

Avaya Integrated Management Troubleshooting

November 2009

Contents

Chapter 1: Site Administration 5

File transfer using FTP fails in Voice Announcement Manager 5
Proposed Solution 6
Proposed Solution 2 7
Proposed Solution 3 8
File Transfer using SCP fails in Voice Announcement Manager 9
Proposed Solution 9
Proposed Solution 2 10
Site Administration features do not work correctly 12
Proposed Solution 12
Site Administration crashes corrupting the persist.dat file 13
Proposed Solution 13
Parsing UTF 8 files in Site Administration causes problems 14
Proposed Solution 14
Delay in executing commands on Communication Manager 15
Proposed Solution 15
Site Administration fails to execute saved import tasks 15
Proposed Solution 16

Chapter 2: Network Management 17

Devices in the Network Management Console tree view appear in red even when there are no alarms 17
Proposed Solution 18
Systemview gets hung or throws a heap space error 19
Proposed solution 19
Network Management Services do not auto-start 19
Proposed Solution 20
Network Management Installation fails when Postgres is not installed right 21
Proposed solution 22
Network Management Services hangs right at the start 23
Proposed Solution 23
Memory issues in Java while opening ENM Log Viewer 23
Proposed Solution 24
Devices not discovered in Network Management Console 25
Proposed Solution 25
A configuration problem does not allow TN boards to be discovered by Software Update Manager 26
Proposed Solution 26
Software Update Manager is not able to discover Communication Manager 27
Proposed Solution 27
Error while upgrading a device — incorrect SNMP parameters 28
Proposed Solution 28
Error while upgrading a device — incorrect SCP parameters 29
Proposed Solution 29
Proposed Solution 2 30

Chapter 3: Performance and Administration 31

Starting or stopping an MSA queue generates an error 31
Proposed Solution 32
Collection does not work right 32
Proposed Solution 33
Collection does not work – 2 33

Proposed Solution....33
The graphical user interface does not launch....34
Proposed Solution....35
Diskspace full....35
Proposed Solution 1....36
Proposed Solution 2....36
Proposed Solution 3....37
Proposed Solution 4....38

Index....39

Chapter 1: Site Administration

File transfer using FTP fails in Voice Announcement Manager

Integrated Management software component and version	Voice Announcement Manager
Installed versions (with service packs/ upgrade path) and other co-resident software with version	Voice Announcement Manager
Host operating system (Linux or Windows) version	All supported versions of Windows
Symptoms that identify the issue	a. During an FTP file transfer Voice Announcement Manager acts as an FTP client and the VAL source (VAL board or media gateway) acts as the FTP server. If FTP fails, the first step should be to find out whether the FTP server is up and running on the VAL source. You can check using the Windows command line with the command > ftp <name of the VAL source> or <IP address of the VAL source> b. Enabling File Transfer: Before testing file transfer through Windows FTP command on the VAL board or media gateway, file transfer should be enabled on the board. To enable file transfer: i. Log in to Communication Manager. ii. Run the command enable filexfer. iii. Enter the login and password iv. If you are using FTP then the secure option should be set to "n". The board address is the board name on which transfer has to be checked.

Note:

Once file transfer to the board/gateway is enabled, use the same login and password to open the FTP to the board. On the board, Announcement files are stored in the directory “r;annc”. After you verify the files transfer, disable the board with the command disable filexfer board <board name>. For the FTP transfer Voice Announcement Manager uses the Active and Passive transfer modes.

Cause of the issue There can be several reasons for FTP file transfer failures. The reasons could be related to network or other issues with a Voice Announcement Manager machine's firewall settings.

Active FTP: In the Active mode FTP, The FTP client (Voice Announcement Manager) does not open the data port on the client machine, it simply tells the server what port it is listening on and the server connects back to the specified port on the client. From the client side firewall this appears to be an outside system initiating a connection to an internal client which is blocked. To do a file transfer using FTP, the ports used are 20 (Data port) and 21 (Control port). The default firewall configuration on the client may not receive data from a server. The default configuration of the Windows Firewall can prevent commonly used applications from functioning.

Proposed Solution

Sometimes FTP file transfers fail in Voice Announcement Manager. The reasons could be related to network or other issues with a Voice Announcement Manager machine's firewall settings.

Prerequisites

Enabling the ports: You can add the program or the ports that a program uses to the Firewall's **Exceptions** list. - By default the **Windows Firewall** asks you if you want to add a program to the **Exceptions** list the first time you use the program. The system displays a message with three choices: **Keep Blocking**, **Unblock**, or **Ask Me Later**.

- **Keep Blocking**: Adds the application to the **Exceptions** list but in a **Disabled** state so that the ports are not opened. By adding the application to the **Exceptions** list, **Windows Firewall** does not prompt you every time it runs.
- **Unblock**: Adds the application to the **Exceptions** list in an **Enabled** state so that the ports are opened.
- **Ask Me Later**: Blocks unsolicited incoming traffic and does not add it to the **Exceptions** list.

The system prompts you again the next time the application is run. You may have installed an FTP client some time and while installing you may have selected the **Keep Blocking** option. In this case FTP through Voice Announcement Manager fails. The firewall policy contains

checks like FTP inbound and FTP outbound. Clearing this options unblocks these ports and allows ACTIVE FTP to work.

To unblock the ports:

1. Click **Start**, and then click **Control Panel**.
2. Double-click **Windows Firewall** (or click **Security Center** and then **Windows Firewall**).
3. In the **Windows Firewall** control panel, click the **Exceptions** tab.
4. Clear the **FTP inbound** and **FTP outbound** check boxes.
5. Click **OK**.

Proposed Solution 2

Sometimes FTP file transfers fail in Voice Announcement Manager. The reasons could be related to network or other issues with a Voice Announcement Manager machine's firewall settings.

