IBM® Tivoli® Netcool/OMNIbus Probe for Cisco Transport Manager 9.0 (CORBA) 1.0

Reference Guide
March 7, 2014

IBM

Note

Before using this information and the product it supports, read the information in Appendix A, "Notices and Trademarks," on page 17.

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 Cisco Transport Manager 9.0 (CORBA) documentation is provided in softcopy format only. To obtain the most recent version, visit the IBM® Tivoli® Knowledge Center:

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

Table 1. Document modification history		
Document version	**Publication date**	**Comments**
SC27-6263-00	March 7, 2014	First IBM publication.

Note : The Probe for Cisco Transport Manager 9.0 (CORBA) was previously documented in the same reference guide as the Probe for Cisco Transport Manager (CORBA). This reference guide documents the Probe for Cisco Transport Manager 9.0 (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 *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 Cisco Transport Manager 9.0 (CORBA)

Cisco Transport Manager (CTM) is an element management system (EMS) for optical networks. It integrates with operations support systems (OSS) using standard protocols.

The Probe for Cisco Transport Manager 9.0 (CORBA) acquires data from Cisco Transport Manager using a Common Object Request Broker Architecture (CORBA) interface.

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 Cisco Transport Manager 9.0 (CORBA).

Table 3. Summary	
Probe target	Cisco Transport Manager version 9.0 CORBA Interface
Probe executable name	`nco_p_cisco_ctm_corba_v9`
Probe installation package	`omnibus-`*`arch`*`-probe-nco-p-cisco-ctm-corba-v9-`*`version`*
Package version	2.0
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=swg21665213
Properties file	`$OMNIHOME/probes/`*`arch`*`/cisco_ctm_corba_v9.props`
Rules file	`$OMNIHOME/probes/`*`arch`*`/cisco_ctm_corba_v9.rules`

Table 3. Summary (continued)	
Requirements	For details of any additional software that this probe requires, refer to the `description.txt` file that is supplied in its download package.
Connection method	CORBA
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 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*.

Setting environment variables

Environment variables are specific preset values that establish the probe's working environment.

After installing the probe, you must include the following directory path as the first entry in the $PATH environment variable:

```
jre_directory/bin
```

where *jre_directory* is the location of your Java Runtime Environment (JRE) files.

Configuring the lookup table

The probe is supplied with a lookup table that contains details of the Managed Element objects that Cisco Transport Manager generates. You might need to update the rules file to include the path to the lookup table.

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

```
$OMNIHOME/probes/includes/
```

The following include command in the rules file assumes that the probe is run from the standard `$OMNIHOME/probes/` directory:

```
table nelookup = "../includes/ManElement.lookup"
```

If you are running the probe from a different directory, change the entry in the rules file to the following path:

```
table nelookup = "/opt/Omnibus/probes/includes/ManElement.lookup"
```

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.

Data acquisition

The probe gathers events from Cisco Transport Manager using a CORBA interface.

Data acquisition is described in the following topics:

- "Connecting to the CORBA interface" on page 4
- "Retrieving alarms" on page 4
- "Status checking" on page 4
- "Timeout" on page 5
- "Backoff strategy" on page 5
- "Command line interface" on page 5
- "Peer-to-peer failover functionality" on page 5
- "Running multiple probes" on page 6

Connecting to the CORBA interface

The probe connects to Cisco Transport Manager using either an Interoperable Object Reference (IOR) file or a Naming Service.

Using IOR files

When using IOR files, the probe gets the object reference of the `EmsSessionFactory_I` object from the IOR file specified by the **`IORFile`** property.

Using a Naming Service

If a value is not specified for the **`IORFile`** property, the probe gets the object reference of the `EmsSessionFactory_I` object from a Naming Service. The probe locates the Naming Service using either the IBM Object Request Broker (ORB) properties or the Naming Context IOR file properties.

You can specify the Naming Service host and port using the **`ORBInitialHost`** and **`ORBInitialPort`** properties.

You can specify the Naming Context IOR file and the location of the `EmsSessionFactory_I` object using the **`NamingContextIORFile`** and **`NamingContextPath`** properties.

Retrieving alarms

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

The probe then connects to the notification service 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 alarms generated after it connects to Cisco Transport Manager.

You can use the **`ResynchBatchSize`** property to specify the maximum number of alarms that the probe retrieves with each resynchronization. The default is 100.

