Monitoring BIND DNS Server

eG Innovations Product Documentation

www.eginnovations.com

eG
Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

BIND is open source software that enables you to publish your Domain Name System (DNS) information on the Internet, and to resolve DNS queries for your users.

BIND implements the DNS protocols. The DNS protocols are part of the core Internet standards. They specify the process by which one computer can find another computer on the basis of its name. The BIND software distribution contains all of the software necessary for asking and answering name service questions.

The BIND software distribution has three parts:

- **Domain Name Resolver:** A resolver is a program that resolves questions about names by sending those questions to appropriate servers and responding appropriately to the servers' replies.
- **Domain Name Authority server:** An authoritative DNS server answers requests from resolvers, using information about the domain names it is authoritative for. You can provide DNS services on the Internet by installing this software on a server and giving it information about your domain names.
- **Tools:** We include a number of diagnostic and operational tools. Some of them, such as the popular DIG tool, are not specific to BIND and can be used with any DNS server.

BIND is by far the most widely used DNS software on the Internet, as it is a transparent open source and is a flexible, full-featured DNS system. This means that if too many DNS queries to BIND fail or are dropped / rejected, your users will experience serious accessibility issues, which in turn may impact their productivity.

To avoid this, administrators should monitor incoming and outgoing queries of BIND DNS and proactively capture errors and failures in name resolution, well before users complain.

eG Enterprise provides 100% web-based monitoring of BIND DNS. Using a specialized monitoring model, eG Enterprise continuously monitors requests to and responses of BIND DNS, and promptly alerts administrators to error responses, failures, and rejections.

To know how eG Enterprise monitors BIND DNS and what statistics it reports, refer to the chapters that will follow

Chapter 2: How Does eG Enterprise Monitor BIND DNS?

eG Enterprise performs agent-based monitoring of BIND DNS. The eG agent should be deployed on the Linux server hosting BIND DNS. To monitor BIND DNS, this agent typically uses a name server control utility in bind called Remote Name Daemon Control (RNDC). RNDC is a command line utility that allows command line control of the administration and operations of a name server, both locally and remotely.

Periodically, the eG agent runs the **rndc stats** command of this utility to pull useful statistics related to the performance of BIND DNS. This command instructs BIND to dump the statistics to a *statistics-file* configured in the configuration file for the named server - */etc/named.conf*. To enable the eG agent to run the **rndc stats** command and then read from the *statistics-file*, the following pre-requisites need to be fulfilled:

- The eG agent install user should have permissions to run the **rndc stats** command and read from the *statistics-file*. To grant these permissions to the eG agent install user, do the following:
  - Edit the sudoers file on the target host and append an entry of the following format to it:

    <eG_agent_install_user>; ALL=(ALL) NOPASSWD:<Command>;

    For instance, if the eG agent install user is eguser, then the entry in the sudoers file should be:

    eguser ALL=(ALL) NOPASSWD: rndc stats
  - Then, save the file.
  - Finally, when configuring the tests for BIND DNS, make sure you set the **USE SUDO** parameter to **Yes**.
- Every test run by the eG agent should be configured with the following details:
  - The absolute/full path of the folder in which RNDC is located;
  - The absolute/full path to the statistics-file to which BIND writes all performance statistics

Chapter 3: How to Monitor BIND DNS Using eG Enterprise?

Follow the broad steps to have BIND DNS monitoring up and running in eG Enterprise:

1. Install the eG agent on the Linux server that hosts BIND DNS;
2. Manage the target BIND DNS using the eG administrative interface;
3. Configure the tests for BIND DNS.

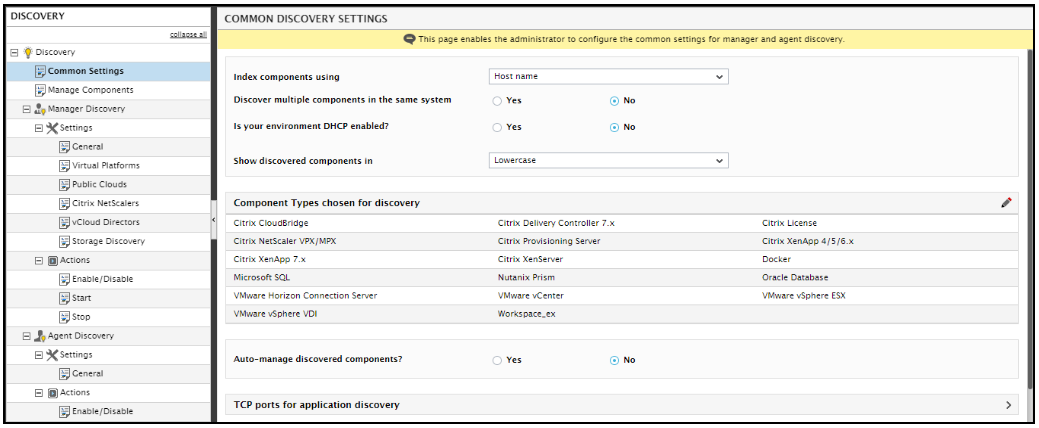
To know how to install an eG agent on Linux, refer to the *eG Installation Guide*. To perform steps 2 and 3 above, follow the procedures detailed in the sub-sections that will follow

3.1 Managing BIND DNS Using eG Enterprise

To achieve this, do the following:

1. Login to the eG admin interface as a user with the Admin role.
2. eG Enterprise uses a port-scanning technique to automatically discover the BIND DNS servers in an environment. By default, BIND DNS listens on port 53. This is the port that eG Enterprise uses for discovery by default. If BIND DNS listens on a different port in your environment, then, before starting discovery, you will have to change the port that eG Enterprise uses for discovery. For this, follow the steps below:

   - Invoke the Admin tile menu and follow the menu sequence, Infrastructure -> Components -> Discovery
   - When Figure 3.1 appears, click the **Common Settings** node in the tree-structure in the left panel of Figure 3.1. The right panel will then change to display many common discovery settings.



COMMON DISCOVERY SETTINGS

This page enables the administrator to configure the common settings for manager and agent discovery.

Index components using: Host name

Discover multiple components in the same system: ○ Yes ● No

Is your environment DHCP enabled? ○ Yes ● No

Show discovered components in: Lowercase

Component Types chosen for discovery

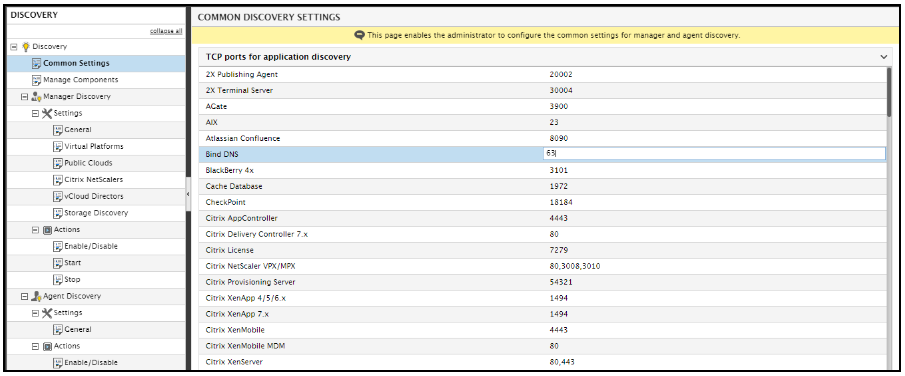
Citrix CloudBridge	Citrix Delivery Controller 7.x	Citrix License
Citrix NetScaler VPX/MPX	Citrix Provisioning Server	Citrix XenApp 4/5/6.x
Citrix XenApp 7.x	Citrix XenServer	Docker
Microsoft SQL	Nutanix Prism	Oracle Database
VMware Horizon Connection Server	VMware vCenter	VMware vSphere ESX
VMware vSphere VDI	Workspace_ex	

Auto-manage discovered components? ○ Yes ● No

TCP ports for application discovery

Figure 3.1: Viewing the common discovery settings

- Scroll down the right panel and expand the **TCP ports for application discovery** section to view the port-based applications that eG Enterprise can monitor and their ports. Once you locate **Bind DNS** in the list, click on the port number displayed against Bind DNS (default: 53), and change the port number (see Figure 3.2).



