ThoughtSpot

ThoughtSpot Disaster Recovery Guide

Release 6.3

November, 2020

910 Hermosa Court, Sunnyvale, California 94085

Table of Contents

About disaster recovery

Summary: ThoughtSpot's disaster recovery prevents data loss if there is a hardware or software failure.

Disaster recovery is the ability to recover from a hardware or software failure or a catastrophic event. ThoughtSpot protects you from data loss in the event of a hardware or software failure or a catastrophic event.

ThoughtSpot takes snapshots of itself automatically at periodic intervals. These can be pulled out as backups at intervals or manually as needed. See the ThoughtSpot Administrator Guide for details on backups, snapshots and restore operations.

The information here addresses disaster recovery specifically. These are some potential types of failure, listed in increasing order of severity:

- **Disk failure** **[See page 3]**

  ThoughtSpot uses replication of stored data. When a disk faila, ThoughtSpot continues to operate.
- **Node failure** **[See page 4]**

  ThoughtSpot uses replication of stored data. When a node fails, ThoughtSpot continues to operate. See also High Availability and resilience [See page 5].
- **Cluster replacement** **[See page 6]**

  Using a mirrored system architecture, you can replace faulty clusters. This approach enables you to rapidly recover an entire system without data loss.

ThoughtSpot supports recovery from disk or node failure within each appliance. You can also architect your system to support loss of an entire appliance, which is the highest level of disaster recovery.

Disk failure

Summary: ThoughtSpot uses replication of stored data. When a disk goes bad, ThoughtSpot continues to operate.

Replacement of a bad disk should be initiated through ThoughtSpot Support in this event, at your earliest convenience.

Symptoms

You should suspect disk failure if you observe these symptoms:

- Performance degrades significantly.
- You receive alert emails beginning with WARNING or CRITICAL that contain DISK_ERROR in the subject.

If you notice these symptoms, contact ThoughtSpot Support.

Disk replacement

The guidelines for disk replacement are:

- Losing one or two disks: The cluster continues to operate, but you should replace the disk(s) at the earliest convenience.
- Losing more than two disks: The cluster continues to operate, but the application may be inaccessible. Replace the disks to restore original operation.

Disk replacement is done on site by ThoughtSpot Support. Disks can be replaced while ThoughtSpot is running. However the disk replacement procedure involves a node restart, so a disruption of up to five minutes can happen, depending on what services are running on that node.

Node failure

Summary: ThoughtSpot uses replication of stored data. When a node fails, ThoughtSpot continues to operate.

To support high availability, your ThoughtSpot instance must have at least three nodes. In a three or more node system, if one node fails, its services will be distributed to the other nodes. The failover is automatic. However, when a node fails, you should contact ThoughtSpot Support about replacing the node when possible.

A node is considered to have failed when one or more of these conditions occur:

- Two or more disks have failed.
- SSD has failed.
- Memory failure.
- Another hardware component has failed (networking, motherboard, power supplies).

Symptoms

You should suspect node failure if you observe these symptoms:

- Performance degrades significantly.
- You receive alert emails beginning with WARNING or CRITICAL, that describe problems with one of the nodes not running.
- A node does not come up upon booting or rebooting the system.

If you notice these symptoms, contact ThoughtSpot Support.

Node replacement

Node replacement is done on site by ThoughtSpot Support. You must schedule a maintenance window, since some downtime is required. For more information, please contact ThoughtSpot Support.

High Availability (HA) and resilience

Summary: Consider these guidelines to ensure HA of ThoughtSpot app, and node resilience.

Requirements for node resilience

- The cluster must have at least 3 nodes.
- The cluster must have spare capacity; if one node fails, the remaining nodes must be able to host and serve all loaded data.

