NetApp

Recovering from system drive failure

StorageGRID

NetApp
October 03, 2025

Table of Contents

Recovering from system drive failure

If the system drive on a software-based Storage Node has failed, the Storage Node is not available to the StorageGRID system. You must complete a specific set of tasks to recover from a system drive failure.

About this task

Use this procedure to recover from a system drive failure on a software-based Storage Node. This procedure includes the steps to follow if any storage volumes also failed or cannot be remounted.

> ⓘ   This procedure applies to software-based Storage Nodes only. You must follow a different procedure to recover an appliance Storage Node.

Recovering a StorageGRID appliance Storage Node
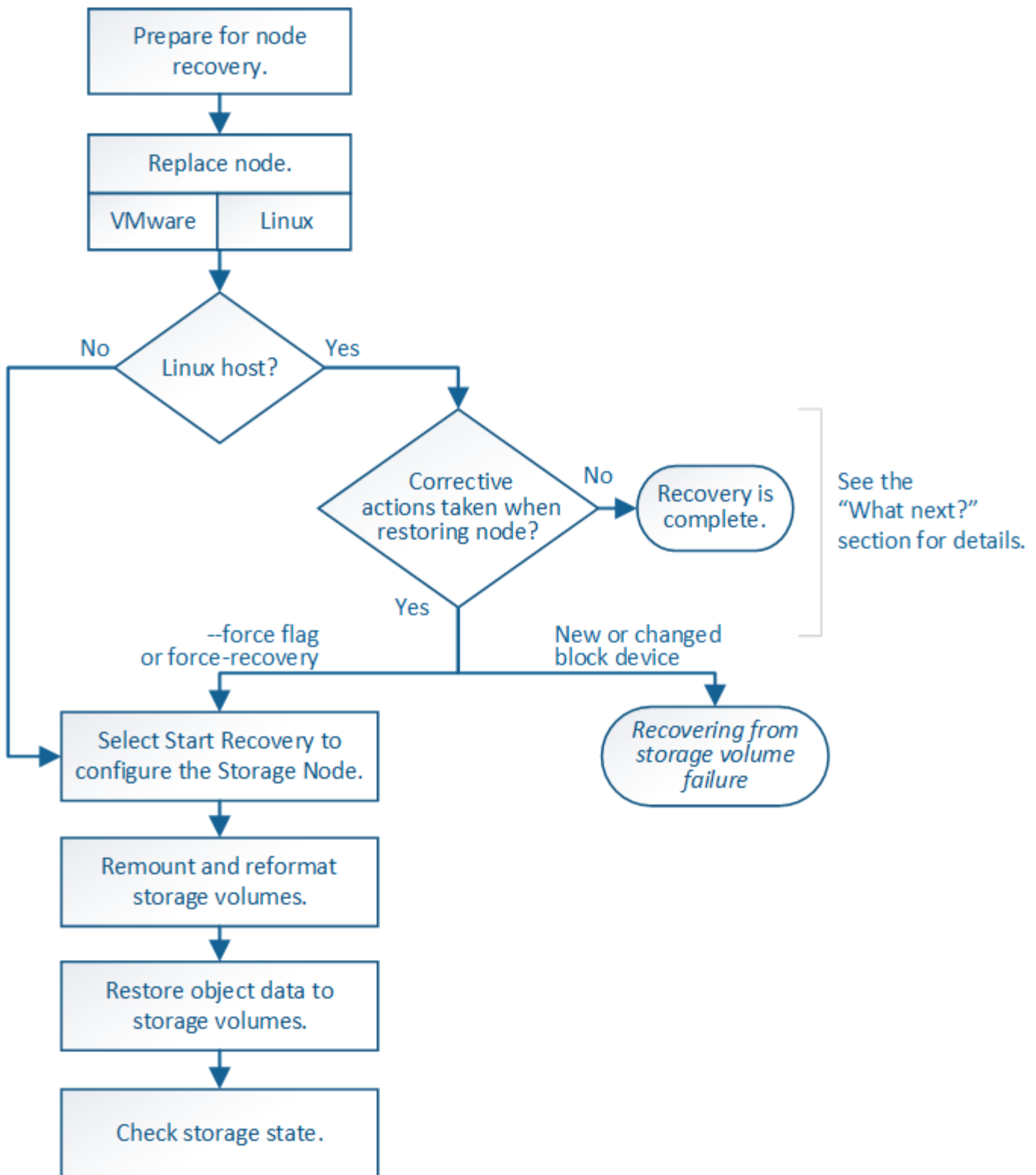
Steps

