Product Support Notice

PSN # PSN004788u

Original publication date: 26-Jul-16. This is Issue #04, published date: 19-Jan-17. | Severity/risk level: High | Urgency: Immediately

Name of problem

SAL Gateway Remote Agent Push – End state of SAL Gateways described.

Products affected

SAL Gateway releases 2.x

Problem description

There was a critical need to upgrade all release 2.x SAL Gateways to SHA-2 before the end of 2016 as described in PSN004539u.

- The SAL Gateway Upgrade Playbook was provided to assist in this process.
- Release 1.x SAL Gateways were exempted because they transitioned to End of Services Support on Oct 1, 2016.

The remote agent push described in this PSN was provided as a "clean-up" mechanism to catch the release 2.x SAL Gateways that were not upgraded. The remote agent push was a method to remotely update the agent software in the SAL Gateway to be SHA-2 compliant. This method did not upgrade the whole SAL Gateway; it only pushed a new agent to the gateway. The remote agent push left the gateways in a state that requires further attention by customers and partners.

Resolution

Customers and partners must understand what can and cannot be done to a SAL Gateway that has received a remote agent push.

If you have a SAL Gateway that is one of the following releases and is still functioning – communicating with the SAL concentrator – then it has most likely received a remote agent push.

- 2.0.x, 2.1.x, 2.2.x, 2.3.x, 2.5.0.x, 2.5.1.x
- Services VM 1.0, Services VM 2.0, Services VM 3.0 without applying SP1

See the SAL Gateway Upgrade Playbook for determining SAL Gateway and SVM versions.

To confirm that these SAL Gateways have received the remote agent push, execute the following from the Linux command line:

```
[user@ve-avaya-sa ~]# service axedaAgent status
AXEDA Agent Application 6.8.1 is running (10521)
```

If the Axeda Agent version is 6.8.1 and the SAL Gateway is one of the releases listed above, it has received a remote agent push. SAL Gateways that have received a remote agent push require special treatment as shown in the following table.

SAL Gateway Updates and Upgrades

SAL Gateway release #	Software Updates (patches and service packs)	Software Upgrade (new minor or major release)
2.0.x w/ remote agent push 2.1.x w/ remote agent push 2.2.x w/ remote agent push 2.3.x w/ remote agent push	Must not apply any SAL software updates. Those updates were created with the intent to be applied on the original SAL Gateway, and may render the SAL Gateway inoperable if applied to one that has a SHA-2 agent.	May be upgraded to SAL Gateway 2.5 w/ SP3
2.5.0.x w/ remote agent push 2.5.1.x w/ remote agent push 2.5.2.x (SHA-2 SP2) 2.5.3.x (SHA-2 SP3)	SP3 for SAL Gateway 2.5 may be applied if not already	May be upgraded to SAL Gateway 3.0 (when released) if current SAL Gateway 2.5 is running on RHEL 6.x
Services VM 1.0 w/ remote agent push Services VM 2.0 w/ remote agent push	Must not apply any SAL software updates. Those updates were created with the intent to be applied on the original SAL Gateway, and may render the SAL Gateway inoperable if applied to one that has a SHA-2 agent.	May be upgraded to Services VM 3.0 w/ SP1
Services VM 3.0 w/ remote agent push Services VM 3.0 w/ SP1	SP1 for Services VM 3.0 may be applied if not already	May be upgraded to Services VM 4.0 (when released)

Applicable to all functioning SAL Gateways, regardless of how they reached SHA-2 compliance, the new SHA-2 agent performs a case-sensitive check (which the previous SHA-1 agent did not) against the SAL concentrator's certificate. This is an added security measure in the new SHA-2 agent. As described in the release notes for the SHA-2 service packs…

Issue	Resolution
The SAL Gateway remote access agent fails to communicate with the SAL Concentrator. This happens if the Common Name [CN] in the concentrator certificate and URL does not exactly match the FQDN entered in the SAL Gateway web UI "Primary Remote Server" and "Secondary Remote Server" fields. For example, the concentrator URL is https://remote.sal.partnerabc.com (with remote.sal.partnerabc.com also being the CN) but the FQDN entered in the SAL Gateway "Remote Server" fields is REMOTE.SAL.PARTNERABC.COM or Remote.sal.partnerabc.com. The error in the xGate.log file is shown as: `ERROR-- xgEnterpriseProxy: Web Client (https://<name>/eMessage): SSL: server's certificate verification failed (error:14090086: SSL routines: SSL3_GET_SERVER_CERTIFICATE:certificate verify failed)`	Update the FQDN entry in the SAL Gateway web UI to exactly match the Common Name [CN] in the concentrator certificate and URL.
Same condition exists for the connection between the SAL Gateway and Policy Server, as administered in the "Policy Server" section of the web UI.	Same resolution.
The remote agent push script automatically checked for a "Remote Server" mismatch and did not execute if the mismatch existed. The mismatch must be resolved manually via the SAL Gateway web UI, and now that the push period has ended, the SAL Gateway must be upgraded for SHA-2 compliance. The script did not check for a "Policy Server" mismatch.	

The remote agent push script backed up the SAL Gateway and restored the software to the original state if the update was unsuccessful, as described in the Patch Notes below.

Workaround or alternative remediation

None

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

Done automatically by remote agent push script

Download

Done automatically by the Avaya SAL infrastructure

Patch install instructions — Service-interrupting?

None – all automated — 1min to restart agent*

Verification

Script automatically verifies correct installation of new agent.

Failure

Script automatically reverts to previous agent if new agent does not install correctly.

Patch uninstall instructions

N/A

*This is not a restart of the SAL Gateway but of the agent that was updated to SHA-2. The restart entails re-establishing the connections to all the managed devices administered in the SAL Gateway.

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.

Business Partner Notes

Additional information for Business Partners

n/a

Avaya Notes

Additional information for Tier 3, Tier 4, and development

n/a