

Transitioning to Splunk Cloud 8.2

1. Splunk Cloud

- Describe Cloud SaaS benefits and features
- Identify Splunk Cloud administrator managed tasks
- Explain the differences between Splunk Enterprise on premise and Splunk Enterprise Cloud

2. User Authentication and Authorization

- Identify Splunk Cloud authentication options
- Add Splunk users using native authentication
- Integrate Splunk with LDAP, Active Directory or SAML
- Understanding Splunk authorization options

3. Index Management and Data Retention

- Understand cloud indexing strategy
- Create indexes in cloud
- Manage data retention and archiving
- Monitor indexing activities

4. Cloud Ingestion - Using forwarders

- Review cloud ingestion strategies
- Understand the role of forwarders in GDI
- Configure forwarding to Splunk Cloud
- Monitoring forwarder connectivity
- Explore optional forwarder settings

5. Cloud Ingestion - Using API, Scripted and HEC Inputs

- Understand how data is ingested using API
- Describe how to use HEC for ingestion
- Know how to deploy scripted inputs

6. Cloud Ingestion - Application Based Inputs

- Understand how inputs are managed using in apps or add-ons
- Describe how customers may use Splunk Stream app
- Deploy Cloud inputs for use on an IDM

7. Installing and Managing Apps

- Understand how apps and add-ons are vetted and installed in Cloud
- Create apps to manage and distribute configurations

8. GDI Performance Considerations

- Understand how event parsing and processing may impact performance
- Use Data Preview to validate and address event creation issues
- Explain how data transformation are defined and invoked

9. Splunk Cloud Support and Troubleshooting

- Troubleshooting Splunk deployments
- Collecting data and use diagnostics or monitoring to investigate
- Overview of how to collect the relevant data for support to troubleshoot