

Stratusphere™: How to perform a backup restore of the Stratusphere Database

Overview

These instructions address the simple use case of backing up a Stratusphere Database. It does NOT supply instructions to backup any other aspects of the Stratusphere Hub OR Database appliances such as SSL certificates, key stores, and user credentials (passwords).

Preparations

1. Do NOT open or save the .sh files on Windows machines. The EOL/Carriage Return formats are different between Windows and Linux. Saving in Windows format causes failure on Linux.
2. If default credentials have been changed, then obtain updated credentials of the FRIEND user accounts on the Stratusphere Hub or Database appliances.

Note: Depending on your platform, use the following credentials:

Default Database Appliance Credentials for FRIEND User

- On-Premises Appliances:
 - **Username:** friend
 - **Password:** sspassword
- AWS Cloud Appliances:
 - **Username:** ec2user
 - **Password:** Your VM Instance ID
- Azure Cloud Appliances:
 - **Username:** az-user or azureuser
 - **Password:** Your VM Instance ID

Default Hub & Collector Appliance Credentials for CONSOLE User

- On-Premises Appliances:
 - **Username:** ssconsole
 - **Password:** sspassword
- AWS Cloud Appliances:
 - **Username:** ec2user
 - **Password:** Your VM Instance ID
- Azure Cloud Appliances:
 - **Username:** az-user or azureuser
 - **Password:** Your VM Instance ID

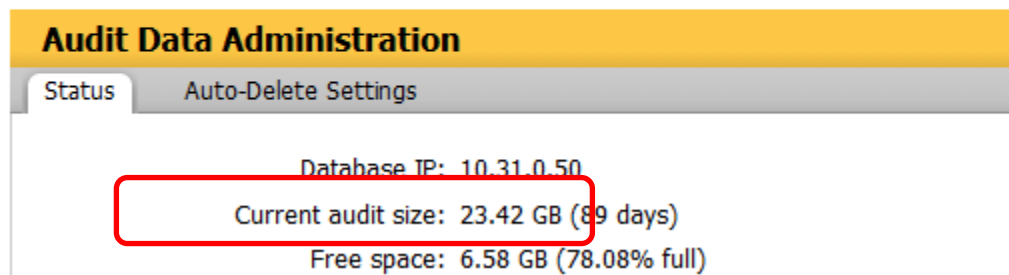
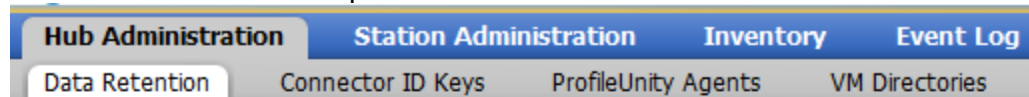
3. Download and install an SSH client like PuTTY or Windows Command Prompt or similar.
4. Download and install an SCP client like WinSCP or Windows Command Prompt or similar.
5. Ensure access to TCP/22 is available to the appliance from your local workstation.

6. The backup restore scripts will display an estimate of the amount of space needed to back up or restore the entire database. Here is information if you are interested in performing the checks yourself:
 - a. Ensure enough space is available on the '/var/lib/pgsql' partition of the source Stratusphere Hub or Database appliance to accommodate the database backup file. To find out the free space available do the following:
 - b. On the source Stratusphere Database appliance local console, log in using the default FRIEND credentials. If any of these credentials have been changed, please obtain and use the modified credentials.
 - c. Execute the following command and enter the password when prompted (default: 'sspassword'):

```
sudo df -h
```

```
[root@586db ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda2       6.2G  1.1G  4.8G  19% /
/dev/sda9        96M  4.2M   87M   5% /tmp
/dev/sda7       934M  170M  715M  20% /var
/dev/sda6       471M   17M  430M   4% /var/tmp
/dev/sda5       471M   20M  426M   5% /var/log
/dev/sda8       184M   17M  158M  10% /var/log/audit
/dev/sda3       934M   18M  867M   2% /home
/dev/sdc1        30G  234M   29G   1% /var/lib/pgsql
/dev/sde1       3.8G  104M  3.5G   3% /var/lib/pgsql_xlog
```

- d. Look for the value under the 'Avail' column for the /var/lib/pgsql partition. This is the available space: 29GB.
- e. The database backup script has an aggressive compression ratio (between 9:1 to 15:1). Use this ratio as a guideline to get an approximate idea of the amount of space needed to accommodate the backup file.
- f. Use the 'Current audit size' field in Stratusphere Web UI's Administration section, under the Hub Administration > Data Retention > Status tab to calculate the estimate size of the backup file.



