Monitoring Domino Application Server

eG Innovations Product Documentation

www.eginnovations.com

eG
Total Performance Visibility

Table of Contents

Table of Figures

1

Chapter 1: Introduction

The Lotus Domino server is an open, secure platform optimized to deliver messaging, applications, and online collaboration that integrates your enterprise systems with dynamic business processes. Used by small and large enterprises alike, the Domino server helps harness the power of the web to facilitate rapid application development, provides an efficient messaging mechanism, and also aids in securing IT environments from unauthorized access.

Owing to its wide usage and the crucial role it plays in the development, delivery, and security of business-critical services, even a semblance of a problem in the functioning of the Domino application server could be perilious to the health, availability, and reliability of a service offering. To avoid such adversities, it is necessary to keep a constant eye on the performance-impacting activities of the Domino application server, so that issues come to light early and are addressed quickly. The eG Enterprises helps administrators in this regard!

2

Chapter 2: How to Monitor Domino Application Server using eG Enterprise?

eG Enterprise monitors the Domino application server in both agent-based and agentless manners. This chapter discusses about how to configure and manage the Domino Application server to work with eG manager.

2.1 Enabling SNMP on a Domino Server

Domino SNMP Agent services are provided by two types of programs:

- **LNSNMP** - The Lotus Notes SNMP agent. As an independent application, LNSNMP is insulated from most Domino server malfunctions and, by itself, adds negligible overhead to the server.
- **Two Domino server add-ins** - the QuerySet Handler and the Event Interceptor.

The QuerySet Handler and the Event Interceptor depend on the Domino server; if the server fails for any reason, these programs fail as well.

The following components comprise the Domino SNMP Agent architecture:

- A platform-specific Master SNMP Agent - An independent, non-Lotus, agent usually supplied with the operating system platform that provides SNMP services for the machine. This SNMP Agent transports the SNMP traps and Get/Set responses across the network to the management station.
- The Domino SNMP Agent consisting of:
    - **LNSNMP Agent** - The Lotus Notes SNMP agent, which receives trap notifications from the Event Interceptor and then forwards them to the management station using the platform-specific SNMP Agent. LNSNMP also handles requests for Domino-related information from the management station by passing the request to the QuerySet Handler and responding back to the management station.
    - **QuerySet Handler** - Which queries server statistics information, sets the value of configurable Domino-based parameters, and returns Domino statistics information to LNSNMP, which then forwards the information to the management station using the platform-specific master SNMP Agent.
    - **Event Interceptor** - Which responds to the SNMP Trap notification for Domino Event Handlers by instructing LNSNMP to issue a trap.

- The Domino MIB - A standard Management Information Base (MIB) file for Lotus Domino servers that can be compiled and used by a network management program such as eG Enterprise.

2.2 Enabling SNMP for a Domino Server on Solaris

To enable SNMP on a Domino server on Solaris, follow the broad steps given below:

- Install the Master SNMP agent on the Domino server
- Configure the Domino SNMP agent to communicate with the Master SNMP agent

Each of these steps has been discussed in great detail below.

2.2.1 Installing and Configuring the Master SNMP Agent on the Domino Server

On Solaris platform, the Domino SNMP Agent uses the SMUX protocol, per RFC 1227, to communicate with the system's Master SNMP Agent. The Solaris Master SNMP Agent does not support the SMUX protocol, making it necessary to substitute a Master SNMP Agent that does. On Solaris platforms, Domino includes a suitable NET-SNMP Master Agent, called NET-SNMPD, already configured to support the SMUX protocol and the Domino SNMP Agent.

Note:

Before using NET-SNMPD, disable any existing Master SNMP Agent. Please follow the steps below for disabling an existing Master SNMP Agent running on Solaris.

- Log in as root.
- Stop the **snmpdx** daemon by typing, **/etc/rc3.d/S76snmpdx stop**.
- Disable the **snmpdx** daemon by issuing the command, **mv /etc/rc3.d/S76snmpdx /etc/rc3.d/s76snmpdx**.

