

Netcool Configuration Manager
6.4.2

*Integration Guide
Integrating with IBM Tivoli Network
Manager IP Edition and IBM Tivoli
Netcool/OMNIBus*



Note

Before using this information and the product it supports, read the information in [“Notices” on page 63.](#)

This edition applies to version 6.4.2 of IBM Tivoli Netcool Configuration Manager (5725-F56) and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright International Business Machines Corporation 2010, 2023.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this publication.....	V
Intended audience.....	v
What this publication contains.....	v
Publications.....	v
Accessibility.....	ix
Tivoli technical training.....	ix
Support information.....	ix
Conventions used in this publication.....	ix
 Chapter 1. Integration overview.....	 1
Benefits.....	1
Data flow.....	2
Integration scenarios.....	5
Isolating network problems.....	6
To isolate and rectify a network problem.....	7
 Chapter 2. Installing and configuring the products.....	 11
Prerequisite products.....	12
Prerequisite information.....	12
Prerequisite tasks.....	14
Exporting custom reports (single server integration architecture).....	14
Installing Network Manager and Tivoli Netcool/OMNIBus.....	15
Installing Netcool Configuration Manager.....	15
Configuring Tivoli Netcool/OMNIBus and Network Manager.....	16
Configuring the SNMP Probe and Netcool/OMNIBus Knowledge Library.....	16
Configuring Netcool Configuration Manager.....	18
 Chapter 3. Integrating the products.....	 21
User role requirements.....	21
Installing the DASH components.....	24
Configuring databases.....	27
Configuring integration with Tivoli Netcool/OMNIBus.....	29
Configuring integration with Network Manager.....	31
Configuring device synchronization.....	32
Configuring the Alerts menu of the AEL.....	34
Migrating reports.....	35
Exporting custom reports (distributed integration architecture).....	36
Importing reports (distributed integration architecture).....	38
Importing reports (single server integration architecture).....	38
Configuring single sign-on.....	39
Creating user groups for DASH.....	40
Creating users for DASH.....	40
Exporting the DASH LTPA keystore.....	41
Configuring single sign-on attributes for DASH.....	42
Enabling SSO for Netcool Configuration Manager.....	43
Importing the DASH LTPA keystore to the Netcool Configuration Manager server.....	43
Configuring single sign-on attributes for Netcool Configuration Manager WebSphere.....	44
Creating and configuring a federated user repository for Netcool Configuration Manager.....	44
 Chapter 4. Upgrading an integrated system.....	 47

Upgrading Netcool Configuration Manager to version 6.4.2.0.....	47
Upgrading Netcool Configuration Manager Reporting.....	49
Chapter 5. Monitoring the integrated solution.....	51
Monitoring devices and events in Network Manager.....	51
Monitoring Netcool Configuration Manager events in the AEL.....	52
Running reports.....	53
Running reports from Network Manager.....	53
Running reports from the AEL.....	54
Running reports from Tivoli Common Reporting.....	54
Netcool Configuration Manager events.....	55
Device operation events.....	55
Policy events.....	56
Resource events.....	58
Unit of work events.....	60
Notices.....	63
Trademarks.....	65
Index.....	67

About this publication

IBM Tivoli Netcool Configuration Manager provides network management and configuration capabilities for network devices, as well as extensive configuration policy thresholding capabilities.

The *IBM Tivoli Netcool Configuration Manager Integration Guide* describes how to integrate IBM Tivoli Netcool Configuration Manager with IBM Tivoli Network Manager IP Edition and IBM Tivoli Netcool/OMNIBus, and provides information about how to use the integrated system to monitor configuration devices and events.

Intended audience

This publication is intended for system administrators who are responsible for installing and integrating Netcool Configuration Manager with Network Manager and Tivoli Netcool/OMNIBus, and for network operators who are responsible for monitoring network events related to configuration changes.

What this publication contains

This publication contains the following sections:

- [Chapter 1, “Integration overview,” on page 1](#)

Provides a graphical overview of how the products in the integration fit together, and outlines the benefits of the integration.

- [Chapter 2, “Installing and configuring the products,” on page 11](#)

Summarizes the installation and configuration steps that are required to get the integrating products to an operational state before configuring the integration.

- [Chapter 3, “Integrating the products,” on page 21](#)

Describes how to configure Tivoli Common Reporting, Network Manager, and the Tivoli Netcool/OMNIBus Web GUI to support the integration.

- [Chapter 4, “Upgrading an integrated system,” on page 47](#)

Describes the steps for upgrading a previously integrated system.

- [Chapter 5, “Monitoring the integrated solution,” on page 51](#)

Describes how to monitor network events for configuration changes and policy violations.

Publications

This section lists publications in the Netcool Configuration Manager PDF document set. The prerequisite publications in the IBM Tivoli Network Manager IP Edition and IBM Tivoli Netcool/OMNIBus library are also listed here. The section also describes how to access Tivoli publications online and how to order Tivoli publications.

Netcool Configuration Manager PDF document set

The following documents are available in the Netcool Configuration Manager library:

- *IBM Tivoli Netcool Configuration Manager Installation and Configuration Guide*

Describes how to install IBM Tivoli Netcool Configuration Manager. It also describes necessary and optional post-installation configuration tasks. This publication is for administrators who need to install and set up IBM Tivoli Netcool Configuration Manager.

- *IBM Tivoli Netcool Configuration Manager User Guide*

Describes user tasks for IBM Tivoli Netcool Configuration Manager, such as how to access reports, use devices, and execute the different utilities to maintain and support Auto-Discovery. This publication is for users working with IBM Tivoli Netcool Configuration Manager.

- *IBM Tivoli Netcool Configuration Manager Administration Guide*

Describes administration tasks for IBM Tivoli Netcool Configuration Manager, such as how to set up user accounts, create and manage the OS registry, administer database and policy exports and imports, and perform housekeeping and security tasks. This publication is for administrators who are responsible for the maintenance and availability of IBM Tivoli Netcool Configuration Manager.

- *IBM Tivoli Netcool Configuration Manager Reference Guide*

Contains reference information about IBM Tivoli Netcool Configuration Manager.

- *IBM Tivoli Netcool Configuration Manager API Guide*

Provides information about how to use the Java API to programmatically access IBM Tivoli Netcool Configuration Manager.

- *IBM Tivoli Netcool Configuration Manager NSM REST API Guide*

Describes the Service Management Interface API.

- *IBM Tivoli Netcool Configuration Manager Integration Guide*

Describes how to integrate Netcool Configuration Manager with Tivoli Netcool/OMNIBus and Network Manager.

- *IBM Tivoli Netcool Configuration Manager Quick Start Guide*

Gets you started with a typical installation for IBM Tivoli Netcool Configuration Manager.

- *IBM Tivoli Netcool Configuration Manager Release Notes*

Gives important and late-breaking information about IBM Tivoli Netcool Configuration Manager. This publication is for deployers and administrators, and should be read first.

Prerequisite publications: IBM Tivoli Network Manager IP Edition

To use the information in this publication effectively when dealing with an integrated installation of Netcool Configuration Manager, Network Manager, and Tivoli Netcool/OMNIBus, you must have some prerequisite knowledge, which you can obtain from the Network Manager documentation, especially the following publications:

- *IBM Tivoli Network Manager IP Edition Release Notes*

Gives important and late-breaking information about IBM Tivoli Network Manager IP Edition. This publication is for deployers and administrators, and should be read first.

- *IBM Tivoli Network Manager Getting Started Guide*

Describes how to set up IBM Tivoli Network Manager IP Edition after you have installed the product. This guide describes how to start the product, make sure it is running correctly, and discover the network. Getting a good network discovery is central to using Network Manager IP Edition successfully. This guide describes how to configure and monitor a first discovery, verify the results of the discovery, configure a production discovery, and how to keep the network topology up to date. Once you have an up-to-date network topology, this guide describes how to make the network topology available to Network Operators, and how to monitor the network. The essential tasks are covered in this short guide, with references to the more detailed, optional, or advanced tasks and reference material in the rest of the documentation set.

- *IBM Tivoli Network Manager IP Edition Product Overview*

Gives an overview of IBM Tivoli Network Manager IP Edition. It describes the product architecture, components and functionality. This publication is for anyone interested in IBM Tivoli Network Manager IP Edition.

- *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*

Describes how to install IBM Tivoli Network Manager IP Edition. It also describes necessary and optional post-installation configuration tasks. This publication is for administrators who need to install and set up IBM Tivoli Network Manager IP Edition.

- *IBM Tivoli Network Manager IP Edition Administration Guide*

Describes administration tasks for IBM Tivoli Network Manager IP Edition, such as how to administer processes, query databases and start and stop the product. This publication is for administrators who are responsible for the maintenance and availability of IBM Tivoli Network Manager IP Edition.

- *IBM Tivoli Network Manager IP Edition Discovery Guide*

Describes how to use IBM Tivoli Network Manager IP Edition to discover your network. This publication is for administrators who are responsible for configuring and running network discovery.

- *IBM Tivoli Network Manager IP Edition Event Management Guide*

Describes how to use IBM Tivoli Network Manager IP Edition to poll network devices, to configure the enrichment of events from network devices, and to manage plug-ins to the Tivoli Netcool/OMNIBus Event Gateway, including configuration of the RCA plug-in for root-cause analysis purposes. This publication is for administrators who are responsible for configuring and running network polling, event enrichment, root-cause analysis, and Event Gateway plug-ins.

- *IBM Tivoli Network Manager IP Edition Network Troubleshooting Guide*

Describes how to use IBM Tivoli Network Manager IP Edition to troubleshoot network problems identified by the product. This publication is for network operators who are responsible for identifying or resolving network problems.

- *IBM Tivoli Network Manager IP Edition Network Visualization Setup Guide*

Describes how to configure the IBM Tivoli Network Manager IP Edition network visualization tools to give your network operators a customized working environment. This publication is for product administrators or team leaders who are responsible for facilitating the work of network operators.

- *IBM Tivoli Network Manager IP Edition Management Database Reference*

Describes the schemas of the component databases in IBM Tivoli Network Manager IP Edition. This publication is for advanced users who need to query the component databases directly.

- *IBM Tivoli Network Manager IP Edition Topology Database Reference*

Describes the schemas of the database used for storing topology data in IBM Tivoli Network Manager IP Edition. This publication is for advanced users who need to query the topology database directly.

- *IBM Tivoli Network Manager IP Edition Language Reference*

Describes the system languages used by IBM Tivoli Network Manager IP Edition, such as the Stitcher language, and the Object Query Language. This publication is for advanced users who need to customize the operation of IBM Tivoli Network Manager IP Edition.

- *IBM Tivoli Network Manager IP Edition Perl API Guide*

Describes the Perl modules that allow developers to write custom applications that interact with the IBM Tivoli Network Manager IP Edition. Examples of custom applications that developers can write include Polling and Discovery Agents. This publication is for advanced Perl developers who need to write such custom applications.

- *IBM Tivoli Monitoring for Tivoli Network Manager IP User's Guide*

Provides information about installing and using IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition. This publication is for system administrators who install and use IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition to monitor and manage IBM Tivoli Network Manager IP Edition resources.

Prerequisite publications: IBM Tivoli Netcool/OMNIBus

To use the information in this publication effectively when dealing with an integrated installation of Netcool Configuration Manager, Network Manager, and Tivoli Netcool/OMNIBus, you must have

some prerequisite knowledge, which you can obtain from the Tivoli Netcool/OMNIBus documentation, especially the following publications:

- *IBM Tivoli Netcool/OMNIBus Installation and Deployment Guide*

Includes installation and upgrade procedures for Tivoli Netcool/OMNIBus, and describes how to configure security and component communications. The publication also includes examples of Tivoli Netcool/OMNIBus architectures and describes how to implement them.

- *IBM Tivoli Netcool/OMNIBus User's Guide*

Provides an overview of the desktop tools and describes the operator tasks related to event management using these tools.

- *IBM Tivoli Netcool/OMNIBus Administration Guide*

Describes how to perform administrative tasks using the Tivoli Netcool/OMNIBus Administrator GUI, command-line tools, and process control. The publication also contains descriptions and examples of ObjectServer SQL syntax and automations.

- *IBM Tivoli Netcool/OMNIBus Probe and Gateway Guide*

Contains introductory and reference information about probes and gateways, including probe rules file syntax and gateway commands.

- *IBM Tivoli Netcool/OMNIBus Web GUI Administration and User's Guide*

Describes how to perform administrative and event visualization tasks using the Tivoli Netcool/OMNIBus Web GUI.

Accessing terminology online

The IBM Terminology website consolidates the terminology from IBM product libraries in one convenient location. You can access the Terminology website at the following Web address:

<http://www.ibm.com/software/globalization/terminology>

Accessing publications online

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli Information Center website at:

<http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp>

Note: If you print PDF documents on other than letter-sized paper, set the option in the **File > Print** window that allows Adobe Reader to print letter-sized pages on your local paper.

Ordering publications

You can order many Tivoli publications online at the following website:

<http://www.elink.ibm.link.ibm.com/publications/servlet/pbi.wss>

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order Tivoli publications. To locate the telephone number of your local representative, perform the following steps:

1. Go to the following website:

<http://www.elink.ibm.link.ibm.com/publications/servlet/pbi.wss>

2. Select your country from the list and click **Go**. The **Welcome to the IBM Publications Center** page is displayed for your country.

3. On the left side of the page, click **About this site** to see an information page that includes the telephone number of your local representative.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully.

With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Tivoli technical training

For Tivoli technical training information, refer to the following IBM Tivoli Education website:

<https://www.ibm.com/training/search?query=tivoli>

Support information

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

Online

Go to the IBM Software Support site at <http://www.ibm.com/software/support/probsub.html> and follow the instructions.

IBM Support Assistant

The IBM Support Assistant (ISA) is a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. The ISA provides quick access to support-related information and serviceability tools for problem determination. To install the ISA software, go to <http://www.ibm.com/software/support/isa>

Conventions used in this publication

This publication uses several conventions for special terms and actions and operating system-dependent commands and paths.

Typeface conventions

This publication uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as **Tip:** and **Operating system considerations:**)
- Keywords and parameters in text

Italic

- Citations (examples: titles of publications, diskettes, and CDs)
- Words defined in text (example: a nonswitched line is called a *point-to-point* line)
- Emphasis of words and letters (words as words example: "Use the word *that* to introduce a restrictive clause."; letters as letters example: "The LUN address must start with the letter *L*.")
- New terms in text (except in a definition list): a *view* is a frame in a workspace that contains data
- Variables and values you must provide: ... where *myname* represents....

Monospace

- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

Operating system-dependent variables and paths

This publication uses the UNIX convention for specifying environment variables and for directory notation.

When using the Windows command line, replace ***\$variable*** with ***%variable%*** for environment variables, and replace each forward slash (/) with a backslash (\) in directory paths. For example, on UNIX systems, the \$NCHOME environment variable specifies the directory where the Network Manager core components are installed. On Windows systems, the same environment variable is %NCHOME%. The names of environment variables are not always the same in the Windows and UNIX environments. For example, %TEMP% in Windows environments is equivalent to \$TMPDIR in UNIX environments.

If you are using the bash shell on a Windows system, you can use the UNIX conventions.

Chapter 1. Integration overview

By integrating Netcool Configuration Manager with Network Manager and Tivoli Netcool/OMNIbus, you enrich the diagnostic information available to operators by adding network configuration and policy management capability. You also reduce the need to maintain separate data records and discovery processes, and increase the ability to cross-reference between network events.

Note:

While Network Manager and DASH can be deployed on Windows systems, the integration with Network Manager is limited by the platforms supported by Netcool Configuration Manager.

Integration packages are therefore not available for Network Manager Windows platforms.

Benefits

The integration of Network Manager, Tivoli Netcool/OMNIbus, and Netcool Configuration Manager consolidates the management of networking events in a single solution.

The integration offers the following benefits:

- Integration prevents the inefficiencies associated with the use of separate products to monitor different aspects of the same network. By sharing specific device information and preserving device groupings and hierarchies between Network Manager, Tivoli Netcool/OMNIbus and Netcool Configuration Manager, you reduce the need to run separate device discoveries. You also reduce the need to maintain separate databases with separate device identifiers and duplicate network data. This improves the efficiency of network administration and monitoring.
- Device configuration problems form a significant percentage of all network problems. By integrating with Netcool Configuration Manager, you create a unified view of network events, including configuration changes made to network devices. This allows you to cross-reference all these event types, thereby helping you to monitor and address networking problems more efficiently from within a single solution.
- The ability to define network policies and enforce compliance with these policies helps you to manage your network more effectively, and also helps you to comply with network standards and regulations. By integrating with Netcool Configuration Manager, you include policy violation events in the list of network events to be monitored.

Integrating the products

You first install the required products and components and ensure that they are in working order as described in [Chapter 2, “Installing and configuring the products,” on page 11](#). You then configure the product integration itself.

Related concepts

[Netcool Configuration Manager events](#)

Use this information to understand the different types of configuration events generated by Netcool Configuration Manager.

[Installing and configuring the products](#)

The products and components that support the integration must be installed, and must be in an operational state before you configure the integration.

Related tasks

[Integrating the products](#)

Netcool Configuration Manager can be integrated with Network Manager.

[Monitoring the integrated solution](#)

When Tivoli Netcool/OMNIbus, Network Manager, and Netcool Configuration Manager are installed in an integrated environment, you can monitor Netcool Configuration Manager events that are generated

from device operation traps, policy traps, resource traps, and unit of work traps. You can also view device-based reports for these events.

Data flow

In an integrated Netcool Configuration Manager, Network Manager, and Tivoli Netcool/OMNIBus solution, data travels from the network resources that are being managed through a number of product components and networking layers, until it is presented to the network operators.

At each stage of this journey, components and processes categorize, cross-reference, and enrich the collected network data. To enable these components and processes to integrate, you perform a number of tasks.

Integrated data flow

The following figure shows the data flow between product components in an integrated environment.

Note: The focus is on data relevant to configuration and compliance policy management, rather than all data.

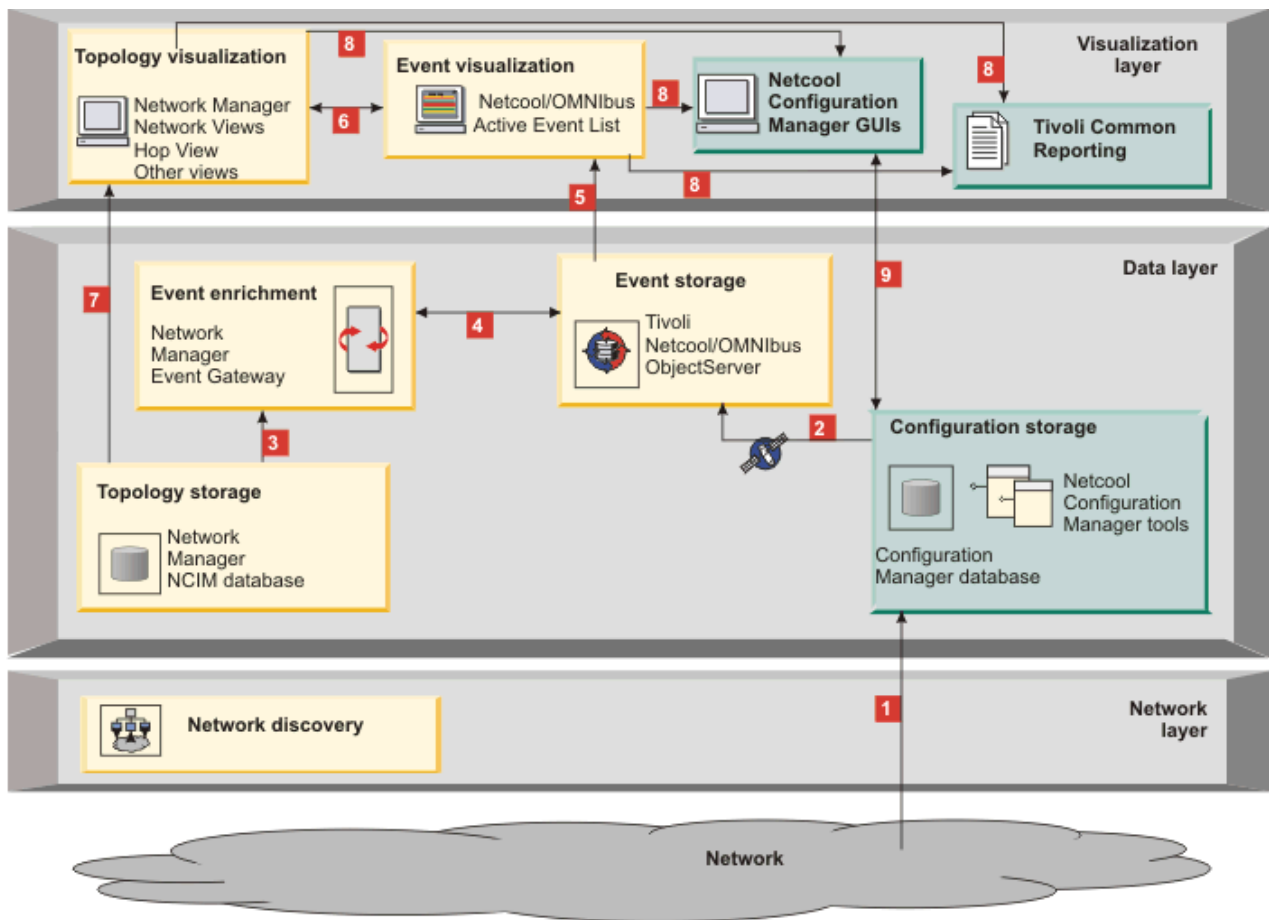


Figure 1. Integrated data flow

1

When a configuration change or policy violation occurs in a network resource, information is sent to Netcool Configuration Manager.