Prerequisites

Enabling the ports: You can add the program or the ports that a program uses to the Firewall's **Exceptions** list. - By default the **Windows Firewall** asks you if you want to add a program to the **Exceptions** list the first time you use the program. The system displays a message with three choices: **Keep Blocking**, **Unblock**, or **Ask Me Later**.

- **Keep Blocking**: Adds the application to the **Exceptions** list but in a **Disabled** state so that the ports are not opened. By adding the application to the **Exceptions** list, **Windows Firewall** does not prompt you every time it runs.
- **Unblock**: Adds the application to the **Exceptions** list in an **Enabled** state so that the ports are opened.
- **Ask Me Later**: Blocks unsolicited incoming traffic and does not add it to the **Exceptions** list.

The system prompts you again the next time the application is run. You may have installed an FTP client some time and while installing you may have selected the **Keep Blocking** option. In this case, FTP through Voice Announcement Manager fails. The firewall policy contains checks like FTP inbound and FTP outbound. Clearing this options unblocks these ports and allows ACTIVE FTP to work.

To open a port in the Windows XP SP2 Firewall

1. Click **Start**, and then click **Control Panel**.
2. Double-click **Windows Firewall** (or click **Security Center** and then **Windows Firewall**).
3. In the `Windows Firewall` control panel, click the **Exceptions** tab.
4. Click **Add Port**.
5. For FTP, add two ports, 20 and 21
6. In the **Name** field, enter the Application followed by an underscore then the Port Type in uppercase followed by an underscore and then the port number TP_TCP_21
7. In the **Port number** field, enter the number being added. This should match the number entered in the **Name** field.
   21
8. Repeat steps 5 and 6 for port 20.
9. Select the radio button for TCP.
10. Click **OK** to add the port.
11. Click **OK** to close the **Windows Firewall** control panel.
12. Restart the computer to enable these choices.

Proposed Solution 3

Sometimes FTP file transfers fail in Voice Announcement Manager. The reasons could be related to network or other issues with a Voice Announcement Manager machine's firewall settings.

Prerequisites

Enabling the ports: You can add the program or the ports that a program uses to the Firewall's **Exceptions** list. - By default the **Windows Firewall** asks you if you want to add a program to the **Exceptions** list the first time you use the program. The system displays a message with three choices: **Keep Blocking**, **Unblock**, or **Ask Me Later**.

- **Keep Blocking**: Adds the application to the **Exceptions** list but in a **Disabled** state so that the ports are not opened. By adding the application to the **Exceptions** list, **Windows Firewall** does not prompt you every time it runs.
- **Unblock**: Adds the application to the **Exceptions** list in an **Enabled** state so that the ports are opened.
- **Ask Me Later**: Blocks unsolicited incoming traffic and does not add it to the **Exceptions** list.

The system prompts you again the next time the application is run. You may have installed an FTP client some time and while installing you may have selected the **Keep Blocking** option.

In this case, FTP through Voice Announcement Manager fails. The firewall policy contains checks like FTP inbound and FTP outbound. Clearing this options unblocks these ports and allows ACTIVE FTP to work.

Passive FTP In some cases if active FTP does not work, changing the FTP connection mode from ACTIVE to PASSIVE might help. This setting can be changed from inside Voice Announcement Manager.

1. Navigate to the menu **File > Edit Application Properties > FTP Connect Mode**.

   In the passive mode FTP the client initiates both connections to the server, solving the firewall problem.
2. Change the FTP mode from ACTIVE to PASSIVE .

Next steps

FTP Logs In Voice Announcement Manager, detailed FTP logs are available in the log files. To set it up:

Navigate to the menu **File > Edit Application properties > FTP Log** option

File Transfer using SCP fails in Voice Announcement Manager

Integrated Management software component and version	Voice Announcement Manager
Installed versions (with service packs/ upgrade path) and other co-resident software with version	Voice Announcement Manager
Host operating system (Linux or Windows) version	All supported versions of Windows
Symptoms that identify the issue	
Cause of the issue	

Proposed Solution

File Transfer using SCP fails in Voice Announcement Manager

Prerequisites

To transfer files on the media gateway through SCP, you need to set SNMP parameters in Voice Announcement Manager. To do that, you have to create a group and a user on the media gateway.

To open a port in the Windows XP SP2 Firewall

1. Click **Start**, and then click **Control Panel**.
2. Double-click **Windows Firewall** (or click **Security Center** and then **Windows Firewall**).
3. In the `Windows Firewall` control panel, click the **Exceptions** tab.
4. Click **Add Port**.
5. For SCP, add a port, 22
6. In the **Name** field, enter the Application followed by an underscore then the Port Type in uppercase followed by an underscore and then the port number
   TP_TCP_22
7. In the **Port number** field, enter the number being added. This should match the number entered in the **Name** field.
   22
8. Select the radio button for TCP.
9. Click **OK** to add the port.
10. Click **OK** to close the **Windows Firewall** control panel.
11. Restart the computer to enable these choices.

Proposed Solution 2

Prerequisites

To transfer files on the media gateway through SCP, you need to set SNMP parameters in Voice Announcement Manager. To do that, you have to create a group and a user on the media gateway.

To create a group on Mediagateway

1. Telnet to media gateway as root/root.
2. Depending on the security model, execute one of the following commands to create a group.

