Release Notes

Published
2022-05-02

JSA 7.5.0 Update Package 1 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, 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.

We recommend the following system settings before you upgrade to JSA Release 7.5.0 Update Package 1:

- 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.

  See "Prerequisites for Installing JSA 7.5.0 Update Package 1 qcow2" on page 2 for more information.

You should be aware of the following:

- The size of the qcow2 image is 17 GB when compressed, and 512 GB when it is uncompressed.
- Ubuntu 18.04 LTS with KVM and Open vSwitch (OVS) are used to validate the image for the KVM.
- Contrail 3.2.12 is validated to run with the image or Kilo or Ocata OpenStack versions.

Prerequisites for Installing JSA 7.5.0 Update Package 1 qcow2

Before you begin, see section "Administrator Notes" on page 1 to understand the system requirements for installing JSA 7.5.0 Update Package 1 using an qcow2 image.

We recommend that you increase the amount of storage allocated to a particular partition on the disk image.

Perform the following steps to expand the disk image or store partition:

NOTE: Shut down the VM before you perform this operation to avoid corrupting the disk that contains the qcow2 image.

1. Expand the qcow2 disk image by using the following command.

```
sudo qemu-img resize --preallocation=falloc vjsa-tacon.qcow2 +512G
Image resized
```

2. Check if there is sufficient disk space for the uncompressed image by using the following command.

```
sudo qemu-img check -r all /vm/vjsa-tacon.qcow2
No errors were found on the image
8388608/8388608 = 100.00% allocated, 0.00% fragmented, 0.00% compressed clusters
Image end offset: 549856870400
```

3. Boot the disk image by using the following command.

```
virsh start vjsa-tacon
```

4. Log in as the root user to JSA by using the JSA console or SSH.

```
virsh console vjsa-tacon
```

5. Run the `parted` command on the disk **/dev/vda** to increase the size of the disk partition. Ensure that you type **fix** when prompted.

```
parted /dev/vda
Using /dev/vda
Welcome to GNU Parted! Type 'help' to view a list of commands
(parted) print
Error: The backup GPT table is not at the end of the disk, as it should be
This might mean that another operating system believes the disk is smaller
Fix, by moving the backup to the end (and removing the old backup)?
Fix/Ignore/Cancel? Fix
Warning: Not all of the space available to /dev/vda appears to be used, you can
fix the GPT to use all of the space (an extra 1073741824 blocks) or continue with the
current setting?
```

6. Reboot the device so that the new partition is reflected in the partition table by using the following command.

```
reboot
```

7. Run the `parted` command to display the free space and note the beginning and ending blocks.

```
(parted) unit s print free
Model: Virtio Block Device (virtblk)
Disk /dev/vda: 2147483648s
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags: pmbr_boot
```

8. Reboot the device to ensure that the new partition fixes are reflected in the partition table.
9. Create a new partition at the end of the existing partition by using the following commands.

```
(parted) mkpart
Partition name? []?
File system type? [ext2]?
Start? 1073737728
End? 2147483614
(parted) unit s print free
Model: Virtio Block Device (virtblk)
Disk /dev/vda: 2147483648s
```

```
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags: pmbr_boot
```

10. Set the partition as a Logical Volume Manager (LVM) partition by using the following commands.

```
(parted) set 7 lvm on
(parted) unit s print free
Model: Virtio Block Device (virtblk)
Disk /dev/vda: 2147483648s
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags: pmbr_boot
```

Table 1 on page 4 shows the updated partition table after creating an LVM partition.

Table 1: Partition Table Information

Number	Start	End	Size	File System	Name Flags
	34s	2047s	2014s	Free Space	
1	2048s	4095s	2048s		bios_grub
2	4096s	2101247s	2097152s	xfs	
3	2101248s	69210111s	67108864s	xfs	
4	69210112s	882888703s	813678592s		lvm

11. Quit the `parted` command and add the new LVM partition as a physical volume to LVM by using the following command.

```
sudo pvs
```

Table 2 on page 5 shows the LVM partition added as a physical volume.

