NetIQ® AppManager® Connector for IBM Tivoli Netcool/OMNIbus

Management Guide

March 2019

Legal Notice

Contents

About this Book and the Library

The NetIQ AppManager product (AppManager) is a comprehensive solution for managing, diagnosing, and analyzing performance, availability, and health for a broad spectrum of operating environments, applications, services, and server hardware.

AppManager provides system administrators with a central, easy-to-use console to view critical server and application resources across the enterprise. With AppManager, administrative staff can monitor computer and application resources, check for potential problems, initiate responsive actions, automate routine tasks, and gather performance data for real-time and historical reporting and analysis.

Intended Audience

This guide provides information for individuals responsible for installing an AppManager module and monitoring specific applications with AppManager.

Other Information in the Library

The library provides the following information resources:

Installation Guide for AppManager

Provides complete information about AppManager pre-installation requirements and step-by-step installation procedures for all AppManager components.

User Guide for AppManager Control Center

Provides complete information about managing groups of computers, including running jobs, responding to events, creating reports, and working with Control Center. A separate guide is available for the AppManager Operator Console.

Administrator Guide for AppManager

Provides information about maintaining an AppManager management site, managing security, using scripts to handle AppManager tasks, and leveraging advanced configuration options.

Upgrade and Migration Guide for AppManager

Provides complete information about how to upgrade from a previous version of AppManager.

Management guides

Provide information about installing and monitoring specific applications with AppManager.

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

The NetIQ AppManager library is available in Adobe Acrobat (PDF) format from the NetIQ Web site: www.netiq.com/support/am/extended/documentation/default.asp?version=AMDocumentation.

Conventions

The library uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

Convention	Use
Bold	◆ Window and menu items ◆ Technical terms, when introduced
Italics	◆ Book and CD-ROM titles ◆ Variable names and values ◆ Emphasized words
`Fixed Font`	◆ File and folder names ◆ Commands and code examples ◆ Text you must type ◆ Text (output) displayed in the command-line interface
Brackets, such as *[value*]	◆ Optional parameters of a command
Braces, such as {*value}*	◆ Required parameters of a command
Logical OR, such as *value1*|*value2*	◆ Exclusive parameters. Choose one parameter.

About NetIQ Corporation

NetIQ, an Attachmate business, is a global leader in systems and security management. With more than 12,000 customers in over 60 countries, NetIQ solutions maximize technology investments and enable IT process improvements to achieve measurable cost savings. The company's portfolio includes award-winning management products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications Management. For more information, please visit www.netiq.com.

Contacting Sales Support

For questions about products, pricing, and capabilities, please contact your local partner. If you cannot contact your partner, please contact our Sales Support team

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, please contact our Technical Support team.

Worldwide:	www.netiq.com/Support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, please visit http://community.netiq.com.

1 Introducing AppManager Connector for Netcool

This chapter provides an overview of the AppManager Connector for Netcool (the connector) and its functionality

Understanding the Connector

The connector formats an AppManager event into a Netcool alert.

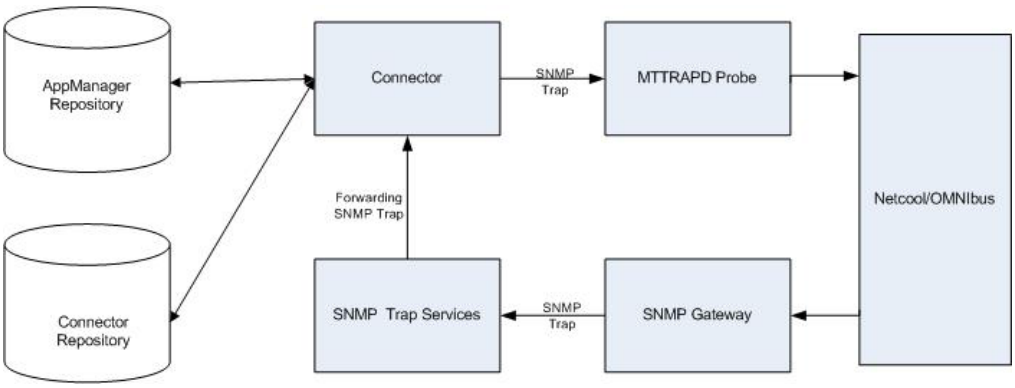
An event is a notification that a condition or activity you are monitoring with NetIQ AppManager has occurred on a managed client.

The connector runs as a Windows service. It automatically formats, filters, forwards the NetIQ AppManager events to the Netcool Multi-Threaded TRAPD (MTTRAPD) probe, and receives SNMP traps from Netcool. The alerts are displayed in the Netcool Event List.

SNMP Gateway is required to perform bi-directional activities. The SNMP Gateway sends Netcool alerts to the connector in the form of traps. The SNMP Trap Services forwards the traps to the connector.

The connector database, `AMNC`, stores information about events based on severity, status, and category.

The following figure illustrates the connector architecture:



AppManager stores events in the AppManager repository. The connector stores forwarded AppManager events in the connector database.

The components in the architecture diagram are defined in the following list:

- **AppManager Repository:** Stores AppManager events. You can install the AppManager repository on the same computer where the connector is installed or on a separate computer.

- **Connector Database:** Stores information about events based on severity, status, and category. You can install the connector database on the same computer where the connector is installed or on a separate computer.
- **Connector:** Formats, filters, forwards the NetIQ AppManager events to the Netcool Multi-Threaded TRAPD (MTTRAPD) probe, and receives SNMP traps from Netcool. You can install the connector on a standalone Windows computer that is networked to access Netcool or on the same computer where Netcool is installed.
- **MTTRAPD Probe:** Receives SNMP traps from the connector. For more information, see "MTTRAPD Rules" on page 18.
- **SNMP Gateway:** Performs bi-directional activities and facilitates communication between Netcool and AppManager. Sends Netcool alerts to the connector in the form of traps. For more information, see "SNMP Gateway" on page 15.
- **SNMP Trap Services:** Receives traps and forwards them to the connector. This service is included with the Windows operating system.

Forwarding AppManager Events to Netcool

When an AppManager Knowledge Script job running on a managed client raises an event, the AppManager agent sends the event information to the management server. The management server then places the event in the AppManager repository.

The connector polls the AppManager repository at regular intervals for new events. When it finds an event that meets the category and severity criteria, the connector sends the event to the Netcool MTTRAPD probe on the ObjectServer computer. ObjectServers store and manage alert information. You can use the Netcool Event List that is present in the `Netcool Suite` program folder to view the events forwarded by the connector.

