# Netcool Configuration Manager
# 6.4.2

## *Installation and Configuration Guide*

2023-4219-01

**Note**

Before using this information and the product it supports, read the information in “Notices” on page 121.

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.

# Contents

# About this publication

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

The *IBM Tivoli Netcool Configuration Manager Installation and Configuration Guide* describes how to install Netcool Configuration Manager. The guide also describes post-installation configuration tasks. This publication is for administrators who need to install and set up Netcool Configuration Manager.

## Intended audience

This publication is intended for administrators who need to install Netcool Configuration Manager and perform post-installation configuration. Readers must be familiar with network management and operating system configuration tasks.

## What this publication contains

This publication contains the following sections:



## 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.ibmlink.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.ibmlink.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. Planning

Use this information to plan a new installation of Netcool Configuration Manager. For upgrading and migrating from existing installations, see the Migration and Upgrading sections instead.

**Related information**

Installing auto-discovery

Use this information to install the Netcool Configuration Manager auto-discovery driver. You must install the most current drivers before installing auto-discovery.

## Architecture

Netcool Configuration Manager can be deployed as either a stand-alone product on one or more servers, or with IBM Tivoli Network Manager IP Edition and IBM Tivoli Netcool/OMNIbus as part of an integrated solution.

All components of Netcool Configuration Manager are installed on each deployed server. However, the compliance server component is switched on or off at install time. You can also switch worker server modes later by running a script.

**Note:** A database must be present before Netcool Configuration Manager is installed.

### Stand-alone product

You can install Netcool Configuration Manager on a single server or distributed on a number of servers. Optionally, you can install Tivoli Common Reporting as part of the same installation procedure. TCR is installed with, and accessed through, the DASH.

DASH is required by Netcool Configuration Manager - Base for both integrated and stand-alone installations, whether installed with or without Tivoli Common Reporting. Various DASH services such as the reporting service are required by WebSphere to run a Netcool Configuration Manager - Base presentation server. DASH is not required for a worker-only installation.

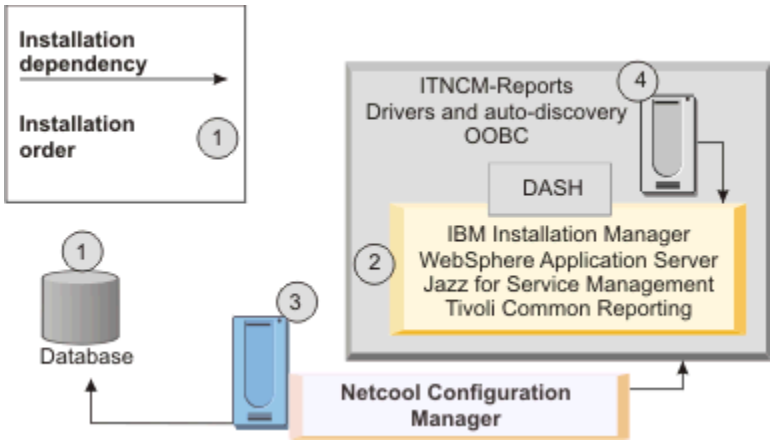


*Figure 1. Stand-alone installation with component dependencies and installation sequence*

1. Install the database first.
2. Install Netcool Configuration Manager prerequisites: IBM Installation Manager, WebSphere application server, Jazz for Service Management, and Tivoli Common Reporting
3. Install Netcool Configuration Manager with the Integration option unselected.

**4**

Install ITNCM-Reports into Tivoli Common Reporting, the Netcool Configuration Manager drivers, the auto-discovery driver, and the OOBC software.

## Integrated product

You can install Netcool Configuration Manager together with IBM Tivoli Network Manager IP Edition and IBM Tivoli Netcool/OMNIbus, either on a single server or on a number of servers.

In such an integrated scenario, you install Network Manager and Tivoli Netcool/OMNIbus before installing Netcool Configuration Manager without Tivoli Common Reporting.

After this, you install ITNCM_Reports and the Activity Viewer into the Network Manager DASH environment.

**Note:** You can use an existing Network Manager and Tivoli Netcool/OMNIbus installation to create such an integrated solution.

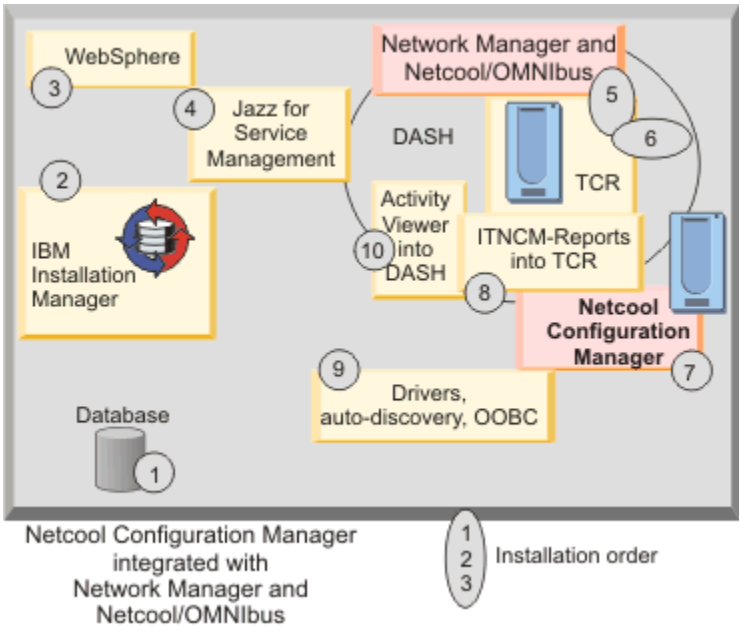


*Figure 2. Integrated installation and installation sequence*

**1**

Install the database first.

**2, 3, 4**

Install Netcool Configuration Manager prerequisites:

- IBM Installation Manager
- WebSphere application server
- Jazz for Service Management
- **Note:** As this is an integrated deployment that will utilize Tivoli Common Reporting in the Network Manager DASH environment, you do not install Tivoli Common Reporting at this time.

**5, 6**

Install Network Manager and Tivoli Netcool/OMNIbus.

This will also install Tivoli Common Reporting within DASH.

**7**

Install Netcool Configuration Manager, with the 'Integrated' option selected.

**8**

Install ITNCM-Reports into Tivoli Common Reporting in the Network Manager DASH environment.

9. Install the Netcool Configuration Manager drivers, the auto-discovery driver, and the OOBC software.

10. Install the Netcool Configuration Manager Activity Viewer into the Network Manager DASH environment.

## Running the IBM Prerequisite Scanner tool

Before you install Netcool Configuration Manager, run the Prerequisite Scanner tool to ensure that you meet all the necessary hardware and software requirements. Only run this tool if it supports the latest version of Netcool Configuration Manager.

Prerequisite Scanner is a tool that checks the configuration of your chosen environment and detects missing prerequisites.

Download the latest version of Prerequisite Scanner for UNIX from IBM Fix Central (http://www.ibm.com/support/fixcentral), extract the package, run the NCM.sh wizard script, and select deployment configuration for the server.

The NCM.sh script optionally lets you define a single parameter, which specifies the release of Netcool Configuration Manager that is being installed in the format of an 8-digit string `vvrrmmff`. In this string, `vv` represents the version, `rr` the release, `mm` the modification and `ff` the fixpack. For Netcool Configuration Manager, each value is padded with a leading zero, so for example Netcool Configuration Manager Version 6.4.1 is `06040100`. If no parameter is supplied, NCM.sh will check the server against the latest version supported by the tool.

**Remember:** If the latest version of Netcool Configuration Manager is not supported yet, use the planning information in the *IBM Tivoli Netcool Configuration Manager - Base Installation and Configuration Guide* to determine your prerequisites.

**Note:** The Prerequisite Scanner tool checks that the hostname of Netcool Configuration Manager servers is in DNS, but this is not mandatory for Netcool Configuration Manager.

**Note:** The Prerequisite Scanner tool (and Netcool Configuration Manager) will not work if `/tmp` is mounted with noexec.

As an alternative to using the wizard, you can use the prerequisite scanner tool directly by specifying Netcool Configuration Manager as the product to be tested. However, you must set and export the environment variables to set the various Netcool Configuration Manager installation options before you run the tool.

```
#./NCM.sh

        Prerequisite scanner for ITNCM 06040100 release.

        Please select your desired deployment for this server:-

        1. Presentation Server + Worker Server : Compliance Core=Enabled :
Reporting = Not to be installed
        2. Presentation Server + Worker Server : Compliance Core=Enabled :
Reporting = To be installed
        3. Presentation Server + Worker Server : Compliance Core=Disabled :
Reporting = Not to be installed
        4. Presentation Server + Worker Server : Compliance Core=Disabled :
Reporting = To be installed

        5. Worker Server : Base=Enabled  : Compliance Eval Engine=Enabled
        6. Worker Server : Base=Enabled  : Compliance Eval Engine=Disabled
        7. Worker Server : Base=Disabled : Compliance Eval Engine=Enabled

        0. Quit

        Select option ->
```

Check the output results of the scanner and resolve any failed checks.

# Hardware requirements

Hardware requirements vary according to the size and composition of your network and the features of Netcool Configuration Manager that you want to use. They are also influenced by your database and operating system configuration.

Ensure that your servers meet at least the minimum hardware requirements before you proceed to an installation.

*Table 1. Netcool Configuration Manager server hardware requirements*

| **Item** | **Requirement** |
|---|---|
| CPU | 2 GHz |
| Memory (64 bit operating systems) | Netcool Configuration Manager components require the following amount of memory:<br>• Presentation JVM: 2GB<br>• Compliance core JVM: 2GB<br>• Reporting JVM: 2GB<br>• Worker Base JVM: 3GB<br>• Worker Compliance engine JVM: 2GB<br>The following examples illustrate the memory requirements for a number of typical deployments:<br>• Presentation server + Compliance core + Worker Base + Reporting: 9GB<br>• Presentation server + Compliance core + Worker Base: 7GB<br>• Presentation server + Compliance core + Reporting: 6GB<br>• Presentation server + Worker Base + Reporting: 7GB<br>• Presentation server + Compliance core: 5GB<br>• Worker Base: 2GB<br>• Compliance evaluation engine only: 2GB<br>• Worker Base + Compliance evaluation engine: 4GB<br>**Note:** These requirements are for Netcool Configuration Manager components only, that is, they do not include the database or operating system memory requirements. Consult the database and OS documentation for more information specific to your OS and database memory needs. |
| Disk space | 10 GB of space is recommended as a base for initial installation. Requirements may change based on individual company needs.<br>The Installer by default uses 5 GB of space in `/tmp`. If `/tmp` isn't large enough, IATEMPDIR can be used to specify another directory instead. The IATEMPDIR environment variable specifies an alternative directory into which the Netcool Configuration Manager installer may extract files before actual installation. However, a small amount of data (about 1MB) will be written to `/tmp` even if IATEMPDIR is being used.<br>**Important: When installing Tivoli Common Reporting:** The IATEMPDIR directory is required when installing Tivoli Common Reporting and you must specify a minimum of 10 GB.<br>**Important: When using the Prerequisite Scanner tool:** The Prerequisite Scanner tool (and Netcool Configuration Manager) will not work if `/tmp` is mounted with noexec. |

| Table 1. Netcool Configuration Manager server hardware requirements (continued) | |
|---|---|
| **Item** | **Requirement** |
| Network interface card | Gigabit Ethernet |
| Database disk space | 500 GB |
| Swap/paging space | Your system should have swap/paging space equivalent to half of the RAM allocated. For example, for 10 GB RAM, you should have 5 GB of paging space. Refer to your database documentation for more detailed database swap/paging space guidelines. |

## Software requirements

Software requirements vary according to the operating system and features of Netcool Configuration Manager that you want to use.

**Note:** If you use Netcool Configuration Manager as part of a solution, you must also check the compatibility of the versions of all component products in the solution documentation. For example, if you use Netcool Operations Insight, check the instructions for *downloading components* for your version of Netcool Operations Insight at https://www.ibm.com/support/knowledgecenter/en/SSTPTP.

| Table 2. Netcool Configuration Manager supported operating systems | |
|---|---|
| **Item** | **Requirement** |
| AIX | 6.1, 7.1, 7.2 and 7.3 iSeries and pSeries<br>**Important:** The GNU version of TAR must be installed before Netcool Configuration Manager, or else the installation will fail. |
| Linux | SuSE Linux Enterprise Server (SLES) 11.0 (x86-64) SP2 and SP3<br>SuSE Linux Enterprise Server (SLES) 12.0 (x86-64)<br>Red Hat Enterprise Linux 6, 7.9, 8.6, 8.7, 8.8, 9.1 (x86-64) and 9.2 (x86-64) |
| Linux on System z | SuSE Linux Enterprise Server (SLES) 12 SP5 (s390x)<br>**Restriction:**<br>Netcool Configuration Manager Version 6.4.2 fix pack 3 and fix pack 4 can only be deployed on Linux on System z as a stand-alone solution deployed on a worker server. Deployments that include Tivoli Common Reporting or the use of the DASH portlets are **not** supported on zLinux.<br>Fix Pack 4 Netcool Configuration Manager Version 6.4.2 fix pack 4 allows the use of Cognos Analytics to view ITNCM Reports on zLinux platforms. Such installations are, however, limited to single-server, stand-alone deployments, with no integration or use of the DASH portlets.<br>See the Cognos Analytics on zLinux table entry for more information, including a list of prerequisites and limitations. |

| Table 3. Netcool Configuration Manager database requirements | |
|---|---|
| **Database** | **Version supported** |
| **Note:** For all database types and versions, use the latest fix pack, unless otherwise specified. | |

| *Table 3. Netcool Configuration Manager database requirements (continued)* | |
|---|---|
| **Database** | **Version supported** |
| DB2 | 10.1<br>10.5<br>Fix Pack 3 11.1<br>Fix Pack 14 11.5 |
| Oracle | 11g R2 (11.2.0.1.0)<br>12c<br>19c<br>**Note:** When you install Netcool Configuration Manager, choose the option **Oracle 11** if you are using Oracle 11, or the option **Oracle 12** if you are using Oracle 12 or 19.<br>**Tip:** Netcool Configuration Manager supports Oracle Real Application Clusters (RAC). If a failover occurs within a single RAC cluster, you do not need to restart Netcool Configuration Manager. If a failover to a separate RAC cluster occurs, you must restart Netcool Configuration Manager on all servers. |

**Note:** The database must be installed before Netcool Configuration Manager. Ensure a minimum 8kb block size per instance.

| *Table 4. Requirements for other products* | |
|---|---|
| **Item** | **Notes** |
| IBM WebSphere Application Server | Before installing the product, you must install IBM WebSphere Application Server V8.5.5.22 or V8.5.5.23 or V8.5.5.24. |
| Jazz for Service Management | Use Jazz for Service Management V1.1.3.19. |
| IBM Installation Manager | Use IBM Installation Manager Version 1.9.2.4 or 1.9.2.5. |
| DASH | DASH is required by Netcool Configuration Manager - Base for both integrated and stand-alone installations, whether installed with or without Tivoli Common Reporting. Various DASH services such as the reporting service are required by WebSphere to run a Netcool Configuration Manager - Base presentation server. DASH is not required for a worker-only installation. |

| *Table 4. Requirements for other products (continued)* | |
|---|---|
| **Item** | **Notes** |
| Tivoli Common Reporting | Use Tivoli Common Reporting Version 3.1.2.1.<br>**Important:** Tivoli Common Reporting prerequisites should be installed on all servers before any other software is installed.<br>Review the requirements for Tivoli Common Reporting to make sure you meet your performance requirements. For detailed information on software and hardware requirements, see the Tivoli Common Reporting information center at the following URL: http://www-01.ibm.com/support/knowledgecenter/SSEKCU/welcome<br>**Restriction:** ITNCM-Reports must be installed in a separate instance of DASH, and cannot reuse that of the Presentation Server if they are being installed on a single server.<br>**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.<br>Fix Pack 3<br>**Restriction:** Neither ITNCM-Reports nor DASH are supported on Linux on System z. |
| Cognos Analytics on zLinux | A deployment of Cognos Analytics on zLinux has the following requirements:<br>• LDAP repository requirements: http://www-969.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=F1C726601C2F11E69AAAC4D0C72C126B&osPlatform=Linux#sw-9<br>• IBM Cognos Analytics 11.0.0 Supported Software Environments: http://www-01.ibm.com/support/docview.wss?uid=swg27047186<br>• IBM Cognos Analytics Server 11.0.5 for Linux on System. Download instructions: http://www-01.ibm.com/support/docview.wss?uid=swg24043090<br>• IBM Cognos Analytics 11.0.13.0. Download instructions: https://www.ibm.com/support/pages/node/718809. |

| *Table 5. Netcool Configuration Manager client software requirements* | |
|---|---|
| **Item** | **Requirement** |
| Web Browser support | Chrome 116<br>Microsoft Edge 116<br>**Note:** A web browser should be installed on the client before any other software is installed. |
| Java Runtime Environment | As of Fix Pack 9, Netcool Configuration Manager supports only JRE 1.8 for the NCM client GUI. You can use the Oracle JRE or the IBM JRE. You can download the IBM JRE from Passport Advantage.<br>Check the JRE requirements of your version of any integrated products such as Network Manager. |

**Note:** ITNCM GUI clients are supported only on Windows.

| *Table 6. Other Netcool Configuration Manager requirements* | |
|---|---|
| **Item** | **Notes** |
| Unlimited Strength policy files | In order to support communications with greater than 128 bits of encryption, Netcool Configuration Manager requires Unlimited Strength policy files.<br>Netcool Configuration Manager Fix Pack 9 and above includes these files. If you have installed Netcool Configuration Manager Fix Pack 8 or below, follow these instructions to download and install the files: https://www.ibm.com/support/pages/node/6173229 |
| BouncyCastle | In order to support more complex encryption algorithms, Netcool Configuration Manager requires the Bouncy Castle JCE.<br>Install Bouncy Castle only for ITNCM v6.4.2 Fix Pack 10 and previous versions to support these algorithms. If you have already installed Bouncy Castle for ITNCM v6.4.2 Fix Pack 11 and later versions, then revert those changes. The BouncyCastle security provider must be listed first in the `ncm_install_dir/jre/jre/lib/security/java.security` file.<br>Follow these instructions to download and install the latest version of the BouncyCastle provider jars: https://www.ibm.com/support/pages/node/6173331 |
| FTP, TFTP, Tar, Unzip, gunzip | This should be installed on all servers before any other software is installed. |
| Network time protocol (NTP) | This should be installed and configured on all servers before any other software is installed. |
| DB2 Runtime Client | **Note:** Required **only** for the following scenarios:<br>• Installations of Netcool Configuration Manager that are not integrated with Network Manager, exercise the option to install Tivoli Common Reporting, and utilize a DB2 database.<br>• Installations of Netcool Configuration Manager that use a DB2 database and are integrated with Network Manager using a different database.<br>• Deployments of Cognos Analytics on zLinux<br>For more information, see “Installing and configuring the DB2 Run Time Client” on page 16. |
| logrotate | This should be installed to run the logcleaner.cnf script to perform housekeeping on log files. |

**Related tasks**

Installing and configuring the DB2 Run Time Client
When not integrating with Network Manager, and installing the Netcool Configuration Manager Tivoli Common Reporting component with a DB2 database, you must obtain and install the DB2 runtime client, catalogue the TCP/IP node (that is, the platform running the DB2 database), and also catalogue the DB2 database instance.

Installing a GUI and worker server
You install Netcool Configuration Manager either on a single server, or on several servers in a distributed architecture. The installation of a GUI and worker server can be part of a stand-alone installation on a single server, or it can be the first step in the installation of a distributed architecture on several servers.

Installing a worker server only

You install a Netcool Configuration Manager worker server as part of a distributed architecture deployed on one or more servers. You install one or more worker servers after having completed the installation of one or more GUI and worker servers.

## FIPS 140-2 requirements

To configure Netcool Configuration Manager with the intent to comply with FIPS 140-2 specifications, you must run Drivers version 20 or later and configure the HTTPS connection setup.

Netcool Configuration Manager cannot be said to be compliant with the FIPS 140–2 standard, and nothing in this information or in the product should be understood as making this claim. However, Netcool Configuration Manager can be configured in a way that has FIPS 140–2 specifications taken into consideration, and this is what is meant by "enabling FIPS 140-2 compliance".

Certificate export/import is required for HTTPS. When Netcool Configuration Manager uses encryption over HTTPS, FIPS-certified ciphers are used. Therefore, configuring the HTTPS connection setup is a prerequisite for enabling FIPS 140-2 mode on Netcool Configuration Manager.

For more information, see “HTTPS connection setup” on page 80.

**Related information**

Enabling and disabling FIPS 140-2 mode
Use this information to either enable or disable FIPS 140-2 mode.

# Chapter 2. Installing

Use this information to install Netcool Configuration Manager. After installation, you perform configuration tasks. For supplementary information on integrating with Network Manager IP Edition and Tivoli Netcool/OMNIbus, see the *IBM Tivoli Netcool Configuration Manager Integration Guide*.

## Downloading Netcool Configuration Manager

The procedure for downloading the product can differ for General Availability (GA) releases and fix packs.

To download Netcool Configuration Manager Drivers, locate the version of Drivers that you want to download in the Drivers Release Notes.

To download Netcool Configuration Manager, locate your version in the following table:

**Note:** If you use Netcool Configuration Manager as part of a solution, you must also check the compatibility of the versions of all component products in the solution documentation. For example, if you use Netcool Operations Insight, check the instructions for *downloading components* for your version of Netcool Operations Insight at https://www.ibm.com/support/knowledgecenter/en/SSTPTP.

*Table 7. Download locations*

| Product version | Download location | More information |
|---|---|---|
| 6.4.2.19 | Fix Central | https://www.ibm.com/support/docview.wss?uid=ibm17048716 |
| 6.4.2.18 | Fix Central | https://www.ibm.com/support/docview.wss?uid=ibm16999239 |
| 6.4.2.17 | Fix Central | https://www.ibm.com/support/docview.wss?uid=ibm16854935 |
| 6.4.2.16 | Fix Central | https://www.ibm.com/support/docview.wss?uid=ibm16558808 |
| 6.4.2.15 | Fix Central | https://www.ibm.com/support/docview.wss?uid=ibm16520366 |
| 6.4.2.14 | Fix Central | https://www.ibm.com/support/docview.wss?uid=ibm16440295 |
| 6.4.2.13 | Fix Central | https://www.ibm.com/support/docview.wss?uid=ibm16364953 |
| 6.4.2.12 | Fix Central | https://www.ibm.com/support/docview.wss?uid=ibm16246117 |
| 6.4.2.11 | Fix Central | https://www.ibm.com/support/docview.wss?uid=ibm16221254 |
| 6.4.2.10 | Fix Central | https://www.ibm.com/support/docview.wss?uid=ibm15737569 |
| 6.4.2.9 | Fix Central | https://www.ibm.com/support/docview.wss?uid=ibm11101189 |
| 6.4.2.8 | Fix Central | http://www.ibm.com/support/docview.wss?uid=ibm10886449 |

| Table 7. Download locations (continued) | | |
|---|---|---|
| **Product version** | **Download location** | **More information** |
| 6.4.2.7 | Fix Central | http://www.ibm.com/support/fixcentral/ |
| 6.4.2.6 | Fix Central | http://www.ibm.com/support/fixcentral/ |
| 6.4.2.5 | Fix Central | http://www.ibm.com/support/fixcentral/ |
| 6.4.2.4 | Passport Advantage | https://www.ibm.com/support/docview.wss?uid=swg24043484 |
| 6.4.2.3 | Fix Central | http://www.ibm.com/support/fixcentral/ |
| 6.4.2.2 | Passport Advantage | http://www.ibm.com/support/docview.wss?uid=swg24042711 |
| 6.4.2.1 | Fix Central | http://www.ibm.com/support/fixcentral/ |
| 6.4.2 | Passport Advantage | http://www.ibm.com/support/docview.wss?uid=swg24041718 |

# Preparing to install

Before you install or upgrade to a new version of Netcool Configuration Manager, you must take note of a number of prerequisites.

The following tasks or components are prerequisites for a successful Netcool Configuration Manager installation. If you do not complete them, the installation will fail.

The components listed in this section are installed with IBM Installation Manager. IBM Installation Manager is provided with the Netcool Configuration Manager V6.4.2 installation package, and is also available as a standalone product.

**Related tasks**

Installing a GUI and worker server
You install Netcool Configuration Manager either on a single server, or on several servers in a distributed architecture. The installation of a GUI and worker server can be part of a stand-alone installation on a single server, or it can be the first step in the installation of a distributed architecture on several servers.

Installing a worker server only
You install a Netcool Configuration Manager worker server as part of a distributed architecture deployed on one or more servers. You install one or more worker servers after having completed the installation of one or more GUI and worker servers.

**Related information**

Installing drivers
Use this information to install Netcool Configuration Manager drivers.

Installing OOBC

Use this information about Netcool Configuration Manager to install the OOBC daemon, install the OOBC software, configure an OOBC daemon, and troubleshoot OOBC installation issues.

## Creating OS user accounts

Netcool Configuration Manager requires a system user and an FTP user that belong to the same user group.

For commands specific to your operating system, refer to your OS documentation.

Netcool Configuration Manager operates under the default system user account 'icosuser' and group 'icosgrp'. Additionally, FTP servers that communicate with devices (GUI and Worker), or that process UOWs (Worker), use the default 'icosftp' user account. Icosgrp, icosuser and icosftp can be changed if your administration circumstances require this. However, the two users must belong to the same group.

**About the FTP user account**

You must create an FTP user account only on a server that is to be the FTP server communicating with devices (GUI & Worker), or that is going to process UOWs (Worker).

The FTP user account must be set up and used to create the network device configuration files, and it must exist on all workers.

The FTP user account is also used for FTP communications.

**Note:** Netcool Configuration Manager requires a designated space as a repository for all network device configuration files. This space will be used regardless of network configuration transfer mode (that is, FTP, TFTP, or streaming).

**Note:** This procedure assumes that the default system user, FTP user, and user group are used.

1. Log into the machine as `root`.
2. Create the `icosgrp` group.
3. Add the `icosuser` user to icosgrp.
4. Set the password for icosuser.

   **Remember:** Make a note of the password, as this will be required to complete the installation and administer the product.
5. Add the `icosftp` user to icosgrp.
6. Set the password for the icosftp user.

   **Remember:** Make a note of the password.
7. To allow general access to the `icosftp` directory, set the folder permissions at 774.

Now, create the installation directories.

## Creating installation directories

You use the **`mkdir`** command to create the installation directories on each server that Netcool Configuration Manager is to be installed.

You must create the installation directories on each server Netcool Configuration Manager will be installed.

1. Log on to the server as `root`
2. Execute the following command:
   `mkdir -p /opt/IBM/tivoli/netcool/ncm`

   **Note:** This is the default directory path.
3. Set the permissions on the install directory by typing:
   `chown icosuser:icosgrp /opt/IBM/tivoli/netcool/ncm`

Now, install the installation directories on the other servers as required. When done, you prepare the database for installation.

# Preparing a database

Before installing the product, you must prepare the database.

## Preparing the Oracle database

Prior to installing or upgrading Netcool Configuration Manager, Oracle database parameters must be set.

To prepare the Oracle database, you update the database, and then create the Oracle user account, before ensuring that all Netcool Configuration Manager Oracle database users have the appropriate system permissions.

**Note:** The default user is *icosuser*, which you can change.

Depending on the platform configuration, calculate your connection pool sizes based on the following default values:

**Note:** These are the minimum Netcool Configuration Manager requirements only.

```
Presentation Server with Compliance enabled

            Worker Server Core  = 55
            Presentation  = 65
            Compliance Core  = 55

                    Total  = 175 ( + 55 if IDT is changed to run standalone)


    Presentation Server with Compliance disabled

            Worker Server Core      = 55
            Presentation  = 65

                    Total  = 120 ( + 55 if IDT is changed to run standalone)


    Worker Server (Base + Compliance Eval Engine)

            Worker Server Core  = 55
            Compliance EE  = 55

                    Total  = 110


    Worker Server (Base only)

            Worker Server Core  = 55

                    Total  = 55


    Worker Server (Evaluation Engine Only)

            Evaluation Engine  = 55

                    Total  = 55


        + 15 for command-line tools
```

**Note:** This procedure assumes that the default *icosuser* is used.

1. Calculate Oracle processes using the formula specified.
2. Specify the following SQL*Plus command to specify the number of processes for the Oracle database: `ALTER SYSTEM SET PROCESSES=`*`value from formula`* `SCOPE=SPFILE`

   Oracle must be restarted for these settings to take effect. Before modifying the Oracle processes of an existing Netcool Configuration Manager deployment, it is necessary to stop all servers accessing the database prior to executing any modifications. In addition it is recommended when the application servers are to be started, that each server is shut down and allowed to restart one at a time before restarting the next one. This will result in a reduced impact on the Oracle database.
3. As the SYSDBA user, create the Oracle user account by executing the following SQL command:

`CREATE USER icosuser IDENTIFIED BY <password>`

4. Using SQL, assign the CONNECT and RESOURCE roles to the user as follows:
   `GRANT connect, resource TO icosuser`
5. Assign the CREATE VIEW privilege to the user as follows:
   `GRANT CREATE VIEW TO icosuser`
6. Assign the CREATE SESSION privilege to the user as follows:
   `GRANT CREATE SESSION TO icosuser`
7. Enable AUTOEXTEND for the database datafiles where the NCM tables will be installed, and set the quota for the database user to UNLIMITED.

   You usually only need to enable AUTOEXTEND and set the quota for `users01.dbf`, using commands similar to the following.

   ```
   alter database datafile '/opt/oracle/12201/db_files/Oracle12/users01.dbf' AUTOEXTEND ON;
   alter user icosuser quota UNLIMITED on users;
   ```

8. Issue the following SQL statement to allocate LOB chunks more efficiently:
   `ALTER SYSTEM SET EVENT='44951 TRACE NAME CONTEXT FOREVER, LEVEL 1024' scope=spfile;`
9. Restart the database.

Now, prepare the operating system for installation.

## Preparing the DB2 database

The following steps to prepare the DB2 database assume that you have already installed your DB2 database instance.

These steps assume that your DB2 instance owner is 'db2inst1'. If your instance owner is not 'db2inst1' then change 'db2inst1' references to your user.

The following steps also assume that the Netcool Configuration Manager database user is different from the instance owner and called 'ncmdbuser'. If you are using db2inst1 as the NCM database user, replace all 'ncmdbuser' references in commands with 'db2inst1'.

1. Login into DB2 Server as the instance owner 'db2inst1'.
2. Create the Netcool Configuration Manager database with a pagesize of 32768:

   ```
   db2 create database ITNCM automatic storage yes pagesize 32768 dft_extent_sz 32
   ```

3. Configure database user privileges.

   ```
   db2 connect to itncm
   ```

   **Note:** The Grant command may fail if your user already has privileges assigned.

   ```
   db2 "GRANT BINDADD,CONNECT,CREATE_NOT_FENCED_ROUTINE,CREATE_EXTERNAL_ROUTINE,
   QUIESCE_CONNECT ON DATABASE TO USER ncmdbuser"
   ```

4. Update the transaction log size:

   ```
   db2 update db cfg using logfilsiz 5000
   db2 update db cfg for itncm using logprimary 200
   db2 update db cfg for itncm using logsecond 50
   ```

5. For versions of DB2 prior to 11.0, increase the database storage used for locking. This step is not needed for DB2 11.0 and above:

   ```
   db2 update db cfg for itncm using LOCKLIST 8192
   ```

6. Commit Changes:

   ```
   db2 commit
   ```

7. Reset the database connection:

```
db2 connect reset
```

### *Installing and configuring the DB2 Run Time Client*

When not integrating with Network Manager, and installing the Netcool Configuration Manager Tivoli Common Reporting component with a DB2 database, you must obtain and install the DB2 runtime client, catalogue the TCP/IP node (that is, the platform running the DB2 database), and also catalogue the DB2 database instance.

You also perform these actions when integrating Netcool Configuration Manager using a DB2 database with a version of Network Manager that does **not** use a DB2 database.

Installation of the DB2 database is a prerequisite, which is described in the DB2 Knowledge Center. You can access the DB2 Knowledge Center at the following link: http://www-01.ibm.com/support/knowledgecenter/SSEPGG_9.5.0/com.ibm.db2.luw.doc/welcome.html

**Restriction:** This procedure applies only to the following two scenarios:

- Installations of Netcool Configuration Manager that are not integrated with Network Manager, exercise the option to install Tivoli Common Reporting, and utilize a DB2 database.
- Installations of Netcool Configuration Manager that use a DB2 database and are integrated with Network Manager using a different database.

For all other scenarios, ignore this procedure and move on to the topic describing how to add regular expression support to the DB2 database.

For information on configuring the DB2 Run Time Client, see the 'Configuring client-to-server connections using the command line processor' topic at the following link: http://www-01.ibm.com/support/knowledgecenter/SSEPGG_9.5.0/com.ibm.db2.luw.qb.client.doc/doc/t0007243.html

You can install the DB2 runtime client after installing Netcool Configuration Manager. If you do, ensure you then catalog the Netcool Configuration Manager database using the same alias that you supplied when installing the Tivoli Common Reporting components.

