IBM® Tivoli® Netcool/OMNIbus Probe for Alcatel-Lucent 5529 (OAD) V6
7.5

Reference Guide
March 12, 2021

IBM

Note

Before using this information and the product it supports, read the information in Appendix A, "Notices and Trademarks," on page 37.

Contents

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 Probe for Alcatel-Lucent 5529 OAD V6 documentation is provided in softcopy format only. To obtain the most recent version, visit the following IBM Documentation page:

https://www.ibm.com/support/knowledgecenter/SSSHTQ_int/omnibus/probes/common/Probes.html

Table 1. Document modification history

Document version	Publication date	Comments
SC22-5420-00	November 4, 2011	First IBM publication.
SC22-5420-01	March 2, 2012	Note about lack of support for SSL communication features when running the AIX version of the probe added to "Summary" on page 1.
SC22-5420-02	August 3, 2012	"Configuring SSL connections" on page 12 added. The following properties added to "Properties and command line options" on page 18: • **CertificateStore** • **CertificateStorePassword** • **TrustStore** • **TrustStorePassword** • **UseSsl**
SC22-5420-03	November 30, 2012	"JMS ports" on page 16 updated. Descriptions for the following properties in "Properties and command line options" on page 18 updated: • **ClusterURL** • **FlushBufferInterval** • **UseSsl**
SC22-5420-04	April 28, 2013	Support extended to OAD version 9.2.
SC22-5420-05	December 6, 2013	"Backoff strategy" on page 15 added. "Additional considerations" on page 13 updated.
SC22-5420-06	June 12, 2014	Support extended to OAD version 9.3. "Summary" on page 1 updated.
SC22-5420-07	July 11, 2014	"Summary" on page 1 updated.

Table 1. Document modification history (continued)		
Document version	**Publication date**	**Comments**
SC22-5420-08	June 11, 2015	Support extended to OAD version 9.4. "Summary" on page 1 updated. "Configuring SSL connections" on page 12 updated. "Using HTTP or HTTPS protocol" on page 15 updated. Descriptions for the following properties added to "Properties and command line options" on page 18 : • **JavaNamingFactoryInitial** • **ResyncRetryInterval** • **HttpHostPort** • **HttpTimeout** • **SingletonServerPort** Description for the **ClusterURL** property updated. **HttpHost** and **HttpPort** properties removed. **Enhancements:** Version 5 of the Probe for Alcatel-Lucent 5529 OAD includes the following enhancements: • **41495**: Functionality added for retrying resynchronization if it initially fails. • **41581**: Functionality added for specifying multiple hosts for the probe to connect to. • **65449**: Support added for Alcatel-Lucent OAD 9.4.
SC22-5420-09	March 10, 2016	Support extended to OAD version 9.5. "Summary" on page 1 updated. "Jar files" on page 4 updated.
SC22-5420-10	September 15, 2016	Guide updated for version 6 of Probe for Alcatel-Lucent 5529 OAD. "Summary" on page 1 updated. Descriptions for the following properties added to "Properties and command line options" on page 18 : • **AxSSSLSupport** • **JndiConfigFile** **Enhancements:** Version 6 of the Probe for Alcatel-Lucent 5529 OAD includes the following enhancements: • **88886**: Provision of additional parameters for SSL connections.
SC22-5420-11	March 14, 2017	Guide updated for Version 7 of Probe for Alcatel-Lucent 5529 OAD. Support extended to OAD version 9.6. "Summary" on page 1 updated. "Jar files" on page 4 updated.

Table 1. Document modification history (continued)		
Document version	**Publication date**	**Comments**
SC22-5420-12	November 23, 2017	Support extended to OAD version 9.6.03. "Summary" on page 1 updated. "Jar files" on page 4 updated.
SC22-5420-13	August 9, 2018	Support extended to OAD version 9.6.05. "Summary" on page 1 updated. "Jar files" on page 4 updated.
SC22-5420-14	June 28, 2019	Support extended to OAD version 9.7. "Summary" on page 1 updated. "Jar files for OAD Version 9.7" on page 10 updated. "Properties and command line options" on page 18 updated.
SC22-5420-15	July 16, 2020	Guide updated for Version 7.5 of Probe for Alcatel-Lucent 5529 OAD. Support extended to OAD version 9.7.03 and 9.7.05. "Summary" on page 1 updated. "Jar files for OAD Version 9.7.03" on page 10 added. "Configuring SSL connections" on page 12 updated. **Fixes:**Version 7.5 of the Probe for Alcatel-Lucent 5529 OAD includes fixes for the following APARs: • **IJ24265**: Introduced new properties: **CertificateStoreType** and **TrustStoreType** both with the default value of JKS. • **IJ07134**: Fixed probe crash issue in Solaris platform by setting io.netty.noUnsafe=true in probe environment file. The issue is caused by a defect reported in JBoss Enterprise Application Platform (JBEAP-5410). • **IJ06495**: Enriching Node field with aliasValue token to avoid unnecessary alarm suppression due to deduplication. • **IJ05710**: Updated README/description.txt to include jar file requirements for integration to OAD version 9.6.03. • **IJ00242**: Fixed issue where probe does not create connection when HEAD request not returning the expected code. The issue was observed when probe attempted connection to OAD version 9.6.03.
SC22-5420-16	March 12, 2021	Support extended to OAD version 9.7.07. "Summary" on page 1 updated. "Jar files for OAD Version 9.7.07" on page 11 added.

Note: The Probe for Alcatel-Lucent 5529 OAD V6 was previously documented in the same reference guide as the Probe for Alcatel-Lucent 5529 OAD. This reference guide documents the Probe for Alcatel-Lucent 5529 OAD V6 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** *arch*
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 Alcatel-Lucent 5529 OAD V6

The Alcatel-Lucent 5529 OSS Alarm Dispatcher (OAD) collects alarms from multiple Alcatel-Lucent Element Management Systems (EMS), and sends them to multiple client Operational Support Systems (OSS) using SOAP/XML requests. The requests pass through the Multi-Technology Operations System Interface (MTOSI).

The Alcatel-Lucent 5529 OAD permits the subscription and filtering mechanism for retrieval of real-time and stored alarms.

The Probe for Alcatel-Lucent 5529 OAD V6 connects to the Alcatel-Lucent 5529 OAD system using the MTOSI/JMS standard interface, and formats the received alarms using the MTOSI 1.1 standard.

This guide contains the following sections:

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 for Alcatel-Lucent 5529 OAD V6.

Table 3. Summary	
Probe target	Alcatel-Lucent/Nokia 5529 OAD versions 6.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.6.03, 9.6.05, 9.6.07, 9.7, 9.7.03, 9.7.05 and 9.7.07 Alcatel-Lucent/Nokia 5520 AMS 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.6.03, 9.6.05, 9.6.07, 9.7, 9.7.03, 9.7.05 and 9.7.07
Probe executable name	`nco_p_alcatel_5529_oad_v6`
Probe installation package	`omnibus-`*`arch`*`-probe-nco-p-alcatel-5529-oad-v6-`*`version`*
Package version	7.5
Probe supported on	For details of supported operating systems, see the following Release Notice on the IBM Software Support Website: https://www-304.ibm.com/support/docview.wss?uid=swg21569435
Properties file	`$OMNIHOME/probes/arch/alcatel_5529_oad_v6.props`

Table 3. Summary (continued)	
Rules file	`$OMNIHOME/probes/arch/alcatel_5529_oad_v6.rules`
Requirements	A list of jar files are required by the probe (they are available from Alcatel-Lucent). For a full list of the required jar files, see "Jar files" on page 4.
	For details of any additional software that this probe requires, refer to the `description.txt` file that is supplied in its download package.
	Requirement for probe to integrate with Alcatel-Lucent OAD 9.6.03 and above
	Java 1.8
	At least probe test-fix version 7.1.
	Requirement for probe to integrate with Alcatel-Lucent OAD 9.7.03 and above
	Java 1.8
	At least probe version 7.5.
	Note: Probe test-fix packages can be acquired via IBM Support.
Connection method	HTTP/HTTPS and JMS
Remote connectivity	The Probe for Alcatel-Lucent 5529 OAD can connect to devices on remote hosts. Details of the remote hosts are specified using the **HttpHostPort** property in the properties file.
Multicultural support	Not 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 *IBM Tivoli Netcool/ OMNIbus Installation and Deployment Guide*.