The first time an event is forwarded to Netcool, its count is displayed as one irrespective of the number of times the event has actually occurred. However, during the subsequent forwards, the correct count of the event is displayed.

Use the connector Configuration Utility to specify configuration options for Netcool. For more information about setting the AppManager repository polling interval, see "Configuring AppManager Event Settings" on page 31.

By default, the AppManager event updates are synchronized from AppManager to Netcool. However, the event updates are not visible in Netcool unless you configure the deduplication and deduplicate_details triggers.

Review the following sections:

- "Configuring the Deduplication Trigger" on page 10
- "Configuring the Deduplicate_details Trigger" on page 11

Configuring the Deduplication Trigger

For the event updates to be visible in Netcool version 7.2.0 / 7.2.1 / 7.3.0 / 7.3.1, you must replace the default deduplication trigger.

To replace the default deduplication trigger:

1. Start **Administrator** in the Netcool Suite program folder.
2. In **NETCOOL/OMNIbus Administrator**, expand **Reports**.

3. Click **ObjectServer**s.
4. Double-click the ObjectServer that handles AppManager events.
5. In the ObjectServer Security dialog box, specify the credentials and click **OK**.
6. Expand **Automation** and click **Triggers**.
7. Double-click the **deduplication** trigger.
8. In the Edit Database Trigger dialog box, click the **Actions** tab.
9. Replace the existing SQL statement with the following:

```
begin
        if(%user.app_name = 'PROBE')
        then
            if((old.LastOccurrence > new.LastOccurrence) or
((old.ProbeSubSecondId >= new.ProbeSubSecondId) and
                                    (old.LastOccurrence = new.LastOccurrence))
and (new.Class!=40235))
             then
                  cancel;
             end if;
         end if;

         set old.Tally = old.Tally + 1;
         set old.LastOccurrence = new.LastOccurrence;
         set old.StateChange = getdate();
         set old.InternalLast = getdate();
         set old.Summary = new.Summary;
         set old.AlertKey = new.AlertKey;
         set old.ProbeSubSecondId = new.ProbeSubSecondId;
         if ((old.Severity = 0) and (new.Severity > 0))
         then
           set old.Severity = new.Severity;
         end if;
end
```

10. Click **OK**.

Configuring the Deduplicate_details Trigger

When the **Collapse duplicate events into a single event** option is enabled for a job, the Connector sends every occurrence of the duplicate event with an updated count and details to Netcool. If **Save to Netcool Details** option is selected to enable the connector to send AppManager event details to Netcool MTTRAPD probe, you cannot view the updated event details unless you modify the deduplicate_details trigger.

To replace the default deduplicate_details trigger:

1. Start **Administrator** in the Netcool Suite program folder.
2. In **NETCOOL/OMNIbus Administrator**, expand **Reports**.
3. Click **ObjectServers**.
4. Double-click the ObjectServer that handles AppManager events.
5. In the ObjectServer Security dialog box, specify the credentials and click **OK**.
6. Expand **Automation** and click **Triggers**.
7. Double-click the **deduplicate_details** trigger.
8. In the Edit Database Trigger dialog box, click the **Actions** tab.

9 Replace the existing SQL statement with the following:

```
declare flag bool;
begin

set flag = true;

for each row srow in alerts.status where srow.Identifier = new.Identifier

Begin
if (srow.Class = 40235) then
set flag = false;
break;
end if;
end;

if (flag=true) then
cancel;
end if;
set old.Detail = new.Detail;
end
```

10 Click **OK**.

Receiving NetIQ Alert Status from Netcool

When you modify an alert status in the Netcool Event List, the SNMP Trap Services receives the trap sent by the SNMP Gateway. The connector receives the forwarded NetIQ-specific alert statuses. The connector updates the connector database with the modified status. The statuses are displayed in the AppManager console.

Recovering the AppManager Repository

If an AppManager repository fails, the connector temporarily stops functioning. When the repository recovers, the connector resumes functioning. The NetIQ specific alerts are stored in the connector database and are forwarded to the AppManager repository when the AppManager repository is restarted.

Stopping the Connector Service

If the connector's service stops, the connector stops. Select **Disable Restart Period** in the Advanced Settings (2) tab of the connector Configuration Utility to forward AppManager events, generated during the downtime, to Netcool. When the NetIQ AppManager / IBM Tivoli Netcool Connector service is restarted, the AppManager events generated during the downtime are forwarded to Netcool.

AppManager Connector Elements

The following table lists the elements that the connector sends to Netcool MTTRAPD probe in the form of SNMP trap:

Connector Element	Varbindint	Description
$ConnectorName	$1	The name of the connector.
$ConnectorVersion	$2	The version number of the connector.
$AMStoreDetail	$3	The alert details in the Netcool Event List.
$QDBName	$4	The name of the AppManager repository.
$QDBHost	$5	The Microsoft SQL Server hosting the repository.
$ConnectorHost	$6	The name of the host for the connector.
$AMSeverity	$7	The original severity of an event in AppManager (1-40).
$AMJobID	$8	The AppManager job ID that originated the event.
$AMEventID	$9	The AppManager event ID for the event.
$AMKSName	$10	The name of the AppManager Knowledge Script (KS) that originated the event.
$AMCategoryName	$11	The name of the AppManager Category the event belongs to.
$AMKSGName	$12	The name of the AppManager Knowledge Script Group (KSG) that originated the event.
$AMKSGID	$13	The ID of the AppManager Knowledge Script Group (KSG) that originated the event. This field is not included in the default `mttrapd.rules` file.
$AMEventCount	$14	The AppManager Event count of the event.
$AMLastOccurTimeUTC	$15	The UTC time of the last occurrence of an AppManager event.
$AMFirstOccurTimeUTC	$16	The UTC time of the first occurrence of an AppManager event.
$AMEventMsg	$17	The short message text for the event.
$NumAMAgentMsgs	$18	Indicates how many AgentMsg<*X*> elements (The value of *X* ranges from 1 to 8) are populated with data.
$AMEventHostIPAddress	$19	The IP address of the computer that originated the event.
$AMEventHostDomainName	$20	The Domain name (NT if Windows, DNS if UNIX). This field is not included in the default `mttrapd.rules` file.
$AMURL	$21	The Web URL to access the AppManager Web Console interface for the event.
$ConnectorID	$22	The unique identifier for the connector that forwarded the event.
$AMEventHost	$23	The agent computer from which the event originated.
$NCSeverity	$24	The level of severity for the event in Netcool.
$AMAcknowledge	$25	Whether the event is acknowledged in AppManager.