- g. So, based on the image above, you would need between $24\text{GB}/9 = 2.6\text{GB}$ and $24\text{GB}/15 = 1.6\text{GB}$ of space for the backup file. In this example, since 2.6GB and 1.6GB is less than 29GB there should be enough space for the backup file to be generated.

-
7. It is **recommended but not required** that all services on the Hub and Collectors are stopped before starting a backup. However, for restoring data all services on the Hub and Collectors **must** be stopped before starting a restore. To do so, log into the console of the Hub and (if any) Collectors using the default CONSOLE credentials. If these have been changed, please use the modified credentials.
 - a. On the console of Hub and Collector Appliance menus, navigate to S) Software Services option.
 - b. Toggle off all running services one at a time on the Hub and Collectors *except the database service (if your database is on the Hub itself and not a separate appliance)*. The script handles turning services off and on if the database is running on the Hub itself, but it does NOT stop any services on Collectors.
 - c. After stopping services on the Hub and Collectors, you are ready to perform a backup restore of the Stratusphere Database.
 8. The scripts for backup and restore can be run in interactive mode and non-interactive command line mode. This document supplies instructions on running backup and restore in interactive mode and in non-interactive mode using command line arguments.

Interactive Instructions

Liquidware recommends performing backup and restores using interactive mode if performing one off backup and restores. The interactive mode displays available options of what the script can do, with feedback on what it is doing, and even an estimate on the amount of time left to perform the backup or restore.

Note: Depending on your platform, use the following credentials:

Default Database Appliance Credentials for FRIEND User

- On-Premises Appliances:
 - **Username:** friend
 - **Password:** sspassword
- AWS Cloud Appliances:
 - **Username:** ec2user
 - **Password:** Your VM Instance ID
- Azure Cloud Appliances:
 - **Username:** az-user or azureuser
 - **Password:** Your VM Instance ID

On the destination database appliance:

1. Open your SCP client to connect & log into the destination appliance running the database using the default FRIEND credentials on port 22. If these default credentials have been changed, please obtain, and use the modified credentials.
2. Upload the restore script from your local desktop folder to the `/home/[username]` folder (where [username] is the FRIEND user for the platform) on the appliance that runs the database i.e., if you run only a Hub database, please upload it to the Hub appliance or if you run a Hub and a Database appliance, please upload it to the Database appliance.
3. Open your SSH client to connect to the database appliance and log in using the default FRIEND credentials. If these default credentials have been changed, please obtain, and use the modified credentials.
4. Execute the following command to set up the script to perform restores. It will create the backups folder with the expected permissions and ownership and exit.

➤ `sudo bash /home/[username]/restoredatabase.vxxx.sh --setup`

where [username] is the FRIEND user for the platform.

```
[friend@10 ~]$ sudo bash /home/friend/backupscripts/backupdatabase.v66x-670x.sh --setup
[sudo] password for friend:
Initiating setup for restoring data...
Completed initial setup.
[friend@10 ~]$
```

Backup database on the production or source database appliance:

1. Open your SCP client to connect & log into the source appliance running the database using the default FRIEND credentials on port 22. If these default credentials have been changed, please obtain, and use the modified credentials.
2. Upload the backup script from your local desktop folder to the `/home/[username]` folder (where [username] is the FRIEND user for the platform) on the appliance that runs the database i.e., if you run only a Hub database, please upload it to the Hub appliance or if you run a Hub and a Database appliance, please upload it to the Database appliance.
3. Open your SSH client to connect to the database appliance and log in using default FRIEND credentials. If these default credentials have been changed, please obtain, and use the modified credentials.
4. Execute the command line to start a backup:

```
➤ sudo bash /home/[username]/backupdatabase.vxxx.sh
```

where [username] is the FRIEND user for the platform. The script will prompt for a password to run as superuser (`su`) – please enter the default FRIEND password. If the password has been changed, please use the modified passwords.