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 IBM Documentation:

https://www.ibm.com/support/knowledgecenter/SSSHTQ_int/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 in IBM Documentation:

https://www.ibm.com/support/knowledgecenter/SSSHTQ_int/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*.

Configuring the probe

After installing the probe, you need to make various configuration settings to suit your environment.

This section contains topics on the Alcatel-Lucent 5529 OAD configuration requirements:

Obtaining the probe-nonnative patch

As well as the basic patch, you must also download the `probe-nonnative` patch.

To obtain the `probe-nonnative` patch:

1. Access the Passport Advantage website: http://www-306.ibm.com/software/howtobuy/passportadvantage/
2. Select **Software Downloads**.
3. Perform a text search on `nonnative`.
4. Select **Expand All** to see all search results.
5. Select the patch that corresponds to your hardware platform.

Configuring Sun Java

If you are using the probe to integrate with Alcatel-Lucent OAD 9.1, you require Sun Java 1.6. The Sun Java 1.6 Java patches are not supplied with the probe.

To instruct the probe to use Sun Java 1.6, you must set the appropriate environment variable.

For Linux and UNIX operating systems, set the $JAVA_HOME environment variable to the location of the JRE path. For example, if the Java executable is in `/usr/lib/j2re1.6/jre/bin/java`, then set $JAVA_HOME to `/usr/lib/j2re1.6/jre`.

For Windows operating systems, set the %PATH% environment variable to the location of the `javaw.exe` executable. For example, if the location of `javaw.exe` is `C:\SUN_Java\Java60\jre\bin\javaw.exe`, then set the %PATH% environment variable to `C:\SUN_Java\Java60\jre\bin`

Jar files

As a part of the configuration process, you must copy various JAR files to the java folder in your Netcool/OMNIbus installation and include their path in your $CLASSPATH environment variable. Which JAR files you copy depends on the version of Alcatel-Lucent 5529 OAD that you are running.

Jar files for OAD Version 9.1

As a part of the configuration process, you must copy various jar files to the `java` folder in your Netcool/OMNIbus installation and include their path in your $CLASSPATH environment variable.

The following JBoss libraries (available from Alcatel-Lucent) are required by the probe when running against OAD version 9.1:

- `axs-mobject-remote-api-5520.jar`
- `commons-logging-1.0.4.jar`
- `concurrent-1.3.4.jar`
- `javassist-3.10.0.GA.jar`
- `jboss-aop-2.1.1.GA.jar`
- `jboss-as-cluster-5.1.0.GA-jboss-ha-legacy-client.jar`
- `jboss-as-cluster-5.1.0.GA.jar`
- `jboss-as-security-5.1.0.GA.jar`
- `jboss-client-5.1.0.CR1.jar`
- `jboss-common-core-2.2.14.GA.jar`
- `jboss-ha-client-1.1.1.GA.jar`
- `jboss-javaee-5.0.1.GA.jar`
- `jboss-logging-spi-2.1.0.GA.jar`
- `jboss-mdr-2.0.1.GA.jar`
- `jboss-messaging-client-1.4.3.GA.jar`
- `jboss-remoting-2.5.1.jar`
- `jboss-security-spi-2.0.3.SP1.jar`
- `jboss-serialization-1.0.3.GA.jar`
- `jbosssx-2.0.3.SP1.jar`
- `jbosssx-client-2.0.3.SP1.jar`
- `jms-1.1.jar`
- `jnp-client-5.0.3.GA.jar`
- `log4j-1.2.13.jar`
- `trove-2.1.1.jar`
- `jaxen-1.1.1.jar`
- `jaxen-jdom-1.0.jar`
- `jdom-1.1.jar`
- `saxpath-1.0-FCS.jar`

Jar files for OAD Version 9.2

As a part of the configuration process, you must copy various jar files to the `java` folder in your Netcool/OMNIbus installation and include their path in your $CLASSPATH environment variable.

The following JBoss libraries (available from Alcatel-Lucent) are required by the probe when running against OAD version 9.2:

- `axs-mobject-remote-api-9.2.10-148894.jar`
- `commons-logging-1.0.4.jar`
- `concurrent-1.3.4.jar`
- `javassist-3.10.0.GA.jar`
- `jaxen-1.1.1.jar`
- `jaxen-jdom-1.0.jar`
- `jboss-aop-2.1.1.GA.jar`
- `jboss-as-cluster-5.1.0.GA-jboss-ha-legacy-client.jar`
- `jboss-as-cluster-5.1.0.GA.jar`
- `jboss-as-security-5.1.0.GA.jar`
- `jboss-client-5.1.0.CR1.jar`
- `jboss-common-core-2.2.14.GA.jar`
- `jboss-ha-client-1.1.1.GA.jar`
- `jboss-javaee-5.0.1.GA.jar`
- `jboss-logging-spi-2.1.0.GA.jar`
- `jboss-mdr-2.0.1.GA.jar`
- `jboss-messaging-client-1.4.6.GA.jar`
- `jboss-remoting.jar`
- `jboss-security-spi-2.0.3.SP1.jar`
- `jboss-serialization-1.0.3.GA.jar`
- `jbosssx-2.0.3.SP1.jar`
- `jbosssx-client-2.0.3.SP1.jar`
- `jdom-1.1.jar`
- `jnp-client-5.0.3.GA.jar`
- `junit-3.8.1.jar`
- `log4j-1.2.13.jar`
- `oad-oss-client-9.2.10_9.2.10-148894.jar`
- `oss-client-utils-1.0.jar`
- `oss-client-utils-src-1.0.jar`
- `saxpath-1.0-FCS.jar`
- `trove-2.1.1.jar`

Jar files for OAD Version 9.3.10

As a part of the configuration process, you must copy various jar files to the `java` folder in your Netcool/OMNIbus installation and include their path in your $CLASSPATH environment variable.

The following JBoss libraries (available from Alcatel-Lucent) are required by the probe when running against OAD version 9.3.10:

- `axs-mobject-remote-api-trunk-236769.jar`
- `commons-logging-1.0.4.jar`
- `concurrent-1.3.4.jar`
- `hornetq-core-client-2.2.071113.jar`
- `hornetq-jms-client-2.2.071113.jar`
- `javassist-3.10.0.GA.jar`
- `jaxen-1.1.jar`

- `jboss-aop-2.1.6.GA.jar`
- `jboss-as-cluster-5.1.0.GA-jboss-ha-legacy-client.jar`
- `jboss-as-security-5.1.0.GA.jar`
- `jboss-client-5.1.0.CR1.jar`
- `jboss-common-core-2.2.14.GA.jar`
- `jboss-ha-client-1.1.1.GA.jar`
- `jboss-javaee-5.0.1.GA.jar`
- `jboss-logging-spi-2.1.0.GA.jar`
- `jboss-mdr-2.0.1.GA.jar`
- `jboss-remoting.jar`
- `jboss-security-spi-2.0.5.SP3-1.jar`
- `jboss-serialization-1.0.3.GA.jar`
- `jbosssx-2.0.5.SP3-1.jar`
- `jbosssx-client-2.0.5.SP3-1.jar`
- `jdom-1.1.jar`
- `jms-1.1.jar`
- `jnp-client-5.0.3.GA.jar`
- `junit-3.8.1.jar`
- `log4j-1.2.14.jar`
- `netty-3.2.3.Final.jar`
- `trove-2.1.1.jar`

Jar files for OAD Version 9.4

As a part of the configuration process, you must copy various jar files to the `java` folder in your Netcool/OMNIbus installation and include their path in your $CLASSPATH environment variable.

The following JBoss libraries (available from Alcatel-Lucent) are required by the probe when running against OAD version 9.4:

- `axs-mobject-remote-api-9.4-xxxxxxx.jar`
- `commons-logging-1.0.4.jar`
- `concurrent-1.3.4.jar`
- `hornetq-core-client-2.3.1.Final-ALU-1.jar`
- `hornetq-jms-client-2.3.1.Final-ALU-1.jar`
- `jaxen-1.1.jar`
- `jboss-aop-2.1.6.GA.jar`
- `jboss-as-security-7.2.0.Final-ALU-8.jar`
- `jboss-client.jar`
- `jdom-1.1.2-ALU-2.jar`
- `jms-1.1.jar`
- `junit-3.8.1.jar`
- `log4j-1.2.14.jar`
- `netty-3.6.2.Final-ALU-1.jar`
- `trove-2.1.1.jar`

Jar files for OAD Version 9.5

As a part of the configuration process, you must copy various jar files to the `java` folder in your Netcool/OMNIbus installation and include their path in your $CLASSPATH environment variable.

