Splunk Deployment Server Update Guide

June 2022

Scenario

In response to a vulnerability in the Splunk Deployment Server (DS) used for all Managed SIEM customers, we instructed all customers to power off their Deployment Server whilst we developed a remediation plan.

The nature of the vulnerability requires the software to be updated before the service is made available on the network again. This document will guide you through the steps needed to complete this process.

Notes

The commands provided in this guide have been successfully tested on Red Hat Enterprise Linux, Ubuntu and CentOS installations. Additional or different steps may be required for other operating systems or custom installations.

Commands are shown in a `monospaced font` and must be typed or copied exactly as shown. An account with sudo capabilities is required. The `sudo` prefixes can be removed from commands if you decide to carry out the update as a root user.

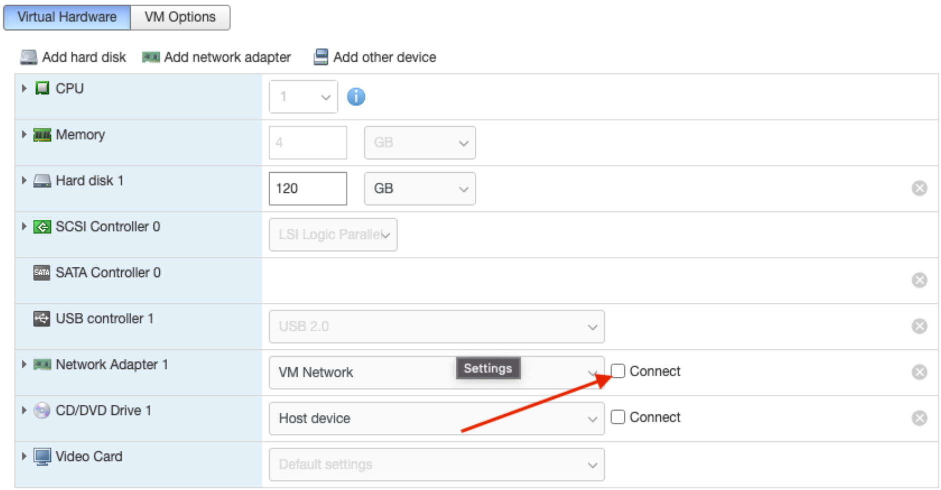
Ensure each step has completed successfully before proceeding to the next.

Screenshots are provided as a guide and may not exactly match your installation.

Disconnect Deployment Server from Network

For a physical machine, disconnect the network cable from the server.

For a virtual machine, disconnect the virtual network adapter in the VM settings. For VMware ESXi, untick the “Connect” box for the network adapter in the VM settings (Figure 1).



CPU	1	
Memory	4 GB	
Hard disk 1	120 GB	
SCSI Controller 0	LSI Logic Parallel	
SATA Controller 0		
USB controller 1	USB 2.0	
Network Adapter 1	VM Network	□ Connect
CD/DVD Drive 1	Host device	□ Connect
Video Card	Default settings	

Figure 1: disconnecting network adapter in VMware ESXi.

Power On the Splunk Deployment Server

Power on the virtual or physical Splunk Deployment Server.

Stop Splunk

Log in locally to the Deployment Server.

Stop Splunk:

```
sudo /opt/splunk/bin/splunk stop
```

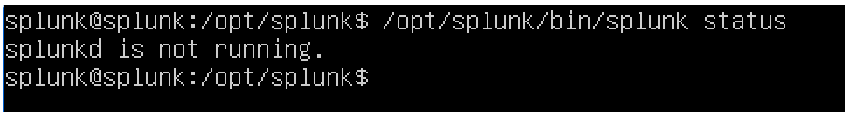
Disable the Splunk service in case reboots are required:

```
sudo /opt/splunk/bin/splunk disable boot-start
```

Check that Splunk is stopped:

```
/opt/splunk/bin/splunk status
```

This should show that “splunkd is not running” (Figure 2).



```
splunk@splunk:/opt/splunk$ /opt/splunk/bin/splunk status
splunkd is not running.
splunk@splunk:/opt/splunk$
```

Figure 2: Splunk is not running.

Connect Deployment Server to Network

With Splunk disabled, the Deployment Server can now be connected to the network. Reconnect either the physical network cable or virtual network adapter.

Optional: Deployment Servers With Restricted External Network Access

The update script automatically downloads the required Splunk installation packages. However, if your Splunk Deployment Server has limited or no Internet access, these packages will need to be downloaded and transferred manually to the Deployment Server.

The steps in this section are not required if your Splunk Deployment Server has HTTPS access to download.splunk.com (for the Splunk installation packages) and raw.githubusercontent.com (for the update script).

The Splunk packages (.tgz files) must not be renamed when downloaded and transferred.

Download the update script:
https://raw.githubusercontent.com/janetuk/Jisc-SIEM/main/jisc_splunk

Transfer the update script to an accessible directory on the Deployment Server (not /opt/splunk or /opt/jisc_splunk).

