Release Notes

Published
2024-02-20

JSA 7.5.0 Update Package 3 SFS

JUNIPER NETWORKS | Engineering Simplicity

Table of Contents

What's New in JSA 7.5.0 Update Package 3 | 1

Installing the JSA 7.5.0 Update Package 3 Software Update | 1

Installation Wrap-up | 3

Clearing the Cache | 4

Known Issues and Limitations | 5

Resolved Issues | 7

What's New in JSA 7.5.0 Update Package 3

For more information about what's new in JSA 7.5.0 Update Package 2, see What's New Guide.

Installing the JSA 7.5.0 Update Package 3 Software Update

JSA 7.5.0 Update Package 3 resolves reported issues from users and administrators from previous JSA versions. This cumulative software update fixes known software issues in your JSA deployment. JSA software updates are installed by using an SFS file. The software update can update all appliances attached to the JSA Console.

The 7.5.0.20220829221022 SFS file can upgrade the following JSA versions to JSA 7.5.0 Update Package 3:

- JSA 7.3.2 (GA - Fix Pack 7)
- JSA 7.3.3 (GA - Fix Pack 11)
- JSA 7.4.0 (GA - Fix Pack 4)
- JSA 7.4.1 (GA - Fix Pack 2)
- JSA 7.4.2 (GA - Fix Pack 3)
- JSA 7.4.3 (GA - Fix Pack 6)
- JSA 7.5.0 (GA - Update Package 2)

This document does not cover all the installation messages and requirements, such as changes to appliance memory requirements or browser requirements for JSA. For more information, see the Juniper Secure Analytics Upgrading JSA to 7.5.0.

Ensure that you take the following precautions:

- Back up your data before you begin any software upgrade. For more information about backup and recovery, see the Juniper Secure Analytics Administration Guide.
- To avoid access errors in your log file, close all open JSA webUI sessions.

- The software update for JSA cannot be installed on a managed host that is at a different software version from the Console. All appliances in the deployment must be at the same software revision to update the entire deployment.
- Verify that all changes are deployed on your appliances. The update cannot install on appliances that have changes that are not deployed.
- If this is a new installation, administrators must review the instructions in the Juniper Secure Analytics Installation Guide.

To install the JSA 7.5.0 Update Package 3 software update:

1. Download the 7.5.0.20220829221022 SFS from the Juniper Customer Support website.
   https://support.juniper.net/support/downloads/
2. Using SSH, log into your system as the root user.
3. To verify you have enough space (5 GB) in **/store/tmp** for the JSA Console, type the following command:
   df -h /tmp /storetmp /store/transient | tee diskchecks.txt
   - Best directory option: **/storetmp**

     It is available on all appliance types at all versions. In JSA 7.5.0 versions /store/tmp is a symlink to the /storetmp partition.

   If the disk check command fails, retype the quotation marks from your terminal, then re-run the command. This command returns the details to both the command window and to a file on the Console named diskchecks.txt. Review this file to ensure that all appliances have **at minimum 5 GB of space available in a directory to copy the SFS** before attempting to move the file to a managed host. If required, free up disk space on any host that fails to have less than 5 GB available.

   NOTE: In JSA 7.3.0 and later, an update to directory structure for STIG compliant directories reduces the size of several partitions. This can impact moving large files to JSA.
4. To create the **/media/updates** directory, type the following command:
   mkdir -p /media/updates
5. Using SCP, copy the files to the JSA Console to the **/storetmp** directory or a location with 5 GB of disk space.
6. Change to the directory where you copied the patch file.
   For example, **cd /storetmp**
7. Unzip the file in the **/storetmp** directory using the bunzip utility:
   bunzip2 7.5.0.20220829221022.sfs.bz2
8. To mount the patch file to the /media/updates directory, type the following command:

mount -o loop -t squashfs /storetmp/7.5.0.20220829221022.sfs /media/updates

9. To run the patch installer, type the following command:

   /media/updates/installer

   NOTE: The first time that you run the software update, there might be a delay before the software update installation menu is displayed.

10. Using the patch installer, select **all**.

    - The **all** option updates the software on all appliances in the following order:
      - Console
      - No order required for remaining appliances. All remaining appliances can be updated in any order the administrator requires.
    - If you do not select the **all** option, you must select your console appliance.

      As of the JSA 2014.6.r4 patch and later, administrators are only provided the option to update **all** or update the Console appliance. Managed hosts are not displayed in the installation menu to ensure that the console is patched first. After the console is patched, a list of managed hosts that can be updated is displayed in the installation menu. This change was made starting with the JSA 2014.6.r4 patch to ensure that the console appliance is always updated before managed hosts to prevent upgrade issues.

