Monitoring Infoblox

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

The Infoblox network services appliance provides reliable, scalable, and secure core network services including DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), IPAM (IP Address Management), IF-MAP, and more. The integrated Infoblox approach combines the simplicity of appliances with the power of advanced distributed database technology to control and automate services while achieving availability, manageability, visibility, and control unparalleled by conventional solutions based on legacy technologies. The Infoblox appliance can be configured and managed through an easy to use Infoblox GUI (Graphical User Interface) that works seamlessly in Windows, Linux and Mac environments using standard web browsers.

Chapter 2: How to Monitor Infoblox Using eG Enterprise?

eG Enterprise monitors the Infoblox appliance in an agentless manner. All that is required for this is a single eG agent on any remote Windows host in the environment. This agent is capable of polling the SNMP MIB of the appliance at regular intervals and collecting metrics pertaining to its performance. Before attempting to monitor the Infoblox appliance, make sure that the appliance is SNMP enabled. There are two broad steps for monitoring the Infoblox appliance;

- Managing the Infoblox appliance
- Configuring the tests

These steps are explained in the following sections.

2.1 Managing the Infoblox

The eG Enterprise cannot automatically discover the Infoblox appliance. This implies that you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To add an Infoblox, 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 *Infoblox* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

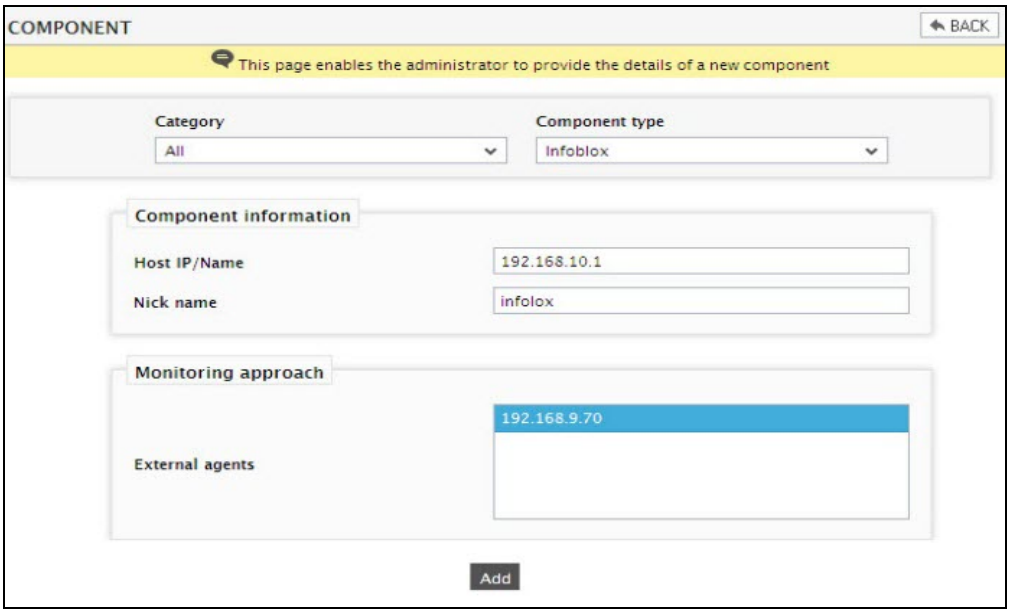

Figure 2.1: Adding an Infoblox

4. Specify the **Host IP** and the **Nick name** of the Infoblox server in Figure 2.1. Then click the **Add** button to register the changes.