1. Download the DB2 Run Time Client.

   The runtime client can be obtained at the IBM Support Portal.

   a. On the IBM Support Portal, navigate to the **Downloads** tab and search for the version of the DB2 Run Time Client that you want to download.
   b. Select the appropriate link to display a table that lists the DB2 download packages.
   c. To download the DB2 Run Time Client, select the appropriate package from the table.

   For more information on the supported versions of DB2, see “Software requirements” on page 5.
2. Install the DB2 Run Time Client as `root` user.

   a) Unzip and untar the file.

   The `rtcl` directory is created.

   b) From the `rtcl` directory, run the `db2_install` command.

   You can install the client locally or anywhere else, such as the `icosuser` home directory.

   **Remember:** You need to specify this directory when installing the Netcool Configuration Manager Tivoli Common Reporting component.

   As part of the installation, the `sqllib` subdirectory is created in the install directory of the runtime client.
3. Catalog the TCP/IP Node (the platform running the DB2 database) using the following command: `db2 catalog tcpip node <node name> remote <db server hostname> server <db port>`

   **Tip:** The node name is at our discretion.

4. Catalog the DB2 database instance using a command similar to the following:

```
db2 catalog database <database name> at node <node name>
```

   For example:

```
db2 catalog database itncm at node dbnode
db2 terminate
```

5. Test your connection using a command similar to the followning:
   `db2 connect to <database name> user <db username>`

   For example:

```
db2 connect to itncm user root
```

**Related reference**

Software requirements

Software requirements vary according to the operating system and features of Netcool Configuration Manager that you want to use.

## *Adding user-defined functions*

Install Netcool Configuration Manager user-defined functions to your database user to prevent the schema installation from reporting errors.

1. Download the Netcool Configuration Manager user-defined function jar (`ibm_tivoli-ncm_db2_udf.jar`) unto the DB2 Server in your Netcool Configuration Manager database user home directory, for example `/home/ncmdbuser`.
2. Login to the DB2 server as Netcool Configuration Manager database user 'ncmdbuser'.
3. Source the db2profile if not already configured in your unix login profile:

```
.  /home/db2inst1/sqllib/db2profile
```

4. Install the user-defined functions:

```
db2 connect to itncm user ncmdbuser using <db password>
db2 "CALL SQLJ.INSTALL_JAR('file:/home/ncmdbuser/ibm_tivoli-ncm_db2_udf.jar',
 ncm_db2_udf)"
db2 "CALL SQLJ.REFRESH_CLASSES()"
```

**Important:** After installing the schema during the installation process, ensure that you grant 'execute' permissions on the functions to your Netcool Configuration Manager database user (after installation has completed).

You now prepare the operating system.

*Troubleshooting: Removing incorrect regex*

Before configuring regular expression support for the DB2 database by installing the appropriate jar file on the DB2 database server, you may need to remove an existing, incorrect Jar file from the DB2 database server first. This is not necessary on a fresh installation, but may be necessary if previous versions have existed.

Before completing these steps, stop the database server.

1. Connect to the existing DB2 database and set the schema, if required.
2. Remove functions by typing the following commands:

```
db2 drop function 'REGEXP_LIKE(CLOB,VARCHAR(512),VARCHAR(3))'
db2 drop function 'REGEXP_LIKE(VARCHAR(3000),VARCHAR(512),VARCHAR(3))'
db2 drop function DECODE_FUNCTION
```

   From Fix Pack 14 onwards, `REGEXP_LIKE` has been renamed to `NCM_REGEXP_LIKE`. Replace both instances of `REGEXP_LIKE` in the above commands with `NCM_REGEXP_LIKE`.

3. Remove the existing jar by typing the following:

```
db2 "CALL SQLJ.REMOVE_JAR(ncm_db2_udf)"
```

where

***ncm_db2_udf***
Is the existing jar.

4. Restart the database server.

You can now install the correct Jar to the DB2 database.

## Preparing the operating system

To prepare the operating system for installation, you edit the hosts and network files, enable the locale on each server, and enable IPv6 for AIX and Linux.

You only need to perform this task for first time installations, not upgrades. This task requires that you be familiar with the following:

**UNIX files, tools, and concepts**
Examples of UNIX tools include the `/etc/host` and `/etc/sysconfig/network` files, `vi` editor, and network-related commands such as `ip` and `ifconfig`. See your operating system documentation for more information.

**Networking concepts**
Some examples of networking concepts include layers, protocols, interfaces, Domain Name System (DNS), and so forth.

**IPv4 configuration**
Having background in IPv4 configuration will help you to understand IPv6 configuration.

**IPv6 concepts**
You can acquire an understanding of IPv6 concepts by consulting with a variety of sources on the Web. One concept you should be familiar with is IPv6 address types.

**Remember:** For deployments on AIX, the GNU version of TAR must be installed before Netcool Configuration Manager is installed.

If networking is not configured properly (for example, if Netcool Configuration Manager is installed against the loopback interface or the server's primary hostname maps to an unroutable IP address) then various components, such as IDT, may not function correctly.

1. Install the locale en_US.UTF-8 on each Netcool Configuration Manager server (that is, GUI and all Workers) before you install Netcool Configuration Manager.
2. Enable IPv6 on the AIX and Linux servers to facilitate IPv6 addressing for imports. See the operating system documentation for information on how to enable IPv6 support.
3. Add the IPv6 address by using either the `ip` or `ifconfig` command. The following example uses the `ip` command on Linux to add an IPv6 address (`fe80::20c:29ff:fea8:b1b8`) with a prefix length of 64, and a device name of `eth0`:

```
# ip -6 addr add fe80::20c:29ff:fea8:b1b8/64 dev eth0
```

The following example uses the `ifconfig` command on Linux to add an IPv6 address (`fe80::20c:29ff:fea8:b1b8`) with a prefix length of 64, and a device name of `eth0`:

```
# ifconfig eth0 inet6 add fe80::20c:29ff:fea8:b1b8/64
```

**Note:** See your IPv6 documentation for information on address types. Depending on where the servers are located and what they need access to will determine which addresses to use.

4. Each server in a distributed environment must be able to resolve the hostname of, and establish network communication to, every other server in the install environment. This can be achieved by ensuring that each server is configured to use a DNS server containing mappings for all servers, or

by ensuring that the /etc/hosts file contains entries for all Netcool Configuration Manager servers. Thus, you can add to the /etc/hosts file:

- The IP address and associated hostname for the DNS server that contains mappings for all servers.

  OR

- The IP address and associated hostname for each server on which Netcool Configuration Manager is installed.

The following example specifies an entry for /etc/hosts that describes a DNS server with an IP address of 192.168.248.30, a hostname of myhost, and a domain name of .ibm.com that contains mappings for all servers in the install environment:

```
192.168.248.30 myhost.ibm.com
```

5. On Linux, ensure that the HOSTNAME in /etc/sysconfig/network is correct and fully qualified.

   For example:
   HOSTNAME=myhost.ibm.com

   **Note:** The hostname specified in the /etc/sysconfig/network file should have a corresponding entry in the /etc/hosts file, as can be seen in the example in the previous step. The IP address of the hostname in /etc/sysconfig/network should be up and running on the primary interface of the server (typically, eth0).

The following example uses the ifconfig command with the -a option to display information on all network interfaces, active or inactive, that reside on the specified server. The primary network interface in the following example is eth0 and it has the IP address mapped to the hostname in /etc/sysconfig/network.

```
ifconfig     -a

cipsec0     Link encap:Ethernet HWaddr 00:0B:FC:F8:01:8F
                   NOARP MTU:1356 Metric:1
                   RX packets:0 errors:0 dropped:0 overruns:0 frame:0
                   TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
                   collisions:0 txqueuelen:1000
                   RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

eth0             Link encap:Ethernet HWaddr 00:0C:29:A8:B1:B8

inet             addr:123.123.123.12 Bcast:123.123.123.123 Mask:255.255.255.0
                    inet6 addr: fe80::20c:29ff:fea8:b1b8/64 Scope:Link
                    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                    RX packets:1326 errors:0 dropped:0 overruns:0 frame:0
                    TX packets:2152 errors:0 dropped:0 overruns:0 carrier:0
               collisions:0 txqueuelen:1000
                    RX bytes:179791 (175.5 KiB) TX bytes:2629566 (2.5 MiB) Interrupt:67
               Base address:0x2000

lo                Link encap:Local Loopback
                   inet addr:127.0.0.1 Mask:255.0.0.0
                   inet6 addr: ::1/128 Scope:Host
                   UP LOOPBACK RUNNING MTU:16436 Metric:1
                   RX packets:232615 errors:0 dropped:0 overruns:0 frame:0
                   TX packets:232615 errors:0 dropped:0 overruns:0 carrier:0
               collisions:0 txqueuelen:0
                   RX bytes:57057016 (54.4 MiB) TX bytes:57057016 (54.4 MiB)

sit0             Link encap:IPv6-in-IPv4
                    NOARP MTU:1480 Metric:1
                    RX packets:0 errors:0 dropped:0 overruns:0 frame:0
                    TX packets:0 errors:0 dropped:0 overruns:0 carrier:0 collisions:0
               txqueuelen:0
                    RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
```

Now, prepare the platforms for installation.

# Preparing the servers

Before installing the product, you must prepare the servers.

## Preparing an AIX installation

If you are planning to install as a non-root user on AIX®, and use SSH to access your AIX server, you must perform extra configuration steps before you access the AIX server. If you use rlogin or telnet to access your AIX server, you do not need to perform these steps. You also need to install the AIX unzip utility before installing Netcool Configuration Manager.

1. Obtain the AIX utilities from the IBM AIX Toolbox for Linux Applications website: http://www-03.ibm.com/systems/power/software/aix/linux/toolbox/altlic.html and follow the online prompts to install the required utilities.
   a) Install the rpm package manager first using the following command:
   `installp -YqacXgd rpm.rte rpm.rte`.
   The rpm package manager allows you to install the other utilities.
   b) As a minimum, download and install the unzip utility using rpm package manager using the following command:
   `rpm - i unzip-`*`version`*`.rpm`.
2. Open the `/etc/ssh/sshd_config` file on the AIX server where you want to install Netcool Configuration Manager.
3. Ensure that the file contains the following line:

```
UseLogin yes
```

4. Save and close the file.

You can now configure the firewall, if required, before using SSH to access the server and install Netcool Configuration Manager.

## Preparing a Linux installation

By default, the hosts file of Red Hat Enterprise Linux sets the FTP host IP to 127.0.0.1. You edit this file to change the hostname and associate it with the appropriate network address.

Ensure that the host name is registered with the DNS.

The following 32-bit libraries must be installed on Red Hat Enterprise Linux 6 platforms (32 and 64 bit versions), or the installation will fail.

- RHEL6: glibc-2.12 and libgcc-4.4.4 or later

1. When installing a Netcool Configuration Manager GUI server or ITNCM-Reports onto a Linux platform, set `nproc` to a value of `131072` to safely account for all the forked threads within processes that could be created.
   For more information, see the following technote: http://www-01.ibm.com/support/docview.wss?uid=swg21648497
2. Open the `/etc/hosts` file and go to the following line:
   `127.0.0.1 localhost hostname`
3. Modify the hostname and associate it with the appropriate network address, as in the following example.

   **Note:** As a rule, each address should have its own line.

```
10.216.1.141 hostname (replace with your system hostname and IP Address)
127.0.0.1 localhost
```

Now, you configure the firewall to ensure uninterrupted operation for the installation and function, before proceeding to the installation.

## Configuring the firewall

To ensure uninterrupted operation, you must ensure that all ports used for device communication are open.

Ensure that all required ports are open.

If you have changed ports from their default values, you can list the ports that are currently in use by Netcool Configuration Manager by running the `/opt/IBM/tivoli/netcool/ncm/bin/utils/portUsage.sh` script.

The following list shows all default ports required during installation.

- 1521 (default Oracle database port; only required if an Oracle database is used)
- 50000 (default DB2 database port; only required if a DB2 database is used)
- 16310 (default WebSphere Application Server HTTP port)
- 16311 (default WebSphere Application secure port)
- 8101 (default admin port)
- 8102 (default Log server admin port)
- 8103 (default Log server port)
- 8104 (default IDT daemon port)
- 16310
- 16311 (if TCR installed)
- 16315
- 16316 (for the ISC Console)

For a complete list of ports used by the product, see *Port Details* in the *IBM Tivoli Netcool Configuration Manager Reference Guide*..

## Installing IBM Installation Manager

IBM Installation Manager is a tool for installing, modifying, updating, and uninstalling IBM® products. Use IBM Installation Manager to install or update Netcool Configuration Manager Version 6.4.2.

**Note:** The compressed file distribution of Netcool Configuration Manager that is available from IBM Passport Advantage and on DVD includes IBM Installation Manager. You only need to download Installation Manager separately if you are installing Netcool Configuration Manager directly from an IBM repository or from a local repository.

For more information about downloading and installing Installation Manager, see http://www-01.ibm.com/support/docview.wss?uid=swg24039708.

For more information about using Installation Manager, see http://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html.

### IBM Installation Manager overview

You can install IBM Installation Manager with a GUI or console, or do a silent installation. Before installation, you must determine which user mode you require.

For more information about installing and using Installation Manager, see the following IBM information center: http://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html

#### User modes

You can install Installation Manager in one of three user modes:

- Administrator mode
- Nonadministrator mode

- Group mode

The user modes determine who can run Installation Manager, where product data is stored, and how different products are managed. Netcool Configuration Manager recommends Installation Manager to be installed in **Group** mode for the product and its pre-requistes.

*Table 8. Supported user modes*

| User mode | Description |
|---|---|
| Group mode | In group mode, you can install any number of instances of Installation Manager. Each instance requires a different data directory. All members of a group can use each instance. Installation Manager automatically sets file permissions so that all members of the group can update the installation. |
| Nonadministrator mode | In Nonadministrator mode, each user account can install one instance of Installation Manager. Information about all of the products that are managed by this instance is stored in a single data directory. Each user account can install multiple instances of Netcool Configuration Manager. |
| Administrator mode | In Administrator mode, an administrator or root user can install one instance of Installation Manager. Information about all of the products that are managed by this instance is stored in a single data directory.<br>Linux UNIX Administrator mode requires root privileges. Root users can install multiple instances of Netcool Configuration Manager. |

## Default directories

The default installation, data, and shared directories are different depending on which user mode you use. The data directory is used to store information about products that are installed with Installation Manager. The shared directory is used to store installation artifacts that can be used or reused by one or more products.

*Table 9. Default directories*

| User mode | Default installation directory | Default data directory | Default shared directory |
|---|---|---|---|
| Group mode | `$HOME/IBM/InstallationManager_Group/eclipse` | `$HOME/var/ibm/InstallationManager_Group` | `$HOME/IBM/IBMIMShared` |
| Nonadministrator mode | `$HOME/IBM/InstallationManager/eclipse` | `$HOME/var/ibm/InstallationManager` | `$HOME/IBM/IBMIMShared` |
| Administrator mode | `/opt/ibm/InstallationManager/eclipse` | `/var/ibm/InstallationManager` | `/opt/ibm/IBMIMShared` |

# Obtaining Installation Manager

IBM Installation Manager is available for download from the IBM Fix Central website.

You must have an IBM ID to download software from IBM Fix Central. You can register for an IBM ID at http://www.ibm.com.

See the following download document for information about downloading and installing IBM Installation Manager: http://www-01.ibm.com/support/docview.wss?uid=swg24039708

The IBM Fix Central website offers two approaches to finding product files: **Select product** and **Find product**. The following instructions apply to the **Find product** option.

1. Open the IBM Fix Central website at the following URL:
   http://www.ibm.com/support/fixcentral/
2. On the **Find product** tab:
   a) Enter IBM Installation Manager in the **Product selector** field.
   b) Select **1.8.2.0** from the **Installed Version** list.
   c) Select your intended host operating system from the **Platform** list and click **Continue**.
3. On the **Identity Fixes** page, choose **Browse for fixes** and **Show fixes that apply to this version (1.8.2.0)**. Click **Continue**.
4. On the **Select Fixes** page, select the installation file appropriate to your intended host operating system and click **Continue**.
5. When prompted, enter your IBM ID user name and password.
6. If your browser has Java enabled, choose the Download Director option. Otherwise, select the HTTP download option.
7. Start the installation file download. Make a note of the download location.

Install Installation Manager.

## Installation Manager response files

To do a silent installation of Netcool Configuration Manager, you must create or record an Installation Manager response file.

Installation Manager response files are XML files that contain the installation configuration for your installation scenario. You can use the following methods to create a response file:

- Manually create a response file.
- Use the Installation Manager `-record` option to record a response file. This option runs a GUI installation and records your chosen configuration in a response file.
- Use the Installation Manager `-skipInstall` option with the `-record` option to record a response file without actually installing Netcool Configuration Manager. This option records your intended installation configuration but does not complete the product installation.
- When you install Netcool Configuration Manager with the Installation Manager console, choose to create a response file for reuse in other installations. This uses the `imcl -c` option and allows you to enter and validate all the information before selecting to generate a response file instead of installing the product.

For more information about creating and deploying response files, see the following IBM information center: http://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html

## Installing Installation Manager (GUI or console)

You can install IBM Installation Manager with a wizard-style GUI or an interactive console.

Take the following actions:

- Extract the contents of the Installation Manager installation file to a suitable temporary directory.
- Ensure that the necessary user permissions are in place for your intended installation, data, and shared directories.
- The console installer does not report required disk space. Ensure that you have enough free space before you start a console installation.

The initial installation steps are different depending on which user mode you use. The steps for completing the installation are common to all user modes and operating systems.

Installation Manager takes account of your current umask settings when it sets the permissions mode of the files and directories that it installs. Using Group mode, Installation Manager ignores any group bits that are set and uses a umask of 2 if the resulting value is 0.

1. To install in Group mode:
   a) Use the id utility to verify that your current effective user group is suitable for the installation. If necessary, use the following command to start a new shell with the correct effective group:
   `newgrp group_name`
   We recommend using the icosgrp for Netcool Configuration Manager.
   b) Use the umask utility to check your umask value. If necessary, change the umask value.
   c) Change to the temporary directory that contains the Installation Manager installation files.
   d) Use the following command to start the installation:

   **GUI installation**
   `./groupinst -dL data_location`

   **Console installation**
   `./groupinstc -c -dL data_location`

   Where *data_location* specifies the data directory. You must specify a data directory that all members of the group can access. Each instance of Installation Manager requires a different data directory
2. Follow the installer instructions to complete the installation. The installer requires the following input at different stages of the installation:

   **GUI installation**

   - In the first panel, select the `Installation Manager` package.
   - Read and accept the license agreement.
   - When prompted, enter an installation directory or accept the default directory.
   - Verify that the total installation size does not exceed the available disk space.
   - When prompted, restart Installation Manager.

   **Console installation**

   - Read and accept the license agreement.
   - When prompted, enter an installation directory or accept the default directory.
   - If required, generate a response file. Enter the directory path and a file name with a `.xml` extension. The response file is generated before installation completes.
   - When prompted, restart Installation Manager.
3. Connect to a repository that contains the products that you want to install:

   A repository can be on a local server or online.
   a) Click **File** > **Preferences**.
   b) If a repository has been set up for you, click **Repositories** and ensure that the correct repositories are selected.
   c) If no repositories have been set up for you, and you want to set up a repository yourself, refer to the information about *managing packages with the Packaging Utility* in the Installation Manager documentation: http://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html
   d) If you want to connect directly to the IBM online repository to access the products to which you are entitled, click Passport Advantage®, select **Conect to Passport Advantage**, and click **Apply**. Click **OK**.

   When you install or update a product, you are prompted for your credentials to access IBM Passport Advantage.

Installation Manager is installed and can now be used to install Netcool Configuration Manager and its pre-requisites.

If required, add the Installation Manager installation directory path to your PATH environment variable.

### Installing Installation Manager (silent)

You can install IBM Installation Manager silently. This is useful if you want identical installation configurations on multiple workstations. You can also use a response file to define the installation configuration, if required.

Take the following actions:

- Extract the contents of the Installation Manager installation file to a suitable temporary directory.
- Read the license agreement. The license agreement file, `license.txt`, is stored in the *`temp_directory`*`/native/license_version.zip` archive.
- Ensure that the necessary user permissions are in place for your intended installation, data, and shared directories.

Installation Manager takes account of your current umask settings when it sets the permissions mode of the files and directories that it installs. Using Group mode, Installation Manager ignores any group bits that are set and uses a umask of 2 if the resulting value is 0.

To install in Group mode:

a) Use the id utility to verify that your current effective user group is suitable for the installation. If necessary, use the following command to start a new shell with the correct effective group:
`newgrp group_name`
We recommend using the icosgrp for Netcool Configuration Manager.

b) Use the umask utility to check your umask value. If necessary, change the umask value.

c) Change to the temporary directory that contains the Installation Manager installation files.

d) Use the following command to start the installation:
`./groupinstc -dL` *`data_location`* `-acceptLicense`

Where *`data_location`* specifies the data directory and the `-acceptLicense` option specifies that you accept the license agreement.

You must specify a data directory that all members of the group can access. Each instance of Installation Manager requires a different data directory.

Installation Manager is installed and can now be used to install Netcool Configuration Manager.

If required, add the Installation Manager installation directory path to your PATH environment variable.

## Installing WebSphere application server

Before installing the product, you must install IBM WebSphere Application Server version 8.5.5.9 and upgrade it to version V8.5.5.22 for Jazz for Service Management. Install IBM WebSphere SDK Java Technology Edition 8.0.5.27 at the same time.

Before upgrading WebSphere Application Server, check that the WebSphere SSL certificate has not expired. By default, the certificate expires after 365 days. For a backup or High Availability cold-standby system you might not notice that the certificate has expired until you attempt to use the fallback option. To renew or replace the certificate, follow the recommended solution in this link: https://www.ibm.com/support/pages/how-do-i-extend-expiration-default-ssl-certificate-websphere-application-server

## Installing Jazz for Service Management

Before installing the product, you must install Jazz for Service Management Version on all presentation servers using the IBM Installation Manager.

DASH is required by Netcool Configuration Manager - Base for both integrated and stand-alone installations, whether installed with or without Tivoli Common Reporting. Various DASH services such as the reporting service are required by WebSphere to run a Netcool Configuration Manager - Base presentation server. DASH is not required for a worker-only installation.

During this step the Installation Manager discovers two required packages in the Jazz repository. Both of these packages must be selected for simultaneous installation:

- Jazz for Service Management extension for IBM WebSphere V8.5.
- Dashboard Application Services Hub V3.1.3.0.

Fix Pack 9 After installing Dashboard Application Services Hub V3.1.3.0, upgrade it to 3.1.3.4 or above.

Fix Pack 9 After you have installed Jazz for Service Management and WebSphere Application Services, check the Java SDK version on the server is at 1.8, as shown in the example below:

```
JazzSM Install location/profile/bin/managesdk.sh -listEnabledProfileAll
CWSDK1004I: Profile JazzSMProfile :
CWSDK1006I: PROFILE_COMMAND_SDK = 1.8_64_bundled
CWSDK1008I: Node JazzSMNode01 SDK name: 1.8_64_bundled
CWSDK1009I: Server server1 SDK name: 1.8_64_bundled
CWSDK1001I: Successfully performed the requested managesdk task.
```

For detailed instructions, see the Jazz for Service Management Knowledge Center: http://www-01.ibm.com/support/knowledgecenter/SSEKCU/welcome?lang=en

**Important:** Depending on the installation type, you may need to install two instances of DASH.

**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 sendITNCMDeviceActivityTraps.sh, do not trigger an Network Manager import into Netcool Configuration Manager, do not use the Netcool Configuration Manager right click menus from TIP.

## Installing Tivoli Common Reporting

Before installing the product, you must install Tivoli Common Reporting Version 3.1.2.0 (if you plan to use ITNCM Reports).

**Restriction:** Fix Pack 3 This topic does not apply to Netcool Configuration Manager installations on Linux on System z.

**Note:** Fix Pack 14 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.

Before installing Tivoli Common Reporting using the IBM Installation Manager., you must install Jazz for Service Management.

For detailed instructions on installing Tivoli Common Reporting, see the 'Installing Reporting Services' topic in the Jazz for Service Management Knowledge Center: http://www-01.ibm.com/support/knowledgecenter/SSEKCU/welcome?lang=en

**Note:**

If you are integrating with Network Manager, you will be installing ITNCM Reports onto the Network Manager Tivoli Common Reporting server, and therefore you do not need to install Tivoli Common Reporting here.

If you are deploying Tivoli Common Reporting in a **non-integrated** environment, it must be installed on its own server.

If you are using DB2, you must catalogue its database.

## [zLinux] Preparing ITNCM Reports for Cognos Analytics

You can view ITNCM Reports on a Netcool Configuration Manager installation on Linux on System z **only** by using Cognos Analytics.

1. Obtain Cognos 11.0.5.0 using the following instructions: http://www-01.ibm.com/support/docview.wss?uid=swg24043081
2. For more information on the LDAP repository requirements, see the following compatibility report: https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=F1C726601C2F11E69AAAC4D0C72C126B

# Installing the product

Netcool Configuration Manager for AIX and Linux are installed using the IBM Installation Manager.

Ensure you have obtained and installed the IBM Installation Manager, as described in “Installing IBM Installation Manager” on page 21.

**Remember:**

If you are planning to integrate your installation with IBM Tivoli Network Manager IP Edition, you may need to perform additional installation and configuration tasks.

Before proceeding with the installation, ensure you have reviewed the *IBM Tivoli Netcool Configuration Manager Integration Guide*.

**Attention:** When using the IBM Installation Manager to install zLinux, you may receive a number of warnings. Ignore these and proceed with the installation.

## Installation information checklist

You can define checklists for all Netcool Configuration Manager servers that are to be installed as part of the deployment. Details you must assemble before installation include server names, passwords and system paths.

### IDT servers

If you have multiple presentation servers in a deployment of Netcool Configuration Manager, one server must be chosen as the main, or master, presentation server. This means that all IDT connections will be passed through this server if you are running IDT in master mode. For more information, see the Administration Guide.

### Netcool Configuration Manager installation information

Fix Pack 2 As part of a presentation server installation, you can install Netcool Configuration Manager using a federated repository.

**Required**
If you are installing into the same DASH instance as an existing deployment of Network Manager and Tivoli Netcool/OMNIbus, using a federated repository is a requirement.

**Optional**
If you are installing into a separate instance of DASH, you can still set up Netcool Configuration Manager authentication with the Tivoli Netcool/OMNIbus Object Server as described in *Creating and configuring a federated user repository for Netcool Configuration Manager* in the *IBM Tivoli Netcool Configuration Manager Integration Guide*.

**Note:** Ensure the default `administrator`, `observer` and `operator` users are created in the federated repository.

**Note:** Do not make use of spaces in any names provided for the checklist.

*Table 10. Installation information checklist for Netcool Configuration Manager*

| Type | Information | Details | Default value |
|---|---|---|---|
| **Note:** If you do not supply a root realm, it defaults to `itncm` | | | |
| License | Accept / reject | You can choose to print the license, or return to the previous screen. If you do not accept the license, the installation is aborted. | none |
| Installation directory | | You can choose your own location.<br>**Note:** Install Manager requires an empty directory for an initial installation of Netcool Configuration Manager. | `/opt/IBM/tivoli/netcool/ncm` |
| Server Installation type | Presentation server + worker server / Worker server | Depends on whether the installation is part of a stand-alone installation, or a distributed installation.<br>**Note:** To improve load balancing, a distributed installation can have more than one 'GUI server + worker server' installation type. | Presentation server + worker server |
| Database | Oracle or DB2 | Must be installed and configured beforehand | DB2 |
| If Oracle database | IP address/ hostname | | |
| | Port | | 1521 |
| | SID | | itncm |
| | Service name | | itncm |
| | Username | | |
| | Password | | |
| If DB2 database | IP address/ hostname | | |
| | Port | | 50000 |
| | Name | | |
| | Alias | | itncm |
| | Username | | |
| | Password | | |
| Netcool Configuration Manager details | Root realm | | ITNCM |
| | Superuser password | | |
| FTP | Server | | |
| | User account | | |
| | Password | | |
| | User account directory | | `/home/icosftp` |

*Table 10. Installation information checklist for Netcool Configuration Manager (continued)*

| Type | Information | Details | Default value |
|---|---|---|---|
| SMTP server | SMTP server | For example, `smtp.IBM.net` | |
| Current server | Instance name | Unique Netcool Configuration Manager server name | |
| If worker server installation type | Activate Configuration-core | Depends on what kind of distributed installation is being performed.<br>**Note:** A mandatory selection in a presentation installation. | Selected |
| | Activate Compliance Core | Depends on what kind of distributed installation is being performed. If not selected during a Presentation server installation, then the Compliance GUI and Compliance Core will not be available. | Selected |
| | Linked Server<br>Not a Linked Server | Enables the worker server about to be installed to reuse the drivers already installed on this server.<br>**Note:** The existing installation must have the drivers installed and the correct deployment keystore files in place. If you choose to link to an existing server, you must provide the installation directory (default = `/opt/IBM/tivoli/netcool/ncm`). | Not a Linked Server |
| Administration ports<br>**Note:** If you are installing a worker server and linking it to an existing Netcool Configuration Manager installation on the same server, the default ports will already be in use. Therefore you must specify new, unused ports. | Admin port | | 8101 |
| | Log server admin port | | 8102 |
| | Log server port | | 8103 |
| | IDT daemon port | | 8104 |
| | Compliance administration port + next five consecutive ports | Specifies the Netcool Configuration Manager - Compliance administration port. The next five consecutive ports will be selected automatically. | 8110 |
| Main IDT Daemon Server | Yes / No | Depends on whether the installation is part of a stand-alone installation, or a distributed installation. Also depends on what kind of distributed installation is being performed. | Yes |
| Network Manager DASH server | NM Hostname | | |
| | NM port to connect to | | 16311 |
| | NM User | | itnmadmin |
| | NM User password | | |
| | NM User password confirmation | | |
| | Realm | The realm to import the devices to | ITNCM/@DOMAINNAME |
| Fix Pack 2 Jazz for Service Management installation options | Using a federated repository | From fix pack 2 onwards you can install Netcool Configuration Manager using a federated repository. This repository requires two groups and three users to be created before the Install Groups. | User names are case-sensitive.<br>**Groups:**<br>• IntellidenUser<br>• IntellidenAdmin User<br>**Users:**<br>• administrator<br>• observer<br>• operator |

| Table 10. Installation information checklist for Netcool Configuration Manager (continued) | | | |
|---|---|---|---|
| **Type** | **Information** | **Details** | **Default value** |
| Jazz for Service Management properties | Configuration for a Presentation Server Only | | |
| | Installation Directory Details | | |
| | AppServer Installation Directory Details | | |
| | User Name | | |
| | Password | | |
| | Automatically Configured Variables | | |
| | Server Name | Selected automatically depending on the JazzSM Installation Directory given | |
| | Server Cell t | | |
| | Server Node | | |
| | HTTP Port | | |
| | HTTPS Port | | |

**Related tasks**

Installing a GUI and worker server
You install Netcool Configuration Manager either on a single server, or on several servers in a distributed architecture. The installation of a GUI and worker server can be part of a stand-alone installation on a single server, or it can be the first step in the installation of a distributed architecture on several servers.

Installing a worker server only
You install a Netcool Configuration Manager worker server as part of a distributed architecture deployed on one or more servers. You install one or more worker servers after having completed the installation of one or more GUI and worker servers.

# Installing a GUI and worker server

You install Netcool Configuration Manager either on a single server, or on several servers in a distributed architecture. The installation of a GUI and worker server can be part of a stand-alone installation on a single server, or it can be the first step in the installation of a distributed architecture on several servers.

Ensure you have completed all required prerequisite tasks, such as the installation of either an Oracle or a DB2 database, as described in “Preparing to install” on page 12.

Gather all the required information, such as hostnames and passwords, as listed in “Installation information checklist” on page 27.

**Important:** Quit all programs before continuing with this installation.

If performing a stand-alone installation of Netcool Configuration Manager, that is, not integrated with Network Manager, ensure you have fulfilled the requirements for Tivoli Common Reporting, if you would like to use its functionality, as listed in “Software requirements” on page 5.

If you are installing ITNCM Reports on the same server as the GUI and worker server, you must install a second instance of DASH. (You only need one instance of WebSphere, however).

If you are preparing to perform an integrated installation, ensure you have consulted the *IBM Tivoli Netcool Configuration Manager Integration Guide* before proceeding.

Perform the following checks before installation:

**Defining sufficient memory (or IBMShared) space**

There can be issues installing Netcool Configuration Manager if there is not enough available memory or IBMShared space.

This problem can be eliminated by allocating more IBMShared space.

**Setting sufficient Oracle process limits**

There may be issues with Oracle responsiveness if there is not a sufficient amount of processes running.

The Oracle process limit must be at least 55 processes per worker server that will be deployed.

**Synchronizing server timings**

It is a requirement that all servers must have their times synced to within 10 seconds of each other for correct operation.

Each server can be synced by setting up the NTP protocol.

**Increasing WebSphere Application Server memory on Linux**

**Note:** Applies only to a scenario where a GUI server or Tivoli Common Reporting is being installed onto a Linux platform.