Table 2: Adding LVM Partition as a Physical Volume

PV	VG	Fmt	Attr	PSize	PFree
/dev/vda4	storerhel	lvm2	a--	<387.99g	0
/dev/vda5	rootrhel	lvm2	a--	67.00g	0

```
pvcreate /dev/vda7
File descriptor 63 (pipe:[3410678]) leaked on pvcreate invocation. Parent PID 8346: -bash
Physical volume "/dev/vda7" successfully created.
```

12. Extend the physical volume group by using the following command.

```
[root@vjsa-tacon ~]# vgextend storerhel /dev/vda7
File descriptor 63 (pipe:[3831444]) leaked on vgextend invocation. Parent PID 8346: -bash
Volume group "storerhel" successfully extended
[root@vjsa-tacon ~]# vgs
File descriptor 63 (pipe:[4057371]) leaked on vgs invocation. Parent PID 8346: -bash
```

The physical volume group is now extended.

13. Use the following command to extend the logical volume of the disk.

```
df -h
```

Table 3: File System Information

File system	Size	Used	Available	Use %	Mounted on
/dev/mapper/ rootrhel-root	13 Gb	3.0 Gb	9.5 Gb	24%	**/**
devtmpfs	32 Gb	0	32 Gb	0%	**/dev**
tmpfs	32 Gb	20 Kb	32 Gb	1%	**/dev/shm**

Table 3: File System Information *(Continued)*

File system	Size	Used	Available	Use %	Mounted on
tmpfs	32 Gb	34 Mb	32 Gb	1%	**/run**
tmpfs	32 Gb	0	32 Gb	0%	**/sys/fs/cgroup**
/dev/mapper/ rootrhel-tmp	3.0 Gb	135 Mb	2.9 Gb	5%	**/tmp**
/dev/vda3	32 Gb	4.8 Gb	28 Gb	15%	**/recovery**
/dev/mapper/ storerhel-store	311 Gb	21 Gb	290 Gb	7%	**/store**
/dev/mapper/ rootrhel-opt	13 Gb	4.3 Gb	8.3 Gb	34%	**/opt**
/dev/mapper/ rootrhel-home	1014 Mb	33 Mb	982 Mb	4%	**/home**
tm/dev/ mapper/ rootrhel- storetmp	15 Gb	44 Mb	15 Gb	1%	**/storetmp**
/dev/mapper/ storerhel- transient	78 Gb	34 Mb	78 Gb	1%	**/transient**

The logical volume is now extended.

14. Extend the file system by using the following command.

```
xfs_growfs /store
```

The file system is now extended.

You have now extended the physical volume group, logical volume of the disk, and the file system as required. You can now install JSA 7.5.0 Update Package 1 using a qcow2 image. See "Installing JSA 7.5.0 Update Package 1 qcow2 on the KVM" on page 7 for information on installing JSA 7.5.0 Update Package 1 using a qcow2 image.

Installing JSA 7.5.0 Update Package 1 qcow2 on the KVM

The size of the qcow2 image is 17 GB when compressed and it is 512 GB when it is uncompressed. We recommend that you increase the amount of storage allocated to a particular partition on the disk image to accommodate the qcow2 image. See "Prerequisites for Installing JSA 7.5.0 Update Package 1 qcow2" on page 2 for more information.

To install JSA 7.5.0 Update Package 1 qcow2 on the KVM:

1. Copy the JSA 7.5.0 Update Package 1 qcow2 image to a safe location on the virtualization host.
2. Clone the image using the following command.

```
qemu-img convert -p -f qcow2 -O qcow2 /iso/JSA7.5.0.UP1.qcow2 /vm/vjsa-tacon.qcow2 -o
preallocation=metadata
```

3. (Recommended) Provide the full disk allocation by using the following command.

```
qemu-img convert -p -f qcow2 -O qcow2 /iso/JSA7.5.0.UP1.qcow2 /vm/vjsa-tacon.qcow2 -o
preallocation=falloc
```

4. Install the virtual KVM device using the `virt-install` command. This command prints the XML necessary to define the VM in the KVM.

```
virt-install --hvm --name JSA7.5.0.UP1-tacon --cpu host --cpuset 2-10,42-50 --vcpus
sockets=18,cores=1,threads=1 --memory 65536 --memorybacking hugepages=yes --disk path=/vm/
vjsatacon. qcow2,format=qcow2 --os-type linux --os-variant rhel7.4 --memballoon virtio --
network network:default,model=virtio --graphics vnc --console pty,target_type=virtio &ndash;-
import &ndash;-print-xml > vjsa-tacon.xml
```

