Monitoring DNS Server

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Domain Name System (DNS) is the name resolution protocol for TCP/IP networks, such as the Internet. Client computers query a DNS server to resolve memorable, alphanumeric DNS names to the IP addresses that computers use to communicate with each other.

Imagine a situation where the DNS server is rendered temporarily unavailable. If a client computer attempts to send across a critical information request to a server at this time, the attempt is sure to fail due to the absence of the DNS server to translate the human-readable DNS name to a machine-readable IP address. In an environment where there is continuous exchange of data between components, such unplanned DNS server failures can result in total chaos!

In order to avoid such problem conditions, the performance of the DNS server should be constantly monitored. This is where the eG Enterprise helps administrators.

Chapter 2: How to Monitor the DNS Server Using eG Enterprise?

eG Enterprise is capable of monitoring the DNS servers in both agent-based and agentless manners. In the agent-based monitoring approach, the eG agent installed on the host monitors the performance of the DNS servers. For monitoring the DNS servers in the agentless manner, install an eG agent on the remote Windows host. This remote agent connects to the DNS server and collects the critical measures pertaining to it's performance.

2.1 Managing the DNS Server

The eG Enterprise can automatically discover the DNS servers. By default, the DNS servers use UDP port 53 for this operation. Auto-discovered DNS servers are set as unmanaged by default. To manage the auto-discovered servers, do the following;

1. Login to the eG administrative interface.
2. Follow Components -> Manage / Unmanage / Delete menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENTS – MANAGE / UNMANAGE** page that appears (see Figure 2.1 and Figure 2.2, choose the auto-discovered DNS server that should be monitored. If the DNS server to be monitored is not auto-discovered, use the **COMPONENTS** page to manually add the server.

