LogRhythm v5.1 Training Syllabus

This document addresses LogRhythm Classroom-based (Section 1) and Web-based Training (Section 2)

Section 1: LogRhythm Classroom-based Training Certifications

LogRhythm certifications are available on completion of the following:

Course 1 **Certified LogRhythm End User and Administrator**

Course 1 is comprised of the following days of training:

- Day 1 – Basic End User
- Days 2 and 3 – Deployment and Administration and Advanced End User
- Successful completion of associated training exercises

Who Should Attend

Course 1 is designed for systems administrators, managers, engineers, and other LogRhythm end users who are responsible for system administrative management.

Course 2 **Certified LogRhythm Rule Developer**

Course 2 is comprised of the following days of training:

- Days 4 and 5 – Rule Development
- Successful completion of associated training exercises

Who Should Attend

Course 2 is designed for systems administrators and engineers who are supporting custom applications or need to do advanced customization and tuning of their LogRhythm deployment. It is recommended that students attending this course have completed Course 1 and have experience using regular expressions.

Course 3 **Two Day On-Site Certified LogRhythm End User and Administrator**

Course 3 is comprised of the following days of training:

- Day 1 – Basic End User and Advanced End User Training
- Day 2 – Advanced End User and Administration

Who Should Attend

Course 3 is designed for systems administrators, managers, engineers, and other LogRhythm end users who are responsible for system administrative management.

Courses 1 and 2 may be taken consecutively or separately.

Course 1: Classroom-based

End-User and Administrator Training

Course 1 consists of three modules:

- End-User Training
- Advanced End-User
- Deployment and Administration

End-User Training introduces you to the data access and analysis front end of the LogRhythm solution. You are introduced to the LogRhythm Console and receive instructions on how to customize for your needs.

Advanced End-User Training instructs you on how to use advanced methods for log and event analysis.

Deployment and Administration instructs you in the administration aspects of the LogRhythm enterprise system to ensure successful and on-going operations.

Day One: Basic End-User Training

Welcome Orientation and Overview

You receive a brief introduction to the facility, area, accommodations, each other, eating arrangements, and a plan for the days ahead. When the class begins, you will receive instructions on how to log into the training environment for hands-on examples and exercises.

LogRhythm Overview and Architecture

Provides you with the pre-requisite foundation for all other training — an overview of LogRhythm Log and Event Management and basic knowledge of:

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

Analysis and Reporting

Provides you 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

Day 1 modules will include instructor-guided, interactive exercises.

Days Two and Three:
Deployment and Administration and Advanced End-User Training

The LogRhythm Deployment, Administration, and Advanced End-User curriculum instructs you in how to use advanced methods for log and event analysis.

Topics to be covered include:

- Log Source Lists and their use as filters for all data access and analysis functions
- Personal Alarms and their use in real-time monitoring
- Alarm and Incident Management
- Report Templates and how to generating custom reports

Deployment and Administration

Items to be covered include:

1. **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 a Log Manager
     - Deploying an Agent
     - Working with the Job Manager
2. **Configuring LogRhythm Agents for Log Collection**
   - Enabling Global Data Management and Global Log Processing Rules
   - 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)
- Enabling Data Loss Defender (DLD)
- Enabling File Integrity Monitor (FIM)

3. **Configuring Message Processing Engine Policies**
    - Data retention and archive settings
    - Log processing and deduplication
    - Event forwarding
    - LogMart forwarding
    - Understanding Risk-Based Prioritization (RBP)
4. **Security Administration**
    - Understanding LogRhythm Security Roles
    - Managing LogRhythm Users
    - Managing Active Directory Synchronization
    - Managing Restricted Analysts
5. **Configuring and Managing Alarms**
    - Alarm rule administration
    - Notification administration
6. **Archive Restoration**
7. **Performance Monitoring and Troubleshooting**
    - LogRhythm Diagnostic Events and Alarms
    - Silent Log Source Detection
    - LogRhythm Performance Counters

Advanced End User

Items to be covered include:

1. **Configuring and Using Log Source Lists**
2. **Creating and Managing Saved Investigations**
3. **Creating and Managing Custom Reports**
4. **Creating and Managing Scheduled Reports**
5. **Creating and Managing Global and Personal Alarm Rules**

Day 2 and 3 modules will include instructor guided interactive exercises.