When installing a Netcool Configuration Manager GUI server or Tivoli Common Reporting onto a Linux platform, set **nproc** to a value of 131072 to safely account for all the forked threads within processes that could be created.

For more information, see the following technote: http://www-01.ibm.com/support/docview.wss?uid=swg21648497

**Attention:** When using the IBM Installation Manager to install zLinux, you may receive a number of warnings. Ignore these and proceed with the installation.

This task describes the installation of a GUI and worker server with the following variations:

- Installation on either AIX or Linux platforms.
- Configuration of a previously installed Oracle or DB2 database.
- Enablement of the compliance core server (required if stand-alone).
- Optional selection of the current server as the main IDT presentation server (required if stand-alone).
- Optional loading of the database schema.
- The steps for starting Installation Manager differ depending on the user mode in which it was installed. The steps for installing with the Installation Manager console are common to all user modes and operating systems. Take note of the following information about permissions on the supported operating systems:
  - Installation Manager takes account of your current umask settings when it sets the permissions mode of the files and directories that it installs.
  - If you use Administrator mode or Nonadministrator mode and your umask is 0, Installation Manager uses a umask of 22.
  - If you use Group mode, Installation Manager ignores any group bits that are set and uses a umask of 2 if the resulting value is 0.

**Tip:** It is recommended to use Install Manager Group Mode for installation.

Respond to each Installation configuration option to ensure it matches your pre-defined Installation Information Checklist.

1. Change to the `/eclipse` subdirectory of the Installation Manager Group installation directory and use the following command to start Installation Manager, as the `icosuser` user:
   `./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
   ```

2. 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**.
3. In the main **Installation Manager** window, click **Install**, and then follow the installation wizard instructions to complete the installation.
   Enter your IBM ID, user name and password if prompted.
   Select from the following installable packages, as required.

| Option | Description |
|---|---|
| **Package** | Description |
| **IBM WebSphere Application Server** | WebSphere® Application Server component on which Jazz for Service Management is based. Required only for a new installation of Jazz for Service Management. |
| **Jazz for Service Management extension for IBM WebSphere 8.5** | Required only for a new installation of Jazz for Service Management.<br>**Note:** You must select v8.5 of Jazz for Service Management extension for IBM WebSphere. |
| **IBM Dashboard Application Services Hub** | Required only for a new installation of Jazz for Service Management. |
| **Network Manager 4.2** | Required only if you want to install an integrated system. |
| **Network Configuration Manager V6.4.2.0** | Required |
| **Reporting Services environment** | Required only if you need the reporting functions that are included in Jazz for Service Management. |

   After you select the packages, the wizard prompts you for some of the following information:

   - Read and accept the license agreement.
   - Specify an Installation Manager shared directory, or accept the default directory.
   - Specify an installation directory for the product, or accept the default directory.
   - For Server Installation Type, select **Presentation Server and Worker Server**.

     **Note:** If you require ITNCM Reports, install this option after you have completed the Netcool Configuration Manager installation.

     **Remember:** If you are installing ITNCM Reports on the same server as the GUI and worker server, you must install a second instance of DASH.
   - Provide information about the Netcool Configuration Manager database, specific configuration information, and the required Jazz for Service Management properties.
   - Complete the Installation.

The IBM Installation Manager installs Netcool Configuration Manager.

If this installation of a GUI and worker server completes a stand-alone installation on a single server, you install the drivers and OOBC software next, as well as (optionally) ITNCM reports. For more information, see “Installing drivers” on page 48, “Installing OOBC” on page 62, and“Installing ITNCM-Reports” on page 42.

After that, you perform a number of post-installation procedures, such as safeguarding the keystore and increasing the Java Heap size. For information on these and other configuration tasks, see Chapter 3, “Configuring,” on page 67.

If this installation was the first step in the installation of a distributed architecture on several servers, you install the worker servers next.

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.

**Related tasks**

Preparing to install
Before you install or upgrade to a new version of Netcool Configuration Manager, you must take note of a number of prerequisites.

Changing platform configuration
You can change platform configuration by running the `setPlatform.sh` script.

Installing ITNCM-Reports
If you are not integrating with Network Manager, which ships with its own version of DASH, you must install ITNCM-Reports separately in order to access the reporting functionality.

Loading the databases
Loading the database for Netcool Configuration Manager builds the schemas and loads the content. You can load the databases during installation, or separately at a later stage.

Installing a worker server only
You install a Netcool Configuration Manager worker server as part of a distributed architecture deployed on one or more servers. You install one or more worker servers after having completed the installation of one or more GUI and worker servers.

Deploying the keystore and user files
For installations using a distributed environment, you must copy the keystore and user files to each server, or else these servers will not be operational.

Increasing the Java Heap size
If it is intended that network resources will have large configuration sizes being processed on the Worker server, an increase in the Java heap size might be required.

Configuring
After installation, you perform a number of post-installation configuration tasks.

Configuring reporting on a stand-alone installation
If Netcool Configuration Manager Reporting has been installed stand-alone, there are a number of configuration steps which must be followed to access the reports.

**Related reference**

Software requirements
Software requirements vary according to the operating system and features of Netcool Configuration Manager that you want to use.

Installation information checklist

You can define checklists for all Netcool Configuration Manager servers that are to be installed as part of the deployment. Details you must assemble before installation include server names, passwords and system paths.

**Related information**

Installing OOBC
Use this information about Netcool Configuration Manager to install the OOBC daemon, install the OOBC software, configure an OOBC daemon, and troubleshoot OOBC installation issues.

## Installing a worker server only

You install a Netcool Configuration Manager worker server as part of a distributed architecture deployed on one or more servers. You install one or more worker servers after having completed the installation of one or more GUI and worker servers.

Ensure you have completed all required prerequisite tasks, such as the installation of either an Oracle or a DB2 database, as described in "Preparing to install" on page 12.

Gather all the required information, such as hostnames and passwords, as listed in "Installation information checklist" on page 27.

**Important:** Quit all programs before continuing with this installation.

If performing a stand-alone installation of Netcool Configuration Manager, that is, not integrated with Network Manager, ensure you have fulfilled the requirements for Tivoli Common Reporting, if you would like to use its functionality, as listed in "Software requirements" on page 5.

If you are preparing to perform an integrated installation, ensure you have consulted the *IBM Tivoli Netcool Configuration Manager Integration Guide* before proceeding.

Perform the following checks before installation:

**Defining sufficient memory (or IBMShared) space**

There can be issues installing Netcool Configuration Manager if there is not enough available memory or IBMShared space.

This problem can be eliminated by allocating more IBMShared space.

**Setting sufficient Oracle process limits**

There may be issues with Oracle responsiveness if there is not a sufficient amount of processes running.

The Oracle process limit must be at least 55 processes per worker server that will be deployed.

**Synchronizing server timings**

It is a requirement that all servers must have their times synced to within 10 seconds of each other for correct operation.

Each server can be synced by setting up the NTP protocol.

**Increasing WebSphere Application Server memory on Linux**

**Note:** Applies only to a scenario where a GUI server or Tivoli Common Reporting is being installed onto a Linux platform.

When installing a Netcool Configuration Manager GUI server or Tivoli Common Reporting onto a Linux platform, set **nproc** to a value of 131072 to safely account for all the forked threads within processes that could be created.

For more information, see the following technote: http://www-01.ibm.com/support/docview.wss?uid=swg21648497

**Attention:** When using the IBM Installation Manager to install zLinux, you may receive a number of warnings. Ignore these and proceed with the installation.

This task describes the installation of a worker server with the following variations:

- Installation on either AIX or Linux platforms.
- Configuration of a previously installed Oracle or DB2 database.

- The steps for starting Installation Manager differ depending on the user mode in which it was installed. The steps for installing with the Installation Manager console are common to all user modes and operating systems. Take note of the following information about permissions on the supported operating systems:
  - Installation Manager takes account of your current umask settings when it sets the permissions mode of the files and directories that it installs.
  - If you use Administrator mode or Nonadministrator mode and your umask is 0, Installation Manager uses a umask of 22.
  - If you use Group mode, Installation Manager ignores any group bits that are set and uses a umask of 2 if the resulting value is 0.

**Tip:** It is recommended to use Install Manager Group Mode for installation.

Respond to each Installation configuration option to ensure it matches your pre-defined Installation Information Checklist.

1. Change to the `/eclipse` subdirectory of the Installation Manager Group installation directory and use the following command to start Installation Manager, as the `icosuser` user:
   `./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
   ```

2. 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**.
3. In the main **Installation Manager** window, click **Install**, and then follow the installation wizard instructions to complete the installation.

   If you have already installed Netcool Configuration Manager, ignore the message that this package is already installed and continue with the installation. There will be a unique directory suggested for the installation. Make sure to select a unique name for this Worker Server and the ports. Enter your IBM ID, user name and password if prompted.
4. After you select the packages, the wizard prompts you for some of the following information:
   - Read and accept the license agreement.
   - Specify an Installation Manager shared directory, or accept the default directory.
   - Specify an installation directory for the product, or accept the default directory.
   - For Server Installation Type, select **Worker Server**.

     **Note:** If you require ITNCM Reports, install this option after you have completed the Netcool Configuration Manager installation.
   - Provide information about the Netcool Configuration Manager database, specific configuration information, and the required Jazz for Service Management properties.

- Complete the Installation.

5. Deploy the keystore and user files. See the following topic for more information: “Deploying the keystore and user files” on page 78

The IBM Installation Manager installs Netcool Configuration Manager.

Repeat this task for all worker server installations.

If this worker server installation completes the distributed deployment of Netcool Configuration Manager, you install the drivers and OOBC software next, as well as (optionally) ITNCM Reports. For more information, see “Installing drivers” on page 48, “Installing OOBC” on page 62, and “Installing ITNCM-Reports” on page 42.

After that, you perform a number of post-installation procedures, such as safeguarding the keystore and increasing the Java Heap size. For information on these and other configuration tasks, see Chapter 3, “Configuring,” on page 67.

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.

**Related tasks**

Preparing to install
Before you install or upgrade to a new version of Netcool Configuration Manager, you must take note of a number of prerequisites.

Changing platform configuration
You can change platform configuration by running the `setPlatform.sh` script.

Installing ITNCM-Reports
If you are not integrating with Network Manager, which ships with its own version of DASH, you must install ITNCM-Reports separately in order to access the reporting functionality.

Installing a GUI and worker server
You install Netcool Configuration Manager either on a single server, or on several servers in a distributed architecture. The installation of a GUI and worker server can be part of a stand-alone installation on a single server, or it can be the first step in the installation of a distributed architecture on several servers.

Configuring
After installation, you perform a number of post-installation configuration tasks.

Deploying the keystore and user files
For installations using a distributed environment, you must copy the keystore and user files to each server, or else these servers will not be operational.

Loading the databases
Loading the database for Netcool Configuration Manager builds the schemas and loads the content. You can load the databases during installation, or separately at a later stage.

Configuring reporting on a stand-alone installation
If Netcool Configuration Manager Reporting has been installed stand-alone, there are a number of configuration steps which must be followed to access the reports.

**Related reference**

Software requirements
Software requirements vary according to the operating system and features of Netcool Configuration Manager that you want to use.

Installation information checklist

You can define checklists for all Netcool Configuration Manager servers that are to be installed as part of the deployment. Details you must assemble before installation include server names, passwords and system paths.

**Related information**

Installing OOBC
Use this information about Netcool Configuration Manager to install the OOBC daemon, install the OOBC software, configure an OOBC daemon, and troubleshoot OOBC installation issues.

## Installing in console mode

You can install Netcool Configuration Manager in console mode. However, if you are installing a presentation server it can only be installed into an existing Jazz for Service Management environment. Jazz for Service Management and IBM WebSphere Application servers do not support installations in console mode. For a complete installation of the Web GUI and the underlying Jazz for Service Management and IBM WebSphere Application Server components, use GUI or silent mode installation.

Ensure you have completed all required prerequisite tasks, such as the installation of either an Oracle or a DB2 database, as described in “Preparing to install” on page 12.

Gather all the required information, such as hostnames and passwords, as listed in “Installation information checklist” on page 27.

**Important:** Quit all programs before continuing with this installation.

If performing a stand-alone installation of Netcool Configuration Manager, that is, not integrated with Network Manager, ensure you have fulfilled the requirements for Tivoli Common Reporting, if you would like to use its functionality, as listed in “Software requirements” on page 5.

If you are preparing to perform an integrated installation, ensure you have consulted the *IBM Tivoli Netcool Configuration Manager Integration Guide* before proceeding.

Perform the following checks before installation:

**Defining sufficient memory (or IBMShared) space**

There can be issues installing Netcool Configuration Manager if there is not enough available memory or IBMShared space.

This problem can be eliminated by allocating more IBMShared space.

**Setting sufficient Oracle process limits**

There may be issues with Oracle responsiveness if there is not a sufficient amount of processes running.

The Oracle process limit must be at least 55 processes per worker server that will be deployed.

**Synchronizing server timings**

It is a requirement that all servers must have their times synced to within 10 seconds of each other for correct operation.

Each server can be synced by setting up the NTP protocol.

**Increasing WebSphere Application Server memory on Linux**

**Note:** Applies only to a scenario where a GUI server or Tivoli Common Reporting is being installed onto a Linux platform.

When installing a Netcool Configuration Manager GUI server or Tivoli Common Reporting onto a Linux platform, set **nproc** to a value of 131072 to safely account for all the forked threads within processes that could be created.

For more information, see the following technote: http://www-01.ibm.com/support/docview.wss?uid=swg21648497

The steps for starting Installation Manager differ depending on the user mode in which it was installed. The steps for installing with the Installation Manager console are common to all user modes and operating systems. Take note of the following information about permissions on the supported operating systems:

- Installation Manager takes account of your current umask settings when it sets the permissions mode of the files and directories that it installs.
- If you use Administrator mode or Nonadministrator mode and your umask is 0, Installation Manager uses a umask of 22.
- If you use Group mode, Installation Manager ignores any group bits that are set and uses a umask of 2 if the resulting value is 0.

**Attention:** When using the IBM Installation Manager to install zLinux, you may receive a number of warnings. Ignore these and proceed with the installation.

1. Change to the `/eclipse/tools` subdirectory of the Installation Manager installation directory.
2. Use one of the following commands to start Installation Manager, as the `icosuser` user:
   ```
   ./imcl -c
   ./imcl -consoleMode
   ```
3. Configure Installation Manager to download package repositories from IBM Passport Advantage:
   a) From the main menu, choose **Preferences** > **Passport Advantage** > **Connect to Passport Advantage**.
   b) When prompted, enter your IBM ID user name and password, and then return to the main menu.
4. From the options on the installer, add the repository that you want to install.
5. From the main menu, select **Install**, then follow the installer instructions to complete the installation.
   The installer requires the following input at different stages of the installation:
   - Select Netcool Configuration Manager.
   - Read and accept the license agreement.
   - Specify an Installation Manager shared directory, or accept the default directory.
   - Specify an installation directory for the product, or accept the default directory.

     **Note:** You need an empty directory for the initial installation.
   - Select the packages you wish to Install. Choose either options one and two, or options one and three of the following choices:

     ```
     1. [ ] Reports
     2. [ ] Presentation Server and Worker Server
     3. [ ] Worker Server
     ```

     **Note:** Ignore the Installation Manager `Incompatible existing package groups` warning. This is expected behaviour and indicates that a new package group must be created for Netcool Configuration Manager.
   - Select each option in the configuration phase and update the values according to your Installation Information Checklist to configure the Netcool Configuration Manager Database, specific configuration information, and Jazz for Service Management properties.
   - Execute the Installation, or generate a response file for use with silent installations on another server if necessary.

     **Note:** When saving the response file, enter the directory path and a file name with a .xml extension. The response file is generated before installation completes.
6. After the installation completes, click **Finish**.

The IBM Installation Manager installs Netcool Configuration Manager.

If this installation of a GUI and worker server completes a stand-alone installation on a single server, you install the drivers and OOBC software next, as well as (optionally) ITNCM Reports. For more information, see “Installing drivers” on page 48, “Installing OOBC” on page 62, and“Installing ITNCM-Reports” on page 42.

After that, you perform a number of post-installation procedures, such as safeguarding the keystore and increasing the Java Heap size. For information on these and other configuration tasks, see Chapter 3, “Configuring,” on page 67.

If this installation was the first step in the installation of a distributed architecture on several servers, you install the worker servers next.

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.

## Installing the product in silent mode

Silent installation requires an XML response file that defines the installation configuration. Silent mode is useful if you want identical installation configurations on multiple workstations.

Set the necessary user permissions for your intended installation directories. See the “IBM Installation Manager overview” on page 21, and the information under 'About this task'.

Close and stop all system processes before beginning silent installation. This includes all monitoring software, databases, and third party packages.

Performing the installation requires full administrative access to the entire system. Full system authorization to read, write, add, and delete all system files and applications must be established before beginning the installation.

Perform the following checks before installation:

**Defining sufficient memory (or SWAP) space**
There can be issues installing Netcool Configuration Manager if there is not enough available memory or SWAP space. This problem can be eliminated by doing one of the following:

- Allocate more SWAP space.
- Separate SWAP and `/tmp`.
- Allocate more space to `/tmp`.

**Setting sufficient Oracle process limits (for Oracle database use only)**
There may be issues with Oracle responsiveness if there is not a sufficient amount of processes running. The Oracle process limit must be at least 55 processes per worker server that will be deployed.

**Synchronizing server timings**
It is a requirement that all servers must have their times synced to within 10 seconds of each other for correct operation. Each server can be synced by setting up the NTP protocol.

**Increasing WebSphere Application Server memory on Linux**

**Note:** Applies only to a scenario where a GUI server or Tivoli Common Reporting is being installed onto a Linux platform.

When installing a Netcool Configuration Manager GUI server or Tivoli Common Reporting onto a Linux platform, set **nproc** to a value of 131072 to safely account for all the forked threads within processes that could be created.

For more information, see the following technote: http://www-01.ibm.com/support/docview.wss?uid=swg21648497

The steps for starting Installation Manager differ depending on the user mode in which it was installed.

The Installation Manager console installation steps are common to all user modes and operating systems. Take note of the following information about permissions on the supported operating systems:

- Installation Manager takes account of your current umask settings when it sets the permissions mode of the files and directories that it installs. If you use Administrator mode or Nonadministrator mode and your umask is 0, Installation Manager uses a umask of 22. If you use Group mode, Installation Manager ignores any group bits that are set and uses a umask of 2 if the resulting value is 0.
- Run one of the following installations without actually installing the product, and record the installation settings:

  **GUI installation**
  For example:

  ```
  IBMIM -record /home/icosuser/response_files/Presentation_Worker.xml

  -skipInstall /tmp/skipInstall
  ```

  **Console installation**
  Follow the steps in "Installing in console mode" on page 37 and generate a silent Install file instead of installing the product.

The response file includes the location of the repository from which the installation package is obtained.

- You can specify a local or remote repository.
- You can have Installation Manager download the package from IBM Passport Advantage.

**Tip:** Response Files are not transferable across different platforms. For example, a response file generated on a Linux machine can not be used on an AIX machine.

**Attention:** When using the IBM Installation Manager to install zLinux, you may receive a number of warnings. Ignore these and proceed with the installation.

1. Record the response file or files.
2. Read the `license.txt` license agreement file, which you can find in the installation package (in `/native/license_version.zip`).
3. Start the silent installation using the following command, as the `icosuser` user:
   `./imcl -input` *`response_file`* `-silent -acceptlicense [-log` *`full_path_to_log_file`*`]`
   Where *`response_file`* is the directory path to the response file that you recorded in step one, and *`full_path_to_log_file`* is the location in which the installation log is created.

**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='/home/icosuser/IBM/IMShared'/>
  </variables>
  <server>
    <repository location='/home/icosuser/repo'/>
  </server>
  <profile id='Netcool Configuration Manager' installLocation='/opt/IBM/tivoli/netcool/ncm'>
    <data key='eclipseLocation' value='/opt/IBM/tivoli/netcool/ncm'/>
    <data key='user.import.profile' value='false'/>
    <!--Update architecture to linux for RHEl and SUSE-->
    <data key='cic.selector.os' value='aix'/>
    <!--Updae architecture to x86_64 for RHEl and SUSE-->
    <data key='cic.selector.arch' value='ppc64'/>
    <data key='cic.selector.ws' value='gtk'/>
    <data key='cic.selector.nl' value='en'/>
    <data key='user.tcr.was.user.name' value='smadmin'/>
    <data key='user.tcr.was.user.password' value=''/>
    <data key='user.tmp.tcr.was.password' value=''/>
    <data key='user.itncm.reports.update' value='false'/>
    <data key='user.tmp.ins.loc' value=''/>
    <data key='user.tcr.jazz.home' value=''/>
    <data key='user.tcr.was.profile.path' value=''/>
    <data key='user.tcr.was.server.name' value=''/>
    <data key='user.itncm.jdbc.type' value='oracle12'/>
    <data key='user.itncm.jdbc.driver' value='oracle.jdbc.driver.OracleDriver'/>
    <data key='user.itncm.jdbc.url' value='jdbc:oracle:thin:@ServerLocation:1521/itncm'/>
    <data key='user.itncm.jdbc.credentials.password' value=''/>
    <data key='user.itncm.jdbc.schema.name' value='itncm'/>
    <data key='user.itncm.jdbc.credentials.user' value='DBUSER'/>
    <data key='user.itncm.jdbc.host' value='ServerLocation'/>
    <data key='user.itncm.jdbc.port' value='1521'/>
```

```
    <data key='user.itncm.jdbc.type.prop' value='oracle'/>
    <data key='user.itncm.user.operator.password' value=''/>
    <!--Set to false for a worker Installation-->
    <data key='user.itncm.gui.active' value='true'/>
    <data key='user.temp.confirm.itnm.pass' value=''/>
    <data key='user.itncm.ftp.credentials.password' value=''/>
    <data key='user.itncm.ftp.host' value='localhost'/>
    <data key='user.itncm.pbcm.log.error.port' value='8112'/>
    <data key='user.itncm.log.port' value='8102'/>
    <data key='user.itncm.ftp.dir' value='/home/icosftp'/>
    <data key='user.itncm.pbcm.log.listen.port' value='8114'/>
    <data key='user.itncm.pbcm.admin.port' value='8110'/>
    <data key='user.itncm.nmentitymapping.port' value='16311'/>
    <data key='user.temp.confirm.ftp.pass' value='icosftp'/>
    <!--Update to WORKER,TRUE,FALSE,DUAL for a worker server-->
    <data key='user.itncm.server.platform.config' value='PRESENTATION,TRUE,FALSE,DUAL'/>
    <data key='user.itncm.root.realm' value='ITNCM'/>
    <data key='user.itncm.log.listen.port' value='8103'/>
    <data key='user.itncm.pbcm.active' value='true'/>
    <data key='user.itncm.user.observer.password' value=''/>
    <data key='user.itncm.user.administrator.password' value=''/>
    <data key='user.itncm.admin.port' value='8101'/>
    <data key='user.itncm.idt.main.server' value='true'/>
    <data key='user.core.smtp.server' value='localhost'/>
    <data key='user.itncm.job.type' value='update'/>
    <data key='user.itncm.nmentitymapping.hostname' value='localhost'/>
    <data key='user.itncm.ftp.credentials.user' value='icosftp'/>
    <data key='user.itncm.nmentitymapping.nm.password' value=''/>
    <data key='user.itncm.pbcm.log.test.port' value='8115'/>
    <data key='user.itncm.main.install.dir' value='/opt/IBM/tivoli/netcool/ncm'/>
    <data key='user.itncm.pbcm.log.debug.port' value='8111'/>
    <data key='user.itncm.nmentitymapping.nm.importrealm' value='ITNCM/@DOMAINNAME'/>
    <data key='user.itncm.worker.linked.rg' value='false'/>
    <data key='user.itncm.admin.manager.server.name' value='instanceName'/>
    <data key='user.itncm.nmentitymapping.base.url' value=''/>
    <data key='user.itncm.pbcm.log.info.port' value='8113'/>
    <data key='user.itncm.worker.active' value='true'/>
    <data key='user.itncm.integrated' value='false'/>
    <data key='user.itncm.idt.port' value='8104'/>
    <data key='user.itncm.nmentitymapping.nm.user' value='itnmadmin'/>
    <data key='user.itncm.server.was.node' value='JazzSMNode01'/>
    <data key='user.was.server.name' value='server1'/>
    <data key='user.was.profile.path' value='/opt/IBM/JazzSM/profile'/>
    <data key='user.was.appserver.dir' value='/opt/IBM/WebSphere/AppServer'/>
    <data key='user.itncm.server.ssl.port' value='16311'/>
    <data key='user.itncm.server.was.cell' value='JazzSMNode01Cell'/>
    <data key='user.was.user.password' value=''/>
    <data key='user.was.user.name' value='smadmin'/>
    <data key='user.tmp.was.password' value=''/>
    <data key='user.itncm.server.http.port' value='16310'/>
    <data key='user.jazz.home' value='/opt/IBM/JazzSM'/>
    <data key='user.was.profile.name' value='JazzSMProfile'/>
  </profile>
  <install modify='false'>
    <!-- Netcool Configuration Manager 6.4.2.0  update features to Jre for a worker server-->
    <offering profile='Netcool Configuration Manager_1' id='com.ibm.tivoli.itncm.configurationmanager.server'
version='6.4.2.20160202_1049' features='liberty' 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='false'/>
  <preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Next, you perform a number of post-installation procedures. For example, if you did not set the **key='user.itncm.jdbc.schema.initialload'** property value of the response file to `true`, you must manually load the schema before you can start Netcool Configuration Manager.

**Warning:** In an upgrade scenario, or if additional presentation servers are being installed, you may need to manually change this value to `false`.

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.

**Related tasks**

Loading the databases
Loading the database for Netcool Configuration Manager builds the schemas and loads the content. You can load the databases during installation, or separately at a later stage.

Configuring reporting on a stand-alone installation
If Netcool Configuration Manager Reporting has been installed stand-alone, there are a number of configuration steps which must be followed to access the reports.

## Installing ITNCM-Reports

If you are not integrating with Network Manager, which ships with its own version of DASH, you must install ITNCM-Reports separately in order to access the reporting functionality.

**Restriction:** Fix Pack 3 This topic does not apply to Netcool Configuration Manager installations on Linux on System z.

Ensure you have completed installation of the following prerequisites:

- Netcool Configuration Manager
- Tivoli Common Reporting

**Restriction:** You must install ITNCM-Reports as the same user that installed Netcool Configuration Manager.

1. Log on to the platform as the same user that installed Netcool Configuration Manager, and perform one of the following steps to launch the installer:

   **GUI Mode**
   Change to the `/eclipse` subdirectory of the Installation Manager Group installation directory, and use the following command to start Installation Manager:

   ```
   ./IBMIM
   ```

   **Console Mode**
   Change to the `/eclipse/tools` subdirectory of the Installation Manager installation director.

   Use one of the following commands to start Installation Manager:

   ```
   ./imcl -c
   ```

   ```
   ./imcl -consoleMode
   ```

2. 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**, then **OK**.

3. In the main **Installation Manager** window, click **Install**, and then follow the installation wizard instructions.
4. Select the **Reporting Services environment** packages, and then provide the following information when prompted by the wizard:
   - Read and accept the license agreement.
   - Specify an Installation Manager shared directory, or accept the default directory.
   - Specify an installation directory for the product, or accept the default directory.
   - Select the Reports feature.
   - Provide connection information about the Netcool Configuration Manager database:
     - Sid/service name/database name(db2)
     - The DB hostname
     - Port
     - Username
     - Password
   - Provide information specific to Tivoli Common Reporting
     - Specify whether it is an integrated or a standalone installation of Netcool Configuration Manager.
     - Provide the installation directory for Tivoli Common Reporting (typically `/opt/IBM/JazzSM`).
     - Provide the correct user name and password for JazzSM.
   - Complete the installation.

Post-installation steps: DB2 configuration

5. 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.

6. Add 'source $HOME/sqllib/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.

7. 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'**.

The installation is complete and Netcool Configuration Manager Reports have been installed into Tivoli Common Reporting.

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 the 'Configuring single sign-on' topic in the *IBM Tivoli Netcool Configuration Manager Integration Guide*.

Ensure Netcool Configuration Manager users have access to HTML items in Tivoli Common Reporting. For more information, see the following Tivoli Common Reporting procedure: https://www-304.ibm.com/support/knowledgecenter/SSNE44_5.2.0/com.ibm.tpc_V52.doc/fqz0_t_reports_security_restricting_capabilities.html

Ensure Netcool Configuration Manager users have access to the ITNCM Reports in the public folder.

1. From the **Main Reporting** window, select **Set Properties** and the **Permissions** tab.
2. Click **Add**, then select **Cognos**, and the group of users to be added to the Selected Entries list.
3. Click **OK**, then select the required group name, and then add **Read**, **Execute** and **Traverse** permissions.
4. Click **OK**.

Ensure Netcool Configuration Manager users have Traverse and Execute access to Report Studio.

For information on how to add user accounts to ITNCM-Reports, see "Configuring reporting on a stand-alone installation" on page 88

**Related tasks**

Installing a GUI and worker server
You install Netcool Configuration Manager either on a single server, or on several servers in a distributed architecture. The installation of a GUI and worker server can be part of a stand-alone installation on a single server, or it can be the first step in the installation of a distributed architecture on several servers.

Installing a worker server only
You install a Netcool Configuration Manager worker server as part of a distributed architecture deployed on one or more servers. You install one or more worker servers after having completed the installation of one or more GUI and worker servers.

Loading the databases
Loading the database for Netcool Configuration Manager builds the schemas and loads the content. You can load the databases during installation, or separately at a later stage.

Configuring reporting on a stand-alone installation
If Netcool Configuration Manager Reporting has been installed stand-alone, there are a number of configuration steps which must be followed to access the reports.

## Installing ITNCM-Reports in silent mode

If you are not integrating with Network Manager, which ships with its own version of DASH, you must install ITNCM-Reports separately in order to access the reporting functionality.

**Restriction:** Fix Pack 3 This topic does not apply to Netcool Configuration Manager installations on Linux on System z.

Ensure you have completed installation of the following prerequisites:

- Netcool Configuration Manager

- Tivoli Common Reporting

**Restriction:** You must install ITNCM-Reports as the same user that installed Netcool Configuration Manager.

1. Log on to the platform as the same user that installed Netcool Configuration Manager, and perform one of the following steps to launch the installer:

   **GUI Mode**
   Change to the `/eclipse` subdirectory of the Installation Manager Group installation directory, and use the following command to start Installation Manager:

   ```
   ./IBMIM -record responseFile -skipInstall agentDataLocation
   ```

   **Console Mode**
   Change to the `/eclipse/tools` subdirectory of the Installation Manager installation director.

   Use one of the following commands to start Installation Manager:

   ```
   ./imcl -c
   ```

   ```
   ./imcl -consoleMode
   ```

2. 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**, then **OK**.
3. In the main **Installation Manager** window, click **Install**, and then follow the installation wizard instructions.
4. Select the **Reporting Services environment** packages, and then provide the following information when prompted by the wizard:
   - Read and accept the license agreement.
   - Specify an Installation Manager shared directory, or accept the default directory.
   - Specify an installation directory for the product, or accept the default directory.
   - Select the **Reports** feature.
   - Provide connection information about the Netcool Configuration Manager database:
     – Sid/service name/database name(db2)
     – The DB hostname
     – Port
     – Username
     – Password
   - Provide information specific to Tivoli Common Reporting
     – Specify whether it is an integrated or a standalone installation of Netcool Configuration Manager.

- Provide the installation directory for Tivoli Common Reporting (typically `/opt/IBM/JazzSM`).
- Provide the correct user name and password for JazzSM.

- Generate the response file:

  **If in Console mode**
  Select 'G' to generate a silent install file.

  **If in GUI mode and having selected `-skipInstall`**
  Select **Install** and the installation will be skipped and the response file generated.

To run the silent install file

5. Change to the `/eclipse/tools` subdirectory of the Installation Manager installation directory, and enter the following command:

```
./imcl input path_name/responseFile.xml  -acceptLicense -showProgess
```

Post-installation steps: DB2 configuration

6. 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.

7. Add "source $HOME/sqllib/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.

8. 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'`**.

The installation is complete and Netcool Configuration Manager Reports have been installed into Tivoli Common Reporting.