5. Print the command output to a file, and then edit the file to complete the static CPU pinning by adding the following information to the XML file.

```
<cputune>
<vcpupin vcpu='0' cpuset='11'/>
<vcpupin vcpu='1' cpuset='51'/>
<vcpupin vcpu='2' cpuset='12'/>
<vcpupin vcpu='3' cpuset='52'/>
<vcpupin vcpu='4' cpuset='13'/>
<vcpupin vcpu='5' cpuset='53'/>
<vcpupin vcpu='6' cpuset='14'/>
<vcpupin vcpu='7' cpuset='54'/>
<vcpupin vcpu='8' cpuset='15'/>
<vcpupin vcpu='9' cpuset='55'/>
<vcpupin vcpu='10' cpuset='16'/>
<vcpupin vcpu='11' cpuset='56'/>
<vcpupin vcpu='12' cpuset='17'/>
<vcpupin vcpu='13' cpuset='57'/>
<vcpupin vcpu='14' cpuset='18'/>
<vcpupin vcpu='15' cpuset='58'/>
<vcpupin vcpu='16' cpuset='19'/>
<vcpupin vcpu='17' cpuset='59'/>
<cputune>
```

6. Define the VM using the following command.

```
virsh define vjsa-tacon.xml
```

The following is an example of the command output:

```
tjencks@svc-virtual1:/vm$ virsh dumpxml JSA7.5.0.UP1-tacon
<domain type='kvm'>
<name>vjsa-tacon>/name>
<uuid>957426e8-e225-4874-ac8f-6a2b7a3236a1</uuid>
<memory unit='KiB'>67108864</memory>
<currentMemory unit='KiB'>67108864</currentMemory>
<memoryBacking>
<hugepages/>
</memoryBacking>
<vcpu placement='static' cpuset='11-19,51-59'>18</vcpu>
<cputune>
```

```
<vcpupin vcpu='0' cpuset='11'/>
<vcpupin vcpu='1' cpuset='51'/>
<vcpupin vcpu='2' cpuset='12'/>
<vcpupin vcpu='3' cpuset='52'/>
<vcpupin vcpu='4' cpuset='13'/>
<vcpupin vcpu='5' cpuset='53'/>
<vcpupin vcpu='6' cpuset='14'/>
<vcpupin vcpu='7' cpuset='54'/>
<vcpupin vcpu='8' cpuset='15'/>
<vcpupin vcpu='9' cpuset='55'/>
<vcpupin vcpu='10' cpuset='16'/>
<vcpupin vcpu='11' cpuset='56'/>
<vcpupin vcpu='12' cpuset='17'/>
<vcpupin vcpu='13' cpuset='57'/>
<vcpupin vcpu='14' cpuset='18'/>
<vcpupin vcpu='15' cpuset='58'/>
<vcpupin vcpu='16' cpuset='19'/>
<vcpupin vcpu='17' cpuset='59'/>
<cputune>
```

7. Start the VM and start the console into the VM by using the following commands.

```
virsh start vjsa-tacon
virsh console vjsa-tacon
```

