

Avaya Solution & Interoperability Test Lab

Application Notes for IBM Tivoli Netcool/OMNIbus Event Management System with Avaya Communication Manager for SNMP Trap Collection - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to activate SNMP alarm notification on Avaya Communication Manager and SNMP trap collection on the IBM Tivoli Netcool/OMNIbus Event Management System. IBM Tivoli Netcool/OMNIbus was compliance tested with an Avaya S8300 Media Server with a G350 Media Gateway, and an Avaya S8700 Media Server with a G650 Media Gateway. The Avaya Media Servers and Gateways were configured to send event information to IBM Tivoli Netcool/OMNIbus using v1 and v2c SNMP traps.

Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required to activate SNMP alarm notification on the Avaya Media Servers and Gateways, and SNMP trap collection on the IBM Tivoli Netcool/OMNIbus Event Management System. Upon detection of a failure, the Avaya Media Servers and Gateways can raise an alarm and send an SNMP trap over the IP network to the designated SNMP trap receiver(s). As a non-intrusive SNMP trap receiver, Netcool/OMNIbus can collect, store, and manage alarm information received from Avaya Communication Manager. Avaya Communication Manager running on the Avaya Media Server reports alarms via SNMP traps according to the configured alarm reporting options.

Figure 1 illustrates an enterprise network comprised of an Avaya S8300 Media Server with a G350 Media Gateway and an Avaya S8700 Media Server with a G650 Media Gateway that connect to the Avaya C363T Converged Stackable Switch. The Avaya Media Servers and Gateways send event and alarm information to the Netcool/OMNIbus Event Management System on UDP port 162 using v1 and v2c SNMP traps. The Avaya S8300 and S8700 Media Servers have an internal SNMP agent that sends SNMP traps directly to the Netcool/OMNIbus ObjectServer. The S8700 Media Server sends all event and alarm information related to the Avaya G650 Media Gateway. Likewise, the S8300 Media Server sends all event and alarm information related to the Avaya G350 Media Gateway. In this configuration, all of the Netcool/OMNIbus software components used in the compliance test were installed in the same server.

The Netcool/OMNIbus components covered in the compliance test included the **MTTrapD Probe**, **ObjectServer**, and **Desktop Client**. The **Flex License Manager** was also used to determine the licensed applications running on the Netcool/OMNIbus system. The Netcool Probe collects SNMP traps received on UDP port 162 and forwards them to the Netcool ObjectServer, which is a database server where all events are stored and managed. The ObjectServer is capable of consolidating repeated events collected by the Probe (also referred to as de-duplication) and correlating related events, such as link down/up events. The ObjectServer converts the traps to human-readable "events" to be viewed and acknowledged with the Desktop application. The Desktop is a graphical tool that is used to view and manage events and can provide a filtered view of color-coded alerts displayed in the Event List. By default, the Desktop application polls the ObjectServer for event information every 60 seconds, or upon demand.





2. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya S8700 Media Server with Avaya G650 Media Gateway	Communication Manager 3.1
	(R013x.01.0.628.6)
Avaya S8300 Media Server with Avaya G350 Media Gateway	Communication Manager 3.1
	(R013x.01.0.628.6)
IBM Tivoli Netcool/OMNIbus	Version 7.0.6
 SNMP Probe 	
 ObjectServer 	
 Desktop Client 	
 Flex License Manager 	
OS – Microsoft Windows XP Professional	
Netcool Knowledge Library (NcKL)	Release 1.2

3. Avaya Media Server SNMP Configuration

This section describes the procedure for configuring the Avaya S8300 and S8700 Media Servers to report alarms to an SNMP trap destination. The required steps are:

- Activating SNMP alarm notification on the Avaya S8300 and S8700 Media Servers.
- Allowing SNMP traps to be output from the Avaya Media Server on UDP port 162.
- Checking that Avaya alarms that should generate SNMP traps are being reported according to the alarm reporting options. The alarm reporting options are specified in the set options form accessible through the System Access Terminal (SAT). See reference [1] for a description of the set options form.

3.1. Configuring SNMP Trap Destinations

The SNMP trap destinations for the Avaya S8300 and S8700 Media Servers are configured through the server's web interface. To access the web interface, launch a web browser and connect to the media server by entering <u>https://<media server IP address></u>. Supply the login and password for an account with super-user privileges. For an S8700 Media Server pair, the SNMP trap destinations need to be configured on each media server. Select **Launch Maintenance Web Interface** from the screen.

