Training Goals:

This course is designed for those Network and/or System administrators tasked with the installation, configuration, and maintenance of the Network Node Manager i (NNMi) product. This course teaches the skills needed to successfully implement the product to manage small, medium, or large networked enterprises. The course includes training on the NNM i Smart Plug-In (NNM iSPI) Performance for Metrics Software, and NNMi Smart Plug-In Engineering Toolset. This course is designed for administrators of NNMi 2018.x. The hands-on lab exercises in this course use NNMi version 2018.05.

Upon successful completion of this course, you should be able to:

- Configure network discovery
- Manipulate NNMi tables and device object records
- Design topology maps
- Configure incidents
- Generate performance graphs
- Generate performance reports
- Perform core administration tasks
- Manage an ESXi virtual environment
- Describe the features available in the iSPI for Engineering Toolset

Audience/Job Roles

This course is intended for network or system administrators and network engineers seeking more in-depth knowledge of Network Node Manager i 2018.x.
CONSPECT:

- Introduction to Network Node Manager i (NNMi) Software
  - Describe how NNMis supports best business practices
  - Describe how NNMi fits in the family of management products
  - Differentiate NNMi and NNMi Advanced feature sets
  - List add-on and integrated products available
  - Describe how NNMi supports efficiency and effectiveness in managing your complex network

- Managing SNMP and ICMP Communication
  - Configure authentication for SNMPv1, SNMPv2, SNMPv3 (individual, region, type, filter, default)
  - Configure alternative authentication names
  - Use an alternate SNMP port or timeout
  - Use an SNMP proxy
  - Use the SNMP Command Line Interface (CLI)

- Discovery Architecture and Operation
  - Describe what NNMi discovers, how far, which objects
  - Describe how NNMi groups discovered objects
  - Describe how NNMi discovers connectivity
  - Describe limits of duplicate IP address management

- Configuring Discovery
  - Turn auto-discover (inventory) on/off
  - Schedule discovery
  - Initiate manual discovery (single, group, all nodes)
  - Expand discovery (single node, from file, for region)
  - Limit discovery (filter by region, type, node or interface level, before/after SNMP query)
  - Recheck node configuration
  - Recheck connectivity
  - Remove discovered objects (individually, by filter, by region)

- Using the Management Console
  - Start the NNMi console
  - Locate workspaces
  - Navigate tables, maps, views, and forms
  - Access object details
  - Working with Performance and Overview Dashboards
- Sort and filter tables
- **Configuring Node and Interface Groups**
  - Describe how node and interface groups are applied in NNMi
  - Configure a group by object type, region, specific object, default
  - Use advanced filtering on object capabilities
- **Customizing Views**
  - Create a map of a node group
  - Place the map in the list of topologymaps
  - Control the default map displayed when the console opens
  - Add a background to amap
  - Control status propagation
  - Add connections to Path View maps
- **Status Monitoring Architecture and Operation**
  - Differentiate between fault monitoring and performance monitoring
  - Identify data gathered for interface monitoring and component health
  - Describe the roles of State Poller service and Causal Engine
  - Describe the operation of neighbor analysis
- **Customizing Status Monitoring**
  - Turn polling on/off (specific nodes, region, type)
  - Set polling interval by node or interface group
  - Set objects to out-of-service mode
  - Select polling protocol and set of data to be gathered
  - Verify the polling settings for an object
  - Perform an on-demand status poll of an object
  - Check polling backlog/performance
  - Exclude objects from status polling (individual, region, type)
- **Configuring Users**
  - Configure a user account for each of your NNMi users with the appropriate capabilities
  - Describe what each user group may access in the console
  - Configure Custom Security groups
  - Configure tenants
  - Configure command-line permissions
  - Audit account activity
- **Troubleshooting Network Issues**
  - Describe the incident life cycle, assignments and ownership, and states
  - View network incidents and incident details
○ Sort and filter incidents
○ Assign and reassign incidents
○ Delete an incident
○ Annotate an incident
○ View historical incidents (closed)
○ Cross-launch to graphical visualization
○ Interpret root cause incidents
○ Launch and interpret network visualization (different types)
○ List nodes, interfaces, and addresses in the network
○ View object details
○ Filter a view by node group or interface group
○ Invoke troubleshooting tools
○ Check the status and configuration of a device
○ Display incidents for a device

○ Troubleshooting Using MIBs
  ○ Describe the use of Management Information Base (MIB) browsing and graphing during troubleshooting
  ○ Graph MIB data
  ○ Browse MIB data

○ Event Monitoring
  ○ Describe event sources and processing

○ Customizing Event Monitoring
  ○ Add and delete event definitions
  ○ Customize event category/severity/message
  ○ Create a new category or family
  ○ Add vendor trap definitions
  ○ Exclude an event from the display
  ○ Block trap storms
  ○ Block reception of events

○ Thresholds and Custom MIB Monitoring
  ○ Configure iSPI Performance for Metrics Software thresholds and incidents
  ○ Configure Custom Polling Threshold Monitoring

○ iSPI Performance for Metrics Software Architecture
  ○ Describe how NNMI passes data to the iSPI for Performance Metrics Software
  ○ Describe how the iSPI Performance for Metrics Software stores data
  ○ Perform basic troubleshooting steps
○ Verify that data is being collected by NNMI
○ Verify that collected data is being used by the iSPI Performance for Metrics Software
○ Check that the iSPI Performance for Metrics Software is configured properly
○ Start the iSPI Performance for Metrics Software service
○ Verify that performance polling is enabled
○ Verify that the iSPI Performance for Metrics Software Home Page opens

○ Viewing Performance Data and Reports
  ○ List the reports available from the iSPI Performance for Metrics Software
  ○ Explain the difference between reports and live reports
  ○ Modify the report settings to change the way a report displays data
  ○ Determine the appropriate report to view based on use cases

○ Administering NNMI
  ○ Customize NNMI console settings
  ○ Back up NNMI data and configuration
  ○ Check NNMI health from the GUI
  ○ Locate NNMI log files
  ○ Move from test to production (import/export tools)

○ Managing Virtualization
  ○ Identify the Hypervisor (ESXi Server) hosting a virtual machine (VM)
  ○ Use a loom map to identify the hosting Hypervisor's Network Interface Card (NIC) that the Virtual Machine is connected to
  ○ Use a wheel map to identify the hosting hypervisor's

○ Appendix A: iSPI Engineering Toolset
  ○ Describe the functionality provided by the iSPI Network Engineering Toolset
  ○ Generate Incident-triggered diagnostic execution
  ○ Generate Trap Analytics reports

**REQUIREMENTS:**

To be successful in this course, you should have the following prerequisites or knowledge.

○ Windows system administration
○ Network protocols
○ Network device administration
Difficulty level

CERTIFICATE:

The participants will obtain certificates signed by Micro Focus (course completion).

TRAINER:

Authorized Micro Focus Trainer.