain
- Software Licensing
- Booting Shell
- Configure Application

# Configure the Network – Local Site

- Power on the R640 by pressing the power button on the front panel.
- At the VMware ESXi main screen, press **F2.**
- Log into the Hypervisor with the username **root** and enter <**password**>.
- On the main menu, click **Configure Management Network** and press **ENTER**.
- Click **Vlan** and press **ENTER**.
- Enter <**vlan**> number and press **ENTER**.
- Click **IPv4**, press **ENTER**.
- Click **Static**, press spacebar.
- Enter <**IP Address**>, <**Subnet Mask**>, <**Default Router**> and press **ENTER.**
- Click **DNS Configuration** and press **ENTER.**
- Click **Use the following DNS server addresses and hostname** and press the spacebar.
- Enter <**Primary DNS Server**> server address, <**Alternate DNS Server**> server address, <**Hostname**> and press **ENTER**.
- Press **ESC** to exit.
- Press **Y** to confirm.
- Press **ESC** to log out of the Hypervisor.

# Configure the Network – Regional Site

- Power on the R640 by pressing the power button on the front panel.
- At the VMware ESXi main screen, press **F2.**
- Log into the Hypervisor with the username **root** and enter <**password**>.
- On the main menu, click **Configure Management Network** and press **ENTER**.
- Click **Vlan** and press **ENTER**.
- Enter <**vlan**> number and press **ENTER**.
- Click **IPv4**, press **ENTER**.
- Click **Static**, press spacebar.
- Enter <**IP Address**>, <**Subnet Mask**>, <**Default Router**> and press **ENTER.**
- Click **DNS Configuration** and press **ENTER.**
- Click **Use the following DNS server addresses and hostname** and press the spacebar.
- Enter <**Primary DNS Server**> server address, <**Alternate DNS Server**> server address, <**Hostname**> and press **ENTER**.
- Press **ESC** to exit.
- Press **Y** to confirm.
- Press **ESC** to log out of the Hypervisor.

# Configure the Network Card Port

- The baseline image for both the local BAN NMS and the regional BAN NMS are pre-configured to use copper connectivity (NIC3 and NIC4).
- If fiber connectivity is to be used, execute the steps outlined in the TO(I), Table 4-3, to configure the BAN NMS appliance for fiber connectivity (NIC1 and NIC2).

# Configure the NTP

| Action | Configuration Command |
|---|---|
| **Set NTP Source** | PS > $NTPServers = <NTP Server IP Address> |
| | PS > Get-VMHost \| Add-VMHostNTPServer $NTPServers |
| | PS > Get-VMHost \| Get-VMHostService \| Where {$_.Label -eq "NTP Daemon"} \| Set-VMHostService -Policy On |
| | PS > Get-VMHost \| Get-VMHostService \| Where {$_.Label -eq "NTP Daemon"} \| Start-VMHostService |

# Configure the Server Certificates

- Creating a Certificate Signing Request.
- Sending Certificate Signing Request Information.
- Receiving the Certificate Signing Request Information.
- Installing the New PKI Server Certification.

# Activating the Image

- Configuring Host Specific Settings
  - Bring Disks Online
  - Joining the Domain
  - Using the Software Licensing User Interface
  - Creating a Certificate Signing Request
  - Sending Certificate Signing Request Information
  - Receiving the Certificate Information
  - Installing the New PKI Server Certificate

# Activating the Image

- Configuration of Database Specific Settings
  - Installation of the SQL Database
- Configuration of Core Specific Settings
  - Update Host Name in Database Tables
  - Run the SolarWinds Configuration Wizard