The following JBoss libraries (available from Alcatel-Lucent) are required by the probe when running against OAD version 9.5:

When running against OAD version 9.5, the probe requires the following JBoss libraries:

- `axs-mobject-api-9.5-xxxxxxx.jar`
- `axs-mobject-remote-api-9.5-xxxxxxx.jar`
- `commons-logging-1.0.4.jar`
- `concurrent-1.3.4.jar`
- `hornetq-core-client-2.3.1.Final-ALU-1.jar`
- `hornetq-jms-client-2.3.1.Final-ALU-1.jar`
- `jaxen-1.1-beta-9.jar`
- `jboss-aop-2.1.6.GA.jar`
- `jboss-as-security-7.2.0.Final-ALU-8.jar`
- `jboss-client.jar`
- `jdom-1.1.2-ALU-2.jar`
- `jms-1.1.jar`
- `junit-3.8.1.jar`
- `log4j-1.2.14.jar`
- `netty-3.6.2.Final-ALU-1.jar`
- `trove-2.1.1.jar`

Jar files for OAD Version 9.5.02

As a part of the configuration process, you must copy various jar files to the `java` folder in your Netcool/OMNIbus installation and include their path in your $CLASSPATH environment variable.

The following JBoss libraries (available from Alcatel-Lucent) are required by the probe when running against OAD version 9.5.02:

- `axs-mobject-api-9.5-xxxxxxx.jar` (**Note**: xxxxxx is the final build number for OAD.)
- `axs-mobject-remote-api-9.5-xxxxxxx.jar`
- `commons-logging-1.0.4.jar`
- `concurrent-1.3.4.jar`
- `hornetq-core-client-2.4.5.Final.jar`
- `hornetq-jms-client-2.4.5.Final.jar`
- `jaxen-1.1-beta-9.jar`
- `jboss-aop-2.1.6.GA.jar`
- `jboss-client.jar`
- `jdom-1.1.2-ALU-2.jar`
- `jms-1.1.jar`
- `junit-3.8.1.jar`
- `log4j-1.2.14.jar`
- `trove-2.1.1.jar`
- `wildfly-security-8.2.1.Final.jar`

The jar files form a part of the server installation and must be copied to the following location:

`$OMNIHOME/probes/java/nco_p_alcatel_5529_oad_v6`

On Windows operating systems, the jar files must be copied to the following location:

`%OMNIHOME%\probes\win32`

You must also include this path in the $CLASSPATH environment variable.

The default install locations for these files (the locations from which you can copy the files) are described in the sections that follow.

Jar files for OAD Version 9.6

As a part of the configuration process, you must copy various jar files to the `java` folder in your Netcool/OMNIbus installation and include their path in your $CLASSPATH environment variable.

The following JBoss libraries (available from Alcatel-Lucent) are required by the probe when running against OAD version 9.6:

- `axs-mobject-api-9.6-xxxxxxx.jar`
- `axs-mobject-remote-api-9.6-xxxxxxx.jar`
- `jboss-client.jar`
- `log4j-1.2.14.jar`

Note: The OAD requires JRE 1.8.

Note: xxxxxx is the final build number for the OAD.

Jar files for OAD Version 9.6.03

As a part of the configuration process, you must copy various jar files to the `java` folder in your Netcool/OMNIbus installation and include their path in your $CLASSPATH environment variable.

The following JBoss libraries (available from Alcatel-Lucent) are required by the probe when running against OAD version 9.6.03:

- `axs-encription-app-9.6.03-xxxxxxx.jar`
- `axs-mobject-api-9.6.03-xxxxxxx.jar`
- `axs-mobject-remote-api-9.6.03-xxxxxxx.jar`
- `commons-io-2.4.jar`
- `jboss-logging-3.3.0.Final.jar`
- `log4j-1.2.14.jar`
- `picketbox-4.9.6.Final.jar`
- `picketbox-infinispan-4.9.6.Final.jar`
- `slf4j-simple-1.7.21.jar`
- `wildfly-client-all.jar`
- `xbean-2.6.0.jar`

The jar files form a part of the server installation and must be copied to the following location:

`$OMNIHOME/probes/java/nco_p_alcatel_5529_oad_v6`

On Windows operating systems, the jar files must be copied to the following location:

`%OMNIHOME%\probes\win32`

You must also include this path in the $CLASSPATH environment variable.

Note: The OAD requires JRE 1.8.

Note: xxxxxx is the final build number for the OAD.

Jar files for OAD Version 9.6.05

As a part of the configuration process, you must copy various jar files to the `java` folder in your Netcool/OMNIbus installation and include their path in your $CLASSPATH environment variable.

The following JBoss libraries (available from Alcatel-Lucent) are required by the probe when running against OAD version 9.6.05:

- `axs-encription-app-9.6.05-xxxxxx.jar`
- `axs-mobject-api-9.6.05-xxxxxx.jar`
- `axs-mobject-remote-api-9.6.05-xxxxxx.jar`
- `commons-io-2.4.jar`
- `jboss-logging-3.3.0.Final.jar`
- `log4j-1.2.14.jar`
- `picketbox-4.9.6.Final.jar`
- `picketbox-infinispan-4.9.6.Final.jar`
- `slf4j-simple-1.7.21.jar`
- `wildfly-client-all.jar`
- `xbean-2.6.0.jar`

The jar files form a part of the server installation and must be copied to the following location:

`$OMNIHOME/probes/java/nco_p_alcatel_5529_oad_v6`

On Windows operating systems, the jar files must be copied to the following location:

`%OMNIHOME%\probes\win32`

You must also include this path in the $CLASSPATH environment variable.

Note: The OAD requires JRE 1.8.

Note: xxxxxx is the final build number for the OAD.

Jar files for OAD Version 9.6.07

As a part of the configuration process, you must copy various jar files to the `java` folder in your Netcool/OMNIbus installation and include their path in your $CLASSPATH environment variable.

The following JBoss libraries (available from Alcatel-Lucent) are required by the probe when running against OAD version 9.6.07:

- `axs-encription-app-9.6.07-xxxxxx.jar`
- `axs-mobject-api-9.6.07-xxxxxx.jar`
- `axs-mobject-remote-api-9.6.07-xxxxxx.jar`
- `commons-io-2.4.jar`
- `jboss-logging-3.3.0.Final.jar`
- `log4j-1.2.14.jar`
- `nco_p_alcatel_5529_oad_v6.jar`
- `picketbox-4.9.6.Final.jar`
- `picketbox-infinispan-4.9.6.Final.jar`
- `slf4j-simple-1.7.21.jar`
- `wildfly-client-all.jar`
- `xbean-2.6.0.jar`

The jar files form a part of the server installation and must be copied to the following location:

`$OMNIHOME/probes/java/nco_p_alcatel_5529_oad_v6`

On Windows operating systems, the jar files must be copied to the following location:

`%OMNIHOME%\probes\win32`

You must also include this path in the $CLASSPATH environment variable.

Note: The OAD requires JRE 1.8.

Note: `xxxxxx` is the final build number for the OAD.

Jar files for OAD Version 9.7

As a part of the configuration process, you must copy various jar files to the `java` folder in your Netcool/OMNIbus installation and include their path in your $CLASSPATH environment variable.

The following JBoss libraries (available from the `oad-oss-client-1.0_9.7.0-xxxxxx/lib` folder of the 5529 OAD sample client) are required by the probe when running against OAD version 9.7:

- `axs-encription-app-9.7.0-xxxxxx.jar`
- `axs-encrypt-utils-9.7.0-xxxxxx.jar`
- `axs-mobject-api-9.7.0-xxxxxx.jar`
- `axs-mobject-remote-api-9.7.0-xxxxxx.jar`
- `commons-io-2.5.jar`
- `jboss-logging-3.3.1.Final.jar`
- `log4j-api-2.11.0.jar`
- `log4j-core-2.11.0.jar`
- `nco_p_alcatel_5529_oad_v6.jar`
- `picketbox-5.0.2.Final.jar`
- `picketbox-infinispan-5.0.2.Final.jar`
- `slf4j-simple-1.7.21.jar`
- `wildfly-client-all.jar`
- `xbean-2.6.0.jar`

The jar files form a part of the server installation and must be copied to the following location:

`$OMNIHOME/probes/java/nco_p_alcatel_5529_oad_v6`

On Windows operating systems, the jar files must be copied to the following location:

`%OMNIHOME%\probes\win32`

You must also include this path in the $CLASSPATH environment variable.

