Cisco Configuration Assurance Solution Reference
IT Sentinel Release Notes

Software Release 11.0

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-7556-01

Cisco Configuration Assurance Solution
Reference
IT Sentinel Release Notes

OPNET IT Sentinel 11.0 Release Notes

These release notes give an overview of the differences between OPNET IT Sentinel Release 11.0 and the previous release. If you are upgrading from a previous release, you should review this document.

Because release notes are sometimes updated after the product documentation is distributed, visit the OPNET website (www.opnet.com/support) often to check for the newest version of these release notes and previous release notes.

Contents

Part number:D00277
Version:5

Release 11.0 Description

OPNET IT Sentinel 11.0 is a significant software update to the OPNET 10.5 major software release. This release contains several new features and enhancements to existing capabilities.This release also fixes many software problems reported in earlier releases.

System Requirements

Be sure to check the latest system requirements on the OPNET website:

www.opnet.com/support

Automation Module Enhancements

Username/Password Support for Automated Logins

In this release, you can specify username and password information for an automation task. The Automation module uses this information to log on to the host computer. This information might be required if the automation task needs to access advanced system resources such as mapped network drives.

Note—This feature is available on Windows systems only.

Scenario Web Reports

An automation task can now generate scenario web reports using the Scenarios > Generate Scenario Web Report menu operation. A scenario web report enables anyone with a web browser to see all subnetworks, objects, and attributes in a scenario.

Encrypted Passwords

IT Sentinel encrypts preferences that specify passwords (including Report Server and license-registration passwords) in the environment database file and the Edit Preferences dialog box.

Note—This feature might be unavailable due to legal restrictions in your country.

Topology Import Enhancements

Device Configuration Import Enhancements

Static PVC Mapping

IT Sentinel now reads static PVC mapping from both Frame Relay and ATM device configuration files. In previous releases, you had the option to create a full-mesh of PVCs or none at all. The imported topology will now correctly show static PVC mapping, when configured. Enhancements in show command support for device configuration import include the following:

- Import Device Configuration Dialog—The PVC creation check box for device configuration import has changed. You may specify that import will Create PVCs or leave the box unselected. If the box is selected, DCI will parse PVC contract parameters from show commands in imported configurations.
- Frame Relay—Traffic contract parameters are set for PVCs with a static mapping. Information from show frame-relay map command is read and used to create a map of the actual PVC configuration in the topology.
- ATM—Static mapping of ATM PVCs is read from the show atm map command. Traffic contract parameters are set based on the static PVC configuration in the device.

New Protocol Support

- EtherChannel
- IP Multicast
- Voice over IP (not supported on Cisco multi-layer switches)

Security and System Management Configuration

Both security and system management commands are now supported for CatOS on Cisco Catalyst Layer-2 switches. Included are

- AAA—Authentication, authorization and accounting
- TACACS+
- Kerberos
- RADIUS
- SNMP
- Logging

Layer-3 Import

You can now configure DCI to import Layer-3 devices only. By setting the preference device_import.layer3_only_import to TRUE, you restrict the import to include the following devices:

- Routers/Layer-3 modules (IOS/JUNOS)
- Router-Switches (Hybrid OS/Native IOS)
- PIX Firewalls

Layer-2 devices (i.e., CatOS switches and IOS switches) will be disregarded during import when this preference is enabled. Connectivity for router-switches is inferred from the VLAN interfaces rather than from CDP information during import. This preference is disabled by default.

Aggregate Interface Support

In this release of IT Sentinel, DCI recognizes and imports aggregate interface configuration. The link configuration of an interface is inferred by way of the aggregate interface of which it is part. Support is provided for

- EtherChannel
- Link Aggregation Control Protocol (LACP)
- Multilink PPP

VNE Server Import Enhancements

Note—To use import from VNE Server in this release, you must have VNE Server version 3.0.