2.2 Configuring the tests

1. When you attempt to sign out, a list of unconfigured tests will appear as shown in Figure 2.2.

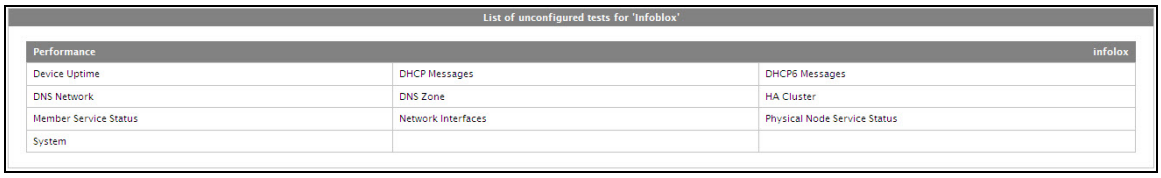

Figure 2.2: List of Unconfigured tests to be configured for the Infoblox

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

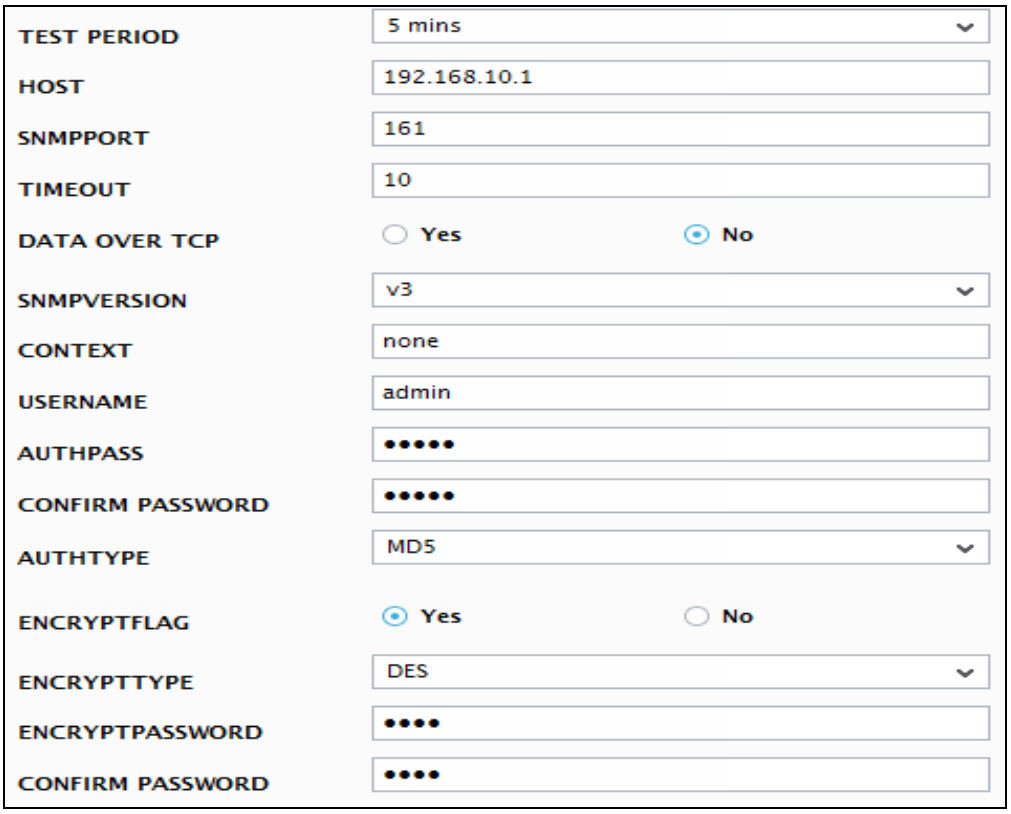

Figure 2.3: Configuring the DHCP Messages test

3. To know how to configure the tests, refer to **Monitoring Infoblox** chapter.
4. Once the **DHCP Messages** test is configured, try to signout of the eG administrative interface. You will be prompted to configure the **Device Uptime** test and the **Network Interfaces** test. To know more about how to configure the **Device Uptime** and **Network Interfaces** tests, refer to the *Monitoring Cisco Router* document.
5. Finally, signout of the administrative interface.

Chapter 3: Monitoring Infoblox

eG Enterprise provides a specialized Infoblox appliance monitoring model (see Figure 3.1) to monitor the services of the Infoblox appliance, the messages transmitted/received through various protocols, the DNS zones in the appliance etc .