What happens during node failure

- When a node loses connection with the main service manager process, it becomes **unhealthy**.
- ThoughtSpot migrates all migratable services that run on the failed node to other (**healthy**) nodes. For all practical purposes, ThoughtSpot ignores the failed node until it reports itself as **healthy**.
- ThoughtSpot rebalances and redistributes the data served from the failed node onto healthy nodes. Healthy nodes read the data from the the HDFS storage layer into the in-memory database processes.

Disruption: impact on users

The process of redistributing and loading the data in the affected tables on HDFS layer from a failed node to the remaining healthy nodes is not instantaneous. The failover may impact the user experience.

Cluster replacement

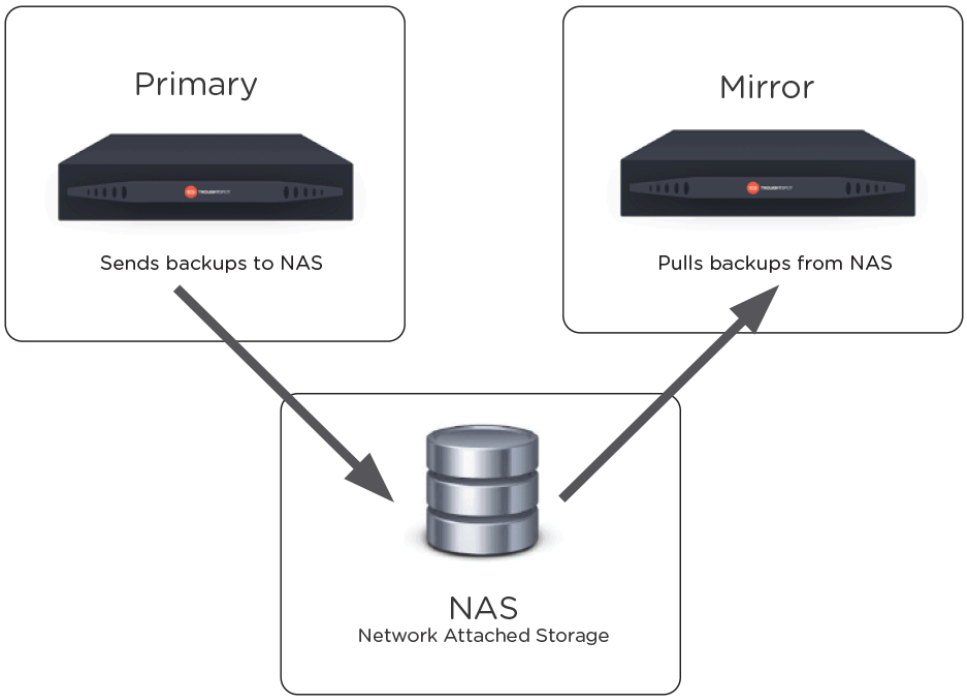
Summary: Cluster replacement can be achieved using a mirrored system architecture. This allows you to recover an entire system very quickly without data loss.

You have the option of architecting your system for fast recovery from a disaster in which you lose an entire ThoughtSpot instance. This involves running two ThoughtSpot appliances in a mirrored configuration. This configuration is used in mission critical systems or for business processes in which ThoughtSpot data has been operationalized.

The two ThoughtSpot instances are called:

- Primary: The production ThoughtSpot instance.
- Mirror: A standby instance that can be placed into service in the event that the primary fails.

In this configuration, the primary initiates periodic full backups of itself. It pushes the backups to a shared NAS (network attached storage). The mirror instance pulls the backups from the shared NAS at defined intervals. It uses each new backup to restore itself to match the production cluster.



- **Mount a NAS file system [See page 0]**

  Some operations, like backup/restore and data loading, require you to either read or write large files. You can mount a NAS (network attached storage) file system for these operations.
- **Set up a disaster recovery configuration [See page 10]** Use this procedure to set up a disaster recovery configuration with a primary and a mirror instance. If the primary cluster fails, the mirror cluster can take over its operations after a small manual intervention. The manual procedure makes the mirror instance into the primary.