Home(Standard Managemer	nt Solutions) - Microsoft Intern	et Explorer	
Elle Edit View Favorites I	(ools <u>H</u> elp		
⇔Back • → - 🗿 🗗 🖄	QSearch ⊡Favorites @M	ala 🕑 🛂 🚽 🖃 🗐	
Address 🕘 https://192.45.80.214	l/cgi-bin/unified		▼ 🖓 Go Links ≫
AVAYA			Integrated Management Standard Management Solutions
Help Log On			
_			
	Installation	The Avaya Installation Wizard allows you to quickly install your system.	Launch Avaya Installation Wizard
		The Avaya Network Region Wizard allows you to quickly administer network regions.	Launch Avava Network Region Wizard
	Administration	The Native Configuration Manager allows you to administer this system using a graphically enhanced SAT applet.	Launch Native Configuration Manager
	Maintenance	The Maintenance Web Interface allows you to maintain, troubleshoot, and configure the media server.	Launch Maintenance Web Interface
	Upgrade	The Upgrade Tool allows you to upgrade all servers, Survivable Processors, G700 Media Gateways, and G350 Media Gateways.	Launch Upgrade Tool
		© 2004 Avaya Inc. All Rights Reserved.	
			*
http://www.avaya.com/			🔒 🎯 Local Intranet 🥼

A main menu is presented along the left hand side of the screen. In the **Alarms** section, click on **SNMP Traps.**



In the SNMP Traps page, click the Add button to add the trap destination and SNMP version.



CRK; Reviewed: SPOC 10/24/2006

Solution & Interoperability Test Lab Application Notes ©2006 Avaya Inc. All Rights Reserved. 5 of 19 Netcool-SNMP.doc In the Add Trap Destination screen, enter the IP address of the Netcool/OMNIbus server (i.e., 192.45.80.59) and enable this SNMP trap destination. To enable SNMP version 1, click the SNMP version 1 box, and provide the community string for the Community name field. Click the Add button at the bottom of the screen to complete the trap configuration for SNMP version 1. To enable SNMP version 2c, click the SNMP version 2c box, select a notification type, and provide the community string for the Community name field. Click the bottom of the screen to complete the trap configuration 2 box, select a notification type, and provide the community string for the Community name field. Click the Add button at the bottom of the screen to complete the trap configuration for SNMP version 2.



The following screen displays the trap information after the trap configuration is completed. The notification type field for version 2c is set to **trap**. The community name for version 1 and 2c is set to **public**.



The **SNMP Traps** configuration allows the Avaya Media Server to send traps for alarms raised by Avaya Communication Manager and alarms related to the media server's operating system and support software. Avaya Communication Manager running on the S8700 Media Server detects internal failures in the G650 Media Gateway and sends all traps when it controls a G650 Media Gateway. Avaya Communication Manager running on the S8300 Media Server detects internal failures in the G350 Media Gateway and sends all traps to the SNMP trap destination.

3.2. Firewall Configuration

The firewall in the Avaya Media Server must allow SNMP traps to be sent on UDP port 162. Click on the **Firewall** option in the Security section of the menu to display the Firewall page. Click on the **Output from Server** checkbox (2nd column) for **snmptrap 162/udp** and click the **Submit** button to submit the form. This is the only port that needs to be enabled for the media server to send SNMP traps. For an S8700 Media Server pair, the Firewall configuration should be performed on each media server.

