SolarWinds Partner Training

Security Event Manager - Participant's Guide

Table of Contents

Architecture and Configuration

SolarWinds® Security Event Manager (formerly Log & Event Manager) is a security information and event management (SIEM) virtual appliance designed to add value to existing security products and increase efficiencies in administering, managing, and monitoring security policies and safeguards on your network.

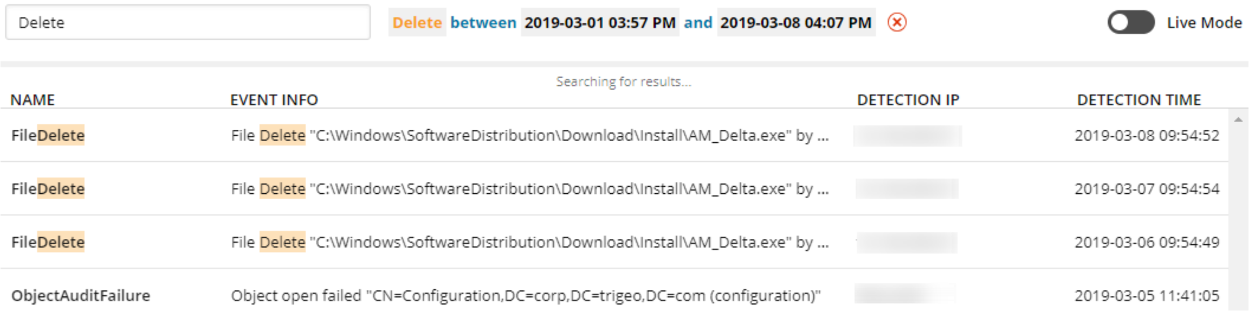
- To learn more, please visit these links:
  - https://documentation.solarwinds.com/en/success_center/SEM/Content/Install_Guide/install-prep/how-SEM-works.htm
  - https://documentation.solarwinds.com/en/success_center/LEM/Content/Admin_Guide/1.0-understanding_sem/SEM-Component-Overview.htm

Managing Nodes and Connectors

Adding Nodes and creating the appropriate Connectors are required steps for your SEM receiving data to perform any of its other functions. Nodes and Connectors can be managed under the Nodes tab of the web console.

- To learn more about this, please visit these links:
  - https://documentation.solarwinds.com/en/Success_Center/SEM/Content/Admin_Guide/New_In_6_6/SEM-node-management.htm
  - https://documentation.solarwinds.com/en/Success_Center/SEM/Content/Admin_Guide/5-add_syslog_and_agent_nodes/sem-managing-connectors.htm

