XC™ Series System Snapshot Analyzer (SSA) User Guide

(1.7.0)

S-2543

Contents

1 About the XC Series SSA User Guide

The *XC™ Series System Snapshot Analyzer (SSA) User Guide* (1.7.0) S-2543 describes how to download, install, and use the SSA software.

Table 1. Revisions to this Publication

Publication Title	Date	Updates
XC™ Series System Snapshot Analyzer (SSA) User Guide (1.7.0) S-2543	July 2018	Supports SSA release 1.7.0.
XC™ Series System Snapshot Analyzer (SSA) User Guide (1.6.5) S-2543	February 2018	Supports SSA release 1.6.5.
XC™ Series System Snapshot Analyzer (SSA) User Guide (1.6.4) S-2543	December 2017	Supports SSA release 1.6.4.
XC™ Series System Snapshot Analyzer (SSA) User Guide (1.6.1) S-2543	October 2017	Supports SSA release 1.6.1.
XC™ Series System Snapshot Analyzer (SSA) User Guide (1.6.0) S-2543	September 2017	Supports SSA release 1.6.0.
XC™ Series System Snapshot Analyzer (SSA) User Guide (1.5.0) S-2543	June 1017	Supports SSA release 1.5.0.
XC™ Series System Snapshot Analyzer (SSA) User Guide (1.4.0) S-2543	March 2017	Supports SSA release 1.4.0.
XC™ Series System Snapshot Analyzer (SSA) User Guide (1.3.0) S-2543	December 2016	Supports SSA release 1.3.0.
XC™ Series System Snapshot Analyzer (SSA) User Guide (SSA 1.2.2) S-2543	September 2016	Supports SSA release 1.2.2.
XC™ Series System Snapshot Analyzer (SSA) User Guide (SSA 1.2.1) S-2543	July 2016	Supports SSA release 1.2.1.
System Snapshot Analyzer (SSA) User Guide	September 2015	Supports revised SSA release.
System Snapshot Analyzer (SSA) User Guide	July 2015	Supports initial SSA release.

Typographic Conventions

`Monospace` Indicates program code, reserved words, library functions, command-line prompts, screen output, file/path names, key strokes (e.g., `Enter` and `Alt-Ctrl-F`), 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 graphical user interface window or element.
`\` (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). Do not type anything after the backslash or the continuation feature will not work correctly.

Scope and Audience

The intended audience are experienced system administrators and Cray service personnel.

Related Resources

- Refer to Cray Field Notice FN 6122 for more information about SSA client release history
- Release notes for SSA are available on *CrayPort*
- A `README` file for SSA is included in `/opt/cray/ssa/default/share/doc/README.plugin-doc` that describes what each plugin in the release was designed to do (this file is also available on *CrayPort*)
- The `ssacli man` page (requires a `module load cray-ssa` beforehand on HPC platforms)
- *Cray SSA White Paper*
- *www.cray.com/support*

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 XC Series system to Cray service. After 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 a 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 XC Series

Download the SSA shepherd software by following guidance in Cray *SFDC Article 6765*, *Getting Started with the Cray System Snapshot Analyzer (SSA)*. Customers can access Article 6765 at *CrayPort*.

A CrayPort account is required to download software and activate a 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 you have active support entitlements and would like to register for CrayPort accounts.

Shepherd Overview

SSA shepherd software is delivered in two packages. One contains the shepherd command line interface (`ssacli`) and libraries. The other contains plugins for the specific Cray platform (Cray XE, Cray XC, ClusterStor/Sonexion, or CS-Storm). These packages are revision matched, with the plugin package dependent on the base shepherd software.

The 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 which 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 which 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 XC Series systems are covered in *Collect and Upload a Snapshot* on page 13.

3.1 SSA Prerequisites

SSA Upload Account Activation

The activation of a 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 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 `shepherd.conf` file distributed with the shepherd.

Configuration of the `sudo` Utility

The shepherd leverages the functionality provided by the `sudo` utility to drop privileges and provide an audit trail of application activity. The `root` user must be able to execute any command, as any user, on installation nodes via `sudo`. The `root` user must not be prompted for a password to execute `sudo` commands. In addition, the `requiretty` setting must not be enabled because `sudo` will not allow the execution of any scheduled jobs via SSA (e.g. those not run directly on a real TTY by an interactive user).

