Product Support Notice

PSN #	PSN020171u				
Original publication date: 8-Jun-15. This is Issue #11, published date: 23-Jan-17.		Severity/risk level	High	Urgency	When convenient
Name of problem	CM is updating SNMP functionality to Net-SNMP.				

Products affected

Avaya Aura® Communication Manager (CM), Release 6.3
Avaya Aura® Solution for Midsize Enterprise, Releases 6.x.x
S8300 Server
S8510 Server
S8800 Server
Common Servers (HP & Dell)

Problem description

This problem occurs in Avaya Aura® Communication Manager (CM) Release 6.3.

CM is updating Simple Network Management Protocol (SNMP) functionality to Net-SNMP.

Resolution

CM is updating Fault Performance Alarming (FPA) SNMP functionality to Net-SNMP in 6.3.100.0/6.3.111.0 and higher 6.3.1xx (load 141) Service Packs (SPs) and releases. There will be two separate CM 6.3 releases going forward, with the only difference being new Net-SNMP functionality. CM 6.3.100.0 /6.3.111.0 (6.3.11.0 CM 6.3 Service Pack 11 equivalent) and higher 6.3.1xx SPs is a new release that includes new Net-SNMP FPA functionality.

Since CM 6.3.100/1xx is a new release/template, when moving from 6.3 load 124 (e.g., 6.3.14.0) to 6.3 load 141 (e.g., 6.3.114.0) you must first upgrade the system to 6.3.100.0 (from load 124 to load 141), and then proceed to activate the load 141 Service Pack (e.g., 6.3.114.0).

Note: Net-SNMP resolves the following known issue with SNMP functionality. Previously, when an SNMP request was sent to the virtual IP address of a duplicated CM pair using the G3 Avaya MIB, the SNMP response was returned from the physical source IP address of the duplicated server responding. This created a condition where the destination IP address of the request did not match the source IP address of the response, which could cause the transaction to be blocked at intervening firewalls.

Releases with new Net-SNMP functionality require changes to Network Management Systems and SNMP alarming. Additional detail can be found in the following documents:
Avaya Aura® Communication Manager SNMP Renewal Quick Reference Guide
Avaya Aura® Communication Manager SNMP Administration and Reference Guide

With Net-SNMP functionality CM MIBs have changed. The AVAYA-AURA-CM-MIB and AVAYA-AURA-CMALARM-MIB can be downloaded directly from a server running CM 6.3.1xx and higher releases.

- The AVAYA-AURA-CM-MIB can be downloaded from the SNMP Access System Management Interface (SMI) page.
- The AVAYA-AURA-CMALARM-MIB can be downloaded from the FP Traps SMI page.

Additionally, in interim and new CM SPs/patches* the existing FPA SNMP functionality will be made permanent. This means no future changes will be provided or allowed to the 6.3.xx SNMP functionality. **Over-writable patch (designed to be activated on top of currently activated CM patches/SPs) 22038 will make the existing SNMP functionality permanent, and will automatically be activated when unpacking interim and new CM SPs/patches* if SP 6.3.1.0 - 6.3.10.0 or custom patches based on these SPs are activated**. Once activated, patch 22038 cannot be deactivated (undone).

Patch 22038 is a part of interim and new CM SPs/patches*. It is not designed to be applied independently, and attempts to apply it independently will fail. Custom CM 6.3 patches created after June 8, 2015 will include and automatically activate (when being unpacked) over-writable patch (designed to be activated on top of currently activated CM patches/SPs) 22038 and will make current SNMP functionality permanent.

* Note: The term “new CM SP/patch” is used to denote CM 6.3.11.1 and higher 6.3 Service Packs (SPs), or CM 6.3 custom patches built after July 23, 2015. The term “old CM SP/patch” is used to denote CM 6.3.10.0 and lower 6.3 SPs, or CM 6.3 custom patches built prior to June 8, 2015. The term “interim CM SP/patch” is used to denote 6.3.11.0 or CM 6.3 custom patches built between June 8, 2015 and July 23, 2015.