2

Netcool Configuration Manager logs the data and sends a corresponding event to the Tivoli Netcool/OMNIBus ObjectServer via the SNMP Probe.

- 3** Network topology data stored in the Network Manager NCIM database is made available to the Event Gateway.
- 4** Netcool Configuration Manager events are passed to the Event Gateway, where they are enriched with network topology data and then returned to the ObjectServer.
- 5** The Active Event List (Tivoli Netcool/OMNIBus) displays configuration change and policy violation events stored in the ObjectServer.
- 6** Event information is shared by the Active Event List and Network Manager views.
- 7** Network Manager GUIs display network topology data stored in the NCIM database. This data is enriched by configuration change and policy event information from the ObjectServer.
- 8**

Configuration changes and policy violations are displayed in the Network Manager and Tivoli Netcool/OMNIBus GUIs.

Using the right-click menus, operators can launch in context across into Tivoli Common Reporting, the Activity Viewer, the Netcool Configuration Manager wizards, and a range of Netcool Configuration Manager UIs for further analysis.
- 9** The full Netcool Configuration Manager functionality remains available through the Netcool Configuration Manager GUIs.

Integration tasks and associated data flow

The following figure shows the post-installation tasks a network administrator performs in order to create an integrated solution.

Remember: Before performing these integration tasks, you must install and then configure the individual products.

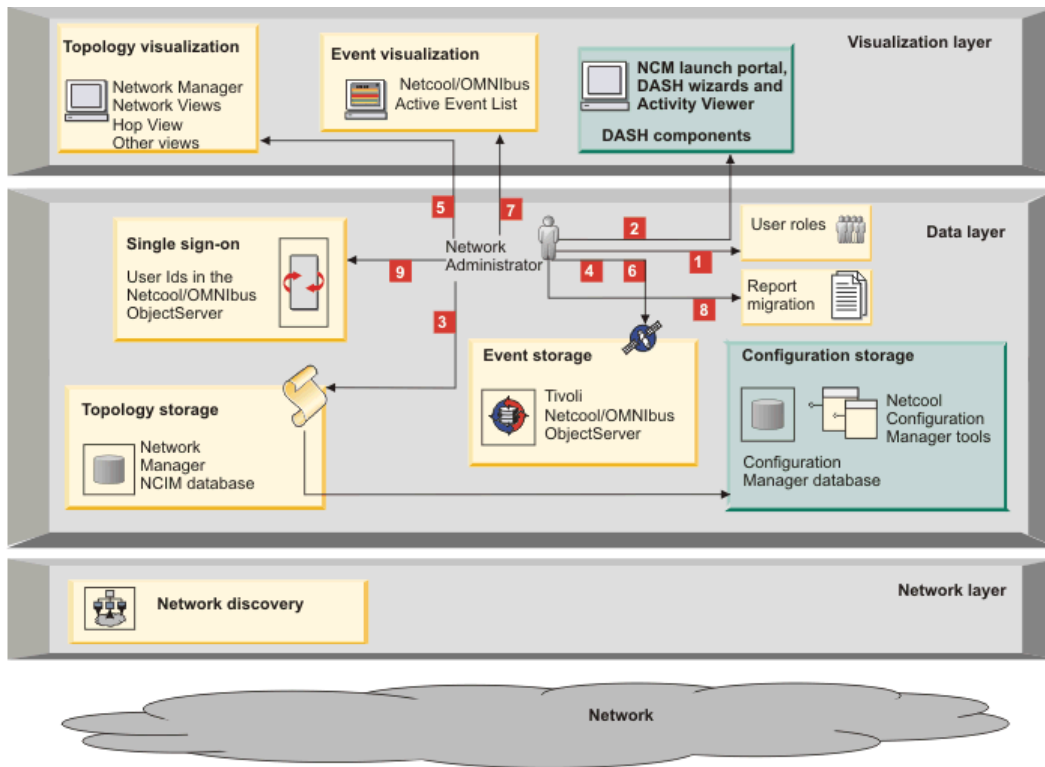


Figure 2. Integration tasks

- 1** Network administrators create and configure the user roles required for access to the Netcool Configuration Manager components that are launched from within DASH
- 2** Network administrators install the Netcool Configuration Manager DASH components.
- 3** Under certain circumstances, such as when different or remote databases are used in an integrated environment, network administrators perform additional database configuration steps.
- 4** Network administrators install the Netcool/OMNibus Knowledge Library (Nickle) files specific to Netcool Configuration Manager.
Note: If you have installed Netcool/OMNibus Knowledge Library Enhanced Probe Rules Version 4.4 Multiplatform English (NcKL4.4) on your Netcool/OMNibus Knowledge Library server, which is the recommended option, you do not need to install these rules files.
- 5** Network administrators copy a number of jar files from the Network Manager GUI server into the Netcool Configuration Manager instance of WebSphere.
- 6** Network administrators configure Netcool Configuration Manager device synchronization to extract the network data discovered by Network Manager.
This extracts the data from the NCIM database and adds it to the Netcool Configuration Manager database.
- 7** Network administrators add Netcool Configuration Manager menus and tools to the Tivoli Netcool/OMNibus AEL.
- 8** To preserve custom reports in an existing installation of Netcool Configuration Manager, you migrate the reports into the Network Manager instance of Tivoli Common Reporting.

9

To prevent multiple logon prompts when using multiple applications within a single integrated solution, you configure single sign-on.

Related conceptsInstalling and configuring the products

The products and components that support the integration must be installed, and must be in an operational state before you configure the integration.

Related tasksIntegrating the products

Netcool Configuration Manager can be integrated with Network Manager.

Monitoring the integrated solution

When Tivoli Netcool/OMNIBus, Network Manager, and Netcool Configuration Manager are installed in an integrated environment, you can monitor Netcool Configuration Manager events that are generated from device operation traps, policy traps, resource traps, and unit of work traps. You can also view device-based reports for these events.

Integration scenarios

View the following integration scenarios for an idea of the functionality an integrated system provides.

Exploiting configuration information for problem isolation

In this scenario, notifications of configuration changes are sent to OMNIBus, which are correlated to network faults and performance indicators to identify the root cause of a network outage. This integration scenario consists of the following steps:

1. A change is made, such as shutting down an interface from Tivoli Netcool Configuration Manager.
2. An event shows up on the Tivoli Netcool OMNIBus Active Event List (AEL).
 - The operator launches the Tivoli Netcool Configuration Manager Activity Viewer in context from the AEL to investigate.
 - The operator drills down further into various integrated interfaces to investigate, such as the Tivoli Common Reporting 'Configuration and OS Change Summary' report and the Network Manager Network Views.
3. The operator corrects the problem by restarting the interface from the Tivoli Netcool Configuration Manager **Submit Configuration Change** wizard, by applying a previous configuration.
 - The operator launches various integrated interfaces to validate the configuration change, such as Network Manager Network Views and the Tivoli Netcool Configuration Manager Queue Manager.
 - Events are cleared on the Tivoli Netcool OMNIBus AEL.

Configuration rollback after misconfiguration

This integration scenario provides a launch-in-context from a network problem to restore network service. This scenario consists of the following steps:

1. A device goes red.
2. The operator is watching the network map and notices the problem.
3. The operator launches a report in context from the device.
4. The operator launches the Tivoli Netcool Configuration Manager Activity Viewer in context from the device.
5. The operator identifies the configuration that needs to be rolled back.
6. The operator applies the rollback in context from Tivoli Netcool Configuration Manager's **Submit Configuration Change** wizard.
7. The device goes green in the network map.

Implementing a new network configuration standard

This scenario uses Tivoli Netcool Configuration Manager's configuration command sets to implement configuration standards across all network devices. The following steps describe the data flow:

1. The administrator has installed the mtrttrapd probe.
2. The administrator wants to enable the network SNMP traps.
3. The administrator launches Tivoli Netcool Configuration Manager.
4. The administrator creates multiple command sets for different devices (such as CISCO IOS, CISCO CATOS, or Juniper JUNOS).
5. The administrator applies the command sets for selected devices.
6. The administrator verifies that mtrttrapd events appear on Netcool OMNIBus.

Ensuring that a configuration is appropriate to support a network service

This scenario uses Tivoli Network Manager's view of network services to apply a compliance policy across a set of network resources to support the network service. The data flow is described as follows:

1. A service provider receives an order to create a new VPN for a new client ZYX, with several branches.
2. Service provider wants to verify that VPN configuration is compliant across all client ZYX facing routers.
3. Tivoli Netcool Configuration Manager administrator creates a MPLS VPN policy for client ZYX.
4. The Tivoli Network Manager administrator launches Tivoli Network Manager and MPLS views.
5. In the Tivoli Network Manager and MPLS view, suitable routers are identified.
6. The Tivoli Netcool Configuration Manager administrator launches the Tivoli Netcool Configuration Manager Applying policies wizard.
7. The Tivoli Netcool Configuration Manager administrator executes the policy against the selected devices. After the policy runs, the Tivoli Network Manager administrator launches in-context compliance reports and sees if the identified devices support the new network service.

Isolating network problems

In this scenario we determine the root cause of a network fault in Tivoli Network Manager and take action to resolve the problem in Tivoli Netcool Configuration Manager using the launch-in-context feature.

Network operations are important for IT organizations, because they provide communication among the services. Without properly working network operations, it is hard to discuss the availability of the service of a business. Indeed, if an organization is a service provider, the importance of network operations is much higher because service availability affects all areas of the service provider's business, so high availability of the network is required. Therefore, there is always a demand for network operations management solutions.

To increase the network operations performance, a monitoring solution that takes action in the shortest possible time is necessary. Integrating Tivoli Network Manager and Tivoli Netcool Configuration Manager lets you use the network monitoring tool to not only determine the root cause of a network problem, but also isolate a possible problem.

This scenario explains how the root cause of a network problem can be identified in Tivoli Network Manager and how the necessary action can be taken in Tivoli Netcool Configuration Manager. The scenario starts with a configuration change performed by a user in Tivoli Netcool Configuration Manager. This change is made by a network operator who monitors the network through Tivoli Network Manager. After making this configuration change, the operator discovers that the change in the configuration of a network device causes a network problem. The operator gathers details about the change from both Tivoli Network Manager and Tivoli Netcool Configuration Manager, and also uses launch-in-context feature that is provided by the integration of these two network tools. As a result, the operator corrects the problem quickly.

In summary, any change in the configuration can be monitored by a network operator, who has a control over the configuration changes in network devices and there shortens the time of resolution.

To isolate and rectify a network problem

A configuration change is performed by a user Tivoli Netcool Configuration Manager. The operator sees an alarm in the Active Event List in Tivoli Network Manager. The operator checks the status of the device (that set off the alarm) in the network map. After recognizing the problem, the operator launches a report of unit work summary by using the launch-in-context feature and observes that there is a configuration change in the network device. Then, the operator launches Tivoli Netcool Configuration Manager from Tivoli Network Manager by using the launch-in-context feature and applies the necessary action to correct the problem. Afterwards, the status of that device is checked in Tivoli Netcool Configuration Manager and we note that the problem is resolved.

Having logged into the DASH framework, you no longer need to verify your individual user credentials for all the integrated products, even when utilizing the launch-in-context capability. This is due to the single-signon functionality introduced in Netcool Configuration Manager version 6.3.

For this scenario, the integration of Tivoli Network Manager and Tivoli Netcool Configuration Manager provides the following benefits:

- Integration allows automatic generation of alarms in the Active Event List of Tivoli Network Manager when any change is applied to a network device in Tivoli Netcool Configuration Manager, which provides more control over configuration changes in network devices.
- Automatic alarm generation in Tivoli Network Manager helps operators to make any configuration changes in a network device, and integration of the tools helps operators to check easily whether these changes cause any network problems.
- Using the launch-in-context feature, which results from the integration of Tivoli Netcool Configuration Manager and Tivoli Network Manager, helps the operator to check configuration changes in Tivoli Netcool Configuration Manager and take action in the shortest possible time.

This integration scenario example consists of the following steps:

1. In Tivoli Netcool Configuration Manager, shut down a device interface.
 - a) Access Netcool Configuration Manager from the Tivoli Integrated Portal thick-client launch portal, then open the **Resource Browser**.
 - b) In the **Resource Browser** navigation tree, expand a specific realm and identify a device, for example 'device-x'.
 - c) In the **Resource Browser** main window, select **device-x**, and then select the **Configurations** tab.
The current configuration and previous (versioned) configurations stored for that device are displayed in the bottom half of the main window,
 - d) Double-click the current configuration for device-x.
The **Configuration Editor** is displayed.
 - e) In the **Configuration Editor** navigation tree, expand the configuration changes available and click the **shutdown** option.
 - f) Select the **Shutdown - Shutdown the selected interface** checkbox, then click **Save**.
Note: You must enter a name for the configuration change.
The draft configuration you have created is displayed in the bottom half of the main window.
 - g) Select the draft configuration you have created and click **Submit**.
The **Submit Configuration Change** wizard is displayed.
 - h) See *Applying versioned configurations* in chapter two of the *IBM Tivoli Netcool Configuration Manager User Guide* for detailed information on completing the Submit Configuration Change wizard.

Note: The configuration change is submitted as a unit of work (UOW) and a unique UOW ID is generated.

By submitting this configuration change, an interface of the network device is being shut down by Tivoli Netcool Configuration Manager. Next, observe the related events and views in the integrated Netcool OMNIBus and Tivoli Network Manager.

2. In the Tivoli Netcool OMNIBus Active Event List (AEL), view the changed device configuration. Then drill down to investigate further.

Note: By default, events for configuration change operations performed in Tivoli Netcool Configuration Manager appear in the AEL with the information Configuration Changed via Command Line displayed in the Summary field.

- a) In the DASH navigation area, click **Availability > Events > Active Event List**

The AEL is displayed.

- b) Identify the configuration change event you submitted in the previous step.

For more information on identifying and monitoring Netcool Configuration Manager events in the AEL, see *Monitoring Netcool Configuration Manager events in the Active Event List* in the *IBM Tivoli Netcool Configuration Manager Integration Guide*.

- c) Open the context menu (right-click) and click **Activity Viewer**.

The Activity Viewer is displayed with summary information recorded against device-x displayed in a sequential timeline view, including the shutdown change executed earlier.

See *Viewing device-specific events in the Activity Viewer* in the *IBM Tivoli Netcool Configuration Manager User Guide* for more information on the Activity Viewer.

- d) You can visualize the device in the Network Manager Network View, or find out more about configuration changes performed on the device by viewing the configuration change summary report in Tivoli Common Reporting.

- To access the report from the Active Event List, right-click the Netcool Configuration Manager event in the AEL, click **Configuration Management > ITNCM Reports**, and then select the **Configuration and OS Change Summary Report** from the submenu. See *Configuration and OS Change Summary* in the *IBM Tivoli Netcool Configuration Manager User Guide* for detailed information on accessing the report and interpreting its content.

- Communication between device-x and neighboring devices has broken down, which will be represented visually. See the Network Manager documentation for more information on using Network Views.

- e) You can also view the finished work in the Netcool Configuration Manager Queue Manager's 'Work That Is Finished' node.

Tip: In **Queue Manager** you can use the UOW ID to find the finished work.

Remember: Access Netcool Configuration Manager in one of the following ways:

- Open Netcool Configuration Manager from the Tivoli Integrated Portal thick-client launch portal.
- Open Netcool Configuration Manager in context from Network Manager by right-clicking a device, and then clicking **Configuration Management > Launch ITNCM** from the pop-up menu.
For more information, see *Monitoring devices and events in Network Manager* in the *IBM Tivoli Netcool Configuration Manager Integration Guide*.

Having identified the change in configuration, the next step in this scenario is to undo the change.

3. Undo the configuration change using the Netcool Configuration Manager Activity Viewer and wizards.

- a) In the Netcool Configuration Manager Activity Viewer, select the previous (versioned) configuration for a device.

- b) Open the **Submit Configuration** wizard and complete the steps in order to apply the configuration to the device (as a unit of work).

See *Applying versioned configurations* in chapter two of the *IBM Tivoli Netcool Configuration Manager User Guide* for detailed information on completing the Submit Configuration Change wizard.

c) Instead of using the wizard, you can undo the configuration change from the Netcool Configuration Manager Resource Browser (and Configuration Editor) instead.

- Return to the Netcool Configuration Manager **Resource Browser** and drill down to device-x.
- Deselect the **Shutdown - Shutdown the selected interface** checkbox, and submit the draft configuration. This opens the **Configuration Editor**.
- Select the draft configuration you have created and click **Submit**. The **Submit Configuration Change** wizard is displayed. Complete as described previously.

The configuration change is submitted as a unit of work (UOW) and a unique UOW ID is generated. The device-x interface is restarted and a Configuration Change event is recorded in the AEL.

4. View the configuration change event in the AEL to verify that the configuration has been changed to a previous version. You can drill down into the available data in the following ways:
- a) Access Network Manager Network Views. Communication between device-x and neighboring devices is shown as restored.
 - b) View the configuration change summary report in Tivoli Common Reporting.
 - c) You can also view the finished work in the Netcool Configuration Manager Queue Manager's 'Work That Is Finished' node, as described in step two.

Chapter 2. Installing and configuring the products

The products and components that support the integration must be installed, and must be in an operational state before you configure the integration.

Before installing the products, ensure that you review the hardware, operating system, software, and communication requirements, and consider your deployment options. Also take note of the user and system permissions that are required for the user performing the installations.

Also, before starting any components or working with any configuration files, set the Network Manager environment variables by sourcing the env.sh script (UNIX or Linux) or env.bat script (Windows). This script is in the Netcool home location, for example:

/opt/IBM/tivoli/netcool or C:\IBM\tivoli\netcool

Required DASH profiles

If a Netcool Configuration Manager presentation server and Netcool Configuration Manager Reports are to be located on the same server, they require installation in separate DASH profiles.

The Netcool Configuration Manager presentation server and Network Manager GUI cannot be installed in the same instance of DASH. They also require separate profiles.

Integrating with Network Manager when failover is enabled

Network Manager has a number of restrictions when failover is enabled, or has actually occurred (see the Network Manager documentation for further details). Therefore the following restrictions apply to an integrated Netcool Configuration Manager system:

- If Network Manager has actually failed over, do not attempt to integrate Netcool Configuration Manager with it.

Netcool Configuration Manager integration or Netcool Configuration Manager integration upgrades should only be performed against Network Manager in normal operation.