- Run the command snmp-server group v3AdminWriteG v3 auth read iso write iso notify iso
- If you are using the security model "No Authentication, No Privacy" then the permissions for the SNMP group you create on the media gateway should also change for group creation: snmp-server group v3AdminWriteNoAuthG v3 noauth read iso write iso notify iso

3. To create a user on Mediagateway — depending on the security model, execute the following commands to create a user.

Options	Description
Security model	Gateway CLI Command
Authentication, Privacy with md5	snmp-server user <MD5Admin3> v3AdminWriteG v3 auth md5 <abcd1234>priv des56 <1234abcd>
Authentication, Privacy with sha	snmp-server user <SHAAdmin4> v3AdminWriteG v3 auth sha<abcd12345>priv des56 <12345abcd>
Authentication, No Privacy with md5	snmp-server user <MD5Admin1> v3ReadWriteG v3 auth md5 <abcd1234>
Authentication, No Privacy with sha	snmp-server user <SHAAdmin2> v3ReadWriteG v3 auth sha <abcd12345>
No Authentication, No Privacy	snmp-server user <AdminNoauth3>v3AdminWriteNoAuthG v3

You create a group using the command snmp-server group v3AdminWriteG v3 auth read iso write iso notify iso. If you select the security model **Authentication No Privatization** then a user is created as snmp-server user asausr2 v3ReadWriteG v3 auth md5 pa55word. In this case `asausr2` is the user name and `pa55word` is the authentication password. While configuring the SCP server, enter the full path for the home directory. For example If the user created is "vam" then the path is `C:\Program Files\copSSH\home\vam`

Note:

If any of the file transfers using FTP, SFTP or SCP fails through Voice Announcement Manager then to verify whether it is a Voice Announcement Manager issue or network problem or firewall port blocking, use WinSCP. WinSCP is an open source SFTP, FTP, SCP client for Windows. Before testing file transfer through WinSCP on a VAL board or media gateway, file transfer should be enabled on the board. File transfer can be enabled with the command enable filexfer. The system may ask you for the login, password and board address on which transfer has to be checked. If you are using SFTP/SCP set `Y` for the secure option. Once the board is enabled, the same login and password can be used in WinSCP to connect to the board. On the board Announcement files are stored in the directory **r;annc**. After the files transfer verification

completes, the board must be disabled with the command disable filexfer board <board name>

Example

Next steps

For file transfers using SFTP, Port 22 is used. Follow similar steps as for FTP to unblock port 22

Site Administration features do not work correctly

Integrated Management software component and version	Site Administration (SA), any version
Installed versions (with service packs/ upgrade path) and other co-resident software and version	Any service pack
Host operating system (Linux or Windows) version	All supported version of Windows
Symptoms that identify the issue	Some features in Site Administration do not work.
Cause of the issue	Not known

Proposed Solution

Some features in Site Administration do not work. When you enable Trace , Site Administration shows data being transferred over OSSI/PCTT. This data is useful for analysis and troubleshooting.

1. . To enable Trace, create the following registry keys and values.

```
HKEY_CURRENT_USER\Software\Avaya\Avaya Site Administration
\Trace
DWORD Value: On
Data: 1
DWORD Value: Enabled
Data: 1
DWORD Value: Capacity
Data: 10000 (decimal)
```

After creating the above registry keys, Site Administration shows the **Trace** tab in the **Status** view.

2. From the context menu of the **Trace** tab, save the trace data to a .txt file.
3. Sent the text file to the Avaya support team for analysis and troubleshooting. The Site Administration engineers can enable Trace and analyze the Trace data.

Site Administration crashes corrupting the persist.dat file

Integrated Management software component and version	Site Administration (SA), any version
Installed versions (with service packs/ upgrade path) and other co-resident software and version	Site Administration version 5.0 or later
Host operating system (Linux or Windows) version	All supported version of Windows
Symptoms that identify the issue	None
Cause of the issue	The configuration file (persist.dat) is corrupted as a result of an application crash.

Proposed Solution

The configuration file (persist.dat) is corrupted as a result of a Site Administration crash.

1. Launch Site Administration.
   Every time Site Administration application closes successfully, it creates a backup of configuration data (persist.dat) in the `<SA_USER_FOLDER>\Backup` folder
2. Close and launch Site Administration again.
   Launching Site Administration again allows you to restore the configuration.
3. Access the **Backup** folder to restore the configuration.

Parsing UTF 8 files in Site Administration causes problems

Integrated Management software component and version	Site Administration (SA)
Installed versions (with service packs/ upgrade path) and other co-resident software and version	Site Administration version 5.0 Service pack 6.0
Host operating system (Linux or Windows) version	All supported version of Windows
Symptoms that identify the issue	While parsing the UTF 8 files because of the Byte Order Mark at the start of the files the scripts do not process data correctly.
Cause of the issue	When you generate files using the Export wizard, Site Administration saves the file in the UTF 8 format. As part of the UTF 8 format, Site Administration writes Byte Order Mark (BOM) of 3 bytes (EF BB BF) at the start of the file. You can use these files generated by Site Administration as an input to run different scripts for processing data.

Proposed Solution

When you generate files using the Export wizard, Site Administration saves the file in the UTF 8 format. As part of the UTF 8 format, Site Administration writes Byte Order Mark (BOM) of 3 bytes (EF BB BF) at the start of the file. You can use these files generated by Site Administration as an input to run different scripts for processing data. While parsing the UTF 8 files because of the Byte Order Mark at the start of the files the scripts do not process data correctly.

1. Navigate to the **Tools> Options > Export** tab.
2. While exporting a file, select to save the file in the ANSI format.

   Site Administration allows you to select the file encoding type between UTF 8 and ANSI

Delay in executing commands on Communication Manager

Integrated Management software component and version	Site Administration (SA)
Installed versions (with service packs/ upgrade path) and other co-resident software and version	Site Administration version 5.0
Host operating system (Linux or Windows) version	All supported version of Windows
Symptoms that identify the issue	When you use the Import and Export wizard, the commands take considerable time to complete when dealing with a large volume of data.
Cause of the issue	Till Site Administration 5.2, the default value for the command delay was 500ms.

Proposed Solution

When you use the Import and Export wizard, the commands take considerable time to complete when dealing with a large volume of data. This is caused by a delay in executing commands on Communication Manager

1. Navigate to the **System > Properties > Connections** tab.
2. Click the **Properties** button for the selected Connection ID.
3. Under the **Advanced** tab, change the value for the **Command (ms):** field.
   In Site Administration version 5.2, the default value has been reduced to 50ms

Site Administration fails to execute saved import tasks

In case of sequential upgrades from older Site Administration versions to newer ones, Site Administration sometimes fails to execute the saved import tasks.