Configure NAS for backup storage

Summary: You can use network attached storage to support backup/restore and data loading.

Some operations, like backup/restore and data loading, require you to either read or write large files. You can mount a NAS (network attached storage) file system for these operations. Currently, ThoughtSpot does not have an option for direct attached storage. Your NAS storage can use whichever drive format you would like.

This procedure shows you how to mount a NAS file system for storing or accessing large files. The file system will be mounted at the same location on each node in the cluster automatically. When any node is restarted, the file system will be mounted again automatically, if it can be found.

When supplying a directory for writing or reading a backup, you can specify the `mount` point as the directory to use. Likewise, you can stage data there for loading.

Backups are written by the Linux user `admin`. If that user does not have permission to write to the NAS file system, you could write the backups to disk (for example `/export/sdc1`, `/export/sdd1`, `/export/sde1`, or `/export/sdf1`) and then set up a cron job that executes as root user and copies the backup to the NAS device every night, then deletes it from the directory.

Do not send the periodic backups or stage files on `/export/sdb1` since it is a name node. It is used internally by Hadoop Distributed File System (HDFS) and if this drive fills up, it can cause serious problems. Do not allow backups or data files to accumulate on ThoughtSpot. If disk space becomes limited, the system will not function normally.

1. Log in to the Linux shell using SSH.
2. Mount the directory to the file system, by issuing the appropriate command:
    - For an NFS (Network File System) directory:

```
tscli nas mount-nfs
   --server <server_NFS_address>
   --path_on_server <path>
   --mount_point <target>
   --options vers=<version>, sec=<security schem
e>, <OPTIONS>
```

Note: Other command-line options are available to forward to the command (default: `noexec`).

- For a CIFS (Common Internet File System) directory:

```
tscli nas mount-cifs
   --server <server_CIFS_address>
   --path_on_server <path>
   --mount_point <target>
   --username <user>
   --password <password>
   --uid <uid>
   --gid <gid>
   --options <OPTIONS>
```

Note: Other command-line options are available to forward to the `mount.cifs` command (default: `noexec`).

3. Use the mounted file system as you wish, specifying it by referring to its mount point.
4. When you are finished with it, you may optionally unmount the NAS file system:

```
tscli nas unmount --dir <directory>
```

Configure disaster recovery

Summary: Use this procedure to set up a disaster recovery configuration with a primary and a mirror instance.

Disaster recovery setup configures periodic backups from the primary to a shared, mirrored storage volume. If the primary cluster fails, then a secondary cluster can take over its operations after a small manual intervention.

Should the production cluster be destroyed, monitoring and alerting notifies the administrator. The administrator can then make the secondary appliance into the new primary, by starting it and recovering from backups generated by the primary.

This system makes it possible for you to restore the last backed up state from the primary to the secondary sever. If you configure daily backups, any metadata or data loaded/created after the last backup is not included in restore.

Prerequisites

Both primary and secondary appliances must use a shared storage volume. You can use an NAS or Samba volume for your share. If you choose NAS, keep in mind that too slow a volume potentially break backups or significantly slow restore performance. The following are good guidelines for choosing storage:

- Provision a dedicated storage volume for periodic backups.
- Do not use the backup volume for loading data or any other purposes. If backups fill up this storage, other components will suffer.
- To ensure better supportability and continuity in case local hard disks go bad, the shared storage volume should be network based.

Thoughtspot supports shared storage by mounting NFS or CIFS/Samba based volumes. Before you begin, make sure you know if the shared volume is Samba or NAS volume. To find out, use the `telnet` command.

Telnet confirms NFS	Telnet confirms Samba

```
$ telnet,2049
    Trying 192.168.2.216...
    Connected to 192.168.2.2
16.
    Escape character is
'^]'.
```

```
$ telnet,445
    Trying 192.168.2.216...
    Connected to 192.168.2.2
16.
    Escape character is '^]'
```

.

