Product Support Notice

PSN # PSN020361u

Original publication date: 11-Oct-2018. This is Issue #24 published date: 9-June-2023.

Severity/risk level Medium Urgency When convenient

Name of problem PSN020361u - Avaya Aura® 8.x Software-only RPM updates

Products affected

Avaya Aura® Application Enablement Services, Release 8.x
Avaya Aura® Communication Manager, Release 8.x
Avaya Aura® Session Manager, Release 8.x
Avaya Aura® System Manager, Release 8.x
Avaya Aura® WebLM (Standalone), Release 8.x
Avaya Aura® Media Server, Release 8.x

Problem description

Avaya Aura® went End of Manufacturer Support (EOMS) on March 6, 2023 as noted in the Product Lifecycle Notice. *Avaya is providing a final Service Pack on 8.1.3.x to cover outstanding bugs that were not able to be included in the February 8.1.3.7 Service Pack.*

The Avaya Aura® Release 8.x and later supports software-only installation. For software-only deployment, the customer owns the operating system and the customer is responsible for licensing, providing and configuring the operating system for use with the Avaya Aura® application.

With the software-only offer, the customer installs and customizes the operating system to meet the requirements for Avaya Aura® applications.

While the customer is responsible for the operating system with software only, it is possible a new RPM version will have a compatibility issue with the Avaya application that will need to be resolved before the RPM can be used. It is very important that new releases of RPMs that are critical for a product have been tested by Avaya before they are used with the Avaya application. Avaya will test and release the latest RPM list on a regular basis in this PSN thus allowing software only customers to update the Avaya Aura application operating systems as quickly as possible while ensuring optimal application stability and performance.

Each software-only offer has a list of required rpms. This can be found in the software-only documentation or in the ISO for each product. In certain cases, within that list are critical rpms that Avaya will need to test before a new version of the RPM should be used. These are specifically referenced in the **critical RPM list** within this document. Required RPMs that are not on this critical rpm list can be updated without testing as it is very unlikely they will affect Avaya application operation. RPMs on the critical RPM list should be used at the version listed.

Some Avaya applications will install customized Avaya versions of some of the RPMs. These are required for the Avaya application to work correctly. The application will install these during installation, and they will be updated via Avaya application service packs and feature packs. These should not be updated separately. Some of these customized RPMs are *optional* and the administrator will be given the choice to install them or not. These are listed within the **do not upgrade** section of the document and have an AV designation within the RPM name.

NOTE: In the software only model the customer is responsible for the Operating System and installing Avaya tested security updates to those RPMs. Avaya Service packs and feature packs will NOT update OS RPMs for software only and it is the customer responsibility to do so. Failure to update operating system RPMs can lead to reduced security of the virtual machine.

This PSN includes instruction for how to install RHEL updates on each Avaya application. Yum update and other version commands should be used carefully to ensure the Red Hat Enterprise operating system is at the correct version of the RPMs. Using general commands such as ‘yum update’ without version control may result in the OS rpms being updated past the supported versions that Avaya has tested. In addition, only Red Hat Enterprise repositories should be enabled when performing any updates. The suggested process for OS RPM updates is to update the critical RPMs to the listed versions. Then create an exclude list that combines the critical rpms and do not update RPMs and provide that list to yum or other update process to update all the other required RPMs.

If a version of any RPM on the system is newer than the tested version in the published critical list it means that RPM has not yet been tested by Avaya and its compatibility with the Avaya application is not yet known. If there is an issue with the Avaya application Avaya services may require the system be reverted to versions of RPMs that are currently supported as part of the issue resolution process.

Consult each product's software only installation documentation for details on the base version of Red Hat currently supported. OS updates should be applied to virtual machines in maintenance windows as detailed in the application documentation as their installation will be service affecting for the product and may require a reboot.

RPM type	Notes	Found	Update guide
Required RPMs	All RPMs needed by the Avaya product to run on Red Hat ™ operating system	Within product installation media or installation documentation	Required RPMs that are not on the critical list can be updated at any time by the customer following OS RPM update process
Critical RPMs	A subset of the required RPMs that are critical to the Avaya application operation. Avaya will test with to ensure no issues are found with the latest version	Within this PSN	Update to the version Avaya has tested with that is listed in this PSN
Do not update RPMs	RPMs that Avaya modifies or provides with the Avaya application installations	Within this PSN	Do not update directly, updates will be provided through Avaya product Service pack and Feature pack updates

Avaya only performs RPM testing on the latest version of Avaya applications. The latest version of the product is required to be used for the continued RPM updates. Aura Release 8.1.3.6 is currently the latest version. Results for previous versions (8.0, 8.0.1.x, 8.1.0, 8.1.1, 8.1.2, 8.1.3, 8.1.3.1, 8.1.3.2, 8.1.3.3, 8.1.3.4, 8.1.3.5, 8.1.3.6, 8.1.3.7) are maintained in the Appendix of this PSN. There will be no additional updates for 8.0 or 8.0.1.

Resolution

Avaya maintains a list of required rpms for the "Software Only" deployment option.
These are applicable to all of the products listed under the "Products affected" section of this PSN except where noted.

CURRENT RELEASES SECTION

Aura 8.1.3.8 GA May 8, 2023 – Certified for Software Only Offer June 9, 2023
This section lists all the latest RPMs for the latest GA version of the products.

IMPORTANT: Any non-RHEL repositories should be disabled prior to executing any updates.
To list enabled repositories execute:

yum repolist enabled

Any non-RHEL repositories should be disabled by setting "enable=0" in the corresponding /etc/yum.repo.d file.
Failure to do so may cause issues with the Avaya application.

Avaya Aura® System Manager 8.1.3.8

Avaya Aura® System Manager critical RPM versions list

java-1.8.0-openjdk-1.8.0.362.b08-1.el7_9.x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.342.b07-1.el7_9.x86_64
java-1.8.0-openjdk-headless-1.8.0.362.b08-1.el7_9.x86_64
java-1.8.0-openjdk-devel-1.8.0.362.b08-1.el7_9.x86_64

Avaya Aura® System Manager do not update RPM version list

postgresql13-13.3-1PGDG.rhel7.x86_64
postgresql13-server-13.3-1PGDG.rhel7.x86_64
postgresql13-contrib-13.3-1PGDG.rhel7.x86_64
postgresql13-libs-13.3-1PGDG.rhel7.x86_64
net-snmp-5.7.3-3.smgr.el7.x86_64
redhat-release-server-7.6-4.el7.x86_64

How to Upgrade System Manager RPMs
Avaya recommends taking a System Manager backup before performing the updates.

Pre Update
If you have a Geo Redundancy setup of System Manager disable Geo as a first step.
If your System Manager is deployed in a virtualize environment then it is also recommended that you take a snapshot of the System Manager virtual machine.

Stop the below Services as root user

systemctl stop crond.service
systemctl stop jboss.service
systemctl stop postgresql.service
systemctl stop spiritAgent.service
systemctl stop cnd.service
systemctl stop systemMonitor.service

Update Commands

Before upgrading JAVA, Copy following files to /swlibrary location:

1. cp $JAVA_HOME/jre/lib/security/java.security /swlibrary/java.security
2. cp $JAVA_HOME/jre/lib/security/java.policy /swlibrary/java.policy
3. cp $JAVA_HOME/jre/lib/security/blacklisted.certs /swlibrary/blacklisted.certs

Update critical RPMs

yum install java-1.8.0-openjdk-debuginfo-1.8.0.342.b07-1.el7_9.x86_64 java-1.8.0-openjdk-headless-1.8.0.362.b08-1.el7_9.x86_64 java-1.8.0-openjdk-devel-1.8.0.362.b08-1.el7_9.x86_64 java-1.8.0-openjdk-1.8.0.362.b08-1.el7_9.x86_64

Restore following files:

cd /swlibrary
cp -f java.security java.policy blacklisted.certs $JAVA_HOME/jre/lib/security/
cd $JAVA_HOME/jre/lib/security/
chown admin:admin java.security java.policy blacklisted.certs
chmod 644 java.security java.policy blacklisted.certs

Update all non-Critical RPMs

yum update -x "java-1.8.0-* postgresql13-* net-snmp redhat-release-server"

Update all critical RPMs with security fixes only

N/A

Post Update

After updating RPMs please reboot System Manager machine instance.

Once the System Manager is up and running post reboot, enable Geo redundancy (Note: this should be done only after you have patched the Secondary System Manager using the same set of instructions)

If you took a snapshot, make sure you remove them once you have successfully completed the process and System Manager is back up and running.

Avaya Aura® Communication Manager 8.1.3.8

Avaya Aura® Communication Manager critical RPM version list

glibc-2.17-326.el7_9.i686
glibc-2.17-326.el7_9.x86_64
glibc-common-2.17-326.el7_9.x86_64
kernel-3.10.0-1160.88.1.el7.x86_64
kernel-headers-3.10.0-1160.88.1.el7.x86_64
kernel-tools-3.10.0-1160.88.1.el7.x86_64
kernel-tools-libs-3.10.0-1160.88.1.el7.x86_64
openssh-clients-7.4p1-22.el7_9.x86_64
openssh-7.4p1-22.el7_9.x86_64
openssh-server-7.4p1-22.el7_9.x86_64
pam-1.1.8-23.el7.x86_64
pam-1.1.8-23.el7.i686

Avaya Aura® Communication Manager do not update RPM version list

redhat-release-server-7.6-4.el7.x86_64
initscripts-9.49.46-1.el7.x86_64

Avaya Aura® Communication Manager optional RPM versions list

If you have used the Avaya version of net-snmp and bash offered at installation time you should not upgrade these and instead use the versions provided by Avaya. You can confirm if you have the Avaya version of net-snmp and/or bash by executing ‘rpm -qa net-snmp*’ and ‘rpm -qa bash*’ and comparing the versions to the Optional Avaya RPMversions listed below or by the ‘AV’ indicator in the version.
The Avaya bash rpm offers additional command logging capability and the Avaya net-snmp rpm offers better performance for SNMP calls when used with Avaya Aura © Communication Manager than the RedHat version and therefore is more suitable if high numbers of SNMP calls will be made against CM although you may choose not to install the Avaya version should you wish to be able to update these with the latest RHEL versions.
To restore the Red Hat version of bash and net-snmp use ‘yum downgrade bash’, ‘yum downgrade net-snmp*’

bash-4.2.46-31.el7.AV1.x86_64
net-snmp-5.7.2-37.el7.AV1.x86_64
net-snmp-agent-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-utils-5.7.2-37.el7.AV1.x86_64

How to Upgrade Communication Manager RPMs

Avaya recommends taking a Communication Manager backup before performing the updates.

Pre Update

Before updating RPMs it is recommended that a full CM backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Communication Manager guide
In a duplex system the RPM update should be done on the standby machine and CM processing should be stopped with a Busy-Out.

Update Commands

Update all critical RPMs with security fixes

yum install glibc-2.17-326.el7_9.i686 glibc-2.17-326.el7_9.x86_64 glibc-common-2.17-326.el7_9.x86_64 kernel-3.10.0-1160.88.1.el7.x86_64 kernel-tools-3.10.0-1160.88.1.el7.x86_64 kernel-tools-libs-3.10.0-1160.88.1.el7.x86_64 kernel-headers-3.10.0-1160.88.1.el7.x86_64 openssh-7.4p1-22.el7_9.x86_64 openssh-clients-7.4p1-22.el7_9.x86_64 openssh-server-7.4p1-22.el7_9.x86_64 pam-1.1.8-23.el7.i686 pam-1.1.8-23.el7.x86_64

Remove the SW-only installation rpm no longer required (optional)

rpm -e -v --nodeps avaya-cm-setup

Update all non-Critical RPMs

yum update -x 'glibc-* kernel-* openssh-* pam-* initscripts redhat-release-server nscd'

Post Update

When the RPM installation is complete restart the virtual machine by issuing the 'reboot' command.
A PAM rpm update can cause login failures to the SAT or the web SMI, if it is the case run these commands as root:
ln -sf /opt/ecs/lib/pam_unix_auth_x86_64.so /usr/lib64/security/pam_unix_auth.so
ln -sf /opt/ecs/lib/pam_unix_auth_i686.so /usr/lib/security/pam_unix_auth.so

Avaya Aura® Session Manager 8.1.3.8

Avaya Aura® Session Manager Avaya tested critical RPM versions list

None

Avaya Aura® Session Manager do not update RPM version list

nginx
postgresql13-*

How to Upgrade Session Manager RPMs

IMPORTANT: Any non-RHEL repositories should be disabled prior to executing any updates. If non-RHEL repositories are being used, it is recommended that /etc/yum.conf be edited to include:

*exclude=nginx postgresql13-**

Pre Update

Avaya recommends taking a Session Manager backup before performing the updates.
This process is service affecting. Session Manager will be out-of-service until it is placed back into "Accept New Service".

1. Place the SM in **Deny New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.

c. Click **Service State**.
d. From the drop-down list box, select **Deny New Service**.
e. Before updating On the confirmation page, click **Confirm**.

2. On the **Session Manager Dashboard** page, wait until **Active Call Count** is zero. Refresh the screen to update the count.
3. Take a VM snapshot prior to making changes.
4. Stop SM with **stop -ac**.
5. Configure yum to point to a Red Hat 7 repository containing the updates.

Update Commands

Update All Non-Critical RPMs

yum update -x "nginx postgresql13-*"

Update Critical with security fixes

N/A

Post Update

After the update, the SM can be placed back in service by:

1. From the SM command line run: **bash /opt/ASMpatch/bin/setup_java.sh**
2. Reboot the SM.
3. From System Manager web console, select **Elements > Session Manager > System Tools > Maintenance Tests.**
   a. Select the Session Manager that was updated.
   b. Select **Execute all Tests.**
   c. Verify that all tests pass. If not, refer to *Troubleshooting Avaya Aura® Session Manager and Maintaining Avaya Aura® Session Manager*.
4. Place the SM in **Accept New Service**.
   a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
   b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
   c. Click **Service State**.
   d. From the drop-down list box, select **Accept New Service**.
   e. On the confirmation page, click **Confirm**.
5. Remove the VM snapshot taken prior to the update.

Avaya Aura® Media Server 8.X

Avaya Aura® Media Server critical RPM versions list

None currently

Avaya Aura® Media Server do not update RPM versions list

None currently

Avaya Aura® Application Enablement Services 8.1.3.8

Avaya Aura® Application Enablement Services critical RPM version list

None

Avaya Aura® Application Enablement Services do not update RPM version list

axis-1.4-AV7.i386
log4j-1.2.17-16.el7_4.noarch
php-7.4.2-1.el7.remi.x86_64
php-cli-7.4.2-1.el7.remi.x86_64
php-common-7.4.2-1.el7.remi.x86_64
php-json-7.4.2-1.el7.remi.x86_64
php-mbstring-7.4.2-1.el7.remi.x86_64
php-soap-7.4.2-1.el7.remi.x86_64
php-xml-7.4.2-1.el7.remi.x86_64
postgresql-9.2.24-1.el7_5.x86_64
postgresql-jdbc-9.2.1002-5.el7.noarch
postgresql-libs-9.2.24-1.el7_5.i686
postgresql-libs-9.2.24-1.el7_5.x86_64
postgresql-server-9.2.24-1.el7_5.x86_64
tomcat-8.5.81-AV.noarch
tomcat-el-3.0-api-8.5.81-AV.noarch
tomcat-jsp-2.3-api-8.5.81-AV.noarch
tomcat-lib-8.5.81-AV.noarch
tomcat-servlet-3.1-api-8.5.81-AV.noarch

Note: log4j updates are given in AES 8.1.3.5. log4j rpm should not be upgraded manually.

How to Upgrade Application Enablement Services RPMs

Pre Update
Note: For upgrading to AE Services 8.1.3.8 in a software-only environment, you must install AE Services 8.1 or 8.1.1 ISO, upgrade it to AE Services 8.1.2.x and then upgrade to AE Services 8.1.3.8

1. Before updating RPMs it is recommended that a full AES backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Application Enablement Services guide.
2. Configure yum to point to a Red Hat 7 repository containing the updates. See Red Hat page for available repositories.
3. Add following line (excluded rpms list) into /etc/yum.conf file**.** "*exclude=axis-*,tomcat-*,redhat-release-server-*,php-*,postgresql -*,log4j-*"*
4. Take backup of the httpd service file- **/usr/lib/systemd/system/httpd.service** in /tmp
5. Take backup of the slapd.conf configuration file - **/etc/openldap/slapd.conf** in /tmp
6. **Important Note: If High Availability is configured, please follow the following steps:**
    a. Update secondary(standby) AES with the OS packages as per the Pre Update, Update and Post Update instructions
    b. Post reboot, wait for aesvcs (*systemctl status aesvcs*) to be in active(running) state.
    c. Synchronize the data between the Primary and the Secondary Server
    d. Perform Failover from Primary to Secondary Server
    e. Update the new Secondary(standby) server with the OS packages as per the Pre Update, Update and Post Update instructions.
    f. Post reboot, wait for aesvcs (*systemctl status aesvcs*) to be in active(running) state.
    g. If required, perform failover from primary to secondary server. (Optional step)

Update Commands

Update All Non-Critical RPMs

yum update -x 'axis-* tomcat-* redhat-release-server-* php-* postgresql-* log4j-*'

Update Critical with security fixes

None

Important Note:
In case the above update command *fails* with the following message:

Transaction check error:
file /etc/openldap/schema/core.schema from install of openldap-servers-2.4.44-20.el7.x86_64 conflicts with file from package aesvcs-userService-config-8.x.x.0.0.x-0.noarch

then perform the following steps:
****Note: The following steps will rebuild the rpm database on your system. Verify that there are no processes with the RPM database files open. Ensure that you have necessary backup.****

- Take back up of existing rpm database by executing below command:
  mv /var/lib/rpm/__db.00 /tmp*
- Rebuild rpm database by executing below command:
  rpm --rebuilddb
- Perform update again by executing below command:
  yum update -x 'axis- tomcat-* redhat-release-server-* php-* postgresql-* log4j-*'*
- If required, restore the rpm database backup that was copied earlier. (**This is an optional step**)

Post Update

- After rpm upgrades check installed "java-1.8.0-openjdk" rpm (rpm -qa | grep java-1.8.0-openjdk) version and recreate "/usr/java/default/" softlink

  cd /usr/java/

  rm -rf default

  ln -s /usr/lib/jvm/java-1.8.0-openjdk default

- If httpd rpm is updated, them rename the file " /etc/httpd/conf.d/autoindex.conf"

  mv /etc/httpd/conf.d/autoindex.conf /etc/httpd/conf.d/autoindex.conf.bkup

  Replace the httpd.service file with the backed up file in service file in Pre Update step

  mv /tmp/httpd.service /usr/lib/systemd/system/httpd.service

  Reload the systemctl daemon: *systemctl daemon-reload* for changes to take effect.

- If openldap rpm is updated, then replace the /etc/openldap/slapd.conf file with the backed up file. The back up was taken in Pre Update Step.
  mv /tmp/slapd.conf /etc/openldap/slapd.conf

- If sudo rpm is being updated, make sure to remove "*session include system-auth*" entry from /etc/pam.d/sudo

  sed -i "/session include system-auth/d" /etc/pam.d/sudo

- If kernel rpm is being updated (> 3.10.1062) and if a DHCP server is configured in the subnet in which AES resides, make the following changes so that AES does not acquire a dynamic IP address post reboot:
  - Edit "/etc/default/grub" to add the highlighted parameter:
    GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb quiet net.ifnames=0 biosdevname=0 rd.neednet=0"
  - Run the command *"grub2-mkconfig -o /boot/grub2/grub.cfg"*

- **Reboot** AES machine instance.

  reboot

Avaya Aura® WebLM (Standalone) 8.1.3.8

Note: Please refer WebLM SW-Only deployment
https://download.avaya.com/css/public/documents/101058240

Avaya Aura® WebLM (Standalone) critical RPM versions list

java-1.8.0-openjdk-headless-1.8.0.372.b07-1.el7_9.x86_64
java-1.8.0-openjdk-devel-1.8.0.372.b07-1.el7_9.x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.51-1.b16.el7_1.x86_64
java-1.8.0-openjdk-1.8.0.372.b07-1.el7_9.x86_64

Avaya Aura® WebLM (Standalone) do not update RPM version list
redhat-release-server-7.6-4.el7.x86_64

yum update -x "redhat-release-server"

How to Upgrade WebLM RPMs

Pre Update

1. If feasible take WebLM instance backup(For VMware take snapshot).
2. Stop below service

   systemctl stop jboss.service

Remove net-snmp RPM:

yum remove net-snmp
(We don't use net-snmp on WebLM, so we need to remove net-snmp irrespective of its any installed version)

Before upgrading JAVA, Copy following files to /opt location:

- cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/java.security /opt/java.security
- cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/java.policy /opt/java.policy
- cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/blacklisted.certs /opt/blacklisted.certs

Update critical RPMs

yum install java-1.8.0-openjdk-debuginfo-1.8.0.51-1.b16.el7_1.x86_64 java-1.8.0-openjdk-headless-1.8.0.372.b07-1.el7_9.x86_64 java-1.8.0-openjdk-devel-1.8.0.372.b07-1.el7_9.x86_64 java-1.8.0-openjdk-1.8.0.372.b07-1.el7_9.x86_64

Restore following files:

cd /opt
cp -f java.security java.policy blacklisted.certs /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/
cd /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/
chmod 644 java.security java.policy blacklisted.certs

Update All Non-Critical RPMs

yum update -x "java-1.8.0-* redhat-release-server"

Update Critical with security fixes
N/A

Post Update

After updating RPMs please reboot WebLM machine instance.

Once installation completed, set the **java path** and reboot the system.

APPENDIX A: PREVIOUS RELEASE SECTION

Avaya only performs RPM testing on the latest version of Avaya applications. The latest version of the product is required to be used for the continued RPM updates. Aura Release 8.1.x is currently the latest version. There will be no additional updates for 8.0 or 8.0.1.x

RELEASE 8.0

Avaya Aura® System Manager 8.0

NOTE: SMGR 8.0.x uses RHEL 7.5 – refer to the *Deploying Avaya Aura® System Manager in Software-Only Environment* guide for more information.

System Manager 8.0 Critical RPMs

None currently

System Manager 8.0 Do Not Update RPMs

java-1.8.0-openjdk-1.8.0.181-3.b13.el7_5.x86_64
java-1.8.0-openjdk-headless-1.8.0.181-3.b13.el7_5.x86_64
java-1.8.0-openjdk-devel-1.8.0.181-3.b13.el7_5.x86_64
postgresql96-contrib-9.6.9-1PGDG.rhel7.x86_64
postgresql96-9.6.9-1PGDG.rhel7.x86_64
postgresql96-server-9.6.9-1PGDG.rhel7.x86_64
postgresql96-libs-9.6.9-1PGDG.rhel7.x86_64
net-snmp-5.7.3-2.smgr.el7.x86_64
openssl-libs-1.0.2k-8.el7.x86_64
openssl-1.0.2k-8.el7.x86_64
rpcbind-0.2.0-44.el7.x86_64
bind-utils-9.9.4-61.el7_5.1.x86_64
bind-license-9.9.4-61.el7_5.1.noarch
bind-libs-9.9.4-61.el7_5.1.x86_64
bind-libs-lite-9.9.4-61.el7_5.1.x86_64
firewalld-filesystem-0.4.4.4-6.el7.noarch
redhat-release-server-7.5-8.el7.x86_64

Avaya Aura® Communication Manager 8.0

Communicaton Manager 8.0 Critical RPMs

glibc-2.17-260.el7.i686
glibc-2.17-260.el7.x86_64
glibc-common-2.17-260.el7.x86_64
kernel-3.10.0-957.el7.x86_64
kernel-tools-3.10.0-957.el7.x86_64
kernel-tools-libs-3.10.0-957.el7.x86_64
openssh-7.4p1-16.el7.x86_64
openssh-server-7.4p1-16.el7.x86_64
openssh-clients-7.4p1-16.el7.x86_64
sudo-1.8.19p2-10.el7.x86_64
pam-1.1.8-18.el7.i686
pam-1.1.8-18.el7.x86_64

initscripts-9.49.39-1.el7.x86_64

Communicaton Manager 8.0 Do Not Update RPMs

bash-4.2.46-29.el7_4.AV1.x86_64 *
net-snmp-5.7.2-28.el7_4.1.AV1.x86_64 *
net-snmp-agent-libs-5.7.2-28.el7_4.1.AV1.x86_64 *
net-snmp-libs-5.7.2-28.el7_4.1.AV1.x86_64 *
net-snmp-utils-5.7.2-28.el7_4.1.AV1.x86_64 *
redhat-release-server-7.4-18.el7.x86_64
* - Only if the optional Avaya provided RPM was installed, there is no need to explicitly exclude those as yum will not update them.