Status checking

The probe checks that the Cisco Transport Manager server is running by sending a ping command every 60 seconds. You can change the frequency of this test using the **`AgentHeartbeat`** property.

Timeout

The probe has a timeout facility that allows it to disconnect from the system if there has been no activity for a predefined amount of time.

You can use the **Timeout** property to specify how long the probe waits for a new alarm before disconnecting from Cisco Transport Manager. If you set the **Timeout** property to 0, the probe never disconnects from the target.

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, it reverts to a backoff strategy.

The probe will try to reestablish a connection after one second, two seconds, then four seconds, and so on, up to a maximum of 4096 seconds. Once the connection is made to the CORBA interface, the probe tries to log in to the device. If the probe fails to log in, it shuts down and tries to connect again. The backoff strategy remains in place until a successful login occurs.

Command line interface

The probe is supplied with a command line interface (CLI). This interface allows you to execute commands using the probe.

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

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

Table 4. CLI commands	
Command	**Description**
help	This command displays online help about the CLI.
nelookup	This command instructs the probe to build the managed element lookup table.
resynch_all	This command allows you to perform a full resynchronization with Cisco Transport Manager.
version	This command displays the version of the probe.

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 5. Properties and command line options

Property name	Command line option	Description
AgentHeartBeat *integer*	`-agentheartbeat` *integer*	Use this property to specify the frequency (in seconds) with which the probe sends a ping command to check that CTM is still running. The default is 60.
CommandPort *integer*	`-commandport` *integer*	Use this property to specify the port through which users can use Telnet to communicate with CTM using the CLI supplied with the probe. The default is 6970. For more information about the CLI, see "Command line interface" on page 5.
CommandPortLimit *integer*	`-commandportlimit` *integer*	Use this property to specify the maximum number of Telnet connections that can be made to the probe. The default is 10.
EncodingStandard *string*	`-encodingstandard` *string*	Use this property to specify the standard used to encode and decode multibyte characters. The default is ISO-8859-1.
ExcludeSeverityCleared *string*	`-excludeseveritycleared` *string*	Use this property to specify whether or not the probe excludes alarms of severity Cleared from those that it retrieves. This property takes the following values: false: The probe does not exclude alarms of severity Cleared. true: The probe excludes alarms of severity Cleared. The default is false.
ExcludeSeverityCritical *string*	`-excludeseveritycritical` *string*	Use this property to specify whether or not the probe excludes alarms of severity Critical from those that it retrieves. This property takes the following values: false: The probe does not exclude alarms of severity Critical. true: The probe excludes alarms of severity Critical. The default is false.

Table 5. Properties and command line options (continued)		
Property name	**Command line option**	**Description**
ExcludeSeverity Indeterminate *string*	`-excludeseverity indeterminate` *string*	Use this property to specify whether or not the probe excludes alarms of severity `Indeterminate` from those that it retrieves. This property takes the following values: `false`: The probe does not exclude alarms of severity `Indeterminate`. `true`: The probe excludes alarms of severity `Indeterminate`. The default is `false`.
ExcludeSeverityMajor *string*	`-excludeseveritymajor` *string*	Use this property to specify whether or not the probe excludes alarms of severity `Major` from those that it retrieves. This property takes the following values: `false`: The probe does not exclude alarms of severity `Major`. true: The probe excludes alarms of severity `Major`. The default is `false`.
ExcludeSeverityMinor *string*	`-excludeseverityminor` *string*	Use this property to specify whether or not the probe excludes alarms of severity `Minor` from those that it retrieves. This property takes the following values: `false`: The probe does not exclude alarms of severity `Minor`. `true`: The probe excludes alarms of severity `Minor`. The default is `false`.
ExcludeSeverityWarning *string*	`-excludeseveritywarning` *string*	Use this property to specify whether or not the probe excludes alarms of severity `Warning` from those that it retrieves. This property takes the following values: `false`: The probe does not exclude alarms of severity `Warning`. `true`: The probe excludes alarms of severity `Warning`. The default is `false`.

