Splunk Enterprise Deployment Practical Lab

Objective

Configure a distributed Splunk environment, demonstrating your understanding of the concepts and best practices for managing enterprise environments. Note that you should use Splunk best practices in your deployment.

Machines

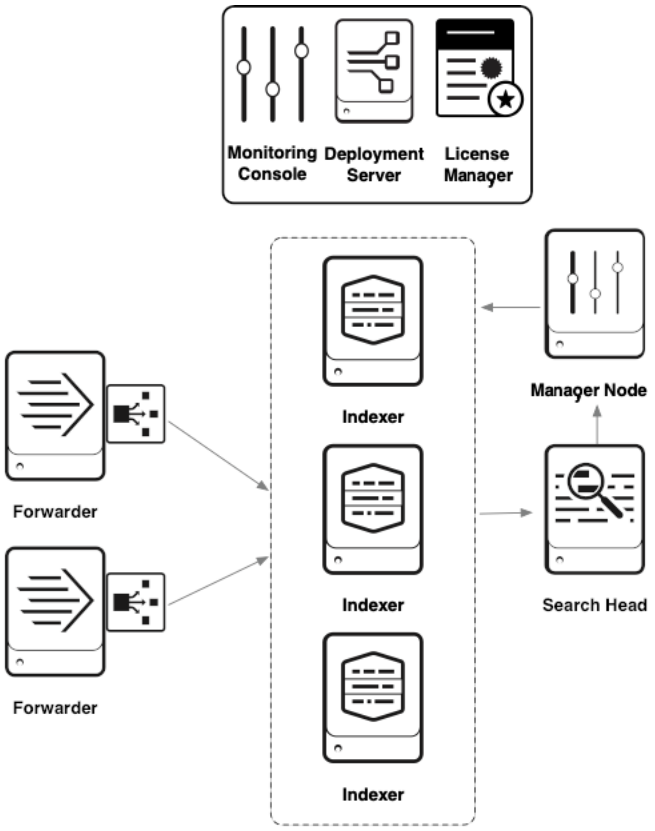
You have access to eight Linux 64-bit machines. These machines are running an AWS version of CentOS Linux. Your instructor will give you login information and IP addresses for each server.

You must use the **Internal IP** addresses in your configuration files, wherever IP addresses are needed. The internal IP addresses exist within a private network, which allows your servers to communicate with each other. In the diagram below, all communication between the servers occurs on the private network, using the internal IP addresses.

The **external IP** addresses allow you to access your servers via the command line or user interface. The external IPs allow you to login or browse to your servers via the public internet.

If you have questions about which IP address to use in any situation, ask your instructor.

Topology Example



splunk>

Phase 1 – Installation

Overview

Install and configure the Splunk deployment on the provided Linux 64-bit machines.

Please use the account designated by your instructor: *archStudent*. Do not create or use any other accounts on the machines. The archStudent account has `root` privileges on all machines; you may use the `sudo` command. You will need to change the default permissions for some directories if you want non-`root` accounts to access them. You may also need to create additional directories to complete the lab. If you are not sure, don't take any risk with the environment.

Use *only* the password specified for Splunk accounts. For all installation tasks, download a supported release of the installation files for Linux 64-bit Splunk Enterprise (or Splunk Universal Forwarder) from http://www.splunk.com/download. If you are unclear about which password to use, ask your instructor.

We suggest that you use the install files with the `.tgz` extension. All of the servers have **wget** installed, so you can use the `wget` command that is provided on the Splunk download success page.

For every task, keep in mind and use, where applicable, Splunk best practices.

Tasks

A. Install the Deployment Server / License Manager / Monitoring Console

1. On the Deployment Server / License Manager / Monitoring Console machine, create the Splunk home directory:
   ```
   sudo mkdir /opt/splunk
   sudo chown archStudent /opt/splunk
   ```
2. Install Splunk in: `/opt/splunk`
   ```
   tar -xzvC /opt/ -f {splunk_file_downloaded_using_wget}
   ```
3. Assign a unique Splunk server name for both internal communications and data to this instance that includes your name and purpose of the instance (i.e., `SMITH-LICENSE`).
4. Configure Splunk using best practices and designate this instance as a license manager. Download the big license from https://splk.it/edu-lab-licenses (password: **open.sesam3**).

B. Install the forwarders

5. Install universal forwarders on the forwarder machines in: `/opt/splunkforwarder`

C. Install the Indexers Cluster for High Availability and Redundancy

6. Install Splunk on the Manager Node and each of the indexer machines in: `/opt/splunk`

   Download the installation files for Linux 64-bit Splunk to each instance. Again, **wget** is available for your use.
7. Assign unique Splunk server names for both internal communication and data to each instance that includes your name and purpose of the instance (i.e., `SMITH-INDEX1`, `SMITH-INDEX2`).

