Corona Technical Services

SolarWinds Log & Event Manager –

Training Project/Implementation Outline

James Kluza

14

Table of Contents

Overview

This document is to be used as a general outline when scheduling or accomplishing a SolarWinds LEM professional services engagement.

Example Project Schedule

- Knowledge Transfer - Introduction to LEM
  - Purpose
  - Licensing
  - Architecture
  - Terms
  - Customer Portal
  - Thwack
- Knowledge Transfer - Planning for LEM
  - Requirements
  - Retention
  - Scalability
  - Pre-engagement Checklist
  - Monitoring logs that aren't ready out of the box
  - Any other decisions that should be considered to ensure a good deployment overall
- Deployment of Appliance
- Configuring Non-Agent Devices
  - Typical commands
- Deploying Agents to Devices
  - Process
  - Upgrade agents process
- Knowledge Transfer - Console Overview
  - Web
  - Desktop
  - Reports
- Knowledge Transfer - Modules
  - OPS Center
  - Monitor
  - Explore
  - Build
  - Manage
  - Analyze
- Knowledge Transfer - Reports Console
  - Purpose
  - Running
  - Filtering

- Scheduling

Pre-engagement Checklist

The following items should be accomplished prior to any installation engagements:

- Validate access to the SolarWinds Customer Portal with SWID and password
- Document license key for the LEM product for use during deployment
- Validate VMware vSphere access and ensure OVF template can be deployed in an initial environment that provides a DHCP scope (after activation process, the appliance can be migrated into any other context with static configuration)
- Ensure the necessary ports are open between the appliance subnet and any other networks on which agents will be deployed or logs will be collected. Ports are as follows:

Port	TVs	Description
25	TCP	Traffic from the SolarWinds LEM appliance to your email server for automated email notifications
139. 445	TCP	Standard Windows file shanng ports used for the SolarWinds LEM Remote Agent Installer and traffic from the SolarWinds LEM appliance to a Windows destination for exporting functions
182	TCP	Traffic from devices sending SNMP trap messages to the SolarWinds LEM appliance
389	TCP	Traffic from the SolarWinds LEM appliance to a designated server (usually a domain controller) for use with the Directory Service tool
514	TCP or UDP	Traffic from devices sending syslog to the SolarWinds LEM appliance
2100	UDP	Traffic from devices sending NetFlow to the SolarWinds LEM appliance
5433	TCP	Traffic from SolarWinds LEM Reports to the SolarWinds LEM appliance

Port	Typo	Description
6343	UDP	Traffic from devices sending sFlow to the SolarWinds LEM appliance
8080	TCP	Non-secure traffic from the SolarWinds LEM Console to the SolarWinds LEM appliance; used during the evaluation period
8443	TCP	Secure traffic from the SolarWinds LEM Console to the SolarWinds LEM appliance; used once SolarWinds LEM is activated
32022	TCP	Non-standard port for SSH traffic to the SolarWinds LEM appliance
37890-37892	TCP	Traffic from SolarWinds LEM Agents to the SolarWinds LEM appliance
37893-37896	TCP	Return traffic from the SolarWinds LEM appliance to SolarWinds LEM Agents

- Download the latest release of the following items from the Customer Portal as close to the implementation date as possible to ensure the latest versions are utilized:
    - LEM Appliance package
        - OVF template
        - Reports Console
    - Desktop Console that consists of two parts
        - Adobe Air
        - Desktop console application
    - Applicable Agents
        - Windows (local and remote installer)
        - Linux (32 and 64 bit)
- Ensure credentials are available for the following
    - Administrator access for any servers on which the agent will be deployed
    - Enable level access on any network devices on which logging will be enabled
    - If LDAP authentication will be utilized, a service account will be required to authenticate to the LDAP server during the query process
    - A CIFS based share for the export of the Appliance certificate during the activation process.
- If a static IP address will be assigned, the following needs to be identified:
    - IP Address
    - Subnet Mask
    - Gateway Address
    - DNS server (multiple recommended)
    - Hostname
- Console Restrictions
    - If access to the console will be restricted, the IP Addresses of the administrator machines will need to be collected
- Report Console Restrictions
    - If the ability to create reports from the report console will be restricted, the IP Addresses of the administrator machines will need to be collected
- Inventory
    - An initial inventory of all machines that will be added for collection to be conducted and classified as the following:
        - OS Based (Windows or Linux)
        - Non---agent Based (Routers, Switches, Firewalls, etc.)
- DNS Entry
    - An accurate DNS entry to the identified IP and hostname needs to be created

Deployment

Appliance

At a minimum, a $^1/_2$ day of effort should be scheduled solely for the process for deploying, activating, and configuring user access on the appliance. The following items are key points during the deployment and configuration process:

- Deploy OVF template in virtual environment
- Deploy desktop console to administrator machine
- Validate appliance access from Desktop Console to facilitate the activation process
- Activate the console
- Activate the Appliance
- Validate SSL access through the Web Console and Desktop Console
- Configure users either local LEM, LDAP Users, or LDAP Groups

Collection

Collection falls into two categories:

- Agent
- Non-Agent

Agent

Agent based collection requires that an agent be deployed on the server on which collection is to occur. This requires administrator or root level access (Windows & Linux respectively) and while both operating systems can be done using a standalone installer, a remote installer is available for Windows based machines.

Non-Agent

Non-Agent based collection occurs when devices such as routers, switches, and firewalls send logging information (Syslog or otherwise) to an identified logging facility (log file) on the Appliance. The Appliance then uses an Appliance based "Connector" to parse these log file repositories and normalize these entries into events in the Appliance. On the Agent based servers, this action occurs at the agent on the server and the real-time alert data is then sent to the Appliance for processing.

Knowledge Transfer

During and after the deployment phase of an engagement, knowledge transfer will occur. Knowledge transfer normally follows a general outline focusing on the following portions of the console and console operation:

- General overview of the console and feature layouts
    - Differences between the Web, Desktop and Report Consoles
- In depth discussion of each of the following modules
    - OPS Center
        - Widgets and their uses
    - Monitor
        - Filters
            - How to create them
            - How to modify
            - How to group
            - How to use as jumping point for nDepth search
    - Explore
        - nDepth
            - Introduction to nDepth
            - How to build queries
            - How to save queries
            - How to build and export nDepth Reports
        - Other Utilities
    - Build
        - Users
            - How to add, modify and delete users
        - Groups
            - The purpose of the different groups
            - How to add, modify and delete groups
        - Rules
            - The purpose of rules
            - How to add, modify, delete and activate rules
    - Manage
        - Appliances
            - Connectors
            - Settings
            - Policies
        - Nodes
            - How to manage nodes
            - How to configure Tools (Connectors)
    - Analyze (This module is discussed in the Reports Console Overview)

- Introduction to Reports Console

- Purpose of the console
- Running reports
- Filtering reports
- Scheduling reports