Table 5. Properties and command line options (continued)		
Property name	**Command line option**	**Description**
FlushBufferInterval *integer*	`-flushbufferinterval` *integer*	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).
GetPublicKey *string*	`-getpublickey` *string*	Use this property to specify whether or not the probe retrieves the latest public encryption key from the CTM server. This property takes the following values: 0: The probe does not retrieve a public key. 1: The probe retrieves a public key. The default is 0. **Note :** The public key is a string that the probe uses to encrypt the user name and password required to connect to CTM.
IORFile *string*	`-iorfile` *string*	Use this property to specify the location of the IOR file. The default is " ".
NamingContextIORFile *string*	`-nsior` *string*	Use this property to specify the location of the IOR file that contains the root context of the Naming Service. The default is " ".
NamingContextPath *string*	`-nspath` *string*	Use this property to specify the location of the `EmsSessionFactory_I` interface object within the Naming Service. The default is " ".

Table 5. Properties and command line options (continued)

Property name	Command line option	Description
NELookup *integer*	`-nelookup` *integer*	Use this property to specify whether or not the probe builds the managed element lookup table at startup. This property takes the following values: 0: The probe does not build the lookup table at startup. 1: The probe builds the lookup table at startup. The default is 0. **Note :** You can use the CLI to instruct the probe to build the lookup file when the probe is already running. For more information, see "Command line interface" on page 5.
NELookupLocation *string*	`-nelookuplocation` *string*	Use this property to specify the location of the lookup table that the probe builds at startup (if the **NELookup** property is set to 1). The default is `$OMNIHOME/probes/ includes/ ManElement.lookup`.
NEBatchSize *integer*	`-nebatchsize` *integer*	Use this property to specify the maximum size of the array that the probe receives when performing a lookup on all managed element objects. The default is 100.
ORBInitialHost *string*	`-orbinitialhost` *string*	Use this property to specify the name of the Naming Service host. The default is `" "`.
ORBInitialPort *integer*	`-orbinitialport` *integer*	Use this property to specify the port number through which to connect to the Naming Service host. The default is 1570.

ORBCharEncoding *string*	`-orbcharencoding` *string*	Use this property to specify the native character encoding set that the Object Request Broker (ORB) uses for character data. Possible values for this property are:
		
		    ISO8859_1
		    UTF8
		
		The default is: UTF8.

Property name	Command line option	Description
ORBLocalHost *string*	`-orblocalhost` *string*	Use this property to specify the local host used by the server-side ORB to place the server's host name or IP address into the IOR of a remote object. The default is: `" "`.
ORBLocalPort *integer*	`-orblocalport` *integer*	Use this property to specify the local port that the ORB listens on for connections from the probe. The default is: `0` (the ORB selects a port at random).

ORBWCharDefault *string*	`-orbwchardefault` *string*	Use this property to specify the wide character (wchar) set that the IBM ORB uses when communicating with other ORBs that do not publish a wchar set. Possible values for this property are:
		
		   UCS2
		   UTF16
		
		The default is: UTF16.

Password *string*	`-password` *string*	Use this property to specify the password used to log in to CTM. The default is `" "`.
ReactOnStateChange *integer*	`-reactonstatechange` *integer*	Use this property to specify whether or not the probe reacts when a `StateChange` alarm is received. This property takes the following values: 1: The probe renews the NE lookup file and performs a resynchronization. 0: The probe does not react. The default is 0.
Resynch *string*	`-noresynch` (This is equivalent to **Resynch** with a value of `false`.) `-resynch` (This is equivalent to **Resynch** with a value of `true`.)	Use this property to specify whether or not the probe requests all active alarms from CTM before acquiring new alarms. This property takes the following values: `false`: The probe does not perform resynchronization. `true`: The probe performs resynchronization. The default is `false`.

Table 5. Properties and command line options (continued)

Table 5. Properties and command line options (continued)

Property name	Command line option	Description
ResynchBatchSize *integer*	`-resynchbatchsize` *integer*	Use this property to specify the maximum number of alarms that the probe retrieves in each batch of resynchronization alarms. The default is `100`.
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 or not the probe attempts to reconnect to CTM following a connection error. This property takes the following values: `false`: The probe shuts down and does not attempt to reconnect. `true`: The probe attempts to reconnect to the system using a backoff strategy. The default is `false`. For more information about the probe's backoff strategy, see "Backoff strategy" on page 5.
Timeout *integer*	`-timeout` *integer*	Use this property to specify the time (in seconds) that the probe waits to receive a new alarm before disconnecting from CTM and shutting down. The default is `0` (the probe never disconnects).
Username *string*	`-username` *string*	Use this property to specify the user name used to log in to CTM. The default is `" "`.

