View for ClusterStor™ System Snapshot Analyzer (SSA) User Guide

(1.7.1)

S-3028

Contents

1 About the View for ClusterStor System Snapshot Analyzer (SSA) User Guide

The *View for ClusterStor™ System Snapshot Analyzer (SSA) User Guide (1.7.1) S-3028* describes how to download, install, and use release 1.7.1 of Cray® System Snapshot Analyzer (SSA) software.

The *View for ClusterStor™Installation and Configuration Guide (1.2.0) S-3025* includes procedures to install View for ClusterStor at a customer site.

Table 1. Record of Revision

Publication Title	Date	Updates
View for ClusterStor™ System Snapshot Analyzer (SSA) User Guide (1.7.1) S-3028	12/7/2018	Release 1.7.1

Scope and Audience

Procedures should be performed by trained Cray system administrators or service providers familiar with ClusterStor software administration.

Typographic Conventions

`Monospace`	Indicates program code, reserved words, library functions, command-line prompts, screen output, file/path names, and other software constructs.
`Monospaced Bold`	Indicates commands that must be entered on a command line or in response to an interactive prompt.
`Oblique` or *`Italics`*	Indicates user-supplied values in commands or syntax definitions.
Proportional Bold	Indicates a **GUI Window**, **GUI element**, cascading menu (**Ctrl**→**Alt**→**Delete**), or key strokes (press **Enter**).
\ (backslash)	At the end of a command line, indicates the Linux® shell line continuation character (lines joined by a backslash are parsed as a single line).

Related Resources

- *Cray SSA White Paper*
- *Cray Customer Support*

Trademarks

The following are trademarks of Cray Inc. and are registered in the United States and other countries: CRAY and design, SONEXION, Urika-GX, and YARCDATA. The following are trademarks of Cray Inc.: APPRENTICE2, CHAPEL, CLUSTER CONNECT, ClusterStor, CRAYDOC, CRAYPAT, CRAYPORT, DATAWARP, ECOPHLEX,

2 SSA Introduction

Cray system snapshot analyzer (SSA) software is support analytics technology that securely collects, analyzes, and uploads (if upload is enabled) product health, configuration, or triage information about a View for ClusterStor system to Cray service. After being captured and uploaded by SSA, the data is analyzed using a sophisticated analytics platform to detect and enumerate changes over time, detect changes in the health state of various aspects of a system, or process triage information to assist with case resolution. Through automation, SSA improves the overall customer experience by reducing the manual effort and time required to report and resolve support issues.

The SSA *shepherd* is the client software that manages the collection, first-level analysis, and secure transport of support telemetry information back to Cray.

For additional information and references on SSA, please visit *www.cray.com/support*. For details on how to activate an SSA account and download SSA software, refer to Cray *SFDC Article 6765*, *Getting Started with the Cray System Snapshot Analyzer (SSA)*.

Request Support for SSA

To request support, contact a Cray support representative or file a service case against the SSA component. The option to submit a request for enhancement (RFE) or defect report (bug) against SSA is also available. Feedback and suggestions are valued and welcomed.

3 Configure SSA for View for ClusterStor

In View for ClusterStor™, the SSA shepherd software is installed on the site's system. By default, only the SSA collection feature is enabled. A CrayPort account is required to activate an SSA account. SSA account activation is required in order to obtain authentication credentials for use during the configuration of SSA for snapshot upload to Cray.

Visit *https://crayport.cray.com* if the customer site has active support entitlements and would like to register for CrayPort accounts.

Shepherd Overview

The SSA shepherd operates in three progressive stages—collect, snapshot, and upload.

Collect Stage The collect stage is responsible for utilizing plugins to perform collection and analysis of system information, and to prepare for subsequent stages.

Snapshot Stage The snapshot stage searches for collections that have not been previously processed. It encodes them into a network friendly format in preparation for upload to Cray®.

Upload Stage The upload stage then takes any snapshots that have not been uploaded and attempts to upload them to Cray for further analysis and processing.

The upload takes place over a secure network connection, using transport layer security (TLS), and is further authenticated using credentials from customer SSA accounts.

The shepherd uses a configurable purge policy to remove older collections or snapshots and is either invoked on-demand or automatically via `cron`.