To use the NET-SNMPD that is provided with Domino, do the following:

1. Login as the root user.
2. Next, install the NET-SNMPD files. Enter this command, changing the Domino executable path if necessary: **cp /opt/lotus/notes/latest/sunspa/net-snmpd* /etc**
3. Arrange for NET-SNMPD to be restarted after a reboot. Enter these commands:

   ln -f -s /etc/net-snmpd.sh /etc/init.d/net-snmpd

In -f -s /etc/init.d/net-snmpd /etc/rc2.d/S76net-snmpd

In -f -s /etc/init.d/net-snmpd /etc/rc1.d/K76net-snmpd

After installation, proceed to configure and start NET-SNMPD. Here is how:

Update the **/etc/net- snmpd.conf** file with appropriate community names for your remote management infrastructure. Community names are set using the **rocommunity** and **rwcommunity** directives. For instance, to set a community named **nppublic**, the command would be: **Set rocommunity value to nppublic**

To manually start NET-SNMPD, login as the root user and issue the command, **/etc/net-snmpd.sh start**. To stop NET-SNMPD, use this command: **/etc/net-snmpd.sh stop**

2.2.2 Configuring the Domino SNMP Agent

The Domino SNMP Agent configuration on Solaris involves the following:

- Configuring the LNSNMP agent to work with the Master SNMP Agent that is provided with the Domino server on Solaris
- Completing the configuration by starting the add-in tasks

Before attempting to configure the Domino SNMP agent, ensure the following:

- The Solaris Master SNMP Agent provided with Domino should be properly installed and configured on the server. Refer to the steps discussed in Section **2.2.1** for the procedure.
- TCP/IP and SNMP should be properly installed and configured on the server. Ensure that the Domino executable and the Domino data directories are in your search path.
- The Domino SNMP Agent is set up to run automatically. Once the Domino SNMP Agent is configured, it is virtually always running, even when Domino is not. If you later upgrade Domino, stop the LNSNMP process, before beginning the upgrade process.

To configure the LNSNMP agent, do the following:

1. Login as the root-user.
2. Stop the LNSNMP process. Enter this command: **Insnmp.sh stop**
3. Stop the NET-SNMP Master Agent by entering this command: **/etc/net-snmpd.sh stop**
4. Start the NET-SNMP Master Agent by entering this command: **/etc/net-snmpd.sh start**
5. Start the LNSNMP process using the command, **Insnmp.sh start**

6. Create a link to the LNSNMP script. Enter this command, changing the Domino executable path if necessary: **ln -f -s /opt/lotus/notes/latest/sunspa/lnsnmp.sh /etc/init.d/lnsnmp**

7. Arrange for LNSNMP to be restarted after a reboot. Enter these commands:

   ln -f -s /etc/init.d/lnsnmp /etc/rc2.d/S77lnsnmp

   ln -f -s /etc/init.d/lnsnmp /etc/rc1.d/K77lnsnmp

After configuring the LNSNMP agent, start the Domino server add-in tasks such as the QuerySet, Event Interceptor, and Statistic Collector tasks. To achieve this, do the following:

1. To support SNMP queries, start the QuerySet add-in task. Enter this command on the Domino Server console: **load quryset**

2. To support SNMP traps for Domino events, start the Event Interceptor add-in task. Enter this command on the Domino Server console: **load intrcpt**

3. To support Domino statistic threshold traps, start the Statistic Collector add-in task. Enter this command on the Domino Server console: **load collect**

4. Arrange for the add-in tasks to be restarted automatically when Domino is next restarted. Add **quryset** and/or **intrcpt** and **collect** to the ServerTasks variable in Domino's **notes.ini** file.