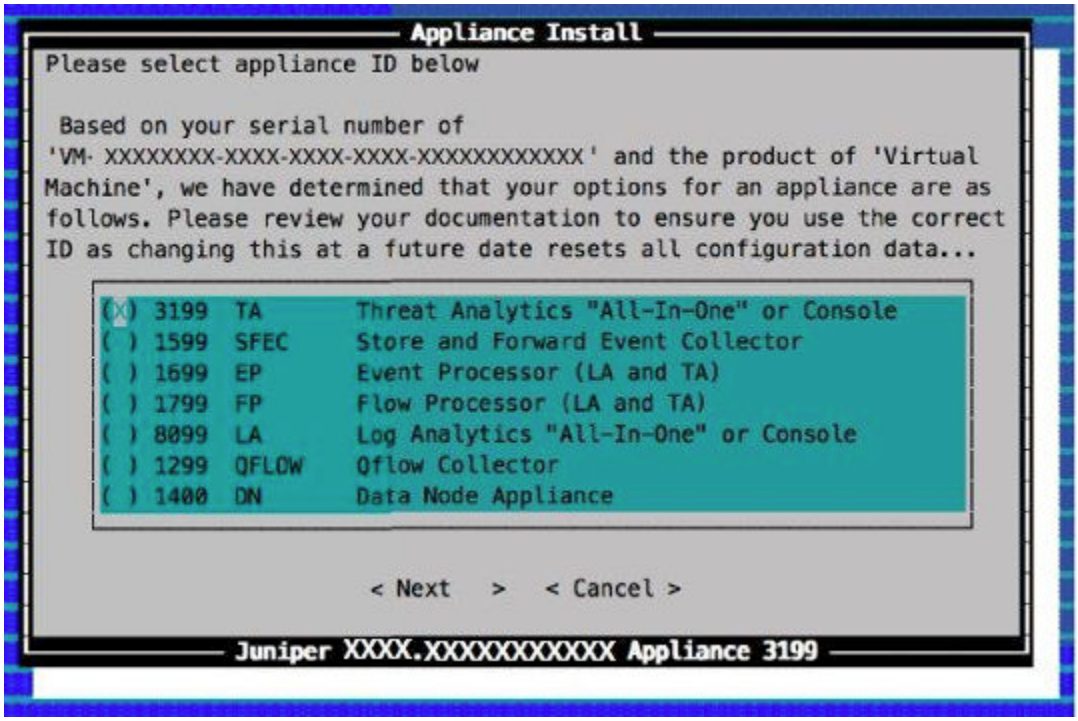
8. Log in as the root user.

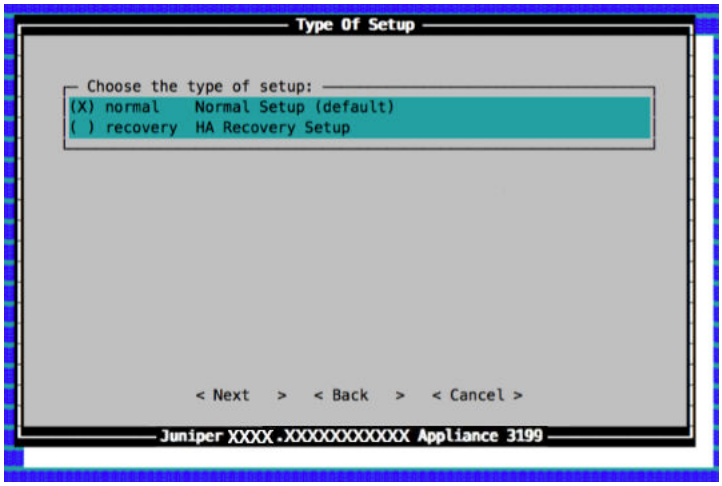
NOTE: A password is not required.

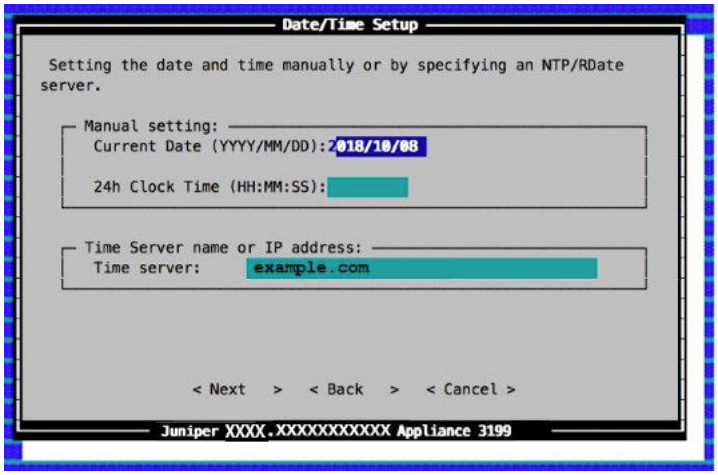
9. Follow the step in the installation wizard for the virtual appliance type you are creating, in this case a **Threat Analytics "All In One" or Console**.