- Netcool Configuration Manager should be integrated only with the Primary Network Manager installation.

Should Network Manager fail over its discovery process (ncp_disco) will not perform any discovery, so Netcool Configuration Manager Import UOWs against the Backup Network Manager domain are not possible.

- If Network Manager has failed over, do not run sendITNCMDDeviceActivityTraps.sh, do not trigger an Network Manager import into Netcool Configuration Manager, do not use the Netcool Configuration Manager right click menus from TIP.

Related tasks

Integrating the products

Netcool Configuration Manager can be integrated with Network Manager.

Upgrading an integrated system

The steps for upgrading a previously integrated system that includes Netcool Configuration Manager version 6.4.1, follow these instructions. For other upgrade paths, see the Netcool Configuration Manager 6.4.1 documentation.

Configuring integration with Tivoli Netcool/OMNIBus

Ensure that you have Netcool/OMNIBus Knowledge Library (NcKL) Enhanced Probe Rules for Netcool Configuration Manager installed on your Tivoli Netcool/OMNIBus server.

Installing the DASH components

For integrated scenarios, Netcool Configuration Manager provides the following DASH components: The Activity Viewer, the DASH wizards, and the Netcool Configuration Manager thick-client launch portal.

Prerequisite products

Specific product versions are required to support the integration. Working knowledge of these products is assumed.

Note: You can integrate IBM Tivoli Netcool Configuration Manager Version 6.4.2 only with IBM Tivoli Network Manager IP Edition Version 4.2. This is due to new and improved integration and installation methods.

The required products and versions are as follows:

- IBM Tivoli Netcool Configuration Manager 6.4.2
- IBM Tivoli Network Manager IP Edition 4.2
- IBM Tivoli Netcool/OMNIBus Core 8.1.0.5
- IBM Tivoli Netcool/OMNIBus WebGUI 8.1.0.4

Prerequisite information

You can define a checklist of information required for the integration of Netcool Configuration Manager, Network Manager IP Edition, and Tivoli Netcool/OMNIBus, such as user names, passwords, and system paths.

Integration checklist

For a detailed Netcool Configuration Manager checklist, see the *IBM Tivoli Netcool Configuration Manager Installation and Configuration Guide*.

The following table lists information you should assemble before integrating the products.

Note: You can replace recommended or default values with your own.

Table 1. Integration information checklist		
Information	Details	Default value
Network Manager NCIM database information		
Note: You can find this information in the DbLogins.DOMAIN.cfg file.		
Database name		
User		
Password		
Server		
Port		
IP address/ hostname		
Network Manager DASH information		
DASH server IP address/ hostname		
User		itnmadmin
Password		itnmadmin

Table 1. Integration information checklist (continued)		
Information	Details	Default value
Netcool Configuration Manager DASH installation information		
Netcool Configuration Manager IP address/hostname		
Port		
HTTP or HTTPS		
Netcool Configuration Manager database information		
Database vendor/type	Oracle or DB2	
Database name		
User		
Password		
Server		
Service name	Required for Tivoli Common Reporting	
SID		
Port		
IP address/ hostname		

About migrating reports

If you have custom reports in an existing Netcool Configuration Manager installation, and are integrating with Network Manager, which has its own Tivoli Common Reporting solution, you migrate your custom reports from the stand-alone to the integrated version of Tivoli Common Reporting.

The report migration procedure is different for single and multiple server integrations.

If you are installing Netcool Configuration Manager and Network Manager on the same server

1. Export the custom reports from the existing Netcool Configuration Manager version of Tivoli Common Reporting and copy them to a safe location.
Note: You export your custom reports before installing Network Manager to prevent the existing reports from being overwritten.
2. Disable and uninstall the existing Netcool Configuration Manager version of Tivoli Common Reporting.
3. Install Network Manager and integrate it with the existing version of Netcool Configuration Manager as documented.
4. Import the custom reports into the Network Manager version of Tivoli Common Reporting.

If you are installing Netcool Configuration Manager and Network Manager on different servers

1. Install Network Manager and integrate it with the existing version of Netcool Configuration Manager as documented.
2. Export the custom reports from the existing Netcool Configuration Manager version of Tivoli Common Reporting and copy them to the Network Manager server.
3. Import the custom reports into the Network Manager version of Tivoli Common Reporting.
4. Disable the existing Netcool Configuration Manager version of Tivoli Common Reporting.

Prerequisite tasks

Review this information for details about how to download the prerequisite products from the IBM® Passport Advantage® website, and install and configure them. After that you proceed to integrating the products.

The high-level installation and configuration steps that are required to get the products in an operational state are provided here for guidance purposes. Detailed installation and configuration information is provided in the individual product and component publications. Some steps are optional. If you already have one or more of these products or components installed and configured in your environment, you can skip that step.

Exporting custom reports (single server integration architecture)

Before you install Network Manager on the same server as your existing Netcool Configuration Manager installation, you must export any custom reports. You also disable and uninstall the existing Netcool Configuration Manager version of Tivoli Common Reporting.

You export reports **before** installing Network Manager only when all of the following circumstances apply to your scenario:

- You are already running Tivoli Common Reporting as part of an existing, non-integrated Netcool Configuration Manager installation.
- You are about to install Network Manager on the same server as your existing version of Netcool Configuration Manager.
- You have customized Netcool Configuration Manager reports that need to be migrated into your planned integrated solution.

When you install the Network Manager version of Tivoli Common Reporting on the same server as your existing version of Netcool Configuration Manager, existing reports are deleted. To migrate such reports into an integrated solution, you export them before installing Network Manager, and then import them again after you have completed all installation and integration tasks.

Remember: You do not have to migrate the standard Netcool Configuration Manager reports, because these will be installed together with the Network Manager version of Tivoli Common Reporting (in addition to a number of Network View reports). You only migrate reports you have customized since installing the standard reports, or new reports you have created.

1. Log into the Netcool Configuration Manager version of Tivoli Common Reporting using the following url:
`http://hostname:16310/ibm/console`
where *hostname* is the name of your Netcool Configuration Manager server and 16310 is the default port number for Tivoli Common Reporting.
2. Click **Reporting > Common Reporting**.
3. Click **Launch** on the toolbar, and then select **Administration** from the drop-down menu.
4. Select the **Configuration** tab, then click **Content Administration**.
5. Click **New Export** to launch the **New Export** wizard.
6. Enter a name and description for the report export, then click **Next**.
7. Accept the default deployment method and click **Next**.
8. Click the **Add** link and select the **ITNCM Reports** checkbox, then move ITNCM Reports to the **Selected Entries** list.
9. Click **OK**, then **Next > Next > Next**, accepting the default values.
10. Select **New archive**, then **Next > Next**, accepting the default values..
11. Click **Finish > Run > OK**.
The reports are exported and the new export archive is displayed.
12. Navigate to the following directory:
`/opt/IBM/tivoli/netcool/ncm/tipv2Components/TCRComponent/cognos/deployment,`

where you can view the report archive, for example:

```
-rw-r--r-- 1 icosuser staff 262637 23 Feb 10:27 ncm_export.zip
```

where `ncm_export.zip` is the report archive.

13. Copy the file to a safe location on the server, such as your home directory.
14. Navigate to the following directory:
`/opt/IBM/tivoli/netcool/ncm/bin/utils/support`
15. Run the `setPlatform.sh` script:
`bash-3.2$ ./setPlatform.sh`, disable Reporting, then exit.
16. Uninstall Tivoli Common Reporting using the `uninstall_reports.sh` script:

```
cd /opt/IBM/tivoli/netcool/ncm  
./reporting/ITNCRMReports/uninstall_reports.sh
```

You have exported the custom reports and uninstalled Tivoli Common Reporting.

Next, you complete the remaining installation and integration tasks. After that, you import the archived reports.

Related tasks

Migrating reports

If you have custom reports in an existing Netcool Configuration Manager installation, and are integrating with Network Manager, which has its own Tivoli Common Reporting solution, you migrate your custom reports from the stand-alone to the integrated version of Tivoli Common Reporting.

Importing reports (single server integration architecture)

After exporting the custom reports, disabling and uninstalling the Netcool Configuration Manager version of Tivoli Common Reporting, and completing all other integration steps, you import the report archive into the Network Manager version of Tivoli Common Reporting,

Installing Network Manager and Tivoli Netcool/OMNIBus

Download and install Network Manager and Tivoli Netcool/OMNIBus, if not already installed.

For installation instructions, see the following IBM Knowledge Center publications:

Tivoli Netcool/OMNIBus

<http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIBus.html>

Network Manager

http://www.ibm.com/support/knowledgecenter/SSSHRK/landingpage/product_welcome_itnm.html

A Note about authentication when installing Tivoli Netcool Network Manager: There are different types of authentication available when installing Network Manager. To ensure that the integration between Network Manager and Netcool Configuration Manager works, you must use the object repository authentication.

Installing Netcool Configuration Manager

You download Netcool Configuration Manager and all required files. You then install Netcool Configuration Manager (without reporting).

One or more requisite Oracle or DB2 databases must be installed before you install Netcool Configuration Manager.

When installing Netcool Configuration Manager, you select the integrated installation option, which installs it without the reporting component. Afterwards, you install reporting into the Tivoli Common Reporting deployment that is part of the Network Manager installation.

Restriction: When installing Netcool Configuration Manager into an integrated solution, you must select **Integrated** when prompted during Netcool Configuration Manager installation, and then install the DASH components as directed, so as not to break the integration.

For download instructions, see <http://www.ibm.com/support/docview.wss?rs=3120&uid=swg24033489>.

For installation instructions, see the relevant information in the IBM Tivoli Netcool Configuration Manager Knowledge Center: <http://www-01.ibm.com/support/knowledgecenter/SS7UH9/welcome>

Configuring Tivoli Netcool/OMNIbus and Network Manager

After installing Tivoli Netcool/OMNIbus and Network Manager, configure and start the products.

For configuration instructions, see the publications in the Tivoli Netcool/OMNIbus and Network Manager information centers at:

- <http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp>

You must configure the products so that they are in an operational state as follows:

- The designated ObjectServers to which events should be forwarded are set up and are running. Any other probes and gateways that you require are also installed and configured. Where necessary, it is assumed that failover has been configured, or two communicating ObjectServers have been set up with a connecting gateway.
- The Web GUI server is configured and running.
- The Network Manager server and all Network Manager processes are running, including Tivoli Netcool/OMNIbus and DASH processes.

Also, make sure that at least one full discovery has completed. This ensures that there is data in the Network Manager NCIM topology database to load into Netcool Configuration Manager.

Tip: To confirm that all Network Manager processes are running, use these commands, executed as the same user that installed Network Manager:

- `itnm_status`
- `itnm_stop`
- `itnm_start`

You can also use the following optional parameter to specify the processes:

ncp

Network Manager processes

For more information about discovering your network in Network Manager, see the *IBM Tivoli Network Manager IP Edition Discovery Guide*.

- Client workstations are set up to connect to the DASH console, which provides access to the Network Manager Web applications and the Web GUI.

Configuring the SNMP Probe and Netcool/OMNIbus Knowledge Library

Netcool Configuration Manager requires the Tivoli Netcool/OMNIbus nco-p-mttrapd probe and the Netcool/OMNIbus Knowledge Library to be installed on the ObjectServer host.

If you have existing custom rules the Netcool/OMNIbus Knowledge Library (NcKL) can be migrated from your previous installation, and the rules specific to Netcool Configuration Manager can be found in your Netcool Configuration Manager Presentation server installation.

If you do not have custom rules, install the latest Netcool/OMNIbus Knowledge Library Version 4.4, which already includes the Netcool Configuration Manager NcKL rules.

For the purposes of this integration, it is considered good practice to have a dedicated probe that can be configured with the set of customized lookup tables and rules that are supplied.

Table 2. Netcool/OMNIBus Knowledge Library configuration

Tivoli Netcool/OMNIBus component	Configuration applied
ObjectServer	The ObjectServer is updated as follows: • New intra-device correlation tables are added to the alerts database. • Supplementary automations are added. • Additional fields are added to the alerts.status table. • The relevant conversions for the new fields are added to the ObjectServer.
SNMP Probe	The following configuration should be applied to the probe: • The Netcool Configuration Manager rules files and lookup files that are provided in the <code>rules.tar.gz</code> file are extracted to a <code>rules</code> subdirectory within the <code>\$NCHOME/etc</code> directory on UNIX or Linux®, or a <code>%NCHOME%\NcKL</code> directory on Windows. For example: UNIX <code>/opt/IBM/tivoli/netcool/etc/rules</code> Windows <code>C:\IBM\tivoli\netcool\NcKL\rules</code> • The <code>\$NCHOME/omnibus/probes/arch/mttrapd.props</code> file is updated to enable the probe to use the updated rules files. The following properties are set in the <code>mttrapd.props</code> file: <pre>RulesFile : "\$NC_RULES_HOME/snmpttrap.rules" MIBFile : "" QuietOutput : 1</pre> Tip: Before starting any components or working with any configuration files, you are required to set the Network Manager environment variables by running the env.sh script (UNIX or Linux) or env.bat script (Windows). This script is in the Netcool® home location; for example, <code>/opt/IBM/tivoli/netcool</code> or <code>C:\IBM\tivoli\netcool</code>. When you run the script, the <code>\$NC_RULES_HOME</code> environment variable is set to the location to which the <code>rules.tar.gz</code> file contents were extracted; that is: • <code>\$NC_RULES_HOME: \$NCHOME/etc/rules</code> • <code>%NC_RULES_HOME%: %NCHOME%\NcKL\rules</code> (Other environment variables, such as <code>\$NCHOME</code>, which depicts the Netcool home location, and <code>\$TIPHOME</code>, which depicts the installation location of DASH, are also set.)

Note that the Netcool/OMNIBus Knowledge Library configuration file named `NcoGateInserts.cfg` is also automatically added to the computer that hosts the Network Manager core components. This file is used for performing topology-based event correlation.

Tips for manually configuring the probe properties:

- Ensure that the **RulesFile** property is specified after the **Name** property. Otherwise, the **Name** property will override the rules file name setting.
- Ensure that the remainder of the probe properties, such as **Server** and **Port**, are appropriately set.

Note: If you installed Tivoli Netcool/OMNIBus, the SNMP Probe, and Netcool/OMNIBus Knowledge Library independently of the Network Manager installer, you will be required to manually apply the configuration to obtain the results outlined in [Table 2 on page 17](#).

Configuring Netcool Configuration Manager

After installing Netcool Configuration Manager, you must perform the standard configuration tasks that are required to set up the product, and then configure the product to support the integration. At a minimum, you must set up a Worker Server resource, create an authentication set, change the server pool sizes, set up realms, import or build policies, and grant permissions to modify compliance policies.

You will require the IP address and port of the probe host computer in order to configure communication between Netcool Configuration Manager and the probe, so have these details at hand.



CAUTION: When configuring Netcool Configuration Manager trap properties, ensure you guard against flooding Network Manager and Tivoli Netcool/OMNIBus with events.

To plan for the event volume that will be sent to your Tivoli Netcool/OMNIBus ObjectServer, be aware that one policy issued against one device generates one event. Therefore it is possible to generate a large number of events in a relatively short period of time if you are operating against a large number of devices.

If you have a large environment, consider filtering to just those events that are of most importance to you. Consult the Tivoli Netcool/OMNIBus documentation for further information.

Compliance policies and processes

At a minimum you must import or build network compliance policies, and grant permissions to modify policies, and to create, modify, schedule and execute processes.

Additionally, you must configure the product to support the integration by setting up a process and adding the relevant policies that are required for achieving operational, security, and regulatory compliance in the network. Ensure that this process is enabled for automatic validations so that the policies are run against a device when it changes, and an event is generated to indicate whether the device is in compliance.

Device configuration

You must also set up a Worker Server resource, create an authentication set, and change the server pool sizes.

Additionally, you must configure SNMP trap settings, and enable event generation for the different event types. To do so, set the following properties in the Systems Manager's **System Properties** window.

Table 3. Netcool Configuration Manager system properties	
Property	Description
Instance Identifier	Specify a unique name for this particular instance of Netcool Configuration Manager.
Network Resource Event Registration	Set this value to <code>True</code> to enable network resource events to be generated and written to the database. The default is <code>True</code> .
Resource Event Registration	Set this value to <code>True</code> to enable resource events to be generated and written to the database. The default is <code>True</code> .
Work Event Registration	Set this value to <code>True</code> to enable work events to be generated and written to the database. The default is <code>True</code> .
Compliance Policy Event Registration	Set this value to <code>True</code> to enable compliance policy events to be generated and written to the database. The default is <code>True</code> .

Table 3. Netcool Configuration Manager system properties (continued)	
Property	Description
SNMP Trap Recipients	Use this property to configure Netcool Configuration Manager to forward events that are generated from SNMP traps to the SNMP Probe. (This property setting also enables the traps to be raised.) Set the value of this property by using the following format: <i>IP_address:port</i> where <i>IP_address</i> is the IP address of the computer on which the SNMP Probe is installed, and <i>port</i> is the port on which the probe is listening. You can use a comma-separated list to specify multiple probe hosts to which all events should be forwarded, as follows: <i>IP_address1:port1,IP_address2:port2,...</i> Important: You must set the SNMP trap recipients before performing device synchronization, otherwise the right-click functionality in Network Manager and Tivoli Netcool/OMNIbus will be restricted.
SNMP Trap Flood Prevention	Specify the minimum time in milliseconds (ms) the system will wait after sending a trap before sending another.
SNMP Trap Retries	Specify the maximum number of times that the system attempts to resend unacknowledged traps.
SNMP Trap Timeout	Specify the maximum time in milliseconds that the system waits for a trap acknowledgement before resending.

You perform a number of Netcool Configuration Manager configuration tasks after the TIP portal has been installed, and the tarball applied. For more information, see [Chapter 3, “Integrating the products,”](#) on page 21.

Related tasks

[Integrating the products](#)

Netcool Configuration Manager can be integrated with Network Manager.

Chapter 3. Integrating the products

Netcool Configuration Manager can be integrated with Network Manager.

The required integration steps are as follows:

Installing the Netcool Configuration Manager DASH components

For integrated scenarios, Netcool Configuration Manager provides the following DASH components: The Activity Viewer, the wizards based in DASH, the Netcool Configuration Manager thick-client launch portal, and the Netcool Configuration Manager report bundle.

Configuring separate database types

If the integrated versions of Netcool Configuration Manager and Network Manager are not using the same type of database, you must update \$NCHOME/etc/setupTCR.sh so that the Netcool Configuration Manager environment script is called. In addition, if Network Manager uses an Informix database in a distributed environment and DASH is not installed on the same server as Network Manager, you must ensure that the correct library jars are used.

Configuring integration with Tivoli Netcool/OMNIBus

You must ensure that you have Netcool/OMNIBus Knowledge Library (NcKL) Enhanced Probe Rules Version 4.4 for Netcool Configuration Manager installed on your Tivoli Netcool/OMNIBus server.

Configuring device synchronization

You must set up synchronization between Netcool Configuration Manager and Network Manager devices.

Configuring the Alerts menu of the Active Event List

You must add access to the Activity Viewer from the Active Event List by configuring the Alerts menu.

Migrating reports

If you have custom Tivoli Common Reporting reports in an existing standalone Netcool Configuration Manager Tivoli Common Reporting installation, and are now integrating with Network Manager, which has its own Tivoli Common Reporting solution, you migrate your custom reports from the stand-alone to the integrated version of Tivoli Common Reporting.

Configuring single sign-on

The single sign-on (SSO) capability in Tivoli products means that you can log on to one Tivoli application and then launch to other Tivoli web-based or web-enabled applications without having to re-enter your user credentials.

Related concepts

Installing and configuring the products

The products and components that support the integration must be installed, and must be in an operational state before you configure the integration.

Related tasks

Configuring Netcool Configuration Manager

Upgrading an integrated system

The steps for upgrading a previously integrated system that includes Netcool Configuration Manager version 6.4.1, follow these instructions. For other upgrade paths, see the Netcool Configuration Manager 6.4.1 documentation.

User role requirements

Certain administrative user roles are required for the integration.