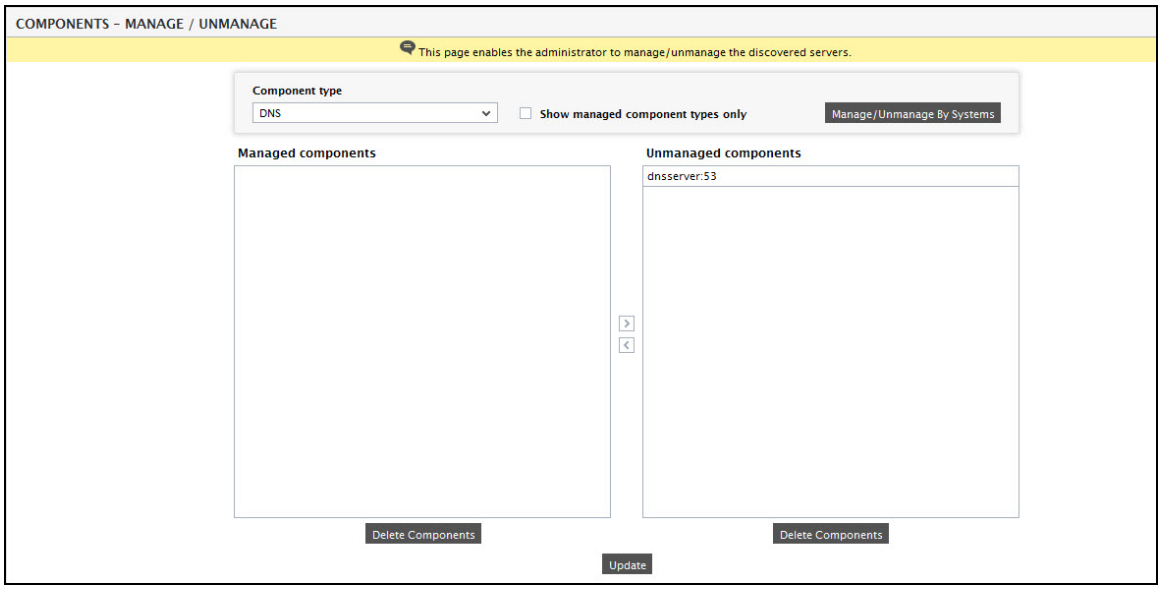

Figure 2.1: Viewing unmanaged DNS servers

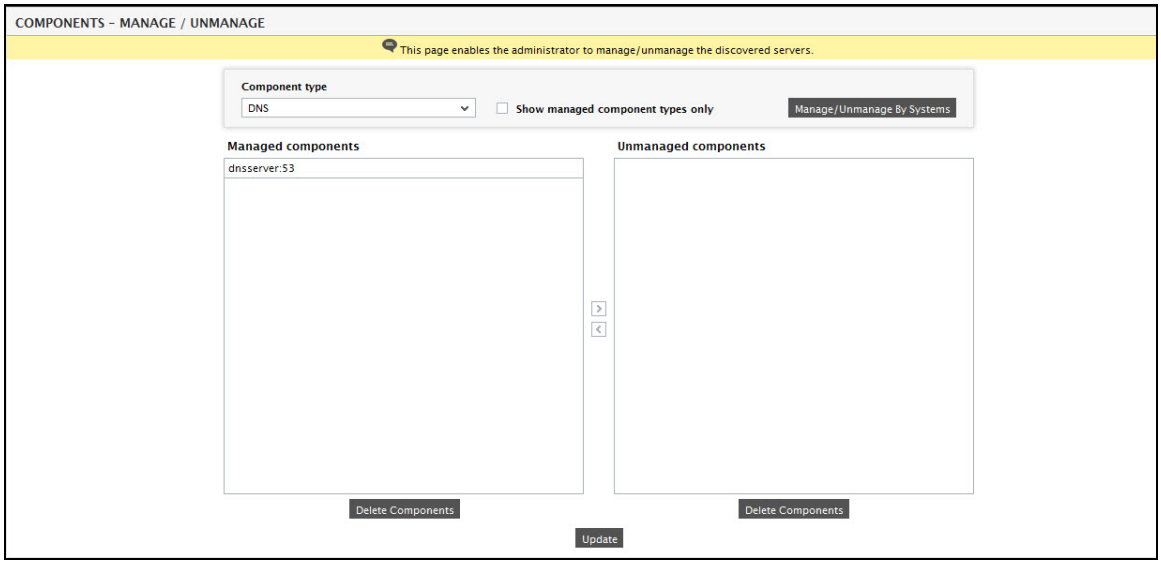

Figure 2.2: Managing DNS servers

4. When you attempt to sign out of the eG administrative interface, you will be prompted to configure the **Processes** test for the DNS server. Click on **Processes** test to configure it. To know how to configure the test, refer to *Monitoring Windows and Unix Servers* document.
5. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring the DNS Servers

eG Enterprise prescribes a specialized *DNS* server monitoring model (see Figure 3.1), which executes tests on the DNS server at pre-configured intervals to determine the following:

- Resource usage levels of the DNS host
- The TCP connection load on the host
- The health of the network traffic to and from the host
- The availability of the DNS server, and its responsiveness to user requests

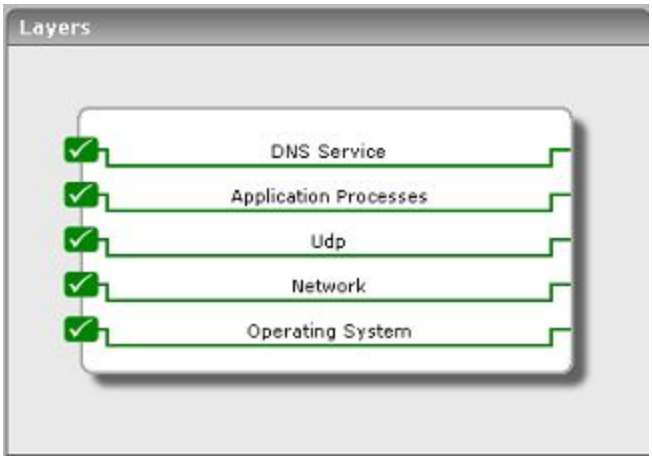

Figure 3.1: eG Enterprise's model of a DNS server

Since the DNS service is based on the UDP protocol, the layer model includes measures of the status of the UDP stack of a host. The **Application Processes** layer tracks the health of the processes corresponding to the DNS server. On Unix systems, the “named” process supports the DNS service.

Since the bottom 4 layers of Figure 3.1 have been extensively discussed in the *Monitoring Unix and Windows Servers* document, let us focus only on the **DNS Service** layer.

3.1 The DNS Service Layer

This layer tracks the health of the DNS service. To measure the state of a DNS server, the eG agent uses a Dns test shown in Figure 3.2.

