HX Data Platform Support

Using TAC Support for Troubleshooting

This section lists common TAC support-assisted tasks, and describes how to configure automatic support options and create HyperFlex support bundles.

Support bundles are a collection of logs from several components within and used by the HX Data Platform. This includes:

- HX Data Platform Installer VM—Logs provide information about installation.

- Controller VM—Logs provide information about the HX Data Platform file system, cluster creation, and cluster expansion.

- VMware ESXi host—Logs provide information about the nodes in the HX storage cluster.

- VMware vCenter—Logs provide information about the HX Data Platform Plug-in and the vCenter server.

TAC uses support bundles to assist in troubleshooting your issues.

Common TAC-Assisted Support Topics

The following is a brief list of support topics that are best handled with Technical Assistance Center (TAC) assistance:

- Adding disks to a node in the HX storage cluster fails to be recognized.

- Adding a node to the HX storage cluster fails.

- Changing the IP address for the HX storage cluster.

- Destroying a cluster, including destroying an encrypted cluster.

- Downgrading the HX Data Platform version.

- Failing HX storage cluster creation.

- Modifying a node rebalance timeout.

- Modifying VDI or VSI optimized deployment for the HX storage cluster.

- Removing a node in a 3-node cluster.

- Replacing a node in a 4-node cluster.

- Replacing a housekeeping SSD on HX240c servers.

- Reusing a removed node in another HX storage cluster.

- Reusing disks from a removed node.

- Setting the `cleaner` schedule for recovering storage.

- Setting the MTU value to something other than 9000.

- Sizing guidance for using non-default larger capacity SSD or HDD per server is supported.

- Uninstalling the HX Data Platform.

- Uninstalling the HX storage cluster.

- Upgrading the HX Data Platform from a version older than HX Data Platform version 1.7.1.

- Using the `stcli` commands `whitelist` or `recreate`.

Auto Support and Smart Call Home for HyperFlex

You can configure the HX storage cluster to send automated email notifications regarding documented events. The data collected in the notifications can be used to help troubleshoot issues in your HX storage cluster.

Auto Support (ASUP)

Auto Support is the alert notification service provided through HX Data Platform. If you enable Auto Support, notifications are sent from HX Data Platform to designated email addresses or email aliases that you want to receive the notifications. Typically, Auto Support is configured during HX storage cluster creation by configuring the SMTP mail server and adding email recipients.

Note Only unauthenticated SMTP is supported for ASUP.

If the **Enable Auto Support** check box was not selected during configuration, Auto Support can be enabled post-cluster creation using the following methods:

Post-Cluster ASUP Configuration Method	Associated Topic
HX Connect user interface	Configuring Auto Support Using HX Connect, on page 3
Command Line Interface (CLI)	Configuring Notification Settings Using CLI, on page 4

Post-Cluster ASUP Configuration Method	Associated Topic
REST APIs	Cisco HyperFlex Support REST APIs on Cisco DevNet.

Auto Support can also be used to connect your HX storage cluster to monitoring tools.

Smart Call Home (SCH)

Smart Call Home is an automated support capability that monitors your HX storage clusters and then flags issues and initiates resolution before your business operations are affected. This results in higher network availability and increased operational efficiency.

Call Home is a product feature embedded in the operating system of Cisco devices that detects and notifies the user of a variety of fault conditions and critical system events. Smart Call Home adds automation and convenience features to enhance basic Call Home functionality. After Smart Call Home is enabled, Call Home messages/alerts are sent to Smart Call Home.

Smart Call Home is included with many Cisco service contracts and includes:

- Automated, around-the-clock device monitoring, proactive diagnostics, real-time email alerts, service ticket notifications, and remediation recommendations.

- Proactive messaging sent to your designated contacts by capturing and processing Call Home diagnostics and inventory alarms. These email messages contain links to the Smart Call Home portal and the TAC case if one was automatically created.