COMMON DISCOVERY SETTINGS

This page enables the administrator to configure the common settings for manager and agent discovery.

TCP ports for application discovery

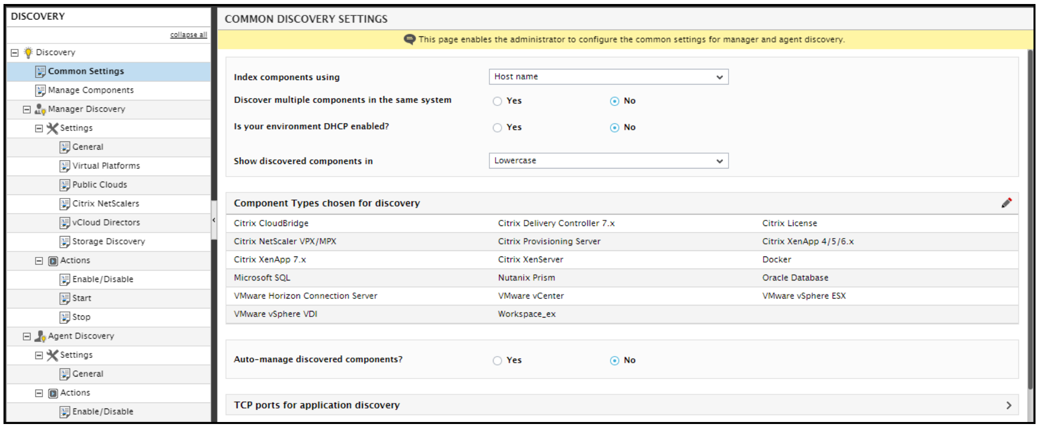
2X Publishing Agent	20002
2X Terminal Server	30004
ACate	3900
AIX	23
Atlassian Confluence	8090
Bind DNS	63
BlackBerry 4x	3101
Cache Database	1972
CheckPoint	18184
Citrix AppController	4443
Citrix Delivery Controller 7.x	80
Citrix License	7279
Citrix NetScaler VPX/MPX	80,3008,3010
Citrix Provisioning Server	54321
Citrix XenApp 4/5/6.x	1494
Citrix XenApp 7.x	1494
Citrix XenMobile	4443
Citrix XenMobile MDM	80
Citrix XenServer	80,443

Figure 3.2: Changing the port number of Bind DNS

3. Then, proceed to begin discovery. To auto-discover BIND DNS, do the following:

- Invoke the Admin tile menu and follow the menu sequence, Infrastructure -> Components -> Discovery

- When 3.1 appears, click the **Common Settings** node in the tree-structure in the left panel of 3.1. The right panel will then change to display many common discovery settings.



COMMON DISCOVERY SETTINGS

This page enables the administrator to configure the common settings for manager and agent discovery.

Index components using: Host name

Discover multiple components in the same system: ○ Yes ● No

Is your environment DHCP enabled? ○ Yes ● No

Show discovered components in: Lowercase

Component Types chosen for discovery

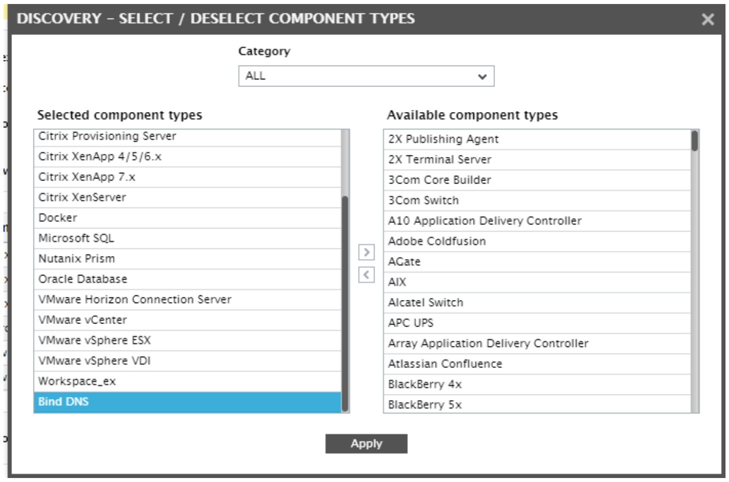
Citrix CloudBridge	Citrix Delivery Controller 7.x	Citrix License
Citrix NetScaler VPX/MPX	Citrix Provisioning Server	Citrix XenApp 4/5/6.x
Citrix XenApp 7.x	Citrix XenServer	Docker
Microsoft SQL	Nutanix Prism	Oracle Database
VMware Horizon Connection Server	VMware vCenter	VMware vSphere ESX
VMware vSphere VDI	Workspace_ex	

Auto-manage discovered components? ○ Yes ● No

TCP ports for application discovery

Figure 3.3: Viewing the common discovery settings

- In the right panel, you will see the **Component Types chosen for discovery** section. Using this section, you can configure all the component types that you want auto-discovered, every time discovery runs. For eG Enterprise to auto-discover BIND DNS, you need to add the **Bind DNS** component-type to this list. For that, first click the ✎ button in the **Component Types chosen for discovery** section. Figure 3.6 will then appear.



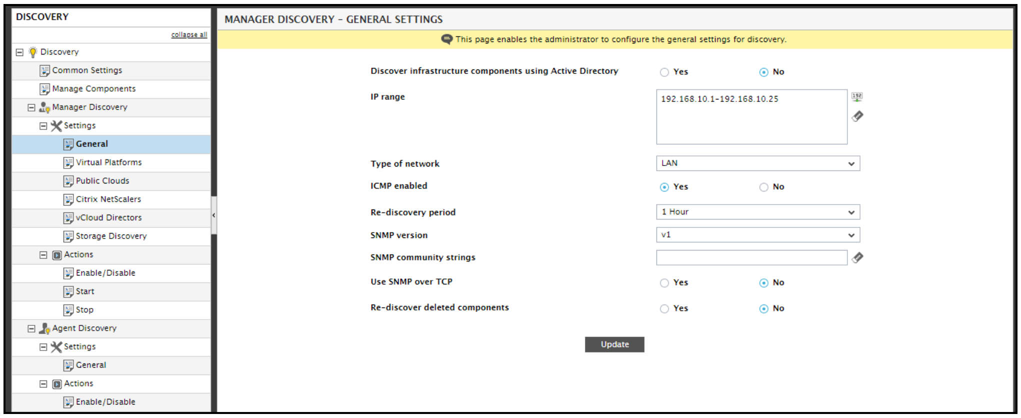
Category: ALL

Selected component types
Citrix Provisioning Server
Citrix XenApp 4/5/6.x
Citrix XenApp 7.x
Citrix XenServer
Docker
Microsoft SQL
Nutanix Prism
Oracle Database
VMware Horizon Connection Server
VMware vCenter
VMware vSphere ESX
VMware vSphere VDI
Workspace_ex
Bind DNS

Available component types
2X Publishing Agent
2X Terminal Server
3Com Core Builder
3Com Switch
A10 Application Delivery Controller
Adobe Coldfusion
AGate
AIX
Alcatel Switch
APC UPS
Array Application Delivery Controller
Atlassian Confluence
BlackBerry 4x
BlackBerry 5x

Figure 3.4: Selecting Bind DNS for discovery

- Pick *Bind DNS* from the **Available component types** list in Figure 3.6 and click the **<** button to transfer the selection to the **Selected component types** list. Finally, click **Apply** in Figure 3.6 to save the changes.
- Next, click the **Settings** sub-node under the Manager -> Discovery node in the tree-structure in the left panel of 3.1. Figure 3.5 will then appear.



