

1 December 2020

LogRhythm University

304 – Cloud Administration Fundamentals Product Training Syllabus



LogRhythm, Inc – 4780 Pearl East Cir Boulder, CO 80301 – (720) 881-5400

www.logrhythm.com

DATE CREATED	TRAINING COURSE SYLLABUS
06/24/2020	304-Cloud Administration Fundamentals
VERSION NO.	CREATED BY
7.4	LogRhythm Training
PROCEDURE NO.	PROCESS OWNER
0	Project Manager
DATE OF LAST UPDATE	LAST UPDATED BY
12/1/2020	Project Manager

304 – Administration Product Training

In this 20-hour course, learn hands-on best practices for day-to-day administrative duties in a LogRhythm Cloud environment.

Once a participant has completed the Cloud Administration Fundamentals Product Training they will be eligible to take the LogRhythm Cloud Administrator exam to receive the corresponding LRCA certification.

INTRODUCTION

WHO SHOULD ATTEND	304 – Cloud Administration Fundamentals Product Training is designed for systems administrators, engineers, and other LogRhythm users who are responsible for the basic maintenance and configuration of the LogRhythm Platform in a cloud environment.
PREREQUISITES	<p>None</p> <p>Some recommendations include (but are not limited to):</p> <ul style="list-style-type: none"> ➤ Introduction to LogRhythm - What is a SIEM? ➤ Introduction to LogRhythm - Administrators and Analysts ➤ What's New in LogRhythm v7.4 ➤ Web Console - An Introduction Video
304 – CLOUD ADMINISTRATION FUNDAMENTALS PRODUCT TRAINING	<p>304 – Cloud Administration Fundamentals Product Training explores the day-to-day activities in the LogRhythm Cloud Platform for administrators. Participants can expect to leave with an understanding of administrative functions within the LogRhythm Client Console and will be equipped with the tools to effectively manage the log data collected through the cloud-based product.</p> <p>The course includes hands-on exercises to provide experience with the administrative functions of the LogRhythm Platform.</p>

304 – Cloud Administration Fundamentals Product Training – Modules and Topics

Administration Fundamentals

The Administration Fundamentals section will explore the day-to-day administrative activities of the LogRhythm Platform as well as introduce the LogRhythm Console's administrative functions.

Participants can expect to leave with an understanding of navigating the LogRhythm Platform and will be equipped with the tools to effectively manage the collection of log data.

This training consists of the following modules:

- Introduction to LogRhythm
- Platform Overview
- System Monitors
- Entities and Log Sources
- Log Source Administration
- Users, Profiles, and Permissions
- Lists
- Alarming and Reporting

AI Engine Fundamentals

Advanced Intelligence Engine (AIE) Fundamentals Training explores the administrative activities for the AI Engine.

Participants can expect to leave with an understanding of how AI Engine functions, an understanding of AI Engine Rule configuration, and familiarity with common threats and attack scenarios for which the rules are configured to monitor.

This training consists of the following modules:

- Introduction to AI Engine
- AI Engine Rules
- Threshold and Unique Values Rule Blocks
- Behavioral Rule Blocks
 - ✓ Whitelist
 - ✓ Statistical
 - ✓ Trend

Certification

LogRhythm Cloud Administrator (LRCA)

By attending and completing the training, participants will be prepared to take an exam to obtain the LogRhythm Cloud Administrator (LRCA) certificate.

The LRCA exam is a written exam comprised of multiple-choice, True or False, and Select All That Apply questions. The exam tests a candidate's knowledge on managing and maintaining the LogRhythm Platform and familiarity with platform functions and features.

Candidates will have 90-minutes to complete the exam. **Candidates must pass the written exam with a score of 70% or more to receive a LogRhythm Cloud Administrator (LRCA) certificate.**