Figure 3.2: Tests mapping to the DNS Service layer

3.1.1 Name Resolutions Test

This test emulates a client accessing a DNS server to issue a query. The query can either request the DNS server to resolve a domain name to an IP address or vice versa. Based on the response reported by the server, measurements are made of the availability and responsiveness of the DNS server.

The DNS service is organized hierarchically, i.e., one DNS server can forward a client request to another server to resolve the client's query. To ensure that the results of the query reflect the state of a DNS server in isolation, a non-recursive query is issued by this test.

Target of the test : A DNS server

Agent deploying the test : An external agent

Outputs of the test : One set of results per target configured.

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	The port on which the specified host is listening
Targets	The IP address or host name to be resolved during the test. Multiple targets can be specified as a comma-separated list.
Recursive	A DNS server supports two types of queries. For a non-recursive query, the DNS

Parameter	Description
	server attempts to respond to the request based on its local cache only. For a recursive query, a DNS server may use other DNS servers to respond to a request. The Recursive flag can be used to determine the type of queries to be issued to a DNS server.
UseEXE	In older versions of the eG Enterprise Suite, this test used native APIs to collect the desired metrics. To ensure backward compatibility with older versions of the solution, this flag has been set to **Yes** by default. Set this flag to **No** if you want the test to use Java APIs instead to determine the availability and responsiveness of the DNS server. **This flag is only relevant if the test is being executed by an external agent operating on a Windows host.**

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
DNS availability	Whether a successful response is received from the DNS server in response to the emulated user request.	Percent	An availability problem can be caused by different factors - e.g., the server process may not be up, a network problem may exist, or there could be a configuration problem with the DNS server.
DNS response time	Time taken (in seconds) by the server to respond to a request.	Secs	An increase in response time can be caused by several factors such as a server bottleneck, a configuration problem with the DNS server, a network problem, etc.

Chapter 4: Monitoring Windows DNS Servers

The eG Enterprise suite automatically discovers DNS servers running on Windows environments. For such servers, the eG Enterprise suite prescribes an exclusive Windows DNS monitoring model depicted by Figure 4.1 below:

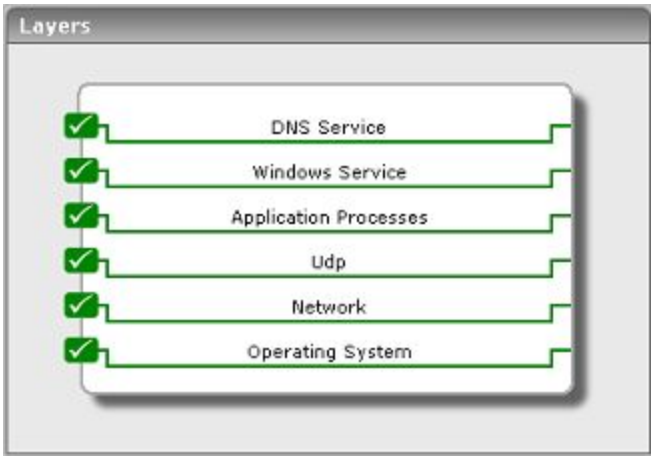

Figure 4.1: Layer model of the Windows DNS server

The additional **Windows Service** layer in Figure 4.1 reveals whether/not the critical DNS service is up and running on the Windows host. This layer and all the 4 layers below it have been discussed extensively in the *Monitoring Windows and Unix Servers* document. The section to come therefore talks only of the **DNS Service** layer.

4.1 The DNS Service Layer

Besides the DNS test that is common to both the DNS and Windows DNS servers, the DNS Service layer of a Windows DNS server is mapped to two additional tests – the WindowsDns test and the DNSEvt test (see Figure 4.2).

Figure 4.2: The DNS Service layer of a Windows DNS server

4.1.1 Windows DNS Test

This test reports various performance statistics pertaining to the DNS server running on Windows.