Integrated Management software component and version.	All Site Administration (SA)

Installed versions (with service packs/ upgrade path) and other co-resident software and version	Any service pack
Host operating system (Linux or Windows) version	All supported versions of Windows
Symptoms that identify the issue	Site Administration sometimes fails to execute the saved Import tasks.
Cause of the issue	Incorrect configuration settings that affect an upgrade

Proposed Solution

During sequential upgrades from older to newer versions, Site Administration sometimes fails to execute saved imported tasks.

1. To resolve this issue, go to the Image wizard.
2. Select an object.
3. Select **Restore Column Order**.

Chapter 2: Network Management

Devices in the Network Management Console tree view appear in red even when there are no alarms

Devices in the Network Management Console tree view do not reflect the correct fault monitoring status. The color of the gateways and Communication Manager applications in the Network Management Console tree view are always red even when there are no alarms or faults.

Integrated Management software component and version	Network Management Console (NMC)
Installed versions (with service packs/ upgrade path) and other co-resident software with version	Network Management Console 4.0 SP 3
Host operating system (Linux or Windows) version	All supported versions of Windows, applicable to both — VMWare and physical machines.

Symptoms that identify the issue	When you run a fresh discovery, and immediately observe the map, all the devices (which are in no alarm state) are in green. Once the nFaultmon polling starts, one by one, the devices in the map start turning red
	When you run a SNMP `Get Request` the MIB item `cmgModuleList` throws an error.
	`avaya.snmp.SNMP_Exception: SNMP Error: Timeout (No error index reported)`
	`Requested vars: [(null : null) <--- (. 1.3.6.1.4.1.6889.2.9.1.1.8.0 : null)]à [Note] This is CMG MIB "cmgModuleList"; which is not accessible`
	`Vars of attempted PDU: [(. 1.3.6.1.4.1.6889.2.9.1.1.8.0 : null)]`

- The G3 MIB does not report the status of following MIB items correctly.

```
avaya.snmp.SNMP_Exception: (.
1.3.6.1.4.1.6889.2.8.1.6.5.0 : null): SNMP Error: No
Such Name
 Requested vars: [(null : null) <--- (.
1.3.6.1.4.1.6889.2.8.1.6.5.0 : null)]
à[Shirish]1.3.6.1.4.1.6889.2.8.1.6.5.0 This is a Gauge
object in the g3Health MIB; it contains the number of
logged major alarms, which is returning a null (ideally
it should be a numeric)
 Vars of attempted PDU: [(.
1.3.6.1.4.1.6889.2.8.1.6.5.0 : null)]
            at
avaya.snmp.SNMP_Session.performRequest(Unknown Source)
```

Proposed Solution

1. Check the `nfaultmon` logs to see if `NFaultmon` reaches all the devices that are managed in Network Management Console. You can verify this by reading the `nfaultmon` logs to see if there are SNMP exceptions.
2. If there are SNMP exceptions in the log file, then check the SNMP parameters for the specific devices for correctness with the help of an MIB Browser.
   The firewall may have perceived the faultmon traffic as port scanning and blocked the ping traffic.
3. If the MIB results are correct for the specified credentials, then proceed with killing the `nFaultmon` process in the Task Manager.

   Note:

   The `nFaultmon` process is an Auto Start process, and needs no restart of the cvserver.

4. Even after working the steps above, if the status of the devices status is red, then there could be a network configuration issue

   An internal firewall could be blocking ping packets initiated by ENM `nFaultmon`.
5. Redo the network configuration settings.

   The firewall should not block the SNMP and ping packets originating from `nFaultmon`.

Systemview gets hung or throws a heap space error

Integrated Management software component and version	Network Management Console (NMC) any version
Installed versions (with service packs/ upgrade path) and other co-resident software and version	Network Management Console 5.0 SP 2
Host operating system (Linux or Windows) version	All supported versions of Windows, applicable to both — VMWare and physical machines.
Symptoms that identify the issue	The Systemview progress bar stops after 20 minutes.
Cause of the issue	If there are too many Communication Manager applications (>= 25), the JVM heap memory for Systemview gets exhausted.

Proposed solution

1. Find out the number of Communication Manager applications, IP phones/Non IP phones, port networks in the customer environment.
2. If the number of devices mentioned in Step 1appears to be large, then check the `Systemview.prl` file for the amount of JVM space allocated (default is 64 MB) for the devices to run.
3. Increase the JVM heap size for Systemview by adding the following keyword - `Xmx500M` in the $commandLine. $commandLine = "$cv_dir/jre/bin/java -Xmx500M $lul_dir...
4. Run IP Discovery.

Network Management Services do not auto-start

On a Network Management Windows system, when you restart the system, Network Management Services do not get automatically restarted.

Integrated Management software component	Network Management
Installed versions (with service packs/ upgrade path) and other co-resident software with version	Network Management 4.0.124 + VMM & (No Network Management 4.0 SP) + Network Management 5.0.13 + SP2 + SP3 + VMM. Then VMM is uninstalled.
Host operating system (Linux or Windows) version	All supported versions of Windows, applicable to both — VMWare and physical machines.
Symptoms of the issue	When you restart the system, Network Management Services do not get automatically restarted.
Cause of the issue	You may be unaware of the upgrade/installation path. Scanning the Windows Registry shows the installation/upgrade path. If Network Management 3.1 traces are also seen in the Registry, this is acceptable as the Registry updates are not made in Network Management 5.0 The VMM Uninstallation may not have happened properly (there maybe VMM related traces of System Variables and other service related entries). So if there are VMM entries in the registry then please check the Registry entries under `HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Services\`.