Note: The OAD requires JRE 1.8.

Note: `xxxxxx` is the final build number for the OAD.

Jar files for OAD Version 9.7.03

As a part of the configuration process, you must copy various jar files to the `java` folder in your Netcool/OMNIbus installation and include their path in your $CLASSPATH environment variable.

The following JBoss libraries (available from the `oad-oss-client-1.0_9.7.03-xxxxxx/lib` folder of the 5529 OAD sample client) are required by the probe when running against OAD version 9.7.03:

- `axs-encription-app-9.7.03-xxxxxx.jar`
- `axs-encrypt-utils-9.7.03-xxxxxx.jar`
- `axs-mobject-api-9.7.03-xxxxxx.jar`
- `axs-mobject-remote-api-9.7.03-xxxxxx.jar`
- `commons-io-2.5.jar`

- `jboss-logging-3.3.1.Final.jar`
- `log4j-api-2.11.0.jar`
- `log4j-core-2.11.0.jar`
- `nco_p_alcatel_5529_oad_v6.jar`
- `oad-oss-client-1_9.7.03-xxxxxx.jar`
- `oss-client-utils-1.0.jar`
- `picketbox-5.0.2.Final.jar`
- `picketbox-infinispan-5.0.2.Final.jar`
- `slf4j-api-1.8.0-beta2.jar`
- `slf4j-simple-1.8.0-beta2.jar`
- `wildfly-client-all.jar`
- `xbean-2.6.0.jar`

The jar files form a part of the server installation and must be copied to the following location:

`$OMNIHOME/probes/java/nco_p_alcatel_5529_oad_v6`

On Windows operating systems, the jar files must be copied to the following location:

`%OMNIHOME%\probes\win32`

You must also include this path in the $CLASSPATH environment variable.

Note: The OAD requires JRE 1.8.

Note: xxxxxx is the final build number for the OAD.

Jar files for OAD Version 9.7.07

As a part of the configuration process, you must copy various jar files to the `java` folder in your Netcool/OMNIbus installation and include their path in your $CLASSPATH environment variable.

The following JBoss libraries (available from the `oad-oss-client-1.0_9.7.07-xxxxxx/lib` folder of the 5529 OAD sample client) are required by the probe when running against OAD version 9.7.07:

- `axs-encription-app-9.7.07-xxxxxx.jar`
- `axs-encrypt-utils-9.7.07-xxxxxx.jar`
- `axs-mobject-api-9.7.07-xxxxxx.jar`
- `axs-mobject-remote-api-9.7.07-xxxxxx.jar`
- `commons-io-2.5.jar`
- `jboss-logging-3.4.1.Final.jar`
- `log4j-api-2.13.2.jar`
- `log4j-core-2.13.2.jar`
- `nco_p_alcatel_5529_oad_v6.jar`
- `picketbox-5.0.3.Final.jar`
- `picketbox-infinispan-5.0.3.Final.jar`
- `slf4j-api-1.8.0-beta2.jar`
- `slf4j-simple-1.8.0-beta2.jar`
- `wildfly-client-all.jar`
- `xbean-2.6.0.jar`

The jar files form a part of the server installation and must be copied to the following location:

`$OMNIHOME/probes/java/nco_p_alcatel_5529_oad_v6`

On Windows operating systems, the jar files must be copied to the following location:

`%OMNIHOME%\probes\win32`

You must also include this path in the $CLASSPATH environment variable.

The keystore file from the `oad-oss-client-1.0_9.7.07-xxxxxx` folder of the 5529 OAD sample client must be copied to the Netcool/OMNIbus server.

Note: The OAD requires JRE 1.8.

Note: `xxxxxx` is the final build number for the OAD.

Configuring SSL connections

You can enable Secure Socket Layer (SSL) encryption of data exchanged over JMS and HTTP. A Java keystore file is required for this HTTPS connection, access to which is specified using the **CertificateStore** and **CertificateStorePassword** properties. The keystore file can be created using the Java `keytool` command.

For general details of JMS connections over SSL guidelines, see https://community.jboss.org/wiki/JMSOverSSL?_sscc=t.

To enable SSL encryption, use the following steps:

1. Use the `keytool` command to generate the keystore by running the following command:

   ```
   keytool -genkey -alias sslprobecert -keyalg RSA -keystore alcateload.jks -
   keysize 2048
   ```

   Note: If you are running more than one probe, you must generate a keystore for each probe and provide a different name for each, for example, `alcateload01.jks`, `alcateload02.jks`, `alcateload03.jks`, and so forth.

2. When prompted for a password, press ENTER to use the same password as the keystore password.

   Note: To reset the password for the probe's Java keystore at a later date, you can use the following command:

   ```
   keytool -storepasswd -new new_storepass -keystore alcateload.jks
   ```

3. Store the keystore file in the following directory:

   `$OMNIHOME/probes/java/keystore/nco_p_alcatel_5529_oad_v6/`

4. Obtain the Alcatel EMS certificate (`alcatelclient.cert`) certificate. Consult your Alcatel documentation for instructions about obtaining certificate files.

5. Import the Alcatel EMS certificate into the keystore file using the following command:

   ```
   keytool -import -trustcacerts -alias alcatelsslclientcert -file
   alcatelclient.cert -keystore alcateload.jks
   ```

6. Verify that the certificate has been imported into the keystore using the following command:

   ```
   keytool -list -v -keystore alcateload.jks
   ```

7. Set the probe's **UseSsl** property to `true` and configure the ports specified with the probe's **HttpHostPort** property to use the default Alcatel EMS HTTPS port, for example, 8443.

8. Specify values for the following probe properties, using the same Java keystore file as both certificate store and trusted certificates store, using the same password for each:

   - **CertificateStore**: Specify the path of the probe's Java keystore that you created.
   - **CertificateStorePassword**: Specify the password that you set for the Java keystore.
   - **TrustStore**: Specify the same value as that set for the **CertificateStore** property.
   - **TrustStorePassword**: Specify the same value as that set for the **CertificateStorePassword** property.

   Note:

The format of the keystore file that the AMS/OAD uses has changed in 9.7.03 from JKS to PKCS12.

Probe version 7.5 has introduced new properties which can be used to configure keystore type:

```
CertificateStoreType: "PKCS12"
TrustStoreType:       "PKCS12"
```

Due to a limitation in IBM Java, the Probe requires Oracle Java rather than IBM Java to connect to the OAD 9.7.03 or later.

Example SSL configuration property settings

The following example shows SSL configuration settings from the properties file of an example Probe for Alcatel-Lucent 5529 OAD:

```
HTTPHostPort                : "198.162.20.21:8443"
UseSsl                      : "true"
CertificateStore            :
"/opt/IBM/tivoli/netcool/omnibus/probes/java/keystore/nco_p_alcatel_5529_oad_v6/
alcateload.jks"
CertificateStorePassword    :     "ECEDBJAGBJFHGD"
TrustStore                  :
"/opt/IBM/tivoli/netcool/omnibus/probes/java/keystore/nco_p_alcatel_5529_oad_v6/
alcateload.jks"
TrustStorePassword          : "ECEDBJAGBJFHGD"
```

Problem and resolution events

To match problem and resolution events correctly, you need to send the relevant alarm details when sending a notification to the probe. Refer to relevant AMS reference guide for details to enable this feature.

Alternatively, use the following steps:

1. Log into the AMS GUI as a 5520 AMS administrator.
2. Open the **Administration** perspective.
3. Navigate under the **EMS Administration Tree** to **Configuration** > **NBI** > **OAD NBI Settings**.
4. Select the **Show Alarm Details in Alarm Change Notifications** checkbox.
5. Click the blue check mark at the top of the page.

Additional considerations

OAD can only function with security enabled for Java Message Service (JMS) Notifications. The probe cannot allow security to be enabled for JMS Notifications and disabled for the Web Services interface at the same time. Therefore, both JMS Notifications and the Web Services interface must have security enabled.