5. The script will display a banner asking the end user to stop services on the Hub and Collectors to keep referential integrity of the database. The script will continue the backup even if the services are not stopped.
6. The script will display the Main Menu. Please select option B to perform a full database backup. Follow the prompts and accept defaults for the backup file location and name.

```
Liquidware Stratusphere Database Backup Script.

Prior to proceeding with a database backup, Liquidware recommends either
shutting down the Hub & Collectors or stopping their relevant services.

To stop services:
Login to the Collector's consoles (if any), and stop services.
This script will stop services on this Hub appliance automatically.

Use credentials of ssconsole to log into the console, and navigate to
S) Software Services option, and toggle off all running services.

Main Menu

S. Setup.
K. Generate SSH Keys.

B. Perform Full Database Backup.

L. List Database Backup files.
D. Download Database Backup file /var/lib/pgsqli/backups/10-251112-portal.db.backup.gz.
R. Remove Database Backup file /var/lib/pgsqli/backups/10-251112-portal.db.backup.gz.

Q. Quit.

Enter your selection? [ S | K | B | L | D | R | Q ] [Default: B]: B

Default Database Backup Folder : /var/lib/pgsqli/backups/
Default Database Backup File   : 10-251112-portal.db.backup.gz

Hit [ENTER] to accept defaults, Q to quit, or
Enter new Backup File (no path): █
```

7. The script will also prompt whether the user wants to:

a. D. Download file.

```
After the backup, what do you want to do with the backup file?
U. Upload file to a remote destination.
D. Download file.
N. Nothing. Just perform a backup and leave the file inplace.
What do you want to do? [U/D/N Default: D]: D
08/29/23 10:03:35 AM EDT: User chose to download file after Backup is complete.

Settings:

Backup full database to: /var/lib/pgsql/backups/10-230829-portal.db.backup.gz
Action to take          : D. Download file.
```

b. U. Uploaded file to a remote destination. The script will prompt the end user to enter the remote appliance IP/DNS address, remote path, and remote username.

```
After the backup, what do you want to do with the backup file?
U. Upload file to a remote destination.
D. Download file.
N. Nothing. Just perform a backup and leave the file inplace.
What do you want to do? [U/D/N Default: D]: U
08/29/23 11:51:16 AM EDT: User chose to upload file after Backup is complete.

Enter IP/DNS address to upload backup file: 10.30.50.130
Enter remote username [friend]: friend
Does 10.30.50.130 support Password (p) or SSH Key pair (k) based authentication?
Default: p [p/k]: p
The script will prompt you to enter a password.
Do you want to generate SSH Keys for 10.30.50.130 [Y/N]: Y
Generating SSH Key for seamless transfer to 10.30.50.130...
Copying SSH Key to 10.30.50.130...
/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
friend@10.30.50.130's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'friend@10.30.50.130'"
and check to make sure that only the key(s) you wanted were added.

Settings:

Backup full database to: /var/lib/pgsql/backups/10-230829-portal.db.backup.gz
Action to take          : U. Upload file to a remote destination.
Upload backup files to : friend@10.30.50.130:/var/lib/pgsql/backups/
```

The script will prompt the end user to:

- Enter the IP/DNS address of the destination to upload the backup file.
- Enter the remote username for the FRIEND user depending on the platform.
- The script will then prompt the end user to decide whether the remote machine accepts password-based authentication or SSH Key Pair based authentication. Select p for password-based authentication.
- The script will prompt whether to generate an SSH key to be copied to the destination to allow password less, seamless transfers in the future.
 - If you select Y, the script will generate a public key to be uploaded to the remote destination and then prompt you to enter the password to authenticate to the remote destination just once and then copy the public key to the remote destination. You will not need to enter a password while uploading to this remote destination again.
 - If you enter N, then you will have to enter the password every time the script needs to upload the backup file to the destination.

c. N. Nothing.

