# Table of Contents

## INTRODUCTION

4

## BEFORE YOU GET STARTED

5

- Configuring a Static IP Address
- Verify Time Zone, Date and Time Settings
- Configure Email Server & Active Directory Integration

## LEM ARCHITECTURE

9

- Protocols and Communication Direction

## LEM CONFIGURATION

11

- Servers & Applications
  - Getting Started Wizard
  - Benefits of LEM Agent
  - Configuration of LEM Agents
  - What is a Connector?
  - Monitoring Applications
- File Integrity Monitoring
  - Features of FIM
  - What can FIM detect?
  - Setting up FIM
- Network Device Monitoring
  - Understanding the Syslog Server on LEM Manager
  - LEM Connectors – Automatic discovery and configuration
  - LEM Connector – Manual configuration
  - LEM Connectors – Important note for Syslog sources
  - Understanding Filters
## Table of Contents

Filter Creation______________________________________________28
More on Filter Conditions____________________________________31
Using Filters for Historical Search____________________________32
Using Filters for Watching Trends____________________________32
Introduction to LEM Active Response Technology______________32
Understanding Correlation Rules______________________________34
Activating Pre-Defined Rules______________________________35
Custom Rules____________________________________________36
Historical Search - nDepth Explorer____________________________38
  Interacting with the nDepth explorer________________________39
  Saving Search Results______________________________________42
LEM Reports – Security, Compliance and Operations Reporting____43
  Select Expert____________________________________________45
  Running Multiple Reports & Compliance Templates_____________46

### ADVANCED DEPLOYMENT SCENARIO________________________________47

  Using Kiwi Syslog Server as a detached Syslog Server___________48
Introduction

This guide is intended to guide you through a typical LEM evaluation once the LEM Manager has been deployed. The instructions to deploy the LEM Virtual Appliance is outlined in the LEM Quick Start Guide. These instructions are also available as short videos for both Hyper-V and VMware vSphere virtual infrastructures.

While we are on the topic of videos, please visit our LEM YouTube Playlist which contains brief videos which walk through topics such as Deploying LEM, Configuring Nodes, Analyzing Logs and many more.

The LEM Architecture section (page 9) of this document provides a high level overview of the LEM architecture. It is highly recommended that you read this section before you start configuring your network devices to send logs to LEM.
Before you get started

Figure 1 LEM Manager - CMC console

Tip: LEM allows various administrative interactions through LEM commands. These commands can be run either from the VM console using a Hypervisor client such as vSphere client, or from an SSH session using a tool such as Putty. The relevant information to connect via SSH is summarized below.

» SSH Port: 32022
» Login: cmc
» Password: password

CONFIGURING A STATIC IP ADDRESS

We recommend configuring a Static IP Address as soon as you deploy the LEM appliance. Firstly, you need to log into your LEM virtual appliance either using SSH (as above) or via the 'console' view in vSphere/Hyper-V.

At the cmc> prompt type 'appliance' and press enter.

At the acm# prompt type 'netconfig' & press enter to configure the network parameters.

Type ‘static’ and then follow the on-screen prompts to enter IP, subnet, gateway, domain & DNS details.
You can then access the LEM Web Console using the static IP address you have set.

Please refer to this video to walk you through the steps listed above: How to Power On and Assign an IP in LEM

**VERIFY TIME ZONE, DATE AND TIME SETTINGS**

There are 2 things to ensure before getting started

1. Ensure that the Time Zone and the System Time on the LEM Manager are accurate. This can be done using the LEM commands `appliance > tzconfig` and `appliance > dateconfig` as shown below.
2. Ensure that the Hypervisor time is accurate. This can be done using the output of the LEM command `manager > viewsysinfo`. Use the spacebar to scroll down in the output until you find the Hypervisor Time and Guest Time values as shown below. Correct the Hypervisor time if it’s not accurate. This is required because the LEM VM is configured to synchronize with the Hypervisor time by default.

```
Virtualization Platform: VMware
Clock
Synchronization : Enabled
Hypervisor Time : 26 Feb 2015 09:07:31
Guest Time : Thu Feb 26 09:07:31 2015
```

**CONFIGURE EMAIL SERVER & ACTIVE DIRECTORY INTEGRATION**

LEM includes a Getting Started Widget within the Ops Center that allows you to easily configure basic setting such as e-mail server settings & AD Integration.

Simply select the ‘Configure Basic LEM Settings’ from the Getting Started Widget:

You can then input the appropriate e-mail server settings on the next screen:
The next step involves configuring LEM to connect to Active Directory. This allows you to use AD credentials to login to LEM and also use LEM to alert you to changes in your AD groups or to monitor AD accounts.
LEM Architecture

LEM’s architecture is uniquely designed for gathering and correlating logs and events in real-time at network speed, and further defend the network using LEM’s Active Response Technology. Figure 2 below illustrates the typical log sources and LEM software components. It also illustrates the direction in which communication is initiated and the network protocols used.

The LEM Manager is a result of the Virtual Appliance that was deployed. The LEM Manager comprises of the following key components:

» Syslog Server

» High compression, search optimized Database

» Web Server

» Correlation Engine

» Hardened Linux OS

For Network Device log sources such as routers, firewalls, and switches, LEM predominantly relies on these devices sending Syslog messages to the Syslog server running on the LEM Manager (If your change management process does not permit adding any further Syslog servers to the network device configurations, refer to the section “Advanced Deployment Scenario” to leverage your existing Syslog Servers)
For **Servers and Applications** running on these servers, LEM largely relies on a LEM Agent installed on these servers. The LEM Agent has a negligible footprint on the server itself, and provides a number of benefits to ensure logs aren’t tampered during collection or transmission while being extremely bandwidth friendly.