Using Events Search, nDepth, and the Reports Application



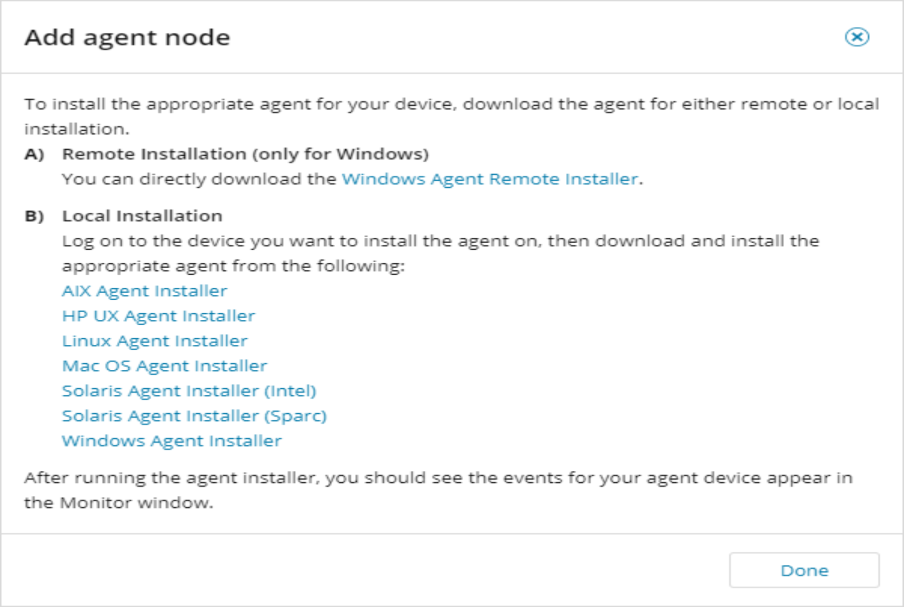
NAME	EVENT INFO	DETECTION IP	DETECTION TIME
FileDelete	File Delete "C:\Windows\SoftwareDistribution\Download\Install\AM_Delta.exe" by ...	[redacted]	2019-03-08 09:54:52
FileDelete	File Delete "C:\Windows\SoftwareDistribution\Download\Install\AM_Delta.exe" by ...	[redacted]	2019-03-07 09:54:54
FileDelete	File Delete "C:\Windows\SoftwareDistribution\Download\Install\AM_Delta.exe" by ...	[redacted]	2019-03-06 09:54:49
ObjectAuditFailure	Object open failed "CN=Configuration,DC=corp,DC=trigeo,DC=com (configuration)"	[redacted]	2019-03-05 11:41:05

There are multiple ways to search the database and retrieve events stored within it. Specifically, we have the Events search for basic keyword queries, nDepth for more complicated queries that may include groups or multiple conditions, and the Reports application to generate predefined reports for compliance and auditing purposes.

- To learn more, please visit these links:
  - https://documentation.solarwinds.com/en/Success_Center/SEM/Content/Admin_Guide/New_In_6_4/SEM-Search-Filter-Historical-Records.htm
  - https://documentation.solarwinds.com/en/Success_Center/SEM/Content/Admin_Guide/11-sem_ndepth/chapter-head-explore-ndepth.htm
  - https://documentation.solarwinds.com/en/Success_Center/SEM/Content/Admin_Guide/12-sem_reports/reports.htm

Deploying Agents, File Integrity Monitoring, and USB Defender

- Deploying Agents



Add agent node

To install the appropriate agent for your device, download the agent for either remote or local installation.

A) **Remote Installation (only for Windows)**
You can directly download the Windows Agent Remote Installer.

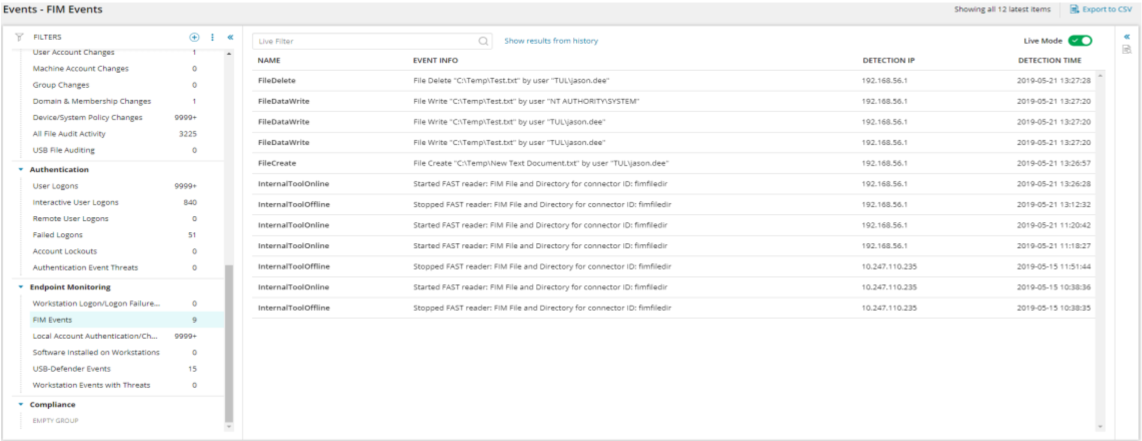
B) **Local Installation**
Log on to the device you want to install the agent on, then download and install the appropriate agent from the following:
AIX Agent Installer
HP UX Agent Installer
Linux Agent Installer
Mac OS Agent Installer
Solaris Agent Installer (Intel)
Solaris Agent Installer (Sparc)
Windows Agent Installer

After running the agent installer, you should see the events for your agent device appear in the Monitor window.

