



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

CÓDIGO:	DURACIÓN:	Precio:
SPL_ADM-FT	32 Hours (4 días)	A consultar

Description

This course is designed for :

- System administrators who are responsible for managing the Splunk Enterprise environment. The course provides the fundamental knowledge of Splunk license manager, indexers and search heads. It covers configuration, management, and monitoring core Splunk Enterprise components.
- Administrators who are responsible for getting data into Splunk Indexers. The course provides the fundamental knowledge of Splunk forwarders and methods to get remote data into Splunk indexers. It covers installation, configuration, management, monitoring, and troubleshooting of Splunk forwarders and Splunk Deployment Server components.

Objetivos

- Splunk Deployment Overview
- License Management
- Splunk Configuration Files
- Splunk Apps
- Index Management
- Users, Roles, and Authentication
- Basic Forwarding
- Distributed Search
- Understand source types
- Manage and deploy forwarders
- Configure data inputs
- File monitors
- Network inputs (TCP/UDP)
- Scripted inputs
- HTTP inputs (via the HTTP Event Collector)
- Customize the input phase parsing process
- Define transformations to modify data before indexing
- Define search time knowledge object configurations

Requisitos Previos

To be successful, students should have a solid understanding of either the following courses:

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

Or the following course : Splunk Power User Fast start

Programa

A) SYSTEM ADMINISTRATOR Module 1 – Deploying Splunk

- Provide an overview of Splunk
- Identify Splunk Enterprise components
- Identify the types of Splunk deployments
- List the steps to install Splunk
- Use Splunk CLI commands
- Explore security best practices

Module 2 – Monitoring Splunk

- Use Splunk Health Report
- Enable the Monitoring Console (MC)
- Use Splunk Assist • Use Splunk Diag

Module 3 – Licensing Splunk

- Identify Splunk license types
- Describe license violations
- Add and remove licenses

Module 4 – Using Configuration Files

- Describe Splunk configuration directory structure
- Understand configuration layering process Use btool to examine configuration settings

Module 5 – Using Apps

- Describe Splunk apps and add-ons
- Install an app on a Splunk instance
- Manage app accessibility and permissions

Module 6 – Creating Indexes

- Learn how Splunk indexes function
- Identify the types of index buckets
- Add and work with indexes
- Overview of metrics index

Module 7 – Managing Index

- Review Splunk Index Management basics
- Identify data retention recommendations
- Identify backup recommendations
- Move and delete index data
- Describe the use of the Fishbucket
- Restore a frozen bucket

Module 8 – Managing Users

- Add Splunk users using native authentication
- Describe user roles in Splunk
- Create a custom role
- Manage users in Splunk

Module 9 – Configuring Basic Forwarding

- Identify forwarder configuration steps
- Configure a Universal Forwarder
- Understand the Deployment Server

Module 10 – Configuring Distributed Search

- Describe how distributed search works
- Define the roles of the search head and search peers

B) DATA ADMINISTRATION Module 1 – Getting Data Into Splunk

- Provide an overview of Splunk

- Describe the Splunk distributed model
- Describe data input types and metadata settings
- Configure initial input testing with Splunk Web
- Testing Indexes with input staging

Module 2 –Config Files and Apps

- Identify Splunk configuration files and directories
- Describe index-time and search-time precedence
- Validate and update configuration files
- Explore Splunk apps and app installation

Module 3 – Configuring Forwarders

- Configure Universal Forwarders
- Configure Heavy Forwarders

Module 4 – Customizing Forwarders

- Configure intermediate forwarders
- Identify additional forwarder options

Module 5 – Managing Forwarders

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

Module 6 – Monitor Inputs

- Create file and directory monitor inputs
- Use optional settings for monitor inputs
- Deploy a remote monitor input

Module 7 – Network Inputs

- Create network (TCP and UDP) inputs
- Describe optional settings for network inputs

Module 8 – Scripted Inputs

- Create a basic scripted input

Module 9 – Agentless Inputs

- Configure Splunk HTTP Event Collector (HEC) agentless input
- Describe Splunk App for Stream

Module 10 – Operating System Inputs

- Identify Linux-specific inputs ▪ Identify Windows-specific inputs

Module 11 – Fine-tuning Inputs

- Understand the default processing that occurs during input phase
- Configure input phase options, such as source type fine-tuning and character set encoding

Module 12 – Parsing Phase and Data Preview

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

Module 13 – Manipulating Input Data

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

Module 14 – Routing Input Data

- Filter data with Ingest Action rules
- Route data with Ingest Action rules
- Route data with TRANSFORMS

Module 15 – Supporting Knowledge Objects

- Define default and custom search time field extractions
- Identify the pros and cons of indexed time field extractions
- Configure indexed field extractions
- Describe default search time extractions
- Manage orphaned knowledge objects

Examen y certificación

Splunk Enterprise Certified Admin (Prereq for this cert is the: Splunk Core Certified Power User)

Más información

NOTE: Make sure to complete a module within a 4 hour time range, do not start a module one day and then end the next day)
Network Secu Data Intelligence AI Cloud

Fechas Programadas

A petición. Gracias por [contactarnos](#).

Información Adicional

[Esta formación también está disponible en modalidad presencial. Por favor contáctenos para más información.](#)