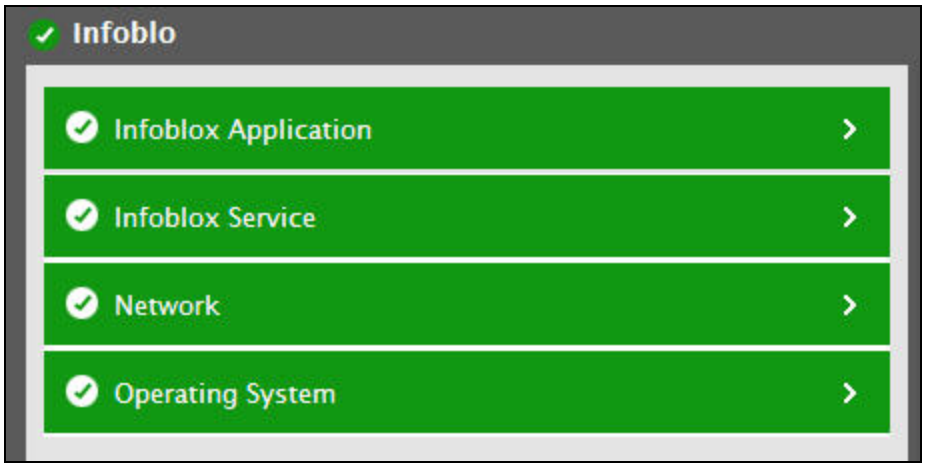

Figure 3.1: The layer model of an Infoblox appliance

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

- Is the CPU, memory and temperature of the Infoblox appliance within optimal limits?
- What is the current stauts of each service running on the Infoblox appliance? What is the current status of the Physical node service?
- Is the Infoblox appliance to be monitored configured in a high availability pair?
- How many messages such as DHCPRequest, DHCPReceive, DHCPRelease etc were transmitted/received through DHCP protocol?
- How many messages such as Solicit, Request, Release, Advertise etc were transmitted/received through DHCP6 protocol?
- How well each DNS zone of the Infoblox appliance handles queries?
- How well the Infoblox appliance handles queries and how well responses are sent from the DNS cache?

- How many replies were sent from an authoritative server and how many from a non authrotative server?

Since the **Network** layer has been dealt with *Monitoring Unix ans Windows Servers* document, the sections to come will discuss the remaining layers of the layer model.

3.1 The Operating System Layer

Using the test mapped to this layer, administators can proactively be alerted to potential resource contentions.

Figure 3.2: The tests mapped to the Hardware layer

3.1.1 System Test

This test reports critical statistics indicating the CPU and memory utilization, temperature of the hardware components of the target Infoblox system. Using this test, administrators can be proactively alerted to potential resource contentions.

Target of the test : An Infoblox appliance

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Infoblox appliance to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the Infoblox appliance 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.
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.

Parameter	Description
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 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

Parameter	Description
	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
CPU utilization	Indicates the percentage of CPU utilized by the Infoblox system.	Percent	A sudden increase in this value could indicate an unexpected/sporadic spike in the CPU usage of the system. A consistent increase however could indicate a gradual, yet steady erosion of CPU resources, and is hence a cause for concern.
Memory utilization	Indicates the percentage of memory utilized by the Infoblox system.	Percent	
Swap memory usage	Indicates the percentage of swap memeory utilized by the Infoblox system.	Percent	
Temperature	Indicates the overall temperature of the	Celcius	The value of this measure should be within normal limits. If the value of this

Measurement	Description	Measurement Unit	Interpretation
	Infoblox system.		measure is high/gradually increasing, it indicates abnormality in the functioning of the system which when left unnoticed will cause severe damage to the system.

3.2 The Infoblox Service Layer

This layer helps you in identifying the current status of the member service, physical node service and the availability of the infoblox system in the high availability mode.