Agents can be downloaded directly from the web console or from the SEM download section of the Customer Portal. You then have multiple options to deploy the agents in your environment.

- To learn more, please visit this link:
  - https://documentation.solarwinds.com/en/Success_Center/SEM/Content/Admin_Guide/4-deploy_sem_agents/sem-agent-install-overview.htm

- ## Windows File Integrity Monitoring



Events - FIM Events

Showing all 12 latest items | Export to CSV

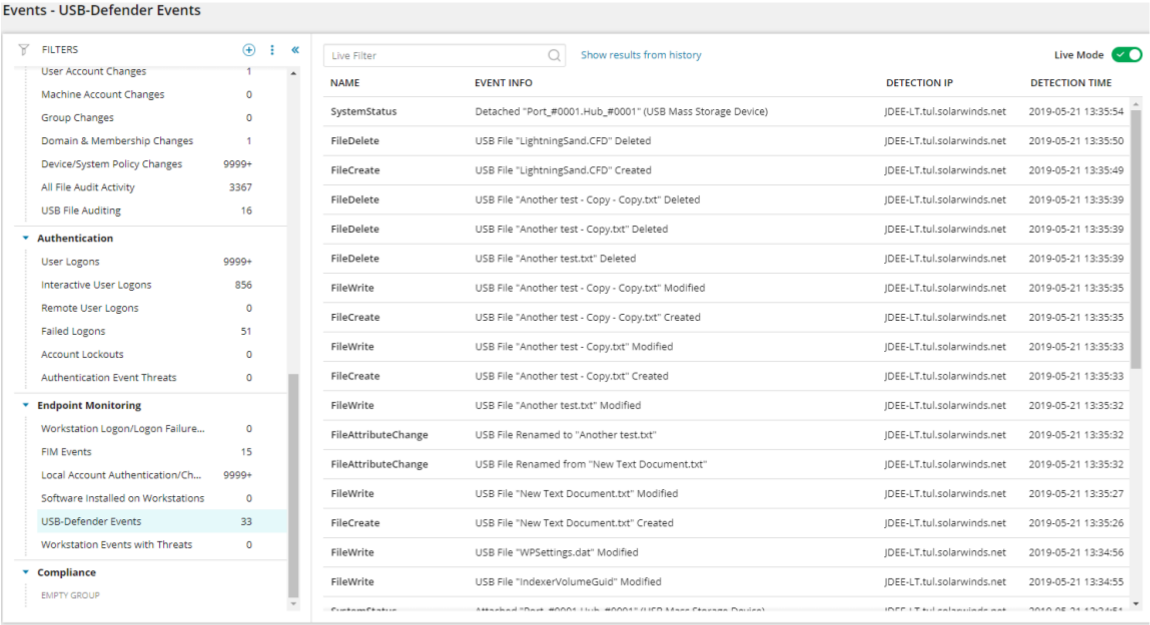
User Account Changes	1
Machine Account Changes	0
Group Changes	0
Domain & Membership Changes	1
Device/System Policy Changes	9999+
All File Audit Activity	3225
USB File Auditing	0
Authentication	
User Logons	9999+
Interactive User Logons	840
Remote User Logons	0
Failed Logons	51
Account Lockouts	0
Authentication Event Threats	0
Endpoint Monitoring	
Workstation Logon/Logon Failure...	0
FIM Events	9
Local Account Authentication/Ch...	9999+
Software Installed on Workstations	0
USB-Defender Events	15
Workstation Events with Threats	0
Compliance	
EMPTY GROUP	