New Protocols

Support for import of the following protocols was added:

- Voice over IP
- IP multicast
- Aggregate interfaces (EtherChannel, Multilink PPP, and LACP)
- Legacy protocols (IPX, RSRB, DLSw+)
- ATM-Frame Relay PVC mapping
- Security parameters on Layer-2 switches
- System management commands on Layer-2 switches

New Devices

Support for the following device types was added:

- Juniper ERX
- Checkpoint Firewall-1

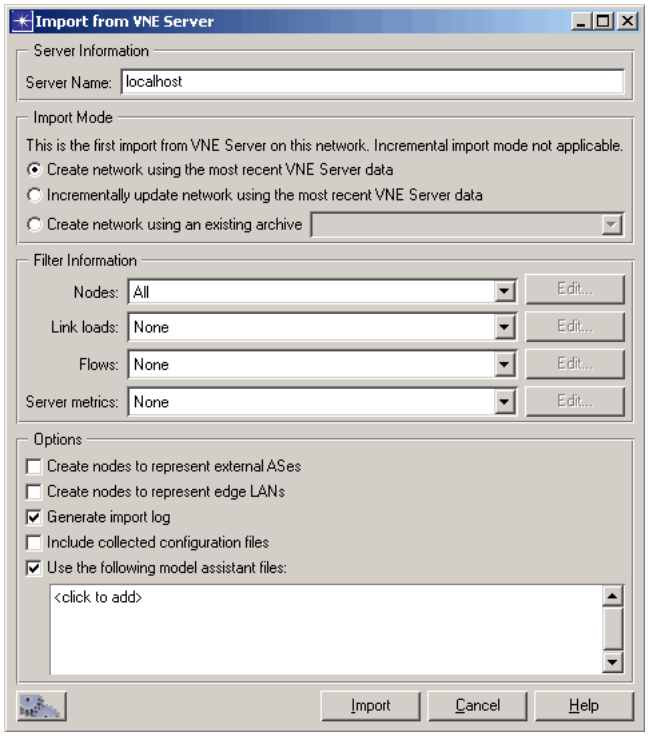
WARNING—Juniper ERX devices are not supported for incremental import.

User Interface Enhancements

Significant enhancements to the user interface for VNE Server import are introduced in this release including

- the ability to specify a VNE Server hostname instead of an .ior file.
- the ability to specify an import mode, including incremental import.
- the ability to selectively filter and import server metric data.
- the ability to include or not include model assistant files during import.

Figure 11.0-1 Import from VNE Server Dialog Box



Incremental Import

Import from VNE Server now includes support for an incremental import. This option will allow you to import just the changes in your network devices since the last import, rather than importing the entire topology again. To determine changes, the import tool examines the timestamp of the last VNE Server import in the IT Sentinel project and imports any changes that have occurred in VNE Server since then.

Note—An incremental import will not take into account changes you make to the network model once it is imported from VNE Server. It is important to save a copy of your the topology immediately after an import from VNE Server and to use that as your baseline for the next incremental import.

Custom Attributes

You may have custom attributes configured in VNE Server. When these exist, they will be mapped as extended attributes during import from VNE Server. The attributes are available for viewing and editing through the Extended Attributes button on the Edit Attributes dialog box.

New Devices

Support for import of the following devices was added:

- Juniper ERX
- Checkpoint Firewall-1

New Protocols

Support for import of the following protocols was added:

- Voice over IP
- IP multicast
- Aggregate interfaces (EtherChannel, GRE Tunnel, Multilink PPP, and LACP)
- Legacy protocols (IPX, RSRB, DLSw+)
- ATM-Frame Relay PVC mapping
- Security parameters on Layer-2 switches
- System management commands on Layer-2 switches

Flow Analysis Enhancements

Default Start Time

The default start time for a flow analysis is now the configured network start time. If no network start time is set, the default time is the earliest profile start time configured on any of the traffic flows in the network. If neither of these values are set, the current time is used for the default start time. This default can be changed, as required.

Common User Interface for ATM and IP Flow Analysis

The IP mode and ATM mode for Flow Analysis have been combined into a single mode. You no longer need to switch modes when changing from an ATM network to an IP network. Further, Flow Analysis lets you analyze networks that are running IP and ATM. Flow Analysis uses the IP settings to analyze the IP portion of the network and the ATM settings to analyze the ATM portion of the network.

By default, Flow Analysis is set up to run on packet-switched networks. To run Flow Analysis on circuit-switched networks, you need to set the flow_analysis_network_mode environment preference to circuit-switched.

Unconnected Interfaces

Flow Analysis now has an option that lets you include or exclude unconnected interfaces from the flow analysis. In earlier releases, connected and unconnected interfaces were included in the analysis.

