Enabling Service Excellence

Monitoring Infoblox

eG Enterprise v6

Restricted Rights Legend

The information contained in this document is confidential and subject to change without notice. No part of this document may be reproduced or disclosed to others without the prior permission of eG Innovations Inc. eG Innovations Inc. makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Trademarks

Microsoft Windows, Windows NT, Windows 2000, Windows 2003 and Windows 2008 are either registered trademarks or trademarks of Microsoft Corporation in United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Copyright

Table of Contents

1

Monitoring Infoblox

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.

eG Enterprise provides a specialized Infoblox appliance monitoring model (see Figure 1) to monitor the services of the Infoblox appliance, the messages transmitted/received through various protocols, the DNS zones in the appliance etc .

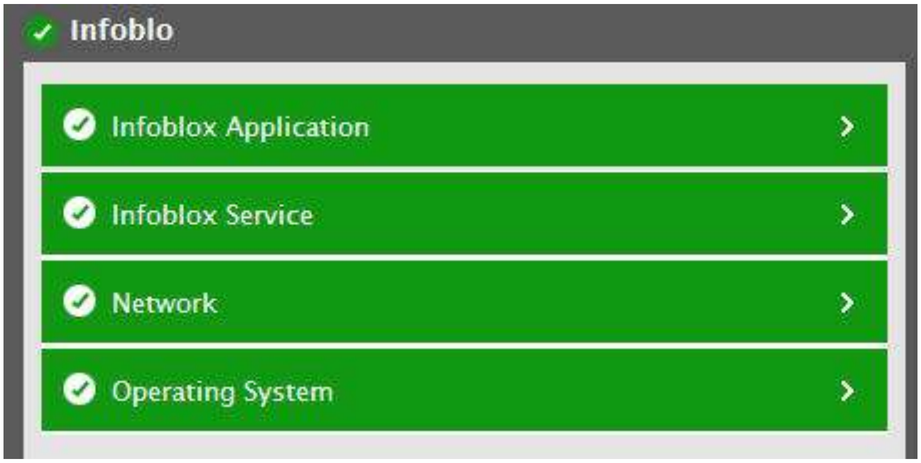


Figure 1: The layer model of an Infoblox appliance

Every layer of Figure 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 Web Servers document, the sections to come will discuss the remaining layers of Figure 1.

1.1 The Operating System Layer

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

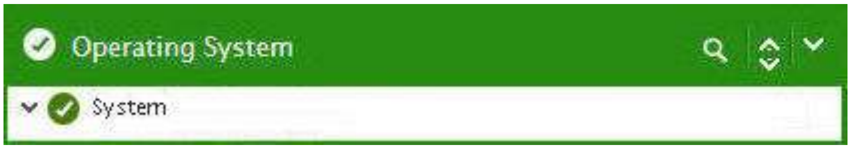


Figure 2: The tests mapped to the Hardware layer

1.1.1 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.

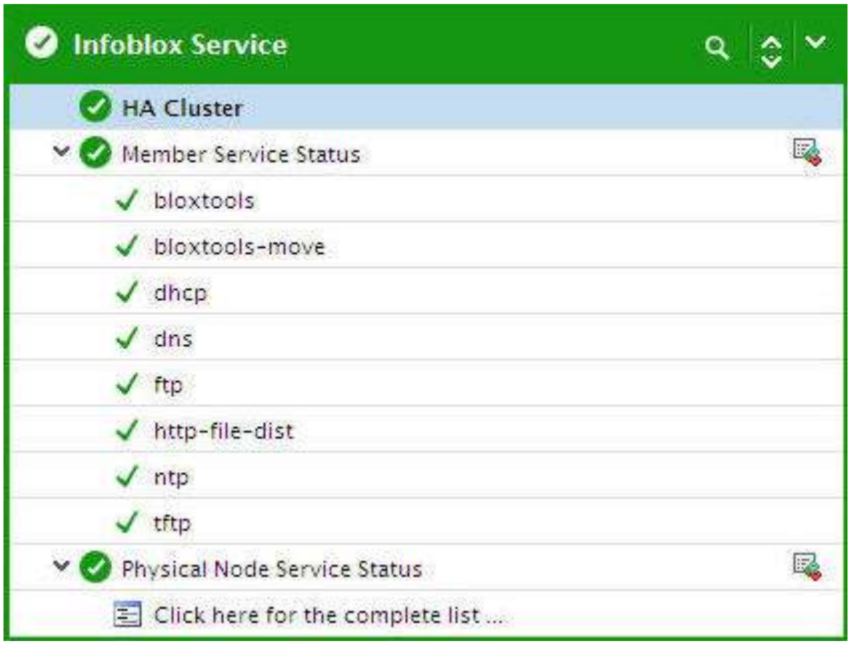
Purpose	Reports critical statistics indicating the CPU and memory utilization, temperature of the hardware components of the target Infoblox system
Target of the test	An Infoblox appliance
Agent deploying the test	An external agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Infoblox 3. **SNMPPORT** – The SNMP Port number of the Infoblox (161 typically) 4. **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. 5. **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.

	6. **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 the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 15. **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 Infoblox over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.
Outputs of the test	One set of results for the Infoblox appliance to be monitored

Measurements made by the test	Measurement	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 Infoblox system.	Celcius	The value of this measure should be within normal limits. If the value of this 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.

1.2 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.



Infoblox Service

HA Cluster

Member Service Status

✓ bloxtools

✓ bloxtools-move

✓ dhcp

✓ dns

✓ ftp

✓ http-file-dist

✓ ntp

✓ tftp

Physical Node Service Status

Click here for the complete list ...

