Release Notes

Published
2024-02-20

JSA 7.5.0 Update Package 7 qcow2

Table of Contents

Administrator Notes

This guide covers the aspects of installing, upgrading and operating a vJSA (virtual Juniper Secure Analytics) appliance on top of a Kernel Virtual Machine (KVM) or Open Stack environment. It is assumed the reader is familiar with KVM, and virtualization and Ubuntu Linux, or Open Stack environments.

The examples in this guide are being executed as follows:

- Initial Install and storage expansion of vJSA image on Ubuntu 18.04 deployment of KVM.
- OpenStack deployment leveraging heat templates.

Prerequisites for Installing JSA 7.5.0 Update Package 7 qcow2

IN THIS SECTION

We recommend the following system settings before you upgrade to JSA Release 7.5.0 Update Package 7 qcow2:

- Instantiate the JSA virtual machines on the same non-uniform memory access (NUMA) as the disk controller or RAID controller on the host system. This optimizes disk I/O operations and avoids crossing the QuickPath Interconnect (QPI).
- Set the NUMA policy as strict for kernel-based virtual machine (KVM) so that memory and CPU resources are all allocated from the same NUMA.
- For best I/O performance, metadata preallocation is recommended as a minimum. Full allocation of the disk is required for maximum performance and is recommended for all installations on the KVM.
- Increase the amount of storage allocated to a particular partition on the disk image.

NOTE: Juniper Networks does not provide any support for installing and configuring the KVM server. You must install the virtual appliance image and configure it as per the recommended specifications for the virtual appliance. Juniper Networks will provide support only after the Juniper Secure Analytics has booted successfully.

The prerequisites to deploy a Juniper Secure Analytics on a KVM server are as follows:

- Knowledge about configuring and installing a KVM server.
- KVM server and supported packages must be installed on your Linux-based system. Contact your Linux vendor or documentation for information about installing KVM.
- An application or method to view the remote system virtual monitor, such as Virtual Machine Manager (VMM), Virtual Network Computing (VNC) Viewer, or any other application.
- Bridge Interface configured according to your environment and at least two free static IP addresses.

Minimum Software Requirements for Installing JSA 7.5.0 Update Package 7 qcow2

The minimum software requirements for installing JSA 7.5.0 Update Package 7 qcow2 are as follows:

- 32-GB RAM
- 16 CPU cores
- 512 GB disk space

Prerequisite Hardware Accessories for JSA 7.5.0 Update Package 7 qcow2

IN THIS SECTION

Before you install JSA products, ensure that you have access to the required hardware accessories and desktop software.

Hardware Accessories

Ensure that you have access to the following hardware components:

- Monitor and keyboard, or a serial console
- Uninterrupted Power Supply (UPS) for all systems that store data, such as JSA console, Event Processor components, or JSA flow processor components
- Null modem cable if you want to connect the system to a serial console

> **NOTE**: JSA products support hardware-based Redundant Array of Independent Disks (RAID) implementations, but do not support software-based RAID installations or hardware assisted RAID installations.

Installing JSA on a Virtual Machine

Create a virtual machine. For more information, see No Link Title.

> **NOTE**: The software installation menu will not be visible in the installation wizard by default. If you want to do JSA software installation, refer to JSA Software only Installations.

After you create your virtual machine, you must install the JSA software on the virtual machine.

1. Log in to the virtual machine by typing **root** for the user name.

   The user name is case-sensitive.
2. Accept the **End User License Agreement**.

   > **TIP**: Press the Spacebar key to advance through the document.
3. Select the appliance type:

- **Appliance Install (purchased as an appliance)**
- **High Availability Appliance**
- **App Host Appliance**
- **Log Analytics Appliance**

> **NOTE**: You can select the appliance type based on the intended appliance functionality.

4. If you selected an appliance for high-availability (HA), select whether the appliance is a console.
5. If you selected an appliance for Log Analytics Appliance, select LA (Log Analytics "All-In-One" or Console 8099).
6. For the type of setup, select **Normal Setup (default)** or **HA Recovery Setup**, and select Next.
7. The Date/Time Setup page appears. Enter the current date in the **Current Date (YYYY/MM/DD)** field in the format displayed. A date is also displayed for your reference. Enter the time in 24-hour format in the **24h Clock Time (HH:MM: SS)** field. Alternatively, you can enter the name or the IP address of the time server to which the time can be synced in the **Time Server** field. After entering the date and time details, select Next.
8. The Select Continent/Area page appears. Select the **Time Zone Continent or Area** as required and select Next. The default value is America.
9. The Time Zone Selection page appears. Select the **Time Zone City or Region** as required and select Next. The default value is New York.
10. If you selected **HA Recovery Setup**, enter the cluster virtual IP address.
11. Select the Internet Protocol version:
    - Select **ipv4** or **ipv6**.
12. If you selected **ipv6**, select **manual** or **auto** for the **Configuration type**.
13. Select the bonded interface setup.
14. Select the management interface.