58700TOP - Microsoft Internet Ex	plorer						
Elle Edit View Favorites Tools	Help						12
4-Back + ⇒ - 🙆 🛃 🖓 🕄	iearch 💽 F	avorites	@Meda 🎯 🗟				
Address () https://192.45.80.214/ogi-b	in/logged_in					2	· @60
AVAYA					In	tegrated Manage Maintenance Web I	ment Pages
Help Exit				٦	his Server: [1] S8700TOP	Duplicate Server: [2] S8	700BOT
Netstat Modem Test Network Time Sync Server Status Summary Process Status Interchange Servers Busy-out Server Release Server Shutdown Server Server Date/Time Software Version Server Configuration Configure Server	The Firew. LAN interf automatic	ewall all Web pe ace to the ally disabl ARNING peration o elp. it	age lets you enab Avaya media se led. : Some network : if or access to the	le network services on t rver. Unselected service services are required for e server.For additional d	he corporate s are proper etails, click		4
Restore Defaults Eject CD-ROM Server Upgrades Pre Upgrade Step Manage Software	Input to Server	Output from Server	Service	Port/Protocol			
Make Upgrade Permanent Boot Partition	R	R	ftp	21/tcp			- 11
IPSI Firmware Upgrades IPSI Version	1	2	ssh	22/tcp			
Download 1P51 Firmware Download Status	2	N	telnet	23/top			
Activate IPSI Upgrade		2	domain	53/udp			
Data Backup/Restore			bootps	67/udp			
Backup Now Backup History			bootpc	68/udp			
Schedule Backup Backup Logs			tftp	69/udp			
View/Restore Data Restore History		2	http	80/tep			
Format PC Card	2	2	oto	123/uda			
Nodem			60000	161/udo			
Server Access License File			secontrae	162/udp			
Authentication File			simpoap	102/000			
Tripwire		M	nttps	44-3ytop			
Install Root Certificate			syslog	514/UOp			
SSH Keys Ethernet Switch Ports	M		hp-sshd	2222/tcp			
Media Gateways Configuration	~		secure-sat	5022/tcp			
Miscellaneous File Synchronization	N N	হ	def-sat echo-request	5023/tcp 8/icmp			
Download Files							
CM Phone Message File Serial Numbers	Submit		Advanced Setti	ing Help			

3.3. Configuring Alarm Reporting Options

Ensure that the alarms the customer would like to have reported to Netcool/OMNIbus have not been downgraded to a warning alarm; otherwise, these alarms will not be reported via an SNMP trap. Log in to the Avaya Communication Manager SAT, and enter the **set options** command to display the ALARM REPORTING OPTIONS form, and check the Major and Minor columns for each alarm type. In summary, if the Major or Minor column is set to **[w]**arning, **[r]**eporting, or **[n]**o, then that alarm type has either been downgraded to warning severity or alarm reporting has been suppressed. However, if the column is set to **[y]**es or **[m]**inor, then an SNMP trap is sent. See reference [1] for more details on the **set options** form.

	-	1 6	0.0
set options	Page	l oi	22
ALARM REPORTING OPTIONS			
Major	Minor		
On-board Station Alarms: y	У		
Off-board Station Alarms: y	У		
On-board Trunk Alarms (Alarm Group 1): y	У		
Off-board Trunk Alarms (Alarm Group 1): y	У		
On-board Trunk Alarms (Alarm Group 2): w	W		
Off-board Trunk Alarms (Alarm Group 2): w	W		
On-board Trunk Alarms (Alarm Group 3): w	W		
Off-board Trunk Alarms (Alarm Group 3): w	W		
On-board Trunk Alarms (Alarm Group 4): w	W		
Off-board Trunk Alarms (Alarm Group 4): w	W		
On-board Adjunct Link Alarms: y	У		
Off-board Adjunct Link Alarms: y	У		
Off-board MASI Link Alarms:	У		
Off-board DS1 Alarms: y	У		
Off-board TCP/IP Link Alarms: y	У		
Off-board Alarms (Other): y	У		
Off-board ATM Network Alarms:	У		

Page 2 of the set options form continues with the alarm reporting options for other alarm types, such as Signaling Group alarms.

set options		Page	2 of	22
	ALARM REPORTING OPTIONS			
	Major	Minor		
	Off-board Firmware Download Alarms:	v		
		1		
	Off-board Signaling Group Alarms:	У		
	Remote Max Alarms:	У		
	Off-board Firmware Download Alarms: Off-board Signaling Group Alarms: Remote Max Alarms:	У У У		

4. Avaya G350 Media Gateway Configuration

This section describes the procedure for configuring the Avaya G350 Media Gateway to report alarms to an SNMP trap destination. As a default, the Avaya G350 Media Gateway forwards all alarms to the media server. In the compliance test, the Avaya G350 Media Gateway registered with the Avaya S8300 Media Server, which was configured as an independent call server (i.e., not a Local Survivable Processor). All alarms were sent to the Avaya S8300 Media Server (192.45.81.11). An administrator may configure another SNMP trap destination by using the following command:

G350-001(super)# snmp-server host <host-addr> <traps|informs> <v1|v2c> <community-name>

The following screen, obtained from the Command Line Interface of the Avaya G350 Media Gateway, displays the SNMP trap configuration used for the compliance test.

```
G350-001(super) # sh snmp
Authentication trap disabled
Community-Access Community-String
_____
              _____
read-only
              ****
              * * * * *
read-write
SNMPv3 Notifications Status
_____
Traps: Enabled
Informs: Enabled Retries: 3 Timeout: 3 seconds
SNMP-Rec-Address Model Level Notification Trap/Inform User name
192.45.81.11 v1 noauth all trap ReadCommN
UDP port: 162 DM
```

Solution & Interoperability Test Lab Application Notes ©2006 Avaya Inc. All Rights Reserved.