SSH Authentication

The `root` user must be allowed passwordless SSH access from the SMW to the boot node. The `root` user must also be allowed passwordless SSH access from the boot node to the SDB node.

3.2 Install the SSA RPM Packages

Prerequisites

This procedure must be performed as the `root` user on the XC Series SMW.

About this task

This procedure installs the base SSA shepherd application and system-specific plugins for systems.

Time Required: Approximately 30 minutes. SSA RPMs can be installed during customer operations.

Packages for XC Series are used in the examples for illustration only. Always download the latest shepherd software specific to the system.

If installing on a high availability (HA) configuration, first perform the RPM installation steps on the active SMW, then on the passive SMW. The SSA software is not synchronized between each SMW. The configuration and

SSA client (shepherd) versions should be kept consistent between each SMW. HA is only supported on XC series systems.

Test the installation of the RPM packages to check for missing dependencies. The shepherd is designed to operate in concert with Cray platforms there should be no missing dependencies. If missing dependencies are encountered, please contact Cray support.

Procedure

1. Log in to the SMW as `root`.

2. If upgrading SSA, disable SSA using *Enable or Disable SSA* on page 18. For HA configurations, the control must set on both nodes in the HA pair.

3. Install the RPM packages.

   ```
   smw# rpm -ivh cray-ssa-shepherd-1.7.0-0.x86_64.rpm \
   cray-ssa-shepherd-ari-plugins-1.7.0-0.x86_64.rpm

   Preparing...                     ########################################### [100%]
      1:cray-ssa-shepherd           ########################################### [50%]

   Setting Alternatives
   --------------------
      2:cray-ssa-shepherd-ari########################################### [100%]
   ```

   Installation of the RPMs yields messages associated with the `alternatives` software. For additional information about how (if the RPM for the platform uses `alternatives`) to manage the active version of shepherd, refer to the `man` page for `update-alternatives` and *Specify a Different Version of SSA* on page 20.

4. Repeat (if installing on an HA configuration) steps 1 through 3 above on the passive SMW.

5. If a previous SSA version is installed, and the `cray-ssa` environment is loaded, unload and reload the `cray-ssa` module to invoke the new version.

   ```
   smw# module unload cray-ssa
   smw# module load cray-ssa
   ```

3.3 Edit the XC Series Shepherd Configuration File

Prerequisites

This procedure must be performed as the `root` user on the XC Series SMW.

About this task

The shepherd uses a single configuration file, `/opt/cray/ssa/default/etc/shepherd.conf`. The configuration file is structured into sections and contained within square brackets (`[control]`). Each section and each of its related parameters includes configuration information. Sections may contain individual or groups of related parameters.

The steps below describe commonly configured parameters for desired shepherd features. Prior to running the shepherd, edit this file on the SMW. If high-availability (HA) is configured on the system, the additional steps at the end of the procedure will need to be completed for installation on the secondary SMW.

Always make a backup copy of the shepherd configuration file for reference.

> **IMPORTANT:** Review the SSA release notes for versions that have compatible configuration files. If the version being installed is compatible with the previous version, simply make a backup copy of the new version's configuration file and overwrite it with the existing shepherd configuration file.

Procedure

1. Login to the SMW as `root`.

- If using an existing compatible configuration file, copy the file to the appropriate location as shown and proceed to step 8.

  ```
  smw#  cd /opt/cray/ssa/default/etc
  smw#  cp -a shepherd.conf shepherd.conf-dist
  smw#  cp -a /opt/cray/ssa/ssa_version/etc/shepherd.conf .
  ```

- If this is an initial installation, proceed to step 2.

2. From the primary SMW, edit `/opt/cray/ssa/default/etc/shepherd.conf` file.

3. 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
```

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

a. Set the serial number of the system.

```
[sysinfo]
serial_num: 9999
```

b. Set the system type.

```
[sysinfo]
system_type: XC40
```

c. Set the system name.

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

d. Set a short system description.