When OAD is installed in a cluster, the notification identifiers for OAD generated alarms assigned by one OAD server do not follow sequentially those assigned by another OAD server. This affects alarms such as `heartbeat` or `eventLossOccured`, . Since Netcool/OMNIbus uses the notification identifier to correlate some alarms in the `EventList`, if the activity has switched from one OAD server to another in the cluster, the `EventList` can potentially correlate unrelated alarms since their notification identifiers can match. This is not applicable to NE or AMS alarms: their notification identifier is constructed in the format `domain_name:number`, so it is unique; the same notification identifier is used for the same alarm across all the cluster nodes.

Running the probe

Probes can be run in a variety of ways. The way you chose depends on a number of factors, including your operating system, your environment, and the any high availability considerations that you may have.

For details about how to run the probe, visit the following page in IBM Documentation:

https://www.ibm.com/support/knowledgecenter/SSSHTQ_int/omnibus/probes/all_probes/wip/concept/running_probe.html

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 for Alcatel-Lucent 5529 OAD connects to the Alcatel-Lucent 5529 OAD system using the HTTP or HTTPS protocol. The probe subscribes to the JMS topic to retrieve new alarms as they are generated. It then sends a resynchronization request by calling the MTOSI **getActiveAlarms** functions.

Data acquisition is described in the following topics:

- "Peer-to-peer failover functionality" on page 14
- "Backoff strategy" on page 15
- "Using HTTP or HTTPS protocol" on page 15
- "Resynchronizing alarms" on page 16
- "Java Message Service" on page 16
- "Using durable subscriptions" on page 17
- "Disabling durable subscriptions" on page 17
- "Java Messaging Service filter" on page 17
- "Inactivity" on page 17
- "Command line interface" on page 17