> **NOTE**: If the interface has a link (cable connected), a plus sign (+) is displayed before the description.

15. In the Network Information Setup window, configure the following network settings and select Next.
    - Hostname: Enter a fully qualified domain name as the system hostname
    - IP Address: Enter the IP address of the system
    - Network Mask: Enter the network mask for the system

- Gateway: Enter the default gateway of the system
- Primary DNS: Enter the primary DNS server address
- Secondary DNS: (Optional) Type the secondary DNS server address
- Public IP: (Optional) Enter the Public IP address of the server

> **NOTE**: If you are configuring this host as a primary host for a high availability (HA) cluster, and you selected **Yes** for auto-configure, you must record the automatically-generated IP address. The generated IP address is entered during HA configuration. For more information, see the *Juniper Secure Analytics High Availability Guide*.

16. If you are installing a Console, enter an **admin** password that meets the following criteria:
    - Contains at least 8 characters
    - Contains at least one uppercase character
    - Contains at least one lowercase character
    - Contains at least one digit
    - Contains at least one special character: @, #, ^, or *.
17. Enter **root** password that meets the following criteria:
    - Contains at least 5 characters
    - Contains no spaces
    - Can include the following special characters: @, #, ^, and *.
18. Click **Next**.
19. Apply your license key.
    a. Log in to JSA.

       The default user name is **admin**. The password is the password of the admin user account that you set during installation.

    b. Click **Login To JSA**.

    c. Click the **Admin** tab.

    d. In the navigation pane, click **System Configuration**.

    e. Click the **System and License Management** icon.

    f. From the **Display** list box, select **Licenses**, and upload your license key.

g. Select the unallocated license and click **Allocate System to License**.

h. From the list of systems, select a system, and click **Allocate System to License**.

i. Click **Deploy License Changes**.

Installing JSA 7.5.0 Update Package 7 qcow2 on the KVM server using VMM

Use the VMM virtual machine client to install the JSA 7.5.0 Update Package 7 qcow2 on a KVM server.

To install the JSA 7.5.0 Update Package 7 qcow2 on a KVM server by using VMM:

1. Download the JSA 7.5.0 Update Package 7 qcow2 image from https://support.juniper.net/support/downloads/ to your local system.

   NOTE: Do not change the name of the JSA 7.5.0 Update Package 7 qcow2 image file that you download from the Juniper Networks support site. If you change the name of the image file, the creation of the JSA 7.5.0 Update Package 7 qcow2 can fail.

2. Launch the VMM client.
3. Select **File > New Virtual Machine** on the menu bar of VMM to install a new virtual machine on a KVM server.

   The New VM dialog box appears and displays. Refer to step 1 of the New VM installation.
4. Under Choose how you would like to install the operating system, click **Import existing disk image**.
5. Click **Forward** to go to the next step.

   Step 2 is displayed.
6. Under Provide the existing storage path, click **Browse**.
7. Under Choose storage volume , click **Browse Local** at the bottom of the dialog box to locate and select the JSA 7.5.0 Update Package 7 qcow2 image file (**.qcow2**) saved on your system.
8. Under Choose an operating system type and version, select Linux for **OS type** and Red Hat Enterprise Linux *version number* for **Version**.

   NOTE: We recommend to use the same Linux version as JSA 7.5.0 Update Package 7 qcow2 is using.

9. Click **Forward** to go to the next step.

Step 3 is displayed.

10. Under Choose Memory and CPU settings, ensure that 4 is set for **CPUs** and select or enter the following value for **Memory (RAM)**:
    - 32768 MB–For the JSA 7.5.0 Update Package 7 qcow2 to be deployed as a Junos Space node or as an FMPM node
11. Click **Forward** to go to the next step.

    Step 4 is displayed.
12. Under Network selection, select the options based on how you want to configure network communication on the JSA 7.5.0 Update Package 7 qcow2 setup.
13. Under Ready to begin the installation, in the Name field, enter a name for the JSA 7.5.0 Update Package 7 qcow2.

Clearing the Cache

After you complete the installation, you must clear your Java cache and your web browser cache before you log in to 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

- If the **Checking that tomcat is running and ready (attempt 0/30)** phase goes past **(attempt 10/30)**, you should use another SSH session to log in to the system's IP address during installation, and remove the `imqbroker` lock file. Restart the `imqbroker` service as follows:

```
systemctl restart imqbroker
```

> **NOTE**: If the installation times out, reboot the system and perform the setup for a second time.

- 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

None.