Note: For single sign-on information, see the related topic links.

DASH user roles

The following DASH roles are required for access to the Netcool Configuration Manager wizards and clients that are launched from within DASH.

Either create a DASH user with the same name as an existing Netcool Configuration Manager user who already has the `IntellidenUser` role, or use an appropriate Network Manager user, such as `itnadmin`, who is already set up as a DASH user.

If you use the Network Manager user, create a corresponding new Netcool Configuration Manager user with the same name (password can differ), and assign the 'IntellidenUser' role to this new user.

Important:

If a DASH user is being created on Network Manager with the same name as an existing Netcool Configuration Manager user, then they also need to be added to an appropriate Network Manager user group.

Alternatively, they must be granted any required Network Manager roles manually.

Additionally, assign the following roles to your DASH user:

- `ncp_rest_api`
- `ncmConfigChange`
- `ncmConfigSynch`
- `ncmIDTUser`
- `ncmPolicyCheck`
- `ncmActivityViewing`
- `ncmConfigViewing`
- `ncmConfigEdit`
- `ncmDashService`

The following table cross-references security requirements between user interfaces, DASH roles, Netcool Configuration Manager functionality, and Netcool Configuration Manager realm content permissions. Use this information to assign DASH roles and define realm content permissions.

Table 4. UI security by DASH roles, Netcool Configuration Manager functionality, and realm content permissions			
Access	DASH role	Functionality	Realm content permissions
Apply Modelled Command Set	<code>ncmConfigChange</code>	Execute Configuration Change	View, Execute
Apply Native Command Set	<code>ncmConfigChange</code>	Execute Configuration Change, Apply Native Command Sets	View, Execute
Synchronize (ITNCM to Device)	<code>ncmConfigSynch</code>	Execute Configuration Synchronization	View, Execute
Submit Configuration	<code>ncmConfigChange</code>	Execute Configuration Change	View, Execute
Apply Policy	<code>ncmPolicyCheck</code>	Execute Compliance Policy	View
View Configuration	<code>ncmConfigViewing</code>	n/a	View
Edit Configuration	<code>ncmConfigEdit</code>	n/a	View, Modify
Compare Configuration	<code>ncmConfigViewing</code>	n/a	View

Table 4. UI security by DASH roles, Netcool Configuration Manager functionality, and realm content permissions (continued)

Access	DASH role	Functionality	Realm content permissions
IDT Automatic	ncmIDTUser	IDT Access, IDT Allow Auto Login	View
IDT Manual	ncmIDTUser	IDT Access, IDT Allow Manual Login	View
Find Device	n/a	n/a	View
View UOW Log	n/a	n/a	n/a
View IDT Log	n/a	n/a	View
Activity Viewer	ncmActivityViewing	n/a	n/a
Device Synchronization	ncp_rest_api	n/a	n/a
Access DASH services (through right-click menus)	ncmDashServices	n/a	n/a

Tivoli Common Reporting user roles

Tivoli Common Reporting and the Netcool Configuration Manager default reports are installed together with the DASH components.

Any user who needs to access reports requires the following permissions:

- The relevant Tivoli Common Reporting roles for accessing the **Reporting** node in the DASH console. Assign these roles to enable users to run reports to which they are authorized from the Tivoli Common Reporting GUI.
- The authorization to access the report set, and the relevant Tivoli Common Reporting roles for working with the reports. Assign these permissions to enable users to run Netcool Configuration Manager reports from Network Manager topology displays, the Active Event List, and the Tivoli Common Reporting GUI.

For information about authorizing access to a report set and assigning roles by user or group, go to the IBM Tivoli® Systems Management Information Center at <http://www-01.ibm.com/support/knowledgecenter/SS3HLM/welcome>, locate the Tivoli Common Reporting documentation node, and search for *authorization* and *user roles*.

Other user roles

To configure the **Alerts** menu in the Web GUI, the ncw_admin role is required.

Related concepts

Configuring single sign-on

The single sign-on (SSO) capability in Tivoli® products means that you can log on to one Tivoli application and then launch to other Tivoli web-based or web-enabled applications without having to re-enter your user credentials.

Related tasks

Installing the DASH components

For integrated scenarios, Netcool Configuration Manager provides the following DASH components: The Activity Viewer, the DASH wizards, and the Netcool Configuration Manager thick-client launch portal.

Configuring separate database types

Under certain circumstances, such as when different or remote databases are used in an integrated environment, you must perform additional database configuration steps.

Configuring integration with Tivoli Netcool/OMNIBus

Ensure that you have Netcool/OMNIBus Knowledge Library (NcKL) Enhanced Probe Rules for Netcool Configuration Manager installed on your Tivoli Netcool/OMNIBus server.

Configuring integration with Network Manager

Copy a number of jar files from the Network Manager GUI server into the Netcool Configuration Manager instance of WebSphere.

Configuring device synchronization

You configure device synchronization to enable Netcool Configuration Manager to use Network Manager for network device discovery.

Configuring the Alerts menu of the Active Event List

You must add access to the Activity Viewer from the Active Event List by configuring the Alerts menu.

Migrating reports

If you have custom reports in an existing Netcool Configuration Manager installation, and are integrating with Network Manager, which has its own Tivoli Common Reporting solution, you migrate your custom reports from the stand-alone to the integrated version of Tivoli Common Reporting.

Importing the DASH LTPA keystore to the Netcool Configuration Manager server

For added security the contents of the LTPA token are encrypted and decrypted using a keystore maintained by WebSphere. In order for two instances of WebSphere to share authentication information via LTPA tokens they must both use the same keystore. The IBM admin console makes this a simple process of exporting the keystore on one instance of WebSphere and importing it into another.

Installing the DASH components

For integrated scenarios, Netcool Configuration Manager provides the following DASH components: The Activity Viewer, the DASH wizards, and the Netcool Configuration Manager thick-client launch portal.

From Version 6.4.2 onwards, Netcool Configuration Manager reporting is no longer installed as part of the DASH components installation, but rather as part of the Netcool Configuration Manager main installation.

Important: Before installing the DASH components, install Netcool Configuration Manager using the 'Integrated' option.

Restriction: The Netcool Configuration Manager DASH components must be installed as the same user who installed Network Manager.

1. Log onto the DASH server.
2. Change to the /eclipse subdirectory of the Installation Manager Group installation directory and use the following command to start Installation Manager:
./IBMIM

To record the installation steps in a response file for use with silent installations on other computers, use the '-record response_file' option. For example:

```
IBMIM -record C:\response_files\install_1.xml
```

3. Configure Installation Manager to download package repositories from IBM Passport Advantage:
 - a) From the main menu, choose **File > Preferences**.
You can set preferences for proxy servers in IBM Installation Manager. Proxy servers enable connections to remote servers from behind a firewall.
 - b) In the **Preferences** window, expand the Internet node and select one of the following options:

FTP Proxy

Select this option to specify a SOCKS proxy host address and a SOCKS proxy port number.

HTTP Proxy

Select this option to enable an HTTP or SOCKS proxy.

- c) Select **Enable proxy server**.
 - d) In the **Preferences** window, select the **Passport Advantage** panel.
 - e) Select **Connect to Passport Advantage**.
 - f) Click **Apply**, and then click **OK**.
4. In the main **Installation Manager** window, click **Install**, select **IBM Dashboard Applications for ITNCM**, and then follow the installation wizard instructions to complete the installation.
 5. Accept the license agreement, select an installation directory, and supply the following details:

Netcool Configuration Manager database details

Sid/service name/database name(db2)

Database hostname

Port

Username

Password

DASH administrative credentials

DASH administrator username (default is smadmin)

DASH administrator password

Network Manager administrative credentials

Default is itnmadmin (or the DASH superuser, who must have the 'ncw_admin' role in DASH

Password

Netcool Configuration Manager presentation server

Connection details to the Netcool Configuration Manager Presentation server

A skip validation option should the Presentation server be unavailable

Tivoli Common Reporting server

Connection details to the Tivoli Common Reporting server

A skip validation option should the Tivoli Common Reporting server be unavailable

6. Complete the installation.

Tip: Best practice recommendation: You can generate a response file through Installation Manager, as in the following example:

```
<?xml version='1.0' encoding='UTF-8'?>
<agent-input>
  <variables>
    <variable name='sharedLocation' value='/opt/IBM/IMShared' />
  </variables>
  <server>
    <repository location='/opt/IBM/IM/output' />
  </server>
  <profile id='IBM Netcool GUI Components' installLocation='/opt/IBM/netcool/gui'>
    <data key='eclipseLocation' value='/opt/IBM/netcool/gui' />
    <data key='user.import.profile' value='false' />
    <!--Update OS to aix for AIX-->
    <data key='cic.selector.os' value='linux' />
    <!--Update architecture to ppc64 for AIX-->
    <data key='cic.selector.arch' value='x86_64' />
    <data key='cic.selector.ws' value='gtk' />
    <data key='user.org.apache.ant.classpath' value='/root/IBM/InstallationManager_Group/eclipse/plugins/
org.apache.ant_1.8.3.v201301120609/lib/ant.jar' />
    <data key='user.org.apache.ant.launcher.classpath' value='/root/IBM/InstallationManager_Group/eclipse/
plugins/org.apache.ant_1.8.3.v201301120609/lib/ant-launcher.jar' />
    <data key='cic.selector.nl' value='en' />
    <data key='user.DashHomeDir' value='/opt/IBM/JazzSM/ui' />
    <data key='user.WasHomeDir' value='/opt/IBM/WebSphere/AppServer' />
    <data key='user.DashHomeUserID' value='smadmin' />
    <data key='user.DashHomeContextRoot' value='/ibm/console' />
    <data key='user.DashHomeWasCell' value='JazzSMNode01Cell' />
    <data key='user.DashHomeWasNode' value='JazzSMNode01' />
    <data key='user.DashHomeWasServerName' value='server1' />
    <data key='user.SaaSEnabled' value='' />
    <data key='user.JAZZSM_HOME,com.ibm.tivoli.netcool.itnm.gui' value='/opt/IBM/JazzSM' />
    <data key='user.WAS_SERVER_NAME,com.ibm.tivoli.netcool.itnm.gui' value='server1' />
    <data key='user.WAS_PROFILE_PATH,com.ibm.tivoli.netcool.itnm.gui' value='/opt/IBM/JazzSM/profile' />
    <data key='user.WAS_USER_NAME,com.ibm.tivoli.netcool.itnm.gui' value='smadmin' />
    <data key='user.itnm.ObjectServerUsername,com.ibm.tivoli.netcool.itnm.gui' value='root' />
```

```

<data key='user.itnm.ObjectServer.skip.validation,com.ibm.tivoli.netcool.itnm.gui' value='false'/>
<data key='user.itnm.ObjectServerHostname,com.ibm.tivoli.netcool.itnm.gui' value='NMGUIServerLocation'/>
<data key='user.itnm.ObjectServerName,com.ibm.tivoli.netcool.itnm.gui' value='NCOMS'/>
<data key='user.itnm.ObjectServer.create.instance,com.ibm.tivoli.netcool.itnm.gui' value='false'/>
<data key='user.itnm.ObjectServerMainPort,com.ibm.tivoli.netcool.itnm.gui' value='4105'/>
<data key='user.itnm.database.server.type,com.ibm.tivoli.netcool.itnm.gui' value='db2'/>
<data key='user.itnm.database.skip.validation,com.ibm.tivoli.netcool.itnm.gui' value='false'/>
<data key='user.itnm.database.name,com.ibm.tivoli.netcool.itnm.gui' value='NCIM'/>
<data key='user.itnm.database.hostname,com.ibm.tivoli.netcool.itnm.gui' value='DatabaseServerLocation'/>
<data key='user.itnm.database.username,com.ibm.tivoli.netcool.itnm.gui' value='db2inst1'/>
<data key='user.itnm.database.create.tables,com.ibm.tivoli.netcool.itnm.gui' value='false'/>
<data key='user.itnm.database.tables.prefix,com.ibm.tivoli.netcool.itnm.gui' value=''/>
<data key='user.itnm.database.port,com.ibm.tivoli.netcool.itnm.gui' value='50001'/>
<data key='user.WAS_USER_NAME' value='smadmin'/>
<data key='user.itnm.ObjectServerItnmAdminUsername,com.ibm.tivoli.netcool.itnm.gui' value='itnadmin'/>
<data key='user.itnm.ObjectServerItnmAdminUsername' value='itnadmin'/>
<data key='user.itncm.database.port' value='1521'/>
<data key='user.itncm.database.schema' value='itncm'/>
<data key='user.itncm.database.type' value='ORACLE_12'/>
<data key='user.itncm.database.username' value='DBUSER'/>
<data key='user.itncm.database.hostname' value='DatabaseServerLocation'/>
<data key='user.itncm.pres.server.port' value='16311'/>
<data key='user.itncm.pres.server.hostname' value='PresentationServerLocation'/>
<data key='user.itncm.pres.server.skip.conn.check' value='true'/>
<data key='user.itncm.pres.server.scheme' value='https'/>
<data key='user.itncm.reports.path' value='/tarf/servlet/dispatch'/>
<data key='user.itncm.reports.skip.conn.check' value='true'/>
<data key='user.itncm.reports.port' value='16311'/>
<data key='user.itncm.reports.hostname' value='TCRServerLocation'/>
<data key='user.itncm.reports.scheme' value='https'/>
<data key='user.WAS_PASSWORD,com.ibm.tivoli.netcool.itnm.gui' value=''/>
<data key='user.itnm.ObjectServerItnmUserPassword,com.ibm.tivoli.netcool.itnm.gui' value=''/>
<data key='user.WAS_PASSWORD' value=''/>
<data key='user.itnm.ObjectServerItnmUserPassword' value=''/>
<data key='user.itncm.database.password' value=''/>
</profile>
<install modify='false'>
  <!-- IBM Dashboard Applications for ITNCM 6.4.2 -->
  <offering profile='IBM Netcool GUI Components' id='com.ibm.tivoli.netcool.itncm.ui.dash' version=
'6.4.2.20160202_1049'
features='main.feature.activityviewer,main.feature.wizard' installFixes='none'/>
</install>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='${sharedLocation}'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>

```

Before you can access the Netcool Configuration Manager DASH components, you must set up the Netcool Configuration Manager DASH users and provide them with appropriate access permission.

Once users have been set up, you access the Netcool Configuration Manager DASH components, that is, the Activity Viewer, the DASH wizards, and the thick-client launch portal in the following ways:

- You launch the stand-alone Netcool Configuration Manager UIs (sometimes referred to as the thick-client UIs), from the DASH thick-client launch portal.
- You access the Activity Viewer, the DASH wizards, and a subset of reports **in context** from Network Manager and Tivoli Netcool/OMNIBus.
- You access the complete reports using the DASH Tivoli Common Reporting GUI.

Related concepts

Configuring single sign-on

The single sign-on (SSO) capability in Tivoli® products means that you can log on to one Tivoli application and then launch to other Tivoli web-based or web-enabled applications without having to re-enter your user credentials.

Installing and configuring the products

The products and components that support the integration must be installed, and must be in an operational state before you configure the integration.

Related tasks

Configuring separate database types

Under certain circumstances, such as when different or remote databases are used in an integrated environment, you must perform additional database configuration steps.

Configuring integration with Tivoli Netcool/OMNIBus

Ensure that you have Netcool/OMNIBus Knowledge Library (NcKL) Enhanced Probe Rules for Netcool Configuration Manager installed on your Tivoli Netcool/OMNIBus server.

Configuring integration with Network Manager

Copy a number of jar files from the Network Manager GUI server into the Netcool Configuration Manager instance of WebSphere.

Configuring device synchronization

You configure device synchronization to enable Netcool Configuration Manager to use Network Manager for network device discovery.

Configuring the Alerts menu of the Active Event List

You must add access to the Activity Viewer from the Active Event List by configuring the Alerts menu.

Migrating reports

If you have custom reports in an existing Netcool Configuration Manager installation, and are integrating with Network Manager, which has its own Tivoli Common Reporting solution, you migrate your custom reports from the stand-alone to the integrated version of Tivoli Common Reporting.

Related reference

User role requirements

Certain administrative user roles are required for the integration.

Configuring separate database types

Under certain circumstances, such as when different or remote databases are used in an integrated environment, you must perform additional database configuration steps.

If you are installing Network Manager and ITNCM-Reports together, and if the Network Manager database is DB2 and on a different server, then its component databases must be cataloged.

If Network Manager uses an Informix database in a distributed environment and DASH is not installed on the same server as Network Manager, you ensure that the correct library jars are used.

1. Required: **If Network Manager and ITNCM-Reports are installed together, and if the Network Manager database is DB2 and on a different server:**

- a) To connect to a DB2 database on a server remote from your TCR Installation, ensure that a DB2 client is installed and the remote database cataloged. When the database server is remote to the WebSphere Application Server node where configuration is taking place, enter the following command at the node to add a TCP/IP node entry to the node directory:

```
db2 catalog tcpip node <NODENAME> remote <REMOTE> server <PORT>
```

where

NODENAME

Specifies a local alias for the node to be cataloged.

REMOTE

Specifies the fully qualified domain name of the remote DB server.

PORT

Is the port on which the database is accessible, typically port 50000.

```
db2 catalog database <database_name> at node <NODENAME>
```

where

database_name

Specifies the DB2 database name.

NODENAME

Is the local alias specified in the previous step.

- b) Add 'source \$HOME/sql/lib/db2profile' to your *<install_user>/ .bash_profile*.

Where \$HOME refers to the home directory of the user which was configured during the installation of the DB2 client to manage the client (usually db2inst1), and *<install_user>* is the user who installed Netcool Configuration Manager, usually 'icosuser'.

Note: The .bash_profile is only used for bash shell, and it will be different for sh, csh or ksh.

- c) Restart your reporting server after this update. However, before restarting the Reporting Server, check that the amended login profile has been sourced.

Tip: For installations which use a DB2 database, Cognos requires 32 bit DB2 client libraries, which will be installed by the 64 bit DB2 client. However, there maybe further dependencies on other 32 bit packages being present on the system; if such errors are reported, you can check this with '**ldd \$library_name**'.

2. Required: **If Network Manager and ITNCM-Reports are installed together, and if the Network Manager database is Oracle:**

- a) To connect to an Oracle database from your TCR Installation, ensure that ITNCM-Reports have been installed, and then update the *itncmEnv.sh* file default location:

```
/opt/IBM/tivoli/netcool/ncm/reports/itncmEnv.sh
```

Export the following variables (where *<install directory>* is the Netcool Configuration Manager installation directory):

ORACLE_HOME

```
ORACLE_HOME=<install directory>/reports/oracle
export ORACLE_HOME
```

TNS_ADMIN

```
TNS_ADMIN=<install directory>/reports/oracle/network/admin
export TNS_ADMIN
```

LD_LIBRARY_PATH

```
LD_LIBRARY_PATH=<install directory>/reports/oracle:$LD_LIBRARY_PATH
export LD_LIBRARY_PATH
```

- b) Create a *tnsnames.ora* file located in *<install directory>/reports/oracle/network/admin/*

- c) Add the NCIM database to the *tnsnames.ora* file.

For example: NCIM = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(Host = <Database Server>)(Port = 1521))) (CONNECT_DATA = (SERVICE_NAME = NCIM)))

- d) Add 'source *<install directory>/reports/itncmEnv.sh*' to your *<install_user>/ .bash_profile*.

Note: The .bash_profile is only used for bash shell, and it will be different for sh, csh or ksh.

- e) Restart your reporting server after this update. However, before restarting the Reporting Server, check that the amended login profile has been sourced.

Related concepts

[Configuring single sign-on](#)

The single sign-on (SSO) capability in Tivoli® products means that you can log on to one Tivoli application and then launch to other Tivoli web-based or web-enabled applications without having to re-enter your user credentials.

Related tasks

Installing the DASH components

For integrated scenarios, Netcool Configuration Manager provides the following DASH components: The Activity Viewer, the DASH wizards, and the Netcool Configuration Manager thick-client launch portal.