   ServerTasks =Update,Replica,Router,Amgr,AdminP,CalConn,Sched,LDAP,quryset,intrcpt,collect

2.3 Enabling SNMP for a Domino Server on Linux

To enable SNMP on a Domino server on Linux, follow the broad steps given below:

- Install the Master SNMP agent on the Domino server
- Configure the Domino SNMP agent to communicate with the Master SNMP agent

Each of these steps has been discussed in great detail below.

2.3.1 Installing and Configuring the Master SNMP Agent on the Domino Server

Like the Solaris platform, on Linux also the Domino SNMP Agent uses the SMUX protocol, per RFC 1227, to communicate with the system's Master SNMP Agent. Some Linux distributions include a Master SNMP Agent that supports the SMUX protocol; others do not. On Linux platforms, Domino includes a suitable NET-SNMP Master Agent, called NET-SNMPD, already configured to support the SMUX protocol and the Domino SNMP Agent.

Note:

Before using NET-SNMPD, disable any existing MasterSNMP Agent. For information on disabling an existing Master SNMP Agent, see your Master SNMP Agent's documentation.

To use the NET-SNMPD that is provided with Domino, do the following:

1. Login as the root user.
2. Next, install the NET-SNMPD files. Enter this command, changing the Domino executable path if necessary: **cp /opt/lotus/notes/latest/linux/net-snmpd* /etc**
3. Arrange for NET-SNMPD to be restarted after a reboot. Enter these commands:

   In -f -s /etc/net-snmpd.sh /etc/rc.d/init.d/net-snmpd

   chkconfig --add net-snmpd

   chkconfig net-snmpd on

After installation, proceed to configure and start NET-SNMPD. Here is how:

Update the **/etc/net- snmpd.conf** file with appropriate community names for your remote management infrastructure. Community names are set using the **rocommunity** and **rwcommunity** directives. For instance, to set a community named **nppublic** , the command would be, **Set rocommunity value to nppublic**.

To manually start NET-SNMPD, login as the root user and issue the command, **/etc/net-snmpd.sh start**. To stop NET-SNMPD, use the command, **/etc/net-snmpd.sh stop**.

2.3.2 Configuring the Domino SNMP Agent

The Domino SNMP Agent configuration on Linux involves the following:

- Configuring the LNSNMP agent to work with the Master SNMP Agent that is provided with Domino on Linux
- Completing the configuration by starting the add-in tasks

Before attempting to configure the Domino SNMP agent, ensure the following:

- The Linux Master SNMP Agent provided with Domino should be properly installed and configured on the server. Refer to the steps discussed in Section **2.2.1** for the procedure.
- TCP/IP and SNMP should be properly installed and configured on the server. Ensure that the Domino executable and the Domino data directories are in your search path.

- The Domino SNMP Agent is set up to run automatically. Once the Domino SNMP Agent is configured, it is virtually always running, even when Domino is not. If you later upgrade Domino, stop the LNSNMP process, before beginning the upgrade process.

To configure the LNSNMP agent, do the following:

- Login as the root-user.
- Stop the LNSNMP process. Enter this command: **lnsnmp.sh stop**
- Stop the NET-SNMP Master Agent by entering this command: **/etc/net-snmpd.sh stop**
- Start the NET-SNMP Master Agent by entering this command: **/etc/net-snmpd.sh start**
- Start the LNSNMP process using the command, **lnsnmp.sh start**.
- Arrange for LNSNMP to be restarted after a reboot. Enter these commands:

```
ln -f -s /opt/lotus/notes/latest/linux/lnsnmp.sh /etc/rc.d/init.d/lnsnmp

chkconfig --add lnsnmp

chkconfig lnsnmp on
```

After configuring the LNSNMP agent, start the Domino server add-in tasks such as the QuerySet, Event Interceptor, and Statistic Collector tasks. To achieve this, do the following:

- To support SNMP queries, start the QuerySet add-in task. Enter this command on the Domino Server console: **load quryset**
- To support SNMP traps for Domino events, start the Event Interceptor add-in task. Enter this command on the Domino Server console: **load intrcpt**
- To support Domino statistic threshold traps, start the Statistic Collector add-in task. Enter this command on the Domino Server console: **load collect**
- Arrange for the add-in tasks to be restarted automatically when Domino is next restarted. Add **quryset** and/or **intrcpt** and **collect** to the ServerTasks variable in Domino’s **notes.ini** file.