# Joining the Domain

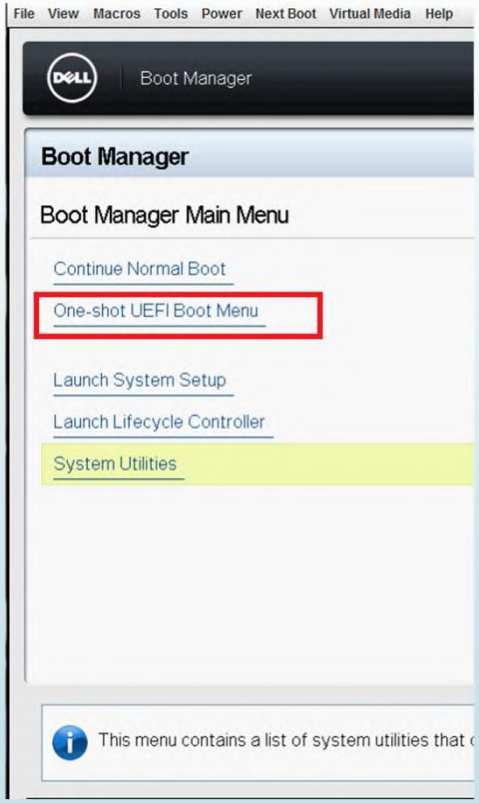
- Execute the following steps to join the BAN NMS server to the domain.
  a. Using a networked AF laptop, remote desktop into the <**NMS IP Address**> for a local BAN NMS, or the <**EOC IP Address**> for a Regional BAN NMS using standard windows procedures.
  b. Log into the server using **nmsadmin** for the username and <**password**>. (See Section 2.6, Table 2-11 for variables)
  c. Open a run prompt and type sysdm.cpl.
  d. Click **Change** and select the domain radio button.
  e. Enter the <**domain name**> and click **OK**.
  f. Enter base supplied domain credentials to join the domain.

# Software Licensing User Interface (UI)

- The following steps illustrate the procedure for activating Windows Server 2016 through the Software Licensing User Interface:
  a. Using a networked AF laptop, remote desktop into the <**NMS IP Address**> for a local BAN NMS, or the <**EOC IP Address**> for a Regional BAN NMS using standard windows procedures.
  b. Log into the server using **nmsadmin** for the username and <**password**>.
  c. Click **START** button.
  d. Type **RUN**.
  e. Type **slui 3** and click **ENTER** (Software Licensing User Interface). This brings up the "Enter a Product Key Dialog" box.
  f. Type in the <product key> provided in the field

# Booting the Shell Environment

- To perform the boot sequence:
  a. Using standard Windows procedures, create a boot CD from the WinPE.iso listed in required media, TO (I), Section 2.10.
  b. Power on the Dell R640:
     1. Press **F11** to display the Boot Manager (Figure 4-1 of TO (I) and choose **One-shot UEFI Boot Menu**.
     2. Choose to **boot from CD\DVD**.
  c. Select **Exit**. The R640 will reboot to the CD\DVD.



# Configuring the Application

- Follow the instruction in Place the installation media in the Server CD ROM Drive.
- Update Host Name in Database Tables.
- Run the SolarWinds Configuration Wizard.
- Logging into the BAN NMS.
- [Applying the] Required Licensing.
  - Generating the License Files.
  - Activating the Licenses.
- Configure the Active Directory Settings.

# Backup Network Configuration Files

- Network Devices configurations will backup to the C: by default.
- Realign default location to the SolarWinds Install path
  - Settings > All Settings > NCM Settings > Configs
    - Edit "Configuration Location" path to SolarWinds install path.

# Backup SQL Database

- The BAN NMS stores configuration and historical data in a database called the SolarWindsOrion database. Follow the steps below to backup this SQL database:
  - Using standard windows procedures, RDP into the NMSDB server.
  - Open SQL Management Studio.
  - After connecting to the NMSDB instance of the Microsoft SQL Server Database Engine, in Object Explorer, click the server name to expand the server tree.
  - Expand **Databases** and select the **SolarWindsOrion** database.
  - Right-click the **SolarWindsOrion** database, point to Tasks, and then click **Back Up**. The Back Up Database dialog box appears.
  - In the Database list box, verify the database name is SolarWindsOrion.
  - In the Backup type list box, select **Full**.
  - For Backup component, click **Database**.
  - Either accept the default backup set name suggested in the Name text box or type a different name for the backup set.
  - Choose the type of backup destination by clicking **Disk**.
  - Choose a destination, the default is E:\Backup\.
  - Click **OK** to complete the backup operation.
  - Repeat steps 3.2 e through 3.2 l for database SolarWindsFlowStorage.

# End of Day – End of Class

- Thank you for allowing me to teach you about the BITI BAN NMS Project and SolarWinds Enterprise Management Tools

# Questions and Answers