Target of the test : A DNS server running on Windows

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every DNS server being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port on which the specified host is listening

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total queries	The rate of queries received by the DNS server	Reqs/sec	Indicates the workload of the DNS server
Total responses	The rate of responses from the DNS server to clients	Resp/sec	Ideally, the total responses should match the total queries. Significant

Measurement	Description	Measurement Unit	Interpretation
			differences between the two can indicate that the DNS server is not able to handle the current workload.
Recursive queries	The rate of recursive queries successfully handled by the DNS server	Reqs/sec	The ratio of recursive queries to total queries indicates the number of queries that required the DNS server to communicate with other DNS servers to resolve the client requests.
Recursive query failures	The rate of recursive queries that could not be resolved by the DNS server	Reqs/sec	Query failures can happen due to various reasons - e.g., requests from clients to invalid domain names/IP addresses, failure in the external network link thereby preventing a DNS server from communicating with other DNS servers on the Internet, failure of a specific DNS server to which a DNS server is forwarding all its requests, etc. A small percentage of failures is to be expected in any production environment. If a significant percentage of failures are happening, this could result in application failures due to DNS errors.
Recursive timeouts	The rate of recursive queries that failed because of timeouts	Reqs/sec	Timeouts can happen because of a poor external link preventing a DNS server from communicating with others. In some cases, improper/invalid domain name resolution requests can also result in timeouts. DNS timeouts can adversely affect application performance and must be monitored continuously.
Zone transfers received	The number of zone transfer requests received by a DNS	Reqs	Zone transfers are resource intensive. Moreover, zone transfers to unauthorized clients can make an IT environment vulnerable to security

Measurement	Description	Measurement Unit	Interpretation
			attacks. Hence, it is important to monitor the number of zone transfer requests and responses on a periodic basis.
Zone transfers failed	The number of zone transfers that were not serviced by the DNS server in the last measurement period	Reqs	Zone transfers may fail either because the DNS server does not have resources, or the request is not valid, or the client requesting the transfer is not authorized to receive the results.

4.1.2 DNS Events Test

This test reports statistical information about the DNS Service events recorded in the DNS Service event log.

Target of the test : A DNS server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for the Filter configured.

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 used by the EventLog Service. Here it is null
LogType	Refers to the type of event logs to be monitored. The default value is *application*.
Policy Based Filter	Using this page, administrators can configure the event sources, event IDs, and event descriptions to be monitored by this test. In order to enable administrators to easily and accurately provide this specification, this page provides the following options: • Manually specify the event sources, IDs, and descriptions in the Filter text area, or, • Select a specification from the predefined filter policies listed in the Filter box For explicit, manual specification of the filter conditions, select the **No** option against the Policy Based Filter field. This is the default selection. To choose from the list of pre-

Parameter	Description
	configured filter policies, or to create a new filter policy and then associate the same with the test, select the **Yes** option against the Policy Based Filter field.
Filter	If the Policy Based Filter flag is set to **No**, then a **Filter** text area will appear, wherein you will have to specify the event sources, event IDs, and event descriptions to be monitored. This specification should be of the following format: *{Displayname}:{event_sources_to_be_included}:{event_sources_to_be_excluded}:{event_IDs_to_be_included}:{event_IDs_to_be_excluded}:{event_descriptions_to_be_included}:{event_descriptions_to_be_excluded}*. For example, assume that the Filter text area takes the value, *OS_events:all:Browse,Print:all:none:all:none*. Here: • *OS_events* is the display name that will appear as a descriptor of the test in the monitor UI; • *all* indicates that all the event sources need to be considered while monitoring. To monitor specific event sources, provide the source names as a comma-separated list. To ensure that none of the event sources are monitored, specify *none*. • Next, to ensure that specific event sources are excluded from monitoring, provide a comma-separated list of source names. Accordingly, in our example, *Browse* and *Print* have been excluded from monitoring. Alternatively, you can use *all* to indicate that all the event sources have to be excluded from monitoring, or *none* to denote that none of the event sources need be excluded. • In the same manner, you can provide a comma-separated list of event IDs that require monitoring. The *all* in our example represents that all the event IDs need to be considered while monitoring. • Similarly, the *none* (following *all* in our example) is indicative of the fact that none of the event IDs need to be excluded from monitoring. On the other hand, if you want to instruct the eG Enterprise system to ignore a few event IDs during monitoring, then provide the IDs as a comma-separated list. Likewise, specifying *all* makes sure that all the event IDs are excluded from monitoring. • The all which follows implies that all events, regardless of description, need to be included for monitoring. To exclude all events, use none. On the other hand, if

