



Avaya Aura™ Midsize Business Template R5.2.1 Release Notes

Issue 3.1
July 2010

INTRODUCTION

This document introduces the General Availability release of the Avaya Aura™ Midsize Business Template Release 5.2.1 and describes known issues. The High Availability feature is being release under Controlled Introduction – please contact Avaya Product Management for additional details.

Please Note: the System Platform section of these Release Notes applies for all Avaya software applications and solutions using System Platform 1.1, including Modular Messaging, Application Enablement Services, System Manager, and Avaya Aura™ for Midsize Enterprises (a.k.a. Midsize Business Template).

SOFTWARE RELEASE VERSIONS

Application Enablement Services Application	File Name
Avaya Aura™ Midsize Business Template	MBT_5.2.1.3.6_with_media_services.iso MBT_5.2.1.3.6_without_media_services.iso Including: <ul style="list-style-type: none">• Communication Manager R5.2.1<ul style="list-style-type: none">o SP 17959o Kernel-xen-2.6.18-128.AV7c• Communication Manager Messaging N5.2.1-13.0 + A902lrf+a + C1317rf+a• Application Enablement Services R5-2-1-103• Media Services 1.1.0.2.1• Utility Server 5.2.1.3.5• Midsize Business Template Installation Wizard build number 4070
Avaya Aura™ System Platform	vsp-1.1.1.0.2.iso with vsp-1.1.1.7.2

Release History:

Date	Build	Change(s)
August 2009	1.0.0.1.12	Controlled Introduction R5.2
November 2009	5.2.1.2.5	General Availability R5.2.1
April 2010	5.2.1.3.6	Service Pack R5.2.1.3.6

MIDSIZE BUSINESS TEMPLATE R5.2.1 OVERVIEW

This section lists in order the known issues for the Midsize Business Template and System Platform. Details on workarounds can be found further in the document. The top 5 issues are in bold.

System Platform

1. **Remote Reboot (aka STONITH) is disabled and not supported on System Platform 1.1.**
2. **Services Port access requires IP forwarding to be turned on.**
3. **Dedicated NIC settings can be lost upon server reboot after failed installation or upgrade resulting in Media services not starting.**
4. **Template installation is blocked when no DNS entry is specified on System Platform and the Template Installation tries to specify it through the Pre-Installation Wizard or EPW.**
5. **The default gateway is mandatory as part of the System Platform installation and the gateway should be valid.**
6. Both servers in a High Availability configuration must be on the same subnet.
7. On an S8510, the raid monitoring service is not started by default.
8. The System Platform 'Local File System' option can only be used for patching.
9. When performing a System Platform upgrade, the upgrade should be committed before performing other actions.
10. High Availability Issue: DRBD devices will not reconnect when the crossover cable is reconnected.
11. Multiple re-installations can result in an out of memory error.
12. Remove cached System Platform patches from previous versions.
13. Cancel template install with the 'SP server' option deletes the OVF file.
14. During a template install, the gateway field for a new bridge is not editable.
15. During System Platform installation, only one default gateway should be configured.
16. The properties "gateway" and "netmask" show up at the bottom of the Network Configuration screen under the Template Properties section.
17. Network configuration is not restored when restore is run from the System Platform WebConsole.
18. Static route configuration is not preserved during backup/restore or upgrade.
19. Restoring a backup archive produced with High Availability active will result in a failure.
20. Express install stores the template in a read-only directory and it cannot be deleted.
21. Clicking on the 'Launch SAL Management Portal' button will fail when executed in the 'Remote Access Mode'.
22. Do not click on the wrench icon to manage an individual virtual machine when logged in via SAL.
23. System Platform upgrade progress on the 'Status' page stalls sometimes on Internet Explorer 6 and Firefox 2.x.
24. During a System Platform upgrade, the 'Wait for User Input Link' does not work all of the time.

25. How the VM status is reported in the WebConsole for stopping a VM.
26. VM shutdown status maybe displayed as 'rebooting' forever.
27. Changing the password the first time you login to WebLM causes Tomcat catalina.out to error and list exceptions.
28. The WebConsole certificate is presented more than once on Internet Explorer 6.
29. The SAL gateway user interface cannot be accessed using Firefox 3 sometimes due to the lack of a valid certificate.
30. On the System Platform WebConsole, if any JavaScript issues are encountered with Internet Explorer 6, the Internet Explorer 6 Security Settings will require modification.
31. High Availability Failover may not occur – Heartbeat Ping Service cannot communicate with the gateway.
32. High Availability Failover will not occur if the gateway firewall rules drop Heartbeat's Ping Packets.
33. Re-establishing a Node into a High Availability Cluster requires manual configuration.
34. When the System Event Log Cache reaches capacity, New Events will not be logged.
35. Backup History shows Successful even after a File Transfer Fails.
36. SAL Gateway User Interface Network Connection Interrupted with Internet Explorer 6 or 7 when shared with the WebConsole.
37. Adding an extra NIC card to an IBM X3550 (S8800) will change the Ethernet port numbers.
38. Platform upgrade executed on High Availability systems can create an issue with Xen configuration file.
39. How to apply System Platform patches on High Availability systems.
40. Moving hard drives from one server to a replacement server requires System Platform and the Template to be re-installed.

Midsize Business Template

1. **System Platform LDAP defined accounts are not used to access AE Services.**
2. **Using the System Platform LDAP defined accounts, e.g. admin or cust on Communication Manager and SIP Enablement Services creates issues.**
3. **The ntpd on both Communication Manager and SIP Enablement Services is enabled by default.**
4. **If Media Services is rebooted or the media gateway is not available when Communication Manager Messaging starts, voicemail becomes unavailable and messages cannot be left or received.**
5. **Dual entries for outgoing calls are made in Communication Manager's CDR for SIP endpoints.**
6. Utility Server CDR Emails are not generated.
7. Public Unknown Numbering is not configured for use by Communication Manager Messaging if the Trunk Configuration is not administered in the Midsize Business Template Installation Wizard.

8. Do not put spaces in DHCP options when editing DHCP Server IP Address Pools on the Utility Server.
9. Phone Firmware on Utility Server for the 96xx Phones is version 3.0 (the 3.1 zip file fails to load onto the Utility Server).
10. Media Services does not support VLAN options and 802.1P/Q tags.
11. The following error records may be shown in Communication Manager error report after the Media Services is started.
12. CDR today's call records show no data.
13. Some Communication Manager features (i.e. TSAPI) are disabled when using WebLM licensing.
14. WinZip may corrupt a number of language files in the Midsize Business Template.
15. When installing System Platform for Midsize Business Template, a valid and working DNS server must be configured.
16. Importing the translations from a standalone SIP Enablement Services server to a Midsize Business Template server with SIP Enablement Services (or vice-versa) is not supported.
17. MyPhone access will be denied when SIP Enablement Services is not configured.