Connector Element	Varbindint	Description
$NCFirstOccurTime	$26	The time of the first occurrence of an AppManager event, converted to Netcool time.
$NCLastOccurTime	$27	The time of the last occurrence of an AppManager event, converted to Netcool time.
$AMParentEventID	$28	The AppManager parent event ID for the event.
$AMAgentMsg	$29	The detailed message text for the event that is populated based on one of the following: ◆ **The AppManager repository contains an AgentMsgShort field:** The message contained in the AgentMsgShort field is populated ◆ **The AppManager repository contains an AgentMsgLong field that has a message whose length is less than 255 bytes:** The message contained in the AgentMsgLong field is populated ◆ **The AppManager repository contains an AgentMsgLong field that has a message whose length is greater than 255 bytes:** The string N/A is populated and the message is divided into a maximum of 8 message chunks with each chunk not exceeding 255 bytes. These message chunks are populated into AMAgentMsg<X> (The value of *X* ranges from 1-8)
$AMAgentMsg<X>	$30 - $37	Up to eight detailed messages. If the AgentMsgLong field has a message whose length is greater than 255 bytes, then the string N/A is populated in $AMAgentMsg. The message is divided into a maximum of 8 message chunks with each chunk not exceeding 255 bytes. These message chunks are populated into AMAgentMsg<X> (The value of *X* ranges from 1-8). Any of the AMAgentMsg<X> elements that is not populated with message remains blank.

Field Mapping

The following table lists the default field mappings for AppManager and Netcool.

Netcool Field	Varbindint	Netcool Elements or AppManager Event Information	Comments
@Node	$23	<AM MachineName>	Host where the event originated (or the connector host)
@AlertKey	$8	<AM Job ID>	
@Manager	$10	<AM KS Name>	
@AlertGroup	$11	<AM Category Name>	
@Agent	$12	<AM KSG Name>	
@Count [@Tally]	$14	<AM Event Count>	
@Summary	$17	<AM Short Event Message>	

Netcool Field	Varbindint	Netcool Elements or AppManager Event Information	Comments
@NodeAlias	$19	<AM Machine Name IP Address>	IP address of the connector host
@URL	$21	<AM Web Console URL of Event>	Only set if AM Web Console is defined as available
@Identifier	$22	<ConnectorID>	Source info on event
@Severity	$24	<Mapped AM Event Severity>	The Netcool mapped severity defined by Config UI
@Acknowledged	$25	<0 or 1 if Acknowledged in AM>	Set to Ack or not
@FirstOccurrence	$26	<AM FirstOccurTime of Event>	
@LastOccurrence	$27	<AM LastOccurTime of Event>	
@Type		0	Defaults to "Type Not Set"
@Class		40235	Set to NetIQ AppManager - DO NOT CHANGE

SNMP Gateway

Configure the SNMP Gateway to send the Netcool traps.

NOTE: When both the ObjectServer Granularity property and the `Gate.Reader.IducFlushRate` property are set to their default values, the gateway's ability to forward alert updates is affected. If the `Gate.SNMP.ForwardUpdates` property is set to TRUE in these conditions, the gateway will not be able to capture all alert updates.

If you find that the event updates are not synchronized from Netcool to AppManager, then you might want to reduce the value of the `Gate.Reader.IducFlushRate` property to 20 seconds or so.

For more information, see Event flush rate at the IBM Web site.

For information on configuring the SNMP Gateway, review the following sections:

- "SNMP Gateway Version 0.0.1395" on page 15
- "SNMP Gateway Version 1.5.1.0 and 1.6.0.0" on page 16

SNMP Gateway Version 0.0.1395

By default, the `G_SNMP.conf` file is available in the following location:

- **On Microsoft Windows computers:** *`$OMNIHOME`*`\ini`
- **On UNIX computers:** *`$OMNIHOME`*`/gates/snmp/`

where *`$OMNIHOME`* is the installation path for IBM Netcool.

You must copy the `G_SNMP.conf` file to the following location on your UNIX computers and edit the file: *`$OMNIHOME`*`/etc/`

The G_SNMP.conf file uses the following syntax:

```
CREATE MAPPING mappingname
{
varbindint = '@fieldname'
[,'varbindint = '@fieldname' [ON INSERT ONLY]]...
);
```

The *mappingname* is the name of the mapping to be created.

The *varbindint* is the integer value for the varbind field that will be written to in the SNMP trap.

The *fieldname* is the name of the field in the ObjectServer alerts.status table.

Mapping for Version 0.0.1395

Replace the mapping supplied in the G_SNMP.conf configuration file with the following content:

```
CREATE MAPPING SNMP_MAP
(
 0 = '@Class',
 1 = '@Identifier',
 2 = '@Node',
 3 = '@Acknowledged',
 4 = '@ExpireTime',
 5 = '@ServerName',
 6 = '@ServerSerial'
);
```

Configure the SNMP writer supplied in the G_SNMP.conf configuration file by replacing the following content:

```
START WRITER SNMP_WRITER
(
TYPE = SNMP,
REVISION = 1,
PORT = 162,
GATEWAY = 'snmphost',
COMMUNITY = 'public',
FORWARD_UPDATES = TRUE,
MAP = SNMP_MAP
);
```

where *snmphost* is the name of the computer to which SNMP Gateway forwards traps.

NOTE: Set the port to be the same as the port configured for SNMP Trap Service. By default, SNMP Trap Service listens to port 162.

SNMP Gateway Version 1.5.1.0 and 1.6.0.0

By default, the NCO_GATE.props file is available in the following location:

- **On Microsoft Windows computers:** *$OMNIHOME*\gates\snmp
- **On UNIX computers:** *$OMNIHOME*/gates/snmp/

where *$OMNIHOME* is the installation path for IBM Netcool.

You must copy the NCO_GATE.props file to the following location on your Windows and UNIX computers and edit the file to suit your environment:

- **On Microsoft Windows computers:** *$OMNIHOME*\etc
- **On UNIX computers:** *$OMNIHOME*/etc/

NOTE: NetIQ Corporation recommends that you copy NCO_GATE.props file to the default folder: *$OMNIHOME*/etc/default

To enable the SNMP Gateway to forward updates to AppManager, edit the following properties in the NCO_GATE.props file:

Property	Value
Gate.MapFile	*$OMNIHOME*/gates/snmp/snmp.map
Gate.SNMP.Community	public
Gate.SNMP.ForwardUpdates	TRUE
Gate.SNMP.Gateway	<*connectorHost*>:<*portnumber*> where *connectorHost* is the name of the Connector computer and *portnumber* is the port configured for SNMP Trap Service. By default, SNMP Trap Service listens to port 162.