Course 2: Classroom-based

Rule Development Training

Days Four and Five (when combined with Course 1): Rule Development

LogRhythm Message Processing Engine (MPE) Rule Development

The Class is designed systems administrators and engineers who are supporting custom applications or need to do advanced customization and tuning of their LogRhythm deployment. It is recommended students attending the class have some experience with LogRhythm and a basic knowledge of Regular Expressions (regex). LogRhythm is a highly flexible and open system that provides the means for you to develop custom rules to meet your organizational data collection and processing demands. Students will learn all aspects of rule development. They will leave the course with the knowledge and tools required to integrate custom logging devices into LogRhythm and customize LogRhythm's support for commercial logging devices. This hands-on course will cover items including:

- Introduction to Regular Expressions
- Rule Function
- Rule Definition
- Parsing and Attributes
- Rule Builder Tool
- Tags (Usage, Parsing, Mapping)
- Base Rules versus Sub Rules
- Naming and Classification

Advanced Alarm Rule Development

Alarm Rules enable automatic detection and notification of specific activity. LogRhythm includes an extremely powerful and flexible system for creating a wide variety of Alarm Rules. This module provides extensive hands training in the development of sophisticated Alarm Rules for detecting activity in support of compliance, security, and operations objectives.

- Overview of the Alarm Rule Processing Engine
- Alarm Thresholds, Grouping, and Suppression
- Log Source Criteria
- Event Criteria
- Day and Time Criteria
- Advanced Notification Options
- Alarm Rule Sharing and Security

Day 4 and 5 modules include interactive instructor guided rule development exercises.

Course 3: Classroom-based

On-Site End-User and Administrator Training

Course 3 consists of three modules:

- End-User Training
- Advanced End-User
- Administration

End-User Training introduces you to the data access and analysis front end of the LogRhythm solution. You are introduced to the LogRhythm Console and receive instructions on how to customize for your needs.

Advanced End-User Training instructs you on how to use advanced methods for log and event analysis.

Administration instructs you in the administration aspects of the LogRhythm enterprise system to ensure successful and on-going operations.

Day One: Basic End-User Training

LogRhythm Overview and Architecture

Provides you with the pre-requisite foundation for all other training — an overview of LogRhythm Log and Event Management and basic knowledge of:

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

Analysis and Reporting

Provides you 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

Day Two:
Administration and Advanced End-User Training

The LogRhythm Deployment, Administration, and Advanced End-User curriculum instructs you in how to use advanced methods for log and event analysis.

Topics to be covered include:

- Log Source Lists and their use as filters for all data access and analysis functions
- Personal Alarms and their use in real-time monitoring
- Alarm and Incident Management
- Report Templates and how to generating custom reports

Advanced End User and Administration

Items to be covered include:

8. **Configuring LogRhythm Agents for Log Collection**
    - Enabling Global Data Management and Global Log Processing Rules
    - 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)
    - Enabling Data Loss Defender (DLD)
    - Enabling File Integrity Monitor (FIM)
9. **Configuring Message Processing Engine Policies**
    - Data retention and archive settings
    - Log processing and deduplication
    - Event forwarding
    - LogMart forwarding
    - Understanding Risk-Based Prioritization (RBP)
10. **Security Administration**
    - Understanding LogRhythm Security Roles
    - Managing LogRhythm Users
    - Managing Active Directory Synchronization
    - Managing Restricted Analysts
11. **Configuring and Managing Alarms**
    - Alarm rule administration
    - Notification administration
    - Creating and Managing Global and Personal Alarm Rules

