Securing Splunk® Cheat Sheet V1.0

https://www.aplura.com/cheatsheets

Universal Rules for Securing Splunk

* Change the password for admin
* Run Splunk with the appropriate user account
* Exercise caution when setting permissions for Splunk user
* Disable port 8089/tcp on Universal Forwarders
* Use a host firewall
* Backup `$SPLUNK_HOME/etc/*` on a regular basis
* Replace the default certificates

Use SSL/TLS on:
* Web Interface (443/8443/tcp)
* Deployment Server (8089/tcp) - replace default certs
* Splunk data ports (9997/9998/tcp)
* Splunk-to-Splunk (8089/tcp) - replace default certs

Run Splunk as the `splunk` user

*nix

* $SPLUNK_HOME should be owned by splunk

```
CLI: chown -R splunk:splunk /opt/splunk/
```

* $SPLUNK_HOME/etc/splunk-launch.conf should be owned by root

```
CLI: chown root: $SPLUNK_HOME/etc/splunk-launch.conf
```

Windows

Reset permissions in $SPLUNK_HOME

```
CLI: icacls.exe “Splunk\*” /q /c /t /reset
```

OSX

The DMG install does NOT go into `/opt` by default. Instead, Splunk is installed into `/Applications/`. The DMG install also does not create a splunk user.

Universal Forwarders - Remove Default Bindings

Splunk binds to all available network interfaces by default on port 8089/tcp. Universal Forwarders are not required to use this port for normal operations. Override the default behavior and configure Splunk to bind to the local loopback address.

server.conf

```
[httpServer]
disableDefaultPort = true

[httpServerListener:127.0.0.1:8089]
ssl = true
```

Windows

Windows

Running Splunk as Local System is preferable to using named account. Only use a domain-based account if there is a well established process for changing service account passwords on a regular basis.

Domain-based accounts will need elevated permissions to utilize some Windows inputs (particularly on Domain Controllers), negating the advantages of a named service account over Local System.

Linux - Create a rule to redirect Splunk Traffic

```
firewalld:
    firewall-cmd --set-default-zone=public
    firewall-cmd --zone=public --add-forward- port=port=443:proto=tcp:toport=8000 —permanent
    firewall-cmd --reload
iptables
    iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT --to-port 8443
Windows
    netsh advfirewall firewall add rule name="Allow Inbound to Splunk Web" dir=in \
    action=allow protocol=TCP localport=443
```

Solaris

Solaris SMF requires a change to the service manifest to add read-all privileges to the splunk user account

```
CLI:
svccfg -s splunkforwarder  setprop start/privileges = astring: \
"basic,net_privaddr,file_dac_read,file_dac_search"
svcadm refresh splunkforwarder
```

Provided by Aplura, LLC. Splunk Consulting and Application Development Services. sales@aplura.com https://www.aplura.com

Many Solutions, One Goal.

SSL(TLS) for Splunk Cheat Sheet

SSL Checklist

1. Create/Procure SSL Certificates
2. Secure the Web UI (port 443/tcp)
3. Secure the indexers (port 9997|9998/tcp)
4. Secure inter-Splunk communications (8089/tcp)

Certificate Checklist

1. Commercial SSL cert or cert from enterprise CA
2. Cert for each Splunk indexer
3. One cert for ALL UFs
4. Cert for inter-Splunk communications

Secure Splunk Web

Create a folder in $SPLUNK_HOME/etc/auth/ for your certs, “mycerts” for example.

web.conf

```
[settings]
serverCert = etc/auth/mycerts/SplunkWeb.pem The file may also contain root and intermediate certificates, if required.
sslVersions = “tls1.2”
```

Secure Splunk Indexer Inputs

inputs.conf

```
[SSL]
serverCert = <path>
sslPassword = <password>
sslVersions = “tls1.2”
requireClientCert = true | false
sslCommonNameToCheck = <commonName1>, ... 'requireClientCert' setting must be set to true.
```

Forwarder Outputs

Note: Use 9997 for non-encrypted traffic and 9998 for encrypted. This will simplify the transition to SSL.

outputs.conf

```
[tcpout:<your SSL output group>]
server = <your_indexer1>:9998, <your_indexer2>:9998
sslPassword = <password>
clientCert = <path> The full path to the client SSL certificate in PEM format.
sslVersions = “tls1.2”
requireClientCert = true | false
sslCommonNameToCheck = <commonName1>, ... 'requireClientCert' setting must be set to true.
```

References

https://wiki.splunk.com/images/f/fb/SplunkTrustApril-SSLipperySlopeRevisited.pdf
http://docs.splunk.com/Documentation/Splunk/latest/Security/AboutsecuringyourSplunkconfigurationwithSSL

Provided by Aplura, LLC. Splunk Consulting and Application Development Services. sales@aplura.com https://www.aplura.com

Many Solutions, One Goal.