      If administrators want to patch systems in series, they can update the console first, then copy the patch to all other appliances and run the software update installer individually on each managed host. The console must be patched before you can run the installer on managed hosts. When updating in parallel, there is no order required in how you update appliances after the console is updated.

      If your Secure Shell (SSH) session is disconnected while the upgrade is in progress, the upgrade continues. When you reopen your SSH session and rerun the installer, the patch installation resumes.

Installation Wrap-up

1. After the patch completes and you have exited the installer, type the following command:

   umount /media/updates

2. Clear your browser cache before logging in to the Console.

3. Delete the SFS file from all appliances.

Results

A summary of the software update installation advises you of any managed host that were not updated. If the software update fails to update a managed host, you can copy the software update to the host and run the installation locally.

After all hosts are updated, administrators can send an email to their team to inform them that they will need to clear their browser cache before logging in to the JSA.

Clearing the Cache

After you install the patch, you must clear your Java cache and your web browser cache before you log into the JSA appliance.

Before you begin

Ensure that you have only one instance of your browser open. If you have multiple versions of your browser open, the cache might fail to clear.

Ensure that the Java Runtime Environment is installed on the desktop system that you use to view the user interface. You can download Java version 1.7 from the Java website: http://java.com/.

About this task

If you use the Microsoft Windows 7 operating system, the Java icon is typically located under the Programs pane.

To clear the cache:

1. Clear your Java cache:
   a. On your desktop, select **Start** > **Control Panel**.
   b. Double-click the Java icon.
   c. In the Temporary Internet Files pane, click **View**.
   d. On the Java Cache Viewer window, select all **Deployment Editor entries**.
   e. Click the Delete icon.
   f. Click **Close**.
   g. Click **OK**.

2. Open your web browser.
3. Clear the cache of your web browser. If you use the Mozilla Firefox web browser, you must clear the cache in the Microsoft Internet Explorer and Mozilla Firefox web browsers.
4. Log in to JSA.

Known Issues and Limitations

The known issues addressed in the JSA 7.5.0 Update Package 3 are listed below:

- Docker services fail to start on JSA appliances that were originally installed at JSA release 2014.8 or earlier, then upgraded to 7.5.0 Update Package 2 Interim Fix 02 or 7.5.0 Update Package 3.

  Before updating to JSA 7.5.0 Update Package 2 Interim Fix 02 run the following command from the JSA Console:

  xfs_info /store | grep ftype

  Review the output to confirm the ftype setting. If the output setting displays "ftype=0", do not proceed with the upgrade to 7.5.0 Update Package 2 Interim Fix 02 or 7.5.0 Update Package 3.

  See KB69793 for additional details.

- If your network connection is behind a firewall, the App Host is unable to communicate with your Console.

  There is no workaround currently.

- After you install JSA 7.5.0, your applications might go down temporarily while they are being upgraded to the latest base image.

- Log Analytics is missing from the installation wizard menu.

- The console displays as an event collector in the System and Licensing, License Appliance Type column.

- Factory reset flatten, wipe, and retain menu options are missing, and flatten is performed automatically. Do not select Factory Reset from the Grub menu unless this is the intended action, as there is no workaround or recovery. Ensure configuration and/or data backups are enabled and regularly copied off the appliance.

- Under certain conditions, the installation will fail on JSA7500 and JSA3800 with the following error: "FileNotFoundError: [Errno 2] No such file or directory: '/proc/2108/cmdline' System setup failed." There is no workaround. Please contact https://support.juniper.net/support/.

- When a JSA system is being built and a reboot occurs during the install configuration, the User Interface admin password can sometimes fail to be set correctly.

  Workaround:

  Change the admin account password in the command-line interface.

  > **NOTE**: This procedure requires that you restart the Tomcat service and deploy changes, resulting in a temporary loss of access to the JSA user interface while services restart. Administrators can complete this procedure during a scheduled maintenance window as users are logged out, exports in the process are interrupted, and scheduled reports might need to be restarted manually.

  - If you do not have access to the admin account from the user interface, it can be necessary to change the admin password from the command-line interface.

    1. Using SSH, log in to the JSA Console as the root user.
    2. To change the admin user password, type:

       ```
       /opt/qradar/support/changePasswd.sh -a
       ```

    3. Enter the new password as prompted.
    4. Confirm the new password.

       ```
       [root@qr750-3199-29271 ~]# /opt/qradar/support/changePasswd.sh -a
       Please enter the new admin password.
       Password:
       Confirm password:
       The admin password has been changed.
       ```

    5. To restart the user interface, type:

       ```
       systemctl restart tomcat
       ```

       > **NOTE**: This command works on JSA versions at JSA 7.3.x and later.