Avaya Aura® Session Manager 8.0

Session Manager 8.0 Critical RPMs

bind-9.9.4-72.el7.x86_64
bind-utils-9.9.4-72.el7.x86_64
bind-libs-lite-9.9.4-72.el7.x86_64
bind-libs-9.9.4-72.el7.x86_64
bind-license-9.9.4-72.el7.noarch
openssl-1.0.2k-16.el7.x86_64
openssl-libs-1.0.2k-16.el7.x86_64
python-firewall-0.4.4.4-6.el7.noarch
firewalld-filesystem-0.4.4.4-6.el7.noarch
firewalld-0.4.4.4-6.el7.noarch
boost-serialization-1.53.0-27.el7.x86_64
pcre-8.32-17.el7.x86_64

Session Manager 8.0 Do Not Update RPMs

java-1.8.0-openjdk-1.8.0.171-8.b10.el7_5.x86_64
java-1.8.0-openjdk-headless-1.8.0.171-8.b10.el7_5.x86_64
java-1.8.0-openjdk-devel-1.8.0.171-8.b10.el7_5.x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.171-8.b10.el7_5.x86_64*****
postgresql96-9.6.1-1PGDG.rhel7.x86_64*****
postgresql96-libs-9.6.1-1PGDG.rhel7.x86_64*****
postgresql96-server-9.6.1-1PGDG.rhel7.x86_64*
nginx-1.12.2-1.el7_4.ngx.x86_64*****
gsoap-2.8.16-8.el7.x86_64*****
redhat-release-server-7.4-18.el7.x86_64
- Indicates that the RPM is included in the SM installer.

Avaya Aura® Application Enablement Services 8.0

AES 8.0 Critical RPMs

kernel-tools-3.10.0-862.3.2.el7.x86_64
kernel-3.10.0-862.3.2.el7.x86_64
kernel-tools-libs-3.10.0-862.3.2.el7.x86_64
java-1.8.0-openjdk-headless-1.8.0.171-8.b10.el7_5.i686
java-1.8.0-openjdk-devel-1.8.0.171-8.b10.el7_5.i686

java-1.8.0-openjdk-1.8.0.171-8.b10.el7_5.i686
python-perf-3.10.0-862.3.2.el7.x86_64
openssl-libs-1.0.2k-12.el7.i686
openssl-1.0.2k-12.el7.x86_64
openssl-libs-1.0.2k-12.el7.x86_64
httpd-2.4.6-67.el7_4.6.x86_64
httpd-tools-2.4.6-67.el7_4.6.x86_64
mod_ssl-2.4.6-67.el7_4.6.x86_64
openssh-server-7.4p1-16.el7.x86_64
openssh-7.4p1-16.el7.x86_64
openssh-clients-7.4p1-16.el7.x86_64

AES 8.0 Do Not Update RPMs

axis-1.4-AV7.i386
mon-0.99.2.6-RHEL5_AV2.noarch
tomcat-7.0.54-2.AV1.noarch
tomcat-el-2.2-api-7.0.54-2.AV1.noarch
tomcat-jsp-2.2-api-7.0.54-2.AV1.noarch
tomcat-lib-7.0.54-2.AV1.noarch
tomcat-servlet-3.0-api-7.0.54-2.AV1.noarch
redhat-release-server-7.4-18.el7.x86_64

Avaya Aura® WebLM 8.0

NOTE: WebLM 8.0.x uses RHEL 7.5 – refer to the *Deploying Avaya Aura® WebLM in Software-Only Environment* guide for more information.

WebLM 8.0 Critical RPMs

None Currently

WebLM 8.0 Do Not Update RPMs

java-1.8.0-openjdk-1.8.0.51-1.b16.el7_1.x86_64
java-1.8.0-openjdk-devel-1.8.0.51-1.b16.el7_1.x86_64
java-1.8.0-openjdk-headless-1.8.0.51-1.b16.el7_1.x86_64
dmidecode-3.0-5.el7.x86_64
redhat-release-server-7.5-8.el7.x86_64

RELEASE 8.0.1

Avaya Aura® System Manager 8.0.1

NOTE: SMGR 8.0.x uses RHEL 7.5 – refer to the *Deploying Avaya Aura® System Manager in Software-Only Environment* guide for more information.

Avaya Aura® System Manager critical RPM versions list

None currently

Avaya Aura® System Manager do not update RPM version list

java-1.8.0-openjdk-1.8.0.191.b12-1.el7_6.x86_64
java-1.8.0-openjdk-devel-1.8.0.191.b12-1.el7_6.x86_64
java-1.8.0-openjdk-headless-1.8.0.191.b12-1.el7_6.x86_64
postgresql96-contrib-9.6.9-1PGDG.rhel7.x86_64
postgresql96-9.6.9-1PGDG.rhel7.x86_64
postgresql96-server-9.6.9-1PGDG.rhel7.x86_64
postgresql96-libs-9.6.9-1PGDG.rhel7.x86_64
net-snmp-5.7.3-2.smgr.el7.x86_64
openssl-libs-1.0.2k-16.el7.x86_64
openssl-1.0.2k-16.el7.x86_64
openssl-libs-1.0.2k-16.el7.i686
xmlsec1-openssl-1.2.20-7.el7_4.x86_64
rpcbind-0.2.0-44.el7.x86_64
bind-utils-9.9.4-61.el7_5.1.x86_64
bind-license-9.9.4-61.el7_5.1.noarch
bind-libs-lite-9.9.4-61.el7_5.1.x86_64
bind-libs-9.9.4-61.el7_5.1.x86_64
firewalld-filesystem-0.4.4.4-14.el7.noarch
redhat-release-server-7.5-8.el7.x86_64

How to Upgrade System Manager RPMs

Avaya recommends taking a System Manager backup before performing the updates.

Pre Update

Stop the below Services as root user

```
systemctl stop crond.service

systemctl stop jboss.service
systemctl stop postgresql.service
systemctl stop spiritAgent.service
systemctl stop cnd.service
```

Update Commands

Update all non-Critical RPMs

yum update -x ‘java-1.8.0-* postgresql96-* net-snmp-* openssl-* rpcbind-* bind-* firewalld-filesystem-* redhat-release-server’

Update all critical RPMs with security fixes only

None

Post Update

After updating RPMs please reboot System Manager machine instance.

Avaya Aura® Communication Manager critical RPM version list

glibc-2.17-260.el7.i686
glibc-2.17-260.el7.x86_64
glibc-common-2.17-260.el7.x86_64
kernel-3.10.0-957.1.3.el7.x86_64
kernel-tools-3.10.0-957.1.3.el7.x86_64
kernel-tools-libs-3.10.0-957.1.3.el7.x86_64
openssh-7.4p1-16.el7.x86_64
openssh-server-7.4p1-16.el7.x86_64
openssh-clients-7.4p1-16.el7.x86_64
pam-1.1.8-18.el7.i686
pam-1.1.8-18.el7.x86_64
sudo-1.8.19p2-10.el7.x86_64
initscripts-9.49.39-1.el7.x86_64

Avaya Aura® Communication Manager do not update RPM version list

bash-4.2.46-29.el7_4.AV1.x86_64
net-snmp-5.7.2-28.el7_4.1.AV1.x86_64
net-snmp-agent-libs-5.7.2-28.el7_4.1.AV1.x86_64
net-snmp-libs-5.7.2-28.el7_4.1.AV1.x86_64
net-snmp-utils-5.7.2-28.el7_4.1.AV1.x86_64
redhat-release-server-7.4-18.el7.x86_64

Avaya Aura® Communication Manager optional RPM versions list

If you have used the Avaya version of net-snmp and bash offered at installation time you should not upgrade these and instead use the versions provided by Avaya. You can confirm if you have the Avaya version of net-snmp and/or bash by executing ‘rpm -qa net-snmp*’ and ‘rpm -qa bash*’ and comparing the versions to the Optional Avaya RPMversions listed below or by the ‘AV’ indicator in the version.
The Avaya bash rpm offers additional command logging capability and the Avaya net-snmp rpm offers better performance for SNMP calls when used with Avaya Aura © Communication Manager than the RedHat version and therefore is more suitable if high numbers of SNMP calls will be made against CM although you may choose not to install the Avaya version should you wish to be able to update these with the latest RHEL versions.

bash-4.2.46-29.el7_4.AV1.x86_64
net-snmp-5.7.2-28.el7_4.1.AV1.x86_64
net-snmp-agent-libs-5.7.2-28.el7_4.1.AV1.x86_64
net-snmp-libs-5.7.2-28.el7_4.1.AV1.x86_64
net-snmp-utils-5.7.2-28.el7_4.1.AV1.x86_64

How to Upgrade Communication Manager RPMs

Avaya recommends taking a Communication Manager backup before performing the updates.

Pre Update

Before updating RPMs it is recommended that a full CM backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Communication Manager guide
In a duplex system the RPM update should be done on the standby machine and CM processing should be stopped with a Busy-Out.

Update Commands

Update all non-Critical RPMs

yum update -x 'glibc-* kernel-* openssh-* pam-* sudo initscripts redhat-release-server'

Update all critical RPMs with security fixes

yum install glibc-2.17-260.el7.i686 glibc-2.17-260.el7.x86_64 glibc-common-2.17-260.el7.x86_64 kernel-3.10.0-957.1.3.el7.x86_64 kernel-tools-3.10.0-957.1.3.el7.x86_64 kernel-tools-libs-3.10.0-957.1.3.el7.x86_64 kernel-devel-3.10.0-957.1.3.el7.x86_64 openssh-7.4p1-16.el7.x86_64 openssh-server-7.4p1-16.el7.x86_64 openssh-clients-7.4p1-16.el7.x86_64 pam-1.1.8-18.el7.x86_64 sudo-1.8.19p2-10.el7.x86_64 initscripts-9.49.39-1.el7.x86_64

Post Update

When the RPM installation is complete restart the virtual machine by issuing the 'reboot' command.

Avaya Aura® Session Manager 8.0.1

Avaya Aura® Session Manager Avaya tested critical RPM versions list

python-firewall-0.4.4.4-6.el7.noarch
firewalld-filesystem-0.4.4.4-6.el7.noarch
firewalld-0.4.4.4-6.el7.noarch

Avaya Aura® Session Manager do not update RPM version list

java-1.8.0-openjdk-1.8.0.191.b12-0.el7_5.x86_64
java-1.8.0-openjdk-headless-1.8.0.191.b12-0.el7_5.x86_64
java-1.8.0-openjdk-devel-1.8.0.191.b12-0.el7_5.x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.191.b12-0.el7_5.x86_64
postgresql96-9.6.1-1PGDG.rhel7.x86_64
postgresql96-libs-9.6.1-1PGDG.rhel7.x86_64
postgresql96-server-9.6.1-1PGDG.rhel7.x86_64
nginx-1.12.2-1.el7_4.ngx.x86_64
gsoap-2.8.16-8.el7.x86_64
redhat-release-server-7.4-18.el7.x86_64
initscripts-9.49.39-1.el7.x86_64

How to Upgrade Session Manager RPMs

Pre Update

Avaya recommends taking a Session Manager backup before performing the updates.
This process is service affecting. Session Manager will be out-of-service until it is placed back into "Accept New Service".

1. Place the SM in **Deny New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Deny New Service**.
    e. Before updating On the confirmation page, click **Confirm**.
2. On the **Session Manager Dashboard** page, wait until **Active Call Count** is zero. Refresh the screen to update the count.
3. Take a VM snapshot prior to making changes.
4. Stop SM with **stop -ac**.

5. Configure yum to point to a Red Hat 7 repository containing the updates.

Update Commands

Update All Non-Critical RPMs

yum update -x 'java-* python-firewall firewalld-* gsoap postgresql96-* nginx redhat-release-server initscripts'

Update Critical with security fixes

yum update firewalld-0.4.4.4-6 firewalld-filesystem-0.4.4.4-6 python-firewall-0.4.4.4-6

Post Update

After the update, the SM can be placed back in service by:

1. Reboot the SM.
2. From System Manager web console, select **Elements > Session Manager > System Tools > Maintenance Tests.**
    a. Select the Session Manager that was updated.
    b. Select **Execute all Tests.**
    c. Verify that all tests pass. If not, refer to *Troubleshooting Avaya Aura® Session Manager and Maintaining Avaya Aura® Session Manager*.
3. Place the SM in **Accept New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Accept New Service**.
    e. On the confirmation page, click **Confirm**.
4. Remove the VM snapshot taken prior to the update.

Avaya Aura® Media Server 8.0

Avaya Aura® Media Server critical RPM versions list

None currently

Avaya Aura® Media Server do not update RPM versions list

None currently

Avaya Aura® Application Enablement Services 8.0.1

Avaya Aura® Application Enablement Services critical RPM version list

None

Avaya Aura® Application Enablement Services do not update RPM version list

axis-1.4-AV7.i386
mon-0.99.2.6-RHEL5_AV2.noarch

tomcat-8.5.34-6.AV1.noarch
tomcat-el-3.0-api-8.5.34-6.AV1.noarch
tomcat-jsp-2.3-api-8.5.34-6.AV1.noarch
tomcat-lib-8.5.34-6.AV1.noarch
tomcat-servlet-3.1-api-8.5.34-6.AV1.noarch
redhat-release-server-7.4-18.el7.x86_64

How to Upgrade Application Enablement Services RPMs

Pre Update

1. Before updating RPMs it is recommended that a full AES backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Application Enablement Services guide
2. Add following line (excluded rpms list) into /etc/yum.conf file. "exclude=axis-*,mon-*,tomcat-*,redhat-release-server-*"

Update Commands

Update All Non-Critical RPMs

yum update -x 'axis-* mon-* tomcat-* redhat-release-server-*'

Update Critical with security fixes

None

Post Update

After rpm upgrades check installed "java-1.8.0-openjdk" rpm (rpm -qa | grep java-1.8.0-openjdk) version and recreate "/usr/java/default/" softlink
cd /usr/java/

rm -rf default

ln -s /usr/lib/jvm/java-1.8.0-openjdk default

If sudo rpm is being updated, make sure to remove "session include system-auth" entry from /etc/pam.d/sudo

sed -i "/session include system-auth/d" /etc/pam.d/sudo

reboot

Avaya Aura® WebLM (Standalone) 8.0.1

NOTE: WebLM 8.0.x uses RHEL 7.5 – refer to the *Deploying Avaya Aura® WebLM in Software-Only Environment* guide for more information.

Avaya Aura® WebLM (Standalone) critical RPM versions list

None currently

Avaya Aura® WebLM (Standalone) do not update RPM version list

java-1.8.0-openjdk-1.8.0.191.b12-1.el7_6.x86_64
java-1.8.0-openjdk-devel-1.8.0.191.b12-1.el7_6.x86_64
java-1.8.0-openjdk-headless-1.8.0.191.b12-1.el7_6.x86_64
dmidecode-3.0-5.el7.x86_64

redhat-release-server-7.4-18.el7.x86_64
net-snmp-libs-5.7.2-33.el7_5.2.x86_64
redhat-release-server-7.5-8.el7.x86_64

How to Upgrade WebLM RPMs

Pre Update

1. If feasible take WebLM instance backup(For VMware take snapshot).
2. Stop below service

   systemctl stop jboss.service

Update Commands

Update All Non-Critical RPMs

yum update -x "java-1.8.0-* dmidecode-* redhat-release-server "

Update Critical with security fixes

None

Post Update

After updating RPMs please reboot WebLM machine instance.

RELEASE 8.0.1.1

Avaya Aura® System Manager 8.0.1.1

NOTE: SMGR 8.0.x uses RHEL 7.5 – refer to the *Deploying Avaya Aura® System Manager in Software-Only Environment* guide for more information.

Avaya Aura® System Manager critical RPM versions list

None currently

Avaya Aura® System Manager do not update RPM version list

java-1.8.0-openjdk-1.8.0.191.b12-1.el7_6.x86_64
java-1.8.0-openjdk-devel-1.8.0.191.b12-1.el7_6.x86_64
java-1.8.0-openjdk-headless-1.8.0.191.b12-1.el7_6.x86_64
postgresql96-contrib-9.6.9-1PGDG.rhel7.x86_64
postgresql96-9.6.9-1PGDG.rhel7.x86_64
postgresql96-server-9.6.9-1PGDG.rhel7.x86_64
postgresql96-libs-9.6.9-1PGDG.rhel7.x86_64
net-snmp-5.7.3-2.smgr.el7.x86_64

openssl-libs-1.0.2k-16.el7.x86_64
openssl-1.0.2k-16.el7.x86_64
openssl-libs-1.0.2k-16.el7.i686
xmlsec1-openssl-1.2.20-7.el7_4.x86_64
rpcbind-0.2.0-44.el7.x86_64
bind-utils-9.9.4-73.el7_6.x86_64
bind-license-9.9.4-73.el7_6.noarch
bind-libs-lite-9.9.4-73.el7_6.x86_64
bind-libs-9.9.4-73.el7_6.x86_64
firewalld-filesystem-0.4.4.4-14.el7.noarch
redhat-release-server-7.5-8.el7.x86_64

How to Upgrade System Manager RPMs

Avaya recommends taking a System Manager backup before performing the updates.

Pre Update

Stop the below Services as root user

systemctl stop crond.service

systemctl stop jboss.service
systemctl stop postgresql.service
systemctl stop spiritAgent.service
systemctl stop cnd.service

Update Commands

Update all non-Critical RPMs

yum update -x "java-1.8.0-* postgresql96-* net-snmp-* openssl-* rpcbind-* bind-* firewalld-filesystem-* redhat-release-server"

Update all critical RPMs with security fixes only

N/A

Post Update

After updating RPMs please reboot System Manager machine instance.

Avaya Aura® Communication Manager 8.0.1.1

Avaya Aura® Communication Manager critical RPM version list

glibc-2.17-260.el7.i686
glibc-2.17-260.el7.x86_64
glibc-common-2.17-260.el7.x86_64
kernel-3.10.0-957.5.1.el7.x86_64
kernel-tools-3.10.0-957.5.1.el7.x86_64
kernel-tools-libs-3.10.0-957.5.1.el7.x86_64
openssh-7.4p1-16.el7.x86_64

openssh-server-7.4p1-16.el7.x86_64
openssh-clients-7.4p1-16.el7.x86_64
pam-1.1.8-18.el7.i686
pam-1.1.8-18.el7.x86_64
sudo-1.8.19p2-10.el7.x86_64
initscripts-9.49.39-1.el7.x86_64

Avaya Aura® Communication Manager do not update RPM version list

bash-4.2.46-29.el7_4.AV1.x86_64
net-snmp-5.7.2-28.el7_4.1.AV1.x86_64
net-snmp-agent-libs-5.7.2-28.el7_4.1.AV1.x86_64
net-snmp-libs-5.7.2-28.el7_4.1.AV1.x86_64
net-snmp-utils-5.7.2-28.el7_4.1.AV1.x86_64
redhat-release-server-7.4-18.el7.x86_64

Avaya Aura® Communication Manager optional RPM versions list

If you have used the Avaya version of net-snmp and bash offered at installation time you should not upgrade these and instead use the versions provided by Avaya. You can confirm if you have the Avaya version of net-snmp and/or bash by executing ‘rpm -qa net-snmp*’ and ‘rpm -qa bash*’ and comparing the versions to the Optional Avaya RPMversions listed below or by the ‘AV’ indicator in the version.
The Avaya bash rpm offers additional command logging capability and the Avaya net-snmp rpm offers better performance for SNMP calls when used with Avaya Aura © Communication Manager than the RedHat version and therefore is more suitable if high numbers of SNMP calls will be made against CM although you may choose not to install the Avaya version should you wish to be able to update these with the latest RHEL versions.

bash-4.2.46-29.el7_4.AV1.x86_64
net-snmp-5.7.2-28.el7_4.1.AV1.x86_64
net-snmp-agent-libs-5.7.2-28.el7_4.1.AV1.x86_64
net-snmp-libs-5.7.2-28.el7_4.1.AV1.x86_64
net-snmp-utils-5.7.2-28.el7_4.1.AV1.x86_64

How to Upgrade Communication Manager RPMs

Avaya recommends taking a Communication Manager backup before performing the updates.

Pre Update

Before updating RPMs it is recommended that a full CM backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Communication Manager guide
In a duplex system the RPM update should be done on the standby machine and CM processing should be stopped with a Busy-Out.

Update Commands

Update all non-Critical RPMs

yum update -x 'glibc-* kernel-* openssh-* pam-* sudo initscripts redhat-release-server'

Update all critical RPMs with security fixes

yum install glibc-2.17-260.el7.i686 glibc-2.17-260.el7.x86_64 glibc-common-2.17-260.el7.x86_64 kernel-3.10.0-957.5.1.el7.x86_64 kernel-tools-3.10.0-957.5.1.el7.x86_64 kernel-tools-libs-3.10.0-957.5.1.el7.x86_64 kernel-devel-3.10.0-957.5.1.el7.x86_64 openssh-7.4p1-16.el7.x86_64 openssh-server-7.4p1-16.el7.x86_64 openssh-clients-7.4p1-16.el7.x86_64 pam-1.1.8-18.el7.x86_64 sudo-1.8.19p2-10.el7.x86_64 initscripts-9.49.39-1.el7.x86_64

Post Update

When the RPM installation is complete restart the virtual machine by issuing the 'reboot' command.

Avaya Aura® Session Manager 8.0.1.1

Avaya Aura® Session Manager Avaya tested critical RPM versions list

None currently

Avaya Aura® Session Manager do not update RPM version list

java-1.8.0-openjdk-1.8.0.191.b12-0.el7_5.x86_64
java-1.8.0-openjdk-headless-1.8.0.191.b12-0.el7_5.x86_64
java-1.8.0-openjdk-devel-1.8.0.191.b12-0.el7_5.x86_64

How to Upgrade Session Manager RPMs

Pre Update

Avaya **recommends taking a Session Manager backup before performing the updates.**
This process is service affecting. Session Manager will be out-of-service until it is placed back into "Accept New Service".

1. Place the SM in **Deny New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Deny New Service**.
    e. Before updating On the confirmation page, click **Confirm**.
2. On the **Session Manager Dashboard** page, wait until **Active Call Count** is zero. Refresh the screen to update the count.
3. Take a VM snapshot prior to making changes.
4. Stop SM with **stop -ac**.
5. Configure yum to point to a Red Hat 7 repository containing the updates.

Update Commands

Update All Non-Critical RPMs

yum update -x "java-*"

Update Critical with security fixes

N/A

Post Update

After the update, the SM can be placed back in service by:

1. Reboot the SM.
2. From System Manager web console, select **Elements > Session Manager > System Tools > Maintenance Tests.**
    a. Select the Session Manager that was updated.
    b. Select **Execute all Tests.**
    c. Verify that all tests pass. If not, refer to *Troubleshooting Avaya Aura® Session Manager and Maintaining Avaya Aura® Session Manager*.
3. Place the SM in **Accept New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.

b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
c. Click **Service State**.
d. From the drop-down list box, select **Accept New Service**.
e. On the confirmation page, click **Confirm**.

4. Remove the VM snapshot taken prior to the update.

Avaya Aura® Media Server 8.0.X

Avaya Aura® Media Server critical RPM versions list

None currently

Avaya Aura® Media Server do not update RPM versions list

None currently

Avaya Aura® Application Enablement Services 8.0.1.1

Avaya Aura® Application Enablement Services critical RPM version list

None

Avaya Aura® Application Enablement Services do not update RPM version list

axis-1.4-AV7.i386
mon-0.99.2.6-RHEL5_AV2.noarch
tomcat-8.5.34-6.AV1.noarch
tomcat-el-3.0-api-8.5.34-6.AV1.noarch
tomcat-jsp-2.3-api-8.5.34-6.AV1.noarch
tomcat-lib-8.5.34-6.AV1.noarch
tomcat-servlet-3.1-api-8.5.34-6.AV1.noarch
redhat-release-server-7.4-18.el7.x86_64

How to Upgrade Application Enablement Services RPMs

Pre Update

1. Before updating RPMs it is recommended that a full AES backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Application Enablement Services guide
2. Add following line (excluded rpms list) into /etc/yum.conf file. "exclude=axis-*,mon-*,tomcat-*,redhat-release-server-*"

Update Commands

Update All Non-Critical RPMs

yum update -x 'axis-* ~~bash-*~~ mon-* tomcat-* redhat-release-server-*'

Update Critical with security fixes

None

Post Update

After rpm upgrades check installed "java-1.8.0-openjdk" rpm (rpm -qa | grep java-1.8.0-openjdk) version and recreate "/usr/java/default/" softlink
cd /usr/java/

rm -rf default

ln -s /usr/lib/jvm/java-1.8.0-openjdk default

If sudo rpm is being updated, make sure to remove "session include system-auth" entry from /etc/pam.d/sudo

sed -i "/session include system-auth/d" /etc/pam.d/sudo

reboot

Avaya Aura® WebLM (Standalone) 8.0.1.1

NOTE: WebLM 8.0.x uses RHEL 7.5 – refer to the *Deploying Avaya Aura® WebLM in Software-Only Environment* guide for more information.

Avaya Aura® WebLM (Standalone) critical RPM versions list

None currently

Avaya Aura® WebLM (Standalone) do not update RPM version list

java-1.8.0-openjdk-1.8.0.191.b12-1.el7_6.x86_64
java-1.8.0-openjdk-devel-1.8.0.191.b12-1.el7_6.x86_64
java-1.8.0-openjdk-headless-1.8.0.191.b12-1.el7_6.x86_64
dmidecode-3.0-5.el7.x86_64
redhat-release-server-7.4-18.el7.x86_64
net-snmp-libs-5.7.2-33.el7_5.2.x86_64
redhat-release-server-7.5-8.el7.x86_64

How to Upgrade WebLM RPMs

Pre Update

1. If feasible take WebLM instance backup(For VMware take snapshot).
2. Stop below service

```
systemctl stop jboss.service
```

Update Commands

Update All Non-Critical RPMs

yum update -x "java-1.8.0-* dmidecode net-snmp-libs redhat-release-server"

Update Critical with security fixes

N/A

Post Update

After updating RPMs please reboot WebLM machine instance.