- Reviewing warnings for Storage Node system drive recovery
- Replacing the Storage Node
- Selecting Start Recovery to configure a Storage Node
- Remounting and reformatting storage volumes ("Manual Steps")
- Restoring object data to a storage volume, if required

Reviewing warnings for Storage Node system drive recovery

Before recovering a failed system drive of a Storage Node, you must review the following warnings.

Storage Nodes have a Cassandra database that includes object metadata. The Cassandra database might be rebuilt in the following circumstances:

- A Storage Node is brought back online after having been offline for more than 15 days.
- A storage volume has failed and been recovered.
- The system drive and one or more storage volumes fails and is recovered.

When Cassandra is rebuilt, the system uses information from other Storage Nodes. If too many Storage Nodes are offline, some Cassandra data might not be available. If Cassandra has been rebuilt recently, Cassandra data might not yet be consistent across the grid. Data loss can occur if Cassandra is rebuilt when too many Storage Nodes are offline or if two or more Storage Nodes are rebuilt within 15 days of each other.

> ! If more than one Storage Node has failed (or is offline), contact technical support. Do not perform the following recovery procedure. Data loss could occur.

> ! If this is the second Storage Node failure in less than 15 days after a Storage Node failure or recovery, contact technical support. Rebuilding Cassandra on two or more Storage Nodes within 15 days can result in data loss.

> (i) If more than one Storage Node at a site has failed, a site recovery procedure might be required. Contact technical support.

How site recovery is performed by technical support

> ! If this Storage Node is in read-only maintenance mode to allow for the retrieval of objects by another Storage Node with failed storage volumes, recover volumes on the Storage Node with failed storage volumes before recovering this failed Storage Node. See the instructions for recovering from loss of storage volumes where the system drive is intact.

> (i) If ILM rules are configured to store only one replicated copy and the copy exists on a storage volume that has failed, you will not be able to recover the object.

> (i) If you encounter a Services: Status - Cassandra (SVST) alarm during recovery, see the monitoring and troubleshooting instructions to recover from the alarm by rebuilding Cassandra. After Cassandra is rebuilt, alarms should clear. If alarms do not clear, contact technical support.

Related information

Monitor & troubleshoot

Warnings and considerations for grid node recovery

Replacing the Storage Node

If the system drive has failed, you must first replace the Storage Node.

You must select the node replacement procedure for your platform. The steps to replace a node are the same for all types of grid nodes.

> ⓘ This procedure applies to software-based Storage Nodes only. You must follow a different procedure to recover an appliance Storage Node.

Recovering a StorageGRID appliance Storage Node

Linux: If you are not sure if your system drive has failed, follow the instructions to replace the node to determine which recovery steps are required.

Platform	Procedure
VMware	Replacing a VMware node
Linux	Replacing a Linux node
OpenStack	NetApp-provided virtual machine disk files and scripts for OpenStack are no longer supported for recovery operations. If you need to recover a node running in an OpenStack deployment, download the files for your Linux operating system. Then, follow the procedure for replacing a Linux node.

Selecting Start Recovery to configure a Storage Node

After replacing a Storage Node, you must select Start Recovery in the Grid Manager to configure the new node as a replacement for the failed node.

What you'll need

- You must be signed in to the Grid Manager using a supported browser.
- You must have the Maintenance or Root Access permission.
- You must have the provisioning passphrase.
- You must have deployed and configured the replacement node.
- You must know the start date of any repair jobs for erasure-coded data.
- You must have verified that the Storage Node has not been rebuilt within the last 15 days.

