

Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Du kan nå oss her

Postboks 6562 ETTERSTAD, 0606 Oslo, Norge

Email: kurs.ecs.no@arrow.com Phone: +47 22 02 81 00



Splunk Enterprise Data Administration

CODE: LENGTH: PRICE:

SPL SE9DA 24 Hours (3 days) kr23,750.00

Description

This 18-hour course is designed for 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

Objectives

Description

- · Understand sourcetypes
- Manage and deploy forwarders
- · Configure data inputs
- · Fire 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

Prerequisites

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

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

OR the following courses:

- Splunk Fundamentals 1
- Splunk Fundamentals 2 (recommended)

Students should also have understand the following course:

• Splunk Enterprise System Administration (recommended)

Programme

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 - Configuration 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

Monitor forwarder manageme

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 Actions rules Mask data with SEDCMD and TRANSFORMS

Module 14 - Routing Input Data

Filter data with Ingest Action rules
Route data with Ingest Action rules
Route data with Transforms
Override sourcetype or host based upon event values

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

Session Dates

Ved forespørsel. Vennligst kontakt oss

Tilleggsinformasjon

Denne treningen er også tilgjengelig som trening på stedet. Kontakt oss for å finne ut mer.