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"
```

Backoff strategy

If the **Retry** property is set to `true`, and the probe fails to establish a connection or loses an existing connection to the device, the probe reverts to a backoff strategy.

The probe's backoff strategy is to try to reestablish a connection at successive intervals of one second, two seconds, four seconds, eight seconds, and so on, up to a maximum of 4096 seconds. When the maximum retry interval is reached, the probe stops trying to reconnect and will not try again until it is restarted.

Using HTTP or HTTPS protocol

The probe builds an HTTP or HTTPS URL connection to the Alcatel-Lucent 5529 OAD system.

Using the HTTP protocol

The probe connects to an HTTP port to send SOAP/XML requests to the host Alcatel-Lucent OAD system. The connection details are specified by the **HttpHostPort** property.

In the **HttpHostPort** property, you can specify either a single `host:port` pair or you can specify a comma-separated list of `host:port` pairs. The **HttpHostPort** property supports both IPv4 and IPv6 addresses.

Rotating endpoints

When the probe starts, it extracts the list of `host:port` pairs from the **HttpHostPort** property. To execute alarm resynchronization or `CommandPort` commands that involve actions in the Alcatel-Lucent OAD system (for example, the **acknowledge_alarm** command), the probe attempts to connect to the nodes in turn in the order listed. When the probe successfully connects to a node, it sends the request to that node and will not attempt to connect to further nodes. If the probe cannot connect to any of the nodes listed in the **HttpHostPort** property, the probe writes a warning message to the probe error log.

Using the HTTPS protocol

The Probe for Alcatel-Lucent 5529 OAD uses Java keystore files and an HTTPS URL Connection to connect directly to the system using the HTTPS protocol.

For the probe to connect to the system in HTTPS mode, enable the SSL connection using the **UseSsl** property. To access the keys and certificates in the Java keystore file required for this HTTPS connection, specify the **CertificateStore** and the **CertificateStorePassword** properties. To attest the certificates in the Java keystore, add the trusted authority certificate using the **TrustedStore** and **TrustedStorePassword** properties.

Note: If a single keystore file contains all the certificates, then set the **CertificateStore** and **TrustedStore** properties to point to the same keystore file. Also, set the **CertificateStorePassword** and **TrustedStorePassword** properties with same value.

Resynchronizing alarms

The Probe for Alcatel-Lucent 5529 OAD resynchronizes with OAD by sending a SOAP/XML request. To specify that the probe performs a resynchronization, set the **Resync** property to `true`. The probe receives a list of all active alarms from the Alcatel-Lucent 5529 OAD system.

Note: You must also configure the **OS.Host** and **OS.Port** properties in the `alcatel_5529_oad_v6.props` file to have the same values as specified in the `$NCHOME/etc/omni.dat` file. You must also specify the **OS.UserName** and **OS.Password**. This ensures that the probe connects properly to the target ObjectServer.

To set the number of alarms that the probe can resynchronize in one connection, use the **AlarmsBatchSize** property. If the number of active alarms in the Alcatel-Lucent 5529 OAD system exceeds the specified value, the probe resynchronizes once again until it receives all the remaining alarms from the Alcatel-Lucent 5529 OAD system.

You can specify that some, or all, of the alarms are cleared following a resynchronization by using the **ResyncSQLCmd** property. Set this property to the SQL command that you want the ObjectServer to perform at the end of the resynchronization. If you do not specify a value for this property, no alarms will be cleared.

Performing partial resynchronization

You can perform a partial resynchronization by limiting which alarms are retrieved using the following filtering properties:

- **AcknowledgeFilter**: This property allows you to select alarms by their acknowledgement state.
- **PerceivedSeverityFilter**: This property allows you to select alarms by their perceived severity.
- **ProbableCauseFilter**: This property allows you to select alarms by their probable cause.
- **ScopeFilter**: This property allows you to select alarms by the device that generated them.

Java Message Service

Java Message Service (JMS) is a set of interfaces and associated semantics that define how the probe accesses the Alcatel-Lucent 5529 OAD system. The JMS topic is a JMS-managed object that distributes the messages between the probe and the Alcatel-Lucent 5529 OAD system.

Connecting to JMS

The Probe for Alcatel-Lucent 5529 OAD retrieves events by connecting directly to Java Messaging Service (JMS) as follows:

1. The probe connects to JMS running on the Alcatel-Lucent 5529 OAD server.
2. The JMS sends asynchronous events to the probe.
3. The probe parses these events and sends them to the ObjectServer.

JMS ports

All JMS ports described in this topic must be enabled on the firewall.

The JMS client application code needs to use JMS port 1099 (regular JNP port) and also the default RMI port bind address.

Subscribing to a JMS topic

On connection with the Alcatel-Lucent 5529 OAD system, the Probe for Alcatel-Lucent 5529 OAD uses the values specified by the **Username** and **Password** properties for authentication, and creates a topic connection.

Note: You can send only one command for each URL connection. After the creation of a topic connection, the Probe for Alcatel-Lucent 5529 OAD subscribes over the MTOSI interface to the topic specified by the **Topic** property.

After each subscription, if resynchronization is enabled, the Probe for Alcatel-Lucent 5529 OAD attempts to retrieve all current active alarms from the Alcatel-Lucent 5529 OAD system.

Using durable subscriptions

When the Probe for Alcatel-Lucent 5529 OAD is running in durable subscription mode, the JMS stores messages published on the specified topic while the subscriber is not active or disconnected from the JMS. The Probe for Alcatel-Lucent 5529 OAD creates a subscriber with durable subscription using the value specified by the **PersistentJmsId** property. When the probe reconnects with the same subscriber value, the JMS sends the stored events.

Disabling durable subscriptions

To disable the durable subscription mode, do not specify a value for the **PersistentJmsId** property; setting the value of the **CleanupPersistentJmsId** property to true makes the Probe for Alcatel-Lucent 5529 OAD unsubscribe from the JMS topic when shutting down.

Note: The probe removes the stored messages once the subscriber receives them, or when they expire, or when the durable subscription is deleted.

Java Messaging Service filter

The probe subscription filters events in a JMS topic using the filter specified by the **JmsFilter** property.

Inactivity

The Probe for Alcatel-Lucent 5529 OAD has a timeout facility that allows it to disconnect from the JMS topic if it fails to receive the next alarm data within a predefined amount of time. You can specify how long the probe waits before disconnecting, using the **Inactivity** property. After this length of time, the probe disconnects from the switch, sends a ProbeWatch message to the ObjectServer, and tries to reconnect. To disable probe reconnection, set the **Retry** property to false.

Command line interface

The Probe for Alcatel-Lucent 5529 OAD is supplied with a command line interface (CLI). This interface allows you to perform commands using the probe (for example, to acknowledge alarms or to request a full resynchronization of the JMS interface). To use the CLI, you must use the **CommandPort** property in the properties file to specify a port through which commands will be sent. When you want to perform commands, telnet to this port.

The following table describes the commands that you can use with the command line interface.

Table 4. CLI commands	
Command	**Description**
`acknowledge_alarm alarmid1 alarmid2 ... alarmidn`	This command allows you to send a request to the OAD server to acknowledge the list of alarms accompanying the command.
`get_active_alarms`	This command allows you to get all active alarms in the MTOSI interface.
`get_active_alarms_count`	This command displays the number of active alarms in the Alcatel-Lucent 5529 OAD system.

Table 4. CLI commands (continued)	
Command	**Description**
`help`	This command displays online help about the CLI.
`version`	This command displays the version of the probe.

Note: As the CLI is based upon telnet connections, you can connect to the Probe for Alcatel-Lucent 5529 OAD from anywhere. This means that simple scripts can be set up to allow users to acknowledge selected events from the Tivoli Netcool/OMNIbus event list by creating desktop tools to telnet to the Probe for Alcatel-Lucent 5529 OAD, send a command, and then close the connection.

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*).

Table 5. Properties and command line options		
Property name	**Command line option**	**Description**
AcknowledgeFilter *string*	`-acknowledgefilter` *string*	Use this property to specify which alarms the probe retrieves during resynchronization based on their acknowledgement state. This property takes the following values: • AI_EVENT_ACKNOWLEDGED • AI_EVENT_ UNACKNOWLEDGED • AI_NA The default is " " **Note:** If you want to retrieve alarms of more than one acknowledgement state, specify them as a comma-separated list. If you leave this property blank, the probe retrieves alarms of all acknowledgement states.
AlarmRetrievalMgr ExtURL *string*	`-alarmretrievalmgr exturl` *string*	Use this property to specify the path to the AlarmRetrievalMgrExt endpoint. The default is `oad/services/ AlarmRetrievalMgrExt`.
AlarmRetrievalMgrU RL *string*	`- alarmretrievalmgrur l` *string*	Use this property to specify the path to the AlarmRetrievalMgr endpoint. The default is `oad/services/ AlarmRetrievalMgr`.

Table 5. Properties and command line options (continued)

Property name	Command line option	Description
AlarmsBatchSize *integer*	-alarmsbatchsize *integer*	Use this property to specify the number of alarms that the probe can receive during each resynchronization. The default is 100.
AxSSSLSupport *string*	-axssslsupport *string* (This is equivalent to **AxSSSLSupport** with a value of true.) -noaxssslsupport id (This is equivalent to **AxSSSLSupport** with a value of false.)	Use this property to enable the setting of AxSSSLSupport parameters for SSL connections. This property takes the following values: false: The probe does not allow the setting of AxSSSLSupport parameters for SSL connections true: The probe allows the setting of AxSSSLSupport parameters for SSL connections The default is false.
CertificateStore *string*	-certificatestore *string*	Use this property to specify the path of the certificate store file. The default is " ".
CertificateStorePassword *string*	-certificatestorepassword *string*	Use this property to specify the password required to access the certificate store file. The default is " ". **Note:** Encrypt the password using nco_g_crypt.
CleanupPersistentJmsId *string*	-cleanuppersistentjmsid *string* (This is equivalent to **CleanupPersistentJmsId** with a value of true.) -nocleanuppersistentjmsid (This is equivalent to **CleanupPersistentJmsId** with a value of false.)	Use this property to specify whether the probe clears the durable JMS subscription of the subscribers before shutting down. This property takes the following values: false: The probe does not clear the durable JMS subscription. true: The probe clears the durable subscription of the JMS subscribers. The default is true.
CertificateStoreType *string*	-certificatestoretype *string*	Use this property to specify the certificate type obtained from the certificate store. The default is JKS.

Table 5. Properties and command line options (continued)		
Property name	**Command line option**	**Description**
ClusterURL *string*	`-clusterurl` *string*	Use this property to specify the IP address and port number of each OAD server in the cluster.
		You must specify this property value as a comma-separated list.