Mapping for Version 1.5.1.0

Replace the mapping supplied in the snmp.map file with the following content:

```
CREATE MAPPING StatusMap
(
'0' = '@Summary',
'1' = '@Severity',
'2' = '@Location',
'3' = '@Node',
'4' = '@AlertGroup',
'5' = '@Acknowledged',
'6' = '@NodeAlias',
'7' = '@Identifier',
'8' = '@Class',
'Node' = '@Node'
);
```

Mapping for Version 1.6.0.0

Replace the mapping supplied in the `snmp.map` file with the following content:

```
CREATE MAPPING StatusMap
(
'0' = '@Class',
'1' = '@Identifier',
'2' = '@NodeAlias',
'3' = '@Acknowledged',
'4' = '@Summary',
'5' = '@Severity',
'6' = '@Location',
'7' = '@Node',
'8' = '@AlertGroup',
'Node' = '@Node'
);
```

MTTRAPD Rules

The MTTRAPD Probe receives SNMP traps from the connector using an internal queue mechanism.

IMPORTANT: AppManager Connector for Netcool 7.4 or later uses the new OID 1.3.6.1.4.1.1691 to send SNMP traps and the new connector name `NetIQ/IBM Tivoli Netcool Connector`.

If you are using any filter on the older OID to receive SNMP traps from AppManager Connector for Netcool 7.2 or a previous version, modify the old OID to 1.3.6.1.4.1.1691 in the `mttrapd.rules` files after upgrading to AppManager Connector for Netcool 7.4 or later.

By default, the `mttrapd.rules` file is available in the following location:

- **On Microsoft Windows computers:** *`$OMNIHOME`*`\probes\win32\`
- **On UNIX computers:** *`$OMNIHOME`*`/probes/`*`platform`*

where *`$OMNIHOME`* is the installation path for IBM Netcool and platform is the name of the UNIX platform on which you have installed Netcool.

In the `mttrapd.rules` file, add the following content under the `if (match($generic-trap, "6"))`loop to ensure that the Netcool fields are mapped to the AppManager Event information:

```
@Identifier=$22    # <ConnectorID>       'Connector ID of trap source
@Node=$23          # <AM MachineName>    'Host that event originated from
@NodeAlias=$19     # <AM MachineName IP Address>'Host's IP address that event
#originated from
@Manager=$10       # <AM KS Name>        ' Knowledge script name
@Agent=$12         # <AM KSG Name>       ' Knowledge script group for this KS
@AlertGroup=$11    # <AM Category Name>  ' Category of the knowledge script
@AlertKey=$8   # <AM JobID>          ' ID of AppManager job that created the event
@Severity=$24 # <Mapped AM event Severity> 'The Netcool mapped severity defined by
#Config UI
@Summary=$17   #<AM Short Event Message> ' Primary AM event message
@LastOccurrence=$27 #<AM LastOccurTime of Event> ' Last occurrence time of event
#in UTC
@FirstOccurrence=$26 #<AM FirstOccurTime of Event> ' First occurrence time of event
#in UTC
@Tally=$14 # <AM Event Count> ' The number of times the event has occurred in AM
update(@Tally)      # Update Alert with Event Count
```

```
@Type="0"        # Defaults to "Type Not Set"
@Class="40235"          # Set to NetIQ AppManager - DO NOT CHANGE
@Acknowledged=$25    # 0, 1, or 2 ' AM status mapped to its Netcool equivalent
@URL=$21 # <AM Web Console URL of Event>'Only set if AM Web Console is defined as
#available

 #Mapping AppManager Acknowledged State to Netcool Acknowledged State
    if (match(@Acknowledged, "1"))
    {

      update(@Acknowledged)
    }

 #Mapping AppManager Closed State to Netcool Acknowledged State
    if (match(@Acknowledged, "2"))
      {

      update(@Acknowledged)
    }

  $AmStoreDetail=$3
  #Check if the user checked save to netcool details in connector Config Utility.
    if (match($AmStoreDetail, "1"))
    {
      #Mapping to Alert Details
      $ConnectorName=$1
      $ConnectorVersion=$2
      $QDBName=$4
      $QDBHost=$5
      $ConnectorHost=$6
      $AMSeverity=$7
      $AMJobID=$8
      $AMEventID=$9
      $AMParentEventID=$28
      $AMKSName=$10
      $AMCategoryName=$11
      $AMKSGName=$12
      $AMFirstOccurTimeUTC=$16
      $AMLastOccurTimeUTC=$15
      $AMEventMsg=$17
      $NumAMAgentMsgs=$18
      $AMAgentMsg=$29
      $AMAgentMsg1=$30
      $AMAgentMsg2=$31
      $AMAgentMsg3=$32
      $AMAgentMsg4=$33
      $AMAgentMsg5=$34
      $AMAgentMsg6=$35
      $AMAgentMsg7=$36
      $AMAgentMsg8=$37

      #Sending the information to Alert Details
      details($ConnectorName,$ConnectorVersion,$QDBName,$QDBHost,$ConnectorHost,
$AMCategoryName,$AMSeverity,$AMEventID,$AMParentEventID,$AMJobID,$AMKSName,
$AMKSGName,$AMFirstOccurTimeUTC,$AMLastOccurTimeUTC,$AMEventMsg,$AMAgentMsg,
$AMAgentMsg1,$AMAgentMsg2,$AMAgentMsg3,$AMAgentMsg4,$AMAgentMsg5,$AMAgentMsg6,
$AMAgentMsg7,$AMAgentMsg8)
}
```

NOTE:

- Do not modify the mappings. You can only change the order of the mappings. You might want to use the sample *connectorInstallFolder*\redist\mttrapd.rules file, which contains the complete configuration for the connector to work with MTTRAPD probe.
- To disable the AppManager acknowledged events from forwarding to Netcool by the connector, comment out the lines in the mttrapd.rules file as follows:

```
#if (match(@Acknowledged, "1"))
#    {

#      update(@Acknowledged)
#    }
```

- To disable the AppManager closed events from forwarding to Netcool by the connector, comment out the lines in the mttrapd.rules file as follows:

```
#if (match(@Acknowledged, "2"))
#    {

#      update(@Acknowledged)
#    }
```

By default, the mttrapd.props file is available in the following location:

- **On Microsoft Windows computers:** *$OMNIHOME*\probes\win32\
- **On UNIX computers:** *$OMNIHOME*/probes/plateform

where *$OMNIHOME* is the installation path for IBM Netcool and platform is the name of the UNIX platform on which you have installed Netcool.

In the mttrapd.props file, specify the same port number that was used to configure the connector, for example Port: 12345, so that the MTTRAPD Probe receives SNMP traps from the connector and events are displayed in the Netcool Event List.