System Platform R1.1 Known Issues and Workarounds

1. **High Availability Issue: Remote Reboot (aka STONITH) is disabled by default and not supported on current version of System Platform High Availability Failover.**

Remote reboot should not be configured when use High Availability

2. **Services Port Access Requires IP forwarding to be turned on.**

If a user is accessing System Platform through the Services port, the user will need to enable IP forwarding on Domain-0 to access CDOM. This can be done by running the following commands.

- login to Domain-0 as admin and "su -" to root login
- echo 1 > /proc/sys/net/ipv4/ip_forward

Once the user has finished his task he should disable the IP forwarding by running the following command as root on dom0.

- login to Domain-0 as admin and "su -" to root login
- echo 0 > /proc/sys/net/ipv4/ip_forward

3. **Media Services may fail to boot after failed or cancelled template installation or upgrade.**

Dedicated NIC settings will be lost upon the next server reboot once the /etc/rc.local symbolic link has been changed to a file. The virtual machine using the dedicated NIC will fail to boot. The actions which will cause the symbolic link to be changed into a file: Failed or cancelled template installation or template upgrade

To detect and workaround this issue:

1. Login to Domain-0 as admin
2. su – to root
 - # su
 - # ll /etc/rc.local

The following “/etc/rc.local | rc.d/rc.local “ should be displayed.

In case the symbolic link doesn't exist, it is recommended that the user executes the following commands:

1. Move the /etc/rc.local file to /etc/rc.d/rc.local
 - # mv -f /etc/rc.local /etc/rc.d/rc.local
2. Create a symbolic link to the file /etc/rc.d/rc.local
 - # ln -s /etc/rc.d/rc.local /etc/rc.local
3. Reboot the server either from the web console or command line.

4. Template Installation is blocked when no DNS entry is specified on System Platform and the Template Installation tries to specify it through Pre-Installation Wizard or EPW.

If a Template needs DNS entry and the SP has not specified one, then it is recommended to add it through the Network Configuration page before proceeding with the Template Installation. If the Template does not require a DNS then it can be set after the Template Installation has finished if needed.

However, If the Template installation specified a DNS entry when SP System does not have a DNS, then the Template installation will hang and Domain-0/CDOM will lose network connectivity.

If Template Install needs a DNS, then a Service Engineer should look for Primary DNS in the **Network Configuration** page and if it is not specified there, then add a Primary DNS and **Save** the Network Configuration and then proceed with Template Installation.

5. Default Gateway is mandatory as part of the System Platform Installation and the gateway should be valid.

6. Both servers in a High Availability configuration must be on the same subnet.

HA requires both servers to be on the same subnet for correct failover operation

7. On an S8510, the raid monitoring service is not started by default.

Without raid monitoring a failed hard-disk in the raid will not create an alarm. To correct this, login to Domain-0 as root and execute the following:

1. #chkconfig --add raid-cli
2. #chkconfig raid-cli on
3. #service raid-cli start

8. The System Platform 'Local File System' option can only be used for patching.

Template installations, template upgrades or platform upgrades are not supported via the local file system only patching.

9. System Platform upgrades should be committed before performing other operations.

During an upgrade, after the system boots up into the new platform build or release, the user is required to 'Commit' or 'Rollback' the upgrade. While the system is waiting for the user to either 'Commit' or 'Rollback', it is strongly advised that the user **NOT** perform any of the following operations:

- Delete,
- Install or
- Upgrade the Template

- **Reboot Domain-0** (Rebooting Domain-0 before committing will automatically roll you back to the old Platform)

Note: System Platform does not prevent the user from performing the operations prior to selecting 'Commit' or 'Rollback'.

If one or more of the above operations is performed, then the operations will actually take effect on the system. Even if the 'Rollback Platform Upgrade' is executed after the actions have been performed, the new changes will be visible in the rolled back System Platform. A "Commit" of the upgrade would be unaffected by the changes made prior to committing the upgrade. Also, if changes were made to the system and neither a "Commit" nor a "Rollback" was performed for the upgrade for 4 hours, then upon the time expiration of the Deadman's switch (4 hours) the system would be automatically rolled back with the same consequences as that of selecting a rollback.

If one or more operations are executed for template related functionality and the user wanted to recover after committing or rolling back the upgrade, then the user needs to manually (through the WebConsole) rollback the changes. An upgrade rollback would, at that point, not be able to roll them back. A 'Commit' of the upgrade, on the other hand, would be unaffected by the changes that the user made prior to committing the System Platform upgrade.

10. High Availability Issue: DRBD devices will not reconnect when the crossover cable is reconnected.

The High Availability feature monitors all network interfaces on regular basis (every 5 minutes) and all DRBD resources for connectivity. Required actions are executed in case the system is not ready. However, if the crossover cable is disconnected for long period of time and reconnected, the system will not detect the missing link on the crossover network interface. To fix this issue, execute following command on both Domain-0s as root:

```
# ifdown eth2 && ifup eth2
```

The next execution of the High Availability monitor will ensure that all DRBD resources are connected and that any changes that occurred on the disk are synced to the standby node.

11. Multiple re-installations can result in an out of memory error.

If a pre-installation web application is used to install a template and a re-install is required (typically if install and delete is done multiple times) an out of permgen memory error can occur.

The 'java.lang.OutOfMemoryError: PermGen space' is a class loader leak.

Tomcat does not garbage collect the Classloader and the classes it loads. Each time you reload the web application context, more copies of these classes are loaded, and as these are stored in the permanent heap generation, it will eventually run out of permgen memory. To resolve this issue, restart the container instead of restarting the context.

Thus, every time the Midsized Business Template preinstall wizard or any pre-installation web application is invoked on System Platform, Tomcat is reloading the web application context thus heightening the risk of the permegen error. The current size of permgen is 128Mb. The permgen memory can be tracked on the web console and an alarm is generated if it exceeds 90%.

To ensure a permgen error doesn't occur please follow these instructions:

1. To re-install the template, you need to delete it first.
2. After deleting the template, restart Tomcat and invoke the pre-installation web application:

Instructions for restarting Tomcat:

- a) Logon to CDom as admin and "su - " to root login
- b) /sbin/service tomcat restart

3. Re-execute the template installation.

12. Remove cached System Platform patches from previous versions.

After each System Platform upgrade, the user (as root) is required to manually run the following command in CDOM to remove cached System Platform patches from previous versions.

```
# rm -rf /vspdata/patch/cache/vsp-patch*
```

13. Cancel template install with the 'SP server' option deletes the OVF file.

Canceling a template installation via 'SP server' will result in the deletion of the OVF file from the System Platform server dir (/vsp-template/..).