		For Alcatel-Lucent OAD 9.3 and earlier, each item in the list must be in the following format:
		ip_address:port_number
		Where:
		ip_address is the IP address of the server on which OAD is running.
		port_number is either 1099 or 1100.
		For Alcatel-Lucent OAD 9.4, each item in the list must be in the following format:
		`remote://`*ip_address:port_number*
		Where:
		ip_address is the IP address of the server on which OAD is running.
		port_number is 4447.
		The default is `" "`. The probe will get the JMS OAD server IP address from the HTTP OAD server.
		Note: If the probe is running on the same server as OAD, you can specify localhost instead of the IP address of the host computer.
		Note: This property is only specified when deploying Alcatel-Lucent 5529 OAD in a clustered environment
CommandPort *integer*	`-commandport` *integer*	Use this property to specify the port to which users can telnet to communicate with the probe using the command line interface (CLI) supplied with the probe.
		The default is 6970.
CommandPortLimit *integer*	`-commandportlimit` *integer*	Use this property to specify the maximum number of telnet connections that the probe allows.
		The default is 10.
DiscoveryGroup *string*	`-discoverygroup` *string*	Use this property to specify the IP address to which the probe sends the discovery query.
		The default is 230.0.0.4.

Property name	Command line option	Description
FlushBufferInterval *integer*	-flushbufferinterval *integer*	Use this property to specify the interval (in seconds) that the probe waits before flushing the buffer contents to the ObjectServer. The default is `0`
HttpHostPort *string*	-httphost *string*	Use this property to specify the name and port number of the host (or hosts) to which the probe connects. You can specify the details of multiple hosts in this property by using a comma-separated list. Each item in the list must be in the following format: *host:port_number* Where: *host* is an IPv4 address, an IPv6 address, or a host name. *port_number* is a port on the host to which the probe connects. The default is `localhost:8843`.
HttpTimeout *integer*	-httptimeout *integer*	Use this property to specify the time (in seconds) that the probe waits on a socket for a connection response, or on an input stream to receive data, before timing out. The default is 10.
Inactivity *integer*	-inactivity *integer*	Use this property to specify the time (in seconds) the probe allows between receiving JMS events before disconnecting from Alcatel-Lucent 5529 OAD. The default is 70.
InventoryRetrievalMgrExtnsURL *string*	-inventoryretrievalmgrextnsurl *string*	Use this property to specify the URL of the Web service to query for the singleton JMS server. The default value is `oad/services/InventoryRetrievalMgrExtns`

Table 5. Properties and command line options (continued)

Table 5. Properties and command line options (continued)		
Property name	**Command line option**	**Description**
JavaNamingFactoryInitial *string*	`-javanamingfactory initial` *string*	Use this property to configure the JNDI naming factory setting that enables the probe to subscribe for JMS notifications.
		For Alcatel-Lucent/Nokia OAD 9.3 and earlier, the default value for this property is `org.jboss.security.jndi.JndiLoginIni tialContextFactory`.
		For OAD 9.4 to 9.6, the default value for this property is `org.jboss.naming.remote.client.Initi alContextFactory`.
		For OAD 9.7 and later, the value for this property is `org.wildfly.naming.client.WildFlyIni tialContextFactory`.
JmsFilter *string*	`-jmsfilter` *string*	Use this property to specify the filter the probe uses to subscribe to events on the JMS.
		The default is `""`.

Table 5. Properties and command line options (continued)		
Property name	**Command line option**	**Description**
JndiConfigFile *string*	`-jndiconfigfile` *string*	Use this property to specify the path to the JNDI properties files for JMS connections.
		On UNIX and Linux platforms, the default is `$OMNIHOME/probes/<arch>/ alcatel_5529_oad_v6.jndi`.
		On Windows platforms, the default is `%OMNIHOME%\\probes\\win32\ \alcatel_5529_oad_v6.jndi`.
		Note: The property values for the JNDI properties file can be encrypted using `nco_aes_crypt` with a key that generated by `nco_keygen`.
		For details of `nco_aes_crypt`, see the following IBM Documentation page:
		https://www.ibm.com/support/ knowledgecenter/en/SSSHTQ_8.1.0/ com.ibm.netcool_OMNIbus.doc_8.1.0/ omnibus/wip/admin/reference/ omn_adm_ncoaescryptcmdlineopts.html
		For details of `nco_keygen`, see the following IBM Documentation page:
		https://www.ibm.com/support/ knowledgecenter/en/SSSHTQ_8.1.0/ com.ibm.netcool_OMNIbus.doc_8.1.0/ omnibus/wip/admin/task/ omn_adm_generatekeyinkeyfile.html
		If you use encryption, you must also set two additional properties: ConfigCryptoAlg and ConfigKeyFile in the probe properties file. For details of these properties, see the following page in IBM Documentation:
		https://www.ibm.com/support/knowledgecenter/ SSSHTQ_8.1.0/ com.ibm.netcool_OMNIbus.doc_8.1.0/ omnibus/wip/probegtwy/reference/ omn_prb_commonprobeprops.html
MaxSameSingleton RetryTime *integer*	`-maxsamesingleton retrytime` *integer*	Use this property to specify the time in minutes that the probe will retry connecting to the same singleton server after a disconnection.
		The default is 10.

Table 5. Properties and command line options (continued)		
Property name	**Command line option**	**Description**
Optimize *string*	-optimize (This is equivalent to **Optimize** with a value of true.) -nooptimize (This is equivalent to **Optimize** with a value of false.)	Use this property to specify whether the probe can run with optimized performance: false: The probe does not run with optimized performance. true: The probe runs with optimized performance. The default is true. **Note:** In optimized performance the probe reduces the number of messages logged into the log file.
OS.Host *string*	-oshost *string*	Use this property to specify the host name of the server where the probe's target ObjectServer is installed. This value must be the same as the value specified in $NCHOME/etc/omni.dat. This property is required to enable the resynchronization feature. The default is localhost.
OS.Password *string*	-ospassword *string*	Use this property to specify the password that the probe uses with the **OS.UserName** property to connect to the ObjectServer during resynchronization operations. This ensures that the resynchronization operation takes place on the same ObjectServer specified in the **Server** property in the alcatel_5529_oad_v6.props file. The default is " ". **Note:** You must specify the password encrypted by nco_g_crypt.
OS.Port *integer*	-osport *integer*	Use this property to specify the port number of the server where the target ObjectServer is installed. This value must be the same as the value specified in $NCHOME/etc/omni.dat. This property is required to enable the resynchronization feature. The default is 4100.
OS.UserName *string*	-osusername *string*	Use this property to specify the user name that the probe uses to connect to the ObjectServer during resynchronization operations. This ensures that the resynchronization operation takes place on the same ObjectServer specified in the **Server** property in the alcatel_5529_oad_v6.props file. The default is root.

Table 5. Properties and command line options (continued)		
Property name	**Command line option**	**Description**
PartitionName *string*	`-partitionname` *string*	Use this property to specify the cluster partition name to which the discovery query should be restricted. The default is `cluster-name`.
Password *string*	`-password` *string*	Use this property to specify the password that the probe uses to authenticate with Alcatel-Lucent 5529 OAD. The default is `""`. **Note:** Use the `nco_g_crypt` utility supplied with Netcool/OMNIbus to encrypt the password. See the *IBM Tivoli Netcool/OMNIbus Administration Guide* .
PerceivedSeverity Filter *string*	`-perceivedseverity filter` *string*	Use this property to specify which alarms the probe retrieves during resynchronization based on their perceived severity. This property takes the following values: • PROP_UPDATE • PS_CLEARED • PS_CRITICAL • PS_INDETERMINATE • PS_MAJOR • PS_MINOR • PS_WARNING The default is `""`. **Note:** If you want to retrieve alarms of more than one perceived severity, specify them as a comma-separated list. If you leave this property blank, the probe retrieves alarms of all perceived severities.
PersistentJmsId *string*	`-persistentjmsid` *string*	Use this property to specify the identifier of the durable subscriber in the JMS. The default is `alcatel_5529_oad_v6`.

Table 5. Properties and command line options (continued)		
Property name	**Command line option**	**Description**
ProbableCauseFilter *string*	`-probablecausefilter` *string*	Use this property to specify which alarms the probe retrieves during resynchronization based on their probable cause.
		Each value that you specify should be in the following format:
		`ru=`*boolean*`,contra=`*boolean*`,type=`*description*
		Where `ru` indicates whether the alarm detected is from a device on a remote network, `contra` indicates whether the alarm detected is related to the source atomic function, and *description* is a predefined MTOSI description of the probable cause.
		Make sure you separate each part of the definition with a comma and do not include spaces.
		The default is `""`.
		Note: If you want to retrieve alarms of more than one probable cause, specify them as a semicolon-separated list. If you leave this property blank, the probe retrieves alarms of all probable causes.
Resync *string*	`-noresync` (This is equivalent to **Resync** with a value of `false`.) `-resync` (This is equivalent to **Resync** with a value of `true`.)	Use this property to specify whether the probe requests all active alarms from the server before acquiring new alarms during startup. This property takes the following values:
		`false`: The probe does not perform resynchronization during startup.
		`true`: The probe performs resynchronization during startup.
		The default is `true`.
		Note: For details about how to specify whether the probe performs a full resynchronization or a partial resynchronization, see "Resynchronizing alarms" on page 16.
		Note: This property does not stop resynchronization requests through the probe **CommandPort** facility.

Table 5. Properties and command line options (continued)		
Property name	**Command line option**	**Description**
ResyncRetryInterval *integer*	-resyncretryinterval *integer*	Use this property to specify the interval (in minutes) that the probe waits between successive attempts to retry the resynchronization operation. You can specify values between 0 and 30. The default value is 3. If you set this property to 0, the probe will make no attempts to retry the resynchronization operation. If you set this property to a value greater than 0, the probe will only retry a resynchronization operation if the previous resynchronization contained exceptions. When the resynchronization operation completes successfully without exceptions, the probe will make no further resynchronization attempts.
ResyncSQLCmd *string*	-resyncsqlcmd *string*	Use this property to specify the SQL command used to clear alarms from the ObjectServer after a resynchronization. If you leave this property blank, the resynchronization will proceed, but no alarms will be cleared. The default is `delete from alerts.status where Manager='Alcatel 5529 OAD V6 probe' and (InternalLast < RESTART_TIMESTAMP).`
Retry *string*	-noretry (This is equivalent to **Retry** with a value of `false`.) -retry (This is equivalent to **Retry** with a value of `true`.)	Use this property to specify whether the probe attempts to reconnect to the 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 `true`.
RetryWait *integer*	-retrywait *integer*	Use this property to specify the waiting time in seconds between retry connection with the singleton server. The default value is 10. **Note:** The maximum value for this property is 15.

Property name	Command line option	Description