- Expedited support from the Cisco Technical Assistance Center (TAC). With Smart Call Home, if an alert is critical enough, a TAC case is automatically generated and routed to the appropriate support team through `https`, with debug and other CLI output attached.

- Customized status reports and performance analysis.

- Web-based access to: all Call Home messages, diagnostics, and recommendations for remediation in one place; TAC case status; and up-to-date inventory and configuration information for all Call Home devices.

To ensure automatic communication among your HX storage cluster, you, and Support, see Configuring Smart Call Home for Data Collection, on page 5.

Configuring Auto Support Using HX Connect

Typically, Auto Support (ASUP) is configured during HX storage cluster creation. If it was not, you can enable it post cluster creation using the HX Connect user interface.

Step 1   Log in to HX Connect.

Step 2   In the banner, click **Edit settings (gear icon)** > **Auto Support Settings** and fill in the following fields.

UI Element	Essential Information
Enable Auto Support (Recommended) check box	Configures Call home for this HX storage cluster by enabling: - Data delivery to Cisco TAC for analysis. - Notifications from Support as part of proactive support.

UI Element	Essential Information
Send service ticket notifications to field	Enter the email address that you want to receive the notifications.
Terms and Conditions check box	End user usage agreement. The check box must be checked to use the Auto-Support feature.
Use Proxy Server check box	• **Web Proxy Server** url • **Port** • **Username** • **Password**

Step 3   Click **OK**.

Step 4   In the banner, click **Edit settings (gear icon)** > **Notifications Settings** and fill in the following fields.

UI Element	Essential Information
Send email notifications for alarms check box	If checked, fill in the following fields: • **Mail Server Address** • **From Address**—Enter the email address used to identify your HX storage cluster in Support service tickets, and as the sender for Auto Support notifications. Support information is currently not sent to this email address. • **Recipient List (Comma separated)**

Step 5   Click **OK**.

Configuring Notification Settings Using CLI

Use the following procedure to configure and verify that you are set up to receive alarm notifications from your HX storage cluster.

✎

Note   Only unauthenticated SMTP is supported for ASUP.

Step 1   Log in to a storage controller VM in your HX storage cluster using `ssh`.

Step 2   Configure the SMTP mail server, then verify the configuration.

Email address used by the SMTP mail server to send email notifications to designated recipients.

Syntax: `stcli services smtp set [-h] --smtp SMTPSERVER --fromaddress FROMADDRESS`

Example:

```
# stcli services smtp set --smtp mailhost.eng.mycompany.com --fromaddress smtpnotice@mycompany.com
# stcli services smtp show
```

Step 3   Enable ASUP notifications.

```
# stcli services asup enable
```

Step 4   Add recipient email addresses, then verify the configuration.

List of email addresses or email aliases to receive email notifications. Separate multiple emails with a space.

Syntax: `stcli services asup recipients add --recipients RECIPIENTS`

Example:

```
# stcli services asup recipients add --recipients user1@mycompany.com user2@mycompany.com
# stcli services asup show
```

Step 5   From the controller VM that owns the eth1:0 IP address for the HX storage cluster, send a test ASUP notification to your email.

```
# sendasup -t
```

To determine the node that owns the eth1:0 IP address, log in to each storage controller VM in your HX storage cluster using `ssh` and run the `ifconfig` command. Running the `sendasup` command from any other node does not return any output and tests are not received by recipients.

Step 6   Configure your email server to allow email to be sent from the IP address of all the storage controller VMs.

Configuring Smart Call Home for Data Collection

Data collection is enabled by default but, during installation, you can opt-out (disable). You can also enable data collection post cluster creation. During an upgrade, Smart Call Home is set up based on your legacy configuration. For example, if `stcli services asup show` is enabled, Smart Call Home is enabled on upgrade.

Data collection about your HX storage cluster is forwarded to Cisco TAC through `https`. If you have a firewall installed, configuring a proxy server for Smart Call Home is completed post cluster creation.