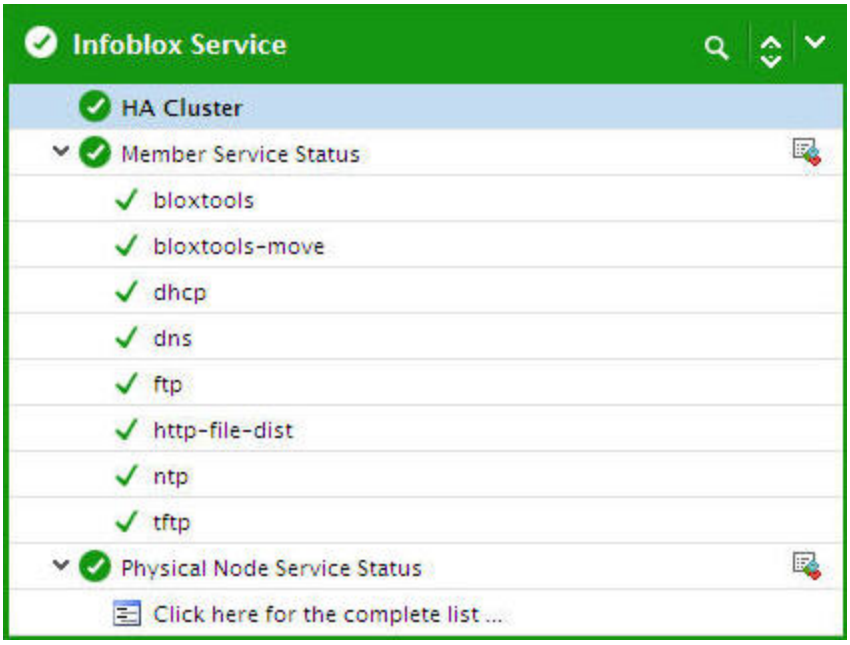

Figure 3.3: The tests mapped to the infoblox Service layer

3.2.1 Member Service Status Test

This test reports the current status of each service running on the Infoblox system.

Target of the test : An Infoblox appliance

Agent deploying the test : An external agent

Outputs of the test : One set of results for each service running on the Infoblox appliance being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the Infoblox appliance 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.
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 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

Parameter	Description
	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
Status	Indicates the current status of this service.		The values reported by this measure and their numeric equivalents are available in the table below:

Measurement	Description	Measurement Unit	Interpretation
			<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Working</td><td>100</td></tr><tr><td>Failed</td><td>1</td></tr><tr><td>Warning</td><td>2</td></tr><tr><td>Inactive</td><td>4</td></tr><tr><td>Unknown</td><td>5</td></tr></table> **Note:** This measure reports the **Measure Value**s listed in the table above to indicate the current status of this service. However, in the graph, this measure is indicated using the Numeric Values listed in the above table.

3.2.2 Physical Node Service Status Test

This test reports the current status of each physical node service of the Infoblox system.

Target of the test : An Infoblox appliance

Agent deploying the test : An external agent

Outputs of the test : One set of results for each physical node service of the Infoblox appliance being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the Infoblox appliance 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.
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

Parameter	Description
	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 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.

Parameter	Description
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
Status	Indicates the current status of this physical node service.		The values reported by this measure and their numeric equivalents are available in the table below: **Measure Value** / **Numeric Value** Working – 100 Failed – 1 Warning – 2 Inactive – 4 Unknown – 5 **Note:**

Measurement	Description	Measurement Unit	Interpretation
			This measure reports the **Measure Value**s listed in the table above to indicate the current status of this physical node service. However, in the graph, this measure is indicated using the Numeric Values listed in the above table.

3.2.3 HA Cluster Test

This test monitors the target Infoblox system and reports whether the infoblox system is configured in a highly available mode or not.

Target of the test : An Infoblox appliance

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Infoblox appliance being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the Infoblox appliance 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.
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

Parameter	Description
	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 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.

Parameter	Description
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
High availability status	Indicates whether/not the Infoblox system is configured in an HA (High availability) pair.		The values reported by this measure and their numeric equivalents are available in the table below: **Measure Value** / **Numeric Value** Configured – 100 Not Configured – 0 **Note:** This measure reports the **Measure Value**s listed in the table above to indicate whether/not the system is configured in an HA pair or not. However, in the graph, this measure is indicated using the Numeric Values listed in the above table.

3.3 The Infoblox Application Layer

Use the tests associated with this layer to figure out the messages transmitted/received through various protocols, the number of queries for which the reply was from an authoritative server, the time taken to respond to such queries etc. This layer on the whole helps administrators to analyze the efficiency of an Infoblox appliance in the target environment.