8. Depending on the size of the database, it may take time to generate a full backup, but the script will display data backed up so far out of the total backup file size estimated along with the amount of time left estimated and the time elapsed.

```
08/29/23 10:03:35 AM EDT: Estimated Backup File Size: 66.665 / 10.582 = 6.299 GB
08/29/23 10:03:35 AM EDT: Info: Adequate disk space exists based on estimated size to backup database.
08/29/23 10:03:35 AM EDT: Changing ownership of /var/lib/pgsql/backups/ to postgres:postgres.
08/29/23 10:03:35 AM EDT: Database backup initiated...
08/29/23 10:14:15 AM EDT: Backed up 3.292 of 6.299 GB (est) Time Left: 00:09:39 (est) Time Elapsed: 00:10:34 \_
```

9. When the backup is finished, the script will restore some permissions on the file systems.

```
08/29/23 10:03:35 AM EDT: Database backup initiated...
08/29/23 10:24:03 AM EDT: Backup up 6.957 GB, Time Elapsed: 00:20:20.
08/29/23 10:24:03 AM EDT: Database backup completed.
08/29/23 10:24:03 AM EDT: Backup file:/var/lib/pgsql/backups/10-230829-portal.db.backup.gz is ready.
08/29/23 10:24:03 AM EDT: Restoring ownership of /var/lib/pgsql/backups/ to friend:friend.
08/29/23 10:24:03 AM EDT: Changing ownership of /var/lib/pgsql/backups/10-230829-portal.db.backup.gz file to 'friend' user.
08/29/23 10:24:03 AM EDT: Changed ownership of backup file to 'friend' user.
08/29/23 10:24:03 AM EDT: Info: Compression Ratio Used: 10.582
08/29/23 10:24:03 AM EDT: Info: Compression Ratio Real: 10.583
```

10. Depending on the options selected above:

- a. If **D**. Download file was selected:

- i. The script will display contents of the `/var/lib/pgsql/backups/` folder and wait until the latest backup file has been downloaded. The script keeps the access open for 3 hours and it can be extended if the file is not downloaded until then.
- ii. Use the same SCP client used above to upload the backup script to download the backup file from the database appliance by navigating to the folder displayed by the backup script to your local desktop.

```
Listing contents of /var/lib/pgsql/backups/:
-rw-r-----. 1 friend friend 7.0G Aug 29 10:24 /var/lib/pgsql/backups/10-230829-portal.db.backup.gz
08/29/23 10:24:03 AM EDT: Use an SCP client (WinSCP) to download backup file(s).
08/29/23 10:24:03 AM EDT: Script times out in 3hrs.
Have the backup file(s) been downloaded? [Y/N/Quit]: _
```

Once downloaded, enter **Y** or **y** to continue.

- b. If **U**. Upload file to a remote destination was selected,

- i. The backup files will be uploaded to the remote location.

```
08/29/23 12:22:45 PM EDT: Uploading backups to 10.30.50.130 to /var/lib/pgsql/backups/...
10-230829-portal.db.backup.gz          100% 7125MB 115.8MB/s 01:01
restore                                100% 0      0.0KB/s 00:00
08/29/23 12:23:49 PM EDT: Completed upload to 10.30.50.130.
```

11. The script may prompt the end user to remove the backup files once they have been downloaded or uploaded.

```
Have the backup file(s) been downloaded? [Y/N/Quit]: Y
Delete backup /var/lib/pgsql/backups/10-230829-portal.db.backup.gz file? [Y/N]: _
```

12. The script then performs house cleaning tasks and displays a banner with instructions on starting services on the Hub and Collectors that may have been stopped prior to starting the backup.

```

Have the backup file(s) been downloaded? [Y/N/Quit]: Y
Delete backup /var/lib/pgsql/backups/10-230829-portal.db.backup.gz file? [Y/N]: Y
08/29/23 10:34:37 AM EDT: Removing /var/lib/pgsql/backups/10-230829-portal.db.backup.gz file...
08/29/23 10:34:38 AM EDT: Removing /var/lib/pgsql/backups/backupdatabase.v662.v1.out file...
08/29/23 10:34:38 AM EDT: Done.
-----
IMPORTANT
If the Hub and Collectors were shut down or their services were stopped,
please ensure the Hub and Collectors are booted up or their services are
restarted.

To start services:
Login to the Collector's consoles (if any), and start services.
This script will start services on this Hub appliance automatically.

Use credentials of sconsole to log into the console, and navigate to
S) Software Services option, and toggle on all running services.
-----
[friend@10 ~]$