New Protocol Support

Flow Analysis now includes support for the following features:

- EtherChannel
- DiffServ
- IP Multicasting
- Layer-3 aggregation
- Voice over IP
- RIP offset lists
- RIP default information
- PVPs
- Frame Relay and FRF .8
- Facility protected FRR

Reporting Enhancements

Change to User-Defined Reports

The interface for defining user-defined reports has been revised. Previously, to define the attributes that were included in a report, you would choose Scenarios > User-Defined Reports > Define Report. In this release, you define the attributes in a report by choosing Edit > Edit Attribute Template.

For more information, see Defining an Attribute Template on page ISU-9-10 of the Sentinel *User Guide*.

Improved Network Difference Reports

Network Difference Reports now have an updated look and include a navigation bar on the left. Report results appear as clickable objects in the body of the report, similar to other OPNET web reports.

Licensing Enhancements

The basic loanable license system built into the OPNET license server now supports loan authorization. Using a loan authorization file, license administrators can specify which licenses can be loaned by a server and which users are allowed to borrow them. For details, see Restricting Loanable Licenses on page AG-4-13 of the *Administrator Guide*.

NetDoctor Enhancements

Rule Library

New rule suites have been added in this release:

- IP multicast
- Link aggregation
- Spanning tree
- Voice over IP

The following rule suites have been significantly enhanced over previous releases:

- AAA
- Administration
- ATM
- IP routing

- Organizational Policies
- NAT
- PIX firewall
- VLANs

Other enhancements to rule suites include

- Charts (bar and pie) added to selected summary rules
- Handling of security and system management on switches
- Handling of VRFs
- Support for auto-template creation
- Support for internationalization on selected suites
- Aggregate interface support for Layer-3 devices
- Aggregate port support for Layer-2 devices
- PIX ACL support
- Juniper firewall filter support

Automatic Template Creation

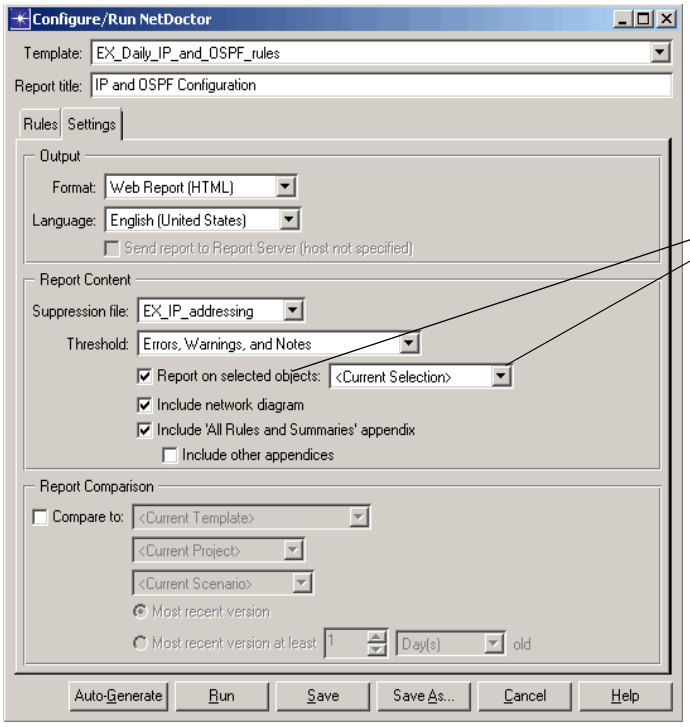
You can now have NetDoctor automatically create a template of rules. This method of creating templates lets you specify broad characteristics of the rules you want to check without having to individually build the rule set. NetDoctor uses this information plus an analysis of your network model to intelligently select rules.

For example, if you are interested in analyzing the security configurations in your network, you can tell NetDoctor to choose security-related rules. NetDoctor then intelligently selects rules related to security that apply to your network model.

Reports on Selected Objects

In this release, support is included for reporting on a selected set of objects. You can select one or more objects in the workspace prior to running NetDoctor and then run the report on just that selection. In the NetDoctor dialog box, a checkbox on the Settings tab allows you to specify reporting on the currently selected objects (default) or saved object selection sets.

Figure 11.0-2 Report on Selected Objects



You can report on currently selected objects or object selections saved previously in an object selection set.