```
[sysinfo]
system_description: XC40 PROD
```

5. 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 22 and skip steps 5 through 7.

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.

6. Optional: Set, in the `[upload]` section, the upload server (`upload_server`) address to an IP address. Or, if using IP name resolution, set an additional X.509 (SSL/TLS) certificate validation option.

   - If using DNS or a local resolution method (e.g., `/etc/hosts`), set `verify_x509_host` to `true`.

     ```
     [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`.

   - If not using DNS (and if a manually configured local resolution method is not desired), set the upload server to an IP address.

     The upload system uses 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.

     1. Set `upload_server` to IP address (using the documented IP above).

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

     2. Set `verify_x509_host` to `false`.

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

7. Save the file and exit.

   After the configuration file is saved (with `master_enabled: true`), the `cron` schedule for the shepherd is activated. The `cron` schedule is located in `/opt/cray/ssa/default/etc/cray-ssa` and is symbolically linked to `/etc/cron.d/cray-ssa`.

8. Load the environment module:

   ```
   smw# module load cray-ssa
   ```

9. Validate the configuration:

   ```
   smw# ssacli --check_conf
   [stdout] Configuration File and CLI Options Valid.
   ```

10. Set the SMW HA node ID on each node in the HA cluster. (Skip this step if not installing to SMW HA).

    a. Load environment module on the active HA node.

    ```
    smwha_n1# module load cray-ssa
    ```

    b. Set HA node ID.

    ```
    smwha_n1# ssacli --set_smw_ha_nodeid n0
    [stdout] ssacli-w:main:294: SMW HA node ID set to 'n0', exiting 0
    ```

    c. Log in to passive HA node.

    ```
    smwha_n1# ssh smwha_n2
    Last login: Sun Oct 1 12:44:12 2017
    ```

    d. Load environment module.

    ```
    smwha_n2# module load cray-ssa
    ```

    e. Set HA node ID.

    ```
    smwha_n2# ssacli --set_smw_ha_nodeid n1
    [stdout] ssacli-w:main:294: SMW HA node ID set to 'n1', exiting 0
    ```

11. Copy the configuration from the active to the passive SMW and validate the configuration on the passive SMW. (Skip this step if not installing HA.)

    a. Use `scp` to copy configuration file.

    ```
    smwha_n1# scp -p /opt/cray/ssa/default/etc/shepherd.conf \
    smwha_n2:/opt/cray/ssa/default/etc/shepherd.conf
    100%   13KB 13.5KB/s  00:00
    ```

    b. Log in to passive HA node.

    ```
    smwha_n1# ssh smwha_n2
    Last login: Sun Oct 2 12:44:12 2017
    ```

    c. Load the environment module.

    ```
    smwha_n2# module load cray-ssa
    ```

    d. Validate the configuration.

    ```
    smwha_n2# ssacli --check_conf
    [stdout] Configuration File and CLI Options Valid.
    ```

12. Enable SSA on the SMW node(s) if previously disabled using `ssacli`.

3.4 Configure CLE Boot and Shutdown for SSA

Prerequisites

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

About this task

SSA collects and processes data against a booted XC Series system. Normally, SSA should be enabled following a normal system boot, and disabled prior to a normal system shutdown. This procedure configures `sudo` and CLE auto boot files to control SSA while booting or shutting down an XC Series system.

Procedure

1. Add the following lines to the `/etc/sudoers` file to enable `crayadm` to execute `ssacli` as `root`. Use the `visudo` utility to edit the `/etc/sudoers` file.

```
crayadm ALL = (root) NOPASSWD: /opt/cray/ssa/default/bin/ssacli -q --master_control disable
crayadm ALL = (root) NOPASSWD: /opt/cray/ssa/default/bin/ssacli -q --master_control enable
crayadm ALL = (root) NOPASSWD: /opt/cray/ssa/default/bin/ssacli -q --master_control status
crayadm ALL = (root) NOPASSWD: /opt/cray/ssa/default/bin/ssacli --master_control disable
crayadm ALL = (root) NOPASSWD: /opt/cray/ssa/default/bin/ssacli --master_control enable
crayadm ALL = (root) NOPASSWD: /opt/cray/ssa/default/bin/ssacli --master_control status
```

2. Edit the boot or shutdown boot automation files to include the following directives:

   To enable SSA, enter this line as one of the final steps after system is booted:

```
lappend actions { crms_exec "/usr/bin/sudo \
/opt/cray/ssa/default/bin/ssacli -q --master_control enable" }
```

   To disable SSA, enter this line as one of the first steps that occurs as part of the shutdown:

```
lappend actions { crms_exec "/usr/bin/sudo \
/opt/cray/ssa/default/bin/ssacli -q --master_control disable" }
```

4 Collect and Upload a Snapshot

Prerequisites

IMPORTANT: This procedure is not necessary if upgrading to a newer version of SSA software.

This procedure must be performed as the `root` user. The output examples in this section have been reduced for the sake of brevity. They will vary depending on the task being performed.

About this task

In version 1.7.0 of the SSA shepherd for XC Series systems, SMW and mainframe processing occurs separately. When `ssacli` is invoked, the stages selected will complete first for the SMW device and then for a mainframe device. Output with `ssacli_wrapper` prepended will indicate what aspect of the system SSA is processing. If running SMW HA, the active node performs the mainframe data collection.

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 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, or channel for short. 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.

Release 1.7.0 contains three run configurations, each targeting a different SSA use case. These run configurations are provided in the table.

Table 2. Supported XC Series Shepherd Run Configurations for SSA 1.7.0

Purpose	Run Set	Output Channel	Scheduled/On-Demand	Frequency
Baselining and detecting change in product configurations	`default`	`default`	Either	Once daily
Product health monitoring	`health`	`health`	Scheduled	Every 15 minutes
Product support bundle capture	`triage`	`triage`	On-demand	As requested

To observe behavior for the `default` run set and channel, perform each stage of the shepherd process separately and review the shepherd output on the system console.

IMPORTANT: This procedure is not necessary if upgrading to a newer version of SSA software.

Procedure

1. Log in to the SMW as `root`.

2. Load the `cray-ssa` environment module.

```
smw# module load cray-ssa
```

3. Execute a collection for the `default` run set and channel (this will take several minutes).

```
smw# ssacli --collect
[stdout] ssacli_wrapper:main:451: **************************************************
[stdout] ssacli_wrapper:main:452: [+] Start SMW processing
[stdout] ssacli_wrapper:main:453:    [-] added run set(s): ['default', 'device_smw_standalone']
[stdout] ssacli_wrapper:main:454:    [-] subsystem name:   smw
[stdout] ssacli_wrapper:main:455:    [-] subsystem part:   n0
[stdout] ssacli_wrapper:main:456: **************************************************
[stdout] MASTER CONTROLS -> (M:True, C:True, S:True, U:True)
[stdout] UI CONTROLS -> (C:True, S:False, U:False)
[stdout] Shepherd Session: 1467772466
[stdout] Exclusive run: Lock file created @ /var/opt/cray/ssa/lock/ssa.lock_channel-default_device-
prod-smw-n0_XC40_9999
[stdout] COLLECT stage start
[stdout] PLOAD: 47 plugin source modules loaded
[stdout] Collection Session:   '1467772466'
[stdout] Collection Directory: '/var/opt/cray/ssa/collection/prod-smw-n0_XC40_9999/default/
1467772466'
[stdout] Collection Channel:   'default'
[stdout] Run Sets:             '['default', 'device_smw_standalone']'
[stdout] Explicit Plugins:     'None'
...
[stdout] ** Entering run-level 10 **
[stdout] Plugin 'shepherd.encode.diagnostic' started
[stdout] Plugin 'shepherd.encode.diagnostic' stopped, return 0, time 85.18
[stdout] 34279331.0 raw bytes collected via directives.
[stdout] no collection directories meet purge requirements
[stdout] COLLECT stage stop (with survivable exception)
[stdout] Collection output directory @ /var/opt/cray/ssa/collection/prod-smw-n0_XC40_9999/default/
1467772466
[stdout] shepherd session stop successfully
[stdout] run took 288.91 seconds
[stdout] ssacli_wrapper:main:472: **
[stdout] ssacli_wrapper:main:473: [*] SMW invocation succeeded with '0'
[stdout] ssacli_wrapper:main:474: **
[stdout] ssacli_wrapper:main:494: **************************************************
[stdout] ssacli_wrapper:main:495: [+] Start Mainframe (p0) processing
[stdout] ssacli_wrapper:main:496:    [-] added run set(s): ['device_mainframe']
[stdout] ssacli_wrapper:main:497:    [-] subsystem name:   mainframe
[stdout] ssacli_wrapper:main:498:    [-] subsystem part:   p0
[stdout] ssacli_wrapper:main:499: **************************************************
[stdout] MASTER CONTROLS -> (M:True, C:True, S:True, U:True)
[stdout] UI CONTROLS -> (C:True, S:False, U:False)
[stdout] Shepherd Session: 1467772755
[stdout] Exclusive run: Lock file created @ /var/opt/cray/ssa/lock/ssa.lock_channel-default_device-
prod-mainframe-p0_XC40_9999
[stdout] COLLECT stage start
[stdout] PLOAD: 48 plugin source modules loaded
[stdout] Collection Session:   '1467772755'
[stdout] Collection Directory: '/var/opt/cray/ssa/collection/prod-mainframe-p0_XC40_9999/default/
1467772755'
[stdout] Collection Channel:   'default'
[stdout] Run Sets:             '['default', 'device_mainframe']'
[stdout] Explicit Plugins:     'None'
...
[stdout] ** Entering run-level 10 **
```