14. During a template install, the gateway field for a new bridge is not editable.

IP address and netmask for the interface may be provided, but are not required. This is the IP address and netmask of the interface of Domain-0 on the new bridge. To route packets to a specific gateway from this interface, static routes may be added using the Static Routes Configuration page.

15. During System Platform installation, only one default gateway should be configured.

Even though you can enter a default gateway for each interface, you should specify only one default gateway (specifying more than one default gateway may result in an unusable internal networking configuration).

16. The properties 'gateway' and 'netmask' show up at the bottom of the Network Configuration screen under the Template Properties section.

These will be ignored in the next release as this is interpreted to be the default gateway and netmask which are already displayed on the screen. Going forward, only properties that end with ".gateway" or ".netmask" would be interpreted as template properties.

17. Network configuration is not restored when restore is run from the System Platform WebConsole.

Do not use the restore functionality to make networking changes. This should be done from the System Platform WebConsole Network Configuration page.

Ensure the network settings are correct before doing a restore.

18. Static route configuration is not preserved during backup/restore or upgrade.

If a restore is performed, then the user should check the Static Route Configuration page in the System Platform WebConsole and ensure the static routes are correct. If you are doing a remote upgrade via a VPN or other connectivity that relies on a static route for connection, before the upgrade change the default gateway to point at your VPN device, then upgrade and re-enter the required static routes and then return the default gateway to it's previous value. This is only required if the static route is being used to point management traffic to the VPN and the upgrade is being done remotely.

19. Restoring a backup archive produced with High Availability active will result in a failure.

If High Availability is configured, running restore from the System Platform WebConsole with a backup archive produced with High Availability active will result in a failure. To workaround this issue, backup with High Availability disabled.

20. Configuring the System Platform internal network 'avprivate' before template installation.

Before installing a template, check the "Network Configuration" page on the System Platform Management console (select Server Management | Network Configuration) to view the addresses allocated on the bridge named "avprivate".

System Platform creates an internal, private bridge that allows virtual machines to communicate with each other. This private bridge does not have any connection on your LAN. During installation, System Platform runs an algorithm to find a set of IP addresses that do not conflict with the addresses configured on the "System Domain Network Configuration" screen. However, it is still possible that the addresses selected conflict with other addresses in your network. Since this private bridge is not connected to your LAN, this address conflict could result in the failure of System Platform or an installed template to route packets correctly (the internal routing tables might not differentiate between this private

bridge and your LAN, causing an application to direct packets to some host on your LAN rather than to another application within the SP server that has that same IP address on the private bridge).

If you change the IP address for Domain-0's interface on avprivate (which appears in the bridge section of the "Network Configuration" page) or for CDM's interface on avprivate (which appears under CDM in the Group by Domain section), the addresses must be consecutive with Domain-0's address 1 less than CDM's (i.e., if CDM's IP address for its interface on avprivate is 172.20.30.5, then Domain-0's must be 172.20.30.4). Also, the netmask for Domain-0's interface on avprivate must be the same as the netmask for cdm's interface on avprivate (i.e., if you change one, you must change the other).

In the event that there is a conflict in the network with the private IP address range, some functions may fail to work properly in System Platform and the installed template. For example, the System Platform WebConsole may be inaccessible from a system that has an IP address in conflict with the private address range.

Another example includes an IP phone that registers with Communication Manager with the same IP address as Domain-0's or CDM's address on avprivate. Packets targeted for the phone might actually instead go to Domain-0 or CDM.

21. Clicking on the 'Launch SAL Management Portal' button will fail when executed in the 'Remote Access Mode'.

In the remote access mode, clicking on 'Launch SAL Management Portal' button can not open the SAL Gateway user interface.

There are two workaround options:

Option 1:

While the HTTPS remote access session is open to the VSPU, before clicking on the link, open a HTTPS remote access session to the SAL Gateway solution element for the particular solution platform deployment. Then click on the "Launch SAL UI" button. This workaround will be effective as long as there is not an HTTPS remote access session already open for a different SAL gateway at this same time. In this case, the second remote access session will be assigned a port number other than 7443.

Option 2:

Edit the file at

/opt/avaya/SAL/gateway/Gateway/DefaultProject/VSPU/Applications.xml. Add the following three lines to the section of the file for the application named 'HTTP(S)':

```
<Port type="connect">
7443
</Port>
```

Then restart the Axeda remote access agent.

If connected locally (i.e., NOT through the Axeda remote access agent) then use 'service axedaAgent restart' to restart the agent.

If connected remotely (i.e., through the Axeda remote access agent) then using 'service axedaAgent restart' will NOT be satisfactory because the remote access connection will be dropped while carrying out the command. Due to the way the command is bound to the shell in which it was initiated, the restart will not be completed. A method that will work to restart the remote access agent is to find the pid in /opt/avaya/SAL/gateway/Gateway/pids/axedaagent.pid and run 'kill -9 <pid>'. This will cause the SAL Watchdog to restart the remote access agent within 5 minutes.

22. Do not click on the wrench icon to manage individual virtual machine when logged in via SAL.

When logged into the CDOM WebConsole (Virtual Machine Management) to manage any of the virtual machines, do not click on the wrench icon to manage the individual virtual machine (if logged in through SAL) due to security host containment requirements.

23. System Platform upgrade progress on the 'Status' page stalls sometimes on Internet Explorer 6 and Firefox 2.x.

This issue was not reproducible on Internet Explorer 7 and Firefox 3 and 3.5. It is recommended to use Internet Explorer 7 or Firefox 3 or Firefox 3.5 for System Platform upgrades.

24. During a System Platform upgrade, the 'Wait for User Input Link' does not work all of the time.

The workaround is to click on the 'Home' button and then click on the 'Platform Upgrade waiting for user to commit' button.

25. How the VM status is reported in the WebConsole for stopping a VM.

On the 'VM Detail' page, the WebConsole allows a user to stop a VM. When the user clicks the stop button, the WebConsole displays a 'stopping' status until the VM stops, and then displays the 'stopped' status. However, after 5 minutes, the VM will stop displaying the 'stopping' status and simply start displaying the state reported by Xen.

26. VM shutdown status maybe displayed as 'rebooting' forever.

If the user selects the reboot button, the VM may never shutdown or restart and the WebConsole will display the 'rebooting' status forever. There is no timeout for the VM shutdown. To shutdown the VM, the xm destroy command will need to be manually issued.