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

```
ls
<?xml version='1.0' encoding='UTF-8'?>
<agent-input>
  <variables>
    <variable name='sharedLocation' value='/home/icosuser//IBM/IBMIMShared'/>
  </variables>
  <server>
    <repository location='/home/icosuser/Repo'/>
  </server>
  <profile id='Netcool Configuration Manager' installLocation='/opt/IBM/tivoli/netcool/ncm'>
    <data key='eclipseLocation' value='/opt/IBM/tivoli/netcool/ncm'/>
    <data key='user.import.profile' value='false'/>
    <!--Update architecture 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.itncm.jdbc.type' value='oracle12'/>
    <data key='user.itncm.jdbc.driver' value='oracle.jdbc.driver.OracleDriver'/>
    <data key='user.itncm.jdbc.url' value='jdbc:oracle:thin:@ServerLocation:1521/itncm'/>
    <data key='user.itncm.jdbc.credentials.password' value=''/>
    <data key='user.itncm.jdbc.schema.name' value='itncm'/>
    <data key='user.itncm.jdbc.credentials.user' value='DBUSER'/>
    <data key='user.itncm.jdbc.host' value='ServerLocation'/>
    <data key='user.itncm.jdbc.port' value='1521'/>
    <data key='user.itncm.jdbc.type.prop' value='oracle'/>
    <data key='user.tcr.was.user.name' value='smadmin'/>
    <data key='user.tcr.was.user.password' value=''/>
    <data key='user.tcr.app.server.home' value='/opt/IBM/WebSphere/AppServer'/>
    <data key='user.tmp.tcr.was.password' value=''/>
    <data key='user.itncm.reports.update' value='false'/>
    <data key='user.tmp.ins.loc' value=''/>
    <data key='user.tcr.WAS_SERVER_NAME' value='server1'/>
    <data key='user.tcr.jazz.home' value='/opt/IBM/JazzSM'/>
    <!--Update to Y for an integrated reports install with NM-->
    <data key='user.tcr.reports.integrated' value='N'/>
    <data key='user.tcr.was.profile.path' value='/opt/IBM/JazzSM/profile'/>
    <data key='user.tcr.was.server.name' value='server1'/>
    <data key='cic.selector.nl' value='en'/>
  </profile>
  <install modify='false'>
    <!-- Netcool Configuration Manager V6.4.2.0 -->
    <offering profile='Netcool Configuration Manager' id='com.ibm.tivoli.itncm.configurationmanager.server'
version='6.4.2.20160202_1049' features='Reports' 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>
```

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 the 'Configuring single sign-on' topic in the *IBM Tivoli Netcool Configuration Manager Integration Guide*.

Ensure Netcool Configuration Manager users have access to HTML items in Tivoli Common Reporting. For more information, see the following Tivoli Common Reporting procedure: https://www-304.ibm.com/support/knowledgecenter/SSNE44_5.2.0/com.ibm.tpc_V52.doc/fqz0_t_reports_security_restricting_capabilities.html

Ensure Netcool Configuration Manager users have access to the ITNCM Reports in the public folder.

1. From the **Main Reporting** window, select **Set Properties** and the **Permissions** tab.
2. Click **Add**, then select **Cognos**, and the group of users to be added to the Selected Entries list.

3. Click **OK**, then select the required group name, and then add **Read**, **Execute** and **Traverse** permissions.
4. Click **OK**.

Ensure Netcool Configuration Manager users have Traverse and Execute access to Report Studio.

For information on how to add user accounts to ITNCM-Reports, see "Configuring reporting on a stand-alone installation" on page 88

**Related tasks**

Loading the databases
Loading the database for Netcool Configuration Manager builds the schemas and loads the content. You can load the databases during installation, or separately at a later stage.

Configuring reporting on a stand-alone installation
If Netcool Configuration Manager Reporting has been installed stand-alone, there are a number of configuration steps which must be followed to access the reports.

## Fix Pack 4 [zLinux] Installing Cognos Analytics

If you are installing Netcool Configuration Manager on Linux on System z, and require access to ITNCM Reports, you must install Cognos Analytics.

Ensure you have obtained Cognos 11.0.5.0 or later, and have installed Netcool Configuration Manager.

You can find the Cognos Analytics Version 11.0 Knowledge Center at the following location: https://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.cbi.doc/welcome.html

Preparing to install

1. Prepare your database, set up your users, and configure your web browser for use with Cognos Analytics. Follow the instructions in the Cognos Analytics Knowledge Center: https://www.ibm.com/support/knowledgecenter/en/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.inst_cr_winux.doc/c_settinguptheenvironment.html#SettingUptheEnvironment
2. Prepare the server components: https://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.inst_cr_winux.doc/t_instsrvrunix.html#instsrvrUNIX
3. Install the DB2 32bit runtime client on the same machine that Cognos Analytics 11.0.5 is installed on.

   You can find suggested settings for creating the content store in DB2 on zLinux at the following location: https://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.inst_cr_winux.doc/c_guidelines_db2_lux_content_store.html

| Option | Description |
|---|---|
| **Source the db2 profile** | Create a profile that sources the sqllib/db2profile from the DB2 user's home directory. |
| | |

## ITNCM Housekeeping

IBM Tivoli Netcool Configuration Manager's database will continue to increase in size indefinitely unless housekeeping is implemented.

For more information, see https://www.ibm.com/support/pages/what-database-housekeeping-should-i-set-after-deploying-itncm.

# Installing drivers

Use this information to install Netcool Configuration Manager drivers.

**Important:** Always refer to driver release notes before installing drivers in case of additional installation requirements.

**Related tasks**

Preparing to install
Before you install or upgrade to a new version of Netcool Configuration Manager, you must take note of a number of prerequisites.

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.

# Drivers overview

The drivers supplied with Netcool Configuration Manager, or obtained from the IBM Passport Advantage Web site, enable Netcool Configuration Manager to communicate with the different devices used within your network. Drivers are installed by the driver installer and consist of scripts and rules used by the application when communicating with the devices. After driver installation, you update your devices with the new drivers.

**Note:** The Netcool Configuration Manager Server might be slow to start after installing several individual drivers, because it revalidates the drivers installed on the system. During this startup period the worker server does not pick up any work.

## Driver capabilities

Drivers are available for use with Netcool Configuration Manager that provide either Standard mode or SmartModel mode capabilities. Your driver requirements are determined by the devices in your network.

**Note:** Before selecting the driver to install, ensure that you have obtained the required device information from your network administrator or equivalent network device expert. Also view the drivers release notes packaged with the drivers for additional information.

These drivers can be installed by downloading them from the IBM Passport Advantage Web site: http://www-01.ibm.com/software/howtobuy/passportadvantage/

**Standard drivers**

When using Standard drivers, Netcool Configuration Manager limits the possible operations that can be performed on the device. Refer to *Custom driver capabilities* in the *IBM Tivoli Netcool Configuration Manager Administration Guide* for more details.

**SmartModel drivers**

When using SmartModel drivers, Netcool Configuration Manager communicates with a device using a tailored set of scripts and metadata for access to an individual device.

SmartModel drivers can also be used in 'Standard' mode, where the generic set of scripts and metadata can be used to access a device if preferred. SmartModel drivers can be used to create Netcool Configuration Manager core compliance modeled definitions.

Drivers are initially installed in 'Standard' mode, and need to be upgraded to SmartModel mode using the SmartModel upgrade tool before the full SmartModel features on the device can be utilised.

Three options for installing drivers are provided: Graphical User Interface (GUI), the console (CLI), or Silent installation.

**Individual installers**

Individual installers provide a method to install a single driver with support for a small set of devices, thereby allowing for smaller downloads.

Individual installers are available for all drivers.

Individual installers may also be made available when support for new devices become available, or by IBM Support to resolve issues with a given driver.

**Important: If you are using command set groups:** When adding or removing Netcool Configuration Manager drivers, you must reevaluate all existing command set groups. Use the ReevaluateGroups option that is part of the icosutil utility located in the `ncm_install_directory/bin` directory to do so. This utility determines if the addition or deletion of drivers has an impact on the coverage of the command set

groups and updates them accordingly. In addition to running the ReevaluateGroups utility following the addition or removal of drivers, you should also manually review the coverage of the command set groups after adding or removing drivers.

## Upgrading to SmartModel

Drivers can be used in SmartModel mode or Standard mode. Drivers installed with Netcool Configuration Manager default to Standard mode until the SmartModel upgrade tool has been run.

The SmartModel installer package also deploys the SmartModel upgrade tool to allow drivers to be upgraded from Standard to SmartModel mode. Once upgraded to SmartModel mode it is not possible to downgrade a driver from SmartModel mode to Standard mode.

Drivers can be upgraded to SmartModel mode either on an individual basis, or for all drivers on the system.

**Tip:** You should perform a driver update of 'All Configurations' from the Netcool Configuration Manager GUI for all devices that have been upgraded from Standard to SmartModel.

## Driver versioning after installation

After installing new Drivers, existing devices may be marked to indicate a newer version of the Driver has been installed. Devices which have been using the old Driver configuration may have an orange or red arrow icon against them, which indicates that a newer version of the same driver or a more optimal driver is installed and available for the device, and they need a Driver update to update to the newer driver. To perform this, select the network resource, right-click, and select Driver Update. Alternately, from the main Netcool Configuration Manager screen, select the search icon (the magnifier), and toggle the *Search by Driver* tab, then select the *Non-Optimal* option and click *Search*. You can then select all or some of the network resources for Driver Update.

Command Sets using the original driver configs are also affected when new drivers are installed. Refer to *Command Set Migration (CmdSetMigration)* in the *IBM Tivoli Netcool Configuration Manager Administration Guide* for additional information on Command Set Migration.

## Individual driver removal

To remove an individual driver, or a group of drivers, perform the following steps:

1. In the Netcool Configuration Manager GUI, open **Systems Manager** > **Drivers**.
2. If the status of the driver(s) to be removed is `Active`, right-click the driver(s), and click **Set Driver Inactive**.
3. Right click the driver(s) to be removed, and click **Delete Driver**.

## Driver uninstallers

When drivers are installed, a corresponding uninstaller named `Uninstall_ITNCM <Drivers Package Name> Drivers` is placed in a directory named `<ITNCM_INSTALLATION_DIRECTORY>/Uninstall_ITNCM <Drivers Package Name> Drivers`.

**CAUTION:** Uninstallers remove all drivers installed by their corresponding installer, including those that are in active use by Netcool Configuration Manager. Consequently, driver uninstallers should only be run when Netcool Configuration Manager is being completely removed from a server.

**Note:** Driver uninstaller directories are not removed during an uninstall of Netcool Configuration Manager, and must be deleted manually.

# Driver installation prerequisites

To ensure that the system on which you are installing the drivers is compatible, there are a number of requirements.

## Netcool Configuration Manager

Ensure you have installed Netcool Configuration Manager before installing the drivers.

If drivers are to be installed centrally, then a Java Runtime Environment is required; otherwise the JRE included with the Netcool Configuration Manager installation is used.

Netcool Configuration Manager installation examples use the default directory path of `/opt/IBM/tivoli/netcool/ncm`. You can override this with a path appropriate to your own requirements.

## Unix utilities

Ensure that the Unix `sort` utility is present on the UNIX server.

## Driver installer space requirements

There can be issues installing the Drivers if there is not enough free disk space. In addition to the core Netcool Configuration Manager requirements, ensure that you have 40 GB of free disk space for driver installation.

## Driver installer directory requirements

The driver installation copies scripts to, and executes scripts from, the `/tmp` directory. Ensure that the `/tmp` directory is **not** mounted using the `noexec` flag, or else driver installation fails.

## Driver installer Java requirements

For Drivers 23, Netcool Configuration Manager must be in a Java 1.8 environment. Perform either of the following two upgrades:

1. Upgrade Netcool Configuration Manager to version 6.4.2.8 or later. See “Upgrading Netcool Configuration Manager to version 6.4.2.0” on page 109.
2. Upgrade the Websphere Java SDK to version 1.8, using the following procedure.

## Upgrading Websphere Java SDK to version 1.8

1. Upgrade IBM WebSphere Application Server version to 8.5.5.9, if it is currently at a lower version, otherwise the SDK upgrade fails with an error.
   a. Download and install IBM WebSphere Application Server 8.5.5.9 from the following link: https://www.ibm.com/support/pages/node/586313
   b. Select **IBM WebSphere Application Server version 8.5.5.9** from the list in IBM Installation Manager.
2. Stop Netcool Configuration Manager by running the following command:

   ```
   NCM_Home/bin#./itncm stop
   ```

3. Check the available and enabled Java versions by running the following commands in the `WebSphere_install_directory/WebSphere/AppServer/bin/` directory:
   a. Run the `./managesdk.sh -listAvailable` command to view the available Java versions associated with IBM WebSphere Application Server. The following example output shows that

there are three Java versions available with the installed version of IBM WebSphere Application Server:

```
CWSDK1003I: Available SDKs:
    CWSDK1005I: SDK name: 1.8_6
    CWSDK1005I: SDK name: 1.6_64
    CWSDK1005I: SDK name: 1.7_64
    CWSDK1001I: Successfully performed the requested managesdk task
```

b. Run the command `./managesdk.sh -listEnabledProfileAll` to show the current IBM WebSphere Application Server Java version used by Netcool Configuration Manager. The example output below shows that Java SDK 1.7 is enabled and that Netcool Configuration Manager is running on the same Java SDK 1.7:

```
CWSDK1004I: Profile JazzSMProfile :
    CWSDK1006I: PROFILE_COMMAND_SDK = 1.7_64
    CWSDK1008I: Node JazzSMNode01 SDK name: 1.7_64
    CWSDK1009I: Server server1 SDK name: 1.7_64
    CWSDK1001I: Successfully performed the requested managesdk task.
```

4. Download and install the IBM WebSphere Application Server Java SDK version 8.0.5.27 from the following location: https://www.ibm.com/support/fixcentral/swg/downloadFixes?parent=ibm~WebSphere&product=ibm/WebSphere/WebSphere+Application+Server&release=8.5.5.9&platform=All&function=fixId&fixids=8.0.5.27-WS-IBMWASJAVA-part2,8.0.5.27-WS-IBMWASJAVA-part1&includeRequisites=1&includeSupersedes=0&downloadMethod=http&source=fc
5. During installation, select **IBM WebSphere SDK Java Technology Edition (Optional) version 8.0.5.27** to upgrade the Java SDK to 1.8.
6. After upgrading, point the symlink of the Netcool Configuration Manager JRE, which is in the NCM installation directory, (by default, `/opt/IBM/tivoli/netcool/ncm`) to Java 1.8:
   a. Back up the existing symlink by renaming the existing directory. For example, `ln -s /opt/IBM/netcool/WebSphere/AppServer/java_1.7_64 jre_1`
   b. Remove the original symlink by removing the `jre` folder from the Netcool Configuration Manager installation directory. For example, use the following command: `rm -rf jre`.
   c. Create a new symlink that points to the Java 1.8 SDK from the NCM installation directory. For example, `ln -s /opt/IBM/netcool/WebSphere/AppServer/java_1.8_64 jre`
   d. When the new symlink is created successfully, remove the backup symlink that you created in step "6.a" on page 52.
7. Enable the JAZZSM profile to point to the Java SDK 1.8 by using the following command.

   ```
   ./managesdk.sh -enableProfile -profileName JazzSMProfile -sdkname version -verbose
   ```

   Where *version* is the Java SDK 1.8 version, for example, `1.8_64`.
8. Start Netcool Configuration Manager.
9. Check the Java version that Netcool Configuration Manager is using by running the following commands:
   a.
   ```
   /opt/IBM/JazzSM/profile/bin/managesdk.sh -listEnabledProfileAll -verbose
   ```
   b.
   ```
   /opt/IBM/tivoli/netcool/ncm/jre/bin/javac -version
   ```
10. If the Java version on the standalone server is 1.8, you must update the unlimited jurisdiction policy files:

a. Rename the `local_policy.jar` and `US_export_policy.jar` files in the path `/opt/IBM/tivoli/netcool/ncm/jre/jre/lib/security/`.
b. Copy the Unlimited jurisdiction policy files from the presentation server for which you upgraded the SDK version to 1.8, in the path `/opt/IBM/tivoli/netcool/ncm/jre/jre/lib/security/policy/unlimited/`.
c. After replacing the jar files, restart the standalone Worker server.

11. For a distributed system, verify the Java version used by Netcool Configuration Manager. If it is not using Java 1.8, contact IBM support.

# Installing standard drivers

Standard drivers can be installed using individual driver installers either via command line (CLI) or GUI, or silently.

## Installing standard drivers via CLI

This task describes how to install the standard drivers using the command line interface (CLI).

Access the `/opt/IBM/tivoli/netcool/ncm/bin` directory, and execute the stop server command: `itncm.sh stop`

1. Log on to the platform as the user that installed Netcool Configuration Manager.
2. Access the directory to which you downloaded the installer.
3. Enter the following command:

```
sh ./driverversion.bin LAX_VM /opt/IBM/tivoli/netcool/ncm/jre/bin/java -i console
```

   where *`driverversion.bin`* is the name of the driver to be installed.
4. Click **Enter** to begin the installation, accept the license agreement, and continue through the prompts.

You must restart Netcool Configuration Manager after the drivers have been installed. Execute the start server command:
`/opt/IBM/tivoli/netcool/ncm/bin/itncm.sh start`

## Installing standard drivers using the GUI

This task describes how to install the standard software drivers using the graphical user interface (GUI).

This task describes how to install the standard drivers using the GUI.

1. Access the `/opt/IBM/tivoli/netcool/ncm/bin` directory, and execute the stop server command as follows:
   `/opt/IBM/tivoli/netcool/ncm/bin/itncm.sh stop`
2. Log on to the platform as the user that installed Netcool Configuration Manager.
3. Access the directory to which you downloaded the installer.
4. Enter the following command:

```
sh ./driverversion.bin LAX_VM /opt/IBM/tivoli/netcool/ncm/jre/bin/java -i gui
```

   where *`driverversion.bin`* is the name of the driver to be installed.
5. To accept the license agreement, select **Next**.
6. Choose the installation directory, or accept the default, then click **Next**.
   The **Pre-Installation Summary** window is displayed.
7. Review the installation details and click **Install**.
   The installation proceeds and when complete, the **Install Complete** window is displayed.
8. Click **Done** to exit the installer.

- Netcool Configuration Manager must be restarted after the drivers have been installed. Execute the start server command:
  `/opt/IBM/tivoli/netcool/ncm/bin/itncm.sh start`
- To ensure that all servers in a distributed environment have the same drivers installed, it is useful to check the driver consistency on all servers. Navigate to the Systems Manager, and access Servers. Driver consistency is indicated by the **Driver Checksum** field against each server.

## Installing standard drivers silently

This task describes how to install the standard drivers using the CLI silent installation facility.

1. Log on to the platform as the user that installed Netcool Configuration Manager.
2. Access the `/opt/IBM/tivoli/netcool/ncm/bin` directory, and execute the stop server command:
   `itncm.sh stop`
3. Access the directory containing the driver installer file.
4. Create an `ITNCM.properties` file that contains `$LICENSE_ACCEPTED$=true`.
5. Enter the following command:

   ```
   sh ./driverversion.bin LAX_VM /opt/IBM/tivoli/netcool/ncm/jre/bin/java -i silent -f
   ITNCM.properties
   ```

   where *driverversion.bin* is the name of the driver to be installed.
6. Press Enter.

Netcool Configuration Manager must be restarted after the drivers have been installed. Execute the start server command:
`/opt/IBM/tivoli/netcool/ncm/bin/itncm.sh start`
To ensure that all servers in a distributed environment have the same drivers installed, it is useful to check the driver consistency on all servers. Navigate to the Systems Manager, and access Servers. Driver consistency is indicated by the **Driver Checksum** field against each server.

## Installing multiple individual device drivers silently

This task describes how to install individual device drivers silently using the command line drivers bulk install script (`drivers_bulk_install.sh`).

**Note:** Before using the bulk installer, at least one driver must be installed on the system so that the `drivers_bulk_installer.sh` script is present in the `install_dir/drivers/bin` directory.

1. Log on to the platform as the user that installed Netcool Configuration Manager.
2. Download the individual driver installers to be installed, and place them in a single directory on the server where you will perform the installation.
3. Copy `drivers_bulk_install.sh` from the `install_dir/drivers/bin` directory to the directory where the driver installers are located.
4. Open or create the file `ITNCM.properties` in a text editor.
5. Edit or create the following installation parameters:

   **$DRIVERS_INSTALL_DIR$**
   You define the directory where the driver subdirectory will be installed, for example:

   `$DRIVERS_INSTALL_DIR$=/opt/IBM/tivoli/netcool/ncm`

   **$LICENSE_ACCEPTED$**
   You must accept the license, or the installation will not proceed. To install, set `$LICENSE_ACCEPTED$=true`
6. Access the `/opt/IBM/tivoli/netcool/ncm/bin` directory, and execute the stop server command:
   `itncm.sh stop`
7. Access the directory containing the downloaded drivers installers, the `ITNCM.properties` file, and the bulk install script and run the installation:

```
./drivers_bulk_install.sh <driver installers dir> ITNCM.properties
```

The silent installation proceeds based on the parameters you have defined in the `ITNCMProperties.txt` file.

This is an example of the installation output with two drivers being installed. Here, the *<driver installers dir>* directory is denoted by '`.`'.

```
[icosuser@ncm-server drivers]# ./drivers_bulk_install.sh . ITNCMProperties.txt
Starting bulk installation

Using download directory: .
Using silent properties: ITNCMProperties.txt
Using derived Java executable: /opt/IBM/tivoli/netcool/ncm/jre/bin/java

Processing ./CiscoRouter76xxS72033PK9SVMZ122.bin
Installation: Successful. (Summary: 119 Successes, 0 Warnings,
0 NonFatalErrors, 0 FatalErrors)
Completed processing ./CiscoRouter76xxS72033PK9SVMZ122.bin

Processing ./CiscoRouterISRG215x.bin
Installation: Successful. (Summary: 119 Successes, 0 Warnings,
0 NonFatalErrors, 0 FatalErrors)
Completed processing ./CiscoRouterISRG215x.bin

Totals: 2 Successes, 0 Fails, 0 Undetermined

Ended bulk installation
```

Netcool Configuration Manager must be restarted after the drivers have been installed. Execute the start server command:
`/opt/IBM/tivoli/netcool/ncm/bin/itncm.sh start`
Once Netcool Configuration Manager has restarted, any newly installed SmartModel drivers will be recognized and catalogued, but they will be in Standard mode. To switch them to SmartModel mode, follow the documentation at “Changing SmartModel drivers from Standard to SmartModel mode” on page 58.
To ensure that all servers in a distributed environment have the same drivers installed, it is useful to check the driver consistency on all servers. Navigate to the Systems Manager, and access Servers. Driver consistency is indicated by the **Driver Checksum** field against each server.

# Installing SmartModel drivers

SmartModel drivers are installed using individual driver installers.

## Installing individual SmartModel drivers via CLI

Individual driver installers are made available as part of the SmartModel packages, and might also be made available by IBM Support to resolve issues with a given driver when supplied with such an installer. This task describes how to install the individual SmartModel drivers using the command line interface (CLI).

Access the `/opt/IBM/tivoli/netcool/ncm/bin` directory, and execute the stop server command:
`itncm.sh stop`

1. Log on to the platform as icosuser.
2. Access the directory to where you have downloaded the installer.
3. Enter the following command:
   `sh ./driverversion.bin LAX_VM /opt/IBM/tivoli/netcool/ncm/jre/bin/java -i console`
   where `driverversion.bin` is the name of the driver to be installed.
4. Click **Enter** to begin the installation.
5. To accept the license agreement, click **Enter**.
6. Continue to click **Enter** to continue with the installation.

Netcool Configuration Manager must be restarted after the drivers have been installed. Execute the start server command:
`/opt/IBM/tivoli/netcool/ncm/bin/itncm.sh start`
Once Netcool Configuration Manager has restarted, any newly installed SmartModel drivers will be recognized and catalogued, but they will be in Standard mode. To switch them to SmartModel mode, follow the documentation at "Changing SmartModel drivers from Standard to SmartModel mode" on page 58.
To ensure that all servers in a distributed environment have the same drivers installed, it is useful to check the driver consistency on all servers. Navigate to the Systems Manager, and access Servers. Driver consistency is indicated by the **Driver Checksum** field against each server.

## Installing individual SmartModel drivers using the GUI

The SmartModel driver installers provide the ability to install drivers using the GUI.

This task describes how to install the SmartModel drivers using the GUI.

1. Access the `/opt/IBM/tivoli/netcool/ncm/bin` directory, and execute the stop server command as follows:
   `/opt/IBM/tivoli/netcool/ncm/bin/itncm.sh stop`
2. Log on to the platform as the user that installed Netcool Configuration Manager.
3. Access the directory to which you downloaded the installer.
4. Enter the following command:

   ```
   sh ./driverversion.bin LAX_VM /opt/IBM/tivoli/netcool/ncm/jre/bin/java -i gui
   ```

   where *driverversion.bin* is the name of the driver to be installed.
5. To accept the license agreement, select **Next**.
6. Choose the installation directory, or accept the default, then click **Next**.
   The **Pre-Installation Summary** window is displayed.
7. Review the installation details and click **Install**.
   The installation proceeds and when complete, the **Install Complete** window is displayed.
8. Click **Done** to exit the installer.

Netcool Configuration Manager must be restarted after the drivers have been installed. Execute the start server command:
`/opt/IBM/tivoli/netcool/ncm/bin/itncm.sh start`
Once Netcool Configuration Manager has restarted, any newly installed SmartModel drivers will be recognized and catalogued, but they will be in Standard mode. To switch them to SmartModel mode, follow the documentation at "Changing SmartModel drivers from Standard to SmartModel mode" on page 58.
To ensure that all servers in a distributed environment have the same drivers installed, it is useful to check the driver consistency on all servers. Navigate to the Systems Manager, and access Servers. Driver consistency is indicated by the **Driver Checksum** field against each server.

## Installing SmartModel drivers silently

This task describes how to install the SmartModel drivers silently using the command line silent installation facility.

Access the `/opt/IBM/tivoli/netcool/ncm/bin` directory, and execute the stop server command:
`itncm.sh stop`

1. Log on to the platform as the user that installed Netcool Configuration Manager.
2. Access the `/opt/IBM/tivoli/netcool/ncm/bin` directory, and execute the stop server command:
   `itncm.sh stop`
3. Access the directory containing the driver installer file.
4. Create an `ITNCM.properties` file that contains `$LICENSE_ACCEPTED$=true`.

5. Enter the following command:

```
sh ./driverversion.bin LAX_VM /opt/IBM/tivoli/netcool/ncm/jre/bin/java -i silent -f
ITNCM.properties
```

   where *driverversion.bin* is the name of the driver to be installed.
6. Press Enter.

The silent installation proceeds based on the parameters you have defined in the `ITNCMDrivers_Silent.properties` file.

Netcool Configuration Manager must be restarted after the drivers have been installed. Execute the start server command:
`/opt/IBM/tivoli/netcool/ncm/bin/itncm.sh start`
Once Netcool Configuration Manager has restarted, any newly installed SmartModel drivers will be recognized and catalogued, but they will be in Standard mode. To switch them to SmartModel mode, follow the documentation at "Changing SmartModel drivers from Standard to SmartModel mode" on page 58.
To ensure that all servers in a distributed environment have the same drivers installed, it is useful to check the driver consistency on all servers. Navigate to the Systems Manager, and access Servers. Driver consistency is indicated by the **Driver Checksum** field against each server.

## Installing multiple individual device drivers silently

This task describes how to install individual device drivers silently using the command line drivers bulk install script (`drivers_bulk_install.sh`).

**Note:** Before using the bulk installer, at least one driver must be installed on the system so that the `drivers_bulk_installer.sh` script is present in the `install_dir/drivers/bin` directory.

1. Log on to the platform as the user that installed Netcool Configuration Manager.
2. Download the individual driver installers to be installed, and place them in a single directory on the server where you will perform the installation.
3. Copy `drivers_bulk_install.sh` from the `install_dir/drivers/bin` directory to the directory where the driver installers are located.
4. Open or create the file `ITNCM.properties` in a text editor.
5. Edit or create the following installation parameters:

   **$DRIVERS_INSTALL_DIR$**
   You define the directory where the driver subdirectory will be installed, for example:
   `$DRIVERS_INSTALL_DIR$=/opt/IBM/tivoli/netcool/ncm`

   **$LICENSE_ACCEPTED$**
   You must accept the license, or the installation will not proceed. To install, set `$LICENSE_ACCEPTED$=true`
6. Access the `/opt/IBM/tivoli/netcool/ncm/bin` directory, and execute the stop server command: `itncm.sh stop`
7. Access the directory containing the downloaded drivers installers, the `ITNCM.properties` file, and the bulk install script and run the installation:

```
./drivers_bulk_install.sh <driver installers dir> ITNCM.properties
```

The silent installation proceeds based on the parameters you have defined in the `ITNCMProperties.txt` file.

This is an example of the installation output with two drivers being installed. Here, the *<driver installers dir>* directory is denoted by '.'.

```
[icosuser@ncm-server drivers]# ./drivers_bulk_install.sh . ITNCMProperties.txt
Starting bulk installation

Using download directory: .
```

```
Using silent properties: ITNCMProperties.txt
Using derived Java executable: /opt/IBM/tivoli/netcool/ncm/jre/bin/java

Processing ./CiscoRouter76xxS72033PK9SVMZ122.bin
Installation: Successful. (Summary: 119 Successes, 0 Warnings,
0 NonFatalErrors, 0 FatalErrors)
Completed processing ./CiscoRouter76xxS72033PK9SVMZ122.bin

Processing ./CiscoRouterISRG215x.bin
Installation: Successful. (Summary: 119 Successes, 0 Warnings,
0 NonFatalErrors, 0 FatalErrors)
Completed processing ./CiscoRouterISRG215x.bin

Totals: 2 Successes, 0 Fails, 0 Undetermined

Ended bulk installation
```

Netcool Configuration Manager must be restarted after the drivers have been installed. Execute the start server command:
`/opt/IBM/tivoli/netcool/ncm/bin/itncm.sh start`
Once Netcool Configuration Manager has restarted, any newly installed SmartModel drivers will be recognized and catalogued, but they will be in Standard mode. To switch them to SmartModel mode, follow the documentation at "Changing SmartModel drivers from Standard to SmartModel mode" on page 58.
To ensure that all servers in a distributed environment have the same drivers installed, it is useful to check the driver consistency on all servers. Navigate to the Systems Manager, and access Servers. Driver consistency is indicated by the **Driver Checksum** field against each server.

## Changing SmartModel drivers from Standard to SmartModel mode

The SmartModel driver installer also deploys the SmartModel upgrade tool to allow drivers to be upgraded from Standard to SmartModel mode. Once upgraded to SmartModel mode it is not possible to downgrade a driver from SmartModel mode to Standard mode.

**Important:** After installing SmartModel drivers, you must have restarted Netcool Configuration Manager in order for the new drivers to be catalogued. If the drivers have not been catalogued before you follow this procedure, it will not take effect.

The smartModelUpgrade.sh tool is installed to `/opt/IBM/tivoli/netcool/ncm/drivers/bin`. Drivers can be upgraded to SmartModel mode either on an individual basis, or for all drivers on the system.

1. Change directory to `/opt/IBM/tivoli/netcool/ncm/drivers/bin` directory and run the SmartModel upgrade script with the appropriate arguments as described here:

   **To put all SmartModel drivers into SmartModel mode**
   `smartModel*Upgrade.sh -all`

   **To put a single SmartModel driver into SmartModel mode**
   `smartModel*Upgrade.sh -uuid IBM-`*`#########-####-####-####-############`*

   where *`########-####-####-####-############`* is the uuid of the driver to be upgraded.

   The driver identifier can be found by using `driverTools.sh -show-details` as described in *Managing device drivers* in the *IBM Tivoli Netcool Configuration Manager - Base System Admin Guide*.
2. In the Netcool Configuration Manager GUI, navigate to the Systems Manager, Drivers screen and click **Tools**, then **Reload Drivers** to refresh the screen and show the new driver support levels.

Drivers have been upgraded from Standard to SmartModel mode, and reloaded.

# Installing auto-discovery

Use this information to install the Netcool Configuration Manager auto-discovery driver. You must install the most current drivers before installing auto-discovery.

## Auto-discovery overview

The Netcool Configuration Manager auto-discovery component determines the network resource Vendor, Type, Model, and Operating System (VTMOS), by sending a series of queries via TELNET, SNMP or SSH to each network resource.

You can obtain the auto-discovery component (ITNCM_Autodiscovery.tar) either from the product media, or by downloading it from the IBM Passport Advantage Web site: http://www-01.ibm.com/software/howtobuy/passportadvantage

There are three options for installing auto-discovery: command line interface console (CLI), graphical user interfcae (GUI), or silent installation.

Once installed, auto-discovery provides the following functionality:

**Update**
Updates to latest version of auto-discovery.

After auto-discovery installation, updates to existing auto-discovery take effect once the server is restarted.

**Important:** By default, an existing Netcool Configuration Manager deployment of auto-discovery will not be updated at install time, unless otherwise specified.

**Restore**
Restores a previously installed version of auto-discovery.

Each time auto-discovery is updated, the previous configuration is saved, and can be restored if required.

See the related links for more information.

**Version**
Displays the current version of auto-discovery in the console.

## Auto-discovery installation prerequisites

Before installing auto-discovery, install Netcool Configuration Manager, as well as the Netcool Configuration Manager drivers. Netcool Configuration Manager requirements are documented in the planning section. It should take one or two minutes to install auto-discovery.

For more information on using the auto-discovery functionality, see *Executing the Auto-Discovery tool* in the *IBM Tivoli Netcool Configuration Manager User Guide*.

**Related information**

Planning
Use this information to plan a new installation of Netcool Configuration Manager. For upgrading and migrating from existing installations, see the Migration and Upgrading sections instead.

# Installing auto-discovery via CLI (all platforms)

The auto-discovery installation is not platform-specific, so only one generic installer is required for installation. This task describes how to install auto-discovery using the command line interface.

Ensure Netcool Configuration Manager and the most current driver packages have been installed.