5. IBM Tivoli Netcool/OMNIbus Configuration

This section describes the procedure for configuring the Netcool/OMNIbus Event Management System to capture SNMP traps. The steps required are:

- Install the Flex license key file
- Install the Netcool Knowledge Library (NCKL) and the Avaya Integration Module for Netcool (IMN)
- Configure the Netcool Probe to receive SNMP traps on UDP port 162
- Configure the Netcool ObjectServer
- Start the Netcool/OMNIbus applications in Windows Services
- Start the Netcool Desktop application to view alerts in the ObjectServer.

All the components were installed and configured by an IBM engineer, prior to the compliance test.

5.1. Install Flex License Key File

Obtain the Flex license keys from IBM Technical Support and copy it to the license.lic file in the C:\Program Files\Netcool\common\license\etc directory. Verify that there is only one file with the .lic extension in this directory. Edit the file and verify the information on the SERVER line in the file. This line should specify the hostname (or IP address) and MAC address of the server where the Flex License Manager is running. The Flex License Manager communicates with other Netcool/OMNIbus applications on TCP port 27000. The format of the SERVER line is: SERVER <Hostname/IP Address> <MAC Address> 27000

The following screen displays the content of a sample license file. Restart the Flex License Manager after copying the license file to the aforementioned directory. The license manager log file, license.log, is located in the C:\Program Files\Netcool\common\license\log directory and can aid in troubleshooting problems where the Netcool applications fail to start.

Note: The license keys are generated for the MAC address of the NIC on the Netcool/OMNIbus server.

```
SERVER 192.45.80.59 000cflaa51ce 27000
VENDOR netcool
USE_SERVER
FEATURE nco_event_nt netcool 20030430 11-apr-2004 10 ck=209 \
SIGN=3B282736318A
FEATURE nco_ove_nt netcool 20030430 11-apr-2004 10 ck=187 \
SIGN=FF63BF9C160E
FEATURE nco_users_nt netcool 20030430 11-apr-2004 10 ck=25 \
SIGN=CF68BF4E400C
FEATURE nco_nco_nt netcool 20030430 11-apr-2004 10 ck=194 \
SIGN=A607F092429C
FEATURE nco_p_mttrapd netcool 20030430 11-apr-2004 10 ck=147 \
SIGN=8B52B50A887C
FEATURE nco_objserv netcool 20030430 11-apr-2004 10 ck=161 \
```

Solution & Interoperability Test Lab Application Notes ©2006 Avaya Inc. All Rights Reserved. 11 of 19 Netcool-SNMP.doc

```
SIGN=2B56AF767778
FEATURE nco_ov_nt netcool 20030430 11-apr-2004 10 ck=170 \
SIGN=D0B9EB709AD6
```

5.2. Install the Netcool Knowledge Library (NcKL) and the Avaya Integration Module for Netcool

The traps that the Avaya Media Servers and Gateways are capable of sending are defined in the Avaya SNMP MIBs. The IBM Tivoli Netcool Technology Program has developed an integration package that is available from IBM Technical Support. The integration package has been tested and validated by IBM Tivoli release engineering, and the package and documentation are available from the IBM Open Process Automation Library (OPAL). The rules file defines how the probe should process Avaya event data to create meaningful Netcool/OMNIbus alerts, and the lookup file assigns values to variables used in the rules file.

The Netcool Knowledge Library installation instructions are described in detail in the installation document that comes with the package. The datasheet for the Avaya Communication Manager IMN describes the required steps to include the rules and lookup files from the integration into the Netcool Knowledge Library.