For **Workstations**, LEM Agent used on Windows workstations is the same as the one used for Windows servers.

Other SolarWinds solutions like Network Performance Monitor (**NPM**), Server & Application Monitor (**SAM**) and Virtualization Manager (**VMan**) can send performance alerts as SNMP Traps to LEM. LEM can correlate these performance alerts with LEM events.

Finally, **LEM Reports Console** can be installed on any number of servers to schedule the execution of over 300 audit proven reports. From a security standpoint, the command `service restrictreports` can be used to limit the IPs that can run these reports. In evaluation mode, LEM Reports can be installed any server / workstation that can access port 9001 of the LEM Manager.

**PROTOCOLS AND COMMUNICATION DIRECTION**

Below is a quick summary of the protocols and communication direction illustrated in **Figure 2**.

» Network devices can send Syslog’s to LEM Manager over TCP or UDP. The direction of this communication is obviously from the network device to the LEM Manager.

» LEM Agents installed on servers and workstations initiate TCP connections to the LEM Manager. So, the Agents push data to the LEM Manager.

» If your log sources that are behind firewalls, refer to this **KB article** to open up the necessary ports.

LEM’s architecture has been designed with security in mind. Refer to this **KB article** for a high level overview of LEM’s many security features for collection, transmission and storage of log data.

**Note:** For the purpose of this document, a typical evaluation scenario is discussed. LEM does use other collection mechanisms such as Web Services, SNMP Traps, etc. Please contact your Account Manager to arrange a technical discussion with an engineer if you the log sources discussed aren’t typical in your environment. LEM’s list of data sources is ever growing, and **800+ sources** listed on the web site is representative and by no means exhaustive.
LEM Configuration

This section provides detailed examples of configuring typical log sources for LEM.

SERVERS & APPLICATIONS

Getting Started Wizard

The easiest way to start understanding the power of LEM is to install an Agent on a Windows server. From the Getting Started Widget within the Ops Center, select ‘Add Nodes to Monitor’. From here you can select the type of node you wish to monitor and the download links to the appropriate agent will be provided, as seen in the following screenshot.

Alternatively, you may download the appropriate agent from the following links:

» Windows Agent Installer
» Windows Remote Agent Installer
» Linux Agent Installer (32-bit)
» Linux Agent Installer (64-bit)
Benefits of LEM Agent

The LEM Agent is the primary means used for data collection from servers, applications and workstations. LEM Agents have a number of security benefits such as

» Capturing the events in **real-time**

» **Encrypting** and **compressing** the data to LEM Manager for efficient & secure transmission

» **Buffering** the events locally if network connectivity is lost to the LEM Manager

» Pro-active network defense by using LEM's 'Active Response' technology. The 'Active Response' Technology is discussed further down in the 'Filters' and 'Rules' section of the document

» Please refer to the Audit Policy and Best Practice KB article in order to confirm logging levels are set correctly on your servers and to ensure you are getting the most out of the LEM Agent. You may also refer to this KB article for more details about the LEM Agent itself.

Configuration of LEM Agents

Once the Agent is installed, the server or workstation node should be licensed as a LEM Node straightaway, and can be seen in the MANAGE>Nodes view of the web console. The Status must remain **Connected** as shown in **Figure 3**.

![Figure 3 LEM Agent Node Status](image)

**KB3611** has troubleshooting tips in the unlikely event that the Agent doesn’t get licensed automatically.
The default LEM Agent configuration collects events from **Windows System**, **Application** and **Security** logs. To generate a LEM Event, restart a Windows service that no impact on other applications. Generally, ‘Print Spooler’ service shown below is a great candidate for this test.

![Print Spooler windows service](image)

In the LEM Web console, click on the MONITOR view. This is the real-time view of all the normalized LEM events. This will instantly display 2 normalized LEM Events – **ServiceStart** and **ServiceStop** as highlighted in Figure 5.

![Normalized LEM Events](image)

Click on the **ServiceStart** or the **ServiceStop** event to view the Event Details, i.e., the normalized fields relevant to the specific event. The screenshot below highlights the fields **DetectionTime**, **ToolAlias**, **ProviderSID**, **ServiceName** and **StartMessage** of a ServiceStart event.

![Event Field of a Normalized LEM Event](image)
The Connectors enabled on the LEM Agent or LEM Manager are responsible for normalizing the original log message content to a LEM Event. Figure 7 shows the “friendly” view of the same event in Windows Event Viewer, and the extracted pieces of information from the original event for the ServiceStart event.

What is a Connector?

For the ‘Print Spooler’ service example, the ‘Windows System’ Connector enabled on the LEM Agent was responsible for mapping events from the Windows System event log to a LEM Normalized Event. The list of enabled Connectors can be seen from the Gear icon of the node (MANAGE > Nodes > for Node > Connectors)
One of the fundamental design premises for LEM is to enable users to make sense of millions of logs without having to learn programming or complex regular expressions. In essence, a LEM Connector is responsible for normalizing an original log message. For example, a **UserLogon** normalized event is generated whether a user logs in successfully on a server or router or a switch. A user logon event is a user logon event from a LEM perspective.