RELEASE 8.1.0

Avaya Aura® System Manager 8.1

Avaya Aura® System Manager critical RPM versions list

None currently

Avaya Aura® System Manager do not update RPM version list

java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-1.8.0.212.b04-0.el7_6.x86_64
postgresql96-9.6.12-1PGDG.rhel7.x86_64
postgresql96-contrib-9.6.12-1PGDG.rhel7.x86_64
postgresql96-server-9.6.12-1PGDG.rhel7.x86_64
postgresql96-libs-9.6.12-1PGDG.rhel7.x86_64
redhat-release-server-7.6-4.el7.x86_64

How to Upgrade System Manager RPMs

Avaya recommends taking a System Manager backup before performing the updates.

Pre Update

Stop the below Services as root user

systemctl stop crond.service

systemctl stop jboss.service
systemctl stop postgresql.service
systemctl stop spiritAgent.service
systemctl stop cnd.service

Update Commands

Update all non-Critical RPMs

yum update -x "java-1.8.0-* postgresql96-* redhat-release-server"

Update all critical RPMs with security fixes only

N/A

Post Update

After updating RPMs please reboot System Manager machine instance.

Avaya Aura® Communication Manager 8.1

Avaya Aura® Communication Manager critical RPM version list

glibc-2.17-260.el7_6.4.i686
glibc-2.17-260.el7_6.4.x86_64
glibc-common-2.17-260.el7_6.4.x86_64
initscripts-9.49.46-1.el7.x86_64
kernel-3.10.0-957.10.1.el7.x86_64
kernel-tools-3.10.0-957.10.1.el7.x86_64
kernel-tools-libs-3.10.0-957.10.1.el7.x86_64
openssh-7.4p1-16.el7.x86_64
openssh-clients-7.4p1-16.el7.x86_64
openssh-server-7.4p1-16.el7.x86_64
pam-1.1.8-22.el7.i686
pam-1.1.8-22.el7.x86_64

Avaya Aura® Communication Manager do not update RPM version list

redhat-release-server-7.6-4.el7.x86_64
initscripts-9.49.46-1.el7.x86_64

Avaya Aura® Communication Manager optional RPM versions list

If you have used the Avaya version of net-snmp and bash offered at installation time you should not upgrade these and instead use the versions provided by Avaya. You can confirm if you have the Avaya version of net-snmp and/or bash by executing ‘rpm -qa net-snmp*’ and ‘rpm -qa bash*’ and comparing the versions to the Optional Avaya RPMversions listed below or by the ‘AV’ indicator in the version.
The Avaya bash rpm offers additional command logging capability and the Avaya net-snmp rpm offers better performance for SNMP calls when used with Avaya Aura © Communication Manager than the RedHat version and therefore is more suitable if high numbers of SNMP calls will be made against CM although you may choose not to install the Avaya version should you wish to be able to update these with the latest RHEL versions.

bash-4.2.46-31.el7.AV1.x86_64
net-snmp-5.7.2-37.el7.AV1.x86_64
net-snmp-agent-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-utils-5.7.2-37.el7.AV1.x86_64

How to Upgrade Communication Manager RPMs

Avaya recommends taking a Communication Manager backup before performing the updates.

Pre Update

Before updating RPMs it is recommended that a full CM backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Communication Manager guide

In a duplex system the RPM update should be done on the standby machine and CM processing should be stopped with a Busy-Out.

Update Commands

Update all non-Critical RPMs

yum update -x 'glibc-* kernel-* openssh-* pam-* initscripts redhat-release-server'

Update all critical RPMs with security fixes

yum install glibc-2.17-260.el7_6.4.i686 glibc-2.17-260.el7_6.4.x86_64 glibc-common-2.17-260.el7_6.4.x86_64 kernel-3.10.0-957.10.1.el7.x86_64 kernel-tools-3.10.0-957.10.1.el7.x86_64 kernel-tools-libs-3.10.0-957.10.1.el7.x86_64 kernel-devel-3.10.0-957.10.1.el7.x86_64 openssh-7.4p1-16.el7.x86_64 openssh-clients-7.4p1-16.el7.x86_64 openssh-server-7.4p1-16.el7.x86_64 pam-1.1.8-22.el7.i686 pam-1.1.8-22.el7.x86_64

Post Update

When the RPM installation is complete restart the virtual machine by issuing the 'reboot' command.

Avaya Aura® Session Manager 8.1

Avaya Aura® Session Manager Avaya tested critical RPM versions list

None currently

Avaya Aura® Session Manager do not update RPM version list

None currently

How to Upgrade Session Manager RPMs

Pre Update

Avaya recommends taking a Session Manager backup before performing the updates.
This process is service affecting. Session Manager will be out-of-service until it is placed back into "Accept New Service".

1. Place the SM in **Deny New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Deny New Service**.
    e. Before updating On the confirmation page, click **Confirm**.
2. On the **Session Manager Dashboard** page, wait until **Active Call Count** is zero. Refresh the screen to update the count.
3. Take a VM snapshot prior to making changes.
4. Stop SM with **stop -ac**.
5. Configure yum to point to a Red Hat 7 repository containing the updates.

Update Commands

Update All Non-Critical RPMs

N/A

Update Critical with security fixes

N/A

Post Update

After the update, the SM can be placed back in service by:

1. Reboot the SM.
2. From System Manager web console, select **Elements > Session Manager > System Tools > Maintenance Tests.**
    a. Select the Session Manager that was updated.
    b. Select **Execute all Tests.**
    c. Verify that all tests pass. If not, refer to *Troubleshooting Avaya Aura® Session Manager and Maintaining Avaya Aura® Session Manager*.
3. Place the SM in **Accept New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Accept New Service**.
    e. On the confirmation page, click **Confirm**.
4. Remove the VM snapshot taken prior to the update.

Avaya Aura® Media Server 8.X

Avaya Aura® Media Server critical RPM versions list

None currently

Avaya Aura® Media Server do not update RPM versions list

None currently

Avaya Aura® Application Enablement Services 8.1

Avaya Aura® Application Enablement Services critical RPM version list

None

Avaya Aura® Application Enablement Services do not update RPM version list

axis-1.4-AV7.i386
mon-0.99.2.6-RHEL5_AV2.noarch
tomcat-8.5.34-6.AV1.noarch
tomcat-el-3.0-api-8.5.34-6.AV1.noarch
tomcat-jsp-2.3-api-8.5.34-6.AV1.noarch
tomcat-lib-8.5.34-6.AV1.noarch
tomcat-servlet-3.1-api-8.5.34-6.AV1.noarch
redhat-release-server-7.6-4.el7.x86_64

How to Upgrade Application Enablement Services RPMs

Pre Update

1. Before updating RPMs it is recommended that a full AES backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Application Enablement Services guide
2. Add following line (excluded rpms list) into /etc/yum.conf file. "exclude=axis-*,mon-*,tomcat-*,redhat-release-server-*"

Update Commands

Update All Non-Critical RPMs

yum update -x 'axis-* mon-* tomcat-* redhat-release-server-*'

Update Critical with security fixes

None

Post Update

After rpm upgrades check installed "java-1.8.0-openjdk" rpm (rpm -qa | grep java-1.8.0-openjdk) version and recreate "/usr/java/default/" softlink:

cd /usr/java/

rm -rf default

ln -s /usr/lib/jvm/java-1.8.0-openjdk default

If sudo rpm is being updated, make sure to remove "session include system-auth" entry from /etc/pam.d/sudo

sed -i "/session include system-auth/d" /etc/pam.d/sudo

reboot

Avaya Aura® WebLM (Standalone) 8.1

Avaya Aura® WebLM (Standalone) critical RPM versions list

None currently

Avaya Aura® WebLM (Standalone) do not update RPM version list

java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-1.8.0.212.b04-0.el7_6.x86_64
redhat-release-server-7.6-4.el7.x86_64

How to Upgrade WebLM RPMs

Pre Update

1. If feasible take WebLM instance backup(For VMware take snapshot).
2. Stop below service

   systemctl stop jboss.service

Update Commands

Update All Non-Critical RPMs

yum update -x "java-1.8.0-* redhat-release-server"

Update Critical with security fixes

N/A

Post Update

After updating RPMs please reboot WebLM machine instance.

RELEASE 8.1.1
Avaya Aura® System Manager 8.1.1

Avaya Aura® System Manager critical RPM versions list

None currently

Avaya Aura® System Manager do not update RPM version list

java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-1.8.0.212.b04-0.el7_6.x86_64
postgresql96-9.6.12-1PGDG.rhel7.x86_64
postgresql96-contrib-9.6.12-1PGDG.rhel7.x86_64
postgresql96-server-9.6.12-1PGDG.rhel7.x86_64
postgresql96-libs-9.6.12-1PGDG.rhel7.x86_64
redhat-release-server-7.6-4.el7.x86_64

How to Upgrade System Manager RPMs

Avaya recommends taking a System Manager backup before performing the updates.

Pre Update

Stop the below Services as root user

systemctl stop crond.service

systemctl stop jboss.service
systemctl stop postgresql.service
systemctl stop spiritAgent.service
systemctl stop cnd.service

Update Commands

Update all non-Critical RPMs

yum update -x "java-1.8.0-* postgresql96-* redhat-release-server"

Update all critical RPMs with security fixes only

N/A

Post Update

After updating RPMs please reboot System Manager machine instance.

Avaya Aura® Communication Manager 8.1.1

Avaya Aura® Communication Manager critical RPM version list

glibc-2.17-292.el7.i686
glibc-2.17-292.el7.x86_64
glibc-common-2.17-292.el7.x86_64
kernel-3.10.0-1062.1.2.el7.x86_64
kernel-tools-3.10.0-1062.1.2.el7.x86_64
kernel-tools-libs-3.10.0-1062.1.2.el7.x86_64
openssh-7.4p1-21.el7.x86_64
openssh-clients-7.4p1-21.el7.x86_64
openssh-server-7.4p1-21.el7.x86_64
pam-1.1.8-22.el7.i686
pam-1.1.8-22.el7.x86_64

Avaya Aura® Communication Manager do not update RPM version list

redhat-release-server-7.6-4.el7.x86_64
initscripts-9.49.46-1.el7.x86_64

Avaya Aura® Communication Manager optional RPM versions list

If you have used the Avaya version of net-snmp and bash offered at installation time you should not upgrade these and instead use the versions provided by Avaya. You can confirm if you have the Avaya version of net-snmp and/or bash by executing ‘rpm -qa net-snmp*’ and ‘rpm -qa bash*’ and comparing the versions to the Optional Avaya RPM versions listed below or by the ‘AV’ indicator in the version.
The Avaya bash rpm offers additional command logging capability and the Avaya net-snmp rpm offers better performance for SNMP calls when used with Avaya Aura © Communication Manager than the RedHat version and therefore is more suitable if high numbers of SNMP calls will be made against CM although you may choose not to install the Avaya version should you wish to be able to update these with the latest RHEL versions.

bash-4.2.46-31.el7.AV1.x86_64
net-snmp-5.7.2-37.el7.AV1.x86_64
net-snmp-agent-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-utils-5.7.2-37.el7.AV1.x86_64

How to Upgrade Communication Manager RPMs

Avaya recommends taking a Communication Manager backup before performing the updates.

Pre Update

Before updating RPMs it is recommended that a full CM backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Communication Manager guide
In a duplex system the RPM update should be done on the standby machine and CM processing should be stopped with a Busy-Out.

Update Commands

Update all non-Critical RPMs

yum update -x 'glibc-* kernel-* openssh-* pam-* initscripts redhat-release-server'

Update all critical RPMs with security fixes

yum install glibc-2.17-292.el7.i686 glibc-2.17-292.el7.x86_64 glibc-common-2.17-292.el7.x86_64 kernel-3.10.0-1062.1.2.el7.x86_64 kernel-tools-3.10.0-1062.1.2.el7.x86_64 kernel-tools-libs-3.10.0-1062.1.2.el7.x86_64 openssh-7.4p1-21.el7.x86_64 openssh-clients-7.4p1-21.el7.x86_64 openssh-server-7.4p1-21.el7.x86_64 pam-1.1.8-22.el7.i686 pam-1.1.8-22.el7.x86_64

Post Update

When the RPM installation is complete restart the virtual machine by issuing the 'reboot' command.

Avaya Aura® Session Manager 8.1.1

Avaya Aura® Session Manager Avaya tested critical RPM versions list

None currently

Avaya Aura® Session Manager do not update RPM version list

None currently

How to Upgrade Session Manager RPMs

Pre Update

Avaya recommends taking a Session Manager backup before performing the updates.
This process is service affecting. Session Manager will be out-of-service until it is placed back into "Accept New Service".

6. Place the SM in **Deny New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Deny New Service**.
    e. Before updating On the confirmation page, click **Confirm**.
7. On the **Session Manager Dashboard** page, wait until **Active Call Count** is zero. Refresh the screen to update the count.
8. Take a VM snapshot prior to making changes.
9. Stop SM with **stop -ac**.
10. Configure yum to point to a Red Hat 7 repository containing the updates.

Update Commands

Update All Non-Critical RPMs

N/A

Update Critical with security fixes

N/A

Post Update

After the update, the SM can be placed back in service by:

6. Reboot the SM.
7. From System Manager web console, select **Elements > Session Manager > System Tools > Maintenance Tests.**
    a. Select the Session Manager that was updated.
    b. Select **Execute all Tests.**
    c. Verify that all tests pass. If not, refer to *Troubleshooting Avaya Aura® Session Manager and Maintaining Avaya Aura® Session Manager*.
8. Place the SM in **Accept New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Accept New Service**.
    e. On the confirmation page, click **Confirm**.
9. Remove the VM snapshot taken prior to the update.

Avaya Aura® Media Server 8.X

Avaya Aura® Media Server critical RPM versions list

None currently

Avaya Aura® Media Server do not update RPM versions list

None currently

Avaya Aura® Application Enablement Services 8.1.1

Avaya Aura® Application Enablement Services critical RPM version list

None

Avaya Aura® Application Enablement Services do not update RPM version list

axis-1.4-AV7.i386
mon-0.99.2.6-RHEL5_AV2.noarch
redhat-release-server-7.6-4.el7.x86_64
tomcat-8.5.42-6.AV1.noarch
tomcat-el-3.0-api-8.5.42-6.AV1.noarch
tomcat-jsp-2.3-api-8.5.42-6.AV1.noarch
tomcat-lib-8.5.42-6.AV1.noarch
tomcat-servlet-3.1-api-8.5.42-6.AV1.noarch

How to Upgrade Application Enablement Services RPMs

Pre Update

7. Before updating RPMs it is recommended that a full AES backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Application Enablement Services guide
8. Add following line (excluded rpms list) into /etc/yum.conf file. "exclude=axis-*,mon-*,tomcat-*,redhat-release-server-*"

Update Commands

Update All Non-Critical RPMs

yum update -x 'axis-* mon-* tomcat-* redhat-release-server-*'

Update Critical with security fixes

None

Post Update

After rpm upgrades check installed "java-1.8.0-openjdk" rpm (rpm -qa | grep java-1.8.0-openjdk) version and recreate "/usr/java/default/" softlink:

cd /usr/java/

rm -rf default

ln -s /usr/lib/jvm/java-1.8.0-openjdk default

If sudo rpm is being updated, make sure to remove "session include system-auth" entry from /etc/pam.d/sudo

sed -i "/session include system-auth/d" /etc/pam.d/sudo

reboot

Avaya Aura® WebLM (Standalone) 8.1.1

Avaya Aura® WebLM (Standalone) critical RPM versions list

None currently

Avaya Aura® WebLM (Standalone) do not update RPM version list

java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.51-1.b16.el7_1.x86_64
java-1.8.0-openjdk-1.8.0.212.b04-0.el7_6.x86_64
redhat-release-server-7.6-4.el7.x86_64

How to Upgrade WebLM RPMs

Pre Update

1. If feasible take WebLM instance backup(For VMware take snapshot).

2. Stop below service

```
systemctl stop jboss.service
```

Update Commands

Update All Non-Critical RPMs

yum update -x "java-1.8.0-* redhat-release-server"

Update Critical with security fixes

N/A

Post Update

After updating RPMs please reboot WebLM machine instance.

RELEASE 8.1.2

Avaya Aura® System Manager 8.1.2

Avaya Aura® System Manager critical RPM versions list

None currently

Avaya Aura® System Manager do not update RPM version list

java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-1.8.0.212.b04-0.el7_6.x86_64
postgresql96-9.6.12-1PGDG.rhel7.x86_64
postgresql96-contrib-9.6.12-1PGDG.rhel7.x86_64
postgresql96-server-9.6.12-1PGDG.rhel7.x86_64
postgresql96-libs-9.6.12-1PGDG.rhel7.x86_64
redhat-release-server-7.6-4.el7.x86_64

How to Upgrade System Manager RPMs

Avaya recommends taking a System Manager backup before performing the updates.

Pre Update

Stop the below Services as root user

```
systemctl stop crond.service

systemctl stop jboss.service
systemctl stop postgresql.service
systemctl stop spiritAgent.service
systemctl stop cnd.service
```

Update Commands

Update all non-Critical RPMs

yum update -x "java-1.8.0-* postgresql96-* redhat-release-server"

Update all critical RPMs with security fixes only

N/A

Post Update

After updating RPMs please reboot System Manager machine instance.

Avaya Aura® Communication Manager 8.1.2

Avaya Aura® Communication Manager critical RPM version list

glibc-2.17-292.el7.i686
glibc-2.17-292.el7.x86_64
glibc-common-2.17-292.el7.x86_64
kernel-3.10.0-1062.9.1.el7.x86_64
kernel-tools-3.10.0-1062.9.1.el7.x86_64
kernel-tools-libs-3.10.0-1062.9.1.el7.x86_64
openssh-7.4p1-21.el7.x86_64
openssh-clients-7.4p1-21.el7.x86_64
openssh-server-7.4p1-21.el7.x86_64
pam-1.1.8-22.el7.i686
pam-1.1.8-22.el7.x86_64

Avaya Aura® Communication Manager do not update RPM version list

redhat-release-server-7.6-4.el7.x86_64
initscripts-9.49.46-1.el7.x86_64

Avaya Aura® Communication Manager optional RPM versions list

If you have used the Avaya version of net-snmp and bash offered at installation time you should not upgrade these and instead use the versions provided by Avaya. You can confirm if you have the Avaya version of net-snmp and/or bash by executing ‘rpm -qa net-snmp*’ and ‘rpm -qa bash*’ and comparing the versions to the Optional Avaya RPMversions listed below or by the ‘AV’ indicator in the version.
The Avaya bash rpm offers additional command logging capability and the Avaya net-snmp rpm offers better performance for SNMP calls when used with Avaya Aura © Communication Manager than the RedHat version and therefore is more suitable if high numbers of SNMP calls will be made against CM although you may choose not to install the Avaya version should you wish to be able to update these with the latest RHEL versions.

bash-4.2.46-31.el7.AV1.x86_64
net-snmp-5.7.2-37.el7.AV1.x86_64
net-snmp-agent-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-utils-5.7.2-37.el7.AV1.x86_64

How to Upgrade Communication Manager RPMs

Avaya recommends taking a Communication Manager backup before performing the updates.

Pre Update

Before updating RPMs it is recommended that a full CM backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Communication Manager guide
In a duplex system the RPM update should be done on the standby machine and CM processing should be stopped with a Busy-Out.

Update Commands

Update all non-Critical RPMs

yum update -x 'glibc-* kernel-* openssh-* pam-* initscripts redhat-release-server'

Update all critical RPMs with security fixes

yum install glibc-2.17-292.el7.i686 glibc-2.17-292.el7.x86_64 glibc-common-2.17-292.el7.x86_64 kernel-3.10.0-1062.9.1.el7.x86_64 kernel-tools-3.10.0-1062.9.1.el7.x86_64 kernel-tools-libs-3.10.0-1062.9.1.el7.x86_64 openssh-7.4p1-21.el7.x86_64 openssh-clients-7.4p1-21.el7.x86_64 openssh-server-7.4p1-21.el7.x86_64 pam-1.1.8-22.el7.i686 pam-1.1.8-22.el7.x86_64

Post Update

When the RPM installation is complete restart the virtual machine by issuing the 'reboot' command.

Avaya Aura® Session Manager 8.1.2

Avaya Aura® Session Manager Avaya tested critical RPM versions list

None currently

Avaya Aura® Session Manager do not update RPM version list

None currently

How to Upgrade Session Manager RPMs

Pre Update

Avaya recommends taking a Session Manager backup before performing the updates.
This process is service affecting. Session Manager will be out-of-service until it is placed back into "Accept New Service".

11. Place the SM in **Deny New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Deny New Service**.
    e. Before updating On the confirmation page, click **Confirm**.
12. On the **Session Manager Dashboard** page, wait until **Active Call Count** is zero. Refresh the screen to update the count.
13. Take a VM snapshot prior to making changes.
14. Stop SM with **stop -ac**.
15. Configure yum to point to a Red Hat 7 repository containing the updates.

Update Commands

Update All Non-Critical RPMs

N/A

Update Critical with security fixes

N/A

Post Update

After the update, the SM can be placed back in service by:

10. Reboot the SM.
11. From System Manager web console, select **Elements > Session Manager > System Tools > Maintenance Tests.**
    a. Select the Session Manager that was updated.
    b. Select **Execute all Tests.**
    c. Verify that all tests pass. If not, refer to *Troubleshooting Avaya Aura® Session Manager and Maintaining Avaya Aura® Session Manager*.
12. Place the SM in **Accept New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Accept New Service**.
    e. On the confirmation page, click **Confirm**.
13. Remove the VM snapshot taken prior to the update.

Avaya Aura® Media Server 8.X

Avaya Aura® Media Server critical RPM versions list

None currently

Avaya Aura® Media Server do not update RPM versions list

None currently

Avaya Aura® Application Enablement Services 8.1.2

Avaya Aura® Application Enablement Services critical RPM version list

None

Avaya Aura® Application Enablement Services do not update RPM version list

axis-1.4-AV7.i386
mon-0.99.2.6-RHEL5_AV2.noarch
redhat-release-server-7.6-4.el7.x86_64
tomcat-8.5.42-6.AV1.noarch
tomcat-el-3.0-api-8.5.42-6.AV1.noarch
tomcat-jsp-2.3-api-8.5.42-6.AV1.noarch
tomcat-lib-8.5.42-6.AV1.noarch
tomcat-servlet-3.1-api-8.5.42-6.AV1.noarch

How to Upgrade Application Enablement Services RPMs

Pre Update

9. Before updating RPMs it is recommended that a full AES backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Application Enablement Services guide
10. Add following line (excluded rpms list) into /etc/yum.conf file. "exclude=axis-*,bash-*,mon-*,tomcat-*,redhat-release-server-*,libuuid-* initscripts-*"

Update Commands

Update All Non-Critical RPMs

yum update -x 'axis-* mon-* tomcat-* redhat-release-server-*'

Update Critical with security fixes

None

Post Update

After rpm upgrades check installed "java-1.8.0-openjdk" rpm (rpm -qa | grep java-1.8.0-openjdk) version and recreate "/usr/java/default/" softlink
cd /usr/java/

rm -rf default

ln -s /usr/lib/jvm/java-1.8.0-openjdk default

If sudo rpm is being updated, make sure to remove "session include system-auth" entry from /etc/pam.d/sudo

sed -i "/session include system-auth/d" /etc/pam.d/sudo

reboot

Avaya Aura® WebLM (Standalone) 8.1.2

Avaya Aura® WebLM (Standalone) critical RPM versions list

None currently

Avaya Aura® WebLM (Standalone) do not update RPM version list

java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.51-1.b16.el7_1.x86_64
java-1.8.0-openjdk-1.8.0.212.b04-0.el7_6.x86_64
redhat-release-server-7.6-4.el7.x86_64

How to Upgrade WebLM RPMs

Pre Update

3. If feasible take WebLM instance backup(For VMware take snapshot).

4. Stop below service

   systemctl stop jboss.service

Update Commands

Update All Non-Critical RPMs

yum update -x "java-1.8.0-* redhat-release-server"

Update Critical with security fixes

N/A

Post Update

After updating RPMs please reboot WebLM machine instance.

RELEASE 8.1.3

IMPORTANT: Any non-RHEL repositories should be disabled prior to executing any updates.
To list enabled repositories execute:

yum repolist enabled

Any non-RHEL repositories should be disabled by setting “enable=0” in the corresponding /etc/yum.repo.d file.
Failure to do so may cause issues with the Avaya application.

Avaya Aura® System Manager 8.1.3

Avaya Aura® System Manager critical RPM versions list

None currently

Avaya Aura® System Manager do not update RPM version list

java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-1.8.0.212.b04-0.el7_6.x86_64
postgresql96-9.6.12-1PGDG.rhel7.x86_64
postgresql96-contrib-9.6.12-1PGDG.rhel7.x86_64
postgresql96-server-9.6.12-1PGDG.rhel7.x86_64
postgresql96-libs-9.6.12-1PGDG.rhel7.x86_64
net-snmp-5.7.3-2.smgr.el7.x86_64
redhat-release-server-7.6-4.el7.x86_64

How to Upgrade System Manager RPMs

Avaya recommends taking a System Manager backup before performing the updates.