NAME	EVENT INFO	DETECTION IP	DETECTION TIME
FileDelete	File Delete "C:\Temp\Test.txt" by user "TUL\jason.dee"	192.168.56.1	2019-05-21 13:27:28
FileDataWrite	File Write "C:\Temp\Test.txt" by user "NT AUTHORITY\SYSTEM"	192.168.56.1	2019-05-21 13:27:20
FileDataWrite	File Write "C:\Temp\Test.txt" by user "TUL\jason.dee"	192.168.56.1	2019-05-21 13:27:20
FileDataWrite	File Write "C:\Temp\Test.txt" by user "TUL\jason.dee"	192.168.56.1	2019-05-21 13:27:20
FileCreate	File Create "C:\Temp\New Text Document.txt" by user "TUL\jason.dee"	192.168.56.1	2019-05-21 13:26:57
InternalToolOnline	Started FAST reader: FIM File and Directory for connector ID: fimfiledir	192.168.56.1	2019-05-21 13:26:28
InternalToolOffline	Stopped FAST reader: FIM File and Directory for connector ID: fimfiledir	192.168.56.1	2019-05-21 13:12:32
InternalToolOnline	Started FAST reader: FIM File and Directory for connector ID: fimfiledir	192.168.56.1	2019-05-21 11:20:42
InternalToolOnline	Started FAST reader: FIM File and Directory for connector ID: fimfiledir	192.168.56.1	2019-05-21 11:18:27
InternalToolOffline	Stopped FAST reader: FIM File and Directory for connector ID: fimfiledir	10.247.110.235	2019-05-15 11:51:44
InternalToolOnline	Started FAST reader: FIM File and Directory for connector ID: fimfiledir	10.247.110.235	2019-05-15 10:38:36
InternalToolOffline	Stopped FAST reader: FIM File and Directory for connector ID: fimfiledir	10.247.110.235	2019-05-15 10:38:35

  - Windows® File Integrity Monitoring increases SIEM intelligence with policy-based auditing of file and registry activity including "reads," "writes," and "deletes." FIM can help you demonstrate compliance of regulations including PCI DSS, HIPAA, and Sarbanes-Oxley, as well as help increase security intelligence to detect insider abuse, zero malware, and advanced persistent threats.

- To learn more, please visit this link:
  - https://documentation.solarwinds.com/en/Success_Center/LEM/Content/Admin_Guide/6.1-configure-lem-to-monitor/lem-file-integrity-monitoring-connectors.htm

- ## USB Defender



Events - USB-Defender Events

User Account Changes	1
Machine Account Changes	0
Group Changes	0
Domain & Membership Changes	1
Device/System Policy Changes	9999+
All File Audit Activity	3367
USB File Auditing	16
Authentication	
User Logons	9999+
Interactive User Logons	856
Remote User Logons	0
Failed Logons	51
Account Lockouts	0
Authentication Event Threats	0
Endpoint Monitoring	
Workstation Logon/Logon Failure...	0
FIM Events	15
Local Account Authentication/Ch...	9999+
Software Installed on Workstations	0
USB-Defender Events	33
Workstation Events with Threats	0
Compliance	
EMPTY GROUP	

