

JUNIPER NETWORKS STRM TECHNICAL NOTE

RESTORING YOUR DATA

JUNE 2008

If you are using STRM 2008.1 and above, you can schedule the backup of your configuration information and data using the STRM Administration Console. The data portion of the backup includes all offenses (including targets and attacker information), asset data, event category information, vulnerability data, event data, and flow data located on STRM.

You can restore your configuration information using the STRM interface, however, you must use the procedures in this document to restore your flow, event, or reporting data. This document includes:

- [Before You Begin](#)
- [Restoring Your Data](#)
- [Troubleshooting Tips](#)



Caution: *If the current configuration of your STRM system differs from the configuration that existed at the time the data was backed up, your system may experience some gaps in information once the data is restored. For example, if the recovered data includes device information from a device that no longer exists, the interface will not display information regarding this removed device.*

Before You Begin

Each managed host in your deployment, including the STRM Console, Flow Processors, and Event Processors create backup files in the `/store/backup/` directory.



Note: *Your system may also include a mount `/store/backup` from an external SAN or NAS service, which allows for long term off-line retention of data, as often required for compliancy regulations, such as, HIPPA and PKI.*

Before you restore the data, consider the following:

- Locate the managed host on which the data is backed up (Console, Flow Processor, or Event Processor).
- Backup files are saved using the following format:

```
backup.<name>.<hostname>_<host ID>.<target date>.<backup type>.<timestamp>.tgz
```

Where:

<name> is the name associated with the backup.

<hostname> is the name of the STRM system hosting the backup file.

<host ID> is the identifier for the STRM system.

<target date> is the date that the backup file was created.

<backup type> is the type of backup. The options are data or config.

<timestamp> is the time that the backup file was created.

- Make sure your /store partition includes adequate space for the data you wish to recover.
- The date and time for the data you wish to recover.

Restoring Your Data

To restore your data:

Step 1 Log in to your STRM Console, as root.

Step 2 Connect to the system on which you wish to store the data. This may be a system host your Console, Event Processor, or Flow Processor.

Step 3 Change the directory:

```
cd /store/backup
```

Step 4 Identify the data files you need to restore by reviewing the date stamps on the listed files:

```
ls -l
```

A list of backup files appear. For example:

```
root@csd6 /store/backup# ls
```

```
backup.scheduled.csd6_2.06_03_2008.config.1204862632982.tgz
```

```
backup.scheduled.csd6_2.07_03_2008.config.1204949036670.tgz
```

```
backup.scheduled.csd6_2.07_03_2008.db.1204948866713.tgz
```

```
backup.scheduled.csd6_2.08_03_2008.config.1205035447658.tgz
```

```
backup.scheduled.csd6_2.20_04_2008.config.1208747057662.tgz
```

```
backup.scheduled.csd6_2.20_04_2008.data.1208747105710.tgz
```

```
backup.scheduled.csd6_2.21_04_2008.config.1208833492837.tgz
```

```
backup.scheduled.csd6_2.21_04_2008.data.1208833780364.tgz
```

```
backup.scheduled.csd6_2.21_04_2008.db.1208833282522.tgz
```

```
backup.scheduled.csd6_2.22_04_2008.config.1208919886899.tgz
```

```
backup.scheduled.csd6_2.22_04_2008.data.1208920422678.tgz
```

```
backup.scheduled.csd6_2.22_04_2008.db.1208919678682.tgz
```

```
backup.scheduled.csd6_2.23_04_2008.config.1209006291557.tgz
```

```
backup.scheduled.csd6_2.23_04_2008.data.1209006842493.tgz
```

```

backup.scheduled.csd6_2.23_04_2008.db.1209006090148.tgz
backup.test.csd6_2.10_03_2008.config.1205160090172.tgz
desc/

```

Step 5 Extract the files you wish to restore.



Note: Make sure the extraction command includes the *P* option, which ensures the files are extracted to their original directory.

```

tar -zxPf /store/backup/backup.<name>.<hostname>._<host
ID>.<target date>.<backup type>.<timestamp>.tgz

```

For example:

```

tar -zxPf
  backup.scheduled.csd9_2.31_03_2008.data.1207033304942.tgz

```

Daily backups capture all data from the previous day, on the host executing the backup. The above example reflects a single, All-in-One Console and includes reports, PDF files, event, and flow data. If you wish to restore data on an Event Processor or Flow Processor that only contains event or flow data, only that data is restored to that host.