Configuring integration with Tivoli Netcool/OMNIBus

Ensure that you have Netcool/OMNIBus Knowledge Library (NcKL) Enhanced Probe Rules for Netcool Configuration Manager installed on your Tivoli Netcool/OMNIBus server.

Configuring integration with Network Manager

Copy a number of jar files from the Network Manager GUI server into the Netcool Configuration Manager instance of WebSphere.

Configuring device synchronization

You configure device synchronization to enable Netcool Configuration Manager to use Network Manager for network device discovery.

Configuring the Alerts menu of the Active Event List

You must add access to the Activity Viewer from the Active Event List by configuring the Alerts menu.

Migrating reports

If you have custom reports in an existing Netcool Configuration Manager installation, and are integrating with Network Manager, which has its own Tivoli Common Reporting solution, you migrate your custom reports from the stand-alone to the integrated version of Tivoli Common Reporting.

Related reference

User role requirements

Certain administrative user roles are required for the integration.

Configuring integration with Tivoli Netcool/OMNIBus

Ensure that you have Netcool/OMNIBus Knowledge Library (NcKL) Enhanced Probe Rules for Netcool Configuration Manager installed on your Tivoli Netcool/OMNIBus server.

Deploy rules specific to Netcool Configuration Manager. These rules have been bundled with Netcool Configuration Manager and deployed on the Netcool Configuration Manager Presentation server during installation, and are located in the `<NCM-INSTALL-DIR>/nckl-rules` directory.

Note: This procedure is no longer required for device synchronization with Network Manager, and the mapping of devices between Netcool Configuration Manager and Network Manager.

The standard Netcool/OMNIBus Knowledge Library configuration must have been applied to the ObjectServer and to the SNMP Probe as part of the prerequisite tasks for the integration. The `$NC_RULES_HOME` environment variable must also have been set on the computer where the probe is installed. This environment variable is set to `$NCHOME/etc/rules` on UNIX or Linux.

Tip: To source the Network Manager environment script, run the following script:

`./opt/IBM/tivoli/netcool/env.sh` where `opt/IBM/tivoli/netcool` is the default Network Manager directory.

Note: If you have existing SNMP Probe custom rules that you want to preserve, create backups as required before deploying the Netcool/OMNIBus Knowledge Library rules in step two.

The location denoted by `$NC_RULES_HOME` holds a set of Netcool/OMNIBus Knowledge Library lookup files and rules files within a number of sub-directories. In particular, the `$NC_RULES_HOME/include-snmpttrap/ibm` subdirectory contains files that can be applied to the SNMP Probe. To support the integration, you must add customized rules for Netcool Configuration Manager to this subdirectory.

Remember: If you have installed Netcool/OMNIBus Knowledge Library (NcKL) Enhanced Probe Rules Version 4.4 Multiplatform English (NcKL4.4) on your Tivoli Netcool/OMNIBus server, which is the recommended option, you do not need to install the ITNCM-specific Rules files, as documented here.

Installing rules files specific to Netcool Configuration Manager (not the recommended option)

1. From the server where you have installed Netcool Configuration Manager, copy the following files:

- `ncm_install_dir/nckl_rules/nckl_rules.zip`

where `ncm_install_dir` represents the installation location of Netcool Configuration Manager, for example `/opt/IBM/tivoli/netcool/ncm`

Copy these files to a temporary location on the computer where the SNMP Probe is installed.

2. Extract the contents of the `nckl_rules.zip` file, and then copy the extracted files to the `$NC_RULES_HOME/include-snmpttrap/ibm` subdirectory.
3. If object server failover has already been configured, proceed to step 4. Otherwise, perform the following steps:
 - a) Go to the folder in which the `mttrapd.props` has been placed, for example `$NCHOME/omnibus/probes/AIX5`, where `AIX5` is specific to your operating system.
 - b) Edit the `mttrapd.props` file by commenting out the backup object server reference:
`#ServerBackup : ''`
4. To ensure that the probe can reference the enhanced lookup and rules files, edit the `$NC_RULES_HOME/snmpttrap.rules` file by uncommenting the following include statements, as shown:

```
include "$NC_RULES_HOME/include-snmpttrap/ibm/ibm.master.include.lookup"
include "$NC_RULES_HOME/include-snmpttrap/ibm/ibm.master.include.rules"
include "$NC_RULES_HOME/include-snmpttrap/ibm/ibm-preclass.include.snmpttrap.rules"
```

5. Run the probe. If the probe was already running, force the probe to re-read the rules file so that the changes can take effect, for example:

Locate the PID of the probe by running the following command on the server running the probe. Look for a process named - `nco_p_mttrapd`

```
ps -eaf | grep mttrapd
kill -9 PID
```

Note: If the probe is installed on a different computer from Network Manager or the DASH portal, you must restart the probe manually.

Related concepts

[Configuring single sign-on](#)

The single sign-on (SSO) capability in Tivoli® products means that you can log on to one Tivoli application and then launch to other Tivoli web-based or web-enabled applications without having to re-enter your user credentials.

[Installing and configuring the products](#)

The products and components that support the integration must be installed, and must be in an operational state before you configure the integration.

Related tasks

[Installing the DASH components](#)

For integrated scenarios, Netcool Configuration Manager provides the following DASH components: The Activity Viewer, the DASH wizards, and the Netcool Configuration Manager thick-client launch portal.

[Configuring separate database types](#)

Under certain circumstances, such as when different or remote databases are used in an integrated environment, you must perform additional database configuration steps.

[Configuring integration with Network Manager](#)

Copy a number of jar files from the Network Manager GUI server into the Netcool Configuration Manager instance of WebSphere.

[Configuring device synchronization](#)

You configure device synchronization to enable Netcool Configuration Manager to use Network Manager for network device discovery.

Configuring the Alerts menu of the Active Event List

You must add access to the Activity Viewer from the Active Event List by configuring the Alerts menu.

Migrating reports

If you have custom reports in an existing Netcool Configuration Manager installation, and are integrating with Network Manager, which has its own Tivoli Common Reporting solution, you migrate your custom reports from the stand-alone to the integrated version of Tivoli Common Reporting.

Configuring the SNMP Probe and Netcool/OMNIBus Knowledge Library

Netcool Configuration Manager requires the Tivoli Netcool/OMNIBus nco-p-mttrapd probe and the Netcool/OMNIBus Knowledge Library to be installed on the ObjectServer host.

Related reference

User role requirements

Certain administrative user roles are required for the integration.

Configuring integration with Network Manager

Copy a number of jar files from the Network Manager GUI server into the Netcool Configuration Manager instance of WebSphere.

Note: The following default locations may differ depending on where WebSphere was installed on your Network Manager and Netcool Configuration Manager servers.

Copy the following jars from the Network Manager GUI server into the corresponding folder in the Netcool Configuration Manager WebSphere instance.

- /opt/IBM/WebSphere/AppServer/etc/vmm4ncos.jks
- /opt/IBM/WebSphere/AppServer/lib/ext/com.ibm.tivoli.ncw.ncosvmm.jar
- /opt/IBM/WebSphere/AppServer/lib/ext/jconn3.jar

Related concepts

Configuring single sign-on

The single sign-on (SSO) capability in Tivoli® products means that you can log on to one Tivoli application and then launch to other Tivoli web-based or web-enabled applications without having to re-enter your user credentials.

Related tasks

Installing the DASH components

For integrated scenarios, Netcool Configuration Manager provides the following DASH components: The Activity Viewer, the DASH wizards, and the Netcool Configuration Manager thick-client launch portal.

Configuring separate database types

Under certain circumstances, such as when different or remote databases are used in an integrated environment, you must perform additional database configuration steps.

Configuring integration with Tivoli Netcool/OMNIBus

Ensure that you have Netcool/OMNIBus Knowledge Library (NcKL) Enhanced Probe Rules for Netcool Configuration Manager installed on your Tivoli Netcool/OMNIBus server.

Configuring device synchronization

You configure device synchronization to enable Netcool Configuration Manager to use Network Manager for network device discovery.

Configuring the Alerts menu of the Active Event List

You must add access to the Activity Viewer from the Active Event List by configuring the Alerts menu.

Migrating reports

If you have custom reports in an existing Netcool Configuration Manager installation, and are integrating with Network Manager, which has its own Tivoli Common Reporting solution, you migrate your custom reports from the stand-alone to the integrated version of Tivoli Common Reporting.

Related reference

User role requirements

Certain administrative user roles are required for the integration.

Configuring device synchronization

You configure device synchronization to enable Netcool Configuration Manager to use Network Manager for network device discovery.

During Netcool Configuration Manager 6.4.2 installation you are asked if the product is to be integrated or not. If you select **Yes** the installer will ask the necessary questions to set up the configuration of device synchronization between Netcool Configuration Manager and Network Manager.

A default value of 24 hours (1440mins) is defined in the Netcool Configuration Manager `rseries.properties` file for the periodic synchronization with Network Manager.

For the initial synchronization, a large number of devices may already have been discovered by Network Manager, and it can take a considerable time before they are imported into Netcool Configuration Manager. (This also applies in a situation where the discovery scope is widened so that a significant number of new devices are added to Network Manager.)

Consequently the devices may not yet appear in the `NMENTITYMAPPING` table in the Netcool Configuration Manager database, and therefore the context tools (right-click tools) from Network Manager will not be available for those devices.

Tip: You can reduce this time by editing the `rseries.properties` file, and changing the mapping period to 60 (for example). This will speed up the process by which devices are added to the autodiscovery queue on Netcool Configuration Manager, but will not change the actual time to import each device configuration.

Tip:

If the password for the itnadmin user has changed on Network Manager, update the locally stored copy on Netcool Configuration Manager as follows:

Use the `icosadmin` script located in `/opt/IBM/tivoli/netcool/ncm/bin`.

For example:

```
icosadmin ChangeNmPassword -u itnadmin -p <new_password>
```

The configuration is stored in the `rseries.properties` file located in the following directory: `<ncm-install-dir>/config/properties/`

Network Manager:

```
NMEntityMappingComponent/baseURL=https://nmguiservername:16311
NMEntityMappingComponent/uri=/ibm/console/nm_rest/topology/devices/domain/NCOMS
NMEntityMappingComponent/uriParam=
NMEntityMappingComponent/uriProps=
####Note: Complete URL = baseURL+uri+uriProps&uriParam

NMEntityMappingComponent/delay=10 ## delay on startup before first run (in minutes)
NMEntityMappingComponent/importRealm=ITNCM/@DOMAINNAME
NMEntityMappingComponent/maxDevicesPerRealm=50
NMEntityMappingComponent/ncmUser=administrator
NMEntityMappingComponent/period=1440 ## Daily (in minutes)
NMEntityMappingComponent/user=itnadmin
NMEntityMappingComponent/passwd=netcool ## Optional: Install stores securely
NMEntityMappingComponent/deviceNameFilter=
NMEntityMappingComponent/allowDuplicateDeviceForSeparateDomains=false
NMEntityMappingComponent/securityComponent=TLSv1.2
```

Note: You can edit this file and the component configuration properties after install if requirements change.

Before device synchronization runs for the first time ensure that the Network Manager Rest API user (in our example 'itnmadmin') has the ncp_rest_api role in DASH.

Device synchronization is now done by a new core component of Netcool Configuration Manager, and is therefore part of Netcool Configuration Manager Component configuration and started automatically when Netcool Configuration Manager starts. Component start up is configured in <ncm-install-dir>/config/server/config.xml

```
<component>
<name>NMEntityMappingComponent</name>
<class>com.intelliden.nmentitemapping.NMEntityMappingComponent</class>
</component>
```

Note: The NMEntityMappingComponent is configured by default so if you wish to stop it being started on Netcool Configuration Manager startup you can comment it out in the config.xml file.

Note: There is a limit of 50 imported devices per Realm in Netcool Configuration Manager. If there are more devices than this in a Network Manager domain, they will be added to sub-realms (labeled 001, 002, etc) in Netcool Configuration Manager.

Troubleshooting NM Component

Verify that the component has started in file:

```
<NCM_INSTALL_DIR>/logs/Server.out
Fri Jul 31 13:30:06 GMT+00:00 2015 - Starting component :
NMEntityMappingComponent
Fri Jul 31 13:30:06 GMT+00:00 2015 - All components started
```

Verify that the config.xml file has the component specified for startup

Verify that the NMEntityMapping table has the new columns required for the new component implementation:

```
"NMENTITYMAPPING" (
"UNIQUEKEY" BIGINT NOT NULL,
"ENTITYID" BIGINT NOT NULL DEFAULT 0,
"RESOURCEBROWSERID" BIGINT NOT NULL DEFAULT 0,
"DOMAINNAME" VARCHAR(64),
"JPAVERSION" BIGINT NOT NULL DEFAULT 1,
"ENTITYNAME" VARCHAR(255),
"ACCESSIPADDRESS" VARCHAR(64),
"SERIALNUMBER" VARCHAR(64),
"VENDORTYPE" VARCHAR(64),
"MODELNAME" VARCHAR(64),
"OSVERSION" VARCHAR(64),
"OSIMAGE" VARCHAR(255),
"OSTYPE" VARCHAR(64),
"HARDWAREVERSION" VARCHAR(64)
)
```

Ensure that the Network Manager Rest API user has the ncp_rest_api role in DASH.

Related concepts

[Configuring single sign-on](#)

The single sign-on (SSO) capability in Tivoli® products means that you can log on to one Tivoli application and then launch to other Tivoli web-based or web-enabled applications without having to re-enter your user credentials.

Related tasks

[Installing the DASH components](#)

For integrated scenarios, Netcool Configuration Manager provides the following DASH components: The Activity Viewer, the DASH wizards, and the Netcool Configuration Manager thick-client launch portal.

[Configuring separate database types](#)

Under certain circumstances, such as when different or remote databases are used in an integrated environment, you must perform additional database configuration steps.

[Configuring integration with Tivoli Netcool/OMNIBus](#)

Ensure that you have Netcool/OMNIBus Knowledge Library (NcKL) Enhanced Probe Rules for Netcool Configuration Manager installed on your Tivoli Netcool/OMNIBus server.

Configuring integration with Network Manager

Copy a number of jar files from the Network Manager GUI server into the Netcool Configuration Manager instance of WebSphere.

Configuring the Alerts menu of the Active Event List

You must add access to the Activity Viewer from the Active Event List by configuring the Alerts menu.

Migrating reports

If you have custom reports in an existing Netcool Configuration Manager installation, and are integrating with Network Manager, which has its own Tivoli Common Reporting solution, you migrate your custom reports from the stand-alone to the integrated version of Tivoli Common Reporting.

Related reference

User role requirements

Certain administrative user roles are required for the integration.

Configuring the Alerts menu of the Active Event List

You must add access to the Activity Viewer from the Active Event List by configuring the Alerts menu.

1. From the navigation pane, click **Administration > Event Management Tools > Menu Configuration**.
2. From the **Available menus** list on the right, select **alerts** and click **Modify**.
3. From the **Menus Editor** window, select **<separator>** from the drop-down list under **Available items**, and then click **Add selected item** to add the item to the **Current items** list.
The **<separator>** item is added as the last item.
4. Under **Available items**, select **menu** from the drop-down list.
The list of all menu items that can be added to the **Alerts** menu is shown.
5. Select the **Configuration Management** item and click **Add selected item**.
The item is added below the **<separator>** item in the **Current items** list.
6. Click **Save** and then click **OK**.

The **Configuration Management** submenu and tools are now available in the **Alerts** menu of the Active Event List, for use with Netcool Configuration Manager events.

Note: Tivoli Netcool/OMNIBus version 7.4 onwards, Active Event List is replaced with Event viewer which allows you to view events in the Web GUI.

Note: Reports Menu options will not be displayed if the selected event is not enriched.

You can optionally create a global filter to restrict the events displayed in the Active Event List to Netcool Configuration Manager events only. You can add this filter to the Web GUI either by using the WAAPI client or by using the Filter Builder. When creating the filter, specify a meaningful name (for example, ITNCEvents) and define the filter condition by specifying the following SQL WHERE clause:

```
where Class = 87724
```

For further information about creating filters, see the *IBM Tivoli Netcool/OMNIBus Web GUI Administration and User's Guide* in the Tivoli Netcool/OMNIBus Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_OMNIBus.doc_7.3.1/omnibus/wip/welcome.htm.

Related concepts

Configuring single sign-on

The single sign-on (SSO) capability in Tivoli® products means that you can log on to one Tivoli application and then launch to other Tivoli web-based or web-enabled applications without having to re-enter your user credentials.

Related tasks

Installing the DASH components

For integrated scenarios, Netcool Configuration Manager provides the following DASH components: The Activity Viewer, the DASH wizards, and the Netcool Configuration Manager thick-client launch portal.

Configuring separate database types

Under certain circumstances, such as when different or remote databases are used in an integrated environment, you must perform additional database configuration steps.

Configuring integration with Tivoli Netcool/OMNIBus

Ensure that you have Netcool/OMNIBus Knowledge Library (NcKL) Enhanced Probe Rules for Netcool Configuration Manager installed on your Tivoli Netcool/OMNIBus server.

Configuring integration with Network Manager

Copy a number of jar files from the Network Manager GUI server into the Netcool Configuration Manager instance of WebSphere.

Configuring device synchronization

You configure device synchronization to enable Netcool Configuration Manager to use Network Manager for network device discovery.

Migrating reports

If you have custom reports in an existing Netcool Configuration Manager installation, and are integrating with Network Manager, which has its own Tivoli Common Reporting solution, you migrate your custom reports from the stand-alone to the integrated version of Tivoli Common Reporting.

Monitoring Netcool Configuration Manager events in the Active Event List

You can monitor Netcool Configuration Manager events in the Active Event List to enable you to identify when configuration changes are made to devices in the network, and to help you ensure that the network configuration complies with your corporate regulations.

Running Netcool Configuration Manager reports

You can run Netcool Configuration Manager reports on network devices to view summary information relating to configuration and compliance. The reports provide information that can be used for fault correlation purposes in Tivoli Netcool/OMNIBus and Network Manager.

Related reference

User role requirements

Certain administrative user roles are required for the integration.

Migrating reports

If you have custom reports in an existing Netcool Configuration Manager installation, and are integrating with Network Manager, which has its own Tivoli Common Reporting solution, you migrate your custom reports from the stand-alone to the integrated version of Tivoli Common Reporting.

If you are installing Network Manager on the same server as your existing Netcool Configuration Manager installation, you must export your custom reports before installing Network Manager.

The report migration procedure is different for single and multiple server integrations.

If you are installing Netcool Configuration Manager and Network Manager on the same server

1. Export the custom reports from the existing Netcool Configuration Manager version of Tivoli Common Reporting and copy them to a safe location.

Note: You export your custom reports before installing Network Manager to prevent the existing reports from being overwritten.

2. Disable and uninstall the existing Netcool Configuration Manager version of Tivoli Common Reporting.
3. Install Network Manager and integrate it with the existing version of Netcool Configuration Manager as documented.
4. Import the custom reports into the Network Manager version of Tivoli Common Reporting.

If you are installing Netcool Configuration Manager and Network Manager on different servers

1. Install Network Manager and integrate it with the existing version of Netcool Configuration Manager as documented.
2. Export the custom reports from the existing Netcool Configuration Manager version of Tivoli Common Reporting and copy them to the Network Manager server.
3. Import the custom reports into the Network Manager version of Tivoli Common Reporting.
4. Disable the existing Netcool Configuration Manager version of Tivoli Common Reporting.

Related concepts

Configuring single sign-on

The single sign-on (SSO) capability in Tivoli® products means that you can log on to one Tivoli application and then launch to other Tivoli web-based or web-enabled applications without having to re-enter your user credentials.

Related tasks

Installing the DASH components

For integrated scenarios, Netcool Configuration Manager provides the following DASH components: The Activity Viewer, the DASH wizards, and the Netcool Configuration Manager thick-client launch portal.

Configuring separate database types

Under certain circumstances, such as when different or remote databases are used in an integrated environment, you must perform additional database configuration steps.

Configuring integration with Tivoli Netcool/OMNIBus

Ensure that you have Netcool/OMNIBus Knowledge Library (NcKL) Enhanced Probe Rules for Netcool Configuration Manager installed on your Tivoli Netcool/OMNIBus server.