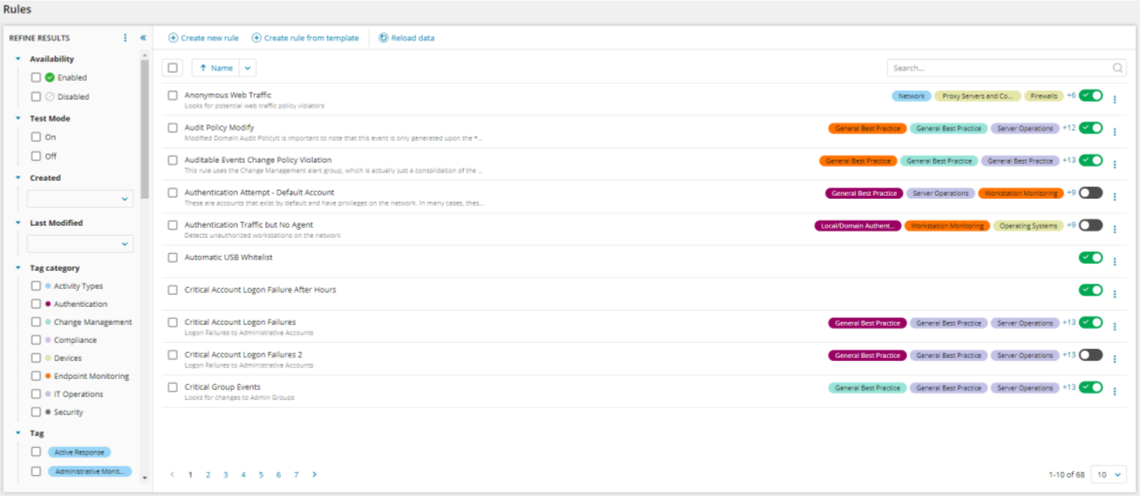
NAME	EVENT INFO	DETECTION IP	DETECTION TIME
SystemStatus	Detached "Port_#0001.Hub_#0001" (USB Mass Storage Device)	JDEE-LT.tul.solarwinds.net	2019-05-21 13:35:54
FileDelete	USB File "LightningSand.CFD" Deleted	JDEE-LT.tul.solarwinds.net	2019-05-21 13:35:50
FileCreate	USB File "LightningSand.CFD" Created	JDEE-LT.tul.solarwinds.net	2019-05-21 13:35:49
FileDelete	USB File "Another test - Copy - Copy.txt" Deleted	JDEE-LT.tul.solarwinds.net	2019-05-21 13:35:39
FileDelete	USB File "Another test - Copy.txt" Deleted	JDEE-LT.tul.solarwinds.net	2019-05-21 13:35:39
FileDelete	USB File "Another test.txt" Deleted	JDEE-LT.tul.solarwinds.net	2019-05-21 13:35:39
FileWrite	USB File "Another test - Copy - Copy.txt" Modified	JDEE-LT.tul.solarwinds.net	2019-05-21 13:35:35
FileCreate	USB File "Another test - Copy - Copy.txt" Created	JDEE-LT.tul.solarwinds.net	2019-05-21 13:35:35
FileWrite	USB File "Another test - Copy.txt" Modified	JDEE-LT.tul.solarwinds.net	2019-05-21 13:35:33
FileCreate	USB File "Another test - Copy.txt" Created	JDEE-LT.tul.solarwinds.net	2019-05-21 13:35:33
FileWrite	USB File "Another test.txt" Modified	JDEE-LT.tul.solarwinds.net	2019-05-21 13:35:32
FileAttributeChange	USB File Renamed to "Another test.txt"	JDEE-LT.tul.solarwinds.net	2019-05-21 13:35:32
FileAttributeChange	USB File Renamed from "New Text Document.txt"	JDEE-LT.tul.solarwinds.net	2019-05-21 13:35:32
FileWrite	USB File "New Text Document.txt" Modified	JDEE-LT.tul.solarwinds.net	2019-05-21 13:35:27
FileCreate	USB File "New Text Document.txt" Created	JDEE-LT.tul.solarwinds.net	2019-05-21 13:35:26
FileWrite	USB File "WPSettings.dat" Modified	JDEE-LT.tul.solarwinds.net	2019-05-21 13:34:56
FileWrite	USB File "IndexerVolumeGuid" Modified	JDEE-LT.tul.solarwinds.net	2019-05-21 13:34:55
SystemStatus	Attached "Port_#0001.Hub_#0001" (USB Mass Storage Device)	JDEE-LT.tul.solarwinds.net	2019-05-21 13:34:51

  - USB Defender® writes events to the Windows Application Log for parsing via the Windows Application connector and use with the USB Defender Local Policy (UDLP) connector. Within the Application Log event, there is additional detail that isn't normalized and sent to SEM but can be used with the UDLP whitelist file to create more complex comparisons and more restrictive policy.

