

IBM® Tivoli® Netcool/OMNIbus Probe for
Nokia-Siemens NetAct 3GPP V6 (CORBA)
5.0

Reference Guide
November 04, 2011



Note

Before using this information and the product it supports, read the information in [Appendix A, “Notices and Trademarks,” on page 29.](#)

Edition notice

This edition (SC22-5411-00) applies to version 5.0 of IBM Tivoli Netcool/OMNIbus Probe for Nokia-Siemens NetAct 3GPP V6 (CORBA) and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright International Business Machines Corporation 2011.**

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

Contents

About this guide.....	V
Document Control Page.....	v
Conventions used in this guide.....	v
 Chapter 1. Probe for Nokia-Siemens NetAct 3GPP V6 (CORBA).....	1
Summary.....	1
Installing probes.....	2
Firewall considerations.....	3
Configuring the lookup table.....	4
Data acquisition.....	4
Connecting to the CORBA interface.....	4
Retrieving objects.....	5
Status checking.....	5
Filtering notifications and alarms.....	5
Command line interface.....	8
Peer-to-peer failover functionality.....	9
Running multiple probes.....	10
Properties and command line options.....	10
Elements.....	15
Error messages.....	18
ProbeWatch messages.....	24
Running the probe.....	27
 Appendix A. Notices and Trademarks.....	29
Notices.....	29
Trademarks.....	30

About this guide

The following sections contain important information about using this guide.

Document Control Page

Use this information to track changes between versions of this guide.

The IBM Tivoli Netcool/OMNIBus Probe for Nokia-Siemens NetAct 3GPP V6 (CORBA) documentation is provided in softcopy format only. To obtain the most recent version, visit the IBM® Tivoli® Information Center:

http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/index.jsp?topic=/com.ibm.tivoli.namomnibus.doc/welcome_ptsm.htm

Table 1. Document modification history		
Document version	Publication date	Comments
SC22-5411-00	November 04, 2011	First IBM publication.

Note : The Probe for Nokia-Siemens NetAct 3GPP V6 (CORBA) was previously documented in the same reference guide as the Probe for Nokia-Siemens NetAct 3GPP V4 (CORBA). This reference guide documents the Probe for Nokia-Siemens NetAct 3GPP V6 (CORBA) only.

Conventions used in this guide

All probe guides use standard conventions for operating system-dependent environment variables and directory paths.

Operating system-dependent variables and paths

All probe guides use standard conventions for specifying environment variables and describing directory paths, depending on what operating systems the probe is supported on.

For probes supported on UNIX and Linux operating systems, probe guides use the standard UNIX conventions such as *\$variable* for environment variables and forward slashes (/) in directory paths. For example:

`$OMNIHOME/probes`

For probes supported only on Windows operating systems, probe guides use the standard Windows conventions such as *%variable%* for environment variables and backward slashes (\) in directory paths. For example:

`%OMNIHOME%\probes`

For probes supported on UNIX, Linux, and Windows operating systems, probe guides use the standard UNIX conventions for specifying environment variables and describing directory paths. When using the Windows command line with these probes, replace the UNIX conventions used in the guide with Windows conventions. If you are using the bash shell on a Windows system, you can use the UNIX conventions.

Note : The names of environment variables are not always the same in Windows and UNIX environments. For example, %TEMP% in Windows environments is equivalent to \$TMPDIR in UNIX and Linux environments. Where such variables are described in the guide, both the UNIX and Windows conventions will be used.

Operating system-specific directory names

Where Tivoli Netcool/OMNIbus files are identified as located within an *arch* directory under NCHOME or OMNIHOME, *arch* is a variable that represents your operating system directory. For example:

\$OMNIHOME/probes/*arch*

The following table lists the directory names used for each operating system.

Note : This probe may not support all of the operating systems specified in the table.

Table 2. Directory names for the arch variable	
Operating system	Directory name represented by <i>arch</i>
AIX® systems	aix5
Red Hat Linux® and SUSE systems	linux2x86
Linux for System z	linux2s390
Solaris systems	solaris2
Windows systems	win32

OMNIHOME location

Probes and older versions of Tivoli Netcool/OMNIbus use the OMNIHOME environment variable in many configuration files. Set the value of OMNIHOME as follows:

- On UNIX and Linux, set \$OMNIHOME to \$NCHOME/omnibus.
- On Windows, set %OMNIHOME% to %NCHOME%\omnibus.

Chapter 1. Probe for Nokia-Siemens NetAct 3GPP V6 (CORBA)

Nokia-Siemens NetAct is a networking and service management Operations Support System (OSS). It provides fault and performance management, service provisioning, support for multiple wireless network technologies, and customer management interfaces. It operates across the radio-access and core subnetworks of next-generation wireless Internet networks.

The Probe for Nokia-Siemens NetAct 3GPP V6 (CORBA) collects alarms from Nokia-Siemens NetAct using a Common Object Request Broker Architecture (CORBA) 3rd Generation Partnership Project (3GPP) interface. The probe acquires data from Nokia-Siemens NetAct devices that support 3GPP version 6.2.0. IBM does not maintain a list of compatible Nokia-Siemens devices.

The probe complies with the following 3GPP standards:

Table 3. Supported 3GPP standards		
3GPP Technical Specification	Version	Object
32.111-3	6.2.0	Alarm Integration Reference Point (IRP)
32.303	6.3.0	Notification IRP
32.363	6.3.0	Entry Point IRP

This guide contains the following sections:

- [“Summary” on page 1](#)
- [“Installing probes” on page 2](#)
- [“Firewall considerations” on page 3](#)
- [“Configuring the lookup table” on page 4](#)
- [“Data acquisition” on page 4](#)
- [“Properties and command line options” on page 10](#)
- [“Elements” on page 15](#)
- [“Error messages” on page 18](#)
- [“ProbeWatch messages” on page 24](#)
- [“Running the probe” on page 27](#)

Summary

Each probe works in a different way to acquire event data from its source, and therefore has specific features, default values, and changeable properties. Use this summary information to learn about this probe.

The following table provides a summary of the probe.