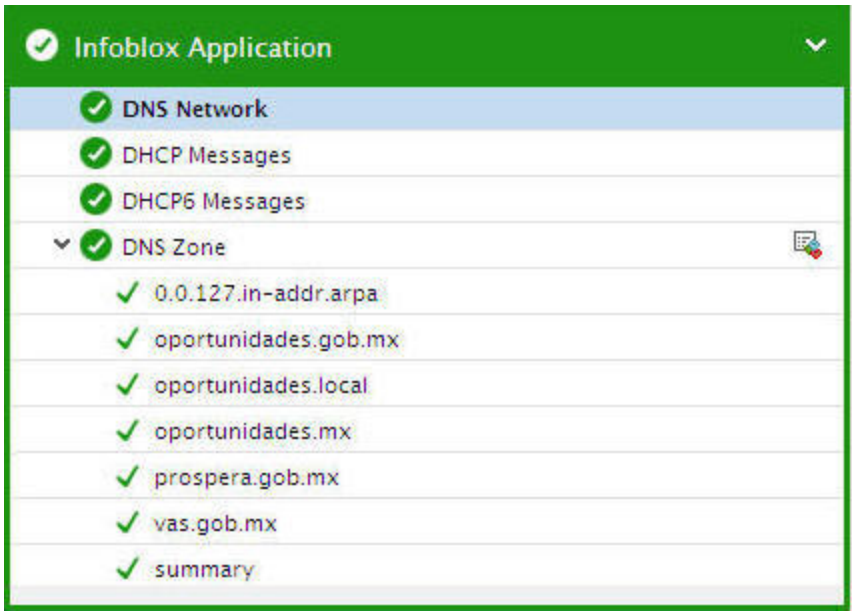

Figure 3.4: The tests mapped to the UPS Service layer

3.3.1 DHCP Messages Test

This test monitors the Infoblox appliance and reports the statistics relating to the messages received/transmitted through DHCP protocol.

Target of the test : An Infoblox appliance

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Infoblox appliance that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the Infoblox appliance for which this test is to be configured.

Parameter	Description
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value 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 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
Discovery messages received	Indicates the rate at which the DHCPDiscover messages were received.	Msgs/sec	The first time a DHCP client computer attempts to log on to the network, it requests IP address information from a DHCP server by broadcasting a DHCPDiscover packet. The source IP address in the packet is 0.0.0.0 because the client does not yet have an IP address. The message is either 342 or 576 bytes long—older versions of Windows use

Measurement	Description	Measurement Unit	Interpretation
			a longer message frame.
Request messages received	Indicates the rate at which the DHCPRequest messages were received.	Requests/sec	When a DHCP client receives a DHCPOffer packet, it responds by broadcasting a DHCPRequest packet that contains the offered IP address, and shows acceptance of the offered IP address. The message is either 342 or 576 bytes long, depending on the length of the corresponding DHCPDiscover message.
Release messages received	Indicates the rate at which the DHCPRelease messages were received.	Releases/sec	A DHCP client sends a DHCPRelease packet to the server to release the IP address and cancel any remaining lease.
Offer messages transmitted	Indicates the rate at which DHCPOffer messages were transmitted.	Msgs/sec	Each DHCP server that receives the client DHCPDiscover packet responds with a DHCPOffer packet containing an unleased IP address and additional TCP/IP configuration information, such as the subnet mask and default gateway. More than one DHCP server can respond with a DHCPOffer packet. The client will accept the first DHCPOffer packet it receives. The message is 342 bytes long.
Ack messages transmitted	Indicates the rate at which DHCPAcknowledge (DHCPAck) messages were transmitted.	Msgs/sec	The selected DHCP server acknowledges the client DHCPRequest for the IP address by sending a DHCPAck packet. At this time the server also forwards any optional configuration parameters. Upon receipt of the DHCPAck, the client can participate on the TCP/IP network and complete its system startup. The message is 342 bytes long.

Measurement	Description	Measurement Unit	Interpretation
Negative ack messages transmitted	Indicates the rate at which DHCPNak (negative acknowledgement) messages were transmitted.	Msgs/sec	If the IP address cannot be used by the client because it is no longer valid or is now used by another computer, the DHCP server responds with a DHCPNak packet, and the client must begin the lease process again. Whenever a DHCP server receives a request for an IP address that is invalid according to the scopes that it is configured with, it sends a DHCPNak message to the client.
Declined messages received	Indicates the rate at which DHCPDecline messages were received.	Msgs/sec	If the DHCP client determines the offered configuration parameters are invalid, it sends a DHCPDecline packet to the server, and the client must begin the lease process again.
Informational messages received	Indicates the rate at which DHCPInform messages were received.	Msgs/sec	When the DHCPInform message type is used, the sender is already externally configured for its IP address on the network, which may or may not have been obtained using DHCP.

3.3.2 DHCP6 Messages Test

This test monitors the Infoblox appliance and reports the statistics relating to the messages that were received/transmitted through DHCP6 protocol.

Target of the test : An Infoblox appliance

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Infoblox appliance that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.

Parameter	Description
Host	The IP address of the Infoblox appliance 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.
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 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

Parameter	Description
	• **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
Solicit messages received	Indicates the rate at which Solicit messages were received through DHCP6 protocol.	Msgs/sec	A client sends a Solicit message to locate servers.
Request messages received	Indicates the rate at which Request messages were received through DHCP6 protocol.	Requests/sec	A client sends a Request message to request configuration parameters, including IP addresses, from a specific server.

Measurement	Description	Measurement Unit	Interpretation
Release messages received	Indicates the rate at which Release messages were received through DHCP6 protocol.	Releases/sec	A client sends a Release message to the server that assigned addresses to the client to indicate that the client will no longer use one or more of the assigned addresses.
Advertisement messages transmitted	Indicates the rate at which Advertise messages were transmitted through DHCP6 protocol.	Msgs/sec	A server sends an Advertise message to indicate that it is available for DHCP service, in response to a Solicit message received from a client.
Reply messages transmitted	Indicates the rate at which Reply messages were transmitted through DHCP6 protocol.	Msgs/sec	A server sends a Reply message containing assigned addresses and configuration parameters in response to a Solicit, Request, Renew, Rebind message received from a client. A server sends a Reply message containing configuration parameters in response to an Information-request message. A server sends a Reply message in response to a Confirm message confirming or denying that the addresses assigned to the client are appropriate to the link to which the client is connected. A server sends a Reply message to acknowledge receipt of a Release or Decline message.
Renewal messages transmitted	Indicates the rate at which Renewal messages were received through DHCP6 protocol.	Msgs/sec	A client sends a Renew message to the server that originally provided the client's addresses and configuration parameters to extend the lifetimes on the addresses assigned to the client and to update other configuration parameters.
Rebind messages received	Indicates the rate at which Rebind messages were received through DHCP6 protocol.	Msgs/sec	A client sends a Rebind message to any available server to extend the lifetimes on the addresses assigned to the client and to update other configuration parameters; this

Measurement	Description	Measurement Unit	Interpretation
			message is sent after a client receives no response to a Renew message.
Declined messages received	Indicates the rate at which Decline messages were received through DHCP6 protocol.	Msgs/sec	A client sends a Decline message to a server to indicate that the client has determined that one or more addresses assigned by the server are already in use on the link to which the client is connected.
Informational messages received	Indicates the rate at which Information-Request messages were received through DHCP6 protocol.	Msgs/sec	A client sends an Information-Request message to a server to request configuration parameters without the assignment of any IP addresses to the client.

3.3.3 DNS Zone Test

This test auto discovers the zones available in the Infoblox appliance and reports the number of DNS referrals, the rate at which responses were successfully made to the appliance, statistics revealing the rate at which queries failed, queries for non existent domains etc. Using this test, administrators cacn identify the zone that is optimally processing the queries without any delays.

Target of the test : An Infoblox appliance

Agent deploying the test : An external agent

Outputs of the test : One set of results for each DNS zone of the Infoblox appliance that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the Infoblox appliance 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.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection

Parameter	Description
	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 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

Parameter	Description
	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
Successful responses	Indicates the rate at which queries were processed successfully i.e., the rate at which queries returned successful responses in this DNS zone.	Resp/sec	A high value is desired for this measure.
DNS referrals	Indicates the number of responses with the DNS referrals from the server in this zone.	Number	
DNS query received for non-existent record	Indicates the rate at which this zone was queried for non existent records.	Queries/sec	

Measurement	Description	Measurement Unit	Interpretation
DNS query received for non-existent domain	Indicates the rate at which this zone was queried for non existent domains.	Queries/sec	
Recursion queries received	Indicates the rate at which recursive name queries were received by this zone.	Queries/sec	With a recursive name query , the DNS client requires that the DNS server responds to the client with either the requested resource record or an error message stating that the record or domain name does not exist. The DNS server cannot just refer the DNS client to a different DNS server. Thus, if a DNS server does not have the requested information when it receives a recursive query, it queries other servers until it gets the information, or until the name query fails. Recursive name queries are generally made by a DNS client to a DNS server, or by a DNS server that is configured to pass unresolved name queries to another DNS server, in the case of a DNS server configured to use a forwarder.
Failed queries	Indicates the rate at which queries failed in this zone.	Queries/sec	Ideally the value of this measure should be zero. A gradual/sudden increase in the value of this measure indicates that the zone is currently experiencing slowdowns or executing a query that is too long to complete.

3.3.4 DNS Network Test

This test reports the efficiency of the Infoblox appliance in an infrastructure by collecting the following information:

- The rate at which the queries are processed and the percentage of queries processed by the DNS cache;
- The time duration for which the reply for incoming queries was received from an authoritative server for the last 5 minutes and 15 minutes respectively;
- The number of queries replied by an authoritative server in the last 5 minutes and last 15 minutes;
- The time duration for which the reply for incoming queries was received from an authoritative server after referencing another server in the last 5 minutes and 15 minutes respectively; and
- The number of queries replied by an authoritative server after referencing another server in the last 5 minutes and last 15 minutes respectively.

Target of the test : An Infoblox appliance

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Infoblox appliance that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the Infoblox appliance 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.
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

Parameter	Description
	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 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

Parameter	Description
	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
DNS cache hit ratio	Indicates the percentage of queries that were serviced by the DNS cache.	Percent	A high value is desired for this measure.
DNS query rate	Indicates the rate at which DNS queries were processed by the system.	Queries/sec	
Non authoritative latency in last 5mins	Indicates the average time during the last 5 minutes the reply for the incoming DNS queries was received from the authoritative server after referencing another server.	Secs	A low value is desired for this measure. An authoritative zone is a zone for which the local (primary or secondary) server references its own data when responding to queries. The local server is authoritative for the data in this zone and responds to queries for this data without referencing another server.
Non auth queries used in last 5mins	Indicates the number of incoming DNS queries for which the reply was given by the authoritative server after referencing another server during the last 5 minutes.	Number	
Non authoritative	Indicates the average time	Secs	A low value is desired for this

Measurement	Description	Measurement Unit	Interpretation
latency in last 15mins	during the last 15 minutes the reply for the incoming DNS queries was received from the authoritative server after referencing another server.		measure.
Non auth queries used in last 15mins	Indicates the number of incoming DNS queries for which reply was given by an authoritative server by referencing another server during the last 15 minutes.	Number	
Authoritative latency in last 5mins	Indicates the average time during the last 5 minutes the reply for the incoming DNS queries was received from an authoritative server.	Secs	
Authoritative queries used in last 5mins	Indicates the number of incoming DNS queries for which reply was received from an authoritative server during the last 5 minutes.	Number	
Authoritative latency in last 15mins	Indicates the average time during the last 15 minutes the reply for the incoming DNS queries was received from an authoritative server.	Secs	
Authoritative queries used in last 15mins	Indicates the number of incoming DNS queries for which authoritative reply was given during the last 5 minutes.	Number	

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.