About this task

If the Storage Node is installed as a container on a Linux host, you must perform this step only if one of these is true:

- You had to use the `--force` flag to import the node, or you issued `storagegrid node force-recovery` *node-name*

- You had to do a full node reinstall, or you needed to restore /var/local.

Steps

1. From the Grid Manager, select **Maintenance** > **Maintenance Tasks** > **Recovery**.

2. Select the grid node you want to recover in the Pending Nodes list.

   Nodes appear in the list after they fail, but you cannot select a node until it has been reinstalled and is ready for recovery.

3. Enter the **Provisioning Passphrase**.

4. Click **Start Recovery**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

	Name	IPv4 Address	State	Recoverable	
⦿	104-217-S1	10.96.104.217	Unknown	✔	

Passphrase

Provisioning Passphrase ••••••

Start Recovery

5. Monitor the progress of the recovery in the Recovering Grid Node table.

   ⓘ While the recovery procedure is running, you can click **Reset** to start a new recovery. An Info dialog box appears, indicating that the node will be left in an indeterminate state if you reset the procedure.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

	Cancel	OK

If you want to retry the recovery after resetting the procedure, you must restore the node to a pre-installed state, as follows:

- **VMware**: Delete the deployed virtual grid node. Then, when you are ready to restart the recovery, redeploy the node.

- **Linux**: Restart the node by running this command on the Linux host: `storagegrid node force-recovery` *node-name*

6. When the Storage Node reaches the stage "Waiting for Manual Steps" stage, go to the next task in the recovery procedure to remount and reformat storage volumes.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Recovering Grid Node

Name	Start Time	Progress	Stage
dc2-s3	2016-09-12 16:12:40 PDT		Waiting For Manual Steps

Reset

Related information

Remounting and reformatting storage volumes ("Manual Steps")

You must manually run two scripts to remount preserved storage volumes and to reformat any failed storage volumes. The first script remounts volumes that are properly formatted as StorageGRID storage volumes. The second script reformats any unmounted volumes, rebuilds Cassandra, if needed, and starts services.

What you'll need

- You have already replaced the hardware for any failed storage volumes that you know require

replacement.

Running the `sn-remount-volumes` script might help you identify additional failed storage volumes.

- You have checked that a Storage Node decommissioning is not in progress, or you have paused the node decommission procedure. (In the Grid Manager, select **Maintenance** > **Maintenance Tasks** > **Decommission**.)
- You have checked that an expansion is not in progress. (In the Grid Manager, select **Maintenance** > **Maintenance Tasks** > **Expansion**.)
- You have reviewed the warnings for Storage Node system drive recovery.

Reviewing warnings for Storage Node system drive recovery

> (!) Contact technical support if more than one Storage Node is offline or if a Storage Node in this grid has been rebuilt in the last 15 days. Do not run the `sn-recovery-postinstall.sh` script. Rebuilding Cassandra on two or more Storage Nodes within 15 days of each other might result in data loss.

About this task

To complete this procedure, you perform these high-level tasks:

- Log in to the recovered Storage Node.
- Run the `sn-remount-volumes` script to remount properly formatted storage volumes. When this script runs, it does the following:
  - Mounts and unmounts each storage volume to replay the XFS journal.
  - Performs an XFS file consistency check.
  - If the file system is consistent, determines if the storage volume is a properly formatted StorageGRID storage volume.
  - If the storage volume is properly formatted, remounts the storage volume. Any existing data on the volume remains intact.
- Review the script output and resolve any issues.
- Run the `sn-recovery-postinstall.sh` script. When this script runs, it does the following.

> (i) Do not reboot a Storage Node during recovery before running `sn-recovery-postinstall.sh` (see the step for post-install script) to reformat the failed storage volumes and restore object metadata. Rebooting the Storage Node before `sn-recovery-postinstall.sh` completes causes errors for services that attempt to start and causes StorageGRID appliance nodes to exit maintenance mode.

  - Reformats any storage volumes that the `sn-remount-volumes` script could not mount or that were found to be improperly formatted.

  > (i) If a storage volume is reformatted, any data on that volume is lost. You must perform an additional procedure to restore object data from other locations in the grid, assuming that ILM rules were configured to store more than one object copy.

