Splunk® Enterprise Securing Splunk Enterprise 7.0.1

How to secure and harden your Splunk software installation

Generated: 12/13/2019 9:52 am
How to secure and harden your Splunk software installation

Use this topic as a checklist and a roadmap for this manual to help you take all of the steps necessary to secure your Splunk software configuration and protect your data.

Set up authenticated users and manage user access

- Secure your Admin password and use it only for administration tasks.
- Use Access Control Lists to restrict user access.
- Set up users and configure Roles and capabilities to control user access.
- Configure user authentication with one of the following methods:
  ♦ Splunk's own built-in system, described in Set up user authentication with Splunk's built-in system.
  ♦ LDAP, described in Set up user authentication with LDAP.
  ♦ A scripted authentication API for use with an external authentication system, such as PAM or RADIUS, described in Set up user authentication with external systems.
- Use one of the following to to create secure one-step login for users:
  ♦ Single Sign on with SAML
  ♦ Multi-factor authentication
  ♦ ProxySSO
  ♦ Reverse-proxy SSO with Apache

Use certificates and encryption to secure communications for your Splunk software configuration

Splunk software comes with a set of default certificates and keys that demonstrate encryption. Splunk recommends deploying your own certificates and configuring them to secure communications. See About securing Splunk with SSL in this manual.

Harden your Splunk software instances to reduce vulnerability and risk

- Secure your indexer clusters and search head clusters.
- Set passwords across multiple servers to ensure consistent authentication.
• Secure your service accounts.

• Harden your KV store port.

**Audit your system regularly**

Audit events contain information that shows you what changed in your Splunk configuration. It gives you the where and when, as well as the identity of the actor who implemented the change. Leveraging audit events provides better security and other benefits:

• Audit your system regularly to monitor user and admin access, as well as other activities that could tip you off to unsafe practices or security breaches.

• Keep an eye on activities within Splunk (such as searches or configuration changes). You can use this information for compliance reporting, troubleshooting, and attribution during incidence response.

• Audit events are especially useful in distributed Splunk configurations for detecting configuration and access control changes across many Splunk Servers.

  To learn more, see Audit Splunk Enterprise activity in this manual.

• Use the file system-based monitoring available out of the box on most Splunk-supported operating systems.

  For more information about monitoring, see Monitor Files and Directories in the *Getting Data In Manual.*