Preparing for failures in the Splunk utility tier

Splunk provides product features to increase availability and recovery options for the search tier (search head clustering) and the indexing tier (indexer clusters and index replication). Administrative functions, such as the deployment server, deployer, and licensing server, rely on best practices to provide their resiliency. This article refers to those functions as the utility tier, and outlines the best practices to ensure their recoverability.

Audience

- Architect
- Engineer

For more about these roles, see Setting Roles & Responsibilities.

Impact of failures on the utility tier

The components of the Splunk utility tier are used for Splunk administration. If any of these components are unavailable or destroyed, the respective functions and resources become unavailable. Note this does not include search heads, indexers, nor forwarders.

<table>
<thead>
<tr>
<th>Component</th>
<th>Impact if offline</th>
<th>Impact if destroyed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment server</td>
<td>No impact to search and indexing functions</td>
<td>Source of truth of environment's configuration destroyed</td>
</tr>
<tr>
<td>Deployer</td>
<td>No impact to search and indexing functions</td>
<td>Default configuration for search head cluster is lost, but can be mostly rebuilt from a SHC member</td>
</tr>
<tr>
<td>Master node</td>
<td>No data redundancy requirements</td>
<td>Default configuration for indexer cluster member is lost, but can be mostly rebuilt from a member</td>
</tr>
<tr>
<td>License server</td>
<td>No impact to indexing functions 72 concurrent hours shuts down search functions See About the</td>
<td>System would need to be rebuilt. No impact to end users if the rebuild happens within 72 hours</td>
</tr>
</tbody>
</table>

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
<table>
<thead>
<tr>
<th>Component</th>
<th>Impact if offline</th>
<th>Impact if destroyed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>connection between the license master and license slaves in the &quot;Splunk Enterprise Admin Manual&quot; for more information.</td>
<td>System would need to be rebuilt. Risk to operations if health and performance visibility and monitoring for search and indexing functions is offline for a long period. Built-in summary data showing insights and long term patterns would be lost. No lasting impact to end users or the overall Splunk platform.</td>
</tr>
<tr>
<td>Monitoring console</td>
<td>No impact to search and indexing functions. Lost health and performance visibility and monitoring for search and indexing functions.</td>
<td></td>
</tr>
</tbody>
</table>

If any of these components are destroyed, it requires effort to rebuild a new instance and update references to the new host's information throughout the environment. You can mitigate these laborious and error-prone efforts by applying best practices.

**Preserve component’s state**

Many customers use virtual machines instead of bare-metal hardware for utility-tier components because virtual machines provide two features that are valuable for utility-tier components:

**Dynamic resource sizing**

- VMs change the hardware specifications of the host as load increases.

**State preservation and transition**

- VMs provide host snapshots that preserve an image of the instance. Some VMs, such as VMotion from VMWare, enable you to instantiate the host image on a new virtual machine.

If you are unable to leverage these benefits from virtual machines, consider putting a configuration backup plan in place. For more information about configuration backups, see *Managing Backup and Response Processes*.

**Preserve networking using DNS entries**

When a utility instance fails or is destroyed, the administrative task to update networking details to all clients, such as host name and IP, can be impractical in large and distributed data center environments. You may be able to avoid that labor by rebuilding a utility component with the same networking details the previous one used used, but this is usually not possible. A best practice is to use DNS CName (canonical name) records as a translation service.
When you establish DNS CNames for your utility instances, you can direct all clients to those DNS entries, and thus never need to rely on the true host and IP of the host hardware. If you have to replace the host hardware, you do not have to try to reuse the same hostname and IP. This also enables you to build new utility instances in parallel to the old with a simple DNS toggle as a cutover.

Applications for load balancing

You can use a similar practice for load balancing on the data collection tier or search tier. In such scenarios, a DNS A record distributes traffic to multiple hosts, which provides you an easy way to scale. Even if you have a single instance acting as your search head or data collection tier, you can use this kind of networking for scalability and easy management.

For load balancing the indexing tier, however, Splunk's native load balancing feature is the best practice for forwarding data to indexers. For more information, see Set up load balancing in the Splunk Enterprise Forwarding Data Manual.

Next steps

Partner with someone who oversees networking at your organization and make sure they understand the goal and the technical details. Draft the disaster recovery plan and verify it with a non-impacting/non-production environment before implementing it in production.