Configuring integration with Network Manager

Copy a number of jar files from the Network Manager GUI server into the Netcool Configuration Manager instance of WebSphere.

Configuring device synchronization

You configure device synchronization to enable Netcool Configuration Manager to use Network Manager for network device discovery.

Configuring the Alerts menu of the Active Event List

You must add access to the Activity Viewer from the Active Event List by configuring the Alerts menu.

Exporting custom reports (single server integration architecture)

Before you install Network Manager on the same server as your existing Netcool Configuration Manager installation, you must export any custom reports. You also disable and uninstall the existing Netcool Configuration Manager version of Tivoli Common Reporting.

Related reference

User role requirements

Certain administrative user roles are required for the integration.

Exporting custom reports (distributed integration architecture)

After you have installed Network Manager on a server other than your existing Netcool Configuration Manager installation and performed all integration tasks, you export your custom reports. You also disable and uninstall the existing Netcool Configuration Manager version of Tivoli Common Reporting.

You export reports **after** installing Network Manager when all of the following circumstances apply to your scenario:

- You are already running Tivoli Common Reporting as part of an existing, non-integrated Netcool Configuration Manager installation.
- You are deploying a distributed integration architecture and have already installed Network Manager on a server other than your existing version of Netcool Configuration Manager.

- You have customized Netcool Configuration Manager reports that need to be migrated into your planned integrated solution.

When you install the Network Manager version of Tivoli Common Reporting on a server other than your existing version of Netcool Configuration Manager, the previous reports as well as the previous version of TCR remain on the Netcool Configuration Manager server. To migrate such reports into an integrated solution, you perform the following tasks:

If you are installing Netcool Configuration Manager and Network Manager on different servers

1. Install Network Manager and integrate it with the existing version of Netcool Configuration Manager as documented.
2. Export the custom reports from the existing Netcool Configuration Manager version of Tivoli Common Reporting and copy them to the Network Manager server.
3. Import the custom reports into the Network Manager version of Tivoli Common Reporting.
4. Disable the existing Netcool Configuration Manager version of Tivoli Common Reporting.

Remember: You do not have to migrate the standard Netcool Configuration Manager reports, because these will be installed together with the Network Manager version of Tivoli Common Reporting (in addition to a number of Network View reports). You only migrate reports you have customized since installing the standard reports, or new reports you have created.

1. Log into the Netcool Configuration Manager version of Tivoli Common Reporting using the following URL:
`http://hostname:16310/ibm/console`
where *hostname* is the name of your Netcool Configuration Manager server and 16310 is the default port number for Tivoli Common Reporting.
2. Click **Reporting > Common Reporting**.
3. Click **Launch** on the toolbar, and then select **Administration** from the drop-down menu.
4. Select the **Configuration** tab, then click **Content Administration**.
5. Click **New Export** to launch the **New Export** wizard.
6. Enter a name and description for the report export, then click **Next**.
7. Accept the default deployment method and click **Next**.
8. Click the **Add** link and select the **ITNCM Reports** checkbox, then move ITNCM Reports to the **Selected Entries** list.
9. Click **OK**, then **Next > Next > Next**, accepting the default values.
10. Select **New archive**, then **Next > Next**, accepting the default values..
11. Click **Finish > Run > OK**.
The reports are exported and the new export archive is displayed.
12. Navigate to the following directory:
`/opt/IBM/tivoli/netcool/ncm/tipv2Components/TCRComponent/cognos/deployment`,
where you can view the report archive, for example:
`-rw-r--r-- 1 icosuser staff 262637 23 Feb 10:27 ncm_export.zip`
where `ncm_export.zip` is the report archive.
13. Copy the file to the following directory on the Network Manager server:
`$TIP_HOME/. . /TCRComponent/cognos/deployment`

You have exported the custom reports and copied them to the Network Manager server.

Next, you import the archived reports into the Network Manager version of Tivoli Common Reporting, and then disable the Netcool Configuration Manager version of Tivoli Common Reporting.

Importing reports (distributed integration architecture)

After exporting the custom reports and copying them to the Network Manager server, you import the archived reports into the Network Manager version of Tivoli Common Reporting, and then disable the version.

You must have exported the custom reports and copied them to the Network Manager server.

1. Log into the Network Manager DASH.
2. Click **Reporting > Common Reporting**.
3. Click **Launch** on the toolbar, and then select **Administration** from the drop-down menu.
4. Select the **Configuration** tab, then click **Content Administration**.
5. Click **New Import** to launch the **New Import** wizard.
A list of available report archives will be displayed.
6. Select the archive that you exported earlier and click **Next**.
7. Select **ITNCM Reports**, then **Next** and **Next** again, accepting the default values.
8. Click **Finish > Run > OK**.
The reports are imported and the new archive is displayed in the list of archives.
9. Close the Common Reporting tab and click the Common Reporting link in the navigation pane.
The custom reports will now be available in the Netcool Configuration Manager version of Tivoli Common Reporting.
10. Navigate to the following directory:
`/opt/IBM/tivoli/netcool/ncm/bin/utl/s/support`
11. Run the `setPlatform.sh` script: `bash-3.2$ ./setPlatform.sh` and disable Reporting, then exit.
When the Netcool Configuration Manager server is restarted, Tivoli Common Reporting will no longer be running.

You have now completed the migration of custom reports in your distributed custom environment.

Importing reports (single server integration architecture)

After exporting the custom reports, disabling and uninstalling the Netcool Configuration Manager version of Tivoli Common Reporting, and completing all other integration steps, you import the report archive into the Network Manager version of Tivoli Common Reporting,

You must have exported the custom reports before installing Network Manager on the same server as your existing Netcool Configuration Manager installation.

1. Log into the Network Manager DASH.
2. Click **Reporting > Common Reporting**.
3. Click **Launch** on the toolbar, and then select **Administration** from the drop-down menu.
4. Select the **Configuration** tab, then click **Content Administration**.
5. Click **New Import** to launch the **New Import** wizard.
A list of available report archives will be displayed.
6. Select the archive that you exported earlier and click **Next**.
7. Select **ITNCM Reports**, then **Next** and **Next** again, accepting the default values.
8. Click **Finish > Run > OK**.
The reports are imported and the new archive is displayed in the list of archives.
9. Close the **Common Reporting** tab and click the **Common Reporting** link in the navigation pane.
The custom reports will now be available in the Netcool Configuration Manager version of Tivoli Common Reporting.

Related tasks

[Exporting custom reports \(single server integration architecture\)](#)

Before you install Network Manager on the same server as your existing Netcool Configuration Manager installation, you must export any custom reports. You also disable and uninstall the existing Netcool Configuration Manager version of Tivoli Common Reporting.

Configuring single sign-on

The single sign-on (SSO) capability in Tivoli® products means that you can log on to one Tivoli application and then launch to other Tivoli web-based or web-enabled applications without having to re-enter your user credentials.

The repository for the user IDs is the Tivoli Netcool/OMNIBus ObjectServer. A user logs on to one of the participating applications, at which time their credentials are authenticated at a central repository. With the credentials authenticated to a central location, the user can then launch from one application to another to view related data or perform actions. Single sign-on can be achieved between applications deployed to DASH servers on multiple machines.

Single sign-on capabilities require that the participating products use Lightweight Third Party Authentication (LTPA) as the authentication mechanism. When SSO is enabled, a cookie is created containing the LTPA token and inserted into the HTTP response. When the user accesses other Web resources in any other application server process in the same Domain Name Service (DNS) domain, the cookie is sent with the request. The LTPA token is then extracted from the cookie and validated. If the request is between different cells of application servers, you must share the LTPA keys and the user registry between the cells for SSO to work. The realm names on each system in the SSO domain are case sensitive and must match exactly. See *Managing LTPA keys from multiple WebSphere® Application Server cells* on the WebSphere Application Server Information Center.

When configuring ITNCM-Reports for an integrated installation, ensure you configure single sign-on (SSO) on the Tivoli Common Reporting server. Specifically, you must configure SSO between the instance of WebSphere that is hosting the Network Manager GUI, and the instance of WebSphere that is hosting ITNCM Reports. This will prevent unwanted login prompts when launching reports from within Network Manager. For more information, see *Configuring WebSphere user registry* in the *IBM Tivoli Netcool Configuration Manager Installation and Configuration Guide*.

Related tasks

[Installing the DASH components](#)

For integrated scenarios, Netcool Configuration Manager provides the following DASH components: The Activity Viewer, the DASH wizards, and the Netcool Configuration Manager thick-client launch portal.

[Configuring separate database types](#)

Under certain circumstances, such as when different or remote databases are used in an integrated environment, you must perform additional database configuration steps.

[Configuring integration with Tivoli Netcool/OMNIBus](#)

Ensure that you have Netcool/OMNIBus Knowledge Library (NcKL) Enhanced Probe Rules for Netcool Configuration Manager installed on your Tivoli Netcool/OMNIBus server.

[Configuring integration with Network Manager](#)

Copy a number of jar files from the Network Manager GUI server into the Netcool Configuration Manager instance of WebSphere.

[Configuring device synchronization](#)

You configure device synchronization to enable Netcool Configuration Manager to use Network Manager for network device discovery.

[Configuring the Alerts menu of the Active Event List](#)

You must add access to the Activity Viewer from the Active Event List by configuring the Alerts menu.

[Migrating reports](#)

If you have custom reports in an existing Netcool Configuration Manager installation, and are integrating with Network Manager, which has its own Tivoli Common Reporting solution, you migrate your custom reports from the stand-alone to the integrated version of Tivoli Common Reporting.

Related reference

User role requirements

Certain administrative user roles are required for the integration.

Creating user groups for DASH

To configure single sign-on (SSO) between DASH and Netcool Configuration Manager, you must create Netcool Configuration Manager groups and roles for DASH.

Note: For SSO between DASH and Netcool Configuration Manager to work, the user groups specified in this procedure must exist in both DASH and Netcool Configuration Manager.

Network Manager and Netcool Configuration Manager users in DASH should use the same authentication type, for example, ObjectServer.

Note: The **IntellidenUser** role needs to be assigned to the **IntellidenUser** group. Similarly, the **IntellidenAdminUser** role needs to be given to the **IntellidenAdminUser** group.

1. Log onto the WebSphere Administrative console of the Network Manager GUI server as the profile owner (for example, smadmin).
2. Create a group by selecting **Users and Groups > Manage Groups > Create**.
3. Enter **IntellidenUser** in the Group name field.
4. Click **Create**, then click **Create Like**.
5. Enter **IntellidenAdminUser** in the Group name field.
IntellidenAdminUser is required for access to Account Management in Netcool Configuration Manager.
6. Click **Create**, then click **Close**.
7. Log off from the WebSphere Administrative console, then log on to the DASH GUI.
8. Select **Console Settings > Roles > IntellidenUser**.
9. Click **Users and Groups > Add Groups > Search**, then select the **IntellidenUser** group, and then click **Add**.
10. Select **Console Settings > Roles > IntellidenAdminUser**.
11. Click **Users and Groups > Add Groups > Search**, then select the **IntellidenAdminUser** group, and then click **Add**.

After creating Netcool Configuration Manager groups and roles for DASH, you create Netcool Configuration Manager users for DASH.

Creating users for DASH

This section explains how to create the Netcool Configuration Manager **Intelliden** super-user as well as the default users: **administrator**, **operator**, and **observer** for DASH.

For single sign-on (SSO) between DASH and Netcool Configuration Manager to work, a user must exist (that is, have an account) in both DASH and Netcool Configuration Manager.

At install time Netcool Configuration Manager automatically creates four users: **Intelliden**, **administrator**, **operator**, and **observer**. Of these users, only the **Intelliden** user must be created in DASH. However, it is advisable that the other users are also created.

Note: Only the username must match, it is not necessary that the passwords also match. After single-sign on configuration is complete, the user password entered in DASH will be used to authenticate a Netcool Configuration Manager login.

This task describes how to create the previously listed Netcool Configuration Manager users for DASH.

1. Log onto the WebSphere console of the Network Manager GUI server as the profile owner (for example, smadmin).
2. Click **Users and Groups > Manage Users**, then click **Create**.
3. Enter Intelliden in the User ID, First name, and Last Name fields.
4. Enter the Intelliden user's password in the Password and Confirm Password fields.
5. Click on **Group Membership** and select **Search**.
6. Highlight the **IntellidenAdminUser** and **IntellidenUser** groups in the matching groups list, and click **Add**, then click **Close**.
7. Click **Create**, then click **Create Like**.
8. Enter administrator in the following fields:
 - User ID
 - First name
 - Last Name
 - Password
 - Confirm password
9. Click on **Group Membership** and select **Search**.
10. Highlight the **IntellidenAdminUser** and **IntellidenUser** groups in the matching groups list, and click **Add**, then click **Close**.
11. Click **Create** and then **Close**.
12. Click **Create**.
13. Enter operator in the following fields:
 - User ID
 - First name
 - Last Name
 - Password
 - Confirm password
14. Click on **Group Membership** and select **Search**.
15. Highlight the **IntellidenUser** group in the matching groups list, and click **Add** and then **Close**.
16. Click **Create**, then click **Create Like**.
17. Enter observer in the following fields:
 - User ID
 - First name
 - Last Name
 - Password
 - Confirm password
18. Click on **Group Membership** and select **Search**.
19. Highlight the **IntellidenUser** group in the matching groups list, and click **Add**, then click **Close**.
20. Click **Create** and then **Close**.

After you have created the Netcool Configuration Manager users for DASH, you export the LTPA keystore to the Netcool Configuration Manager server.

Exporting the DASH LTPA keystore

For added security the contents of the LTPA token are encrypted and decrypted using a keystore (referred to in the subsequent procedure as the LTPA keystore) maintained by WebSphere. In order for two instances of WebSphere to share authentication information via LTPA tokens they must both use the

same LTPA keystore. The IBM Admin Console makes this a simple process of exporting the LTPA keystore on one instance of WebSphere and importing it into another.

This task describes how to export the LTPA keystore from the instance of WebSphere running on the Network Manager DASH server to the instance of WebSphere running on the Netcool Configuration Manager server for keystore synchronization.

1. Launch the DASH Admin Console. For example: http://www.nm_gui_server_ip.com:16310/ibm/console.
2. Navigate to **Settings > WebSphere Administrative Console**.
3. Click **Security > Global security**.
4. Under the **Authentication mechanisms and expiration** tab, click **LTPA**.
5. Under the **Cross-cell single sign-on** tab, enter a password in the Password and Confirm password fields.
The password will subsequently be used to import the LTPA keystore on the Netcool Configuration Manager server.
6. Enter the directory and filename you want the LTPA keystore to be exported to in the **Fully qualified key file name** field.
7. Complete by clicking **Export keys**.
8. Transfer the LTPA keystore to the Netcool Configuration Manager server.

You will receive a message indicating that the LTPA keystore has been exported successfully.

You now configure the SSO attributes for DASH.

Related tasks

Importing the DASH LTPA keystore to the Netcool Configuration Manager server

For added security the contents of the LTPA token are encrypted and decrypted using a keystore maintained by WebSphere. In order for two instances of WebSphere to share authentication information via LTPA tokens they must both use the same keystore. The IBM admin console makes this a simple process of exporting the keystore on one instance of WebSphere and importing it into another.

Configuring single sign-on attributes for DASH

Configuring SSO is a prerequisite to integrating products that are deployed on multiple servers. All DASH server instances must point to the central user registry.

Use these instructions to configure single sign-on attributes for the DASH.

1. Launch the DASH Admin Console. For example: http://www.nm_gui_server_ip.com:16310/ibm/console.
2. Navigate to **Settings > WebSphere Administrative Console**.
3. Select **Security**, then click **Global Security > Web and SIP Security > Single sign on (SSO)**.
4. In the **Authentication** area, expand Web security, then click **Global Security > Web and SIP Security (on the Authentication area) > Single sign on (SSO)**.
5. Select the **Enabled** option if SSO is disabled.
6. Deselect **Requires SSL**.
7. Enter the fully-qualified domain names in the Domain name field where SSO is effective. If the domain name is not fully qualified, the DASH server does not set a domain name value for the LTPAToken cookie and SSO is valid only for the server that created the cookie. For SSO to work across Tivoli® applications, their application servers must be installed in the same domain (use the same domain name). See below for an example.
8. Deselect the **Interoperability Mode** option.
9. Deselect the **Web inbound security attribute propagation** option.
10. Click **OK**, then save your changes.
11. Stop and restart all the DASH server instances. Log out of the WebSphere Administrative Console.

If DASH is installed on **server1.ibm.com** and Netcool Configuration Manager is installed on **server2.ibm.com**, then enter a value of **.ibm.com**.

You enable SSO on Netcool Configuration Manager next.

Related tasks

[Importing the DASH LTPA keystore to the Netcool Configuration Manager server](#)

For added security the contents of the LTPA token are encrypted and decrypted using a keystore maintained by WebSphere. In order for two instances of WebSphere to share authentication information via LTPA tokens they must both use the same keystore. The IBM admin console makes this a simple process of exporting the keystore on one instance of WebSphere and importing it into another.

Enabling SSO for Netcool Configuration Manager

Both Netcool Configuration Manager and Netcool Configuration Manager WebSphere must be configured to enable SSO.

This task describes how to enable SSO for Netcool Configuration Manager if it was not enabled during installation.

1. Navigate to `$NCM_installation_dir/Utils` .
2. Run the `configSSO.sh` script, for example:

```
cd /opt/IBM/tivoli/netcool/ncm/bin/Utils ./configSSO.sh enable
```

When SSO is enabled, the interface to Netcool Configuration Manager must accept an LTPA token as a means of authentication. This is achieved by importing the LTPA keystore to the Netcool Configuration Manager server.

Importing the DASH LTPA keystore to the Netcool Configuration Manager server

For added security the contents of the LTPA token are encrypted and decrypted using a keystore maintained by WebSphere. In order for two instances of WebSphere to share authentication information via LTPA tokens they must both use the same keystore. The IBM admin console makes this a simple process of exporting the keystore on one instance of WebSphere and importing it into another.

You must have exported the LTPA keystore from the instance of WebSphere running on the Network Manager DASH server and copied it to the Netcool Configuration Manager server in a previous task.

In this procedure you will import that LTPA keystore to the instance of WebSphere running on the Netcool Configuration Manager server.

1. Logon to the WebSphere Administrative Console for the Netcool Configuration Manager Presentation Server using the superuser name and password specified at install time (typically Intelliden).

For example: `http://NCM_presentation_server:16316/ibm/console`

2. Click **Security > Global security**.
3. Under **Authentication mechanisms and expiration**, click **LTPA**.
4. Under **Cross-cell single sign-on**, enter the password in the Password and Confirm password fields. This password is the one that was used when the LTPA keystore was exported from DASH.
5. Enter the LTPA keystore file name in the Fully qualified key file name field. This is the LTPA keystore that was exported from DASH.
6. Click **Import keys**.
7. Click **Save directly to the master configuration**.

You should now configure single sign-on attributes for the WebSphere instance running on the Netcool Configuration Manager server.

Related tasks

[Exporting the DASH LTPA keystore](#)

For added security the contents of the LTPA token are encrypted and decrypted using a keystore (referred to in the subsequent procedure as the LTPA keystore) maintained by WebSphere. In order for two instances of WebSphere to share authentication information via LTPA tokens they must both use the same LTPA keystore. The IBM Admin Console makes this a simple process of exporting the LTPA keystore on one instance of WebSphere and importing it into another.

Configuring single sign-on attributes for DASH

Configuring SSO is a prerequisite to integrating products that are deployed on multiple servers. All DASH server instances must point to the central user registry.

Related reference

User role requirements

Certain administrative user roles are required for the integration.

Configuring single sign-on attributes for Netcool Configuration Manager WebSphere

Configuring SSO is a prerequisite to integrating products that are deployed on multiple servers. All eWAS server instances must point to the central user registry.

This procedure is performed on the Netcool Configuration Manager eWAS instance running on the Netcool Configuration Manager server.

1. Logon to the WebSphere Administrative Console for the Netcool Configuration Manager Presentation Server using the superuser name and password specified at install time (typically Intelliden).

