solarwinds SmartStart Self-Led Project Plan for Security Event Manager Instruction Manual

solarwinds SmartStart Self-Led Project Plan for Security Event Manager

Contents

INSTALLATION

Confirming Installation for SEM

You'll perform a health check on an existing SolarWinds® Security Event Manager (SEM) installation to ensure it's set up correctly and fully upgraded to the most recent version.

Documentation

Verify system requirements

System requirements allow you to properly size SEM with the correct resources based on your needs and license. We'll review your license and adjust the SEM resources accordingly.

Documentation

Deploy SEM

Steps for installing and upgrading SolarWinds Security Event Manager on Microsoft Hyper-V and VMware vSphere.

Documentation

SEM activation

Steps on how to activate your Security Event Manager license with the online and offline methods.

Documentation

ACCESS AND APPLICATIONS

Explain SSH and CMC console

The SEM command-line interface (CLI)—using the CMC console and showing SSH. The CMC provides a command-line interface for performing routine administrative tasks on the SEM VM.

Documentation

In addition to accessing your SolarWinds SEM virtual appliance using the virtual console in your VM client, you can also access your SEM appliance using a Secure Shell (SSH) client. This provides access to the command-line interface for the SEM appliance over a secure, non-standard SSH port.

Documentation

Set up email

Configure the Email Active Response Connector. This will allow us to send an email when a rule fires or when a scheduled saved search runs.

Documentation

Configure LDAP

In this section, we'll set up and configure LDAP for the SEM. LDAP allows us to use a domain account instead of local SEM accounts.

Documentation

CONFIGURE NETWORK DEVICES TO SEND DATA TO SEM

Install a few agents, communicate installation options

In this section, we'll deploy agents to mission-critical servers/workstations. The agents allow SEM to directly read the server's logs and report back to SEM in real time. SolarWinds provides SEM agents for these operating systems:

- Microsoft Windows (local and remote installers)
- Linux
- Mac OS X
- Solaris on Intel
- Solaris on Sparc
- HPUX on Itanium
- AIX

[Documentation](#)

Verify/set up firewall

When you add a syslog device to SEM, you select a connector specific to the network device you're adding. The connector normalizes the log data into a standard format compared with logs received from other vendors' devices.

[Documentation](#)

- Set up any other syslog devices:

Explain connector profiles

Connector profiles manage and monitor similar SEM agents across your network. The following two use cases are the most common for this type of component:

- Configure and manage connectors at the profile level to reduce the amount of work you must do for large SEM agent deployments
- Create filters, rules, and searches using your connector profiles as groups of SEM agents. For example, create a filter to show you all web traffic from computers in your domain controller connector profile

[Documentation](#)

FIM

FIM can detect unauthorized modifications to configuration files, executables, log and audit files, content files, database files, web files, and so on. When FIM detects a monitored file has changed, it logs an event. The event then prompts SEM to execute the configured action. You can build correlation rules to act as a second-level filter to alert if certain activity patterns occur (not just single instances). When an alert is triggered, the data is in context with your network and other system log data.

[Documentation](#)

VIEW REAL-TIME DATA, SEARCH FOR DATA, AND CREATE RULES

Demonstrate the SEM dashboard

Access the SEM dashboard to highlight and summarize trends and suspicious activity through a series of interactive widgets. You can create, edit, and arrange widgets to display log data in various tables and graphs based on filters within your events viewer.

SEM provides a library of widgets, or you can create your own by using filters you've customized to monitor specific activity. If your widget includes charts, you can click a specific line, bar, or pie wedge to open the source filter. The corresponding filter opens the events viewer and displays the targeted filter information. The filter lists only the events corresponding with the selected chart item.

[Documentation](#)

Real-time data under live events

The SEM console provides instant access to live event monitoring and filtering and historical record archives for in-depth analysis and troubleshooting. You can quickly switch between real-time event streaming and historical log views based on user-defined date and time parameters within the console view.

Documentation

SEM filters

Filters capture events and alerts taking place on your network. (In SEM, the terms event and alert are interchangeable.

The SEM console uses event filters to manage events. You can turn filters on and off, pause filters to sort or investigate events, perform actions to respond to events, and configure filters to notify you when they capture an event. Filters can also display widgets, which are charts and graphs designed to visually represent the event data.

Filter conditions can be broad or specific. For example, you can create a filter without conditions to capture all events regardless of the source or event type, or you can create a filter with one specific condition, such as “UserLogon Exists,” which only captures user logon events.