Pre Update

Stop the below Services as root user

systemctl stop crond.service

systemctl stop jboss.service
systemctl stop postgresql.service
systemctl stop spiritAgent.service
systemctl stop cnd.service

Update Commands

Update all non-Critical RPMs

yum update -x "java-1.8.0-* postgresql96-* net-snmp redhat-release-server"

Update all critical RPMs with security fixes only

N/A

Post Update

After updating RPMs please reboot System Manager machine instance.

IMPORTANT NOTE– Restart system monitor service manually if it is not in running state after reboot.

- Login to System Manager CLI using administrative account and then switch to root account.
- Run the command to check system monitor service status "**systemctl status systemMonitor.service**"
- If the System Monitor service is not running then run the command "**systemctl start systemMonitor.service**" to start service.

Avaya Aura® Communication Manager 8.1.3

Avaya Aura® Communication Manager critical RPM version list

glibc-2.17-292.el7.i686
glibc-2.17-292.el7.x86_64
glibc-common-2.17-292.el7.x86_64
kernel-3.10.0-1127.19.1.el7.x86_64
kernel-tools-libs-3.10.0-1127.19.1.el7.x86_64
kernel-tools-3.10.0-1127.19.1.el7.x86_64
openssh-clients-7.4p1-21.el7.x86_64
openssh-7.4p1-21.el7.x86_64
openssh-server-7.4p1-21.el7.x86_64
pam-1.1.8-22.el7.x86_64
pam-1.1.8-22.el7.i686

Avaya Aura® Communication Manager do not update RPM version list

redhat-release-server-7.6-4.el7.x86_64
initscripts-9.49.46-1.el7.x86_64

Avaya Aura® Communication Manager optional RPM versions list

If you have used the Avaya version of net-snmp and bash offered at installation time you should not upgrade these and instead use the versions provided by Avaya. You can confirm if you have the Avaya version of net-snmp and/or bash by

executing ‘rpm -qa net-snmp*’ and ‘rpm -qa bash*’ and comparing the versions to the Optional Avaya RPMversions listed below or by the ‘AV’ indicator in the version.
The Avaya bash rpm offers additional command logging capability and the Avaya net-snmp rpm offers better performance for SNMP calls when used with Avaya Aura © Communication Manager than the RedHat version and therefore is more suitable if high numbers of SNMP calls will be made against CM although you may choose not to install the Avaya version should you wish to be able to update these with the latest RHEL versions.

bash-4.2.46-31.el7.AV1.x86_64
net-snmp-5.7.2-37.el7.AV1.x86_64
net-snmp-agent-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-utils-5.7.2-37.el7.AV1.x86_64

Note An updated CM 8.1 SW-only .iso file for use in new installations is available for download from PLDS: CM-08.1.0.0.890-e67-1.iso, PLDS ID CM000001544.

How to Upgrade Communication Manager RPMs

Avaya recommends taking a Communication Manager backup before performing the updates.

Pre Update

Before updating RPMs it is recommended that a full CM backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Communication Manager guide
In a duplex system the RPM update should be done on the standby machine and CM processing should be stopped with a Busy-Out.

Update Commands

Update all critical RPMs with security fixes

yum install glibc-2.17-292.el7.i686 glibc-2.17-292.el7.x86_64 glibc-common-2.17-292.el7.x86_64 kernel-3.10.0-1127.19.1.el7.x86_64 kernel-tools-3.10.0-1127.19.1.el7.x86_64 kernel-tools-libs-3.10.0-1127.19.1.el7.x86_64 openssh-7.4p1-21.el7.x86_64 openssh-clients-7.4p1-21.el7.x86_64 openssh-server-7.4p1-21.el7.x86_64 pam-1.1.8-22.el7.i686 pam-1.1.8-22.el7.x86_64

Remove the SW-only installation rpm no longer required

rpm -e -v --nodeps avaya-cm-setup

Update all non-Critical RPMs

yum update -x 'glibc-* kernel-* openssh-* pam-* initscripts redhat-release-server'

Post Update

When the RPM installation is complete restart the virtual machine by issuing the 'reboot' command.

Avaya Aura® Session Manager 8.1.3

Avaya Aura® Session Manager Avaya tested critical RPM versions list

None currently

Avaya Aura® Session Manager do not update RPM version list

nginx
postgres96-*

How to Upgrade Session Manager RPMs

IMPORTANT: Any non-RHEL repositories should be disabled prior to executing any updates. If non-RHEL repositories are being used, it is recommended that /etc/yum.conf be edited to include:

*exclude=nginx postgresql96-**

Pre Update

Avaya recommends taking a Session Manager backup before performing the updates.
This process is service affecting. Session Manager will be out-of-service until it is placed back into "Accept New Service".

16. Place the SM in **Deny New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Deny New Service**.
    e. Before updating On the confirmation page, click **Confirm**.
17. On the **Session Manager Dashboard** page, wait until **Active Call Count** is zero. Refresh the screen to update the count.
18. Take a VM snapshot prior to making changes.
19. Stop SM with **stop -ac**.
20. Configure yum to point to a Red Hat 7 repository containing the updates.

Update Commands

Update All Non-Critical RPMs

yum update -x “nginx postgresql96-*”

Update Critical with security fixes

N/A

Post Update

After the update, the SM can be placed back in service by:

14. Reboot the SM.
15. From System Manager web console, select **Elements > Session Manager > System Tools > Maintenance Tests.**
    a. Select the Session Manager that was updated.
    b. Select **Execute all Tests.**
    c. Verify that all tests pass. If not, refer to *Troubleshooting Avaya Aura® Session Manager and Maintaining Avaya Aura® Session Manager*.
16. Place the SM in **Accept New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Accept New Service**.
    e. On the confirmation page, click **Confirm**.
17. Remove the VM snapshot taken prior to the update.

Avaya Aura® Media Server 8.X

Avaya Aura® Media Server critical RPM versions list

None currently

Avaya Aura® Media Server do not update RPM versions list

None currently

Avaya Aura® Application Enablement Services 8.1.3

Avaya Aura® Application Enablement Services critical RPM version list

None

Avaya Aura® Application Enablement Services do not update RPM version list

axis-1.4-AV7.i386
redhat-release-server-7.6-4.el7.x86_64
tomcat-8.5.57-6.AV1.noarch
tomcat-el-3.0-api-8.5.57-6.AV1.noarch
tomcat-jsp-2.3-api-8.5.57-6.AV1.noarch
tomcat-lib-8.5.57-6.AV1.noarch
tomcat-servlet-3.1-api-8.5.57-6.AV1.noarch
php-soap-7.4.2-1.el7.remi.x86_64
php-json-7.4.2-1.el7.remi.x86_64
php-common-7.4.2-1.el7.remi.x86_64
php-7.4.2-1.el7.remi.x86_64
php-cli-7.4.2-1.el7.remi.x86_64
php-xml-7.4.2-1.el7.remi.x86_64
php-mbstring-7.4.2-1.el7.remi.x86_64

How to Upgrade Application Enablement Services RPMs

Pre Update
Note: For upgrading to AE Services 8.1.3 in a software-only environment, you must install AE Services 8.1 or 8.1.1 ISO, upgrade it to AE Services 8.1.2.x and then upgrade to AE Services 8.1.3.

11. Before updating RPMs it is recommended that a full AES backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Application Enablement Services guide.
12. Configure yum to point to a Red Hat 7 repository containing the updates. See Red Hat page for available repositories.
13. Add following line (excluded rpms list) into /etc/yum.conf file**.** "*exclude=axis-*,tomcat-*,redhat-release-server-*,php-*"*
14. Take backup of the httpd service file- **/usr/lib/systemd/system/httpd.service** in /tmp
15. **Important Note: If High Availability is configured, please follow the following steps:**
    a. Update secondary(standby) AES with the OS packages as per the Pre Update, Update and Post Update instructions
    b. Post reboot, wait for aesvcs (*systemctl status aesvcs*) to be in active(running) state.
    c. Synchronize the data between the Primary and the Secondary Server
    d. Perform Failover from Primary to Secondary Server
    e. Update the new Secondary(standby) server with the OS packages as per the Pre Update, Update and Post Update instructions.
    f. Post reboot, wait for aesvcs (*systemctl status aesvcs*) to be in active(running) state.

g. If required, perform failover from primary to secondary server. (Optional step)

Update Commands

Update All Non-Critical RPMs

yum update -x 'axis- tomcat-* redhat-release-server-* php-*'*

Update Critical with security fixes

None

Important Note:
In case the above update command *fails* with the following message:

Transaction check error:
file /etc/openldap/schema/core.schema from install of openldap-servers-2.4.44-20.el7.x86_64 conflicts with file from package aesvcs-userService-config-8.x.x.0.0.x-0.noarch

then perform the following steps:

****Note: The following steps will rebuild the rpm database on your system. Verify that there are no processes with the RPM database files open. Ensure that you have necessary backup.****

- Take back up of existing rpm database by executing below command:
  mv /var/lib/rpm/__db.00 /tmp*
- Rebuild rpm database by executing below command:
  rpm --rebuilddb
- Perform update again by executing below command:
  yum update -x 'axis- tomcat-* redhat-release-server-* php-*'*
- If required, restore the rpm database backup that was copied earlier. (**This is an optional step**)

Post Update

- After rpm upgrades check installed "java-1.8.0-openjdk" rpm (rpm -qa | grep java-1.8.0-openjdk) version and recreate "/usr/java/default/" softlink

  cd /usr/java/

  rm -rf default

  ln -s /usr/lib/jvm/java-1.8.0-openjdk default

- If httpd rpm is updated, them rename the file " /etc/httpd/conf.d/autoindex.conf"

  mv /etc/httpd/conf.d/autoindex.conf /etc/httpd/conf.d/autoindex.conf.bkup

  Replace the httpd.service file with the backed up file in service file in Pre Update step

  mv /tmp/httpd.service /usr/lib/systemd/system/httpd.service

  Reload the systemctl daemon: *systemctl daemon-reload* for changes to take effect.

- If sudo rpm is being updated, make sure to remove "*session include system-auth*" entry from /etc/pam.d/sudo

  sed -i "/session include system-auth/d" /etc/pam.d/sudo

- If kernel rpm is being updated (> 3.10.1062) and if a DHCP server is configured in the subnet in which AES resides, make the following changes so that AES does not acquire a dynamic IP address post reboot:

- Edit "/etc/default/grub" to add the highlighted parameter:
  GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb quiet net.ifnames=0 biosdevname=0 rd.neednet=0"
- Run the command *"grub2-mkconfig -o /boot/grub2/grub.cfg"*

- **Reboot** AES machine instance.

  reboot

Avaya Aura® WebLM (Standalone) 8.1.3

Avaya Aura® WebLM (Standalone) critical RPM versions list

None currently

Avaya Aura® WebLM (Standalone) do not update RPM version list

java-1.8.0-openjdk-headless-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-devel-1.8.0.212.b04-0.el7_6.x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.51-1.b16.el7_1.x86_64
java-1.8.0-openjdk-1.8.0.212.b04-0.el7_6.x86_64
net-snmp-5.7.2-43.el7_7.3.x86_64
redhat-release-server-7.6-4.el7.x86_64

How to Upgrade WebLM RPMs

Pre Update

5. If feasible take WebLM instance backup(For VMware take snapshot).
6. Stop below service

   systemctl stop jboss.service

Update Commands

Update All Non-Critical RPMs

yum update -x "java-1.8.0-* net-snmp redhat-release-server"

Update Critical with security fixes

N/A

Post Update

After updating RPMs please reboot

RELEASE 8.1.3.1

Aura 8.1.3.1 February 8, 2021 – Certified for Software Only May 11, 2021
This section lists all the latest RPMs for the latest GA version of the products.

IMPORTANT: Any non-RHEL repositories should be disabled prior to executing any updates.
To list enabled repositories execute:

yum repolist enabled

Any non-RHEL repositories should be disabled by setting “enable=0” in the corresponding /etc/yum.repo.d file.
Failure to do so may cause issues with the Avaya application.

Avaya Aura® System Manager 8.1.3.1

Avaya Aura® System Manager critical RPM versions list
Note: java rpms updated from version used in 8.1.3.0.

java-1.8.0-openjdk-debuginfo-1.8.0.272.b10-1.el7_9.x86_64
java-1.8.0-openjdk-headless-1.8.0.272.b10-1.el7_9.x86_64
java-1.8.0-openjdk-devel-1.8.0.272.b10-1.el7_9.x86_64
java-1.8.0-openjdk-1.8.0.272.b10-1.el7_9.x86_64

Avaya Aura® System Manager do not update RPM version list

postgresql96-libs-9.6.17-1PGDG.rhel7.x86_64
postgresql96-9.6.17-1PGDG.rhel7.x86_64
postgresql96-contrib-9.6.17-1PGDG.rhel7.x86_64
postgresql96-server-9.6.17-1PGDG.rhel7.x86_64
net-snmp-5.7.3-2.smgr.el7.x86_64
redhat-release-server-7.6-4.el7.x86_64

How to Upgrade System Manager RPMs
Avaya recommends taking a System Manager backup before performing the updates.

Pre Update
If you have a Geo Redundancy setup of System Manager disable Geo as a first step.
If your System Manager is deployed in a virtualize environment then it is also recommended that you take a snapshot of the System Manager virtual machine.

Stop the below Services as root user

systemctl stop crond.service
systemctl stop jboss.service
systemctl stop postgresql.service
systemctl stop spiritAgent.service
systemctl stop cnd.service
systemctl stop systemMonitor.service

Update Commands

Update critical RPMs

yum install java-1.8.0-openjdk-debuginfo-1.8.0.272.b10-1.el7_9.x86_64 java-1.8.0-openjdk-headless-1.8.0.272.b10-1.el7_9.x86_64 java-1.8.0-openjdk-devel-1.8.0.272.b10-1.el7_9.x86_64 java-1.8.0-openjdk-1.8.0.272.b10-1.el7_9.x86_64

Update all non-Critical RPMs

yum update -x "java-1.8.0-* postgresql96-* net-snmp redhat-release-server"

Update all critical RPMs with security fixes only

N/A

Post Update

After updating RPMs please reboot System Manager machine instance.

Once the System Manager is up and running post reboot, enable Geo redundancy (Note: this should be done only after you have patched the Secondary System Manager using the same set of instructions)

If you took a snapshot, make sure you remove them once you have successfully completed the process and System Manager is back up and running.

IMPORTANT NOTE– Restart system monitor service manually if it is not in running state after reboot.

- Login to System Manager CLI using administrative account and then switch to root account.
- Run the command to check system monitor service status "**systemctl status systemMonitor.service**"

If the System Monitor service is not running then run the command "**systemctl start systemMonitor.service**" to start service.

Avaya Aura® Communication Manager 8.1.3.1

Avaya Aura® Communication Manager critical RPM version list

glibc-2.17-323.el7_9.i686
glibc-2.17-323.el7_9.x86_64
glibc-common-2.17-323.el7_9.x86_64
kernel-3.10.0-1160.11.1.el7.x86_64
kernel-tools-libs-3.10.0-1160.11.1.el7.x86_64
kernel-tools-3.10.0-1160.11.1.el7.x86_64
openssh-clients-7.4p1-21.el7.x86_64
openssh-7.4p1-21.el7.x86_64
openssh-server-7.4p1-21.el7.x86_64
pam-1.1.8-23.el7.x86_64
pam-1.1.8-23.el7.i686

Avaya Aura® Communication Manager do not update RPM version list

redhat-release-server-7.6-4.el7.x86_64
initscripts-9.49.46-1.el7.x86_64

Avaya Aura® Communication Manager optional RPM versions list

If you have used the Avaya version of net-snmp and bash offered at installation time you should not upgrade these and instead use the versions provided by Avaya. You can confirm if you have the Avaya version of net-snmp and/or bash by executing 'rpm -qa net-snmp*' and 'rpm -qa bash*' and comparing the versions to the Optional Avaya RPMversions listed below or by the 'AV' indicator in the version.
The Avaya bash rpm offers additional command logging capability and the Avaya net-snmp rpm offers better performance for SNMP calls when used with Avaya Aura © Communication Manager than the RedHat version and therefore is more suitable if high numbers of SNMP calls will be made against CM although you may choose not to install the Avaya version should you wish to be able to update these with the latest RHEL versions.

bash-4.2.46-31.el7.AV1.x86_64
net-snmp-5.7.2-37.el7.AV1.x86_64
net-snmp-agent-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-utils-5.7.2-37.el7.AV1.x86_64

How to Upgrade Communication Manager RPMs

Avaya recommends taking a Communication Manager backup before performing the updates.

Pre Update

Before updating RPMs it is recommended that a full CM backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Communication Manager guide
In a duplex system the RPM update should be done on the standby machine and CM processing should be stopped with a Busy-Out.

Update Commands

Update all critical RPMs with security fixes

yum install glibc-2.17-323.el7_9.i686 glibc-2.17-323.el7_9.x86_64 glibc-common-2.17-323.el7_9.x86_64 kernel-3.10.0-1160.11.1.el7.x86_64 kernel-tools-3.10.0-1160.11.1.el7.x86_64 kernel-tools-libs-3.10.0-1160.11.1.el7.x86_64 openssh-7.4p1-21.el7.x86_64 openssh-clients-7.4p1-21.el7.x86_64 openssh-server-7.4p1-21.el7.x86_64 pam-1.1.8-23.el7.i686 pam-1.1.8-23.el7.x86_64

Remove the SW-only installation rpm no longer required

rpm -e -v --nodeps avaya-cm-setup

Update all non-Critical RPMs

yum update -x 'glibc-* kernel-* openssh-* pam-* initscripts redhat-release-server'

Post Update

When the RPM installation is complete restart the virtual machine by issuing the 'reboot' command.

Avaya Aura® Session Manager 8.1.3.1

Avaya Aura® Session Manager Avaya tested critical RPM versions list

None currently

Avaya Aura® Session Manager do not update RPM version list

nginx
postgresql96-*

How to Upgrade Session Manager RPMs

IMPORTANT: Any non-RHEL repositories should be disabled prior to executing any updates. If non-RHEL repositories are being used, it is recommended that /etc/yum.conf be edited to include:

*exclude=nginx postgresql96-**

Pre Update

Avaya recommends taking a Session Manager backup before performing the updates.
This process is service affecting. Session Manager will be out-of-service until it is placed back into "Accept New Service".

21. Place the SM in **Deny New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Deny New Service**.
    e. Before updating On the confirmation page, click **Confirm**.

22. On the **Session Manager Dashboard** page, wait until **Active Call Count** is zero. Refresh the screen to update the count.
23. Take a VM snapshot prior to making changes.
24. Stop SM with **stop -ac**.
25. Configure yum to point to a Red Hat 7 repository containing the updates.

Update Commands

Update All Non-Critical RPMs

yum update -x “nginx postgresql96-*”

Update Critical with security fixes

N/A

Post Update

After the update, the SM can be placed back in service by:

18. Reboot the SM.
19. From System Manager web console, select **Elements > Session Manager > System Tools > Maintenance Tests.**
    a. Select the Session Manager that was updated.
    b. Select **Execute all Tests.**
    c. Verify that all tests pass. If not, refer to *Troubleshooting Avaya Aura® Session Manager and Maintaining Avaya Aura® Session Manager*.
20. Place the SM in **Accept New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Accept New Service**.
    e. On the confirmation page, click **Confirm**.
21. Remove the VM snapshot taken prior to the update.

Avaya Aura® Media Server 8.X

Avaya Aura® Media Server critical RPM versions list

None currently

Avaya Aura® Media Server do not update RPM versions list

None currently

Avaya Aura® Application Enablement Services 8.1.3.1

Avaya Aura® Application Enablement Services critical RPM version list

None

Avaya Aura® Application Enablement Services do not update RPM version list

axis-1.4-AV7.i386
redhat-release-server-7.6-4.el7.x86_64
tomcat-8.5.57-6.AV1.noarch
tomcat-el-3.0-api-8.5.57-6.AV1.noarch
tomcat-jsp-2.3-api-8.5.57-6.AV1.noarch
tomcat-lib-8.5.57-6.AV1.noarch
tomcat-servlet-3.1-api-8.5.57-6.AV1.noarch
php-soap-7.4.2-1.el7.remi.x86_64
php-json-7.4.2-1.el7.remi.x86_64
php-common-7.4.2-1.el7.remi.x86_64
php-7.4.2-1.el7.remi.x86_64
php-cli-7.4.2-1.el7.remi.x86_64
php-xml-7.4.2-1.el7.remi.x86_64
php-mbstring-7.4.2-1.el7.remi.x86_64

How to Upgrade Application Enablement Services RPMs

Pre Update

Note: For upgrading to AE Services 8.1.3.1 in a software-only environment, you must install AE Services 8.1 or 8.1.1 ISO, upgrade it to AE Services 8.1.2.x and then upgrade to AE Services 8.1.3.1

16. Before updating RPMs it is recommended that a full AES backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Application Enablement Services guide.
17. Configure yum to point to a Red Hat 7 repository containing the updates. See Red Hat page for available repositories.
18. Add following line (excluded rpms list) into /etc/yum.conf file**.** "*exclude=axis-*,tomcat-*,redhat-release-server-*,php-**"
19. Take backup of the httpd service file- **/usr/lib/systemd/system/httpd.service** in /tmp
20. Take backup of the slapd.conf configuration file - **/etc/openldap/slapd.conf** in /tmp
21. **Important Note: If High Availability is configured, please follow the following steps:**
    a. Update secondary(standby) AES with the OS packages as per the Pre Update, Update and Post Update instructions
    b. Post reboot, wait for aesvcs (*systemctl status aesvcs*) to be in active(running) state.
    c. Synchronize the data between the Primary and the Secondary Server
    d. Perform Failover from Primary to Secondary Server
    e. Update the new Secondary(standby) server with the OS packages as per the Pre Update, Update and Post Update instructions.
    f. Post reboot, wait for aesvcs (*systemctl status aesvcs*) to be in active(running) state.
    g. If required, perform failover from primary to secondary server. (Optional step)

Update Commands

Update All Non-Critical RPMs

yum update -x 'axis-* tomcat-* redhat-release-server-* php-*'

Update Critical with security fixes

None

Important Note:

In case the above update command *fails* with the following message:

Transaction check error:

file /etc/openldap/schema/core.schema from install of openldap-servers-2.4.44-20.el7.x86_64 conflicts with file from package aesvcs-userService-config-8.x.x.0.0.x-0.noarch

then perform the following steps:

****Note: The following steps will rebuild the rpm database on your system. Verify that there are no processes with the RPM database files open. Ensure that you have necessary backup.****

- Take back up of existing rpm database by executing below command:
  mv /var/lib/rpm/__db.00 /tmp*

- Rebuild rpm database by executing below command:
  rpm --rebuilddb
- Perform update again by executing below command:
  yum update -x 'axis- tomcat-* redhat-release-server-* php-*'*
- If required, restore the rpm database backup that was copied earlier. (**This is an optional step**)

Post Update

- After rpm upgrades check installed "java-1.8.0-openjdk" rpm (rpm -qa | grep java-1.8.0-openjdk) version and recreate "/usr/java/default/" softlink

  cd /usr/java/

  rm -rf default

  ln -s /usr/lib/jvm/java-1.8.0-openjdk default

- If httpd rpm is updated, them rename the file " /etc/httpd/conf.d/autoindex.conf"

  mv /etc/httpd/conf.d/autoindex.conf /etc/httpd/conf.d/autoindex.conf.bkup

  Replace the httpd.service file with the backed up file in service file in Pre Update step

  mv /tmp/httpd.service /usr/lib/systemd/system/httpd.service

  Reload the systemctl daemon: *systemctl daemon-reload* for changes to take effect.

- If openldap rpm is updated, then replace the /etc/openldap/slapd.conf file with the backed up file. The back up was taken in Pre Update Step.
  mv /tmp/slapd.conf /etc/openldap/slapd.conf

- If sudo rpm is being updated, make sure to remove "*session include system-auth*" entry from /etc/pam.d/sudo

  sed -i "/session include system-auth/d" /etc/pam.d/sudo

- If kernel rpm is being updated (> 3.10.1062) and if a DHCP server is configured in the subnet in which AES resides, make the following changes so that AES does not acquire a dynamic IP address post reboot:
  - Edit "/etc/default/grub" to add the highlighted parameter:
    GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb quiet net.ifnames=0 biosdevname=0 rd.neednet=0"
  - Run the command *"grub2-mkconfig -o /boot/grub2/grub.cfg"*

- **Reboot** AES machine instance.

  reboot

Avaya Aura® WebLM (Standalone) 8.1.3.1

Avaya Aura® WebLM (Standalone) critical RPM versions list

java-1.8.0-openjdk-debuginfo-1.8.0.272.b10-1.el7_9.x86_64
java-1.8.0-openjdk-headless-1.8.0.272.b10-1.el7_9.x86_64
java-1.8.0-openjdk-devel-1.8.0.272.b10-1.el7_9.x86_64
java-1.8.0-openjdk-1.8.0.272.b10-1.el7_9.x86_64

Avaya Aura® WebLM (Standalone) do not update RPM version list

net-snmp-5.7.2-43.el7_7.3.x86_64
redhat-release-server-7.6-4.el7.x86_64

How to Upgrade WebLM RPMs

Pre Update

7. If feasible take WebLM instance backup(For VMware take snapshot).
8. Stop below service

   systemctl stop jboss.service

Update Commands

Update critical RPMs

yum install java-1.8.0-openjdk-debuginfo-1.8.0.272.b10-1.el7_9.x86_64 java-1.8.0-openjdk-headless-1.8.0.272.b10-1.el7_9.x86_64 java-1.8.0-openjdk-devel-1.8.0.272.b10-1.el7_9.x86_64 java-1.8.0-openjdk-1.8.0.272.b10-1.el7_9.x86_64

Update All Non-Critical RPMs

yum update -x "java-1.8.0-* net-snmp redhat-release-server"

Update Critical with security fixes

N/A

Post Update

After updating RPMs please reboot WebLM machine instance.