When new CM SPs/patches* are activated, old CM SPs/patches* can be unpacked and activated afterwards (downgrade/rollback is allowed). **When interim CM SPs/patches* are activated, old CM SPs/patches* can no longer be activated and will fail at the unpack step (downgrade/rollback is not allowed)** with errors similar to the following (in this case an attempt is made to activate 6.3.6.0 after SP 6.3.11.0 is activated):

unpacking file /var/home/ftp/pub/03.0.124.0-21591.tar.gz
xdelta: /opt/updates/03.0.124.0-21591/objects/mvmgt: Checksum validation failed,
expected: b19c63b0de76e2ea779c127831419bd2, received: 683ef12acbba7e0412930dab0b211343
xdelta: /opt/ecssw-03.0.124.0/mvmgt: Checksum validation failed, expected: 2b424
86a97513cc5bd8a5dfc60deef78, received: b19c63b0de76e2ea779c127831419bd2
xdelta failed for file /opt/updates/03.0.124.0-21591/mvmgt.update.
unpacking of /var/home/ftp/pub/03.0.124.0-21591.tar.gz failed:65280

Therefore, if interim CM SPs/patches* are currently activated, and there is a need to activate old CM SPs/patches*, the proper steps are to activate a new CM SP/patch* and then activate the desired old CM SP/patch*. For example, if 6.3.11.0 is activated, and there is a need to downgrade/rollback to 6.3.10.0, 6.3.11.1 should be activated and then 6.3.10.0 can be activated immediately after 6.3.11.1 is activated.

The CM 6.3.xx.0 and 6.3.1xx.0 releases/SPs will be compatible for survivable servers. This means that for the determination of survivable server SP/Release compatibility 6.3.xx.0 and 6.3.1xx.0 are compatible if the xx are identical numbers, or the xx on the survivable server is a higher number than the xx on the primary server pair. For example, the following server configurations are compatible:

- A primary server running CM 6.3.1.0 – 6.3.11.0 and survivable servers running CM 6.3.111.0 and higher SPs.
- A primary server running CM 6.3.12.0 and survivable servers running CM 6.3.112.0 and higher SPs.
- A primary server running CM 6.3.13.0 and survivable servers running CM 6.3.113.0 and higher SPs.
- A primary server running CM 6.3.111.0 and survivable servers running CM 6.3.11.0 and higher SPs.
- A primary server running CM 6.3.112.0 and survivable servers running CM 6.3.12.0 and higher SPs.
- A primary server running CM 6.3.113.0 and survivable servers running CM 6.3.13.0 and higher SPs.
- Etc.

The following are examples of server configurations that are not compatible:

- A primary server running CM 6.3.12.0 and survivable servers running CM 6.3.111.0
- A primary server running CM 6.3.13.0 and survivable servers running CM 6.3.111.0 or 6.3.112.0
- A primary server running CM 6.3.14.0 and survivable servers running CM 6.3.113.0/6.3.112.0/6.3.111.0
- A primary server running CM 6.3.111.0 and survivable servers running CM 6.3.10.0 and lower SPs.
- A primary server running CM 6.3.112.0 and survivable servers running CM 6.3.11.0 and lower SPs.
- Etc.

The CM 6.3.xx.0 and 6.3.1xx.0 releases/SPs are not compatible for active and standby servers in a duplicated server pair. Active and standby servers in a duplicated server pair must run the exact same CM patch/SP. For example, shadowing/refresh and filesync will fail if an active server is running 6.3.11.0 and the standby server is running 6.3.111.0.

* Note: The term “new CM SP/patch” is used to denote CM 6.3.11.1 and higher 6.3 Service Packs (SPs), or CM 6.3 custom patches built after July 23, 2015. The term “old CM SP/patch” is used to denote CM 6.3.10.0 and lower 6.3 SPs, or CM 6.3 custom patches built prior to June 8, 2015. The term “interim CM SP/patch” is used to denote 6.3.11.0 or CM 6.3 custom patches built between June 8, 2015 and July 23, 2015.

The remaining information presented in this section applies to interim CM SPs/patches* only. Disregard this information if interim CM SPs/patches* are not being used.