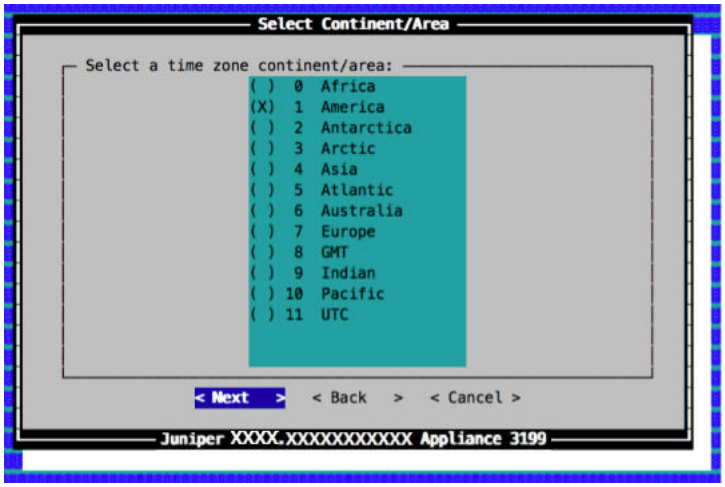
   a. Log in as the root user at the prompt (a password is not required). If you are prompted for a p assword, there is some error with the installation. Please contact Juniper Customer Support.

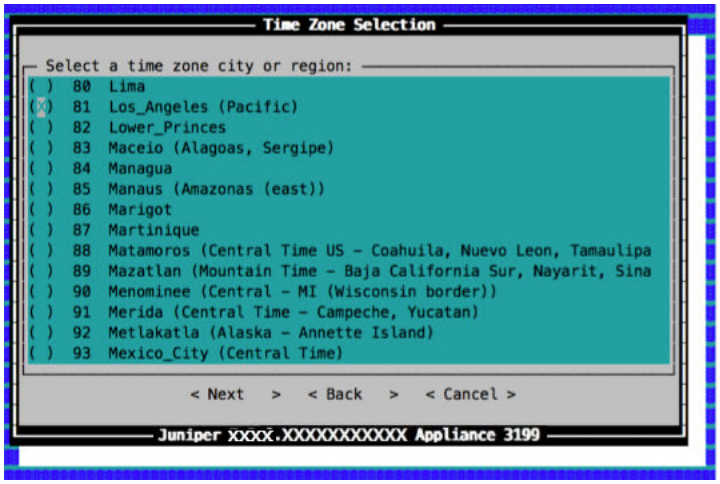
   b. Accept the EULA license and proceed with the installation. Provide information in the installation wizard when prompted.

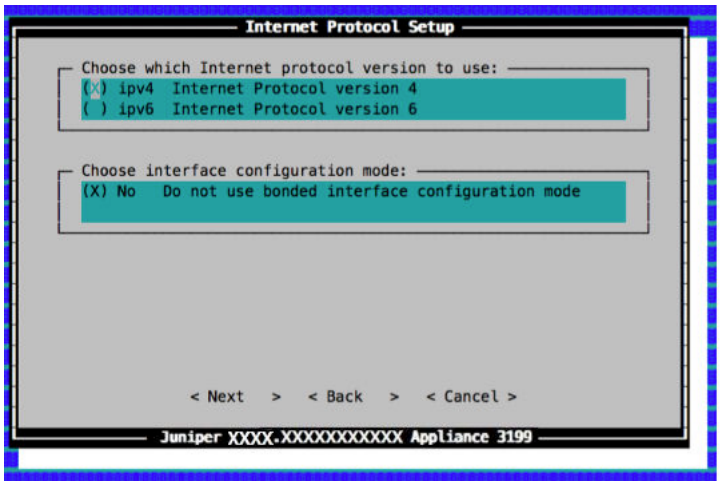

Appliance Install
Please select appliance ID below
Based on your serial number of
'VM- XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX' and the product of 'Virtual Machine', we have determined that your options for an appliance are as follows. Please review your documentation to ensure you use the correct ID as changing this at a future date resets all configuration data...
(X) 3199 TA Threat Analytics "All-In-One" or Console
( ) 1599 SFEC Store and Forward Event Collector
( ) 1699 EP Event Processor (LA and TA)
( ) 1799 FP Flow Processor (LA and TA)
( ) 8099 LA Log Analytics "All-In-One" or Console
( ) 1299 QFLOW Qflow Collector
( ) 1400 DN Data Node Appliance
< Next > < Cancel >
Juniper XXXX.XXXXXXXXXX Appliance 3199