  ServerTasks =Update,Replica,Router,Amgr,AdminP,CalConn,Sched,LDAP,quryset,intrcpt,collect

2.4 Enabling SNMP for a Domino Server on AIX

To enable SNMP on an AIX Domino server, you will have to configure the Domino SNMP agent. This involves ensuring that the LNSNMP process communicates with the SNMPD subsystem (on the AIX installation of Domino) using the SMUX protocol.

However, prior to configuring the Domino SNMP agent, make sure that the following are in place:

- TCP/IP and SNMP should be properly installed and configured on the server. Also, make sure that the Domino executable and the Domino data directories are in your search path
- The trap destinations and community names for AIX should be appropriately configured in the /etc/snmpd.conf file for your remote management infrastructure. Remember to keep the view identifiers unique for each trap destination.
- The Domino SNMP Agent is set up to run automatically. This means that once the Domino SNMP Agent is configured, it is virtually always running, even when Domino is not. If you later upgrade Domino you should stop the LNSNMP process before beginning the upgrade process.

Next, proceed to configure the Domino SNMP agent, using the procedure explained below:

1. Login as the root user.
2. Stop the LNSNMP process. Enter this command: **lnsnmp.sh stop**
3. Stop the SNMPD (SNMP Daemon) subsystem. The Simple Network Management Protocol (SNMP) daemon is a background server process that can be run on any Transmission Control Protocol/Internet Protocol (TCP/IP) workstation host. The daemon, acting as SNMP agent, receives, authenticates, and processes SNMP requests from manager applications. This daemon is installed and started by default on AIX systems. To stop SNMPD, enter this command: **stopsrc -s snmpd**
4. Configure SNMPD to accept LNSNMP as an SMUX peer. Add the following line to the **/etc/snmpd.peers** file: **"Lotus Notes Agent" 1.3.6.1.4.1.334.72 "NotesPasswd"**
5. Configure SNMPD to accept an SMUX association from LNSNMP. Add the following line to /**etc/snmpd.conf: smux 1.3.6.1.4.1.334.72 NotesPasswd**
6. Start the SNMPD subsystem. Enter this command: **startsrc -s snmpd**
7. Start the LNSNMP process. Enter this command: **lnsnmp.sh start**
8. Create a link to the LNSNMP script. Enter this command, changing the Domino executable path if necessary: **ln -f -s /opt/lotus/notes/latest/ibmpow/lnsnmp.sh /etc/lnsnmp.rc**
9. Arrange for LNSNMP to be restarted after a reboot. Add the following line to the end of the **/etc/rc.tcpip** file: **/etc/lnsnmp.rc start**

After configuring the LNSNMP agent, start the Domino server add-in tasks such as the QuerySet, Event Interceptor, and Statistic Collector tasks, using the procedure discussed in Section **2.3.2**.

2.5 Enabling SNMP for a Domino Server on Windows

To enable SNMP on a Windows Domino server, follow the broad steps given below:

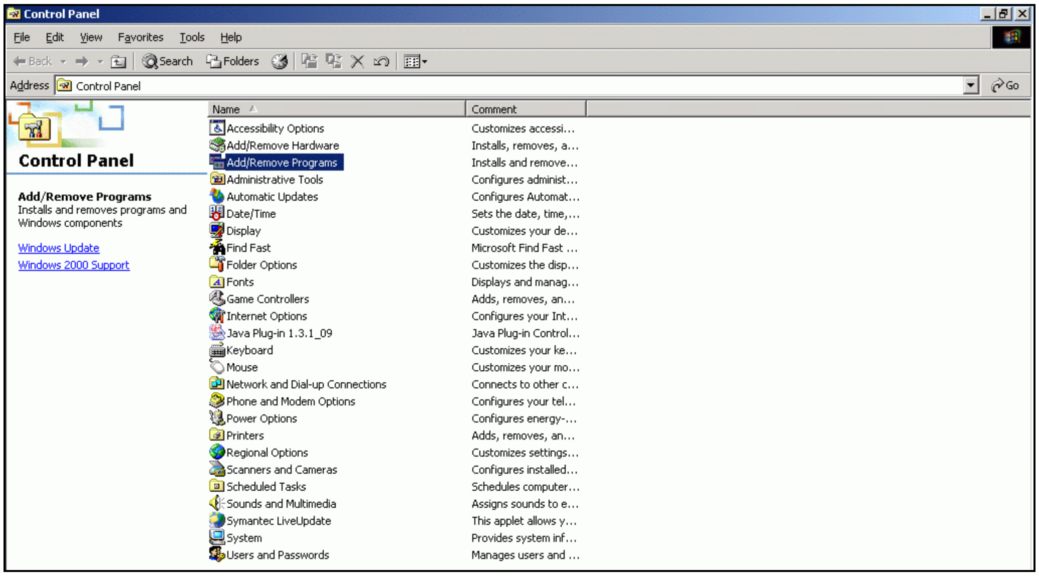
- Install the Windows SNMP service on the target host
- Install the LNSNMP agent (i.e., the Lotus Domino SNMP agent) on the target host
- Configure the Lotus Domino SNMP agent as a service on the target host

Each of these steps is discussed in great detail in the sections to come.

2.5.1 Installing the Windows SNMP Service

To install the SNMP service on Windows 2000, do the following:

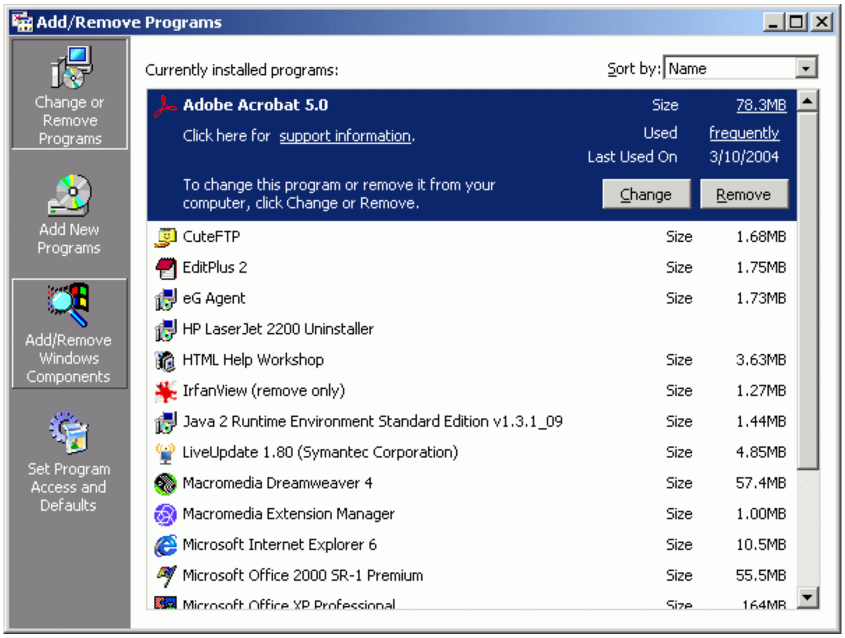
1. Login to the Windows 2000 system as an administrator.
2. Click on the **Start** button on the taskbar, and follow the menu sequence: Settings -> Control Panel.
3. Double-click on the **Add/Remove Programs** option in the Control Panel window (see Figure 2.1).