```
[stdout] Plugin 'shepherd.encode.diagnostic' started
[stdout] Plugin 'shepherd.encode.diagnostic' stopped, return 0, time 90.79
[stdout] 24100623.0 raw bytes collected via directives.
[stdout] no collection directories meet purge requirements
[stdout] COLLECT stage stop (normally)
[stdout] Collection output directory @ /var/opt/cray/ssa/collection/prod-mainframe-p0_XC40_9999/
default/1467772755
[stdout] shepherd session stop successfully
[stdout] run took 486.02 seconds
[stdout] ssacli_wrapper:main:511: **
[stdout] ssacli_wrapper:main:512: [*] Mainframe invocation succeeded with '0'
[stdout] ssacli_wrapper:main:513: **
```

If the `COLLECT` stage stops either normally or as stated with survivable exception, the collection process was successful. The shepherd creates a text report named `collection_report.txt` in the output directory displayed. The output directory is in the form:

```
/var/opt/cray/ssa/collection/collection_device/default/timestamp
```

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

- Information about the shepherd
- Storage space used by the collection
- Status of health checks performed during the collection
- Platform summary information
- A plugin execution summary trace

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

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

```
smw# ssacli --snapshot
[stdout] ssacli_wrapper:main:451: **************************************************
[stdout] ssacli_wrapper:main:452: [+] Start SMW processing
[stdout] ssacli_wrapper:main:453:    [-] added run set(s): ['default', 'device_smw_standalone']
[stdout] ssacli_wrapper:main:454:    [-] subsystem name:   smw
[stdout] ssacli_wrapper:main:455:    [-] subsystem part:   n0
[stdout] ssacli_wrapper:main:456: **************************************************
[stdout] MASTER CONTROLS -> (M:True, C:True, S:True, U:True)
[stdout] UI CONTROLS -> (C:False, S:True, U:False)
[stdout] Shepherd Session: 1467773299
[stdout] Exclusive run: Lock file created @ /var/opt/cray/ssa/lock/ssa.lock_channel-default_device-
prod-mainframe-p0_XC40_9999
[stdout] Starting SNAPSHOT stage
[stdout] Added '/var/opt/cray/ssa/collection/prod-smw-n0_XC40_9999/default/1467772466' to snapshot
source list
[stdout] Est 25196634 bytes needed to snapshot, based on raw storage of 1 collection(s)
[stdout] Snapshot encoding dir created at '/var/opt/cray/ssa/snapshot/default/isodx/cto01/Linux/out/
prod-smw-n0_XC40_9999/1467772466'
[stdout] no snapshot directories meet purge requirements
[stdout] Stopping SNAPSHOT stage normally
[stdout] shepherd session stop successfully
[stdout] run took 9.22 seconds
[stdout] ssacli_wrapper:main:472: **
[stdout] ssacli_wrapper:main:473: [*] SMW invocation succeeded with '0'
[stdout] ssacli_wrapper:main:474: **
[stdout] ssacli_wrapper:main:494: **************************************************
[stdout] ssacli_wrapper:main:495: [+] Start Mainframe (p0) processing
[stdout] ssacli_wrapper:main:496:    [-] added run set(s): ['default', 'device_mainframe']
[stdout] ssacli_wrapper:main:497:    [-] subsystem name:   mainframe
[stdout] ssacli_wrapper:main:498:    [-] subsystem part:   p0
[stdout] ssacli_wrapper:main:499: **************************************************
[stdout] MASTER CONTROLS -> (M:True, C:True, S:True, U:True)
[stdout] UI CONTROLS -> (C:False, S:True, U:False)
[stdout] Shepherd Session: 1467773309
[stdout] Exclusive run: Lock file created @ /var/opt/cray/ssa/lock/ssa.lock_channel-default_device-
prod-mainframe-p0_XC40_9999
```