RELEASE 8.1.3.2

Aura 8.1.3.2 June 14, 2021 – Certified for Software Only Offer July 09, 2021
This section lists all the latest RPMs for the latest GA version of the products.

IMPORTANT: Any non-RHEL repositories should be disabled prior to executing any updates.
To list enabled repositories execute:
yum repolist enabled
Any non-RHEL repositories should be disabled by setting “enable=0” in the corresponding /etc/yum.repo.d file.
Failure to do so may cause issues with the Avaya application.

Avaya Aura® System Manager 8.1.3.2

Avaya Aura® System Manager critical RPM versions list
Note: java rpms updated from version used in 8.1.3.0.

java-1.8.0-openjdk-debuginfo-1.8.0.292.b10-1.el7_9.x86_64.rpm
java-1.8.0-openjdk-headless-1.8.0.292.b10-1.el7_9.x86_64.rpm
java-1.8.0-openjdk-devel-1.8.0.292.b10-1.el7_9.x86_64.rpm
java-1.8.0-openjdk-1.8.0.292.b10-1.el7_9.x86_64.rpm

Avaya Aura® System Manager do not update RPM version list

postgresql96-libs-9.6.17-1PGDG.rhel7.x86_64
postgresql96-9.6.17-1PGDG.rhel7.x86_64
postgresql96-contrib-9.6.17-1PGDG.rhel7.x86_64
postgresql96-server-9.6.17-1PGDG.rhel7.x86_64
net-snmp-5.7.3-3.smgr.el7.x86_64
redhat-release-server-7.6-4.el7.x86_64

How to Upgrade System Manager RPMs
Avaya recommends taking a System Manager backup before performing the updates.

Pre Update
If you have a Geo Redundancy setup of System Manager disable Geo as a first step.
If your System Manager is deployed in a virtualize environment then it is also recommended that you take a snapshot of the System Manager virtual machine.

Stop the below Services as root user

systemctl stop crond.service
systemctl stop jboss.service
systemctl stop postgresql.service
systemctl stop spiritAgent.service
systemctl stop cnd.service
systemctl stop systemMonitor.service

Update Commands

Before upgrading JAVA, Copy following files to /swlibrary location:

1. cp $JAVA_HOME/jre/lib/security/java.security /swlibrary/java.security
2. cp $JAVA_HOME/jre/lib/security/java.policy /swlibrary/java.policy
3. cp $JAVA_HOME/jre/lib/security/blacklisted.certs /swlibrary/blacklisted.certs

Update critical RPMs

yum install java-1.8.0-openjdk-debuginfo-1.8.0.292.b10-1.el7_9.x86_64 java-1.8.0-openjdk-headless-1.8.0.292.b10-1.el7_9.x86_64 java-1.8.0-openjdk-devel-1.8.0.292.b10-1.el7_9.x86_64 java-1.8.0-openjdk-1.8.0.292.b10-1.el7_9.x86_64

Restore following files:

cd /swlibrary
cp -f java.security java.policy blacklisted.certs $JAVA_HOME/jre/lib/security/
cd $JAVA_HOME/jre/lib/security/
chown admin:admin java.security java.policy blacklisted.certs
chmod 644 java.security java.policy blacklisted.certs

Update all non-Critical RPMs

yum update -x "java-1.8.0-* postgresql96-* net-snmp redhat-release-server"

Update all critical RPMs with security fixes only

N/A

Post Update

After updating RPMs please reboot System Manager machine instance.

Once the System Manager is up and running post reboot, enable Geo redundancy (Note: this should be done only after you have patched the Secondary System Manager using the same set of instructions)

If you took a snapshot, make sure you remove them once you have successfully completed the process and System Manager is back up and running.

IMPORTANT NOTE– Restart system monitor service manually if it is not in running state after reboot.

- Login to System Manager CLI using administrative account and then switch to root account.
- Run the command to check system monitor service status "**systemctl status systemMonitor.service**"

If the System Monitor service is not running then run the command "**systemctl start systemMonitor.service**" to start service.

Avaya Aura® Communication Manager 8.1.3.2

Avaya Aura® Communication Manager critical RPM version list

glibc-2.17-323.el7_9.i686
glibc-2.17-323.el7_9.x86_64
glibc-common-2.17-323.el7_9.x86_64
kernel-3.10.0-1160.24.1.el7.x86_64
kernel-tools-libs-3.10.0-1160.24.1.el7.x86_64
kernel-tools-3.10.0-1160.24.1.el7.x86_64
openssh-clients-7.4p1-21.el7.x86_64
openssh-7.4p1-21.el7.x86_64
openssh-server-7.4p1-21.el7.x86_64
pam-1.1.8-23.el7.x86_64
pam-1.1.8-23.el7.i686

Avaya Aura® Communication Manager do not update RPM version list

redhat-release-server-7.6-4.el7.x86_64
initscripts-9.49.46-1.el7.x86_64

Avaya Aura® Communication Manager optional RPM versions list

If you have used the Avaya version of net-snmp and bash offered at installation time you should not upgrade these and instead use the versions provided by Avaya. You can confirm if you have the Avaya version of net-snmp and/or bash by executing 'rpm -qa net-snmp*' and 'rpm -qa bash*' and comparing the versions to the Optional Avaya RPMversions listed below or by the 'AV' indicator in the version.
The Avaya bash rpm offers additional command logging capability and the Avaya net-snmp rpm offers better performance for SNMP calls when used with Avaya Aura © Communication Manager than the RedHat version and therefore is more suitable if high numbers of SNMP calls will be made against CM although you may choose not to install the Avaya version should you wish to be able to update these with the latest RHEL versions.

bash-4.2.46-31.el7.AV1.x86_64
net-snmp-5.7.2-37.el7.AV1.x86_64
net-snmp-agent-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-utils-5.7.2-37.el7.AV1.x86_64

How to Upgrade Communication Manager RPMs

Avaya recommends taking a Communication Manager backup before performing the updates.

Pre Update

Before updating RPMs it is recommended that a full CM backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Communication Manager guide
In a duplex system the RPM update should be done on the standby machine and CM processing should be stopped with a Busy-Out.

Update Commands

Update all critical RPMs with security fixes

yum install glibc-2.17-323.el7_9.i686 glibc-2.17-323.el7_9.x86_64 glibc-common-2.17-323.el7_9.x86_64 kernel-3.10.0-1160.24.1.el7.x86_64 kernel-tools-3.10.0-1160.24.1.el7.x86_64 kernel-tools-libs-3.10.0-1160.24.1.el7.x86_64 openssh-7.4p1-21.el7.x86_64 openssh-clients-7.4p1-21.el7.x86_64 openssh-server-7.4p1-21.el7.x86_64 pam-1.1.8-23.el7.i686 pam-1.1.8-23.el7.x86_64

Remove the SW-only installation rpm no longer required

rpm -e -v --nodeps avaya-cm-setup

Update all non-Critical RPMs

yum update -x 'glibc-* kernel-* openssh-* pam-* initscripts redhat-release-server nscd'

Post Update

When the RPM installation is complete restart the virtual machine by issuing the 'reboot' command.

Avaya Aura® Session Manager 8.1.3.2

Avaya Aura® Session Manager Avaya tested critical RPM versions list

None currently

Avaya Aura® Session Manager do not update RPM version list

nginx
postgresql96-*

How to Upgrade Session Manager RPMs

IMPORTANT: Any non-RHEL repositories should be disabled prior to executing any updates. If non-RHEL repositories are being used, it is recommended that /etc/yum.conf be edited to include:

*exclude=nginx postgresql96-**

Pre Update

Avaya recommends taking a Session Manager backup before performing the updates.
This process is service affecting. Session Manager will be out-of-service until it is placed back into "Accept New Service".

26. Place the SM in **Deny New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Deny New Service**.
    e. Before updating On the confirmation page, click **Confirm**.
27. On the **Session Manager Dashboard** page, wait until **Active Call Count** is zero. Refresh the screen to update the count.
28. Take a VM snapshot prior to making changes.
29. Stop SM with **stop -ac**.
30. Configure yum to point to a Red Hat 7 repository containing the updates.

Update Commands

Update All Non-Critical RPMs

yum update -x “nginx postgresql96-*”

Update Critical with security fixes

N/A

Post Update

After the update, the SM can be placed back in service by:

22. Reboot the SM.
23. From System Manager web console, select **Elements > Session Manager > System Tools > Maintenance Tests.**
    a. Select the Session Manager that was updated.
    b. Select **Execute all Tests.**
    c. Verify that all tests pass. If not, refer to *Troubleshooting Avaya Aura® Session Manager and Maintaining Avaya Aura® Session Manager*.
24. Place the SM in **Accept New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Accept New Service**.
    e. On the confirmation page, click **Confirm**.
25. Remove the VM snapshot taken prior to the update.

Avaya Aura® Media Server 8.X

Avaya Aura® Media Server critical RPM versions list

None currently

Avaya Aura® Media Server do not update RPM versions list

None currently

Avaya Aura® Application Enablement Services 8.1.3.2

Avaya Aura® Application Enablement Services critical RPM version list

None

Avaya Aura® Application Enablement Services do not update RPM version list

axis-1.4-AV7.i386
php-7.4.2-1.el7.remi.x86_64
php-cli-7.4.2-1.el7.remi.x86_64
php-common-7.4.2-1.el7.remi.x86_64
php-json-7.4.2-1.el7.remi.x86_64
php-mbstring-7.4.2-1.el7.remi.x86_64
php-soap-7.4.2-1.el7.remi.x86_64
php-xml-7.4.2-1.el7.remi.x86_64

tomcat-8.5.57-6.AV1.noarch
tomcat-el-3.0-api-8.5.57-6.AV1.noarch
tomcat-jsp-2.3-api-8.5.57-6.AV1.noarch
tomcat-lib-8.5.57-6.AV1.noarch
tomcat-servlet-3.1-api-8.5.57-6.AV1.noarch

How to Upgrade Application Enablement Services RPMs

Pre Update

Note: For upgrading to AE Services 8.1.3.2 in a software-only environment, you must install AE Services 8.1 or 8.1.1 ISO, upgrade it to AE Services 8.1.2.x and then upgrade to AE Services 8.1.3.2

22. Before updating RPMs it is recommended that a full AES backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Application Enablement Services guide.
23. Configure yum to point to a Red Hat 7 repository containing the updates. See Red Hat page for available repositories.
24. Add following line (excluded rpms list) into /etc/yum.conf file**.** "*exclude=axis-*,tomcat-*,redhat-release-server-*,php-*"*
25. Take backup of the httpd service file- **/usr/lib/systemd/system/httpd.service** in /tmp
26. Take backup of the slapd.conf configuration file - **/etc/openldap/slapd.conf** in /tmp
27. **Important Note: If High Availability is configured, please follow the following steps:**
    a. Update secondary(standby) AES with the OS packages as per the Pre Update, Update and Post Update instructions
    b. Post reboot, wait for aesvcs (*systemctl status aesvcs*) to be in active(running) state.
    c. Synchronize the data between the Primary and the Secondary Server
    d. Perform Failover from Primary to Secondary Server
    e. Update the new Secondary(standby) server with the OS packages as per the Pre Update, Update and Post Update instructions.
    f. Post reboot, wait for aesvcs (*systemctl status aesvcs*) to be in active(running) state.
    g. If required, perform failover from primary to secondary server. (Optional step)

Update Commands

Update All Non-Critical RPMs

yum update -x 'axis-* tomcat-* redhat-release-server-* php-*'

Update Critical with security fixes

None

Important Note:

In case the above update command *fails* with the following message:

Transaction check error:

file /etc/openldap/schema/core.schema from install of openldap-servers-2.4.44-20.el7.x86_64 conflicts with file from package aesvcs-userService-config-8.x.x.0.0.x-0.noarch

then perform the following steps:

****Note: The following steps will rebuild the rpm database on your system. Verify that there are no processes with the RPM database files open. Ensure that you have necessary backup.****

- Take back up of existing rpm database by executing below command:
  mv /var/lib/rpm/__db.00 /tmp*
- Rebuild rpm database by executing below command:
  rpm --rebuilddb
- Perform update again by executing below command:
  yum update -x 'axis- tomcat-* redhat-release-server-* php-*'*
- If required, restore the rpm database backup that was copied earlier. (**This is an optional step**)

Post Update

- After rpm upgrades check installed "java-1.8.0-openjdk" rpm (rpm -qa | grep java-1.8.0-openjdk) version and recreate "/usr/java/default/" softlink

  cd /usr/java/

  rm -rf default

  ln -s /usr/lib/jvm/java-1.8.0-openjdk default

- If httpd rpm is updated, them rename the file " /etc/httpd/conf.d/autoindex.conf"

  mv /etc/httpd/conf.d/autoindex.conf /etc/httpd/conf.d/autoindex.conf.bkup

  Replace the httpd.service file with the backed up file in service file in Pre Update step

  mv /tmp/httpd.service /usr/lib/systemd/system/httpd.service

  Reload the systemctl daemon: *systemctl daemon-reload* for changes to take effect.

- If openldap rpm is updated, then replace the /etc/openldap/slapd.conf file with the backed up file. The back up was taken in Pre Update Step.
  mv /tmp/slapd.conf /etc/openldap/slapd.conf

- If sudo rpm is being updated, make sure to remove "*session include system-auth*" entry from /etc/pam.d/sudo

  sed -i "/session include system-auth/d" /etc/pam.d/sudo

- If kernel rpm is being updated (> 3.10.1062) and if a DHCP server is configured in the subnet in which AES resides, make the following changes so that AES does not acquire a dynamic IP address post reboot:
  - Edit "/etc/default/grub" to add the highlighted parameter:
    GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb quiet net.ifnames=0 biosdevname=0 rd.neednet=0"
  - Run the command *"grub2-mkconfig -o /boot/grub2/grub.cfg"*

- **Reboot** AES machine instance.

  reboot

Avaya Aura® WebLM (Standalone) 8.1.3.2

Avaya Aura® WebLM (Standalone) critical RPM versions list

java-1.8.0-openjdk-debuginfo-1.8.0.292.b10-1.el7_9.x86_64.rpm
java-1.8.0-openjdk-headless-1.8.0.292.b10-1.el7_9.x86_64.rpm
java-1.8.0-openjdk-devel-1.8.0.292.b10-1.el7_9.x86_64.rpm
java-1.8.0-openjdk-1.8.0.292.b10-1.el7_9.x86_64.rpm

Avaya Aura® WebLM (Standalone) do not update RPM version list

redhat-release-server-7.6-4.el7.x86_64

How to Upgrade WebLM RPMs

Pre Update

9. If feasible take WebLM instance backup(For VMware take snapshot).
10. Stop below service

    systemctl stop jboss.service

Remove net-snmp RPM:

yum remove net-snmp

Before upgrading JAVA, Copy following files to /opt location:

1. cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/java.security /opt/java.security
2. cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/java.policy /opt/java.policy
3. cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/blacklisted.certs /opt/blacklisted.certs

Update critical RPMs

yum install java-1.8.0-openjdk-debuginfo-1.8.0.292.b10-1.el7_9.x86_64 java-1.8.0-openjdk-headless-1.8.0.292.b10-1.el7_9.x86_64 java-1.8.0-openjdk-devel-1.8.0.292.b10-1.el7_9.x86_64 java-1.8.0-openjdk-1.8.0.292.b10-1.el7_9.x86_64

Restore following files:

```
# cd /opt
# cp -f java.security java.policy blacklisted.certs /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/
# cd /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/
# chmod 644 java.security java.policy blacklisted.certs
```

Update All Non-Critical RPMs

yum update -x "java-1.8.0-* redhat-release-server"

Update Critical with security fixes

N/A

Post Update

After updating RPMs please reboot WebLM machine instance.

RELEASE 8.1.3.4

Aura 8.1.3.4 GA February 22, 2022 – Certified for Software Only Offer March 07, 2022
This section lists all the latest RPMs for the latest GA version of the products.

IMPORTANT: Any non-RHEL repositories should be disabled prior to executing any updates.
To list enabled repositories execute:

yum repolist enabled

Any non-RHEL repositories should be disabled by setting “enable=0” in the corresponding /etc/yum.repo.d file.
Failure to do so may cause issues with the Avaya application.

Avaya Aura® System Manager 8.1.3.4

Avaya Aura® System Manager critical RPM versions list
Note: java rpms updated from version used in 8.1.3.3.

java-1.8.0-openjdk-debuginfo-1.8.0.312.b07-1.el7_9.x86_64.rpm
java-1.8.0-openjdk-headless-1.8.0.312.b07-1.el7_9.x86_64.rpm
java-1.8.0-openjdk-devel-1.8.0.312.b07-1.el7_9.x86_64.rpm
java-1.8.0-openjdk-1.8.0.312.b07-1.el7_9.x86_64.rpm

Avaya Aura® System Manager do not update RPM version list

postgresql13-13.3-1PGDG.rhel7.x86_64
postgresql13-server-13.3-1PGDG.rhel7.x86_64
postgresql13-contrib-13.3-1PGDG.rhel7.x86_64
postgresql13-libs-13.3-1PGDG.rhel7.x86_64
net-snmp-5.7.3-3.smgr.el7.x86_64
redhat-release-server-7.6-4.el7.x86_64

How to Upgrade System Manager RPMs
Avaya recommends taking a System Manager backup before performing the updates.

Pre Update
If you have a Geo Redundancy setup of System Manager disable Geo as a first step.
If your System Manager is deployed in a virtualize environment then it is also recommended that you take a snapshot of the System Manager virtual machine.

Stop the below Services as root user

systemctl stop crond.service
systemctl stop jboss.service
systemctl stop postgresql.service
systemctl stop spiritAgent.service
systemctl stop cnd.service
systemctl stop systemMonitor.service

Update Commands

Before upgrading JAVA, Copy following files to /swlibrary location:
1. cp $JAVA_HOME/jre/lib/security/java.security /swlibrary/java.security
2. cp $JAVA_HOME/jre/lib/security/java.policy /swlibrary/java.policy
3. cp $JAVA_HOME/jre/lib/security/blacklisted.certs /swlibrary/blacklisted.certs

Update critical RPMs

yum install java-1.8.0-openjdk-debuginfo-1.8.0.312.b07-1.el7_9.x86_64 java-1.8.0-openjdk-headless-1.8.0.312.b07-1.el7_9.x86_64 java-1.8.0-openjdk-devel-1.8.0.312.b07-1.el7_9.x86_64 java-1.8.0-openjdk-1.8.0.312.b07-1.el7_9.x86_64

Restore following files:
cd /swlibrary
cp -f java.security java.policy blacklisted.certs $JAVA_HOME/jre/lib/security/
cd $JAVA_HOME/jre/lib/security/
chown admin:admin java.security java.policy blacklisted.certs
chmod 644 java.security java.policy blacklisted.certs

Update all non-Critical RPMs

yum update -x "java-1.8.0-* postgresql13-* net-snmp redhat-release-server"

Update all critical RPMs with security fixes only

N/A

Post Update

After updating RPMs please reboot System Manager machine instance.

Once the System Manager is up and running post reboot, enable Geo redundancy (Note: this should be done only after you have patched the Secondary System Manager using the same set of instructions)

If you took a snapshot, make sure you remove them once you have successfully completed the process and System Manager is back up and running.

IMPORTANT NOTE– Restart system monitor service manually if it is not in running state after reboot.

- Login to System Manager CLI using administrative account and then switch to root account.
- Run the command to check system monitor service status "**systemctl status systemMonitor.service**"

If the System Monitor service is not running then run the command "**systemctl start systemMonitor.service**" to start service.

Avaya Aura® Communication Manager 8.1.3.4

Avaya Aura® Communication Manager critical RPM version list

glibc-2.17-323.el7_9.i686
glibc-2.17-323.el7_9.x86_64
glibc-common-2.17-323.el7_9.x86_64
kernel-3.10.0-1160.49.1.el7.x86_64
kernel-tools-libs-3.10.0-1160.49.1.el7.x86_64
kernel-tools-3.10.0-1160.49.1.el7.x86_64
openssh-clients-7.4p1-22.el7_9.x86_64
openssh-7.4p1-22.el7_9.x86_64
openssh-server-7.4p1-22.el7_9.x86_64
pam-1.1.8-23.el7.x86_64
pam-1.1.8-23.el7.i686

Avaya Aura® Communication Manager do not update RPM version list

redhat-release-server-7.6-4.el7.x86_64
initscripts-9.49.46-1.el7.x86_64

Avaya Aura® Communication Manager optional RPM versions list

If you have used the Avaya version of net-snmp and bash offered at installation time you should not upgrade these and instead use the versions provided by Avaya. You can confirm if you have the Avaya version of net-snmp and/or bash by executing 'rpm -qa net-snmp*' and 'rpm -qa bash*' and comparing the versions to the Optional Avaya RPMversions listed below or by the 'AV' indicator in the version.
The Avaya bash rpm offers additional command logging capability and the Avaya net-snmp rpm offers better performance for SNMP calls when used with Avaya Aura © Communication Manager than the RedHat version and therefore is more suitable if high numbers of SNMP calls will be made against CM although you may choose not to install the Avaya version should you wish to be able to update these with the latest RHEL versions.
To restore the Red Hat version of bash and net-snmp use 'yum downgrade bash', 'yum downgrade net-snmp*'

bash-4.2.46-31.el7.AV1.x86_64
net-snmp-5.7.2-37.el7.AV1.x86_64
net-snmp-agent-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-utils-5.7.2-37.el7.AV1.x86_64

How to Upgrade Communication Manager RPMs

Avaya recommends taking a Communication Manager backup before performing the updates.

Pre Update

Before updating RPMs it is recommended that a full CM backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Communication Manager guide
In a duplex system the RPM update should be done on the standby machine and CM processing should be stopped with a Busy-Out.

Update Commands

Update all critical RPMs with security fixes

yum install glibc-2.17-323.el7_9.i686 glibc-2.17-323.el7_9.x86_64 glibc-common-2.17-323.el7_9.x86_64 kernel-3.10.0-1160.49.1.el7.x86_64 kernel-tools-3.10.0-1160.49.1.el7.x86_64 kernel-tools-libs-3.10.0-1160.49.1.el7.x86_64 openssh-7.4p1-22.el7_9.x86_64 openssh-clients-7.4p1-22.el7_9.x86_64 openssh-server-7.4p1-22.el7_9.x86_64 pam-1.1.8-23.el7.i686 pam-1.1.8-23.el7.x86_64

Remove the SW-only installation rpm no longer required

rpm -e -v --nodeps avaya-cm-setup

Update all non-Critical RPMs

yum update -x 'glibc-* kernel-* openssh-* pam-* initscripts redhat-release-server nscd'

Post Update

When the RPM installation is complete restart the virtual machine by issuing the 'reboot' command.

Avaya Aura® Session Manager 8.1.3.4

Avaya Aura® Session Manager Avaya tested critical RPM versions list

java-1.8.0-openjdk*

Avaya Aura® Session Manager do not update RPM version list

nginx
postgresql13-*

How to Upgrade Session Manager RPMs

IMPORTANT: Any non-RHEL repositories should be disabled prior to executing any updates. If non-RHEL repositories are being used, it is recommended that /etc/yum.conf be edited to include:

*exclude=nginx postgresql13-**

Pre Update

Avaya recommends taking a Session Manager backup before performing the updates.
This process is service affecting. Session Manager will be out-of-service until it is placed back into "Accept New Service".

31. Place the SM in **Deny New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.

b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
c. Click **Service State**.
d. From the drop-down list box, select **Deny New Service**.
e. Before updating On the confirmation page, click **Confirm**.

32. On the **Session Manager Dashboard** page, wait until **Active Call Count** is zero. Refresh the screen to update the count.
33. Take a VM snapshot prior to making changes.
34. Stop SM with **stop -ac**.
35. Configure yum to point to a Red Hat 8 repository containing the updates.

Update Commands

Update All Non-Critical RPMs

yum update -x "nginx postgresql13-* java-1.8.0-openjdk*"

Update Critical with security fixes

cp $JAVA_HOME/jre/lib/security/java.security /tmp

yum update java-1.8.0-openjdk*

mv /tmp/java.security $JAVA_HOME/jre/lib/security

Post Update

After the update, the SM can be placed back in service by:

26. Reboot the SM.
27. From System Manager web console, select **Elements > Session Manager > System Tools > Maintenance Tests.**
    a. Select the Session Manager that was updated.
    b. Select **Execute all Tests.**
    c. Verify that all tests pass. If not, refer to *Troubleshooting Avaya Aura® Session Manager and Maintaining Avaya Aura® Session Manager*.
28. Place the SM in **Accept New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Accept New Service**.
    e. On the confirmation page, click **Confirm**.
29. Remove the VM snapshot taken prior to the update.