27. Changing the password the first time you login to WebLM causes Tomcat catalina.out to error and lists exceptions.

This issue resides in WebLM standalone releases (all releases up to 4.5.5). The issue does not impact WebLM functionality.

28. The WebConsole certificate is presented more than once on Internet Explorer 6.

The WebConsole certificate is presented more than once while launching pop-ups like License Management or SAL on Internet Explorer 6.

29. The SAL gateway user interface cannot be accessed using Firefox 3 sometimes due to the lack of a valid certificate.

Internet Explorer 6 & 7 and Firefox 2 are supported by the SAL Gateway user interface.

30. Internet Explorer 6 JavaScript issues with WebConsole:

On the System Platform WebConsole, if any JavaScript issues are encountered with Internet Explorer 6 (you will notice JavaScript errors if the JavaScript debugger is enabled on the browser), modify the Internet Explorer 6 Security Settings as follows:

1. Go to **Tools | Internet Options | Security** Tab.
2. Click '**Custom Level**' button.
3. Select the **Enable** radio-button for '**Script ActiveX controls marked safe for scripting**'.

31. High Availability Failover may not occur – Heartbeat Ping Service cannot communicate with the gateway.

The heartbeat is configured to use the ping service between the High Availability nodes and the gateway using unicast UDP communication on port 694. The heartbeat's ping service to the gateway should only use ICMP requests which don't require port 694 to be opened.

The following entry:

"ucast avpublic <default gateway IP> # Public PING target (switch)"
should be removed from the *"ha.cf"* file located in the following directories */etc/ha.d* and */opt/avaya/ha/resources* on both the active and standby boxes.

Removing this line will result in the correct ping service operation. To apply these changes, follow the steps outlined below. The System Platform High Availability Failover must be stopped and is a service interrupting operation that should be scheduled accordingly.

1. Stop High Availability Failover Mode from the System Platform WebConsole.
2. Log in to the preferred Domain-0 and su to root.
3. Execute following command:

```
sed -i.ucast_fix -e '/# Public PING target (switch)/d'  
/opt/avaya/ha/resources/ha.cf
```

4. To confirm the entry was successfully removed, execute the following command and no output should be returned.

```
cat /opt/avaya/ha/resources/ha.cf | grep Public
```

5. Repeat steps 2, 3 and 4 for the standby Domain-0.
6. Start High Availability Failover Mode from preferred System Platform WebConsole.

32. High Availability Failover will not occur if the gateway firewall rules drop Heartbeat's Ping Packets.

Heartbeat uses the utility service "pingd" to monitor the ability of cluster nodes to communicate to the network by sending an ICMP request from each node (Primary and Standby Domain-0) to the default network gateway and expects a response back from the gateway. This service sets payload with node-identifying data and checks that the data in replied packet payload are correct. The size of the ICMP ping packets is in the range of 132 - 256 bytes. If firewall rules are applied against the ping service (at the gateway), specifically packet size restriction, it should allow for packet sizes up to 256 bytes. If the packet size restrictions are applied, ensure the packet size is 256 bytes.

33. Re-establishing a Node into a High Availability Cluster requires manual configuration.

When the active server is running in standalone mode, the process of incorporating the failed server into the High Availability cluster to work in High Availability mode will not work from the WebConsole. Specifically, "Stop Failover Mode" will fail. The WebConsole is redirected to the reboot page, but it is not redirected to the login page. A series of manual steps needs to be executed to bring the standby node back online to function in the High Availability mode.

Please note that this process depends on the node type (preferred or standby) to be re-established into the High Availability cluster again. Specifically, steps 12-17 are only needed when the node to be re-established is the preferred node.

To re-enable the reinstalled standby node in the High Availability system:

1. Open SSH session to the active Domain-0 and su to root:

```
su -
```

Password:

2. From SSH session to the active Domain-0 execute:

```
/opt/avaya/ha/scripts/crmutil stop-domain --name dom0
```

3. Ensure that all resources except STONITH resources are stopped - from SSH session to the active Domain-0 execute:

```
a. crm_mon -1
```

```

=====
Last updated: Thu Nov 26 15:40:16 2009
Current DC: vspha1.example.com (24b5c8b5-0767-4365-9e24-
20dc9bc48ed1)
Version: 1.0.2-c02b459053bfa44d509a2a0e0247b291d93662b7
2 Nodes configured.
3 Resources configured.
=====
Node: vspha1.example.com (24b5c8b5-0767-4365-9e24-
20dc9bc48ed1): online
Node: vspha2.example.com (c861c9d0-9209-45cb-a3a7-
d590df1dd4be): OFFLINE
Clone Set: fencing
stonith-resource:0 (stonith:null): Started vspha1.example.com
stonith-resource:1 (stonith:null): Stopped

```

b. xm list

Name	ID	Mem	VCPU	State	Time(s)
Domain-0	0	512	4	r-----	88.0
udom	1024	1			276.3
aes ...					

c. cat /proc/drbd

```

version: 8.3.2 (api:88/proto:86-90)
GIT-hash: dd7985327f146f33b86d4bff5ca8c94234ce840e build by
mockbuild@v20z-x86-64.home.local, 2009-08-29 14:08:07
0: cs:WFCConnection ro:Secondary/Unknown ds:UpToDate/Outdated C r-
---
ns:0 nr:0 dw:4120 dr:1852 al:1 bm:4 lo:0 pe:0 ua:0 ap:0 ep:1 wo:b oos:8
1: cs:WFCConnection ro:Secondary/Unknown ds:UpToDate/Outdated C r-
---
ns:0 nr:0 dw:197376 dr:388270 al:123 bm:308 lo:0 pe:0 ua:0 ap:0 ep:1
wo:f oos:19876
2: cs:WFCConnection ro:Secondary/Unknown ds:UpToDate/Outdated C r-
---
ns:0 nr:0 dw:4112 dr:546 al:1 bm:4 lo:0 pe:0 ua:0 ap:0 ep:1 wo:b oos:4
3: cs:WFCConnection ro:Secondary/Unknown ds:UpToDate/Outdated C r-
---
ns:0 nr:0 dw:219612 dr:25466 al:26 bm:55 lo:0 pe:0 ua:0 ap:0 ep:1 wo:f
oos:47556

```

4. From SSH session to the active Domain-0 execute:

- /opt/avaya/ha/scripts/stop_vspha.sh primary*
- mount | grep /template-env*
/dev/mapper/VolGroup00-lv_tmpl_env on /template-env type ext3 (rw)