  - Rebuilds the Cassandra database on the node, if needed.

◦ Starts the services on the Storage Node.

Steps

1. Log in to the recovered Storage Node:

   a. Enter the following command: `ssh admin@`*`grid_node_IP`*

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.

2. Run the first script to remount any properly formatted storage volumes.

   (i) If all storage volumes are new and need to be formatted, or if all storage volumes have failed, you can skip this step and run the second script to reformat all unmounted storage volumes.

   a. Run the script: `sn-remount-volumes`

   This script might take hours to run on storage volumes that contain data.

   b. As the script runs, review the output and answer any prompts.

   (i) As required, you can use the `tail -f` command to monitor the contents of the script's log file (`/var/local/log/sn-remount-volumes.log`). The log file contains more detailed information than the command line output.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
```

remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policy.

Do not continue to the next step if you believe that the data
remaining on
this volume cannot be rebuilt from elsewhere in the grid (for
example, if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policy.

```
Do not continue to the next step if you believe that the data
remaining on
this volume cannot be rebuilt from elsewhere in the grid (for
example, if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
```

The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.

In the example output, one storage volume was remounted successfully and three storage volumes
had errors.

- /dev/sdb passed the XFS file system consistency check and had a valid volume structure, so it
  was remounted successfully. Data on devices that are remounted by the script is preserved.

- /dev/sdc failed the XFS file system consistency check because the storage volume was new or
  corrupt.

- /dev/sdd could not be mounted because the disk was uninitialized or the disk's superblock was
  corrupted. When the script cannot mount a storage volume, it asks if you want to run the file system
  consistency check.

    - If the storage volume is attached to a new disk, answer **N** to the prompt. You do not need check
      the file system on a new disk.

    - If the storage volume is attached to an existing disk, answer **Y** to the prompt. You can use the
      results of the file system check to determine the source of the corruption. The results are saved
      in the /var/local/log/sn-remount-volumes.log log file.

- /dev/sde passed the XFS file system consistency check and had a valid volume structure;
  however, the LDR node ID in the volID file did not match the ID for this Storage Node (the
  configured LDR noid displayed at the top). This message indicates that this volume belongs to
  another Storage Node.

3. Review the script output and resolve any issues.

   (i) If a storage volume failed the XFS file system consistency check or could not be mounted,
       carefully review the error messages in the output. You must understand the implications of
       running the sn-recovery-postinstall.sh script on these volumes.
```

a. Check to make sure that the results include an entry for all of the volumes you expected. If any volumes are not listed, rerun the script.

b. Review the messages for all mounted devices. Make sure there are no errors indicating that a storage volume does not belong to this Storage Node.

   In the example, the output for `/dev/sde` includes the following error message:

   ```
   Error: This volume does not belong to this node. Fix the attached
   volume and re-run this script.
   ```

   > (!) If a storage volume is reported as belonging to another Storage Node, contact technical support. If you run the `sn-recovery-postinstall.sh` script, the storage volume will be reformatted, which might cause data loss.

c. If any storage devices could not be mounted, make a note of the device name, and repair or replace the device.

   > (i) You must repair or replace any storage devices that could not be mounted.

   You will use the device name to look up the volume ID, which is required input when you run the `repair-data` script to restore object data to the volume (the next procedure).

d. After repairing or replacing all unmountable devices, run the `sn-remount-volumes` script again to confirm that all storage volumes that can be remounted have been remounted.

   > (i) If a storage volume cannot be mounted or is improperly formatted, and you continue to the next step, the volume and any data on the volume will be deleted. If you had two copies of object data, you will have only a single copy until you complete the next procedure (restoring object data).

   > (!) Do not run the `sn-recovery-postinstall.sh` script if you believe that the data remaining on a failed storage volume cannot be rebuilt from elsewhere in the grid (for example, if your ILM policy uses a rule that makes only one copy or if volumes have failed on multiple nodes). Instead, contact technical support to determine how to recover your data.