Table 4. Summary	
Probe target	Nokia-Siemens NetAct 3GPP interface V6
Probe executable name	nco_p_nokia_netact_3gpp_v6

Table 4. Summary (continued)	
Probe installation package	<code>omnibus-arch-probe-nco-p-nokia-netact-3gpp-v6-version</code>
Package version	5.0
Probe supported on	For details of the operating system versions on which this probe is supported, see the following page on the IBM Tivoli Netcool Knowledge Center: https://www-304.ibm.com/support/docview.wss?uid=swg21568039
Properties file	<code>\$OMNIHOME/probes/arch/nokia_netact_3gpp_v6.props</code>
Rules file	<code>\$OMNIHOME/probes/arch/nokia_netact_3gpp_v6.rules</code>
Requirements	One of the following versions of IBM Tivoli Netcool/OMNIBus: • V7.2.0 with Interim Fix 4 (7.2.0.7-IF0004) installed • V7.2.1 with Interim Fix 3 (7.2.1.5-IF0003) installed • V7.3.0 • V7.3.1 Nonnative Probe Server: <code>probe-nonnative-base-14</code> IBM Object Request Broker (IBM ORB, supplied with Netcool/OMNIBus) Java™ Runtime Environment (JRE) 1.5
Connection method	CORBA
Multicultural support	Available
Peer-to-peer failover functionality	Available
IP environment	IPv4 and IPv6
Federal Information Processing Standards (FIPS)	IBM Tivoli Netcool/OMNIBus uses the FIPS 140-2 approved cryptographic provider: IBM Crypto for C (ICC) certificate 384 for cryptography. This certificate is listed on the NIST website at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2004.htm . For details about configuring Netcool/OMNIBus for FIPS 140-2 mode, see the <i>IBM Tivoli Netcool/OMNIBus Installation and Deployment Guide</i> .

Installing probes

All probes are installed in a similar way. The process involves downloading the appropriate installation package for your operating system, installing the appropriate files for the version of Netcool/OMNIBus that you are running, and configuring the probe to suit your environment.

The installation process consists of the following steps:

1. Downloading the installation package for the probe from the Passport Advantage Online website.

Each probe has a single installation package for each operating system supported. For details about how to locate and download the installation package for your operating system, visit the following page on the IBM Tivoli Knowledge Center:

http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/omnibus/probes/all_probes/wip/reference/install_download_intro.html

2. Installing the probe using the installation package.

The installation package contains the appropriate files for all supported versions of Netcool/OMNIBus. For details about how to install the probe to run with your version of Netcool/OMNIBus, visit the following page on the IBM Tivoli Knowledge Center:

http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/omnibus/probes/all_probes/wip/reference/install_install_intro.html

3. Configuring the probe.

This guide contains details of the essential configuration required to run this probe. It combines topics that are common to all probes and topics that are peculiar to this probe. For details about additional configuration that is common to all probes, see the *IBM Tivoli Netcool/OMNIBus Probe and Gateway Guide*.

Firewall considerations

When using CORBA probes in conjunction with a firewall, the firewall must be configured so that the probe can connect to the target system.

Most CORBA probes can act as both a server (listening for connections from the target system) and a client (connecting to the port on the target system to which the system writes events). If you are using the probe in conjunction with a firewall, you must add the appropriate firewall rules to enable this dual behavior.

There are three possible firewall protection scenarios, for which you must determine port numbers before adding firewall rules:

1. If the host on which the probe is running is behind a firewall, you must determine what remote host and port number the probe will connect to.
2. If the host on which the target system is running is behind a firewall, you must determine the incoming port on which the probe will listen and to which the target system will connect.
3. If each host is secured with its own firewall, you must determine the following four ports:
 - a. The outgoing port (or port range) for the probe.
 - b. The hostname and port of the target system.
 - c. The outgoing port on which the target system sends events if the probe is running as a client.
 - d. The incoming port on which the probe listens for incoming events.

Note : Most, but not all, CORBA probes listen on the port specified by the **ORBLocalPort** property. The default value for this property is 0, which means that an available port is selected at random. If the probe is behind a firewall, the value of the **ORBLocalPort** property must be specified as a fixed port number.

CORBA probes that use EventManager or NotificationManager objects may use different hosts and ports from those that use NamingService and EntryPoint objects. If the probe is configured to get object references from a NamingService or EntryPoint object, you must obtain the host and port information from the system administrator of the target system. When you have this information, you can add the appropriate firewall rules.

Configuring the lookup table

The probe is supplied with a lookup table that contains details of the various types of alarms that Nokia-Siemens NetAct generates. You might need to update the rules file to include the path to the lookup table.

At installation, the `Corba_3gpp_V620.lookup` file supplied with the probe installation package is installed to the following location:

`$OMNIHOME/probes/includes/`

To reference the lookup table from the rules file, add the following line to the rules file:

```
include "$OMNIHOME/probes/includes/Corba_3gpp_V620.lookup"
```

The include command assumes that the probe is run from the standard `$OMNIHOME/probes/` directory. If you are running the probe from a different directory, use the absolute directory path to the lookup table. Do not use the `$OMNIHOME` environment variable in this directory path.

Data acquisition

Each probe uses a different method to acquire data. Which method the probe uses depends on the target system from which it receives data.

The probe gathers alarms from Nokia-Siemens NetAct using a CORBA 3GPP interface.

Data acquisition is described in the following topics:

- [“Connecting to the CORBA interface” on page 4](#)
- [“Retrieving objects” on page 5](#)
- [“Status checking” on page 5](#)
- [“Filtering notifications and alarms” on page 5](#)
- [“Command line interface” on page 8](#)
- [“Peer-to-peer failover functionality” on page 9](#)
- [“Running multiple probes” on page 10](#)

Connecting to the CORBA interface

The probe acts as an Integration Reference Point (IRP) Manager and connects to the Nokia-Siemens NetAct system using a CORBA 3GPP interface.

The AlarmIRP and NotificationIRP CORBA objects form a part of the IRP agent to which the probe connects.

Depending on your operating environment, use one of the following connection configurations:

1. Option 1 - specify values for the following properties:

- **NetActServerName** - the name of the Nokia-Siemens NetAct server to which the probe connects to retrieve the Naming Context IOR file.
- **NetActServerPort** - the port on the Nokia-Siemens NetAct server through which the probe connects to retrieve the Naming Context IOR file.
- **NamingServiceIORRequest** - specify the command that the probe uses to upload the CORBA Naming Service IOR.
- **AlarmIrpName** - specify the name used to resolve the Alarm IRP in the CORBA Naming Service.
- **NotificationIrpName** - specify the name used to resolve the Notification IRP in the CORBA Naming Service.