```
[stdout] Starting SNAPSHOT stage
[stdout] Added '/var/opt/cray/ssa/collection/prod-mainframe-p0_XC40_9999/default/1467772755' to
snapshot source list
[stdout] Est 19806218 bytes needed to snapshot, based on raw storage of 1 collection(s)
[stdout] Snapshot encoding dir created at '/var/opt/cray/ssa/snapshot/default/isodx/cto01/Linux/out/
prod-mainframe-p0_XC40_9999/1467772755'
[stdout] no snapshot directories meet purge requirements
[stdout] Stopping SNAPSHOT stage normally
[stdout] shepherd session stop successfully
[stdout] run took 6.27 seconds
[stdout] ssacli_wrapper:main:511: **
[stdout] ssacli_wrapper:main:512: [*] Mainframe invocation succeeded with '0'
[stdout] ssacli_wrapper:main:513: **
```

The SNAPSHOT stage should complete normally. Please report any other status to Cray support.

5. Execute an upload for the default run set and channel.

```
smw# ssacli --upload
[stdout] ssacli_wrapper:main:451: **************************************************
[stdout] ssacli_wrapper:main:452: [+] Start SMW processing
[stdout] ssacli_wrapper:main:453:    [-] added run set(s): ['default', 'device_smw_standalone']
[stdout] ssacli_wrapper:main:454:    [-] subsystem name:   smw
[stdout] ssacli_wrapper:main:455:    [-] subsystem part:   n0
[stdout] ssacli_wrapper:main:456: **************************************************
[stdout] MASTER CONTROLS -> (M:True, C:True, S:True, U:True)
[stdout] UI CONTROLS -> (C:False, S:False, U:True)
[stdout] Shepherd Session: 1467773504
[stdout] Exclusive run: Lock file created @ /var/opt/cray/ssa/lock/ssa.lock_channel-default_device-
prod-smw-n0_XC40_9999
[stdout] Starting UPLOAD stage
[stdout] Upload Organization: cto01
[stdout] Upload Server: ssa.cray.com
[stdout] Upload Device: prod-smw-n0_XC40_9999
[stdout] Stopping UPLOAD stage normally
[stdout] shepherd session stop successfully
[stdout] run took 4.23 seconds
[stdout] ssacli_wrapper:main:472: **
[stdout] ssacli_wrapper:main:473: [*] SMW invocation succeeded with '0'
[stdout] ssacli_wrapper:main:474: **
[stdout] ssacli_wrapper:main:494: **************************************************
[stdout] ssacli_wrapper:main:495: [+] Start Mainframe (p0) processing
[stdout] ssacli_wrapper:main:496:    [-] added run set(s): ['default', 'device_mainframe']
[stdout] ssacli_wrapper:main:497:    [-] subsystem name:   mainframe
[stdout] ssacli_wrapper:main:498:    [-] subsystem part:   p0
[stdout] ssacli_wrapper:main:499: **************************************************
[stdout] MASTER CONTROLS -> (M:True, C:True, S:True, U:True)
[stdout] UI CONTROLS -> (C:False, S:False, U:True)
[stdout] Shepherd Session: 1467773509
[stdout] Exclusive run: Lock file created @ /var/opt/cray/ssa/lock/ssa.lock_channel-default_device-
prod-mainframe-p0_XC40_9999
[stdout] Starting UPLOAD stage
[stdout] Upload Organization: cto01
[stdout] Upload Server: ssa.cray.com
[stdout] Upload Device: prod-mainframe-p0_XC40_9999
[stdout] Stopping UPLOAD stage normally
[stdout] shepherd session stop successfully
[stdout] run took 4.23 seconds
[stdout] ssacli_wrapper:main:511: **
[stdout] ssacli_wrapper:main:512: [*] Mainframe invocation succeeded with '0'
[stdout] ssacli_wrapper:main:513: **
```

The UPLOAD stage should complete successfully. If the stage does not complete successfully, ensure the connectivity requirement and upload credientials are correct. 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.

6. Optional: If this is an initial install, repeat steps 3 through 5 above for the `triage` run set and channel. Add `--runset=triage` and `--channel=triage` to each of the `ssacli` command lines for `--collect`, `--snapshot`, and `--upload`.

