Managing backup and restore processes

Get expert guidelines for establishing a Splunk backup and restore policy to ensure system continuity in case of a failure, outage, or mistake.

Part of a successful Splunk implementation is establishing regular backups. You'll need to identify backup and restore points, and make regular backups of your Splunk configuration files to ensure system continuity in case of a failure, outage, or mistake.

Audience

- Engineer
- Architect

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

Splunk backup policy best practices

The $SPLUNK_HOME/etc/ directory and its subdirectories contain all the settings for your Splunk installation and all apps, including saved searches, user accounts, tags, custom source type names, and other configuration information.

Back up to a separate location

Backing up to a separate location is a best practice for resiliency. Backing up to a different disk or mount than Splunk is installed on can reduce single points of failure.

Back up single points of failure

Back up any single points of failure, such as a single indexer, single instance deployment, and single search head, and utility tier resources, such as the deployment server, deployer, master node, license server.

Back up at least one search head cluster (SHC) member periodically

As a best practice, periodically back up the SHC state to ensure you can restore knowledge objects in their current state in case of a catastrophic failure. For details about what to back up on the SHC and how, see Back up and restore search head cluster settings in the Splunk Enterprise Distributed Search manual.

Implement some form of version control

Having some way of preserving state between versions is a best practice so you can roll back in case of an error.
• Standard. Scripted input that kicks off a specific diagnostic (or just an `$SPLUNK_HOME/etc/` directory) and cleans old copies to prevent filling up the file system. See Generate a diagnostic file in the Splunk Troubleshooting manual.

• Intermediate. Scripted input that checks into a source control system, such as Git.

• Advanced. A custom solution using source control that provides managed restoration.

More resources

• For your Unix environment, see the app Stateful Snapshot for Splunk on Splunkbase.

• For more about configuration files, see Backup configuration information in the Splunk Enterprise Admin Manual.

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.