2. Option 2 - specify values for the following properties:

- **NamingServiceHost** - specify the name of the host machine where the CORBA Naming Service is running.

- **NamingServicePort** - specify the port on which the CORBA Naming Service listens.
- **AlarmIrpName** - specify the name used to resolve the Alarm IRP in the CORBA Naming Service.
- **NotificationIrpName** - specify the name used to resolve the Notification IRP in the CORBA Naming Service.

3. Option 3 - specify values for the following properties:

- **EntryPointIrpFile** - specify the location of the file that contains the IOR of the EntryPoint IRP object.
- **NotificationIrpName** - specify the name used to resolve the Notification IRP in the CORBA Naming Service.
- **AlarmIrpName** - specify the name used to resolve the Alarm IRP in the CORBA Naming Service.

Retrieving objects

If the **Resynch** property is set to true, the probe initially receives a list of all active alarms from the AlarmIRP server.

The probe then connects to the NotificationIRP server and uses the CORBA notification push model to receive new alarms from the server as they are generated. If the **Resynch** property is set to false, the probe only receives new alarms.

Status checking

This section contains information about the status checking method of the probe.

The probe checks the status of the IRP agent every 60 seconds. You can change this frequency if required using the **Agentheartbeat** property.

Filtering notifications and alarms

This section contains information about how to enable the retrieval of notifications and alarms from the target system.

The **NotificationFilter** and **AlarmFilter** properties allow you to specify the notifications and alarms that the probe receives from the target device.

When you use these properties, you must use the actual token names. For example, the token `h` represents the element `NV_PERCEIVED_SEVERITY`. So to specify that the probe is only sent notifications with a perceived severity of 3, set the **NotificationFilter** property to `$h == 3`.

You can specify more complex filters using AND, OR, and NOT statements. For example, to specify that the probe is sent notifications with a perceived severity of 3 or 4, set the **NotificationFilter** property to the following value:

```
($h == 3) OR ($h == 4)
```

The following table lists the token/element mappings available for the **AlarmFilter** and **NotificationFilter** properties:

Table 5. Token/element mappings	
Token	Element
a	NV_NOTIFICATION_ID
b	NV_EVENT_TIME
c	NV_SYSTEM_DN
d	NV_MANAGED_OBJECT_CLASS

Table 5. Token/element mappings (continued)

Token	Element
e	NV_MANAGED_OBJECT_INSTANCE
f	NV_ALARM_ID
ff	NV_ALARM_LIST_ALIGNMENT_REQUIREMENT
g	NV_PROBABLE_CAUSE
gg	NV_SERVICE_USER
h	NV_PERCEIVED_SEVERITY
hh	NV_SERVICE_PROVIDER
i	NV_SPECIFIC_PROBLEM
ii	NV_SECURITY_ALARM_DETECTOR
j	NV_ADDITIONAL_TEXT
jj	NV_VENDOR_SPECIFIC_ALARM_TYPE
k	NV_ACK_TIME
l	NV_ACK_USER_ID
m	NV_ACK_SYSTEM_ID
n	NV_ACK_STATE
o	NV_COMMENTS
p	NV_BACKED_UP_STATUS
q	NV_BACK_UP_OBJECT
r	NV_THRESHOLD_INFO
s	NV_TREND_INDICATION
t	NV_STATE_CHANGE_DEFINITION
u	NV_MONITORED_ATTRIBUTES
v	NV_PROPOSED_REPAIR_ACTIONS
w	NV_CORRELATED_NOTIFICATIONS
x	NV_REASON
y	CLEAR_USER_ID

Table 5. Token/element mappings (continued)	
Token	Element
z	CLEAR_SYSTEM_ID

Filters

This section describes the filters that help retrieve matching elements.

The probe retrieves elements by using a filter that associates an ObjectServer field with its expected value. Filters take the following format:

<attribute_name> <attribute_comparison_operator> <attribute_value>

The following table lists the valid operators and attribute values for the available ObjectServer fields:

Table 6. Valid operators and attribute values		
Name of the attribute	Valid operators	Valid attribute values
alarmType	==	COMMUNICATIONS_ALARM ENVIRONMENTAL_ALARM EQUIPMENT_ALARM PROCESSING_ERROR_ALARM QUALITY_OF_SERVICE_ALARM
managedObjectClass	==	The filtering of elements sent from the device can only be configured in Nokia-Siemens NetAct. For details of the syntax required for filtering object classes, refer to your CORBA documentation or contact your system administrator. Note : An attribute value of 0 retrieves any matching alarms from both the 3GPP interface and the Nokia-Siemens NetAct system.
perceivedSeverity	== < <= > >=	CRITICAL MAJOR MINOR WARNING CLEARED

Valid filters

The following filters are examples of valid filters:

1. (managedObjectClass == SubNetwork) OR (managedObjectClass == ManagedElement) OR (managedObjectClass == ManagedFunction) AND (NOT alarmType == PROCESSING_ERROR_ALARM)
2. (alarmType == ENVIRONMENTAL_ALARM) OR (perceivedSeverity <= MINOR)
3. (alarmType == ENVIRONMENTAL_ALARM) OR (NOT perceivedSeverity == WARNING)

Invalid filters

The following filters are examples of invalid filters that will not work:

1. (perceivedSeverity == WARNING) OR (managedObjectInstance == SubNetwork=Nokia-1)
2. (alarmType == ENVIRONMENTAL_ALARM) AND (probableCause < 1000)
3. (alarmType < ENVIRONMENTAL_ALARM)

Command line interface

The probe has a command line interface (CLI) that you can use to issue commands.

To use the CLI, use the **CommandPort** property to specify a port through which commands can be sent. Use Telnet to send commands to this port.

