

Dell PowerStore

Service Scripts Guide

Version 4.1

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

Additional Resources.....	7
Chapter 1: Introduction.....	8
Audience.....	8
Running the service scripts.....	8
Chapter 2: Service Commands.....	9
Shut down and reboot an appliance (svc_appliance).....	10
Reboot an appliance (svc_appliance reboot).....	11
Shut down an appliance (svc_appliance shutdown).....	11
Provision an appliance (svc_appliance_provisioning).....	12
Capture array configuration data (svc_arrayconfig).....	12
Get a system snapshot with the svc_arrayconfig service script.....	13
Capture current cluster configuration (svc_arrayconfig run).....	14
Manage CAC and PIV (svc_cac_piv_mgmt).....	15
Make space on the root partition (svc_cleanup).....	16
Clear the DIMM state value on a specific node (svc_clear_dimm_ce_state).....	17
Clear firmware update (svc_clear_fw_update_alert).....	17
Shut down a SAN cluster (svc_cluster).....	18
Diagnose a create cluster failure (svc_cluster_diag).....	19
Cluster management (svc_cluster_management).....	21
Remove and reattach an appliance.....	23
Enable or disable counter collection (svc_cnt).....	23
Enable counter collection (svc_cnt enable).....	24
Disable counter collection (svc_cnt disable).....	24
See the collection status (svc_cnt status).....	25
Restart the collection service (svc_cnt restart).....	25
Enable the 1-second collection profile (svc_cnt performance).....	25
Disable the 1-second collection profile (svc_cnt performance_disable).....	26
Configure new SLICs (svc_commit_slic).....	26
Show the security compliance state (svc_compliance_mode).....	28
Check status of or restart container (svc_container_mgmt).....	29
Support materials (svc_dc).....	29
Generate a support materials bundle (svc_dc run).....	30
Delete a support materials bundle (svc_dc delete).....	32
List support materials (svc_dc list).....	32
List all support material profiles (svc_dc list_profiles).....	33
List all system dump files (svc_dc list_dumps).....	34
Download an existing support materials bundle (svc_dc download).....	35
Upload a support materials bundle (svc_dc upload).....	36
Enable or disable DDSD (svc_dd).....	36
System diagnostics (svc_diag).....	37
Check upgrade conversion status (svc_dip_upgrade_check).....	40
Check DIP upgrade conversion status (svc_dip_upgrade_check status).....	41

Check datapath stats (svc_dp_oos_check).....	41
Collect flash and NVMe statistics (svc_drive_stats).....	42
Factory reset (svc_factory_reset).....	43
Get a report on unreducible data (svc_get_unreducible_dp_stats).....	44
Get report on unreducible data (svc_get_unreducible_stats).....	45
Perform a health check on the appliance (svc_health_check).....	46
Help (svc_help).....	47
Hypervisor diagnostics (svc_hypervisor).....	48
Set limits for import service (svc_import_config).....	49
Set import configuration limits (svc_import_config set).....	50
See all import configurations (svc_import_config list).....	51
Inject troubleshooting software tool (svc_inject).....	51
Install service tools (svc_inject run).....	52
Delete an injected service tool (svc_inject delete).....	52
Display information about a specific package (svc_inject info).....	53
Generate a root or recovery package key (svc_inject generate-key).....	53
Deactivate service escalation (svc_inject deactivate).....	54
View service escalation status (svc_inject status).....	54
Review system journal logs (svc_journalctl).....	55
Check the license status of appliances in a cluster (svc_license_status).....	57
Install the PowerStore system (svc_manufacturing).....	58
See and update MFS settings for SecurID (svc_mfa_state)	59
Retrieve information system information (svc_mgmt_operations).....	60
Retrieve information as a root user (svc_mgmt_operations all_top_level_commands).....	62
See command details (svc_mgmt_operations command_detail).....	63
Show and filter command records (svc_mgmt_operations command_hierarchy_for_cleanup).....	64
Display the command tree (svc_mgmt_operations command_tree).....	66
Migrate a cluster or DVS to another vCenter (svc_migrate_to_vcenter).....	68
Migrate to vCenter (svc_migrate_from_vcenter migrate_to_vcenter).....	69
Restore the vCenter configuration (svc_migrate_to_vcenter restore_on_vcenter).....	70
Remove empty proxy switches (svc_migrate_to_vcenter fix_restore_issues).....	71
Enable or disable autodownload (svc_modify_autodownload).....	71
Run service scripts using SSH tunneling (svc_nas).....	72
Download the ACL database of a file system (svc_nas nas_svc_acldb_dump).....	73
Manage Dynamic Access Control (svc_nas nas_svc_dac).....	74
Generate NAS output files (svc_nas nas_svc_data_protection).....	76
Generate an SDNAS archive file (svc_nas nas_svc_dc).....	79
Manage NAS servers (svc_nas nas_svc_nas).....	80
Manage an IMT import (svc_nas nas_svc_imt).....	81
Display the SDNAS log (svc_nas nas_svc_log).....	83
Show statistics for NDMP and PAX backup sessions (svc_nas nas_svc_paxstats).....	84
Run a Linux tcpdump (svc_nas nas_svc_tcpdump).....	85
Back up NAS server configuration (svc_nas_cbr).....	87
See CIFS issues (svc_nas_cifssupport).....	87
Advanced NAS settings (svc_nas_tools and svc_nas_global_tools).....	94
Enter maintenance mode (svc_nas_maintenance_mode).....	99
Display inode usage (svc_nas_storagecheck).....	100
Get NAS server information and manage settings (svc_nas_tools).....	101
Retrieve NAS server net devices and IP addresses (svc_nasserver_to_netdevice).....	102
See network information (svc_networkcheck).....	103

Show ARP records cache settings (svc_networkcheck arp).....	104
Perform network and system checks (svc_networkcheck info).....	105
Check server port availability (svc_networkcheck tracer).....	105
Check the TCP port (svc_networkcheck tcp).....	105
Show network device driver and hardware information (svc_networkcheck ethtool).....	106
Ping an IPv4 target (svc_networkcheck ping).....	107
Ping an IPv6 target (svc_networkcheck ping6).....	108
Show network connections (svc_networkcheck netstat).....	108
Perform a DNS check (svc_networkcheck dns).....	108
See system bond devices (svc_networkcheck bond_list).....	109
Show interface names (svc_networkcheck interfaces).....	110
Reboot, shut down, and turn on a node (svc_node).....	111
Turn a node off (svc_node power_off).....	112
Turn on the peer node (svc_node power_on).....	113
Reboot a node (svc_node reboot).....	113
Shut down a node (svc_node shutdown).....	114
Peer node status (svc_node status).....	115
Control node affinity (svc_node_affinity_balance).....	115
Enable node affinity balancing (svc_node_affinity_balance enable).....	116
Disable node affinity balancing (svc_node_affinity_balance_disable).....	116
Display node affinity balancing status (svc_node_affinity_balance_status).....	117
Check and fix the NTP status (svc_ntp_ctl).....	117
Customize validation service parameters (svc_onv_customizing).....	118
Set onv parameters and their values (svc_onv_customizing set).....	119
List ongoing parameters (svc_onv_customizing list_onv_parameters)	120
Get a specific parameter (svc_onv_customizing get).....	120
Disable password reset (svc_password_mgmt).....	120
Enable and prevent passwords from being recovered (svc_password_mgmt_recovery).....	121
Send REST requests through the service container (svc_pstcli).....	122
Troubleshoot and repair (svc_remote_support).....	127
List the remote configuration (svc_remote_support list).....	128
Modify the remote support configuration (svc_remote_support_modify).....	129
Modify contact information (svc_remote_support modify_contact).....	130
Reinitialize the remote support configuration (svc_remote_support reinitialize).....	130
Restart SupportAssist (svc_remote_support restart).....	131
Check the connectivity status (svc_remote_support connectivity).....	131
Manage the remote syslog (svc_remote_syslog).....	131
Refresh the expired Unity SSL certificate (svc_remote_system_certificate_operations).....	132
Remove appliance (svc_remove_appliance).....	133
Renew certificates (svc_renew_certificates).....	134
Renew a specific certificate, or all certificates (svc_renew_certificate run).....	135
Show certificates for renewal (svc_renew_certificates list).....	136
Renew VASA certificates (svc_renew_vasa_self_signed_certificate).....	136
Repair software (svc_repair).....	137
Replace the DPE (svc_replace_dpe).....	137
Replace the DPE (svc_replace_dpe auto).....	138
Replace the DPE (svc_replace_dpe manual).....	139
Service mode operation (svc_rescue_state).....	139
Unlock a secure snapshot (svc_secure_snapshot).....	140
Grant service user access (svc_service_config).....	141

Gain root privileges (svc_service_shell).....	142
Software recovery (svc_software_recovery).....	143
Connect to the peer node service container (svc_ssh_peer).....	143
Collect system information (svc_system_info).....	144
Monitor network traffic (svc_tcpdump).....	145
View capacity metrics (svc_volume_space_metrics).....	146
Complete the recovery process (svc_wear_trickle_write).....	147
Appendix A: System Journal Fields.....	149
Field descriptions.....	149

As part of an improvement effort, revisions of the software and hardware are periodically released. Some functions that are described in this document are not supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information about product features. Contact your service provider if a product does not function properly or does not function as described in this document.

 **NOTE:** PowerStore X model customers: For the latest how-to technical manuals and guides for your model, download the *PowerStore 3.2.x Documentation Set* from the PowerStore Documentation page at dell.com/powerstoredocs.

Where to get help

Support, product, and licensing information can be obtained as follows:

- **Product information**—For product and feature documentation or release notes, go to the PowerStore Documentation page at dell.com/powerstoredocs.
- **Troubleshooting**—For information about products, software updates, licensing, and service go to [Dell Support](#) and locate the appropriate product support page.
- **Technical support**—For technical support and service requests, go to [Dell Support](#) and locate the **Service Requests** page. To open a service request, you must have a valid support agreement. Contact your Sales Representative for details about obtaining a valid support agreement or to answer any questions about your account.

Introduction

PowerStore includes service scripts that enable you to diagnose issues, solve common problems, perform certain operational tasks, and recover your system from an error state. These scripts provide in-depth level of information and a lower level of system control than is available through other interfaces such as PowerStore Manager, CLI, and REST API. This document describes these service scripts and how you can use them.

NOTE: The service scripts that are described in this document are a subset of the operating environment software tools for servicing your system. You can use the CLI or REST API for scriptable system configuration for additional capability. For more information about these interfaces, see the *PowerStore CLI Guide* and *PowerStore REST API Developers Guide*.

This chapter contains the following topics:

Topics:

- [Audience](#)
- [Running the service scripts](#)

Audience

Although no special knowledge is needed to run most of the service commands or understand the results, the service commands are designed with storage system administrators, field service personnel, and support personnel in mind. The service commands run on the PowerStore appliance's Linux-based operating environment. Ensure that you are familiar with the Linux shell, associated commands, PowerStore's installed hardware, and the PowerStore operating environment.

Certain commands may require more training or require you to obtain root privileges. If the command description specifies more training or greater privileges, do not run the commands without an approval from your authorized service representative.

Running the service scripts

Prerequisites

- Obtain the password for the Service account.
- In PowerStore Manager, under **Settings**, enable SSH.
- Download and install an SSH client, such as PuTTY, to a computer that has network access to the cluster. You use the SSH client to run the scripts.

About this task

To run the service scripts:

Steps

1. Launch an SSH client, and connect to the cluster using the management IP address.
For example, in PuTTY, enter the management IP for the destination.
2. Enter the username and password for the service account to log in to the system.
Once logged in, you should be connected directly to the serviceability docker container.
3. Type the name of the script to run.

For example, to see the list of scripts, type the following: `svc_help`

Each script includes a `--help` option. Type a space and `--help` after the name of a script for usage information as seen in the following example:

```
svc_diag --help
```

Service Commands

This chapter contains the following topics:

Topics:

- Shut down and reboot an appliance (svc_appliance)
- Provision an appliance (svc_appliance_provisioning)
- Capture array configuration data (svc_arrayconfig)
- Manage CAC and PIV (svc_cac_piv_mgmt)
- Make space on the root partition (svc_cleanup)
- Clear the DIMM state value on a specific node (svc_clear_dimm_ce_state)
- Clear firmware update (svc_clear_fw_update_alert)
- Shut down a SAN cluster (svc_cluster)
- Diagnose a create cluster failure (svc_cluster_diag)
- Cluster management (svc_cluster_management)
- Enable or disable counter collection (svc_cnt)
- Configure new SLICs (svc_commit_slic)
- Show the security compliance state (svc_compliance_mode)
- Check status of or restart container (svc_container_mgmt)
- Support materials (svc_dc)
- Enable or disable DDSD (svc_dd)
- System diagnostics (svc_diag)
- Check upgrade conversion status (svc_dip_upgrade_check)
- Check datapath stats (svc_dp_oos_check)
- Collect flash and NVMe statistics (svc_drive_stats)
- Factory reset (svc_factory_reset)
- Get a report on unreducible data (svc_get_unreducible_dp_stats)
- Get report on unreducible data (svc_get_unreducible_stats)
- Perform a health check on the appliance (svc_health_check)
- Help (svc_help)
- Hypervisor diagnostics (svc_hypervisor)
- Set limits for import service (svc_import_config)
- Inject troubleshooting software tool (svc_inject)
- Review system journal logs (svc_journalctl)
- Check the license status of appliances in a cluster (svc_license_status)
- Install the PowerStore system (svc_manufacturing)
- See and update MFS settings for SecurID (svc_mfa_state)
- Retrieve information system information (svc_mgmt_operations)
- Migrate a cluster or DVS to another vCenter (svc_migrate_to_vcenter)
- Enable or disable autodownload (svc_modify_autodownload)
- Run service scripts using SSH tunneling (svc_nas)
- Back up NAS server configuration (svc_nas_cbr)
- See CIFS issues (svc_nas_cifssupport)
- Advanced NAS settings (svc_nas_tools and svc_nas_global_tools)
- Enter maintenance mode (svc_nas_maintenance_mode)
- Display inode usage (svc_nas_storagecheck)
- Get NAS server information and manage settings (svc_nas_tools)
- Retrieve NAS server net devices and IP addresses (svc_nasserver_to_netdevice)
- See network information (svc_networkcheck)
- Reboot, shut down, and turn on a node (svc_node)
- Control node affinity (svc_node_affinity_balance)

- Check and fix the NTP status (svc_ntp_ctl)
- Customize validation service parameters (svc_onv_customizing)
- Disable password reset (svc_password_mgmt)
- Send REST requests through the service container (svc_pstcli)
- Troubleshoot and repair (svc_remote_support)
- Manage the remote syslog (svc_remote_syslog)
- Refresh the expired Unity SSL certificate (svc_remote_system_certificate_operations)
- Remove appliance (svc_remove_appliance)
- Renew certificates (svc_renew_certificates)
- Renew VASA certificates (svc_renew_vasa_self_signed_certificate)
- Repair software (svc_repair)
- Replace the DPE (svc_replace_dpe)
- Service mode operation (svc_rescue_state)
- Unlock a secure snapshot (svc_secure_snapshot)
- Grant service user access (svc_service_config)
- Gain root privileges (svc_service_shell)
- Software recovery (svc_software_recovery)
- Connect to the peer node service container (svc_ssh_peer)
- Collect system information (svc_system_info)
- Monitor network traffic (svc_tcpdump)
- View capacity metrics (svc_volume_space_metrics)
- Complete the recovery process (svc_wear_trickle_write)

Shut down and reboot an appliance (svc_appliance)

This service script allows you to perform a managed shutdown and reboot of a single appliance in SAN mode.

Usage

Function	Diagnostic and recovery
Mode	Normal or Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	No
May cause data unavailability?	Yes
May cause data loss?	No
Scope	Appliance
Prerequisites	None

Format

```
svc_appliance [-h] [-d] {reboot,shutdown}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Qualifier	Description
-d, --debug	Increase logging level to debug and print logs to console.

Actions

Action	Description
reboot	Reboot an appliance.
shutdown	Shut down an appliance.

Reboot an appliance (svc_appliance reboot)

This service script is used to reboot an appliance.

i NOTE: This option should be used only if recommended by your service provider. The standard procedure is to always reboot the nodes one by one, and not simultaneously, unless support recommends otherwise.

Format

```
svc_appliance reboot [-h] [-a] [-f] [-d]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-a, --async	Run in asynchronous mode.
-f, --force	Ignore warnings when starting the action; force reboot, which may result in data becoming unavailable.
-d, --debug	Initiate verbose logging for debugging purposes.

Shut down an appliance (svc_appliance shutdown)

This service script enables you to shut down an appliance.

Format

```
svc_appliance shutdown [-h] [-a] [-f] [-d]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-a, --async	Run in asynchronous mode.
-f, --force	Ignore warnings and force a shutdown, which may result in data becoming unavailable.
-d, --debug	Initiate verbose logging for debugging purposes.

Provision an appliance (svc_appliance_provisioning)

This service script enables or disables the autoprovisioning function on a selected appliance.

Usage

Function	Configuration
Mode	Service and Normal
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Appliance
Prerequisites	None

Format

```
svc_appliance_provisioning [-h] {enable,list,disable}
```

Optional Arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
enable	Enable provisioning on the appliance.
list	List provisioning on the appliance.
disable	Disable provisioning on the appliance.

Usage Example

The following example shows appliance provisioning being disabled for appliance A2. After disablement, new storage objects are not placed on appliance A2:

```
svc_appliance_provisioning disable A2
```

Capture array configuration data (svc_arrayconfig)

This service script captures a snapshot of the current cluster configuration.

NOTE: The **svc_array_config** service script can only be run on the primary node. This script cannot be run from the secondary node.

Usage

Function	Diagnostic
Mode	Normal
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	Primary appliance must be operating in normal mode.

Format

```
svc_arrayconfig [-h] {run}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
run	Capture the current cluster configuration.

Get a system snapshot with the **svc_arrayconfig** service script

About this task

If you do not have root access, you can use the **svc_arrayconfig** service command to create JSON files. You can .zip those files into a single file, and download that file from the system.

NOTE: The **svc_array_config** service script can only be run on the primary node. This script cannot be run from the secondary node.

In PowerStoreOS versions 3.0 and later, the cluster IP address is found on secondary node B. To run the script and download the system snapshot file, you must have the node management IP address.

If you use the PowerStoreOS CLI, you can connect to the peer using the **svc_ssh_peer** service command. However, if you use WinSCP or another tool to download the system snapshot file, you must have the node management IP address of node A to allow node B to connect to it.

Steps

1. Log in to the service container as the service user.

2. Run the **svc_array_config** command to create JSON file outputs into a subdirectory under `/home/service/user`: **\$ svc_arrayconfig run -o /home/service/user/capture**
3. Verify that those file outputs are in the `/home/service/user/capture` directory: **\$ ls -la capture |wc -l 112**
4. From the `/home/service/user` directory, bundle the JSON files into a `tar.tgz` file called `array_config_collections.tar.tgz`.

```
$ tar -zcvf array_config_collection.tar.tgz capture/*
$ ls /home/service/user/array*
array_config_collection.tar.tgz
```

5. Download the `array_config_collections.tar.tgz` bundle from the `/home/service/user` directory/.

Capture current cluster configuration (svc_arrayconfig run)

This service script captures the current cluster configuration while offering an array of subcommands for specific actions.

NOTE: The **svc_array_config** service script can only be run on the primary node. This script cannot be run from the secondary node.

Format

```
svc_arrayconfig run [-h] [-l value] [-c value] [-m] [-f {json,csv}]
                    [-t {full,delta,metrics,full_metrics}] [-b value]
                    [--timestamp value] [--response value]
                    [--ts value] [--ts_query value]
```

Optional arguments

Qualifier	Description
<code>-h, --help</code>	Show the help message and exit.
<code>-l, --limit</code>	Specify a file size (in MB) limit. The default is no limit.
<code>-t {full, delta, full_metrics, metrics}, --type {full,delta, metrics, full_metrics}</code>	Specify the type of capture to perform. If the type is delta, and then you must specify the <code>--base</code> option to also specify the base from which to produce the delta.
<code>-b, --base</code>	The base directory from which to produce a delta. The base is an output directory of a previous 'full' capture.
<code>-f {json,csv}, --format {json,csv}</code>	The format of the output capture files. The default format is JSON.
<code>-c, --config</code>	Specify the configuration file to use to control the configuration capture.
<code>-m, --master-only</code>	Only run if this command is being invoked from one of the nodes on the primary appliance.
<code>--timestamp</code>	The base timestamp used to derive the capture time range. Format is 'YYYY-MM-DD HH:mm:ss'. Defaults to now if unspecified or empty string.
<code>--response</code>	A path name that specifies where to write response data (if any).
<code>--ts</code>	Timestamp to be set on filename and full metrics objects.
<code>--ts_query</code>	Timestamp to be used for sql queries.

Manage CAC and PIV (svc_cac_piv_mgmt)

This service script enables you to manage Common Access Card (CAC) and Personal Identity Verification (PIV) certificates, role mappings, and CAC/PIV configurations.

If you encounter login issues, those issues might be the result of the certificate status being out of synchronization with the system. You can restart Control Path (CP) using the **svc_cac_piv_mgmt** script to force the remediation service to resolve the synchronization issue.

Usage

Function	System operations
Mode	Normal or Service
Usage	Normal or Service
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_cac_piv_mgmt [-h] [-v]
{modify_config,create_ca_cert_chain,delete_cert_role_mapping,modify_cert_role_mapping,get_cert_role_mapping,get_config,create_cert_role_mapping,get_ca_cert_chain}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
modify-config	Modify the CAC/PIV configuration. For detailed subcommand usage, call the help flag: <code>svc_cac_piv_mgmt modify config --help</code>
create_ca_cert_chain,	Create a CA certificate chain.
delete_cert_role_mapping	Delete an existing certificate or role-mapping instance.
modify_cert_role_mapping	Modify an existing certificate or role-mapping instance.
get_cert_role_mapping	Get existing certificate or role-mapping instances.
get_config	Get the CAC/PIV configuration.
create_cert_role_mapping	Create a certificate or role-mapping instance. For detailed sub- command usage, call the help flag:

Action	Description
get_ca_cert_chain	Get the CA certificate chain instances.
clear_config	Clear the CAC/PIV property.

Make space on the root partition (svc_cleanup)

This service script allows service personnel or customers to gain access to a node where the root partition is 100% full. This script enables access by removing a large file that is consuming space on the root partition.

The cleanup deletes old data collections, old journal logs, and old core dumps.

Verify that the root partition is full. If the root partition is not full, the system asks if you want to continue.

Remove old data collections from `/cyc_var/cyc_service/data_collection`. If a data collection is not found, you can find old journal logs in `/var/log/journal` and delete oldest one.

If a journal log is not found, you can find a core dump at `/cyc_var/cyc_dumps/processed/` and delete it.

Usage

Function	System Operations
Mode	Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Node
Prerequisites	None

Format

```
svc_cleanup [-h] [-a] [-j] [-c] [-t] [-d] [-y]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-d, --dataCollection	Clean up the data collections.
-c, --coreDump	Clean up stored core files.
-a, --all	Clean up the data collections, core dumps, journals, logs, and temporary data collection directory.
-j, --journalFiles	Clean up the journal files.
-t, --tmpDataCollection	Clean up the temporary data collection directory.
-y, --noConfirm	Bypass confirmation messages.

Clear the DIMM state value on a specific node (svc_clear_dimm_ce_state)

This service script enables you to clear the dual inline memory module (DIMM) correctable errors (CE) state persistent value for a DIMM on a specified node.

Usage

Function	System Operations
Mode	Normal
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Node
Prerequisites	None

Format

```
svc_clear_dimm_ce_state [-h] {clear_state}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
clear_state	Clears the DIMM CE state on a specified node.

Clear firmware update (svc_clear_fw_update_alert)

This service script enables you to clear the firmware update alert on a given node.

Usage

Function	Diagnostic
Mode	Normal or Service
Usage	General use

Requires service user password?	No
Requires root privileges?	Yes
May cause data unavailability?	No
May cause data loss?	No
Scope	Node
Prerequisites	None

Format

```
svc_clear_fw_update_alert [-h] {clear_alert}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
clear_alert	Clears the firmware update alert on a given node.

Positional arguments

Qualifier	Description
A	One node that is in a node pair.
B	One node that is in a node pair.

Example

The following example shows the firmware update alerts being cleared on nodes A and B:

```
svc_clear_fw_update_alert clear_alert [-h] {A,B}
```

Shut down a SAN cluster (svc_cluster)

This service script enables you to shut down all the appliances in a SAN cluster. This operation can only be performed on SAN clusters.

Usage

Function	Diagnostic and Recovery
Mode	Normal or Service

Usage	Service
Requires service user password?	Yes
Requires root privileges?	No
May cause data unavailability?	Yes
May cause data loss?	No
Scope	Cluster
Prerequisites	The master appliance must be operating in normal mode.

Format

```
svc_cluster [-h] {shutdown} [-f] [-d]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-d, --debug	Initiate verbose logging for debugging purposes.
-f, --force	Ignore warnings. Force a shutdown that might result in data becoming unavailable.

Actions

Action	Description
shutdown	Shut down all the appliances in a SAN cluster. This operation is only allowed for SAN clusters.

Diagnose a create cluster failure (svc_cluster_diag)

This service script is intended to be run in order to help troubleshoot issues that may happen during create cluster, adding an appliance, or removing an appliance.