Name	Comment
Accessibility Options	Customizes accessi...
Add/Remove Hardware	Installs, removes, a...
Add/Remove Programs	Installs and remove...
Administrative Tools	Configures administ...
Automatic Updates	Configures Automat...
Date/Time	Sets the date, time,...
Display	Customizes your de...
Find Fast	Microsoft Find Fast ...
Folder Options	Customizes the disp...
Fonts	Displays and manag...
Game Controllers	Adds, removes, an...
Internet Options	Configures your Int...
Java Plug-in 1.3.1_09	Java Plug-in Control...
Keyboard	Customizes your ke...
Mouse	Customizes your mo...
Network and Dial-up Connections	Connects to other c...
Phone and Modem Options	Configures your tel...
Power Options	Configures energy-...
Printers	Adds, removes, an...
Regional Options	Customizes settings...
Scanners and Cameras	Configures installed...
Scheduled Tasks	Schedules computer...
Sounds and Multimedia	Assigns sounds to e...
Symantec LiveUpdate	This applet allows y...
System	Provides system inf...
Users and Passwords	Manages users and ...

Figure 2.1: The Add/Remove Programs option in the Control Panel window

4. Next, select the **Add/Remove Windows Components** option from the **Add/Remove Programs** dialog box (see Figure 2.2).


Add/Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Set Program Access and Defaults
Sort by: Name
Change
Remove

Currently installed programs:

Adobe Acrobat 5.0 Size 78.3MB

Click here for support information. Used frequently

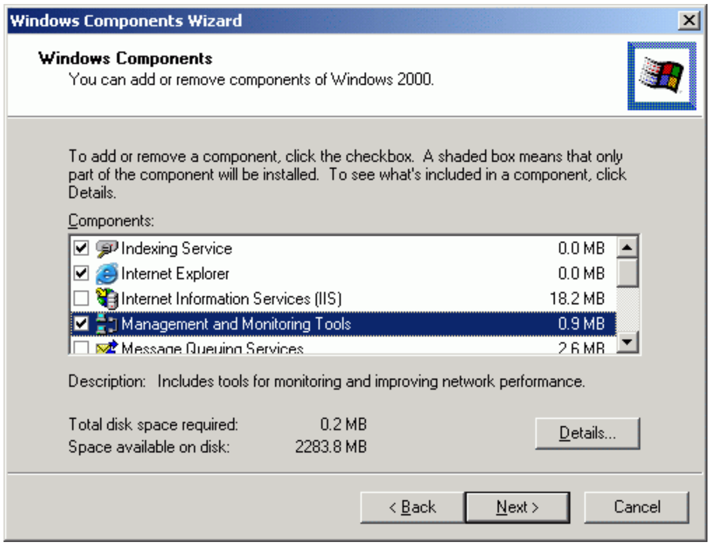
Last Used On 3/10/2004

To change this program or remove it from your computer, click Change or Remove.

CuteFTP	Size	1.68MB
EditPlus 2	Size	1.75MB
eG Agent	Size	1.73MB
HP LaserJet 2200 Uninstaller		
HTML Help Workshop	Size	3.63MB
IrfanView (remove only)	Size	1.27MB
Java 2 Runtime Environment Standard Edition v1.3.1_09	Size	1.44MB
LiveUpdate 1.80 (Symantec Corporation)	Size	4.85MB
Macromedia Dreamweaver 4	Size	57.4MB
Macromedia Extension Manager	Size	1.00MB
Microsoft Internet Explorer 6	Size	10.5MB
Microsoft Office 2000 SR-1 Premium	Size	55.5MB
Microsoft Office XP Professional	Size	164MB

Figure 2.2: Select the Add/Remove Windows Components option

5. Then, a list of windows components that can be added will appear. Select the **Management and Monitoring Tools** option from this list, and click the **Details** button to view more details about it (see Figure 2.3).