The following table lists the commands that you can use with the CLI:

Table 7. CLI commands	
Command	Description
acknowledge_alarm	This command allows you to acknowledge an alarm in the 3GPP interface. Note : This command takes as a parameter the NV_ALARM_ID of the alarm being acknowledged. Only one alarm can be acknowledged at a time.
exit/quit	This command closes the connection.
help	This command displays online help about the CLI.
resynch_all	This command allows you to perform a full resynchronization with the 3GPP interface. Note : Successful resynchronization requires that the Resynch property is set to true.
resynch_filter	This command allows you to a perform partial resynchronization with the 3GPP interface. Note : This command takes as a parameter a filter in the same format as the AlarmFilter property. For details, see “Filtering notifications and alarms” on page 5 .
unacknowledge_alarm	This command allows you to unacknowledge an alarm in the 3GPP interface. Note : This command is not currently supported by Nokia-Siemens NetAct.
userid_acknowledge_alarm	This command allows you to acknowledge an alarm in the 3GPP interface by specifying the NV_ALARM_ID and NV_ACK_USER_ID parameters. These parameters are specified by the AckSystemId and AckUserId properties.
userid_clear_alarm <i>userid</i>	This command allows you to clear an alarm created by a specific user ID.

Table 7. CLI commands (continued)	
Command	Description
userid_unacknowledge_alarm	This command allows you to un-acknowledge an alarm in the 3GPP interface by specifying the NV_ALARM_ID and NV_ACK_USER_ID parameters.
version	This command displays the version of the probe.

Note : Since the CLI uses Telnet connections, you can connect to the probe from anywhere. This means that simple scripts can be set up to allow users to acknowledge selected events from the Netcool/OMNIbus event list. You can create desktop tools that use Telnet to connect to the probe, send a command, and then close the connection.

Peer-to-peer failover functionality

The probe supports failover configurations where two probes run simultaneously. One probe acts as the master probe, sending events to the ObjectServer; the other acts as the slave probe on standby. If the master probe fails, the slave probe activates.

While the slave probe receives heartbeats from the master probe, it does not forward events to the ObjectServer. If the master probe shuts down, the slave probe stops receiving heartbeats from the master and any events it receives thereafter are forwarded to the ObjectServer on behalf of the master probe. When the master probe is running again, the slave probe continues to receive events, but no longer sends them to the ObjectServer.

Example property file settings for peer-to-peer failover

You set the peer-to-peer failover mode in the properties files of the master and slave probes. The settings differ for a master probe and slave probe.

Note : In the examples, make sure to use the full path for the property value. In other words replace \$OMNIHOME with the full path. For example: /opt/IBM/tivoli/netcool.

The following example shows the peer-to-peer settings from the properties file of a master probe:

```
Server      : "NCOMS"
RulesFile   : "master_rules_file"
MessageLog  : "master_log_file"
PeerHost    : "slave_hostname"
PeerPort    : 6789 # [communication port between master and slave probe]
Mode        : "master"
PidFile     : "master_pid_file"
```

The following example shows the peer-to-peer settings from the properties file of the corresponding slave probe:

```
Server      : "NCOMS"
RulesFile   : "slave_rules_file"
MessageLog  : "slave_log_file"
PeerHost    : "master_hostname"
PeerPort    : 6789 # [communication port between master and slave probe]
Mode        : "slave"
PidFile     : "slave_pid_file"
```

Running multiple probes

You can run multiple instances of the probe.

For each running instance, specify a different port to which the server listens using the **ORBLocalPort** property.

Running multiple probes in a failover configuration

If you have implemented a peer-to-peer failover configuration, both the master probe and the slave probe have their own Object Request Broker (ORB) local port.

Where you are running this configuration in conjunction with a firewall, add the receiving port of each probe to the firewall rules. The direction of the connection is from the target system to the master or slave probe.

You set the peer-to-peer failover mode in the properties files of the master and slave probes.

Include the following peer-to-peer settings in the master's probe properties file:

```
PeerHost      : "slave_hostname"
PeerPort      : 5555 # [communication port between master and slave probes]
```

Include the following peer-to-peer settings in the slave's probe properties file:

```
PeerHost      : "master_hostname"
PeerPort      : 5555 # [communication port between master and slave probes]
```

Properties and command line options

You use properties to specify how the probe interacts with the device. You can override the default values by using the properties file or the command line options.

The following table describes the properties and command line options specific to this probe. For information about default properties and command line options, see the *IBM Tivoli Netcool/OMNIBus Probe and Gateway Guide* (SC14-7608).

Table 8. Properties and command line options		
Property name	Command line option	Description
AckSystemId <i>string</i>	-acksystemid <i>string</i>	Use this property to specify the processing system on which the IRP Manager runs. This is used by the acknowledge_alarm CLI function. The default is "".
AckUserId <i>string</i>	-ackuserid <i>string</i>	Use this property to specify the name of the user acknowledging the alarm. This is used by the acknowledge_alarm CLI function. The default is "".
Agentheartbeat <i>integer</i>	-agentheartbeat <i>integer</i>	Use this property to specify the frequency (in seconds) with which the probe checks the status of the IRP agent. The default is 60.

Table 8. Properties and command line options (continued)

Property name	Command line option	Description
AlarmFilter <i>string</i>	-alarmfilter <i>string</i>	Use this property to specify the filter the Alarm IRP uses to limit the alarms sent to the probe. The default is "".
AlarmIrpName <i>string</i>	-alarmirpname <i>string</i>	Use this property to specify the name of the Alarm IRP Agent used by the Naming Service. The default is 32.111-3 V6.2. Note : The value of this property can differ between NetAct systems. For example, it might take the following format: NokiaNetact3gppv6AlarmIRP.
BeatInterval <i>integer</i>	-beatinterval <i>integer</i>	Use this property to specify the heartbeat interval for peer-to-peer failover. The default is 2.
ClearSystemId <i>string</i>	-clearsystemid <i>string</i>	Use this property to specify the system identifier that the <code>userid_clear_alarms</code> CLI command clears. The default is "".
ClearUserId <i>string</i>	-clearuserid <i>string</i>	Use this property to specify the user clearing the alarms using the <code>userid_clear_alarms</code> CLI command. The default is "".
CommandPort <i>integer</i>	-commandport <i>integer</i>	Use this property to specify the port through which users can connect to the 3GPP interface using the Command Line Interface (CLI) supplied with the probe. For details about the CLI, see “Command line interface” on page 8 . The default is 6970.
CommandPortLimit <i>integer</i>	-commandportlimit <i>integer</i>	Use this property to specify the maximum number of Telnet connections that can be made to the probe. The default is 10.
EntryPointIrpFile <i>string</i>	-entrypointirpfile <i>string</i>	Use this property to specify the location of the file that contains the IOR of the EntryPoint IRP object. The default is "".