2 Installing the Connector

This chapter provides installation instructions and describes system requirements for the AppManager Connector for Netcool.

This chapter assumes you have AppManager installed. For more information about installing AppManager or about AppManager system requirements, see the *Installation Guide for AppManager*, which is available on the AppManager Documentation page.

System Requirements

For the latest information about supported software versions and the availability of connector updates, visit the AppManager Supported Products page. Unless noted otherwise, this module supports all updates, hotfixes, and service packs for the releases listed below.

IMPORTANT: Ensure that the SNMP Trap Windows Service on the Connector computer is running because the NetIQ AppManager/ IBM Tivoli Trap Receiver depends on the SNMP Trap Windows service to receive traps from the Netcool SNMP Gateway.

AppManager Connector for Netcool has the following system requirements:

Software/Hardware	Version
NetIQ AppManager	8.0.3, 8.2, 9.1, 9.2, 9.5, or later
Microsoft Windows operating system on the Connector computer	One of the following: ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows Server 2008 R2 ◆ Windows Server 2008 (32-bit and 64-bit) ◆ Windows Server 2003 R2 (32-bit or 64-bit) ◆ Windows Server 2016 (64-bit)
Microsoft SQL Server on the Connector database computer	One of the following: ◆ SQL Server 2014 ◆ SQL Server 2012 R2 ◆ SQL Server 2012 ◆ SQL Server 2008 R2 (32-bit and 64-bit) ◆ SQL Server 2008 (32-bit and 64-bit) ◆ SQL Server 2005 ◆ SQL Server 2016 (64-bit)
IBM Tivoli Netcool/OMNIbus	8.1, 7.4.0, 7.3.1, 7.3.0, 7.2.1, 7.2.0, or 7.1
IBM Tivoli Netcool MTTRAPD Probe	7.0.1857, 11.0.0, 12.0.0, or later

Software/Hardware	Version
IBM Tivoli Netcool SNMP Gateway Server	1.6.0.0, 1.5.1.0, or 0.0.1395
MDAC on the Connector computer	2.6 or later

Although the connector is supported only on Windows servers, it can communicate with Netcool installed on one of the following UNIX platforms:

- Sun SPARCstation or UltraSPARC with Solaris 11 (64-bit)
- Sun SPARCstation or UltraSPARC with Solaris 10 (32-bit and 64-bit)
- Sun SPARCstation or UltraSPARC with Solaris 9 (32-bit and 64-bit)
- Sun SPARCstation or UltraSPARC with Solaris 8 (32-bit and 64-bit)
- HP-9000 Series with HP-UX 11.i (v2 and v3)
- Red Hat Enterprise Linux 6 and 7 (64-bit)
- Red Hat Enterprise Linux 5.2 and 5.0 (32-bit and 64-bit)

Account Requirements

The connector setup program requires access to various administrator privileges and user account information to install the connector components. Before installing the connector, configure all the accounts except the Microsoft SQL Server account for the connector database.

The following table lists the accounts required by the connector setup program:

To	You Need
Install the connector	A Windows local user account or a domain account in the local administrator group of the computer where you have installed the connector to run the `NetIQ AppManager/IBM Tivoli Netcool Connector` service and the connector's component - COM server `AMNCServer.exe`. The COM server must have access to all repositories and depends on the security mode of the Microsoft SQL Server instances for the AppManager repository and connector database.
Install the connector database	The `sa` account. The connector setup program requires the Microsoft SQL Server `sa` account to install the connector database (AMNC). After you install the database, you can change the database owner to another account.
Configure the connector to access the AppManager repository and connector database	A Microsoft SQL Server login account that you want the connector COM server to use to access the AppManager repository and connector database. This Microsoft SQL Server account must have read, write, and system administration rights on the AppManager repository and connector database.
Create custom Netcool fields in the Netcool ObjectServer	An account that has permission to administer various services of the Netcool ObjectServer.

Installing the Connector

Install the connector on any Windows computer that has network access to the computer where Netcool is installed. Netcool can be installed on a Windows computer or on a UNIX computer. You must install the connector database on a Microsoft SQL Server computer.

You can install the connector, connector database, Netcool, and AppManager repository on either a standalone Windows computer or on separate computers, depending on the needs of your enterprise.

You must be logged in as a member of the local Administrators group with permission to run as a service or as a domain user with Administrator privilege.

To install the connector and connector database:

1. Run the setup program, `AM_Netcool_Setup.exe`, on the computer where you want to install the connector.
2. In the Welcome dialog box, click **Next**.
3. In the License Agreement dialog box, read the license agreement and click **Yes** to accept.
4. In the Select Features dialog box, select the connector components you want to install and click **Next**.
   - Select **NetIQ AppManager/IBM Tivoli Netcool Connector** to install the connector files.
   - Select **Create Connector Database** to create the connector database.

   NOTE: Select both options to install the connector on the local computer and install the connector database on a specified Microsoft SQL Server computer (local or remote). By default, both the options are selected. If you are upgrading from a previous release or installing a hotfix, you must reinstall the connector database by selecting **Create Connector Database** in the Select Features dialog box.
5. In the Choose Destination Location dialog box, specify the location where you want to install the connector and click **Next**.

   NOTE: Do not install the connector on a network drive.
6. In the AppManager Repository Information dialog, specify the AppManager repository to which you want the connector to connect and click **Next**.

Field	Description
AppManager Repository Host	Specify the name of the AppManager repository computer from which you share event information.
SQL Instance (if any)	Specify the name of the Microsoft SQL Server instance. To specify the default instance, leave the field blank.
Database Name	Specify the name of the AppManager repository.
User	Specify the Microsoft SQL Server user account to access the AppManager repository. The user account must have read, write, and system administration rights on the AppManager repository.
Password	Specify the password that accompanies the user name.

7. In the AppManager Web Console Information dialog, provide the computer name where the AppManager Web Management Server is installed and click **Next**.

NOTE: If you want to respond to AppManager events in the AppManager Operator Web Console, you must configure the connector to specify the name of the corresponding AppManager Web Management Server. For more information, see "Configuring AppManager Web Console Server" on page 30.

8 In the AM/Netcool Connector Database Information dialog, specify the computer name of the connector and click **Next**.

Field	Description
Connector Database Host	Specify the name of the connector database.
SQL Instance (if any)	Specify the name of the Microsoft SQL Server instance. To specify the default instance, leave the field blank.
Database Name	Specify the name for the new connector database. The default is `AMNC`. To prevent the loss of information on events with the same event ID that came from different AppManager repositories, do not configure multiple Netcool connectors to use the same connector database.
User	Provide the Microsoft SQL Server user account to access the AppManager repository.
Password	Specify the password that accompanies the user name.