Proposed Solution

On a Network Management Windows system, when you restart the system, Network Management Services do not get automatically restarted.

1. Check JBoss, pgsql8.1 & cvserver to see if auto-start of Network Management Services does not happen because of the interdependency of services
   A Registry Trace of the above services will appear under `HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Services\` in the Windows Registry of your system.
2. Check the following entries in the Registry Key values for the following services (including the details of the following keys Enum & Security also) in registry under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\`

   - pgsql8.1 - ActiveMQ
   - AvayaCS
   - AvayaDECM-4r-1
   - AvayaJBoss404
   - AvayaJBossPIM
   - cvserver (most importantly)

3. Create a dependency of the windows service `pgsql-8.x` on the following. Dependency of `pgsql8.3` in Network Management 5.2 and `pgsql-8.1` in Network Management 4.0/5.0 for the Windows Service `AvayaJBoss404`. Dependency of `pgsql8.3 à` in Network Management 5.2 and `pgsql-8.1 à` in Network Management 4.0/5.0 for the Windows Service `cvserver`?
4. Reinstall the Network Management Server Service by running the file `reinstallService.bat` under `\Program Files\Avaya\Network Management\lul\bin`.

   Stop the Avaya Services before executing this step.
5. Follow this process to create a dependency of a service.
   a. Invoke the Windows Registry editor.
   b. Go to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\` in the registry
   c. Find the entry for `cvserver`
   d. Create a new multi-string value named `DependOnService` for `cvserver`. The value should be the process name of `AvayaJBoss404`
6. Restart Windows.

Network Management Installation fails when Postgres is not installed right

Integrated Management software component and version	Network Management (NM)
Installed versions (with service packs/ upgrade path) and other co-resident software and version	Network Management 5.2
Host operating system (Linux or Windows) version	All supported versions of Windows
Symptoms that identify the issue	Try to install Postgres that is present in the Network Management CD manually:\Install\Postgres and it fails

throwing an error about permissions on its data directory. `initdb log` has the following content

```
-------------------- fixing permissions on
existing directory C:/Program Files/
PostgreSQL/8.1/data ... ok creating directory
C:/Program Files/PostgreSQL/8.1/data/
global ... initdb: could not create directory
"C:/Program Files": File exists initdb:
removing contents of data directory "C:/
Program Files/PostgreSQL/8.1/data"
--------------------
```

Cause of the issue

As a Postgres user, you need to have a read permission for Postgres (that means the permissions should be assigned to the group category **everybody** for the following. folders:

- C:\
- C:\Program Files

The Postgres installer creates the following folders:

- C:\Program Files\PostgreSQL
- C:\Program Files\PostgreSQL \Data

The top parent folders like C:\ , C:\Program Files are expected to have the read permission. If they do not have the read permission, that could cause the problem.

Proposed solution

When you install Network Management, you must make sure that a Postgres user has read permission for Postgres for top directories like: `C:\` and `C:\Program Files`

Prerequisites

1. Make sure folders like `C: C:\Program Files` have read permissions for the group category **everybody**
2. Also refer the following links:

   `http://www.jitterbit.com/PhpBB/viewtopic.php?f=7&t=585&p=2534`

   `http://www.postgresql.org/docs/faqs.FAQ_windows.html#2.5`

Network Management Services hangs right at the start

Integrated Management software component and version	Network Management Console (NMC) any version
Installed versions (with service packs/ upgrade path) and other co-resident software and version	Network Management Any version
Host operating system (Linux or Windows) version	All supported versions of Windows
Symptoms that identify the issue	Network Management Services hangs right at the start
Cause of the issue	Some other software or service is Probably running and blocking Network Management Console from using the SNMP trap port 162.

Proposed Solution

Network Management Services hangs right at the start.

1. Stop any software or service that is using the SNMP port 162.
2. Restart the Network Management services.

Memory issues in Java while opening ENM Log Viewer

When you open large ENM application log files, you may encounter an OutOfMemory error. The Enterprise Network Management Log Viewer window does not respond for a long time.

Integrated Management software component and version	Network Management Console 5.2
Installed versions (with service packs/ upgrade path) and other co-resident software and version	Any service pack
Host operating system (Linux or Windows) version	All supported version of Windows

Symptoms that identify the issue	Occasionally, when you open large Enterprise Network Management application log files (around 10 MB size), you may encounter the OutOfMemory error. The Enterprise Network Management Log Viewer window does not respond for a long time (over 20 seconds).
Cause of the issue	This issue occurs when you open files that are over 10MB.

Proposed Solution

You may sometimes face Java memory issues when you open large log files using the ENM Log Viewer. You can resolve this issue by increasing the heap size of the Java memory.

1. To open Java console, do one of the following:
   a. Right-click the java icon on the system tray, and click **Open Control Panel**
   b. Select **Start** > **Control Panel** > **Java.**
2. Click the **Java** tab at the top of the **Java Control Panel** window.
3. Click **View** under the **Java Applet Runtime Settings** option.
   The system displays the **Java Runtime Settings** dialog box.
4. Double-click the **Java Runtime Parameters** text box in the table for version 1.6.0_11.
   ENM 5.2 uses JRE version 1.6.0_11.
   The cursor is shown on the text box and you can now enter the runtime parameters.
5. The default maximum heap size for JRE 1.6.0_11 is 64MB. Increase the heap size to 128MB or higher, using the –Xmx128m option. The command line java parameter for setting the maximum heap size is as follows:

   ```
   -Xmx<size>set maximum Java heap size
   ```

6. Click OK.

Note:
The ENM Log Viewer cannot open log files on the server if it is launched from a client machine. The logs need to be available locally or on a shared network drive. The ENM Log Viewer does not manipulate the content of the open log files.