This script performs the following functions:

1. Search for a hardware check in the journal.

This step looks for hardware faults that may have happened before the create cluster operation.

2. Run a current hardware check on this system using `svc_diag list --icw_hardware`.

Running the script shows any hardware issues in the system. This step is useful if the create cluster operation has failed with the message `UNCONFIGURED_FAULTED`.

If there is a hardware fault, a create cluster operation cannot be performed. If a fault is detected, the state changes to `UNCONFIGURED_FAULTED` and the create cluster operation fails. This check finds the hardware fault.

3. Ask if you want to perform a data collect.

This step is critical after a create cluster operation failure and allows the data to be collected before the log rotation.

This step also allows the user to set an IP for the system. This way the user can use the direct path to the data collect and the IP address to copy off the data collect from the system.

Usage

Function	Diagnostic
Mode	Normal and Service
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	Yes
May cause data loss?	Yes
Scope	Node, cluster
Prerequisites	None

Format

```
svc_cluster_diag [-h] [-w] [-d] [-e] [-i]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-w, --warningLevel	Display WARN level logs.
-i, --infoLevel	Display INFO level logs.
-e, --errorLevel	Display ERROR level logs.
-d, --debugLevel	Display DEBUG level logs.

Example

The following output indicates that no logs are available and the system is running a support materials bundle after you have entered the `svc_cluster_diag -w` command:

```
svc_cluster_diag -w

The log statements that are needed to collect information for the command:
'journalctl --utc -t control-path | egrep "\[CC\]" | grep WARN' are no longer
available

Would you like to perform a data collection? Please enter 'yes' or 'no'
yes

Running data collection - This might take awhile

data collection ID f10a1ebb-5727-4a84-aa29-58df29274bcc
Status           OK
HTTP Code        201
```

Cluster management (svc_cluster_management)

This service script enables service providers to attach, detach, and view the status of each appliance in a cluster. If an appliance in a two-appliance cluster fails or can no longer communicate with the other appliance, the remaining appliance becomes unmanageable.

You can ask your service provider to detach the failed appliance from the cluster and restore the ability to manage the remaining appliance. Once the issue with the appliance is resolved, you can use the prep-attach and attach commands to reattach the appliance back into the cluster.

Usage

Function	Recovery
Mode	Normal
Usage	Service
Requires service user password?	N/A
Requires root privileges?	Yes
Might this cause data unavailability?	Yes
Might this cause data loss?	No
Scope	Appliance
Prerequisites	None

Format

```
svc_cluster_management [-h] [e] [-n <value>]
{GetClusterStatus,DetachFailedAppliance,PrepReattachAppliance,ReattachAppliance,MovePrimaryAppliance}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-e, --eligibility_check	Show the nodes that are eligible to be the cluster primary node.
-n, --nodeid	Specify the node that becomes the new cluster primary node.

Actions

Action	Description
GetClusterStatus	Display current cluster status.
DetachFailedAppliance	Detach a failed appliance.
ReattachAppliance	Reattach an appliance.
PrepReattachAppliance	Prepare an appliance for reattachment.
MovePrimaryAppliance	Move the primary role to a different appliance.

Action	Description
	 NOTE: Do not run perform the MovePrimaryAppliance action if the data path is offline or in a read-only mode. Performing the action at those times results in a loss of cluster management.

Positional arguments

Qualifier	Description
-n	Show the help message and exit.

Example

The following example shows the node with the ID 4 being designated as the primary cluster appliance:

```
svc_cluster_management MovePrimaryAppliance -n 4
```

Remove and reattach an appliance

1. If a two-appliance cluster has a failed appliance, you can use the `svc_cluster_management` script to detach the appliance and reattach it when the problem is resolved.

```
svc_cluster_management status
---CLUSTER STATUS---

local is primary: False
master id: 0

---APPLIANCE LIST---
id: 2
name: appliance_j8xxmd2
ip address: fd73:51fc:80d:0:201:4471:dcbb:4bce
online: False
id: 1
name: appliance_j8y1nd2
ip address: fd73:51fc:80d:0:201:4432:1df9:41da
online: True
```

2. Detach the failed appliance: `svc_cluster_management detach`

```
svc_cluster_management detach
detach failed appliance success!
```

3. Prepare to attach the appliance back to the cluster: `svc_cluster_management prep_attach`

```
svc_cluster_management prep_attach
prep reattach appliance success
```

4. Attach the appliance back to the cluster: `svc_cluster_management attach`

```
svc_cluster_management attach
reattach appliance success
```

Remove and reattach an appliance

If a two-appliance cluster has a failed appliance, you can use the `svc_cluster_management` script to detach the appliance and reattach it when the problem is resolved.

Steps

1. Run the following command to view the status of the appliances in the cluster: `svc_cluster_management status`
- ```
svc_cluster_management status

---CLUSTER STATUS---

 local is master: False
 master id: 0

---APPLIANCE LIST---

 id: 2
 name: appliance_j8xxmd2
 ip address: fd73:51fc:80d:0:201:4471:dcbb:4bce
 online: False

 id: 1
 name: appliance_j8ylnd2
 ip address: fd73:51fc:80d:0:201:4432:1df9:41da
 online: True
```
2. Detach the failed appliance: `svc_cluster_management detach`
- ```
svc_cluster_management detach

detach failed appliance success!
```
3. Prepare to attach the appliance back to the cluster: `svc_cluster_management prep_attach`
- ```
svc_cluster_management prep_attach

prep reattach appliance success
```
4. Attach the appliance back to the cluster: `svc_cluster_management attach`
- ```
svc_cluster_management attach

reattach appliance success
```

Enable or disable counter collection (svc_cnt)

This service script allows you to enable and disable counter collection. This script also enables you to change the configuration to enable or disable a one-second collection profile.

Format

```
svc_cnt [-h] [-d] {status,enable,restart,disable,performance,performance_disable}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Qualifier	Description
-d, --debug	Initiate verbose logging for debug.

Actions

Qualifier	Description
status	This action displays the status of the collection service on each node. In addition, this action shows the amount of space that is taken up by xcounters recordings on the Base System Container (BSC) for each node. This action also shows how many files there are for each node.
enable	This action enables the counter collection service. The service is enabled by default. This action is useful if the collection service has been manually disabled by the <code>svc_cnt disable</code> command.
restart	This action restarts the collection service. This action is useful if the counter configuration profile has been updated on the BSC and a reload is required.
disable	This action disables the counter collection service. The collection service is enabled by default; disabling the service takes effect for each node until a BSC restart occurs. After the BSC restart, the service is reenabled automatically by BSC startup procedures.
performance	This action enables the 1-second collection profile. This action is used mostly during investigations into appliance performance issues. A service restart is required after you run this command in order for the 1-second collection to start.
performance_disable	This action disables the 1-second collection profile. A service restart is required after you run this command in order for the 1-second collection to stop.

Enable counter collection (svc_cnt enable)

This service script allows you to enable the counter collection service.

Format

```
svc_cnt enable [-h]
```

Optional Arguments

Qualifier	Description
-h, --help	Show this help message and exit.

Disable counter collection (svc_cnt disable)

This service script allows you to disable the counter collection service.

Format

```
svc_cnt disable [-h]
```

Optional Arguments

Qualifier	Description
-h, --help	Show this help message and exit.

See the collection status (svc_cnt status)

This service script enables you to display the status of the collection service on each node.

Format

```
svc_cnt status [-h]
```

Optional Arguments

Qualifier	Description
-h, --help	Show this help message and exit.

Restart the collection service (svc_cnt restart)

This service script enables you to restart the collection service.

Format

```
svc_cnt restart [-h]
```

Optional Arguments

Qualifier	Description
-h, --help	Show this help message and exit.

Enable the 1-second collection profile (svc_cnt performance)

This service script enables the 1-second collection profile, which is useful during investigations into appliance performance issues.

A service restart is required after you run this command in order for the 1-second collection to start.

Format

```
svc_cnt performance [-h]
```

Optional Arguments

Qualifier	Description
-h, --help	Show this help message and exit.

Disable the 1-second collection profile (svc_cnt performance_disable)

This service script disables the 1-second collection profile.

A service restart is required after you run this command in order for the 1-second collection to stop.

Format

```
svc_cnt performance_disable [-h]
```

Optional Arguments

Qualifier	Description
-h, --help	Show this help message and exit.

Configure new SLICs (svc_commit_slic)

This service script activates commit pair of SLIC logic. Use this script after you insert the SLICs into slots. The script enables you to create all necessary configuration for new SLICs on this appliance and on remote appliances (in the cluster). This script must be started on primary node.

Specify the number of slots for which you want to configure SLICs. If no SLICs are ready, an error message is returned.

Three types of objects must be configured when adding a SLIC and running the commit SLIC operation:

- Autodiscovered hardware objects: These objects include SFP and FEPort.
These objects are discovered automatically after the SLIC is inserted and before the commit procedure.
- Network configurations: These objects include the target and net device.
These objects are created during the commit procedure.
- Cluster-wide configurations: These objects include the IP port, remote target, and remote NVMe port.
These objects are created across the cluster, not just on the appliance.

Usage

Function	System Operations
Mode	Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	No
May cause data unavailability?	Yes
May cause data loss?	No

Scope	Node
Prerequisites	None

Format

```
svc_commit_slic [-h] [-v] {status,reset,activate,replay}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-v, --verbose	Output more details.

Actions

Qualifier	Description
activate	Activate the commit procedure. If there are no SLICs that are ready to be committed, the service script returns an error message. Create configuration (Targets, Network Devices, NVMe ports) for inserted IOMs.
replay	Continue a failed commit procedure. In HA configurations, the commit operation is restarted automatically. Replay should be used if either the <code>activate</code> or <code>activate --resume</code> command reports a failed state. It is a best practice to retry the <code>activate</code> or <code>activate --resume</code> action before attempting the <code>replay</code> command.
status	Show information about the SLICs in specific slots and objects that are configured on these SLICs. Use this command before running the <code>activate</code> command to check that all autodiscovered objects are configured. After running the <code>activate</code> command, use the <code>status</code> command to confirm that the configuration has been created successfully. The <code>status</code> command also includes the option <code>--raw</code> that displays more information about the configured objects in a JSON format.
reset	Terminate the commit procedure if an unrecoverable failure occurs and reset the activation state machine. This action does not clean the already created configuration. Use with caution.

Usage Examples

```
svc_commit_slic activate 1
    Configure inserted SLICs with slot index 1

svc_commit_slic activate 0 --resume
    Resume commit procedure if it is interrupted by HA case (a component or node reboot)

svc_commit_slic status 0
    Show info about the SLICs, its children objects and activation state machine status
    for specific SLICs

svc_commit_slic reset 0
    Resets activation state machine, if there is no activation in progress.

svc_commit_slic replay 1
    Recover and retry activation if previous run fails
```

```
svc_commit_slic replay 1 --cp_only
  Call replay only for cluster reconfiguration (IP ports, SCSI Targets, NVMe ports)
```

Show the security compliance state (svc_compliance_mode)

This script enables you to display current security hardened states such as STIG and FIPS compliance. You can also use this script to rollback a failed instance. In addition, you can use this script to see the current Security and Technical Information Guides (STIG) and root partition encryption (RPE) statuses.

Although the scope of this script is cluster-level, rollbacks must occur individually for each appliance.

Usage

Function	System Operations
Mode	Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	No
May cause data unavailability?	Yes
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_compliance_mode status [-h] {status,rollback}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
status	Shows the status of security compliance modes. The status can be on, off, or faulted.
rollback	Enables you to roll back or cancel the hardening operation.

Example

The following command shows the current STIG and RPE statuses:

```
svc_compliance_mode status
```

STIG is currently ENABLED.
RPE is currently DISABLED.

Check status of or restart container (svc_container_mgmt)

This service script enables you to check the status of a container or restart it. Currently, you can only restart the CP container.

Usage

Function	System Operations
Mode	Normal and Service
Usage	General Use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Appliance
Prerequisites	None

Format

```
svc_container_mgmt [-h] {status,restart}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
status	Show the status of the container.
restart	Restart the container.

Support materials (svc_dc)

This service script generates a support materials bundle, or data collection (dc) bundle, for technical analysis. Depending on the option you choose, support materials can include system logs, configuration details, and other diagnostic information.

Use this information to analyze performance issues, or send it to your service provider so they can diagnose and help you resolve the issues. This process does not collect user data.

Usage

Function	Diagnostic
Mode	Normal or Service
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_dc [-h] [-v] {run,delete,list,list_profiles,list_dumps,download,upload}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-v, --version	Show the programs version number and exit.

Actions

Action	Description
run	Run a data collection.
delete	Delete an existing data collection.
list	List all data collections or details for one collection.
list_dumps	List all system dumps for the entire cluster.
list_profiles	List data collection profiles.
download	Download an existing support materials bundle.
upload	Upload an existing data collection.

Generate a support materials bundle (svc_dc run)

This service script is used to generate a new support materials bundle, or data collection, on the local appliance using the default profile. A support materials archive is generated for each appliance in a cluster and stored locally on the appliance.

Format

```
svc_dc run [-h] [--debug] [-v] [--output {json}] [-p <value>] [-a <value>] [-vol  
<value>] [-vvol <value>]  
          [-d <value>] [-u] [-t
```

```
{last_24_hours,last_48_hours,last_1_week,last_2_weeks,custom}}
[-from LOG_FROM_TIMESTAMP <value>] [-to LOG_TO_TIMESTAMP <value>]
```

Optional arguments

Qualifier	Description
-a, --appliances	List of appliance IDs to include, in the format of A1, A2, and so on. Use <code>svc_diag --basic</code> to find the ID of this appliance.  NOTE: The default value for this option is local appliance only.
-vol, --volumes	List of volume IDs to include.
-vvol, --virtual_volumes	List of virtual volumes IDs to include.
-p, --profiles	List of profiles to use.
-d, --description	The text description associated with the data collection.
-h, --help	Show the help message and exit.
--u, --upload	Upload the generated DC.
--debug	Initiate verbose logging for debug.
-v, --verbose	Initiate verbose command output.
--output {json}	Show output in the JSON format.
-t {last_24_hours,last_48_hours,last_1_week,last_2_weeks,custom}, --timeframe {last_24_hours,last_48_hours,last_1_week,last_2_weeks,custom}	The timeframe from which the journal logs are collected. If custom is chosen, the -from or -to option is required.
-from LOG_FROM_TIMESTAMP, --log_from LOG_FROM_TIMESTAMP	This flag is only to be used with -t=custom option . Timestamp should be in YYYY-MM-DD HH:mm:ss format in UTC time zone.
-to LOG_TO_TIMESTAMP, --log_to LOG_TO_TIMESTAMP	This flag is only to be used with -t=custom option . Timestamp should be in YYYY-MM-DD HH:mm:ss format in UTC time zone.

Example

Generate a new support materials bundle on appliances APM00162303297 and APM00152832910 using the Essential profile. Gather support materials on the local appliance using the default profile. Each appliance in a cluster gathers its own support materials archive and stores it locally on that appliance.

```
svc_dc run --profiles=essential --appliance=APM00162303297,APM00152832910

start_timestamp    status  description          creator_type  profile  appliances
2019-05-20 17:49:33 Success  SR 87936386         Scheduled    Ess,Det  APM00162303297+1
2019-05-21 12:10:31 Success  SR 87936386         System      Ess,Det  APM00152832910
2019-05-21 17:49:33 Success  SR 87936386         Scheduled    Perf     APM00162303297+1
```

Delete a support materials bundle (svc_dc delete)

This service script is used to delete a support materials bundle. If no ID is specified, the script runs in interactive mode. All saved support materials bundles appear. Pick the bundle that you want to delete by using a short identifier. If an ID is specified, that support materials bundle is deleted.

Format

```
svc_dc delete [-h] [--debug] [-v] [--output {json}] [id]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--debug	Initiate verbose logging for debug.
-v, --verbose	Initiate verbose command output.
--output {json}	Show the output in JSON format.

Positional arguments

Qualifier	Description
id	Data collection index ID.

Example

The following example shows the `svc_dc delete` command being run in interactive mode. The command lists all collections; a collection would be deleted when its index number is entered.

```
svc_dc delete

Index start_timestamp      id
0      2019-09-15 19:01:24  b3a42a8a-874b-4dfa-b812-1e0a9a35f105
1      2019-09-15 20:25:26  d97e6a7a-4eeb-4edb-b6bc-c1e80f787576
2      2019-09-15 20:26:05  0fcd64ae-9b50-4143-8bba-af817b6e9910
3      2019-09-15 20:52:17  40bb350f-9924-4c3d-b982-ec3c61087442
4      2019-09-18 16:02:46  9f82faec-2d32-48ad-b40c-02a36c30ab09
5      2019-09-18 16:13:12  77aed64d-7282-45b7-a691-d069a05b009b
6      2019-09-18 16:13:46  a773fd98-ce53-4ce3-8b67-60dae42b03a9
7      2019-09-18 18:24:35  a9ec44a0-09c2-47dc-baef-7a8e4a7bd3c3
8      2019-09-18 18:28:43  683a4339-0c25-4445-b5fc-9e9f16a5f4d0

Select a data collection index (q to quit): 4
```

List support materials (svc_dc list)

This service script is used to retrieve a summary of support materials across all appliances in the cluster or the local appliance. When you run this script on the master appliance, the support materials inventory is retrieved across all appliances in the cluster. If you run this script on an appliance that is not the master, only the inventory on the appliance is retrieved.

Format

```
svc_dc list [-h] [--debug] [-v] [--output {json}] [id]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--debug	Initiate verbose logging for debug.
-v, --verbose	Initiate verbose command output.
--output {json}	Specify the output format. JSON is the only available output format. Without JSON, the command fails.

Positional arguments

Qualifier	Description
id	Specify the data collection index ID.

Example

Retrieve the list of support materials bundles on the master appliance using the `verbose` option to retrieve additional information.

```
svc_dc list --verbose

start_timestamp    status  description  creator_type  profiles  id      appliances
2019-09-20 17:49:33 Success
APM00162303297
2019-09-21 12:10:31 Success
APM00152832910
2019-09-21 17:49:33 Success
APM00162303297
2019-09-22 17:49:33 Success
APM00162303297

Scheduled        Scheduled        Scheduled        Scheduled
System           Ess,Det         Ess,Det,Hyp+1    Ess,Det
b3a42a8a         d97e6a7a        8b0a69c2         b6bc2a8a
```

List all support material profiles (svc_dc list_profiles)

This service script is used to list the available data collection profiles and descriptions.

Format

```
svc_dc list_profiles [-h] [--debug] [-v] [--output {json}]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Qualifier	Description
--debug	Initiate verbose logging for debug.
-v, --verbose	Initiate verbose command output.
--output {json}	Render the output in JSON format.

Example

Retrieve the support materials profiles using the **svc_dc list_profiles** script. The following example lists all the valid profile values:

```
svc_dc list_profiles
Name                Prompt
essential           Collect essential data.
detailed            Collect detailed information.
hypervisor          My problem may involve the hypervisor
controlpathHeapDump Collect CP information.
nas                 Collect NAS information.
```

List all system dump files (svc_dc list_dumps)

This service script is used to retrieve all available system dump files for the entire cluster, when run on the master appliance. If you run this script on an appliance that is not the master, only the inventory for the local appliance is retrieved.

Format

```
svc_dc list_dumps [-h] [--debug] [-v] [--output {json}] [id]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--debug	Initiate verbose logging for debug.
-v, --verbose	Initiate verbose command output.
--output {json}	Specify the output format.

Positional arguments

Qualifier	Description
id	Data collection index ID.

Example

The following example would generate a list of the system dumps found on this cluster. The verbose option would include additional information.

```
svc_dc list_dumps --verbose
List a summary of the system dumps on the cluster.
```

Download an existing support materials bundle (svc_dc download)

This service script is used to download a support materials bundle to the provided destination. If no ID is specified, the script runs in interactive mode. All saved support materials bundles appear, and you can pick the bundle that you want to download using a short identifier. If an ID is specified, that support materials bundle is downloaded.

Format

```
svc_dc download [-h] [--debug] [-v] [--output {json}] [--ip value] [--path value] [--username value] [-do] [-so] [id value]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--debug	Initiate verbose logging for debug.
-v, --verbose	Initiate verbose command output.
--output {json}	Specify the JSON output format.
--ip	Destination IP on the remote host.
--path	Destination path on the remote host
--username	Username for the remote host
-do, --dump_only	Download dump data only.
-so, --service_only	Download service data only.

Positional arguments

Qualifier	Description
id	Data collection index ID.

Required name arguments

Qualifier	Description
-ip	Destination IP address on the remote host.
-path	Destination path on the remote host.
-username	Username for the remote host.
-password	Password associated with the remote username.

Example

Run the following command to download a support materials bundle with the identifier 40bb350f-9924-4c3d-b982-ec3c61087442 to the /home/eng directory:

```
svc_dc download --ip=10.12.13.45 --path=/home/eng  
--username=tom
```

```
--password=password  
40bb350f-9924-4c3d-b982-ec3c61087442
```

Upload a support materials bundle (svc_dc upload)

This service script is used to upload a data collection to CloudIQ through Secure Remote Services. If no data collection id is specified, the command runs in interactive mode. This script lists all collections and allows you to select the collection to upload using a short identifier. If you specify an ID for a collection, that collection is uploaded. The option `--skip-cp` is used to upload the data collection without using CP, even CP is working.

Format

```
svc_dc upload [-h] [--debug] [-v] [--output {json}] [--skip-cp] [-f] [id]
```

Positional Arguments

Qualifier	Description
id	Unique identifier of the support materials bundle.

Optional Arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--debug	Initiate verbose logging for debug.
-v, --verbose	Initiate verbose command output.
--output {json}	Render output in the JSON format.
--skip-cp	Upload support materials without CP, even if CP is working.
-f, --force	Force an upload of support materials even if the materials are already uploaded.

Enable or disable DDSD (svc_dd)

This script allows you to enable or disable Data Domain Storage Direct (DDSD) and DD Boost logging on a PowerStore system.

Usage

Function	System Operations
Mode	Service
Usage	Service
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster

Prerequisites	None
---------------	------

Format

```
svc_dd [-h] [--enable_ddsd_logging] [--disable_ddsd_logging] [--set_ddsd_warning]
[--set_ddsd_debug] [--set_ddsd_info] [--set_ddsd_error] [--set_ddboost_info]
[--set_ddboost_debug] [--enable_ddboost_logging] [--disable_ddboost_logging] [--
set_ddboost_error]
[--show_logging]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--enable_ddsd_logging	Enable DDSD logging.
--disable_ddsd_logging	Disable DDSD logging.
--set_ddsd_warning	Set the DDSD warning level.
--set_ddsd_debug	Set the DDSD debugging level.
--set_ddsd_info	Set the DDSD information level.
--set_ddsd_error	Set the DDSD error level.
--set_ddboost_info	Set the DD Boost information level.
--set_ddboost_debug	Set the DD Boost debugging level.
--enable_ddboost_logging	Enable DD Boost logging.
--disable_ddboost_logging	Disable DD Boost logging.
--set_ddboost_warning	Set the DD Boost warning level.
--set_ddboost_error	Set the DD Boost error level.
--show_logging	Show the status of DD Boost and DDSD logs. This option also shows the time that has elapsed since the DD Boost log was enabled.

System diagnostics (svc_diag)

This service script is used as your first tool when diagnosing issues with your system. The script enables you to check for specific issues and gather system information. This information includes the current system topology, key configuration information, and the statuses of certain major system components.

Usage

Function	Diagnostic
Mode	Normal and Service
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No

May cause data loss?	No
Scope	Appliance
Prerequisites	None

Format

```
svc_diag [-h] [-v] {run,list}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-v, --verbose	List additional content.

Actions

Action	Description
run	Run a diagnostic check. For detailed subcommand usage, use the help flag (<code>svc_diag run --help</code>).
list	List diagnostic information. For detailed subcommand usage, use the help flag (<code>svc_diag list --help</code>).

Available options for diagnostic checks (run)

Option	Description
-h, --help	Show the help message and exit.
--cw_hardware	Run the diagnostics to check for any hardware-related issues that may cause the initial configuration to fail.
--network	Run the diagnostics to check the network configuration. To check the management network cabling, specify <code>--mgmt_cabling_check</code> as an additional argument.
--workloads	Run the diagnostics to check whether an appliance contains any workloads such as storage or virtual machines.

