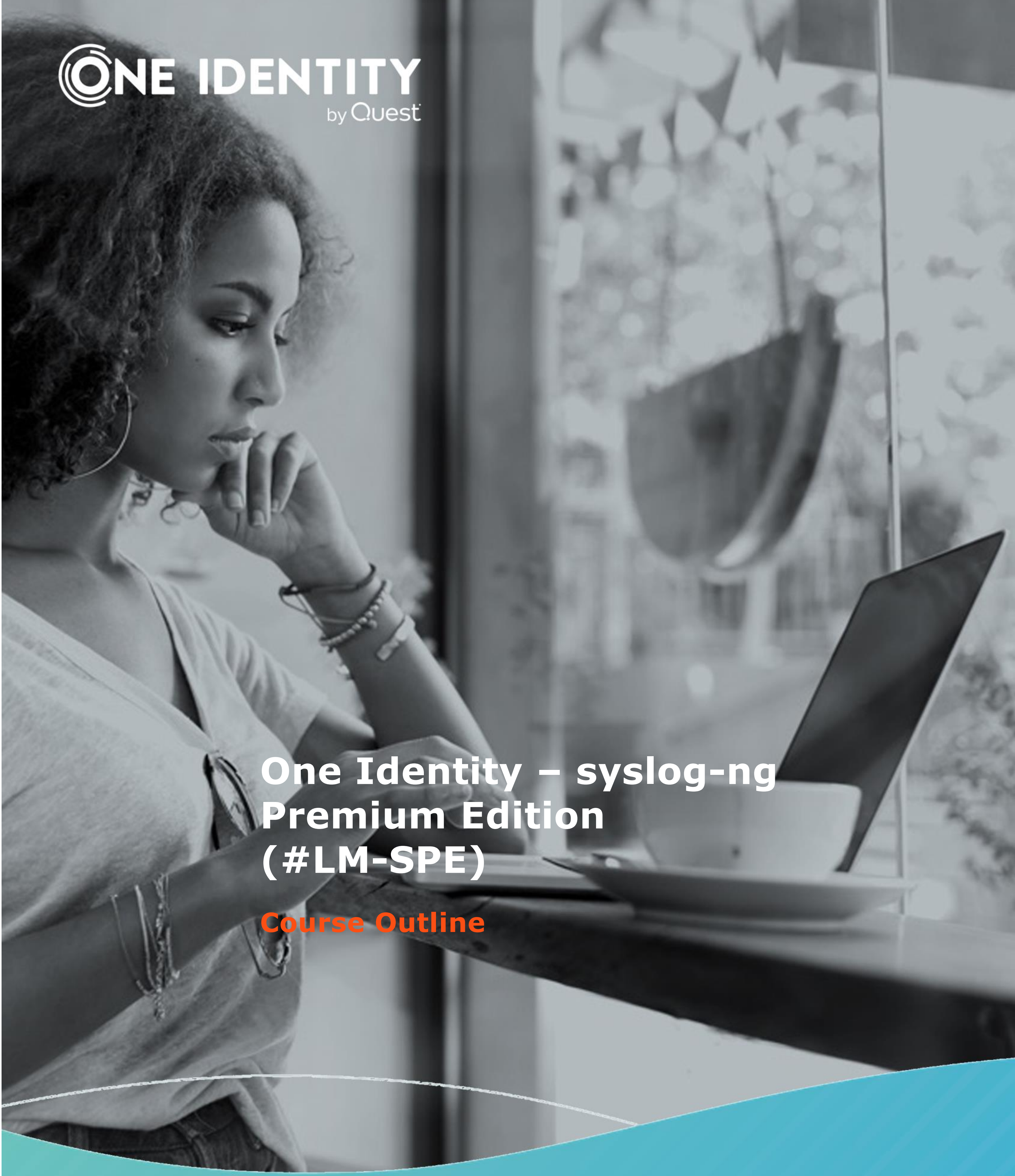

One Identity – syslog-ng Premium Edition (#LM-SPE)

Course Outline

Course Outline - syslog-ng Premium Edition (#LM-SPE)

Overview

The purpose of this course is to provide students with a general overview of the One Identity syslog-ng Premium Edition feature-set, installation, configuration and customization of the solution framework as well an overview of the main business processes that are part of the solution framework. This course focuses on lab performance and was developed for people just interested how syslog-ng Premium Edition can be installed configured.