Access the Netcool Configuration Manager installation directory (the default is `/opt/IBM/tivoli/netcool/ncm/bin`), and execute the stop server command `itncm.sh stop`

**Warning:**

Before executing the auto-discovery installer, make a backup of the existing auto-discovery XML files located in the following directory: */ncm install dir*/autodiscovery/xml.

Autodiscovery version 6.6.0 and above requires Java 1.8 as a prerequisite. The auto-discovery installer overwrites all files in this directory. After the installer has completed, review the backup files and recreate your custom changes as required.

1. Log on to the server as the user that installed Netcool Configuration Manager. The default is icosuser.
2. Access the directory where you have downloaded the installer.
3. Type sh./autodiscovery-*version*.bin LAX_VM */opt/IBM/tivoli/netcool/ncm/jre/bin/java* -i console
   where *version* is the auto-discovery installer version, and */opt/IBM/tivoli/netcool/ncm/jre/bin/java* is the default directory.
4. Click **Enter** to begin the installation, then **Enter** again to continue.
5. To accept the license agreement, select **1**.
6. When asked to choose the install folder, you must ensure that this is the directory containing the drivers folder. The default, which you can change, is /opt/ibm/tivoli/netcool/ncm
7. Updates to auto-discovery automatically take effect once the server is restarted. To accept this, choose **1**.

   **Tip:** You have the option to immediately apply auto-discovery updates in the following ways, if required:

   - To **automatically** deploy the latest auto-discovery version immediately, choose **2**, then enter a valid Netcool Configuration Manager directory when prompted at the next screen.
     Your current version of auto-discovery is updated immediately.
   - To **manually** deploy the latest auto-discovery version, access the /opt/IBM/Tivoli/drivers/autodiscovery/bin folder and run the following command:
     autodiscoveryUtil <<itncm_install_path>> -u (You can perform this manual update at any time.)
8. Check the installation summary details, and click **Enter** to continue.

   After the autodiscovery installation is complete, the last statement of the installation can be ignored. The statement is shown below:

```
Install Complete
---------------
The installation of Autodiscovery version x.x.x is complete, but some errors occurred during
the install.
```

   Log files are found in the install_dir/drivers/autodiscovery/logs directory.

## Installing auto-discovery via GUI (all platforms)

The auto-discovery installation is not platform-specific, so only one generic installer is required for installation. This task describes how to install auto-discovery using the GUI.

Ensure Netcool Configuration Manager and the most current driver packages have been installed.

Access the Netcool Configuration Manager installation directory (the default is /opt/IBM/tivoli/netcool/ncm/bin), and execute the stop server command itncm.sh stop

**Warning:** Before executing the auto-discovery installer, make a backup of the existing auto-discovery XML files located in the following directory: /<*ncm install dir*>/autodiscovery/xml
The auto-discovery installer overwrites all files in this directory. Once the installer has completed, review the backup files and recreate your custom changes as required.

1. Log on to the server as the user that installed Netcool Configuration Manager. The default is icosuser.
2. Access the directory where you have downloaded the installer.

3. Type `sh./autodiscovery-`*`version`*`.bin LAX_VM` */opt/IBM/tivoli/netcool/ncm/jre/bin/java* `-i gui`
   where *version* is the auto-discovery installer version, and */opt/IBM/tivoli/netcool/ncm/jre/bin/java* is the default directory.
4. Click **Enter** to begin the installation, then **Next** to continue.
5. Accept the license agreement, then click **Next**.
6. When asked to choose the install folder, you must ensure that this is the directory containing the drivers folder. The default, which you can change, is `/opt/ibm/tivoli/netcool/ncm`
7. Updates to auto-discovery automatically take effect once the server is restarted. To accept this, select **No**.

   **Tip:** You have the option to immediately apply auto-discovery updates in the following ways, if required:

   - To **automatically** deploy the latest auto-discovery version immediately, choose **Yes** and **Next**, then enter a valid Netcool Configuration Manager directory when prompted at the next screen.
     Your current version of auto-discovery is updated immediately.
   - To **manually** deploy the latest auto-discovery version, access the `/opt/IBM/Tivoli/drivers/autodiscovery/bin` folder and run the following command:
     `autodiscoveryUtil <<itncm_install_path>> -u` (You can perform this manual update at any time.)
8. Check the pre-installation summary details, and click **Install** to continue.

The installation proceeds and the results are displayed. If you have chosen auto-update, those results are also displayed. Click **Done** to exit the installer.

## Installing auto-discovery in silent mode

You install auto-discovery in silent mode by firstly editing the properties file (`autodiscovery.properties`), and then launching the installer with the silent command (`-i silent`) suffixed.

Close and stop all system processes before beginning silent installation. This includes all monitoring software, databases, and third party packages.

Performing the installation requires full administrative access to the entire system. Full system authorization to read, write, add, and delete all system files and applications must be established before beginning the installation.

**Warning:** Before executing the auto-discovery installer, make a backup of the existing auto-discovery XML files located in the following directory: */<ncm install dir>/autodiscovery/xml*
The auto-discovery installer overwrites all files in this directory. Once the installer has completed, review the backup files and recreate your custom changes as required.

Installation parameters are defined in the `autodiscovery.properties` file. You can replace any suggested default values with your own.

**Tip:** There are two methods of referencing the properties file:

**The default documented here (step 3)**
Use the `-f` flag to explicitly reference the file, regardless of name or location. For example:

`sh ./autodiscovery-`*`version`*`.bin -i silent -f` *`myproperties.properties`*

where`autodiscovery-`*`version`*`.bin` is the name of your installer, and *myproperties.properties* is the location and name of your properties file.

**Optional**
Use a properties file with the same filename as the installer and located in the same directory.

However, the extension of the properties file must be changed to `.properties`, for example for an installation using the `autodiscovery-`*`version`*`.bin` file, you change the properties file name to `autodiscovery-`*`version`*`.properties`.

When silently installing auto-discovery, you must ensure that the **$LICENSE_ACCEPTED$** property is set to `true`.

Installing the product in silent mode should take one or two minutes, excluding preparation time and the installation of any prerequisite software.

1. From the directory which contains the installer, open `autodiscovery.properties` in a text editor.
2. Edit the installation parameters as required.
3. Type the following command:
   `sh./autodiscovery-`*`version`*`.bin LAX_VM` */opt/IBM/tivoli/netcool/ncm/jre/bin/java* `-i silent -f` */file_path/mypropertiesfile.properties*
   where *`version`* is the auto-discovery installer version, and */opt/IBM/tivoli/netcool/ncm/jre/bin/java* is the default directory.

# Installing OOBC

Use this information about Netcool Configuration Manager to install the OOBC daemon, install the OOBC software, configure an OOBC daemon, and troubleshoot OOBC installation issues.

**Related tasks**

Preparing to install
Before you install or upgrade to a new version of Netcool Configuration Manager, you must take note of a number of prerequisites.

Installing a GUI and worker server
You install Netcool Configuration Manager either on a single server, or on several servers in a distributed architecture. The installation of a GUI and worker server can be part of a stand-alone installation on a single server, or it can be the first step in the installation of a distributed architecture on several servers.

Installing a worker server only
You install a Netcool Configuration Manager worker server as part of a distributed architecture deployed on one or more servers. You install one or more worker servers after having completed the installation of one or more GUI and worker servers.

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.

**Related information**

Configuring OOBC
Use this information about Netcool Configuration Manager to configure OOBC.

## Extracting OOBC software

The OOBC software is in an archived format suited for the operating system environment that you have chosen.

This task requires you to download the installer.

1. Netcool Configuration Manager can be installed using either the product media, or by downloading it from the IBM Passport Advantage® Web site:
   http://www.ibm.com/software/howtobuy/passportadvantage/
2. Retrieve the correct download for the operating system you are using.
3. Download the `.tgz` file.
4. Use the following gunzip command to unpack the file, and then tar to untar it:

```
gunzip -c --stdout filename.tgz | tar xf -
```

**Related information**

Configuring OOBC
Use this information about Netcool Configuration Manager to configure OOBC.

## Prerequisites

Set JAVA_HOME in the machine.

A running syslog daemon is a prerequisite for OOBC to work.

**Tip:** In order to receive messages from the network using an internet domain socket with the syslog service, use the **-r** parameter when performing a Linux syslog daemon installation. (The default is to not receive any messages from the network.)

The OOBC software can be installed a number of times. Each time the software is installed a new run directory is created in the root of the OOBC software tree. Each new run directory has a unique name (for example, run1, run2, run3, and so forth). Each OOBC run directory is configurable without impacting other OOBC run instances. This allows for a single server machine to host multiple OOBC daemons where each daemon is processing its own `syslog` file (or any suitable log file). This task requires you to install an OOBC daemon.

1. Create a directory where you unzip and install OOBC software (OutOfBandChange is the directory name used as an example in this documentation, user can use any appropriate name), copy the oobc.zip file extracted in the previous page (Extracting OOBC Software page).
2. Unzip the OOBC zip file using unzip command. For a Unix platform, you must manually set the permissions before being able to execute the install script (for example, the `chmod` command).
3. Now, you install the OOBC software.

**Related information**

Configuring OOBC
Use this information about Netcool Configuration Manager to configure OOBC.

## Installing OOBC software

These steps explain how to install the OOBC software.

Install the OOBC software after you extract the OOBC installers and setup prerequisites. Navigate to the directory where you have unzipped the oobc.zip, the installer file (install.sh) is available in the same unzipped directory.

**Important:** Execute as a user with superuser privilege.

1. Access the directory containing the OOBC installer. The location of the directory depends on where you unzipped the `oobc.zip` file. The path is: *<OutOfBandChange>*.
2. Run the OOBC installer by typing the following command and then clicking **Enter**:

   ```
   ./install.sh
   ```

3. The Installation path is requested for the new OOBC Run directory. Remember, multiple OOBC Run Directories can be installed:

   ```
   Beginning install process for new OOBC Run directory:
   /opt/OutOfBandChange/run1
   ```

   Click **Enter** to accept the default path.
4. The installer requests Unix ownership. This user (Example: root) has to be able to read the input system log file.

   ```
   Enter the Unix owner of the OOBC software? [root]
   ```

   Click **Enter** to accept the default user provided, or enter an alternative user name.
5. The installer requests the Netcool Configuration Manager server name:

```
Enter the servername of the ITNCM? [FQDN]/hostname
```

Enter the server name where Netcool Configuration Manager is installed, and click **Enter**.

6. The installer asks if the Netcool Configuration Manager server is running HTTPS:

```
Is the ITNCM running a secure connection (https)? [no]
```

Type **Yes** or **No** to indicate whether Netcool Configuration Manager is being run on a server running HTTPS, and then click **Enter**.

7. The installer requests the port on which Netcool Configuration Manager is running:

```
What port is the ITNCM running on [16310]?
```

Enter the Netcool Configuration Manager port number, and click **Enter**.

8. The installer requests the user name of the user to be logged into Netcool Configuration Manager. The user has to exist with the appropriate activities assigned to the group:

```
What user do you want to login to the ITNCM as [OOBCUser]?
```

Enter the user that will be logged intoNetcool Configuration Manager, and click **Enter**.

9. The installer requests the password for the user specified in the previous step:

```
Enter clear text password:
```

Enter the Netcool Configuration Manager user password, and click **Enter**.

10. The installer requests the Worker Server (server on which Netcool Configuration Manager executes work) username:

```
Enter the worker user id ITNCM executes work as [Worker1]?
```

Click **Enter** to accept the default Worker User ID, and click **Enter** again. The value entered here will be skipped when present in the Syslog. If multiple user entries are required, additional values can be added under <ITNCM-users> after install.

11. The installer requests the Worker Server address:

```
Enter the worker server address[123.123.123.123]
```

Click **Enter** to accept the default Worker server address, or enter an alternative. Worker Servers are specified as IP addresses. If multiple Worker Server entries are required, additional values can be added under <worker-servers> after install.

12. The installer requests an authorized third party user ID. This user does not require notification when an activity is recorded.

```
Enter an authorized 3rd party user id that does not require notification
when activity is recorded in the syslog [3rdPartyUser]?
```

Click **Enter** to accept the default third Party User ID. If multiple user entries are required, then more values can be added under <authorized-users> after install.

13. The installer requests the path to the syslog file as input:

```
Enter the full path to the syslog file to be parsed:
[/var/log/messages]
```

Enter the path to the log, or click **Enter** to accept the default.

14. The installer requests the path to the syslog save file:

```
Enter the full path to the syslog saver file:
[/opt/OutOfBandChange/run1/log.syslog-messages]
```

Enter the path to the log, or click **Enter** to accept the default.

15. The installer displays a message similar to the following:

    **Example**

    ```
    ITNCM OOBC Install Properties:
    Install Owner: root
    Install Directory: /opt/OutOfBandChange/run1
    ITNCM URL: iiop://FQDN/hostname:16310/
    Syslog File: /var/log/messages
    OOBC User: OOBCUser
    User Password: d8adea5c67c7c9d4
    ITNCM Worker: ITNCM
    3rd Party User: 3rdPartyUser
    Worker Server: 123.123.123.123
    Syslog Message Storage File: /opt/OutOfBandChange/run1/log.syslog messages
    Is this OK? (yes,no)
    Yes
    ```

    Type **Yes** and click **Enter** to accept the information.

The installation proceeds and a message similar to the following displays once the install completes:

```
Copying Configuration Files
Setting permissions
BUILD SUCCESSFUL
Total time: 52 seconds
```

If the installation of the OOBC software is successful your next task is to configure a daemon. Otherwise, read the troubleshooting installation issues to resolve the most commonly encountered OOBC installation issues.

**Related information**

Configuring OOBC

Use this information about Netcool Configuration Manager to configure OOBC.

## Configuring a daemon

Configure an OOBC daemon on the server after you complete the OOBC software installation.

1. Change directory to the run directory which was specified during the installation process. For example:

   ```
   cd /opt/OutOfBandChange/run1
   ```

2. Edit the `oobc.properties.xml` file.
3. Make any other customizations to this configuration file that is required for your environment.

Now, you configure the OOBC software.

**Related information**

Configuring OOBC

Use this information about Netcool Configuration Manager to configure OOBC.

## Troubleshooting the OOBC software installation

This section is designed to help troubleshoot some of the most commonly encountered OOBC installation issues.

### Issue #1

An installer issue that may arise is when the following error is generated:

```
bash-2.05$ ./install.sh
BUILD FAILED
/opt/OutOfBandChange/install.xml:427: The next generated
install directory [/opt/OutOfBandChange/run1] already exists.

Please review the current install directories and then edit the
install.properties file resetting any one of the install.xxx properties to
```

```
a suitable value such that the next generated directory does not exist.
When you have done this, re-run this install script.
Total time: 0 seconds
```

This will occur when there is an existing run1 directory. This can be fixed by either deleting/moving/renaming the run1 files system or modifying the `install.properties` file. This would occur when two OOBC daemons are needed on the same machine to monitor two different files.

**Related information**

Configuring OOBC
Use this information about Netcool Configuration Manager to configure OOBC.

# Chapter 3. Configuring

After installation, you perform a number of post-installation configuration tasks.

**Related tasks**

Installing a GUI and worker server

You install Netcool Configuration Manager either on a single server, or on several servers in a distributed architecture. The installation of a GUI and worker server can be part of a stand-alone installation on a single server, or it can be the first step in the installation of a distributed architecture on several servers.

Installing a worker server only

You install a Netcool Configuration Manager worker server as part of a distributed architecture deployed on one or more servers. You install one or more worker servers after having completed the installation of one or more GUI and worker servers.

## Configuring housekeeping for log files

After installing, you must set up housekeeping for log files.

If you are using Fix Pack 11 or earlier version, run the `logcleaner.sh` script to perform housekeeping on log files. For information on how to run the script, see *Performing housekeeping on log files* in the *IBM Tivoli Netcool Configuration Manager Administration Guide*.

If you are using Fix Pack 12 or later version, perform the following:

- Before you execute the logcleaner activity, verify that the logrotate is set up. If not done, you should set it up by installing logrotate utility and set the scheduling.
- Run the `logcleaner.cnf` script to perform housekeeping on log files. For information on how to run the script, see *Performing housekeeping on log files* in the *IBM Tivoli Netcool Configuration Manager Administration Guide*.

## Customizing the appearance of the GUI

You can customize some text and images that are used in the GUI.

### Creating a keystore and self signed certificate

To customize the appearance of a Configuration or Compliance GUI, you must have a keystore with a signed certificate. If you already have a keystore with a certificate signed by a certificate Authority, you do not need to perform this task.

The script that customizes Netcool Configuration Manager Configuration and Compliance GUIs modifies `.jar` files. Therefore, the script requires keystore information in order to run.

To make keystore information available, you must create a keystore, then export and import a self-signed certificate.

1. Create a keystore using the `keytool` command in the Netcool Configuration Manager Java installation.

   You must provide domain identity information, for example, your name, company, and country.

   For instructions on creating a keystore, see the following information: https://docs.oracle.com/javase/8/docs/technotes/tools/unix/keytool.html and https://docs.oracle.com/javase/tutorial/security/toolsign/step3.html

   The following example creates a keystore called `KeyStore.jks`, which is valid for four years:

   ```
   keytool -genkey -alias customerxxxalias -keyalg RSA -keypass customerxxxkey1
   -storepass customerxxxstore1 -keystore KeyStore.jks -keysize 2048 -validity 1461
   ```

2. Export a self-signed certificate for the keystore.

For instructions on creating a certificate using the keytool command, see the following information: https://docs.oracle.com/javase/tutorial/security/toolsign/step5.html

The following example creates a self-signed certificate called `customerxxx.cer` for importing on to a GUI client truststore:

```
keytool -export -keystore KeyStore.jks -alias customerxxxalias
-file customerxxx.cer
```

3. On the GUI client machine, import the self-signed certificate, as an administrator user, into the `cacerts` keystore of the installed Java, by using the `keytool` command.

   For instructions on importing a certificate using the keytool command, see the following information: https://docs.oracle.com/javase/8/docs/technotes/tools/unix/keytool.html

   The following example imports the self-signed certificate in `customerxxx.cer` for key alias `customerxxxalias` into the Java `cacacerts` keystore on Linux:

   ```
   sudo keytool -import -trustcacerts -keystore
   "/usr/lib/jvm/java-8-openjdk-i386/jre/lib/security/cacerts" -storepass
   changeit -noprompt -alias customerxxxalias -file "customerxxx.cer"
   ```

   In the example above, `changeit` is the default `cacerts` keystore password for a Java installation. On Windows, run a command prompt window as Adminstrator instead of using the `sudo` prefix.

## Creating a resource archive

A resource archive is a collection of text and image files that you can use to customize the appearance of a Netcool Configuration Manager GUI.

To create a resource archive file, complete the following steps.

1. Make a copy of the example resource file.

   The example file is here: *ncm_install_dir*`/ncm/config/properties/ibm-tivoli-itncm-vendor-resource-bundle-example.zip`
2. Unzip the resource archive.

   The resource archive, by default, contains the following files:

   ```
   vendor.properties
   /images/ITNCM_C_Splash.png
   /images/tivoli.gif
   /images/IBM_logo_Black.gif
   /images/tivoli-brandmark.gif
   /images/ITNCM_Splash.png
   /images/ibm-logo-white.gif
   /images/focusframeIcon.gif
   /images/compliance_NCM_logo.png
   /images/ibm-logo-black.gif
   /images/NCM_logo.png
   ```
3. Modify text strings as required in the `vendor.properties` file.

   The `vendor.properties` file contains the following property categories:

   - **vendor.web**, for properties of web front end pages, such as web login pages.
   - **vendor.base.gui**, for config GUI properties.
   - **vendor.gui**, for compliance GUI properties.
   - **vendor.report**, for reports properties.

   The only properties that should be changed for reporting are the properties and images in the `vendor.report` section.

   **Note:** Ensure that the replacement strings contain nearly the same number of characters as the default strings.
4. Replace any of the default images in the `images/` directory with your own images.

**Note:** Ensure that replacement images are of the same size as the default images.

5. In the `vendor.properties` file, rename any references to images whose names have changed.
6. Remove any unchanged entries from the `vendor.properties` file.
7. Create a zip file that contains the updated files, with the same structure as the default resource archive.

   This zip file is used as input to the rebranding scripts.

## Customizing configuration and compliance servers

You can customize some text and images that are used in the configuration and compliance GUIs by using the `brand.sh` script.

Before running the script, ensure that you have a keystore and certificate, as described in "Creating a keystore and self signed certificate" on page 67. Create a resource archive that contains the changes you want to make, as described in "Creating a resource archive" on page 68.

The script is located here: *ncm_install_dir*`/ncm/bin/utils/support/brand.sh`

1. Ensure that the path to the Java bin directory is included in the environment's path.

   You can use a command similar to the following example:

   ```
   export PATH=path_to_WAS_install_dir/IBM/WebSphere/AppServer/java/bin:$PATH
   ```

2. Ensure that the `zip` utility is installed.

   You can use a command similar to the following to install the utility:

   ```
   yum install zip
   ```

3. Run the script by using a command similar to the following:

   ```
   brand.sh -a path_to_resource_archive.zip -s keystore_password
   ```

   The following table describes the required and optional arguments.

*Table 11. Command-line options for the brand.sh script*

| Option | Description |
|---|---|
| `-a` *path_to_resource_archive.zip* | Required. Full path to the resource archive. |
| `-s` *keystore_password* | Required. Keystore password for the keystore file. |
| `-b` *base_directory* | Optional. Base directory for the target Netcool Configuration Manager installation. The default is: `/opt/IBM/tivoli/netcool/ncm`. |
| `-c` *keystore_file* | Optional. Java keystore file for signing the resource bundle jar. The default value is: `/headless/.keystore`. |
| `-k` *key_alias* | Optional. Alias for the key to use when signing the resource bundle jar. The default value is: `mykey`. The given alias must refer to a valid key in the specified keystore file. |
| `-K` *key_password* | Optional. Key password. The default is the same as keystore password. |
| `-t` *working_directory* | Optional. A temporary working directory. The default value is: `/var/tmp/brand_221219_180153_5043_tmp.d`. |

| *Table 11. Command-line options for the brand.sh script (continued)* | |
|---|---|
| **Option** | **Description** |
| `-l log_mode` | Optional. The logging mode. Allowed values are any one of the following:<br>• FATAL<br>• ERROR<br>• WARN<br>• INFO<br>• DEBUG |
| `-v` | Optional. Using this option turns on verbose mode, which generates a log file. Verbose mode is off by default. Turning on verbose mode is equivalent to using the option `-l DEBUG`. |
| `-h` | Optional. Print this usage message and exit successfully. |

4. Restart Netcool Configuration Manager. Clear the Web Start client-side cache and restart the browser to ensure that all changes are displayed correctly.

   The branding changes are visible in the compliance and configuration GUIs.

The following example supplies keystore information to the script:

```
./brand.sh -a /opt/IBM/tivoli/netcool/ncm/bin/utils/support/ibm-tivoli-itncm-vendor-resource-
bundle-example.zip
 -s "customerxxxstore1" -K "customerxxxkey1" -k "customerxxxalias"
-l DEBUG -c /opt/IBM/tivoli/netcool/ncm/bin/utils/support/KeyStore.jks
```

## Customizing reporting servers

You can customize some text and images that are used in the reporting GUIs by using the `reports_brand.sh` script.

Before running the script, ensure that you have a keystore and certificate, as described in "Creating a keystore and self signed certificate" on page 67. Create a resource archive that contains the changes you want to make, as described in "Creating a resource archive" on page 68.

The script is located here: *ncm_install_dir*`/ncm/bin/utils/support/reports_brand.sh`

1. Ensure that the path to the Java bin directory is included in the environment's path.

   You can use a command similar to the following example:

   ```
   export PATH=path_to_WAS_install_dir/IBM/WebSphere/AppServer/java/bin:$PATH
   ```

2. Ensure that the `zip` utility is installed.

   You can use a command similar to the following to install the utility:

   ```
   yum install zip
   ```

3. Run the script by using a command similar to the following:

   ```
   reports_brand.sh -a path_to_resource_archive.zip -C cognos_root_path
   ```

   The following table describes the required and optional arguments.

| *Table 12. Command-line options for the brand.sh script* | |
|---|---|
| **Option** | **Description** |
| `-a` *`path_to_resource_archive.zip`* | Required. Full path to the resource archive. |
| `-C` *`cognos_directory`* | Required. The root directory of the Cognos installation. The default value is: `/opt/IBM/tivoli/tipv2Components/TCRComponent/cognos`. The root directory is the one that contains the following subdirectories:<br>• properties<br>• license<br>• bin<br>• temp<br>• install<br>• lib<br>• logs<br>• ui<br>• var<br>• etc<br>• data<br>• reporting<br>• profile |
| `-t` *`working_directory`* | Optional. A temporary working directory. The default value is: `/var/tmp/brand_221219_180153_5043_tmp.d`. |
| `-l` *`log_mode`* | Optional. The logging mode. Allowed values are any one of the following:<br>• FATAL<br>• ERROR<br>• WARN<br>• INFO<br>• DEBUG<br>Setting the logging mode to `DEBUG` logs details of the images and properties that are changed. |
| `-v` | Optional. Using this option turns on verbose mode, which generates a log file. Verbose mode is off by default. Turning on verbose mode is equivalent to using the option `-l DEBUG`. |
| `-h` | Optional. Print this usage message and exit successfully. |

4. Restart ITNCM Reports.

   The branding changes are visible in the report pages, except the initial DASH portal page.

The following example supplies the required arguments to the script:

```
./reports_brand.sh -C /opt/IBM/netcool/TCRJazzSM
-a ibm-tivoli-itncm-vendor-resource-bundle-example.zip -l DEBUG
```

## Reverting customizations

You can revert the changes made by the rebranding scripts.

Running the `brand.sh` or `reports_brand.sh` script creates another script that can revert the changes.

1. To revert the changes to the configuration and compliance GUIs, run the script that was identified in the log output when the `brand.sh` script was run.

   The following extract shows example output from the `brand.sh` script:

   ```
   [17/12/19 16:19:38]  [INFO]: [870] To revert these changes execute this script:
   [/opt/IBM/tivoli/netcool/ncm/bin/utils/support/branding_backup.d/brand_171219_161830_11707/
   branding_restore_brand_171219_161830_11707.sh].
   ```

2. To revert the changes to the reports, run the script that was identified in the log output when the `reports_brand.sh` script was run.

   The following extract shows example output from the `reports_brand.sh` script:

   ```
   [17/12/19 04:22:46]   [INFO]: [387] To revert these changes execute this script:
   [/root/bmd/branding/reporting_brand_restore_reports_brand_171219_042244_23303.sh].
   ```

# Configuring WebSphere Application Server for Network Service Manager

Starting from Netcool Configuration Manager V6.4.2 fix pack 6, you must configure IBM WebSphere Application Server in order to use JSON with the NSM REST API.

Complete the following steps to configure IBM WebSphere Application Server.

1. Copy the following files from the `/profile/installedApps/JazzSMNode01Cell/Intelliden R-Series.ear/ibm_tivoli-nsm.war/WEB-INF/lib/` directory within the Jazz for Service Management installation directory to the top level of the Jazz for Service Management installation directory.
   - jackson-mapper-asl-1.9.11.jar
   - jackson-core-asl-1.9.11.jar
2. Create a new shared library:
   a) Log in to IBM WebSphere Application Server console at `https://server:16316/ibm/console/logon.jsp` by using the Intelliden user ID and password.
   b) Click **Environment** > **Shared Library** > **New**.
   c) Select the following scope:
   `cells:JazzSMNode01Cell:nodes:JazzSMNode01:servers:server1`
   d) Enter a meaningful name for the new library.
   e) Add the full path to the libraries that you copied in the **Classpath** field.

      For example:

      ```
      /opt/home/icosuser/jackson-mapper-asl-1.9.11.jar
      /opt/home/icosuser/jackson-core-asl-1.9.11.jar
      ```

   f) Check **Use an isolated class loader for this shared library**.
   g) Save the changes.
3. Associate the new shared library with the NSM application.

a) Click **Servers** > **Server Types** > **Websphere application servers**.
   A list of servers is displayed.
b) Click the server that you want to use with the REST API.
c) In the **Configuration tab**, click **Installed applications** in the **Applcations** section.
   A list of installed applications is displayed.
d) Click **Intelliden R-Series**.
   The **Configuration** tab is displayed.
e) In the **References** section, click **Shared library references**.
   A list of shared libraries is displayed.
f) Select **NCM Service Management** and click **Reference shared libraries**.
   A list of available libraries is displayed.
g) Select the library that you created previously, and move it from the **Available** list to the **Selected** list.
h) Save your changes and exit the console.

4. Back up and edit the AppServer/properties/amm.filter.properties file within the IBM WebSphere Application Server installation directory.
5. Append the following lines to the end of the file:

```
Ignore-Scanning-Packages = javassist, \
                           org.antlr, \
                           org.apache.avalon, \
                           org.apache.batik, \
                           org.apache.bcel, \
                           org.apache.commons, \
                           org.apache.log4j, \
                           org.apache.poi, \
                           org.apache.regexp, \
                           org.apache.xalan,  \
                           org.apache.xerces,  \
                           org.apache.xml,  \
                           org.apache.xpath,  \
                           org.ajax4jsf, \
                           org.dbunit, \
                           org.richfaces, \
                           org.jboss.el, \
                           org.jchrontab, \
                           org.omg, \
                           org.seasar, \
                           org.slf4j,  \
                           com.thoughtworks.xstream.converters.reflection,  \
                           com.thoughtworks.xstream.mapper
```

6. Restart the Netcool Configuration Manager Presentation server where NSM is used.

## Loading the databases

Loading the database for Netcool Configuration Manager builds the schemas and loads the content. You can load the databases during installation, or separately at a later stage.

It is a requirement that the Oracle instance is reachable, and the user account credentials are active.

All relevant tables, keys and sequences are built in preparation for the database content. The scripts then create the content, such as realms, security settings, properties, searches, and other required functions.

**Important:** In a distributed architecture the schema must be loaded from one Netcool Configuration Manager GUI server only. If the database schema has already been loaded during installation, do not load it again.

**CAUTION:** Loading the database schema removes any existing Netcool Configuration Manager database schema, removing all existing data.

1. Access the directory containing the utilities:
   /opt/IBM/tivoli/netcool/ncm/bin/utils/database

2. Run the load schema script. If the installation is part of a distributed setup, execute the `loadDBSchema.sh` script from the main GUI server.
   `sh ./loadDBSchema.sh`

   This script creates a log file called `dbload.log` in *ncm_install_dir*`/logs`.

   **Tip:** This log file should be checked regularly, as errors from this script are not displayed on the console.
3. Required: **For DB2 databases only:** Grant regex execute permissions as required.

   For example:

   ```
   db2 grant execute on function 'NCM_REGEXP_LIKE(CLOB,VARCHAR(512),VARCHAR(3))' to 'db2inst1'
   db2 grant execute on function 'NCM_REGEXP_LIKE(VARCHAR(3000),VARCHAR(512),VARCHAR(3))' to
   'db2inst1'
   db2 grant execute on function 'DECODE_FUNCTION' to 'db2inst1'
   ```

   **Note:** UDF names like `NCM_REGEXP_LIKE` are only valid from Fix Pack 14 onwards. For Fix Pack 13 and previous fix packs, use the examples below.

   ```
   db2 grant execute on function 'REGEXP_LIKE(CLOB,VARCHAR(512),VARCHAR(3))'
   to 'db2inst1'
   db2 grant execute on
   function 'REGEXP_LIKE(VARCHAR(3000),VARCHAR(512),VARCHAR(3))' to 'db2inst1'
   db2 grant execute on function 'DECODE_FUNCTION' to 'db2inst1'
   ```
4. Required: **For Tivoli Common Reporting:** Configure Tivoli Common Reporting to use your enterprise database. For detailed information, see the Tivoli Common Reporting information center.

**Related tasks**

Installing a GUI and worker server
You install Netcool Configuration Manager either on a single server, or on several servers in a distributed architecture. The installation of a GUI and worker server can be part of a stand-alone installation on a single server, or it can be the first step in the installation of a distributed architecture on several servers.

Installing the product in silent mode
Silent installation requires an XML response file that defines the installation configuration. Silent mode is useful if you want identical installation configurations on multiple workstations.

Installing a worker server only
You install a Netcool Configuration Manager worker server as part of a distributed architecture deployed on one or more servers. You install one or more worker servers after having completed the installation of one or more GUI and worker servers.

Installing ITNCM-Reports
If you are not integrating with Network Manager, which ships with its own version of DASH, you must install ITNCM-Reports separately in order to access the reporting functionality.

Installing ITNCM-Reports in silent mode
If you are not integrating with Network Manager, which ships with its own version of DASH, you must install ITNCM-Reports separately in order to access the reporting functionality.

# Configuring DB2 HADR

Netcool Configuration Manager can be configured to use the DB2 High Availability and Disaster Recovery (HADR) feature.

Reference the following IBM Redbook: *High Availability and Disaster Recovery Options for DB2 for Linux, UNIX, and Windows* (SG24-7363-02), where it describes the options to configure DB2 HADR. The Redbook can be obtained at the following location:
http://www.redbooks.ibm.com/redbooks/pdfs/sg247363.pdf

Also reference the DB2 documentation for the specific DB2 release that you have installed.