MANAGER DISCOVERY - GENERAL SETTINGS

This page enables the administrator to configure the general settings for discovery.

Discover infrastructure components using Active Directory ○ Yes ● No

IP range: 192.168.10.1-192.168.10.25

Type of network: LAN

ICMP enabled ● Yes ○ No

Re-discovery period: 1 Hour

SNMP version: v1

SNMP community strings:

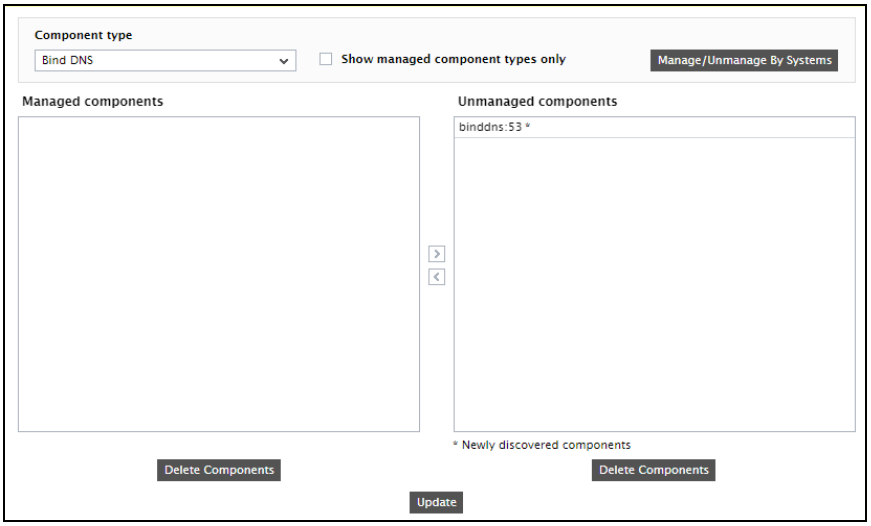
Use SNMP over TCP ○ Yes ● No

Re-discover deleted components ○ Yes ● No

Figure 3.5: Configuring manager discovery settings

- Provide an **IP range** for discovery in Figure 3.5 and click the **Update** button to register the changes.
- Finally, click the **Start** sub-node under the **Actions** node in the tree-structure to begin discovery.

4. Once discovery ends, proceed to figure out which BIND DNS servers have been automatically discovered by eG Enterprise. For that, invoke the Admin tile menu and follow the Infrastructure-> Components -> Manage/Unmanage/Delete menu sequence. Figure 3.6 will then appear.



Component type: Bind DNS

□ Show managed component types only

Managed components

Unmanaged components

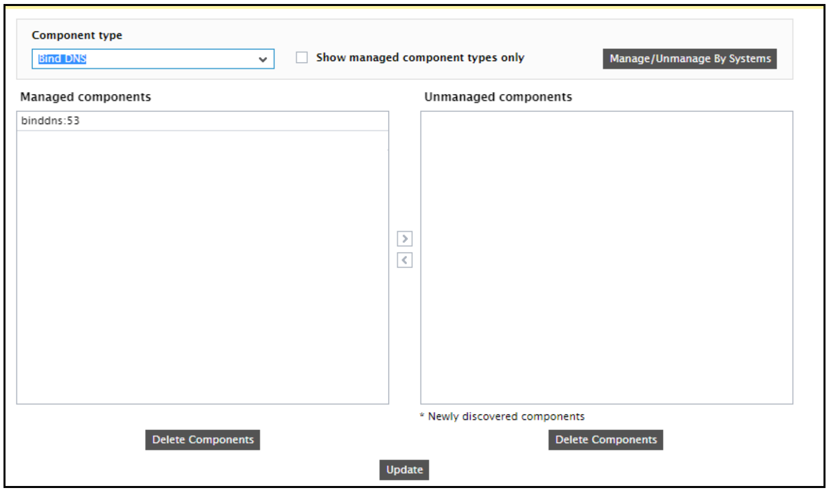
binddns:53 *

* Newly discovered components

Figure 3.6: Selecting the BIND DNS server to be monitored

5. Select Bind DNS as the Component type in Figure 3.6 . The auto-discovered BIND DNS servers will then appear in the **Unmanaged components** list. Newly discovered servers will be indicated by an asterisk (*) suffix.

6. To manage a discovered BIND DNS server, select the server from the **Unmanaged components** list and click the **<** button in Figure 3.6. This will transfer the selection to the **Managed components** list (see Figure 3.7).



Component type: Bind DNS

□ Show managed component types only

Managed components: binddns:53

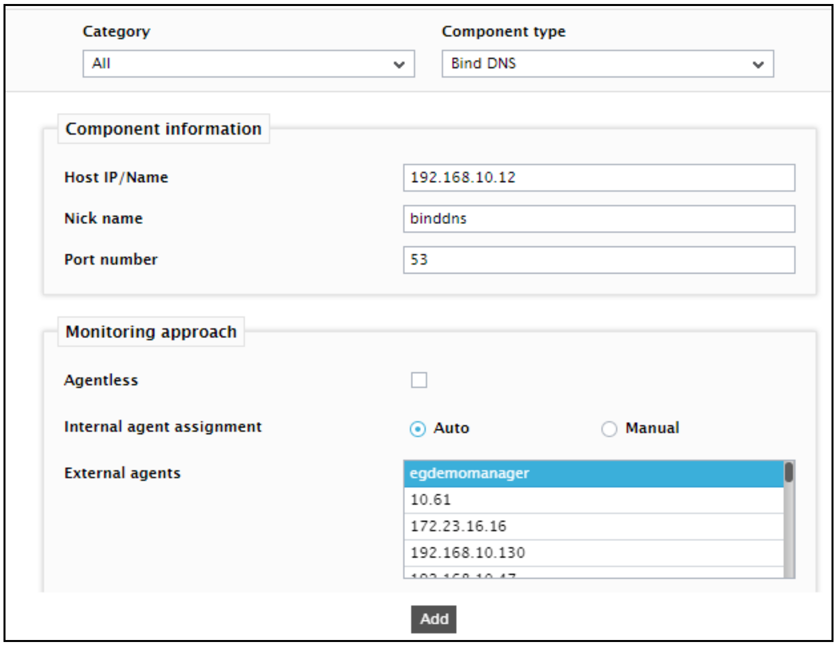
Unmanaged components:

Figure 3.7: Managing a BIND DNS server

7. Finally, click the **Update** button.

If for some reason the eG manager is unable to auto-discover the BIND DNS server, you can manually add the server for monitoring. For that, do the following:

1. Invoke the Admin tile menu and follow the Infrastructure -> Components -> Add/Modify menu sequence. In the page that appears next, select *Bind DNS* as the **Component type** and click the **Add New Component** button. Figure 3.8 will then appear.