```

13. The backup is now complete.
14. By default, a log file is created under `/home/[username]/backupdatabase.vxxx.log` – where [username] is the FRIEND user for the platform the appliance is running on. Check this log file for status or any error messages. There is functionality to rotate the log if it gets above 5MB and to keep the last 5 log files so that the logs do not take up too much space on the appliance. If asked, provide this log file back to Liquidware.

Restore database on the destination database appliance:

1. Open your SCP client to connect & log into the destination appliance running the database using the default FRIEND credentials on port 22. If these default credentials have been changed, please obtain, and use the modified credentials.
2. Upload the backup restore script from your local desktop folder to the `/home/[username]` folder (where [username] is the FRIEND user for the platform) on the appliance that runs the database i.e., if you run only a Hub database, please upload it to the Hub appliance or if you run a Hub and a Database appliance, please upload it to the Database appliance.
3. Open your SSH client to connect to the appliance and log in using default FRIEND credentials. If these default credentials have been changed, please obtain, and use the modified credentials.
4. Execute the command line to start a backup:


```
➤ sudo bash /home/[username]/restoredatabase.vxxx.sh
```

where [username] is the FRIEND user for the platform. The script will prompt the user to enter the password to run as superuser (su) – please enter the default FIREND password. If the password has been changed, please use the modified passwords.

5. The script will display a banner asking the end user to stop services on the Hub and Collectors to keep referential integrity of the database.
6. The script will prompt the user on whether they need to upload the database backup file.

```
-----
Liquidware Stratusphere Database Restore Script.
-----

Prior to proceeding with a database restore, Liquidware recommends either
shutting down the Hub & Collectors or stopping their relevant services.

To stop services:
Login to the Collector's consoles (if any), and stop services.
This script will stop services on this Hub appliance automatically.

Use credentials of sconsole to log into the console, and navigate to
S) Software Services option, and toggle off all running services.
-----

Do you need to upload the backup file? [Y/N]: _
```

- a. If the user enters Y, it will allow access to the /var/lib/pgsql/backups/ folder to allow the local FRIEND user to upload the backup file to this location using a SCP client. Use the same credentials used to upload the restore script to the /home/friend folder above but upload the file to /var/lib/pgsql/backups/ folder.

```
Do you need to upload the backup file? [Y/N]: Y

- Please upload to /var/lib/pgsql/backups/.
- Permissions are granted temporarily to permit uploads.
- DO NOT CTRL-C out of this script. It might leave your appliance vulnerable.

- Use an SCP client (WinSCP) to upload the file using 'friend' credentials.
- Navigate to /var/lib/pgsql/backups/.
- Script will time out in 3.0 hours.

Has the file been uploaded to /var/lib/pgsql/backups/? [Y/N/Quit]: _
```

- b. If the user enters N, it will list the contents of /var/lib/pgsql/backups/ folder.
7. Once uploaded, enter Y.
 8. It will then search for the latest backup file in /var/lib/pgsql/backups/ folder with the right extension of "*.db.backup.gz" and populates the file as the default option where the end user can hit ENTER to accept the default backup file.

```
Has the file been uploaded to /var/lib/pgsql/backups/? [Y/N/Quit]: Y
08/29/23 12:46:14 PM EDT: Restore permissions on /var/lib/pgsql/backups/ folder...
08/29/23 12:46:14 PM EDT: Restore ownership of friend:friend on /var/lib/pgsql/backups/ folder...
Enter database backup file path name or [ENTER] to confirm:
[/var/lib/pgsql/backups/10-230829-portal.db.backup.gz]: _
```