Download the Splunk v8.2.6 package:
https://download.splunk.com/products/splunk/releases/8.2.6/linux/splunk-8.2.6-a6fe1ee8894b-Linux-x86_64.tgz

Download the Splunk v9.0.0 package:
https://download.splunk.com/products/splunk/releases/9.0.0/linux/splunk-9.0.0-6818ac46f2ec-Linux-x86_64.tgz

Create the update working directory on the Deployment Server:

```
sudo mkdir /opt/jisc_splunk
```

Transfer the Splunk v8.2.6 and v9.0.0 packages to /opt/jisc_splunk on the Deployment Server. Reminder: filenames must not be changed.

End of optional steps.

Update Splunk

If you have not followed the optional steps listed above, additional network changes, e.g. firewall settings, may be needed to allow the update script and Splunk packages to be downloaded directly to your Splunk Deployment Server. This is specific to your network and is beyond the scope of this guide.

On the Deployment Server, download the update script to an accessible directory (not /opt/splunk) (not required if already manually transferred to the server):

```
wget https://raw.githubusercontent.com/janetuk/Jisc-
SIEM/main/jisc_splunk
```

Make the update script executable:

```
chmod 755 jisc_splunk
```

Disable Splunk Deployment Server:

```
sudo ./jisc_splunk --splunk disable_deployment_server
```

Important: Splunk must be upgraded to v8.2.6 before it can be upgraded to v9.0.0.

Upgrade Splunk to v8.2.6 (answer **y** to agree with license when prompted):

```
sudo ./jisc_splunk --target 8.2.6 --cmd upgrade,deploy
```

Upgrade from Splunk v8.2.6 to v9.0.0 (answer **y** to agree with license when prompted, answer **y** to perform migration and upgrade without previewing configuration changes if prompted):

```
sudo ./jisc_splunk --target 9.0.0 --cmd upgrade,deploy
```

Enable Deployment Server:

```
sudo ./jisc_splunk --splunk enable_deployment_server
```

Restart Splunk:

```
sudo /opt/splunk/bin/splunk restart
```

Check Splunk

Check that Splunk is running:

```
/opt/splunk/bin/splunk status
```

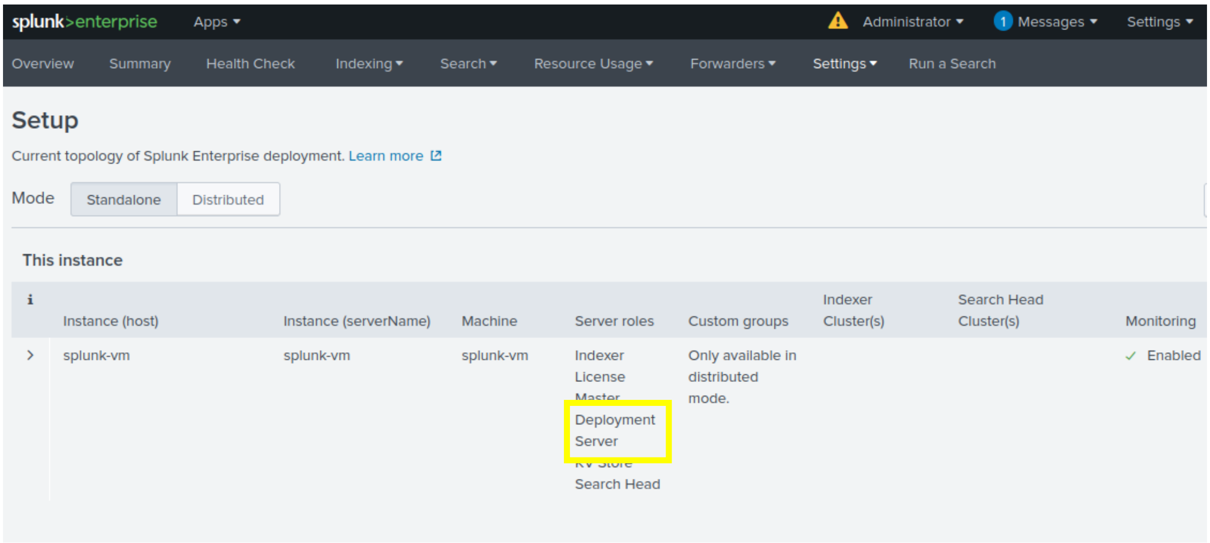
Check that Splunk has been upgraded to v9.0.0:

```
/opt/splunk/bin/splunk version
```

Login to the Deployment Server's Splunk web interface.

Navigate to Settings → Monitoring Console → Settings → General Setup.

Check that the Deployment Server role is listed (Figure 3).



Setup

Current topology of Splunk Enterprise deployment. Learn more

This instance

i	Instance (host)	Instance (serverName)	Machine	Server roles	Custom groups	Indexer Cluster(s)	Search Head Cluster(s)	Monitoring
>	splunk-vm	splunk-vm	splunk-vm	Indexer License Master Deployment Server KV Store Search Head	Only available in distributed mode.			✓ Enabled

Figure 3: Splunk web interface with Deployment Server enabled.

Final Steps

Once you are happy that the updated Deployment Server is running correctly, you can remove the temporary update files and delete the working directory:

```
sudo ./jisc_splunk --cmd clean
```

Delete the update script if no longer needed:

```
rm jisc_splunk
```

This completes the update process. Your Deployment Server is now running Splunk v9.0.0 with boot start enabled.

Please notify Jisc that you have completed the update so that we can ensure data is being received correctly from your Deployment Server.

End of update guide.