7. Repeat steps 1 through 6 on passive node if SMW HA is used.

5 Common Administrative Tasks

5.1 Enable or Disable SSA

Prerequisites

System snapshot analyzer (SSA) is installed on the XC Series system SMW.

About this task

The ability to control SSA via `ssacli` was introduced in version 1.4.0. If a version prior to 1.4.0 is installed, then SSA must be enabled or disabled using the `shepherd.conf` configuration file.

Cray recommends that SSA be enabled and disabled using the `ssacli`, as opposed to 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` to enable or disable SSA from the command line.

> **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.

Procedure

1. Log in to the SMW as `root`.

2. Load the SSA environment module.

   ```
   smw# module load cray-ssa
   ```

3. Disable SSA.

   ```
   smw# ssacli --master_control disable
   [stdout] UI master_control initial state set to (disabled)
   ```

4. Enable SSA.

   ```
   smw# ssacli --master_control enable
   [stdout] UI master_control initial state set to (enabled)
   ```

5. Check status.

   ```
   smw# ssacli --master_control status
   [stdout] UI master_control status is (enabled)
   ```

5.2 Upload On-demand Snapshots to Cray

Prerequisites

System snapshot analyzer (SSA) is installed on the XC Series system SMW.

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

1. Log in to the SMW as `root`.

2. Make sure the SSA environment module is loaded.

   ```
   smw# module load cray-ssa
   ```

3. Upload and on-demand snapshot to Cray.

   ```
   smw# ssacli
   ```

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

   ```
   smw# ssacli –-ref ‘sfdc:100000’ --runset=triage --channel=triage
   ```

5.3 Enable crayadm User to Run SSA

Prerequisites

System snapshot analyzer (SSA) is installed on the XC Series system SMW.

About this task

XC Series system administrators may prefer to configure the SMW to run SSA as the `crayadm` user. This is not typical, nor required.

To allow `crayadm` user to run SSA 1.7.0 on XC Series systems,

Procedure

1. Log in to the SMW as `root`.

2. Make sure the SSA environment module is loaded.

```
smw# module load cray-ssa
```

3. Use the visudo utility to edit the /etc/sudoers file.

4. Add the following line to the /etc/sudoers file to enable crayadm to execute the ssacli as root without a password:

   ```
   crayadm ALL = (root) NOPASSWD: /opt/cray/ssa/default/bin/ssacli
   ```

   The crayadm user can now run SSA using the sudo ssacli command.

5.4 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.

5.5 Specify a Different Version of SSA

Prerequisites

System snapshot analyzer (SSA) is installed on the XC Series system SMW.

About this task

SSA uses the alternatives software to manage the active version when multiple versions are installed on XC Series systems. The SSA versions list shown in the procedure is for illustration only.

Procedure

1. Log in to the SMW as root.

2. Load the SSA environment module.

   ```
   smw# module load cray-ssa
   ```

3. To list the available versions for SSA.

   ```
   smw# update-alternatives --display cray-ssa
   cray-ssa - status is auto.
    link currently points to /opt/cray/ssa/1.6.4-0
   /opt/cray/ssa/1.1.0-3 - priority 001001000003
   /opt/cray/ssa/1.2.2-0 - priority 001002002000
   /opt/cray/ssa/1.3.0-3 - priority 001003000003
   /opt/cray/ssa/1.4.0-3 - priority 001004000003
   ```