8. Configure the indexer cluster with a replication factor of 2 and search factor of 2.

9. Configure the indexer cluster for three replicated indexes: **`soc`**, **`bcgames`**, and **`infra`**.

D. Install the Search Head

10. Install Splunk on the Search Head machine in: `/opt/splunk`
11. Assign a unique Splunk server name for both internal communication and data to this instance that includes your last name and purpose of the instance (i.e., `SMITH-SEARCH`).
12. Configure the Search Head to search the indexer cluster. Use the internal IP addresses to refer to the indexers.

E. Forward internal logs to the Indexers

13. Configure Search Head Forwarding for the Search Head, DS/LM/MC, and Cluster Manager Splunk instances.

F. Configure the Monitoring Console

14. Configure the Monitoring Console (MC) on the DS/LM/MC instance to monitor the ***entire*** environment.

Phase 2 – Configure Data Inputs and Fields

A. Configure and deploy the data inputs

NOTE: You must use the Deployment Server to deploy apps for all data inputs.

Forwarder 1

1. Deploy the 'Splunk Add-On for Unix and Linux', to monitor all files in `/var/log` and send them to the **`soc`** index.
2. Monitor `access.log` from all three `www*` directories (`/opt/log/www*`) and send them to the **`infra`** index. The host value for these events should be derived from the third directory segment in the pathname (for example, `www1`).

Forwarder 2

3. Monitor `dreamcrusher.xml` from `/opt/log/crashlog` and send it to the **`bcgames`** index.
4. Monitor `cisco_ironport_web.log` from `/opt/log/cisco_router1` and send it to the **`infra`** index.
5. Monitor `cisco_ironport_mail.log from /opt/log/cisco_router1` and send it to the **`infra`** index.

Confirmation

6. From the Search Head, confirm the index-time parsing for all data sources: timestamp, line-breaking, host, source, sourcetype. As you test your inputs, any incorrectly parsed data must be removed from the indexes.

B. Create field extractions

7. Make sure the following fields are being extracted for the `/var/log/secure` file:
   - user
   - src_ip
8. Create the following search-time field extractions for `cisco_ironport_web.log`:
   - user (example: `doc@demo.com`)
   - domain (example: `www.adventureindonesia.com`)
   - url (example: `http://www.adventureindonesia.com/images/komodo/komodo.jpg`)
9. Create the following search-time field extractions for `cisco_ironport_mail.log` (field values should all be numeric):
   - mid
   - icid
   - dcid
10. Create the following search-time field extractions for `dreamcrusher.xml`:
    - Infiltrators
    - AttackVessel

Phase 3 – Reporting

In this phase, you will create reports and dashboards. The dashboard names will be Soc, Infra, and Game Activity. The dashboard panels are to be powered by the reports.

A. Create the following report and add to the SOC dashboard

1. For the /var/log/`secure` input, display a count of failed logins in the last 60 minutes by `user` and `src_ip`.
   Name the panel: **Failed Logins by User – Last 60 minutes**

B. Create the following reports and add to the INFRA dashboard

2. For `access.log`, display a count of web server errors in the last 24 hours by status code and host.
   Name the panel: **Web Server Errors – Last 24 hours**
3. For `cisco_ironport_web.log`, list all events in the last 24 hours that contained either `.exe` or `.bat`.
   Name the panel: **Suspect Events Summary – Last 24 hours**

4. For `cisco_ironport_web.log`, count the number of suspect events from the above search for each user and present it in a table.
   Name the panel: **Suspect Events Summary by User – Last 24 hours**
5. For `cisco_ironport_mail.log`, group events correlated with common values for the mid, `dcid`, and `icid` fields, then search for the term REJECT.
   Name the panel: **Rejected Email Transactions – Last 24 hours**

C. Create the following report and add to the GAME ACTIVITY dashboard

6. For `dreamcrusher.xml`, calculate (sum) the total number of `Infiltrators` for each `AttackVessel`.
   Name the panel: **AttackVessel usage - All Time**

D. Check your environment

7. Ensure the deployment is ready for production, only the required data is indexed and correctly parsed, test the automation and high availability.

Wrap-up

A. Create a diag for each server

On each of your instances:

1. Run the `./splunk diag` command. This will place the diag file in the `SPLUNK_HOME` directory.
2. Rename each diag file with: `YOURNAME-InstanceType.tar.gz`
3. Move the diag to your home directory: `/home/archStudent`

Inform the customer/instructor about the end of your mission, including any pertinent information

4. A customer could not guess the splunk usernames, passwords, secrets
5. If some tasks could not be achieved, name them. It's better than letting the customer finding out there is no redundancy or not auto start.