The supported run configurations for the shepherd for View for ClusterStor systems are covered in *Collect and Upload a Snapshot* on page 9.

3.1 SSA Prerequisites

SSA Upload Account Activation

The activation of an SSA account in CrayPort is required in order to obtain the organization name and passphrase to use in the configuration of SSA for the upload of snapshot information to Cray®.

Network Connectivity

The shepherd application only initiates an outbound network connection—over TCP/IP (version 4) TCP port 443 —to the network host `ssa.cray.com`. Cray does not initiate an inbound connection to the customer network/

system. The outbound network session is established only long enough to submit a snapshot of information to Cray. Then it terminates.

To communicate with the Cray upload system, outbound connectivity must be provided from the user site as described. Optionally, a local network proxy (HTTP, SOCKS) can be utilized through features in the shepherd application. For additional details about how to configure a proxy, refer to the comments in the `/etc/sma-data/ssa/shepherd.conf` file that is installed on the View server.

3.2 Edit the View for ClusterStor Shepherd Configuration File

Prerequisites

Prerequisites

This procedure must be performed as the `root` user.

About this task

About this task

The View for ClusterStor shepherd uses a single configuration file, `/etc/sma-data/ssa/shepherd.conf`. The configuration file is structured into sections and contained within square brackets, for example `[control]`. Each section and each of its related parameters contain a header of descriptive configuration information. Sections may contain individual or groups of related parameters. Prior to running the shepherd, edit this file on the View for ClusterStor server.

The steps below describe commonly configured parameters for desired shepherd features.

Always make a backup copy of the shepherd configuration file (`shepherd.conf`) for reference.

Procedure

Procedure

1. Log in to the View for ClusterStor server as `root`.

2. Make a backup copy of the `shepherd.conf` file.

```
hostname# cd /etc/sma-data/ssa
hostname# cp -a shepherd.conf shepherd.conf.`date +%Y%m%d.%H%M`
```

3. Edit the `/etc/sma-data/ssa/shepherd.conf` file from the View for ClusterStor server.

4. Enable the shepherd master operation mode. This configuration setting allows all stages (collection, snapshot, upload) to be active.

   Set `master_enabled: true` in the `[control]` section.

```
[control]
master_enabled: true
```

5. Set system identification information in the `[sysinfo]` section.

a. Set the system serial number.

```
[sysinfo]
serial_num: 99999
```

b. Set the system type.

```
[sysinfo]
system_type: VIEWCLS
```

c. Set the system name.

```
[sysinfo]
system_name: prod
```

d. Set a short system description.

```
[sysinfo]
system_description: VIEWCLS PROD
```

6. Set upload information in the `[upload]` section.

> **IMPORTANT:** If SSA must be run in local mode, (no information is uploaded to Cray), see *Configure SSA for Local Only Mode* on page 15 and skip steps *6* on page 8 through *7* on page 8.

The `upload_server`, `upload_org`, and `upload_pw` parameters in the `[upload]` section must be set before using the snapshot or upload stages.

a. Set the organization, received when the SSA account was activated, that snapshots will be uploaded for.

```
[upload]
upload_org: cto01
```

b. Set the password received when the SSA account was activated.

```
[upload]
upload_pw: SuperSecretPassword
```

These parameters must be set for a successful authentication and upload of SSA information to Cray.

7. Make one of the following modifications in the `[upload]` section.

a. Optional: Set the `upload_server` parameter to the IP address of the upload server, if not using DNS and if a manually configured local resolution method is not desired.

```
[upload]
upload_server: 136.162.62.191
```

> **NOTE:** The upload system uses, at the time of this writing, a single IP address, `136.162.62.191`. This IP address should resolve via a DNS `PTR` reference to an `A` record ending in `.cray.com`. Any changes in SSA upload addressing will be communicated directly to customers by Cray.

Also, ensure that `verify_x509_host` is set to `false`.

```
[upload]
verify_x509_host: false
```

b. Optional: Set an additional X.509 (SSL/TLS) certificate validation option, if using DNS or a local resolution method (e.g., `/etc/hosts`).

```
[upload]
verify_x509_host: true
```

This enables additional protection within the shepherd to validate that the subject name in the X.509 SSL/TLS certificate matches that of the server (ssa.cray.com), allows resolution of the DNS name ssa.cray.com, adds a small amount of security to the upload process, and should be enabled if using a suitable resolution method. The certificate chain for the SSA upload system is maintained locally within the shepherd application (isolated from other certificate stores on the system). The CA bundle file is located in `/opt/cray/ssa/default/etc/ssl/ssa.pem`.