```
/opt/cray/ssa/1.5.0-3 - priority 001005000003
/opt/cray/ssa/1.6.0-3 - priority 001006000003
/opt/cray/ssa/1.6.4-0 - priority 001006004000
Current `best' version is /opt/cray/ssa/1.6.4-0.
```

4. Specify a target version path.

```
smw# update-alternatives --set cray-ssa /opt/cray/ssa/version
Using '/opt/cray/ssa/version' to provide 'cray-ssa'.
```

5. Reload the SSA environment module.

```
smw# module unload cray-ssa
smw# module load cray-ssa
```

5.6 Specify the Latest Version of SSA Automatically

Prerequisites

System snapshot analyzer (SSA) is installed on the XC Series system SMW.

About this task

SSA uses the `alternatives` software to manage the active version when multiple versions are installed on XC Series systems. The SSA versions list shown in the procedure is for illustration only.

Procedure

1. Log in to the SMW as `root`.

2. Load the SSA environment module.

```
smw# module load cray-ssa
```

3. To list the available versions for SSA.

```
smw# update-alternatives --display cray-ssa
cray-ssa - status is auto.
 link currently points to /opt/cray/ssa/1.6.4-0
/opt/cray/ssa/1.1.0-3 - priority 001001000003
/opt/cray/ssa/1.2.2-0 - priority 001002002000
/opt/cray/ssa/1.3.0-3 - priority 001003000003
/opt/cray/ssa/1.4.0-3 - priority 001004000003
/opt/cray/ssa/1.5.0-3 - priority 001005000003
/opt/cray/ssa/1.6.0-3 - priority 001006000003
/opt/cray/ssa/1.6.4-0 - priority 001006004000
Current `best' version is /opt/cray/ssa/1.6.4-0.
```

4. To select the most recent SSA version automatically:

```
smw# update-alternatives --auto cray-ssa
cray-ssa - status is auto.
```

```
 link currently points to /opt/cray/ssa/1.6.4-0
/opt/cray/ssa/1.1.0-3 - priority 001001000003
/opt/cray/ssa/1.2.2-0 - priority 001002002000
/opt/cray/ssa/1.3.0-3 - priority 001003000003
/opt/cray/ssa/1.4.0-3 - priority 001004000003
/opt/cray/ssa/1.5.0-3 - priority 001005000003
/opt/cray/ssa/1.6.0-3 - priority 001006000003
/opt/cray/ssa/1.6.4-0 - priority 001006004000
Current `best' version is /opt/cray/ssa/1.6.4-0.
```

5. Reload the SSA environment module.

```
smw# module unload cray-ssa
smw# module load cray-ssa
```

5.7 Configure SSA for Local Only Mode

Prerequisites

System snapshot analyzer (SSA) is installed on the XC Series system SMW.

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

1. Log in to the SMW as `root`.

2. Unload the SSA environment module.

```
smw# module unload cray-ssa
```

3. Edit the `shepherd.conf` file.

4. In the `[control]` section, change the `snapshot_enabled` setting to `false`.

5. Change the `upload_enabled` setting to `false`.

6. 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
```

7. Comment out the `upload_org` setting.

8. Comment out the `upload_pw` setting.

9. Save the shepherd.conf file.

10. Load the cray-ssa environment module.

    ```
    smw# module load cray-ssa
    ```

11. Validate the configuration.

    ```
    smw#  ssacli --check_conf
    [stdout] Configuration File and CLI Options Valid.
    ```

5.8 Locate Collection and Snapshot Repositories

XC Series SSA 1.7.0 shepherd collection and snapshot repository locations are defined in the /opt/cray/ssa/default/etc/shepherd.conf file on the SMW.

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 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.