Enterprise Computing Solutions - Education Services

OFERTA FORMATIVA

Detalles de contacto

Avda Europa 21, 28108 Alcobendas

Email: formacion.ecs.es@arrow.com
Phone: +34 91 761 21 51

Splunk 9.0 Cloud Administration

CÓDIGO:	DURACIÓN:	Precio:
SPL_S9CA	32 Hours (4 días)	A consultar

Description

This 18-hour Instructor led course is for administrators new to Splunk Cloud and those wanting to become more experienced in managingSplunk Cloud instances.
The course provides administrators with the opportunity to gain the skills, knowledge and best practices for data management and system configuration for data collection and ingestion required in a Splunk Cloud environment to create a productive Splunk SaaS deployment.
The hands-on labs provide the opportunity to learn and ask questions on how to manage and maintain the platform, the users and how to effectively get data into Splunk Cloud. Modules include data inputs and forwarder configuration, data management, user accounts, and basic monitoring and problem isolation.
Note: Splunk Cloud Administration and Transitioning to Splunk Cloud SHOULD NOT be taken together as both are designed to develop Splunk Cloud specific skills and as such there is some overlap.

Objetivos

Course Topics
▪ Splunk Cloud overview
▪ Managing user authentication and authorization in Splunk
▪ Managing Splunk indexes
▪ Using Splunk configuration files
▪ Configuring and managing Splunk forwarders
▪ Configuring inputs to Cloud, including files and directories from forwarders, API, Scripted, HEC and Application based inputs
▪ Exploring the parsing phase and data preview
▪ Manipulating raw data
▪ Installing and managing applications
▪ Problem isolation and working with Splunk Cloud support

Requisitos Previos

To be successful, students should have a working knowledge of the
topics covered in the following courses:

- What is Splunk?
- Intro to Splunk
- Using Fields
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions

Programa

Module 1 – Splunk Cloud Overview
▪ Describe Splunk Cloud features and topology
▪ Identify Splunk Cloud administrator managed tasks
▪ List the primary Splunk Enterprise on-prem and Splunk Cloud administrator tasks
▪ Explain Splunk Cloud data ingestion strategies
Module 2 – Managing Users
▪ Identify Splunk Cloud authentication options
▪ Add Splunk users using native authentication

▪ Integrate Splunk with LDAP, Active Directory or SAML
▪ Create a custom role
▪ Manage users in Splunk
▪ Use Workload Management to manage user resource usage

Module 3 – Managing Indexes

▪ Understand cloud indexing strategy
▪ Define and create indexes
▪ Manage data retention and archiving
▪ Delete and mask data from an index
▪ Monitor indexing activities

Module 4 – Using Configuration Files

▪ Describe Splunk configuration directory structure
▪ Describe the configuration layering process with index and search time precedence
▪ Use Splunk tools to examine configuration settings such as btool

Module 5 – Configuring Forwarders

▪ List Splunk forwarder types
▪ Understand the role of forwarders
▪ Configure a forwarder to send data to Splunk Cloud
▪ Test the forwarder connection
▪ Describe optional forwarder settings

Module 6 – Managing Forwarders

▪ Describe Splunk Deployment Server (DS)
▪ Manage forwarders using deployment apps
▪ Configure deployment clients and client groups
▪ Monitor forwarder management activities

Module 7 – Forwarder Inputs

▪ Describe the Splunk process for inputting data
▪ Creating network inputs
▪ Create file and directory monitor inputs
▪ Use optional settings for monitor inputs

Module 8 –API, Scripted and HEC Inputs

▪ Create REST API inputs
▪ Create a basic scripted input
▪ Identify Linux-specific inputs
▪ Identify Windows-specific inputs
▪ Create Splunk HTTP Event Collector (HEC) agentless inputs

Module 9 – Application Based Inputs

▪ Understand how inputs are managed using apps or add-ons
▪ Explore Cloud inputs using Splunk Connect for Syslog, Data Manager, Inputs Data Manager (IDM), Splunk Edge Processor, and Splunk Edge Hub

Module 10 – Fine-tuning Inputs

▪ Describe the default processing that occurs during the input phase
▪ Configure input phase options, such as source type fine-tuning and character set encoding
▪ Reset file check pointers on a forwarder using the btprobe command

Module 11 – Parsing Phase and Data Preview

▪ Describe the default processing that occurs during parsing
▪ Optimize and configure event line breaking
▪ Modify how timestamps and time zones are extracted or assigned to events
▪ Use Data Preview to validate event creation during the parsing phase

Module 12 – Manipulating Raw Data

▪ Explore Splunk transformation methods
▪ Mask data with SEDCMD and TRANSFORMS
▪ Override sourcetype or host based upon event values
▪ Create rulesets with Ingest Actions
▪ Mask data with Ingest Action rules

Module 13 – Installing and Managing Apps

▪ Review the process for installing apps
▪ Define the purpose of private apps
▪ Upload private apps
▪ Describe how apps are managed

Module 14 – Managing Splunk Cloud

▪ Describe Splunk connected experience apps such as Splunk Secure Gateway
▪ Monitor and manage resource utilization by business units and users using Splunk App for Chargeback
▪ Perform self-service administrative tasks in Splunk Cloud using the Admin Config Service

Module 15 – Supporting Splunk Cloud

▪ Know how to isolate problems before contacting Splunk Cloud Support
▪ Use Isolation Troubleshooting

▪ Define the process for engaging Splunk Support
▪ Improve Mean Time to Resolution (MTTR) by using clear communication, diagnostic tools, monitoring and the CMC Appendix
▪ Explore Splunk security fundamentals

Fechas Programadas

A petición. Gracias por contactarnos.

Información Adicional

Esta formación también está disponible en modalidad presencial. Por favor contáctenos para más información.