4. Run the `sn-recovery-postinstall.sh` script: `sn-recovery-postinstall.sh`

   This script reformats any storage volumes that could not be mounted or that were found to be improperly formatted; rebuilds the Cassandra database on the node, if needed; and starts the services on the Storage Node.

   Be aware of the following:

   - The script might take hours to run.
   - In general, you should leave the SSH session alone while the script is running.
   - Do not press **Ctrl+C** while the SSH session is active.
   - The script will run in the background if a network disruption occurs and terminates the SSH session,

but you can view the progress from the Recovery page.

- If the Storage Node uses the RSM service, the script might appear to stall for 5 minutes as node services are restarted. This 5-minute delay is expected whenever the RSM service boots for the first time.

> (i) The RSM service is present on Storage Nodes that include the ADC service.

> (i) Some StorageGRID recovery procedures use Reaper to handle Cassandra repairs. Repairs occur automatically as soon as the related or required services have started. You might notice script output that mentions "reaper" or "Cassandra repair." If you see an error message indicating the repair has failed, run the command indicated in the error message.

5. As the `sn-recovery-postinstall.sh` script runs, monitor the Recovery page in the Grid Manager.

   The Progress bar and the Stage column on the Recovery page provide a high-level status of the `sn-recovery-postinstall.sh` script.

After the `sn-recovery-postinstall.sh` script has started services on the node, you can restore object data to any storage volumes that were formatted by the script, as described in that procedure.

Related information

Reviewing warnings for Storage Node system drive recovery

Restoring object data to a storage volume, if required

Restoring object data to a storage volume, if required

If the `sn-recovery-postinstall.sh` script is needed to reformat one or more failed storage volumes, you must restore object data to the reformatted storage volume from other Storage Nodes and Archive Nodes. These steps are not required unless one or more storage volumes were reformatted.

What you'll need

- You must have confirmed that the recovered Storage Node has a Connection State of **Connected*** ✓ on

the *Nodes > **Overview** tab in the Grid Manager.

About this task

Object data can be restored from other Storage Nodes, an Archive Node, or a Cloud Storage Pool, assuming that the grid's ILM rules were configured such that object copies are available.

> ⓘ   If an ILM rule was configured to store only one replicated copy and that copy existed on a storage volume that failed, you will not be able to recover the object.

> ⓘ   If the only remaining copy of an object is in a Cloud Storage Pool, StorageGRID must issue multiple requests to the Cloud Storage Pool endpoint to restore object data. Before performing this procedure, contact technical support for help in estimating the recovery time frame and the associated costs.

> ⓘ   If the only remaining copy of an object is on an Archive Node, object data is retrieved from the Archive Node. Due to the latency associated with retrievals from external archival storage systems, restoring object data to a Storage Node from an Archive Node takes longer than restoring copies from other Storage Nodes.

To restore object data, you run the `repair-data` script. This script begins the process of restoring object data and works with ILM scanning to ensure that ILM rules are met. You use different options with the `repair-data` script, based on whether you are restoring replicated data or erasure coded data, as follows:

- **Replicated data**: Two commands are available for restoring replicated data, based on whether you need to repair the entire node or only certain volumes on the node:

```
repair-data start-replicated-node-repair
```

```
repair-data start-replicated-volume-repair
```

- **Erasure coded (EC) data**: Two commands are available for restoring erasure coded data, based on whether you need to repair the entire node or only certain volumes on the node:

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Repairs of erasure coded data can begin while some Storage Nodes are offline. Repair will complete after all nodes are available. You can track repairs of erasure coded data with this command:

```
repair-data show-ec-repair-status
```

(i) The EC repair job temporarily reserves a large amount of storage. Storage alerts might be triggered, but will resolve when the repair is complete. If there is not enough storage for the reservation, the EC repair job will fail. Storage reservations are released when the EC repair job completes, whether the job failed or succeeded.

For more information on using the `repair-data` script, enter `repair-data --help` from the command line of the primary Admin Node.

Steps

1. Log in to the primary Admin Node:

   a. Enter the following command: `ssh admin@primary_Admin_Node_IP`

   b. Enter the password listed in the `Passwords.txt` file.

   c. Enter the following command to switch to root: `su -`

   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.