5.3. Configure the Netcool SNMP Probe

The Probe properties file defines the environment in which the probe runs. For example, it includes the location of the rules file, the UDP port on which SNMP traps are received, and the ObjectServer name, amongst other parameters. The mttrapd.props property file contains all of the probe's default parameter settings (lines commented out) and is located in the C:\Program Files\Netcool\etc\rules directory. To override a value, add a line at the end of the file with the parameter name, followed by a colon, and then the parameter value. The following screen shows an example of the **RulesFile** parameter being overridden.

Verify that all of the default settings are being used, including UDP port 162, the ObjectServer name "NCOMS", and the default path to the rules file. The default probe rules file is called mttrapd.rules and it is located in the C:\Program Files\Netcool\etc\rules directory.

Note: The probe must be configured to read the snmptrap.rules file in the Netcool Knowledge Library directory. The default path for the Netcool Knowledge Library is C:\Program Files\Netcool\etc\rules.

5.4. Configure the Netcool ObjectServer

To access the Server Editor, select Start→Programs→Netcool OMNIbus→System Utilities→ Server Editor. The ObjectServer configuration specifies the host name (or IP address) and port number that the Probe and the Desktop clients should use to establish a connection to the ObjectServer. Two entries, indexed by the ObjectServer's name (e.g., NCOMS), were created during the installation and should be checked for appropriate values. The ObjectServer's configuration details can be updated through the Server Editor. There should be two entries in the Server Editor for the ObjectServer, a client entry and a listener entry. The client entry, highlighted in Figure 2, specifies the host name (or IP address) and port number that the SNMP Probe and Desktop clients should use to connect to the ObjectServer. The Listener entry, highlighted in Figure 3, is used by the ObjectServer to respond to client requests. For the client and listener entries, the IP address of the server machine, 192.45.80.59 and TCP port number 4100 were specified.

<u>S</u> erver	Host	Port SS	SL Driver
ICOMS cube		4100	Winsock TCP/IP
Listeners: cube	3	4100	Winsock TCP/IP
Server 🦵 Listener	□ SSL		Priority -
Server 🦵 Listener NCOMS	□	100 💽 🔤 Ad	d Priority
Server Г Listener Name: NCOMS Lost: cube	└ SSL → Port 4	100 💌 🔤 🖂	d Priority Raise Lower
Server 「」Listener Name: NCOMS Host: Coube Qriver: Winsock TCP/	r SST ▲ Fort 4	100 💌 Ad	d Priority <u>Raise</u> Lower st Show <u>G</u> roups

Figure 2: Server Editor (Client Entry)

Netcool/OMNIbus S	erver Editor			
<u>S</u> erver	Host	Port	SSL	Driver
NCOMS cube Listeners: cube		4100 4100		Winsock TCP/IP Winsock TCP/IP
Server J Listener	□ <u>5</u> SL		6dd	Priority
		I _B	emo⊻e	Lower
Driver: Winsock TCP/IF	>	-	Iest	Groups
		1		

Figure 3: Server Editor (Listener Entry)

5.5. Start the Netcool/OMNIbus Applications

After the installation of the Netcool/OMNIbus software, the following three Components are added to the Windows Services.

- NCO MTTrapD Probe
- NCO Object Server
- Netcool Flex License Manager

These software components need to be running, as indicated by the **started** state in **Figure 4**, to capture and view SNMP traps. To check the process, navigate to **Start** \rightarrow **Settings** \rightarrow **Control Panel**, select **Administrative Tools**, and select **Services**. To start the applications manually, they must be started in the following order: Flex License Manager, Object Server, and then MTTrapD Probe. If any of the Netcool/OMNIbus applications fail to start, check the license key file.

Services					_ 0	×
<u>Action</u> <u>V</u> iew	← → 🖮 💽 🚰 🔮 🗉	3 😫] ▶ ■ ॥ ■>				
Tree	Name 🛆	Description	Status	Startup Type	Log On As	
Services (Local)	🖏 Logical Disk Manager Admini	Administrative service for disk management r		Manual	LocalSystem	
9 1 9	McAfee Framework Service	Shared component framework for McAfee pr	Started	Automatic	LocalSystem	
	🆓 Messenger	Sends and receives messages transmitted by		Disabled	LocalSystem	
l í	NCO MTTrapD Probe		Started	Manual	LocalSystem	
ļļļ	NCO Object Server	Netcool OMNIbus ObjectServer	Started	Manual	LocalSystem	
	Net Logon	Supports pass-through authentication of acc		Manual	LocalSystem	
(Netcool Flex License Manager	Flex License server for Netcool Product Suite.	Started) Automatic	LocalSystem	
	NetMeeting Remote Deskto	Allows authorized people to remotely access		Manual	LocalSystem	
	Network Associates McShield		Started	Automatic	LocalSystem	-1
]/49		<u></u>	• • •		