Avaya Aura® Media Server 8.X

Avaya Aura® Media Server critical RPM versions list

None currently

Avaya Aura® Media Server do not update RPM versions list

None currently

Avaya Aura® Application Enablement Services 8.1.3.4

Avaya Aura® Application Enablement Services critical RPM version list

None

Avaya Aura® Application Enablement Services do not update RPM version list

axis-1.4-AV7.i386
php-7.4.2-1.el7.remi.x86_64
php-cli-7.4.2-1.el7.remi.x86_64
php-common-7.4.2-1.el7.remi.x86_64
php-json-7.4.2-1.el7.remi.x86_64
php-mbstring-7.4.2-1.el7.remi.x86_64
php-soap-7.4.2-1.el7.remi.x86_64
php-xml-7.4.2-1.el7.remi.x86_64
tomcat-8.5.69-6.AV1.noarch
tomcat-el-3.0-api-8.5.69-6.AV1.noarch
tomcat-jsp-2.3-api-8.5.69-6.AV1.noarch
tomcat-lib-8.5.69-6.AV1.noarch
tomcat-servlet-3.1-api-8.5.69-6.AV1.noarch

How to Upgrade Application Enablement Services RPMs

Pre Update
Note: For upgrading to AE Services 8.1.3.4 in a software-only environment, you must install AE Services 8.1 or 8.1.1 ISO, upgrade it to AE Services 8.1.2.x and then upgrade to AE Services 8.1.3.4

28. Before updating RPMs it is recommended that a full AES backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Application Enablement Services guide.
29. Configure yum to point to a Red Hat 7 repository containing the updates. See Red Hat page for available repositories.
30. Add following line (excluded rpms list) into /etc/yum.conf file**.** "*exclude=axis-*,tomcat-*,redhat-release-server-*,php-**"
31. Take backup of the httpd service file- **/usr/lib/systemd/system/httpd.service** in /tmp
32. Take backup of the slapd.conf configuration file - **/etc/openldap/slapd.conf** in /tmp
33. **Important Note: If High Availability is configured, please follow the following steps:**
    a. Update secondary(standby) AES with the OS packages as per the Pre Update, Update and Post Update instructions
    b. Post reboot, wait for aesvcs (*systemctl status aesvcs*) to be in active(running) state.
    c. Synchronize the data between the Primary and the Secondary Server
    d. Perform Failover from Primary to Secondary Server
    e. Update the new Secondary(standby) server with the OS packages as per the Pre Update, Update and Post Update instructions.
    f. Post reboot, wait for aesvcs (*systemctl status aesvcs*) to be in active(running) state.
    g. If required, perform failover from primary to secondary server. (Optional step)

Update Commands

Update All Non-Critical RPMs

yum update -x 'axis-* tomcat-* redhat-release-server-* php-*'

Update Critical with security fixes

None

Important Note:
In case the above update command *fails* with the following message:

Transaction check error:

file /etc/openldap/schema/core.schema from install of openldap-servers-2.4.44-20.el7.x86_64 conflicts with file from package aesvcs-userService-config-8.x.x.0.0.x-0.noarch

then perform the following steps:

****Note: The following steps will rebuild the rpm database on your system. Verify that there are no processes with the RPM database files open. Ensure that you have necessary backup.****

- Take back up of existing rpm database by executing below command:
  mv /var/lib/rpm/__db.00 /tmp*
- Rebuild rpm database by executing below command:
  rpm --rebuilddb
- Perform update again by executing below command:
  yum update -x 'axis- tomcat-* redhat-release-server-* php-*'*
- If required, restore the rpm database backup that was copied earlier. (**This is an optional step**)

Post Update

- After rpm upgrades check installed "java-1.8.0-openjdk" rpm (rpm -qa | grep java-1.8.0-openjdk) version and recreate "/usr/java/default/" softlink

  cd /usr/java/

  rm -rf default

  ln -s /usr/lib/jvm/java-1.8.0-openjdk default

- If httpd rpm is updated, them rename the file " /etc/httpd/conf.d/autoindex.conf"

  mv /etc/httpd/conf.d/autoindex.conf /etc/httpd/conf.d/autoindex.conf.bkup

  Replace the httpd.service file with the backed up file in service file in Pre Update step

  mv /tmp/httpd.service /usr/lib/systemd/system/httpd.service

  Reload the systemctl daemon: *systemctl daemon-reload* for changes to take effect.

- If openldap rpm is updated, then replace the /etc/openldap/slapd.conf file with the backed up file. The back up was taken in Pre Update Step.
  mv /tmp/slapd.conf /etc/openldap/slapd.conf

- If sudo rpm is being updated, make sure to remove "*session include system-auth*" entry from /etc/pam.d/sudo

  sed -i "/session include system-auth/d" /etc/pam.d/sudo

- If kernel rpm is being updated (> 3.10.1062) and if a DHCP server is configured in the subnet in which AES resides, make the following changes so that AES does not acquire a dynamic IP address post reboot:
  - Edit "/etc/default/grub" to add the highlighted parameter:
    GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb quiet net.ifnames=0 biosdevname=0 rd.neednet=0"
  - Run the command *"grub2-mkconfig -o /boot/grub2/grub.cfg"*

- **Reboot** AES machine instance.

  reboot

Avaya Aura® WebLM (Standalone) 8.1.3.4

Avaya Aura® WebLM (Standalone) critical RPM versions list

java-1.8.0-openjdk-debuginfo-1.8.0.312.b07-1.el7_9.x86_64.rpm
java-1.8.0-openjdk-headless-1.8.0.312.b07-1.el7_9.x86_64.rpm
java-1.8.0-openjdk-devel-1.8.0.312.b07-1.el7_9.x86_64.rpm
java-1.8.0-openjdk-1.8.0.312.b07-1.el7_9.x86_64.rpm

Avaya Aura® WebLM (Standalone) do not update RPM version list

redhat-release-server-7.6-4.el7.x86_64

How to Upgrade WebLM RPMs

Pre Update

11. If feasible take WebLM instance backup(For VMware take snapshot).
12. Stop below service

    systemctl stop jboss.service

Remove net-snmp RPM:

yum remove net-snmp
(We don't use net-snmp on WebLM, so we need to remove net-snmp irrespective of its any installed version)

Before upgrading JAVA, Copy following files to /opt location:

1. cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/java.security /opt/java.security
2. cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/java.policy /opt/java.policy
3. cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/blacklisted.certs /opt/blacklisted.certs

Update critical RPMs

yum install java-1.8.0-openjdk-debuginfo-1.8.0.312.b07-1.el7_9.x86_64 java-1.8.0-openjdk-headless-1.8.0.312.b07-1.el7_9.x86_64 java-1.8.0-openjdk-devel-1.8.0.312.b07-1.el7_9.x86_64 java-1.8.0-openjdk-1.8.0.312.b07-1.el7_9.x86_64

Restore following files:

```
# cd /opt
# cp -f java.security java.policy blacklisted.certs /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/
# cd /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/
# chmod 644 java.security java.policy blacklisted.certs
```

Update All Non-Critical RPMs

yum update -x "java-1.8.0-* redhat-release-server"

Update Critical with security fixes

N/A

Post Update

After updating RPMs please reboot WebLM machine instance.

RELEASE 8.1.3.3

Aura 8.1.3.3 October 11, 2021 – Certified for Software Only Offer November 11, 2021
This section lists all the latest RPMs for the latest GA version of the products.

IMPORTANT: Any non-RHEL repositories should be disabled prior to executing any updates.
To list enabled repositories execute:

yum repolist enabled

Any non-RHEL repositories should be disabled by setting "enable=0" in the corresponding /etc/yum.repo.d file.
Failure to do so may cause issues with the Avaya application.

Avaya Aura® System Manager 8.1.3.3

Avaya Aura® System Manager critical RPM versions list
Note:

1. *Postgresql has been upgraded from 9.6 to 13*
2. *java rpms updated from version used in 8.1.3.2.*

java-1.8.0-openjdk-debuginfo-1.8.0.302.b08-0.el7_9.x86_64.rpm
java-1.8.0-openjdk-headless-1.8.0.302.b08-0.el7_9.x86_64.rpm
java-1.8.0-openjdk-devel-1.8.0.302.b08-0.el7_9.x86_64.rpm
java-1.8.0-openjdk-1.8.0.302.b08-0.el7_9.x86_64.rpm

Avaya Aura® System Manager do not update RPM version list

postgresql13-13.3-1PGDG.rhel7.x86_64
postgresql13-server-13.3-1PGDG.rhel7.x86_64
postgresql13-contrib-13.3-1PGDG.rhel7.x86_64
postgresql13-libs-13.3-1PGDG.rhel7.x86_64
net-snmp-5.7.3-3.smgr.el7.x86_64
redhat-release-server-7.6-4.el7.x86_64

How to Upgrade System Manager RPMs
Avaya recommends taking a System Manager backup before performing the updates.

Pre Update
If you have a Geo Redundancy setup of System Manager disable Geo as a first step.
If your System Manager is deployed in a virtualize environment then it is also recommended that you take a snapshot of the System Manager virtual machine.

Stop the below Services as root user

systemctl stop crond.service
systemctl stop jboss.service
systemctl stop postgresql.service
systemctl stop spiritAgent.service
systemctl stop cnd.service
systemctl stop systemMonitor.service

Update Commands

Before upgrading JAVA, Copy following files to /swlibrary location:

1. cp $JAVA_HOME/jre/lib/security/java.security /swlibrary/java.security
2. cp $JAVA_HOME/jre/lib/security/java.policy /swlibrary/java.policy
3. cp $JAVA_HOME/jre/lib/security/blacklisted.certs /swlibrary/blacklisted.certs

Update critical RPMs

yum install java-1.8.0-openjdk-debuginfo-1.8.0.302.b08-0.el7_9.x86_64 java-1.8.0-openjdk-headless-1.8.0.302.b08-0.el7_9.x86_64 java-1.8.0-openjdk-devel-1.8.0.302.b08-0.el7_9.x86_64 java-1.8.0-openjdk-1.8.0.302.b08-0.el7_9.x86_64

Restore following files:

```
# cd /swlibrary
# cp -f java.security java.policy blacklisted.certs $JAVA_HOME/jre/lib/security/
# cd  $JAVA_HOME/jre/lib/security/
# chown admin:admin java.security java.policy blacklisted.certs
# chmod 644 java.security java.policy blacklisted.certs
```

Update all non-Critical RPMs

yum update -x "java-1.8.0-* postgresql13-* net-snmp redhat-release-server"

Update all critical RPMs with security fixes only

N/A

Post Update

After updating RPMs please reboot System Manager machine instance.

Once the System Manager is up and running post reboot, enable Geo redundancy (Note: this should be done only after you have patched the Secondary System Manager using the same set of instructions)

If you took a snapshot, make sure you remove them once you have successfully completed the process and System Manager is back up and running.

IMPORTANT NOTE– Restart system monitor service manually if it is not in running state after reboot.

- Login to System Manager CLI using administrative account and then switch to root account.
- Run the command to check system monitor service status "**systemctl status systemMonitor.service**"

If the System Monitor service is not running then run the command "**systemctl start systemMonitor.service**" to start service.

Avaya Aura® Communication Manager 8.1.3.3

Avaya Aura® Communication Manager critical RPM version list

glibc-2.17-323.el7_9.i686
glibc-2.17-323.el7_9.x86_64
glibc-common-2.17-323.el7_9.x86_64
kernel-3.10.0-1160.42.2.el7.x86_64
kernel-tools-libs-3.10.0-1160.42.2.el7.x86_64
kernel-tools-3.10.0-1160.42.2.el7.x86_64
openssh-clients-7.4p1-21.el7.x86_64
openssh-7.4p1-21.el7.x86_64
openssh-server-7.4p1-21.el7.x86_64
pam-1.1.8-23.el7.x86_64
pam-1.1.8-23.el7.i686

Avaya Aura® Communication Manager do not update RPM version list

redhat-release-server-7.6-4.el7.x86_64
initscripts-9.49.46-1.el7.x86_64

Avaya Aura® Communication Manager optional RPM versions list

If you have used the Avaya version of net-snmp and bash offered at installation time you should not upgrade these and instead use the versions provided by Avaya. You can confirm if you have the Avaya version of net-snmp and/or bash by executing ‘rpm -qa net-snmp*’ and ‘rpm -qa bash*’ and comparing the versions to the Optional Avaya RPMversions listed below or by the ‘AV’ indicator in the version.
The Avaya bash rpm offers additional command logging capability and the Avaya net-snmp rpm offers better performance for SNMP calls when used with Avaya Aura © Communication Manager than the RedHat version and therefore is more suitable if high numbers of SNMP calls will be made against CM although you may choose not to install the Avaya version should you wish to be able to update these with the latest RHEL versions.

bash-4.2.46-31.el7.AV1.x86_64
net-snmp-5.7.2-37.el7.AV1.x86_64
net-snmp-agent-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-utils-5.7.2-37.el7.AV1.x86_64

How to Upgrade Communication Manager RPMs

Avaya recommends taking a Communication Manager backup before performing the updates.

Pre Update

Before updating RPMs it is recommended that a full CM backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Communication Manager guide
In a duplex system the RPM update should be done on the standby machine and CM processing should be stopped with a Busy-Out.

Update Commands

Update all critical RPMs with security fixes

yum install glibc-2.17-323.el7_9.i686 glibc-2.17-323.el7_9.x86_64 glibc-common-2.17-323.el7_9.x86_64 kernel-3.10.0-1160.42.2.el7.x86_64 kernel-tools-3.10.0-1160.42.2.el7.x86_64 kernel-tools-libs-3.10.0-1160.42.2.el7.x86_64 openssh-7.4p1-21.el7.x86_64 openssh-clients-7.4p1-21.el7.x86_64 openssh-server-7.4p1-21.el7.x86_64 pam-1.1.8-23.el7.i686 pam-1.1.8-23.el7.x86_64

Remove the SW-only installation rpm no longer required

rpm -e -v --nodeps avaya-cm-setup

Update all non-Critical RPMs

yum update -x 'glibc-* kernel-* openssh-* pam-* initscripts redhat-release-server nscd'

Post Update

When the RPM installation is complete restart the virtual machine by issuing the 'reboot' command.

Avaya Aura® Session Manager 8.1.3.3

Avaya Aura® Session Manager Avaya tested critical RPM versions list

None currently

Avaya Aura® Session Manager do not update RPM version list

nginx
postgresql13-*

How to Upgrade Session Manager RPMs

IMPORTANT: Any non-RHEL repositories should be disabled prior to executing any updates. If non-RHEL repositories are being used, it is recommended that /etc/yum.conf be edited to include:

*exclude=nginx postgresql13-**

Pre Update

Avaya recommends taking a Session Manager backup before performing the updates.
This process is service affecting. Session Manager will be out-of-service until it is placed back into "Accept New Service".

36. Place the SM in **Deny New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Deny New Service**.
    e. Before updating On the confirmation page, click **Confirm**.
37. On the **Session Manager Dashboard** page, wait until **Active Call Count** is zero. Refresh the screen to update the count.
38. Take a VM snapshot prior to making changes.
39. Stop SM with **stop -ac**.
40. Configure yum to point to a Red Hat 7 repository containing the updates.

Update Commands

Update All Non-Critical RPMs

yum update -x “nginx postgresql13-*”

Update Critical with security fixes

N/A

Post Update

After the update, the SM can be placed back in service by:

30. Reboot the SM.
31. From System Manager web console, select **Elements > Session Manager > System Tools > Maintenance Tests.**
    a. Select the Session Manager that was updated.
    b. Select **Execute all Tests.**
    c. Verify that all tests pass. If not, refer to *Troubleshooting Avaya Aura® Session Manager and Maintaining Avaya Aura® Session Manager*.
32. Place the SM in **Accept New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Accept New Service**.
    e. On the confirmation page, click **Confirm**.

33. Remove the VM snapshot taken prior to the update.

Avaya Aura® Media Server 8.X

Avaya Aura® Media Server critical RPM versions list

None currently

Avaya Aura® Media Server do not update RPM versions list

None currently

Avaya Aura® Application Enablement Services 8.1.3.3

Avaya Aura® Application Enablement Services critical RPM version list

None

Avaya Aura® Application Enablement Services do not update RPM version list

axis-1.4-AV7.i386
php-7.4.2-1.el7.remi.x86_64
php-cli-7.4.2-1.el7.remi.x86_64
php-common-7.4.2-1.el7.remi.x86_64
php-json-7.4.2-1.el7.remi.x86_64
php-mbstring-7.4.2-1.el7.remi.x86_64
php-soap-7.4.2-1.el7.remi.x86_64
php-xml-7.4.2-1.el7.remi.x86_64
tomcat-8.5.69-6.AV1.noarch
tomcat-el-3.0-api-8.5.69-6.AV1.noarch
tomcat-jsp-2.3-api-8.5.69-6.AV1.noarch
tomcat-lib-8.5.69-6.AV1.noarch
tomcat-servlet-3.1-api-8.5.69-6.AV1.noarch

How to Upgrade Application Enablement Services RPMs

Pre Update
Note: For upgrading to AE Services 8.1.3.3 in a software-only environment, you must install AE Services 8.1 or 8.1.1 ISO, upgrade it to AE Services 8.1.2.x and then upgrade to AE Services 8.1.3.3

34. Before updating RPMs it is recommended that a full AES backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Application Enablement Services guide.
35. Configure yum to point to a Red Hat 7 repository containing the updates. See Red Hat page for available repositories.
36. Add following line (excluded rpms list) into /etc/yum.conf file**.** "*exclude=axis-*,tomcat-*,redhat-release-server-*,php-**"
37. Take backup of the httpd service file- **/usr/lib/systemd/system/httpd.service** in /tmp
38. Take backup of the slapd.conf configuration file - **/etc/openldap/slapd.conf** in /tmp
39. **Important Note: If High Availability is configured, please follow the following steps:**
    a. Update secondary(standby) AES with the OS packages as per the Pre Update, Update and Post Update instructions
    b. Post reboot, wait for aesvcs (*systemctl status aesvcs*) to be in active(running) state.
    c. Synchronize the data between the Primary and the Secondary Server
    d. Perform Failover from Primary to Secondary Server

e. Update the new Secondary(standby) server with the OS packages as per the Pre Update, Update and Post Update instructions.
f. Post reboot, wait for aesvcs (*systemctl status aesvcs*) to be in active(running) state.
g. If required, perform failover from primary to secondary server. (Optional step)

Update Commands

Update All Non-Critical RPMs

yum update -x 'axis-* tomcat-* redhat-release-server-* php-*'

Update Critical with security fixes

None

Important Note:
In case the above update command *fails* with the following message:

Transaction check error:
file /etc/openldap/schema/core.schema from install of openldap-servers-2.4.44-20.el7.x86_64 conflicts with file from package aesvcs-userService-config-8.x.x.0.0.x-0.noarch

then perform the following steps:
****Note: The following steps will rebuild the rpm database on your system. Verify that there are no processes with the RPM database files open. Ensure that you have necessary backup.****

- Take back up of existing rpm database by executing below command:
  mv /var/lib/rpm/__db.00 /tmp*
- Rebuild rpm database by executing below command:
  rpm --rebuilddb
- Perform update again by executing below command:
  yum update -x 'axis- tomcat-* redhat-release-server-* php-*'*
- If required, restore the rpm database backup that was copied earlier. (**This is an optional step**)

Post Update

- After rpm upgrades check installed "java-1.8.0-openjdk" rpm (rpm -qa | grep java-1.8.0-openjdk) version and recreate "/usr/java/default/" softlink

  cd /usr/java/

  rm -rf default

  ln -s /usr/lib/jvm/java-1.8.0-openjdk default

- If httpd rpm is updated, them rename the file " /etc/httpd/conf.d/autoindex.conf"

  mv /etc/httpd/conf.d/autoindex.conf /etc/httpd/conf.d/autoindex.conf.bkup

  Replace the httpd.service file with the backed up file in service file in Pre Update step

  mv /tmp/httpd.service /usr/lib/systemd/system/httpd.service

  Reload the systemctl daemon: *systemctl daemon-reload* for changes to take effect.

- If openldap rpm is updated, then replace the /etc/openldap/slapd.conf file with the backed up file. The back up was taken in Pre Update Step.
  mv /tmp/slapd.conf /etc/openldap/slapd.conf

- If sudo rpm is being updated, make sure to remove "*session include system-auth*" entry from /etc/pam.d/sudo

  sed -i "/session include system-auth/d" /etc/pam.d/sudo

- If kernel rpm is being updated (> 3.10.1062) and if a DHCP server is configured in the subnet in which AES resides, make the following changes so that AES does not acquire a dynamic IP address post reboot:
  - Edit "/etc/default/grub" to add the highlighted parameter:
    GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb quiet net.ifnames=0 biosdevname=0 rd.neednet=0"
  - Run the command *"grub2-mkconfig -o /boot/grub2/grub.cfg"*

- **Reboot** AES machine instance.

  reboot

Avaya Aura® WebLM (Standalone) 8.1.3.3

Avaya Aura® WebLM (Standalone) critical RPM versions list

java-1.8.0-openjdk-debuginfo-1.8.0.302.b08-0.el7_9.x86_64.rpm
java-1.8.0-openjdk-headless-1.8.0.302.b08-0.el7_9.x86_64.rpm
java-1.8.0-openjdk-devel-1.8.0.302.b08-0.el7_9.x86_64.rpm
java-1.8.0-openjdk-1.8.0.302.b08-0.el7_9.x86_64.rpm

Avaya Aura® WebLM (Standalone) do not update RPM version list

redhat-release-server-7.6-4.el7.x86_64

How to Upgrade WebLM RPMs

Pre Update

13. If feasible take WebLM instance backup(For VMware take snapshot).
14. Stop below service

    systemctl stop jboss.service

Remove net-snmp RPM:

yum remove net-snmp
(We don't use net-snmp on WebLM, so we need to remove net-snmp irrespective of its any installed version)

Before upgrading JAVA, Copy following files to /opt location:

1. cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/java.security /opt/java.security
2. cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/java.policy /opt/java.policy
3. cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/blacklisted.certs /opt/blacklisted.certs

Update critical RPMs

yum install java-1.8.0-openjdk-debuginfo-1.8.0.302.b08-0.el7_9.x86_64 java-1.8.0-openjdk-headless-1.8.0.302.b08-0.el7_9.x86_64 java-1.8.0-openjdk-devel-1.8.0.302.b08-0.el7_9.x86_64 java-1.8.0-openjdk-1.8.0.302.b08-0.el7_9.x86_64

Restore following files:

```
# cd /opt
# cp -f java.security java.policy blacklisted.certs /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/
# cd /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/
# chmod 644 java.security java.policy blacklisted.certs
```

Update All Non-Critical RPMs

yum update -x "java-1.8.0-* redhat-release-server"

Update Critical with security fixes

N/A

Post Update

After updating RPMs please reboot WebLM machine instance.

RELEASE 8.1.3.5

Aura 8.1.3.5 GA June 21, 2022 – Certified for Software Only Offer July 07, 2022

This section lists all the latest RPMs for the latest GA version of the products.

IMPORTANT: Any non-RHEL repositories should be disabled prior to executing any updates.
To list enabled repositories execute:

yum repolist enabled

Any non-RHEL repositories should be disabled by setting “enable=0” in the corresponding /etc/yum.repo.d file.
Failure to do so may cause issues with the Avaya application.

Avaya Aura® System Manager 8.1.3.5

Avaya Aura® System Manager critical RPM versions list

Note: java rpms updated from version used in 8.1.3.4.

java-1.8.0-openjdk-1.8.0.332.b09-1.el7_9.x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.332.b09-1.el7_9.x86_64
java-1.8.0-openjdk-headless-1.8.0.332.b09-1.el7_9.x86_64
java-1.8.0-openjdk-devel-1.8.0.332.b09-1.el7_9.x86_64

Avaya Aura® System Manager do not update RPM version list

postgresql13-13.3-1PGDG.rhel7.x86_64
postgresql13-server-13.3-1PGDG.rhel7.x86_64
postgresql13-contrib-13.3-1PGDG.rhel7.x86_64
postgresql13-libs-13.3-1PGDG.rhel7.x86_64
net-snmp-5.7.3-3.smgr.el7.x86_64
redhat-release-server-7.6-4.el7.x86_64

How to Upgrade System Manager RPMs
Avaya recommends taking a System Manager backup before performing the updates.

Pre Update
If you have a Geo Redundancy setup of System Manager disable Geo as a first step.

If your System Manager is deployed in a virtualize environment then it is also recommended that you take a snapshot of the System Manager virtual machine.

Stop the below Services as root user

```
systemctl stop crond.service
systemctl stop jboss.service
systemctl stop postgresql.service
systemctl stop spiritAgent.service
systemctl stop cnd.service
systemctl stop systemMonitor.service
```

Update Commands

Before upgrading JAVA, Copy following files to /swlibrary location:

1. cp $JAVA_HOME/jre/lib/security/java.security /swlibrary/java.security
2. cp $JAVA_HOME/jre/lib/security/java.policy /swlibrary/java.policy
3. cp $JAVA_HOME/jre/lib/security/blacklisted.certs /swlibrary/blacklisted.certs

Update critical RPMs

```
yum install java-1.8.0-openjdk-debuginfo-1.8.0.332.b09-1.el7_9.x86_64 java-1.8.0-openjdk-headless-1.8.0.332.b09-1.el7_9.x86_64 java-1.8.0-openjdk-devel-1.8.0.332.b09-1.el7_9.x86_64 java-1.8.0-openjdk-1.8.0.332.b09-1.el7_9.x86_64
```

Restore following files:

```
# cd /swlibrary
# cp -f java.security java.policy blacklisted.certs $JAVA_HOME/jre/lib/security/
# cd  $JAVA_HOME/jre/lib/security/
# chown admin:admin java.security java.policy blacklisted.certs
# chmod 644 java.security java.policy blacklisted.certs
```

Update all non-Critical RPMs

```
yum update -x   "java-1.8.0-* postgresql13-* net-snmp redhat-release-server"
```

Update all critical RPMs with security fixes only

N/A

Post Update

After updating RPMs please reboot System Manager machine instance.