2. Use the `/etc/hosts` file to find the hostname of the Storage Node for the restored storage volumes. To see a list of all nodes in the grid, enter the following: `cat /etc/hosts`

3. If all storage volumes have failed, repair the entire node. (If only some volumes have failed, go to the next step.)

   (i) You cannot run `repair-data` operations for more than one node at the same time. To recover multiple nodes, contact technical support.

   ◦ If your grid includes replicated data, use the `repair-data start-replicated-node-repair` command with the `--nodes` option to repair the entire Storage Node.

   This command repairs the replicated data on a Storage Node named SG-DC-SN3:

   ```
   repair-data start-replicated-node-repair --nodes SG-DC-SN3
   ```

   (i) As object data is restored, the **Objects Lost** alert is triggered if the StorageGRID system cannot locate replicated object data. Alerts might be triggered on Storage Nodes throughout the system. You should determine the cause of the loss and if recovery is possible. See the instructions for monitoring and troubleshooting StorageGRID.

   ◦ If your grid contains erasure coded data, use the `repair-data start-ec-node-repair` command with the `--nodes` option to repair the entire Storage Node.

   This command repairs the erasure coded data on a Storage Node named SG-DC-SN3:

   ```
   repair-data start-ec-node-repair --nodes SG-DC-SN3
   ```

   The operation returns a unique `repair ID` that identifies this `repair_data` operation. Use this

`repair ID` to track the progress and result of the `repair_data` operation. No other feedback is returned as the recovery process completes.

> (i) Repairs of erasure coded data can begin while some Storage Nodes are offline. Repair will complete after all nodes are available.

   ◦ If your grid has both replicated and erasure coded data, run both commands.

4. If only some of the volumes have failed, repair the affected volumes.

   Enter the volume IDs in hexadecimal. For example, `0000` is the first volume and `000F` is the sixteenth volume. You can specify one volume, a range of volumes, or multiple volumes that are not in a sequence.

   All the volumes must be on the same Storage Node. If you need to restore volumes for more than one Storage Node, contact technical support.

   ◦ If your grid contains replicated data, use the `start-replicated-volume-repair` command with the `--nodes` option to identify the node. Then add either the `--volumes` or `--volume-range` option, as shown in the following examples.

   Single volume: This command restores replicated data to volume `0002` on a Storage Node named SG-DC-SN3:

   ```
   repair-data start-replicated-volume-repair --nodes SG-DC-SN3
   --volumes 0002
   ```

   Range of volumes: This command restores replicated data to all volumes in the range `0003` to `0009` on a Storage Node named SG-DC-SN3:

   ```
   repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume
   -range 0003-0009
   ```

   Multiple volumes not in a sequence: This command restores replicated data to volumes `0001`, `0005`, and `0008` on a Storage Node named SG-DC-SN3:

   ```
   repair-data start-replicated-volume-repair --nodes SG-DC-SN3
   --volumes 0001,0005,0008
   ```

   > (i) As object data is restored, the **Objects Lost** alert is triggered if the StorageGRID system cannot locate replicated object data. Alerts might be triggered on Storage Nodes throughout the system. You should determine the cause of the loss and if recovery is possible. See the instructions for monitoring and troubleshooting StorageGRID.

   ◦ If your grid contains erasure coded data, use the `start-ec-volume-repair` command with the `--nodes` option to identify the node. Then add either the `--volumes` or `--volume-range` option, as shown in the following examples.

   Single volume: This command restores erasure coded data to volume `0007` on a Storage Node

named SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Range of volumes: This command restores erasure coded data to all volumes in the range `0004` to `0006` on a Storage Node named SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range
0004-0006
```

Multiple volumes not in a sequence: This command restores erasure coded data to volumes `000A`, `000C`, and `000E` on a Storage Node named SG-DC-SN3:

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes
000A,000C,000E
```

The `repair-data` operation returns a unique `repair ID` that identifies this `repair_data` operation. Use this `repair ID` to track the progress and result of the `repair_data` operation. No other feedback is returned as the recovery process completes.

