Deploying Splunk Enterprise

Script File

- deploy_splunk_enterprise.sh

Script Parameters

- SPLUNK_PARENT_FOLDER (-p)
  - Where Splunk will be deployed under.
  - Example: **/opt**
- SPLUNK_SERVER_NAME (-h)
  - The host name what will be used by Splunk and mapped to DNS service
  - Example: **sh01**
- UPDATE_DNS (-d)
  - Whether to execute the DNS update script as part of initial deployment
  - Example: **true**
- SLIM_DOWN (-s)
  - Whether to reduce the size of the default shipped indexes to fit within AWS t2.micro instance default storage of 8GiB
  - Splunk will not function with doing this step
  - Example: **true**
- SPLUNK_SERVER_VERSION (-v)
  - It is important to determine what version of Splunk that is required.
  - Example: **8.1.2**
- SPLUNK_SERVER_BUILD (-b)
  - It is important to determine what build of Splunk that is required.
  - Example: **545206cc9f70**
- CREATE_DNS_CRON_JOB (-c)
  - Whether to create a CRON job to run the DNS update script every 5 minutes
  - Example: **true**

Example Usage:

sudo bash deploy_splunk_enterprise.sh -p /opt -h sh01 -v 8.1.2 -b 545206cc9f70 -c true -d true -s true

Deploying Splunk Universal Forwarder

Script File

- deploy_splunk_forwarder.sh

Script Parameters

- SPLUNK_PARENT_FOLDER (-p)
  - Where Splunk will be deployed under.
  - Example: **/opt**
- SPLUNK_SERVER_NAME (-h)
  - The host name what will be used by Splunk and mapped to DNS service
  - Example: **sh01**
- UPDATE_DNS (-d)
  - Whether to execute the DNS update script as part of initial deployment
  - Example: **true**
- SPLUNK_SERVER_VERSION (-v)
  - It is important to determine what version of Splunk that is required.
  - Example: **8.1.2**
- SPLUNK_SERVER_BUILD (-b)
  - It is important to determine what build of Splunk that is required.
  - Example: **545206cc9f70**
- CREATE_DNS_CRON_JOB (-c)
  - Whether to create a CRON job to run the DNS update script every 5 minutes
  - Example: **true**

Example Usage:

sudo bash deploy_splunk_forwarder.sh -p /opt -h sh01 -v 8.1.2 -b 545206cc9f70 -c true -d true -s true

Creating and Deploying Splunk Base Apps

Script File

- create_splunk_base_apps.sh

Script Parameters

- SPLUNK_PARENT_FOLDER (-p)
  - Where Splunk will be deployed under.
  - Example: **/opt**
- COPY_BASE_APPS (-C)
  - Whether to copy the base apps or just create them
  - Example: **true**
- INDEXER_SERVER_LIST (-i)
  - List of indexers available
  - Not looking at indexer discovery currently. Good learning opportunity to add.
  - Example: **idx01-int.bsides.dns.splunkstudy.club:9997, idx02-int.bsides.dns.splunkstudy.club:9997**
- DEPLOYMENT_SERVER (-d)
  - Location of deployment server if used
  - Example: **ds01-int.bsides.dns.splunkstudy.club:8089**
- SPLUNK_OS_USERNAME (-u)
  - The non-root user account that Splunk will run under
  - Not best practice but the ssh user account could be used (e.g. ubuntu)
  - Example: **splunk**
- SPLUNK_OS_USERGROUP (-g)
  - The group that the splunk account belongs to
  - Not best practice but the ssh user account group could be used (e.g. ubuntu)
  - Example: **splunk**
- BASE_APPS_LIST (-z)
  - The list of apps being requested.
  - The script caters for two simple base apps. [deployment_client_app and forwarder_outputs_app]
  - Example **deployment_client_app, forwarder_outputs_app**
- SPLUNK_DEPLOYMENT_ROLE (-r)
  - User to determine the folder to place apps in
  - /etc/apps for a deployment client and etc/deployment-apps for a deployment server
  - Example: either **deploymentclient** or **deploymentserver**

Example Usage:

sudo bash create_splunk_base_apps.sh -p /opt -c true -i "idx01-int.bsides.dns.splunkstudy.club:9997" -d "ds01-int.bsides.dns.splunkstudy.club:8089" -u ubuntu -g ubuntu -z "deployment_client_app,forwarder_outputs_app" -r deploymentclient

Updating DNS records

Script File

- update_splunk_dns.sh

Script Parameters

- DNS_LOG_FILE (-l)
  - The file to be appended to with logs from the script execution
  - Example: **/home/ubuntu/update_splunk_dns.log**

Example Usage:

sudo bash update_splunk_dns.sh /home/ubuntu/update_splunk_dns.log