Parameter	Description
	you provide a comma-separated list of event descriptions, then the events with the specified descriptions will alone be monitored. Event descriptions can be of any of the following forms - desc*, or desc, or *desc*,or desc*, or desc1*desc2, etc. desc here refers to any string that forms part of the description. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters. • In the same way, you can also provide a comma-separated list of event descriptions to be excluded from monitoring. Here again, the specification can be of any of the following forms: desc*, or desc, or *desc*,or desc*, or desc1*desc2, etc. desc here refers to any string that forms part of the description. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters. In our example however, none is specified, indicating that no event descriptions are to be excluded from monitoring. If you use all instead, it would mean that all event descriptions are to be excluded from monitoring. By default, the filter parameter contains the value: *all:all:none:all:none:all:none*. Multiple filters are to be separated by semi-colons (;). **Note:** The event sources and event IDs specified here should be exactly the same as that which appears in the Event Viewer window. On the other hand, if the Policy Based Filter flag is set to **Yes**, then a **Filter** list box will appear, displaying the filter policies that pre-exist in the eG Enterprise system. A filter policy typically comprises of a specific set of event sources, event IDs, and event descriptions to be monitored. This specification is built into the policy in the following format: *{Policyname}:{event_sources_to_be_included}:{event_sources_to_be_excluded}:{event_IDs_to_be_included}:{event_IDs_to_be_excluded}:{event_descriptions_to_be_included}:{event_descriptions_to_be_excluded}* To monitor a specific combination of event sources, event IDs, and event descriptions, you can choose the corresponding filter policy from the Filter list box. Multiple filter policies can be so selected. Alternatively, you can modify any of the existing policies to suit your needs, or create a new filter policy. To facilitate this, a **Click here** link appears just above the test configuration section, once the **Yes** option is chosen

Parameter	Description
	against Policy Based Filter. Clicking on the **Click here** link leads you to a page where you can modify the existing policies or create a new one. The changed policy or the new policy can then be associated with the test by selecting the policy name from the Filter list box in this page.
UseWMI	The eG agent can either use **WMI** to extract event log statistics or directly parse the event logs using **event log APIs**. If the UseWMI flag is **Yes**, then **WMI** is used. If not, the **event log APIs** are used. This option is provided because on some Windows 2000 systems (especially ones with service pack 3 or lower), the use of WMI access to event logs can cause the CPU usage of the WinMgmt process to shoot up. On such systems, set the UseWMI parameter value to **No**.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
DNS Errors	This refers to the number of DNS Service events that were generated.	Number	A very low value (zero) indicates that the DNS Service is in a healthy state without any potential problems. An increasing trend or high value

Measurement	Description	Measurement Unit	Interpretation
			indicates the existence of problems like loss of functionality or data. The detailed diagnosis capability, if enabled, lists the description of specific events. Please check the Application Logs in the Event Log Viewer for more details.
DNS information count	This refers to the number of DNS Service information events generated when the test was last executed.	Number	A change in the value of this measure may indicate infrequent but successful operations performed by the DNS Service. The detailed diagnosis capability, if enabled, lists the description of specific events.
DNS Warnings	This refers to the number of warnings that were generated when the test was last executed.	Number	A high value of this measure indicates problems that may not have an immediate impact, but may cause future problems in the DNS Service. The detailed diagnosis capability, if enabled, lists the description of specific events.

4.1.3 DNS Server Checks Test

If the DNS server is inaccessible or is unable to provide domain name resolution services, then users may be denied access to their mission-critical servers and applications. Under such circumstances, you may want to quickly check what is stalling the operations of your DNS server, so that the source of the issue can be isolated and eliminated. This test enables you to perform such a check, periodically. To perform this check, this test uses the **DCDIAG** utility that ships with Windows 2003 Support Tools and is built into Windows 2008 R2 and Windows 2008 Server. **DCDIAG** is a command-line tool that encapsulates detailed knowledge of how to identify abnormal behavior in a system. For validating DNS health, the **DCDIAG** utility runs six tests, each of which reports the current state of a critical performance aspect of the DNS server; these DNS tests are as follows:

a. **Authentication**: This test is run by default and checks the following:

   - Are domain controllers registered in DNS?
   - Can they be pinged?
   - Do they have Lightweight Directory Access Protocol/Remote Procedure Call (LDAP/RPC)?

b. **Basic**: Performs basic DNS tests, including network connectivity, DNS client configuration, service availability, and zone existence.

c. **Forwarders**: Performs the **Basic** tests, and also checks the configuration of forwarders

d. **Delegation:** Performs the **Basic** tests, and also checks for proper delegations

e. **Dynamic Update:** Performs the **Basic** tests, and also determines if dynamic update is enabled in the Active Directory zone

f. **Record Registration**: Performs the **Basic** tests, and also checks if the address (A), canonical name (CNAME) and well-known service (SRV) resource records are registered. In addition, creates an inventory report based on the test results.