LEM Connectors is the foundation for enabling this ‘point and click’ intelligence as you will learn with LEM Rules further ahead in this document.

### Monitoring Applications

Now that a LEM Agent has been setup, and LEM Connector design has been understood, you can proceed to instruct LEM Agent to monitor additional applications or configure the servers to log additional security information. Active Directory log monitoring and File Auditing are great next steps. The process to monitor other applications like IIS, DHCP, DNS, etc. is simply a matter of enabling the appropriate connectors similar to the steps described below for Active Directory.

**Active Directory**

Active Directory is the most widely used authentication mechanism, and hence central to maintain any sort of audit trail related to authorized access and change management. Install the LEM Agent on your AD/Domain Controllers to track failed user logons, successful logons, password changes/resets, account lockouts, group changes and many more authentication and change management events. Simply enable the ‘Windows Directory Service Log’ Connector on the Windows node as shown below.

![Active Directory Connector](Figure 10 Active Directory Connector)
**Databases**  
LEM has the ability to audit database activity on many platforms including Oracle & MS SQL.

To configure SQL log monitoring, you will need to install the LEM agent on the SQL server. You also require LEM’s SQL Auditor to be installed. Please see here for configuration instructions - [Configuring MSSQL Auditor on a LEM Agent](#).

With regards to Oracle, LEM can receive logs from Oracle on Windows and UNIX platforms. Please see here for configuration instructions - [Integrating your Oracle database with SolarWinds LEM](#).

**Work Stations**  
LEM can process logs from Windows workstations. By installing the LEM agent on workstations, it can greatly increase visibility into user activity and can complement your existing endpoint protection strategy. Some useful information can be captured from workstations including launching of prohibited applications, software installation, Windows critical, error and warning events, local file auditing, local user logons, USB device activity and more. The agent will also allow us to perform active responses on workstations such as killing suspicious processes, detaching USB devices and sending pop up messages to users.

Thanks to LEM Workstation Edition add-on license, monitoring workstation logs is very cost-effective & affordable.

For more information on LEM Workstation Edition, please see [Why & How of Workstation Monitoring with LEM](#).

**FILE INTEGRITY MONITORING**  
File Integrity Monitoring (FIM) provides the ability to monitor, track and audit files of all types for unauthorized changes that may lead to a data breach by a malicious attack. Using FIM, you can detect changes to critical files and registry keys, both to ensure systems are free of compromise & to ensure critical data is not being changed by unauthorized modifications of systems, configurations, executables, log and audit files, content files, databases & web files. If FIM detects a change in a file you are monitoring, it is logged. LEM then takes those logs and performs the configured action. Correlation rules can be built to act as a second-level filter to only actively send an alert to certain patterns of activity (not just single instances), and when an alert is triggered, the data is in context with your network and other system log data with a SIEM like LEM, you can also respond with administrative action.
Features of FIM


» Allows you to configure the logic of files/directories and registry keys/values to monitor for different types of access (create, write, delete, change permissions/metadata).

» Provides the ability to standardize configurations across many systems.

» Provides monitoring templates which can be used to monitor the basics. Also allows the option of creating & customizing your own monitors.

» Provides templates for rules, filters & reports to assist in including FIM events quickly.

What can FIM detect?

» Insider abuse by auditing files directly through intelligent correlation rules. Integration with AD settings can disable accounts & change user/group rights.

» If a critical registry key is changed. For example a new service is installed, software is installed, a key gets added to ‘hide’ data in an unexpected area.

» If a new driver or similar device is installed. Adds a layer of defense to anti-virus software for detecting viruses that mask as ‘similarly’ named files.

» If critical business files are accessed & who is accessing them. Detects potential abuse, unexpected access or changes to sensitive data.

» If files are moved. Usually when users move directories into other directories.

» Zero-day exploits, which is an attack that takes advantage of security vulnerabilities, the same day the vulnerability becomes known. FIM can trigger an alert letting you know there has been a file change by a potential malware or Trojan & can automatically stop the running malware process.

» Advanced Persistent Threats by inserting a granular, file-based auditing into the existing event stream to pinpoint attacks and help block them in progress.
Setting up FIM

1. To add a FIM connector:

2. Navigate to Manage > Nodes to see a listing of all the nodes being monitored by LEM.

3. Select the desired node, then click the gear icon next to it and select Connectors.

4. Enter FIM in the Refine Results pane. The search results in FIM Registry and also FIM Directory and Files.

5. Select either a FIM file and Directory or a FIM Registry.

6. Click the gear icon next to the FIM Connector profile you want to work with, then select New to create a new connector. The Connector Configuration window displays.

7. Select a Monitor from the Monitor Templates pane, and then click the gear icon and select Add to selected monitors. The Monitor Template then moves to the Selected Monitor pane.

8. Click Save if you do not wish to edit the selected Monitor.

9. As seen from the previous screenshot, you can apply one of our out of the box templates or create your own custom monitors. Custom monitors allow you to create sets of conditions, with each condition containing granular configuration or exactly what file system events you’re interested in monitoring. To setup a custom monitor, click on the Add Custom Monitor button from the Connector Configuration window.
Adding Conditions

1. Click Add New.

2. Click Browse to select a File/Directory or Registry to watch.

3. Click OK.

4. Select whether the files are recursive or non-recursive. See below for more information.
   - Recursive: The folder selected and all its sub-folders which match the given mask will be monitored for corresponding selected operations.
   - Non-recursive: Only the files in the selected folders will be monitored.