5. From SSH session to the active Domain-0 execute:
 - a. `/opt/avaya/ha/scripts/crmutil remove-domain --name dom0`
 - b. `crm_mon -1`

```

=====
Last updated: Thu Nov 26 15:46:06 2009
Current DC: vspha1.example.com (24b5c8b5-0767-4365-9e24-20dc9bc48ed1)
2 Nodes configured.
0 Resources configured.
=====

Node: vspha1.example.com (24b5c8b5-0767-4365-9e24-20dc9bc48ed1): online
Node: vspha2.example.com (c861c9d0-9209-45cb-a3a7-d590df1dd4be):
OFFLINE

Failed actions:
udom-drbd-udom0_start_0 (node=vspha1.example.com, call=29, rc=1,
status=complete): unknown error

```
6. From SSH session to the active Domain-0 execute:
 - a. `PEER_NAME=`crm_mon -1 | grep OFFLINE | awk '{print $2}'``
 - b. `echo $PEER_NAME`
`vspha2.example.com`
7. From SSH session to the active Domain-0 execute:
 - a. `crm node delete $PEER_NAME`
 - b. `crm_mon -1`

```

=====
Last updated: Thu Nov 26 15:50:50 2009
Current DC: vspha1.example.com (24b5c8b5-0767-4365-9e24-20dc9bc48ed1)
1 Nodes configured.
0 Resources configured.
=====

Node: vspha1.example.com (24b5c8b5-0767-4365-9e24-20dc9bc48ed1): online

```
8. From SSH session to the active Domain-0 execute:
 - a. `service heartbeat stop`
 - b. `crm_mon -1`

```

Connection to cluster failed: connection failed

```

9. From SSH session to the active Domain-0 execute:

- a. *rm -f /var/lib/heartbeat/pengine/**
- b. *rm -f /var/lib/heartbeat/crm/**
- c. *rm -f /var/lib/heartbeat/hb_**
- d. *rm -f /var/lib/heartbeat/*hostcache*
- e. *ll /var/lib/heartbeat/**
prw----- 1 root root 0 Nov 26 15:50 /var/lib/heartbeat/fifo

/var/lib/heartbeat/cores:

total 24

drwx----- 2 hacluster haclient 4096 Nov 20 2008 hacluster

drwx----- 2 nobody nobody 4096 Nov 20 2008 nobody

drwx----- 2 root root 4096 Nov 20 2008 root

/var/lib/heartbeat/crm:

total 0

/var/lib/heartbeat/pengine:

total 0

10. From SSH session to the active Domain-0 execute:

- a. *service drbd stop*
Stopping all DRBD resources: .
- b. *cat /proc/drbd*
cat: /proc/drbd: No such file or directory

11. From SSH session to the active Domain-0 execute:

- a. *sed -i -e*
's/GLOBAL_STATUS=STARTED/GLOBAL_STATUS=CONFIGURED/'
/opt/avaya/ha/scripts/vspha.conf
- b. *cat /opt/avaya/ha/scripts/vspha.conf | grep GLOBAL_STATUS*
GLOBAL_STATUS=CONFIGURED

12. Check whether currently active node is preferred or standby node. If the node is preferred node, go to step 18. If the node is not preferred, continue with all of the following steps. The user should not try to reinstall the preferred node unless instructed to do so.

To check if the currently active node is the preferred node, from SSH session to the active Domain-0 execute as root:

- a. *source /opt/avaya/ha/scripts/vspha.conf*
- b. *ifconfig \$NETWORK_INTERFACE | grep " addr:\$PRI_IP_ADDR "*

If this command did not return any output, currently active node is NOT preferred node - perform steps 13-17.

If this command returned output with IP address, broadcast and netmask currently active node IS preferred node – do not perform steps 13-17 and continue directly to step 18.

13. From SSH session to the active Domain-0 execute:

a. `echo $SEC_UDOM_MAC_ADDR`

An example output: 00:16:3e:28:18:fe

Make a note of this MAC address. It will be referenced as <MAC_ADDR> in following steps.

b. `echo $SEC_UDOM_IP_ADDR`

An example output: 135.64.30.44

Make a note of this IP address. It will be referenced as <IP_ADDR> in following steps.

14. Swap the node roles. From the SSH session to the active Domain-0 execute:

a. `sed -i -e '/PRI_[^U]/s/PRI_/TMP_/' /opt/avaya/ha/scripts/vspha.conf`

b. `sed -i -e '/SEC_[^U]/s/SEC_/PRI_/' /opt/avaya/ha/scripts/vspha.conf`

c. `sed -i -e '/TMP_/s/TMP_/SEC_/' /opt/avaya/ha/scripts/vspha.conf`

Note: The active node has now become the new preferred node.

15. Update the reference to the current Domain-0 in the SSL key file. From the SSH session to the active Domain-0 execute:

```
sed -i -e "/tomcat@/s#/$PRI_FULL_NAME#/$SEC_FULL_NAME#g"
/root/.ssh/authorized_keys
```

16. Reinstall the preferred node with the same System Platform version as currently active node. If it was reinstalled before this point, repeat the installation as the previous installation has failed. When reinstalling the formerly preferred failed node, ensure to use standby CDOM IP address (value referenced as <IP_ADDR> retrieved in step 13.-b.) as CDOM still uses preferred node CDOM IP address.

17. When preferred node is reinstalled and its WebConsole is accessible, log in to its Domain-0 as admin user and execute following sequence of commands. Please replace every occurrence of <MAC_ADDR> with the real value of the MAC address retrieved in step 13(a) when typing the commands.

a. `su -`

b. `sed -i -e '/^vif /s/mac=00:16:3e:[^,]*/mac=<MAC_ADDR>/' /etc/xen/udom`

c. `ssh cdom.vsp`

d. `sed -i -e '/^HWADDR=/a\MACADDR=<MAC_ADDR>'
/etc/sysconfig/network-scripts/ifcfg-eth0`