Available options for listing diagnostic information (list)

Option	Description
--basic	List a high-level topology of the cluster and its state along with the appliances and nodes that are found in the cluster.
--alerts	List the last ten active, unacknowledged alerts. Use the following additional arguments to list further specific information: <code>--closed</code>—List the alerts that were closed in the last 24 hours. <code>--acknowledged</code>—List the last ten acknowledged alerts. To view alerts, closed and acknowledged, in the last 24 hours, you can specify both these arguments together. For example, <code>--alerts --closed --acknowledged</code>
--hardware	List all information that is related to the hardware. You can specify the following additional arguments to list information about specific components:

Option	Description
	• <code>--fault_status</code>—List information from the fault status register • <code>--inventory</code>—List the hardware inventory • <code>--sensors</code>—List sensor information • <code>--sel</code>—List serial log (SEL) information • <code>--firmware</code>—List firmware information • <code>--local_drive</code>—List local drive Smartdata information • <code>--dimm</code>—List DIMM information
<code>--storage</code>	List all information that is related to the storage. To view information about the RAID configuration on the appliance, specify <code>--raid</code> as an additional argument.
<code>--nvme_drive</code>	List all information about the nonvolatile memory express (NVMe) drives in the appliance.
<code>--network</code>	List network configuration information. To view information about management network cabling, specify <code>--mgmt_cabling</code> as an additional argument.
<code>--icw_hardware</code>	List all information that is related to the hardware checks during initial configuration.
<code>--workloads</code>	List information about the workloads, such as storage resources, hosts, and virtual machines, on the appliance. You can specify the following additional arguments to list specific workloads: • <code>--jobs</code> • <code>--sdnas</code> • <code>--volume</code> • <code>--hosts</code> • <code>--host_groups</code> • <code>--vm_vvols</code>
<code>--hypervisor</code>	List diagnostic information for the hypervisor. This information includes information about the vSphere Installation Bundles (VIBs) and changes that are made after the installation.
<code>--show_drives</code>	List the drives on the system.
<code>--expansion_resume</code>	Show the output for any attached expansion shelves (DAEs) that are connected.
<code>--cluster</code>	Show information about the cluster.
<code>--services</code>	List all system services across nodes and containers.
<code>--info</code>	Get information such as the node ID, appliance name, service tag, model, IP, and so on.
<code>--energy_star</code>	List all Energy Star-related information for the appliance. Power and temperature information is collected; this information can be sent to APEX IOPS Observability. APEX AIOps Observability is updated to display this data, providing insight into the system's carbon footprint and enabling you to track the energy efficiency and sustainability impact of your system.

Example

Use the following command to view local drive Smartdata:

```
svc_diag list --hardware --sub_options local_drive

Hardware: ===== Local Drive Smartdata =====

smartctl 7.0 2018-12-30 r4883 [x86_64-linux-4.14.19-coreos-r9999.1551750807-541] (local
build)
Copyright (C) 2002-18, Bruce Allen, Christian Franke, www.smartmontools.org

=== START OF INFORMATION SECTION ===
Model Family:      SMART Modular Technologies mSATA XR+ M.2 2280 SafeData MLC
Device Model:      SHM2S86Q240GLM22EM                118000653
Serial Number:     SPG18040AR2
Firmware Version:  FW1146
User Capacity:     240,057,409,536 bytes [240 GB]
Sector Size:       512 bytes logical/physical
```

```
Rotation Rate:      Solid State Device
Form Factor:        M.2
Device is:          In smartctl database [for details use: -P show]
ATA Version is:     ACS-2 (minor revision not indicated)
SATA Version is:    SATA 3.1, 6.0 Gb/s (current: 6.0 Gb/s)
Local Time is:      Tue Apr  2 19:25:58 2019 UTC
SMART support is:   Available - device has SMART capability.
SMART support is:   Enabled
```

Example

Use the following command to list all the Energy Star-related information for the appliance:

```
svc_diag list --energy_star

***** System Energy Star Information *****
Base Enclosure:
  Air Inlet Temperature (Celsius) : 22.00 (valid)
  Input Power (Watts)             : 1360.00 (valid)
Total Appliance InputPower (Watts) : 1360 (valid)
```

Check upgrade conversion status (svc_dip_upgrade_check)

This script displays the current data-in-place (DIP) upgrade conversion status for the appliance and related nodes.

Usage

Function	Diagnostic
Mode	Normal and Service
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_dip_upgrade_check [-h] [-d] [-f] [-p] [-e] {status}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-d, --debug	Initiate verbose logging for debugging purposes.

Qualifier	Description
-f, --File	Send the output to a log file.
-p, --platform	Show basic platform information using the IPMI tool.
-e, --engineer	Show a detailed DIP upgrade status from SYM.

Actions

Action	Description
status	Get the DIP upgrade status.

Check DIP upgrade conversion status (svc_dip_upgrade_check status)

This service script enables you to get detailed output about the status of the data-in-place (DIP) conversion.

Format

```
svc_dip_upgrade_check status [-h] [-d] [-e] [-p]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-d, --debug	Initiate verbose logging for debugging purposes.
-e, --engineer	Get detailed output on the DIP upgrade status from SYM.
-p, --platform	Get basic platform information through the IPMI tool.

Check datapath stats (svc_dp_oos_check)

This service script enables you to check the datapath stats under out-of-space status.

Usage

Function	Diagnostic
Mode	Normal and Service
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Appliance

Prerequisites	None
---------------	------

Format

```
svc_dp_oos_check [-h] [-dc] [-f]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-dc, --dc	Send the output to screen.
-f, --File	Send the output to a log file.

Collect flash and NVMe statistics (svc_drive_stats)

This service script collects flash and NVME stats from each drive in an appliance and stores that data in a file. This data sent to Dell EMC support if SupportAssist has been enabled.

Usage

Function	Diagnostic
Mode	Normal or Service
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Appliance
Prerequisites	None

Format

```
svc_drive_stats [-h] [-v] {list,run}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-v, --verbose	Initiate verbose logging for debugging purposes.

Actions

Action	Description
list	List the drive statistics collection. For details, run the --sub_options argument (<code>svc_drive_stats list --smartData --sub_options</code>).
run	Run the drive statistics collection. For details, run the --sub_options argument (<code>svc_drive_stats run --<option> --sub_options</code>).

Factory reset (svc_factory_reset)

This service script returns an appliance back to its factory-delivered state, deleting all user data and persistent configurations. You can run this script only on the master appliance.

This script is used to factory reset both nodes of a system. Both nodes must be put in service mode before running this script.

 **NOTE:** The script must be run on Node A.

To put a node in service mode, run the following commands:

- `svc_rescue_state set` (on Node A and Node B)
- `svc_node reboot` (on Node A and Node B)
- `svc_factory_reset` (on Node A only)

 WARNING:

- **This script starts a system-wide operation that resets both nodes in the system to their factory-delivered states.**
- **Only trained service personnel should run this script.**

For more information about resetting an appliance back to the factory-delivered state, see the *PowerStore Security Configuration Guide*.

Usage

Function	Recovery
Mode	Service
Usage	Technical Service
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	Yes
May cause data loss?	Yes
Scope	Appliance
Prerequisites	• Obtain a support materials bundle, and consult with your service provider. • Ensure that both nodes in the appliance are in service mode.

Format

```
svc_factory_reset [-h] [-p | --powerstoreos] [-c | --healthcheck]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-p, --powerstoreos	Use this option to factory reset the appliance to a different OS version.
-c, --healthcheck	Use this option to only run the health check.

Get a report on unreducible data (svc_get_unreducible_dp_stats)

This service script enables you to see the unreducible data statistics at the tenant level and volume family level.

 **NOTE:** This service script only shows the data for one appliance.

Perform the following steps to run the script properly:

1. Install the script: **svc_get_unreducible_dp_stats install**
2. Run the script: **svc_get_unreducible_dp_stats execute**
3. List the history results: **svc_get_unreducible_dp_stats list_results**
4. Get a specific result from the history result list: **svc_get_unreducible_dp_stats get_result -f value**
5. Remove all the results and uninstall the list: **svc_get_unreducible_dp_stats uninstall**

Usage

Function	System Operations
Mode	Normal or Service
Usage	General use
Requires service user password?	Yes
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Appliance
Prerequisites	PowerStoreOS 2.1

Format

```
svc_get_unreducible_dp_stats [-h] {get_result,list_results,execute,install,uninstall}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Positional arguments

Qualifier	Description
install	Install the <code>svc_get_unreducible_dp_stats</code> script.
uninstall	Uninstall the <code>svc_get_unreducible_dp_stats</code> script.
execute	Run the <code>svc_get_unreducible_dp_stats</code> script.
list_results	List the history results.
get_result	Get a specific result from the history list.

Get report on unreducible data (svc_get_unreducible_stats)

This service script analyzes appliance data and enables you to create an unreducible data report for an appliance and a volume family.

Usage

Function	System Operations
Mode	Normal or Service
Usage	General use
Requires service user password?	Yes
Requires root privileges?	Yes
May cause data unavailability?	No
May cause data loss?	No
Scope	Appliance
Prerequisites	PowerStoreOS 2.1

Format

```
svc_get_unreducible_stats [-h] {install,uninstall,execute,status,stop,list_results}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Positional arguments

Qualifier	Description
install	Create a results folder in the SVC container. This argument also performs the following functions: Creates folders for scripts and results in the BSC container.

Qualifier	Description
	• Copies script files to the BSC container. • Creates certificates files in the BSC container for REST calls to the CP.
uninstall	Removes all script files and folders from the BSC container and deletes certificates. Additional argument: • <code>--removes_local_results/-r [true/false]</code>: Indicates whether to also delete result files in the SVC container.
execute	Runs the BSC script anew to get unreducible stats. If you want to stop the operation, press Ctrl+C to trigger a graceful exit. Additional arguments: • <code>--size_threshold/-s</code>: VE-compressed size to be considered unreducible in the range of 0-4K. The default is 3968. • <code>--rest_port/-r</code>: Designates the port for rest calls to the CP. This argument is optional. The default port is 443.
status	Returns the run status of the script (not running or running and progress percentage).
stop	Stops a script that is running.
list_results	Returns a list of available result files in the BSC container.
get_results	Copies a specific results file from the BSC container to the SVC container. Additional argument: • <code>--file_name /-f</code>: The name of the file to be copied.
recover	Recovers the previous run based on the results file. Additional arguments: • <code>--size_threshold /-s</code>: VE-compressed size to be considered as unreducible in the range 0-4K. Optional. The default is 3968. • <code>--file_name /-f</code>: The name of file to recover.

Perform a health check on the appliance (svc_health_check)

This service script enables you to perform a health check on an appliance and list other appliance health checks.

Usage

Function	Diagnostic
Mode	Normal or Service
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Appliance
Prerequisites	None

Format

```
svc_health_check [-h] {run,list,list-profiles,list-health_checks}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Positional arguments

Qualifier	Description
run	Start an appliance health check.
list	List the preview health checks.
list-profiles	List the profiles health checks.
list-health_checks	List the health checks.

Help (svc_help)

This service script lists the available service scripts.

Usage

Function	System operations
Mode	Normal or Service
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_help [-h] [-a] [-s | --script]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Qualifier	Description
-a, --all	Show all scripts.
-s, --script	Show the help message for the script.

Hypervisor diagnostics (svc_hypervisor)

This service script enables you to collect support materials from the hypervisor on the appliances. This script also enables you to take a snapshot of the current hypervisor installation so that your service provider can identify any changes to the installation.

 **NOTE:** This script only applies to ESXi-related information.

Usage

Function	Diagnostic
Mode	Normal and Service
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Node
Prerequisites	Only applies to PowerStore X model appliances.

Format

```
svc_hypervisor [-h] {run}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
run	Collect support materials from the hypervisor on the appliance. Use the -o or -output argument to specify a directory where you want to save the collected materials.

Example

The following command shows support materials being collected and saved:

```
svc_hypervisor run --output /home/user32/hypervisor/download/
```

```

vm-support v3.3: 10:48:41, action threads 4

Non-fatal errors encountered during the run:
  Cmd "/usr/sbin/vmkping -D -v" failed with exit code 255
Please attach this file when submitting an incident report.
To file a support incident, go to http://www.vmware.com/support/sr/sr_login.jsp

To see the files collected, check '/vmfs/volumes/9XFVDH2.A.INTERNAL/esx-H0111-
host-1-2019-05-01--10.48-2358636.tgz'

Finished successfully.
/home/user32/hypervisor/download/esx-H0111-host-1-2019-05-01--10.48-2358636.tgz
Script svc_hypervisor finished successfully

```

Set limits for import service (svc_import_config)

This service script enables you to modify the configuration of the import service.

Usage

Function	Configuration
Mode	Service and Normal
Usage	Technical Service
Requires service user password?	Yes
Requires root privileges?	Yes
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_import_config [-h] {set,list}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Qualifier	Description
set	Set import configuration limits.
list	See a list of all import configurations from the management database.

Set import configuration limits (svc_import_config set)

This script enables you to set limits for an import configuration.

Format

```
svc_import_config set [-h] [--max_remote_systems <value>] [--max_import_host_systems  
<value>]  
[--max_non_disruptive_import_sessions_mirror_limit <value>] [--  
max_import_sessions_in_copy <value>]  
[--max_agentless_import_sessions_mirror_limit <value>]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--max_remote_systems	Set the maximum number of external Dell systems supported for import.
--max_import_host_systems	Set the maximum number of host systems supported for import.
--max_non_disruptive_import_sessions_mirror_limit	Set the maximum number of nondisruptive import sessions allowed with the mirror-enabled state. The system will not start a new nondisruptive active import session if the collective count of import sessions with background copy and nondisruptive ready-for-cutover is above this limit. Volume group import sessions do not count toward this limit, but each member import session does.
--max_import_sessions_in_copy	Set the maximum number of active import sessions that are supported for background copy operations. The number of new active sessions that can be started on the system varies based on the number of import sessions in the ready for cutover state. This limit should be always lesser than the max_import_sessions_in_ready_for_cutover limit.
--max_agentless_import_sessions_mirror_limit	Set the maximum number of agentless import sessions allowed with a mirror-enabled state. The system will not start a new agentless active import session if the collective count of import sessions with background copy and agentless ready for cutover is above this limit. Volume group import sessions do not count toward this limit, but each member import session does.

See all import configurations (svc_import_config list)

This service script enables you to retrieve a list of all import configurations from the management database.

Format

```
svc_import_config list [-h]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Inject troubleshooting software tool (svc_inject)

This service script provides you a secure and simple way to install validated service tools, copy software upgrade files, or install secure remote support recovery packages.

Usage

Function	Recovery
Mode	Normal
Usage	Service
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Node or Appliance
Prerequisites	Ensure that you copy the tool or package to the primary node on the appliance.

Format

```
svc_inject [-h] {status,info,generate-key,run,deactivate,delete}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
run	Install the service tool or package you have specified or enable service escalation.
delete	Delete an injected service tool or package.
info	Display information about a specific package.
generate-key	Generate a root or SupportAssist recovery package key.
deactivate	Deactivate the service escalation.
status	Report the service escalation status.

Install service tools (svc_inject run)

This service script installs a package or enables a service escalation.

Format

```
svc_inject run [-h] [-s] [-q] {package}
```

Optional Arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-s, --single	Specify this argument to install the tool on the current node only.
-q, --quiet	Suppress any additional prompts or messages.

Positional Arguments

Qualifier	Description
package	The full path to the package OR the response key for the root injection key.

Example

```
svc_inject run 18328-61346-CD9BD-AD4DC-A33B2-B8EDF-FC4BC-FD15D-00
Current Challenge: FFCD6-29923-77FEB-70E6E-B97E7-3E879

INFO: Response successfully validated!
INFO: Enabling tool ...
INFO: Successfully enabled svc_service_shell
INFO: Run "svc_service_shell" to be granted root level access for servicing this system

Script svc_inject finished successfully
```

Delete an injected service tool (svc_inject delete)

This service script deletes an injected service tool.

Format

```
svc_inject delete [-h] {tool_name}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Positional arguments

Qualifier	Description
tool_name	The name of the injected tool.

Example

```
svc_inject delete test_esx_image-0.5.0.487325.tgz.bin  
[No response if deletion was successful]
```

Display information about a specific package (svc_inject info)

This service script shows information about an injected tool.

Format

```
svc_inject info [-h] tool_name
```

Optional Arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Positional arguments

Qualifier	Description
tool_name	The name of the injected tool.

Generate a root or recovery package key (svc_inject generate-key)

This service script generates a root or SupportAssist recovery package key.

Format

```
svc_inject generate-key [-h] [-s] [r]
```

Optional Arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-s, --srs	Specify this argument to generate a SupportAssist recovery package key.
-r, --root	Specify this argument to generate a root injection key.

Example

```
svc_inject generate-key -r
Current Challenge: 671FD-217B7-2F7CC-AB547-45814-40D99
```

Deactivate service escalation (svc_inject deactivate)

This service script deactivates service escalation.

Format

```
svc_inject deactivate [-h]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Example

```
svc_inject deactivate
Service escalation has been deactivated
```

View service escalation status (svc_inject status)

This service script reports service escalation status.

Format

```
svc_inject status [-h]
```

Optional Arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Example

```
svc_inject status
INFO: Access is currently DISABLED
INFO: Current attempt is: 0 (MAX: 3)

Script svc_inject finished successfully
```

Review system journal logs (svc_journalctl)

This service script enables you to view log messages from the system journal in a consistent format. It also enables you to specify additional arguments and to filter or display additional information. Use this script as a triage tool to troubleshoot issues.

Usage

Function	Diagnostic and Recovery
Mode	Service
Usage	Service
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Node
Prerequisites	None

Format

```
svc_journalctl [-h][-r][-b ID][-k][-t value][-p value][-g value][--case-sensitive=TRUE/  
FALSE][-S value][-U value][--system][--user][-D value][--file value][-f][--output-fields  
value]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-r, --reverse	Show the newest entries first.
-b, --boot	Show current boot or the boot for the specified ID.
-k, --dmesg	Show the kernel message log from the current boot.
-t, --identifier	Show entries with the specified syslog identifier.

Qualifier	Description
-p, --priority	Filter output by message priorities or priority range.
-g, --grep	Filter output to entries where the specified field matches the specified regular expression.
--case-sensitive	Make pattern matching case sensitive or case insensitive. Valid values are <i>TRUE</i> or <i>FALSE</i> .
-S, --since	Show entries not older than the specified date.
-U, --until	Show entries not newer than the specified date.
--system	Show the system journal.
--user	Show the user journal for the current user.
-D, --directory	Show journal files from the specified directory.
--file	Show the specified journal file.
-f, --follow	Show only the most recent journal entries, and continuously print new entries as they are appended to the journal.
--output-fields	Show a comma-separated list of the fields that you want to include in the output.

Fields

The system journal contains entries with information (binary data) stored in fields with specific meaning. In addition, you can use the optional arguments to filter the information that is based on these fields or on the value that these fields contain. For example:

- The following command establishes a basic field matching query to view log messages associated with the `Platform` component. The command has a marker value of `NDU` and a message priority level of `ERROR`:

```
svc_journalctl COMPONENT=Platform MARKER=NDU PRIORITY=ERROR
```

- The following command enables you to search for a specific case-sensitive text pattern in the log messages associated with the `Platform` component:

```
svc_journalctl -g --case-sensitive=TRUE CONTEXT_ID=456abc COMPONENT=Platform
```

For more information about the journal fields, see [System Journal Fields](#).

Output Format

When you run the script, the output appears in a set order of default fields. The following is a sample of the default output from the script:

```
2019 Mar 11 14:51:45 FNM00175000815-A DEBUG CC CP bedrock.config.ConfigManagerVerticle
vert.x-eventloop-thread-0 no_ctx_id Starting to set injector.
```

Where:

Field	Value
__REALTIME_TIMESTAMP	2019 Mar 11 14:51:45
_HOSTNAME	FNM00175000815-A
PRIORITY	DEBUG
MARKER	CC
COMPONENT	CP
SUB_COMPONENT	bedrock.config.ConfigManagerVerticle
THREAD_NAME	vert.x-eventloop-thread-0

Field	Value
CONTEXT_ID	no_ctx_id
MESSAGE	Starting to set injector.

If you want to view additional fields in the output, specify them in the `--output-fields` argument. For example:

```
svc_journalctl --output-fields=CODE_LINE, CODE_FUNC

2019 Mar 11 14:51:45 FNM00175000815-A DEBUG CC CP bedrock.config.ConfigManagerVerticle
vert.x-eventloop-thread-0 no_ctx_id [814] [validatePlatformResponseStateTask] Starting
to set injector.
```

Where:

Field	Value
CODE_LINE	[814]
CODE_FUNC	[validatePlatformResponseStateTask]

Check the license status of appliances in a cluster (svc_license_status)

This service script enables you to see the license status for appliances in the cluster.

Usage

Function	System Operations
Mode	Normal
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Node
Prerequisites	None

Format

```
svc_license_status [-h] {list}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
list	Get the license status for each appliance in the cluster.

Install the PowerStore system (svc_manufacturing)

This service script eases the installation process and includes options to assist with automation and triage processes.

 **CAUTION:** Only trained service personnel should use this script.

Usage

Function	Configuration
Mode	Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	Yes
May cause data unavailability?	Yes
May cause data loss?	Yes
Scope	Node or appliance
Prerequisites	None

Format

```
svc_manufacturing [-h] [--firmware_report_full] [--check_mfg_mode_flag]
                  [--health_check] [--disable_kernel_messages]
                  [--eve_args] [--show_reinit_states]
                  [--firmware_report] [--stack_up] [--show_ssd]
                  [--show_network] [--show_dare]
                  [--network_ip_and_gateway_value]
                  [--run_all_triage] [--show_psus] [--verify_stack_up]
                  [--hardware_report] [--eve_download]
                  [--disable_network] [--verify_stack_down]
                  [--stack_down] [--enable_network]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--health_check	Perform a health check.
--eve_args	Show the arguments for the eve_download command.
--firmware_report	Show firmware information.
--stack_up	Bring the stack up.
--show_network	Display network interfaces with IP addresses.

Qualifier	Description
--network_ip_and_gateway	Specify the network IP or netmask gateway.
--show_psus	Show power supply information.
--eve_download	Download the EVE.
--hardware_report	Display resume information.
--enable_network	Enable the network.
--stack_down	Bring the stack down.
--firmware_report_full	Show detailed firmware information.
--check_mfg_mode_flag	Verify that the manufacturing process is not still in progress.
--disable_kernel_messages	Turn off kernel debug messaging.
--show_reinit_states	Display the contents of the <code>cyc_state</code> directory.
--show_ssd	Display SSD information.
--show_dare	Display D@RE information.
--run_all_triage	Run the full suite of triage commands.
--verify_stack_up	Verify that the operating system stack is up.
--disable_network	Disable the network.
--verify_stack_down	Verify that the operating system is in the factory state.

Example

The following example shows how to enable the network, specifying the network IP address and gateway:

```
svc_manufacturing --enable_network --network_ip_and_gateway 'network IP address/gateway server'
```

See and update MFS settings for SecurID (svc_mfa_state)

This service script enables you to list and update the multifactor authentication (MFA) bypass settings of the SecurID feature.

This script can be run from either node of the appliance.

Function	System Operations
Mode	Service
Usage	Service
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_mfa_state [-h] {set,list}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
set	Specify the MFA bypass setting.
list	List the MFA bypass settings.

Retrieve information system information (svc_mgmt_operations)

This service script enables you to retrieve system information using the service tool. The service tool retrieves information from the command table and the job_request table.

Usage

Function	Diagnostic
Mode	Normal or Service
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_mgmt_operations [-h] {all_locks,all_top_level_commands,command_tree,commands_by_type,
pending_locks,granted_locks_with_pending_locks,command_type_summary,failed_top_level_commands,
command_by_id,locks_by_command_id,locks_by_resource_id,command_hierarchy_for_cleanup,command_detail}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
all_locks	Query the lock request table for all locks.
all_top_level_commands	Query the command table for all top-level successful commands.
command_tree	Query the command tree.
commands_by_type	Query the command table by the command type.
command_type_summary	Query the command table by the type summary.
failed_top_level_commands	Query the command table for all top-level failed commands.
command_by_id	Query the command table by the command ID.
locks_by_command_id	Query the lock request table by the command ID.
locks_by_resource_id	Query the lock request table by the resource ID.
pending_locks	Query for all pending locks.
granted_locks_with_pending_locks	Query all granted locks with pending locks.
command_hierarchy_for_cleanup	Show the hierarchy and all associated records for given commands.
command_detail	Query command details.