5. Enter a Mask, for example *exe or directory*.

6. For a FIM File/Directory, select Create, Read, Write, and Delete for Directory, File, Permissions, and Other operations. For a FIM Registry, select Create, Read, Write, and Delete for Key Value and operations. For more information on other, refer to the Microsoft MSDN information.
7. Click Save.

LEM lets you browse the file system of your remote node right from the manager UI making it that much easier to specify directories.

FIM makes full use of templates. You can use ours, add to ours, create your own, share between administrators, and so on. We’ve also extended this FIM logic to the Windows registry.

In LEM, FIM becomes yet another source of data that you can log, analyze, and take action upon. With correlation rules, the more information sources you have the more accurate and decisive your alerts and other automatic responses can be.

Please refer to the following brief video, which walks through the above steps: Configuring File Integrity Monitoring.

**NETWORK DEVICE MONITORING**

Almost every LEM implementation includes log sources from network devices like firewalls, routers and switches. There are a number of good reasons to monitor logs from these devices.

For firewalls, LEM can capture various information from firewall logs including:

» Connections permitted or denied by firewall rules

» User Activity

» Cut-through-proxy activity

» Protocol Usage

» Intrusion detection activity
These can be used to understand if firewall rules and ACLs are working as intended, identify network attacks, security breaches, etc.

For routers and switches, LEM can collect information such as port flapping, Duplex mismatch errors and hardware failures related to fan, power supply, etc.

For information about additional use cases, please see the following document - LEM Use Cases

**Understanding the Syslog Server on LEM Manager**

As mentioned earlier, LEM predominantly uses Syslog to gather logs from network devices such as firewalls, routers and switches. The Syslog Server on the LEM Manager listens on the standard port number 514. The Syslog server saves the logs to the LEM Manager’s file system under the /var/log partition. The filename depends on the target facility configured on the network device. Most network devices allow definition of a facility while defining the syslog server. In Figure 11 below, the Cisco router is logging to the Syslog server on IP 10.130.2.170 and to the local4 facility.

![Figure 11 Syslog Configuration on a Cisco router](image)

The mapping of the Syslog facility to the filenames on LEM Manager are shown below.

<table>
<thead>
<tr>
<th>SYSLOG FACILITY</th>
<th>LOG FILE FOR CONNECTOR CONFIGURATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local0</td>
<td>/var/log/local0.log</td>
</tr>
<tr>
<td>Local1</td>
<td>/var/log/local1.log</td>
</tr>
<tr>
<td>Local2</td>
<td>/var/log/local2.log</td>
</tr>
<tr>
<td>Local3</td>
<td>/var/log/local3.log</td>
</tr>
<tr>
<td>Local4</td>
<td>/var/log/local4.log</td>
</tr>
<tr>
<td>Local5</td>
<td>/var/log/local5.log</td>
</tr>
<tr>
<td>Local6</td>
<td>/var/log/local6.log</td>
</tr>
<tr>
<td>Local7</td>
<td>/var/log/local7.log</td>
</tr>
</tbody>
</table>

LEM Users do not have direct access to the file system since the OS is hardened. The appliance > checklogs command allows users to view the contents of these files. The checklogs command can also be used to verify if the original logs are reaching LEM’s Syslog server. In Figure 12, the checklogs command is showing that there are no network devices logging to facilities local1, local3, local4, local5 and local7 since the file sizes are empty. On the contrary, facilities local0, local2 and local6 are receiving logs from various network devices.
The OS hardening also ensures these original logs are tamper-proof, which is important for complying with many audit and regulatory requirements.

The Connectors defined on the LEM Manager read these original logs to normalize to LEM Events. (If you skipped the section on LEM Agents, refer to the section on ‘What is a Connector?’ to understand about Connectors). LEM Connectors can be enabled manually or automatically. The automatic procedure is discussed first.

**LEM Connectors – Automatic discovery and configuration**

This assumes that the network devices are already configured to send logs via Syslog to LEM Manager. There are two methods of adding syslog nodes, either from the ‘Getting Started’ widget or using ‘Scan Nodes’.

**Getting Started Widget**

From the Ops Center ‘Getting Started’ widget, select ‘Add Nodes to Monitor’:
Next step is to select the ‘Syslog’ option:

This method is used to add a specific node that successfully sends syslog’s to LEM. Simply enter the IP address & the vendor of the log source, click the checkbox ‘I have configured this node so that LEM can receive its syslog messages’ and click next. LEM then scans all the Syslog facilities for messages from the specified source IP. If the messages successfully match the appropriate LEM connectors, the source IP can be added as a LEM node using the appropriate connectors. The IP and the matching connector(s) discovered is shown in Figure 13 below.

If LEM is unable to add a Node using this method, either the logs aren’t reaching LEM at all or LEM hasn’t detected enough messages to determine the Connectors accurately.
Scan for New Nodes
This method is used to scan all Syslog facilities for any new log sources.

Browse to Manage -> Nodes -> Scan for New Nodes

If there are new Nodes found, LEM will display a banner like below

When you click on ‘View now’, the discovery / scan results will be displayed and provide a chance to confirm the connectors you would like to enable as shown in Figure 15.

![Figure 15 'Scan for new Nodes' result](image)

LEM Connector – Manual configuration

All the Connectors that can be defined on the LEM Manager can be found under MANAGE > Appliances > Gear Icon (⚙️) > Connectors as shown below.
You can search for a connector from the categorized list of device types such as Firewalls, Routers, Switches, IDS & IPS and many more. Figure 16 shows the results for searching on the word ‘Cisco’.

![Figure 16 Connector Search](image)

By this time, you would have realized that the Gear icon is your friend. Click on the Gear icon next to the relevant Connector and click on ‘New’

![Figure 17 Syslog Connector definition](image)

This will allow you to apply an instance of this Connector on one of the Syslog files saved on the LEM manager. There are really only 2 specific pieces of information to be provided.

1. **Alias**: This is simply an alias for an instance of the Connector

2. **Log File**: The syslog file on the file system for this Connector instance to read

In the example below, the default Alias of Cisco PIX and IOS has been modified to Cisco Logs, and the Log File has been changed from /var/log/local2.log to /var/log/local4.log. This is because the Cisco devices in this network are configured to log to Facility local4 of the logging host (LEM Manager).
WARNING: Do NOT change the Output from 'Alert' to 'nDepth' or 'Alert, nDepth'. Please speak to a SolarWinds engineer to understand these options. The use cases to enable an 'nDepth' output are few and far between.

![Figure 18 Connector Definition Warning](image)

**Cisco Device Example**

This again assumes that a Cisco device is configured to log to the LEM Manager. If you are not sure which facility the device is logging to, you can always set the facility explicitly. For example, running the command `logging facility local4` will set the facility to local4.

Enable the ‘Cisco PIX and IOS’ Connector on the LEM Manager as per the instructions in the ‘LEM Connector – Manual configuration’ section.

An easy way to generate a LEM Event is to enter the `config terminal` on a Cisco device, and exit with ‘Control Z’, as shown below.

![Figure 19 Cisco device - config terminal](image)

This will result in a PolicyModify event as shown below. As mentioned previously, real-time events are seen in the MONITOR view.

![Figure 20 LEM Event - PolicyModify](image)
In the example below, the PolicyModify event details contain the login used (admin), and also the source machine (10.130.1.124) from which the configuration change was attempted.

**LEM Connector – Manual configuration**

To summarize the process to configure LEM to handle Syslog’s from network device, it is really just a 2 step process:

1. Configure the device to send logs to LEM using Syslog, and to a particular facility (e.g., local0).
2. Configure the appropriate LEM connector to read the logs corresponding to the facility in Step 1. The connector maybe be enabled automatically or manually.

**IMPORTANT**: It is important to note that Step 1 needs to be done for every network device that would send logs to LEM, but Step 2 is done only once per device type. For example, if there are 100 Cisco routers and switches in your network, Step 1 needs to be done on all the devices whereas Step 2 (enabling the Cisco PIX and IOS connector) needs to be done only once as long as all the 100 devices are logging to the same facility on the LEM Manager. The effort involved in Step 1 can be minimized using a bulk configuration change management solution such as SolarWinds Network Configuration Manager.

At this point, LEM should be handling from logs from at least 1 server and 1 network device. You should be familiar with (normalized) LEM events, and the notion of a LEM Connector. The rest of the document will focus on using the dashboard to view, search, correlate and respond to these events.
UNDERSTANDING FILTERS

This section will introduce you to LEM filters, which can be seen in the Filters pane of the MONITOR view as shown in Figure 22. LEM Filters are important for 3 reasons

1. It allows you to watch LEM events of interest in real-time.
2. It allows you to watch trends in the OPS CENTER view
3. It allows you to easily perform historical searches

LEM Filter Groups are simply logical groups of these filters. LEM ships with a default set of Filter Groups and associated Filters. Some of the default Filter Groups are Overview, Security, Compliance, Change Management, and Authentication.

Filter Creation

Double-click on any of the default Filters to view the Filter definition. A Filter definition essentially has 2 parts as shown in Figure 23.

4. Conditions (This is Mandatory)
5. Notifications (This is Optional)
It is very easy drag and drop process to create new filters. The Filter editor is shown in Figure 23 below. A typical LEM filter condition is defined using one or more of the following:

- A LEM Event (Search, Select and Drag an Event from the Event List)
- Fields with an LEM Event (Search, Select an Event and Drag a Field from the Event Fields)
- A LEM Event Group (Select and Drag an Event Group from the Event Groups)
- Fields common to a LEM Event Group (Select an Event Group, and Drag a Field from the Event Group Fields)

The filter condition can include additional advanced items like User-Defined Groups, Connector Profiles, Directory Service Groups, Time of Day Sets, etc.

A new Filter or Filter Group can be created by clicking on the + button in the Filters pane of the MONITOR view as shown in Figure 24 below.

Creating a Custom Filter – Example 1
This example will show how to filter all Windows Service Stop and Start events. In the Filter editor, search for the word ‘service’
And simply drag and drop the LEM Events into the Conditions section of the editor.

This filter matches on **ServiceStart** OR **ServiceStop** events. The screenshot below shows the symbols used for the logical operators (AND, OR) used in the editor, and the logic can be toggled by clicking on these symbols.

This new filter can be created in an existing Filter Group or in a brand new Filter Group. The matching events can then be viewed in real-time in the Event Grid of the MONITOR view.
Creating a Custom Filter – Example 2

This example uses Event Fields in the filtering condition and also defines a Notification. The possible options for Notifications are shown below. This example displays a pop-up message in the console when 3 Logon failures are detected anywhere in the network for the SolarWinds\ Administrator domain account.

In this example, rather than dragging the UserLogonFailure event, drag the fields Destination-Domain and DestinationAccount of the UserLogonFailure event. Please note that both the fields have been dragged into the same condition group, and the AND logical operator is used.

More on Filter Conditions

There are a few handy things to note about Filter Conditions. The UserLogonFailure.DestinationAccount field will be used for as an example for the notes below.

» The filter conditions can also use an asterisk (*) for wildcard matches.
  • Admin* will match true for DestinationAccount of admin, Administrator, and any other account that starts with ‘admin’
  • All matches are case insensitive. UserLogonFailure.DestinationAccount = ad* is equivalent to UserLogonFailure.DestinationAccount = AdMin*

» Click on the = sign to toggle to negate the condition (≠, i.e., not equal to)
If an Event field needs to match or not match on a group of values, it is easier to create a User Defined Group (from MANAGE > Groups) and drag the group into the condition value.

- If the DestinationAccount can be say for instance, ‘administrator, helpdesk-adm, or backup-adm’, then create a User Defined Group for these accounts called ‘Demo Admins Group’ for these accounts.
- The filter condition would look like the screenshot below. Please note the symbol used to match on a User Defined Group.

Using Filters for Historical Search

It is very easy to leverage a LEM filter to perform a historical search. The historical search feature within LEM is called ’nDepth’. Simply click on any of the LEM filters, then the Gear Icon and choose the ‘Send to nDepth’ menu option to search for events matching the chosen Filter historically.

Using Filters for Watching Trends

The various charts with the OPS CENTER view is really just a trend for a specific Filter. It is possible to add more Widgets to this view using default or custom filters.

Introduction to LEM Active Response Technology

It is possible to respond to LEM events directly from the LEM console. There are a variety of active responses to choose from such as – Shutdown a Service, Block an IP, Disable a Domain User, Disable a Local User, etc. Before you can leverage this powerful technology from LEM, you must ensure that the Active Response Connectors are enabled on either the LEM Agent or the LEM Manager. In the example below, the ‘Windows Active Response’ Connector has been enabled on a Windows Agent node.
The Respond menu is available from the All Events pane of the MONITOR view.

To perform a response, simply click on an event and choose ‘All Actions...’ from the Respond menu, then pick the action from the Action drop down. You can then drag and drop the appropriate Event fields. In the screenshot below, the **DetectionIP** and **ServiceName** fields have been dragged into the appropriate fields of the ‘Start Windows Service’ action. Click OK to start the PrintSpooler service from LEM!
UNDERSTANDING CORRELATION RULES

Correlation rules allow you to instantly detect security, operational and compliance issues including external breaches, insider abuse, policy violations, application availability, performance problems and more. LEM comes with over 700 built-in event correlation rules and easy-to-understand categorization. Categories include Authentication, Change Management, Devices (IDS, Firewall, Router, etc.), IT Operations and more. These rules are accessible from the Build > Rules view. LEM performs in-memory correlation on the LEM Manager, which allows it to respond in real-time.

The Rules view above shows all the pre-defined rules in the 'Rules' pane, and the 'Rule Templates' used for these pre-defined rules. The enabled rules are easy to locate from the 'Enabled' column of the Rules pane. The Rule Templates are read-only, and can be Cloned (using the Gear icon next to the Rule Template) to create a custom Rule.

Understanding Rules is not very different from understand Filters. A Rule definition has 3 parts to it, and all of them are mandatory.

1. **Correlations**
2. **Correlation Time**
3. **Actions**

To view the definition of a rule, just click on the Gear icon and click Edit. You are then presented with the following screen which shows the Rule Status (think of it as a spell check for rule creation), the correlations, correlation time and actions that will occur if the rule triggers.
**Activating Pre-Defined Rules**

From the Getting Started widget, select ‘Define Rules and Configure Alerts’

You are then presented with the ‘Show Rules Category’ screen, where you can select the type of rule(s) you wish to enable, e.g. Authentication, IT Operations, Security, Compliance and more.
Simply select a category of rules you wish to enable and click next. In this example we will enable ‘Group Change’ rules, which is included within the Change Management category. Rules included under ‘Group Changes’ rules are displayed, such as Group Created, Machine Added to Group, User Added to Group, OU Deleted and more.

Once you click next, the ‘Rule Settings’ page is then displayed which allows you to configure your e-mail server settings & e-mail recipients.

You can also select e-mail recipients using your existing LEM users, alternatively you can add another user from here also.

Custom Rules

To create a rule from scratch, simply click on the + icon on the top right of the BUILD > Rules view. You then simply use the same drag and drop method you used in the Filters section to define the correlation. The following examples will show how to be alerted or to define an Active Response when a series of Failed Authentication events are detected from your AD servers.
Part 1: Define the Rule Condition

To define the condition below, simply drag the FailedAuthentication event into the Correlations section of the Rule editor. Event Fields, Event Groups, and Event Group Fields can also be used to define Correlations very similar to how Conditions are defined in the Filter Creation section.

Part 2: Define the Correlation Time

The next step would be to define the correlation time, i.e., volume of events that match the Correlations conditions as well as the rolling time window over which the correlation must be evaluated. The ‘Response Window’ setting doesn’t come into play if the time on the LEM manager and all the log sources are in sync. However, if the times are out of sync or if there is a delay in the LEM events reaching the LEM Manager (maybe because of unreliable WAN links, for example), this Window defines the tolerance for which these ‘delayed’ events must still be correlated. In the example shown below, the Correlation so far is on 3 FailedAuthentication Events in a rolling 30 second time window

Depending on the correlation rule, there is also an advanced threshold setting that is very useful to further refine the correlation rule. This is accessible from the Advanced icon in the ‘Correlation Time’ section of the Rule editor.
By clicking on the icon, you can choose a Field from the Events in scope, choose the Same or Distinct correlation criteria, and click on the + sign. So, the rule has now been modified to correlate on ‘3 FailedAuthentication Events in a rolling 30 second time window for the Same Destination Account’.

You can define further variations of this such as ‘x FailedAuthentication events in xx seconds, all from the same SourceMachine’, etc. by choosing appropriate fields of the LEM Events being correlated.

Part 3: Define the Action
The Action part of the Rule definition allows you to define how you would like LEM to defend the network for Correlated events. The full list of LEM actions is shown below. For the example being discussed, ‘Disable Domain User Account’, ‘Shutdown Machine’, are some relevant choices to make for this example.
For this exercise, a ‘Send Email Message’ action is shown below. The ‘Default’ email template has been chosen (More email templates can be defined in the BUILD > Groups view), select Recipients (More LEM users can be defined in the BUILD > Users view), and drag the event fields into the expected template inputs. Also notice how the Rules Status changed to OK! Once the rule has been completely defined.

The ‘Activate Rules’ button

Finally, the Rule must be Enabled and Activated. Use the Gear Icon to enable the rule, and the ‘Activate Rules’ button to activate all modified and new rules.

Just to re-iterate, you must click on  to activate all modified and new Rules. Otherwise, these new & modified rules will NOT take effect.

HISTORICAL SEARCH - nDEPTH EXPLORER

LEM’s “nDepth” explorer provides intuitive, interactive, and user-friendly interface for historically searching both normalized LEM events as well as original log messages. nDepth enables you to easily analyze events and view log data in a way that makes sense for truly fast and effective event forensics, troubleshooting, and root cause analysis.

To access the nDepth Explorer go to EXPLORE > nDepth view. As noted previously in the Filters section, any of the filters can be thrown into nDepth for searching events historically.
The nDepth toolbar consists of various powerful visualization techniques such as Word Cloud, Tree maps, Bar charts, Line graphs, Pie charts, Bubble charts and Result details.

For any of the nDepth queries, you can change the default Time Range of ‘Last 10 minutes’. Other choices are ‘Last 30 minutes’, ‘Last hour’, ‘Last 2 hours’, ‘Last day’, ‘Last week’, ‘Custom’. Be sure to click on the Play button for the revised time frame to be applied to nDepth search results.

This will display a histogram pane, and Result Details pane and various filtering options. All of these Panes are fully interactive, and some common ways of interacting with the search results are discussed below.

**Interacting with the nDepth explorer**

**List pane**
In the List pane, all the fields like Event Names, Detection IPs, Tool Alias, IP Address fields are ranked in descending order. Simply double click on any of these values in the List pane and then click on the Play button for nDepth to refine the results further.

**Histogram**
Simply double click on any of the bars in the histogram to have nDepth zoom into that time range. Notice how the Time Range changes to ‘Custom’ automatically. nDepth always displays the time range in terms of start time and end time on top of the histogram.
Result Details

By default, nDepth displays the Result Details pane.

If you have moved away to another visualization technique using the nDepth toolbar, you can get back to the Result Details pane by clicking on the icon shown below.

The Results Details pane displays all the matching LEM Events, and also its Event Fields. You can mark and select any text from an Event Field data, and double click to effectively perform a key word search on top of the current search criteria.

Click the 'Play' button to refine the results based on this keyword search. Notice how the histogram change compared to the results shown above, and also how the keywords are highlighted in every Event of the Result Details pane.
Event Search

It is also possible to build a search query using the Events section in the list pane. Simply select the event name and any relevant fields you wish to base your query on. Drag to the search bar, click play and the logs will be displayed.

Keyword Search

If you need to type keywords to search, you can switch from the Drag & Drop mode to Text Input Mode. This can be done using the slider bar shown below.

Word Cloud

Word Cloud is a very powerful visualization technique available for nDepth Search results. The font size is proportional to the number of hits in the search results. Obviously, the largest font implies the maximum number of hits, and everything else proportionately lower. Just like the Results pane, you can double click on any word displayed in the Word Cloud, and click on the Play button to refine the results. This can be a very effective tool for analyzing large log volumes, particularly for firewall logs.
Saving Search Results

The search criteria can be saved for quick and easy access for future nDepth searches. This is done from the ‘Save As’ menu option under the Gear icon next to the ‘Explore’ button.

Exporting Search Results

Once you have the logs you need in the result details pane, it can be exported to CSV or PDF formats.

To export to CSV simply click on the Gear icon within the result details pane, and then ‘Export to CSV’.

To generate a PDF report, click on the Gear icon next to the ‘Explore’ button and then select ‘Export’. This will then create a report with bar charts, line graphs, pie charts, normalized logs and more.