Configure and test your shared volume

Your shared volume should have a minimum of 15GB free and at least 20GB for a full backup. To configure and mount the shared volume on the primary and mirror appliances, complete the following steps:

1. SSH into the primary appliance.
2. Ensure that the primary appliance has a ThoughtSpot cluster up and running.

   The primary appliance contains the cluster you are protecting with the recovery plan.
3. Create a directory to act as your *mount_point*.

   ```
   sudo mkdir <mount_point>
   ```
4. Set the directory owner to `admin`.

   ```
   sudo chown -R admin:admin <mount_point>
   ```
5. Use the `tscli nas` subcommand to create a NAS mount on all of the cluster nodes. Run `tscli nas mount-nfs` or `tscli nas mount-cifs`.

Use the command-line help (`tscli nas -h`) or the documentation to view all the nas subcommand options [See page 0]. Below are some samples to help you:

Example invocations	
Samba share:	`tscli nas mount-cifs --server 192.168.4.216 --path_on_server /bigstore_share --mount_point /mnt --username admin --password sambashare --uid 1001 --gid 1001`
Samba share with Windows AD authentication	`tscli nas mount-cifs --server 172.27.1.75 --path_on_server /elc --mount_point /home/admin/etl/external_datadir --username COMPANYCO/thoughtspot_svc --password 'ts123PDI!' --uid 1001 --gid 1001`
NFS	`tscli nas mount-nfs --server 192.168.4.132 --path_on_server /data/toolchain --mount_point /mnt`

6. Log into the target machine.
7. Ensure that the target machine is running a ThoughtSpot cluster. Note that the clusters on the primary and target machines do not need to be on the same ThoughtSpot version.

   If a cluster is not running on the target machine, contact ThoughtSpot Support [See page 0] to create a cluster.

8. Repeat steps 3-5 on the target machine.

   The target machine and the primary machine should both be accessing the shared volume. The configuration of the mount point should be identical on both machines.

9. Test the configuration by creating a file as the `admin` user.

   ```
   touch <mount_point>/testfile
   ```

10. Return to the primary server and make sure you can edit the file.

    ```
    touch <mount_point>/testfile
    ```

Configure the backup and start the mirror

1. If you haven't already done so, SSH into the primary server.
2. Use the `tscli backup-policy create` command.

   The command opens a `vi` editor for you to configure the backup policy. Make sure your policy points to the NAS mount in the primary appliance.

   When choosing times and frequencies for periodic backups, you should choose a reasonable frequency. Do not schedule backups too close together, since a backup cannot start when another backup is still running. Avoid backing up when the system is experiencing a heavy load, such as peak usage or a large data load.

   If you are unfamiliar with the policy format, see Configure periodic backups [See page 0].
3. Write and save the file to store your configuration.

   By default, newly created policies are automatically enabled.
4. Verify the policy using the `tscli backup periodic-config <name>` command.

   Use the `<name>` from the policy you created in the previous step.
5. SSH into the secondary recovery appliance.
6. Use the `tscli dr-mirror` subcommand to start the mirror cluster.

   ```
   tscli dr-mirror start
   ```
7. Verify that the cluster has started running in mirror mode

```
tscli dr-mirror status
```

It may take some time for the cluster to begin acting as a mirror.

Recovery operations

If the primary cluster fails, the secondary cluster can take over its operations after a small manual intervention. The manual procedure makes the secondary instance into the primary.

> ❗ **Warning:** You should perform this procedure under the supervision of ThoughtSpot customer support.

1. Contact ThoughtSpot customer support.
2. If the primary ThoughtSpot cluster is still running, stop it and disconnect it from the network.
3. SSH into the secondary cluster.
4. Stop the mirror cluster.

```
tscli dr-mirror stop
```

5. Verify the mirror has stopped.

```
tscli dr-mirror status
```

6. Start the new primary cluster.

```
tscli cluster start
```

7. Deploy a new mirror.
8. Set up a backup policy on your new primary cluster.