8. Save the file and exit.

After the configuration file is saved (with `master_enabled: true`) the `cron` schedule for the shepherd will be activated.

9. Restart SMA:

```
hostname# systemctl restart sma
```

10. Validate the configuration.

```
hostname# /root/sma-sos/ssacli --check_conf
[stdout] Configuration File and CLI Options Valid.
```

3.3 Collect and Upload a Snapshot

About this task

About this task

This procedure describes steps to collect and upload a snapshot using SSA shepherd.

SSA terminology:

Run Set Each (shepherd) plugin is associated with zero or more plugin run sets. A run set is an alpha-numeric, textual label for a configuration that the shepherd uses to select plugins for execution. If `ssacli` is not invoked with `--runset` options, the default run set is `default`. Plugins can, and often are, associated with multiple plugin run sets.

Output Channel Every shepherd collection and related snapshot is associated with exactly one output channel (channel). A channel is an alpha-numeric label. If `ssacli` is not invoked with the `--channel` option, the default channel is `default`. Channels allow information collected and reported by SSA to be categorized by use.

Procedure

Procedure

1. Execute a collection for the `default` run set and channel.

   The execution time can take anywhere from 60s to several minutes.

```
hostname# /root/sma-sos/ssacli --collect
[stdout] UI master_control status is (enabled) [no control file created]
[stdout] MASTER CONTROLS -> (M:True, C:True, S:True, U:True)
[stdout] UI CONTROLS -> (C:True, S:False, U:False)
[stdout] Shepherd Session: 1538310933
[stdout] Exclusive run: Lock file created @ /root/ssa-shepherd/var/opt/cray/ssa/lock/
ssa.lock_channel-default_device-ssa_WB_notserialized
[stdout] COLLECT stage start
[stdout] PLOAD: 1 plugin source modules loaded
[stdout] Collection Session: '1538310933'
[stdout] Collection Directory: '/etc/sma-data/ssa/sos/var/opt/cray/ssa/collection/
ssa_WB_notserialized/default/1538310933'
[stdout] Collection Channel: 'default'
[stdout] Run Sets: '['default']'
[stdout] Explicit Plugins: 'None'
[stdout] ** Entering run-level 1 **
[stdout] Plugin 'sma.healthcheck.plugin' started
[stdout] Plugin 'sma.healthcheck.plugin' stopped, return 0, time 76.18
[stdout] 38020.0 raw bytes collected via directives.
[stdout] no collection directories meet purge requirements
[stdout] COLLECT stage stop (normally)
[stdout] Collection output directory @ /etc/sma-data/ssa/sos/var/opt/cray/ssa/collection/
ssa_WB_notserialized/default/1538310933
[stdout] shepherd session stop successfully
[stdout] run took 76.22 seconds
```

   If the `COLLECT` stage stops either normally or with survivable exception, the collection process was successful. The shepherd creates a text report named `sma_healthcheck.txt` in the collection output directory located in:

```
/etc/sma-data/ssa/var/opt/cray/ssa/collection/< collection_device>/default/<timestamp>
```

   This report provides a high-level summary of the collection, including:

   - Information on the shepherd
   - Amount of storage consumed by the collection
   - The status of health checks the shepherd performed during the collection
   - We collect the following health information:
     - Build version
     - Install date
     - Email notification setting
     - Retention policy setting
     - System uptime
     - Containers uptime
     - CPU and memory usage. Memory limits of containers
     - Container logs size
     - Creation dates
     - Basic container status
     - Confirmation that GUI is accessible
     - CPU and memory usage of the containers

- ○ `mpstat` information
- ○ `pidstat` information
- ○ Top CPU information of the containers
- ○ Disk space usage
- ○ Count of the number of jobs in the database
- ○ `grep` of common errors in the miscellaneous container log files
- ○ Confirmation that all streaming processes are running
- ○ Check of Elasticsearch JVM HEAP usage
- ○ A look for CRITICAL alarms

This report can be useful to local operators in reviewing system status and high-level configuration. Survivable exceptions are part of the shepherd design. Individual plugins can fail in controlled ways, report these failures, and continue operation.