Category: All

Component type: Bind DNS

Component information

Host IP/Name: 192.168.10.12

Nick name: binddns

Port number: 53

Monitoring approach

Agentless: □

Internal agent assignment: ● Auto ○ Manual

External agents:
- egdemomanager
- 10.61
- 172.23.16.16
- 192.168.10.130

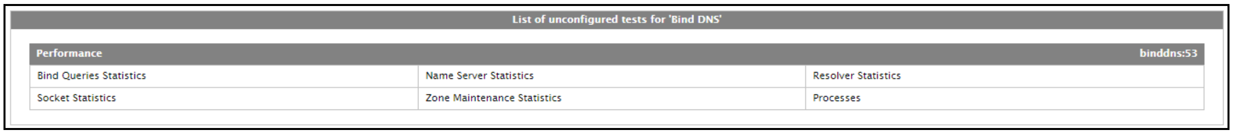
Figure 3.8: Manually adding a BIND DNS server

2. In Figure 3.8, specify the **Host IP/Name** of the BIND DNS server to be monitored and also assign a unique **Nick name** for that server.

3. Then, assign an **External agent** to monitor the network connectivity and traffic to/from the server and click the **Add** button in Figure 3.8 to add the server for monitoring.

3.2 Configuring Tests for the BIND DNS Server

Once you manage / manually add the BIND DNS server to be monitored, proceed to configure the tests for the server. For that, first attempt to sign out of the eG admin interface by clicking the **Sign out** button at the right, top corner of the eG admin interface. This will bring up the list of unconfigured tests for the BIND DNS server that has been managed (see Figure 3.9).

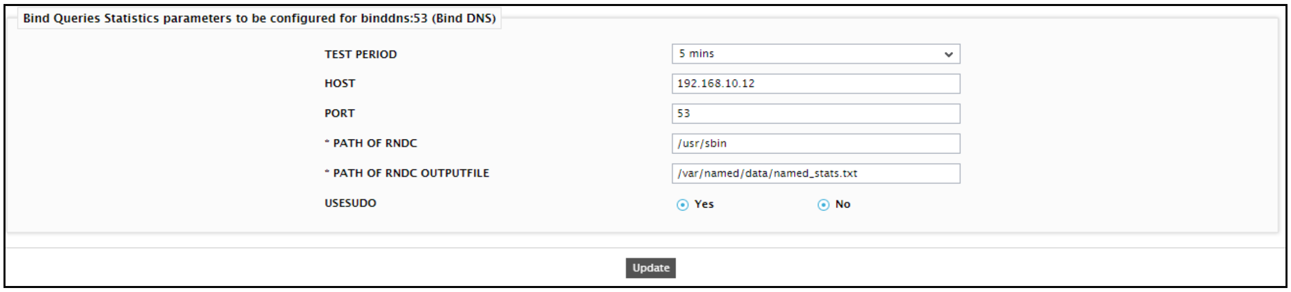


List of unconfigured tests for 'Bind DNS'

Performance		binddns:53
Bind Queries Statistics	Name Server Statistics	Resolver Statistics
Socket Statistics	Zone Maintenance Statistics	Processes

Figure 3.9: The list of unconfigured tests for the BIND DNS server

Click on any test in Figure 3.9 to configure it. For instance, clicking on the **Bind Query Statistics** test will reveal Figure 3.10, which displays the parameters that test takes and those that require manual configuration.

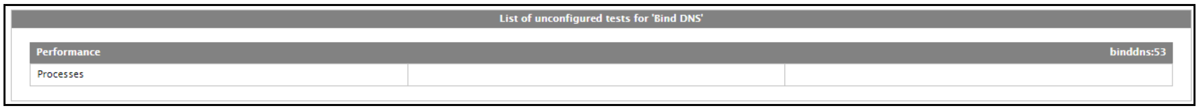


Bind Queries Statistics parameters to be configured for binddns:53 (Bind DNS)

TEST PERIOD	5 mins
HOST	192.168.10.12
PORT	53
* PATH OF RNDC	/usr/sbin
* PATH OF RNDC OUTPUTFILE	/var/named/data/named_stats.txt
USESUDO	● Yes ● No

Figure 3.10: Configuring the Bind Query Statistics test

To know how to configure this test, refer to the Section **4.1.1** topic. After successfully configuring this test, click the **Update** button in Figure 3.10 and once again attempt to Sign out of the eG admin interface. You will now be prompted to configure the **Processes** test (seeFigure 3.11).

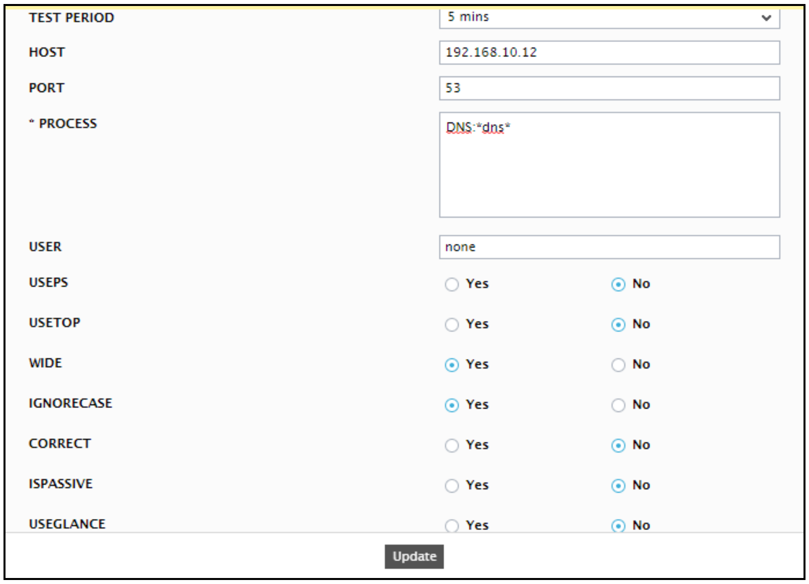


List of unconfigured tests for 'Bind DNS'

Performance		binddns:53
Processes		

Figure 3.11: The Processes test awaiting configuration

Click on the **Processes** test to configure it. Figure 3.12 will then appear displaying the parameters of **Processes** test.



TEST PERIOD	5 mins
HOST	192.168.10.12
PORT	53
* PROCESS	DNS:*dns*
USER	none
USEPS	○ Yes ● No
USETOP	○ Yes ● No
WIDE	● Yes ○ No
IGNORECASE	● Yes ○ No
CORRECT	○ Yes ● No
ISPASSIVE	○ Yes ● No
USEGLANCE	○ Yes ● No

Figure 3.12: Configuring Processes test

To know how to configure the parameters displayed in **Figure 4**, refer to the Processes Test topic in the *Monitoring Unix and Windows Servers* document. Once the **Processes** test is configured, click the **Update** button to register the changes and sign out of the eG admin interface.

Chapter 4: Monitoring BIND DNS

After correctly configuring the tests for BIND DNS, sign out of the eG admin interface. Then, log into the eG monitoring interface for viewing the current state of the managed BIND DNS server and the performance statistics it reports.

To report the real-time state and performance metrics of a BIND DNS server in the eG monitoring console, eG Enterprise uses a specialized Bind DNS monitoring model.