Once the System Manager is up and running post reboot, enable Geo redundancy (Note: this should be done only after you have patched the Secondary System Manager using the same set of instructions)

If you took a snapshot, make sure you remove them once you have successfully completed the process and System Manager is back up and running.

IMPORTANT NOTE– Restart system monitor service manually if it is not in running state after reboot.

- Login to System Manager CLI using administrative account and then switch to root account.
- Run the command to check system monitor service status "**systemctl status systemMonitor.service**"

If the System Monitor service is not running then run the command "**systemctl start systemMonitor.service**" to start service.

Avaya Aura® Communication Manager 8.1.3.5.1

Updated September 2, 2022 With the introduction of CM 8.1.3.5.1 Service Pack with Hot Fix, the 8.1.3.5.0 Service pack 01.0.890.0-27485.tar is now obsolete. It is highly recommended that customers on 8.1.3.5.0 apply the 8.1.3.5.1 Service Pack with Hot Fix

(01.0.890.0-27598.tar). Reference PCN2095S and the Avaya Aura 8.1.x Release Notes for details on the update delivered to CM 8.1.3.5.1.
There are no changes to the instructions or rpm lists below with the introduction of CM 8.1.3.5.1.

Avaya Aura® Communication Manager critical RPM version list

glibc-2.17-326.el7_9.i686
glibc-2.17-326.el7_9.x86_64
glibc-common-2.17-326.el7_9.x86_64
kernel-3.10.0-1160.62.1.el7.x86_64
kernel-tools-libs-3.10.0-1160.62.1.el7.x86_64
kernel-tools-3.10.0-1160.62.1.el7.x86_64
openssh-clients-7.4p1-22.el7_9.x86_64
openssh-7.4p1-22.el7_9.x86_64
openssh-server-7.4p1-22.el7_9.x86_64
pam-1.1.8-23.el7.x86_64
pam-1.1.8-23.el7.i686

Avaya Aura® Communication Manager do not update RPM version list

redhat-release-server-7.6-4.el7.x86_64
initscripts-9.49.46-1.el7.x86_64

Avaya Aura® Communication Manager optional RPM versions list

If you have used the Avaya version of net-snmp and bash offered at installation time you should not upgrade these and instead use the versions provided by Avaya. You can confirm if you have the Avaya version of net-snmp and/or bash by executing ‘rpm -qa net-snmp*’ and ‘rpm -qa bash*’ and comparing the versions to the Optional Avaya RPMversions listed below or by the ‘AV’ indicator in the version.
The Avaya bash rpm offers additional command logging capability and the Avaya net-snmp rpm offers better performance for SNMP calls when used with Avaya Aura © Communication Manager than the RedHat version and therefore is more suitable if high numbers of SNMP calls will be made against CM although you may choose not to install the Avaya version should you wish to be able to update these with the latest RHEL versions.
To restore the Red Hat version of bash and net-snmp use ‘yum downgrade bash’, ‘yum downgrade net-snmp*’

bash-4.2.46-31.el7.AV1.x86_64
net-snmp-5.7.2-37.el7.AV1.x86_64
net-snmp-agent-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-utils-5.7.2-37.el7.AV1.x86_64

How to Upgrade Communication Manager RPMs

Avaya recommends taking a Communication Manager backup before performing the updates.

Pre Update

Before updating RPMs it is recommended that a full CM backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Communication Manager guide
In a duplex system the RPM update should be done on the standby machine and CM processing should be stopped with a Busy-Out.

Update Commands

Update all critical RPMs with security fixes

yum install glibc-2.17-326.el7_9.i686 glibc-2.17-326.el7_9.x86_64 glibc-common-2.17-326.el7_9.x86_64 kernel-3.10.0-1160.62.1.el7.x86_64 kernel-tools-3.10.0-1160.62.1.el7.x86_64 kernel-tools-libs-3.10.0-1160.62.1.el7.x86_64 openssh-

7.4p1-22.el7_9.x86_64 openssh-clients-7.4p1-22.el7_9.x86_64 openssh-server-7.4p1-22.el7_9.x86_64 pam-1.1.8-23.el7.i686 pam-1.1.8-23.el7.x86_64

Remove the SW-only installation rpm no longer required

rpm -e -v --nodeps avaya-cm-setup

Update all non-Critical RPMs

yum update -x 'glibc-* kernel-* openssh-* pam-* initscripts redhat-release-server nscd'

Post Update

When the RPM installation is complete restart the virtual machine by issuing the 'reboot' command.

Avaya Aura® Session Manager 8.1.3.5

Avaya Aura® Session Manager Avaya tested critical RPM versions list

None

Avaya Aura® Session Manager do not update RPM version list

java-1.8.0-openjdk-*
nginx
postgresql13-*

How to Upgrade Session Manager RPMs

IMPORTANT: Any non-RHEL repositories should be disabled prior to executing any updates. If non-RHEL repositories are being used, it is recommended that /etc/yum.conf be edited to include:

exclude=java-1.8.0-openjdk- nginx postgresql13-**

Pre Update

Avaya recommends taking a Session Manager backup before performing the updates.
This process is service affecting. Session Manager will be out-of-service until it is placed back into "Accept New Service".

41. Place the SM in **Deny New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Deny New Service**.
    e. Before updating On the confirmation page, click **Confirm**.
42. On the **Session Manager Dashboard** page, wait until **Active Call Count** is zero. Refresh the screen to update the count.
43. Take a VM snapshot prior to making changes.
44. Stop SM with **stop -ac**.
45. Configure yum to point to a Red Hat 7 repository containing the updates.

Update Commands

Update All Non-Critical RPMs

yum update -x "java-1.8.0-openjdk-* nginx postgresql13-*"

Update Critical with security fixes

N/A

Post Update

After the update, the SM can be placed back in service by:

34. Reboot the SM.
35. From System Manager web console, select **Elements > Session Manager > System Tools > Maintenance Tests.**
    a. Select the Session Manager that was updated.
    b. Select **Execute all Tests.**
    c. Verify that all tests pass. If not, refer to *Troubleshooting Avaya Aura® Session Manager and Maintaining Avaya Aura® Session Manager*.
36. Place the SM in **Accept New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Accept New Service**.
    e. On the confirmation page, click **Confirm**.
37. Remove the VM snapshot taken prior to the update.

Avaya Aura® Media Server 8.X

Avaya Aura® Media Server critical RPM versions list

None currently

Avaya Aura® Media Server do not update RPM versions list

None currently

Avaya Aura® Application Enablement Services 8.1.3.5

Avaya Aura® Application Enablement Services critical RPM version list

None

Avaya Aura® Application Enablement Services do not update RPM version list

axis-1.4-AV7.i386
php-7.4.2-1.el7.remi.x86_64
php-cli-7.4.2-1.el7.remi.x86_64
php-common-7.4.2-1.el7.remi.x86_64
php-json-7.4.2-1.el7.remi.x86_64
php-mbstring-7.4.2-1.el7.remi.x86_64
php-soap-7.4.2-1.el7.remi.x86_64
php-xml-7.4.2-1.el7.remi.x86_64
postgresql-9.2.24-1.el7_5.x86_64
postgresql-jdbc-9.2.1002-5.el7.noarch
postgresql-libs-9.2.24-1.el7_5.i686
postgresql-libs-9.2.24-1.el7_5.x86_64
postgresql-server-9.2.24-1.el7_5.x86_64

tomcat-8.5.75-AV.noarch
tomcat-el-3.0-api-8.5.75-AV.noarch
tomcat-jsp-2.3-api-8.5.75-AV.noarch
tomcat-lib-8.5.75-AV.noarch
tomcat-servlet-3.1-api-8.5.75-AV.noarch

How to Upgrade Application Enablement Services RPMs

Pre Update

Note: For upgrading to AE Services 8.1.3.5 in a software-only environment, you must install AE Services 8.1 or 8.1.1 ISO, upgrade it to AE Services 8.1.2.x and then upgrade to AE Services 8.1.3.5

40. Before updating RPMs it is recommended that a full AES backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Application Enablement Services guide.
41. Configure yum to point to a Red Hat 7 repository containing the updates. See Red Hat page for available repositories.
42. Add following line (excluded rpms list) into /etc/yum.conf file**.** "*exclude=axis-*,tomcat-*,redhat-release-server-*,php-*,postgresql -*"*
43. Take backup of the httpd service file- **/usr/lib/systemd/system/httpd.service** in /tmp
44. Take backup of the slapd.conf configuration file - **/etc/openldap/slapd.conf** in /tmp
45. **Important Note: If High Availability is configured, please follow the following steps:**
    a. Update secondary(standby) AES with the OS packages as per the Pre Update, Update and Post Update instructions
    b. Post reboot, wait for aesvcs (*systemctl status aesvcs*) to be in active(running) state.
    c. Synchronize the data between the Primary and the Secondary Server
    d. Perform Failover from Primary to Secondary Server
    e. Update the new Secondary(standby) server with the OS packages as per the Pre Update, Update and Post Update instructions.
    f. Post reboot, wait for aesvcs (*systemctl status aesvcs*) to be in active(running) state.
    g. If required, perform failover from primary to secondary server. (Optional step)

Update Commands

Update All Non-Critical RPMs

yum update -x 'axis-* tomcat-* redhat-release-server-* php-* postgresql-* '

Update Critical with security fixes

None

Important Note:

In case the above update command *fails* with the following message:

Transaction check error:

file /etc/openldap/schema/core.schema from install of openldap-servers-2.4.44-20.el7.x86_64 conflicts with file from package aesvcs-userService-config-8.x.x.0.0.x-0.noarch

then perform the following steps:

****Note: The following steps will rebuild the rpm database on your system. Verify that there are no processes with the RPM database files open. Ensure that you have necessary backup.****

- Take back up of existing rpm database by executing below command:
  mv /var/lib/rpm/__db.00 /tmp*
- Rebuild rpm database by executing below command:
  rpm --rebuilddb
- Perform update again by executing below command:
  yum update -x 'axis- tomcat-* redhat-release-server-* php-*'*
- If required, restore the rpm database backup that was copied earlier. (**This is an optional step**)

Post Update

- After rpm upgrades check installed "java-1.8.0-openjdk" rpm (rpm -qa | grep java-1.8.0-openjdk) version and recreate "/usr/java/default/" softlink

  cd /usr/java/

  rm -rf default

  ln -s /usr/lib/jvm/java-1.8.0-openjdk default

- If httpd rpm is updated, them rename the file " /etc/httpd/conf.d/autoindex.conf"

  mv /etc/httpd/conf.d/autoindex.conf /etc/httpd/conf.d/autoindex.conf.bkup

  Replace the httpd.service file with the backed up file in service file in Pre Update step

  mv /tmp/httpd.service /usr/lib/systemd/system/httpd.service

  Reload the systemctl daemon: *systemctl daemon-reload* for changes to take effect.

- If openldap rpm is updated, then replace the /etc/openldap/slapd.conf file with the backed up file. The back up was taken in Pre Update Step.
  mv /tmp/slapd.conf /etc/openldap/slapd.conf

- If sudo rpm is being updated, make sure to remove "*session include system-auth*" entry from /etc/pam.d/sudo

  sed -i "/session include system-auth/d" /etc/pam.d/sudo

- If kernel rpm is being updated (> 3.10.1062) and if a DHCP server is configured in the subnet in which AES resides, make the following changes so that AES does not acquire a dynamic IP address post reboot:
  - Edit "/etc/default/grub" to add the highlighted parameter:
    GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb quiet net.ifnames=0 biosdevname=0 rd.neednet=0"
  - Run the command *"grub2-mkconfig -o /boot/grub2/grub.cfg"*

- **Reboot** AES machine instance.

  reboot

Avaya Aura® WebLM (Standalone) 8.1.3.5

Avaya Aura® WebLM (Standalone) critical RPM versions list

java-1.8.0-openjdk-1.8.0.332.b09-1.el7_9.x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.332.b09-1.el7_9.x86_64
java-1.8.0-openjdk-headless-1.8.0.332.b09-1.el7_9.x86_64
java-1.8.0-openjdk-devel-1.8.0.332.b09-1.el7_9.x86_64

Avaya Aura® WebLM (Standalone) do not update RPM version list

redhat-release-server-7.6-4.el7.x86_64

How to Upgrade WebLM RPMs

Pre Update

15. If feasible take WebLM instance backup(For VMware take snapshot).
16. Stop below service

    systemctl stop jboss.service

Remove net-snmp RPM:

yum remove net-snmp
(We don't use net-snmp on WebLM, so we need to remove net-snmp irrespective of its any installed version)

Before upgrading JAVA, Copy following files to /opt location:

1. cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/java.security /opt/java.security
2. cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/java.policy /opt/java.policy
3. cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/blacklisted.certs /opt/blacklisted.certs

Update critical RPMs

yum install java-1.8.0-openjdk-debuginfo-1.8.0.332.b09-1.el7_9.x86_64 java-1.8.0-openjdk-headless-1.8.0.332.b09-1.el7_9.x86_64 java-1.8.0-openjdk-devel-1.8.0.332.b09-1.el7_9.x86_64 java-1.8.0-openjdk-1.8.0.332.b09-1.el7_9.x86_64

Restore following files:

```
# cd /opt
# cp -f java.security java.policy blacklisted.certs /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/
# cd /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/
# chmod 644 java.security java.policy blacklisted.certs
```

Update All Non-Critical RPMs

yum update -x "java-1.8.0-* redhat-release-server"

Update Critical with security fixes

N/A

Post Update

After updating RPMs please reboot WebLM machine instance.

RELEASE 8.1.3.6

Aura 8.1.3.6 GA October 21, 2022 – Certified for Software Only Offer November 21, 2022
This section lists all the latest RPMs for the latest GA version of the products.

IMPORTANT: Any non-RHEL repositories should be disabled prior to executing any updates.
To list enabled repositories execute:

yum repolist enabled

Any non-RHEL repositories should be disabled by setting "enable=0" in the corresponding /etc/yum.repo.d file.
Failure to do so may cause issues with the Avaya application.

Avaya Aura® System Manager 8.1.3.6

Avaya Aura® System Manager critical RPM versions list
Note: java rpms updated from version used in 8.1.3.4.

java-1.8.0-openjdk-1.8.0.342.b07-1.el7_9.x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.342.b07-1.el7_9.x86_64
java-1.8.0-openjdk-headless-1.8.0.342.b07-1.el7_9.x86_64
java-1.8.0-openjdk-devel-1.8.0.342.b07-1.el7_9.x86_64

Avaya Aura® System Manager do not update RPM version list

postgresql13-13.3-1PGDG.rhel7.x86_64
postgresql13-server-13.3-1PGDG.rhel7.x86_64
postgresql13-contrib-13.3-1PGDG.rhel7.x86_64
postgresql13-libs-13.3-1PGDG.rhel7.x86_64
net-snmp-5.7.3-3.smgr.el7.x86_64
redhat-release-server-7.6-4.el7.x86_64

How to Upgrade System Manager RPMs
Avaya recommends taking a System Manager backup before performing the updates.

Pre Update
If you have a Geo Redundancy setup of System Manager disable Geo as a first step.
If your System Manager is deployed in a virtualize environment then it is also recommended that you take a snapshot of the System Manager virtual machine.

Stop the below Services as root user

systemctl stop crond.service
systemctl stop jboss.service
systemctl stop postgresql.service
systemctl stop spiritAgent.service
systemctl stop cnd.service
systemctl stop systemMonitor.service

Update Commands

Before upgrading JAVA, Copy following files to /swlibrary location:
1. cp $JAVA_HOME/jre/lib/security/java.security /swlibrary/java.security
2. cp $JAVA_HOME/jre/lib/security/java.policy /swlibrary/java.policy
3. cp $JAVA_HOME/jre/lib/security/blacklisted.certs /swlibrary/blacklisted.certs

Update critical RPMs

yum install java-1.8.0-openjdk-debuginfo-1.8.0.342.b07-1.el7_9.x86_64 java-1.8.0-openjdk-headless-1.8.0.342.b07-1.el7_9.x86_64 java-1.8.0-openjdk-devel-1.8.0.342.b07-1.el7_9.x86_64 java-1.8.0-openjdk-1.8.0.342.b07-1.el7_9.x86_64

Restore following files:
cd /swlibrary
cp -f java.security java.policy blacklisted.certs $JAVA_HOME/jre/lib/security/
cd $JAVA_HOME/jre/lib/security/
chown admin:admin java.security java.policy blacklisted.certs
chmod 644 java.security java.policy blacklisted.certs

Update all non-Critical RPMs

yum update -x "java-1.8.0-* postgresql13-* net-snmp redhat-release-server"

Update all critical RPMs with security fixes only

N/A

Post Update

After updating RPMs please reboot System Manager machine instance.

Once the System Manager is up and running post reboot, enable Geo redundancy (Note: this should be done only after you have patched the Secondary System Manager using the same set of instructions)

If you took a snapshot, make sure you remove them once you have successfully completed the process and System Manager is back up and running.

IMPORTANT NOTE– Restart system monitor service manually if it is not in running state after reboot.

- Login to System Manager CLI using administrative account and then switch to root account.
- Run the command to check system monitor service status "**systemctl status systemMonitor.service**"

If the System Monitor service is not running then run the command "**systemctl start systemMonitor.service**" to start service.

Avaya Aura® Communication Manager 8.1.3.6

Avaya Aura® Communication Manager critical RPM version list

glibc-2.17-326.el7_9.i686
glibc-2.17-326.el7_9.x86_64
glibc-common-2.17-326.el7_9.x86_64
kernel-3.10.0-1160.76.1.el7.x86_64
kernel-headers-3.10.0-1160.76.1.el7.x86_64
kernel-tools-3.10.0-1160.76.1.el7.x86_64
kernel-tools-libs-3.10.0-1160.76.1.el7.x86_64
openssh-clients-7.4p1-22.el7_9.x86_64
openssh-7.4p1-22.el7_9.x86_64
openssh-server-7.4p1-22.el7_9.x86_64
pam-1.1.8-23.el7.x86_64
pam-1.1.8-23.el7.i686

Avaya Aura® Communication Manager do not update RPM version list

redhat-release-server-7.6-4.el7.x86_64
initscripts-9.49.46-1.el7.x86_64

Avaya Aura® Communication Manager optional RPM versions list

If you have used the Avaya version of net-snmp and bash offered at installation time you should not upgrade these and instead use the versions provided by Avaya. You can confirm if you have the Avaya version of net-snmp and/or bash by executing 'rpm -qa net-snmp*' and 'rpm -qa bash*' and comparing the versions to the Optional Avaya RPMversions listed below or by the 'AV' indicator in the version.
The Avaya bash rpm offers additional command logging capability and the Avaya net-snmp rpm offers better performance for SNMP calls when used with Avaya Aura © Communication Manager than the RedHat version and therefore is more suitable if high numbers of SNMP calls will be made against CM although you may choose not to install the Avaya version should you wish to be able to update these with the latest RHEL versions.
To restore the Red Hat version of bash and net-snmp use 'yum downgrade bash', 'yum downgrade net-snmp*'

bash-4.2.46-31.el7.AV1.x86_64
net-snmp-5.7.2-37.el7.AV1.x86_64

net-snmp-agent-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-utils-5.7.2-37.el7.AV1.x86_64

How to Upgrade Communication Manager RPMs

Avaya recommends taking a Communication Manager backup before performing the updates.

Pre Update

Before updating RPMs it is recommended that a full CM backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Communication Manager guide
In a duplex system the RPM update should be done on the standby machine and CM processing should be stopped with a Busy-Out.

Update Commands

Update all critical RPMs with security fixes

yum install glibc-2.17-326.el7_9.i686 glibc-2.17-326.el7_9.x86_64 glibc-common-2.17-326.el7_9.x86_64 kernel-3.10.0-1160.76.1.el7.x86_64 kernel-tools-3.10.0-1160.76.1.el7.x86_64 kernel-tools-libs-3.10.0-1160.76.1.el7.x86_64 kernel-headers-3.10.0-1160.76.1.el7.x86_64 openssh-7.4p1-22.el7_9.x86_64 openssh-clients-7.4p1-22.el7_9.x86_64 openssh-server-7.4p1-22.el7_9.x86_64 pam-1.1.8-23.el7.i686 pam-1.1.8-23.el7.x86_64

Remove the SW-only installation rpm no longer required (optional)

rpm -e -v --nodeps avaya-cm-setup

Update all non-Critical RPMs

yum update -x 'glibc-* kernel-* openssh-* pam-* initscripts redhat-release-server nscd'

Post Update

When the RPM installation is complete restart the virtual machine by issuing the 'reboot' command.
A PAM rpm update can cause login failures to the SAT or the web SMI, if it is the case run these commands as root:
ln -sf /opt/ecs/lib/pam_unix_auth_x86_64.so /usr/lib64/security/pam_unix_auth.so
ln -sf /opt/ecs/lib/pam_unix_auth_i686.so /usr/lib/security/pam_unix_auth.so

Avaya Aura® Session Manager 8.1.3.6

Avaya Aura® Session Manager Avaya tested critical RPM versions list

None

Avaya Aura® Session Manager do not update RPM version list

nginx
postgresql13-*

How to Upgrade Session Manager RPMs

IMPORTANT: Any non-RHEL repositories should be disabled prior to executing any updates. If non-RHEL repositories are being used, it is recommended that /etc/yum.conf be edited to include:

*exclude=nginx postgresql13-**

Pre Update

Avaya recommends taking a Session Manager backup before performing the updates.
This process is service affecting. Session Manager will be out-of-service until it is placed back into "Accept New Service".

46. Place the SM in **Deny New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Deny New Service**.
    e. Before updating On the confirmation page, click **Confirm**.
47. On the **Session Manager Dashboard** page, wait until **Active Call Count** is zero. Refresh the screen to update the count.
48. Take a VM snapshot prior to making changes.
49. Stop SM with **stop -ac**.
50. Configure yum to point to a Red Hat 7 repository containing the updates.

Update Commands

Update All Non-Critical RPMs

yum update -x "nginx postgresql13-*"

Update Critical with security fixes

N/A

Post Update

After the update, the SM can be placed back in service by:

38. From the SM command line run: **bash /opt/ASMpatch/bin/setup_java.sh**
39. Reboot the SM.
40. From System Manager web console, select **Elements > Session Manager > System Tools > Maintenance Tests.**
    a. Select the Session Manager that was updated.
    b. Select **Execute all Tests.**
    c. Verify that all tests pass. If not, refer to *Troubleshooting Avaya Aura® Session Manager and Maintaining Avaya Aura® Session Manager*.
41. Place the SM in **Accept New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Accept New Service**.
    e. On the confirmation page, click **Confirm**.
42. Remove the VM snapshot taken prior to the update.

Avaya Aura® Media Server 8.X

Avaya Aura® Media Server critical RPM versions list

None currently

Avaya Aura® Media Server do not update RPM versions list

None currently

Avaya Aura® Application Enablement Services 8.1.3.6

Avaya Aura® Application Enablement Services critical RPM version list

None

Avaya Aura® Application Enablement Services do not update RPM version list

axis-1.4-AV7.i386
php-7.4.2-1.el7.remi.x86_64
php-cli-7.4.2-1.el7.remi.x86_64
php-common-7.4.2-1.el7.remi.x86_64
php-json-7.4.2-1.el7.remi.x86_64
php-mbstring-7.4.2-1.el7.remi.x86_64
php-soap-7.4.2-1.el7.remi.x86_64
php-xml-7.4.2-1.el7.remi.x86_64
postgresql-9.2.24-1.el7_5.x86_64
postgresql-jdbc-9.2.1002-5.el7.noarch
postgresql-libs-9.2.24-1.el7_5.i686
postgresql-libs-9.2.24-1.el7_5.x86_64
postgresql-server-9.2.24-1.el7_5.x86_64
tomcat-8.5.81-AV.noarch
tomcat-el-3.0-api-8.5.81-AV.noarch
tomcat-jsp-2.3-api-8.5.81-AV.noarch
tomcat-lib-8.5.81-AV.noarch
tomcat-servlet-3.1-api-8.5.81-AV.noarch
log4j-1.2.17-16.el7_4.noarch

Note: log4j updates are given in AES 8.1.3.5. log4j rpm should not be upgraded manually.