Any old CM SPs/patches* that are removed from CM before or after an interim CM SP/patch* is unpacked, can no longer be unpacked or activated in the future. This has the following implications:

1. The act of activating CM SPs/patches from the System Platform Webconsole causes the currently activated CM SP/patch to be deactivated and removed from CM.
    a. This means that if an interim CM SP/patch* is activated from the System Platform Webconsole, the old CM SP/patch* that was previously activated cannot be unpacked or activated in the future.
2. In order to be able to activate/reactivate old CM SP/patches* after interim CM SPs/patches* are unpacked/activated, the old CM SP/patch* must be in the unpacked or activated state (See 1 and 1a above for information on how activating an interim CM SP/patch* from System Platform Webconsole affects the ability to reactivate the currently activated old CM SP/patch*).
    a. In an unpacked state means the SP/patch shows a status of unpacked on the Manager Updates page in the CM System Management Interface (SMI) or CLI "swversion" command output. It shows a status of installed on the System Platform Webconsole Server Management > Patch Management page.
    b. In an activated state means the SP/patch shows a status of activated on the Manager Updates page in the CM System Management Interface (SMI) or CLI "swversion" command output. It shows a status of active on the System Platform Webconsole Server Management > Patch Management page.
3. If there is a need to unpack/activate an old CM SP/patch* that was removed, or never on the system, after an interim CM SP/patch* has been unpacked/activated, a new CM SP/patch* should be activated first and then the old CM SP/patch* can be activated. Another option is to contact Avaya Technical Support and a new SP/patch* with identical content of the old SP/patch* can be provided. The new SP/patch* with identical content will not be blocked from being unpacked/activated.

There is a known issue that might occur when unpacking/activating an interim CM SP/patch* if the Bash shell vulnerability (Shellshock) patch 21904 has been previously activated. The known issue causes over-writable patch 22038 to not show/display as activated, even though it did actually activate. If this occurs do not deactivate the interim CM SP/patch* because the patch activation was successful.

To summarize:

- Any old CM SPs/patches* that are removed from CM before an interim CM SP/patch* is unpacked/activated, can no longer be unpacked or activated in the future.
- Leave current old CM SPs/patches* on the system as is, in unpacked or activated states, until after interim CM SPs/patches* that include 22038 have been unpacked. This allows old CM active SPs/patches* currently on the system to be reactivated in the future (see 1 and 1a above for an exception involving activation via System Platform Webconsole).
- If there is a need to unpack/activate an old CM SP/patch* that was removed or not on the system when an interim CM SP/patch* was unpacked/activated, activate a new CM SP/patch* first and then the old CM SP/patch* can be activated.

Note: Going forward, software fixes for old FPA SNMP functionality will not be provided. Software fixes for FPA SNMP will only be provided on FPA Net-SNMP functionality in 6.3.100/6.3.111.0 and higher SPs/Releases.

* Note: The term "new CM SP/patch" is used to denote CM 6.3.11.1 and higher 6.3 Service Packs (SPs), or CM 6.3 custom patches built after July 23, 2015. The term "old CM SP/patch" is used to denote CM 6.3.10.0 and lower 6.3 SPs, or CM 6.3 custom patches built prior to June 8, 2015. The term "interim CM SP/patch" is used to denote 6.3.11.0 or CM 6.3 custom patches built between June 8, 2015 and July 23, 2015.

Workaround or alternative remediation

n/a

Remarks

n/a

Patch Notes

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

Backup before applying the patch

Always

Download

Service Packs can be downloaded from "**support.avaya.com**". Custom patches must be provided by Avaya Support.

Patch install instructions	Service-interrupting?
Patch activation instructions are available on "**support.avaya.com**". CM Service Pack/patch activation is	Yes

service impacting on non-duplicated servers, and on all servers running CM 5.2 and lower releases. For duplicated servers running CM 5.2.1 and higher releases, SPs/patches can be activated in a connection preserving manner.

Note: Review the Resolution section of this document for all caveats when activating CM 6.3.11.0 or CM custom patches built between June 8, 2015 and July 23, 2015 (CM interim SPs/patches).

Verification

Patch installation instructions include verification instructions.

Failure

Contact Technical Support.

Patch uninstall instructions

Once activated, patch 22038 cannot be deactivated.

Security Notes

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

Security risks

n/a

Avaya Security Vulnerability Classification

Not Susceptible

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.