CrowdStrike University

CROWDSTRIKE UNIVERSITY

LOG 200
FALCON LOGSCALE FOR ADMINISTRATORS

COURSE OVERVIEW

Do you want to learn to configure and maintain the main components of LogScale in an installed instance? Are you looking to create a repository and configure ingestion, parse data, and learn about LogScale-specific administrative tasks?

In this course, you will walk through the steps and techniques you can use to administer the Falcon LogScale environment, manage authentication and authorization, and explore how data gets into LogScale.

LEARNING OBJECTIVES

By the end of this course, you will be able to:

- Explain the purpose, functions, and features of LogScale
- Administer the LogScale environment
- Administer LogScale users and the user interface
- Troubleshoot errors in the LogScale environment

PREREQUISITES

- Complete LOG 101: Getting Started with LogScale
- Comprehend course curriculum presented in English
- Basic knowledge and/or experience with Microsoft Windows and Linux environments
- Working knowledge of log management and regular expressions

CLASS MATERIAL

Download your Learner Guide and Lab Guide from CrowdStrike University once the class starts.

2-day program | 4 credits

HOW YOU WILL LEARN

This instructor-led course includes 13 hands-on labs that allow you to practice and apply what you've learned.

AUDIENCE

Take this class if you are a system administrator, DevOps engineer, or responsible for configuring and managing a LogScale instance.

REGISTRATION

For a list of scheduled courses and registration access, please log in to your CrowdStrike University account. This course requires four (4) training credits. If you do not have access to CrowdStrike University, need to purchase training credits or need more information, please contact sales@crowdstrike.com.

CrowdStrike University

LOG 200: Falcon LogScale for Administrators

CREATING RESPOSITORIES AND VIEWS

- Create and configure a repository
- Create a view and configure basic view information
- Search across repositories
- Compare the various special repositories in LogScale

INGESTING DATA

- Recall the stages of getting data into LogScale
- Explain key ingest methods
- Recall how data is parsed and filtered
- Describe the data digestion phase
- Configure digest rules
- Describe the storing phase
- Recall key data storage rules
- Ingest data with and without encryption
- Parse data

BUILDING AND MAINTAINING DASHBOARDS

- Create and configure LogScale dashboards
- Manage dashboards
- Recall the main operations that can be performed with each dashboard
- Compare the various dashboard widgets

SETTING UP AUTOMATION AND ALERTS

- Explain the difference between scheduled searches and alerts
- Create scheduled searches in LogScale
- Create and manage alerts in LogScale
- Configure automated actions in LogScale

INSTALLING PACKAGES

- Recall the purpose of LogScale packages
- Review how to create a package
- Find, install, and update packages

GENERAL LOGSCALE ADMINISTRATION

- Implement quotas and blocklists
- Use Health Checks to review the health of the LogScale server
- Explain the key components of log management
- Recall how LogScale stores an audit trail of user actions
- Compare metrics that can be used to monitor and operate LogScale
- Describe the purpose, function, and components of a LogScale cluster
- Use the Insights package to monitor and observe a LogScale cluster

SECURITY AND AUTHENTICATION

- Compare the various LogScale authentication methods
- Assign user permissions
- Describe what LogScale logs about itself
- Configure security and authentication settings
- Customize the LogScale experience with API integrations

TROUBLESHOOTING

- Perform standard administrative troubleshooting tasks in LogScale
- Identify typical third-party troubleshooting concerns
- Recall available support options

This instructor-led course includes **13 hands-on labs** that allow you to practice and apply what you've learned.