Documentation

Analyze historical data in SEM

The historical data search engine can locate any event data passing through a SEM instance. You can use the historical data search to conduct custom searches, investigate your search results and event data, and act on your findings.

Documentation

Purpose for rules, configure a couple of rules, & test the rules

Rules monitor event traffic and automatically respond to security events in real time, whether you’re monitoring the console or not. When an event (or a series of events) meets a rule condition, the rule prompts SEM to act. A response action can be discreet (for example, sending a notification to select users by email) or active (for example, blocking an IP address or stopping a process).

Documentation

Explain event groups and email templates

- About SEM Rules:
  Rules can respond to one or more events. In many cases, you can base rules on several events that SEM correlates trigger an action. You can also configure a rule to look for a single event
  Rules play a key role in detecting operational and compliance issues on your networks, such as external breaches, insider abuse, and policy violations. The SEM console ships with a set of preconfigured rules to help you get started
  Documentation
- Create a new rule:

Documentation

Explain event groups & email templates

- **About SEM groups:**
  Groups in SEM are objects organizing related elements for use with rules and filters. Groups can contain elements such as events, IP addresses, computer names, user accounts, etc. After a group is defined, it can be referenced from multiple rules and filters
  Documentation
- **Create email templates for use with SEM rules:**
  Email templates are preformatted messages SEM sends to users when alert events trigger a rule
  Documentation

CREATE SCHEDULED HISTORICAL DATA SEARCHES, & SCHEDULED REPORTS

Create several historical data searches

- **Analyze historical data in SEM:**
  The historical data search engine can locate any event data passing through a particular SEM instance. You can use the historical data search to conduct custom searches, investigate your search results and event data, and act on your findings
  Documentation

Manage, load, and schedule saved search queries

- Display saved queries by clicking the icon next to search and selecting “Browse saved queries”:
  Documentation
- Scheduling a query enables it to be run automatically at set times and days, and the results are sent to one or more email addresses:
  Documentation

Walk through reports console

The SEM reports application converts SEM database data into information you can use to troubleshoot and identify network problems. Run reports on your Security Event Manager database to view events and trends and make informed decisions about your network activity. You can run over 200 standard and industry-specific reports to help you make informed decisions about your network security.

Documentation

Walk through the database maintenance report

The SEM database maintenance report shows a snapshot of your current database utilization. This report can give you log retention in GB and days.
Documentation

Use the select expert tool to create a more focused SEM report

The select expert tool lets you execute queries to create a smaller, more focused report from a larger text-based report.

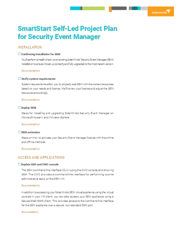
You can use this tool when viewing the text-based view of a report in the preview frame. You can't use this tool with the default graphical view displayed when you first run the report.
Documentation

UPGRADE SEM

Upgrade SEM

A new version of SEM may come out during our time together, and if possible, we'll upgrade SEM during the SmartStart Engagement.
Documentation

Documents / Resources

 SmartStart Self-Led Project Plan for Security Event Manager INSTALLATION □ Confirming Installation for SEM You'll perform a health check on an existing SolarWinds' Security Event Manager (SEM) installation to ensure it's set up correctly and fully upgraded to the most recent version. Documentation □ Verify system requirements System requirements allow you to properly size SEM with the correct resources based on your needs and license. We'll review your license and adjust the SEM resources accordingly. Documentation □ Deploy SEM Steps for installing and upgrading SolarWinds Security Event Manager on Microsoft Hyper-V and VMware vSphere. Documentation □ SEM activation Steps on how to activate your Security Event Manager license with the online and offline methods. Documentation ACCESS AND APPLICATIONS □ Explain SSH and CMC console The SEM command-line interface (CLI)—using the CMC console and showing SSH. The CMC provides a command-line interface for performing routine administrative tasks on the SEM VM. Documentation In addition to accessing your SolarWinds SEM virtual appliance using the virtual console in your VM client, you can also access your SEM appliance using a Secure Shell (SSH) client. This provides access to the command-line interface for the SEM appliance over a secure, non-standard SSH port. Documentation	solarwinds SmartStart Self-Led Project Plan for Security Event Manager [pdf] Instruction Manual SmartStart Self-Led Project Plan for Security Event Manager, Self-Led Project Plan for Security Event Manager, Project Plan for Security Event Manager, Security Event Manager