Release Notes

Published
2024-02-21

JSA 7.5.0 Update Package 7 ISO

JUNIPER NETWORKS | Engineering Simplicity

Table of Contents

Administrator Notes | 1

What's New in JSA 7.5.0 Update Package 7 | 1

Installing the JSA 7.5.0 Update Package 7 | 1

Installation Wrap-up | 2

Clearing the Cache | 2

Known Issues and Limitations | 3

Resolved Issues | 5

Administrator Notes

About this Installation

These instructions are intended to assist administrators when installing JSA 7.5.0 Update Package 7 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 7.

What's New in JSA 7.5.0 Update Package 7

For more information about what's new in JSA 7.5.0 Update Package 7, see What's New Guide.

Installing the JSA 7.5.0 Update Package 7

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 7 — To upgrade to JSA 7.5.0 Update Package 7, see the Upgrading Juniper Secure Analytics to 7.5.0 Guide.
- Installing JSA — For installation instructions, see the Juniper Secure Analytics Installation Guide.

To install the JSA 7.5.0 Update Package 7 ISO:

1. Download the 7.5.0.UP7.iso from the Juniper Customer Support website.
   https://support.juniper.net/support/downloads/
2. Using SSH, log in to the Console as the root user.
3. To run the ISO installer on the Console, type the following command:
   /media/cdrom/setup

   NOTE: Installing JSA 7.5.0 should take approximately 2 hours on a Console appliance.
4. Wait for the Console primary update to complete.

Installation Wrap-up

1. After all hosts are updated, you must clear you browser cache before logging in to the JSA Console.
2. To unmount the `/media/cdrom` directory on all hosts, type:

   /opt/qradar/support/all_servers.sh -C -k “umount /media/cdrom"
3. Delete the ISO file from all appliances.
4. If you use WinCollect agents version 7.2.6 or latest, you must reinstall the SFS file on the JSA Console. This is due to issues where the ISO replaces the SFS on the Console with WinCollect 7.2.5.
5. Review any static routes or customized routing. As mentioned in the administrator notes, all routes were removed and will need to be reconfigured after the upgrade completes.
6. Review any iptable rules that are configured to see if the interface names that have changed in JSA 7.5.0 due to the Red Hat Enterprise 7 operating system updates affect them. Update any iptables rules that use Red Hat 6 interface naming conventions.

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 7 are listed below:

- After upgrading to JSA 7.5.0 Update Package 5, WinCollect 7.X agents can experience management or configuration change errors.
- It is possible for autoupdates to revert to a previous version of autoupdates after upgrading. This will cause autoupdate to not work as intended.

  After you upgrade to JSA 7.5.0 or later, type the following command to check your autoupdate version:

  /opt/qradar/bin/UpdateConfs.pl -v

- After you install JSA 7.5.0, your applications might go down temporarily while they are being upgraded to the latest base image.
- After upgrading some apps remain in "error" state on deployments with more than 30 apps. Restart the apps by using the qappmanager: **/opt/qradar/support/qappmanager**.
- When adding a Data Node to a cluster, they must either all be encrypted, or all be unencrypted. You cannot add both encrypted and unencrypted Data Nodes to the same cluster.
- 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 7 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 you upgrade 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.

- Reports generate with incorrect chart data and column name with some advanced searches (AQL).
- Log sources deleted from within log source groups can still appear in the JSA user interface.
- "There was a problem saving the log source type configuration" after clicking save on the DSM editor page.
- JSA content pack can cause offenses to be triggered off of source IP instead of custom event property configured in rule.
- Reports can be sent to user addresses in "multiple reports" option when "single report option" is selected.
- Benign error similar to the following is visible in patches.log file can be observed during or after a JSA patch or upgrade.

  Error: `display callback failed: 'ascii' codec can't encode character u'\u2018' in position 0: ordinal not in range`.

- JSA patching can fail due to disk space requirements when adequate space is available.
- Routing rule displays a blank page when the install is a software appliance on JSA 7.5.0 Update Package 1.

- Performance issues can occur when JSA attempts a reload of sensor devices when log sources exceed 2 million.
- Scheduled weekly or monthly reports display "no data for chart" after upgrading to JSA 7.5.0 Update Package 5.
- App install fails during docker build with "an exception occurred while waiting for task to complete" error.
- Sorting by column in the offenses tab removes search filters.
- Tomcat might go out of memory during deployments when the user has millions of log sources.
- System notification displays incorrect message when the tomcat certificate is due to expire.
- Poor scalability in reference data cache resulting in degrading search performance when using filters and tests.
- Users unable to export license information from JSA console gui.
- JSA asset creation events can display a generic identity:0 in the created by field for asset profiler events.
- Upgrade can complete and display an error about a custom properties script trying to insert or update a table.
- Offense search can add unexpected filters to the current search parameters after closing an offense.
- Services can experience out of memory issues due to large certificate revocation lists (CLRS).
- Reports tab can display as blank if the template file for a removed user is missing.
- Rule wizard cannot transition to the next page properly when rule response updates a reference table.
- JSA system anomaly detection engine (ADE) rules can generate extra rules when modified multiple times.
- Anomaly rule enabling "test the [this accumulated property] value of each log source separately" displays application error.
- Offense summary for match count rules does not return all results for the event/flow count field.
- Rule tests with multiple reference set values can display "an error has occurred saving your rule".
- Flow processors in different domains can experience connection issues.
- Upgrading a detached app host appliance fails as the upgrade is waiting on docker and conman services.

- Standby HA appliances can run keystore certificate validator on inactive hosts causing benign log messages.
- Log activity tab can display event ID and category as N/A when the payloads are parsed and mapped correctly.
- Users cannot open the rules wizard from the offenses tab on JSA 7.5.0 Update Package 6.
- Applications might fail to restart after apphost upgraded from JSA 7.5.0 Update Package 5 to JSA 7.5.0 Update Package 6.
- Unknown or stored events can route incorrectly to the sim generic log source in JSA 7.5.0 Update Package 4 and later.
- Reference data import fails with number format exception due to invalid number converter.
- Risks tab might not load after an upgrade to JSA 7.5.0 Update Package 6.
- Events can stop processing when pipeline disk monitor detects the disk spillover threshold is crossed.
- Reports that use the "include date in email subject only" does not behave as expected.
- Ariel processes might not allocate enough memory for memory-heavy operations, causing slower searches.
- Advanced searches (AQL) that use the "in" operator do not use indexes as expected.
- Rule wizard for ADE rules does not preserve the state of the "test separately" check box.
- Scheduled daily reports do not generate on a weekend as expected.
- JSA cannot log in while the LDAP server is unresponsive, which can lead to tomcat errors.
- PCAP data not stored in Ariel or displayed after an upgrade to JSA 7.5.0 Update Package 2 or later.
- JSA applications can get stuck in an error state after an upgrade to JSA 7.5.0 Update Package 6.
- The tzdata DST rules for America/Santiago are out of date and have the incorrect date for switchover to DST.
- Flow processor services can experience service start or restart issues due to libpcap update for older avx2 processors.
- User management window does not display as expected from the Admin tab when the language preference is non-English.

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.