Note   In HyperFlex Data Platform release 2.5(1.a), Smart Call Home Service Request (SR) generation does not use a proxy server.

Using Smart Call Home requires the following:

- A Cisco.com ID associated with a corresponding Cisco Unified Computing Support Service or Cisco Unified Computing Mission Critical Support Service contract for your company.

- Cisco Unified Computing Support Service or Cisco Unified Computing Mission Critical Support Service for the device to be registered.

Step 1   Log in to a storage controller VM in your HX storage cluster.

Step 2   Register your HX storage cluster with Support.

Registering your HX storage cluster adds identification to the collected data and automatically enables Smart Call Home. To register your HX storage cluster, you need to specify an email address. After registration, this email address receives support notifications whenever there is an issue and a TAC service request is generated.

Note	Upon configuring Smart Call Home in Hyperflex, an email will be sent to the configured address containing a link to complete registration. If this step is not completed, the device will remain in an inactive state and an automatic Service Request will not be opened.

Syntax:

```
stcli services sch set [-h] --email EMAILADDRESS
```

Example:

```
# stcli services sch set --email name@company.com
```

Step 3 Verify data flow from your HX storage cluster to Support is operational.

Operational data flow ensures that pertinent information is readily available to help Support troubleshoot any issues that might arise.

`--all` option runs the commands on all the nodes in the HX cluster.

```
# asupcli [--all] ping
```

If you upgraded your HX storage cluster from HyperFlex 1.7.1 to 2.1.1b, also run the following command:

```
# asupcli [--all] post --type alert
```

Contact Support if you receive the following error:

```
root@ucs-stctlvm-554-1:/tmp# asupcli post --type alert
/bin/sh: 1: ansible: not found
Failed to post - not enough arguments for format string
root@ucs-stctlvm-554-1:/tmp#
```

Step 4 (Optional) Configure a proxy server to enable Smart Call Home access through port 443.

If your HX storage cluster is behind a firewall, after cluster creation, you must configure the Smart Call Home proxy server. Support collects data at the `url: https://diag.hyperflex.io:443` endpoint.

a. Clear any existing registration email and proxy settings.

```
# stcli services sch clear
```

b. Set the proxy and registration email.

Syntax:

stcli services sch set [-h] --email EMAILADDRESS [--proxy-url PROXYURL] [--proxy-port PROXYPORT] [--proxy-user PROXYUSER] [--portal-url PORTALURL] [--enable-proxy ENABLEPROXY]

Syntax Description	Option	Required or Optional	Description
	--email EMAILADDRESS	Required.	Add an email address for someone to receive email from Cisco support. Recommendation is to use a distribution list or alias.
	--enable-proxy ENABLEPROXY	Optional.	Explicitly enable or disable use of proxy.
	--portal-url PORTALURL	Optional.	Specify an alternative Smart Call Home portal URL, if applicable.
	--proxy-url PROXYURL	Optional.	Specify the HTTP proxy URL, if applicable.

Option	Required or Optional	Description
--proxy-port PROXYPORT	Optional.	Specify the HTTP proxy port, if applicable.
--proxy-user PROXYUSER	Optional.	Specify the HTTP proxy user, if applicable. Specify the HTTP proxy password, when prompted.

Example:

```
# stcli services sch set
  --email name@company.com
  --proxy-url www.company.com
  --proxy-port 443
  --proxy-user admin
  --proxy-password adminpassword
```

c. Ping to verify the proxy server is working and data can flow from your HX storage cluster to the Support location.

```
# asupcli [--all] ping
```

`--all` option runs the command on all the nodes in the HX cluster.

Step 5 Verify Smart Call Home is enabled.

When Smart Call Home configuration is `set`, it is automatically enabled.

```
# stcli services sch show
```

If Smart Call Home is disabled, enable it manually.

```
# stcli services sch enable
```

Step 6 Enable Auto Support (ASUP) notifications.