12. **Archive Restoration**
13. **Performance Monitoring and Troubleshooting**
    - LogRhythm Diagnostic Events and Alarms
    - Silent Log Source Detection
    - LogRhythm Performance Counters

Advanced End User

Items to be covered include:

1. **Configuring and Using Log Source Lists**
2. **Creating and Managing Saved Investigations**
3. **Creating and Managing Custom Reports**
4. **Creating and Managing Scheduled Reports**
5. **Creating and Managing Global and Personal Alarm Rules**

LogRhythm 5.1 Web-based Training

Web-based training is delivered from the **LogRhythm Learning Center**. The classes are videos downloaded/streamed from the web. We recommend that all users take advantage of this training.

There are two ways to leverage LogRhythm web-based training:

1) *Self-Service:* Customers may access the **LogRhythm Learning Center** and its growing list of online courses via the LogRhythm Support site (with a valid login).
2) *Instructor-led* –A Certified LogRhythm Trainer introduces/runs the videos and monitors the class to answer chat-style questions during the videos. A question and answer period is provided between Modules. During the Q&A period the instructor can provide answers to specific questions or perform additional demonstrations.

   Instructor-led courses are can be scheduled based on demand/availability.

   For Q3 2010 we will run the first course, **Searching in LogRhythm**, at 1000 MST on the first Friday of each month.

For appropriate quality, please ensure you leverage a high speed (DSL minimum) connection.

The video portion of each course is planned to be a total of 1-2 hours in length depending on the topic addressed. The course is divided into 4-5 modules of approximately 10 to 25 minutes each. The instructor-led classes are planned to be 1 hour longer than the self-service video classes.

The first course was launched in July 2010 and additional courses can be expected roughly once per quarter (Reporting and Alarming are the next planned courses). One course is currently available:

Course 1 Searching in LogRhythm - In this course you will learn: LogRhythm's approach to turn incoming log data into searchable information, to organize an efficient search, the tool (Search Wizard) to build a search, and common approaches to working with Search Results. In addition there will be solid examples and scenarios to reinforce the learning.

Course 1 is comprised of 5 Modules:

Module 1: Anatomy of a Log - In this module you will learn how LogRhythm makes sense of incoming log messages and turns the mountains of log data into meaningful information. Understanding how LogRhythm handles logs is a critical building block for anyone looking to search their LogRhythm Deployment.

Module 2: Anatomy of a Search – In this module you will learn the how LogRhythm Search works. Just as understanding how LogRhythm handles logs is a first building block, understanding how LogRhythm Search works is a critical second step in efficiently organizing a search in your LogRhythm Deployment.

Module 3: Search Wizard – In this module you will learn how to construct a search using the LogRhythm Search Wizard. Building on the concepts and examples in the first two modules you will be able to efficiently construct a search.

Module 4: Working with Search Results – In this module you will learn common approaches to working with Search Results, including common tools with examples.

Module 5: Specific Examples and Scenarios - In this module you will be exposed to additional examples and scenarios that are typical for many LogRhythm Deployments. This is focused, task oriented examples that describe real world questions our Professional Services Engineers often must address.

Who Should Attend

Any end user that wishes to understand search and the options available within LogRhythm

LogRhythm Training Pricing

Training Courses – Outline

Classroom-based Training

Course 1 - End User and Administration (3 days) **$ 3600 per seat**
Available via Boulder Classroom setting only

Course 2 - Rule Development (2 days) **$ 3000 per seat**
Available via Boulder Classroom setting only

Course 3 – End User and Administration (2 days) **$ 12,000 up to 10 seats**
Maximum of 10 Seats, available On-Site via classroom setting only

Course 1 and Course 2 - Purchased together (5 days) **$ 5000 per seat**
**Certification training is available via Boulder classroom setting only at a Boulder area facility.*

Web-based Training

Self Service **Free for 2010**
Available via LogRhythm Support Portal

Instructor Led courses (2-3 hours per course) **$ 250 per seat**
Available to schedule on request – Instructor runs video sessions and is available for Chat during videos and Q&A/additional instruction between videos