Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS B.V., Kromme Schaft 5, 3991 AR Houten, The Netherlands

Email: education.ecs.nl@arrow.com
Phone: +31 20 582 6109

Splunk Enterprise Administration Fast Start (TU 375)

CODE:	LENGTH:	PRICE:
SPL_ADM-FT	40 Hours (5 days)	€3,750.00

Description

This fast start prepares Splunk Enterprise administrators to install, configure, and deploy on-premises Splunk environments. Combining content from :

- Splunk Enterprise System Administration and
- Splunk Enterprise Data Administration,
- the course provides the foundational knowledge and recommended practices needed to support core platform administration, manage data onboarding, and maintain reliable data ingestion across the environment.

Splunk product version in this training : 10.4

Objectives

Splunk Enterprise System Administration:
− Identify Splunk components and understand the basics of a Splunk deployment
− Monitor Splunk operations and licensing
− Explore Splunk configuration files
− Install a Splunk app
− Create and manage Splunk indexes
− Create users and roles in Splunk
Splunk Enterprise Data Administration:
− Understand source types
− Manage and deploy forwarders with agent management
− Configure data inputs:

- File monitors
- Network inputs (TCP/UDP)
- Scripted inputs
- HTTP inputs (via the HTTP Event Collector)

− Customize the parsing process
− Define transformations to modify raw data before it is indexed
− Define search time knowledge object configurations

Audience

Splunk Enterprise administrators

Prerequisites

• To be successful, learners must meet the following prerequisites:
• Basic understanding of Linux administration
• Familiarity with the Splunk architecture
• Basic knowledge of performing searches using SPL
• Completed the following courses or equivalent experiences:
• Exploring Splunk Platform Ecosystem
• Splunk User track

Programme

Part 1 – Core Splunk Administration
Module 1 – Deploy Splunk

- Provide an overview of Splunk.
- Identify Splunk Enterprise components and deployment types.
- List installation prerequisites and installation steps.
- Use Splunk CLI commands.
- Explore recommended security practices.

Lab: Configure a Splunk Server (15 min)
Module 2 – Monitor Splunk

- Use the Splunk Health Report.
- Enable and use the Monitoring Console.
- Use Splunk Diag and RapidDiag.

Lab: Monitor Splunk (20 min)
Module 3 – License Splunk

- Identify Splunk license types and violations.
- Install a Splunk license.
- Configure a License Manager, license peers, and license pools.
- Manage license warnings and monitor license usage.

Lab: License Splunk (15 min)
Module 4 – Use Configuration Files

- Describe the Splunk configuration directory structure.
- Explore configuration layering at index time and search time.
- Use Splunk tools such as btool to examine configuration settings.

Lab: Use Configuration Files (20 min)
Module 5 – Use Apps

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

Lab: Use Apps (15 min)
Module 6 – Create Indexes

- Describe how Splunk indexes function.
- Identify index bucket types.
- Create and work with indexes.
- Describe metrics indexes.

Lab: Create Indexes (20 min)
Module 7 – Manage Indexes

- Review index-management fundamentals.
- Identify retention and backup recommendations.
- Move and delete indexed data.
- Describe the fishbucket.
- Restore a frozen bucket.

Lab: Manage Indexes (20 min)
Module 8 – Manage Users

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

Lab: Manage Users and Roles (15 min)

Part 2 – Data Collection and Forwarder Management
Module 9 – Get Data into Splunk

- Describe the Splunk distributed model.
- Describe data-input types and metadata settings.
- Configure initial input testing with Splunk Web.
- Test indexes using input staging.

Lab: Get Data into Splunk (15 min)
Module 10 – Configure Forwarders

- Configure Universal Forwarders.

- Configure Heavy Forwarders.

Lab: Configure Forwarders (20–25 min)
Module 11 – Customize Forwarders

- Configure intermediate forwarders.
- Identify additional forwarding options.

Lab: Customize Forwarders (20 min)
Module 12 – Manage Agents

- Explain agent-management features, benefits, and components.
- Configure agents and create deployment apps.
- Deploy apps through server classes.
- Monitor forwarder and agent-management activity.

Lab: Manage Agents (45 min)
Module 13 – Monitor Inputs

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

Lab: File Monitor Input (30–35 min)
Module 14 – Network Inputs

- Create TCP and UDP network inputs.
- Describe optional network-input settings.

Lab: Network Inputs (15 min)
Module 15 – Scripted Inputs

- Create a basic scripted input.
- Describe how scripted inputs are created and deployed.
- Identify risks associated with scripted inputs.

Lab: Scripted Inputs (10 min)
Module 16 – HEC Inputs

- Configure Splunk HTTP Event Collector.
- Describe HEC deployment options and indexer acknowledgement.
- Monitor HEC activity using the Monitoring Console.
- Examine Splunk Edge Hub and describe Splunk App for Stream.

Lab: HEC Inputs (15 min)

Part 3 – Data Processing and Knowledge Objects
Module 17 – Fine-tune Inputs

- Understand default input-phase processing.
- Configure input-phase options, including source-type fine-tuning and character-set encoding.

Lab: Fine-tune Inputs (10–15 min)
Module 18 – Parsing Phase and Data Preview

- Understand default parsing-phase processing.
- Optimize and configure event line breaking.
- Explain timestamp and time-zone extraction.
- Use Data Preview to validate event creation.

Lab: Create New Source Types (20–25 min)
Module 19 – Manipulate Input Data

- Explore Splunk transformation methods.
- Create rulesets with Ingest Actions.
- Mask data using Ingest Actions, SEDCMD, and TRANSFORMS.
- Override source type or host based on event values.

Lab: Manipulate Input Data (40 min)
Module 20 – Filter and Route Input Data

- Route and filter events using classic TRANSFORMS methods.
- Send events from Heavy Forwarders to selected indexer groups.
- Use Ingest Actions for conditional routing and filtering.

Lab: Route Input Data (30 min)
Module 21 – Support Knowledge Objects

- Define default and custom search-time field extractions.
- Identify benefits and drawbacks of indexed-time field extraction.
- Configure indexed-field extractions.

- Describe default search-time extractions.
- Manage orphaned knowledge objects.

Lab: Support Knowledge Objects (5–10 min)
Appendices
Appendix A – Upgrading Splunk

- Review upgrade considerations, terminology changes, dependencies, and security resources.

Lab: No dedicated lab specified.
Appendix B – Operating System Inputs

- Explore Linux JournalD inputs and Windows-specific inputs, including Event Logs, performance data, Active Directory, Registry, WMI, and PowerShell.

Lab: No dedicated lab specified.

Test and Certification

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

Session Dates

On request. Please contact us

Additional Information

This training is also available as onsite training. Please contact us to find out more.