Typically, Auto Support (ASUP) is configured during HX storage cluster creation. If it was not, you can enable it post cluster creation using HX Connect or CLI. For more information, see Auto Support and Smart Call Home for HyperFlex.

Cisco HX Data Platform Support Bundles

You can generate a support bundle through command line interface.

Through the HX Connect user interface, you can also generate a support bundle that collects the logs from every selected controller VM and ESXi host in the HX storage cluster. The vCenter logs are not collected through HX Connect.

All support bundle timestamps are listed in the UTC timezone regardless of cluster timezone or server timezone settings.

After you generate a support bundle, you can upload it to the HX Data Platform FTP server for use by TAC. You can also download an existing support bundle. Support bundle types are:

Generating a Support Bundle Using HX Connect

You can use the HX Connect user interface to generate a support bundle that collects the logs from every controller VM and ESXi host in the local HX storage cluster. If you are using replication to protect your virtual machines and their data, when you need to generate a support bundle, you also need to generate a support bundle from the remote HX storage cluster. The vCenter logs are not collected through HX Connect.

Note If you are generating a support bundle using the CLI, then the support bundle is displayed as **Other** type in HX Connect user interface.

Before you begin

Note If you are using HXDP version 3.5(2a) or 3.5(2b) do not use HX Connect. We recommend that you use the CLI of individual SCVMs to generate the storfs bundle.

Creating logs from HX Connect may cause storfs to crash causing a Hyperflex cluster outage.

Step 1 Log in to HX Connect.

Step 2 In the banner, click **Edit settings (gear icon)** > **Support Bundle**.

Alternatively, click **System Information** > **Support Bundle**.

Note You must have either FQDN or IP address to access HX Connect and not just the host name

Step 3 Click **Generate**.

Creating the support bundle can take one to two hours.

Step 4 When the support bundle displays, click *supportBundle.zip* to download the file to your local computer.

Downloading the support bundle can take one to two hours.

You download an existing support bundle in the same way.

What to do next

You can now upload the file to the HX Data Platform FTP server.

Generating an Audit Log

When you generate a support bundle through the HX Connect user interface, audit logs are automatically included.

Step 1 Generate and download a support bundle. See

If you prefer, you can download an existing support bundle.

Step 2   Unzip the support bundle and extract the files to your local computer.

Step 3   In each controller VM, search for `/var/log/shell.log`.

Step 4   Open each `shell.log` file and search for the audit trail records using keyword **stcli**.

This log contains an audit of `stcli` calls that are invoked in the shell.

Example:

```
2017-07-14T16:48:39.135+00:00 SpringpathControllerHOCBY4KNF1 shell: [pid=20396, uid=0] stcli cluster
 restart
```

Where

- `2017-07-14T16:48:39.135+00:00` is the time when the `stcli` command was invoked.

- `uid=0` specifies the user ID of the user who invoked the `stcli` command. In the example, the user ID is `0` and the user is root.

- `stcli cluster restart` command provides the `stcli` command that was executed.

Step 5   In each controller VM, search for `/var/log/springpath/audit-rest.log`.

Step 6   Open each `audit-rest.log` file and search for the audit trail records using keyword **audit**.

This log contains an audit of REST APIs.

Example:

```
2017-06-29-23:26:38.096 - Audit - 127.0.0.1 -> 127.0.0.1 - create
 /rest/datastores/00000000d8902473:00000000000100ef?action=mount; 200; administrator@vsphere.local
555ms
```

Where

- `2017-06-29-23:26:38.096` is the time when the REST API was invoked.

- `127.0.0.1` is the IP address from which the call arrived.

- `create` is the action that was performed.

- `/rest/datastores/00000000d8902473:00000000000100ef?action=mount` is the resource that is accessed with parameters.

- `200` is the HTTP status of this action.

- `administrator@vsphere.local` is the user who invoked this REST API.

- `555ms` is the time taken for this operation.