Figure 4: Netcool/OMNIbus Applications in Windows Services

CRK; Reviewed:	
SPOC 10/24/2006	

Solution & Interoperability Test Lab Application Notes ©2006 Avaya Inc. All Rights Reserved. 14 of 19 Netcool-SNMP.doc

5.6. Start the Event List Application

The alert or event information stored in the Netcool ObjectServer can be viewed through the Event List application in the Desktop Tools. To start the Event List application, select **Start→Programs→Netcool OMNIbus→Event List**. Log in with the appropriate username and password. In the Event List Login window, specify the ObjectServer to connect to, which is NCOMS in this case. Click on the **OK** button.

\approx	Please enter your Username and Password to continue.
Username:	Jroot
Password:	жинин
Server:	NCOMS
361761.	

Figure 5: Event List Login Window

After logging in, the Monitor Box window is displayed, as shown in **Figure 6**. The Monitor Box window contains monitor boxes that represent a list of events that match a particular criteria or filter. A monitor box is identified by its name located at the top of each monitor box, such as "All Events" or events captured in the "Last 10 Min...". To view the event information for a particular monitor box, click on the ellipsis button. The Event List illustrated in **Figure 7** is displayed.



Figure 6: Event List - Monitor Box Window

Netcool/O	MNIbus E	vent List : Filter="	Avaya CM"	, View="Defaul	t"				
Ele Edit Vew	Alerts	Cools Help							
😫 🗮 🗖	ð 📥	Ауауа СМ	- Q	Default		¥	○ ↑ To	p[OFF] 🛛 💡	
Node	Count			Summary		Last Occurrence	Alert Group	Alert Key	Type
S8700T0P	2	0S1 ISBN Trunk Ala	m (Eabinet:	01, Carrier A, Slot:	07, Port; 22)	17/07/2006 21:14:15	ISDN-TRK	Cabinet 01, Carier A, Slot 07, Port 22	Problem
S8700T0P	2	DS1 ISBN Trunk Ala	m (Cabinet:	01, Carrier A, Slot:	07, Port 23)	17/07/2006 21:14:15	ISDN-TRK	Cabinet 01, Carier A, Slot 07, Port 23	Problem
\$8700TOP	2	ISON-PRI Signaling L	ink Port Alam	n (Cabinat 01, Ca	nier: A, Slot 07, Port 24]	17/07/2006 21:14:15	ISDN-PLK	Cabinet 01, Carrier: A. Slot 07, Port 24	Problem
\$8700T0P		End of ISDN-PRI Sig	paling Link P	ort Alarm [Cabinel	01, Carrier, A. Slot: 07, .	17/07/2006 21 07:33	ISDN-PLK	Cabinet: 01, Carrier: A, Slot 07, Port 24	Resolution
\$8700T0P		UDS1 Interface Circu	it Pack Alam	(Dabinet: 01, Dan	ie: A. Slot: 09)	17/07/2006 21:09:33	UDS1-BD	Cabinet 01, Carrier: A. Slot 09	Problem
S870010P	1	End of: UDS1 Interfa	ce Circuit Pac	k Alam Cabinet	01, Carrier: A, Slot 09	17/07/2006 21 09:33	UDS1-BD	Cabinet 01, Carrier: A, Slot 03	Resolution
58/0010P	2	UDS1 Interface Circu	it Pack Alam	Cabinet: 01, Can	ec A, Slot: 10]	17/07/2006 21:09:33	0051-80	Cabinet 01, Camer A, Slot 10	Problem
58/0010P	2	0051 Intellace Circu	I Pack Alem	Cabinet: 01, Can	ec A, 500(10)	1770772006 21:09:33	0051-8D	Cabinet 01, Caner: A, Slot 10	Phoblem
56/0010P		End of UDS1 Interta	ce Circuit Pac	A Marn [Cabinet	01, Caffer: A. Slot: 10	1770772006/21302:33	0051-80	Cabinet 01, Caner, A. Slot 10	necolution
SBRUUTUP		UDST Interface Lincu	it Pack /Marm	Cabinet UIL Can	et A. Slot: 12]	1770772305/2757:13	0051-80	Cabinet UL Camer: A. Slot 12	mobiem