Example

The following command reports information for the command tree for single or multiple commands, depending upon which option is chosen:

```
svc_mgmt_operations command_tree [-h] [--command_type <value>] [--failed_commands] [--all_commands]
[--command_id <value>]
```

```
Query command tree using query type EnumQueryCommand.all_top_level_commands
=====
+ CreateClusterCommand: 9238b9f7-03b9-4ca2-90fd-8550506b8617 - 0:07:50.057000,
2019-03-19 16:15:59.385000+00:00 / 2019-03-19 16:23:49.442000+00:00
  +---SystemDataCollectionCommand: e566df31-49c4-4924-ad3f-e958122e57a7 -
0:01:03.672000, 2019-03-19 16:23:49.500000+00:00 / 2019-03-19 16:24:53.172000+00:00
    +---FiremanCommand: 65b7469f-9712-4b92-b1df-57132e43a783 - 0:01:03.250000,
2019-03-19 16:23:49.869000+00:00 / 2019-03-19 16:24:53.119000+00:00
      +---CheckAndUpdateLocalConfigStateCommand: 85d67f90-4bc9-4779-80de-a4c8251620a4 -
0:00:00.015000, 2019-03-19 16:23:49.108000+00:00 / 2019-03-19 16:23:49.123000+00:00
        +---UpdateClusterSoftwareInstalledCommand: 3fcf074a-bf39-4ac3-821d-67da230f9a51 -
0:00:00.053000, 2019-03-19 16:23:48.957000+00:00 / 2019-03-19 16:23:49.010000+00:00
          +---InsertX509CertificateCommand: 2e3d2cb1-4aa7-435c-ab41-a34ccc75b3a5 -
0:00:00.583000, 2019-03-19 16:23:48.265000+00:00 / 2019-03-19 16:23:48.848000+00:00
            +---InsertX509CertificateCommand: dc05f685-e94b-4748-9ad0-4511b5aaad99 -
0:00:00.311000, 2019-03-19 16:23:47.456000+00:00 / 2019-03-19 16:23:47.767000+00:00
              +---InsertX509CertificateCommand: 14268e96-87fc-46db-9c68-ed3bea63037e -
0:00:00.563000, 2019-03-19 16:23:46.839000+00:00 / 2019-03-19 16:23:47.402000+00:00
                +---InsertX509CertificateCommand: a1904d62-97fb-4eaf-8480-1249e8cf060b -
0:00:00.314000, 2019-03-19 16:23:46.476000+00:00 / 2019-03-19 16:23:46.790000+00:00
```

```

+---InsertX509CertificateCommand: ce22f112-f9fe-4c28-b95e-6d7089257d1f -
0:00:00.315000, 2019-03-19 16:23:42.823000+00:00 / 2019-03-19 16:23:43.138000+00:00
+---InsertX509CertificateCommand: 0d0046d5-7700-4978-badc-f916252aed2c -
0:00:00.418000, 2019-03-19 16:23:29.845000+00:00 / 2019-03-19 16:23:30.263000+00:00
+---SaveClusterNetworkObjectsCommand: 62dbffb5-a207-4098-a226-a9e6a0fa0d6d -
0:00:00.051000, 2019-03-19 16:23:08.579000+00:00 / 2019-03-19 16:23:08.630000+00:00
+---UpdateMtuCommand: 73727a67-b5ce-4e70-86f3-ee5ad383ce1d - 0:00:00.971000,
2019-03-19 16:23:05.614000+00:00 / 2019-03-19 16:23:06.585000+00:00
+---PerformUpdateMtuCommand: 38e0b04f-ba03-49ad-9b4e-b573a3af32c4 -
0:00:00.207000, 2019-03-19 16:23:06.274000+00:00 / 2019-03-19 16:23:06.481000+00:00
+---GetDarePropertiesCommand: f18864e1-7a20-426b-912d-f75d8ac82258 - 0:00:00.034000,
2019-03-19 16:23:05.152000+00:00 / 2019-03-19 16:23:05.186000+00:00
+---JoinClusterCommand: b0798f68-eb1c-4ba4-aeeb-3ccedcdad52f - 0:07:01.089000,
2019-03-19 16:16:03.961000+00:00 / 2019-03-19 16:23:05.050000+00:00
+---ModifySSHConfigCommand: e69d580a-f226-4dce-b170-cab9a45d0e33 - 0:00:01.713000,
2019-03-19 16:23:03.180000+00:00 / 2019-03-19 16:23:04.893000+00:00
+---CreateStorageContainerCommand: 7a23b7fd-d09f-4965-8838-57cbe744a631 -
0:00:00.656000, 2019-03-19 16:23:02.284000+00:00 / 2019-03-19 16:23:02.940000+00:00
+---QueryAndSaveSoftwareInstalledCommand: cb999a45-fe40-4203-802f-f7726c36a86b -
0:00:00.664000, 2019-03-19 16:22:56.681000+00:00 / 2019-03-19 16:22:57.345000+00:00

=====
=====

+ PlatformEventSendCommand: ef27ab54-cb8b-483f-9836-e3e782525564 - 0:00:22.442000,
2019-03-19 16:23:02.246000+00:00 / 2019-03-19 16:23:24.688000+00:00

=====
=====

+ CreateLocalSystemCommand: 1a57f5fc-e63f-494c-85ac-ffc4fa95e2a2 - 0:00:21.017000,
2019-03-19 16:23:49.265000+00:00 / 2019-03-19 16:24:10.282000+00:00
+---CreateRediscoverTransitConnectionCommand: e480f0a2-0596-4e1d-b4ff-cfac4b271285 -
0:00:08.363000, 2019-03-19 16:24:01.908000+00:00 / 2019-03-19 16:24:10.271000+00:00
+---CreateTransitConnCommand: 0ea9a5c0-7445-4b6c-895e-2c2708c0f6b1 -
0:00:00.613000, 2019-03-19 16:24:09.627000+00:00 / 2019-03-19 16:24:10.240000+00:00
+---CreateHostCommand: 406bb834-5267-4e8f-9156-994cc07a3476 - 0:00:00.881000,
2019-03-19 16:23:52.687000+00:00 / 2019-03-19 16:23:53.568000+00:00
+---ConnectHostToStorageCommand: b9d2c573-4b0b-46cf-a126-ala4e42e2e88 -
0:00:00.629000, 2019-03-19 16:23:52.877000+00:00 / 2019-03-19 16:23:53.506000+00:00
+---AddEndPointToInitiatorGroupCommand: ee340164-355b-4313-a39b-209f20824ce1 -
0:00:00.156000, 2019-03-19 16:23:53.294000+00:00 / 2019-03-19 16:23:53.450000+00:00
+---AddEndPointToInitiatorGroupCommand: 1605ea79-683a-4a59-b561-e6545ccdcc89 -
0:00:00.116000, 2019-03-19 16:23:53.284000+00:00 / 2019-03-19 16:23:53.400000+00:00
+---AddInitiatorCommand: alfd4ee-9c84-4cb8-8073-4845b3057786 -
0:00:00.104000, 2019-03-19 16:23:53.145000+00:00 / 2019-03-19 16:23:53.249000+00:00
+---AddInitiatorCommand: 4f501a6e-6781-4fe9-854b-97d21ea08866 -
0:00:00.089000, 2019-03-19 16:23:53.144000+00:00 / 2019-03-19 16:23:53.233000+00:00
+---AddInitiatorGroupCommand: 13ad6e5c-191b-4346-9d3f-b9a65140b527 -
0:00:00.187000, 2019-03-19 16:23:52.927000+00:00 / 2019-03-19 16:23:53.114000+00:00

=====
=====

+ ApplianceRemoteSupportConnectivityStatusCommand: 8148cc9d-9aa7-44cc-b66c-5a5d495b1e25
- 0:00:00.004000, 2019-03-19 20:07:57.130000+00:00 / 2019-03-19 20:07:57.134000+00:00

Completed Query command tree using query type EnumQueryCommand.all_top_level_commands

```

Retrieve information as a root user (svc_mgmt_operations all_top_level_commands)

This service script enables you to retrieve information using the service tool as a root user. The service tool retrieves information from the command table for all top level successful commands.

Format

```
svc_mgmt_operations all_top_level_commands [-h] [--sort_processing_time]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--sort_processing_time	Sort processing time.

See command details (svc_mgmt_operations command_detail)

This service script enables you to query commands using filters and see details for each command.

Usage

Function	Diagnostic
Mode	Normal or Service
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_mgmt_operations command_detail [-h] [--command_id <value>]
[--command_type [command_type value]] [--command_state [{INITIAL,QUEUED,RUNNING,
COMPLETED}]] [--start_after <value>] [--end_after
<value>] [--processing_longer_than <value>]
[--processing_shorter_than <value>] [--top_level_commands]
[--response_status [{OK,VALIDATION_ERROR,NOT_FOUND_ERROR,ERROR,INTERNAL_ERROR,
UNKNOWN,RUNNING,CANCELLED,UNRECOVERABLE_ERROR,BUSY} [{OK,VALIDATION_ERROR,
NOT_FOUND_ERROR,ERROR,INTERNAL_ERROR,UNKNOWN,RUNNING,CANCELLED,UNRECOVERABLE_ERROR,
BUSY} ...]]] [--response_state {CREATED,ACKNOWLEDGED}]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--command_id	Show the command by ID.
--command_type	Show commands that match the specified command type.
--command_state	Show commands that match the specified command state.

Qualifier	Description
--start_before	Show commands that started before the specified time.
--end_before	Show commands that ended before the specified time.
--start_after	Show commands that started after the specified time.
--end_after	Show commands that ended after the specified time.
--processing_longer_than	Show commands with a processing time longer than the specified interval.
--processing_shorter_than	Show commands with a processing time shorter than the specified interval.
--top_level_commands	Filter nontop-level commands.
--response_status	Show commands that match the specified response status.
--response_state	Show commands that match the specified response state.

Example

The following example shows detailed output for the command **svc_mgmt_operations command_detail** when searching for error responses within a one-day period:

```
svc_mgmt_operations command_detail --response_status ERROR --end_before "1 day ago"
Query command details using filter (end_time < (current_timestamp - interval '1 day'))
AND (response_status = 'ERROR')
=====
=====
Command : com.emc.cyclone.contexts.elicense.domain.commands.LicenseRetrieveCommand
id : 9alcee95-6854-4e1b-84c1-d87d8ece660c
command type : com.emc.cyclone.contexts.elicense.domain.commands.LicenseRetrieveCommand
internal : False
command json :
{"executionLocation":"CLUSTER_MASTER","userRole":"","is_restartable":true,"submit_time":"
2021-10-13T08:06:45.473142Z","is_encrypted":false,"canQueue":true,"retention_period":0}
work unit status : FAILED
perc. complete : 100
processing time: 0:00:39.854691
start time : 2021-10-13 08:06:45.762335+00:00
end time : 2021-10-13 08:07:25.617026+00:00
completion time : None
percent. completed time : 100
status response : ERROR
response class name : com.emc.bedrock.command.SimpleCommandResponse
messages : [{"code": "0xE0D010020005", "@class":
"com.emc.bedrock.core.LocalizableMessage", "severity": "ERROR", "arguments": ["Failed to
get the token"], "description": null, "localizedMessage": null, "resourceBundleName":
"com.emc.cyclone.messages.elicense.Elicense", "encodedLocalizedJson": null}]
json response : {}
```

Show and filter command records (svc_mgmt_operations command_hierarchy_for_cleanup)

This service script shows all the records that are associated with commands. You can filter these records according to the type of command and the various states of the commands.

Usage

Function	Diagnostic
Mode	Normal or Service
Usage	General use

Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_mgmt_operations command_hierarchy_for_cleanup [-h] [--command_id <value>]
[--command_type [command_type value]] [--command_state [{INITIAL,QUEUED,RUNNING,
COMPLETED}]] [--start_after <value>] [--end_after
<value>] [--processing_longer_than <value>]
[--processing_shorter_than <value>] [--top_level_commands]
[--response_status [{OK,VALIDATION_ERROR,NOT_FOUND_ERROR,ERROR,INTERNAL_ERROR,
UNKNOWN,RUNNING,CANCELLED,UNRECOVERABLE_ERROR,BUSY} [{OK,VALIDATION_ERROR,
NOT_FOUND_ERROR,ERROR,INTERNAL_ERROR,UNKNOWN,RUNNING,CANCELLED,UNRECOVERABLE_ERROR,
BUSY} ...]]] [--response_state {CREATED,ACKNOWLEDGED}]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--command_type	Show commands that match the specified command type.
--command_state	Show commands that match the specified command state. You can filter the records to only show commands in the following states: • INITIAL • QUEUED • RUNNING • COMPLETED
--start_before	Show commands that started before the specified time.
--end_before	Show commands that ended before the specified time.
--start_after	Show commands that started after the specified time.
--end_after	Show commands that ended after the specified time.
--processing_longer_than	Show commands with a processing time longer than the specified interval.
--processing_shorter_than	Show commands with a processing time shorter than the specified interval.
--top_level_commands	Filter nontop-level commands.
--response_status	Show commands that match the specified response status. You can filter the records to only show commands in the following states: • OK • VALIDATION_ERROR • NOT_FOUND_ERROR • ERROR • INTERNAL_ERROR • UNKNOWN • RUNNING • CANCELLED • UNRECOVERABLE_ERROR

Qualifier	Description
	BUSY
--response_state	Show commands that match the specified response state. You can filter the records to only show commands in the following states: CREATED ACKNOWLEDGED

Positional arguments

Qualifier	Description
command_id	Show the hierarchy of commands; enter each UUID separated by commas.

Example

The following example shows a query and output for finding running and initial commands:

```
svc_mgmt_operations command_hierarchy_for_cleanup --command_state INITIAL RUNNING
Command hierarchy for cleanup using filter command_state IN ('INITIAL', 'RUNNING')
+ command: 99d81ed0-0989-46b8-b033-ba3d6a87bdc4 - DoPingCommand RUNNING Resource:
None (None)
* work_unit: 7f1a1776-d832-4373-a139-1a6c7758e9fa - [internal]
IN_PROGRESS Progress: 0%
Time: 2021-10-14T10:06:53.156319+00:00 / None
```

Display the command tree (svc_mgmt_operations command_tree)

This service script displays the command tree for single or multiple commands, depending upon the option that you enter.

Usage

Function	Diagnostic
Mode	Normal or Service
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_mgmt_operations command_tree [-h] [--all_commands] [--failed_commands]
[--command_id <value>] [--command_type [command_type
value]] [--command_state [{INITIAL,QUEUED,RUNNING,COMPLETED}]]
[--start_after <value>]
[--end_after <value>] [--processing_longer_than <value>]
[--processing_shorter_than <value>] [--top_level_commands]
[--response_status [{OK,VALIDATION_ERROR,NOT_FOUND_ERROR,ERROR,INTERNAL_ERROR,
UNKNOWN,RUNNING,CANCELLED,UNRECOVERABLE_ERROR,BUSY} [{OK,VALIDATION_ERROR,
```

```
NOT_FOUND_ERROR,ERROR,INTERNAL_ERROR,UNKNOWN,RUNNING,CANCELLED,UNRECOVERABLE_ERROR,
BUSY} ...]]] [--response_state {CREATED,ACKNOWLEDGED}]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--all_commands	Show top-level commands with the response status OK.
--failed_commands	Show top-level commands with the response status ERROR.
--command_id	Show the command by ID.
--command_type	Show commands that match the specified command type.
--command_state	Show commands that match the specified command state. You can filter the records to only show commands in the following states: • INITIAL • QUEUED • RUNNING • COMPLETED
--start_before	Show commands that started before the specified time.
--end_before	Show commands that ended before the specified time.
--start_after	Show commands that started after the specified time.
--end_after	Show commands that ended after the specified time.
--processing_longer_than	Show commands with a processing time longer than the specified interval.
--processing_shorter_than	Show commands with a processing time shorter than the specified interval.
--top_level_commands	Filter nontop-level commands.
--response_status	Show commands that match the specified response status. You can filter the records to only show commands in the following states: • OK • VALIDATION_ERROR • NOT_FOUND_ERROR • ERROR • INTERNAL_ERROR • UNKNOWN • RUNNING • CANCELLED • UNRECOVERABLE_ERROR • BUSY
--response_state	Show commands that match the specified response state. You can filter the records to only show commands in the following states: • CREATED • ACKNOWLEDGED

Example

The following example shows the output for the command **svc_mgmt_operations command_tree** when searching for error responses within a one-day period:

```
svc_mgmt_operations command_tree --response_status ERROR --end_before "1 day ago"
Query command tree using filter (end_time < (current_timestamp - interval '1 day')) AND
```

```

(response_status = 'ERROR')
=====
=====

+ LicenseRetrieveCommand: 9a1cee95-6854-4e1b-84c1-d87d8ece660c - 0:00:39.854691,
2021-10-13 08:06:45.762335+00:00 / 2021-10-13 08:07:25.617026+00:00

=====
=====

+ SupportMetricsCaptureCommand: 2ba04890-33a2-460a-9486-95f35851bea0 - 0:00:12.819054,
2021-10-13 08:54:52.413837+00:00 / 2021-10-13 08:55:05.232891+00:00
+---FiremanCommand: 57d9a1ba-005c-4d1b-aaee-7e4b96d985e9 - 0:00:12.151396, 2021-10-13
08:54:52.765127+00:00 / 2021-10-13 08:55:04.916523+00:00

=====
=====

+ SupportMetricsCaptureCommand: 2e2766ca-02f7-43ff-b236-5b45709a396b - 0:00:10.893175,
2021-10-13 09:44:52.418265+00:00 / 2021-10-13 09:45:03.311440+00:00
+---FiremanCommand: f135af21-5a11-462e-a96d-7388a6ae2cad - 0:00:10.520132, 2021-10-13
09:44:52.761297+00:00 / 2021-10-13 09:45:03.281429+00:00

=====
=====

+ EventsAlertsAgingCommand: bc14dfdf-5d06-499d-a0e1-9808e82d1d03 - 0:00:00.082732,
2021-10-13 08:09:34.234645+00:00 / 2021-10-13 08:09:34.317377+00:00

Completed Query command tree using filter (end_time < (current_timestamp - interval '1
day')) AND (response_status = 'ERROR')

```

Migrate a cluster or DVS to another vCenter (svc_migrate_to_vcenter)

This service script enables you to restore or migrate a PowerStore Cluster and Distributed Virtual Switch (DVS) configuration from one vCenter to another.

Usage

Function	Diagnostic
Mode	Normal or Service
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	vCenter
Prerequisites	None

Format

```
svc_migrate_to_vcenter [-h] [--verbose] [--quiet] [--force] [--debug]  
{restore_on_vcenter,  
migrate_to_vcenter,fix_restore_issues}
```

Optional arguments

Action	Description
-h, --help	Show this help message and exit.
--verbose	Initiate verbose logging for debugging.
--quiet	Suppress any additional prompts or messages.
--force	Ignore warnings; force a reboot that might result in data becoming unavailable.
--debug	Increase the logging level to debug and print logs to the console.

Actions

Action	Description
restore_on_vcenter	Restore the vCenter configuration if access to the previous vCenter is lost.
migrate_to_vcenter	Migrate PowerStore from one vCenter to another.
fix_restore_issues	Remove empty proxy switches from ESXs if needed. Run this command if prompted by the restore_on_vcenter or migrate_to_vcenter commands.

Migrate to vCenter (svc_migrate_from_vcenter migrate_to_vcenter)

This service script migrates PowerStore from one vCenter to another.

Format

```
svc_migrate_from_vcenter migrate_to_vcenter [-h] [--generate_config] config
```

Optional arguments

Action	Description
-h, --help	Show the help message and exit.
--generate_config	Only generate template config and finish.

Positional arguments

Action	Description
config	JSON config file that should have the following structure: <pre>{'cluster_name': '<Optional. Allows to redefine name for ESX cluster in a new vCenter>', 'old_vcenter': {'password': '<Password for current vCenter>'}, 'esxs': [{'host': '<ESXi IP/host>', 'password': '<ESXi root password>'}, {'host': '<ESXi IP/host>', 'password': '<ESXi root password>'}], 'power_store': {'password': '<PowerStore password>', 'user': '<PowerStore user>'}, 'provider_name': '<Optional. Allows to redefine Storage provider name in a new vCenter>', 'vcenter': {'host': '<vCenter IP/host>', 'password': '<vCenter password>', 'user': '<vCenter username>'}, 'data_center_name': '<Optional. Allows to redefine Data Center name in a new vCenter>'}</pre>

Restore the vCenter configuration (svc_migrate_to_vcenter restore_on_vcenter)

This service script restores the vCenter configuration if access to the previous vCenter has been lost.

Format

```
usage: svc_migrate_to_vcenter restore_on_vcenter [-h] [--generate_config] config
```

Optional arguments

Action	Description
-h, --help	Show the help message and exit.
--generate_config	Only generate the template configuration and finish.

Positional arguments

Action	Description
config	The JSON config file should have the following structure: <pre>{'data_center_name': '<Optional. Allows to redefine Data Center name in a new vCenter>', 'provider_name': '<Optional. Allows to redefine Storage provider name in a new vCenter>', 'cluster_name': '<Optional. Allows to redefine name for ESX cluster in a new vCenter>', 'esxs': [{'host': '<ESXi IP/host>', 'password': '<ESXi root password>'}, {'host': '<ESXi IP/host>', 'password': '<ESXi root password>'}], 'vcenter': {'host': '<vCenter IP/host>', 'password': '<vCenter password>', 'user': '<vCenter username>'}, 'power_store': {'password': '<PowerStore password>', 'user': '<PowerStore user>'}}</pre>

Remove empty proxy switches (svc_migrate_to_vcenter fix_restore_issues)

This service script removes empty proxy switches from ESXs if needed. Run this command if prompted by the `restore_on_vcenter` or `migrate_to_vcenter` commands.

Format

```
svc_migrate_to_vcenter fix_restore_issues [-h] [--generate_config] config
```

Optional arguments

Action	Description
<code>-h, --help</code>	Show the help message and exit.
<code>--generate_config</code>	Only generate the template configuration and finish.

Positional arguments

Action	Description
<code>config</code>	The JSON config file that should have the following structure: <pre>{'cluster_name': '<Cluster name>', 'vcenter': { 'host': '<vCenter IP/host>', 'password': '<vCenter password>', 'user': '<vCenter username>' }, 'data_center_name': '<Datacenter name>' }</pre>

Enable or disable autodownload (svc_modify_autodownload)

The service script enables you to enable or disable the autodownload feature.

Usage

Function	System Operations
Mode	Normal
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Node
Prerequisites	None

Format

```
svc_modify_autodownload [-h] [-t] [-e] [-d]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-t, --trigger	Trigger an autodownload check.
-e, --enable	Enable autodownload.
-d, --disable	Disable autodownload.

Run service scripts using SSH tunneling (svc_nas)

This service script enables you to run NAS service scripts from the service container to provide unified serviceability in addition to faster diagnosis and remediation.

Usage

Function	Diagnostic
Mode	Normal or Service
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_nas [-h] [-d]{download,list,run}
```

Optional arguments

Action	Description
-h, --help	Show this help message and exit.
-d, --debug	Increase logging level to debug and print logs to console.

Actions

Action	Description
download	Download files generated by the NAS scripts. <code>svc_nas download <username> <destination ip-address> <destination path></code> . A list of available files is presented with the option to select multiple files at once to download.
list	List the supported NAS scripts.
run	Run the specified NAS service script in the format: <code>svc_nas run <script> <script-options></code> .

Specific SDNAS scripts

The following additional commands enable you to run SDNAS scripts through the service container:

Script	Description
<code>nas_svc_acldb_dump</code>	Downloads the ACL database of an online file system.
<code>nas_svc_dac</code>	Enables you to manage Dynamic Access Control (DAC).
<code>nas_svc_dataprotection</code>	Manages data protection.
<code>nas_svc_dc</code>	Generates an archive file with SDNAS materials.
<code>nas_svc_imt</code>	Performs actions on an inband migration tool (IMT).
<code>nas_svc_log</code>	Display all available SDNAS logs.
<code>nas_svc_nas</code>	Enables you to manage NAS servers.
<code>nas_svc_paxstats</code>	Displays advanced statistics for NDMP and PAX backup sessions.
<code>nas_svc_tcpdump</code>	Enables you to run a Linux tcpdump operation.

Download the ACL database of a file system (`svc_nas nas_svc_acldb_dump`)

This script downloads the ACL database of an online file system to enable you to troubleshoot security issues.

Usage

Function	Diagnostic
Mode	Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	Yes
May cause data unavailability?	Yes
May cause data loss?	No
Scope	Node
Prerequisites	None

Format

```
svc_nas nas_svc_acldb_dump [-h] {<NAS server name> options} [-d] [-fs <file system name>] [-o <target directory>]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-d, --dump	Dump the ACL database.
-fs	Specify the file system by name.
-o, --outpath	Specify the target directory. If the directory does not exist, it is created.

Manage Dynamic Access Control (svc_nas nas_svc_dac)

This script enables you to manage Microsoft Dynamic Access Control (DAC), which allows you to establish access rules.

Usage

Function	System Operations
Mode	Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	No
May cause data unavailability?	Yes
May cause data loss?	No
Scope	Node
Prerequisites	None

Format

```
svc_nas nas_svc_dac [-h] [-e {ALL}] [-d {ALL}] [-s {ALL}] [--cap-staging-enable <value>]
[cap-staging-disable <value>] [-v <value>] [-i --dn value {--dn <distinguished policy name>}]
[-p <compname> --dn <value>] [-v <value>] [--delete <value>] [--add-recovery-rule <value>
--rule-name <value> {--resource-condition <value>} {--effective-security <value>}]
[--delete-recovery-rule <value> --rule-name <value> {--resource-condition <value>}
{--effective-security <value>}]
```

Optional arguments

Table 1. Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-e, --enable	Enable DAC on the system VDM. You must specify ALL.

Table 1. Optional arguments (continued)

Qualifier	Description
-d, --disable	Disable DAC on the system VDM. You must specify ALL.
-s, --state	Show the current state of DAC on the system VDM. You must specify ALL.
--cap-staging-enable	Enable evaluation of proposed permissions for the system VDM.
--cap-staging-disable	Disable evaluation of proposed permissions for the system VDM. This setting is the default.
-v, --verbosity	Set the level for log messages associated with the system VDM. Specifying a dbg2 or dbg3 level reduces system performance.
-i, --info	Show details of all policies in the policy manager. <pre>svc_nas nas_svc_dac [-i --info <value>></pre> You can specify a policy by adding the following: • The distinguished name • The policy ID
-p, --preload	Load the policy with the specified distinguished name into the policy manager associated with the Active Directory system name.
-r, --refresh	Refresh all policies in the policy manager associated with the Active Directory system name. Policies that no longer exist in the Active Directory are deleted.
-d, --delete	Delete the policy with the specified policy ID from the policy manager associated with the Active Directory system name.
--add-recovery-rule	Add a recovery rule with the specified distinguished name to the policy manager associated with the Active Directory system name. You can specify the following with this command: • The rule name is the name of the new rule. • --resource_condition is an expression that is used to determine the resources the new recovery rule applies to. Omitting this option (or specifying the empty string) means that the new rule is applicable to all resources. • --effective_security is an SDDL ACL that specifies the effective security for the new recovery rule.
--delete-recovery-rule	Delete a recovery rule with the specified distinguished name to the policy manager associated with the Active Directory system name.