Devices not discovered in Network Management Console

Integrated Management software component and version	Network Management Console (NMC) any version
Installed versions (with service packs/ upgrade path) and other co-resident software and version	Network Management All versions
Host operating system (Linux or Windows) version	All supported versions of Windows
Symptoms that identify the issue	Some devices in the network are not discovered in Network Management Console. They may be Communication Manager applications, gateways, LSPs, ESSes, or any other devices.
Cause of the issue	Improper or missing SNMP settings on the device(s). Improper or missing SNMP settings in Network Management Console. Network device (for example, a firewall or router) blocking discovery packets (ping/ icmp) from reaching the device. Subnet mask of the network in which device resides has not been added to the Network Management Console discovery list.

Proposed Solution

Some devices in the network are not discovered in Network Management Console. They may be Communication Manager applications, gateways, LSPs, ESSes, or any other devices.

1. Check that the SNMP settings (v1 or v3) on the device(s) that need to be discovered in Network Management Console are configured correctly.
2. Also make sure that the SNMP settings are properly configured (with proper timeout and retry values) in Network Management Console.
3. Check that the network device is not blocking the discovery packets from reaching the device(s). The device should be reachable using IP and SNMP, to be discovered in Network Management Console.
4. Ensure that the subnet/ mask of the network in which the device resides has been added to the Network Management Console discovery list.

A configuration problem does not allow TN boards to be discovered by Software Update Manager

Integrated Management software component and version	Software Update Manager
Installed versions (with service packs/ upgrade path) and other co-resident software with version	Network Management, any version
Host operating system (Linux or Windows) version	All supported versions of Windows
Symptoms that identify the issue	Software Update Manager does not discover Communication Manager's TN boards.
Cause of the issue	A configuration problem that does not allow TN boards to be discovered by Software Update Manager. This happens when the correct Communication Manager login parameters have not been provided in Network Management Console's **CM Servers Passwords** tab, or when SNMP write community for this Communication Manager is not set in the **SNMP** tab of the Network Management Console Options window.

Proposed Solution

A configuration problem that does not allow TN boards to be discovered by Software Update Manager. This happens when the correct Communication Manager login parameters have not been provided in Network Management Console's **CM Servers Passwords** tab, or when SNMP write community for this Communication Manager is not set in the **SNMP** tab of the Network Management Console Options window..

1. Navigate to the **NMC** > **File** > **Options** > **CM Servers Passwords** tab.
2. Provide the Communication Manager IP address and correct Communication Manager login parameters.
3. Modify the SNMP parameters for a device in the current network map as follows:
   a. Select the device in Network Management Console.
   b. Select **Edit** > **Modify** .

The system displays the **Modify Device** dialog box with the selected device's parameters.

c. Navigate to the **SNMP Access** tab and edit the device's SNMP parameters. Enter the correct **write community**.

d. Click **Apply**.

Software Update Manager is not able to discover Communication Manager

Integrated Management software component and version	Software Update Manager (SUM)
Installed versions (with service packs/ upgrade path) and other co-resident software and version	Network Management , any version
Host operating system (Linux or Windows) version	All supported versions of Windows

Symptoms that identify the issue	Navigate to the Software Update Manager logs.
	You see
	`Couldn't find connection parameters for S8xx server`
	or
	`Unable to detect Communication Manager information: could not open SSH session: KBI Authentication failed`
	error messages in the Software Update Manager logs

Cause of the issue	The correct Communication Manager login parameters have not been provided in the **NMC** > **File** > **Options** > **CM Servers Password** tab.

Proposed Solution

The correct Communication Manager login parameters have not been provided in the NMC> **CM Servers Passwords** tab. Therefore, Software Update Manager is unable to discover Communication Manager.

1. Navigate to the **NMC** > **File** > **Options** > **CM Servers Passwords** tab.
2. Enter the Communication Manager IP address and correct Communication Manager login parameters.

Error while upgrading a device — incorrect SNMP parameters

Integrated Management software component and version	Software Update Manager
Installed versions (with service packs/ upgrade path) and other co-resident software with version	Network Management, any version
Host operating system (Linux or Windows) version	All supported versions of Windows
Symptoms that identify the issue	You see the error message: `Failed to set TFTP parameters` in the Software Update Manager logs.
Cause of the issue	This is a configuration issue. When the correct SNMP community is not set in either Network Management Device or in the device which is being upgraded, you receive a `Failed to set TFTP parameters` error message. Enter the correct SNMP **write community** at both instances.

Proposed Solution

This is a configuration issue. When the correct SNMP community is not set in either NMC or in the device which is being upgraded, you receive a `Failed to set TFTP parameters` error message.

1. Go to the device and set the required SNMP paramaters.
2. Add or modify the SNMP parameters for the device in the current network map as follows:

a. Select the device in the Network Management Console.
b. Select **Edit** > **Modify** .
   The system displays the **Modify Device** dialog box with the selected device and its parameters.
c. Navigate to the **SNMP Access** tab.
d. Edit the device's SNMP paramaters.
e. Enter the correct **write community**.
f. Click **Apply**.

Error while upgrading a device — incorrect SCP parameters

Integrated Management software component and version	Software Update Manager
Installed versions (with service packs/ upgrade path) and other co-resident software with version	Network Management , any version except a fresh ENM 5.2.24
Host operating system (Linux or Windows) version	All supported versions of Windows

Symptoms that identify the issue	When you try to upgrade the device, you receive the error message
	`Download failed: SCP error: invalid login parameters`
	or
	`SCP error: Invalid username/password`

Cause of the issue	Either the incorrect SCP parameters have been entered in the Software Update Manager 's software library or the SCP password has expired.

Proposed Solution

When you try to upgrade a device you receive the error message:
`Download failed: SCP error: invalid login parameters`
or
`SCP error: Invalid username/password`
Either the incorrect SCP parameters have been entered in the Software Update Manager software library or the SCP password has expired.

1. Navigate to **SUM** > **Software Library** .
2. Enter the correct SCP parameters in the fields **SCP User Name**, **SCP password**, and **SCP secure path**.
3. Upgrade again.

