Hewlett Packard Enterprise

Server Automation

Server Automation Alert: SHA1 Deprecation

Software version: 9.1x, 10.0x, 10.1x, 10.2x (Enterprise or Ultimate editions of SA); SAVA (Standard or Premium editions)

Document release date: May 2016

Software release date: 2014

Contents

Issue that Requires Attention

SHA1 Deprecation

https://community.qualys.com/blogs/securitylabs/2014/09/09/sha1-deprecation-what-you-need-to-know

Certificates used by secure websites are signed using hashing algorithms. SHA1 is one such hashing algorithm. Feasibility of breaking SHA1 has increased in the recent past and can lead to potential exposure of secure communication. Microsoft, Google and Mozilla have recently announced they won't be accepting SHA1 certificates post 2016.

HPE has investigated this vulnerability in relation to Server Automation (SA). SA creates self-signed certificates using SHA1 algorithm during installation. They are used for secure communication between various components of SA and communication with clients. HPE recommends that you perform the mitigating actions described in the next section.

Immediate Mitigation

1. Existing SA meshes can be converted to SHA256 only by a full core recertification. Detailed steps on recertification process is listed in SA Administration Guide - SA Core Recertification section.

   Note that on SA versions 10.10 - 10.22, a Patch (Rollup hot fix) has to be deployed before being able to use the SHA256 signing algorithm option for recertification (QCCR1D219041). In 10.23 and later there is no need for this Patch.

   Older SA versions (10.0x and 9.1x) must be upgraded before attempting a core recertification with SHA256. Upgrading to 10.22 or above is preferred.

   SAVA 2.0 can be upgraded to DCAA. SA in DCAA 1.1 is 10.21. Apply Patch (Rollup hot fix) of SA 10.21 and recertify the core. Migration guide for SAVA 2.0 to DCAA can be found here: https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/KM01500495

   Customers with SAVA 1.0 should also look into converting to use DCAA.

   Please contact SA Support for the available Patches (Rollup hot fixes).

2. Links to Administration guides are provided in the following table.

SA Version	Administration guide download link
Server Automation 10.1x	https://softwaresupport.hpe.com/km/KM00774463/hp_man_SA_10.1_AdministrationGuide_pdf.pdf
Server Automation 10.2x	https://softwaresupport.hpe.com/km/KM01253505/hp_man_SA_10.2_AdministrationGuide_pdf.pdf
Server Automation 10.22	https://softwaresupport.hpe.com/km/KM02030066/SA_10.22_UG_Administration.pdf

Send documentation feedback

If you have comments about this document, you can send them to hpsa-docs@hpe.com.

Legal notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted rights legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright notice

Trademark notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

RED HAT READY™ Logo and RED HAT CERTIFIED PARTNER™ Logo are trademarks of Red Hat, Inc.

The OpenStack word mark and the Square O Design, together or apart, are trademarks or registered trademarks of OpenStack Foundation in the United States and other countries, and are used with the OpenStack Foundation's permission.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to the following URL and sign-in or register: https://softwaresupport.hp.com/

Select Manuals from the Dashboard menu to view all available documentation. Use the search and filter functions to find documentation, whitepapers, and other information sources.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your Hewlett Packard Enterprise sales representative for details.

Support

Visit the Hewlett Packard Enterprise Software Support Online web site at https://softwaresupport.hp.com/