The nDepth Export preview window then opens.
From there you can then customize each page by deleting graphs, adding new graphs from the items tab on the top left. You can also delete an entire page by clicking the X icon on the top right of the page. Simply click Export to PDF to export the report.

For more information please see this video: Using nDepth and Reports to Search and Analyse Log Data

**LEM REPORTS – SECURITY, COMPLIANCE AND OPERATIONS REPORTING**

Log and Event Manager streamlines security, compliance and operations reporting by providing an intuitive reporting console with hundreds of built-in templates along with the ability to easily customize reports based on your specific needs.

Reports can be created with different levels of data and graphics, including master reports, detailed reports and top-level reports. You can also schedule report generation and delivery or run on-demand. You can also export reports to multiple formats, including TXT, PDF, CSV, DOC, XLS and HTML.

The reports console is separate from the web console and is installed locally on a workstation or server as represented in the architecture diagram. In order to access data in the database on the appliance, an ODBC connection is established (automatically) between the local machine and the LEM appliance.
Reports are broken into categories such as Authentication, Change Management, File Audit, Machine Audit, Network Events and Network Traffic Audit. There are different levels within the reports such as Master, Detail and Top. The master reports will run every report below itself, until the next master report. It is also possible to run individual detail reports if needed.

In this example the three detail reports will run if you select the master Authentication report.

To run a report on demand simply double click on the report:

In the next window you can select your start and end date for the report.
The report is then generated:

![Figure 51 LEM Sample Report](image)

**Select Expert**

Once your report is complete it is possible to query specific data out of a report using the Select Expert tool.

![Select Expert](image)

Click ‘New’ and select the appropriate field from the Fields list.
Choose the ‘is equal to’ operator:

![Select Expert Dialog Box]

You can then manually type into the box or select the value from the dropdown menu:

![Select Expert Dialog Box]

Click the ‘Export’ button to export a copy of your custom report.

For more information on Select Expert please see this KB: Filtering and Exporting LEM Reports.

**Running Multiple Report & Compliance Templates**

It is possible to select multiple reports at the same time by using the drop down menu within the Report Title. Simply select the reports and then click the Run button. Alternatively you can use the schedule button to run the reports at a specified time.
LEM Reports also makes compliance reporting very easy with pre-packaged, audit proven templates for a wide range of standards including PCI, SOX, GPG13, ISO and HIPAA. These templates can be accessed from the 'Manage > Categories' section of LEM Reports.

Ensure ‘Industry Reports’ is selected under Categories:

ADVANCED DEPLOYMENT SCENARIO

LEM Agent’s features such as encryption, compression and buffering can also be leveraged to capture logs from remote locations across WAN links in a secure & bandwidth friendly manner even across unreliable WAN links. A sample deployment scenario is shown below where there are 2 locations (location A and location B). The same techniques discussed here can also be used when your change management processes do not allow adding further logging hosts on your network devices.
The essential design principle here is to detach / distribute the Syslog servers rather than using the Syslog server on the LEM Manager. In the deployment shown above, both Location A and Location B have a Syslog server installed locally. As discussed previously, the LEM connectors are responsible for normalizing original log messages into LEM Events. When a detached Syslog server is used, a LEM Agent must be installed on this detached Syslog server. The relevant Connectors must be enabled on the LEM Agent as opposed to enabling them on the LEM Manager. Please note that the automatic scanning of logs does not apply to the LEM Agent. However, new nodes are discovered by the enabled Connectors.

The next section provides specific instructions for using Kiwi Syslog server as the detached Syslog server for LEM

**Using Kiwi Syslog Server as a detached Syslog Server**

1. Install Kiwi Syslog server
2. Run Kiwi Syslog
3. Chose File > Setup and confirm the log file path for the log to file action.

4. Install LEM Agent onto the Kiwi Syslog Server

5. Open the LEM console

6. Select Manage Nodes and locate the node that is running the Kiwi Syslog server and LEM Agent.

7. Select the Gear Icon and choose ‘Connectors’

8. From the various Connectors, select the type of syslog message you wish to interpret from the Kiwi Syslog server such as ‘Cisco PIX and IOS’

9. Select the Gear icon and select ‘New’
10. Configure the Alias for this instance of the Connector and specify the log path obtained in step 3 and Select Save.

Hint – Use the word ‘Kiwi’ or the location in the Alias field to assist with Filters.

11. Chose the Gear icon next to your newly created connector and select ‘Start’. When the Connector successfully starts it will have a green arrow beside it.

12. This Alias can be leveraged to create your LEM Filters

13. Review and consolidate your logs from Kiwi on your LEM Manager!
MORE ABOUT SOLARWINDS®

SolarWinds delivers powerful and affordable IT management and monitoring software to over 100,000 customers worldwide—from Global 1000 enterprises to Mike’s Car Wash. SolarWinds products give you the power to get things done and solve problems fast, without the barriers to try, buy, deploy, and use that are associated with the “enterprise” IT monitoring solutions.

Additional LEM Resources:

» LEM Related Videos: LEM Playlist on YouTube

» SolarWinds THWACK® Community: Solarwinds thwack online community adds value to IT pros

» LEM on THWACK®

» Follow us On Twitter: @solarwinds

For questions or to schedule a free consultation with a Log & Event Manager expert,

Call/Email us: Phone: 1.866.530.8100 Email: sales@solarwinds.com

© 2015 SolarWinds Worldwide, LLC. All rights reserved.

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.