Table 8. Properties and command line options (continued)

Property name	Command line option	Description
FlushBufferInterval <i>integer</i>	-flushbufferinterval <i>integer</i>	Use this property to specify how often (in seconds) the probe flushes all alerts in the buffer to the ObjectServer. The default is 0 (which instructs the probe to never flush the alerts to the ObjectServer).
InstanceId <i>string</i>	-instanceid <i>string</i>	Use this property to specify a unique identifier for the instance of the probe. This property allows you to run multiple instances of the probe on the same machine. The default is "".
Mode <i>string</i>	-mode <i>string</i>	Use this property to specify the role of an instance of the probe in a peer-to-peer failover relationship. This property takes the following values: master: The instance is the master probe. slave: The instance is the slave probe. standard: There is no failover relationship. The default is standard.
NamingServiceIORRequest <i>string</i>	-namingserviceiorrequest <i>string</i>	Use this property to specify the command that the probe uses to upload the CORBA Naming Service IOR. The default is GET /cgi-bin /get_nbif_ior.
NamingServiceHost <i>string</i>	-namingservicehost <i>string</i>	Use this property to specify the host running the CORBA Naming Service. The default is localhost.
NamingServicePort <i>integer</i>	-namingserviceport <i>integer</i>	Use this property to specify the port on which the CORBA Naming Service listens. The default is 5001.
NetActServerName <i>string</i>	-netactservername <i>string</i>	Use this property to specify the name of the Nokia-Siemens NetAct server to which the probe connects to retrieve the Naming Context IOR file. The default is "".

Table 8. Properties and command line options (continued)

Property name	Command line option	Description
NetActServerPort <i>integer</i>	<code>-netactserverport integer</code>	Use this property to specify the port on the Nokia-Siemens NetAct server through which the probe connects to retrieve the Naming Context IOR file. The default is 10115.
NotificationCategories <i>string</i>	<code>-notificationcategories string</code>	Use this property to specify the notification categories that the probe subscribes to. The default is "" (the probe subscribes to all categories). Note : To specify multiple categories, separate them using semicolons, in the following format: category1; category2; categoryn For example, to subscribe to the alarms and heartbeat events, use the following value: ALARM IRP V1.0.0; CS IRP V1.0.0
NotificationFilter <i>string</i>	<code>-notificationfilter string</code>	Use this property to specify the filter that the Notification IRP uses to limit the notifications sent to the probe. The default is "".
NotificationIrpName <i>string</i>	<code>-notificationirpname string</code>	Use this property to specify the name of the Notification IRP Agent used by the Naming Service. The default is 32.303 V6.1. Note : The value of this property can differ between NetAct systems. For example, it might take the following format: NokiaNetact3gppv6NotificationIRP
ORBCharEncoding <i>string</i>	<code>-orbcharencoding string</code>	Use this property to specify the native character encoding set used by the Object Request Broker (ORB) for character data. The default is UTF8. This property can also take the value ISO8859_1.

Table 8. Properties and command line options (continued)

Property name	Command line option	Description
ORBLocalHostName <i>string</i>	-orblocalhostname <i>string</i>	Use this property to specify the local host name used by the server-side ORB to place the server's host name into the IOR of a remote object. The default is "".
ORBLocalPort <i>integer</i>	-orblocalport <i>integer</i>	Use this property to specify the local port to which the ORB listens. The default is 0 (the ORB selects an available port at random).
ORBWCharDefault <i>string</i>	-orbwchardefault <i>string</i>	Use this property to specify what wide character (wchar) set the IBM ORB uses when communicating with other ORBs that do not publish a wchar set. The default is UTF16. This property can also take the value UCS2.
PeerHost <i>string</i>	-peerhost <i>string</i>	Use this property to specify the host to which the probe fails over in a peer-to-peer failover configuration. The default is localhost.
PeerPort <i>integer</i>	-peerport <i>integer</i>	Use this property to specify the port through which the master and slave probes communicate in a peer-to-peer failover configuration. The default is 9999.
Resynch <i>string</i>	-resynch (This is equivalent to Resynch with a value of true.) -noresynch (This is equivalent to Resynch with a value of false.)	Use this property to specify whether the probe requests all active alarms from the Nokia-Siemens NetAct system before connecting to the notification service for new alarms. This property takes the following values: false: The probe does not perform resynchronization. true: The probe performs resynchronization at startup. The default is false.

Table 8. Properties and command line options (continued)

Property name	Command line option	Description
Retry <i>string</i>	-retry <i>string</i>	Use this property to specify whether the probe attempts to reconnect to the Nokia-Siemens NetAct system following a timeout. This property takes the following values: false: The probe does not attempt to reconnect to the system true: The probe attempts to reconnect to the system The default is false.
TimeTick <i>integer</i>	-timetick <i>integer</i>	Use this property to specify the lifetime (in minutes) of the Notification IRP session on the 3GPP server. The default is 0 (there is no time limit for the session).
Timeout <i>integer</i>	-timeout <i>integer</i>	Use this property to specify the time period (in seconds) that the probe waits for the next alarm before disconnecting. The default is 0 (which instructs the probe to never disconnect).

Elements

The probe breaks event data down into tokens and parses them into elements. Elements are used to assign values to ObjectServer fields; the field values contain the event details in a form that the ObjectServer understands.

The following table describes the elements that the probe generates. Not all the elements described are generated for each event. The elements that the probe generates depend on the event type.

Table 9. Elements

Element name	Element description
AttributeValue(<i>element_name</i>)	This element contains the value of an element being monitored. This element is generated dynamically and its content is dependent on the IRP agent. Note : The <i>element_name</i> part of this element can be the name of any of the other elements in this table.
AttributeValueChange(<i>element_name</i>)	This element indicates how the value of the element being monitored has changed. Note : The <i>element_name</i> part of this element can be the name of any of the other elements in this table.

