



Juniper Secure Analytics

Partition Splitting

Release 7.5.0

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Published: 2022-5-2

Copyright Notice

Copyright © 2022 Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc.

The following terms are trademarks or registered trademarks of other companies:

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.



All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense. The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: Reorient or relocate the receiving antenna. Increase the separation between the equipment and receiver. Consult the dealer or an experienced radio/TV technician for help. Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT, SUBJECT TO THE MODIFICATIONS SET FORTH BELOW ON THIS PAGE, ARE SET FORTH IN THE INFORMATION PACKET SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

Partition Splitting
Release 7.5.0

Copyright © 2022, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

May 2022—Partition Splitting

The information in this document is current as of the date listed in the revision history.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>, as modified by the following text, which shall be treated under the EULA as an Entitlement Document taking precedence over any conflicting provisions of such EULA as regards such software:

As regards software accompanying the STRM products (the "Program"), such software contains software licensed by Q1 Labs and is further accompanied by third-party software that is described in the applicable documentation or materials provided by Juniper Networks.

For the convenience of Licensee, the Program may be accompanied by a third party operating system. The operating system is not part of the Program, and is licensed directly by the operating system provider (e.g., Red Hat Inc., Novell Inc., etc.) to Licensee. Neither Juniper Networks nor Q1 Labs is a party to the license between Licensee and the third party operating system provider, and the Program includes the third party operating system "AS IS", without representation or warranty, express or implied, including any implied warranty of merchantability, fitness for a particular purpose or non-infringement. For an installed Red Hat operating system, see the license file: /usr/share/doc/redhat-release-server-6Server/EULA.

By downloading, installing or using such software, you agree to the terms and conditions of that EULA as so modified.

CONTENTS

1 PARTITION SPLITTING

Before You Begin	7
Partition Splitting Script	8
Partitioning the High Availability Cluster Hosts	8
Disconnecting the High Availability Cluster.	9
Partitioning the Primary High Availability Host	9
Partitioning the Secondary High Availability Host.	10

1

PARTITION SPLITTING

This document provides information on how to use a Juniper Secure Analytics (JSA) script to create a partition and move the `/store/ariel/persistent_data` location and contents into the new partition for systems running High Availability.

This technical note only applies to high availability systems.

The partition splitting process affects both the primary and secondary high availability hosts. Before running the script, you must remove the high availability secondary from the high availability cluster configuration. This script takes several hours to complete. During this time, the secondary host is offline, however, the primary host continues to collect data and is still available to access using the user interface. The script performs the required actions and preserves the data integrity of the contents of the `/store` location. After the script is complete, you can reconfigure your high availability cluster.

Unless otherwise noted, all references to JSA refer to JSA and Log Manager. References to flows do not apply to Log Manager.

Before You Begin

Before you begin, you must have the following:

- Advanced knowledge of the Linux operating system.
- Administrative privileges for the JSA software.
- Administrative privileges for the systems running JSA and high availability.

Be aware that there are potential risks involved with running the partition script.

- Determine the disc capacity of the system. You must give the new partition an appropriate size. Typically, the new partition should be approximately 25% the size of the `/store` location. The script does not have safeguards in place to prevent the introduction of values that are incorrect or too large.
- Investigate and find the root cause of your performance issues before you run the script. Partitioning and migrating the `/store` location can resolve throttling issues where high availability data replication is the reason for the slowdown.

- There is a low risk of data loss. Make sure that the host has sufficient space for a new partition. For example, if you have 100 GB of free space, you should not allocate a 400 GB partition.

For technical assistance, contact Juniper Customer Support.

Partition Splitting Script

If you have experienced performance issues caused by high availability data replication that partition splitting can resolve, you can use the partition splitting script to modify the boundaries of the `/store/` partition and move the associated temporary results to the newly created partition.

This document provides information on preparing, configuring, and running the partition splitting script available with your JSA installation.

To prepare and run the partitioning script, you need to log on to JSA as an administrator, and then SSH to both the primary and secondary high availability host.

The script is stored in the bin directory of JSA: `/opt/qradar/bin`. The script takes two commands:

- **size** - Sets the disc space required for the new partition.
- **continue** - Resumes the processing after a reboot.

The partitioning script contains the complete set of instructions required; running the script may take several hours. You may be prompted to restart the host, if so, you can resume the script with the **continue** command.

Partitioning the High Availability Cluster Hosts

Running the partition splitting script, requires disconnecting the high availability cluster.

After disconnecting the high availability cluster, run the partitioning script on each of the two high availability systems. The script can take several hours to complete, however, you can run the partition splitting script on both hosts at the same time. After the script is complete on both hosts, you must reconnect the high availability cluster.

To partition the high availability cluster hosts, perform the following procedures:

- 1 Disconnect the high availability Cluster.
For more information see, **Disconnecting the High Availability Cluster**
- 2 Run the partition splitting script on the primary and secondary high availability hosts:
 - **Partitioning the Primary High Availability Host**

- **Partitioning the Secondary High Availability Host**

- 3 Reconnect the high availability cluster. For information on reconnecting the high availability cluster, see the *Adding an high availability Cluster* section in your *Juniper Secure Analytics Administration Guide*.

Disconnecting the High Availability Cluster

You can disconnect the high availability cluster.

Procedure:

- Step 1** Click the Admin tab.
- Step 2** On the navigation menu, click **System Configuration**.
- Step 3** On the System Configuration panel, click the **System and License Management** icon.
- Step 4** In the System and License Management window, select the high availability host you want to remove.
- Step 5** From the **High Availability** menu, select **Remove high availability Host**.
- Step 6** Click **OK**.

Result:

When you remove an high availability host, the host restarts.

Partitioning the Primary High Availability Host

You can partition the primary high availability host

Procedure:

- Step 1** Using SSH, log into the primary high availability host as the `root` user:
Username: `root`
Password: `<password>`
- Step 2** Change to the `/opt/qradar/bin` directory.
- Step 3** Type `./create_cursor_partition.sh size=<size>.`
`<size>` should be approximately one quarter the `/store` capacity. `<size>` is written as a numeric value and the measurement specification. The partition size on the primary and secondary high availability host must be the same. Type the measurement using one of the following:

- `m` for Megabyte
- `G` for Gigabyte
- `T` for Terabyte

If the script prompts you to restart the host, do the following steps:

- a Restart the primary host and log in as the `root` user.
- b Change to the `/opt/qradar/bin` directory.

- c Type the following command to restart the script:
`./create_cursor_partition.sh --continue.`

Step 4 To check the partition when the script has finished, type `df -h`.

Partitioning the Secondary High Availability Host

You can partition the secondary high availability host.

Procedure:

Step 1 Using SSH, log into the secondary high availability host as the `root` user:

Username: `root`

Password: `<password>`

Step 2 Change to the `/opt/qradar/bin` directory.

Step 3 Type `./create_cursor_partition.sh size=<size>.`

`<size>` should be approximately one quarter the `/store` capacity. `<size>` is written as a numeric value and the measurement specification. The partition size on the primary and secondary high availability host must be the same. Type the measurement using one of the following:

- `M` for Megabyte
- `G` for Gigabyte
- `T` for Terabyte

If the script prompts you to restart the host, perform the following steps:

- a Restart the secondary host and log in as the `root` user.
- b Change to the `/opt/qradar/bin` directory.
- c Type the following command to restart the script:
`./create_cursor_partition.sh --continue.`

Step 4 To check the partition when the script has finished, type `df -h`.

5 Reconnect the high availability cluster.

For more information on reconnecting an high availability cluster, see the *Juniper Secure Analytics High Availability Guide*.