**Note:** If you are using IBM Data Server Driver for JDBC and SQLJ version 3.50 or later, then client license files are not required for direct connections to DB2. For more information, see the following related DB2

topic in the IBM Knowledge Center: https://www.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.apdv.java.doc/src/tpc/imjcc_t0010264.html

HADR is a database replication method that provides a high availability solution for both partial and complete site failures. This task describes how to configure Netcool Configuration Manager with DB2 HADR Automatic Client Reroute option.

1. Configure the HADR DB2 servers using the detailed HADR configuration procedures in the Redbook or DB2 documentation.

   When configuring HADR, ensure that the following is true:

   - Primary and standby servers must have the same operating system and patch level.
   - The Netcool Configuration Manager database user credentials must be the same on DB2 primary and standby servers.
   - Management of HADR archive logs on both Primary and Standby DB2 servers has been discussed with your database administrator.
   - On each DB2 server ensure that the hostname matches the entry in <db2home>/sqllib/db2nodes.cfg
2. Once DB2 has been configured for HADR, stop all running NCM instances.
3. Execute the DB2 'list db directory' command for each DB2 instance, taking note of the output.
4. If DB2 servers are configured in a direct IP mode, (that is, not sharing a virtual IP address), then for each Netcool Configuration Manager instance, edit the rseries.properties file in `<NCM_INSTALL_DIR>/config/properties`, and modify the jpa/connUrl property to include details of the client reroute servers.

   For example:
   ```
   jpa/connUrl=jdbc:db2://<Primary DB2 Server Fully
   Qualified Host Name>:<Primary DB2 Server Port>/
   itncm:clientRerouteAlternateServerName=<Standby DB2 Server Fully Qualified
   Host Name>;clientRerouteAlternatePortNumber=<Standby DB2 Server Port>;
   ```
5. If the DB2 servers are sharing a Virtual IP (VIP), edit `/<ncm install path>/config/properties/rseries.properties` and modify the hostname for the jpa/connUrl variable so that it matches the DB2 VIP/hostname.
   For ACR the DB2 VIP/hostname should be seen in the 'Alternate server hostname' field from the 'list db directory' command executed in step 3.
6. If you are using DB2 version 10.1:
   a) Download the IBM Data Server Driver for JDBC that matches your DB2 release and fixpack version from Fix Central at the following address:
   http://www.ibm.com/support/fixcentral/
   b) On each Netcool Configuration Manager instance, back up the DB JDBC client jars db2jcc4.jar and db2jcc_license_cu.jar found in `<NCM_INSTALL_DIR>/lib` to a safe location.
   c) Extract the downloaded driver, and take the jars db2jcc4.jar and db2jcc_license_cu.jar and place them in the `<NCM_INSTALL_DIR>/lib` directory.
7. Restart all Netcool Configuration Manager instances.

   **Note:** When the primary database fails (hardware failure/forced shutdown), the following is expected:

   - There may be a delay of up to 120 seconds for the switch to the standby database to take place.
   - The Netcool Configuration Manager user interface will freeze until the standby database takes over from the primary.
   - UoWs which are currently executing will fail. A database exception will be written to the Intelliden log with the DB2 error code -4498, this error message also appears in the UOW log. You should re-queue failed UoWs.
   - No notification will appear in the Netcool Configuration Manager UI to show that a database switch has occurred.
   - Tivoli Common Reporting reports will show the egg timer during the switchover.

- The Netcool Configuration Manager account management page will take longer to process adding or editing users and groups, while it waits for the switchover to complete.
- A wizard initialization error may be generated by the DASH Wizard during a database takeover from primary to standby. If this occurs, reapply the DASH Wizard operation.

# Configuring immediate execution (Native Command Set workflow)

The 'immediate execution' workflow is a mechanism to reserve threads for dealing with high priority native command set execution via the Java or SOAP API.

The new API methods are described in the API examples topic.

See *Applying an immediate or high priority native command set to a device* in the *IBM Tivoli Netcool Configuration Manager NSM REST API Guide*.

1. Open `/<ncm install path>/config/properties/rseries.properties` within a text editor.
2. Edit the variable 'WorkerAdminManager/immediateNCSPoolSize' to modify the thread count reserved for the immediate execution workflow.

   **Note:** The variable 'WorkerAdminManager/maxHighPriorityPoolSize' is used in Netcool Configuration Manager 6.4.1.1 to modify the thread count reserved for the immediate execution workflow.
3. Open the GUI and select the Servers pane within the Systems Manager.
4. Edit the variable 'Max Normal Pool Size' to modify the worker server's normal thread pool.

   **Note:** Reduce the 'Max Normal Pool Size' by the same value configured for the 'WorkerAdminManager/maxHighPriorityPoolSize' for each affected worker server.

**Related tasks**

Configuring high priority queue
The High Priority Queue is a mechanism to reserve threads for dealing with high priority Units of Work created through the GUI.

# Configuring high priority queue

The High Priority Queue is a mechanism to reserve threads for dealing with high priority Units of Work created through the GUI.

During the creation of a Unit of Work the priority can be set to indicate its importance, and set it to execute before lower priority work.

The following procedure describes how to reserve threads to deal specifically with High Priority Units of Work.

For related information on setting an immediate workflow execution, or on creating a high priority import UoW, see the following topics:

- "Configuring immediate execution (Native Command Set workflow)" on page 76
- *Importing devices* in the *IBM Tivoli Netcool Configuration Manager User Guide*.

1. Open the GUI and select the Servers pane within the Systems Manager.
2. Edit the variable 'Max High Priority Pool Size' to modify the worker server's high priority thread pool.
3. Edit the variable 'Max Normal Pool Size' to modify the worker server's normal thread pool.
4. Select OK to save the new thread pool configuration.

**Related tasks**

Configuring immediate execution (Native Command Set workflow)
The 'immediate execution' workflow is a mechanism to reserve threads for dealing with high priority native command set execution via the Java or SOAP API.

**Related reference**

Configuring a pre-emptive high-priority queue

The pre-emptive high-priority queue feature allows a task in an executing high-priority Unit of Work (UOW) to pre-empt an executing task that holds the device lock on the same device.

# Configuring a pre-emptive high-priority queue

The pre-emptive high-priority queue feature allows a task in an executing high-priority Unit of Work (UOW) to pre-empt an executing task that holds the device lock on the same device.

## Behavior

The pre-emptive task interrupts the executing task being pre-empted and requests that it discontinue its operations and release the device lock. Once released, the pre-emptive task acquires the device lock and executes its operations. A pre-emptive task cannot itself be pre-empted.

A task in a UOW will pre-empt another task if and only if all of the following are true:

- The pre-emptive task's UOW priority is set to High.
- Both the pre-emptive task and the task to be pre-empted are modifying the same device.
- Both the pre-emptive task and the task to be pre-empted execute on the same Worker server.
- The task to be pre-empted is in an Executing work state.
- The task to be pre-empted is executing either an Import or a Synchronize Device to ITNCM operation.
- The high-priority queue feature is configured.
- The pre-emptive high-priority feature is configured, as described below.

**Note:** The task to be pre-empted's device driver must support pre-emption in order for this feature to function correctly. If the underlying driver does not support pre-emption, the pre-empted task, although interrupted, will not discontinue its operations and release the device lock in the manner described above, causing the interrupting pre-emptive task to fail.

## Configuration

The pre-emptive high-priority queue feature is configured on a per Worker server basis via a number of properties in the following file:
`<NCM_Install_Directory>/config/properties/rseries.properties`

*Table 13. Pre-emptive high-priority queue properties*

| Property name | Default value | Details |
|---|---|---|
| `WorkerAdminManager/ preEmptiveHighPriorityQueueActive` | `false` | This property enables (`true`) or disables (`false`) the pre-emptive high-priority queue feature on the Worker server. |
| `WorkerAdminManager/ preEmptiveHighPriorityQueueTimeout` | `600000` | The maximum time in milliseconds (ms) that a pre-emptive task will wait to acquire a lock form a pre-empted task after it has been interrupted. If the pre-emptive task does not acquire it within this time, it will fail. The default value is ten minutes. |

| Table 13. Pre-emptive high-priority queue properties (continued) | | |
|---|---|---|
| **Property name** | **Default value** | **Details** |
| `WorkerAdminManager/ preEmptiveHighPriorityQueueDeviceSleep` | `60000` | The time in milliseconds (ms) that a pre-emptive task will sleep following acquisition of the device lock from the pre-empted task in order to allow the device to reset. The default value is one minute. |
| `WorkerAdminManager/ preEmptiveHighPriorityQueueDeviceVendor1` `WorkerAdminManager/ preEmptiveHighPriorityQueueDeviceType1` | `Alcatel` `PON` | This property pair defines a Vendor/Type class of devices whose drivers support pre-emption. Additional Vendor/Type device classes whose drivers support pre-emption can be inserted as a new property pair of the same name with an incremented index, as in the code example below this table: |

**Example**

```
WorkerAdminManager/preEmptiveHighPriorityQueueDeviceVendor2=SomeVendor
WorkerAdminManager/preEmptiveHighPriorityQueueDeviceType2=SomeType
```

**Note:** After modifying `rseries.properties`, the Worker server needs to be restarted for the changes to take effect.

**Related tasks**

Configuring high priority queue
The High Priority Queue is a mechanism to reserve threads for dealing with high priority Units of Work created through the GUI.

# Deploying the keystore and user files

For installations using a distributed environment, you must copy the keystore and user files to each server, or else these servers will not be operational.

The default keystore and user files names are:

- `.intelliden.keystore`
- `.intelliden.user`

The following procedure assumes that default installation locations have been used.

**Important:** This applies to any additional presentation servers and worker servers (apart from linked worker servers).

1. Rename the following files on each worker server (the default location is `/opt/IBM/tivoli/netcool/ncm/config/properties`):

```
mv .intelliden.keystore .intelliden.keystore.original
mv .intelliden.user .intelliden.user.original
```

2. From the GUI + Worker server, from which both the **loadDBContent** and **loadDBSchema** scripts were executed, copy the `.intelliden.keystore` and `.intelliden.user` files to the following location on each worker server:
   `/opt/IBM/tivoli/netcool/ncm/config/properties`
3. Set each keystore file on each server to 'read-only' using the following command:

```
chmod 444 /opt/IBM/tivoli/netcool/ncm/config/properties/.intelliden.keystore
chmod 444 /opt/IBM/tivoli/netcool/ncm/config/properties/.intelliden.user
```

**Related tasks**

Installing a GUI and worker server
You install Netcool Configuration Manager either on a single server, or on several servers in a distributed architecture. The installation of a GUI and worker server can be part of a stand-alone installation on a single server, or it can be the first step in the installation of a distributed architecture on several servers.

Installing a worker server only
You install a Netcool Configuration Manager worker server as part of a distributed architecture deployed on one or more servers. You install one or more worker servers after having completed the installation of one or more GUI and worker servers.

# Increasing the Java Heap size

If it is intended that network resources will have large configuration sizes being processed on the Worker server, an increase in the Java heap size might be required.

The default Netcool Configuration Manager Java heap size will fail if used for the processing of large configurations. The maximum this may be increased to on 32-bit systems is 2048 MB, while for 64-bit systems there is no limit. A 64-bit JRE is highly recommended.

**Restriction:** You are restricted by the resources of your server.

**Note:** If you have a distributed setup, you need to modify the server memory settings on each server.

To increase the Java heap size, you need to locate and edit the Memory Environment script.

To set the heap space for a presentation server

1. Open
   `/<ncm install path>/bin/utils/support/setEnv.sh`
2. Edit the following WebSphere parameters as required:
   - WEBSPHERE_INITIALHEAP_SIZE
   - WEBSPHERE_MAXIMUMHEAP_SIZE
   - WEBSPHERE_MAXPERM_SIZE
3. Execute `/<ncm install path>/bin/utils/support/setWSMem.sh` to set the memory variables updated within 'setEnv.sh'.

For worker servers (including linked and standalone), and on the presentation server

4. Open
   `/<ncm install path>/bin/utils/support/setEnv.sh`
5. Edit WORKER_MEM_ARGS as required.

   **Note:** Do **NOT** run setWSMem.sh.

For IDT servers

6. Open
   `/<ncm install path>/bin/utils/support/setEnv.sh`
7. Edit IDT_MEM_ARGS as required.

   **Important:** Do **NOT** run setWSMem.sh.

After making any of these changes, restart Netcool Configuration Manager.

**Related tasks**

Installing a GUI and worker server

You install Netcool Configuration Manager either on a single server, or on several servers in a distributed architecture. The installation of a GUI and worker server can be part of a stand-alone installation on a single server, or it can be the first step in the installation of a distributed architecture on several servers.

### Configuring the Java Heap size for immediate execution (Native Command Set workflow)

In order not to overstress the system, the safest approach is for you to reduce the normal execution thread count by the number of the new immediate execution threads that you have configured.

If you choose to add the new thread pool as additional threads, then you must increase the resources for the server in question.

- If you are adding Immediate Execution threads, add (or allow) a further 200MB of RAM per thread.

For example if you currently have a 4GB Heap configured for running 20 normal execution threads on the Worker Server, and wish to add a further 2 Immediate execution threads, then the JVM Heap allocation should be increased to 4.4GB.

**Note:** The server should have enough physical or virtual RAM available to accommodate JVM Memory increases, including any memory requirements for the operating system, other applications or utilities that are run on the server.

## Internal housekeeping

By default Internal Housekeeping is not automatically run as a component. This must be manually configured by updating the `config.xml` file.

1. Access the `/opt/IBM/tivoli/netcool/ncm/config/server` directory.
2. Edit the `config.xml` file to add the Internal Housekeeping component.

   For example:

```
<component>
        <name>InternalHousekeepingComponent</name>
        <class>
        com.intelliden.internalhousekeeping.InternalHousekeepingComponent
        </class>
</component>
```

3. Save the changes made to the `config.xml` file.

For more information on housekeeping, see the *IBM Tivoli Netcool Configuration Manager Administration Guide* .

## HTTPS connection setup

This task provides information about configuring the https connection setup.

Make sure that you have selected the Secure checkbox on the UI launch screen.

You must be familiar with the command line and a text editor such as vi to perform this task.

1. To configure https connections, following the steps for 'Creating a CA certificate in SSL'.
   This procedure can be found at http://www-01.ibm.com/support/knowledgecenter/SS7JFU_7.0.0/com.ibm.websphere.express.doc/info/exp/ae/tsec_7createcacert.html
2. You will then need to make a change to the`rseries.properties` file. Access`/opt/IBM/tivoli/netcool/ncm/config/properties`.
3. Use a text editor such as vi to edit the `rseries.properties` file.
4. The configurable property is `WAS/protocol`. This should be set to**`https`**.

5. Save the changes made to the properties file, and exit.

You will need to restart the server for the changes to take effect.

## Enabling Transport Layer Security (TLS) 1.2

You can configure Netcool Configuration Manager to use the TLS 1.2 protocol.

To enable TLS 1.2, complete the following steps.

1. Edit the `/opt/IBM/tivoli/netcool/ncm/config/properties/rseries.properties` file.
2. Set the `WAS/protocol` property to `https`.
3. Save the changes made to the properties file, and exit.
4. Restart the Netcool Configuration Manager server.
5. Log into the Netcool Configuration Manager client and run the following script with one of the valid options:

   ```
   ncm/bin/utils/configFIPSmode.sh disabled | warn | strict
   ```

   Where:

   - `disabled` — Disables FIPS 140-2 mode. In this mode there is no guarantee that either server or client is using a FIPS compliant cipher for secure communications and the availability of a FIPS compliant cipher provider is not checked on either the server or the client.
   - `warn` — Enables FIPS 140-2 mode. When Netcool Configuration Manager is operating in FIPS WARN mode, the system issues a warning to any user attempting a secure connection using a non-FIPS compliant algorithm on the client. Such clients have the option of proceeding with their secure connection using their non-FIPS compliant provider or aborting the connection. GUI clients are warned by a pop up dialogue when connecting (in both SSO and login mode). Java API clients are warned that their secure connection is non-FIPS compliant through an exception of class `com.intelliden.icos.SecurityException`. During system start up (`itncm.sh start`) the system prints a warning message on the console (STDERR) if the IBMJCEFIPS provider is not configured in the server's JRE.
   - `strict` — Enables FIPS 140-2 mode. This option allows only FIPS compliant algorithms. Use of non-FIPS algorithms will be prevented. In other words, clients (including API clients) that attempt to make a secure connection, but are not using a FIPS compliant cipher provider are rejected by the Netcool Configuration Manager server. GUI clients are informed via a pop up dialogue. Java API clients receive an exception of class `com.intelliden.icos.SystemException`.

   **Note:** You only need to run this script once from one of the Presentation servers. In STRICT mode, if the server's JRE is not configured with the IBMJCEFIPS provider, the system will not start up (and `itncm.sh start` will print an error message and exit with error code 1).
6. On each Presentation Server, log into the WAS console from the following URL:

   ```
   http://hostname:16316/ibm/console
   ```

   a) At the **User ID:** field, specify the super user ID.

   b) At the **Password:** field, specify the super user password.
7. Configure Netcool Configuration Manager to use the National Institute of Standards and Technology (NIST) Special Publications 800-131a (SP800-131) standard.

   a) Click **Security** > **SSL certificate and key management**.

   b) Select **Manage FIPS** under Configuration Settings, then select **SP800-131**.

   c) Click **Apply** and **OK**, then click **Save** under messages.
8. Configure `java.security` to enable IBMJCEFIPS:

   **Note:** Perform this and subsequent steps on both the Presentation and Worker servers.

a) Open the *install_dir*/eWAS/java/jre/lib/security/java.security file in a text editor.

b) Uncomment the IBMJCEFIPS provider (com.ibm.crypto.fips.provider.IBMJCEFIPS) entry before the IBMJCE provider entry, and also renumber the other providers in the provider list.

The IBMJCEFIPS provider must be in the `java.security` file provider list. See the example at the end of this topic.

9. Enable your browser to use TLS 1.2. Refer to the documentation for your browser, platform and version combination.

Use the following steps as examples:

- Microsoft Internet Explorer: Open Internet Explorer and click **Tools** > **Internet Options**. On the **Advanced** tab, select the **Use TLS 1.2** option.
- Firefox: Enter `about:config` in the address bar. Locate the `security.tls.version.min` property. Right-click the property and click **Modify**. Set the value to 3.

10. Optional: Export Lightweight Third Party Authentication keys so applications that use these LTPA keys can be reconfigured.

a) In the navigation pane, click **Settings** > **Websphere Admin Console** and click **Launch Websphere Admin Console**.

b) In the WebSphere Application Server administrative console, select **Settings** > **Global security**.

c) In the Global security page, from the Authentication area, click the **LTPA** link.

d) Under **Cross-cell single sign-on**, specify a key file and provide a filename and password for the file that will contain the exported LTPA keys.

e) Click **Export keys**.

11. Optional: For SSO, enable FIPS for any other application server, then import the updated LTPA keys from the first server into these servers:

a) Copy the LTPA key file to another application server computer.

b) In the navigation pane, click **Settings** > **Websphere Admin Console** and click **Launch Websphere Admin Console**.

c) In the WebSphere Application Server administrative console, select **Settings** > **Global security**.

d) In the Global security page, from the Authentication area, click the **LTPA** link.

e) Under **Cross-cell single sign-on**, provide the filename and password from above for the file that contains the exported LTPA keys.

f) Click **Import keys**.

12. Edit the `profile/properties/ssl.client.props` file within the Jazz for Service Management installation directory, and set the `com.ibm.ssl.protocol` to `TLSv1.2`.
13. Restart the Netcool Configuration Manager server.

## Configuration of eventpollers.xml file

In a deployment of two or more Netcool Configuration Manager presentation servers with one Network Manager IP Editionserver reporting SNMP traps raised by Netcool Configuration Manager, two events are generated by default for each presentation server when a UOW is submitted on one server.

The default eventpollers.xml file is configured to work optimally with one presentation server. In a deployment strategy encompassing n Netcool Configuration Manager presentation servers, where n > 1, the file must be changed. The `eventpollers.xml` file is located under `/opt/IBM/tivoli/netcool/ncm/config/server`.

**Note:** The pollerid must be the same on both servers.

## Creating a Worker server general resource

You must update the server name for the default Worker Server general resource (GR) that has been created.

Ensure that the Netcool Configuration Manager server is running.

1. Navigate to the Resource Browser by locating it within the tree structure on the left hand side of the screen.
2. Locate the Worker server GR, right click to select, then click **Edit**.
3. Replace the server id with that of your Worker Server name.

   For example:

```
<workserver>
        <server id="<Name of your Server>">
                <delayseconds>0</delayseconds>
        </server>
</workserver>
```

4. Save the changes, exit the text editor, and then restart Netcool Configuration Manager.

## Importing sample compliance policies

You can import sample compliance policies. These policies have been installed by default, and after you have imported them they will be available in the Netcool Configuration Manager - Compliance UI.

Before sample policies can be viewed, access permissions must be granted.

**Note:** Policies exported from a previous version of Netcool Configuration Manager can be imported into the most current version, but some errors may be reported.

1. Locate the sample policy folder:
   `/opt/IBM/tivoli/netcool/ncm/compliance/db/export/samplePolicies`
2. Copy the sample policies from the original location to the following directory:
   `/opt/IBM/tivoli/netcool/ncm/compliance/db/export/tables`

   You can use the following command:

```
cp /opt/IBM/tivoli/netcool/ncm/compliance/db/export/samplePolicies/
sample_policies.tar
/opt/IBM/tivoli/netcool/ncm/compliance/db/export/tables
```

3. Locate the `/opt/IBM/tivoli/netcool/ncm/compliance/db/export/tables` directory and access the `sample_policies.tar` tar file. You can use the following command:
   `tar xvf sample_policies.tar`

   **CAUTION:** This step overwrites existing policies. Back up existing policy xml files, if required.
4. In the `/opt/IBM/tivoli/netcool/ncm/compliance/bin/utils` directory, run the following script to install the sample policies, and merge these with any existing policies:
   `./dbImport.sh`
5. To grant access privileges to the users who requires read access to the sample policies, use **AdminUser SecurityRealm Access Control**, and then add the user to **Allowed Groups**.

## Enabling auto-restart of Netcool Configuration Manager after reboot

You must enable the automatic restart of Netcool Configuration Manager after a server reboot.

1. Login to the server as `root`.
2. Access the utils folder. The default directory is: `../ncm/bin/utils`

3. Within this directory, run the command enabling automatic startup following reboot:
   `./createAutoStart.sh`

## Changing platform configuration

You can change platform configuration by running the `setPlatform.sh` script.

Use this script to change the configuration of a platform. When you run it, you get the current status.

1. Run the script by typing the following command: `bash-3.2$ ./setPlatform.sh`
   The current platform configuration is displayed.
   For example:

```
Platform Type = GUI + Worker Server
Compliance Core = Enabled
Reporting = Enabled
Do you wish to change the current configuration of this deployment? [y/n]
```

2. Change the current configuration as required.

The list of options presented depends on you current configuration. For example, you may be offered the following choices:

```
1. GUI + Worker Server : Compliance Core=Enabled
2. GUI + Worker Server : Compliance Core=Disabled
3. Worker Server : Base=Enabled  | Compliance Eval Engine=Enabled
4. Worker Server : Base=Enabled  | Compliance Eval Engine=Disabled
5. Worker Server : Base=Disabled | Compliance Eval Engine=Enabled
6. Reporting=Enabled
7. Reporting=Disabled
0. Exit this utility

Please choose an option from the list above (1-7) or 0 to exit this utility.
```

**Related tasks**

Installing a GUI and worker server
You install Netcool Configuration Manager either on a single server, or on several servers in a distributed architecture. The installation of a GUI and worker server can be part of a stand-alone installation on a single server, or it can be the first step in the installation of a distributed architecture on several servers.

Installing a worker server only
You install a Netcool Configuration Manager worker server as part of a distributed architecture deployed on one or more servers. You install one or more worker servers after having completed the installation of one or more GUI and worker servers.

## Configuring mail servers

You configure the mail server properties for both Netcool Configuration Manager - Base and Netcool Configuration Manager - Compliance.

You configure mail server properties in the `rseries.properties` and `WorkFlowManager.properties` files.

1. To configure the mail server for the Netcool Configuration Manager - Base presentation and worker servers, perform the following edits for each server:
   a) Access `rseries.properties`:
      i) `cd <install_dir>/config/properties`
      ii) `vi rseries.properties`
   b) Search for the `core/smtp` property and enter the mail server hostname.
   c) Set `Notification/sendmail= true`
2. To configure the mail server for the Netcool Configuration Manager - Compliance server, perform the following edits for each server:

a) Access `WorkFlowManager.properties`:

i) `cd <install_dir>/compliance/config/properties`

ii) `vi WorkFlowManager.properties`

b) Search for the `mailHost` property and enter the mail server hostname.

c) Optionally, change the settings for the following properties:

- `mailFrom`
- `mailDebug` (set to `true` to log debug information to Netcool Configuration Manager - Compliance log files)

3. When done, restart Netcool Configuration Manager.

## Enabling and disabling FIPS 140-2 mode

Use this information to either enable or disable FIPS 140-2 mode.

The following table identifies the available scenarios for enabling FIPS 140-2 mode on Netcool Configuration Manager.

**Note:** Before enabling FIPS 140-2 mode, ensure that you have configured the HTTPS connection setup.

For more information, see "HTTPS connection setup" on page 80.

| FIPS enable scenarios | Main steps |
|---|---|
| Netcool Configuration Manager stand alone without Tivoli Common Reporting | 1. Enable FIPS 140-2 mode for the embedded WebSphere Application Server (eWAS)<br>2. Enable FIPS 140-2 mode for the eWAS JRE<br>3. Enable FIPS 140-2 mode for Netcool Configuration Manager |
| Netcool Configuration Manager stand alone with Tivoli Common Reporting | 1. Enable FIPS 140-2 mode for the embedded eWAS<br>2. Enable FIPS 140-2 mode for the embedded eWAS JRE<br>3. Enable FIPS 140-2 mode for Netcool Configuration Manager<br>4. Enable FIPS 140-2 mode for Tivoli Common Reporting |
| Netcool Configuration Manager bundled with Network Manager IP Edition and Tivoli Netcool/OMNIbus | 1. Enable FIPS 140-2 mode for the embedded eWAS<br>2. Enable FIPS 140-2 mode for the embedded eWAS JRE<br>3. Enable FIPS 140-2 mode for Netcool Configuration Manager<br>4. Enable FIPS 140-2 mode for Tivoli Common Reporting<br>5. Enable FIPS 140-2 mode for Network Manager IP Edition and Tivoli Netcool/OMNIbus |

The following table identifies the available scenarios for disabling FIPS 140-2 mode on Netcool Configuration ManagerITNCM.

| FIPS disable scenarios | Main steps |
|---|---|
| Netcool Configuration Manager stand alone without Tivoli Common Reporting | 1. Run the `configFIPSmode.sh` script with the `disabled` option. |
| Netcool Configuration Manager stand alone with Tivoli Common Reporting | 1. Run the `configFIPSmode.sh` script with the `disabled` option. |

| FIPS disable scenarios | Main steps |
|---|---|
| Netcool Configuration Manager bundled with Network Manager IP Edition and Tivoli Netcool/OMNIbus | 1. Run the `configFIPSmode.sh` script with the `disabled` option.<br>2. Disable FIPS 140-2 mode for Network Manager IP Edition and Tivoli Netcool/OMNIbus |

**Related reference**

FIPS 140-2 requirements

To configure Netcool Configuration Manager with the intent to comply with FIPS 140-2 specifications, you must run Drivers version 20 or later and configure the HTTPS connection setup.

## Enabling FIPS

You can configure Netcool Configuration Manager to use Federal Information Processing Standard Java™ Secure Socket Extension files.

Ensure you have completed the HTTPS set up task: "HTTPS connection setup" on page 80

Follow these steps to enable FIPS 140–2 mode for the embedded WebSphere Application Server (eWAS), embedded eWAS JRE, and Netcool Configuration Manager.

1. Log into the Netcool Configuration Manager client and run the following script with one of the valid options:

   ```
   ncm/bin/utils/configFIPSmode.sh disabled | warn | strict
   ```

   Where:

   - `disabled` — Disables FIPS 140-2 mode. In this mode there is no guarantee that either server or client is using a FIPS compliant cipher for secure communications and the availability of a FIPS compliant cipher provider is not checked on either the server or the client.
   - `warn` — Enables FIPS 140-2 mode. When Netcool Configuration Manager is operating in FIPS WARN mode, the system issues a warning to any user attempting a secure connection using a non-FIPS compliant algorithm on the client. Such clients have the option of proceeding with their secure connection using their non-FIPS compliant provider or aborting the connection. GUI clients are warned by a pop up dialogue when connecting (in both SSO and login mode). Java API clients are warned that their secure connection is non-FIPS compliant through an exception of class `com.intelliden.icos.SecurityException`. During system start up (`itncm.sh start`) the system prints a warning message on the console (STDERR) if the IBMJCEFIPS provider is not configured in the server's JRE.
   - `strict` — Enables FIPS 140-2 mode. This option allows only FIPS compliant algorithms. Use of non-FIPS algorithms will be prevented. In other words, clients (including API clients) that attempt to make a secure connection, but are not using a FIPS compliant cipher provider are rejected by the Netcool Configuration Manager server. GUI clients are informed via a pop up dialogue. Java API clients receive an exception of class `com.intelliden.icos.SystemException`.

   **Note:** You only need to run this script once from one of the Presentation servers. In STRICT mode, if the server's JRE is not configured with the IBMJCEFIPS provider, the system will not start up (and `itncm.sh start` will print an error message and exit with error code 1).
2. On each Presentation Server, log into the Integrated Solutions Console (ISC) from the following URL:

   ```
   http://hostname:18100/ibm/console
   ```

   a) At the **User ID:** field, specify the super user ID.

   b) At the **Password:** field, specify the super user password.
3. Configure Netcool Configuration Manager to use FIPS.

   a) Click **Security** > **SSL certificate and key management**.

b) Select **Manage Fips** under Configuration Settings, then select **Enable FIPS 140-2**.

c) Click **Apply** and **OK**, then click **Save** under messages.

d) Log out of the ISC.

4. Configure `java.security` to enable IBMJCEFIPS:

   **Note:** Perform this and subsequent steps on both the Presentation and Worker servers.

   a) Open the *install_dir*/eWAS/java/jre/lib/security/java.security file in a text editor.

   b) Uncomment the IBMJCEFIPS provider (com.ibm.crypto.fips.provider.IBMJCEFIPS) entry before the IBMJCE provider entry, and also renumber the other providers in the provider list.

   The IBMJCEFIPS provider must be in the `java.security` file provider list. See the example at the end of this topic.

5. Enable your browser to use Transport Layer Security (TLS) 1.0:

   - Microsoft Internet Explorer: Open the Internet Explorer and click **Tools** > **Internet Options**. On the **Advanced** tab, select the **Use TLS 1.0** option.
   - Firefox: TLS 1.0 is enabled by default.

6. Export Lightweight Third Party Authentication keys so applications that use these LTPA keys can be reconfigured.

   a) In the navigation pane, click **Settings** > **Websphere Admin Console** and click **Launch Websphere Admin Console**.

   b) In the WebSphere Application Server administrative console, select **Settings** > **Global security**.

   c) In the Global security page, from the Authentication area, click the **LTPA** link.

   d) Under **Cross-cell single sign-on**, specify a key file and provide a filename and password for the file that will contain the exported LTPA keys.

   e) Click **Export keys**.

7. For SSO, enable FIPS for any other application server, then import the updated LTPA keys from the first server into these servers:

   a) Copy the LTPA key file to another application server computer.

   b) In the navigation pane, click **Settings** > **Websphere Admin Console** and click **Launch Websphere Admin Console**.

   c) In the WebSphere Application Server administrative console, select **Settings** > **Global security**.

   d) In the Global security page, from the Authentication area, click the **LTPA** link.

   e) Under **Cross-cell single sign-on**, provide the filename and password from above for the file that contains the exported LTPA keys.

   f) Click **Import keys**.

8. Restart the Netcool Configuration Manager server.

The *install_dir*/eWAS/java/jre/lib/security/java.security file looks like this when IBMJCEFIPS is enabled on a Linux or AIX system:

```
security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.jsse.IBMJSSEProvider
security.provider.4=com.ibm.jsse2.IBMJSSEProvider2
security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
security.provider.6=com.ibm.security.cert.IBMCertPath
security.provider.7=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl
security.provider.8=com.ibm.security.cmskeystore.CMSProvider
security.provider.9=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
security.provider.10=com.ibm.security.sasl.IBMSASL
security.provider.11=com.ibm.xml.crypto.IBMXMLCryptoProvider
security.provider.12=com.ibm.xml.enc.IBMXMLEncProvider
security.provider.13=org.apache.harmony.security.provider.PolicyProvider
```

### Connecting to the Webstart GUI with FIPS enabled

This section explains how to connect to the webstart GUI when FIPS is enabled.

1. Configure java.security to enable IBMJCEFIPS.
   a) Open the *JAVA_HOME*/java/jre/lib/security/java.security file in a text editor.
   b) Add the IBMJCEFIPS provider (security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS) entry before any other entry, and also renumber the other providers in the provider list. The IBMJCEFIPS provider must be in the java.security file provider list.
2. Export the default trust certificate from the presentation server you wish to connect to from Install_dir/eWAS/profiles/RSeries/etc/trust.p12.