Proposed Solution 2

When you try to upgrade a device you receive the error message:
`Download failed: SCP error: invalid login parameters`
or
`SCP error: Invalid username/password`
Either the incorrect SCP parameters have been entered in the Software Update Manager software library or the SCP password has expired.

1. To check if the SCP password has expired, log in to the ENM server using the SCP parameters (using Putty or any such software).

   If login fails with the correct parameters, then the SCP Server password may have expired
2. If the SCP password has expired, then do one of the following:
   - Reset the SCP password using the **Programs** > **Avaya** > **Tools** > **SCP User Configuration** > **Change Password** option
   - Create a new SCP user using **Programs** > **Avaya** > **Tools** > **SCP User Configuration** .

   You must restart the system for this step.
3. Enter the new SCP parameters in the fields **SCP User Name**, **SCP password**, and **SCP secure path**.

Chapter 3: Performance and Administration

Starting or stopping an MSA queue generates an error

When you attempt to start or stop an MSA queue by using the Queue Manager control buttons from the MSA Resources or System Resources menu you receive an error message stating that the queue cannot be started or stopped.

Integrated Management software component and version	MultiSite Administration (MSA), any version
Installed versions (with service packs/ upgrade path) and other co-resident software and version	Any service pack
Host operating system (Linux or Windows) version	Any supported Red Hat Linux version with or without VMWare
Symptoms that identify the issue	a. Check the process ID of the pq MSA process (`ps-u mcm`) b. Check whether the `pq.lck` file has the same process ID (cat /var/avaya/msa/switch//<PBX Name>/check/pq.lck) **Note:** When they are not identical MSA queues do not work correctly.
Cause of the issue	The process ID stored in the pq.lck file under the `/var/avaya/msa/switch/<PBX Name>/ /check` folder does not match the Linux process ID of the pq process. This issue is likely to happen after an unexpected shutdown of the Linux operating system (like a power outage)

Proposed Solution

When you attempt to start or stop an MultiSite Administration queue by using the Queue Manager control buttons from the MultiSite Administration Resources or System Resources menu you receive an error message stating that the queue cannot be started or stopped.

1. Log on to the Linux console as root.
2. To stop MultiSite Administration Services, enter service msa-server stop
3. Delete or rename the pq.lck file. rm `/var/avaya/msa/switch/<PBX>/check/pq.lck`
4. To start MultiSite Administration Services, enter service msa-server start
5. Rerun the process above for all PBXs that have the same issue.

Collection does not work right

Integrated Management software component and version	Fault and Performance Manager (FPM), any version
Installed versions (with service packs/ upgrade path) and other co-resident software and version	Any service pack
Host operating system (Linux or Windows) version	Any supported Red Hat Linux version with or without VMWare
Symptoms that identify the issue	When using the Fault and Performance Manager you receive an exception from the voice systems. `Collection: No terminal type prompt` This is because the collection for the voice system is not working.
Cause of the issue	The user account of the user logged into the voice system in the Integrated Management Database has not been correctly configured.

Proposed Solution

When using the Fault and Performance Manager you receive an exception from the voice system.
`Collection: No terminal type prompt`
This is because the collection for the voice system is not working.

1. Enter the cmuseradd command when you log in using the appropriate login type (super-user) and profile.
2. Enter the SAT commandchange user-profile to check if the profile has been enabled and has shell access
3. Log in to the voice system using this user account and connect to SAT.
4. Check if there are any errors.
5. Add this user account to the Integrated Management Database under the voice system.

Collection does not work – 2

Integrated Management software component and version	Fault and Performance Manager (FPM), any version
Installed versions (with service packs/ upgrade path) and other co-resident software and version	Any service pack
Host operating system (Linux or Windows) version	Any supported Red Hat Linux version with or without VMWare
Symptoms that identify the issue	In Fault and Performance Manager you receive an exception from the voice system `Collection: Unable to set up trap filters due to processing errors.`
Cause of the issue	The SNMP setting in Communication Manager or in Fault and Performance Manager have not been correctly configured.

Proposed Solution

In Fault and Performance Manager you receive an exception from the voice system

`Collection: Unable to set up trap filters due to processing errors.`

1. Check to see if SNMP V1 and V2 have been enabled in Avaya Integrated Management Database and also on the Communication Manager maintenance server SNMP agents page.
2. Check to see if the SNMP V1 and V2 community names match in both Integrated Management Database and Communication Manager.
3. Check to see if the Communication Manager firewall settings have been correctly configured for SNMP ports.
4. Add a new filter on the Alarms/Filter form of the Fault and Performance Manager application and save the new settings.
5. Navigate to the the `mvmgt.conf` file on the Communication Manager server.
6. Run cat /etc/snmp/mvmgt.conf to see if there is a line with the IP address information of the Fault and Performance Manager server and the specified filter settings.
7. Check to see when this file was updated by running the ls -la /etc/snmp/mvmgt.conf command.

The graphical user interface does not launch

Integrated Management software component and version	Fault and Performance Manager (FPM), and Multisite Administration
Installed versions (with service packs/ upgrade path) and other co-resident software and version	FPM, any service pack and MSA 5.0
Host operating system (Linux or Windows) version	Any supported Red Hat Linux version with or without VMWare
Symptoms that identify the issue	When you click the link for Fault and Performance Manager or Multisite Administration on the Integrated Management launch page, the graphical user interface does not launch.
Cause of the issue	The client machine probably has a higher version of JRE installed that the application does not support. Fault and Performance Manager and Multisite Administration 5.0 support JRE 1.5.x. If JRE 1.6.x is also installed and if the **Enable the next generation Java Plug-In** option is selected in the Java plug-in , the system creates a problem.

Proposed Solution

When you click the link for Fault and Performance Manager or Multisite Administration on the Integrated Management launch page, the graphical user interface does not launch.