58/0010P	2	UDST Intenace Cacu	r Pack Alam	Labriet UI, Can	ec A, 510(:12]	17/07/2006 21:11:40	UDS1-8D	Cabinet 01, Caner: A. Slot 12	Problem
SB/0010P	4	UDST Interace Circu	I Pack Alam	(Labinet UI, Can	RCA. 500(12)	177077200521:11:40	0051-80	Cabinet 01, Caner: A. Slot 12	Problem
000000000		LID 64 June 6 Circuit	2 Deals Allera	Code and Colored	UT. Certer: ALSIOC 12	17/07/2005 21:07:33	UDG1-BD	Cabinet 01, Carler A, Slot 12	Debler
50700TUP		UDST Interace Circu	Pack Alam	Cabinet Of Car	ies A. Sibt 12.)	17/07/2006 21:08:33	UDS1-8D	Cabinet 01, Carley & Slot 12	Picolem
SBYOUTUP		UDST Interace Citto	Pack Alam	(cabinet of . can	REALSHOCTS]	1770772006 21:03:33	0051-80	Cabinet 01, Canier, A, Slot 13	Problem
-0200.1		Madia Catavan Alar	(Det. 001)	watern Eusennet	or, Cener, A. SICC (3)	17/07/2008 21:07:33	NED CTWAY	Reg 001	Dahlan
-9300-1		Media Gateway Man	CPat Off			17/07/2006 20:58:38	MEDIGTWY	Pole 001	Protein
+00001		Fod at Made Cater	a Mars 1 Da	+ 0213		17/07/2006 20:07:40	MEDICTWA	Pole 001	Procent
+9200.1	2	DC1 Interface Marks	Modele Alam	(Dat (005/4)		17/07/2006 21:00:39	MG-DG1	Port 001M4	Dahlen
-03001	2	East at: DC1 Isherback	Media Medi	A Alam (Pat 00	Set 5	17/07/2006 21:00:35	MG-DOT	Day 0/1/4	Protein
v9300.1	2	Dicital Line Media Mr	date Alarm 1	Part: 000/001		17/07/2005 20:59:59	MGLDCP	Port 001WS	Dashiera
100001		East of Digital Line M	adio Madrif (Name I Post 00145		12/02/2006 20:50:50	MGLOCP	Date 0011/C	Productin
45300-1	1	Integrated Againg Ma	dia Module A	Inth LEast 000V7		17/07/2005 20:58:38	MG-IAMM	Port 001V7	Panhiero
48300-1		End of Integrated An	alog Media M	Inchile Alarm I Port	008/21	17/07/2005 20:58:38	MG-IAMM	Port 001V7	Resolution
SSZORTOP		LAE Services Session	Alam (Pat-	01.1		12/02/2005 21:02:10	AESWISES	Port 01	Paphiem
\$870010P	1	AE Services Session	Alarm (Port:	011		17/07/2006 20:30:41	AESW-SES	Pot 01	Paphiem
S8700TOP	1	End of AE Services	Section Alarn	For 011		17/07/2005 20:30:41	AESVISES	Fot 01	Resolution
\$8700TOP		IP Server Interface A	am (Port 0)	1A.1		17/07/2006 21:07:33	IP/SVB	Port 01A	Problem
\$870010P		End of IP Server live	riace Alam I	Port DIA I		17/07/2005 21:08:10	IP/SVB	Port 01A	Resolution
S8700T0P	1	AE Service: Session	Alarm [Part:	021		17/07/2006 21:02:10	AESV-SES	Port 02	Problem
\$8700T0P	1	AE Services Session	Alarm [Port:	02)		17/07/2006 20:30:41	AESV-SES	Port 02	Problem
S8700T0P	1	End of AE Services	Section Alarm	[Port 02]		17/07/2005 20:30.41	ABSV SES	Port 02	Resolution
<						17 07 0000 00 00 00	- Longer		>
	57		0		44	15		11	0
row selected					19/09/2006 21:23:55	root		CUBE [PR1]	
								,	

Figure 7: Event List Window

The Event List displays event information in a scrollable list that is color-coded based on the severity of the alert or event. The colors and severity levels supported by Netcool/OMNIbus are summarized in **Table 1**. Events captured by the Netcool Probe are assigned a severity in the rules file generated in Section 5.2. For more information on using the Event List application, refer to reference [5].