Course:	Syslog-ng Premium Edition (#LM-SPE)
Audience:	Customer, sales and Technical Sales
Language:	English
Duration:	2FIXME days (remote)
Prerequisite:	None

Topics

- Overview of the feature-set of syslog-ng Premium Edition
- Introduction to syslog protocols (RFC3164, RFC5424 and Eventlog)
- Installation and basic settings of syslog-ng PE
- Using Macros and Templates to reformat syslog messages
- Setup filters
- Manage syslog-ng daemon from the command line
- Transferring messages via the network and securing them
- Collect messages from windows machines
- Storing messages in logstores and encrypt them.
- Parsing messages by message parser modules and reformat them by rewrite modules
- Store messages in SQL databases
- Classify messages with the radix tree algorithm based patterndb
- Advanced setting and syslog-ng internals
- Troubleshooting syslog-ng PE

Training Course Details

Please note: Agenda, Labs and Demos show all available parts for an existing Training module. Depending on the course, smaller parts of it might not be taught or performed. Typically, suitable Labs must be taught but Demos could be selected during a training.

Topics	Labs
Introduction syslog-ng PE **Training Module: SPE-INT** • History of syslog • Protocol Overview • Syslog-ng worjing miodes and licensing model	• -
Simple syslog-ng settings **Training Module: SPE-SST** • How to configure syslog-ng • Confg objects of syslog-ng configuration files	• Install syslog-ng PE • Collect messages from local sources (file and system) • Store messages in local destinations
Macros and Templates in syslog-ng **Training Module: SPE-MAT** • What are macros, templates and nv-pairs • What are template functions • How to use them	• Modify message format by template • Use marcros in file names and path • Convert messages to WELF by template function
Filters **Training Module: SPE-FLT** • Filters in syslog-ng • Combine filters • Optimize filters	• Create and use filters
Command line tools **Training Module: SPE-CMD** • Start, stop and manage syslog-ng from the command line	• Start syslog-ng from command line • Change syslog-ng verbosity
Networking **Training Module: SPE-NET** • Transfer messages via legacy protocol • Transfer messages via syslog protocol • Secured message transfer • Reliable message transfer	• Transfer messages via network() driver • Configure encrypted message transfer • Configure a relay server
Windows Messaging **Training Module: SPE-CWE** • Windows logging subsystem • Collect messages with syslog-ng agent for Windows • Collect messages with WEC	• Install and configure syslog-ng Agent • Transfer EventLog via the agent
Logstore **Training Module: SPE-LST** • Logstore file format • Configure and display logstore • Encrypt and decrypt logstore	• Create a logstores • Enctypt logstores • Displa logstores

Topics	Labs
Message Parsing **Training Module: SPE-MPR** • What parsers do • Type of parsers • Using parsers	• Using CSV parser • Using K-V parser
Database support **Training Module: SPE-DBS** • Storing messages in SQL servers • Fetching log messages from SQL databases	• Instert messages in MySQL database
Message Content Manipulation **Training Module: SPE-MCM** • Rewrite messages • Conditional rewrite • Pseudonimize and anonymize messages	• Rewrite messages on a relay • Rewrite message body
Message Classification **Training Module: SPE-MCL** • The pattern-db message parser	• Setup pattern-db parser
Syslog-ng and the Cloud **Training Moduel: SPE-CLD** • The HTTP destination • Google PUB/SUB destination • Google Stack driver destination • Splunk destination • ElasticSearch destination	• -
Advanced settings **Training Module: SPE-ADS** • Internals of syslog-ng • Message flow and limits • Disk buffering • Monitoring syslog-ng • Tricks of the configuration file	• -
Troubleshooting syslog-ng **Training Module: SPE-TRB** • Troubleshooting syslog-ng settings • Troubleshooting syslog-ng Agent for Windows	• -