Figure 3: The tests mapped to the infoblox Service layer

1.2.1 Member Service Status Test

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

Purpose	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
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Infoblox 3. **SNMPPORT** – The SNMP Port number of the Infoblox (161 typically) 4. **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. 5. **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.

	6. **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 the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 15. **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 Infoblox over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.
Outputs of the test	One set of results for each service running on the Infoblox appliance being monitored

<table>
<tr><th>Measurements made by the test</th><th>Measurement</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td><b>Status:</b>
Indicates the current status of this service.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<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>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current status of this service. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td></tr>
</table>

1.2.2 Physical Node Service Status Test

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

Purpose	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

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Infoblox 3. **SNMPPORT** – The SNMP Port number of the Infoblox (161 typically) 4. **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. 5. **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.

	6. **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 the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 15. **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 Infoblox over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.
Outputs of the test	One set of results for each physical node service of the Infoblox appliance being monitored

<table>
<tr><th>Measurements made by the test</th><th>Measurement</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td><b>Status:</b>
Indicates the current status of this physical node service.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<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>
<b>Note:</b>
This measure reports the <b>Measure Values</b> 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 <b>Numeric Values</b> listed in the above table.</td></tr>
</table>

1.2.3 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.

Purpose	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

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Infoblox 3. **SNMPPORT** – The SNMP Port number of the Infoblox (161 typically) 4. **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. 5. **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.

	6. **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 the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 15. **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 Infoblox over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.
Outputs of the test	One set of results for the Infoblox appliance being monitored

<table>
<tr><th>Measurements made by the test</th><th>Measurement</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td><b>High availability status:</b>
Indicates whether/not the Infoblox system is configured in an HA (High availability) pair.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Configured</td><td>100</td></tr><tr><td>Not Configured</td><td>0</td></tr></table><b>Note:</b>
This measure reports the <b>Measure Values</b> 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 <b>Numeric Values</b> listed in the above table.</td></tr>
</table>

1.3 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.

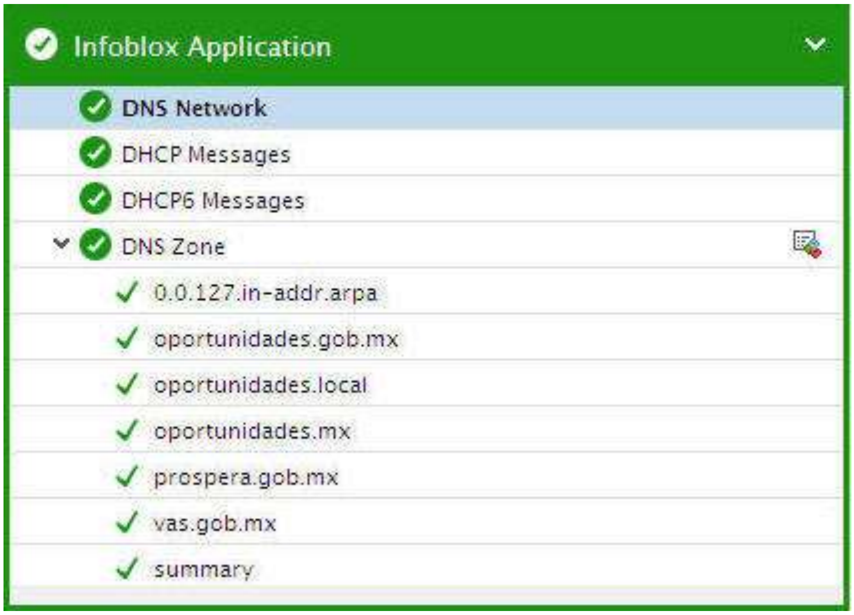


Figure 4: The tests mapped to the UPS Service layer

1.3.1 DHCP Messages Test

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

Purpose	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

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Infoblox 3. **SNMPPORT** – The SNMP Port number of the Infoblox (161 typically) 4. **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. 5. **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. 6. **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 the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the 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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

	15. **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 Infoblox over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for the Infoblox appliance that is to be monitored		
Measurements made by the test	**Measurement**	**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 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.
	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.

1.3.2 DHCP6 Messages Test

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

Purpose	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

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Infoblox 3. **SNMPPORT** – The SNMP Port number of the Infoblox (161 typically) 4. **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. 5. **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. 6. **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 the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the 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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

	15. **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 Infoblox over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for the Infoblox appliance that is to be monitored		
Measurements made by the test	**Measurement**	**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.
	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 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.

1.3.3 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.

Purpose	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
Target of the test	An Infoblox appliance
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Infoblox 3. **SNMPPORT** – The SNMP Port number of the Infoblox (161 typically) 4. **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. 5. **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. 6. **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 the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the 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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

	15. **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 Infoblox over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for each DNS zone of the Infoblox appliance that is to be monitored		
Measurements made by the test	**Measurement**	**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	
	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.

1.3.4 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.

Purpose	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

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Infoblox 3. **SNMPPORT** – The SNMP Port number of the Infoblox (161 typically) 4. **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. 5. **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. 6. **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 the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the 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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

	15. **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 Infoblox over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for the Infoblox appliance that is to be monitored		
Measurements made by the test	**Measurement**	**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 latency in last 15mins: Indicates the average time during the last 15 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.

	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	

2

Conclusion

This document has described in detail the monitoring paradigm used and the measurement capabilities of the eG Enterprise suite of products with respect to the **Infoblox** appliance. For details of how to administer and use the eG Enterprise suite of products, refer to the user manuals.

We will be adding new measurement capabilities into the future versions of the eG Enterprise suite. If you can identify new capabilities that you would like us to incorporate in the eG Enterprise suite of products, please contact support@eginnovations.com. We look forward to your support and cooperation. Any feedback regarding this manual or any other aspects of the eG Enterprise suite can be forwarded to feedback@eginnovations.com.