- The USB Defender Local Policy (UDLP) connector enables a SEM Agent to enforce restrictions on USB devices, even when the Agent is not connected to the SEM Manager. Instead of using rules when disconnected, the connector uses a list of permitted users or devices. The Agent compares the fields in all USB device-attached events to a locally stored whitelist of users or devices. If none of the fields match an entry on the list, the Agent detaches the device.
- USB Defender automatically detects changes to the whitelist file and reloads it when the manager distributes updated data to the agent. The USB Defender service does not need to restart.

- To learn more, please visit these links:
  - https://documentation.solarwinds.com/en/Success_Center/SEM/Content/Admin_Guide/9-sem_response_actions/sem-detach-usb-active-response.htm
  - https://documentation.solarwinds.com/en/Success_Center/SEM/Content/Admin_Guide/New_in_6_7/sem-configure-usb-defender-local-policy-connector.htm

Building Rules and Using Automated Actions



□ Anonymous Web Traffic Looks for potential web traffic policy violators	Network · Proxy Servers and Co... · Firewalls +6	✓
□ Audit Policy Modify Modified Domain Audit PolicyIt is important to note that this event is only generated upon the *...	General Best Practice · General Best Practice · Server Operations +12	✓
□ Auditable Events Change Policy Violation This rule uses the Change Management alert group, which is actually just a consolidation of the ...	General Best Practice · General Best Practice · General Best Practice +13	✓
□ Authentication Attempt - Default Account These are accounts that exist by default and have privileges on the network. In many cases, thes...	General Best Practice · Server Operations · Workstation Monitoring +9	○
□ Authentication Traffic but No Agent Detects unauthorized workstations on the network	Local/Domain Authent... · Workstation Monitoring · Operating Systems +9	○
□ Automatic USB Whitelist		✓
□ Critical Account Logon Failure After Hours		✓
□ Critical Account Logon Failures Logon Failures to Administrative Accounts	General Best Practice · General Best Practice · Server Operations +13	✓
□ Critical Account Logon Failures 2 Logon Failures to Administrative Accounts	General Best Practice · General Best Practice · Server Operations +13	○
□ Critical Group Events Looks for changes to Admin Groups	General Best Practice · General Best Practice · Server Operations +13	✓

SEM Rules allow you to receive immediate notification or immediately execute automated actions on the event criteria you specify. Some actions can send commands back to your Windows machines or network devices via the use of Active Response Connectors.

- To learn more, please visit these links:
  - https://documentation.solarwinds.com/en/Success_Center/LEM/Content/Admin_Guide/10-lem_rules/lem-rules.htm
  - https://documentation.solarwinds.com/en/Success_Center/SEM/Content/Admin_Guide/New_in_6_7/SEM-Configure-active-response-connector.htm

Managing Groups

There are multiple types of groups contained in SEM that can be used in your nDepth or Rules for more advanced or more easily managed queries.

- To learn more, please visit these links:

- https://documentation.solarwinds.com/en/Success_Center/SEM/Content/Admin_Guide/6.5-sem_groups/sem-groups-view-features.htm
- https://documentation.solarwinds.com/en/Success_Center/SEM/Content/Admin_Guide/6.5-sem_groups/sem-configuring-user-defined-groups.htm

SEM System Requirements

Use the following tables to plan your Security Event Manager deployment to suit your network environment. Server sizing is affected by:

- The number of nodes and network traffic. Consider event throughput and performance degradation when planning the size of your deployment. As the number of nodes and network traffic increase, the size of your deployment will need to grow with it. For example, if you are running a small deployment and notice performance degradation at 300 nodes, move to a medium implementation.
- You are storing original (raw) log messages in addition to normalized log messages. If you'll be saving unique log messages, increase the CPU and memory resource requirements by 50%. See your hypervisor documentation for more information.