    6. Log in to the user interface as an administrator.
    7. Click Admin tab > Advanced > Deploy Full Configuration.

    Important:

Performing a Deploy Full Configuration results in services being restarted. While services are restarting, event processing stops until services restart. Scheduled reports that are in progress need to be manually restarted by users. Administrators with strict outage policies are advised to complete the Deploy Full Configuration step during a scheduled maintenance window for their organization.

Results:

After the service restarts, the admin account password is changed.

Resolved Issues

The resolved issues addressed in the JSA 7.5.0 Update Package 3 are listed below:

- "Unable to create function: 'inoffense' null" response when using AQL function.
- Reference_data_collections api does not close connection to postgres leading to “too many clients” errors.
- Deleting elements from reference maps with the API or Reference Data Management app can fail with an error.
- API searches using local_destination_address can fail on assets with a large number of vulnerabilities.
- Data can be returned slower than expected when querying from the JSA API api/config/extension_management/extensions.
- App install fails during docker build with "an exception occurred while waiting for task to complete" error.
- Applications can stop and report free data issues due to devicemapper driver.
- App container fails because app health check failure threshold incorrectly set to 1.
- After upgrading to JSA 7.5.0 Update Package 2, group-based LDAP authentication with active directory might stop working.
- Restoring a configuration backup fails if the backup archive is also present in the **/storetmp/** directory.
- JSA continues to use the Geo2Lite MaxMind database for geodata information when MaxMind subscription configured.
- Large /store filesystems can cause High Availability 7.5.0 GA installs to improperly set up the partition layout.

- Pretest fails when running **/media/updates/installer -t** because MKS files not pushed.
- "Q1CertificateException: checkCertificatePinning failed" error messages in Log Activity as Sim Generic events.
- Unable to edit or enable/disable log source extensions on JSA 7.5.0 Update Package 2.
- The certificate pinning validation does not take into account property file settings.
- Filtering and searching by log source type filter can fail after changes are made using LSM app.
- Database rebuild on managed host fails due to multiple postgresql versions existing.
- Unable to create bonded interface on JSA 7.5.0.
- Offenses summary page loads slow in JSA 7.5.0 Update Package 1 and higher.
- Offenses are not renamed within the window configured in the rule response limiter.
- Offense Details report in PDF format can cause report_runner to go out of memory.
- QVM exception screen does not load from the history page.
- Estimated time to process results of scan increases if no assets are detected in the scan.
- **ReferenceDataUtil.sh** script fails to update some database tables as expected.
- 'The attachment size is too large' message is written to JSA logging regardless of a mail failure reason.
- Routing rule displays a blank page when the install is a software appliance on JSA 7.5.0 Update Package 1.
- Normalized flow forwarding using routing rules does not forward flow payloads.
- Anomaly issue in JSA 7.5.0 Update Package 2 prevent rules wizard from launching and affects offense creation.
- Next button in rule and report wizard disabled for chrome 102.0.5005.61
- Special characters in rule names can cause 'checking disability' when adding as test to another rule.
- Deleted log source type is still visible in rule wizard.
- Source IP or Destination IP filter is not an available test option for 'Common' Rules.
- Events can stop being written to disk unexpectedly following MaxMind geodata updates.
- Geographic settings can fail to work as expected when an incorrect UserId as been input.

- DSM and protocol RPMs might not be installed due to incompatible version error when updating from JSA 7.3.x to JSA 7.5.0 Update Package 2.
- Postgres v11 update in JSA 7.5.0 Update Package 2 can fail due to a type difference on the local host.
- Replication fails with secure boot status error after an upgrade to JSA 7.5.0 Update Package 1.
- Patch pre-test can fail with '[ERROR] There are X backups in progress. please wait for them to complete...'.
- JSA tabs might be slow due to cache changes in JSA 7.3.3 Fix Pack 12, JSA 7.4.3 Fix Pack 6, and JSA 7.5.0 Update Package 2.
- Unable to load User Management page in non-English locales.
- Scaserver threads reduced to 15 after JSA 7.5.0 Update Package 2 upgrade.
- The software menu displays unsupported functionalities.
- The appliance menu displays unsupported functionalities.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Copyright © 2024 Juniper Networks, Inc. All rights reserved.