Table 9. Elements (continued)

Element name	Element description
CLEAR_SYSTEM_ID	This element indicates whether the system identifier has been cleared.
CLEAR_USER_ID	This element indicates whether the user identifier has been cleared.
DOMAIN_NAME	This element contains the name of the domain where the notification was generated.
EVENT_NAME	This element contains the extended event type for this IRP.
EVENT_TYPE	This element contains the event type of the notification.
NV_ACK_STATE	This element indicates the acknowledgement state of the alarm.
NV_ACK_SYSTEM_ID	This element contains the system ID of the IRP Manager processing the notification.
NV_ACK_TIME	This element contains the time at which the user acknowledged the alarm.
NV_ACK_USER_ID	This element identifies the last user who changed the acknowledgement state.
NV_ADDITIONAL_TEXT	This element provides information about the network element that generated the alarm.
NV_ALARM_ID	This element contains the identification information about the alarm as it appears in the alarm list.
NV_ALARM_LIST_ALIGNMENT_REQUIREMENT	This element indicates whether the alarm list requires alignment.
NV_BACK_UP_OBJECT	This element contains the Distinguished Name (DN) of the backup object.
NV_BACKED_UP_STATUS	This element identifies whether the object has been backed up.
NV_COMMENTS	This element contains the comment about the alarm.
NV_CORRELATED_NOTIFICATIONS_notif_ID_Set	This element contains the set of notifications to which this notification is considered to be correlated. This element is generated dynamically and its content is dependent on the IRP agent.

<i>Table 9. Elements (continued)</i>	
Element name	Element description
NV_CORRELATED_NOTIFICATIONS_SOURCE	This element contains the source of the notification set.
NV_EVENT_TIME	This element contains the time at which the event occurred.
NV_MANAGED_OBJECT_CLASS	This element shows the managed object class of the network resource.
NV_MANAGED_OBJECT_INSTANCE	This element contains the managed object instance of the network resource.
NV_MONITORED_ATTRIBUTE	This element contains the managed object attribute of the network resource.
NV_NOTIFICATION_ID	This element contains identification information for the notification.
NV_PERCEIVED_SEVERITY	This element indicates the relative level of urgency of the alarm.
NV_PROBABLE_CAUSE	This element provides further information about the probable cause of the alarm.
NV_PROPOSED_REPAIR_ACTIONS	This element contains the proposed repair actions for the notification.
NV_REASON	This element contains the reason that triggered the proposed repair action.
NV_SECURITY_ALARM_DETECTOR	This element contains the identifier of the detector of the security alarm.
NV_SERVICE_PROVIDER	This element contains the name of the service provider.
NV_SERVICE_USER	This element contains further information about the problem that the notification relates to.
NV_SPECIFIC_PROBLEM	This element contains further information about the problem that the notification relates to.
NV_STATE_CHANGE_DEFINITION	This element contains information about the status change of the alarm.
NV_SYSTEM_DN	This element contains the distinguished name (DN) used to identify the system.
NV_THRESHOLD_INFO	This element contains information about a threshold that has been crossed.

Table 9. Elements (continued)	
Element name	Element description
NV_TREND_INDICATION	This element indicates how an observed condition has changed.
NV_VENDOR_SPECIFIC_ALARM_TYPE	This element contains the alarm type specific to the vendor.

Error messages

Error messages provide information about problems that occur while running the probe. You can use the information that they contain to resolve such problems.

The following table describes the error messages specific to this probe. For information about generic error messages, see the *IBM Tivoli Netcool/OMNIBus Probe and Gateway Guide (SC14-7608)*.

Table 10. Error messages		
Error	Description	Action
A problem while connecting to AlarmIRP or NotificationIRPBAD_PARAM Exception i.e one or more of the in/out parameter is null: +e Cannot proceed. Shutting down! CORBA.OBJECT_NOT_EXIST exception raised. NotificationIRP is down! InvalidParameter Exception NetcoolIRPManager: Exception occurred. Stack trace to stderr OperationNotSupported Exception Unexpected CORBA Exception	The probe could not connect to AlarmIRP or NotificationIRP points due to a problem with the CORBA interface.	Check that the Nokia-Siemens NetAct server is running correctly. Refer to your CORBA documentation.
Cannot initialize the Orb: " + e:	The probe encountered a problem during initialization of the Object Request Broker (ORB).	Ensure that the \$CLASSPATH environment variable contains the path to the IBM ORB . jar files.

Table 10. Error messages (continued)

Error	Description	Action
<i>Command_Port</i> Error occurred <i>Command_Port</i> Failed to get <i>CommandPortLimit</i> property - using 10 <i>Command_Port</i> Failed to get property <i>CommandPort</i> <i>Command_Port</i> Failed to send <i>probewatch</i> message! <i>Command_Port host</i> Failed to close command socket <i>Command_Port host</i> Failed to get socket <i>IO</i> <i>Command_Port host</i> Failed to read command <i>Command_Port</i> Thread shutting down due to error! <i>NetcoolIRPManager</i>: Failed to <i>acknowledge_alarms()</i> <i>NetcoolIRPManager</i>: Failed to <i>Unacknowledge_alarms()</i>	The probe encountered a problem with the command port CLI function.	Check that you have specified the command port correctly. Check the connection between the probe and the command port.
<i>Command_Port</i> Thread shutting down due to error!	The probe encountered a problem with the command port CLI function.	Check that the CommandPort property has the correct value. Check that the <i>nco_p_nonnative</i> process is running correctly.
<i>Command_Port</i> Failed to open listening socket, shutting down Thread!	The probe could not open a listening socket on the command port specified.	Specify a different port in the CommandPort property.
COMMUNICATION FAILURE Exception i.e Server is dead <i>GetSubscriptionStatus</i> Exception	The probe could not connect to the Nokia-Siemens NetAct server.	Check that the Nokia-Siemens NetAct server is running correctly.
Error to parse event completely Failed to parse event completely Name is null, cannot create Element <i>NetcoolIRPManager</i>: Category Value NOT supported: Discarding Alarm <i>NetcoolIRPManager</i>: Error when parsing event	The probe cannot parse the alarm. This is probably because the alarm is in a format that the probe cannot understand.	Check that the Nokia-Siemens NetAct server is running correctly.