9 In the AppManager/Netcool COM Security Configuration Information dialog, specify the user account for the connector's COM server and click **Next**.

Field	Description
User	Provide the name of the Windows login account you want to designate as the account for the COM server. **NOTE:** The account must be a local account or a domain account with local administrator privileges and have permission to run as a service.
Password	Specify the password that accompanies the user name.
Confirm Password	Re-enter the password for the user name.

10 In the Service Configuration Information dialog, specify the service account under which you want the connector service to run and click **Next**.

Field	Description
User	Provide the name of the Windows login account you want to designate as the account for the NetIQ AppManager/ IBM Tivoli Netcool connector service. **NOTE:** The account must be a local account or a domain account with local Admin privileges and have permission to run as a service.
Password	Specify the password that accompanies the user name.
Confirm Password	Re-enter the password for the user name.

11 Review the settings in the Start Copying Files dialog box and click **Next** to start copying the program files.

12 Click **Finish** to complete the installation. When the setup program completes, the Configuration Utility is displayed. For more information, see Chapter 3, “Configuring the Connector,” on page 27.

The `AM2NetcoolInstall.log` file lists all changes and problems encountered during the installation process. By default, this file is located in the user’s `temp` folder.

Uninstalling the Connector

Before uninstalling the connector, make sure that no users are connected to the connector database.

You can uninstall the connector using the **Add or Remove Programs** feature in the Control Panel.

3 Configuring the Connector

This chapter provides instructions to configure the connector by using the NetIQ AppManager Connector for Netcool Configuration Utility.

The Configuration Utility includes both basic and advanced configuration options. The various configuration options are available under the tabs.

If you have User Account Control enabled, launch the Configuration Utility with the *Run as administrator* option. Running the utility as an administrator allows you to apply changes to the configuration and ensures you can restart the connector services properly.

Mapping AppManager to Netcool Severity Levels

AppManager has 40 severity levels and Netcool has six severity levels. You can map the AppManager severity levels to Netcool severity levels. Use the **AM to Netcool Severity Mapping** tab to map the AppManager severity levels to Netcool severity levels and to delete the severity mappings.

To map the AppManager severity levels to Netcool severity levels:

1. On the AM to Netcool Severity Mapping tab, select one or more AppManager severity levels in the NetIQ AppManager Severity panel.
2. In the IBM Tivoli Netcool Severity panel, select the Netcool severity level.
3. Click **Map Severity**.

   The following table lists the default mappings:

AppManager Severity Level	Netcool Severity Level
AppManager events with severity level between 1 and 5.	Critical Error
AppManager events with severity level between 6 and 10.	Major Error
AppManager events with severity level between 11 and 20.	Minor Error
AppManager events with severity level between 21 and 30.	Warning
AppManager events with severity level between 31 and 35.	Indeterminate
AppManager events with severity level between 36 and 40.	Clear

Deleting Severity Mappings

To modify a severity mapping level, delete the severity mapping you specified earlier.

To delete a severity mapping:

1. On the AM to Netcool Severity Mapping tab, select the severity mapping you want to delete.
2. Click **Delete Selected Severity Mapping**, or click **Clear All Mappings** to delete all the severity mappings.

Adding a Netcool Group

Use the Netcool Configuration tab to configure the following:

- NCO Multi-threaded TRAPD Probe groupings
- Netcool settings

To add a Netcool group:

1. On the Netcool Configuration tab, click **Add Group**.
2. Specify a name for the Netcool group and click **OK**.
3. Click **Add Machine** and complete the following fields:

Parameter	Description
Machine Name	Computer name (or IP address) of the Netcool ObjectServer.
Port	The communication port number. **NOTE:** Set the port to be the same as the port configured in the properties file of the MTTRAPD probe to listen to the SNMP trap. By default, MTTRAPD probe listens to port 162.

4. Select **Save to Netcool Details** to enable the connector to send AppManager event details to Netcool MTTRAPD probe.
5. Click **Apply** to complete the configuration.

Configuring AppManager Severity Filtering

Use the AM Severity Filtering tab to filter severity levels. Filtered AppManager severity levels are not forwarded to Netcool MTTRAPD probe. The left pane should only contain event severity levels that you want to forward to Netcool.

To filter AppManager Severity Levels:

1. On the **AM Severity Filtering** tab, highlight your selections in the left pane and click the **right arrow** button to move selections to the right pane.
2. ***If you do not want to filter any AppManager event***, click **Forward All**. By default, all AppManager severity levels are forwarded to Netcool.
3. Click **OK.**

Configuring AppManager Category Filtering

Use the AM Category Filtering tab to filter event categories sent to Netcool. The left pane should only contain event categories that you want to forward to Netcool.

To filter AppManager categories:

1. On the AM Category Filtering tab, highlight the category you want to filter and click the **right arrow** button to move the filtered selection to the right pane.
2. ***If you do not want to filter any of the listed AppManager categories***, click **Forward All**.

3 ***If you want the connector to forward the custom categories***, select **Forward All Unlisted Categories**.

4 Click **OK**.

Configuring AppManager Database Parameters

You can specify the AppManager database parameters if you had not specified the values during the connector installation. You can also modify the AppManager database parameters using the Configuration Utility.

On the DataBase Configuration tab, complete the following fields:

Field	Description
DB Host Name	Specify the name of the computer that hosts the AppManager repository.
DB Instance Name (if any)	Specify the database instance name. If there is only one instance, leave this field blank.
AM Database Name	Specify the name of the AppManager repository. Specify the name of the repository if you had chosen another name other than the default name (QDB) during the AppManager installation.
Use Integrated Security	Select this option to specify the connector server account, which is a domain Windows account with dbo permission to access the repository.
Valid User Name	Specify the user name for a valid account that has permission to access the Microsoft SQL Server on the computer that hosts the connector database. **NOTE:** Do not enter the user name if Integrated Security is enabled on the connector database. If you must use a Microsoft SQL Server account, give full (owner) permission to the account.
Password	Specify the password that accompanies the user name. **NOTE:** Do not enter the password if Integrated Security is enabled.

Configuring AppManager and Netcool Connector Database Parameters

You can specify the AppManager and Netcool connector database parameters if you did not specify the values during the connector installation. You can also modify the parameters using the Configuration Utility.

On the DataBase Configuration tab, complete the following fields**:**

Field	Description
DB Host Name	Specify the name of the computer that hosts the connector database.
DB Instance Name (if any)	Specify the DB Instance name. If there is only one instance, leave this field blank.
Database Name	Specify the name of the AppManager/Netcool connector database. Specify the name of the database, if you have chosen another name other than the default name (AMNC) during the connector installation.