Positional arguments

Qualifier	Description
--dn	Specify the distinguished name in the policy manager that is associated with the Active Directory computer name: <pre>svc_nas nas_svc_dac --info <value> --dn <value></pre>

Qualifier	Description
--id	Specify the policy in the policy manager associated with the Active Directory computer name: <pre>svc_nas nas_svc_dac --info <value> --id <value></pre>
--rule-name	Add the name of the new rule: <pre>svc_nas nas_svc_dac --add-recovery-rule <value> --rule-name <value></pre>
--resource-condition	Specify the resources to which the new recovery rule applies: <pre>svc_nas nas_svc_dac --resource-condition <value></pre>
--effective-security	This SDDL ACL specifies the effective security for the new recovery rule: <pre>svc_nas nas_svc_dac effective-security <value></pre>

Generate NAS output files (svc_nas nas_svc_data_protection)

This script enables advanced management of data protection for replication sessions, remote systems, and data protection networks.

Usage

Function	System Operations
Mode	Normal
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_nas run nas_svc_dataprotection -h {nasServer | remoteSystem | dpNetwork} {actions}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Arguments for nasServer

```
nas_svc_dataprotection nasServer [-h] [-vdmoid <NAS server id>] [-action  
-fsoid <file system id> {listreplicationinfo [-f],displayinfo,validate,cleanupdb,
```

```
cleanupcmddb, cleanupfsreplicationsession, displaydntasks, displaycltasks, cleanupcltasks, repair,
remove, -
path, startsession, stopsession, failoversession, switchoversession, switchtoproductionmode}]
```

Qualifier	Description
-h, --help	Show the help message and exit.
-vdmoid	The ID of the NAS server.
-action	Perform the specified action.
-fsoid	The ID of the file system replication version set.
-path	The NAS server path.

Actions for nasServer

Action	Description
listreplicationinfo [-f, -force]	List replication objects of the NAS server from databases. The NAS server must be in service mode when <i>-force</i> is set to allow the command to run even if the NAS server is not in service mode.
displayinfo	Display the NAS server in-memory replication session information.
validate	Validate all replication databases for the NAS server.
cleanupdb	Clean up all databases that are related to the NAS server replication objects.
cleanupcmddb	Clean up command and command cmd queue databases.
cleanupfsreplicationsession -fsId	Remove all records that are related to one FS replication session from replication databases. The format of the command is as follows: <pre>nas_svc_dataprotection nasServer -action cleanupfsreplicationsession -fsId <FS replication version set ID></pre>
displaydntasks	Display all data node tasks that are related to the NAS server replication session.
displaycltasks	Display all cluster tasks that are related to the NAS server replication session.
cleanupcltasks	Terminate all cluster tasks that are related to the NAS server replication session.
repair	Repair a NAS server replication database. The format of the command is as follows: <pre>nas_svc_dataprotection nasServer -action repair -path <path> -content <database content></pre>
remove	Remove a NAS server replication database. The format of the command is as follows: <pre>nas_svc_dataprotection nasServer -action remove -path <path></pre>
startsession	Specify the ID of the file system start with the reverse option when reverse is set. The format of the command is as follows: <pre>nas_svc_dataprotection nasServer -action startsession -fsoid <GUID> [-reverse]</pre>

Action	Description
stopsession	Specify the ID of the file system stop with local mode when local is set. The format of the command is as follows: <pre>nas_svc_dataprotection nasServer -action stopsession -fsoid <GUID> [-local]</pre>
failoversession	Fail over the replication session of the specified file system. The format of the command is as follows: <pre>nas_svc_dataprotection nasServer -action failoversession -fsoid <GUID></pre>
switchoversession	Switch over to another replication session. The format of the command is as follows: <pre>nas_svc_dataprotection nasServer -action switchoversession -fsoid <GUID></pre>
switchtoproductionmode	Switch the NAS server to destination mode.

Arguments for remoteSystem

```
nas_svc_dataprotection remoteSystem [-h] {-list {-all | -inuse} -info -id <-rsid> -sessionID <session id> -add -remove -delete
```

Qualifier	Description
-h, --help	Show the help message and exit.
-list	List the remote systems. You can list either -all for all the remote systems or -inuse for only the systems in use.
-info	Display information about a specified remote system from the database. The format of the command is as follows: <pre>nas_svc_dataprotection remoteSystem -info -id <rsid></pre>
-id	The ID of the remote system. The format of the command is as follows: <pre>nas_svc_dataprotection remoteSystem -info -id <rsid> -sessionId <id></pre>
-sessionId	The ID of the session. The format of the command is as follows: <pre>nas_svc_dataprotection remoteSystem -info -id <rsid> -sessionId <id></pre>
-add	Add a specified session to a specific remote system. The format of the command is as follows: <pre>nas_svc_dataprotection remoteSystem -add -id <rsid> -sessionId <id></pre>
-remove	Remove a specified session ID from a specific remote system. The format of the command is as follows: <pre>nas_svc_dataprotection remoteSystem -remove -id <rsid> -sessionId <id></pre>
-delete	Delete the specified remote system database record. The format of the command is as follows: <pre>nas_svc_dataprotection remoteSystem -delete -id <rsid></pre>

Arguments for dpNetwork

```
nas_svc_dataprotection dpNetwork [-h] -list {-all | -inuse} -info -repair -cleanuporphan  
-id <data protection network id> -silent
```

Qualifier	Description
-h, --help	Show the help message and exit.
-list	List the data protection networks. You can list either -all for all the remote systems or -inuse for only the systems in use.
-info	Display data protection network information.
-repair	Repair the database record of the data protection network cluster.
-id	The ID of the data protection network.
-cleanuporphan	Delete orphan data protection network interfaces.
-silent	No questions are asked.

Generate an SDNAS archive file (svc_nas nas_svc_dc)

This service script generates an archive file with SDNAS materials. You can download this archive through REST using the supportMaterial REST objects.

The script collects system information and SDNAS materials for triaging and resolving problems. The data collected includes system configurations, logs, run-time data, and other information. Running this script without any options retrieves the full data.

Usage

Function	System Operations
Mode	Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	No
May cause data unavailability?	Yes
May cause data loss?	No
Scope	Node
Prerequisites	None

Format

```
svc_nas nas_svc_dc [-h] [-collect] [-noEtc]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-collect	Collect SDNAS materials (default).

Qualifier	Description
-noEtc	Do not collect the .etc directory of the NAS servers.

Manage NAS servers (svc_nas nas_svc_nas)

This script allows you to manage NAS servers at an advanced level, including managing NAS server parameters, database maintenance, and network troubleshooting.

Usage

Function	System Operations
Mode	Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	No
May cause data unavailability?	Yes
May cause data loss?	No
Scope	Node
Prerequisites	None

Format

```
svc_nas nas_svc_nas {<NAS_server_name> | ALL} [-cava] [-checkup] [-dbms] [-dhsm] [-orphan] [-dns] [-ds] [-eventpub] [-fs] [-kerberos] [-ldap] [-list] [-lockd] [-nis] [-param] [-restart] [-security] [-vhdx]
```

Optional arguments

Qualifier	Description
-cava	Manages the anti-virus service settings of the specified NAS server.
-checkup	Run internal tests that help to root cause potential configuration or environmental errors.
-dbms	Perform the operation on databases.
-dhsm	Perform DHSM operations
-orphan	List or delete orphan Smb share or Nfs export
-dns	Display the DNS settings of the NAS server and perform a DNS lookup.
-ds	Display the Windows Directory Service.
-eventpub	Display file event publishing settings and connection status to CEPA servers
-fs	Upload or download a file to the .etc directory of the NAS server.
-kerberos	Display the current Kerberos settings of the NAS server.
-ldap	Display the LDAP settings of the NAS server and perform LDAP operations.
-list	Display the list of NAS servers.
-lockd	Manage file locks on the NAS servers.

Qualifier	Description
-nis	Display the NIS settings of the NAS server and perform an NIS lookup.
-param	Manage the parameters of the NAS server.
-restart	Restart the specified NAS server.
-security	Display security components (PKI certificates and more)
-vhdx	Display VHDX metadata (Hyper-V virtual disk files).

Manage an IMT import (svc_nas nas_svc_imt)

This service script enables you to manage an In-band Migration Tool (IMT) import. You can use this script to perform such actions as forcibly clearing failed nodes to allow a stalled IMT import to finish.

Usage

Function	System Operations
Mode	Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	No
May cause data unavailability?	Yes
May cause data loss?	No
Scope	Node
Prerequisites	None

Format

```
svc_nas run nas_svc_imt -h <NAS server name> [-i { <import session id> | --all | --failed}] [-n {id | --all}] [-f] [-s] [-r] [-c] [-d] [-l] [-t]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message.
-i, --show-imports	Show the ID and state of file system imports for the specified NAS server. The format of the command is as follows: <pre>nas_svc_imt <NAS server name> [-i --show-imports] [--all --failed]</pre> You can filter the file system imports by including one of the following: • id: Show the ID of a specific file system import session. • --all: Show the state of all file system imports. • --failed: Show only the file system imports that failed. The import state is one of the following: • MIS_EXECUTING: The import is actively processing nodes. • MIS_PAUSED: The import is paused by the user or due to a fault.

Qualifier	Description
	• MIS_WAITING_FOR_RESYNC: The import is idle but with one or more persistently failed nodes. Use nas_svc_imt --show-failed-nodes for more information. • MIS_SYNCING: The import is idle and has no persistently failed nodes; it is pending completion. • MIS_COMPLETE: The import has completed successfully. • MIS_CANCELLED: The import has been canceled. • MIS_FAILED: The import failed due to an unrecoverable error.
-n, --show-failed-nodes	Show the identity (the ino) and path of the persistently failed nodes for the specified file system import. The ino is the decimal inode number of a directory or file on the target file system. The format of the command is as follows: <pre>nas_svc_imt <NAS server name> [-n --show-failed-nodes] {<import session id> --all}</pre> You can filter the list of file system imports with failed nodes by including one of the following: • id: Show the ID of a specific file system import session. • --all: Show the identity (or ino) and path of the persistently failed nodes for all the file system imports for the specified NAS server.
-f, --show-dirty-files	Show the identity (or ino) and path of the dirty files for the specified file system import. The format of the command is as follows: <pre>nas_svc_imt <NAS server name> [-f --show-dirty-files] {<import session id> --all}</pre> You can filter the list of file system imports with failed nodes by including one of the following: • id: Show the ID of a specific file system import session. • --all: Show the identity and path of the dirty files for all the file system imports for the specified NAS server.
-s, --show-nodes	Show the import details of the specified node or nodes if more than one --node option is present. The ino is the decimal inode number of a directory or file on the target file system. The format of the command is as follows: <pre>nas_svc_imt <NAS server name> [-s --shownodes] --node <ino></pre> The reported node state is one of the following: • MNS_NONE: The node is not part of the import, or it has not yet been discovered by the import. • MNS_PENDING: The node has been discovered and is part of the import but it has not yet been processed. • MNS_FAILED: The node is part of the import but an error was encountered during processing or when attempting to apply a subsequent client modification to the node. • MNS_MOVING: The node is now being processed. • MNS_MOVED: The node has been successfully processed. • MNS_STREAM: The node is a named stream that is part of the import.
-r, --resync-nodes	Trigger a resync of the specified node or nodes if more than one --node option is present. The ino is the decimal inode number of a directory or file on the target file system. The format of the command is as follows: <pre>nas_svc_imt <NAS server name> [-r --resync-nodes] <import session id> --node <ino></pre> If the specified nodes do not match their counterpart on the source file system, a task is asynchronously performed to reimport each of the specified nodes.

Qualifier	Description
-c, --clear-failed-nodes	Forcibly clear the error on specified persistently failed node or nodes if more than one --node option is present associated with the given file system import. The ino is the decimal inode number of a directory or file on the target file system. The format of the command is as follows: <pre>nas_svc_imt <NAS server name> [-c --clear-failed-nodes] <import session id> [--yes] --node <ino></pre> When an error is forcibly cleared on a node (in other words, a directory or file), the contents might not be the same on the source and target. These differences should be resolved manually after import completion. Confirmation of this action is necessary either through the interactive prompt or by specifying --yes.
-d, --drop-failed-nodes	Drop the specified node (or nodes if more than one --node option is present) from the given file system import. The ino is the decimal inode number of a directory or file on the target file system. The format of the command is as follows: <pre>nas_svc_imt <NAS server name> [-d --drop-failed-nodes] <import session id> [--yes] --node <ino></pre> The import does not perform processing on a dropped node or not even attempt writes. Differences should be expected and must be resolved manually after import completion. Confirmation of this action is necessary through either the interactive prompt or by specifying --yes.
-l, --list-dhsm-conns	Lists the HTTP and HTTPS connections that have been migrated to the destination of the specified file system import. The format of the command is as follows: <pre>nas_svc_imt <NAS server name> --list-dhsm-conns <import session id></pre>
-t, --set-dhsm-conn	Set which HTTP or HTTPS connection should be made the active DHSM connection on the destination of the specified file system import. The <cid> is the connection ID. The format of the command is as follows: <pre>nas_svc_imt <NAS server name> --set-dhsm-conn <import session id> --cid <cid></pre>

Display the SDNAS log (svc_nas nas_svc_log)

The service script enables you to display all available SDNAS logs. You can also display logs that are active and updated within a specific time.

Usage

Function	System Operations
Mode	Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	No
May cause data unavailability?	Yes
May cause data loss?	No
Scope	Node
Prerequisites	None

Format

```
svc_nas run nas_svc_log -h [-f | --full] [-s | --short] [-l | --last <sec>]  
[-b | --before <sec>] [-n | --new]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message.
-f, --full	Display all available SDNAS logs.
-l, --last	Display the log for the last specified number of seconds.
-b, --before	Display the log older than the specified number of seconds.
--new	Display the log since the last time the <code>nas_svc_log</code> command was run.
--short	Display the active log.

Show statistics for NDMP and PAX backup sessions (svc_nas nas_svc_paxstats)

This script displays the advanced statistics for NDMP and PAX backup sessions that are in progress on the NAS servers.

Usage

Function	Diagnostic
Mode	Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Node
Prerequisites	None

Format

```
svc_nas nas_svc_paxstats { SVDM_A | SVDM_B | ALL } -stats {-reset | -verbose}
```

Optional arguments

Qualifier	Description
-stats	Display the NDMP and PAX backups statistics counters that are in progress. -verbose: Display the NDMP and PAX backups advanced statistics counters that are in progress. -reset: Reset the NDMP and PAX backups statistics counters.

Positional arguments

Qualifier	Description
SVDM_A	NAS server A.
SVDM_B	NAS server B.
ALL	Both NAS servers.

Run a Linux tcpdump (svc_nas nas_svc_tcpdump)

This service script allows you to run a Linux tcpdump operation on a system interface for diagnostic purposes.

The output from this command is saved in rotating files of fixed size. When an output file grows either to the size defined by `-C` or to a different maximum size, the output is redirected to another file. This other file has the same base name but a different suffix. The suffix is a digit from 0 to the value defined by either the `-w` option or an internally defined maximum rotation value. Rotating files are created in numerical order.

Usage

Function	Diagnostic
Mode	Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	No
May cause data unavailability?	Yes
May cause data loss?	No
Scope	Node
Prerequisites	None

Format

```
svc_nas nas_svc_tcpdump [-h] [-i <interface>] [-w <file name>]
[-W <rotations>] [-C <size>] [-s <number of bytes>]
[-t {1,2,3,4}] [-v {1,2,3}] [-D] [-F <filter file>] [-e] [-n] [-q]
[-T <timeout>] [-p <path>] [-y <data link type>]
[-L] [-K <tcpdump session ID>]
```

Optional arguments

Table 2. Optional arguments

Qualifier	Description
<code>-h, --help</code>	Show the help message and exit.
<code>-i, --interface</code>	Specify the interface to be used to capture information. The default interface for the host namespace is <code>mgmt0</code> ; for SDNAS, the default is <code>eth_mgmt</code> .
<code>-w, --filename</code>	Specify the base file name for the output files. The default name is <code>dump.out</code> .

Table 2. Optional arguments (continued)

Qualifier	Description
-W, --rotations	Specify the number of files for output. The default is 5. The maximum number is 20.
-C, --size	Specify the size of each output file in MB. The default is 50. The maximum size is 200.
-s, --snaplen	Capture this specified number of bytes of data from each packet rather than the default 65535. 0 means the default value.
-t, --timestamp	Add the corresponding number (1, 2, 3, or 4) to the timestamp command to specify how you want the timestamp to appear in the output: 1. Do not print a timestamp on each dump line. 2. Print an unformatted timestamp on each dump line. 3. Print a delta (in microseconds) between current and previous line on each dump line. 4. Print a timestamp in the default format preceded by the date on each dump line.
-v, --verbosity	Specify the verbosity of the output, with 3 being most verbose.
-D, --dump_intf	Print the list of the network interfaces available on the system and on which the tcpdump operation can capture packets.
-F, --input _expr	Use the file as input for the filter expression. The file should be in the tcpdump directory.
-e, --llheader	Print the link-level header on each dump line.
-n, --no_addr	Do not convert addresses such as host addresses, port numbers, and so on, to names.
-q, --quiet	Print abridged protocol information to make the output lines shorter.
-T, --timeout	Define the timeout before stopping the trace. The timeout format is xy, where x is a number and y is the unit of measurement for time (second, minute, hour, day). Some examples are 30s, 10m, 5h, 2d. If you want the trace to keep running, set the timeout to no. The default is no.
-p, --path	Specify the path for the output file storage; the default is /opt/sdnas/log/svc_output. The path that is specified must be an existing directory under /opt/sdnas/log/svc_output.
-y, --dlink	Set the data link type to datalinktype to use while capturing packets.
-L, --list	List active tcpdump sessions.
-K, --kill	Kill all tcpdump sessions or a specific session by designating its ID.

Back up NAS server configuration (svc_nas_cbr)

This service script enables you to back up all NAS server configurations on the cluster and also view previously backed up configurations. When you run this script, the backup archive is created in a `.tar` format. To restore a NAS server from a backup archive, contact your service provider.

Usage

Function	Diagnostic and Recovery
Mode	Service
Usage	Service
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Appliance
Prerequisites	None

Format

```
svc_nas_cbr [-h] [-b]
```

Optional arguments

Qualifier	Description
<code>-h, --help</code>	Show the help message and exit.
<code>-b, --backup</code>	Back up the NAS server configurations.

Example

Use the following command to back up your NAS server configuration:

```
svc_nas_cbr --backup  
  
http://fd9f:1e6a:2ab0::201:4438:71f7:d:3085/api/instances/supportMaterial/5ccac68b-a14a-66e7-863e-9ada1b00938e  
CBR file: SDNAS_cbr_data_20190502_102926UTC.tar created on node 2
```

See CIFS issues (svc_nas_cifssupport)

This service script enables you to view information for troubleshooting CIFS-related issues. It displays information about network connectivity to domain controllers, access rights, credentials, access logs, and other related items for a specific NAS server or all NAS servers.

 **NOTE:** Ensure that you run this script on the primary node of the appliance.

Usage

Function	Diagnostic
Mode	Normal or Service
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Appliance
Prerequisites	None

Format

```
svc_nas_cifssupport [-h] [--server value] [--args="<value>"]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--args	NAS service command arguments.  NOTE: Arguments must be preceded by hyphens. For example: <code>svc_nas_cifssupport --args="<>"</code>

Positional arguments

Qualifier	Description
--server	Specify the name of the NAS server that you want to run the specific action on.

Options

Use the `--args` argument to specify additional options.

[-h | -help | --help | <no option>]

Display help and exit. Use this option with `svc_nas_cifssupport` to view the top-level options for the command. To view the options and parameters for a top-level option, use the `-help` option after the top-level option. For example, the output of `svc_nas_cifssupport --server nas 1 --args="-setspn -help"` provides detailed usage information about the `-setspn` option.

-accessright

Compute the effective access rights for a user on a file system resource.

Usage:

```
svc_nas_cifssupport --server <server name> | --args="-accessright  
{-user <user_name> [-domain <domain_name>] | -sid <SID>}} {{-path  
<path_name> [-stop_on_symlink]}} | -share <share_name>}"
```

-user <user_name> [-domain <domain_name>] | -sid <SID>

Specify the user name and domain or the SID of the user.

{-path <path_name> [-stop_on_symlink]} | -share <share_name>

Specify the file system resource.

-acl

Dump or display the Access Control List (ACL) for the specified file system resource.

Usage:

```
svc_nas_cifssupport --server <server name> | ALL --args="-acl
  {{-path <pathname>
  [-stop_on_symlink]}
  |-share <sharename>}
  [-verbose]
  [-aclext]
  |-fs <filesystem_name>
  {-printstats
  | -resetall
   {[-path <path>]
   | [-owner]
   | [-group]
   | [-dacl]
   | [-sacl]}}"
```

-path <pathname>

Display the ACL of the pathname.

-stop_on_symlink

Display the ACL of the symbolic link, instead of the target of the link.

-verbose

Display more information about the ACL.

-aclext

Dump additional details about conditional ACEs and resource attributes that are present.

-fs <filesystem_name>

Name of the file system.

-printstats

Get the ACL statistics on the file system.

-resetall

Reset all ACL on the file system (set everyone with full control).

-path <path>

Copy ACL of the given path to all the other files of the file system. If you specify one of the following options (-owner, -group, -dacl, and -sac1), copy only the relevant items. You can use these options together or combine them as you need.

-owner

Reset owners.

-group

Reset groups.

-dacl

Reset DACL.

-sac1

Reset SACL.

-audit

Audit the current CIFS (clients) connections on the SMB server.

Usage:

```
svc_nas_cifssupport --server <server name> | ALL --args="-audit
  -user <user_name> | -client <client_name>
  | -full"
```

-user <user_name>

Audit connections for the specified user.

-client <client_name>

Audit connections for the specified client or IP address.

-full

Display more details about the file opens per connection.

-builtinclient

Audit the current domain controller connections on the SMB server built-in client.

Usage:

```
svc_nas_cifssupport --server <server name> | ALL --args="-builtinclient"
```

-checkup

Perform internal configuration tests to discover the root cause of potential configuration or environmental errors.

Usage:

```
svc_nas_cifssupport --server<server name> | ALL --args="-checkup [-full] [-info]"
```

-full

Perform additional tests, which could take a significant amount of time.

-info

Display information about the test that is executed by the command.

-cred

Display or build a Windows user credential. Use this command to troubleshoot user access control issues.

Usage:

```
svc_nas_cifssupport --server <server name> | ALL --args="-cred {-user <user_name> -domain <domain_name> | -sid <SID> | -uname <unix_name>} [-build] [-credext]"
```

-user <user_name> -domain <domain_name>

The name and domain of the user.

-sid <SID>

The SID of the user in decimal form.

-uname <unix_name>

The UNIX name or numerical ID (using the convention @uid=xxxx,gid=yyyy@, with xxxx and yyyy the decimal numerical value of the uid and the primary gid, respectively) of the user.

 **NOTE:** Setting the default UID to 0, or to a user which will be resolved at UID 0, will grant that user full root access. Ensure that this value is not set to 0 for users who should not have full access.

-build

Build the credential for a user that has not yet connected the SMB server.

 **NOTE:** This option requires a domain administrator ID/ password.

-credext

Include additional details of the claims that are present in the Kerberos ticket. This is only for Dynamic Access Control (DAC).

-gpo

List (-info) or force update (-update) the Windows global policy objects (GPOs) that are applied to the SMB server.

Usage:

```
svc_nas_cifssupport --server <server name> | ALL --args="-gpo [-info] [-update]"
```

-homedir

Enable or disable the SMB home directories. Once the feature is enabled, a homedir file containing the name of the SMB users and their related home directory must be uploaded to the NAS server using the `uemcli /net/nas/server` CLI command. Once this is done, SMB users can connect to the SMB HOME share.

Usage:

```
svc_nas_cifssupport --server <server name> | ALL --args="-homedir [-enable] | [-disable]"
```

[-enable]

Enables the home directories feature.

[-disable]

Disables the home directories feature.

-Join

Join the specified server to a Windows Active Directory (AD) domain, move it to another organizational unit (OU), or collect information about it from the Domain Controller (DC).

Usage:

```
svc_nas_cifssupport --server <server name> | ALL --args="-Join  
-compname <comp_name> -domain <full_domain_name> -admin  
<admin_name> [-ou <organizational_unit>] [-option {reuse |  
resetserverpasswd | addservice=nfs}]"
```

-admin <admin_name>

Specify an account that has administrator privileges on the specified domain. The password must be provided when prompted.

-ou <organizational_unit>

Specify the OU in which to place or move the specified computer.

-option {reuse | resetserverpasswd | -addservice=nfs}

reuse

Allow the specified computer to join the server by taking ownership of an existing computer account in the Windows AD domain that matches the computer name that is specified in the command.

resetserverpasswd

Reset the server password on the DC.

-addservice=nfs

Add an NFS SPN for the specified server in Active Directory for secure NFS.

-logontrace

Log user or machine logon attempts for the specified IP address or for all clients when no IP address is specified.

Usage:

```
svc_nas_cifssupport --server <server name> | ALL --args="-logontrace {-  
enable <ip_address> | -disable | -list}"
```

-lsarpc

Query the specified Windows user identifier for an account specified by user name or SID (security identifier) and return the corresponding Unix UID.

Usage:

```
svc_nas_cifssupport --server <server name> | ALL --args="-lsarpc  
-nb <comp_name> {-user <user_name> | -sid <SID> [hex=<0/1>] |  
-priv}"
```

-nb <comp_name>

Specify the netbios name of the server.