   **Example command to export certificate:**
   ```
   Install_dir/eWAS/java/jre/bin/keytool -export -alias default -storepass
   WebAS -file Install_dir/ncmtrust.crt -storetype PKCS12 -keystore
   Install_dir/eWAS/profiles/RSeries/etc/trust.p12
   ```
3. Import the exported certificate from step 2 to your local Java cacert.

   **Example command:**
   ```
   c:\Program Files\IBM\Java70\jre\bin>keytool.exe -import -alias ncmaix01trust
   -trustcacerts -file C:\ncmaix01trust.crt -keystore "C:\Program Files\IBM\
   Java70\jre\lib\security\cacerts"
   ```
   - When prompted for the password the default for the java keystore is 'changeit' unless the user has previously changed it.
   - Accept the certificate.

If you are enabling FIPS 140-2 mode for Netcool Configuration Manager stand alone with Tivoli Common Reporting, your next task is to enable FIPS 140-2 mode on Tivoli Common Reporting.

For information on enabling FIPS 140-2 mode for Tivoli Common Reporting, see the 'Enabling Federal Information Processing Standard' topic at the following URL: www-01.ibm.com/support/knowledgecenter/SSH2DF_2.1.0/ttcr_enabling_fips_overview.html.

## Disabling FIPS

You can configure Netcool Configuration Manager to not use Federal Information Processing Standard Java Secure Socket Extension files.

Follow these steps to disable FIPS 140–2 mode for the embedded WebSphere Application Server (eWAS), embedded eWAS JRE, and Netcool Configuration Manager.

Log into the Netcool Configuration Manager client and run the following script with the `disabled` option:

```
ncm/bin/utils/configFIPSmode.sh disabled
```

Where:

- `disabled` — Disables FIPS 140-2 mode.

**Note:** You only need to run this script once from one of the Presentation Servers.

# Configuring reporting on a stand-alone installation

If Netcool Configuration Manager Reporting has been installed stand-alone, there are a number of configuration steps which must be followed to access the reports.

**Restriction:** Fix Pack 3 This topic **does not** apply to Netcool Configuration Manager installations on Linux on System z.

Access the Tivoli Common Reporting installation directory, for example `/opt/IBM/JazzSM/profiles/bin` and execute the start server command:

```
startServer.sh server1
```

This should start the Tivoli Common Reporting Server.

This task describes how to configure Netcool Configuration Manager Reporting on a stand-alone installation.

1. Launch the WebSphere administration console on which Reporting Services has been installed using one of the following two ways (it may be different to the one hosting the main NCM Presentation Server):
   - Connect to the port directly.
   - Launch it from within DASH, from where Common Reporting can be accessed.
2. The WebSphere Administration console login screen displays. Log in as the DASH administration user, and use the password you supplied at install time.
3. On the left hand side of the screen, expand the **Users and Groups** selection. Next, click on **Manage Users**.
4. Select the **Create** button. Create a user that matches a user in Netcool Configuration Manager , for example, administrator. Select the **Create** button to complete.
5. From the menu choices on the left hand side of the screen, click on the **User Roles** link, and select the **Search** button. The user you just created will be displayed. Click on that user.
6. From the **Available Roles** menu, select the **`tcrPortalOperator`** role checkbox. Click on the **Save** button to finish.
7. Log out of the DASH, and log back in as the user you have just created.
8. Expand the **Reporting** option, and click on the **ITNCMReports** link.

For more information, see the *IBM Tivoli Netcool Configuration Manager User Guide*.

**Related tasks**

Installing the product in silent mode
Silent installation requires an XML response file that defines the installation configuration. Silent mode is useful if you want identical installation configurations on multiple workstations.

Installing a GUI and worker server
You install Netcool Configuration Manager either on a single server, or on several servers in a distributed architecture. The installation of a GUI and worker server can be part of a stand-alone installation on a single server, or it can be the first step in the installation of a distributed architecture on several servers.

Installing a worker server only
You install a Netcool Configuration Manager worker server as part of a distributed architecture deployed on one or more servers. You install one or more worker servers after having completed the installation of one or more GUI and worker servers.

Installing ITNCM-Reports
If you are not integrating with Network Manager, which ships with its own version of DASH, you must install ITNCM-Reports separately in order to access the reporting functionality.

Installing ITNCM-Reports in silent mode
If you are not integrating with Network Manager, which ships with its own version of DASH, you must install ITNCM-Reports separately in order to access the reporting functionality.

## [zLinux] Configuring Cognos Analytics for ITNCM Reports

To configure ITNCM Reports for Cognos Analytics for an installation of Netcool Configuration Manager on Linux on System z, you must perform a number of configuration tasks in the order suggested.

**Restriction:** This section **only** applies to Netcool Configuration Manager installations on Linux on System z.

## [zLinux] Configuring LDAP for Cognos Analytics

When installing Netcool Configuration Manager on Linux on System z and using Cognos Analytics to view ITNCM reports, you must configure the LDAP server on Cognos Analytics, and then add the LDAP user IDs to the Netcool Configuration Manager administrator group.

**Restriction:** This topic **only** applies to Netcool Configuration Manager installations on Linux on System z.

For information on LDAP v3 namespace configuration in Cognos, see the following IBM Support document: http://www-01.ibm.com/support/docview.wss?uid=swg21612936

1. Configure an LDAP Namespace.

   For instructions, see the following configuration topic in the Cognos Analytics Knowledge Center: https://www.ibm.com/support/knowledgecenter/en/SSEP7J_10.1.1/com.ibm.swg.ba.cognos.c8pp_inst.10.1.1.doc/t_configureanldapnamespace.html
2. In ITNCM Account Administration, add all the LDAP user IDs that are to run ITNCM Reports for Cognos Analytics to the Netcool Configuration Manager administrator group.

## [zLinux] Preparing Cognos to connect to a DB2 content store

Use the Cognos Configuration tool to prepare Cognos Analytics for a DB2 connection.

**Restriction:** This topic **only** applies to Netcool Configuration Manager installations on Linux on System z.

1. Use the Cognos Configuration tool to create a DB2 content store database configuration, generate the DDL and then execute the generated DDL.

   For information on generating a script file to create a database for a DB2 content store, see the following Knowledge Center topic: https://www.ibm.com/support/knowledgecenter/en/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.inst_cr_winux.doc/t_db2contentstorescript.html
2. Use the Cognos Configuration tool to configure the Cognos URIs.

## [zLinux] Cataloging the DB2 database

When installing Netcool Configuration Manager on Linux on System z, and using Cognos Analytics to view ITNCM reports, you must obtain and install the DB2 runtime client, catalogue the TCP/IP node (that is, the platform running the DB2 database), and also catalogue the DB2 database instance.

**Restriction:** This topic **only** applies to Netcool Configuration Manager installations on Linux on System z.

Installation of the DB2 database is a prerequisite, which is described in the DB2 Knowledge Center. You can access the DB2 Knowledge Center at the following link: http://www-01.ibm.com/support/knowledgecenter/SSEPGG_9.5.0/com.ibm.db2.luw.doc/welcome.html

For information on configuring the DB2 Run Time Client, see the 'Configuring client-to-server connections using the command line processor' topic at the following link: http://www-01.ibm.com/support/knowledgecenter/SSEPGG_9.5.0/com.ibm.db2.luw.qb.client.doc/doc/t0007243.html

You can install the DB2 runtime client after installing Netcool Configuration Manager. If you do, ensure you then catalog the Netcool Configuration Manager database using the same alias that you used during the Netcool Configuration Manager installation.

1. Download the DB2 Run Time Client.

   The runtime client can be obtained at the IBM Support Portal.

   a. On the IBM Support Portal, navigate to the **Downloads** tab and search for the version of the DB2 Run Time Client that you want to download.
   b. Select the appropriate link to display a table that lists the DB2 download packages.
   c. To download the DB2 Run Time Client, select the appropriate package from the table.

   For more information on the supported versions of DB2, see “Software requirements” on page 5.
2. Install the DB2 Run Time Client as `root` user.

a) Unzip and untar the file.

The `rtcl` directory is created.

b) From the `rtcl` directory, run the `db2_install` command.

You can install the client locally or anywhere else, such as the `icosuser` home directory.

**Remember:** You need to specify this directory when installing the Netcool Configuration Manager.

As part of the installation, the `sqllib` subdirectory is created in the install directory of the runtime client.

3. Catalog the TCP/IP Node (the platform running the DB2 database) using the following command:
`db2 catalog tcpip node <node name> remote <db server's fully qualified domain name> server <db port>`

**Tip:** The node name is discretionary.

4. Catalog the DB2 database instance using the following command:

```
db2 catalog database <database name> at node <node name>
db2 catalog database itncm at node dbnode
db2 terminate
```

5. Test your connection using the following command:
`db2 connect to <database name> user <db username>`

## [zLinux] Sourcing the DB2 client library and sourcing the DB2 profile

To use Cognos Analytics to access ITNCM Reports, you source the DB2 client library and the DB2 profile.

Source the DB2 client library

1. Within the DB2 client install directory, add `/opt/ibm/db2/V9.5/lib32` to `/etc/ld.so.conf` and then issue the **`ldconfig`** command to regenerate dynamically linked libraries.

Source the DB2 profile

2. Create a profile that sources the `sqllib/db2profile` from the DB2 user's home directory.

For example, the content of your profile will be similar to the following:

```
if
[-f/home/db2user/sqllib/db2profile];then
./home/db2user/sqllib/db2profile
fi
```

Configure LDAP

3. Use the Cognos Configuration tool to configure an LDAP server as a user repository.

For more information on LDAP v3 namespace configuration in Cognos, see the following IBM Support technote: http://www-01.ibm.com/support/docview.wss?uid=swg21612936

4. Configure an LDAP namespace, as described in the following Knowledge Center topic:

https://www.ibm.com/support/knowledgecenter/en/SSEP7J_10.1.1/com.ibm.swg.ba.cognos.c8pp_inst.10.1.1.doc/t_configureanldapnamespace.html

## [zLinux] Configuring the Cognos datasource

To use Cognos Analytics to access ITNCM Reports, you configure a data source for the ITNCM database.

**Restriction:** Fix Pack 3 This topic **only** applies to Netcool Configuration Manager installations on Linux on System z.

You can access the Cognos Analytics Version 11.0 Knowledge Center for more data source and connections information at the following location: https://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.ug_cra.doc/c_datasources.html

**DB2 Data Sources**

https://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.ug_cra.doc/c_db2_ds.html#DB2_ds

**Creating a data source connection**
https://www.ibm.com/support/knowledgecenter/SSEP7J_11.0.0/com.ibm.swg.ba.cognos.ug_cra.doc/t_asg_createdatasource.html#ASG_CreateDataSource

1. In IBM Cognos Administration, select the Configuration tab, then click **Data Source Connections** > **New Data Source**.
2. On the name and description page, enter `ITNCM` in the **Name** field. Optionally, enter a description and screen tip, and then click **Next**.
3. On the connection page, open the **Type** drop-down list, and select **New Data Source**.

   The New Data Source wizard opens.
4. Select **IBM DB2** from the list of data sources.
5. Deselect **Configure JDBC Connection**, then click **Next**.
6. Specify the connection parameters for the connection string.

   **DB2 database name**
   Enter the ITNCM database name

   **Signon**
   Provide the user ID and password

   **Testing**
   Test the connection before proceeding

## [zLinux] Securing access to Cognos Connection

Before allowing zLinux users to view the reports, you restrict access to Cognos Connection to authorized users only.

**Restriction:** This topic **only** applies to Netcool Configuration Manager installations on Linux on System z.

When you add an authentication provider in Cognos Configuration, all users in the directory have access to IBM Cognos Connection. To secure access, see the techniques documented at the following location:https://www.ibm.com/support/knowledgecenter/en/SSEP7J_10.2.0/com.ibm.swg.ba.cognos.crn_arch.10.2.0.doc/c_securing_access_to_cognos_connection.html

You can use the Cognos namespace to restrict access. Before you use this method, ensure that authorized users and groups belong to at least one IBM Cognos group or role. For more information, see the following Cognos Knowledge Center topic: https://www.ibm.com/support/knowledgecenter/en/SSEP7J_10.2.0/com.ibm.swg.ba.cognos.crn_arch.10.2.0.doc/c_restrict_user_access_to_the_cognos_namespace.html

1. In Cognos Connection: For ITNCM Reports, create the following roles: `NCM_Admin` and `NCM_User`, and then add LDAP user IDs to these roles.
2. In Cognos Connection (for the ITNCM reports): Set permissions for members of the NCM_User roles to **Traverse** and **Execute** only.
3. Optional: Add the user accounts, groups, and roles created in your authentication provider to the Cognos namespace.
4. Remove the group `Everyone` from the built-in and predefined Cognos groups and roles.

   **Note:** By default, the group `Everyone` is a member of all built-in and predefined groups and roles in the Cognos namespace.

## [zLinux] RHEL and SUSE: Configuring an Oracle datasource to use ODBC

First you install platform-specific versions of unixODBC, then configure them.

**Restriction:** This topic **only** applies to Netcool Configuration Manager installations on Linux on System z.

Install unixODBC

1. Perform the following platform-specific installation steps for unixODBC.

- For SUSE Linux Enterprise Server 12, you compile the unixODBC Driver Manager on Linux operating systems for use with CLI and ODBC applications. For the s390x platform, unixODBC needs to be compiled as a 31-bit application.

  a. Download the latest unixODBC source code from the following location: http://www.unixodbc.org

  b. Untar the source files:

  ```
  gunzip unixODBC-2.3.4.tar.gz
  tar -xvf unixODBC-2.3.4.tar
  ```

  c. Install the gcc-32bit Compiler package:

  ```
  [root]:#~ zypper install gcc-32bit
  ```

  d. Set the following environment variables:

  ```
  [root]:# export CFLAGS=-m31 LDFLAGS=-m31 CXXFLAGS=-m31
  ```

  e. Change to the `/install_location/unixODBC-2.3.4` directory.

  f. Install the driver manager in the default `/usr/localprefix` directory:

  ```
  ./configure
  ```

  g. Build and install the driver manager:

  ```
  make
  make install
  ```

  Libraries are copied to the `[prefix]/libdirectory`, and executable files are copied to the `[prefix]/bindirectory`

  h. Add the unixODBC library directory `/usr/local/lib` to `/etc/ld.so.conf` and issue the ldconfig command to regenerate dynamically linked libraries.

- For RHEL 7, you install 31 bit unixODBC pkg and associated dependencies for zLinux:

  ```
  [root]# yum install unixODBC.s390
  ```

Configure unixODBC

2. Download the appropriate versions of the Oracle Instant Client Package from the following Oracle support site: http://www.oracle.com/technetwork/topics/zlinuxsoft-096525.html

   - Oracle Instant Client Package Basic 31bit
   - Oracle Instant Client Package ODBC 31bit

   Example for Oracle 12.1.0.2.0:

   **instantclient-basic-linux.zseries31-12.1.0.2.0.zip**
   Unpack the Oracle Instant Client Package Basic 31bit into `/opt/oracle/clients` to create the instantclient_12_1 file.

   **instantclient-odbc-linux.zseries31-12.1.0.2.0.zip**
   Unpack Oracle Instant Client Package ODBC 31bit into the same directory.

3. Create `/etc/oracle/tnsnames.ora` and define the ITNCM DB connection details.

   ```
   ITNCM= (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)
   (HOST = <Fully qualified Domain Name>)(PORT = <Port on which
   the Oracle database is listening>)) ) (CONNECT_DATA =
   (SERVER = DEDICATED) (SERVICE_NAME = ITNCM) (INSTANCE_NAME=ORCL) ))
   ```

   **Tip:** INSTANCE_NAME is usually ORCL

   Check the SERVICE_NAME and INSTANCE_NAME using the lsnrctl application, status command on the server running the ITNCM Oracle database.

Example `tnsnames.ora`:

```
ITNCM= (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)
(HOST = myhost.example.com)(PORT = 1521)) )
(CONNECT_DATA = (SERVER = DEDICATED)
(SERVICE_NAME = ITNCM) (INSTANCE_NAME=ORCL) ))
```

4. Point to the location of the `tnsnames.ora` file using one of the following techniques:
   - Create a profile script `/etc/profile.d/oracle_instant_client.sh` to define the location of the tnsnames.ora file.
   - Export the TNS_ADMIN variable that points to the directory containing the tnsnames.ora file.

     ```
     export TNS_ADMIN=/etc/oracle

     #!/bin/bash
     TNS_ADMIN=/etc/oracle
     export TNS_ADMIN
     ```

     Source the oracle_instant_client if not already configured in your unix login profile

     ```
     . /etc/profile.d/oracle_instant_client.sh
     ```

     Verify that the TNS_ADMIN environment variable is set correctly

     ```
     [root]# echo $TNS_ADMIN
     ```
5. Add the Oracle library directory `/opt/oracle/clients/instantclient_12_1` to `/etc/ld.so.conf` and use the ldconfig command to regenerate dynamically linked libraries.
6. Configure and install the unixODBC Driver Manager by locating the `odncinst.ini` and `odbc.ini` files using the `odbcinst` command.

   ```
   root]# odbcinst -j
   unixODBC 2.3.1
   DRIVERS............: /etc/odbcinst.ini
   SYSTEM DATA SOURCES: /etc/odbc.ini
   FILE DATA SOURCES..: /etc/ODBCDataSources
   USER DATA SOURCES..: /root/.odbc.ini
   SQLULEN Size.......: 4
   SQLLEN Size........: 4
   SQLSETPOSIROW Size.: 2
   ```
7. Configure `odncinst.ini` and `odbc.ini`

   a) `odncinst.ini` example:

   ```
   [OracleODBC-12c]
   Description=TEST ODBC
   Driver=/opt/oracle/clients/instantclient_12_1/libsqora.so.12.1
   Setup=
   FileUsage=1
   CPTimeout=5
   CPReuse=5
   UsageCount=5
   ```

   **Note:** The 'Driver' value is the path to the Oracle libsqora.so.12.1 library.

   b) `odbc.ini` example:

   ```
   [ITNCM]
   Description="TEST"
   Driver=OracleODBC-12c
   DSN=OracleODBC-12c
   ServerName=ITNCM
   ```
8. After you have configured `odncinst.ini` and `odbc.ini` you install the driver and system DSN:

   a) Install the driver:

   ```
   [root]# odbcinst -i -d -f /etc/odbcinst.ini
   odbcinst: Driver installed. Usage count increased to 5.
      Target directory is /etc
   ```

```
odbcinst: Driver installed. Usage count increased to 5.
   Target directory is /etc
```

b) Install system DNS:

```
[root]# odbcinst -i -s -l -f /etc/odbc.ini
```

c) Test your system DSN installation by listing your installed data sources:

```
[root] # odbcinst -s -q
[ITNCM]
```

d) Use the isql tool to test a connection to the ITNCM database via ODBC.

```
[root]# isql -v ITNCM <UserID> <Password>
+---------------------------------------+
| Connected! |
| |
| sql-statement |
| help [tablename] |
| quit |
| |
+---------------------------------------+
SQL>
```

9. As the root user, change the access permissions to r-w for the directory containing the `odncinst.ini` and `odbc.ini` files.
10. Configure a ODBC datasource to connect to the ITNCM db in Cognos.
    a) In IBM Cognos Administration, select the Configuration tab, then click **Data Source Connections** > **New Data Source**.
    b) On the name and description page, enter `ITNCM` in the **Name** field. Optionally, enter a description and screen tip, and then click **Next**.
    c) On the connection page, open the **Type** drop-down list, and select **New Data Source**.
    d) Select **IBM Oracle** from the list of data sources.
    e) Deselect **Configure JDBC Connection**, then click **Next**.
    f) Specify the connection parameters for the connection string.
11. In Netcool Configuration Manager **ITNCM Account Management** > **Users**: In order for a user ID to be able to run the reports, map the LDAP user IDs exactly into Netcool Configuration Manager and assign the user ID to the Administrator group.

## [zLinux] Import ITNCM Reports into Cognos Analytics

To use Cognos Analytics to access ITNCM Reports, you import ITNCM Reports into Cognos Analytics.

**Restriction:** This topic only applies to Netcool Configuration Manager installations on Linux on System z.

Deploy ITNCM Reports installation files

1. As icosuser, unzip `ITNCMReportsForCognosAnalytics.zip` to the `$ITNCM_HOME/temp` directory.
2. Run `./install_ncm_reports.sh` to copy the required ITNCM reports and related files into the relevant Cognos directories.

Import ITNCM Reports into Cognos Analytics

3. In IBM Cognos Administration, select the Content Administration tab, then click **New Import**.
   The **New Import** wizard is displayed.
4. In the deployment archive, select **ITNCM_Cognos_Reports_StandAlone**
5. Select the public folders, directory and library content - New Import wizard
6. On the Public folders, directory and library content, select **/../ITNCM Reports**, then click **Next**.
7. Specify the general options. Accept the default settings, and click **Next**.
8. Review the summary, and when satisfied, click **Next**.

9. Select **Action Save** and run once, then click **Finish**.

   ITNCM Reports should now be loaded and visible.
10. In Netcool Configuration Manager **ITNCM Account Management** > **Users**: In order for a user ID to be able to run the reports, map the LDAP user IDs exactly into Netcool Configuration Manager and assign the user ID to the Administrator group.
11. Disable anonymous access to IBM Cognos Components.

    See the following topic in the Knowledge Center for more information: https://www.ibm.com/support/knowledgecenter/SSEP7J_10.2.1/com.ibm.swg.ba.cognos.c8pp_inst.10.2.1.doc/t_disable_anon_logon_plumtree.html

## Configuring WebSphere user registry

From Version 6.4.2 onwards, Netcool Configuration Manager fully supports WebSphere user registries.

The default stand-alone version of Netcool Configuration Manager uses an RseriesUserRegistry, while in the default integrated scenario the Tivoli Netcool/OMNIbus user registry used by Network Manager is referenced.

In the stand alone configuration it is possible to point to a different UserRegistry (for example an LDAP). Any registry that Websphere accepts will function. The configuration of the registry is implementation dependent. If a user registry other than RSeriesUserRegistry is used, user accounts (such as IDs and passwords) will be managed outside of Netcool Configuration Manager in the user registry.

**Remote UserRegistry** (that is, not RSeriesUserRegistry)

1. Open the WebSphere administrative console..
2. Select **Security** > **Global security**.
3. In the **User account repository** section, set the realm to **something other than** 'theRealm'.
4. Select the realm definition, and configure the realm as per the remote user registry instructions.
5. Create an IntellidenUser group in the user repository. Depending on the repository type this may be done in a different application or at the **Users and Groups** > **Manage Groups** page.
6. Create an IntellidenAdminUser group in the user repository, and add at least one user to the IntellidenAdminUser group. Depending on the repository type this may be done in a different application or at the **Users and Groups** > **Manage Groups** page.
7. Any user that should have access to the application **must** be added to the IntellidenUser group, and this includes the users added to the IntellidenAdminUser group. Depending on the repository type this may be done in a different application or at the **Users and Groups** > **Manage Groups** page.

   Once the above changes are made and the system restarted, users may login to the application using the credentials from the remote repository. Users in the IntellidenAdminUser group will be able to perform administrative functions on the application, and users in the IntellidenUser group will be able to log into the system.

**Local UserRepository**

8. Open the WebSphere administrative console..
9. Select **Security** > **Global security**.
10. Enable administrative security.
11. Enable application security.
12. In the **User account repository** section, set the realm to `theRealm`.
13. Set the realm definition to `Standalone custom registry`.
14. Configure the realm by setting the following values:

    **Primary administrative user name**
    Intelliden

    **Server user identity**
    Automatically generated server identity

**Custom registry class name**
com.ibm.websphere.intelliden.RSeriesUserRegistry

All user and group editing is performed within Netcool Configuration Manager.

# Configuring OOBC

Use this information about Netcool Configuration Manager to configure OOBC.

**Related tasks**

Configuring a daemon
Configure an OOBC daemon on the server after you complete the OOBC software installation.

Prerequisites
Set JAVA_HOME in the machine.

Extracting OOBC software
The OOBC software is in an archived format suited for the operating system environment that you have chosen.

Installing OOBC software
These steps explain how to install the OOBC software.

**Related reference**

Troubleshooting the OOBC software installation
This section is designed to help troubleshoot some of the most commonly encountered OOBC installation issues.

**Related information**

Installing OOBC
Use this information about Netcool Configuration Manager to install the OOBC daemon, install the OOBC software, configure an OOBC daemon, and troubleshoot OOBC installation issues.

## OOBC system prerequisites

You must ensure that the configuration of devices, OOBC and syslogd meets certain requirements in order to allow communication between these components. Devices need to send syslog messages when their configuration is changed, and send the syslog messages in a format that will be parsable by the OOBC daemon.

### Communication prerequisites

The sample OOBC default configuration file described in "OOBC default configuration file" on page 98 contains the following configuration:

```
"
</log-pattern>
<!-- this pattern matches the most common log messages like
Apr 17 11:53:24 test_3-2 12984: Apr 17 07:52:23.318 %SYS-5-CONFIG_I: Configured
from console by cisco on console
-->
<log-pattern actionName="ConfigSyncIn" uowPriority="LOW" notifyName="
FileNotifier">
<pattern>([A-S][a-u][by]\
s+\d{1,2}\s+\d{2}:\d{2}:\d{2})\s+\[?([\.A-Za-z0-9_-
]+)\]?[\.\S+]*\s+.*?SYS-5-CONFIG_I:\s(Configured\
sfrom.*by\s(.*)\s+on\s(.*$))</pattern>
"
```

In order to produce syslog messages in the format above, the configuration for a Cisco device, for example, must contain the following line:

```
service timestamps log datetime
```

In order to send the message to the syslog daemon, logging for the Cisco has to be configured at 'notification' level, and the IP address of the syslog server must be provided in the device configuration, as in the following examples:

```
logging buffered 4096 notifications
logging 192.168.30.112
```

In this example `4096` is the size of the log, and `192.168.30.112` is the IP address of the syslog server.

# OOBC default configuration file

The `oobc.properties.xml` file is the default configuration file for the OOBC software.

All configuration parameters are set in this file except for LOG4J property settings, which are in the `log4j2.xml` file.

**Note:** In versions of Netcool Configuration Manager prior to Fix Pack 16, the LOG4J property settings file was called `log4j.xml`.

The XML schema for the `oobc.properties.xml` configuration file can be found in the installation directory of the OOBC software.

### Sample

The following is an example `oobc.properties.xml` file with sample values. The remainder of this section will dissect each portion of the XML file and explain its purpose.

```
<?xml version="1.0"?>
<out-of-band-change xmlns="http://intelliden.com/oobc/properties"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="
http://intelliden.com/oobc/properties
..\OutOfBandProperties.xsd">
<!-- Properties to configure what and how we monitor -->
<monitor>
<logFile>/opt/OutOfBandChange/run1/local7.log</logFile>
<markerFile>/opt/OutOfBandChange/run1/log.marker</markerFile>
<syslogMessageSaverFile>/opt/OutOfBandChange/run1/log.syslog-messages</
syslogMessageSaverFile>
<recoveryFile>/opt/OutOfBandChange/run1/log.recovery</recoveryFile>
<pollFrequencySeconds>5</pollFrequencySeconds>
<rollupAlgorithm>IdleTimeout</rollupAlgorithm>
<rollupFrequencySeconds>1800</rollupFrequencySeconds>
<fatalRestartSeconds>15</fatalRestartSeconds>
<notifyOnUnmanaged>true</notifyOnUnmanaged>
</monitor>
<!-- ITNCM API access settings -->
<intelliden-server>
<host>10.0.0.2</host>
<port>16310</port>
<user>OOBCUser</user>
<password>ce6f3ea926ad712172f8f9d7a67ccc07</password>
<protocol>iiop</protocol>
<initialContextFactory>com.ibm.websphere.naming.WsnInitialContext-
Factory</initialContextFactory>
</intelliden-server>
<!-- List of ITNCM and other third party system users -->
<!-- List of ITNCM worker servers -->
<worker-servers>
<server>intelliden</server>
</worker-servers>
<syslog-users>
<!-- ITNCM system users do work on behalf of ITNCM.
Syslog entries that contain these user ID's are skipped. -->
<intelliden-users>
<user>intelliden</user>
</intelliden-users>
<!-- Third party system users do work that needs synchronizationinto ITNCM but
    nobody needs to be notified. -->
<authorized-users>
<user>3rdPartyUser</user>
</authorized-users>
</syslog-users>
<syslog-match>
<!-- this pattern matches the most common log messages like
```

```
Apr 17 06:46:24 test_2-1 12980: Apr 17 02:46:23.318 EDT: %SYS-
5-CONFIG_I: Configured from console by unknown on vty0 (10.0.0.1)
-->
<log-pattern actionName="ConfigSyncIn" uowPriority="LOW" notifyName="
FileNotifier">
<pattern>([A-S][a-u][by]\
s+\d{1,2}\s+\d{2}:\d{2}:\d{2})\s+\[?([\.A-Za-z0-9_-
]+)\]?[\.\S+]*\s+.*?SYS-5-CONFIG_I:\s(Configured\
sfrom.*by\s(.*)\s+on\s(.*$))</pattern>
<timeStampIndex>1</timeStampIndex>
<dnsNameIndex>2</dnsNameIndex>
<userIdIndex>4</userIdIndex>
<descriptionIndex>3</descriptionIndex>
<sourceHostIndex>5</sourceHostIndex>
</log-pattern>
<!-- this pattern matches the most common log messages like
Apr 17 11:53:24 test_3-2 12984: Apr 17 07:52:23.318
%SYS-5-CONFIG_I: Configured from console by cisco on console
-->
<log-pattern actionName="ConfigSyncIn" uowPriority="LOW" notifyName="
FileNotifier">
<pattern>([A-S][a-u][by]\
s+\d{1,2}\s+\d{2}:\d{2}:\d{2})\s+\[?([\.A-Za-z0-9_-
]+)\]?[\.\S+]*\s+.*?SYS-5-CONFIG_I:\s(Configured\
sfrom.*by\s(.*)\s+on\s(.*$))</pattern>
<timeStampIndex>1</timeStampIndex>
<dnsNameIndex>2</dnsNameIndex>
<userIdIndex>4</userIdIndex>
<descriptionIndex>3</descriptionIndex>
<sourceHostIndex>5</sourceHostIndex>
</log-pattern>
<!-- this pattern matches the most common log messages like
Apr 17 11:53:24 test_3-2 12984: Apr 17 07:52:23.318
%SYS-5-CONFIG_I: Configured from console by vty0 (10.0.0.1)
-->
<log-pattern actionName="ConfigSyncIn" uowPriority="LOW" notifyName="
FileNotifier">
<pattern>([A-S][a-u][by]\
s+\d{1,2}\s+\d{2}:\d{2}:\d{2})\s+\[?([\.A-Za-z0-9_-
]+)\]?[\.\S+]*\s+.*?SYS-5-CONFIG_I:\s(Configured\
sfrom.*by\s(.*)\s+on\s(.*$))</pattern>
<timeStampIndex>1</timeStampIndex>
<dnsNameIndex>2</dnsNameIndex>
<userIdIndex>4</userIdIndex>
<descriptionIndex>3</descriptionIndex>
<sourceHostIndex>5</sourceHostIndex>
</log-pattern>
<log-pattern actionName="Import" uowPriority="HIGH" notifyName="FileNotifier">
<pattern>([A-S][a-u][by]\
s+\d{1,2}\s+\d{2}:\d{2}:\d{2})\s+\[?([\.A-Za-z0-9_-
]+)\]?[\.\S+]*\s+.*?SYS-5-SUMTHIN_ELSE:\s(Configured\
sfrom.*by\s(.*)\s+on\s(.*$))</pattern>
<timeStampIndex>1</timeStampIndex>
<dnsNameIndex>2</dnsNameIndex>
<userIdIndex>4</userIdIndex>
<descriptionIndex>3</descriptionIndex>
<sourceHostIndex>5</sourceHostIndex>
</log-pattern>
<log-pattern actionName="Reload" uowPriority="MEDIUM" notifyName="
FileNotifier">
<pattern>([A-S][a-u][by]\
s+\d{1,2}\s+\d{2}:\d{2}:\d{2})\s+\[?([\.A-Za-z0-9_-
]+)\]?[\.\S+]*\s+.*?SYS-5-RELOAD:\s(Reload\srequested\
sby\s(.*)\s+on\s(.*$))</pattern>
<timeStampIndex>1</timeStampIndex>
<dnsNameIndex>2</dnsNameIndex>
<userIdIndex>4</userIdIndex>
<descriptionIndex>3</descriptionIndex>
<sourceHostIndex>5</sourceHostIndex>
</log-pattern>
</syslog-match>
<!--
All current implementations of the OutOfBandAction interface.
These actions are referenced by name from a log-pattern match.
An instance of the OutOfBandAction class is invoked whenever a syslog
match is found. It is the responsibility of the action object
to take whatever steps are necessary to synchronize the out-of-band
changes to the network device with ITNCM or vice versa.
-->
<actions>
<action name="Import" priority="2">
<className>com.intelliden.oobc.impl.ImportFromDevice</className>
```

```
<properties>
<property name="overrideConflicts" value="true"/>
</properties>
</action>
<action name="ConfigSyncIn" priority="3">
<className>com.intelliden.oobc.impl.SynchronizeFromDevice</
className>
<properties>
<property name="overrideConflicts" value="true"/>
</properties>
</action>
<action name="Reload" priority="1">
<className>com.intelliden.oobc.impl.ReloadAction</className>
<properties>
<property name="overrideConflicts" value="true"/>
<property name="secondsBetweenUOWs" value="30"/>
<property name="realmPath" value="ITNCM/commandSets"/>
<property name="commandSetName" value="testCommandSet"/>
</properties>
</action>
</actions>
<!--
The default implementation of the OutOfBandNotifier interface.
The OutOfBandNotifier is notified of non-ITNCM and un-Authorized
user access to an ITNCM managed network resources.
The following implementation is a file notifier which writes formatted
messages to the output file.
-->
<notifiers>
<notify name="FileNotifier" priority="1">
<className>com.intelliden.oobc.impl.FileSerializer</className>
<pollFrequency>5000</pollFrequency>
<properties>
<property name="outFile" value="/opt/OutOfBandChange/run2/
notification.log"/>
<property name="format"
value="{0,date,yyyyMMddHHmmss'Z'}|{1}|ITNCMAlarm|{2}|{3} of
{4} syslog events. {5}"/>
<property name="formatDNF"
value="{0,date,yyyyMMddHHmmss'Z'}|{1}|ITNCMNot-
Found|{2}|Device {1} not currently managed by ITNCM. {3} of {4} syslog
events. {5}"/>
</properties>
</notify>
</notifiers>
</out-of-band-change>
```

# Configure out-of-band change

The <out-of-band-change> section of the oobc.properties.xml file contains the elements that define some administrative XML information as well as XML schema name space.