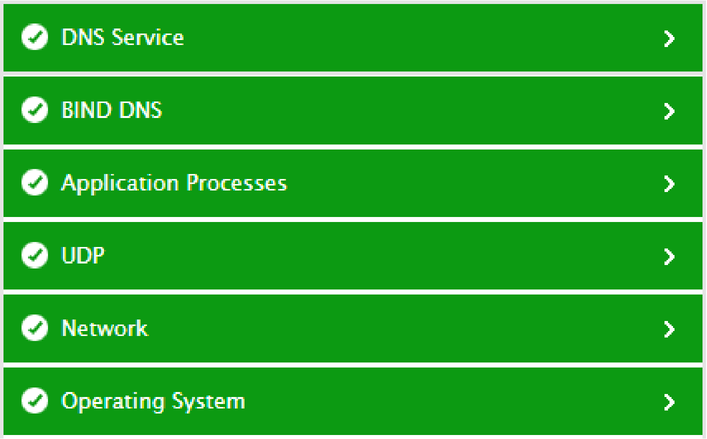


Figure 4.1: Layer model of BIND DNS

Each layer of this hierarchical model is mapped to tests that periodically verify and report on the availability, responsiveness, and operational efficiency of BIND DNS. Using the measures reported by these tests, administrators can find quick and accurate answers to persistent performance queries related to BIND DNS; these include the following:

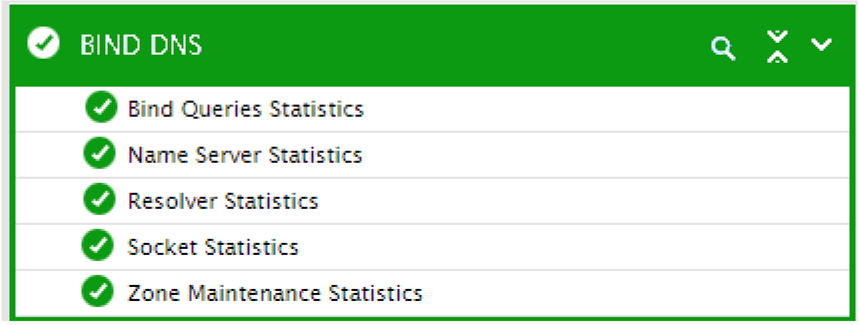
- Is the BIND DNS server accessible over the network? If so, how responsive is it to requests?
- What is the query load on BIND DNS? What Resource Record is contributing to that load? Is the server sized with adequate resources to handle the load?
- Did any query to BIND DNS result in an error response? If so, what type of response is it and what caused it?
- Were any queries rejected?
- Were any queries dropped?
- Is the resolver program delaying query processing? Are any queries taking an unusually long time to be processed by the resolver?

- Did any query fail at the resolver?
- Did the resolver retry many queries?
- Did the resolver receiver any error responses for the queries it forwarded? If so, what type of responses?
- Were zone transfers smooth, or did any transfer requests fail?
- Were notifies rejected during zone transfers?
- Did socket binding fail?

The bottom 4 layers of Figure 4.1 have been dealt with elaborately in the *Monitoring Unix and Windows Servers* document. The topmost layer, the **DNS Service** layer, has been discussed thoroughly in the *Monitoring DNS Server* document. The sub-section that will follow therefore will therefore discuss the **BIND DNS** layer only.

4.1 The BIND DNS Layer

The tests mapped to this layer monitor the queries to the bind server and reveal how well the server processes the queries. In addition, the tests also point to bottlenecks in query processing at the resolver and tracks zone transfers to capture transfer failures.



BIND DNS

- Bind Queries Statistics
- Name Server Statistics
- Resolver Statistics
- Socket Statistics
- Zone Maintenance Statistics

Figure 4.2: The tests mapped to the BIND DNS layer

4.1.1 Bind Queries Statistics Test

To be able to understand the workload of BIND DNS, you should track the flow of queries into the server and out of it (to other DNS servers). This is what the Bind Query Statistics test does. This test reports the count of incoming and outgoing queries for each Resource Record (RR) type of the target BIND DNS. Resource Records define data types in the Domain Name System (DNS). Typically, they are stored in binary format internally for use by the BIND DNS. When zone transfers are performed, Resource Records are sent across the network in text format. Some of the common RR types are as follows: A, AAAA, A6, AFSDB, CNAME, DNAME, DNSKEY, SRV, etc.

Using this test, administrators can easily assess the current load on the server and rapidly detect a potential overload condition. Moreover, in times of abnormal load, you can use this test to identify the RR that is seeing maximum traffic and is thus contributing to the load.

Target of the test : A BIND DNS server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Resource Record type in BIND DNS

Configurable parameters for the test

Parameter	**Description**
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	Refers to the port at which the specified host listens to. By default, this is 53.
Path of RNDC	To monitor BIND DNS, this test uses a name server control utility in bind called Remote Name Daemon Control (RNDC). RNDC is a command line utility that allows command line control of the administration and operations of a name server, both locally and remotely. Periodically, this test runs the **rndc stats** command of this utility to pull metrics of interest. To enable the test to run this command, configure the full path to the folder where RNDC is located, against Path of RNDC. The default location of RNDC is */usr/sbin*. If it is installed in a different location in your environment, then specify the same here.
Path of RNDC Output File	This test runs the **rndc stats** command of to pull metrics of interest from the target BIND DNS server. This command instructs BIND to dump the statistics to a *statistics-file* configured in the configuration file for the named server - */etc/named.conf*. To enable this test to read from this *statistics-file*, specify the full path to the *statistics-file* against Path of RNDC Output File. By default, metrics are written to the *named_stats.txt* file in the */var/named/data/* folder. If chroot is enabled, then this file will typically be available in the */var/named/chroot/var/named/data* folder.
Use SUDO	To run this test and report metrics, the eG agent install user should have permissions to run the **rndc stats** command and read from the *statistics-file*. If the eG agent install user possesses these privileges, then set the Use SUDO flag to **No**. If the eG agent install user does not have the required permissions, then do the following: • Edit the sudoers file on the target host and append an entry of the following format to it:

Parameter	Description
	<eG_agent_install_user>; ALL=(ALL) NOPASSWD:<Command>; For instance, if the eG agent install user is *eguser*, then the entry in the sudoers file should be: *eguser ALL=(ALL) NOPASSWD: rndc stats* • Then, save the file. • Finally, set the Use SUDO parameter to **Yes**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Incoming queries	Indicates the number of incoming queries for this Resource Record type.	Number	These are good measures of the current workload of BIND DNS. In the event of an overload, you can compare these metrics across RRs to know which RR is contributing to the load.
Outgoing queries	Indicates the number of outgoing queries for this Resource Record type.	Number	

4.1.2 Bind Name-Server Statistics Test

The efficiency of BIND DNS depends upon how well it handles the name resolution queries it receives. If BIND DNS is able to successfully service very few queries, and has been unable to service majority of the queries, it is a clear indicator of the poor health of BIND DNS. The Bind Name-Server Statistics test sheds light on such irregularities, prompts administrators to rapidly initiate corrective actions, and thus restore the BIND DNS to normalcy.

This test tracks the name resolution queries to BIND DNS and reports the count of queries that were processed successfully, the number of queries that failed, and the number that was dropped/rejected. This way, the test points to issues in query processing. Additionally, the test also captures the response codes returned by BIND DNS , thereby revealing error responses to administrators and their probable causes.