-user <user_name> | -sid <SID>

Specify the username or the SID.

hex=<0/1>

Specify if the SID is given in decimal (0) or hexadecimal (1) format.

-priv

List all available privileges on the domain. This can be used to resolve foreign language issues.

-nltest

Simulate an NTLM user authentication on the server by specifying a domain user name and password pair. Use this command to troubleshoot connection issues or test DC connections. This command only applies to servers that are joined to a Windows domain.

Usage:

```
svc_nas_cifssupport --server <server name> | ALL --args="-nltest  
-nb <comp_name> {-user <user_name> -dom <domain> -usrpwd  
<user_password> [-wkst <client_name>]}"
```

-wkst <client_name>

Optionally set a workstation name in the NTLM request.

-pdcdump

Display information about every SMB server DC in use at the NAS server level. This command only applies to servers that are joined to a Windows domain.

Usage:

```
svc_nas_cifssupport --server <server name> | ALL --args="-pdcdump"
```

-pingdc

Check the network connectivity of the CIFS server that is specified by the NetBIOS name or computer name with a domain controller. Once connectivity is established, the command verifies that a CIFS server can access and use the domain controller services. This command only applies to servers that are joined to a Windows domain.

Usage:

```
svc_nas_cifssupport --server <server name> | ALL --args="-pingdc  
-compname <comp_name> [-dc <netbios_DC_name>] [-verbose]"
```

-samr

Query the groups a user belongs to using either the user name or SID.

Usage:

```
svc_nas_cifssupport --server <server name> | ALL --args="-samr -nb  
<comp_name> {-sid <SID> | -user <user_name>}"
```

-secmap

Access the Secure Mapping database that acts as a cache mechanism to relate Windows SIDs to UNIX UIDs.



NOTE: Modifying a SID to UID mapping can impact security. Use with caution.

Usage:

```
svc_nas_cifssupport --server <server name> | ALL --args="-secmap  
-list"
```

```

[ -user <user_name> -domain <domain_name>
| -domain <domain_name>
| -sid <SID>
| -uid <user_id>
| -gid <group_id> ]
| -create {-name <name> -domain <domain_name> | -sid <SID> }
| -update {-name <name> -domain <domain_name> | -sid <SID> }
| -delete {-name <name> -domain <domain_name> | -sid <SID> }
| -export [-file <filename>]
| -import -file <filename>
| -report"

```

-list [-user <user_name> -domain <domain_name> | -domain <domain_name> | -sid <SID> | -uid <user_id> | -gid <group_id>]

Access the Secure Mapping database that acts as a cache mechanism to relate Windows SIDs to UNIX UIDs.

-create {-name <name> -domain <domain_name> | -sid <SID> }

Add a new mapping entry in the Secure Mapping database.

-update {-name <name> -domain <domain_name> | -sid <SID> }

Update a mapping entry from the Secure Mapping database.

-delete {-name <name> -domain <domain_name> | -sid <SID> }

Delete a mapping entry from the Secure Mapping database.

-export [-file <filename>]

Export Secure Mapping database to the specified file.

-import -file <filename>

Import Secure Mapping database from the specified file.

-report

Display Secure Mapping database health and content.

-setspn

Manage Windows security principals (SPNs) of the specified computer that is joined to AD.



NOTE: SPNs are required for domain configurations in which the DNS domain is different than authentication domain (Kerberos realm). For example, if the DNS server zone includes a DNS CNAME record that maps `compname.<domain1 FQDN>` to `compname.<server's domain FQDN>`, then the SPN host `compname.<domain1 FQDN>` must be added for the `compname`.

Usage:

```

svc_nas_cifssupport --server <server_name> | ALL --args="-setspn
-list compname=<comp_name> | -add <SPN>
compname=<comp_name>,domain=<full_domain_name>,admin=<admin_name>
| -delete <SPN>"

```

-list compname=<comp_name>

Display all SPNs for the specified FQDN server, both for the SMB server and for the KDC Windows AD entry.

-add <SPN> compname=<comp_name>,domain=<full_domain_name>,admin=<admin_name>

Add the specified SPN to both the NAS server and AD.

-delete <SPN>

Delete the specified SPN for both the NAS server and AD.

-smbhash

Troubleshoot issues with the Microsoft Windows Branch caching mechanism. BranchCache V1 and BranchCache V2 are supported.

Usage:

```

svc_nas_cifssupport --server <server_name> | ALL --args="-smbhash
-hashgen <path> [-recursive] [-minsize <size>]
| -hashdel <path> [-recursive]
| -abort <id>
| -info

```

```
| -fsusage <fs_name>
| -exclusionfilter <filter>
| -audit {enable | disable} [-task] [-service] [-access]
| -cleanup <fs_name> [-all | -unusedfor <days> | -unusedsince
<date>]"
```

-hashgen <path> [-recursive] [-minsize <size>]

Generate all SMB hash files for the specified path. If `-recursive` is used, the SMB hash is recursively generated for the subdirectories.

-hashdel <path> [-recursive]

Delete all SMB hash files for the specified path.

-abort <id>

Cancel the specified pending or ongoing request (hash file generation or deletion). The ID for the request is in the output of `-info`.

-info

Show detailed information for the hash generation service.

-fsusage <fs_name>

Display the SMB hash file disk usage for the specified file system.

-exclusionfilter <filter>

Do not generate an SMB hash file for files that match the exclusion filter.

-audit {enable | disable} [-task] [-service] [-access]

Enable the generation of audits in the smbhash event log.

-cleanup <fs_name> [-all | -unusedfor <days> | -unusedsince <date>]

Clean up the SMB hash files for the specified file system.

-Unjoin

Unjoin the specified machine from its AD domain. If dynamic DNS is employed, the entry is removed from AD and DNS. The password for the specified account with domain administrator privileges must be provided when prompted.

Usage:

```
svc_nas_cifssupport --server <server_name> | ALL --args="-Unjoin
-compname <comp_name> -domain <full_domain_name> -admin
<admin_name>"
```

Example

Use the following command to view the ACL for the `smbshare` share on the `nas1` NAS server:

```
svc_nas_cifssupport --server nas1 --args="-acl -share smbshare"

nas1 :done

ACL DUMP REPORT

Share      : \\\nas1\\smbshare
UID        : 0
GID        : 1
Rights     : rwxr-xr-x
```

Advanced NAS settings (svc_nas_tools and svc_nas_global_tools)

These service scripts enable you to view and customize the parameters of various NAS server components. The default values of the NAS server parameters satisfy most use cases, but this script enables you to adjust the parameters based on your business need.

Although both `svc_nas_tools` and `svc_nas_global_tools` scripts use the same arguments and options, their application is different:

- Use the `svc_nas_tools` script to review and customize parameters for a specific NAS server.
- Use the `svc_nas_global_tools` script to review and customize parameters for all NAS servers in the cluster.

Run without `args` to see the NAS internal usage.

Usage

Function	Diagnostic
Mode	Normal or Service
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_nas_tools [-h] [--server value] [--args="<value>"]
```

```
svc_nas_global_tools [-h] [--args="<value>"]
```

Optional arguments

Qualifier	Description
<code>-h, --help</code>	Show the help message and exit.
<code>--args NAS_CMD_ARGS</code>	Service command arguments. NOTE: A double hyphen must precede the arguments. For example: <code>svc_nas_tools --args="<value>"</code> The arguments <code>-dbms</code>, <code>-kerberos</code>, <code>-restart</code> and <code>-vhdx</code> do not apply to <code>svc_nas_global_tools</code>.

Options

Use the `--args` argument to specify the following additional options:

`[-h | -help | --help | <no option>]`

Display help and exit. Use this option with `svc_nas_tools` to view the top-level options for a command. To view the options and parameters for a top-level option, use the `-help` option after the top-level option. For example, the output of `svc_nas_tools --server nas 1 -args="-stats -help"` provides detailed information about the `-setspn` option.

`-cava`

Display the status of antivirus service of the NAS server, including the connection state to Celerra AntiVirus Agent (CAVA) servers, the number of files checked and their progress.

Usage:

```
svc_nas_tools <NAS_server_name> --args="-cava
[ -stats
| -set accesstime={ now | none | [[[[yy]mm]dd]hh]mm[.ss] }]
| -fsscan [ <fs_mountpath> { -list | -create | -delete } ]]"
```

-stats

Display statistics counters of the antivirus service.

-set accesstime={ now | none | [[[[yy]mm]dd]hh]mm[.ss] }]

Enable scan-on-first-read and change the access time setting, where:

- Specify **now** to Enable the scan-on-first-read feature and set the reference time to now.
- Specify **none** to disable the scan-on-first-read feature.
- Specify **[[[[yy]mm]dd]hh]mm[.ss]** to enable the scan-on-first-read feature and set the reference time according the specified value.

-fsscan [<fs_mountpath> { -list | -create | -delete }]

Start, stop, or view the status of a full file system scan, where:

- **<fs_mountpath>** option enables you to specify the location of the file system to be scanned.
- The **-list** option displays the scan status for the specified file system.
- The **-create** option initializes a full scan on the file system **<fs_name>** and the offline options allow the file system scan on all offline files. By default, offline file systems are not included.
- The **-delete** option stops the scan.



NOTE: If no file system is specified, this option displays the file system scan status for all file systems.

-dbms

Manage NAS server databases.

Usage:

```
svc_nas_tools <NAS_server_name> --args="-dbms
-list [<db_name>]
| -compact [<db_name>]
| -stats [-reset]
| -backup -target <path_name>
| -restore -source <path_name> [-silent]]"
```

-list [<dbName>]

Display NAS server databases.

-compact [<dbName>]

Compact NAS server databases.

-stats [-reset]

Display statistics about NAS server databases.

-backup -target <pathname>

Perform an online backup of the NAS server database environment.

-restore -source <pathname> [-silent]

Restore the NAS server database environment from backup files.

-dns

Display current DNS settings of the NAS server.

Usage:

```
svc_nas_tools <NAS_server_name> --args="-dns
[-dump
| -lookup{
    -host <host_name>
    | -addr <ipv4_or_ipv6_address>}]]"
```

-dump

Display the current DNS cache content.

-lookup {-host <host_name> | -addr <ipv4_or_ipv6_address>}

Provides lookup information about the specified resource.

-ds

Display the Windows Directory Service information.

Usage:

```
svc_nas_tools <NAS_server_name> --args="-ds  
[-dump] "
```

-dump

Display the Windows Directory Service cache.

-kerberos

Display the current Kerberos settings of the NAS server.

Usage:

```
svc_nas_tools <NAS_server_name> --args="-kerberos  
| -listrealms  
| -listspn  
| -keytab [-v]  
| -conf  
| -log [-all] "
```

 **NOTE:** This option does not apply to the `svc_nas_global_tools` script.

-listrealms

List the Kerberos realms that are configured on the NAS server.

-listspn

List the Kerberos service principles defined in Active Directory (AD) and keytab (joined CIFS server).

-keytab

Dump the Kerberos key table of the NAS server.

-conf

Dump the Kerberos configuration file for this NAS server.

-log [-all]

Extract Kerberos logs from the NAS server recent log.

 **NOTE:** The `-all` option scans the full server log.

-ldap

Display current LDAP settings of the NAS server.

Usage:

```
svc_nas_tools <NAS_server_name> --args="-ldap  
| -refresh  
| -lookup {  
    -user <username>  
    | -group <groupname>  
    | -uid <uid>  
    | -gid <gid>  
    | -hostbyname <hostname>  
    | -netgroup <groupname>} "
```

-refresh

If LDAP is configured with no static IP, refresh the IPs of the LDAP servers of the domain from DNS.

-lookup {-user <username> | -group <groupname> | -uid <uid> | -gid <gid> | -hostbyname <hostname> | -netgroup <groupname>}

Provides lookup information about the specified resource for troubleshooting purposes.

-lockd

Manage file locks on the NAS servers.

Usage:

```
svc_nas_tools <NAS_server_name> --args="-lockd
| -list
| -info -fldp <address>
| -remove -fldp <address> -credp <address>
| -stat [-reset]"
```

-list

Display the locked files on the NAS server with their count of locks; The files are ordered per file-system. Each file is identified by its inode number, and also by a fldp=<address> token for use with the -info option.

-info -fldp <address>

Show detailed information about the specific file; For each file lock, this command also displays the credp=<address> token. You can use this token with the -remove option.

-remove -fldp <address> -credp <address>

On the file identified by the fldp value, use this command to remove any range lock that matches the given lock credential.

-stat [-reset]

Show (and optionally reset) the statistics about file locks. The statistics counters are global to the SDNAS feature, and may be related to other NAS servers in the same node.

-nis

Display current NIS settings of the NAS server.

Usage:

```
svc_nas_tools <NAS_server_name> --args="-nis
[-lookup{
  -user {-name <user_name> | -uid <unix_user_id>}
  | -group {-name <group_name> | -gid <group_unix_id>}
  | -host {-name <host_name> | -addr <host_ip_address>}
  | -netgroup {-name <group_name> | -member <host_name>}}]"
```

-lookup {-user {-name <user_name> | -uid <unix_user_id>} | -group {-name <group_name> | -gid <group_unix_id>} | -host {-name <host_name> | -addr <host_ip_address>} | -netgroup {-name <group_name> | -member <host_name>}}

Provides lookup information about the specified resource for troubleshooting purposes.

-param

Display or modify NAS server parameter facilities.

Usage:

```
svc_nas_tools <NAS_server_name> --args="-param
{ -info
| -facility {<facility> | -all} -list
| -facility {<facility> | -all} -info {<param_name> [-verbose] |
-all}
| -facility <facility> -modify <param_name> -value <new_value>}"
```

-info

Display all NAS parameter facilities.

-facility {<facility> | -all} -list

Display all NAS parameter values of the specified facility for the specified NAS server.

-facility {<facility> | -all} -info {<paramname> [-verbose]} | -all

Display the details of the specified NAS parameter of the specified facility for the specified NAS server.

-facility <facility> -modify <paramname> -value <newvalue>

Modify the value of the specified NAS parameter of the specified facility for the specified NAS server.

-restart

Restart the specified NAS server. The output from the `-info` or `-modify` command informs the user if this is required for the specified parameter.

 **NOTE:** This option does not apply to the `svc_nas_global_tools` script.

Usage:

```
svc_nas_tools <NAS_server_name> --args="-restart [-silent]"
```

-silent

Do not request user confirmation before restarting the NAS server.

-vhdx -file

Display the VHDX metadata (Hyper-V virtual disk files).

 **NOTE:** This option does not apply to the `svc_nas_global_tools` script.

Usage:

```
svc_nas_tools <NAS_server_name> --args="-vhdx -file <vhdx file> [-verbose]"
```

-verbose

Display the VHDX metadata, including SCSI PRs.

Example

Use the following command to view the ACL for the `smbshare` share on the `nas1` NAS server:

```
svc_nas_tools --server NasServer4461 --args="-param -facility ldap -list"
```

NasServer4461:

param_name	facility	default	current	configured
SecurityLayer	ldap	2	2	
cacheMaxGroups	ldap	10000	10000	
cacheMaxHosts	ldap	10000	10000	

Enter maintenance mode (svc_nas_maintenance_mode)

The service script enables you to place the NAS node in maintenance mode as well as exit maintenance mode and see the current status of the NAS node.

Usage

Function	System Operations
Mode	Normal or Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	Yes

May cause data unavailability?	Yes
May cause data loss?	No
Scope	Node
Prerequisites	1. NAS must be installed on both nodes. 2. The NAS docker must be up and running on both nodes. 3. Both nodes must be healthy.

Format

```
svc_nas_maintenance_mode [-h] [enter, exit, status]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
enter	Place the NAS node into the maintenance mode.
exit	Exit the NAS node from maintenance mode.
status	Get the current status of the NAS node for maintenance purposes.

Display inode usage (svc_nas_storagecheck)

This service script enables you to display the inode usage of all file systems in an appliance.

Usage

Function	Diagnostic
Mode	Normal or Service
Usage	General
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Node
Prerequisites	A NAS server and at least one file system.

Format

```
svc_nas_storagecheck [-h] [-i]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
-i	Show the inode usage of all file systems in the appliance.

Get NAS server information and manage settings (svc_nas_tools)

This service script enables you to get and set information for a specific NAS server.

Format

```
svc_nas_tools [-h] [--server value] [--args value]
```

Usage

Function	Diagnostic
Mode	Normal or Service
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--args	Use a specific option for the service command argument.

Positional arguments

Qualifier	Description
<code>--server</code>	Specify the name of the NAS server.

Other arguments

The following table shows the available options that are used to manage the NAS server. You must use the `--args` argument with these options, as shown in the following example:

```
svc_nas_tools --server nas1 --args="-dns"
```

Qualifier	Description
<code>-cava</code>	Manages the anti-virus service settings of the specified NAS server.
<code>-dbms</code>	Perform an operation on databases.
<code>-dns</code>	Display the DNS settings of the NAS server and perform a DNS lookup.
<code>-ds</code>	Display the Windows Directory Service.
<code>-file</code>	Upload or download a file to the <code>/etc</code> directory of the NAS server.
<code>-kerberos</code>	Display current Kerberos settings of the NAS server.
<code>-ldap</code>	Display the LDAP settings of the NAS server and perform LDAP operations.
<code>-lockd</code>	Manage file locks on the NAS servers.
<code>-nis</code>	Display the NIS settings of the NAS server and perform an NIS lookup.
<code>-param</code>	Manage the NAS server parameters.
<code>-restart</code>	Restart the specified NAS server.
<code>-vhdx</code>	Display metadata for Hyper-V virtual disk files (VHDX).

Retrieve NAS server net devices and IP addresses (svc_nasserver_to_netdevice)

This service script enables you to use a NAS server name to retrieve file interface IP addresses and net devices that are associated with that NAS server.

Usage

Function	System Operations
Mode	Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	No
May cause data unavailability?	Yes
May cause data loss?	No
Scope	Node

Prerequisites	None
---------------	------

Format

```
svc_nasserver_to_netdevice [-h] --server <value>
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Required arguments

Qualifier	Description
--server	The name of the NAS server.

See network information (svc_networkcheck)

This service script enables you to collect information about the appliance network and run a set of network diagnostic tools.

Usage

Function	Diagnostic
Mode	Normal and Service
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Appliance
Prerequisites	None

Format

```
svc_networkcheck [-h]
{arp,info,tracert,tpc,ethtool,ping,interfaces,ping6,netstat,dns,bond_list}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
arp	Show Address Resolution Protocol (ARP) records cache settings.
info	Perform network and system checks.
tracert	Perform a traceroute to the IP (either IPv4 or IPv6).
tpc	Perform a TCP port check using Telnet.
ethtool	Show information about the network device driver and hardware settings.
ping	Ping the IP or hostname of an IPv4 target. The information is listed in the output of the <code>svc_networkcheck interfaces</code> command.
interfaces	Show interface names, IPs, and connections.
ping6	Ping the IP or hostname for the IPv6 target. The information is listed in the output of the <code>svc_networkcheck interfaces</code> command.
netstat	Perform a <code>netstat</code> operation on the node.
dns	Perform a DNS check using the <code>dig</code> tool.
bond_list	Show system bond devices and their settings.

Show ARP records cache settings (svc_networkcheck arp)

This service script displays the settings for the ARP records cache.

Format

```
svc_networkcheck arp [-h] {ipv4,ipv6}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Positional arguments

Action	Description
ipv4	Show the ARP records cache settings for IP protocol version IPv4.
ipv6	Show the ARP records cache settings for IP protocol version IPv6.

Example

Use the following command to view the values of ARP settings for ipv4:

```
svc_networkcheck arp ipv4

=== Node status: Normal Mode ===

===== [FNM00175201431-A] [Wed Dec 23 14:18:03 UTC 2020] Beginning Run
=====
```

The values of ARP settings for ipv4:

```
net.ipv4.neigh.default.gc_thresh1 = 1024
net.ipv4.neigh.default.gc_thresh2 = 4096
net.ipv4.neigh.default.gc_thresh3 = 16384
```

```
===== [FNM00175201431-A] [Wed Dec 23 14:18:03 UTC 2020] End of Run
=====
```

Perform network and system checks (svc_networkcheck info)

This script enables you to perform network and system checks on the following: NTP, date, time, IP, DNS, ARP, and netstat.

Format

```
svc_networkcheck info [-h]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Check server port availability (svc_networkcheck tracert)

This service script enables you to perform a traceroute operation to the IP whether it is IPv4 or IPv6. The operation tracks the route that packets take from an IP network to a host.

Format

```
svc_networkcheck tracert [-h] [-N {host,sdnas}] destination
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-N, --namespace	Define the network namespace (host or SDNAS).

Positional arguments

Action	Description
destination	The destination to which the packets are sent.

Check the TCP port (svc_networkcheck tcp)

This service script enables you to check the port availability on a specific server to ensure that you can establish a TCP connection.

Format

```
svc_networkcheck tcp [-h] [server <value>] [port <value>]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Positional arguments

Action	Description
server	Check the availability of a server (IP or hostname).
port	Check the availability of a specific port.

Example

The following example uses the `svc_networkcheck tracert` command to check whether an SSH connection can be established with a remote server:

```
svc_networkcheck tcp <ip address>
===== tpc =====
Escape character is '^]'.
--- INFO: the tcp listening port <ip address> is available
```

Show network device driver and hardware information (svc_networkcheck ethtool)

This service script enables you to display information about the network device driver and the hardware settings.

Format

```
svc_networkcheck ethtool [-h] devname {value | all}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Positional arguments

Action	Description
devname	Specify the network device name or enter <code>all</code> to show information about all network devices.

Ping an IPv4 target (svc_networkcheck ping)

The service script enables you to ping the IPv4 target using either the hostname or IP address.

Format

```
svc_networkcheck ping [-h] [-s {1500,9000}] [-I <value>] [-m <value>]
                    [-c <value>] [-f] [-N {host,sdnas}] destination
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-s, --mtu	Ping with the given MTU value (1500 or 9000).
-I, --sip	Specifies the ping source IP address or interface name.
-m, --mark	Specifies the NAS connection mark that is used to find the source IP.
-c, --count	Specifies the time when the system stops sending ECHO_REQUEST packets.
-f, --fragmentation	Prevent packet fragmentation.
-N, --namespace	Defines the network namespace (host or SDNAS).

Positional arguments

Action	Description
destination	Specify the IP address or hostname.

Example

Use the following command to view the values of ping operation of the <ip> or <hostname> IPv4 target.

```
svc_networkcheck ping 10.244.192.93 -c 3 --mtu 1500 --mark 10

=== Node status: Normal Mode ===

===== [FNM00175201431-A][Wed Dec 23 09:28:08 UTC 2020] Beginning Run
=====

PING 10.244.192.93 (10.244.192.93) 1500(1528) bytes of data.
1508 bytes from 10.244.192.93: icmp_seq=1 ttl=62 time=0.356 ms

1508 bytes from 10.244.192.93: icmp_seq=2 ttl=62 time=0.407 ms

1508 bytes from 10.244.192.93: icmp_seq=3 ttl=62 time=0.383 ms

--- 10.244.192.93 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2045ms
rtt min/avg/max/mdev = 0.356/0.382/0.407/0.020 ms

===== [FNM00175201431-A][Wed Dec 23 09:28:10 UTC 2020] End of Run
=====
```

Ping an IPv6 target (svc_networkcheck ping6)

The service script enables you to ping the IPv6 target using either the hostname or IP address.

Format

```
usage: svc_networkcheck ping6 [-h] [--mtu {1500,9000}] [--sip SIP]
                                [--mark MARK] [--count COUNT] [-f]
                                [-N {host,sdnas}]
                                destination
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-s, --mtu	Ping with the given MTU value (1500 or 9000).
-I, --sip	Specifies the ping source IP address or interface name.
-m, --mark	Specifies the NAS connection mark that is used to find the source IP.
-c, --count	Specifies the time when the system stops sending ECHO_REQUEST packets.
-f, --fragmentation	Prevent packet fragmentation.
-N, --namespace	Defines the network namespace (host or SDNAS).

Positional arguments

Action	Description
destination	Specify the IP address or hostname.

Show network connections (svc_networkcheck netstat)

This service script enables you to use the **netstat** tool to display node network connections.

Format

```
svc_networkcheck netstat [-h]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Perform a DNS check (svc_networkcheck dns)

This service script enables you to perform a domain name system check using the dig tool.

Format

```
svc_networkcheck dns [-h] name
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Positional arguments

Action	Description
name	Specify the name of the resource record that you want to find.

See system bond devices (svc_networkcheck bond_list)

This service script enables you to see system bond devices and their settings.

Format

```
svc_networkcheck bond_list -h
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Example

The following example show the output of the `svc_networkcheck bond_list` command:

```
svc_networkcheck bond_list
bond0: system bond (not allowed to change options)
  - options:
    mode=802.3ad

  - alerts: No active alerts found

  - ports:
    ens7f3:
      Link up: up
      Carrier: 1
      Bonding State: active
      MAC: 0c:48:c6:73:67:5f
      PERM_MAC: 0c:48:c6:73:67:5f
      MTU: 1500
      Speed: 25000
      Duplex: full
      Aggregator id: 1
    ens7f2:
      Link up: up
      Carrier: 1
      Bonding State: backup
```

```

        MAC: 0c:48:c6:73:67:5f
        PERM_MAC: 0c:48:c6:73:67:5e
        MTU: 1500
        Speed: 25000
        Duplex: full
        Aggregator id: 2
bond1: unknown bond (not allowed to change options)
  - options:
    mode=802.3ad miimon=200 updelay=0 downdelay=0 xmit_hash_policy=layer2+3
lacp_rate=slow

  - alerts:
    The exception from appliance_list is: global name 'ListAppliances' is not defined
    Alert id : f2779470-496a-4d49-a086-bef6dabc2209
    Error Code : 0x01807a02
    Severity : Major
    Timestamp (UTC) : 2021-10-26 19:00:03+00
    Appliance Name : A1
    Resource Type : bond
    Resource Name : BaseEnclosure-NodeA-bond1
    Description : One or more bond ports are in link down state or Link Aggregation
Control Protocol (LACP) is in degraded state.