e. `sed -i -e 's/^HWADDR=/#HWADDR=/' /etc/sysconfig/network-
scripts/ifcfg-eth0`

f. `ifdown eth0; ifup eth0`

- g. Please ensure that you can access WebConsole using <IP_ADDR> IP address.
18. From SSH session to Domain-0 on active node execute:
xm start udom
19. The WebConsole of the active node should redirect after couple of minutes.
After the redirect, perform the following:
- Log on to WebConsole as admin
 - Go to Server Management -> Failover
 - Click "Remove Failover" button and confirm the warning
20. From SSH session to Domain-0 on active node execute as root:
- ssh cdom.vsp sed -i -e '/dom0-standby.vsp/d' /etc/hosts*
 - ssh cdom.vsp cat /etc/hosts | grep dom0*
<Dom-0 IP> dom0.vsp
21. From SSH session to Domain-0 on active node execute as root:
- sed -i -e '/^\$PEER_NAME,/d' /root/.ssh/known_hosts*
 - cat /root/.ssh/known_hosts | grep \$PEER_NAME*
<no output expected>
22. From SSH session to Domain-0 on active node execute as root:
- sed -i -e '/root@\$PEER_NAME\$/d' /root/.ssh/authorized_keys*
 - cat /root/.ssh/authorized_keys | grep \$PEER_NAME*
<no output expected>
23. On the WebConsole of the active node logged in as admin:
- Go to Server Management | Failover
 - Click "Configure Failover" button
 - Provide IP address of remote (reinstalled) node cdom
 - Provide password for user 'admin'
 - Ensure that 'Remote Reboot' option is disabled
 - Click Configure button
24. On the WebConsole of the active node logged in as admin:
- Go to Server Management | Failover
 - Click "Start Failover Mode" button and confirm warning
 - WebConsole is redirected to reboot page
 - After couple of minutes it is redirected to login page
 - Log in to WebConsole as admin again
 - Check the progress of DRBD sync process

34. When the System Event Log Cache reaches capacity, New Events will not be logged.

There is no automated mechanism in place to clear the System Event Log cache when it becomes full. New events will not be logged if the cache isn't cleared. The maximum number of entries is 512.

Manual steps to clear the cache and preserve old entries are as follows:

1. Log into Domain-0 as root account.

```
# su - root  
Password:<root's password>
```

2. List cached System Event Log events. The following command will display all of the events available in the cache:

```
# ipmitool sel list
```

3. Backup all the System Event Log events to /root/sel_events_1.txt in case to be referred to in the future:

```
# ipmitool sel list > /root/sel_events_1.txt
```

4. Empty System Event Log cache.

```
# ipmitool sel clear
```

5. Verify whether the System Event Log entry is empty. The output of this command will be much less than the output in step b).

```
# ipmitool sel list
```

The System Event Log entry may be full again in the future. To avoid this from happening, administrators may consider adding the tasks described above to cron as shown in step 6.

6. Add a cron job to clear System Event Log entries every 5 minutes.

```
# crontab -e
```

At this point, 'vi' should be launched and some existing cron jobs may be displayed.

```
PATH=/opt/avaya/vsp/bin:/bin:/usr/bin  
PYTHONPATH=/opt/avaya/ha/lib  
*/5 * * * * /opt/avaya/ha/scripts/monitor-hardware
```

```
*/2 * * * * find /var/lib/xen/boot_* -mmin +1 -delete
```

Please don't change any existing lines! Instead, append the following line to the end of the file:

```
*/5 * * * * /usr/bin/ipmitool sel clear
```

The final result of the file will be displayed as follows:

```
PATH=/opt/avaya/vsp/bin:/bin:/usr/bin  
PYTHONPATH=/opt/avaya/ha/lib  
*/5 * * * * /opt/avaya/ha/scripts/monitor-hardware  
*/2 * * * * find /var/lib/xen/boot_* -mmin +1 -delete  
*/5 * * * * /usr/bin/ipmitool sel clear
```

7. Save the changes.

35. Backup History shows Successful even after a File Transfer Fails.

If backup from the web console fails to transfer the backup archive to an SFTP server or email to a user it still shows the backup status as "Successful". The backup status history doesn't reflect the status of the backup archive transfer, it only reflects whether the backup was run successfully on the System Platform server and the backup archive was created locally in CDOM under `vspdata/backup/archive/`.

If a backup is unable to transfer the backup archive to an SFTP server or email to a user, it will send an alarm to the Avaya SAL gateway or NMS if it is configured. If the SAL gateway and NMS are not configured, then the user can review the backup alarms in the Log viewer of the WebConsole by selecting 'Event Logs' with 'Error' level and filtering on 'backup'.

For example:

```
Jan 6 10:32:45 - udom2.du.rnd.avaya.com - Error - O_AVPC22017 - Backup  
archive backup_udom2_2010_01_06_10_32_41.tgz could not be sent on server  
135.64.30.16.  
Jan 6 10:32:45 - udom2.du.rnd.avaya.com - Error - - An error  
occurred while trying to send the archive  
backup_udom2_2010_01_06_10_32_41.tgz on 135.64.30.16. SFTP Ex:3:  
Permission denied
```

36. SAL Gateway User Interface Network Connection Interrupted with Internet Explorer 6 or 7 when shared with the WebConsole.

On both Internet Explorer 6 and 7, when the SAL Gateway User Interface and the System Platform WebConsole share the same Internet Explorer process, the SAL Gateway User Interface will periodically report "Network Connection

Interrupted" messages and request a reload of the SAL gateway User Interface pages. This issue occurs with Internet Explorer 6 and when accessing the SAL Gateway via the "Launch SAL Gateway Management Portal" button in the System Platform WebConsole. Internet Explorer 6 or 7 should not be used to access the SAL Gateway through the "Launch SAL Gateway Management Portal".

Workaround:

1. Open two Internet Explorer windows by clicking on the Internet Explorer icon the Windows desktop twice;
2. Open the SAL Gateway User Interface via <https://CdomIPAddress:7443/spirit-gw/> in one Internet Explorer window and open the System Platform WebConsole via <https://CdomIPAddress/webconsole> in the other;
3. Check the task manager on Windows to make sure there are two new iexplore.exe processes in the task manager window.

Microsoft has provided a fix for this issue (Internet Explorer 7 and earlier versions) which can be downloaded from <http://support.microsoft.com/kb/282402>.

The same issue may happen in Firefox 2. Similar to the solution for Internet Explorer 6 and 7, open two Firefox 2 windows to workaround the issue.

This issue does not occur in Internet Explorer 8 or Firefox 3. On these browsers, users can log in to the System Platform WebConsole, go to "Server Management" | "SAL Gateway Management" and click the button "Launch SAL Gateway Management Portal" to access the SAL Gateway.

37. Adding an extra NIC card to an IBM X3550 (S8800) will change the Ethernet port numbers.

Verify all the Ethernet ports.

For example, adding an extra NIC card can result in the following:

New Cards = eth0 and eth1

- eth0 moved to eth2
- eth1 moved to eth3
- eth2 moved to eth4
- eth3 moved to eth5

38. Platform upgrade executed on High Availability systems can create an issue with Xen configuration file.

If the Platform upgrade is executed first on the Preferred system and then on the Standby system, the upgrade of the Standby system will force the Preferred CDOM to restore the backed up data during the reboot of CDOM. On high availability systems, this reboot is executed during the "Start HA" procedure.