(i) Repairs of erasure coded data can begin while some Storage Nodes are offline. Repair will complete after all nodes are available.

   ◦ If your grid has both replicated and erasure coded data, run both commands.

5. Monitor the repair of replicated data.

   a. Select **Nodes** > **Storage Node being repaired** > **ILM**.

   b. Use the attributes in the Evaluation section to determine if repairs are complete.

      When repairs are complete, the Awaiting - All attribute indicates 0 objects.

   c. To monitor the repair in more detail, select **Support** > **Tools** > **Grid Topology**.

   d. Select **grid** > **Storage Node being repaired** > **LDR** > **Data Store**.

   e. Use a combination of the following attributes to determine, as well as possible, if replicated repairs are complete.

      (i) Cassandra inconsistencies might be present, and failed repairs are not tracked.

      ▪ **Repairs Attempted (XRPA)**: Use this attribute to track the progress of replicated repairs. This attribute increases each time a Storage Node tries to repair a high-risk object. When this attribute does not increase for a period longer than the current scan period (provided by the **Scan Period — Estimated** attribute), it means that ILM scanning found no high-risk objects that need to be repaired on any nodes.

         (i) High-risk objects are objects that are at risk of being completely lost. This does not include objects that do not satisfy their ILM configuration.

- **Scan Period — Estimated (XSCM)**: Use this attribute to estimate when a policy change will be applied to previously ingested objects. If the **Repairs Attempted** attribute does not increase for a period longer than the current scan period, it is probable that replicated repairs are done. Note that the scan period can change. The **Scan Period — Estimated (XSCM)** attribute applies to the entire grid and is the maximum of all node scan periods. You can query the **Scan Period — Estimated** attribute history for the grid to determine an appropriate time frame.

6. Monitor the repair of erasure coded data, and retry any requests that might have failed.

   a. Determine the status of erasure coded data repairs:

      ▪ Use this command to see the status of a specific `repair-data` operation:

      ```
      repair-data show-ec-repair-status --repair-id repair ID
      ```

      ▪ Use this command to list all repairs:

      ```
      repair-data show-ec-repair-status
      ```

      The output lists information, including `repair ID`, for all previously and currently running repairs.

      ```
      root@DC1-ADM1:~ # repair-data show-ec-repair-status

      Repair ID Scope Start Time End Time State Est Bytes
      Affected/Repaired Retry Repair
      =================================================================
      ================
      949283 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:27:06.9 Success
      17359 17359 No
      949292 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:37:06.9 Failure
      17359 0 Yes
      949294 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:47:06.9 Failure
      17359 0 Yes
      949299 DC1-S-99-10(Volumes: 1,2) 2016-11-30T15:57:06.9 Failure
      17359 0 Yes
      ```

   b. If the output shows that the repair operation failed, use the `--repair-id` option to retry the repair.

      This command retries a failed node repair, using the repair ID 83930030303133434:

      ```
      repair-data start-ec-node-repair --repair-id 83930030303133434
      ```

      This command retries a failed volume repair, using the repair ID 83930030303133434:

```
repair-data start-ec-volume-repair --repair-id 83930030303133434
```

Related information

[Administer StorageGRID](#)

[Monitor & troubleshoot](#)

Checking the storage state after recovering a Storage Node system drive

After recovering the system drive for a Storage Node, you must verify that the desired state of the Storage Node is set to online and ensure that the state will be online by default whenever the Storage Node server is restarted.

What you'll need

- You must be signed in to the Grid Manager using a supported browser.
- The Storage Node has been recovered, and data recovery is complete.

Steps

1. Select **Support** > **Tools** > **Grid Topology**.

2. Check the values of **Recovered Storage Node** > **LDR** > **Storage** > **Storage State — Desired** and **Storage State — Current**.

   The value of both attributes should be Online.

3. If the Storage State — Desired is set to Read-only, complete the following steps:

   a. Click the **Configuration** tab.

   b. From the **Storage State — Desired** drop-down list, select **Online**.

   c. Click **Apply Changes**.

   d. Click the **Overview** tab and confirm that the values of **Storage State — Desired** and **Storage State — Current** are updated to Online.