2. Execute a snapshot for the `default` run set and channel.

```
hostname# /root/sma-sos/ssacli --snapshot
[stdout] UI master_control status is (enabled) [no control file created]
[stdout] MASTER CONTROLS -> (M:True, C:True, S:True, U:True)
[stdout] UI CONTROLS -> (C:False, S:True, U:False)
[stdout] Shepherd Session: 1538311533
[stdout] Exclusive run: Lock file created @ /root/ssa-shepherd/var/opt/cray/ssa/lock/
ssa.lock_channel-default_device-ssa_WB_notserialized
[stdout] Starting SNAPSHOT stage
[stdout] Added '/etc/sma-data/ssa/sos/var/opt/cray/ssa/collection/ssa_WB_notserialized/default/
1538310933' to snapshot source list
[stdout] Est 57098 bytes needed to snapshot, based on raw storage of 1 collection(s)
[stdout] Snapshot encoding dir created at '/etc/sma-data/ssa/sos/var/opt/cray/ssa/snapshot/default/
isodx/cqat01/Linux/out/ssa_WB_notserialized/1538310933'
[stdout] no snapshot directories meet purge requirements
[stdout] Stopping SNAPSHOT stage normally
[stdout] shepherd session stop successfully
[stdout] run took 0.03 seconds
```

The `SNAPSHOT` stage should complete normally. Report other status messages to Cray support.

3. Invoke an upload of the `default` run set and channel.

```
hostname# /root/sma-sos/ssacli --upload
[stdout] UI master_control status is (enabled) [no control file created]
[stdout] MASTER CONTROLS -> (M:True, C:True, S:True, U:True)
[stdout] UI CONTROLS -> (C:False, S:False, U:True)
[stdout] Shepherd Session: 1538311787
[stdout] Exclusive run: Lock file created @ /root/ssa-shepherd/var/opt/cray/ssa/lock/
ssa.lock_channel-default_device-ssa_WB_notserialized
[stdout] Starting UPLOAD stage
[stdout] Upload Organization: cqat01
[stdout] Upload Server: 172.30.88.231
[stdout] Upload Device: ssa_WB_notserialized
[stdout] --
[stdout] Upload Statistics: 2018-09-30T12:49:48.267778UTC
[stdout] total size: 0, transferred: 0, progress: 0%
[stdout] elapsed time: --:--:--, remaining time (est): --:--:--
[stdout] speed: 0/s, avg speed: 0/s
[stdout] --
[stdout] Upload Statistics: 2018-09-30T12:49:49.268319UTC
[stdout] total size: 19175, transferred: 19175, progress: 100%
[stdout] elapsed time: 0:00:01, remaining time (est): --:--:--
[stdout] speed: 18743/s, avg speed: 18728/s
[stdout] --
[stdout] Upload transfer complete, waiting on server snapshot receipt
[stdout] Stopping UPLOAD stage normally
[stdout] shepherd session stop successfully
[stdout] run took 15.71 seconds
```

The `UPLOAD` stage should complete successfully. If the stage does not complete successfully, ensure the connectivity requirement has been met. Then report the issue to Cray support.

If the process above completes successfully, the first snapshot of the system support information is uploaded to Cray.

> **NOTE:** Cray recommends that the `triage` step be completed on an initial install of SSA to make sure there are no issues when collecting a triage snapshot.

4. Collect a triage bundle if there is a more serious issue with SMA. Repeat steps 1 through 3 for the `triage` run set and channel. Add `--scenario=triage` to each of the `ssacli` command lines for `--collect`, `--snapshot`, and `--upload`.

   ```
   hostname# /root/sma-sos/ssacli --runset=triage --channel=triage
   ```

4 Common Administrative Tasks

4.1 Enable or Disable SSA

Prerequisites

Prerequisites

System snapshot analyzer (SSA) is installed on the View for ClusterStor server.

About this task

About this task

> **IMPORTANT:** Disable SSA prior to performing system maintenance to prevent erroneous health reports from being sent to Cray®. Disabling SSA does not halt existing ssacli sessions but will prevent new sessions from starting. After maintenance is complete, enable SSA for system monitoring and reporting.