Field	Description
Use Integrated Security	Select this option to specify the connector server account, which is a domain Windows account with dbo permission to access the repository.
Valid User Name	Specify the user name for a valid account that has permission to access the Microsoft SQL Server on the computer that hosts the connector database. **NOTE:** Do not enter the user name if Integrated Security is enabled on the connector database. If you must use a Microsoft SQL Server account, give full (owner) permission to the account.
Password	Specify the password that accompanies the user name. **NOTE:** Do not enter the password if Integrated Security is enabled.

Configuring AppManager Web Host Server Information

You can specify the AppManager Web host server information if you did not specify the Web server name during the connector installation.

On the DataBase Configuration tab, provide the name of the AppManager Web Server in the **Web Server Name** field.

Configuring AppManager Web Console Server

The connector provides a feature to launch the AppManager Web Console from the Netcool Event List for viewing selected AppManager events. To use this feature, the AppManager Web Console server must be installed and configured.

To configure AppManager Web Console server:

1. Copy the `EventDetailsByURL.asp` and `autologineventByURL.asp` files to the AppManager Web Console server's *`%AppManager%`*`\Web` folder. The files are located in the connector server's *`%ConnectorInstallPath%`*`\redist` folder.
2. On the AppManager Web Console server where you copied the files, open the `autologineventByURL.asp` file.
3. Specify the following information in the `autologineventByURL.asp file` and save the changes:
   - **Name:** Specify the user name to connect to the connector database.
   - **Password:** Specify the password that accompanies the user name.
   - **Computer:** Specify the name of the computer where the connector database is installed.
   - **Repository:** Specify the name of the connector database.
   - **NTAuthentication:** Specify a valid Windows account
4. From the Netcool Event List pane, right-click the forwarded AppManager events.
5. On the Tools menu, click **URL** to open the AppManager Web Console.

Configuring AppManager Event Settings

You can control the polling intervals between the connector and the AppManager repository by configuring the event settings.

On the Advanced Settings (1) tab, complete the following fields:

Field	Description
Poll for AM Events every X (seconds)	Select the frequency with which the connector has to poll the AppManager repository for new events.
Retrieve Max # of Events each Interval	Select the rate at which the connector has to retrieve new events.
Poll for AM Updates every X (seconds)	Select the frequency at which the connector has to poll the AppManager repository for events whose status has been changed.

Configuring Netcool Alert Settings

You can specify the frequency and rate with which the connector forwards AppManager events to Netcool as alerts.

On the Advanced Settings (1) tab, complete the following fields:

Field	Description
Send Max # of Updates to Netcool each Interval	Select the rate at which the connector has to forward updated information to Netcool.
Send Max # of Alerts each Interval	Select the rate at which the connector has to send new AppManager events to Netcool.

Enabling the Use of FQDN in Netcool Alerts

You can choose to provide the fully qualified domain name (FQDN) of the agent computer in alerts from AppManager in the Netcool console. If you do not select this option, the hostname of the agent computer appears just as it does in the AppManager console TreeView pane.

On the Advanced Settings (1) tab, select **Use FQDN of source of alerts sent to Netcool**.

Disabling AppManager Event Synchronization

If event synchronization is disabled and an AppManager event is acknowledged before it is forwarded to Netcool by the connector, the resolution state for this AppManager alert is **Ack** in Netcool.

On the Advanced Settings (1) tab, select **Disable Synchronization of AppManager with NetCool** to ensure that changes to AppManager event status are not synchronized from AppManager to Netcool. It will also erase the contents of the event mapping table in the connector database.

Forwarding Previous Events When Starting a New Database

In previous releases, when you started with a new AppManager Netcool database after a new release or hotfix, the connector would forward to AppManager every event from the past that was in the repository. Now you can limit the number of events the connector sends by entering the event ID of the last event that you encountered before you upgraded the connector.

On the Advanced Settings (1) tab, in the Last AM event ID forwarded to Netcool field, type the event ID of the last event that was forwarded out of the repository. When you start the new database, the connector will start from the next event ID and will not forward any events before that event.

NOTE: If you leave this option set to zero, when you start the new database, the connector forwards to AppManager every past event in the repository.

Deleting Events from Netcool

When you acknowledge an alert, the NetIQ event status is mapped to **Ack**. You can also delete an event from the Netcool repository.

To delete events from Netcool:

1. Start **Administrator** in the Netcool Suite program folder.
2. In NETCOOL/OMNIbus Administrator, expand **Navigator**.
3. Expand the `root` directory.
4. Double-click the ObjectServer. The ObjectServer Security dialog box is displayed.
5. Log in as `root`.
6. Expand **Menu** and click **Tools**.
7. In the Tools list, right-click **Delete Action** and select **Edit Tool**.
8. On the SQL tab, replace the existing SQL commands with the following:

```
update alerts.status set Acknowledged = 2, ExpireTime=2 where Serial in
($selected_rows.Serial);

flush iduc
```

9. On the SQL tab, ensure the **Enabled** check box is selected and click **OK**.
10. In the Netcool/OMNIbus Event List, on the **File** menu, select **Resync** and then select **All**.
11. Select the alerts you want to delete.
12. Right-click the alerts and select **Delete**.

NOTE: The Delete Action tool sets the Expire Time to 2 and Acknowledged status to 2. After two minutes, the expire trigger deletes the alert from Netcool Event List.In the Netcool/OMNIbus Administrator window, click Automation and then click Triggers. Ensure that Enabled and Group Enabled columns are set to true in the expire trigger.

Configuring Updates and Validation Settings

Use the Advanced Settings (2) tab to define connector configuration and validation settings. Complete the following fields:

Field	Description
Check for Configuration Updates every X (minutes)	Specify the interval in which the connector should look for configuration updates. **NOTE:** This does not check for updates to database accounts. If you change a database account, you must restart the connector service for the changes to take effect.
Disable Validation Checking	Select this check box to disable the statistical sampling that looks for errors in the correlation between AppManager events that have not been modified for a specified number of days.
Run Validation Check every X (hours)	When an AppManager operator marks an event for deletion, it may get deleted from the AppManager repository before the connector is aware of the status change. For this reason, there may be AppManager events that do not correlate with any alerts sent to the Netcool TRAPD Probe or AppManager repository.
Hour when full validation may be performed	When validation checking with a statistical sampling uncovers uncorrelated AppManager events, a full validation will be run on AppManager events that have not been modified for a specified number of days. The full validation process can be time consuming. Select this option to schedule full validation at a convenient time.
Check unchanged events older than X (days)	Specify the number of days to wait before removing unmodified AppManager events from the connector cache during the full validation check.
Disable Restart Period	Select this option to disable the restart function. If this check box is selected, the connector forwards all the alerts and events that have occurred since the connector service stopped.
Server Restart Period (minutes)	If the connector service has stopped, use this field to determine how far back in time it should go to fetch the alerts and events after it restarts. If the **Server Restart Period** field is set to one hour, for example, the behavior is as follows: ◆ If the connector service restarts within one hour of the time it stopped, it will process and forward all of the alerts and events that have occurred since it stopped. ◆ If the service restarts more than an hour after it stopped, it will process and forward *only* the last *ten* AppManager events that occurred before it restarted. The Server Restart Period behavior does not apply to downtime of database connections, or any other failovers.
Error Logging Level	This refers to the logging of the connector service. Select the drop-down list to set the level for logging the connector service. The error logs are created in `\Program Files\NetIQ\temp\NetIQ_debug\<name of machine>\AMNC.log`.
Enable/Disable Logging	Select this option to choose Error Logging type or no logging.

Field	Description
Max Log Size (MB)	Select this option to set a limit to the log file size. When the log reaches the specified limit, it is copied to a backup file (replacing the previous one) so that the disk space used is twice the Max Log Size. If Max Log Size is set to zero, there is no limit on the file size.

Configuring COM Connection

Use the COM Configuration tab to Specify the COM Configuration details:

Field	Description
Interactive User (Use only for Debug Testing)	This mode is for use by NetIQ Technical Support only. **NOTE:** The connector service should be stopped before running in debug mode.
This User (Enter a Valid User Account to run the Server under)	The connector application runs as a Windows service that runs a COM server (the AMNCServer process). Enter an account (user name and password) for the AMNCServer process.

For any database computer with security set to Integrated Security Mode (also called “Windows only”), the AMNCServer process user name and password must match those of the user’s administrative account on that computer. For more information, see “Account Requirements” on page 22.

Installing a Connector Backup

You can install more than one connector for failover purposes. If the primary connector becomes unavailable, the secondary connector acts as a backup to send and receive events. However, for the backup connector to receive alert updates from Netcool, you need a separate instance of the SNMP Gateway that can forward updates to the backup connector.

To configure a two-connector failover system:

1. Install two separate connectors on two independent computers. For information, see “Installing the Connector” on page 23
2. Ensure that both connectors use the same AppManager repository. Using two different AppManager repositories might result in the loss of event information on events with the same event ID that came from different AppManager repositories.
3. Ensure that both connectors use the same connector database.
4. Configure each connector to have the same filtering and polling values. These values are maintained on each computer where you have installed the connector, along with the rules and properties files.

NOTE: Repeat the process if there are more than two connectors.

One connector will be designated as the primary one where you can configure the following parameters:

- AM Event ID field (if used)

- AM Event Source field (if used)
- Restart Period
- Netcool Save Details

A secondary connector does not allow you to change these values.

4 Working with AppManager Events

This chapter describes how to use IBM Tivoli Netcool and AppManager to manage AppManager events generated in your organization.

Working with Events

After you install the connector, you can view event status from either the AppManager console or the Netcool Event List.

For more information on managing events from the AppManager console, see the *Administrator Guide for AppManager*.

The connector formats an AppManager event into a Netcool alert, providing administrators with detailed troubleshooting information.

To view and acknowledge the alert details:

1. Double-click a Netcool alert in the Alert Status dialog box.
2. On the Alert Details tab, right-click the alert in the Netcool Event List and select **Acknowledge**. The connector forwards the event status to the AppManager console. For more information on using the Netcool Event List, see the *Netcool/OMNIbus User Guide.*

Working with Event Collapsing

When you enable event collapsing in AppManager, AppManager forwards duplicate events as a single event to Netcool. Netcool displays each subsequent occurrence as a single occurrence of the same event. The subsequent events have the same identification number as the original event and are displayed with time-stamps of their occurrences.

Whenever the parent event in AppManager generates a child event, the event displays as **New** in the Netcool console.

AppManager events, by default, are displayed in an ascending order (parent event, followed by child events that display the most recent event first). Depending on your configuration, Netcool alerts display corresponding child events in descending order, beginning with older child events followed by newer child events.

You can also set other options in AppManager, which then affect how events are displayed in Netcool. For example, you can set AppManager to automatically close events if an event condition does not exist.

For more information on event collapsing and automatically closing events, see the *Administrator Guide for AppManager*.

Troubleshooting

If new or updated AppManager events are not showing up as alerts in the Netcool console, then data is not flowing from AppManager to Netcool. Take the following steps to rectify the problem:

- Ensure `AMNCServer.exe` is running. This program enables the flow of data from AppManager to Netcool.
- If `AMNCServer.exe` is not running, restart the NetIQ AM/IBM Tivoli Netcool Connector Service (`amncservice.exe`), which will restart `AMNCServer.exe` and resume the flow of data.
- If `AMNCServer.exe` is running, check `AMNC.log` to verify the time of the last log entry. If no entries have been written to the log in a while, then the `AMNCServer.exe` process may be hung or locked up. Stop `AMNCServer.exe` and restart `AMNCService.exe`. `AMNCServer.exe` will start as well and begin processing AppManager events that are to be sent to Netcool.

If the AppManager console does not reflect updated event statuses from actions occurring in Netcool, then data is not flowing from Netcool to AppManager. Take the following steps to rectify the problem.

- Ensure the SNMP Trap Service, `snmptrap.exe`, is running. This Windows service enables AppManager to receive traps. Start the service if it is not running.
- Ensure `SNMPTrapReceiverFromNC.exe` is running.

  If `SNMPTrapReceiverFromNC.exe` is not running, restart the NetIQ Trap Receiver service, `AMNCTrapRecv.exe`, which will, in turn, start `SNMPTrapReceverFromNC.exe`.

  If `SNMPTrapReceiverFromNC.exe` is running, check `SnmpTrapHandler.log` for log entries. If initialization was successful and `SNMPTrapReceiverFromNC.exe` is running, but no updates have been written to the log in a while, then trap updates are not being received from Netcool. Ensure `snmptrap.exe` is running.
- If `snmptrap.exe` and `SNMPTrapReceiverFromNC.exe` are running and log entries are being recorded, restart Netcool.

If the AppManager events are not able to synchronize from the Netcool console to the AppManager console, perform the following:

- Specify the community name string as a `public` in the SNMP service and select the appropriate permission level in the community rights. The default is **READ ONLY**.
- Restart the SNMP service.

NOTE: If the connector and the IBM Netcool are on a separate machine, the community name string must be specified on the machine in which the IBM Netcool is installed.