Target of the test : A BIND DNS server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the target BIND DNS

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	Refers to the port at which the specified host listens to. By default, this is 53.
Path of RNDC	To monitor BIND DNS, this test uses a name server control utility in bind called Remote Name Daemon Control (RNDC). RNDC is a command line utility that allows command line control of the administration and operations of a name server, both locally and remotely. Periodically, this test runs the **rndc stats** command of this utility to pull metrics of interest. To enable the test to run this command, configure the full path to the folder where RNDC is located, against Path of RNDC. The default location of RNDC is */usr/sbin*. If it is installed in a different location in your environment, then specify the same here.
Path of RNDC Output File	This test runs the **rndc stats** command of to pull metrics of interest from the target BIND DNS server. This command instructs BIND to dump the statistics to a *statistics-file* configured in the configuration file for the named server - */etc/named.conf*. To enable this test to read from this *statistics-file*, specify the full path to the *statistics-file* against Path of RNDC Output File. By default, metrics are written to the *named_stats.txt* file in the */var/named/data/* folder. If chroot is enabled, then this file will typically be available in the */var/named/chroot/var/named/data* folder.
Use SUDO	To run this test and report metrics, the eG agent install user should have permissions to run the **rndc stats** command and read from the *statistics-file*. If the eG agent install user possesses these privileges, then set the Use SUDO flag to **No**. If the eG agent install user does not have the required permissions, then do the following: • Edit the sudoers file on the target host and append an entry of the following format to it: *<eG_agent_install_user>; ALL=(ALL) NOPASSWD:<Command>;* For instance, if the eG agent install user is *eguser*, then the entry in the sudoers file should be: *eguser ALL=(ALL) NOPASSWD: rndc stats* • Then, save the file. • Finally, set the Use SUDO parameter to **Yes**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
IPv4 requests received	Indicates the number of IPv4 requests received by BIND DNS.	Number	These are good measures of the current workload of BIND DNS.
IPv6 requests received	Indicates the number of IPv6 requests received by BIND DNS.	Number	
Queries resulted in successful answer	Indicates the number of query which returns a NOERROR response.	Number	A high value is desired for this measure.
Queries resulted in authoritative answer	Indicates the number of queries that obtained response from the name servers, that have been configured by an original source.	Number	An authoritative name server provides actual answer to your DNS queries such as – mail server IP address or web site IP address (A resource record). It provides original and definitive answers to DNS queries. It does not provide just cached answers that were obtained from another name server. Therefore it only returns answers to queries about domain names that are installed in its configuration system. The value of this measure represents the count of queries that were processed by authoritative name servers.
Queries resulted in non-authoritative answer	Indicates the number of queries that obtain response from the Non-Authoritative name servers.	Number	
Queries resulted in nxrrset	Indicates the number of queries for which the name server returned the response NXRRSET.	Number	The value of this measure denotes the number of queries the name server handled that resulted in responses saying that the type of record the querier requested did not exist for the

Measurement	Description	Measurement Unit	Interpretation
			domain name it specified. Ideally, the value of this measure should be 0.
Queries resulted in SERVFAIL	Indicates the number of queries that resulted in SERVFAIL error.	Number	The value of this measure indicates the number of queries that the server failed to complete because of errors when communicating with the delegated name server. Ideally, the value of this measure should be 0.
Queries resulted in NXDOMAIN	Indicates the number of queries that resulted in NXDOMAIN error.	Number	The NXDOMAIN error occurs when the domain name queried does not exist. Ideally, the value of this measure should be 0.
Queries resulted in referral answer	Indicates the number of queries that resulted in a referral answer.	Number	The term referral indicates a response to a query which does not contain an answer section (it is empty) but which contains one or more authoritative name servers that are closer to the required query question.
Duplicate queries received	Indicates the number of queries which the server attempted to recurse, but discovered an existing query with the same IP address, port, query ID, name, type and class already being processed.	Number	
TCP requests received	Indicates the number of TCP requests received.	Number	
Auth queries rejected	Indicates the number of authoritative queries rejected.	Number	Ideally, these measures should report the value 0.
Recursive queries	Indicates the number of	Number	

Measurement	Description	Measurement Unit	Interpretation
rejected	recursive queries rejected.		
Update requests rejected	Indicates the number of update requests rejected.	Number	
Responses sent	Indicates the number of responses sent.	Number	
Queries dropped	Indicates the number of recursive queries dropped as there exists an excessive number of queries of same name, type and class.	Number	Ideally, the value of this measure should be 0.
Other query failures	Indicates the number of other query failures.	Number	Ideally, the value of this measure should be 0.
Queries caused recursion	Indicates the number of NS records that pointed to an incorrect host.	Number	A recursive query is one which the server attempts to service using its local cache. If it cannot find an answer, it will query other DNS servers until it finds the answer. The server will then respond to the original query with the results from each server's query. Ideally, the value of this measure should be 0 - i.e., recursion should be disabled. This is because, servers that support recursive queries are vulnerable to fake requests from a spoofed IP address (the victim of the attack). The spoofed IP address can get overwhelmed by the number of DNS results it receives and be unable to serve regular Internet traffic. This is called an Amplifier attack because this method takes advantage of DNS servers to reflect the attack onto a target while also amplifying the volume of packets sent to the victim. A consequence of this activity is that

Measurement	Description	Measurement Unit	Interpretation
			third party Network administrators who detect these requests may block your IP addresses. Your server could even be placed upon DNS blacklists.
Requests with EDNS(0) received	Indicates the number of EDNS(0) messages received.	Number	Extension mechanisms for DNS (EDNS) is a specification for expanding the size of several parameters of the Domain Name System (DNS) protocol which had size restrictions that the Internet engineering community deemed too limited for increasing functionality of the protocol. EDNS adds information to DNS messages in the form of pseudo-Resource Records ("pseudo-RRs") included in the "additional data" section of a DNS message. Note that this section exists in both requests and responses. EDNS introduces a single pseudo-RR type: *OPT*. As pseudo-RRs, *OPT* type RRs never appear in any zone file; they exist only in messages, fabricated by the DNS participants. The OPT pseudo-record provides space for up to 16 flags and it extends the space for the response code. The overall size of the UDP packet and the version number (at present 0) are contained in the OPT record. A variable length data field allows further information to be registered in future versions of the protocol.
Requests with EDNS(0) sent	Indicates the number of EDNS(0) messages sent.	Number	

4.1.3 Bind Resolver Statistics Test

A resolver is a program that resolves questions about names by sending those questions to appropriate servers and responding appropriately to the servers' replies. In the most common application, a web browser uses a local stub resolver library on the same computer to look up names in the DNS. That stub resolver is part of the operating system. (Many operating system distributions use the BIND resolver library.) The stub resolver usually will forward queries to a caching resolver, a server or group of servers on the network dedicated to DNS services. Those resolvers will send queries to one or multiple authoritative servers in order to find the IP address for that DNS name.

This means that latencies/errors experienced by the resolver can cause overall query processing by BIND DNS to significantly slow down. This is why, where name resolution queries take too long to provide answers, administrators should look at how much time the resolver program took to process those queries and if any queries failed at the resolver. The Bind Resolver Statistics test provides administrators with this insight.

This test monitors the queries sent/forwarded by the resolver program , and measures the average round trip time of the queries. Administrators are alerted if even one query registers an abnormally high round trip time. Query failures are also brought to the immediate attention of administrators, so that they can investigate the reason for the same and fix it. In addition, the test also tracks the responses received by the resolver program to queries it forwarded. In the process, the test sheds light on error responses and the probable reason for those errors.