The **DNS Server Checks** test uses the **DCDIAG.exe** to execute each of the above-mentioned tests at configured intervals, reports the output of each test, promptly captures current/potential DNS failures, and provides detailed diagnostics describing the reasons for the failure. This way, administrators are enabled to troubleshoot DNS-related issues quickly and efficiently.

Note:

For this test to run, the **DCDIAG.exe** should be available in the <WINDOWS_ INSTALL_ dir>\windows\system32 directory of the DNS server to be monitored. The **DCDIAG** utility ships with the Windows Server 2003 Support Tools and is built into Windows 2008 R2 and Windows Server 2008. This utility may hence not be available in older versions of the Windows operating system. When monitoring the AD server on such Windows hosts, this test will run only if the **DCDIAG.exe** is copied from the <WINDOWS_INSTALL_dir>\windows\system32 directory of any Windows 2003 (or higher) host in the environment to the same directory on the target host.

Target of the test : A DNS server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for every test that **DCDIAG** executes.

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	The port on which the specified host is listening
Domain, UserName, Password, and Confirm Password	In order to execute the **DCDIAG** command, the eG agent has to be configured with *Enterprise Admin* privileges. Therefore, specify the domain name and login credentials of a user who has been assigned the *Enterprise Admin* account in the Domain, UserName and Password text boxes. Confirm the password you provide by retyping it in the Confirm Password text box.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Reports the output returned by this test.		Each test that **DCDIAG** runs will report one of the following values as the output: • Fail • Pass • Warning This test will report the same output as the value of the *Status* measure.

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>The numeric values that correspond to these outputs are indicated below:

<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Fail</td><td>0</td></tr><tr><td>Pass</td><td>1</td></tr><tr><td>Warning</td><td>2</td></tr></table>
Note:

By default, this measure reports the Output/Measure Values listed in the table above as values of the Status measure. In the graph of the Status measure however, these measure values are represented using their numeric equivalents only - i.e., 0 to 2.

You can use the detailed diagnosis of this measure to view detailed descriptions of failures (if any). This information will help in investigating the reasons for the failure and fixing them.</td></tr>
</table>

Chapter 5: Externally Monitoring DNS Servers

eG Enterprise offers the DNS server or the Windows DNS server model (discussed previously), which not only checks how well the DNS server performs host name resolutions, but also indicates how healthy the DNS server host is by reporting a wide variety of operating system-level metrics. However, some administrators might not have access to the DNS server for installing agents. To enable such administrators to deploy an eG agent on a remote host to monitor just the availability of the DNS server, and determine how quickly the server can resolve a host name to an IP address or vice-versa, eG Enterprise offers an External DNS server model (see Figure 5.1).

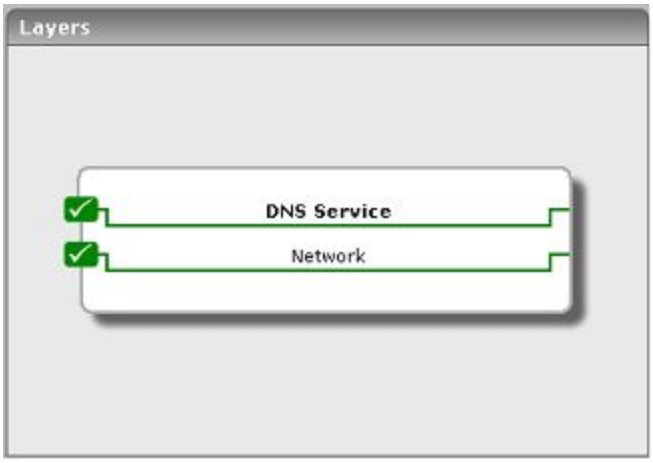

Figure 5.1: Layer model of the External DNS server

The **DNS Service** layer of this model uses an external agent to execute a Dns test, which emulates a user request to the DNS server to ascertain its availability and responsiveness. The **Network** test associated with the **Network** layer performs periodic network health checks.

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.