Table 10. Error messages (continued)

Error	Description	Action
Failed to get timeout property value, defaulting to 0	The probe could not get the timeout value, and is not going to time out.	Check the value of the Timeout property is correct. Change the value if necessary.
Failed to connect to the Naming Context: " + e:	The probe could not connect to the NamingContext.	Check that the NamingServiceHost and NamingServicePort properties have the correct values.
Failed to resolve the NotificationIRP object: " + e:	The probe could not resolve the NotificationIRP object as the object is not registered in the NamingService.	Check that the NotificationIrpName property has the correct value.
Name is null, cannot create Element	The probe could not create the matching element for an unknown field found in an alarm. Parsing of the remaining known fields continues.	Check whether the default fields of the ObjectServer are modified.
NetcoolIRPManager: Failed to send event	The probe could not send the parsed event to the ObjectServer.	Check whether the ObjectServer is running correctly.
NetcoolIRPManager: Failed to retrieve AlarmIRP object from security interface NetcoolIRPManager: Failed to retrieve NotificationIRP object from security interface login: Failed to get IRP object: +ex login: Unknown exception occurred +ex	The probe could not get either the AlarmIRP or the NotificationIRP object. (ex in the error message specifies the related Java exception.)	Check that the AlarmIrpName and NotificationIrpName properties have the correct values.
NetcoolIRPManager: Failed to find IOR file <i>filename</i>	The probe could not locate the IRP Manager as the <i>filename</i> does not exist.	Check that the IRP Manager is set up correctly.
NetcoolIRPManager: Failed to perform resynch Failed to perform resynch Failed to iterate through resynch alarms	The probe could not resynchronize the alarms.	Check that Nokia-Siemens NetAct server is running correctly. Check that the Resynch property has the correct value.

Table 10. Error messages (continued)

Error	Description	Action
NetcoolIRPManager: Stack Trace to stderr:	The probe could not connect to AlarmIRP or NotificationIRP points due to a problem with the CORBA interface.	Use this message from the Netcool® IRP Manager while debugging.
NetcoolIRPManager: <i>Notificationirp</i> property needs to be set NetcoolIRPManager: Both <i>NameServiceHost</i> and <i>NSPort</i> property needs to be set NetcoolIRPManager: <i>Alarmirp</i> property needs to be set	The probe could not find one or more properties required to connect to the Nokia-Siemens NetAct server.	Check that the properties given in the error message have the correct values.
Failed to connect to the Naming Context : + e	The probe cannot connect to the NamingContext.	Check that the NamingServiceHost and NamingServicePort properties have the correct values.
Failed to resolve the AlarmIRP object : + e	The AlarmIRP object is not registered in the Naming Service with the AlarmIrpName provided in the properties file.	Check that AlarmIrpName property has the correct value.
Failed to resolve the NotificationIRP object : + e	The NotificationIRP object is not registered in the Naming Service with the NotificationIrpName provided in the properties file.	Check that the NotificationIrpName property has the correct value.
NetcoolIRPManager: Failed to retrieve AlarmIRP object from security interface NetcoolIRPManager: Failed to retrieve NotificationIRP object from security interface Failed to narrow Security IRP interface : " +ex' Problem while trying to connect to the IRP points : "+e login: Failed to get IRP object : " +ex login: Unknown exception occurred " +ex	Failed to get either the AlarmIRP or NotificationIRP object. There is a problem with the CORBA interface.	Refer to your CORBA documentation.

Table 10. Error messages (continued)

Error	Description	Action
NetcoolIRPManager: Failed to find IOR file ' ' +ior_file+ ' '	The probe could not locate the IRP Manager as the <i>filename</i> does not exist.	Check that the IRP Manager has been set up correctly.
Failed to perform resynch Failed to ping notification service	There is a problem with the resynchronization process.	Check that Nokia-Siemens NetAct server is running correctly. Check that you have specified the resynchronization parameters correctly.
"Communication failure - lost connection to NoticiationIRP: " +e "CORBA.TRANSIENT exception raised. NotificationIRP is down!" "CORBA.OBJECT_NOT_EXIST exception raised. NotificationIRP is down!" "BAD_PARAM Exception i.e one or more of the in/out parameter is null: " +e "CORBA Exception stack trace to stderr: " +e "Failed to Connect : " +e" Either, the server is not running, the IOR is out of date, or probe cannot reach remote Server!" "Failed to Connect : " +e" Cannot proceed. Shutting down!"	The probe could not connect to the NotificationIRP point in the Nokia-Siemens NetAct system.	Check whether the Nokia-Siemens NetActserver is still running.
Failed to iterate through resynch alarms	The probe failed to get the alarm list or failed to perform resynchronization of alarms.	Check that the Nokia-Siemens NetAct server is running correctly. Check that the Resynch property is set correctly.
NetcoolIRPManager: Failed to acknowledge_alarms() : +e NetcoolIRPManager: Failed to Unacknowledge_alarms() : +e	The probe could not acknowledge the alarms.	Check that you have specified the command port correctly. Check the connection between the probe and the command port.
NetcoolIRPManager: ERROR when parsing a notification event NetcoolIRPManager: Stack Trace to stderr: + e	The probe has a problem during initialization of the ORB.	Ensure that the \$CLASSPATH environment variable contains the path to the IBM ORB . jar files.

Table 10. Error messages (continued)

Error	Description	Action
NetcoolIRPManager: Failed to send event : +e	The probe could not forward the event to the ObjectServer.	Check that the ObjectServer is still running.
Name is null, cannot create Element	The probe could not find one of the expected element for the event.	Check the log file that stores the alarms for the syntax error. If the probe is run in debug mode, the alarm is printed in the log file created by the probe. Also check that the alarm is in the correct format. Note : This inability of the probe to create element does not affect the parsing of the rest of the fields.
[Command Port] Failed to get CommandPortLimit property - using 10	The probe could not retrieve the value of the CommandPortLimit property.	Check that the CommandPortLimit property has the correct value. Note : As the default value is set to 10, this error does not affect the behavior of the probe.
[Command Port] Failed to get property 'CommandPort' [Command Port] Failed to open listening socket, shutting down Thread! [Command Port] Thread shutting down due to error!	The probe has failed to unacknowledge the alarms.	Check that the NV_ALARM_ID specified by the CLI is correct.
[Command Port] Error occurred :+e	A problem occurred while the user attempted to connect to the CommandPort, or while the user sent a command.	Check that the CommandPortLimit property has the correct value.
[Command Port] host Failed to get socket IO : "+e	There was a problem with command port functionality.	Check that you have specified the command port correctly. Check the connection between the probe and the command port.