Severity	Description	Desktop Color
5	Critical	Red
4	Major	Orange
3	Minor	Yellow
2	Informational	Blue
1	Indeterminate	Purple
0	Clear	Green

Table 1: Netcool/OMNIbus Severity Levels

6. Interoperability Compliance Testing

The objective of the interoperability compliance test was to verify that the Netcool/OMNIbus Event Management System could receive v1 and v2c SNMP traps from the Avaya G350 Media Gateway, Avaya S8300 and S8700 Media Servers. The collected SNMP traps were viewed with the Netcool Event List application.

6.1. General Test Approach

All test cases were performed manually. The general test approach used for the compliance testing included:

- Generating v1 and v2c SNMP traps from the Avaya S8300 and S8700 Media Servers.
- Using a protocol analyzer to verify that SNMP traps were sent from the Avaya Media Servers to the Netcool/OMNIbus system.
- Viewing the SNMP traps with the Netcool Desktop application.

6.2. Test Results

All tests were completed successfully. Netcool/OMNIbus successfully captured and processed the event information sent by the Avaya Media Servers and Gateways using v1and v2c SNMP traps. Importing the Avaya SNMP MIBs using a Netcool rules file is necessary to achieve interoperability between the Avaya Media Servers and Gateways and Netcool/OMNIbus. The customer should contact IBM Technical Support for assistance in developing the trap rules.

7. Verification Steps

To verify the network management solution using the Netcool/OMNIbus Event Management System to capture SNMP traps from the Avaya Media Servers and Gateways, the following steps were performed:

- Check IP communication between the Avaya Media Servers and Gateways and Netcool/OMNIbus server using the "ping" command.
- Verify that the Netcool/OMNIbus applications are running under Windows Services.
- Generate an event or alarm, such as restarting the Master SNMP Agent on the web interface, from each Avaya Media Server and Gateway and verify that the SNMP trap was received. A protocol analyzer may be used to verify that the Avaya Media Server sent the SNMP trap to the Netcool/OMNIbus server.

If the event or alarm is not displayed in the Netcool Event List, check the following items:

- Check that the Event List application is not incorrectly filtering out events/alarms.
- Check that the alarm reporting options in the Avaya Communication Manager set options form are allowing the appropriate alarms to be reported.
- Check the SNMP trap destinations in the Avaya Media Servers and Gateways.
- Check that the firewall in the Avaya Media Server is allowing SNMP traps to be sent on UDP port 162.
- Check that the SNMP Probe is listening for SNMP traps on UDP port 162.
- Using a protocol analyzer, check whether the SNMP trap is sent to the Netcool/OMNIbus server.

8. Support

Technical support for the IBM Tivoli Netcool/OMNIbus Event Management System can be obtained by contacting the IBM Technical support via the support link at <u>askibm@vnet.ibm.com</u> or by calling the support telephone number at 1-800-IBM-SERV (1-800-426-7378).

9. Conclusion

These Application Notes illustrate the configuration steps required to enable the IBM Tivoli Netcool/OMNIbus Event Management System to monitor a network of Avaya Media Servers and Gateways for significant events and alarms. Compliance testing was successful as Netcool/OMNIbus captured v1 and v2c SNMP traps sent by the Avaya Media Servers and Gateways. Netcool/OMNIbus also processed the event information and displayed it in a meaningful way.

10. Additional References

This section references the Avaya and IBM Tivoli product documentation relevant to these Application Notes. The following Avaya product documentation can be found at <u>http://support.avaya.com</u>.

- [1] Maintenance Alarms for Avaya Communication Manager 3.1, Media Gateways and Servers, Issue 2, February 2006, 03-300430
- [2] Maintenance Commands for Avaya Communication Manager 3.1, Media Gateways and Servers, Issue 2, February 2006, 03-300431

The following IBM Tivoli product documentation was referenced during the interoperability compliance test. To acquire the following documentation, contact IBM technical support.

- [3] Netcool/OMNIbus 7.0.6 Installation and Deployment Guide
- [4] Netcool/OMNIbus 7.0.6 Administration Guide
- [5] Netcool/OMNIbus 7.0.6 User Guide
- [6] Micromuse Standards for Probe Rules Files

©2006 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by [®] and TM are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.