Language Option for Reports

NetDoctor now supports reports in languages other than English. The open architecture allows you to include additional languages. When creating a template, you can specify the language in which you wish to generate the report, and you can save the setting along with the template.

You can also specify an output language for a NetDoctor report when using the menu option NetDoctor > Run NetDoctor.

Viewing Recent Reports

You can now retrieve a configurable number of reports previously generated by NetDoctor. In past releases, NetDoctor stored data from multiple runs, but you could only view the last report that was created. Now you can view previous reports in the output format of your choice. This feature is accessed from NetDoctor > View Recent NetDoctor Reports.

Message Suppression Files

If you have message suppression files created using a prior release of OPNET, they will not work in this release. Only new suppression files, created using OPNET 11.0, will work.

New Charts

Charts are now incorporated into NetDoctor reports to illustrate the results. This includes bar and pie charts designed to enhance the information presented.

Customizing NetDoctor

Adding/Editing Rule Parameters

The ability to add and edit rule parameters has been enhanced. Instead of creating parameters with editable string values, you can now specify the values from which you will select. Support has also been added to let you specify a number type as an integer or double rather than simply “number”.

WARNING—If you have custom rules that contain parameters, they will not work in this release until you update them. For instructions, refer to the Customizing NetDoctor chapter in the User Guide, Editing a Rule on page ND-4-15. If you encounter problems or need assistance, please contact OPNET Technical Support.

Rule Development

If you create or edit a summary rule that uses groups, you can select the “Filter on Selected Objects” checkbox. If this box is selected, NetDoctor calls the filter handler only if the “Report on selected objects” checkbox is selected on the Settings tab of the Configure/Run NetDoctor dialog box.

Additional Color Choices

NetDoctor now supports four additional user-specified color options in reports.

Internationalization

This release of NetDoctor lets you generate reports in other languages.

Charting

NetDoctor supports charting within this release. This includes the ability to customize different kinds of charts within reports (e.g., bar chart, pie chart).

API Enhancements

This release includes support for new classes, methods and functions and modifications to existing APIs. For example,

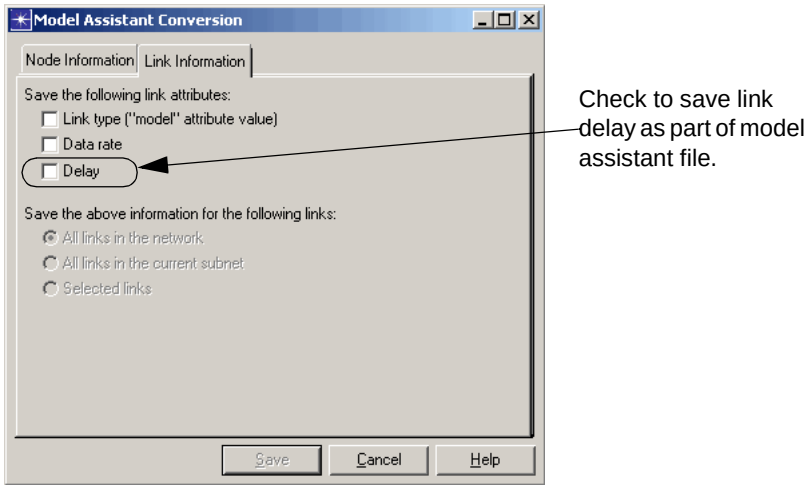
- The new method *Port.get_technology_type()* can be used to determine the link technology of a port. This method returns a *Port_Technology_Type.*
- *Report_Run.report_on_selected_objects()* checks to see if the Run on Selected Objects check box is selected, and *Node.is_selected()* checks to see if an individual node is selected in the network model.

Miscellaneous Enhancements

Model Assistant File Changes

You can now save link delay as part of a model assistant file. Select Topology > Model Assistant > Save Current Topology to File. Observe the new Delay checkbox on the Link Information tab, shown in Figure 11.0-3.

Figure 11.0-3 Saving Link Delay in Model Assistant File



Memory Improvements

Sentinel now uses 40 to 60 percent less memory (RAM) to represent network models that contain large numbers of objects. For example, a network that used about 500 MB of memory in release 10.5 now uses between 200 MB and 300 MB.