Step 7   Collect all audit trail records from the previous steps and save them in separate files.

Collecting Logs from Controller VMs

There are two options for collecting controller VM logs.

Step 1   **Option 1**

   a)   Log in to each controller VM using `ssh`.

b) Run the command: `storfs-support`

Generating the logs takes about 2 minutes.

c) Locate the `tar.gz` log file in the `/var/support` directory. For example:

`storfs-support_2016-06-22--06-06-33_ucs--stctlvm-123-1.eng.storvisor.com.tar.gz`

d) Upload the `tar.gz` file from the controller VM to the HX Data Platform FTP server.

Step 2 **Option 2**

a) Log in to each controller VM using `ssh`.

b) Run the command: `asupcli [--all] post --type asup`

`--all` option runs the command on all the nodes in the HX cluster.

c) If Smart Call Home is disabled, the `tar.gz` file that is generated can be found in the `/var/support/asup_default` directory.

This file also contains the log from the respective ESXi host.

d) Upload the `tar.gz` file from the controller VM to the HX Data Platform FTP server.

Collecting Logs from ESXi Hosts

There are two options for collecting ESXi host logs.

Step 1 **Option 1**

a) Log in to each ESXi host using `ssh`.

b) Run the command: `vm-support`

Generating the logs takes about 5 minutes.

c) Locate the `.tgz` file in the `/var/tmp` directory. For example:

`esx-localhost-2016-06-22--06.09.tgz`

d) Upload the `.tgz` file from the ESXi host to the HX Data Platform FTP server.

Step 2 **Option 2**

a) Log in to each controller VM using `ssh`.

b) Run the command: `asupcli collect --type esx --subtype full`

c) Upload the `tar.gz` file in the `/var/support/esx-asup-default` directory from each controller VM to the HX Data Platform FTP server.

The `tar.gz` file contains only ESXi logs. If TAC requested all logs, see .

Out of Space Error When Generating a Support Bundle

An out of space error occurs when the storage controller VM does not have sufficient space left to generate the support bundle, typically due to the size of the core file or previously-generated log files consuming space. The following error displays when you are using the `vm-support` command to generate support bundles:

```
error = [Errno 28] No space left
```

To generate a support bundle when you receive this error:

Step 1   Delete or move the core file and existing log files to a location outside of the storage controller VM.

Step 2   Log in to the command line of the storage controller VM.

Step 3   Generate a light support bundle.

```
# storfs-support
```

Collecting Deployment Logs from the Cisco HX Data Platform Installer VM

Step 1   Log in to the HX Data Platform Installer VM using `ssh` and the following credentials:

- Username: **root**

- Password (Default): **Cisco123**

  Note   Systems ship with a default password of `Cisco123` that must be changed during installation. You cannot continue installation unless you specify a new user supplied password.

Step 2   Run the command: `deployment-support`

Generating the logs takes less than a minute.

Step 3   Locate the `tar.gz` logs in the `/var/support` directory. For example:

```
storfs-support_2016-06-22--06-25-35_Cisco-HX-Data-Platform-Installer.tar.gz
```

Step 4   Upload the `.tar.gz` file to the Cisco FTP server.

Collecting Logs from the vCenter Server

Step 1   Log in to the vCenter server using `ssh`.

Step 2   Run the command: `vc-support -l`

Generating the logs takes about 10-20 minutes depending on the number of nodes that are running in the vCenter server.

Step 3   Locate the logs in the `/storage/log` directory.

Step 4 Upload the logs to the Cisco FTP server.

Collecting Logs from vSphere Web Client

You can selectively collect all or some of the logs for the Cisco HX Data Platform storage cluster ESXi hosts, controller VMs, and vCenter server through thevSphere Web Client.

Step 1 Log in to the vSphere Web Client. Through the **Navigator**, select **vCenter Inventory Lists** > **Resources** > **vCenter Servers** > *server*.

Step 2 Right-click the vCenter server for the HX Data Platform cluster and select **Export System Logs**.

