Monitoring Local Director

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

A load balancer distributes requests among multiple application servers, with a view to optimally utilizing the available servers. Besides providing scalability and performance enhancements, a load balancer also improves reliability. For example, many load balancers can monitor the status of the different servers they support, and if one of the servers stops responding, a load balancer is able to reroute requests to one of the other servers. By providing a unified virtual image to service requestors, a load balancer enables continuous access to multiple redundant servers for Internet-based e-commerce applications.

In IT infrastructures, load balancers have been used predominantly to balance traffic among multiple web servers. While the traffic they handle has been predominantly TCP-based, recently, some of these load balancers have also been used to handle UDP traffic. Cisco's Local Director product is a very popular load balancer used in IT infrastructures.

This document explains how to manage and monitor the Local Director product using the eG Enterprise Suite.

Chapter 2: How does eG Enterprise Monitor Local Director?

The eG Enterprise is capable of monitoring the Local Director in an *agentless* manner using the SNMP. The eG external agent periodically polls the SNMP MIB of the Local Director and fetching metrics related to the performance of the Local Director. This sections that follow describe how to manage and monitor the Local Director.

2.1 Managing the Local Director

The eG Enterprise cannot automatically discover a Local Director so that you need to manually add the component for monitoring. To manage a Local Director component, do the following:

1. Log into the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENTS** page that appears next, select *Local Director* as the **Component type**. Then, click the **Add New Component** button. This will invoke Chapter 2.

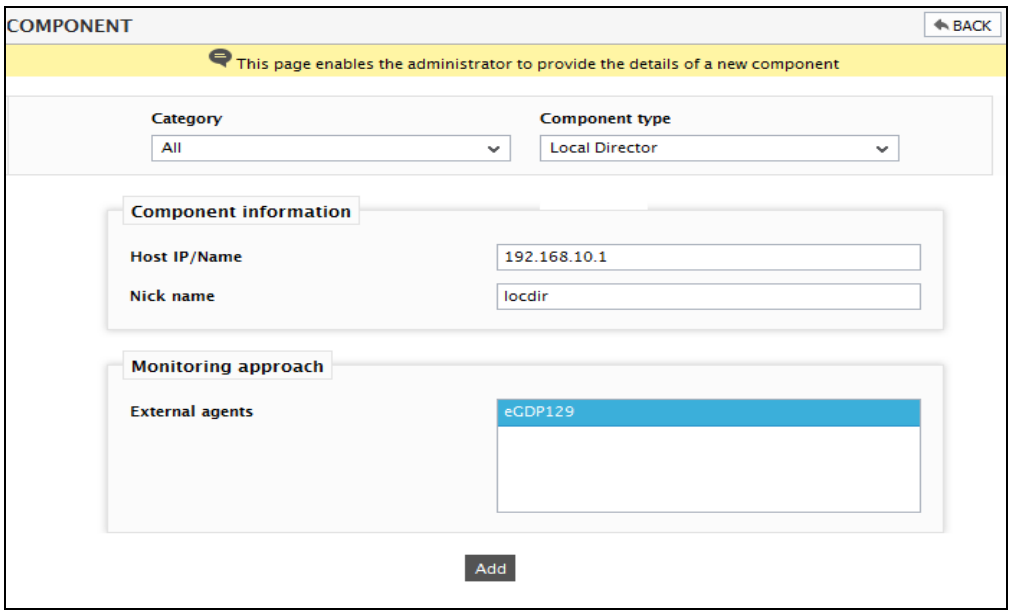

Figure 2.1: Adding a new Local Director

4. Specify **Host IP/Name** and **Nick name** for the Local Director as shown in Figure 2.1. Then, click on the **Add** button to configure the Local Director component.

5. Now, attempt to sign out of the eG administrative interface. Doing so will list all the unconfigured tests of the Local Director as shown in Figure 2.2.

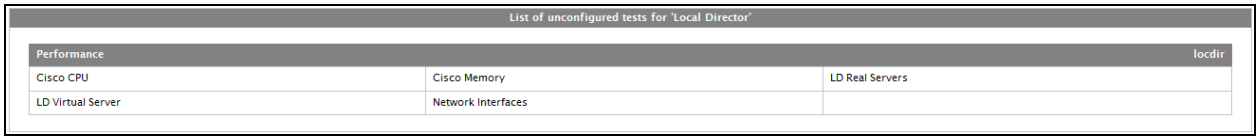

Figure 2.2: List of unconfigured tests for the Local Director

6. Click on the **Cisco CPU** test to configure it. To know how to configure the test, refer to *Monitoring Cisco Router* document.
7. Then, try to signout of the eG administrative interfaces. This time, you will be prompted to configure the **LD Real Servers** and **LD Virtual Server** tests. Now click on the **LD Real Servers** test. To know how to configure the test, refer to Section **3.3.1**.
8. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring Local Directors

The eG Enterprise suite includes specialized tests that track the status of a Local Director. The layer model that is used to monitor a Local Director is shown in Figure 3.1.

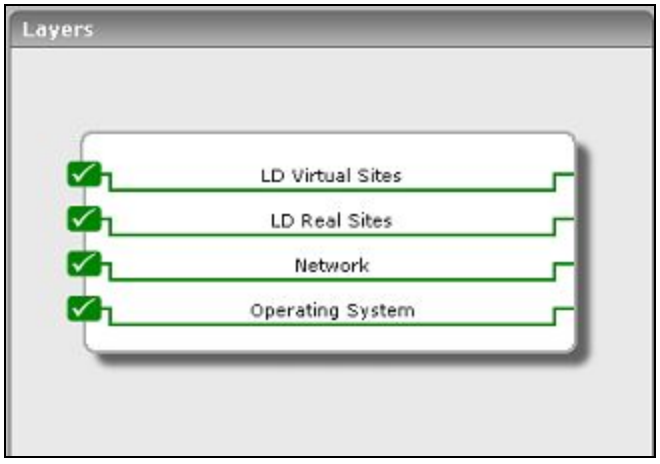

Figure 3.1: Layer model for a Local Director

The following sections discuss each of the layers of Figure 3.1.

3.1 The Operating System Layer

This layer tracks the resource usage of the Local Director (see Figure 3.2).

Figure 3.2: The tests mapped to the Operating System layer of a Local Director

Both the tests depicted by Figure 3.2 have been discussed elaborately in *Monitoring Cisco Router* document.

3.2 The Network Layer

The tests mapped to this layer measure the following:

- The network connectivity of the Local Director and the health of transmissions to and from the Local Director;
- The overall health of all network interfaces configured for the Local Director

Figure 3.3: The tests mapped to the Network layer of a Local Director

The tests depicted by Figure 3.3 have been handled in *Monitoring Cisco Router* document.

3.3 The LD Real Sites Layer

This layer tracks the statistics pertaining to the real servers of the Local Director using the LdRealServer test shown in Figure 3.4.

Figure 3.4: Tests mapping to the LD Real Sites layer

3.3.1 LD Real Servers Test

This test monitors the real servers connected to a Local Director using the snmpwalk command for the OID values provided by the MIB of the Local Director.

Target of the test : A Local Director

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Local Director being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the monitored target.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPversion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPversion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when **v3** is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a

Parameter	Description
	contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
Authpass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm password	Confirm the Authpass by retyping it here.
Authtype	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
Encryptflag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
Encrypttype	If this Encryptflag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the Encrypttype list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
Encryptpassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
State	This measure depicts the state of the server.	Number	The state of the server is good if the value reported by this measure is 1. On the other hand the state is unknown, if the value is –1. Any other value reported by this measure signifies that the server is bad.
Connection rate	Indicates the rate at which connections are made by the Local Director.	Conns/Sec	A sudden increase in the number of connections established on a host can indicate either an increase in load to one or more of the applications executing on the host, or that one or more of the applications are experiencing a problem like a slow down.
Data rate	Indicates the rate of transfer of data.	MB/Sec	A significantly high value denotes a heavy traffic in the network.

3.4 The LD Virtual Sites Layer

This layer tracks the statistics pertaining to the virtual servers of the Local Director using the LdVirtualServer test shown in Figure 3.5.

Figure 3.5: Tests mapping to the LD Virtual Sites layer

3.4.1 LD Virtual Server Test

This test monitors the virtual servers of the Local Directors for the OID values provided by the MIB of the Local Director.

Target of the test : A Local Director

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Local Director being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the monitored target.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPversion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPversion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when **v3** is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a

Parameter	Description
	contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
Authpass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm password	Confirm the Authpass by retyping it here.
Authtype	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
Encryptflag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
Encrypttype	If this Encryptflag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the Encrypttype list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
Encryptpassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
State	This measure depicts the state of the server.	Number	The state of the server is good if the value reported by this measure is 1. On the other hand the state is unknown, if the value is –1. Any other value reported by this measure signifies that the server is bad.
Connection rate	Indicates the rate at which connections are made by the Local Director.	Conns/Sec	A sudden increase in the number of connections established on a host can indicate either an increase in load to one or more of the applications executing on the host, or that one or more of the applications are experiencing a problem like a slow down.
Data rate	Indicates the rate of transfer of data.	MB/Sec	A significantly high value denotes a heavy traffic in the network.

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.