

# TECHNICAL NOTE

## RESTORING YOUR CONFIGURATION AND DATA

OCTOBER 2009

You need to backup STRM Data before re-imaging or upgrading the devices. STRM backup consists of Configuration (Config) backup and Data backup. You can backup your configuration information and data using the STRM Admin interface.



**Note:** *Offenses cannot be restored as backing up offenses is not possible. For more information about backing up your configuration and data, see the STRM Administration Guide.*

If you are using STRM 2009.1 and above, you can restore your configuration information using the STRM interface, however, you must use the procedures in this document to restore your data. This document provides information on restoring your STRM including:

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

---

### Before You Begin

Each managed host in your deployment, including the STRM Console, creates all 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. For example, PKI.*

Before you restore the data, consider the following:

- If you are restoring data on a newly installed Console, you must restore the configuration backup before restoring the data backup.
- Locate the managed host on which the data is backed up.
- All systems in your deployment with storage capabilities will store the backups locally in the following directory: `/store/backup`. All backup files are saved using the following format:

`backup.<name>.<hostname_hostID>.<target date>.<backup type>.<timestamp>.tgz`

Where:

`<name>` is the name associated with the backup.

`<hostname_hostID>` is the name of the STRM system hosting the backup file followed by the identifier for the STRM system.

`<target date>` is the date that the backup file was created. The format of the target date is `<date>_<month>_<year>`.

`<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 (/store/ariel)` directory includes adequate space (if your deployment includes a separate mount point for that volume) for the data you want to recover.
- Identify the date and time for the data you want to recover.

---

## Restoring Your Configuration

STRM Config backup consists of:

- views config - Different views stored on STRM
- custom rules config - Custom rules added by user
- deployment config - Deployment configuration in a distributed (multi-box) environment
- users config - STRM users details
- sentry config - Alerts generated
- license - STRM license details

By default STRM backs up configuration. To restore the configuration information:

- Step 1** Login to STRM webui.
- Step 2** Select the config backup you want to restore.
- Step 3** Click Restore to restore the backup.

---

## Restoring Your Data

STRM Data Backup consists of:

- event data - Log data from devices
- flow data - Flow data from devices
- hostprofile data - Network hierachy and hosts
- reports data - Reports generated, including custom reports
- audit log - Audit logs of STRM

To restore your data:

**Step 1** Log in to STRM as root.

**Step 2** Stop the services in the following order:

```
service hostcontext stop
service tomcat stop
service imq stop
service postgresql stop
```



**Note:** If you are restoring data on a non-Console system, you only need to stop the `hostcontext` service.

**Step 3** Change the directory:

```
cd /store/backup
```

**Step 4** Locate the data files you need to restore:

```
ls -l
```

A list of backup files appear.

For example:

```
total 391528
-rw-r--r--  1 root root 16780568 Apr  2 00:00
backup.scheduled.csd9_2.01_04_2008.config.1207119651365.tgz
-rw-r--r--  1 root root  77382262 Apr  2 00:02
backup.scheduled.csd9_2.01_04_2008.data.1207119722164.tgz
-rw-r--r--  1 root root   9487517 Apr  2 00:00
backup.scheduled.csd9_2.01_04_2008.db.1207119624313.tgz
-rw-r--r--  1 root root  16724841 Mar 30 00:00
backup.scheduled.csd9_2.29_03_2008.config.1206860449624.tgz
-rw-r--r--  1 root root   69970426 Mar 30 00:01
backup.scheduled.csd9_2.29_03_2008.data.1206860499469.tgz
drwxr-xr-x  2 root root    4096 Apr  2 08:58 desc
```



**Note:** If no backup files are listed, skip [Step 6](#) and [Step 8](#).

**Step 5** Change the directory to the root directory:

```
cd /
```

The root directory appears. If you are restoring data on a non-Console managed host and no backup files were listed in [Step 4](#), go to [Step 10](#).