  - ports:
    ens2f1:
      Link up: up
      Carrier: 1
      Bonding State: active
      MAC: 00:60:16:b9:53:4d
      PERM_MAC: 00:60:16:b9:53:4d
      MTU: 1500
      Speed: 25000
      Duplex: full
      Aggregator id: 1
    ens2f0:
      Link up: up
      Carrier: 1
      Bonding State: backup
      MAC: 00:60:16:b9:53:4d
      PERM_MAC: 00:60:16:b9:53:4c
      MTU: 1500
      Speed: 25000
      Duplex: full
      Aggregator id: 2

```

Show interface names (svc_networkcheck interfaces)

This service script enables you to show interface names, IPs, and connection marks for the node.

Format

```
svc_networkcheck interfaces [-h] [-N {host,sdnas}]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-N, --namespace	Define the network namespace (host or SDNAS).

Positional arguments

Qualifier	Description
host	Defines the network namespace as host.
sdnas	Defines the network namespace as SDNAS.

Example

Use the following command to view interface names, IPs, and connection marks.

```
svc_networkcheck interfaces --namespace sdnas

=== Node status: Normal Mode ===

===== [FNM00175201431-A][Wed Dec 23 09:32:00 UTC 2020] Beginning Run
=====

===== sdnas: ip addr show =====

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth_svc@if47: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 0a:c6:09:ee:a6:35 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 128.221.255.34/30 scope global eth_svc
        valid_lft forever preferred_lft forever
41: eth_mgmt@if27: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 66:6b:e2:88:b9:3d brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fdea:4915:d43d:0:201:44bd:3c1f:dlca/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fdea:4915:d43d:0:201:442d:a826:c80/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::646b:e2ff:fe88:b93d/64 scope link
    link
        valid_lft forever preferred_lft forever
42: eth_data0@if27: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 5e:94:db:2b:e8:17 brd ff:ff:ff:ff:ff:ff link-netnsid 0

===== sdnas: ip ru show =====
0:      from all lookup local
218:    from all fwmark 0x8002 lookup 4
219:    from all fwmark 0x8001 lookup 2
220:    from all lookup 220
32765:  from all fwmark 0x8000/0x8000 lookup 1 unreachable
32766:  from all lookup main
32767:  from all lookup default
65535:  from all fwmark 0x8001 lookup 3 unreachable
65535:  from all fwmark 0x8002 lookup 5 unreachable

===== [FNM00175201431-A][Wed Dec 23 09:32:00 UTC 2020] End of Run
=====
```

Reboot, shut down, and turn on a node (svc_node)

This service script enables you to cleanly reboot or turn on a node. This script also enables you to stop the controller VM on the node so the node can be placed in Maintenance mode in VMware vSphere.

This command can only be used for operations that are performed on a single node.

Usage

Function	Diagnostic and Recovery
Mode	Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	No
May cause data unavailability?	Yes
May cause data loss?	No
Scope	Node
Prerequisites	None

Format

```
svc_node [-h] [-d] {status,power_on,power_off,reboot,shutdown}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-d, --debug	Increase the logging level to debug and print logs to the console.

Actions

Action	Description
status	Provides the network connectivity status and power status of the peer node.
power_on	Power on the peer node.
power_off	Turn off power to a node. This action is equivalent to an abrupt or hard power off.
reboot	Reboot the node.  NOTE: This action causes the node to restart immediately.
shutdown	Shut down a node by cleanly powering it off. All services are stopped in the appropriate order.

Turn a node off (svc_node power_off)

This service script is used to turn off power to a node. This script is the equivalent of a hard power off action.

Format

```
svc_node power_off [-h] [-f] [-d] {local,peer}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-f, --force	Skip any prepower off node checks and user confirmation prompts.
-d, --debug	Initiate verbose logging for debugging purposes.

Positional arguments

Qualifier	Description
local	Specify this argument to indicate that you want to turn off the local, or primary, node of an appliance.
peer	Specify this argument to indicate that you want to turn off the peer, or secondary, node of an appliance.

Considerations

Appliance state	Personality	Notes
Configured or unconfigured	SAN or HCI	Turns off power to the node or nodes.

Turn on the peer node (svc_node power_on)

This service script turns on a peer node that is running in SAN mode.

Format

```
svc_node power_on [-h] [-d]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-d, --debug	Initiate verbose logging for debug.

Reboot a node (svc_node reboot)

This service script is used to reboot a node.

Format

```
svc_node reboot [-h] [-a] [-f] [-d] {local,peer}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-a, --async	Run in asynchronous mode.
-f, --force	Ignore warnings; force a reboot that might result in data becoming unavailable.
-d, --debug	Initiate verbose logging for debugging purposes.

Positional arguments

Qualifier	Description
local	Specify this argument to indicate that you want to turn off the local, or primary, node of an appliance.
peer	Specify this argument to indicate that you want to turn off the peer, or secondary, node of an appliance.

Considerations

Appliance state	Personality	Notes
Configured or unconfigured	SAN or HCI	If the node is not in service mode, you see a warning that the node is running workloads. You can use the <code>--force</code> option to override the warning and start a reboot.

Shut down a node (svc_node shutdown)

This service script cleanly shuts down a node running in SAN mode. All services are stopped in the appropriate order.

Format

```
svc_node shutdown [-h] [-a] [-f] [-d] {local,peer}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-a, --async	Run in asynchronous mode.
-f, --force	Ignore warnings; force shutdown which may result in data becoming unavailable.
-d, --debug	Initiate verbose logging for debugging purposes.

Positional arguments

Qualifier	Description
local	Specify this argument to indicate that you want to turn off the local, or primary, node of an appliance.
peer	Specify this argument to indicate that you want to turn off the peer, or secondary, node of an appliance.

Considerations

Appliance state	Personality	Notes
Configured	SAN	If the node is not in service mode, you see a warning that the node is running workloads. You can use the <code>--force</code> option to override the warning and power off the node.
Unconfigured	HCI	This operation is only supported when the script is run from the control path maintenance mode service. The script stops the PowerStore VM to allow the node to enter VMware maintenance mode.

Peer node status (svc_node status)

This service script displays the network connectivity status and power status of the peer node.

Format

```
svc_node status [-h] [-d] [-o]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-d, --debug	Initiate verbose logging for debug.
-o, --output	Show network connectivity and power status in JSON format.

Control node affinity (svc_node_affinity_balance)

This service script enables you to use the resource balancer to control node affinity and I/O processing within a cluster.

Usage

Function	System Operations
Mode	Normal and Service
Usage	General Use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_node_affinity_balance [-h] [--help] {status,disable,enable}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-d, --debug	Initiate verbose logging for debugging purposes.

Actions

Action	Description
status	Display the status of node affinity balancing within the cluster.
disable	Disable node affinity balancing within the cluster.
enable	Enable node affinity balancing within the cluster.

Enable node affinity balancing (svc_node_affinity_balance enable)

This service script enables you to change the status of node affinity balancing to active mode. Node balancing operations evaluate the performance of the cluster and generate recommendations to balance I/O processing between the nodes.

Format

```
svc_node_affinity_balance enable [-h] [-d]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-d, --debug	Initiate verbose logging for debugging purposes.

Disable node affinity balancing (svc_node_affinity_balance_disable)

Disable node affinity balancing within the cluster.

Format

```
svc_node_affinity_balance disable [-h] [-d]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-d, --debug	Initiate verbose logging for debugging purposes.

Display node affinity balancing status (svc_node_affinity_balance_status)

This service script enables you to display the status of node affinity balancing operations within the cluster.

Format

```
svc_node_affinity_balance status [-h] [-d]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-d, --debug	Initiate verbose logging for debugging purposes.

Check and fix the NTP status (svc_ntp_ctl)

This service script enables you to check the status of NTP on each node. You can also force a sync to the NTP service locally or for both nodes on the array.

Usage

Function	Diagnostic
Mode	Normal and Service
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Appliance
Prerequisites	None

Format

```
svc_ntp_ctl [-h] [--set] [--local] [--server SERVER] [--color] [--nocolor]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--set	Sync the time to the first valid server.
--local	Run locally only and skip the peer.

Qualifier	Description
--server	Manually specify the server or servers to use.
--color	Force color output even on nonterminals.
--nocolor	Do not use color on the terminal.

Customize validation service parameters (svc_onv_customizing)

This service script enables you to customize different parameters of ongoing validation services such as NTP validation, DNS validation, and others.

In addition, this script allows you to override the default parameters of ongoing validation services and list the overridden parameters.

NOTE: The current values for the validation parameters can be displayed using the **svc_onv_customizing list_onv_parameters** script.

Here is the list of ongoing validation parameters that you can override:

- NTP
 - NTP validation delay: This parameter is the interval between NTP validation cycles.
 - NTP alert skip threshold: This parameter is the number of alerts to skip before publishing an alert in PowerStore Manager. This parameter prevents alert flickering in unstable network environments.
 - NTP verbosity interval: This parameter is the interval between verbose logging operations for NTP validation procedures.
- DNS
 - DNS validation delay: This parameter is the interval between DNS validation cycles.
 - DNS verbosity interval: This parameter is the interval between performing verbose logging operations for DNS validation procedures.
- VMware
 - VMware validation delay: This parameter is the interval between VMware validation cycles.
 - VMware verbosity interval: This parameter is the interval between performing verbose logging operations for VMware validation procedures.
- vCenter
 - vCenter validation delay: This parameter is the interval between vCenter validation cycles.
 - vCenter alert skip threshold: This parameter is the number of alerts to skip before publishing a customer-visible alert in PowerStore Manager. This parameter is helpful for unstable network environments to prevent alert flickering.
 - vCenter verbosity interval: This parameter is the interval between performing verbose logging operations for vCenter validation procedure.
- Address conflict detection
 - Address conflict detection validation delay: This parameter is the interval between address conflict detection validation cycles.
 - Address conflict detection verbosity interval: This parameter is the interval between performing verbose logging for address conflict detection validation procedures.
- Basic connectivity validation
 - Basic connectivity validation delay (intercluster connectivity checks): This parameter is the interval between intercluster connectivity validation cycles.
 - Basic connectivity verbosity interval: This parameter is the interval between performing verbose logging operations for intercluster connectivity validation procedures.
- Connection validation: These parameters validate L2D, physical switches, bonds, cabling, and MTU.
 - Connection validation delay: This parameter is the interval between connection validation cycles.
 - Connection verbosity interval: This parameter is the interval between performing verbose logging operations for connection validation procedures.
- Storage connectivity validation
 - Storage connectivity validation delay (intercluster connectivity validation for storage networks): This parameter is the interval between storage connectivity validation cycles.
 - Storage connectivity verbosity interval: The parameter is the interval between performing verbose logging operations for validation storage network procedures.

- Storage connectivity max validation track size: This parameter is the size of the buffer for tracking storage networks that were recently validated. If storage networks are stored in the buffer, the validation for them is skipped during next validation cycle. If the maximum validation track size is 0, no storage networks are tracked, and all storage networks are validated during each validation cycle.
- Storage connectivity validation window size: This parameter is the number of skipped validation cycles between validation procedures for a given storage network.

Usage

Function	System Operations
Mode	Normal and Service
Usage	General use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_onv_customizing [-h] {set,list_onv_parameters,get}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
set	Set the value for a specified ongoing validation parameter.
list_onv_parameters	List onv parameters and their current values.
get	Get the value of a specific ongoing validation parameter.

Set onv parameters and their values (svc_onv_customizing set)

This service script enables you to set the value for a specified ongoing validation parameter.

Format

```
svc_onv_customizing set [-h] [--ntp_validation_delay <value>]
[--ntp_alert_skip_threshold <value>] [--dns_validation_delay <value>]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--ntp_validation_delay	Change the validation period of the NTP service.
--ntp_alert_skip_threshold	Change the number of alerts about NTP problems to skip before publishing an alert.
--dns_validation_delay	Change the validation period of the DNS service.

List ongoing parameters (svc_onv_customizing list_onv_parameters)

This service script enables you to list all the ongoing parameters and their current values.

Format

```
svc_onv_customizing list_onv_parameters -h
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Get a specific parameter (svc_onv_customizing get)

This service script enables you to get the value of a specific ongoing validation parameter.

Format

```
svc_onv_customizing get [-h] [--ntp_validation_delay <value>]  
[--ntp_alert_skip_threshold <value>] [--dns_validation_delay <value>]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--ntp_validation_delay	Get the current validation period of the NTP service.
--ntp_alert_skip_threshold	Get the current number of alerts about NTP problems to skip before publishing an alert.
--dns_validation_delay	Get the current validation period of the DNS service.

Disable password reset (svc_password_mgmt)

This service script enables you to prevent the service and administrator passwords from being reset. If you disable the password reset capability, lost passwords cannot be recovered.

Usage

Function	Configuration
Mode	Service and Normal
Usage	Technical Service
Requires service user password?	Yes
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_password_mgmt [-h] {recovery}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
recovery	Enable or disable the emergency password recovery.

Enable and prevent passwords from being recovered (svc_password_mgmt_recovery)

This script disables the ability to restore default admin and service user passwords. Once the ability to reset the passwords is disabled, there is no nondestructive way access the cluster if the passwords are lost.

Format

```
svc_password_mgmt recovery [-h] [-s] [-e] [-D]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-e, --enable	Enable the password emergency recovery option.
-D, --disable	Disable the password emergency recovery option.

Qualifier	Description
-s, --status	Display the current emergency recovery configuration.

Example

Use the following command to disable the emergency password recovery option:

```
svc_password_mgmt recovery --disable
INFO: Disabling password emergency recovery option...done
```

Send REST requests through the service container (svc_pstcli)

This service script enables you to send REST requests within the service container without having to provide a username and password.

This script uses certificate-based authentication and does not accept usernames and passwords.

Usage

Function	Configuration
Mode	Service and Normal
Usage	Technical Service
Requires service user password?	Yes
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_pstcli [-h] all
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.  NOTE: To get a full list of available commands, enter --help all . To get help on specific command category, enter --help <command or category name> .

Actions

Action	Description
all	Show all commands.

Command categories

The following table lists the command categories that are found on the target system:

Category	Description
Compute	Manage host configurations, virtual machines, and VMware integration.
Migration	Manage data imports and data migration from remote systems.
Monitoring	View event logs and alerts.
Protection	Manage replication and data protection rules, and witnesses.
Settings	Configure general settings on the system, including the following: • Networking • Licensing • Updates
Storage	Manage the storage configuration of the system: • Create and delete storage resources. • Configure NAS servers.
Support	Manage service user credentials and perform service actions on the system.
System_and_Hardware	Manage hardware, view component health status, and change the cluster configuration.

Available subcommands for each category

Category	Description
Compute	• <code>discovered_initiator</code> • <code>host</code> • <code>host_group</code> • <code>host_virtual_volume_mapping</code> • <code>host_volume_mapping</code> • <code>initiator</code> • <code>vcenter</code> • <code>virtual_machine</code> • <code>vsphere_host</code> • <code>vsphere_host_license_assignment</code>
Migration	• <code>file_import_interface</code> • <code>import_host_volume</code> • <code>import_session</code> • <code>import_unity_consistency_group</code> • <code>import_vmax_volume</code> • <code>import_xtremio_consistency_group</code> • <code>file_import_nas_server</code> • <code>import_netapp</code> • <code>import_storage_center</code> • <code>import_unity_volume</code>

Category	Description
	• <code>import_vnx_array</code> • <code>import_xtremio_volume</code> • <code>file_import_session</code> • <code>import_netapp_volume</code> • <code>import_storage_center_consistency_group</code> • <code>import_universal_volume</code> • <code>import_vnx_consistency_group migration_recommendation</code> • <code>import_host_initiator</code> • <code>import_psgroup</code> • <code>import_storage_center_volume</code> • <code>import_vmax</code> • <code>import_vnx_volume</code> • <code>migration_session</code> • <code>import_host_system</code> • <code>import_psgroup_volume</code> • <code>import_unity</code> • <code>import_vmax_storage_group</code> • <code>import_xtremio</code>
Monitoring	• <code>alert</code> • <code>event</code> • <code>fast_metrics_config</code> • <code>job</code> • <code>metrics</code> • <code>remote_syslog_server</code>
Protection	• <code>policy</code> • <code>remote_system</code> • <code>replication_rule</code> • <code>replication_session</code> • <code>snapshot_rule</code> • <code>storage_container_destination</code> • <code>witness</code>
Settings	• <code>audit_event</code> • <code>email_notify_destination</code> • <code>keystore_archive</code> • <code>ldap_domain</code> • <code>login_banner</code> • <code>network</code> • <code>physical_switch</code> • <code>smtp_config</code> • <code>software_installed</code> • <code>chap_config</code> • <code>ip_pool_address</code> • <code>kmip_config</code> • <code>license</code> • <code>login_session</code> • <code>ntp</code> • <code>role</code> • <code>dns</code> • <code>ip_port</code> • <code>ldap_account</code>

Category	Description
	• local_user • mfa_securid • nvme_discovered_cdc • security_config • software_component • x509_certificate
Storage	• datastore • file_events_pool • file_interface • file_ldap • file_system • file_virus_checker • nfs_export • recycle_bin • smb_server • virtual_volume • file_dhsm_config • file_events_publisher • file_interface_route • file_ndmp • file_tree_quota • io_limit_rule • nfs_server • recycle_bin_config • smb_share • volume • file_dns • file_ftp • file_kerberos • file_nis • file_user_quota • nas_server • performance_rule • replication_group • storage_container • volume_group
Support	• datacollection • maintenance_window • metrics_archive • remote_support_contac • service_config • service_user
System_and_Hardware	• appliance • bond • cluster • discovered_appliance • eth_be_port • eth_port • fc_port • fsn

Category	Description
	• hardware • node • sas_port • veth_port

Using subcommands

Some subcommands have additional options that you can use.

Example 1

The following example shows the general use of the **svc_pstcli** script:

```
svc_pstcli
Perform a single action on an object on the destination system.
  pstcli [-d <address>] [-port <number>] [-u <user_name>] [-p <password>] [-t <token> |
-tokenSecure] [-ssl { interactive | reject | accept | store }] [-header] <object>
<action> [<qualifiers>]

Open a session with the destination system to perform multiple actions.
  pstcli [-d <address>] [-port <number>] [-u <user_name>] [-p <password>] [-t <token> |
-tokenSecure] [-ssl { interactive | reject | accept | store }] [-header] -session

Get detailed help on CLI client options.
  pstcli help { CMD | -session | -version | -save_cred | -remove_cred |
-remove_all_creds | -default | -cert_list | -cert_del | -cert_clear | -clear_cache }

Remote certificate:
1:      Thumbprint algorithm = sha1
      Thumbprint             = 17 fa 04 73 0e 0e f3 4c 68 4f 6f de 47 46 55 a8 af d8 30 23
      Serial number          = 53 cc 3f 4b 62 88 3b ba
      Issuer                  = CN=Dell EMC PowerStore CA AZ3S74UN,O=Dell EMC,ST=MA,C=US
      Subject                  =
SERIAL=8423df8395cce6054d47b55626ae3f61ceeb32bd2febf41b0aa558f7af2b87c3,CN=ManagementHTTP
.PS50480cbe7bf8,OU=PowerStore,O=Dell,L=Hopkinton,ST=Massachusetts,C=US

      Valid from              = 10/26/2023 03:41:36 AM
      Valid to                 = 10/25/2028 03:41:36 AM

Would you like to:
  [1] Accept the certificate for this session
  [2] Reject the certificate
  [3] Accept and store
Please input your selection (The default selection is [1]):
List of command categories available on the target system:
  Compute          - Manage host configurations, virtual machines and VMware
integration
  Migration         - Manage data import and data migration from remote systems
  Monitoring        - View event logs and alerts
  Protection        - Manage replication and data protection rules, and witnesses
  Settings          - Configure general settings on the system including:
                    * Networking
                    * Licensing
                    * Updates
  Storage           - Storage configuration of the system:
                    * Create delete storage resources
                    * Configure NAS servers
  Support           - Manage service user credentials, perform service actions on the
system
  System_and_Hardware - Manage hardware, view component health status, change cluster
configuration

To get a full list of commands use "help all".
To get help on a specific command or category use "help <command or category name>".
```

Example 2

The following example shows the use of the **discovered_initiator** subcommand:

```
svc_pstcli help discovered_initiator
Actions:
  [show]
    discovered_initiator show [ -select <field>,... ] [ -sort <sort field>[+|-],... ] [
    -offset <value> ] [ { -limit <value> | -all } ] [ -query <value> ] [ -output { nvp | csv
    [ -table ] [
      -noformat ] | table | json [ -raw ] } ]

  Where <field> is one of:
    name, nvme_transport_addresses, nvme_transport_types, nvme_transport_types_l10n,
    protocol_type, protocol_type_l10n

  Where <sort field> is one of:
    name, nvme_transport_addresses, nvme_transport_types, nvme_transport_types_l10n,
    protocol_type, protocol_type_l10n
```

Example 3

The following example shows a query for installed software:

```
svc_pstcli software_installed show

# | appliance.id | id | release_version | installed_date |
-----+-----+-----+-----+-----+
1 | 459eb057-09c8-4d26-a3d8-ccd49a489afc | 3.6.1.0 | 10/27/2023
03:38:38 AM | A1
2 | 8cd33e30-0f12-42b1-808a-bb6706591050 | 3.6.1.0 | 10/27/2023 03:38:38 AM
```

Example 4

The following example shows a query for DNS settings:

```
svc_pstcli dns show

# | id | addresses
---+---+-----
1 | DNS1 | 10.244.53.108
| | 10.228.254.66
[SVC:service@CG6N7W3-A user]$
```

Troubleshoot and repair (svc_remote_support)

This service script enables you to troubleshoot and repair the appliance using the SupportAssist feature.

Usage

Function	Diagnostic
Mode	Normal or Service
Usage	Service
Requires service user password?	No

Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Appliance
Prerequisites	The firewall must be configured correctly.

Format

```
svc_remote_support [-h] {modify,list,connectivity,modify_contact,reinitialize,restart}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
modify	Modify the remote support configuration. Configuring SupportAssist does not include connection verification. Use the <code>--CONNECTIVITY_COMMAND</code> argument to verify connections. The SupportAssist configuration using this script is not persistent and therefore is not saved in the management database. When a node or appliance fails, configuration and connectivity information might be lost. In such cases, you must revert the configuration to the cluster configuration using the <code>--revert_changes_to_db</code> option or the <code>--REINITIALIZATION_COMMAND</code> argument.
list	List the components of the remote support configuration. If SupportAssist is enabled, this script also reports the eVE docker container status.
modify_contact	Modify the remote support user contact information and credentials.
restart	SupportAssist only. Restart the eVE docker on the current appliance if enabled.
connectivity	List the appliance remote support connectivity status.
reinitialize	SupportAssist only. Reinitialize the eVE docker on the current appliance if enabled. This action stops the container, restarts it, and reprovisions the container.  NOTE: When this command is used, the SupportAssist configuration and connectivity might be lost or temporarily lost. The SupportAssist configuration is reverted to the cluster configuration.

List the remote configuration (svc_remote_support list)

This service script lists the remote support configurations.

Format

```
svc_remote_support list [-h]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Modify the remote support configuration (svc_remote_support_modify)

This service script modifies the remote support configuration. Configuring SupportAssist does not verify the remote support connection. Use the `--CONNECTIVITY_COMMAND` argument for the `svc_remote_support` command to verify connections.

The SupportAssist configuration that is established using this script is not persistent and is not saved in the management database. Upon node or appliance failure, configuration and connectivity information may be lost. In such cases, you must restore the configuration back to the cluster configuration using `--revert_changes_to_db` option or the `--REINITIALIZATION_COMMAND` argument.

Format

```
svc_remote_support modify [-h] [--gateway_address value]
                           [--revert_changes_to_db]
                           [--proxy_password value]
                           [--proxy_port value] [--disable]
                           [--proxy_address value]
                           [--i_accept_license_agreement]
                           [--proxy_user value]
                           [--type
{SUPPORT_ASSIST__Direct_Tier3,SUPPORT_ASSIST__Gateway_Tier3}]
                           [--force_disable]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--gateway_address	The address of the gateway endpoint.
--revert_changes_to_db	Revert the SupportAssist configuration back to the cluster configuration.
--proxy_password	Use the proxy password.
--proxy_port	Specify the proxy port.
--disable	Disable support assist.
--proxy_address	Use the proxy address.
--i_accept_license_agreement	Accept the license agreement.
--proxy_user	Specify the proxy user.
--type	Modify the type of SupportAssist. There are two types: • SUPPORT_ASSIST__Direct_Tier3 • SUPPORT_ASSIST__Gateway_Tier3
--force_disable	Disables SupportAssist even if there is no active end-to-end connection.

Use case

If you decommission a gateway before disabling SupportAssist on a cluster, the appliance cannot communicate with the decommissioned gateway. The appliance also cannot migrate to a new gateway. Using the `--force_disable` argument on each appliance allows you to disable SupportAssist.

Modify contact information (svc_remote_support modify_contact)

This service script modifies the remote support configuration.

Format

```
svc_remote_support modify_contact [-h] [--phone value] [--first_name value]
[--last_name value] [--email value] contact_id
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--first_name	Specify the first name of the contact.
--last_name	Specify the last name of the contact.
--email	Specify the contact email.
--phone	Specify the contact mobile phone.

