Stratusphere™ Enabling Privacy Mode – Anonymizing User and Machine Names

Overview

Liquidware understands and respects privacy related issues and concerns of its users across the world. Whether it may be due to government regulations or some organizations ensuring privacy of its users, there are legitimate requirements for enabling the option to anonymize end user names and machine names within Stratusphere.

Liquidware offers the ability to totally anonymize end user names and machine names within Stratusphere. It must be noted that once this privacy mode is enabled, **each existing and new registered user name and machine within the Stratusphere Database will be anonymized in a single one-way hash. The conversion is permanent and cannot be undone**. Privacy mode can be disabled; however, the user and machine names already anonymized stay anonymized permanently. Any user name and machine name registration received after disabling privacy mode will be stored in plain text and will not be hashed.

Using the privacy mode may make Stratusphere reporting harder to read and follow since instead of user names and machines names, the end user will only see randomized pieces of text representing users and machines.

Preparation

1. Procure any change controls required to make changes to the production Stratusphere Hub & Database appliances.
2. Acquire credentials of the '`friend`' and '`root`' users to access the console of the Stratusphere Hub, Database, and Collector appliances.
3. Procure access to the local console of the Stratusphere Hub, Database, and Collector Appliances depending on the hypervisor on which the Hub is housed. Alternatively, PuTTY can also be used to access the console of the Hub, Database, and Collector provided SSH (TCP/22) access is allowed to the appliances.

Instructions to Enable Privacy Mode

> ***Once Privacy mode is enabled the user and machine names already anonymized stay anonymized permanently even if Privacy mode is disabled at a later date.***

1. Using an SSH client like PuTTY, log into the Stratusphere Hub console using credentials for the **friend** user. Then use credentials for the **root** user to switch to the root using the 'su -' command. Unless changed, the default password for both users is '`sspassword`'.
2. Execute the following command to invoke a limited shell prompt:
   ```
   > /opt/tnt/bin/mgrconfig
   ```
3. On the new shell prompt, execute the following commands to anonymize user and/or machine names within the Stratusphere Database:
   ```
   > set system user privacy on
   ```

```
> set system machine privacy on
```

4. To save and quit enter the following commands:
```
> write
> quit
```
5. Enter **CTRL+D** twice to log out of root and friend SSH sessions and quit the SSH PuTTY client.

Please provide some time for Stratusphere to begin its anonymizing process. Once completed, please log into the Administration section of the Stratusphere Web UI and navigate to **Inventory > Machines** and **Inventory > Users** tabs to verify if the names have been anonymized.

Instructions to Disable Privacy Mode

1. Using an SSH client like PuTTY, log into the Stratusphere Hub console using credentials for the **friend** user. Then use credentials for the **root** user to switch to the root using the 'su -' command. Unless changed, the default password for both users is '`sspassword`'.
2. Execute the following command to invoke a limited shell prompt:
```
> /opt/tnt/bin/mgrconfig
```
3. On the new shell prompt, execute the following commands to anonymize user and/or machine names within the Stratusphere Database:
```
> set system user privacy off
> set system machine privacy off
```
4. To save and quit enter the following commands:
```
> write
> quit
```
5. Enter **CTRL+D** twice to log out of root and friend SSH sessions and quit the SSH PuTTY client.

All users and machines registering for the first time since disabling privacy mode will now show up as plain text and will not be hashed. Users and machines that were previously anonymized under Privacy mode will remain anonymized.