For example http://NCM_presentation_server:16316/ibm/console

2. In the **Authentication** area, expand Web security then click Single sign-on.
3. Select the **Enabled** option if SSO is disabled.
4. Deselect **Requires SSL**.
5. Leave the domain name blank in the **Domain name** field.
6. Deselect the **Interoperability Mode** option.
7. Deselect the **Web inbound security attribute propagation** option.
8. Click **Apply** to save your changes.
9. Click **Save Directly to the Master Configuration**.

You create a federated user repository for Netcool Configuration Manager next.

Creating and configuring a federated user repository for Netcool Configuration Manager

The first step for authenticating by using a Tivoli Netcool/OMNIBus ObjectServer is to create a federated user repository for Netcool Configuration Manager.

Important: Before attempting this procedure, complete the following task: [“Configuring integration with Network Manager” on page 31](#)

A federated user repository is built on Virtual Member Manager (VMM), which provides the ability to map entries from multiple individual user repositories into a single virtual repository. The federated user repository consists of a single named realm, which is a set of independent user repositories. Each user repository may be an entire external user repository.

This task describes how to create and configure a federated user repository for Netcool Configuration Manager.

1. Launch the WebSphere Administrative Console from `http://<ncmserver-hostname-ip>:<16316>/ibm/console` and login using the Netcool Configuration Manager superuser name and password specified during installation.

Note: The port number may be different for a non-standard installation.

2. Select **Security > Global security**.
3. Under the User account repository, select **Federated repositories** from the Available realm definitions field, and click **Configure**.
4. Under Repositories in the realm, select **Add repositories (LDAP, custom, etc)**.
5. Under General Properties, select **New Repository > Custom Repository**
6. Update the ObjectServer VMM properties as described here (or per your custom repository):

Repository identifier

NetcoolObjectServer

Repository adapter class name

com.ibm.tivoli.tip.vmm4ncos.ObjectServerAdapter

Custom Properties

Add the following four properties:

Note: Find the exact details from the repository viewable on the Network Manager Gui Administrative Console.

Table 5. Custom Properties	
Name (case-sensitive)	Value
username	ObjectServer administrator user name
password	ObjectServer encrypted administrator user password
port1	Object Server port number
host1	Object Server hostname/IP address

7. Click **Apply** and save your changes directly to the master configuration.
8. Under General properties of Repository Reference, update the Unique distinguished name to `o=netcool10bjectServerRepository`
9. Click **OK** and save your changes directly to the master configuration, then click **OK** again.
10. The local repository may not contain IDs that are also in Netcool Configuration Manager. To mitigate, perform one of the following steps:
 - Remove the local file repository from the federation of repositories.
 - Remove all the conflicting users from the local file repository.
11. If prompted, enter the WebSphere Administrator user password in the **Password** and **Confirm Password** fields, and click **OK**.
12. In Global security under the User account repository, select **Federated Repositories** from the Available realm definitions field, and click **Set as current**.
13. Click **Apply** and save your changes directly to the master configuration.
14. Log out of the Administrative Console.
15. Stop the Netcool Configuration Manager server using the `./itncm.sh stop` command. Then start the Netcool Configuration Manager server using the `./itncm.sh start` command.

Netcool Configuration Manager will now authenticate with the ObjectServer VMM.

The Netcool Configuration Manager Superuser has been reverted to the user created during the Dash profile Installation (which is smadmin by default)

Chapter 4. Upgrading an integrated system

The steps for upgrading a previously integrated system that includes Netcool Configuration Manager version 6.4.1, follow these instructions. For other upgrade paths, see the Netcool Configuration Manager 6.4.1 documentation.

Related concepts

[Installing and configuring the products](#)

The products and components that support the integration must be installed, and must be in an operational state before you configure the integration.

Related tasks

[Integrating the products](#)

Netcool Configuration Manager can be integrated with Network Manager.

Upgrading Netcool Configuration Manager to version 6.4.2.0

To upgrade from Netcool Configuration Manager version 6.4.1 to version 6.4.2.0, follow these instructions.

These instructions are for upgrading from a previous major version, for example V6.4.1.0, to V6.4.2.0. To apply fix packs, for example to move from V6.4.2.0 to V6.4.2.x, first upgrade to V6.4.2.0 and then apply the fix pack.

For instructions about installing fix packs, refer to the Release Notes PDF for the fix pack you want to install.

If you have customized any entries in properties files, you might see validation messages about changes to default values in properties files during installation. Change the values as suggested by the message and retry. Do not skip the validation checks, because this can cause undesired functionality in your upgraded installation. Make a list of any customized values prior to performing the upgrade. Once the upgrade has been completed, you must manually make those changes again in the files. Properties files that are commonly modified include the `/config/properties/rseries.properties` and `ITNCM.properties` files.

Tip: When installing on the same server as an existing, older version of Netcool Configuration Manager, ensure that before installation you back up the properties files from the home directory to a different location. For example:

```
cp $HOME/.rseries.properties $HOME/.rseries.properties_backup
```

If you are an Oracle database user and have commented out the `HADRErrorCodes=-4498` key/value, (which is only needed by DB2 database users), the upgrade process will remove the `'#'`, and it will no longer be commented out, which is the default for the `rseries.properties` file. Therefore if you require that this value be commented out, you need to do so again after upgrading.

Restriction: You must install Netcool Configuration Manager in a different location to any previous versions.

Note: After upgrading to Netcool Configuration Manager V6.4.2, you must install the latest drivers, and also reconfigure or reinstall ODBC:

Drivers

As a default, and as previously, drivers are installed to the following location: `<ncm install directory>/drivers`

See the Drivers installation documentation for more information.

ODBC

Reinstall or reconfigure ODBC to point to the new Netcool Configuration Manager installation.

1. Update to supported database if necessary.

Note: Supported database versions are DB2 10.1 and 10.5, and Oracle 11g and 12c.

2. Ensure you have the IBM Installation Manager Version 1.8.2 (or newer) present on your system.

- Install Installation Manager 1.8.2 using the group install script.
- Upgrade your current Installation Manager to 1.8.2:
 - a. In the Installation Manager UI, click **File > Preferences > Updates**.
 - b. Select **Search for Installation Manager updates**.
 - c. Click **Apply**, then **OK**.

The update to the latest Installation Manager will occur on next usage.

3. Set the IBM_JAVA_OPTIONS environment variable to include:

```
"-Dcom.ibm.tivoli.itncm.panels.utils.KeystoreManager=/installDir/
config/properties"
```

where /installDir/config/properties is the configuration directory from the previous installation. For example:

```
export IBM_JAVA_OPTIONS="-Dcom.ibm.tivoli.itncm.panels.utils.KeystoreManager=
/opt/IBM/tivoli/netcool/ncm/config/properties"
```

4. Perform a new installation of Netcool Configuration Manager.

Execute the IBM Installation Manager from \$HOME/IBM/InstallationManager_Group/eclipse

- a) During the installation, point to the database updated in step one.
- b) Use the DASH credentials that were originally used when Netcool Configuration Manager was installed. The default username was Intelliden.

Important: Do not accept the default username of smadmin. Your installation might continue, but fail later.

5. Upgrade the database schema to the latest version on the main presentation server only, by running the following command:

```
install_dir/bin/utils/database/upgrade/upgradeDBSchema.sh version
```

Where *version* is the older version of the product that you are upgrading from. For example:

```
/opt/IBM/tivoli/netcool/ncm/bin/utils/database/upgrade/upgradeDBSchema.sh 6.4.2.5
```

6. Copy the .intelliden.keystore and .intelliden.user files from the previous version to the current version of installDir/config/properties.

7. Copy the .itncm.cmkeystore and .itncm.cmusers files from the previous version to the current version of installDir/compliance/config/properties.

Clear the browser cache

After upgrading, clear the cache on any browsers that you use to work with Netcool Configuration Manager.

Help

To access the Help documentation (or 'User Assistance'), you must modify the system property ITNCM Help URL:

- 1. Select **Systems Manager** on the navigation tree.
- 2. Click **Tools > System Properties**.
- 3. Select **ITNCM Help URL**, and update the host and port number to the DASH installation.

Customizing the rseries.properties file

If you have customized your rseries.properties file, these will be overwritten during an upgrade. You must manually make those changes again.

Specifically, if you are an Oracle database user who requires that the HADRErrorCodes=-4498 key/value be commented out, you must again do so after upgrading.

Multiple presentation servers

If you have more than one presentation servers, you must edit the `/opt/IBM/tivoli/netcool/ncm/eventpollers.xml` file and change the 'pollerid' so that it matches all of the presentation servers.

For more details, see *Configuration of eventpollers.xml file* in the *IBM Tivoli Netcool Configuration Manager - Base Installation and Configuration Guide*.

OOBC and Drivers

Install the latest Drivers.

Reconfigure or reinstall OOBC.

Upgrading Netcool Configuration Manager Reporting

If you have a stand-alone installation of Tivoli Common Reporting as part of your Netcool Configuration Manager version 6.3.0.x or 6.4.x installation, you must upgrade both Netcool Configuration Manager and Tivoli Common Reporting to version 6.4.2.

Ensure you have upgraded Netcool Configuration Manager to version 6.4.2.

Export any additional custom Reports from your existing Reports Installation. See the Cognos documentation for details on how to do this.

Ensure you have JazzSM Reporting Services installed. For more information see http://www-01.ibm.com/support/knowledgecenter/SSEKCU_1.1.2.1/com.ibm.psc.doc/install/tcr_t_install.html

Note: If you are using JazzSM V1.1.3.11 or later versions, Tivoli Common Reporting is not supported. For more information, refer to <https://www.ibm.com/support/pages/node/6210342>.

You must upgrade Tivoli Common Reporting to version 6.4.2 regardless of whether it is installed on the existing Netcool Configuration Manager server or on a separate server.

You need the JazzSM Administrative username and password for Reporting Services.

You need the Netcool Configuration Manager database details.

Use IBM Installation Manager to Install the ITNCM-Reports.

- To do a silent install, create or record an Installation Manager response file. Use the `-record response_file` option.
- For example, create or record a skipInstall:

```
IBMIM.exe -record C:\response_files\install_1.xml -skipInstall  
C:\Temp\skipInstall
```

To install the ITNCM-Reports with the Installation Manager GUI

Note: A separate DASH profile is required for Tivoli Common Reporting, that is, the existing ones for the Netcool Configuration Manager or Network Manager GUI components cannot be used.

1. Change to the `/eclipse` subdirectory of the Installation Manager installation directory.
2. Use the following command to start the Installation Manager wizard: `./IBMIM`
3. In the main Installation Manager window, click **Install**.
4. Select Netcool Configuration Manager, and then select the Reports offering.
5. Fill in the Netcool Configuration Manager database details.
6. Fill in the JazzSM details ensuring the Installation directory is the correct Reporting Services Installation.

To install the ITNCM-Reports component with the Installation Manager console

7. Change to the `/eclipse/tools` subdirectory of the Installation Manager installation directory.
8. Use the following command to start the Installation Manager wizard: `./imcl -c`

9. From the Main Menu, select **Install**.
10. Select Netcool Configuration Manager, and then select the Reports offering.
11. Fill in the Netcool Configuration Manager database details.
12. Fill in the JazzSM details ensuring the Installation directory is the correct Reporting Services Installation.

To silently Install the ITNCM-Reports

13. Change to the /eclipse/tools subdirectory of the Installation Manager installation directory.
14. Use the following command to start the removal:

```
./imcl -input response_file -silent -log /tmp/install_log.xml  
-acceptLicense
```

Where response_file is the directory path to the response file that defines the install configuration.

Import any custom reports into Tivoli Common Reporting

15. On the Server copy the exported custom Reports zip file to <JazzSM Dir>/reporting/cognos/deployment/
16. Log into JazzSM as the administrator, and select **Common Reporting** from the left hand side.
17. Select **Administration** from the Launch drop down list on the right hand side.
18. Select **Configuration**, and then **Content Administration**.
19. Select “New Import” from the options available on the right hand side.
20. Here you can select the custom reports and follow on screen instructions to import them into your new ITNCM Reporting services.

Reporting Services manual configuration

21. Ensure all users in the Netcool Configuration Manager database which are to have access to the reports are duplicated on the Reporting Server to allow successful execution of reports.
22. Ensure all users have access to the public folder and have access to the HTML Items in Report capabilities.

Installation Manager installs the reports into Reporting Services.

Chapter 5. Monitoring the integrated solution

When Tivoli Netcool/OMNIBus, Network Manager, and Netcool Configuration Manager are installed in an integrated environment, you can monitor Netcool Configuration Manager events that are generated from device operation traps, policy traps, resource traps, and unit of work traps. You can also view device-based reports for these events.

Once you have integrated the systems, you can perform the following tests:

- Netcool Configuration Manager is working (both the configuration and compliance components).
- Device synchronization has provided Netcool Configuration Manager with devices in NCM, which should be in a managed state.
- You should have more than one UOW event in the Tivoli Netcool/OMNIBus Active Event List (AEL). You can create these events by importing, synchronizing, or creating a UOW in Netcool Configuration Manager.
- You should have more than one policy set up and run, at least one of which passes.
- You should confirm use of the IDT on more than one device in Netcool Configuration Manager.
- You should verify that the devices in Netcool Configuration Manager match those in Network Manager.

Monitoring devices and events in Network Manager

You can use the Network Manager topology visualization GUIs to visualize the devices that you seeded from Network Manager. Where relevant, event icons are shown against a device.

Use the following Network Manager topology visualization GUIs to view devices:

Network Views

Useful for browsing for a device based on, for example, vendor, type, or device collection. Network Views show devices that match a network view definition; for example, all Cisco devices, or all devices in a specified subnet.

Use the following multi-portlet GUIs to view events and devices simultaneously:

Network Health View

Shows the Network Views in the top portlet and the Active Event List in the lower portlet.

For more information about visualizing devices in Network Manager, see the *IBM Tivoli Network Manager IP Edition Topology Visualization Guide*.

To determine if an event shown against a device in a topology view is a configuration event, perform one of the following actions:

- If you are in the Network Health View, select the device. The related events are displayed in the lower Active Event List portlet.
- If you are in the Network Views, right-click the device and click **Show Events**. The Active Event List opens in a separate browser window containing the events on the selected device.

From the Active Event List, you can identify Netcool Configuration Manager events by sorting on the **Class** column. Netcool Configuration Manager events have class **ITNCM**.

Note: You can ignore the aforementioned class column information because Tivoli Netcool/OMNIBus version 7.4 onwards, Active Event List is replaced with Event viewer. The Event viewer allows you to view class type information from summary column with Alert group as TopClasses.

Using the context menu in any of the Network Manager GUIs, you can perform the following operations on Netcool Configuration Manager devices:

- You can launch the following Netcool Configuration Manager GUIs:

- To launch the core Netcool Configuration Manager GUI in a new browser window, right-click a device and then click **Configuration Management > ITNCM Launch > Launch ITNCM** from the pop-up menu.
- To launch the Netcool Configuration Manager core compliance GUI in a new browser window, right-click a device and then click **Configuration Management > ITNCM Launch > Launch ITNCM - Compliance** from the pop-up menu.
- To launch the Netcool Configuration Manager Activity Viewer as a TIP portlet, right-click a device and then click **Configuration Management > Device Activity Sequence** from the pop-up menu.
- To launch the Netcool Configuration Manager Apply (modeled) Command Set wizard as a TIP portlet, right-click a device and then click **Configuration Management > ITNCM Wizard > Apply Modelled Command Set** from the pop-up menu.
- To launch the Netcool Configuration Manager Apply Native Command Set wizard as a TIP portlet, right-click a device and then click **Configuration Management > ITNCM Wizard > Apply Native Command Set** from the pop-up menu.
- To launch the Netcool Configuration Manager Policy Validation wizard as a TIP portlet, right-click a device and then click **Configuration Management > ITNCM Wizard > Apply Policy** from the pop-up menu.
- To launch the Netcool Configuration Manager Synchronize Configuration wizard as a TIP portlet, right-click a device and then click **Configuration Management > ITNCM Wizard > Synchronize (Device to ITNCM)** from the pop-up menu.

After launching the GUIs, you can navigate the interface and access the relevant windows that enable you to view further details about the selected devices. For example, from the Netcool Configuration Manager Activity Viewer, you can launch the Submit Configuration wizard or the IBM Tivoli Netcool Configuration Manager Device Terminal (IDT).

- You can access some of the reports on the selected device.
- You can perform the standard Network Manager actions that are available from the context menu.

For more information on the actions you can perform in Network Manager, see the *IBM Tivoli Network Manager IP Edition Topology Visualization Guide*.

Related concepts

Netcool Configuration Manager events

Use this information to understand the different types of configuration events generated by Netcool Configuration Manager.

Monitoring Netcool Configuration Manager events in the Active Event List

You can monitor Netcool Configuration Manager events in the Active Event List to enable you to identify when configuration changes are made to devices in the network, and to help you ensure that the network configuration complies with your corporate regulations.

You can monitor Netcool Configuration Manager events from the Active Event List if your system is configured to support this feature.

To identify Netcool Configuration Manager events in the Active Event List, you can perform either of the following actions:

- Apply a filter to display Netcool Configuration Manager events only. This filter must have been created by your system administrator, in which case you can select it from the **Filters** list.
- Sort on the Class column, if this column is available in your current view. By default, the Class entry is **ITNCM**, although this value can be changed by your system administrator.

Note: You can ignore the aforementioned class column information because Tivoli Netcool/OMNIBus version 7.4 onwards, Active Event List is replaced with Event viewer. The Event viewer allows you to view class type information from summary column with Alert group as TopClasses.

For information about applying filters, sorting columns in the Active Event List, or adding columns to a view, see the *IBM Tivoli Netcool/OMNIBus Web GUI Administration and User's Guide* in the Tivoli Netcool/OMNIBus Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_OMNIBus.doc_7.3.1/omnibus/wip/welcome.htm.

From the Active Event List, you can perform the following operations on Netcool Configuration Manager events:

- You can launch the Netcool Configuration Manager Activity Viewer as a TIP portlet; right-click an event and then click **Configuration Management > Device Activity Sequence** from the pop-up menu.
- You can run a report on the device that is associated with a selected event.
- You can perform the standard actions that are available from the **Alerts** menu. For example, you can right-click an event and then click **Information** (or double-click the event) to view its complete set of details.

For general information about monitoring events in the Active Event List, see the *IBM Tivoli Netcool/OMNIBus Web GUI Administration and User's Guide*.

Related concepts

Netcool Configuration Manager events

Use this information to understand the different types of configuration events generated by Netcool Configuration Manager.

Related tasks

Running reports from the Active Event List

You can run Netcool Configuration Manager reports from the Active Event List if your system is configured to support this feature.

Running Netcool Configuration Manager reports

You can run Netcool Configuration Manager reports on network devices to view summary information relating to configuration and compliance. The reports provide information that can be used for fault correlation purposes in Tivoli Netcool/OMNIBus and Network Manager.

You can run the reports from any Network Manager topology visualization GUI, from the Active Event List, and from the Tivoli Common Reporting GUI. When you run a report from Network Manager or from the Active Event List, the report is formatted using the current data. When you run a report from the Tivoli Common Reporting GUI, you can change the default report parameters and can choose the format in which the report is rendered.

For some of the reports, you can click embedded links to drill down to further reports.

To run Netcool Configuration Manager reports, you must have the relevant access permissions, which are controlled by your administrator.

Running reports from Network Manager

You can run Netcool Configuration Manager reports from Network Manager if your system is configured to support this feature.

To run reports from Network Manager:

1. In the Network Views, right-click a device, and then click **Configuration Management > ITNCM Reports**.
2. Click one of the report names in the submenu.

The report is formatted using the current data and is displayed in HTML format in a browser window.

Running reports from the Active Event List

You can run Netcool Configuration Manager reports from the Active Event List if your system is configured to support this feature.

To identify Netcool Configuration Manager events in the Active Event List, you can perform either of the following actions:

- Apply a filter to display Netcool Configuration Manager events only. This filter must have been created by your system administrator, in which case you can select it from the **Filters** list.
- Sort on the Class column, if this column is available in your current view. By default, the Class entry is **ITNCM**, although this value can be changed by your system administrator.