Positional arguments

Qualifier	Description
contact_id	Contact ID - 0 or 1.

Reinitialize the remote support configuration (svc_remote_support reinitialize)

This service script is used to reinitialize the eVE docker on the current appliance if enabled. This script stops the container, restarts it, and reprovisions it.

 **NOTE:** When this command is used, the SupportAssist configuration and connectivity information might be lost or temporarily be lost. The SupportAssist configuration is reverted to the cluster configuration.

Format

```
svc_remote_support reinitialize [-h]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Restart SupportAssist (svc_remote_support restart)

This service script is used in embedded SRS only. Restart the eVE docker on the current appliance if enabled.

Format

```
svc_remote_support restart [-h]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Use case

If SupportAssist cannot be configured or connect to Dell EMC Support, `svc_remote_support restart --factory_reset` enables you to reinitialize SupportAssist.

Check the connectivity status (svc_remote_support connectivity)

This service script lists the remote support connectivity status of the appliance.

Format

```
svc_remote_support connectivity [-h]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Manage the remote syslog (svc_remote_syslog)

This service script is a remote syslog service debugging helper tool.

Usage

Function	Diagnostic
Mode	Normal or Service
Usage	Service
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No

Scope	Cluster
Prerequisites	The firewall must be configured correctly.

Format

```
svc_remote_syslog [-h] [-t value] [-m value] [-r] [-lc] [-ls]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-t ,--test	Verify remote syslog server network connectivity. Usage example: <code>svc_remote_syslog --test '129bf965-cb3e-4294-8edc-cdcbf0f7e72a'</code> or <code>svc_remote_syslog --test '129bf965-cb3e-4294-8edc-cdcbf0f7e72a' --message 'My test message'</code> .
-m ,--message	The test message to send to the remote server. Usage example: <code>svc_remote_syslog --test '129bf965-cb3e-4294-8edc-cdcbf0f7e72a' --message 'My test message'</code> .
-r, --reinit	Reinitialize the remote syslog service. Usage example: <code>svc_remote_syslog --reinit</code> .
-lc, --list_remote_server_config	List remote server configuration instances. Usage example: <code>svc_remote_syslog --list_remote_server_config</code> .
-ls, --list_remote_logging_sync	List remote server sync instances. Usage example: <code>svc_remote_syslog --list_remote_logging_sync</code> .

Refresh the expired Unity SSL certificate (svc_remote_system_certificate_operations)

This service script enables you to refresh the expired Unity remote system SSL certificate in PowerStore SDNAS.

Usage

Function	System Operations
Mode	Normal and Service
Usage	Service
Requires service user password?	Not available through REST
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Appliance
Prerequisites	The Unity remote system must have been added to the PowerStore array.

Format

```
svc_remote_system_certificate_operations [-h] [-r]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Required arguments

Qualifier	Description
-r, --renew_unity_certificate	Renew the expired Unity certificate.

Remove appliance (svc_remove_appliance)

This service script enables you to remove an appliance from the cluster without migrating existing data or workloads. When you run the script, it displays the associated storage resources and workloads for the appliance you specified.

 **NOTE:** Run this script only on the master node.

Migrate the relevant storage resources and workloads to another appliance before removing it from the cluster. If there are data protection operations in progress, the script is unable to remove the appliance. However, the script enables you to stop any replication operations.

CAUTION:

- **Removing the appliance using this script is not an ideal use case. Ensure that you really want to remove the appliance.**
- **This script not only removes the appliance, but also resets it back to original factory settings and shuts it down.**
- **Although the IP addresses assigned to the appliance remain with the cluster and are marked as unused, all data is removed.**
- **The script does not block user commands or actions. Ensure that users are notified not to create any storage resources or virtual machines when you begin migrating data off the appliance. If new storage resources and virtual machines are created during this operation, the workloads may get placed on the appliance you are trying to remove.**

Ensure that all relevant storage resources and workloads are migrated to another appliance before you proceed.

You cannot remove a master appliance. See the Knowledgebase article - HOW17166 for more information.

Usage

Function	Diagnostic and Recovery
Mode	Service
Usage	Service
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	Yes

May cause data loss?	Yes
Scope	Appliance
Prerequisites	• Ensure that all workloads (virtual machines or storage resources) are migrated to another appliance in the cluster. • Before you remove the appliance, you might want to ensure that you place the ESXi host in maintenance mode and remove it from the ESXi cluster. See the Knowledgebase article - HOW17164 for more information.

Format

```
svc_remove_appliance [-h] [-d] [--limit <value>]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-d, --debug	Initiate verbose logging for debug.
--limit	Limit the number of workload items to display.

Renew certificates (svc_renew_certificates)

This service script enables you to renew PowerStore CA signed certificates .

Usage

Function	System operations
Mode	Normal or Service
Usage	Normal or Service
Requires service user password?	Yes
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_renew_certificates [-h] [-d] [-v] {list,run}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-d, --debug	Initiate verbose logging for debugging operations.
-v, --verbose	Initiate verbose command output.

Actions

Action	Description
list	List all available certificates for renewal.
run,	Renews the certificate type that you specify for renewal, or renews all certificates.

Renew a specific certificate, or all certificates (svc_renew_certificate run)

This service script enables you to renew a specified PowerStorecertificate or all certificates, depending on the command arguments.

Format

```
svc_renew_certificates run -h  
{all,replication_mutual_authentication,powerstore_cluster_server_internal,powerstore_cluster_server_external,powerstore_cluster_server_client}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
all	Renew all certificates.
replication_mutual_authentication,	Renew the PowerStore replication mutual authentication certificate.
powerstore_cluster_server_internal	Renew the PowerStore cluster server internal certificate.
powerstore_cluster_server__external	Renew the PowerStore cluster server external certificate.
powerstore_cluster_server_client	Renew the PowerStore cluster client certificate.

Show certificates for renewal (svc_renew_certificates list)

This script enables you to list all the certificates that are available for renewal.

Format

```
svc_renew_certificates list [-h] [-d]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-d, --debug	Initiate verbose logging for debugging operations.

Renew VASA certificates (svc_renew_vasa_self_signed_certificate)

This script enables you to renew a VASA Server PowerStore CA signed certificate.

Usage

Function	System operations
Mode	Normal or Service
Usage	Normal or Service
Requires service user password?	Yes
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_renew_vasa_self_signed_certificate [-h] [--force] [--verbose] [--debug] [--quiet]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-d, --debug	Initiate verbose logging for debugging operations.
-v, --verbose	Initiate verbose command output.

Qualifier	Description
--quiet	Suppress any additional prompts or messages.

Repair software (svc_repair)

This service script enables you to repair the software while keeping persistent configuration information such as hostname, host registration, and user data. This per-node operation overwrites the system partition with a software image that is stored on a back-end system device.

Usage

Function	Diagnostic
Mode	Normal or Service
Usage	Service
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	The firewall must be configured correctly.

Format

```
svc_repair [-h] [--backup]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--backup	Back up the ESXi network configuration.

Replace the DPE (svc_replace_dpe)

This service script enables you to perform a DPE replacement.

 **WARNING: Only trained service personnel should use this script.**

Ensure that the following conditions are met before running this script:

- Only one node should be installed in the DPE.
- The system type must have been set using the Post Utilities.
- After setting the system type, the node should be rebooted.

The node reboots into service mode.

When the node enters service mode, run the script. The node must be in service mode to execute the script.

Perform the following steps after the script is run:

1. Remove both power cables from the DPE.
2. Once the node is powered off, insert the other Node into the DPE.
3. Plug in both power cables and boot both nodes.

The system should boot normally.

Usage

Function	Diagnostic
Mode	Normal or Service
Usage	Service
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	The firewall must be configured correctly.

Format

```
svc_replace_dpe [-h] [-d] {auto,manual}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-d, --debug	Increase logging level to debug and print logs to console.

Actions

Qualifier	Description
auto	Updates the required DPE resumes when performing a DPE replacement.
manual	Performs a DPE replacement using user supplied DPE Resume values. It should only be run when the auto replacement failed to obtain the resume values from the system. The user will be prompted for the following chassis resume values: • Product Serial Number EMC_Vendor SN/Service Tag EMC_WWN Seed • Product Part Number WARNING: This utility is for trained service personnel only.

Replace the DPE (svc_replace_dpe auto)

This service script is used to update the required DPE resumes when performing a DPE replacement.

Format

```
svc_replace_dpe auto [-h] [-d]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-d, --debug	Initiate verbose logging for debug.

Replace the DPE (svc_replace_dpe manual)

This service script performs a DPE replacement using user supplied DPE Resume values. It should only be run when the auto replacement failed to obtain the resume values from the system. The user will be prompted for the following chassis resume values:

Product Serial Number EMC_Vendor SN/Service Tag EMC_WWN Seed Product

Part Number WARNING: This utility is for trained service personnel only.

Format

```
svc_replace_dpe manual [-h] [-d]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-d, --debug	Initiate verbose logging for debug.

Service mode operation (svc_rescue_state)

This service script enables you to check whether the node is in service Mode.

Usage

Function	Diagnostic
Mode	Normal and Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Node
Prerequisites	None

Format

```
svc_rescue_state [-h] {clear,set,list}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
clear	Clear the current boot mode. After running this command, you must reboot the node to return it to normal mode.
set	Set the boot mode for service mode. After running this command, you must reboot the node for it to enter service mode.
list	List the available boot modes for this node.

Unlock a secure snapshot (svc_secure_snapshot)

This service script enables you to unlock a secure snapshot.

Usage

Function	System operations
Mode	Normal or Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	Yes
May cause data unavailability?	No
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_secure_snapshot [-h] {unlock} [id]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
unlock	Unlock a secure snapshot by using its ID.

Positional arguments

Qualifier	Description
id	The ID of the secure snapshot.

Grant service user access (svc_service_config)

This service script enables you to grant service users the ability to log in to the primary node of an appliance. You can also delete service user access and list which users have login access to the primary node.

Usage

Function	System operations
Mode	Normal or Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	Yes
May cause data unavailability?	No
May cause data loss?	No
Scope	Appliance
Prerequisites	None

Format

```
svc_service_config [-h] {enable,list,disable}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
enable	Enable SSH access for the service user on an appliance.
list	List the SSH configuration.
disable	Disable SSH access for the service user on an appliance.

Gain root privileges (svc_service_shell)

This service script enables you to gain root privileges and run commands that require root privileges.

Before using the `svc_service_shell` script, you must enable it using the `svc_inject` script:

- 1. Generate a key to enable root escalation: `svc_inject generate-key --root`
- 2. Contact your service provider to get response key.
- 3. Copy the response key and use it with the `svc_inject` script to enable root escalation: `svc_inject run <response_key>`

If the command successfully completes, you are granted root level access and can run the `service_shell` script as shown in the following example:

```
svc_inject run
194E3-2CDB8-1B367-D3D51-C9100-28BDA-5BDC0-906F9-00

Current Challenge:
19478-FC2C3-06C82-5FD3D-3A5F7-E73A9

INFO: Response successfully validated!
INFO: Enabling tool ...
INFO: Successfully enabled svc_service_shell
INFO: Run "svc_service_shell" to be granted root level access for servicing this system
```

See [Inject troubleshooting software tool \(svc_inject\)](#) for more information about the `svc_inject` script.

Usage

Function	Recovery
Mode	Normal or Service
Usage	Service
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Node
Prerequisites	None

Format

```
svc_service_shell [-h] [--cmd SHELL_CMD_ARGS]
```

Optional arguments

Table 3. Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--cmd SHELL_CMD_ARGS	Use this Linux command to gain elevated privileges in a Linux system and perform such functions as diagnosing and triaging a system.

Software recovery (svc_software_recovery)

This service script enables you to create a bootable software recovery image on a USB drive. After the image is created, you can use the USB drive to reimage the peer node or a node in another appliance.

Usage

Function	Diagnostic and Recovery
Mode	Service
Usage	Service
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Appliance
Prerequisites	None

Format

```
svc_software_recovery [-h] --usbcreate [--newcfg] [--savecfgforce]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
--usbcreate	Create a bootable USB recovery drive that you can use to recover the peer node.
--newcfg	Create a bootable USB installer drive. You can use this action to completely reinitialize a node to the factory state.
--savecfgforce	Create a generic bootable USB recovery device. Other manual steps may be required for a full recovery.

Connect to the peer node service container (svc_ssh_peer)

This service script enables you to securely connect through SSH from the local node as the service user to the service container of the peer node as the service user.

Usage

Function	System Operations
Mode	Normal and Service
Usage	General Use
Requires service user password?	No

Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Node
Prerequisites	The peer appliance must be available through the network interconnect, and the peer service container must be active.

Format

```
svc_ssh_peer
```

Collect system information (svc_system_info)

This service script enables you to collect system information including on disk space, sensors, drives, and other components. This information is collected in a text file.

Function	System Operations
Mode	Normal or Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	Yes
May cause data unavailability?	Yes
May cause data loss?	No
Scope	Cluster
Prerequisites	None

Format

```
svc_system_info [-h] {run,download}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Positional arguments

Qualifier	Description
run	Collect system information.
download	Download the text file that contains system information.

Monitor network traffic (svc_tcpdump)

This service script enables you to monitor network traffic and open a specific interface in order to run a **tcpdump** operation. You can save all output to rotating files.

Usage

Function	System Operations
Mode	Normal and Service
Usage	General Use
Requires service user password?	No
Requires root privileges?	No
May cause data unavailability?	No
May cause data loss?	No
Scope	Node
Prerequisites	None

Format

```
svc_tcpdump [-h] [-i <value>] [-w <value>] [-W <value>]
[-C <value>] [-s <value>] [-t {1,2,3,4}] [-v {1,2,3}] [-D] [-F <value>]
[-e] [-n] [-q] [-T <value>] [-N {host,file}] [-Q {in,out,inout}]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-i, --interface	Specifies the interface that you want to use to capture information. The default interface for the host namespace is mgmt0. The default namespace for file is eth_data0.
-w, --filename	The base file name for the output files. The default is dump.out.  NOTE: This option requires root privileges.
-W, --rotations	Specifies the number of files for output. The default is 5, and the maximum is 20.
-C, --size	Specifies the size of each output file in MB. The default is 50, and the maximum is 200.
-s, --snaplen	Captures a specified number of bytes from each packet instead of the default value. The default value is 65535.0.
-t, --timestamp	Specify a specific timestamp command ranging from 1 to 4 . The timestamp commands are as follows: • 1: Do not print a timestamp on each dump line. • 2: Print an unformatted timestamp on each dump line. • 3: Print a delta, which is measured in microseconds, between the current line and the previous line for each dump line. • 4: Print a timestamp in the default format. The default format shows the date before each timestamp.
-v, --verbosity	Specify how verbose you want the output to be. The maximum is 3 .

Qualifier	Description
-D, --dump_intfs	Print the list of network interfaces available on the system and on which the tcpdump operation can capture packets.
-F, --input_expr	Specify a file to use as input for the filter expression. The file must be in the <code>/cyc_var/cyc_service/tcpdump</code> directory.
-a, --add_filter	Create a file with filter expression from user input. This option can only be used with the <code>input_expr</code> option. If the <code>input_expr</code> option is present, a filename is created with the value from that option. Otherwise, a random filter filename is generated in the following format: <code>tcpdump_filter_XXXX.txt</code>
-e, --llheader	Print the link-level header on each dump line.
-n, --no_addr	Do not convert addresses such as host addresses or port numbers to names.
-q, --quiet	Print less protocol information so that the output is shorter.
-T, --timeout	Specifies the amount of time that can elapse before stopping the trace. The timeout format is <code>xy</code> , where <code>x</code> is a number and <code>y</code> indicates the units that are used to measure time (seconds, minutes, hours, days - for example, 30s , 10m , 5h , 2d). Set the timeout to <code>no</code> to never stop the trace. The default is <code>no</code> .  NOTE: This option requires root privileges.
-N, --namespace	Define the network namespace as <code>host</code> or <code>file</code> . The default is <code>host</code> . The NAS server namespace is <code>file</code> .
-Q, direction	Choose the send or receive direction for which packets should be captured. Possible values are in , out , and inout .

View capacity metrics (svc_volume_space_metrics)

This service script shows detailed information about the available space on volume families. You can use the arguments to specify how you want the information to be displayed.

This script is primarily used when the appliance is out of space (OOS). If the appliance is not in the OOS state, you can force the operation.

Usage

Function	System operations
Mode	Normal or Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	Yes
May cause data unavailability?	No
May cause data loss?	No
Scope	Appliance
Prerequisites	None

Format

```
svc_volume_space_metrics [-h] [-d] [-v] [-i ID] [-n Name]
                        [-s {name,cap}] [-g GT] [-c] [-j]
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.
-d, --detail	Show detailed output.
-v, --vertical	Show space metrics in a vertical format.
-i, --id	Display space metrics for a single volume family by ID.
-n, --name	Display space metrics for a single volume family by name of Volume/FS/vVol.
-s {name, cap} , --sort {name, cap}	Display volume families in order by name or capacity.
-g, --gt	Only display the volume families that consume space that is greater than the specified value.
-c, --csv	Place the output in a CSV file.
-j, --json	Place the output in a JSON file.

Complete the recovery process (svc_wear_trickle_write)

This service script enables you to complete the manual recovery process once the system enters wear trickle write mode.

Usage

Function	System Operations
Mode	Service
Usage	Service
Requires service user password?	Yes
Requires root privileges?	Yes
May cause data unavailability?	Yes
May cause data loss?	No
Scope	Node
Prerequisites	None

Format

```
svc_wear_trickle_write [-h]
{exit_trickle,enable_policy,show_drives,list_policy,disable_policy}
```

Optional arguments

Qualifier	Description
-h, --help	Show the help message and exit.

Actions

Action	Description
exit_trickle	Manually exit wear trickle write mode. Use this command after the recovery procedure is complete. If you want to continue using the worn-out drives and exit trickle write mode, you must disable the exit trickle write policy before using this command.
enable_policy	Enable wear the trickle-write policy. The wear trickle-write policy is enabled by default.
show_drives	List all worn-out SSD drives in the system.
list_policy	Get the current wear trickle-write policy setting.
disable_policy	Disable the wear trickle-write policy.

System Journal Fields

Information in the system journal are stored in fields. When you run the `svc_journalctl`, you can choose to display information from these fields or filter the output based on the information in these fields. This appendix describes the fields available for use in the journal:

Topics:

- [Field descriptions](#)

Field descriptions

The core logging framework relies on the systemd journal services provided by the underlying CoreOS operating system. In addition to the default fields available with systemd journal in CoreOS, there are custom fields available for use with the cluster. The following table lists the descriptions of all the fields available for use.

Table 4. Journal field descriptions

Type	Name	Description
Default	__CURSOR	Unique identifier that describes the position of the entry in the journal.
Default	__MONOTONIC_TIMESTAMP	The monotonic clock timestamp indicating the time elapsed between a certain event and the time when the entry in the journal occurred.
Default	__REALTIME_TIMESTAMP	The wall clock timestamp indicating the point in time when the entry was logged in the journal.
Default	_AUDIT_LOGINUID, _AUDIT_SESSION	The session and login UID of the process from where the journal entry originates from.
Default	_BOOT_ID	The kernel boot ID of the boot in which the message was generated.
Default	_CAP_EFFECTIVE	The effective capabilities of the process from where the journal entry originates from.
Default	_CMDLINE	The command line of the process the journal entry originates from
Default	_COMM	The name of the process the journal entry originates from.
Default	_EXE	The executable path of the process the journal entry originates from.
Default	_GID	The group ID of the process the journal entry originates from.
Default	_HOSTNAME	The name of the originating host.
Default	_KERNEL_DEVICE	The name of the kernel device.
Default	_KERNEL_SUBSYSTEM	The name of the kernel subsystem.
Default	_LINE_BREAK	Indicates that the log message in the standard output/error stream was not terminated with a normal newline character.
Default	_MACHINE_ID	Machine ID of the host from where the journal entry originates from.
Default	_PID	The process ID of the process the journal entry originates from.

Table 4. Journal field descriptions (continued)

Type	Name	Description
Default	_SELINUX_CONTEXT	The SELinux security context (label) of the process from where the journal entry originates from.
Default	_SOURCE_REALTIME_TIMESTAMP	Earliest trusted timestamp of the message.
Default	_STREAM_ID	Unique identifier of the stream connection when it was first created.
Default	_SYSTEMD_CGROUP, _SYSTEMD_INVOCATION_ID, _SYSTEMD_OWNER_UID, _SYSTEMD_SESSION, _SYSTEMD_SLICE, _SYSTEMD_UNIT, _SYSTEMD_USER_UNIT	Systemd information of the process the journal entry originates from.
Default	_TRANSPORT	Information on how the journal service received the message entry.
Default	_UDEV_DEVLINK	The low-level Unix error number causing this entry.
Default	_UDEV_DEVNODE	The device node path of this device in /dev.
Default	_UDEV_SYSNAME	The kernel device name as it shows up in the device tree below /sys.
Default	_UID	The user ID of the process the journal entry originates from.
Custom	AUDIT_TIMESTAMP, AUDIT_USERNAME, AUDIT_IS_SUCCESSFUL, AUDIT_CLIENT_ADDRESS, AUDIT_SERVER_ADDRESS, AUDIT_APPLIANCE_ID, AUDIT_JOB_ID, AUDIT_RESOURCE_TYPE, AUDIT_RESOURCE_ACTION, AUDIT_RESOURCE_ID, AUDIT_RESOURCE_NAME, AUDIT_MESSAGE_CODE, AUDIT_MESSAGE_L10N, AUDIT_REQUEST_BODY	Additional fields used in the audit logs.
Default	CODE_FILE	Source file name that contains the code generating the message.
Default	CODE_FUNC	Function name in the code generating the message.
Default	CODE_LINE	Location of the code in the source file generating the message.
Custom	COMPONENT	The logging component. Values include: • CP—Components that enable management of the cluster. • DP—Backend data engine components. • Platform—Backend platform or base storage container (BSC) components. • Service—Serviceability or service container components. • Fireman—Backend services responsible for handling communications between internal components. • PostGres—PostGres services.
Custom	CONTEXT_ID	Unique identifier to track requests.
Default	COREDUMP_UNIT, COREDUMP_USER_UNIT	Used to annotate messages containing coredumps from system and session units.

Table 4. Journal field descriptions (continued)

Type	Name	Description
Default	ERRNO	Low-level Unix-based error number associated with the entry in the journal.
Custom	MARKER	Unique string used to quickly identify certain events or conditions. Values include: REST, RemoteSupport, ZMQ, NDU (non-disruptive upgrades), CC (cluster creation), LUN, ConfigurationCapture, Event, RB (resource balancer), Import, PhysicalInventory, IDF (platform ID files), DATAMOBILITY, NETWORK, DataCollection, and Host.
Default	MESSAGE	The message string for the entry in the systemd journal.
Default	MESSAGE_ID	Unique identifier of the message.
Default	OBJECT_AUDIT_LOGINUID, OBJECT_AUDIT_SESSION, OBJECT_CMDLINE, OBJECT_COMM, OBJECT_EXE, OBJECT_GID, OBJECT_PID, OBJECT_SYSTEMD_CGROUP, OBJECT_SYSTEMD_OWNER_UID, OBJECT_SYSTEMD_SESSION, OBJECT_SYSTEMD_UNIT, OBJECT_SYSTEMD_USER_UNIT, OBJECT_UID	Additional fields added automatically by the systemd journal.
Custom	OBJECT_CURRENT_STATE_NAME	Current state name associated with the object.
Custom	OBJECT_HANDLE	Unique identifier used to represent a resource managed within the cluster.
Custom	OBJECT_ID	Unique identifier of the object for which you want to retrieve information from the system journal.
Custom	OBJECT_OPERATION	Type of operation associated with the object.
Custom	OBJECT_SUB_TYPE	The sub-type of the object for which you want to retrieve information from the system journal.
Custom	OBJECT_TYPE	Type of the object for which you want to retrieve information from the system journal.
Default	PRIORITY	Journal message level. Valid levels are: ● CRITICAL—Events that demand immediate attention. ● ERROR—Events that indicate problems, but do not require immediate attention. ● WARN—Events that provide a warning about potential problems or indicates that a component is not in an ideal state. ● INFO—Informational messages that provide details on the running status and changes to the system. ● DEBUG—Verbose status, such as progress or success messages.
Custom	ROOT_COMMAND_ID	Context ID of the primary request.
Custom	STATUS_CODE	Status code that represents a response to a particular request.
Custom	SUB_COMPONENT	The sub-component associated with the message.
Default	SYSLOG_FACILITY	Syslog compatibility field that contains the name of the facility.
Default	SYSLOG_IDENTIFIER	Syslog compatibility field that contains the unique identifier.

Table 4. Journal field descriptions (continued)

Type	Name	Description
Default	SYSLOG_PID	Syslog compatibility field that contains the process identifier.
Custom	THREAD_NAME	Name of the thread logging the message.