Step 3 From the **Source** panel, select the servers from which you want to collect the logs.

Step 4 Optionally, to include the vCenter logs, select **Include vCenter Server and vSphere Web Client logs**, and click **Next**.

Step 5 From the **Ready to Complete** panel, select the system logs to include.

    Select **Virtual Machines** to ensure the logs from the controller VMs for each selected server are included.

Step 6 Click **Generate Log Bundle**.

    Generating the logs takes about 40-50 minutes.

Step 7 When the logs are completed:
a) Click **Download Log Bundle**.
b) Specify a location to download the support bundle. For example, download the files to your local PC.
c) Click **Finish**.
d) Upload the files to the Cisco FTP server.

Collecting Logs from the Cisco HX Data Platform Plug-in

You can use the HX Data Platform Plug-in to collect the logs for just the HX storage cluster ESXi hosts and controller VMs.

Step 1 Log in to vSphere Web Client. Through the **Navigator**, select **vCenter Inventory Lists** > **Resources** > **Clusters** > *cluster*.

Step 2 Right-click an HX Data Platform cluster and select **Cisco HX Data Platform** > **Support**.

Step 3 Click **Generate Log Bundle**.

    Generating the logs takes about 40-50 minutes.

Step 4 When the logs are completed:
a) Click **Download Log Bundle**.
b) Specify a location to download the support bundle. For example, download the files to your local PC.
c) Click **Finish**.

d) Upload the files to the Cisco FTP server.

Downloading an Existing Support Bundle

Note   You can download a support bundle you generate up to midnight (12:00 a.m.) of the local controller VM time. HyperFlex stores two support bundle logs. When generating a new support bundle, the oldest one is deleted automatically.

Step 1   Log in to vSphere Web Client. Through the **Navigator**, select **vCenter Inventory Lists** > **Resources** > **Clusters**.

Step 2   Right-click the *cluster* and select **HX Data Platform Plug-in** > **Support** to display the **Support** dialog box.

Note   Select the *cluster* from the vSphere Web Client, not the HX Data Platform Plug-in.

Step 3   Click **Download Support Bundle** (enabled).

Step 4   Specify a download location (such as your local computer) to save the support bundle. You can then upload the file to the HX Data Platform FTP server.

Uploading Support Bundles

After you generate a support bundle, you can upload it to the HX Data Platform FTP server using one of the following methods:

- ftp—Use port 21.

- sftp—Use port 22.

- https—Use port 443.

Uploading Support Bundles using ftp or sftp

Before you begin

Generate a support bundle.

Step 1   Open your FTP Client (such as Filezilla) and connect to the HX Data Platform FTP server using the following information:

Option	Description
Host	`https://ftp.springpathinc.com`
Port	ftp = `21` sftp = `22`

Option	Description
Username	`cisco`
Password	`cisco`

Step 2 After you connect to the HX Data Platform FTP server, create a folder with the Support case number.

Step 3 Change directory to the new folder.

Step 4 Upload the support bundle log files to this folder.

Step 5 When the uploads are complete, contact Cisco Technical Assistance Center (TAC) and tell them the upload directory name.

Step 6 Free up space in your HX storage cluster by deleting the content in `/var/support/`.

Uploading Support Bundles using https

Before you begin

Generate a support bundle.

Step 1 Open a browser window, navigate to the HX Data Platform FTP server URL hosted by Springpath, and log in using the following information:

Option	Description
URL	`https://ftp.springpathinc.com`
Username	`cisco`
Password	`cisco`

Step 2 After you connect to the HX Data Platform FTP server, create a folder with the Support case number.

Step 3 Change directory to the new folder.

Step 4 Upload the support bundle log files to this folder.

Step 5 When the uploads are complete, contact Cisco Technical Assistance Center (TAC) and tell them the upload directory name.

Step 6 Free up space in your HX storage cluster by deleting the content in `/var/support/`.