Note: You can ignore the aforementioned class column information because Tivoli Netcool/OMNIBus version 7.4 onwards, Active Event List is replaced with Event viewer. The Event viewer allows you to view class type information from summary column with Alert group as TopClasses.

For information about applying filters, sorting columns in the Active Event List, or adding columns to a view, see the *IBM Tivoli Netcool/OMNIBus Web GUI Administration and User's Guide* in the Tivoli Netcool/OMNIBus Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_OMNIBus.doc_7.3.1/omnibus/wip/welcome.htm.

To run reports from the Active Event List:

1. Right-click a Netcool Configuration Manager event and then click **Configuration Management > ITNCM Reports**.
2. Click one of the report names in the submenu.

The report is formatted using the current data and is displayed in HTML format in a new browser window.

Running reports from Tivoli Common Reporting

You can run reports from the Tivoli Common Reporting GUI if your system is configured to support this feature. Run Netcool Configuration Manager reports from the Tivoli Common Reporting GUI if you want to use the standard reporting features that are not available from the Network Manager topology visualization GUI or the Active Event List.

To run reports from the Tivoli Common Reporting GUI:

1. Log on to the DASH console if not already logged on.
2. From the navigation pane, click **Reporting > Common Reporting > ITNCM Reporting**.
3. From the **Navigation** tab of the **Tivoli Common Reporting** pane, expand the report navigation tree by clicking **Tivoli Reports > ITNCM Reports**.
4. Click a report name in the navigation tree, and then from the **Reports** pane, perform one of the following actions:
 - To view the report in the default HTML format in a new browser window or tab, click the **Reports** icon  that is adjacent to the report title.
 - To choose whether to view the report in HTML, PDF, Microsoft Excel, or Adobe Postscript, right-click the report title, click **View As** in the pop-up menu, and choose your required display format.
5. Complete the **On-Demand Report Parameters** window as follows:
 - a) Specify the report parameters that you want to use. An entity name is always required in the **EntityName** field; for example, an IP address. Some of the reports also require a reporting period (or date range) to be set.
 - b) Click **Run** to generate the report.

The report is formatted using the specified parameters and is displayed in your chosen report viewer.

For more information about running reports from Tivoli Common Reporting, see the Tivoli Common Reporting documentation in the IBM Tivoli Systems Management Information Center at <http://www-01.ibm.com/support/knowledgecenter/SS3HLM/welcome>.

Netcool Configuration Manager events

Use this information to understand the different types of configuration events generated by Netcool Configuration Manager.

Device operation events

Device operation events indicate the success or failure of configuration activities against a device.

An individual device change, for example, the loading of a configuration onto a device, is known in Netcool Configuration Manager as a task. The completion of a task on a device causes an event to be generated.

In addition to indicating that a task has been completed on a device, device operation events also indicate whether the device configuration was changed as a result of the task.

Device operation events can be identified using the **Agent** field, which has the value `Task trap` for device operation events. Device operation events are categorized by event ID, as described in the following table. The **EventId** field does not display by default in the **Active Event List**. Your system administrator can add the **EventId** field to the columns displayed in the **Active Event List**.

For information about applying filters, sorting columns in the Active Event List, or adding columns to a view, see the *IBM Tivoli Netcool/OMNIBus Web GUI Administration and User's Guide* in the Tivoli Netcool/OMNIBus Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_OMNIBus.doc_7.3.1/omnibus/wip/welcome.htm.

Table 6. Device operation events		
Agent	EventId	Description
Task trap	SNMPTRAP-ibm-ITNCM-MIB-itncmTaskAuthenticationFailureTrap	There has been an authentication failure against a specified device as part of a specified unit of work (UOW).
	SNMPTRAP-ibm-ITNCM-MIB-itncmTaskDeviceCommsFailureTrap	There has been a communications failure against a specified device as part of a specified UOW task. The reason for the failure is given in the event.
	SNMPTRAP-ibm-ITNCM-MIB-itncmTaskDeviceModelChangeTrap	A device revision has been detected for a specified device as part of a specified UOW task. The reason is given in the event.
	SNMPTRAP-ibm-ITNCM-MIB-itncmTaskFailureTrap	A rollback operation has failed against a specified device as part of a specified UOW task.
	SNMPTRAP-ibm-ITNCM-MIB-itncmTaskSuccessTrap	A task has been successful against a specified device as part of a specified UOW task operation.
	SNMPTRAP-ibm-ITNCM-MIB-itncmAutodiscoveryTaskFailureTrap	An unknown trap has been received.

Device operation event fields

Use this information to understand the fields in device operation events.

The following fields specific to Netcool Configuration Manager are presented within device operation events.

Table 7. Fields in device operation events	
Column name	Description
Node	Name of the device. This value corresponds to the device name provided in the device seed file from Network Manager.
Agent	Contains the text Task trap, identifying this event as a IBM Tivoli Netcool Configuration Manager device operation event.
AlertGroup	Contains the text Task trap, identifying this event as a IBM Tivoli Netcool Configuration Manager device operation event.
AlertKey	Contains a combination of the following data: - Name of the device. This value corresponds to the device name provided in the device seed file from Network Manager. - Unique ID for the device. This value corresponds to the entity ID for the device provided when Netcool Configuration Manager was seeded with devices from Network Manager. This value corresponds to the entity ID of the device in the Network Manager NCIM topology database.
LocalNodeAlias	Name of the device. This value corresponds to the device name provided in the device seed file from Network Manager.
NmosEntityId	Unique ID for the device. This value corresponds to the entity ID for the device provided when Netcool Configuration Manager was seeded with devices from Network Manager. This value corresponds to the entity ID of the device in the Network Manager NCIM topology database.
Summary	The textual summary of the cause of the alert.
Identifier	Contains a combination of data in the event and enables deduplication of events based on UOW on a device.

For information about the full set of event fields, see the *IBM Tivoli Netcool/OMNIBus Administration Guide* in the Tivoli Netcool/OMNIBus Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_OMNIBus.doc_7.3.1/omnibus/wip/welcome.htm.

Policy events

Policy events indicate that a configuration policy has failed against a device, or that a previous configuration policy failure has now been cleared.

Netcool Configuration Manager provides facilities for policy checks to be carried out against a device or set of devices. The execution mechanism for applying a compliance policy or set of policies against a device or set of devices is known as a process.

Policy events are generated against the device that registered the policy failure.

Note: If a policy against a device fails, then subsequent passes of the same policy against the same device removes the failure event.

Policy events can be identified using the **Agent** field, which has the value `Policy trap` for policy events. Policy events are categorized by event ID, as described in the following table. Use this information to determine whether further action is necessary. The **EventId** field does not display by default in the **Active Event List**. Your system administrator can add the **EventId** field to the columns displayed in the **Active Event List**.

For information about applying filters, sorting columns in the Active Event List, or adding columns to a view, see the *IBM Tivoli Netcool/OMNIBus Web GUI Administration and User's Guide* in the Tivoli Netcool/OMNIBus Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_OMNIBus.doc_7.3.1/omnibus/wip/welcome.htm.

Table 8. Policy events		
Agent	EventId	Summary
Policy trap	SNMPTRAP-ibm-ITNCM-MIB-itncmPolicyCompliantTrap	The device specified in the event is now compliant with the vendor policy specified in the event.
	SNMPTRAP-ibm-ITNCM-MIB-itncmPolicyViolationTrap	The device specified in the event has violated the vendor policy specified in the event.
	SNMPTRAP-ibm-ITNCM-MIB-itncmPolicyExemptTrap	The device specified in the event is exempt from vendor policy specified in the event.
	SNMPTRAP-ibm-ITNCM-MIB-itncmPolicyNotAssessedTrap	The device specified in the event has not been assessed for compliance with the policy specified in the event.

Policy event fields

Use this information to understand the fields in policy events.

The following Netcool Configuration Manager-specific fields are presented within policy events.

Table 9. Fields in policy events	
Column name	Description
Node	Name of the device. This value corresponds to the device name provided in the device seed file from Network Manager.
Agent	Contains the text <code>Policy trap</code> , identifying this event as a IBM Tivoli Netcool Configuration Manager policy event.
AlertGroup	Contains the text <code>Policy trap</code> , identifying this event as a IBM Tivoli Netcool Configuration Manager policy event.

Table 9. Fields in policy events (continued)	
Column name	Description
AlertKey	Contains a combination of the following data: • Name of the device. This value corresponds to the device name provided in the device seed file from Network Manager. • Unique ID for the device. This value corresponds to the entity ID for the device provided when Netcool Configuration Manager was seeded with devices from Network Manager. This value corresponds to the entity ID of the device in the Network Manager NCIM topology database. • Name of the policy applied. • Key of the policy applied.
LocalNodeAlias	Unique ID for the device. This value corresponds to the entity ID for the device provided when Netcool Configuration Manager was seeded with devices from Network Manager. This value corresponds to the entity ID of the device in the Network Manager NCIM topology database.
NmosEntityId	Unique ID for the device. This value corresponds to the entity ID for the device provided when Netcool Configuration Manager was seeded with devices from Network Manager. This value corresponds to the entity ID of the device in the Network Manager NCIM topology database.
Summary	The textual summary of the cause of the alert.
Identifier	Contains a combination of data in the event and enables deduplication of events based on policy instance, version, and device.

For information about the full set of event fields, see the *IBM Tivoli Netcool/OMNIBus Administration Guide* in the Tivoli Netcool/OMNIBus Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_OMNIBus.doc_7.3.1/omnibus/wip/welcome.htm.

Resource events

Resource events indicate that a Netcool Configuration Manager system resource has been added, modified, or deleted.

A resource event is generated when any of the following Netcool Configuration Manager system resources is added, modified, renamed, or deleted:

- Devices
- Realms
- Native command sets
- Modelled command sets

Resource events are generated against the Netcool Configuration Manager server.

Resource events can be identified using the **Agent** field, which has the value `Device` trap for resource events. Resource events are categorized by event ID, as described in the following table. Use this information to determine whether further action is necessary. The **EventId** field does not display by default in the **Active Event List**. Your system administrator can add the **EventId** field to the columns displayed in the **Active Event List**.

For information about applying filters, sorting columns in the Active Event List, or adding columns to a view, see the *IBM Tivoli Netcool/OMNIBus Web GUI Administration and User's Guide* in the

Table 10. Resource events		
Agent	EventId	Description
Device trap	SNMPTRAP-ibm-ITNCM-MIB-itncmResourceDeviceActivityTrap	An action such as add, modify, delete, and so on, has been performed on a specified resource.
	SNMPTRAP-ibm-ITNCM-MIB-itncmResourceRealmActivityTrap	An action such as add, modify, delete, and so on, has been performed on a specified realm.
	SNMPTRAP-ibm-ITNCM-MIB-itncmResourceCommandActivityTrap	An action such as add, modify, delete, and so on, has been performed on a specified resource.

Resource event fields

Use this information to understand the fields in resource events.

The following fields specific to Netcool Configuration Manager are presented within resource events.

Table 11. Fields in resource events	
Column name	Description
Agent	Contains the text ITNCM Device trap, identifying this event as a IBM Tivoli Netcool Configuration Manager resource event.
AlertGroup	Contains the text Resource event, identifying this event as a IBM Tivoli Netcool Configuration Manager resource event.
AlertKey	Contains a combination of the following data: • Display name of the resource. • Unique key for the resource. • Type of the resources.
LocalNodeAlias	Contains the Netcool Configuration Manager instance name.
Summary	The textual summary of the cause of the alert.
Identifier	Contains a combination of data in the event and enables deduplication of events based on resource and Netcool Configuration Manager instance name.

For information about the full set of event fields, see the *IBM Tivoli Netcool/OMNIBus Administration Guide* in the Tivoli Netcool/OMNIBus Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_OMNIBus.doc_7.3.1/omnibus/wip/welcome.htm.

Unit of work events

Unit of work (UOW) events indicate that a UOW has completed a certain stage within the UOW lifecycle.

A UOW groups together a configuration task against a set of devices. For example, a single UOW might involve the upgrade of the IOS revision on 30 Cisco devices. At the completion of each stage within a UOW, an event is generated. UOW stages are as follows:

- Ready for execution
- Executing
- Finished

UOW events are generated against the Netcool Configuration Manager server.

UOW events can be identified using the **Agent** field, which has the value UOW trap for UOW events. UOW events are categorized by event ID, as described in the following table. Use this information to determine whether further action is necessary. The **EventId** field does not display by default in the **Active Event List**. Your system administrator can add the **EventId** field to the columns displayed in the **Active Event List**.

For information about applying filters, sorting columns in the Active Event List, or adding columns to a view, see the *IBM Tivoli Netcool/OMNIBus Web GUI Administration and User's Guide* in the Tivoli Netcool/OMNIBus Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_OMNIBus.doc_7.3.1/omnibus/wip/welcome.htm.

Table 12. Device operation events		
Agent	EventId	Description
UOW trap	SNMPTRAP-ibm-ITNCM-MIB-itncmUOWOSUpgrade	An OS upgrade UOW has been submitted and is currently in one of the following states: • Ready for execution • Executing • Finished • Cancelled • Expired • Unknown The event includes the display name of the UOW that encapsulates the device change.
	SNMPTRAP-ibm-ITNCM-MIB-itncmUOWConfigurationActivity SNMPTRAP-ibm-ITNCM-MIB-itncmUOWConfigurationRetrieval SNMPTRAP-ibm-ITNCM-MIB-itncmUOWDeviceAccessTrap SNMPTRAP-ibm-ITNCM-MIB-itncmUOWDriverUpdateTrap	A UOW activity such as import, configuration synchronization, or command set application has been submitted and is currently in one of the following states: • Ready for execution • Executing • Finished • Cancelled • Expired • Unknown The event includes the display name of the UOW that encapsulates the device change.

Unit of work event fields

Use this information to understand the fields in unit of work (UOW) events.

The following fields specific to Netcool Configuration Manager are presented within UOW events.

Table 13. Fields in UOW events	
Column name	Description
Agent	Contains the text UOW trap, identifying this event as a IBM Tivoli Netcool Configuration Manager UOW event.
AlertGroup	Contains the text UOW trap, identifying this event as a IBM Tivoli Netcool Configuration Manager UOW event.

Table 13. Fields in UOW events (continued)

Column name	Description
AlertKey	Contains a combination of the following data: • Unique key for the UOW. • Name of the UOW that encapsulates the device change. • Type of UOW that is being executed against the device; for example, import, configuration synchronization, or command set application.
LocalNodeAlias	Contains the Netcool Configuration Manager instance name.
Summary	The textual summary of the cause of the alert.
Identifier	Contains a combination of data in the event and enables deduplication of events based on UOW and Netcool Configuration Manager instance name.

For information about the full set of event fields, see the *IBM Tivoli Netcool/OMNIBus Administration Guide* in the Tivoli Netcool/OMNIBus Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_OMNIBus.doc_7.3.1/omnibus/wip/welcome.htm.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
958/NH04
IBM Centre, St Leonards
601 Pacific Hwy
St Leonards, NSW, 2069

Australia

IBM Corporation
896471/H128B
76 Upper Ground
London SE1 9PZ
United Kingdom

IBM Corporation
JBF1/SOM1
294 Route 100
Somers, NY, 10589-0100
United States of America

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© your company name (year). Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. (year). All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, ibm.com®, Netcool, Passport Advantage, Tivoli, the Tivoli logo, and WebSphere are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, Portable Document Format (PDF), PostScript, and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

"Powered by Cryptzone MindTerm" is copyright 1997 – 2017 Cryptzone North America, Inc. All rights reserved.

Other company, product, or service names may be trademarks or service marks of others.

Index

A

- accessibility [ix](#)
- Active Event List
 - Activity Viewer access [34](#)
 - configuring Alerts menu [34](#)
 - monitoring events [52](#)
 - running reports [54](#)

B

- benefits of integration [1](#)

C

- configure
 - single sign-on [39](#)
- configuring
 - Active Event List Alerts menu [34](#)
 - Activity Viewer [34](#)
 - integration [21](#)
 - Netcool Configuration Manager [18](#)
 - Netcool/OMNIbus Knowledge Library [16](#)
 - Network Manager [16](#)
 - SNMP Probe [16](#)
 - Tivoli Netcool/OMNIbus [16](#)
- conventions, typeface [ix](#)
- customized rules
 - installing [29](#)

D

- DASH
 - install [24](#)
- DASH attributes
 - for single sign-on [42](#)
- DASH LTPA keystore, exporting
 - for single sign-on [41](#)
- DASH LTPA keystore, importing into Netcool Configuration Manager
 - for single sign-on [43](#)
- device operation event fields [56](#)
- device operation events [55](#)
- device synchronization
 - setting up [32](#)
- devices
 - monitoring in Network Manager [51](#)

E

- education
 - see Tivoli technical training [ix](#)
- enabling
 - single sign-on [43](#)
- environment variables, notation [ix](#)

- event fields
 - device operation events [56](#)
 - policy events [57](#)
 - resource events [59](#)
 - unit of work (UOW) events [61](#)
- event types [55](#)
- events
 - device operation [55](#)
 - monitoring in Active Event List [52](#)
 - monitoring in Network Manager [51](#)
 - policy [56](#)
 - resource [58](#)
 - unit of work [60](#)
 - UOW [60](#)

I

- install
 - DASH [24](#)
- installing
 - customized rules [29](#)
 - Netcool Configuration Manager [15](#)
 - Network Manager [15](#)
 - Tivoli Netcool/OMNIbus [15](#)
- integrating
 - Network Manager jar files [31](#)
- integrating with Network Manager [31](#)
- integration
 - benefits [1](#)
 - conceptual diagrams [2](#)
 - configuring [21](#)
 - data flow [2](#)
 - integration process [2](#)
 - prerequisite products [12](#)
 - prerequisite tasks [14](#)
 - process overview [1](#)
 - upgrading [47](#)
 - user role requirements [21](#)

J

- jars [31](#)

M

- manuals [v](#)
- monitoring
 - devices and events in Network Manager [51](#)
 - events in Active Event List [52](#)

O

- online publications [v](#)
- ordering publications [v](#)

P

- policy event fields [57](#)
- policy events [56](#)
- prerequisite products [12](#)
- prerequisite tasks
 - integration [14](#)
- publications [v](#)

R

- reports
 - exporting
 - distributed architecture [36](#)
 - single server integrated architecture [14](#)
 - importing
 - distributed architecture [38](#)
 - single server integrated architecture [38](#)
 - migrating [35](#)
 - running [53](#)
 - running from Active Event List [54](#)
 - running from Network Manager [53](#)
 - running from Tivoli Common Reporting [54](#)
- resource event fields [59](#)
- resource events [58](#)
- running
 - reports [53](#)
 - reports from Active Event List [54](#)
 - reports from Network Manager [53](#)
 - reports from Tivoli Common Reporting [54](#)

S

- single sign-on
 - configure [39](#)
 - configuring WebSphere attributes [44](#)
 - create user groups [40](#)
 - create users [40](#)
 - creating and configuring federated user repository [44](#)
 - DASH attributes [42](#)
 - enabling [43](#)
 - exporting the DASH LTPA keystore [41](#)
 - importing the DASH LTPA keystore for Netcool Configuration Manager [43](#)
- support information [ix](#)

T

- Tivoli Common Reporting
 - running reports [54](#)
- Tivoli software information center [v](#)
- Tivoli technical training [ix](#)
- training, Tivoli technical [ix](#)
- typeface conventions [ix](#)
- types of event [55](#)

U

- unit of work (UOW) event fields [61](#)
- unit of work events [60](#)
- UOW events [60](#)
- upgrading
 - integration [47](#)

- user groups, create for single sign-on [40](#)
- user repository, creating for single sign-on [44](#)
- user roles
 - Other [21](#)
 - TCR [21](#)
 - TIP [21](#)
- users, create for single sign-on [40](#)

V

- variables, notation for [ix](#)

W

- WebSphere attributes for single sign-on [44](#)



Part Number:

Printed in the Republic of Ireland

2023-4219-01



(1P) P/N: