Monitoring Load Balancer VA R20

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

The Loadbalancer.org appliance runs on the GNU/Linux operating system with a custom kernel configured for load balancing. Loadbalancer.org appliances enable two or more servers to be combined into a cluster. This enables inbound requests to be distributed across multiple servers which provides improved performance, reliability and resilience. Appliances can also be deployed as a clustered pair which creates a highly-available configuration.

Since application delivery delays, inefficiencies, and failures can cause prolonged service outages and cost an enterprise money and reputation, the continuous operation and good health of the load balancer is of great importance. Therefore, it is imperative that the Load Balancer should be continuously monitored to avert such eventualities. This is where eG Enterprise helps administrators! eG Enterprise has developed an exclusive *Load Balancer VA R20* monitoring model for this purpose.

Chapter 2: How to Monitor Load Balancer VA R20?

eG Enterprise monitors the Load Balancer VA R20 using an eG external agent on any remote host in the environment. This agent is capable of monitoring the performance of the load balancer appliance by polling the SNMP MIB of the load balancer.

2.1 Pre-requisites for Monitoring the Load Balancer VA R20

To enable the eG agent to collect performance metrics from the Load Balancer VA R20, the following pre-requisites should be fulfilled:

- The load balancer should be SNMP-enabled.
- The eG external agent should be able to access the target load balancer over the network.

Once the pre-requisites are fulfilled, manage the target load balancer using the eG administrative interface. The procedure has been discussed in Section **2.2**.

2.2 Managing the Load Balancer VA R20

The eG Enterprise cannot automatically discover the Load Balancer VA R20. Therefore, you need to manually add the component for monitoring. To manage a Load Balancer VA R20 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 **COMPONENT** page that appears next, select Load Balancer VA R20 as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

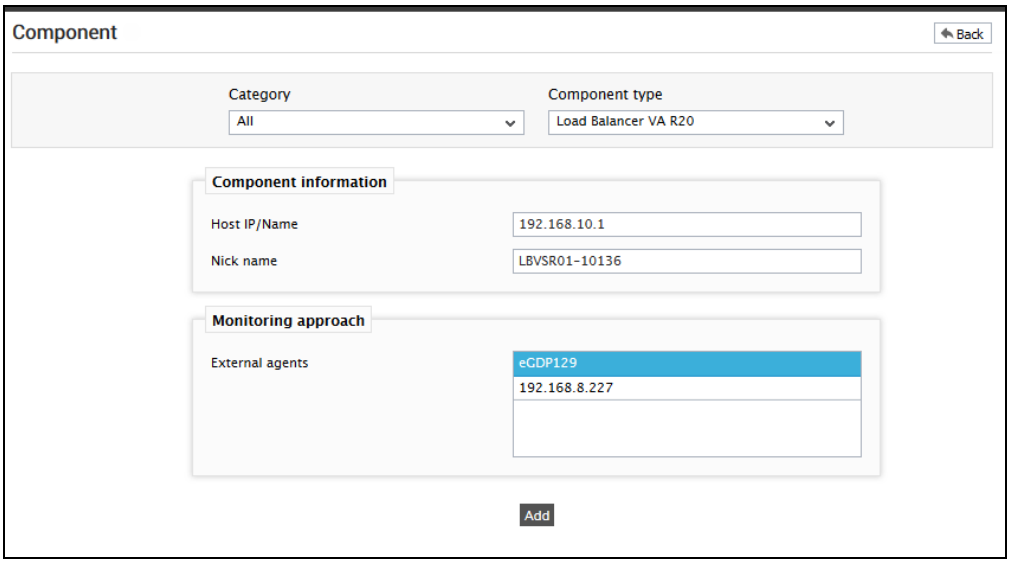

Figure 2.1: Adding a Load Balancer VA R20 appliance

4. Specify the **Host IP/Name** and the **Nick name** of the Load Balancer VA R20 appliance in Figure 2.1. Then, click the **Add** button to register the changes.
5. When you attempt to sign out, a list of unconfigured tests will appear as shown in Figure 2.2.

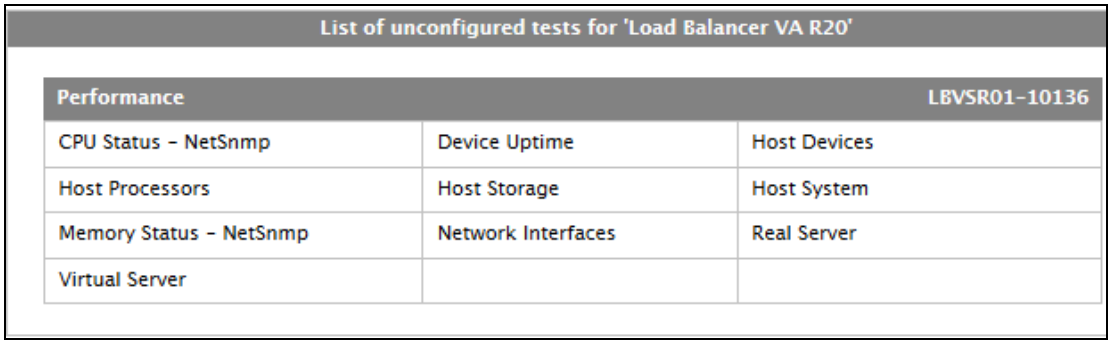

Figure 2.2: List of unconfigured tests to be configured for the Load Balancer VA R20 appliance

6. Click on any test in the list of unconfigured tests. For instance, click on the **Virtual Server** test to configure it. In the page that appears, specify the parameters as shown in Figure 2.3.

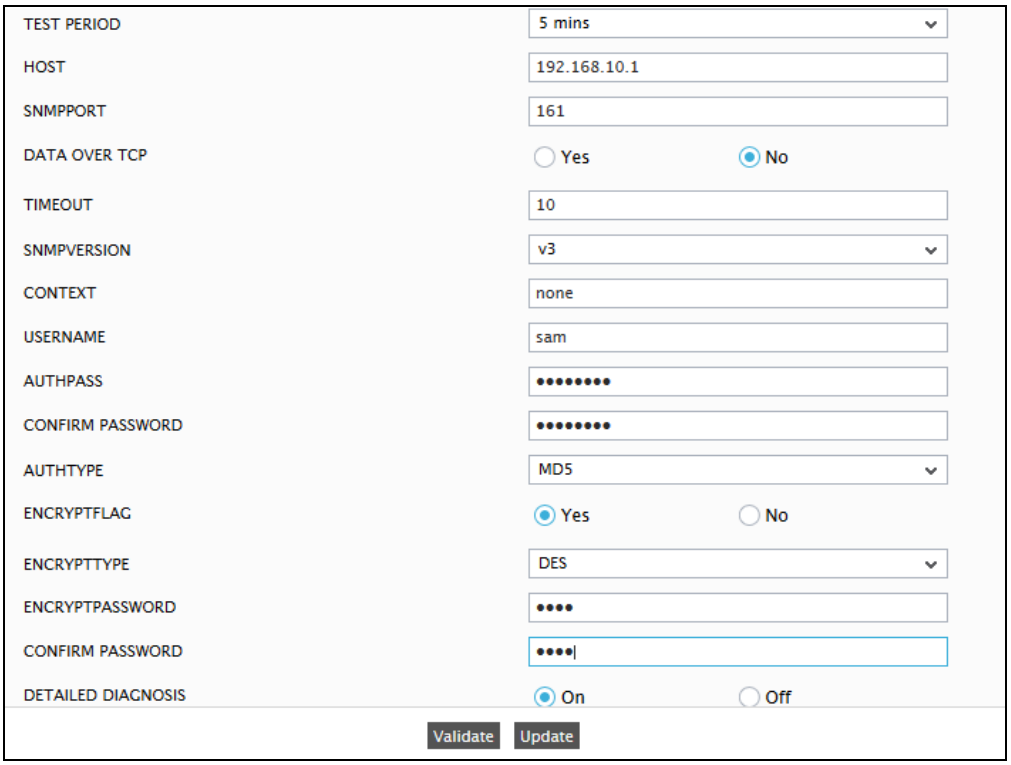

Figure 2.3: Configuring the A10 CPU test

7. To know how to configure parameters, refer to Virtual Server Test.
8. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring Load Balancer VA R20

To ensure continuous operation of the Loadbalancer.org appliances, eG Enterprise provides a specialized *Load Balancer VA R20* monitoring model (see Figure 3.1).

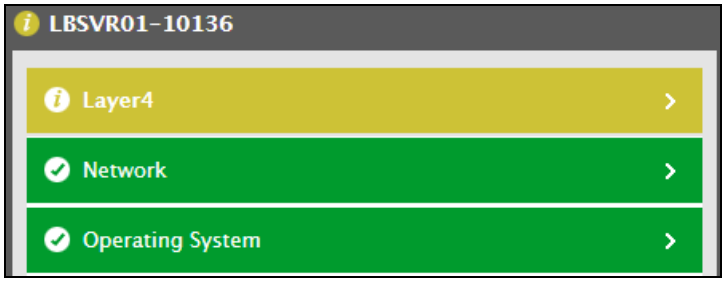

Figure 3.1: The layer model of the Load Balancer VA R20

Every layer of Figure 3.1 is mapped to a variety of tests which connect to the SNMP MIB of the target load balancer to collect critical statistics pertaining to its performance. The metrics reported by these tests enable administrators to answer the following questions:

- How well the real server is processing client traffic? Which server is handling the maximum traffic?
- How many real servers are associated with each virtual server?
- How well the virtual server is processing client traffic? Which virtual server is handling the maximum traffic?

Since the **Network** and Operating System layers have been dealt in detail in the *Monitoring Unix and Windows Servers* document, the sections to come will discuss the Layer4 layer of Figure 3.1.

3.1 The Layer4 Layer

This layer tracks the statistics pertaining to the client traffic processing ability of the virtual servers and the real servers associated to the virtual server.

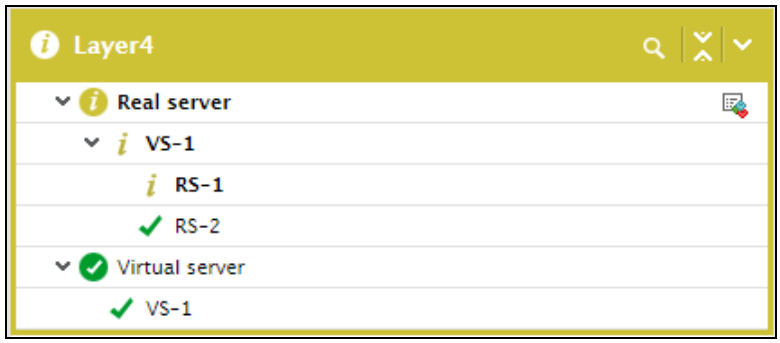

Figure 3.2: Tests mapping to the Layer4 layer

3.1.1 Real Server Test

Real servers are those that are bound to a virtual server in a server farm of the load balancer. Whenever a client request is received, the virtual server bound to the real server responds to those requests by channelizing the requests to the real servers that are currently available. If the real servers are experiencing any technical glitch or a slowdown or if the real servers are currently overloaded, the target load balancer may not be effective in responding to the client requests thus causing inconsistencies in the load balancing functionality. To avoid such inconsistencies, it is necessary to monitor the request processing ability of the real servers round the clock. This is where the **Real Server** test exactly helps!

For each real server grouped on the virtual server that is configured on the target load balancer, this test reveals how well each server processes client requests. In addition, this test detects inconsistencies in load- balancing early on and warns administrators of possible deviations proactively.