The restore can overwrite configuration files that are used by System Platform High Availability Failover. The system will still behave correctly, even after repeated reboots of CDOM; however, if the user initiates a “Stop HA” procedure later, the System Platform CDOM will not boot up indicating that there is no connection to WebConsole or SAL.

Resolution:

To prevent the issue, execute the Platform upgrade in the following sequence:

1. Stop Failover Mode
2. Execute Platform upgrade of the Standby system
3. Commit Platform upgrade of the Standby system
4. Execute Platform upgrade of the Preferred system
5. Commit Platform upgrade of the Preferred system
6. Start Failover Mode

Note that the order of upgrades of Preferred and Standby systems is essential.

Optional Platform upgrade sequence:

1. Stop Failover Mode
2. Remove Failover
3. Reinstall Standby system with upgraded version
4. Execute platform upgrade of the Preferred system
5. Commit platform upgrade of the Preferred system
6. Configure Failover from Preferred system
7. Start Failover Mode

How to determine which system is Preferred and which is Standby:

After the “Stop Failover Mode” operation, the WebConsole header information indicates which system is being accessed as shown in Figures 1 and 2.

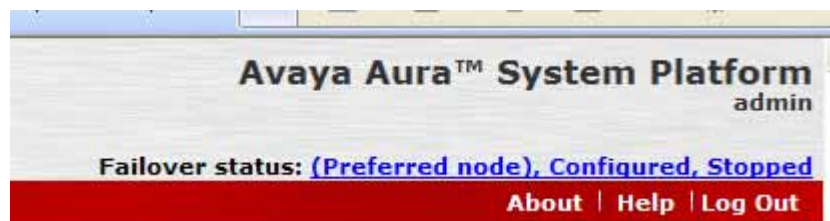


Figure 1: Preferred System Header Information

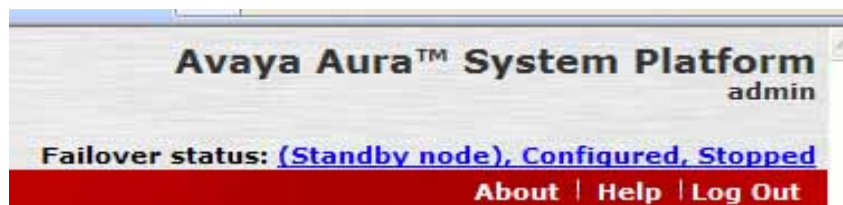


Figure 2: Standby System Header Information

How to determine if an upgraded system has a problem:

Log in as an Administrator via an ssh connection to Domain-0 on the Preferred system.

If High Availability has not been started, execute the following:

1. # su –
2. # cat /etc/xen/udom | grep ^disk | awk -F'phy:' '{print \$2}'

Expected result:

/dev/VolGroup00/udom1,xvda,w", "

3. # xm list udom -l | grep phy:

Expected result:

(uname phy:**/dev/VolGroup00/udom1**)
(uname phy:/dev/VolGroup00/udomswap)
(uname phy:/dev/VolGroup00/vsp-template)
(uname phy:/dev/VolGroup00/udomdata)

Compare the logical volume retrieved in step 2 and the first logical volume retrieved in step 3. If they are equal, the system is setup correctly. If they are different (e.g. /dev/VolGroup00/udom and /dev/VolGroup00/udom1), the Platform upgrade was executed in the wrong order. If CDOM was already rebooted, the configuration files have been modified. Proceed to the section "How to Fix the System".

If High Availability has been started, execute the following:

1. # su –
2. # cat /etc/xen/udom | grep ^disk

Expected correct result:

disk = ["phy:/dev/drbd1,xvda,w",
"phy:/dev/VolGroup00/udomswap,xvdb,w", "phy:/dev/drbd2,xvdd,w",
"phy:/dev/drbd3,xvdg,w"]

Note: all the logical volumes, except swap partition, are using DRBD resources.

Result identifying an issue:

disk = ["phy:/dev/drbd1,xvda,w",
"phy:/dev/VolGroup00/udomswap,xvdb,w",
"phy:/dev/VolGroup00/vsp-template,xvdd,w",
"phy:/dev/VolGroup00/udomdata,xvdg,w"]

Note: the first logical volume is using DRBD resource but all the other logical volumes, including swap partition, are using bare logical volumes.

How to Fix the System:

To fix the system for both cases (before and after starting High Availability), login to Domian-0 as an Administrator on the Standby system via an ssh connection and execute the following:

1. # su -
2. scp /etc/xen/udom <IP address of Preferred Dom-0>:/etc/xen

39. How to apply System Platform patches on High Availability systems.

If the patch includes a Domain-0 patch, apply the patch to both systems (Preferred and Standby). For a High Availability systems, execute the “Stop HA” command before applying the patch. The patch must be applied to both WebConsoles.

Note: If the patch was applied before “Stop HA”, it must be removed. Otherwise, it will prevent the installation of the patch on the Standby system.

To install the patch on both systems, perform the following steps:

1. Login into WebConsole as an Administrator and navigate to “Server Management” | “Failover”.
2. Press the “Stop Failover Mode” button and confirm the displayed warning.
3. The WebConsole will redirect to the reboot page followed by the login page.
4. Login to the WebConsole of the Preferred system and apply the patch.
5. Login to the WebConsole of the Standby system and apply the patch.
6. On the WebConsole of the Preferred system, navigate to “Server Management” | “Failover”.
7. Press the “Start Failover Mode” button and confirm the displayed warning.
8. WebConsole will redirect to reboot page followed by the login page.

40. Moving hard drives from one server to a replacement server requires System Platform and the Template to be re-installed.

If hard drives are moved to a new server, System Platform needs to be re-installed. In the event of a chassis failure of a server and the existing hard drives being moved to the replacement hardware System Platform needs to be re-installed.

All existing data on the hard drives will be lost. The Disaster Recovery procedure in the event of chassis failure will be to move the hard drives to the new chassis, re-install System Platform and then reload the customer configuration from a remote backup file. It is important to maintain remote system backups. If the server chassis fails without a remote backup file, it will need to be reconfigured manually.

If a single hard drive is moved into an existing raid to replace a failed hard drive, re-installation is not required as the operation works correctly.

Midsize Business Template R5.2.1 Known Issues and Workarounds

1. **System Platform LDAP defined accounts not used to access AE Services.**
LDAP authentication is disabled for AE Services in this release, i.e. System Platform defined accounts such as admin and cust will not allow access to AE Services.

Workaround:

Use AE Services standard accounts for access, e.g. avaya, craft, etc.

2. **Issues will be encountered when using System Platform LDAP defined accounts, e.g. admin or cust on Communication Manager and SIP Enablement Services.**

For SIP Enablement Services, the home directory does not exist when logging in via ssh using a System Platform LDAP defined account.