How to Upgrade Application Enablement Services RPMs

Pre Update
Note: For upgrading to AE Services 8.1.3.6 in a software-only environment, you must install AE Services 8.1 or 8.1.1 ISO, upgrade it to AE Services 8.1.2.x and then upgrade to AE Services 8.1.3.6

46. Before updating RPMs it is recommended that a full AES backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Application Enablement Services guide.
47. Configure yum to point to a Red Hat 7 repository containing the updates. See Red Hat page for available repositories.
48. Add following line (excluded rpms list) into /etc/yum.conf file**.** "*exclude=axis-*,tomcat-*,redhat-release-server-*,php-*,postgresql -*,log4j-**"
49. Take backup of the httpd service file- **/usr/lib/systemd/system/httpd.service** in /tmp
50. Take backup of the slapd.conf configuration file - **/etc/openldap/slapd.conf** in /tmp
51. **Important Note: If High Availability is configured, please follow the following steps:**
    a. Update secondary(standby) AES with the OS packages as per the Pre Update, Update and Post Update instructions
    b. Post reboot, wait for aesvcs (*systemctl status aesvcs*) to be in active(running) state.
    c. Synchronize the data between the Primary and the Secondary Server
    d. Perform Failover from Primary to Secondary Server
    e. Update the new Secondary(standby) server with the OS packages as per the Pre Update, Update and Post Update instructions.

f. Post reboot, wait for aesvcs (*systemctl status aesvcs*) to be in active(running) state.
g. If required, perform failover from primary to secondary server. (Optional step)

Update Commands

Update All Non-Critical RPMs

yum update -x 'axis-* tomcat-* redhat-release-server-* php-* postgresql-* log4j-*'

Update Critical with security fixes

None

Important Note:
In case the above update command *fails* with the following message:

Transaction check error:
file /etc/openldap/schema/core.schema from install of openldap-servers-2.4.44-20.el7.x86_64 conflicts with file from package aesvcs-userService-config-8.x.x.0.0.x-0.noarch

then perform the following steps:
****Note: The following steps will rebuild the rpm database on your system. Verify that there are no processes with the RPM database files open. Ensure that you have necessary backup.****

- Take back up of existing rpm database by executing below command:
  mv /var/lib/rpm/__db.00 /tmp*
- Rebuild rpm database by executing below command:
  rpm --rebuilddb
- Perform update again by executing below command:
  yum update -x 'axis- tomcat-* redhat-release-server-* php-* postgresql-* log4j-*'*
- If required, restore the rpm database backup that was copied earlier. (**This is an optional step**)

Post Update

- After rpm upgrades check installed "java-1.8.0-openjdk" rpm (rpm -qa | grep java-1.8.0-openjdk) version and recreate "/usr/java/default/" softlink

  cd /usr/java/

  rm -rf default

  ln -s /usr/lib/jvm/java-1.8.0-openjdk default

- If httpd rpm is updated, them rename the file " /etc/httpd/conf.d/autoindex.conf"

  mv /etc/httpd/conf.d/autoindex.conf /etc/httpd/conf.d/autoindex.conf.bkup

  Replace the httpd.service file with the backed up file in service file in Pre Update step

  mv /tmp/httpd.service /usr/lib/systemd/system/httpd.service

  Reload the systemctl daemon: *systemctl daemon-reload* for changes to take effect.

- If openldap rpm is updated, then replace the /etc/openldap/slapd.conf file with the backed up file. The back up was taken in Pre Update Step.
  mv /tmp/slapd.conf /etc/openldap/slapd.conf

- If sudo rpm is being updated, make sure to remove "*session include system-auth*" entry from /etc/pam.d/sudo

sed -i "/session include system-auth/d" /etc/pam.d/sudo

- If kernel rpm is being updated (> 3.10.1062) and if a DHCP server is configured in the subnet in which AES resides, make the following changes so that AES does not acquire a dynamic IP address post reboot:
    - Edit "/etc/default/grub" to add the highlighted parameter:
      GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb quiet net.ifnames=0 biosdevname=0 rd.neednet=0"
    - Run the command *"grub2-mkconfig -o /boot/grub2/grub.cfg"*

- **Reboot** AES machine instance.

  reboot

Avaya Aura® WebLM (Standalone) 8.1.3.6

Avaya Aura® WebLM (Standalone) critical RPM versions list

java-1.8.0-openjdk-1.8.0.342.b07-1.el7_9.x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.342.b07-1.el7_9.x86_64
java-1.8.0-openjdk-headless-1.8.0.342.b07-1.el7_9.x86_64
java-1.8.0-openjdk-devel-1.8.0.342.b07-1.el7_9.x86_64

Avaya Aura® WebLM (Standalone) do not update RPM version list

redhat-release-server-7.6-4.el7.x86_64

How to Upgrade WebLM RPMs

Pre Update

17. If feasible take WebLM instance backup(For VMware take snapshot).
18. Stop below service

    systemctl stop jboss.service

Remove net-snmp RPM:

yum remove net-snmp
(We don't use net-snmp on WebLM, so we need to remove net-snmp irrespective of its any installed version)

Before upgrading JAVA, Copy following files to /opt location:

1. cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/java.security /opt/java.security
2. cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/java.policy /opt/java.policy
3. cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/blacklisted.certs /opt/blacklisted.certs

Update critical RPMs

yum install java-1.8.0-openjdk-debuginfo-1.8.0.342.b07-1.el7_9.x86_64 java-1.8.0-openjdk-headless-1.8.0.342.b07-1.el7_9.x86_64 java-1.8.0-openjdk-devel-1.8.0.342.b07-1.el7_9.x86_64 java-1.8.0-openjdk-1.8.0.342.b07-1.el7_9.x86_64

Restore following files:

cd /opt
cp -f java.security java.policy blacklisted.certs /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/

```
# cd /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/
# chmod 644 java.security java.policy blacklisted.certs
```

Update All Non-Critical RPMs

yum update -x "java-1.8.0-* redhat-release-server"

Update Critical with security fixes

N/A

Post Update

After updating RPMs please reboot WebLM machine instance.

Aura 8.1.3.7 GA February 21, 2023 – Certified for Software Only Offer March 20, 2023
This section lists all the latest RPMs for the latest GA version of the products.

IMPORTANT: Any non-RHEL repositories should be disabled prior to executing any updates.
To list enabled repositories execute:
yum repolist enabled
Any non-RHEL repositories should be disabled by setting “enable=0” in the corresponding /etc/yum.repo.d file.
Failure to do so may cause issues with the Avaya application.

Avaya Aura® System Manager 8.1.3.7

Avaya Aura® System Manager critical RPM versions list

java-1.8.0-openjdk-1.8.0.362.b08-1.el7_9.x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.342.b07-1.el7_9.x86_64
java-1.8.0-openjdk-headless-1.8.0.362.b08-1.el7_9.x86_64
java-1.8.0-openjdk-devel-1.8.0.362.b08-1.el7_9.x86_64

Avaya Aura® System Manager do not update RPM version list

postgresql13-13.3-1PGDG.rhel7.x86_64
postgresql13-server-13.3-1PGDG.rhel7.x86_64
postgresql13-contrib-13.3-1PGDG.rhel7.x86_64
postgresql13-libs-13.3-1PGDG.rhel7.x86_64
net-snmp-5.7.3-3.smgr.el7.x86_64
redhat-release-server-7.6-4.el7.x86_64

How to Upgrade System Manager RPMs
Avaya recommends taking a System Manager backup before performing the updates.

Pre Update
If you have a Geo Redundancy setup of System Manager disable Geo as a first step.
If your System Manager is deployed in a virtualize environment then it is also recommended that you take a snapshot of the System Manager virtual machine.

Stop the below Services as root user

```
systemctl stop crond.service
```

systemctl stop jboss.service
systemctl stop postgresql.service
systemctl stop spiritAgent.service
systemctl stop cnd.service
systemctl stop systemMonitor.service

Update Commands

Before upgrading JAVA, Copy following files to /swlibrary location:

1. cp $JAVA_HOME/jre/lib/security/java.security /swlibrary/java.security
2. cp $JAVA_HOME/jre/lib/security/java.policy /swlibrary/java.policy
3. cp $JAVA_HOME/jre/lib/security/blacklisted.certs /swlibrary/blacklisted.certs

Update critical RPMs

yum install java-1.8.0-openjdk-debuginfo-1.8.0.342.b07-1.el7_9.x86_64 java-1.8.0-openjdk-headless-1.8.0.362.b08-1.el7_9.x86_64 java-1.8.0-openjdk-devel-1.8.0.362.b08-1.el7_9.x86_64 java-1.8.0-openjdk-1.8.0.362.b08-1.el7_9.x86_64

Restore following files:

cd /swlibrary
cp -f java.security java.policy blacklisted.certs $JAVA_HOME/jre/lib/security/
cd $JAVA_HOME/jre/lib/security/
chown admin:admin java.security java.policy blacklisted.certs
chmod 644 java.security java.policy blacklisted.certs

Update all non-Critical RPMs

yum update -x "java-1.8.0-* postgresql13-* net-snmp redhat-release-server"

Update all critical RPMs with security fixes only

N/A

Post Update

After updating RPMs please reboot System Manager machine instance.

Once the System Manager is up and running post reboot, enable Geo redundancy (Note: this should be done only after you have patched the Secondary System Manager using the same set of instructions)

If you took a snapshot, make sure you remove them once you have successfully completed the process and System Manager is back up and running.

Avaya Aura® Communication Manager 8.1.3.7

Avaya Aura® Communication Manager critical RPM version list

glibc-2.17-326.el7_9.i686
glibc-2.17-326.el7_9.x86_64
glibc-common-2.17-326.el7_9.x86_64
kernel-3.10.0-1160.80.1.el7.x86_64
kernel-headers-3.10.0-1160.80.1.el7.x86_64
kernel-tools-3.10.0-1160.80.1.el7.x86_64
kernel-tools-libs-3.10.0-1160.80.1.el7.x86_64
openssh-clients-7.4p1-22.el7_9.x86_64
openssh-7.4p1-22.el7_9.x86_64
openssh-server-7.4p1-22.el7_9.x86_64
pam-1.1.8-23.el7.x86_64

pam-1.1.8-23.el7.i686

Avaya Aura® Communication Manager do not update RPM version list

redhat-release-server-7.6-4.el7.x86_64
initscripts-9.49.46-1.el7.x86_64

Avaya Aura® Communication Manager optional RPM versions list

If you have used the Avaya version of net-snmp and bash offered at installation time you should not upgrade these and instead use the versions provided by Avaya. You can confirm if you have the Avaya version of net-snmp and/or bash by executing ‘rpm -qa net-snmp*’ and ‘rpm -qa bash*’ and comparing the versions to the Optional Avaya RPMversions listed below or by the ‘AV’ indicator in the version.
The Avaya bash rpm offers additional command logging capability and the Avaya net-snmp rpm offers better performance for SNMP calls when used with Avaya Aura © Communication Manager than the RedHat version and therefore is more suitable if high numbers of SNMP calls will be made against CM although you may choose not to install the Avaya version should you wish to be able to update these with the latest RHEL versions.
To restore the Red Hat version of bash and net-snmp use ‘yum downgrade bash’, ‘yum downgrade net-snmp*’

bash-4.2.46-31.el7.AV1.x86_64
net-snmp-5.7.2-37.el7.AV1.x86_64
net-snmp-agent-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-libs-5.7.2-37.el7.AV1.x86_64
net-snmp-utils-5.7.2-37.el7.AV1.x86_64

How to Upgrade Communication Manager RPMs

Avaya recommends taking a Communication Manager backup before performing the updates.

Pre Update

Before updating RPMs it is recommended that a full CM backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Communication Manager guide
In a duplex system the RPM update should be done on the standby machine and CM processing should be stopped with a Busy-Out.

Update Commands

Update all critical RPMs with security fixes

yum install glibc-2.17-326.el7_9.i686 glibc-2.17-326.el7_9.x86_64 glibc-common-2.17-326.el7_9.x86_64 kernel-3.10.0-1160.80.1.el7.x86_64 kernel-tools-3.10.0-1160.80.1.el7.x86_64 kernel-tools-libs-3.10.0-1160.80.1.el7.x86_64 kernel-headers-3.10.0-1160.80.1.el7.x86_64 openssh-7.4p1-22.el7_9.x86_64 openssh-clients-7.4p1-22.el7_9.x86_64 openssh-server-7.4p1-22.el7_9.x86_64 pam-1.1.8-23.el7.i686 pam-1.1.8-23.el7.x86_64

Remove the SW-only installation rpm no longer required (optional)

rpm -e -v --nodeps avaya-cm-setup

Update all non-Critical RPMs

yum update -x 'glibc-* kernel-* openssh-* pam-* initscripts redhat-release-server nscd'

Post Update

When the RPM installation is complete restart the virtual machine by issuing the 'reboot' command.
A PAM rpm update can cause login failures to the SAT or the web SMI, if it is the case run these commands as root:
ln -sf /opt/ecs/lib/pam_unix_auth_x86_64.so /usr/lib64/security/pam_unix_auth.so
ln -sf /opt/ecs/lib/pam_unix_auth_i686.so /usr/lib/security/pam_unix_auth.so

Avaya Aura® Session Manager 8.1.3.7

Avaya Aura® Session Manager Avaya tested critical RPM versions list

None

Avaya Aura® Session Manager do not update RPM version list

nginx
postgresql13-*

How to Upgrade Session Manager RPMs

IMPORTANT: Any non-RHEL repositories should be disabled prior to executing any updates. If non-RHEL repositories are being used, it is recommended that /etc/yum.conf be edited to include:

*exclude=nginx postgresql13-**

Pre Update

Avaya recommends taking a Session Manager backup before performing the updates.
This process is service affecting. Session Manager will be out-of-service until it is placed back into "Accept New Service".

51. Place the SM in **Deny New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Deny New Service**.
    e. Before updating On the confirmation page, click **Confirm**.
52. On the **Session Manager Dashboard** page, wait until **Active Call Count** is zero. Refresh the screen to update the count.
53. Take a VM snapshot prior to making changes.
54. Stop SM with **stop -ac**.
55. Configure yum to point to a Red Hat 7 repository containing the updates.

Update Commands

Update All Non-Critical RPMs

yum update -x "nginx postgresql13-*"

Update Critical with security fixes

N/A

Post Update

After the update, the SM can be placed back in service by:
43. From the SM command line run: **bash /opt/ASMpatch/bin/setup_java.sh**
44. Reboot the SM.
45. From System Manager web console, select **Elements > Session Manager > System Tools > Maintenance Tests.**
    a. Select the Session Manager that was updated.
    b. Select **Execute all Tests.**

c. Verify that all tests pass. If not, refer to *Troubleshooting Avaya Aura® Session Manager and Maintaining Avaya Aura® Session Manager*.

46. Place the SM in **Accept New Service**.
    a. On the home page of System Manager Web Console, Under **Elements**, click **Session Manager**.
    b. On the **Session Manager Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the **Session Manager Instances** table.
    c. Click **Service State**.
    d. From the drop-down list box, select **Accept New Service**.
    e. On the confirmation page, click **Confirm**.
47. Remove the VM snapshot taken prior to the update.

Avaya Aura® Media Server 8.X

Avaya Aura® Media Server critical RPM versions list

None currently

Avaya Aura® Media Server do not update RPM versions list

None currently

Avaya Aura® Application Enablement Services 8.1.3.7

Avaya Aura® Application Enablement Services critical RPM version list

None

Avaya Aura® Application Enablement Services do not update RPM version list

axis-1.4-AV7.i386
php-7.4.2-1.el7.remi.x86_64
php-cli-7.4.2-1.el7.remi.x86_64
php-common-7.4.2-1.el7.remi.x86_64
php-json-7.4.2-1.el7.remi.x86_64
php-mbstring-7.4.2-1.el7.remi.x86_64
php-soap-7.4.2-1.el7.remi.x86_64
php-xml-7.4.2-1.el7.remi.x86_64
postgresql-9.2.24-1.el7_5.x86_64
postgresql-jdbc-9.2.1002-5.el7.noarch
postgresql-libs-9.2.24-1.el7_5.i686
postgresql-libs-9.2.24-1.el7_5.x86_64
postgresql-server-9.2.24-1.el7_5.x86_64
tomcat-8.5.81-AV.noarch
tomcat-el-3.0-api-8.5.81-AV.noarch
tomcat-jsp-2.3-api-8.5.81-AV.noarch
tomcat-lib-8.5.81-AV.noarch
tomcat-servlet-3.1-api-8.5.81-AV.noarch
log4j-1.2.17-16.el7_4.noarch

Note: log4j updates are given in AES 8.1.3.5. log4j rpm should not be upgraded manually.

How to Upgrade Application Enablement Services RPMs

Pre Update

Note: For upgrading to AE Services 8.1.3.7 in a software-only environment, you must install AE Services 8.1 or 8.1.1 ISO, upgrade it to AE Services 8.1.2.x and then upgrade to AE Services 8.1.3.7

52. Before updating RPMs it is recommended that a full AES backup and/or a virtual machine snapshot are performed. For more information, refer to the Backup and restore section of the Administering Avaya Aura Application Enablement Services guide.
53. Configure yum to point to a Red Hat 7 repository containing the updates. See Red Hat page for available repositories.
54. Add following line (excluded rpms list) into /etc/yum.conf file**.** "*exclude=axis-*,tomcat-*,redhat-release-server-*,php-*,postgresql -*,log4j-*"*
55. Take backup of the httpd service file- **/usr/lib/systemd/system/httpd.service** in /tmp
56. Take backup of the slapd.conf configuration file - **/etc/openldap/slapd.conf** in /tmp
57. **Important Note: If High Availability is configured, please follow the following steps:**
    a. Update secondary(standby) AES with the OS packages as per the Pre Update, Update and Post Update instructions
    b. Post reboot, wait for aesvcs (*systemctl status aesvcs*) to be in active(running) state.
    c. Synchronize the data between the Primary and the Secondary Server
    d. Perform Failover from Primary to Secondary Server
    e. Update the new Secondary(standby) server with the OS packages as per the Pre Update, Update and Post Update instructions.
    f. Post reboot, wait for aesvcs (*systemctl status aesvcs*) to be in active(running) state.
    g. If required, perform failover from primary to secondary server. (Optional step)

Update Commands

Update All Non-Critical RPMs

yum update -x 'axis-* tomcat-* redhat-release-server-* php-* postgresql-* log4j-*'

Update Critical with security fixes

None

Important Note:

In case the above update command *fails* with the following message:

Transaction check error:

file /etc/openldap/schema/core.schema from install of openldap-servers-2.4.44-20.el7.x86_64 conflicts with file from package aesvcs-userService-config-8.x.x.0.0.x-0.noarch

then perform the following steps:

****Note: The following steps will rebuild the rpm database on your system. Verify that there are no processes with the RPM database files open. Ensure that you have necessary backup.****

- Take back up of existing rpm database by executing below command:
  mv /var/lib/rpm/__db.00 /tmp*
- Rebuild rpm database by executing below command:
  rpm --rebuilddb
- Perform update again by executing below command:
  yum update -x 'axis- tomcat-* redhat-release-server-* php-* postgresql-* log4j-*'*
- If required, restore the rpm database backup that was copied earlier. (**This is an optional step**)

Post Update

- After rpm upgrades check installed "java-1.8.0-openjdk" rpm (rpm -qa | grep java-1.8.0-openjdk) version and recreate "/usr/java/default/" softlink

cd /usr/java/

rm -rf default

ln -s /usr/lib/jvm/java-1.8.0-openjdk default

- If httpd rpm is updated, them rename the file " /etc/httpd/conf.d/autoindex.conf"

  mv /etc/httpd/conf.d/autoindex.conf /etc/httpd/conf.d/autoindex.conf.bkup

  Replace the httpd.service file with the backed up file in service file in Pre Update step

  mv /tmp/httpd.service /usr/lib/systemd/system/httpd.service

  Reload the systemctl daemon: *systemctl daemon-reload* for changes to take effect.

- If openldap rpm is updated, then replace the /etc/openldap/slapd.conf file with the backed up file. The back up was taken in Pre Update Step.
  mv /tmp/slapd.conf /etc/openldap/slapd.conf

- If sudo rpm is being updated, make sure to remove "*session include system-auth*" entry from /etc/pam.d/sudo

  sed -i "/session include system-auth/d" /etc/pam.d/sudo

- If kernel rpm is being updated (> 3.10.1062) and if a DHCP server is configured in the subnet in which AES resides, make the following changes so that AES does not acquire a dynamic IP address post reboot:
  - Edit "/etc/default/grub" to add the highlighted parameter:
    GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb quiet net.ifnames=0 biosdevname=0 rd.neednet=0"
  - Run the command *"grub2-mkconfig -o /boot/grub2/grub.cfg"*

- **Reboot** AES machine instance.

  reboot

Avaya Aura® WebLM (Standalone) 8.1.3.7

Note: Please refer WebLM SW-Only deployment guide
https://download.avaya.com/css/public/documents/101058240

Avaya Aura® WebLM (Standalone) critical RPM versions list

java-1.8.0-openjdk-devel-1.8.0.362.b08-1.el7_9.x86_64
java-1.8.0-openjdk-headless-1.8.0.362.b08-1.el7_9.x86_64
java-1.8.0-openjdk-1.8.0.362.b08-1.el7_9.x86_64
java-1.8.0-openjdk-debuginfo-1.8.0.51-1.b16.el7_1.x86_64

Avaya Aura® WebLM (Standalone) do not update RPM version list
redhat-release-server-7.6-4.el7.x86_64

How to Upgrade WebLM RPMs

Pre Update

1. If feasible take WebLM instance backup(For VMware take snapshot).
2. Stop below service

   systemctl stop jboss.service

Remove net-snmp RPM:

yum remove net-snmp

(We don’t use net-snmp on WebLM, so we need to remove net-snmp irrespective of its any installed version)

Before upgrading JAVA, Copy following files to /opt location:

1. cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/java.security /opt/java.security
2. cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/java.policy /opt/java.policy
3. cp /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/blacklisted.certs /opt/blacklisted.certs

Update critical RPMs

yum install java-1.8.0-openjdk-debuginfo-1.8.0.51-1.b16.el7_1.x86_64 java-1.8.0-openjdk-headless-1.8.0.362.b08-1.el7_9.x86_64 java-1.8.0-openjdk-devel-1.8.0.362.b08-1.el7_9.x86_64 java-1.8.0-openjdk-1.8.0.362.b08-1.el7_9.x86_64

Restore following files:

cd /opt
cp -f java.security java.policy blacklisted.certs /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/
cd /usr/lib/jvm/java-1.8.0-openjdk/jre/lib/security/
chmod 644 java.security java.policy blacklisted.certs

Update All Non-Critical RPMs

yum update -x "java-1.8.0-* redhat-release*"

Update Critical with security fixes

N/A

Post Update

After updating RPMs please reboot WebLM machine instance.

Once installation completed, set the **java path** and reboot the system.

Workaround or alternative remediation
n/a

Remarks

Issue 2: January 4, 2019 –

- 8.0 Revision 2.0
- 8.0.1 Revision 1.0

Issue 3: January 9, 2019 – Updated to provide CM and SM instructions

Issue 4: February 18, 2019 – Updated with latest 8.0.1 test results. AES 8.0 critical rpms changed to "None".

Issue 5: February 25, 2019 – Updated yum install instructions for WebLM.

Issue 6: April 24, 2019 –Updated to provide 8.0.1.1. 8.0.1 moved to Appendix.

Issue 7: June 30, 2019 – Updated to provide 8.1. 8.0.1.1 moved to Appendix.

Issue 8: July 3, 2019 – Updated SMGR & WebLM "do not update RPM version" lists for 8.1, RH version is redhat-release-server-7.6-4.el7.x86_64

Issue 9: July 8, 2019 – Updated SMGR & WebLM "do not update RPM version" lists for 8.0 and 8.0.1.x, RH version is redhat-release-server-7.5-8.el7.x86_64. Updated list of CM critical rpms to add pam rpms.

Issue 10: Oct 4, 2019 – Updated AES "Do Not Update rpm" list to remove bash & initscripts. Update commands modified to reflect those changes.

Issue 11: Nov 4, 2019 – Updated to provide 8.1.1, 8.1.0 moved to Appendix.

Issue 12: Dec 30, 2019 – Updated AES Pre Update section to remove bash, libuuid and initscripts.

Issue 13: Apr 28, 2020 – Updated to include 8.1.2, also initscripts update to earlier CM releases, 8.1.1 moved to Appendix.

Issue 14: Oct 29, 2020 – Updated to provide 8.1.3, 8.1.2 moved to Appendix.

Issue 15: May 11, 2021 – Updated to provide 8.1.3.1, 8.1.3 move to Appendix. SMGR java versions updated.

Issue 16: May 19, 2021 – Updated the Pre Update and Post Update section for AES 8.1.3.1. Steps for backup and restore of /etc/openldap/slapd.conf are added in case of openldap rpm update. Updated the WebLM 8.1.3.1 section to highlight java version update change to 272 from original 292 posted in Issue 15.

Issue 17: July 09, 2021 – Updated to provide 8.1.3.2, 8.1.3.1 moved to Appendix.

Issue 18: November 11, 2021 -- Updated to provide 8.1.3.3, 8.1.3.2 moved to Appendix.

Issue 19: March 07, 2022 -- Updated to provide 8.1.3.4, 8.1.3.3 moved to Appendix.

Issue 20: July 07, 2022 -- Updated to provide 8.1.3.5, 8.1.3.4 moved to Appendix.

Issue 21: September 02, 2022 – Updated to reflect introduction of CM 8.1.3.5.1.

Issue 22: November 21, 2022 -- Updated to provide 8.1.3.6; 8.1.3.5 moved to Appendix.

Issue 23: March 20, 2023 – Updated to provide 8.1.3.7; 8.1.3.6 moved to Appendix.

Issue 24: June 9, 2023 – Updated to provide 8.1.3.8, 8.1.3.7 moved to Appendix.;

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch	
n/a	
Download	
n/a	
Patch install instructions	**Service-interrupting?**
n/a	Yes
Verification	
n/a	
Failure	
n/a	
Patch uninstall instructions	
n/a	

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

Failure to keep updated to latest tested version of the application RPMs may reduce the security of the system.

Avaya Security Vulnerability Classification

n/a

Mitigation

n/a

If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support Terms of Use.