Target of the test : A Load Balancer VA R20

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Virtual server:Real server* combination on the target load balancer being monitored

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is

Parameter	Description
	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 storage node. 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 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

Parameter	Description
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
Current connections	Indicates the number of connections handled by this real server during the last measurement period.	Number	This measure is a good indicator of load on the real server. The detailed diagnosis of this measure lists the IP address and the port number of the real server through which the server is associated with the virtual server.
Received packets	Indicates the number of packets received by this	Number	Compare the value of this measure across the real servers to figure out

Measurement	Description	Measurement Unit	Interpretation
	real server during the last measurement period.		the real server that is receiving the maximum number of packets.
Transmitted packets	Indicates the number of packets transmitted by this real server during the last measurement period.	Number	Compare the value of this measure across the real servers to figure out the real server that is transmitting the maximum number of packets.
Received data	Indicates the amount of data received by this real server during the last measurement period.	KB	Compare the value of this measure across the real servers to figure out the real server that is receiving the maximum amount of data.
Transmitted data	Indicates the amount of data transmitted by this real server during the last measurement period.	KB	Compare the value of this measure across the real servers to figure out the real server that is transmitting the maximum amount of data.
Received packet rate	Indicates the rate at which packets were received by this real server.	Packets/sec	
Transmitted packet rate	Indicates the rate at which packets were transmitted by this real server.	Packets/sec	
Received data rate	Indicates the rate at which data was received by this real server.	KB/sec	
Transmitted data rate	Indicates the rate at which data was transmitted by this real server.	KB/sec	

3.1.2 Virtual Server Test

The Load Balancer consists of multiple virtual servers which, in turn, consists of an IP address and port. This virtual server is bound to a number of physical servers a.k.a real servers within a server farm. A virtual server is capable of performing the following:

- Distribute client requests across multiple servers to balance server load;
- Apply various behavioral settings to a specific type of traffic;

- Enable persistence for a specific type of traffic;
- Direct traffic according to user-written rules

In addition, virtual servers can also be used in the following ways:

- Directing traffic to a load balancing pool;
- Sharing an IP address with a VLAN node;
- Forwarding traffic to a specific destination IP address;
- Increasing the speed of processing HTTP traffic;
- Increasing the speed of processing Layer 4 traffic;
- Relaying DHCP traffic

If the virtual servers are not able to manage the traffic and divert client requests to servers that are managing fewer requests, poor performance and outages cannot be avoided. Also, irregularities in load balancing can cause significant delay in request processing thus affecting the user experience with the load balancer. To avoid this, you can configure the periodic execution of the **Virtual Server** test.

For each virtual server configured on the target load balancer, this test continuously monitors the load on the load-balancing virtual servers and reveals how well each virtual server processes client requests. In addition, this test detects inconsistencies in load- balancing early on and warns administrators of possible deviations proactively.

Target of the test : A Load Balancer VA R20

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Virtual server* on the target load balancer being monitored

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.

Parameter	Description
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 storage node. 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 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

Parameter	Description
	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
Associated real server	Indicates the number of real servers associated with this virtual server.	Number	The detailed diagnosis of this measure lists the name of the real server associated with the virtual server and the IP address through which the real server was connected to the virtual server.
Current connections	Indicates the number of connections handled by this virtual server during the last measurement period.	Number	This measure is a good indicator of load on the virtual server.

Measurement	Description	Measurement Unit	Interpretation
Received packets	Indicates the number of packets received by this virtual server during the last measurement period.	Number	Compare the value of this measure across the virtual servers to figure out the virtual server that is receiving the maximum number of packets.
Transmitted packets	Indicates the number of packets transmitted by this virtual server during the last measurement period.	Number	Compare the value of this measure across the virtual servers to figure out the virtual server that is transmitting the maximum number of packets.
Received data	Indicates the amount of data received by this virtual server during the last measurement period.	KB	Compare the value of this measure across the virtual servers to figure out the virtual server that is receiving the maximum amount of data.
Transmitted data	Indicates the amount of data transmitted by this virtual server during the last measurement period.	KB	Compare the value of this measure across the real servers to figure out the virtual server that is transmitting the maximum amount of data.
Received packet rate	Indicates the rate at which packets were received by this virtual server.	Packets/sec	
Transmitted packet rate	Indicates the rate at which packets were transmitted by this virtual server.	Packets/sec	
Received data rate	Indicates the rate at which data was received by this virtual server.	KB/sec	
Transmitted data rate	Indicates the rate at which data was transmitted by this virtual server.	KB/sec	

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.