SEM Deployments

- Small Deployment

					Per Day	
Maximum Nodes	Set Up Combinations (Devices)		Minimum HW Requirements		Received Events	Triggered Rules
Up to 500	Security	5 to 10	Processor	2 – 4 cores 2.0 GHz or faster	Up to 35 Million	Up to 500
	Network (w/ or w/o workstations)	10 to 250	Memory	8 GB		
	Servers	30 to 150	HD Space	250 GB with 40 – 200 IOPS		
			Network	1 GBE NIC		

- Medium Deployment

					Per Day	
Maximum Nodes	Set Up Combinations (Devices)		Minimum HW Requirements		Received Events	Triggered Rules
300 up to 2,000	Security	10 to 25	Processor	6 – 10 cores 2.0 GHz or faster	30 to 50 Million	Up to 1,000
	Network (w/ or w/o workstations)	10 to 250		16 to 48 GB RAM		

			Memory	1 TB hard drive with 200 – 400 IOPS		
	Servers	30 to 150	HD Space	1 GBE NIC		
			Network	6 – 10 cores 2.0 GHz or faster		

- Large Deployment

					Per Day	
Maximum Nodes	Set Up Combinations (Devices)		Minimum HW Requirements		Received Events	Triggered Rules
More than 1,000	Security	10 to 25	Processor	10 – 16 core processors at 2.0 GHz	200 to 400 Million	Up to 5,000
	Network (w/ or w/o workstations)	250 to 1,000		48 GB RAM or more		
			Memory	2 TB hard drive with 400 or more IOPS		
	Servers	500 to 1,000	HD Space	1 GBE NIC		
			Network	10 – 16 core processors at 2.0 GHz		

- For more information about sizing criteria, VM hardware requirements, SEM software requirements, SEM agent hardware and software requirements, and SEM reports application hardware and software requirements, visit:
  - https://documentation.solarwinds.com/en/success_center/SEM/content/System_Requirements/SEM_6-6_system_requirements.htm
  - https://documentation.solarwinds.com/en/Success_Center/LEM/Content/Admin_Guide/2-lem_set-up_config_maintenance/lem-configure-log-message-storage-ndepth-search.htm

SEM Installation Guide

- For complete information on how to install SEM, please visit:
  - https://documentation.solarwinds.com/en/Success_Center/SEM/Content/SEM_Installation_Guide.htm

SolarWinds SEM Port and Firewall Requirements

Any firewalls standing between any two points of communication should allow inbound or outbound traffic across the specified ports to ensure that SEM works properly.

In the table, "inbound" assumes the SEM VM is behind the firewall, and firewall rules allow network traffic through the firewall to the SEM VM.

- To learn more, please visit this link
  - https://support.solarwinds.com/SuccessCenter/s/article/SolarWinds-SEM-Port-and-Firewall-Requirement

Allocate CPU and Memory Resources to the SEM

By default, SEM deploys with 8GB of RAM and 2 CPUs on the VMware ESX(i) and Microsoft Hyper-V platforms. For SEM to work properly, you must allocate enough CPU and memory resources to the SEM VM.

- To learn more, please visit this link:
  - https://documentation.solarwinds.com/en/success_center/SEM/content/Admin_Guide/2-SEM_set-up_config_maintenance/allocate-cpu-and-memory.htm

Audit Policies and Best Practices for SEM

Windows Audit Policy determines the verbosity of Windows Security Logs on domain controllers and other computers on the domain. The recommendations in this document have been found to be most effective from both a best practice and compliance standpoint and are based on customer experience and recommendations from Microsoft.

- To learn more, please visit this link:
  - https://support.solarwinds.com/SuccessCenter/s/article/Audit-Policies-and-Best-Practices-for-SEM