If you **only** wish to restore specific event, flow, or reporting data, you must also include an extraction path filter to limit the restored files using the following commands:

```

Event Data: tar -zxPf backup.<name>.<hostname>._<host ID>.<target
date>.<backup type>.<timestamp>.tgz /store/ariel/events

```

```

Flow Data: tar -zxPf backup.<name>.<hostname>._<host ID>.<target
date>.<backup type>.<timestamp>.tgz /store/ariel/flows

```

```

Reporting Data: tar -zxPf backup.<name>.<hostname>._<host
ID>.<target date>.<backup type>.<timestamp>.tgz
/store/reporting

```



Note: If you wish to maintain the restored data, you may increase your data retention settings to prevent the nightly disk maintenance routines from deleting your restored data. To ensure your restored data is not deleted, review [Step 8](#).

Step 6 Verify the files are restored by investigating one of the restored directories:

```

cd /store/ariel/flows/payloads/<yyyy/mm/dd>

```

For example:

```

cd /store/ariel/flows/payloads/2008/3/31

```

```

ls

```

```

0 1 10 11 12 13 14 15 16 17 18 19 2 20 21 22 23
3 4 5 6 7 8 9

```

You can view the restored directories that are created for each hour of the day. If directories are missing, this may indicate that no data was captured for that time period. For example, the list of files in one of the restored directories may include:

```

ls 0 |more

```

```

payload_flows~0_0~eb8d3826c5724b01~b56774a558286d05
payload_flows~10_0~ecfb94ded5814c4d~9c5d33d0ec9ec0a6
payload_flows~1_0~94fca21391be44ea~bd32d5dbe8c6a60a
payload_flows~11_0~4d98ae53d2354d41~bde1b8f0684e3829
payload_flows~12_0~2c45af65412c41c6~af424b6b3e5c2e48
payload_flows~13_0~388fe28e9484859~8ca4462103a72bfb
payload_flows~14_0~3e2c90e566d442ca~b7bb031ae09876db
payload_flows~15_0~d382f047a5164281~b2d99a661a9a8e28
payload_flows~16_0~3e18d2a93a1746ca~914d4395a0756c4b
payload_flows~17_0~13383fec3302441f~b237970768894b79
payload_flows~18_0~dcaa5df8d3764c65~a125bd6ca4cd3b76
payload_flows~19_0~d1ea417c7faf4551~869ef92249918994

```

Step 7 Verify the restored data is now available:

- a Log into the STRM interface.
- b Click the Event Viewer or Flow Viewer tab.
- c Select **Search > Edit Search** from the drop-down list box.
The search window appears.
- d In the Time Range box, select the Specific Interval option.
- e Specify the data of the data you just restored in [Step 5](#).
- f Click **Filter**.
- g View the results to verify the restored data.

Step 8 Optional. If your data retention for this type of data is configured for a time of period that is less than the data you just restored (for example, 1 month and the data you restored is 2 months old), then the STRM disk maintenance utility automatically deletes this data at 2am of the following day. To avoid the automatic deletion of the restored files, you can increase your disk retention settings to include this time period or use the following procedure to mark restored data as protected to ensure the files are not deleted:



Note: *Increasing your disk retention period may impact the available disk space on your system.*

- a Open the following file:

```
/opt/qradar/conf/diskmaintd.conf
```

An example of the file includes:

```
cat diskmaintd.conf
```

```
# Diskmaintd configuration file. Currently only supported
section is the
```

```
# list of files/directories to not cleanup.
```

```
#
```

```
[path_to_keep]
```

```
# Specify on a line the path to a file or directory to keep.  
Path is absolute.
```

```
# For example: /store/ariel/flows/records/2007/1/1/8
```

- b On each host that has restored data, add the subdirectories of the restored data to the file.

For example, if you wish to maintain the restored flow data:

```
/store/ariel/flows/payloads/2008/3/31
```

```
/store/ariel/flows/records/2008/3/31
```

Troubleshooting Tips

If you have restored your data files and the restored data is not available in the STRM interface, we recommend that you verify the following:

- Verify that you have restored the data to the proper location.
For example, the restored files need to be located in the `/store` directory, however, if you did not include the P option in the extraction command (see [Step 5](#)), the files are restored in the directory in which you entered the `/store/backup/store` directory.
- Ensure all proper file permissions are correctly configured. Typically, files are restored with the original permissions. However, if the files are owned by root, this may cause issues. If this is the case, adjust the files permissions using the `chown` and `chmod` commands. For assistance, please contact Juniper Networks Customer Support.

Copyright Notice

Copyright © 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or 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.

Part Number 530-025630-01