For Communication Manager, it is not possible to use the SAT command when logged in using a System Platform LDAP defined account.

Workaround:

Use customer defined local accounts for Communication Manager and SIP Enablement Services.

3. **The ntpd on both Communication Manager and SIP Enablement Services is enabled by default.**

The ntpd on both Communication Manager and SIP Enablement Services is enabled by default and cannot be disabled.

Workaround:

Disable NTP port on both Communication Manager and SIP Enablement Services firewalls via the relevant maintenance pages.

4. **If Media Services is rebooted or the media gateway is not available when Communication Manager Messaging starts, voicemail becomes unavailable and messages cannot be left or received.**

Workaround:

Non-persistent fix - Stop and restart Communication Manager Messaging to rectify the problem.

Persistent fix - Load CMM RFU C1317rf+a.rpm to fix the problem using the System Platform WebConsole Patch Management feature.

5. Dual entries for outgoing calls are made in Communication Manager's CDR for SIP endpoints.

When making an external call from a SIP endpoint, following disconnection, dual entries will be made to Communication Manager's CDR. One entry will detail the call to the Called Party whilst the other entry will detail the call for the outgoing trunk used (Called Party number will be shown as the TAC code of the outgoing trunk used).

Workaround:

Either ignore the CDR entries that detail the TAC code for outgoing trunks or via SAT on Communication Manager, or set the 'CDR Reports' for the SIP Trunk to 'n'.

6. Utility Server CDR emails are not generated.

Although the configuration screens for the sending of CDR emails are all fully operational on the Utility Server, no CDR emails will be successfully generated in this release.

Workaround:

None, it's not possible to send Utility Server generated CDR emails in this release.

7. Public Unknown Numbering is not configured for use by Communication Manager Messaging if the Trunk Configuration is not administered in the Midsize Business Template Installation Wizard.

This will result in calls being unable to transfer to Communication Manager Messaging voicemail, e.g. calling subscribers are unable to leave messages when forwarded to voicemail.

Workaround:

Add entries in the Public Unknown Numbering form on Communication Manager using SAT, e.g.: (the example below is for a 5-digit extension length).

Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	CPN Len
5	1	—	—	5
5	2	—	—	5
5	3	—	—	5
5	4	—	—	5
5	5	—	—	5
5	6	—	—	5
5	7	—	—	5

8. Do not put spaces in DHCP options when editing DHCP Server IP Address Pools on the Utility Server.

Spaces should not be necessary and if used, will result in the line after the space being displayed incorrectly.

9. Phone Firmware on Utility Server for the 96xx Phones is version 3.0 (the 3.1 zip file fails to load onto the Utility Server).

When available, later releases of the Phone Firmware can be obtained from Support.Avaya.com. The current 3.1 zip file (h323-111609.zip) format on the Support.Avaya.com fails to load onto the Utility Server.

Workaround:

Extract files from the zip file and then re-zip them without putting them in a sub directory. Currently the 96xx-h323-111609 sub directory prevents correct extraction of the zip files.

10. Media Services does not support VLAN options and 802.1P/Q tags.

Ethernet options and VLAN value for the Media Services TN2302B board set through SAT 'IP interface' screen will be ignored. The default 'Auto negotiation' mode will be used for the Ethernet option and for the VLAN tag, the default 'no vlan' is used. 802.1P/Q Parameters set through SAT 'IP network region' screen will be ignored. The default 'no 802.1P/Q tag' is used.

11. The following error records may be shown in Communication Manager error report after the Media Services is started.

The following environmental errors are from Media Services. There is no active environmental monitoring in the Media Services. These errors will not cause any problems during normal operations.

Error Type	Mtce Name	Port
257	CAB-MTCE	01
513	CAB-MTCE	01

The following errors are caused by empty virtual slots in the Media Service cabinet. They will not cause any problems during normal operations.

Error Type	Mtce Name	Port
28	CONFIG	
29	CONFIG	
59	CONFIG	
60	CONFIG	
61	CONFIG	
66	CONFIG	

12. CDR today's call records show no data.

The CDR collector in CM outputs data with a time delay of several hours. Therefore today's calls may not show up until the next day. The data is not lost it just isn't delivered to the Utility Server CDR database straight away.

13. Some Communication Manager features (i.e. TSAPI) are disabled when using WebLM licensing.

Workaround:

Apply CM5.2.1 SP0.

14. WinZip may corrupt a number of language files in the Midsize Business Template.

If extracting files from a Midsize Business Template ISO image within a Windows environment, e.g. when extracting the files to a USB stick, do not use WinZip as this application has been found to corrupt a number of the contained Communication Manager Messaging language files.

Workaround:

Use a different Windows application to extract the files.

15. When installing System Platform for Midsize Business Template, a valid and working DNS server must be configured.

Failure to have a valid DNS server defined on System Platform when installing the Midsize Business Template can result in both the Avaya Communication Manager and Avaya SIP Enablement Server Virtual Machines becoming inaccessible and unstable.

Workaround:

Where a system has been installed without a valid DNS server, update this to a valid value via the System Platform WebConsole Network Configuration menu item and then reboot the server.

16. Importing the translations from a standalone SIP Enablement Services server to a Midsize Business Template server with SIP Enablement Services (or vice-versa) is not supported.

SIP Enablement Services will not start after the import. SIP Enablement Services on a Midsize Business Template must be configured using the administrative tools or from an imported file from another Midsize Business Template with SIP Enablement Services.

17. MyPhone access will be denied when SIP Enablement Services is not configured.

This issue occurs with a full installation of Midsize Business Template and where the option to not configure SIP is selected resulting in the core SIP Enablement Services database is not being configured with default parameters. The Administrative Web Pages on the SIP Enablement Services Server provide access to complete the installation of SES, thus allowing MyPhone to operate. Please refer to the Installing, Administering, Maintaining, and Troubleshooting Avaya Aura™ SIP Enablement Services guide to configure a simplex server.

If the installation is performed with SIP configured (a minimal installation time), MyPhone operates correctly.

Resolved Issues

1. **96xx H.323 and SIP Firmware has been updated in the Utility Server.**
2. **The CDR Email Engine has been fixed.**
Although the SMI pages allowed full configuration of CDR Emails, none were actually generated. This has been resolved.
3. **The NTP Client ran by default in Communications Manager and SIP Enablement Services.**
This issue has been corrected.
4. **Communication Manager and SIP Enablement Services plug-ins removed host entries from /etc/hosts.**
This issue caused installation failures of Communication Manager and SIP Enablement Services. This issue has been resolved.