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 6. Elements

Element name	Element description
`$additionalInfo`	This element provides additional information about the alarm.
`$additionalText`	This element contains a brief description of the problem being reported by the alarm.

Table 6. Elements (continued)	
Element name	**Element description**
`$affectedTPList`	This element indicates whether the list of termination points affected by the problem is reported by the alarm.
`$domain_name`	This element shows the domain where the event occurred.
`$emsTime`	This element displays the time at which the alarm was reported by CTM.
`$event_type`	This element indicates the type of the alarm. Possible values are: • `communicationsAlarm` • `environmentalAlarm` • `equipmentAlarm` • `processingErrorAlarm` • `qualityofServiceAlarm`
`$event_name`	This element shows the name of the event.
`$isClearable`	This element indicates whether or not the alarm can be cleared. Possible values are: • true • false
`$layerRate`	This element identifies the layer to which the alarm applies.
`$nativeEMSName`	This element shows the name of the object reporting the alarm as given in the CTM user interface.
`$nativeProbableCause`	This element indicates the probable cause as given in the CTM user interface.
`$neTime`	This element shows the time at which the error occurred in the network element.
`$notificationId`	This element contains the unique identifier of the alarm. This is derived from the serial number of the alarm as used by CTM.
`$objectName`	This element shows the name of the object reporting the alarm.
`$objectType`	This element shows the type of object reporting the alarm.
`$perceivedSeverity`	This element indicates the perceived severity of the alarm.

Table 6. Elements *(continued)*	
Element name	**Element description**
`$probableCause`	This element identifies the probable cause of the alarm.
`$probableCauseQualifier`	This element contains the qualifier used to classify the alarm type.
`$serviceAffecting`	This element indicates whether or not the alarm has affected the service.

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 7. Error messages		
Error	**Description**	**Action**

`Failed to connect to Naming Service`
 	
`The CORBA service is not running on the expected Host/Port/IOR`
	The probe failed to connect to the Naming Service. Either the Naming Service is not running on the specified host and port, or the IOR specified for the Naming Service is not correct.	Check that the Naming Service is running on the specified host and port and that the Naming Context IOR is correct.

`Failed to get interface version information`
 	
`Failed to ping Cisco server`
	The probe failed to call a method on CTM.	Check that CTM is running correctly and that the IOR files are up to date.

`Failed to get object reference from IOR file`
 	
`Failed to get object from IOR file`
 	
`Failed to find file, please check file exists!`
 	
`Failed to convert IOR to object`
 	
`Please check that the interface is running and the probe is using up to date IOR files`
	The probe failed to get the object reference from the IOR file. Either the requested IOR file was not found or it did not contain a valid IOR file.	Check that the IOR file exists and that it is a valid IOR file.

Table 7. Error messages (continued)		
Error	**Description**	**Action**

`Failed to narrow object reference`
 	
`Failed to narrow manager reference`
	The probe failed to narrow the object reference to the interface object.	This is a CORBA-related error and indicates a problem with the CORBA installation.

`Failed to resolve Naming Context`
 	
`Exception raised when locating server`
	The probe failed to resolve the Naming Context path to find the server object. Either the Naming Context path is invalid or it does not exist.	Check the **NamingContext Path** property.

`Name is null, cannot create element`
 	
`Cannot parse typevalue_type : name`
 	
`Failed to parse alarm`
	The probe failed to parse the alarm.	Check that the alarm conforms to the `StructuredEvent` format.

Troubleshooting

Various issues arise as users work with the probe. Troubleshooting information is provided to help you diagnose and resolve such issues.

Time token formats

When the time zone that the probe or Cisco Transport Manager is operating in changes, the probe might deliver alerts to the ObjectServer with an unknown or incorrect time format.

As a workaround, you can update the `datetotime` function in the rules file to convert the time tokens generated by the probe to UNIX time.

The following code example shows how to convert the time token $neTime (the time at which an error occurred in a network element) to UNIX time:

```
$UNIXDateTime = datetotime($neTime, "%Y%m%d%H%M%S")

@FirstOccurrence = $UNIXDateTime
@LastOccurrence = $UNIXDateTime
```

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

17

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.

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

IBM ®