**Step 6** Extract the files to their original directory.

```
tar -zxvPf
/store/backup/backup.<name>.<hostname_hostID>.<target
date>.<backup type>.<timestamp>.tgz
```

For example:

```

tar -zxvPf
/store/backup/backup.scheduled.csd9_2.31_03_2008.data.120703330
4942.tgz
/store/tmp/backup/database.dump
/var/log/audit/audit.log
/store/reporting/reports/logos/default.png
/store/reporting/reports/admin/reports/DAILY##admin##1e3d00ea
-69d0-4cda-859c-b7ae72bf7ffa##1204174811979/XLS/1e3d00ea-69d0-
4cda-859c-b7ae72bf7ffa.xls
/store/reporting/reports/admin/reports/DAILY##admin##1e3d00ea
-69d0-4cda-859c-b7ae72bf7ffa##1204174811979/data.xml
/store/reporting/reports/admin/reports/DAILY##admin##1e3d00ea
-69d0-4cda-859c-b7ae72bf7ffa##1204174811979/PDF/1e3d00ea-69d0-
4cda-859c-b7ae72bf7ffa.pdf
/store/reporting/reports/admin/reports/DAILY##admin##Daily At
A Glance Network Security Health
Summary##1204174825109/data.xml
/store/reporting/reports/admin/reports/DAILY##admin##Daily At
A Glance Network Security Health
Summary##1204174825109/PDF/Daily At A Glance Network Security
Health Summary.pdf
/store/reporting/reports/admin/reports/DAILY##admin##Daily
Attacker and Target Summary##1204174839555/data.xml
/store/reporting/reports/admin/reports/DAILY##admin##Daily
Attacker and Target Summary##1204174839555/PDF/Daily Attacker
and Target Summary.pdf
/store/reporting/reports/admin/reports/DAILY##admin##Daily
Delta Network Usage Summary##1204174853767/data.xml
/store/reporting/reports/admin/reports/DAILY##admin##Daily
Delta Network Usage Summary##1204174853767/PDF/Daily Delta
Network Usage Summary.pdf
/store/reporting/reports/admin/reports/DAILY##admin##Daily
Enterprise Network Usage Summary##1204174868310/data.xml
/store/reporting/reports/admin/reports/DAILY##admin##Daily
Enterprise Network Usage Summary##1204174868310/PDF/Daily
Enterprise Network Usage Summary.pdf
/store/reporting/reports/admin/reports/DAILY##admin##Daily
Executive Application Usage Summary##1204174882593/data.xml
/store/reporting/reports/admin/reports/DAILY##admin##Daily
Executive Application Usage Summary##1204174882593/PDF/Daily
Executive Application Usage Summary.pdf

```



**Note:** Data backups on a daily basis capture all data for that day on each host. The above example reflects a single, All-in-One Console and includes reports, PDF files, event, and flow data. If you want to restore data on a managed host that only contains event or flow data, only that data is restored to that host.



**Note:** If you want 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 3 in Verifying That Your Data is Restored](#).

If you are restoring data on a non-Console system, go to [Step 10](#).

**Step 7** Create the PostgreSQL database, users, and schemas:

```
/opt/strm/bin/flatten_db.pl -l /var/log/strm-sql.log -f -y -n -d
/store/postgres
```

This command also restarts the PostgreSQL service. If no backup files were listed in [Step 4](#), go to [Step 9](#).

**Step 8** Restore the database to the state when backup was performed:

```
pg_restore -c -U postgres -v -d strm
/store/tmp/backup/database.dump
```

**Step 9** Clean and re-index the database:

```
psql -U postgres strm
VACUUM ANALYZE
REINDEX DATABASE strm
\q
```

**Step 10** Restart the services in the following order:

```
service imq start
service tomcat start
service hostcontext start
```



**Note:** If you are restoring data on a non-Console system, you only need to restart the *hostcontext* service.

## Verifying That Your Data is Restored

To verify that your data has been restored correctly:

**Step 1** 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 2** Verify the restored data is now available:

- a Log into the STRM interface.
- b Click the **Events** or **Flows** 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 time range of the data you just restored in [Step 6](#).
- f Click **Filter**.
- g View the results to verify the restored data.

**Step 3** 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), the STRM disk maintenance utility automatically deletes this data at 2 am 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 want 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 entered `cd` instead of `cd /` in [Step 5](#), the files would be restored in the directory in which you entered the command (the `/root/store` directory). Also, if you omitted [Step 5](#), the files would be restored in 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.

Published: 2009-10-12