



LogRhythm Official Training

Certified LogRhythm Administrator

5th August 2010

V1.2

Contact Information:

Janne Nyman

Solutions Consultant, EMEA

LogRhythm, Inc.

email : janne.nyman@LogRhythm.com

www.logrhythm.com

Introduction

The purpose of this document is to define the course content and recommended participant for the Certified LogRhythm Administrator course.

The Certified LogRhythm Administrator course is aimed at people that will use the LogRhythm Log and Event Management solution on a daily basis to investigate and alert on relevant events within their organization. The Certified LogRhythm Administrator course introduces the student to the data access and analysis front end of the LogRhythm solution. Students are also introduced to the LogRhythm Console and how to customize it to their needs

Prerequisites and Length

This course is a two day course. There are no prerequisites for attending this course.

Scope

This guide is for use by LogRhythm end user customers.

Course Content

Welcome Orientation and Overview

Participants will be provided with a brief introduction to the facility, area, accommodations, each other, eating arrangements, and plan for the days ahead.

LogRhythm Overview & Architecture

This training module will provide the student with an overview of LogRhythm Log and Event Management. This session will provide students with the basic knowledge to understand:

- ☐☐☐ LogRhythm terminology
- ☐☐☐ LogRhythm log data hierarchy
- ☐☐☐ LogRhythm logical objects
- ☐☐☐ LogRhythm Knowledge Base
- ☐☐☐ LogRhythm Solution Architecture

The LogRhythm Overview & Architecture training module provides the pre-requisite foundation knowledge for all other training.

Section One: Analysis & Reporting

This training module then goes on to provide the student with a working knowledge of:

- ☰ The LogRhythm Dashboard
- ☰ Real-time monitoring and analysis of events and alarms
- ☰ The LogRhythm Investigator
- ☰ Historic/forensic log and event data analysis
- ☰ The LogRhythm Tail Utility
- ☰ Real-time access to raw log data
- ☰ The LogRhythm Quick Search Toolbar
- ☰ The LogRhythm Report Center
- ☰ Configuration and generation of reports for compliance, security, and operations

Section Two: Deployment & Administration

This training module goes on to provide the student with a working knowledge of:

- ☰ Deployment Management
 - Managing LogRhythm Logical objects
 - Entities, Networks, and Hosts
 - Log Managers
 - Agents
 - Log Sources
 - Message Processing Engine Policies
 - Alarm Rules
 - People and Users
 - Common Deployment tasks
 - Adding Entities, Networks, and Hosts
 - Deploying an Agent
- ☰ Introduction to Configuring LogRhythm Agents for Log Collection
 - Collecting Windows Event Logs
 - Collecting Flat File Logs
 - Collecting Syslog
 - Collecting Netflow
 - Collecting Checkpoint Firewall Logs
 - Collecting Database data with the Universal Database Log Adapter (UDLA)
- ☰ Security Administration
 - Understanding LogRhythm Security Roles

- Managing LogRhythm Users
- Managing Restricted Analysts

- ☰ Configuring and Managing Alarms
 - Alarm rule administration
 - Notification administration

- ☰ Archive Restoration

- ☰ Configuring & Using Log Source Lists

- ☰ Creating & Managing Saved Investigations

- ☰ Creating & Managing Custom Reports

- ☰ Creating & Managing Scheduled Reports

- ☰ Creating & Managing Alarm Rules
 - Global Alarm Rules
 - Personal Alarm Rules