9. The script then continues to do the following:

```
Enter database backup file path name or [ENTER] to confirm:
[/var/lib/pgsql/backups/10-230829-portal.db.backup.gz]:

- Settings -----
  Interactivity : 1
  BackupFilePath: /var/lib/pgsql/backups/10-230829-portal.db.backup.gz
  BackupPath    : /var/lib/pgsql/backups/
  BackupFile    : 10-230829-portal.db.backup.gz
  Restore licence: y

08/29/23 12:48:12 PM EDT: Backup File /var/lib/pgsql/backups/10-230829-portal.db.backup.gz Size: 6.957 GB
08/29/23 12:48:12 PM EDT: Estimated Database Size: 12.868 x 6.957 = 89.522 GB
08/29/23 12:48:12 PM EDT: Estimated Database Space Required: 119.362 GB
08/29/23 12:48:12 PM EDT: Disk Space Allocated: 127.988 GB on /dev/sdc1
08/29/23 12:48:12 PM EDT: Info: Adequate disk space exists based on estimated size to restore database.
08/29/23 12:48:12 PM EDT: Asking lwl-backend-priv service to stop...
08/29/23 12:48:12 PM EDT: Asking lwl-backend service to stop...
08/29/23 12:48:14 PM EDT: Asking lwl-smx service to stop...
08/29/23 12:48:16 PM EDT: Asking lwl-cidd service to stop...
08/29/23 12:48:16 PM EDT: Restarting Postgres 12 service...
08/29/23 12:48:17 PM EDT: Waiting 10s for database to start...
Existing database will be dropped and restored from the backup.
Proceed? [Y/N/Q]: _
```

- a. Display the settings it is configured with.

- b. Check whether there is adequate space to restore the database.
 - c. Stopping relevant services on the local appliance.
 - d. Check whether there are active connections to the database, and if so, it **will not continue** if there are active connections.
 - e. Restart the database service to clear out any connections.
 - f. And finally, prompt the end user for confirmation to continue with dropping the existing database and continue with the restoration. Please enter Y to continue.
10. The script will then continue to do the following:

```
Proceed? [Y/N/Q]: Y
08/29/23 12:56:06 PM EDT: Setting owners of /var/lib/pgsql/backups/ to postgres:postgres...
08/29/23 12:56:06 PM EDT: Setting owners of /var/lib/pgsql/backups/10-230829-portal.db.backup.gz to postgres:postgres...
08/29/23 12:56:06 PM EDT: Backing up existing license...
08/29/23 12:56:07 PM EDT: Restarting Postgres 12 service...
08/29/23 12:56:07 PM EDT: Dropping portal database now...
08/29/23 12:56:10 PM EDT: Backup File /var/lib/pgsql/backups/10-230829-portal.db.backup.gz Size: 6.957 GB
08/29/23 12:56:10 PM EDT: Estimated Database Size: 12.868 x 6.957 = 89.522 GB
08/29/23 12:56:10 PM EDT: Restoring database from /var/lib/pgsql/backups/10-230829-portal.db.backup.gz...
08/29/23 12:56:45 PM EDT: Restored .529 of 89.522 GB (est) Time Left: 01:24:06 (est) Time Elapsed:00:00:30 |
```

- a. It will supply access for reading the backup file to the Postgres service so that it can be restored from.
 - b. It will then continue to drop the existing database and begin restoring the entire database.
 - c. The script should display estimates on the size of the database to be restored, and the amount of time it will take to restore it.
11. Once the restore is complete, it will:

```
08/29/23 12:56:10 PM EDT: Restoring database from /var/lib/pgsql/backups/10-230829-portal.db.backup.gz...
08/29/23 01:30:38 PM EDT: Restored 66.370 GB. Time Elapsed:00:34:21.08/29/23 01:30:38 PM EDT: Database restore completed.
08/29/23 01:30:38 PM EDT: Restarting Postgres 12 service...
08/29/23 01:30:40 PM EDT: Restoring existing license...
08/29/23 01:30:40 PM EDT: Restore permissions on /var/lib/pgsql/backups/ folder...
08/29/23 01:30:40 PM EDT: Restore ownership of friend:friend on /var/lib/pgsql/backups/ folder...
08/29/23 01:30:40 PM EDT: Restore permissions on /var/lib/pgsql/backups/10-230829-portal.db.backup.gz file...
08/29/23 01:30:40 PM EDT: Restore ownership friend:friend on /var/lib/pgsql/backups/10-230829-portal.db.backup.gz file...
08/29/23 01:30:40 PM EDT: Info: Compression Ratio Used: 12.868
08/29/23 01:30:40 PM EDT: Info: Compression Ratio Real: 13.874
08/29/23 01:30:40 PM EDT: Asking lwl-backend-priv service to start...
08/29/23 01:30:51 PM EDT: Asking lwl-backend service to start...
08/29/23 01:31:01 PM EDT: Asking lwl-smx service to start...
08/29/23 01:31:11 PM EDT: Asking lwl-cidd service to start...
Here is a list of Collectors where services need to be started:
```