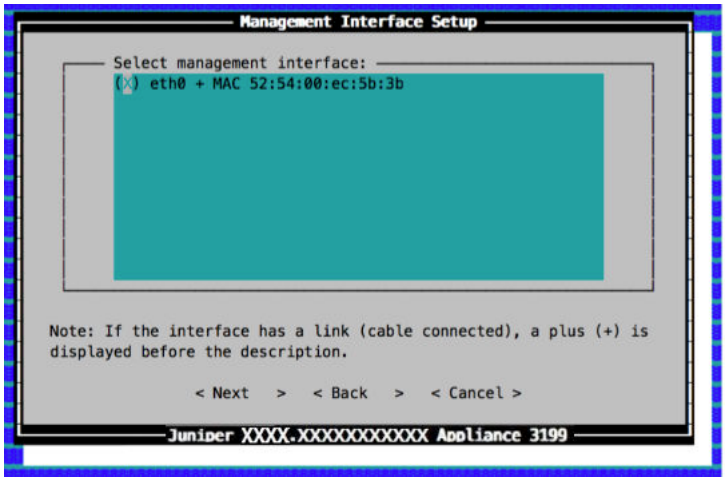

Type Of Setup
Choose the type of setup:
(X) normal Normal Setup (default)
( ) recovery HA Recovery Setup
< Next > < Back > < Cancel >
Juniper XXXX.XXXXXXXXXX Appliance 3199

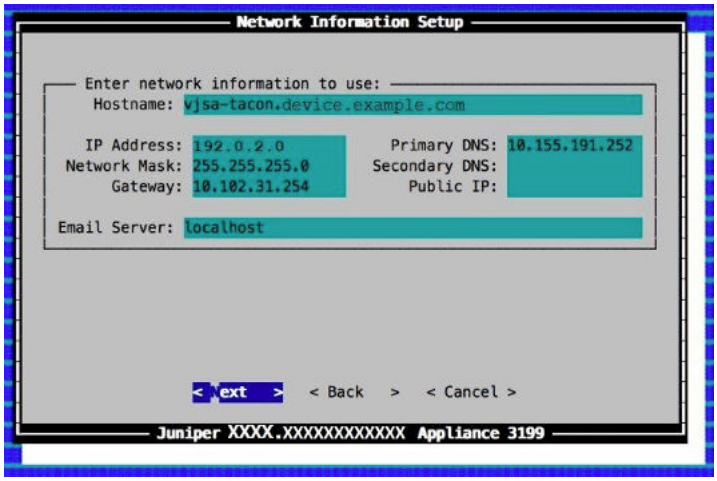

Date/Time Setup
Setting the date and time manually or by specifying an NTP/RDate server.
Manual setting:
Current Date (YYYY/MM/DD): 2018/10/08
24h Clock Time (HH:MM:SS):
Time Server name or IP address:
Time server: example.com
< Next > < Back > < Cancel >
Juniper XXXX.XXXXXXXXXX Appliance 3199

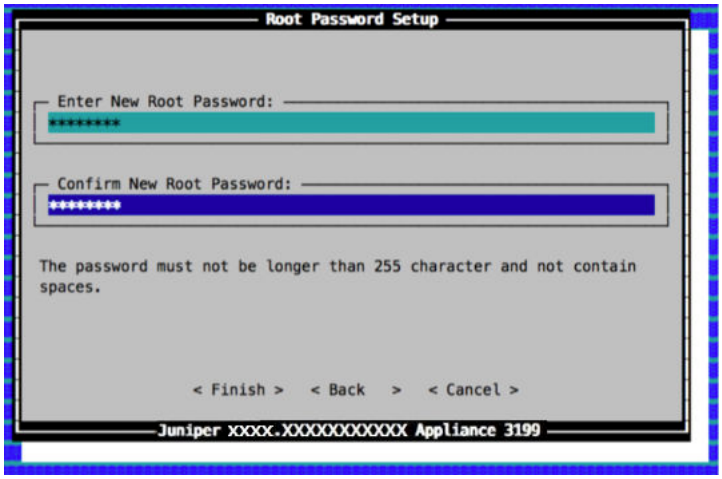

Select Continent/Area
Select a time zone continent/area:
( ) 0 Africa
(X) 1 America
( ) 2 Antarctica
( ) 3 Arctic
( ) 4 Asia
( ) 5 Atlantic
( ) 6 Australia
( ) 7 Europe
( ) 8 GMT
( ) 9 Indian
( ) 10 Pacific
( ) 11 UTC
< Next > < Back > < Cancel >
Juniper XXXX.XXXXXXXXXX Appliance 3199