Table 10. Error messages (continued)

Error	Description	Action
[Command Port] host Failed to read command : "+e [Command Port] host Failed to close command socket : +e	The probe found that there is a problem with command port functionality.	Check that you have specified the command port correctly. Check the connection between the probe and the command port.

ProbeWatch messages

During normal operations, the probe generates ProbeWatch messages and sends them to the ObjectServer. These messages tell the ObjectServer how the probe is running.

The following table describes the raw ProbeWatch error messages that the probe generates. For information about generic error messages, see the *IBM Tivoli Netcool/OMNIBus Probe and Gateway Guide* (SC14-7608).

Table 11. ProbeWatch messages

ProbeWatch message	Description	Triggers or causes
Communication failure - lost connection to NoticiationIRP Failed to get subscripton status CORBA TIMEOUT Exception while trying to get subscription status from NotificationIRP Failed to connect to NotificationIRP: <i>ae.reason</i> Shutting down Failed to Connect: Either, the server is not running, the IOR is out of date, or probe cannot reach remote Server CORBA.OBJECT _NOT_EXIST Exception: Lost connection to NotificationIRP CORBA.TRANSIENT Exception: Lost connection to NotificationIRP	The probe has failed to get the subscription status from the Notification IRP.	The notification service is not available.

Table 11. ProbeWatch messages (continued)

ProbeWatch message	Description	Triggers or causes
Connection to NotificationIRP server has been established	The probe has successfully established a connection to the Notification IRP.	The probe has successfully subscribed to the Notification service.
Detaching subscription	The probe is disconnecting from the Notification IRP.	Either the probe has not received any events for the specified timeout period, the probe is shutting down, or the probe has received a stop signal.
END SYNCHRONIZATION	The probe is closing the synchronization process.	The probe has finished receiving alarms from the alarm list.
Failed to get IRP Outline (GetIRPOutline exception caught when calling get_IRP_outline) Failed to get IRP reference (GetIRPReference exception caught when calling get_IRP_reference) Failed to get IRP references - invalid parameter (InvalidParameter exception caught when calling get_IRP_reference)	The probe could not get either the AlarmIRP or the Notification IRP object.	The AlarmirpName or NotificationirpName properties have incorrect values.
Failed to listen for commands on port number <i>listening_port</i>	The probe could not open the socket specified by the port to listen for commands.	The specified port is in use for another process.
Failed to log in to interface (InvalidParameter exception caught when calling get_IRP_outline)s	The probe could not login to the Nokia NetAct 3GPP server.	The Nokia-Siemens NetAct server is not running correctly. There is a connection error with the Nokia-Siemens NetAct server. The IOR is out of date. The probe does not have appropriate permissions required to log in to the Nokia-Siemens NetAct server.
Going Down	The probe is shutting down.	The probe has started shutting down the connection.

Table 11. ProbeWatch messages (continued)

ProbeWatch message	Description	Triggers or causes
Inactivity: No events received for <i>timeout</i> seconds	The probe has exceeded the time out period already set.	The probe did not receive events for the specified period.
Invalid IRPVersion (InvalidIRPVersion exception caught when calling <code>get_IRP_outline()</code>)	The probe could not get the Notification IRP object due to invalid IRP version.	Incorrect value set for the NotificationIrpVersion property.
NetcoolIRPManager: Failed to find IOR file <i>alarmirp_ior_file</i>	The probe has failed to get the IOR file specified.	The AlarmirpFile property in the properties file has an incorrect value.
NetcoolIRPManager: Failed to find IOR file <i>ior_file</i> g	The probe could not find the IOR file specified.	The AlarmirpFile or NotificationirpFile properties have incorrect values.
NetcoolIRPManager: Failed to find IOR file <i>notificationirp_ior_file</i>	The probe has failed to get the IOR file.	The NotificationirpFile property has an incorrect value.
PermissionDenied (PermissionDenied exception caught when calling <code>get_IRP_outline()</code> s	The probe could not login to the Nokia-Siemens NetAct server.	The probe does not have appropriate permissions required to log in to the Nokia-Siemens NetAct server.
Running	The probe is successfully running.	The probe has started functioning.
START SYNCHRONIZATION	The probe is synchronizing the events.	The probe has started receiving alarms from the alarm list.
SYNCHRONIZATION FAILED	The probe could not get new alarms.	The probe failed to get the alarm list, or failed to perform resynchronization of alarms.
Unable to get events	The probe could not get events from Nokia-Siemens NetAct.	The probe has failed to get events.

Table 11. ProbeWatch messages (continued)

ProbeWatch message	Description	Triggers or causes
Unexpected fatal error when connecting to interface Unexpected fatal error when getting IRP reference from Entry Point IRP Unexpected fatal error while getting IRP Outline Unexpected fatal error, failed to connect	The probe has received a fatal error message from the GIF/FM process.	The error message contains information about the cause of the fatal error.
Will listen for commands on port number <i>listening_port</i>	The probe is listening for commands on the port specified.	The port specified is ready to receive commands.

Running the probe

Before running the probe for the first time, you must specify a minimum set of properties.

Depending on which method you use to connect to the CORBA 3GPP interface, you must specify values for the properties described in [“Connecting to the CORBA interface”](#) on page 4.

Use the following command to start the probe:

```
$OMNIHOME/probes/nco_p_nokia_netact_3gpp_v6
```

Running multiple probes

You can run multiple instances of the probe on the same machine. For each running instance, use the **ORBLocalport** property to specify a different port to which the server listens. You must also specify a unique identifier for the probe instance using the **InstanceId** property.

Shutting down the probe

To stop an instance of the probe, issue a stop signal to the process associated with that probe instance.

Appendix A. Notices and Trademarks

This appendix contains the following sections:

- Notices
- Trademarks

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 (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing 2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, 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 want 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
Software Interoperability Coordinator, Department 49XA

3605 Highway 52 N
Rochester, MN 55901
U.S.A.

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 information 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.

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

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

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

Trademarks

IBM, the IBM logo, ibm.com, AIX, Tivoli, zSeries, and Netcool are trademarks of International Business Machines Corporation in the United States, other countries, or both.

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.

Intel, Intel Inside (logos), MMX, and Pentium are trademarks of Intel Corporation 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.

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

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

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



SC22-5411-00