name	ip
labvsx1-collector2	10.0.60.62
labvsx2-collector2	10.0.60.63
Stratusphere Hub	10.31.0.100
ux-demo-coll	10.31.0.101

(4 rows)

- a. Restart the database service.
 - b. Any existing license will be restored.
 - c. Restore any permissions on the /var/lib/pgsql/backups/ folders and files.
 - d. Any relevant services running on the appliance will be started.
 - e. If there are any Collectors, it will display a list of them where services will need to be started.
12. The script may prompt the user to decide whether to remove the backup files.

```
Delete backup /var/lib/pgsql/backups/10-230829-portal.db.backup.gz file? [Y/N]:
```

- The script then performs house cleaning tasks and displays a banner with instructions on starting services on the Hub and Collectors that may have been stopped prior to starting the restore.

```
08/29/23 01:35:19 PM EDT: Done.
-----
IMPORTANT
If the Hub and Collectors were shut down or their services were stopped,
please ensure the Hub and Collectors are booted up or their services are
restarted.

To start services:
Login to the Collector's consoles (if any), and start services.
This script will start services on this Hub appliance automatically.

Use credentials of sconsole to log into the console, and navigate to
S) Software Services option, and toggle on all running services.

The appliance will now be rebooted.
-----
08/29/23 01:35:19 PM EDT: Rebooting appliance in 60 seconds...
```

- The restore is now complete and the appliance will reboot in 60 seconds.
- By default, a log file is created under `/home/[username]/restoredatabase.vxxx.log` -- where [username] is the FRIEND user for the platform the appliance is running on. Check this log file for status or any error messages. There is functionality to rotate the log if it gets above 5MB and to keep the last 5 log files so that the logs do not take up too much space on the appliance. If asked, provide this log file back to Liquidware.

Command line Instructions

Liquidware recommends running backup and restore in command line mode if they need to be scheduled to occur at fixed intervals during a day of the week or hour of day. The backup script can be scheduled to create backups and then upload them to a remote destination database appliance automatically. Similarly, the restore scripts can be scheduled to look for a new backup uploaded by the source database appliance and then perform a restore on the local database.

Note: Depending on your platform, use the following credentials:

Default Database Appliance Credentials for FRIEND User

- On-Premises Appliances:
 - **Username:** friend
 - **Password:** sspassword
- AWS Cloud Appliances:
 - **Username:** ec2user
 - **Password:** Your VM Instance ID
- Azure Cloud Appliances:
 - **Username:** az-user or azureuser
 - **Password:** Your VM Instance ID

On the destination database appliance:

1. Open your SCP client to connect & log into the destination appliance running the database using the default FRIEND credentials on port 22. If these default credentials have been changed, please obtain, and use the modified credentials.
2. Upload the backup script from your local desktop folder to the `/home/[username]` folder (where [username] is the FRIEND user for the platform) on the appliance that runs the database i.e., if you run only a Hub database, please upload it to the Hub appliance or if you run a Hub and a Database appliance, please upload it to the Database appliance.
3. Open your SSH client to connect to the database appliance and log in using the default FRIEND credentials. If these default credentials have been changed, please obtain, and use the modified credentials.
4. Execute the following command to set up the script to perform restores. It will create the backups folder with the expected permissions and ownership and exit.
 - `sudo bash /home/[username]/restoredatabase.vxxx.sh --setup`
where [username] is the FRIEND user for the platform.

