Release Notes

Published
2024-02-20

JSA 7.5.0 Update Package 3 ISO

JUNIPER NETWORKS | Engineering Simplicity

Table of Contents

Administrator Notes | 1

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

Installing the JSA 7.5.0 Update Package 3 | 1

Known Issues and Limitations | 1

Resolved Issues | 3

Administrator Notes

About this Installation

These instructions are intended to assist administrators when installing JSA 7.5.0 Update Package 3 by using an ISO file. This ISO can install JSA, JSA Risk Manager, JSA Vulnerability Manager products to version JSA 7.5.0 Update Package 3.

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 3, see What's New Guide.

Installing the JSA 7.5.0 Update Package 3

To install JSA software:

- System Requirements — For information about hardware and software compatibility, see the detailed system requirements in the Juniper Secure Analytics Installation Guide.
- Upgrading to JSA 7.5.0 Update Package 3 — To upgrade to JSA 7.5.0 Update Package 3, see the Upgrading Juniper Secure Analytics to 7.5.0 Guide.
- Installing JSA — For installation instructions, see the Juniper Secure Analytics Installation Guide.

Known Issues and Limitations

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

- 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.

- '9804.install' fails when managed host is removed from deployment before upgrading to JSA 7.5.0.
- If you have WinCollect 7.3.xx installed when you upgrade to JSA 7.5.0, the JSA patch pre-test can fail when the check_yum.sh pre-test does not clean out the old yum cache.
- 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.