Steps to switch between Java Plug-ins:

1. Navigate to **Start** > **Control Panel** > **Java Control Panel .**
2. Click the **Advance** tab in **Java Control Panel**.
3. Scroll down to the **Java Plug-in** entry.
4. Clear the check box **Enable next-generation Java Plug-in**.
5. Click OK and restart the browser.

Note:
The Java 6 Update 10 (6u10) includes a brand-new implementation of the Java Plug-in, which is used by default as long as you are using Firefox 3 or Internet Explorer. The new Java Plug-in is enabled by default. However, if there are issues running applets with the new Java Plug-in, you can change to the old Java plug-in without any manual manipulation of the windows registry or moving files.

Diskspace full

Integrated Management software component and version	Fault and Performance Manager (FPM)
Installed versions (with service packs/ upgrade path) and other co-resident software and version	Fault and Performance Manager, any service pack
Host operating system (Linux or Windows) version	Any supported Red Hat Linux version with or without VMWare
Symptoms that identify the issue	The /var partition gets full
Cause of the issue	The system installs the Integrated Management database management system (postgresql) in the `/var` partition of the `/var/avaya/db` directory. It has two databases, IMD and MFPM.

MFPM is the database for Fault and Performance Manager which can grow to large volumes and consume the maximum memory available in the `/var` partition. The Fault and Performance Manager application can be set up to register disk space failure exceptions for the /var partition. By default it is set to register a minor exception if the disk space (`/var` partition) is 70% full and a major exception if the disk space (`/var` partition) is 90% full. For more information, see System Exceptions panel topic in *Fault and Performance Manager* help.

Related topics:

[Proposed Solution 1](#) on page 36
[Proposed Solution 2](#) on page 36
[Proposed Solution 3](#) on page 37
[Proposed Solution 4](#) on page 38

Proposed Solution 1

Move the MFPM database backup files (if any) to a location other than `/var`

1. Check if the `/var/Avaya/IMX.y` directory contains the `IMX.yBackup.tgz` file. For the IM 5.2 release the directory is`/var/Avaya/IM5.2` and the file is `IM5.2Backup.tgz`.
2. Move this file to a location other than /var or delete the file if it is no longer required
3. Move or delete other backup files (if any) from the /var partition created by the BackupAlarmParams, BackupMFPM, BackupMFPMConfigData or BackupRestoreFPM scripts.

Note:

For the BackupAlarmParams, BackupMFPM, BackupMFPMConfigData or BackupRestoreFPM scripts, use a backup file destination directory other than the /var partition.

Proposed Solution 2

Set up the MFPM database maintenance scripts. Run the BackupRestoreFPM script or run the Fixcounts script. These two scripts will free-up some of the database objects marked for deletion.

1. Log in to the server with root privileges.
2. Open a terminal and run one of the following command:
   - `[root@fpmvm1-1 ~]# BackupRestoreFPM /home/someuser/fpmbackup`
   - `[root@fpmvm1-1 ~]# FixCounts`

Note:

You can schedule the BackupRestoreFPM script to run every week using Linux cron jobs. Use the FixCounts script only when necessary as the script might take a long time to run. Either run the BackupRestoreFPM script manually as mentioned above or use the Integrated Management Backup and Restore utility to schedule a backup and restore. You can contact Avaya Support to run the scripts.

Proposed Solution 3

Se tup Fault and Performance Manager to store only the required data in the database. You will require more disk space if you increase the maximum days to store exception records in the System Exceptions screen. The default is 30.

1. Review the collection frequency of necessary reports. An hourly report consumes more disk space than daily or weekly reports.

   In the Threshold Alarm Panel, you can set the collection frequency for the following frequently used reports to Daily or Weekly:

   - CLAN PPP
   - IP DSP Resources
   - Trunk Groups
   - Routing Patterns

   Additionally you can delete unwanted entries (Daily, Weekly or Hourly) of the above mentioned reports to free up disk space. For more information, see Threshold Alarm Panel topic in *Fault and Performance Manager* help.
2. In the Fault and Performance Manager Administration interface, clear the **Store Exception?** checkbox for:
   - Trunk Exceptions
   - Trunk Group Exceptions

Note:
Contact Avaya Support to tune Fault and Performance Manager to store only required data in the database.

Proposed Solution 4

Increase the disk space

- If you have unused space in the hard drive, increase the allocated disk space by extending the LVM groups. LVM is a Logical Volume Manager for Linux that allocates space on mass storage devices. For information on how to create LVM Groups, see the*Performance and Administration Installation and Upgrade* guide.
- Increase the allocated disk space by adding a new disk.

Note:
Contact your Linux administrator or Avaya Support to add a new disk.

Index

C

Command
    Communication Manager 15
Communication Manager 28

D

Device Discovery 25
Device Upgrade 28
diskspace
    diskspace full 35
    diskspace maintenance 35

E

ENM Log Viewer 23, 24
    Java memory 23

F

File Transfer FTP 5
File Transfer SCP 10
FPM 32–35
    collection 32
    Collection 33, 34

I

imported tasks 16

M

MSA
    FPM
        GUI
            JRE 34
        Launch
            Java Plug-in 35
MSA Queue 31
MSA Queue resolution 32

N

NM Installation
    Postgres 21
NM Installation resolution 22
NM Services 23
NM Services auto-start 20
NMC 25
NMC Systemview 19
NMC Systemview error resolution 19
NMC tree view 17
NMC Tree View red 18
no alarms 17

P

persist.dat 13

S

SA 12, 14–16
    Administration 12
    commands 15
    import tasks 15
    UTF 8
        ANSI files 14
SA crash 13
SUM 26–30
    Communication Manager 27
    TN Boards 26
    Upgrade Device 28, 29

T

TN Boards 26

U

Upgrade Device 30
UTF 8 parsing 14

V

VAM 5–10
    File Transfer SCP 9, 10