Target of the test : A BIND DNS server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the target BIND DNS

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	Refers to the port at which the specified host listens to. By default, this is 53.
Path of RNDC	To monitor BIND DNS, this test uses a name server control utility in bind called Remote Name Daemon Control (RNDC). RNDC is a command line utility that allows command line control of the administration and operations of a name server, both locally and remotely. Periodically, this test runs the **rndc stats** command of this utility

Parameter	Description
	to pull metrics of interest. To enable the test to run this command, configure the full path to the folder where RNDC is located, against Path of RNDC. The default location of RNDC is */usr/sbin*. If it is installed in a different location in your environment, then specify the same here.
Path of RNDC Output File	This test runs the **rndc stats** command of to pull metrics of interest from the target BIND DNS server. This command instructs BIND to dump the statistics to a *statistics-file* configured in the configuration file for the named server - */etc/named.conf*. To enable this test to read from this *statistics-file*, specify the full path to the *statistics-file* against Path of RNDC Output File. By default, metrics are written to the *named_stats.txt* file in the */var/named/data/* folder. If chroot is enabled, then this file will typically be available in the */var/named/chroot/var/named/data* folder.
Use SUDO	To run this test and report metrics, the eG agent install user should have permissions to run the **rndc stats** command and read from the *statistics-file*. If the eG agent install user possesses these privileges, then set the Use SUDO flag to **No**. If the eG agent install user does not have the required permissions, then do the following: • Edit the sudoers file on the target host and append an entry of the following format to it: *<eG_agent_install_user>; ALL=(ALL) NOPASSWD:<Command>;* For instance, if the eG agent install user is *eguser*, then the entry in the sudoers file should be: *eguser ALL=(ALL) NOPASSWD: rndc stats* • Then, save the file. • Finally, set the Use SUDO parameter to **Yes**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
IPv4 queries sent	Indicates the number of IPv4 queries sent by the resolver.	Number	These are good measures of the current workload of the resolver program.
IPv6 queries sent	Indicates the number of IPv6 queries sent by the resolver.	Number	

Measurement	Description	Measurement Unit	Interpretation
IPv4 responses received	Indicates the number of IPv4 responses received by the resolver.	Number	
IPv6 responses received	Indicates the number of IPv6 responses received by the resolver.	Number	
Queries resulted in successful answer	Indicates the number of queries which returned a NOERROR response.	Number	A high value is desired for this measure.
Queries with RTT less than 10ms	Indicates the number of queries with round trip time (RTT) less than 10 ms.	Number	A high value is desired for this measure.
Queries with RTT 10 to 100ms	Indicates the number of queries with round trip time (RTT) between 10 ms and 100 ms.	Number	Ideally, the value of this measure should be 0. A non-zero value indicates that one/more queries are slow.
Queries with RTT 100 to 500ms	Indicates the number of queries with round trip time (RTT) between 100 ms and 500 ms.	Number	Ideally, the value of this measure should be 0. A non-zero value indicates that one/more queries are slow.
Queries with RTT 500 to 800ms	Indicates the number of queries with round trip time (RTT) between 500 ms and 800 ms.	Number	Ideally, the value of this measure should be 0. A non-zero value indicates that one/more queries are slow.
Queries with RTT 800 to 1600ms	Indicates the number of queries with round trip time (RTT) between 800 ms and 1600 ms.	Number	Ideally, the value of this measure should be 0. A non-zero value indicates that one/more queries are slow.
Queries with RTT more than 1600ms	Indicates the number of queries with round trip time (RTT) over 1600 ms.	Number	Ideally, the value of this measure should be 0. A non-zero value indicates that one/more queries are slow.
NXDOMAIN received	Indicates the number of queries that resulted in NXDOMAIN error.	Number	The NXDOMAIN error occurs when the domain name queried does not exist. Ideally, the value of this measure should

Measurement	Description	Measurement Unit	Interpretation
			be 0.
SERVFAIL received	Indicates the number of queries that resulted in SERVFAIL error.	Number	The value of this measure indicates the number of queries that the server failed to complete because of errors when communicating with the delegated name server. Ideally, the value of this measure should be 0.
FORMERR received	Indicates the number of queries that resulted in FORMERR error.	Number	A non-zero value of this measure indicates that one/more FORMERR errors have occurred. A FORMERR refers to a DNS query format error.
Other errors received	Indicates the number of queries that resulted in errors other than the NXDOMAIN, SERVFAIL, and FORMERR errors.	Number	Ideally, the value of this measure should be 0.
Query retries	Indicates the number of query retries that were performed by the resolver program.	Number	Higher the number of retries slower will be query processing. Ideally therefore, this measure value should be very low.
Query timeouts	Indicates the number of query timeouts.	Number	The default timeout value for the first round of queries at the resolver is 5 seconds er name server. After each round of queries, the resolver doubles the initial timeout. BIND 8.2 and previous resolvers send a total of four rounds of queries; BIND 8.2.1 and later resolvers send two. There is no way to modify the timeouts in a Windows resolver. However, the default timeouts are fairly short in newer Windows resolvers (one second for the first query in Windows 2000, for example), so adjusting them may not be necessary.

Measurement	Description	Measurement Unit	Interpretation
Lame delegations received	Indicates the number of queries that could not be serviced due to lame delegations.	Number	A lame delegation occurs when an authoritative DNS server (eg. .com) has a delegation (eg.lamedelegation.com) to other DNS server that are not authoritative for this zone. Ideally, the value of this measure should be 0.
IPv4 NS address fetches	Indicates the number of IPv4 NS address fetches invoked.	Number	
IPv4 NS address fetch failed	Indicates the number of IPv4 NS address fetches failed.	Number	Ideally, the value of this measure should be 0.
EDNS(0) query failures	Indicates the number of EDNS(0) query failures.	Number	Extension mechanisms for DNS (EDNS) is a specification for expanding the size of several parameters of the Domain Name System (DNS) protocol which had size restrictions that the Internet engineering community deemed too limited for increasing functionality of the protocol. EDNS adds information to DNS messages in the form of pseudo-Resource Records ("pseudo-RR"s) included in the "additional data" section of a DNS message. Note that this section exists in both requests and responses. EDNS introduces a single pseudo-RR type: *OPT*. As pseudo-RRs, *OPT* type RRs never appear in any zone file; they exist only in messages, fabricated by the DNS participants. The OPT pseudo-record provides space for up to 16 flags and it extends the space for the response code. The

Measurement	Description	Measurement Unit	Interpretation
			overall size of the UDP packet and the version number (at present 0) are contained in the OPT record. A variable length data field allows further information to be registered in future versions of the protocol. Ideally, the value of this measure should be 0.

4.1.4 Bind Socket Statistics Test

This test reports UDP and TCP I/O statistics for every socket type on BIND DNS. The socket types monitored include *IPv4, IPv6, FDWatch, and Unix (Domain)*.

Target of the test : A BIND DNS server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each socket type supported by the target BIND DNS.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	Refers to the port at which the specified host listens to. By default, this is 53.
Path of RNDC	To monitor BIND DNS, this test uses a name server control utility in bind called Remote Name Daemon Control (RNDC). RNDC is a command line utility that allows command line control of the administration and operations of a name server, both locally and remotely. Periodically, this test runs the **rndc stats** command of this utility to pull metrics of interest. To enable the test to run this command, configure the full path to the folder where RNDC is located, against Path of RNDC. The default location of RNDC is */usr/sbin*. If it is installed in a different location in your environment, then specify the same here.
Path of RNDC Output File	This test runs the **rndc stats** command of to pull metrics of interest from the target BIND DNS server. This command instructs BIND to dump the statistics to a

Parameter	Description
	statistics-file configured in the configuration file for the named server - */etc/named.conf*. To enable this test to read from this *statistics-file*, specify the full path to the *statistics-file* against Path of RNDC Output File. By default, metrics are written to the *named_stats.txt* file in the */var/named/data/* folder. If chroot is enabled, then this file will typically be available in the */var/named/chroot/var/named/data* folder.
Use SUDO	To run this test and report metrics, the eG agent install user should have permissions to run the **rndc stats** command and read from the *statistics-file*. If the eG agent install user possesses these privileges, then set the Use SUDO flag to **No**. If the eG agent install user does not have the required permissions, then do the following: • Edit the sudoers file on the target host and append an entry of the following format to it: *<eG_agent_install_user>; ALL=(ALL) NOPASSWD:<Command>;* For instance, if the eG agent install user is *eguser*, then the entry in the sudoers file should be: *eguser ALL=(ALL) NOPASSWD: rndc stats* • Then, save the file. • Finally, set the Use SUDO parameter to **Yes**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
UDP sockets opened	Indicates the number of UDP sockets of this type that are open.	Number	This measure will not be reported for the FDWatch socket type.
UDP sockets closed	Indicates the number of UDP sockets of this type that are closed.	Number	
UDP socket bind failures	Indicates the number of failures of binding UDP sockets of this type.	Number	
UDP connections established	Indicates the number of UDP connections successfully established	Number	