## XML Syntax

The following example shows the XML code for the out-of-band-change element:

```
<out-of-band-change
xmlns="http://intelliden.com/oobc/properties"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://intelliden.com/oobc/properties
..\OutOfBandProperties.xsd">
```

## Description

The top portion of the document contains some administrative XML information such as the version of XML and the associated schema for this file.

The root element of this XML document is the <out-of-band-change> element. It has a default XML Schema name space which refers to the OutOfBandPropertes.xsd. The only other XML Schema name space declared is the 'xsi' name space for the XML Schema data types.

## Configure monitor

The <monitor> section of the oobc.properties.xml file contains the elements that control the basic behavior of the OutOfBandChange daemon.

### XML Syntax

The following example shows the XML code for the <monitor> element:

```
<monitor>
<logFile>@syslog.file.name@</logFile>
<markerFile>@oobc.marker.file@</markerFile>
<syslogMessageSaverFile>@oobc.syslog.saver.file@</syslogMessageSaverFile>
<recoveryFile>@oobc.recovery.file@</recoveryFile>
<pollFrequencySeconds>5</pollFrequencySeconds>
<rollupAlgorithm>IdleTimeout</rollupAlgorithm>
<rollupFrequencySeconds>1800</rollupFrequencySeconds>
<fatalRestartSeconds>15</fatalRestartSeconds>
<notifyOnUnmanaged>true</notifyOnUnmanaged>
</monitor>
```

### Description

The <monitor> section of the oobc.properties.xml file gives fine control over what syslog file is monitored and how often the background threads will poll event queues, rollup events, and restart after failure.

The following table describes the XML elements specified within the <monitor> section of the oobc.properties.xml file:

| XML element | Description |
|---|---|
| <logFile> | The readable syslog output file that this daemon will process. The value can be any local or network file path to the syslog output file. |
| <markerFile> | A local or network path to a file that is writable by the daemon. It maintains a byte count of the next line in the syslog file to read. The default value for this file name is the name of the <logFile> file with an extension of marker. |
| <recoveryFile> | The prefix path to a pair of files used by the OOBC to store in memory state such that the OOBC may recover the next time it starts up. |
| <pollFrequencySeconds> | Used by the NotifierThread as the number of seconds to wait for an event on the Event Queue. After this time expires and no events have arrived the NotifierThread will "passivate" (if not already in a quiescent state) all of its Notify class instances. Then, before reading from the Event Queue again, it will check its internal run flag to see if this thread should continue on or exit.<br><br>Also used by the ParserThread as the number of seconds to sleep when there is no other data to read from the syslog file. After sleeping the specified number of seconds it will check its keepRunning flag to determined if it should continue on or exit. |
| <rollupAlgorithm> | The algorithm used for consolidating multiple parsed syslog events. The legal values are StaticInterval, DynamicInterval, and IdleTimeout. |
| <rollupFrequencySeconds> | The number of seconds that the daemon will wait between rollup cycles. As events are parsed from the syslog file they are placed in |

| XML element | Description |
|---|---|
| | an 'Event Rollup Queue'. This queue takes like events (events from the same network device) and collapses them into a single event. When the rollup cycle is invoked, only the 'Rolled up Event' is acted upon by this daemon. |
| <fatalRestartSeconds> | The number of seconds that the daemon will wait after a failure causes the shutdown but before the restart of the background daemon threads. |
| <notifyOnUnmanaged> | A true or false value indicating whether a syslog event, received on a device not currently managed by ITNCM - Base, should be written to the output notification log. |

# Configure Netcool Configuration Manager server

The <intelliden-server> section of the oobc.properties.xml file contains the elements that define all of the parameters required to communicate (via the API) with the Netcool Configuration Manager server.

## XML Syntax

The following example shows the XML code for the <intelliden-server> element:

```
<intelliden-server>
<host>@intelliden.host@</host>
<port>@intelliden.port@</port>
<user>@intelliden.user@</user>
<password>@intelliden.pass@</password>
<protocol>@intelliden.protocol@</protocol>
<initialContextFactory>com.ibm.websphere.naming.WsnInitialContextFactory</
    initialContextFactory>
</intelliden-server>
```

## Description

The <intelliden-server> section of the oobc.properties.xml file gives fine control over server and protocol information as well as user and password details.

The following table describes the XML elements specified within the <intelliden-server> section of the oobc.properties.xml file:

*Table 14. The intelliden-server XML elements in the oobc.properties.xml file*

| XML element | Description |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |

# Configuring HTTPS

You must perform extra steps in order to configure OOBC to use HTTPS for communication with the Presentation Server.

To configure OOBC to use HTTPS for communication with the Presentation Server, complete the following steps.

1. Save the root CA certificate to the OOBC user's home directory.

a) If you installed your own certificates for HTTPS, transfer the root CA certificate to the home directory of the user account that installed OOBC. If you are using the default Websphere-generated certificates, log on to the WebSphere Console of the Presentation Server that OOBC connects to using the Intelliden username and password and a URL such as:

```
https://presentationHostname:16316/ibm/console
```

b) Click **Security** > **SSL certificate and key management** > **Key stores and certificates** > **NodeDefaultTrustStore** > **Signer certificates**.

c) Select the root certificate and click **Extract**.

d) Enter a file name for the extracted certificate such as `/home/netcool/itncm_presentation_rootca.crt`, leave the Data type as `Base64-encoded ASCII data`, and click **OK**.

e) Transfer the extracted certificate to the home directory of the user account that installed OOBC.

2. Import the certificate into the OOBC JRE cacerts keystore, using a command similar to the following example:

```
netcool$ cd /$JAVA_HOME/jre/

netcool$ ./bin/keytool -import -trustcacerts -keystore lib/security/cacerts
 -storepass changeit -file ~/itncm_presentation_rootca.crt -alias itncm_presentation

Owner: CN=g01m06.lab.local, OU=Root Certificate, OU=JazzSMNode01Cell, OU=JazzSMNode01,
O=IBM, C=US
Issuer: CN=g01m06.lab.local, OU=Root Certificate, OU=JazzSMNode01Cell, OU=JazzSMNode01,
O=IBM, C=US
Serial number: 656bda3723d0
Valid from: 01/03/17 14:03 until: 26/02/32 14:03
...
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

3. Edit the `oobc.properties.xml` file so that the `<protocol>` element contains `iiops` and the `<port>` element contains the Netcool Configuration Manager Presentation Server HTTPS port (16311 by default). The file should look similar to the following example.

```
    <intelliden-server>
        <host>itncm.ibm.com</host>
        <port>16311</port>
        <user>OOBCUser</user>
        <password>f62fb89d73347cb4fc8bdc9dedf5620e</password>
        <protocol>iiops</protocol>
        <initialContextFactory>com.ibm.websphere.naming.WsnInitialContextFactory</
initialContextFactory>
    </intelliden-server>
```

4. Restart OOBC.

## Configure syslog users

The `<syslog-users>` section of the `oobc.properties.xml` file contains the elements that define user IDs.

### XML Syntax

The following example shows the XML code for the `<syslog-users>` element:

```
<syslog-users>
<!-- ITNCM system users do work on behalf of ITNCM.
Syslog entries that contain these user ID's are skipped. -->
<intelliden-users>
<user>@intelliden.worker@</user>
</intelliden-users>
<!-- Third party system users do work that needs synchronization
into ITNCM but nobody needs to be notified. -->
<authorized-users>
<user>@3rd.party.user@</user>
```

```
</authorized-users>
</syslog-users>
```

### Description

The <syslog-users> section of the oobc.properties.xml file defines two unique sets of user IDs. There are three types of users that the OutOfBandChange daemon looks for. First there is the ITNCM - Base user that performs all the Units of Work. Any syslog entry showing work performed by this user is automatically disregarded since it was technically done within the bounds of ITNCM - Base. The <intelliden-users> element can occur only once but can contain multiple <user> elements. Typically only the icosftpuser is required since this is the default user account that performs device updates from ITNCM - Base.

The second category of users is the Authorized 3rd Party users. These users are typically system users of 3rd party applications that are allowed to make direct changes to the device. In this case no external notification is required but a synchronization action must occur to keep ITNCM - Base up to date with the contents on the network device. The <authorized-users> element must only occur once but it can contain multiple <user> entries, one for each 3rd party user that may make changes directly to the network device.

The final category of users encompasses all users not in the ITNCM - Base or 3rd Party categories. These users have gone outside of the control of ITNCM - Base to make changes and therefore are both a non-ITNCM - Base and un-authorized user. In this case, an action is performed to synchronize the device with ITNCM - Base and a notification is made to an external system.

The following table describes the XML elements specified within the syslog-users section of the oobc.properties.xml file:

| XML element | Description |
|---|---|
| <intelliden-users> | Must occur only once and represents the set of users that are in the 'Intelliden' category of users. |
| <authorized-users> | Must occur only once and represents all users in the 'Authorized 3rd Party' category. |
| <user> | A child element of both <authorized-users> and <intelliden-users>. There can be multiple peer <user> elements. This field should contain the user id as it is found in the syslog file. |

## Configure syslog match

The <syslog-match> section of the oobc.properties.xml file contains the elements that describe how the OutOfBandChange daemon should parse the syslog file.

### XML Syntax

The following example shows the XML code for the <syslog-match> element:

```
<syslog-match>
<!-- Matches Sthe most common log messages like
Apr 17 06:46:24 test_2-1 12980: Apr 17 02:46:23.318 EDT: %SYS-5-CONFIG_I:
    Configured from console by unknown on vty0 (10.0.0.1) -->
<log-pattern actionName="ConfigSyncIn" uowPriority="LOW" notifyName="
FileNotifier">
<pattern>([A-S][a-u][by]\
s+\d{1,2}\s+\d{2}:\d{2}:\d{2})\s+\[?([\.A-Za-z0-9_-
]+)\]?[\.\S+]*\s+.*?SYS-5-CONFIG_I:\s(Configured\
sfrom.*by\s(.*)\s+on\s(.*$))</pattern>
<timeStampIndex>1</timeStampIndex>
<dnsNameIndex>2</dnsNameIndex>
<userIdIndex>4</userIdIndex>
<descriptionIndex>3</descriptionIndex>
```

```
<sourceHostIndex>5</sourceHostIndex>
</log-pattern>
<!-- this pattern matches the most common log messages like
Apr 17 11:53:24 test_3-2 12984: Apr 17 07:52:23.318 EDT:
%SYS-5-CONFIG_I: Configured from console by vty0 (10.0.0.1)
-->
<log-pattern actionName="ConfigSyncIn" uowPriority="LOW" notifyName="
FileNotifier">
<pattern>([A-S][a-u][by]\
s+\d{1,2}\s+\d{2}:\d{2}:\d{2})\s+\[?([\.A-Za-z0-9_-
]+)\]?[\.\S+]*\s+.*?SYS-5-CONFIG_I:\s(Configured\
sfrom.*by\s(.*)\s+on\s(.*$))</pattern>
<timeStampIndex>1</timeStampIndex>
<dnsNameIndex>2</dnsNameIndex>
<userIdIndex>4</userIdIndex>
<descriptionIndex>3</descriptionIndex>
<sourceHostIndex>5</sourceHostIndex>
</log-pattern>
<log-pattern actionName="Import" uowPriority="HIGH" notifyName="
FileNotifier">
<pattern>([A-S][a-u][by]\
s+\d{1,2}\s+\d{2}:\d{2}:\d{2})\s+\[?([\.A-Za-z0-9_-
]+)\]?[\.\S+]*\s+.*?SYS-5-SUMTHIN_ELSE:\s(Configured\
sfrom.*by\s(.*)\s+on\s(.*$))</pattern>
<timeStampIndex>1</timeStampIndex>
<dnsNameIndex>2</dnsNameIndex>
<userIdIndex>4</userIdIndex>
<descriptionIndex>3</descriptionIndex>
<sourceHostIndex>5</sourceHostIndex>
</log-pattern>
<log-pattern actionName="Reload" uowPriority="MEDIUM" notifyName="
FileNotifier">
<pattern>([A-S][a-u][by]\
s+\d{1,2}\s+\d{2}:\d{2}:\d{2})\s+\[?([\.A-Za-z0-9_-
]+)\]?[\.\S+]*\s+.*?SYS-5-RELOAD:\s(Reload\srequested\
sby\s(.*)\s+on\s(.*$))</pattern>
<timeStampIndex>1</timeStampIndex>
<dnsNameIndex>2</dnsNameIndex>
<userIdIndex>4</userIdIndex>
<descriptionIndex>3</descriptionIndex>
<sourceHostIndex>5</sourceHostIndex>
</log-pattern>
</syslog-match>
```

### Description

The <syslog-match> section of the oobc.properties.xml file gives fine control over what syslog entries are considered an 'Out-Of-Band' change as well as what 'actions' and 'notifications' must occur because of the 'Out-Of-Band' change. There is only one <syslog-match> element but it will typically contain multiple <log-pattern> elements for each of the various types of entries found in a typical syslog file.

The following table describes the XML elements specified within the <syslog-match> section of the oobc.properties.xml file:

*Table 15. The syslog-match XML elements in the oobc.properties.xml file*

| XML element | Description |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |

## Configure actions

The <actions> section of the oobc.properties.xml file contains the elements that describe the different synchronization actions that can be invoked.

### XML Syntax

The following example shows the XML code for the <actions> element:

```
<actions>
<action name="Reload" uowPriority="HIGH" priority="1">
<className>com.intelliden.oobc.impl.ReloadAction</className>
<properties>
<property name="overrideConflicts" value="true"/>
<property name="secondsBetweenUOWs" value="30"/>
<property name="realmPath" value="capstonec/commandsets"/>
<property name="commandSetName" value="SetupSyslog"/>
</properties>
</action>
</actions>
```

### Description

The <actions> section of the oobc.properties.xml file contains the elements that describe the different synchronization actions that can be invoked. As 'Out-Of-Band' changes occur, some 'action' must occur to synchronize ITNCM - Base with the network device. The types of synchronization actions that can occur will be described within individual <action> elements.

The following table describes the XML elements specified within the <actions> section of the oobc.properties.xml file:

*Table 16.*

| XML element | Description |
|---|---|
| | |
| | |
| | |
| | |

### Handling work conflicts

By default, ITNCM - Base will reject UOWs (Units of Work) submitted against devices with other UOWS pending or executing. The OOBC software can be configured to override this behavior. To allow UOWs to be submitted against devices with pending work, add the overrideConflicts property with a value of true to the action representing the type of UOW you wish to submit. For example:

```
<action name="Import" priority="2">
<className>com.intelliden.oobc.impl.ImportFromDevice</className>
<properties>
<property name="someproperty" value="somevalue"/>
<property name="overrideConflicts" value="true"/>
<property name="someotherproperty" value="someothervalue"/>
</properties>
</action>
```

## Configure notifiers

The <notifiers> section of the oobc.properties.xml file contains the elements that describe the different notifications that can be invoked.

### XML Syntax

The following example shows the XML code for the <notifiers> element:

```
<notifiers>
<notify name="FileNotifier" priority="1">
<className>com.intelliden.oobc.impl.FileSerializer</className>
<pollFrequency>5000</pollFrequency>
<properties>
<property name="outFile" value="logs/OOBCNotification.log"/>
<property name="format" value="{0,date,yyyyMMddHHmmss'Z'}|{1}|IntellidenAlarm
|{2}|{3} of {4} syslog events. {5}"/>
<property name="formatDNF" value="{0,date,yyyyMMddHHmmss'Z'}|{1}|
IntellidenDeviceNotFound|{2}|Device {1} not currently managed by Intelliden.
{3} of {4} syslog events. {5}"/>
</properties>
```

```
</notify>
</notifiers>
```

## Description

The <notifiers> section of the oobc.properties.xml file contains the elements that describe the different notifications that can be invoked. As 'Out-Of-Band' changes occur some 'notifications' must occur to alert personnel about changes to a network device. The types of notifications that can occur will be described within individual <notify> elements.

The following table describes the XML elements specified within the <notifiers> section of the oobc.properties.xml file:

*Table 17. The notifiers XML elements in the oobc.properties.xml file*

| XML element | Description |
|---|---|
| | |
| | |
| | |
| | |

# Chapter 4. Upgrading

Use this information to upgrade Netcool Configuration Manager from version 6.4.1.x or version 6.4.2.x.

**Important:** If you have an earlier version of Netcool Configuration Manager, you must follow the upgrade procedures in the Netcool Configuration Manager version 6.4.1 documentation.

**Note:** If you use Netcool Configuration Manager as part of a solution, you must also check the compatibility of the versions of all component products in the solution documentation. For example, if you use Netcool Operations Insight, check the instructions for *downloading components* for your version of Netcool Operations Insight at https://www.ibm.com/support/knowledgecenter/en/SSTPTP.

## 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.property` 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 OOBC:

**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.

**OOBC**
Reinstall or reconfigure OOBC 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.

**Related information**

Installing OOBC

Use this information about Netcool Configuration Manager to install the OOBC daemon, install the OOBC software, configure an OOBC daemon, and troubleshoot OOBC installation issues.

Installing drivers

Use this information to install Netcool Configuration Manager drivers.

# 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 Administratrive 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. Uninstalling

Use the scripts and instructions provided to uninstall the product.

## Uninstalling Netcool Configuration Manager

To uninstall Netcool Configuration Manager use IBM Installation Manager.

You need the Intelliden username and password to uninstall the product.

Use IBM Installation Manager to remove Netcool Configuration Manager.

To do a silent removal, 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
```

**Create uninstall response file using the created skipInstall**

```
IBMIM.exe -record C:\response_files\uninstall_1.xml -skipInstall
C:\Temp\skipInstall
```

**To remove Netcool Configuration Manager with the Installation Manager GUI**

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 **Uninstall**.
4. Select the offerings that you want to remove.
5. Follow the installation wizard instructions to complete the removal. Optionally, remove all information from the install by selecting **Delete all configuration and log information as part of the uninstall**.

**To remove Netcool Configuration Manager with the Installation Manager console**

6. Change to the `/eclipse/tools` subdirectory of the Installation Manager installation directory.
7. Use the following command to start the Installation Manager wizard:
   `./imcl -c`
8. From the Main Menu, select **Uninstall**.
9. Select the offerings that you want to remove.
10. Follow the installation wizard instructions to complete the removal. Optionally remove all information from the install by selecting **Delete all configuration and log information as part of the uninstall**.

**To silently remove Netcool Configuration Manager**

11. Change to the `/eclipse/tools` subdirectory of the Installation Manager installation directory.
12. 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 removal configuration.

The Installation Manager removes only the files and directories that it installed, unless the optional flag is selected during uninstall.

The JazzSM Administrative username and password are reset to the original installation username and password.

**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='/home/icosuser/IBM/IMShared'/>
  </variables>
  <server>
    <repository location='/home/icosuser/repo'/>
  </server>
  <profile id='Network Configuration Manager' installLocation='/opt/IBM/tivoli/netcool/ncm'>
    <data key='eclipseLocation' value='/opt/IBM/tivoli/netcool/ncm'/>
    <data key='user.import.profile' value='false'/>
    <!--Update architecture to linux for RHEl and SUSE-->
    <data key='cic.selector.os' value='aix'/>
    <!--Updae architecture to x86_64 for RHEl and SUSE-->
    <data key='cic.selector.arch' value='ppc64'/>
    <data key='cic.selector.ws' value='gtk'/>
    <data key='cic.selector.nl' value='en'/>
    <data key='user.tcr.was.user.name' value='smadmin'/>
    <data key='user.tcr.was.user.password' value=''/>
    <data key='user.tmp.tcr.was.password' value=''/>
    <data key='user.itncm.reports.update' value='false'/>
    <data key='user.tmp.ins.loc' value=''/>
    <data key='user.tcr.jazz.home' value=''/>
    <data key='user.tcr.was.profile.path' value=''/>
    <data key='user.tcr.was.server.name' value=''/>
    <data key='user.itncm.jdbc.type' value='oracle12'/>
    <data key='user.itncm.jdbc.driver' value='oracle.jdbc.driver.OracleDriver'/>
    <data key='user.itncm.jdbc.url' value='jdbc:oracle:thin:@ServerLocation:1521/itncm'/>
    <data key='user.itncm.jdbc.credentials.password' value=''/>
    <data key='user.itncm.jdbc.schema.name' value='itncm'/>
    <data key='user.itncm.jdbc.credentials.user' value='DBUSER'/>
    <data key='user.itncm.jdbc.host' value='ServerLocation'/>
    <data key='user.itncm.jdbc.port' value='1521'/>
    <data key='user.itncm.jdbc.type.prop' value='oracle'/>
    <data key='user.itncm.user.operator.password' value=''/>
    <data key='user.itncm.gui.active' value='true'/>
    <data key='user.temp.confirm.itnm.pass' value='netcool'/>
    <data key='user.itncm.ftp.credentials.password' value=''/>
    <data key='user.itncm.ftp.host' value='localhost'/>
    <data key='user.itncm.log.port' value='8102'/>
    <data key='user.itncm.ftp.dir' value='/home/icosftp'/>
    <data key='user.itncm.pbcm.log.error.port' value='8112'/>
    <data key='user.itncm.pbcm.admin.port' value='8110'/>
    <data key='user.itncm.pbcm.log.listen.port' value='8114'/>
    <data key='user.itncm.nmentitymapping.port' value='16311'/>
    <data key='user.temp.confirm.ftp.pass' value='icosftp'/>
    <data key='user.itncm.server.platform.config' value='PRESENTATION,TRUE,FALSE,DUAL'/>
    <data key='user.itncm.root.realm' value='ITNCM'/>
    <data key='user.itncm.log.listen.port' value='8103'/>
    <data key='user.itncm.pbcm.active' value='true'/>
    <data key='user.itncm.user.observer.password' value=''/>
    <data key='user.itncm.user.administrator.password' value=''/>
    <data key='user.itncm.idt.main.server' value='true'/>
    <data key='user.itncm.admin.port' value='8101'/>
    <data key='user.core.smtp.server' value='localhost'/>
    <data key='user.itncm.job.type' value='update'/>
    <data key='user.itncm.nmentitymapping.hostname' value='ncmdev10.hursley.ibm.com'/>
    <data key='user.itncm.ftp.credentials.user' value='icosftp'/>
    <data key='user.itncm.nmentitymapping.nm.password' value=''/>
    <data key='user.itncm.pbcm.log.test.port' value='8115'/>
    <data key='user.itncm.main.install.dir' value='/opt/IBM/tivoli/netcool/ncm'/>
    <data key='user.itncm.nmentitymapping.nm.importrealm' value='ITNCM/@DOMAINNAME'/>
    <data key='user.itncm.pbcm.log.debug.port' value='8111'/>
    <data key='user.itncm.worker.linked.rg' value='false'/>
    <data key='user.itncm.admin.manager.server.name' value='instanceName'/>
    <data key='user.itncm.nmentitymapping.base.url' value=''/>
    <data key='user.itncm.pbcm.log.info.port' value='8113'/>
    <data key='user.itncm.worker.active' value='true'/>
    <data key='user.itncm.integrated' value='true'/>
    <data key='user.itncm.idt.port' value='8104'/>
    <data key='user.itncm.nmentitymapping.nm.user' value='itnmadmin'/>
    <data key='user.itncm.server.was.node' value='JazzSMNode01'/>
    <data key='user.was.server.name' value='server1'/>
    <data key='user.was.profile.path' value='/opt/IBM/JazzSM/profile'/>
    <data key='user.was.appserver.dir' value='/opt/IBM/WebSphere/AppServer'/>
    <data key='user.itncm.server.ssl.port' value='16311'/>
    <data key='user.itncm.server.was.cell' value='JazzSMNode01Cell'/>
    <data key='user.was.user.name' value='smadmin'/>
    <data key='user.tmp.was.password' value=''/>
    <data key='user.itncm.server.http.port' value='16310'/>
    <data key='user.jazz.home' value='/opt/IBM/JazzSM'/>
    <data key='user.was.profile.name' value='JazzSMProfile'/>
    <!--Set to false to keep additional log information, clean directory removes all folders and files from
```

```
the install directory-->
    <data key='user.itncm.clean.directory' value='true'/>
    <data key='user.was.user.password' value=''/>
  </profile>
  <uninstall modify='false'>
    <offering profile='Network Configuration Manager' id='com.ibm.tivoli.itncm.configurationmanager.server'
version='6.4.2.20160121_0525'/>
  </uninstall>
  <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='false'/>
  <preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

# Uninstalling ITNCM-Reports

To uninstall Netcool Configuration Manager Tivoli Common Reporting use IBM Installation Manager.

You need the JazzSM Administrative username and password to uninstall the product.

Use IBM Installation Manager to remove the ITNCM-Reports.

**Tip:** To do a silent removal, create or record an Installation Manager response file. For more information, see the 'Record a response file with Installation Manager' topic in the IBM Installation Manager Knowledge center:

http://www-01.ibm.com/support/knowledgecenter/SSDV2W_1.8.2/com.ibm.silentinstall12.doc/topics/t_silent_create_response_files_IM.html.

**To remove ITNCM-Reports with the Installation Manager GUI**

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 **Uninstall**.
4. Select the offerings that you want to remove and follow the installation wizard instructions to complete the removal.

**To remove ITNCM-Reports with the Installation Manager console**

5. Change to the `/eclipse/tools` subdirectory of the Installation Manager installation directory.
6. Use the following command to start the Installation Manager wizard:
   `./imcl -c`
7. From the Main Menu, select **Uninstall**.
8. Select the offerings that you want to remove, and follow the installation wizard instructions to complete the removal.

**To silently remove ITNCM-Reports**

9. Change to the `/eclipse/tools` subdirectory of the Installation Manager installation directory.
10. 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 removal configuration.

The Installation Manager removes only the files and directories that it installed.

**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='/home/icosuser//IBM/IBMIMShared'/>
  </variables>
  <server>
    <repository location='/home/icosuser/Repo'/>
  </server>
  <profile id='Netcool Configuration Manager' installLocation='/opt/IBM/tivoli/netcool/ncm'>
    <data key='eclipseLocation' value='/opt/IBM/tivoli/netcool/ncm'/>
    <data key='user.import.profile' value='false'/>
    <!--Update architecture to aix for AIX-->
    <data key='cic.selector.os' value='linux'/>
    <!--Updae architecture to ppc64 for AIX-->
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='gtk'/>
    <data key='user.itncm.jdbc.type' value='oracle12'/>
    <data key='user.itncm.jdbc.driver' value='oracle.jdbc.driver.OracleDriver'/>
    <data key='user.itncm.jdbc.url' value='jdbc:oracle:thin:@ServerLocation:1521/itncm'/>
    <data key='user.itncm.jdbc.credentials.password' value=''/>
    <data key='user.itncm.jdbc.schema.name' value='itncm'/>
    <data key='user.itncm.jdbc.credentials.user' value='DBUSER'/>
    <data key='user.itncm.jdbc.host' value='ncmlnx02.hursley.ibm.com'/>
    <data key='user.itncm.jdbc.port' value='1521'/>
    <data key='user.itncm.jdbc.type.prop' value='oracle'/>
    <data key='user.tcr.was.user.name' value='smadmin'/>
    <data key='user.tcr.app.server.home' value='/opt/IBM/WebSphere/AppServer'/>
    <data key='user.itncm.reports.update' value='false'/>
    <data key='user.tcr.WAS_SERVER_NAME' value='server1'/>
    <data key='user.tcr.jazz.home' value='/opt/IBM/JazzSM'/>
    <data key='user.tcr.reports.integrated' value='N'/>
    <data key='user.tcr.was.profile.path' value='/opt/IBM/JazzSM/profile'/>
    <data key='user.tcr.was.server.name' value='server1'/>
    <data key='cic.selector.nl' value='en'/>
    <data key='user.tcr.was.user.password' value=''/>
  </profile>
  <uninstall modify='false'>
    <offering profile='Netcool Configuration Manager' id='com.ibm.tivoli.itncm.configurationmanager.server'
version='6.4.2.20160202_1049'/>
  </uninstall>
  <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>
```

# Uninstalling 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. To uninstall these components, use IBM Installation Manager.

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

1. Log onto the DASH server as the same user who installed the Netcool Configuration Manager DASH components.
2. Change to the `/eclipse` subdirectory of the Installation Manager Group installation directory, and use the following command to start the Installation Manager wizard:

   ```
   ./IBMIM
   ```

   **Tip:** 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\uninstall_1.xml
```

3. In the main **Installation Manager window**, click **Uninstall**, and then select **IBM Dashboard Applications for ITNCM**.
4. Follow the uninstallation wizard instructions.

   The Uninstall Wizard will request the following details:

   **DASH administrative credentials**
   Enter the DASH administrator username (the default is `sysadmin`).

   Enter the DASH administrator password.

   **Network Manager administrative credentials**
   Enter either the Network Manager administrative username (the default is `badminton`), or the name of the DASH Super User (who must have the ncw_admin role in DASH).

   Enter the appropriate user password.
5. Complete the removal of the Netcool Configuration Manager DASH components.

The Installation Manager removes only the files and directories that it installed.

**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/Repo'/>
  </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='ncmdev10.hursley.ibm.com'/>
    <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='4100'/>
    <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='ncmlnx02.hursley.ibm.com'/>
    <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='itnmadmin'/>
    <data key='user.itnm.ObjectServerItnmAdminUsername' value='itnmadmin'/>
    <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='aix01'/>
    <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='false'/>
```

```
    <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=''/>
  </profile>
  <uninstall modify='false'>
    <offering profile='IBM Netcool GUI Components' id='com.ibm.tivoli.netcool.itncm.ui.dash'
version='6.4.2.20160202_1049'/>
  </uninstall>
  <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>
```

You may have to manually remove some or all of the following Netcool Configuration Manager user roles:

- IntellidenUser
- IntellidenAdminUser
- ncmActivityViewing
- ncmConfigChange
- ncmConfigEdit
- ncmConfigSynch
- ncmConfigViewing
- ncmIDTUser
- ncmPolicyCheckncmDashService

Review these roles in the 'User role requirements' topic of the *IBM Tivoli Netcool Configuration Manager Integration Guide*.

# Uninstalling OOBC Software

Use this information about Netcool Configuration Manager to uninstall OOBC daemons and OOBC software.

## Uninstalling an OOBC daemon

Uninstall an OOBC daemon by following the steps in this section.

Since the OOBC software can be installed multiple times on a single machine, the uninstall process consists of 1) running a script for each OOBC run directory (daemon) created and then 2) manually removing the software. The following procedure outlines how to uninstall OOBC software.

1. Log on to the platform as `root`.
2. Access the directory containing the OOBC installer. The default is `/opt/OutOfBandChange`.
3. The installer requests the installation path for the new OOBC run directory. As already mentioned, multiple OOBC Run Directories can be installed.

```
Enter path to OOBC run directory to be removed?
e.g. /opt/OutOfBandChange/run1
```

Press Enter to accept the path.

4. The installer requests that you confirm the removal of the specified OOBC run time configuration:

```
Beginning UN-Install process for pre-existing OOBC Run directory:
/opt/OutOfBandChange/run1
Are you sure you want to remove this OOBC runtime configuration? (yes,no)
yes
BUILD SUCCESSFUL
Total time: 12 seconds
```

Now, you can uninstall the OOBC software.

## Uninstalling OOBC software

Uninstall OOBC software by following the steps in this section.

After all run directories have been uninstalled then you can simply remove the OOBC install root directory from your system.

1. Change directory to `/opt`:

```
# cd /opt
```

2. Remove the OOBC install root directory for your system. For example:

```
# rm -rf OutOfBandChange
```

# 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.

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" 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

Part Number:

Printed in the Republic of Ireland

(1P) P/N:

2023-4219-01