Time Zone Selection
Select a time zone city or region:
( ) 80 Lima
(X) 81 Los_Angeles (Pacific)
( ) 82 Lower_Princes
( ) 83 Maceio (Alagoas, Sergipe)
( ) 84 Managua
( ) 85 Manaus (Amazonas (east))
( ) 86 Marigot
( ) 87 Martinique
( ) 88 Matamoros (Central Time US - Coahuila, Nuevo Leon, Tamaulipa
( ) 89 Mazatlan (Mountain Time - Baja California Sur, Nayarit, Sina
( ) 90 Menominee (Central - MI (Wisconsin border))
( ) 91 Merida (Central Time - Campeche, Yucatan)
( ) 92 Metlakatla (Alaska - Annette Island)
( ) 93 Mexico_City (Central Time)
< Next > < Back > < Cancel >
Juniper XXXX.XXXXXXXXXX Appliance 3199


Internet Protocol Setup
Choose which Internet protocol version to use:
(X) ipv4 Internet Protocol version 4
( ) ipv6 Internet Protocol version 6
Choose interface configuration mode:
(X) No Do not use bonded interface configuration mode
< Next > < Back > < Cancel >
Juniper XXXX.XXXXXXXXXX Appliance 3199


Management Interface Setup
Select management interface:
(X) eth0 + MAC 52:54:00:ec:5b:3b
Note: If the interface has a link (cable connected), a plus (+) is displayed before the description.
< Next > < Back > < Cancel >
Juniper XXXX.XXXXXXXXXX Appliance 3199


Network Information Setup
Enter network information to use:
Hostname: vjsa-tacon.device.example.com
IP Address: 192.0.2.0
Network Mask: 255.255.255.0
Gateway: 10.102.31.254
Primary DNS: 10.155.191.252
Secondary DNS:
Public IP:
Email Server: localhost
< Next > < Back > < Cancel >
Juniper XXXX.XXXXXXXXXX Appliance 3199



c. When you select **Finish**, the installation is started. This process can take up to 6 hours depending on the speed of your system. Although it might appear as if the system is not responding at times, wait for the installation to complete.

   The following output indicates a successful installation of a console:

```
Installing JSA changes...
psql: could not connect to server: No such file or directory
Is the server running locally and accepting
connections on Unix domain socket "/var/run/postgresql/.s.PGSQL.5432"?
Activating system with key 003V41-5T7A3E-077N7N-54512G.
Appliance ID is 3199.
Installing 'TA Threat Analytics "All-In-One" or console' with id 3199.
Configuring network...
Setting time server to ntp.juniper.net.
Synching time with server 'ntp.juniper.net'
8 Oct 16:42:41 ntpdate[10395]: adjust time server 66.129.233.81 offset -0.000348 sec
Restarting postgresql-qrd
```

```
Running changeQradarPassword
Stopping hostcontext
Stopping httpd
Stopping tomcat
1: waiting for port 7676 to start
2: waiting for port 7676 to start
3: waiting for port 7676 to start
Mon Oct 8 16:43:39 PDT 2018 [setup-imq.sh] OK: IMQ Setup Completed
Stopping httpd
Stopping tomcat
Updating db user password
OK: Post Import Actions For Vulnerability Tables Are Successfully Completed.OK: Reseting
Of Sequences Of Asset Related q_catalog Tables Is
Successfully CompleteInstalling DSM rpms: done.
Decompressing QidMap file /opt/qradar/conf/templates/1522167900442.qidmap-import.xml.xz...
Importing /opt/qradar/conf/templates/1522167900442.qidmap-import.xml
Finished updating QIDMap, took 1073 seconds to complete.
```

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.

- The administrator password is not set appropriately by the setup scripts. After installing the console, change the administrator password through the CLI by using the following steps:

1. Connect to your console using SSH as the root user.
2. Set the password by running the following command:

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

3. Enter the new password when prompted.
4. Reenter the new password when prompted.

5. Restart the UI service with the following command:

```
service tomcat restart
```

6. Log in to the UI with the administrator account and the new password.
7. **Perform deploy** changes.

The administrator account password is now changed.

Resolved Issues

None.