To automate control changes based on booted system state, administrators should integrate status information and enable/disable functionality into system boot control scripts. After maintenance operations are complete, enable SSA on the View for ClusterStor server.

When possible, Cray recommends that SSA be enabled and disabled using the ssacli command, instead of making modifications to the master_enabled control setting in the shepherd.conf file. Make sure the master_enabled setting in the shepherd.conf file is set to true, then use the ssacli command to enable or disable SSA from the command line.

> **NOTE:** These settings will not be preserved over systemctl restarts of SMA. If these settings need to be preserved over SMA restarts, it may be necessary to modify the master_enabled control setting in the shepherd.conf file.

Procedure

Procedure

1. Log in to the View for ClusterStor server as root.

2. Disable SSA.

```
hostname# /root/sma-sos/ssacli --master_control disable
[stdout] UI master_control initial state set to (disabled)
```

3. Enable SSA.

```
hostname# /root/sma-sos/ssacli --master_control enable
[stdout] UI master_control initial state set to (enabled)
```

4. Check status.

```
hostname# /root/sma-sos/ssacli --master_control status
[stdout] UI master_control status is (enabled)
```

4.2 Upload On-demand Snapshots to Cray

Prerequisites

Prerequisites

System snapshot analyzer (SSA) is installed on the View for ClusterStor server.

About this task

About this task

Cray ®service may request a site to upload a configuration baseline snapshot or triage snapshot specifying an SFDC case number. SFDC case `100000` is used in this example.

Procedure

Procedure

1. Log in to the View for ClusterStor server as `root`.

2. Upload an on-demand snapshot to Cray.

```
hostname# /root/sma-sos/ssacli
```

3. Upload a triage snapshot to Cray and substitute the case number(s) associated with the service request(s) on the command line.

```
hostname# /root/sma-sos/ssacli --ref 'sfdc:100000' --runset=triage
--channel=triage
```

4.3 Control Shepherd Verbosity and Debug Behavior

The `STDOUT` verbosity of the console messages from shepherd can be controlled using two CLI flags: `--quiet` and `--debug`. The `--quiet` option displays errors only to `STDERR` if they occur (including survivable errors). The `--debug` setting is highly verbose.

The location of the shepherd log files is defined in the `[sysconf]` section of the `shepherd.conf` file with the `log_dir` setting.

4.4 Configure SSA for Local Only Mode

Prerequisites

Prerequisites

System snapshot analyzer (SSA) is installed on the View for ClusterStor server.

About this task

About this task

There may be a requirement to run SSA in local only mode (information is not uploaded to Cray®). Use this procedure to enable SSA to run in local only mode.

> **IMPORTANT:** When SSA is run in local mode, no information is uploaded to Cray.

Procedure

Procedure

1. Log in to the View for ClusterStor server as `root`.
2. Edit the `/etc/sma-data/ssa/shepherd.conf` file.
3. In the `[control]` section, change the `snapshot_enabled` setting to `false`.
4. Change the `upload_enabled` setting to `false`.
5. Comment out the `upload_server` setting in the `[upload]` section.

   Type a pound sign (`#`) as the first character of the line to comment out that setting.

   ```
   #upload_server: ssa.cray.com
   ```
6. Comment out the `upload_org` setting.
7. Comment out the `upload_pw` setting.
8. Save the `/etc/sma-data/ssa/shepherd.conf` file.
9. Restart SMA.

   ```
   hostname# systemctl restart sma
   ```
10. Validate the configuration.

    ```
    hostname#  /root/sma-sos/ssacli --check_conf
    [stdout] Configuration File and CLI Options Valid.
    ```

4.5 Locate Collection and Snapshot Repositories

View for ClusterStor SSA 1.7.1 shepherd collection and snapshot repository locations are defined in the `/etc/sma-data/ssa/shepherd.conf` file on the View for ClusterStor server.

- The `[collection]` section `collection_dir` parameter defines the path name for the collection repository.
- The `[snapshot]` section `snapshot_dir` parameter defines the path name for the snapshot repository.

⚠ **CAUTION:** Manual modifications to the contents of either of these directories is not supported and can lead to unpredictable shepherd operation. Do not modify the contents of these directories unless instructed to do so by Cray Support.