Splunk Enterprise Data Administration

Category: AI, Data & Analytics | **Vendor:** Splunk

Duration: 24.00 hours (3 days) **19.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

This course is for administrators who are responsible for getting data into Splunk.

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 Agent Management Server components.

Please note that classes may run across three days, consisting of 6 hour sessions each day. The course has 18 hours of content.

About This Course

This course is for administrators who are responsible for getting data into Splunk.

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 Agent Management Server components.

Please note that classes may run across three days, consisting of 6 hour sessions each day. The course has 18 hours of content.

Who Should Attend

- Administrators

Prerequisites & Entry Requirements

General Prerequisites:

To be successful, students must have completed these Splunk Education course(s) or have equivalent working knowledge:

- Exploring Splunk Platform Ecosystem
- Splunk User Track
- Splunk Enterprise System Administration (SESA)

Detailed Course Outline

Module 1 – Get 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
- Test 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 apps installation

Module 3 – Configure Forwarders

- Configure universal forwarders
- Configure heavy forwarders

Module 4 – Customize Forwarder

- Configure intermediate forwarders
- Identify additional forwarder options

Module 5 - Manage Agents

- Explain the features and benefits of agent management

- List the agent management components
- Configure agents
- Create deployment apps
- Deploy apps to agents using server classes created in agent management
- Monitor forwarder activity using the Monitoring Console
- Monitor agent 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
- Describe the process for creating and deploying scripted inputs
- Identify the potential risks associated with scripted inputs

Module 9 – Agentless Inputs

- Configure Splunk HTTP Event Collector (HEC)
- Describe HEC deployment options
- Explain how HEC indexer acknowledgement works
- Monitor HEC activity using the MC
- Examine Splunk Edge Hub
- Describe Splunk App for Stream

Module 10 – Operating System Inputs

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

Module 11 – Fine-tune Inputs

- Understand the default processing that occurs during input phase
- Configure input phase options

Module 12 – Parse Phase and Data Preview

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

Module 13 – Manipulate 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 base upon event values

Module 14 - Route Input Data

- Route and filter events using classic TRANSFORMS methods
- Use TRANSFORMS and forwarding groups to send events from heavy forwards to specific groups of indexers
- Use Ingest Actions to conditionally route and filter events

Module 15 – Support Knowledge Objects

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

Frequently Asked Questions

Q: What delivery options are available for Splunk Enterprise Data Administration?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 3-day Splunk Enterprise Data Administration course provides up to 19.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Splunk Enterprise Data Administration training?

The training takes place over 3 day(s), with each day lasting approximately 24.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Splunk Enterprise Data Administration?

Yes, we provide corporate training, dedicated training, and closed classes for Splunk Enterprise Data Administration. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Splunk Enterprise Data Administration, Splunk Enterprise Administrator, SEDA

Q: Why choose Nexus Human for Splunk Enterprise Data Administration?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Splunk Enterprise Data Administration training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)