Backup database on the production or source database appliance:

1. Open your SCP client to connect & log into the source appliance running the database using the default FRIEND credentials on port 22. If these default credentials have been changed, please obtain, and use the modified credentials.

2. Upload the backup script from your local desktop folder to the `/home/[username]` folder (where [username] is the FRIEND user for the platform) on the appliance that runs the database i.e., if you run only a Hub database, please upload it to the Hub appliance or if you run a Hub and a Database appliance, please upload it to the Database appliance.
3. Open your SSH client to connect to the database appliance and log in using the default FRIEND credentials. If these default credentials have been changed, please obtain, and use the modified credentials.
4. Execute the following command to set up the script to perform backups. It will create the backups folder with the expected permissions and ownership and exit.

➤ `sudo bash /home/[username]/backupdatabase.vxxx.sh --setup`
where [username] is the FRIEND user for the platform.

5. Execute the following command to generate SSH Keys and copy it to the remote destination location for password less, seamless file transfers.

➤ `sudo bash /home/[username]/backupdatabase.vxxx.sh --keyGen`

Follow the prompts to enter the remote destination IP/DNS address and remote username. The script will generate a SSH Key and copy it to the remote destination so that future file transfers can occur seamlessly with no user input.

6. Execute the command line to start a backup and upload it to a remote destination database appliance:

➤ `sudo bash /home/[username]/backupdatabase.vxxx.sh -b
/var/lib/pgsql/backups/portal.db.backup.gz -r
[remote.ip.dns.address] -p /var/lib/pgsql/backups/ -u username`

where [username] is the FRIEND user for the platform.

Here is a brief explanation of the command line arguments:

- b is the backup file path which must be within `/var/lib/pgsql/backups` folder with a `*.db.backup.gz` extension. Any other location or extension will be rejected.
- r is the remote destination database appliance IP or DNS address
- p is the remote file path which should be `/var/lib/pgsql/backups/`
- u is the FRIEND username on the remote appliance.

Restore database on the destination database appliance:

1. Open your SCP client to connect & log into the destination appliance running the database using the default FRIEND credentials on port 22. If these default credentials have been changed, please obtain, and use the modified credentials.
2. Upload the backup script from your local desktop folder to the `/home/[username]` folder (where [username] is the FRIEND user for the platform) on the appliance that runs the database i.e., if you run only a Hub database, please upload it to the Hub appliance or if you run a Hub and a Database appliance, please upload it to the Database appliance.
3. Open your SSH client to connect to the database appliance and log in using the default FRIEND credentials. If these default credentials have been changed, please obtain, and use the modified credentials.

4. Execute the following command to set up the script to perform restores. It will create the backups folder with the expected permissions and ownership and exit.

➤ `sudo bash /home/[username]/restoredatabase.vxxx.sh --setup`
where [username] is the FRIEND user for the platform.

5. Execute the command line to start a restore on a database appliance:

➤ `sudo bash /home/[username]/restoredatabase.vxxx.sh -b /var/lib/pgsql/backups/portal.db.backup.gz`

where [username] is the FRIEND user for the platform.

Here is a brief explanation of the command line arguments:

-b is the backup file path which must be within /var/lib/pgsql/backups folder with a *.db.backup.gz extension. Any other location or extension will be rejected.

Error Checking

As part of daily operations, there can be errors on execution of the backup and restore scripts. Liquidware recommends checking the log files for errors so that action can be taken sooner rather than later.

Backup Script

On the source production appliance that hosts the Stratusphere Database, the backup script creates a log output every time it executes a backup. It is available under /home/friend/backupdatabase.v66x.log or /home/[username]/backupdatabase.v66x.log where [username] is the FRIEND user for the platform.

Restore Script

On the destination production appliance that hosts the Stratusphere Database, the restore script creates a log output every time it executes a restore. It is available under /home/friend/restoredatabase.v66x.log or /home/[username]/restoredatabase.v66x.log where [username] is the FRIEND user for the platform.