ScopeFilter *string*	-scopefilter *string*	Use this property to specify which alarms the probe retrieves during resynchronization based on their device type. Each value that you specify should be in the following format: mdNm=*manufacturer*,meNm=*device* Where *manufacturer* is the name of the manufacturer of the device from which the alarms originated and *device* is the name of the device itself. Make sure you separate each part of the definition with a comma and do not include spaces. The default is " ". **Note:** If you want to retrieve alarms of more than one device type, specify them as a semicolon-separated list. If you leave this property blank, the probe retrieves alarms of all device types.
SingletonServerPort *integer*	-singletonserverport *integer*	Use this property to specify the port number on the singleton server to which the probe connects. For Alcatel-Lucent OAD 9.3 and earlier, the default value for this property is 1099 or below. For Alcatel-Lucent OAD 9.4, the default value for this property is 4447.
Topic *string*	-topic *string*	Use this property to specify the JMS topic to which the probe subscribes. The default is topic/Fault.
TrustStore *string*	-truststore *string*	Use this property to specify the file path of the truststore file. The default is " ".
TrustStorePassword *string*	-truststorepassword *string*	Use this property to specify the password required to access the truststore file containing the trusted certificates. The default is " ".
TrustStoreType *string*	-truststoretype *string*	Use this property to specify the type of truststore specified by **TrustStore** property. The default value is JKS.

Table 5. Properties and command line options (continued)

Table 5. Properties and command line options (continued)

Property name	Command line option	Description
UseSsl *string*	-nossl (This is equivalent to **UseSsl** with a value of false.) -usessl (This is equivalent to **UseSsl** with a value of true.)	Use this property to enable SSL authentication when connecting to Alcatel-Lucent 5529 OAD. This property takes the following values: false: SSL is not used when connecting to the system. true: SSL is used when connecting to the system. The default is true. **Note:** If **UseSsl** is set to true, the **HttpPort** must be configured to use the Alcatel-Lucent OAD HTTPS port. The default Alcatel-Lucent OAD HTTPS port is 8443. You must also configure the following properties for the Probe for the Alcatel-Lucent 5529 OAD: • **CertificateStore** • **CertificateStorePassword** • **TrustStore** • **TrustStorePassword**
Username *string*	-username *string*	Use this property to specify the user name with which the probe logs onto Alcatel-Lucent 5529 OAD. The default is " ".
XmlFileDebug *string*	-xmlfiledebug *string*	Use this property to specify the XML file that the probe replays. The default is " ". **Note:** This file is used for debugging purposes only.

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 for Alcatel-Lucent 5529 OAD generates. Not all the elements described are generated for each event; the elements that the probe generates depends upon the event type.

Table 6. Elements

Element name	Element description
$acknowledgeIndication	This element indicates the status of the acknowledgement.

Table 6. Elements (continued)

Element name	Element description
$activeAlarmCount	This element contains the number of active alarms in the Alcatel-Lucent 5529 OAD system.
$activityName	This element indicates the name of the activity.
$activityStatus	This element indicates the status of the activity.
$AdditionalText	This element displays additional information about the alarm.
$AffectedTPList0_*Object Name*	This element displays a list of termination points affected for the Object specified.
$aliasName_0…n $aliasValue_0…n	This element displays a list of the aliases used to describe the network entity as per the user interface of the operating system.
$batchSequenceEndOfReply	This element indicates whether there are any more alarms to be resynchronized.
$batchSequenceNumber	This element displays the sequence number of batches received.
$clearedTimeStamp	This element displays the time at which the alarm was cleared.
$commpressionType	This element displays the type of compression used for the event.
$communicationStyle	This element displays the inter component communication style.
$correlatedNotifications0..n_ *Object Name*	This element displays the notification identifier with its optional object name.
$correlationId	This element displays the correlation identifier for CLEAR traps received.
$destinationURI	This element displays the URI of the event destination.
$endTime	This element displays the time an event loss was cleared.
$failureReplytoURI	This element displays the URI of the system that is expecting the failure reply response to this event.
$fileLocationURI	This element indicates the location of the schema file.
$isClearable	This element indicates if the event is clearable (or is itself a clear).

Element name	Element description
$iteratorReferenceURI	This element displays the URI to the iterator.
$lastAcknowledgedTimeStamp	This element displays the time at which the alarm was last acknowledged.
$lastModificationTimeStamp	This element displays the time at which the alarm was last modified.
$layerRate	This element displays the layer to which the event is related.
$msgType	This element displays the message associated with the event.
$msgName	This element displays the name of the message template.
$nativeProbableCause	This element indicates the probable cause of the event as defined in the user interface of the operating system.
$neTime	This element displays the time of the alarm as provided by the network element.
$notificationId	This element displays the identifier of the notification.
$objectName_*Object Name*	This element displays the event information on the specified object.
$ObjectType	This element displays the type of object.
$osNM	This element displays the full distinguished name of the object reporting the notification.
$OsTime	This element displays the time when the operating system reported the event.
$PackingType	This element displays the packing type of the source.
$PerceivedSeverity	This element displays the severity of the alarm.
$Priority	This element displays the priority as defined by the Alcatel-Lucent 5529 OAD system.
$probableCause_contra	This element relates to the probable cause of the event, indicating the direction of the signal related to the event.
$probableCause_ru	This element relates to the probable cause of the event, indicating the location of the network resource.
$probableCause_type	This element relates to the probable cause of the event, indicating the type code of the probable cause.

Table 6. Elements (continued)

Table 6. Elements (continued)

Element name	Element description
`$rcaiIndicator`	This element indicates whether the alarm is a root cause alarm or a raw alarm.
`$replyToURI`	This element displays the URI of the system that is expecting a response to this message.
`$requestedBatchSize`	This element displays the number of alarms that the probe expects as a batch from the Alcatel-Lucent 5529 OAD system.
`$security`	This element indicates the security status of the event.
`$securityType`	This element indicates the mode of security used when connecting to the network element.
`$senderURI`	This element contains the URI of the message sender.
`$serviceAffecting`	This element indicates if the alarm has affected service.
`$specificProblem_0…n`	This element identifies the specific cause within the Probable cause of the alarm.
`$startTime`	This element displays the time an event loss occurred.
`$timestamp`	This element displays the time when the event has occurred.
`$type`	This element identifies the specific value within the Probable cause of the alarm.
`$x733_BackupObject_`*`Object Name`*	This element indicates whether the object emitting the alarm has been backed-up.

`$X733_EventType`	This element displays the type of the alarm as per ITU-T X.733:
	
	`communicationsAlarm`
	
	`environmentalAlarm`
	
	`equipmentAlarm`
	
	`processingErrorAlarm`
	
	`qualityofServiceAlarm`

`$x733_TrendIndication`	This element indicates the current severity trend of the object.

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*.

Table 7. Error messages		
Error	**Description**	**Action**
Cannot execute *command* as the connection object is being used by other process. Where *command* can be getActiveAlarms, getActiveAlarmsCount, or acknowledgeAlarms.	Either a command was sent to the probe while the probe was performing an alarm resynchronization, or the probe is attempting to retry a resynchronization operation but a resynchronization operation (initiated through the CommandPort) is already active.	Wait until the probe has stopped its resynchronization operation before issuing commands to the probe through the CommandPort.
Cannot re-open the connection, giving up	The probe could not make the HTTP connection with the Alcatel-Lucent 5529 OAD system during alarm resynchronization iterations.	Check the connection between the system on which the probe is running and the Alcatel-Lucent 5529 OAD system.
The command didn't succeed, due to authentication pbs Make sure your 'Username' and 'Password' properties values are correct Failed to retrieve *Username* property value : *value* Failed to set the Authenticator object	The probe could not make the HTTP connection with the Alcatel-Lucent 5529 OAD system.	Check that the values set for the **UserName** and **Password** properties are correct.
Error while setting following field in the event : *field_name* :*value* Error while trying to create and initialize a new NSProbeEvent Error while sending event to the OS	The probe could not assign the value for the specified field.	Check the connection between the system on which the probe is running and the Alcatel-Lucent 5529 OAD system.

Table 7. Error messages (continued)		
Error	**Description**	**Action**
At least one of the certificate properties is empty It's unlikely SSL will be set-up correctly	The probe could not find the required information for SSL connection.	Check that the **CertificateStore**, **CertificateStorePassword**, **TrustStore**, **TrustStorePassword** properties are set to the correct values. If there is only one keystore containing all certificates, ensure both the **CertificateStore** and **TrustStore** properties are set to the same Keystore.
Password is incorrect length (ensure it has been encrypted using nco_g_crypt)	The probe found that the password entered did not adhere to the security standards.	Check the value entered for the **Password** property has been encrypted by nco_g_crypt.

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 ProbeWatch messages, see the *IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide*.

Table 8. ProbeWatch messages		
ProbeWatch message	**Description**	**Triggers/causes**
START SYNCHRONIZATION	This indicates that resynchronization has started. The probe issues a getActiveAlarms request to retrieve active alarms from the Alcatel-Lucent 5529 OAD system.	The probe has reconnected to a JMS server and the **Resync** property is set to true.
No Events received for *inactivity* seconds	The probe did not receive events for the specified period.	The probe has exceeded the time out period already set.
SYNCHRONIZATION FAILED	The probe failed to obtain active alarms from the remote server.	The remote server may be unavailable because of a network outage. Check the log files for more information.
END SYNCHRONIZATION	The probe retrieved all current active alarms from the Alcatel-Lucent 5529 OAD system.	The probe has completed resynchronization with the Alcatel-Lucent 5529 OAD system.

Known issue

Probe not able to parse some long events correctly

The probe may not be able to parse certain long events correctly and so will write an exception to the log file.

The following example illustrates one such exception :

```
Exception while parsing : org.xml.sax.SAXParseException: Element type
"alu:packagealu" must be followed by either attribute specifications, ">" or
"/>".
```

In this case, the space between `alu:package` and `alu` was trimmed which caused the exception to occur.

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 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
Software Interoperability Coordinator, Department 49XA

37

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.

IBM ®