Measurement	Description	Measurement Unit	Interpretation
	with sockets of this type.		
TCP sockets opened	Indicates the number of TCP sockets of this type that are open.	Number	This measure will not be reported for the FDWatch socket type.
TCP sockets closed	Indicates the number of TCP sockets of this type that are closed.	Number	
TCP socket connect failures	Indicates the number of failed connection attempts to TCP sockets of this type.	Number	Ideally, the value of this measure should be 0.
TCP connections established	Indicates the number of TCP connections successfully established with sockets of this type.	Number	
TCP send errors	Indicates the number of errors in TCP send operations of this socket type.	Number	Ideally, the value of this measure should be 0.
TCP received errors	Indicates the number of errors in TCP receive operations of this socket type.	Number	Ideally, the value of this measure should be 0.

4.1.5 Bind Zone Maintenance Statistics Test

A zone is a point of delegation in the DNS tree. A zone consists of those contiguous parts of the domain tree for which a name server has complete information and over which it has authority. It contains all domain names from a certain point downward in the domain tree except those which are delegated to other zones. A delegation point is marked by one or more NS records in the parent zone, which should be matched by equivalent NS records at the root of the delegated zone.

The data for each zone is stored in a name server, which answers queries about the zone using the DNS protocol.

Each zone is served by at least one authoritative name server, which contains the complete data for the zone. The authoritative server where the master copy of the zone data is maintained is called the primary master server, or simply the primary. The other authoritative servers, the slave servers (also known as secondary servers) load the zone contents from another server using a replication process known as a zone transfer. Typically the data are transferred directly from the primary master, but it is also possible to transfer it from another slave. In other words, a slave server may itself act as a master to a subordinate slave server.

A zone transfer is typically triggered under the following circumstances:

- Refresher timer expiry: Each zone's SOA record holds a refresh timer that all slave servers receiving a copy of the zone should use. The refresh timer tells a slave server how often it should ask one of the master servers to which it has been configured to refer for an SOA record. This is then compared to the SOA the slave is holding - if it is the same, there is nothing to be done (and the slave waits until the next refresh interval expiry). There is also a retry timer which is applied if the refresh attempt fails (none of the master servers could be contacted). And finally, there's an expire timer - if the slave has been unable to contact another master for this period, then it stops serving data from that zone. (Note that restarting the slave will reset any 'expired' zones, so if they have a copy of the zone backed up to file, they will then resume serving the expired zone.)
- Notify received: When an authoritative (master or slave) server updates a zone, it can send out notifications to other servers that it has changed. This causes the recipients to set their 'next refresh' time to 'now' and to queue a zone refresh.

Sometimes, zone transfers may fail. If administrators are not promptly alerted to such anomalies, then the zone data on one/more slaves may not be in sync with that of the primary master for long time periods. In some other cases, slaves may reject NOTIFY requests from the primary master. If such inconsistencies go undetected, then some slaves may remain oblivious to changes made to zone data on the master, thereby failing to initiate a much-needed zone transfer. To avoid such abnormalities, it is imperative that zone transfers are monitored. This is exactly what the Bind Zone Maintenance Statistics test does!

This test monitors zone transfers, tracks the notifies sent and received during the transfers, and in the process, captures transfer failures and rejected notifies. This way, administrators can instantly detect issues hampering zone transfers and can rapidly initiate measures to resolve those issues, so that the zone data on the primary master and slaves remain in sync always.

Target of the test : A BIND DNS server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the target BIND DNS

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	Refers to the port at which the specified host listens to. By default, this is 53.
Path of RNDC	To monitor BIND DNS, this test uses a name server control utility in bind called Remote Name Daemon Control (RNDC). RNDC is a command line utility that allows command line control of the administration and operations of a name server, both locally and remotely. Periodically, this test runs the **rndc stats** command of this utility to pull metrics of interest. To enable the test to run this command, configure the full path to the folder where RNDC is located, against Path of RNDC. The default location of RNDC is */usr/sbin*. If it is installed in a different location in your environment, then specify the same here.
Path of RNDC Output File	This test runs the **rndc stats** command of to pull metrics of interest from the target BIND DNS server. This command instructs BIND to dump the statistics to a *statistics-file* configured in the configuration file for the named server - */etc/named.conf*. To enable this test to read from this *statistics-file*, specify the full path to the *statistics-file* against Path of RNDC Output File. By default, metrics are written to the *named_stats.txt* file in the */var/named/data/* folder. If chroot is enabled, then this file will typically be available in the */var/named/chroot/var/named/data* folder.
Use SUDO	To run this test and report metrics, the eG agent install user should have permissions to run the **rndc stats** command and read from the *statistics-file*. If the eG agent install user possesses these privileges, then set the Use SUDO flag to **No**. If the eG agent install user does not have the required permissions, then do the following: • Edit the sudoers file on the target host and append an entry of the following format to it: *<eG_agent_install_user>; ALL=(ALL) NOPASSWD:<Command>;* For instance, if the eG agent install user is *eguser*, then the entry in the sudoers file should be: *eguser ALL=(ALL) NOPASSWD: rndc stats* • Then, save the file. • Finally, set the Use SUDO parameter to **Yes**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
IPv4 notifies sent	Indicates the number of IPv4 notifies sent during zone transfers.	Number	
IPv4 notifies received	Indicates the number of IPv4 notifies received during zone transfers.	Number	
IPv6 notifies sent	Indicates the number of IPv6 notifies sent during zone transfers.	Number	
IPv6 notifies received	Indicates the number of IPv6 notifies received during zone transfers.	Number	
Transfer requests succeeded	Indicates the number of zone transfer requests that succeeded.	Number	A high value is desired for this measure.
Transfer requests failed	Indicates the number of transfer requests that failed.	Number	Ideally, the value of this measure should be 0. A non-zero value denotes that one/more transfer requests failed. Common reasons for zone transfer failures are as follows: • If the TCP connection between master and slave is reset, it can cause the zone transfer to fail. This TCP connection can get reset due to the **tcp-listen-queue** not being increased in line with the real-time load. **tcp-listen-queue** is a subtle control setting (although not applicable to all OS environments). When there is a high rate of inbound TCP connections, it controls how

Measurement	Description	Measurement Unit	Interpretation
			many connections can be queued before they are accepted by the application. If named has already reached both the limit on concurrent zone transfers, and the limit specified by tcp-listen-queue, then any new inbound TCP connections will be dropped. If you're expecting a high rate of zone transfers or that zone transfer requests will be competing for master server resources, then you should increase this configuration option, whose default is 3 (increased to 10 from BIND 9.10, 9.9.4, 9.8.6 and 9.6-ESV-R10). • Master is inaccessible from the slave due to routing or firewall issues;
Notifies rejected	Indicates the number of zone transfer requests that were rejected.	Number	When a slave receives a NOTIFY request for a zone from one of its configured master name servers, it responds with a NOTIFY response. If a slave is not able to directly communicate with the primary master and uses another slave as their master, it will reject the NOTIFY request from the master.

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.