Windows Components

You can add or remove components of Windows 2000.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	Indexing Service	0.0 MB
☑	Internet Explorer	0.0 MB
□	Internet Information Services (IIS)	18.2 MB
☑	Management and Monitoring Tools	0.9 MB
□	Message Queuing Services	2.6 MB

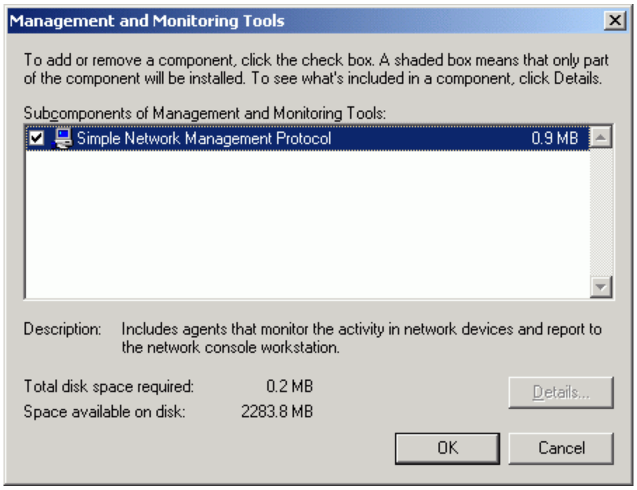
Description: Includes tools for monitoring and improving network performance.

Total disk space required: 0.2 MB

Space available on disk: 2283.8 MB

Figure 2.3: Selecting the Management and Monitoring Tools option

6. From the list that appears next, select the **Simple Network Management Protocol** (SNMP) option to add it. Then, click the **OK** button (see Figure 2.4).



Management and Monitoring Tools

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Management and Monitoring Tools:

☑ Simple Network Management Protocol 0.9 MB

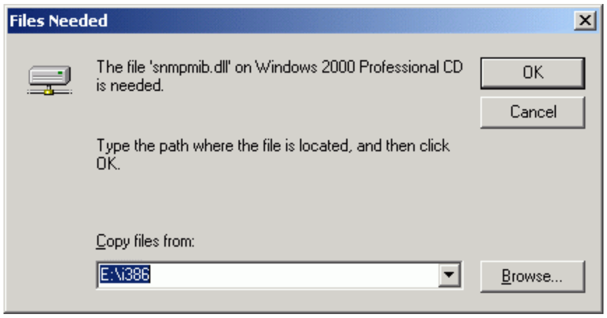
Description: Includes agents that monitor the activity in network devices and report to the network console workstation.

Total disk space required: 0.2 MB

Space available on disk: 2283.8 MB

Figure 2.4: Selecting the SNMP option

7. You will then return to Figure 2.3. Click the **Next** button here to proceed with installing the **SNMP** service.
8. If you are prompted for the path to the Windows 2000 installation CD, provide the correct path, and click on the **OK** button to begin installing the **SNMP** service (see Figure 2.5).



Files Needed

The file 'snmpmib.dll' on Windows 2000 Professional CD is needed.

Type the path where the file is located, and then click OK.

Copy files from: E:\i386

Figure 2.5: Providing the path to the Windows 2000 CD

2.5.2 Installing the LNSNMP Agent

To install the LNSNMP agent, do the following:

1. Run the **nvinst.exe** executable that is available in the <DOMINO_INSTALL_DIR>/w32intel folder.
2. Once execution begins, setup will prompt you to choose one of the following options:

```
Domino Management Agent for Windows NT installation.
```

```
Copyright (c) 1994-1999, Lotus Development Corporation.  All Rights Reserved.

Lotus Domino Management Agent Install (Version 5.0)
Installation Options
---------------------------------------------------

   1) Install Domino SNMP Agent Software
   2) Install Domino Mail Reflector Software
   3) Install Both Options 1 and 2
   Q) Quit Installation

   Choice (1/2/3/Q): 1
```

3. To install the LNSNMP agent, enter **1** as the **Choice**.
4. Setup will then request your confirmation for adding the Collector task. Enter **y** to add the task.

```
The "Collector" task is not currently configured to run on this system.  This task is necessary if you want Notes to generate events based on statistics thresholds.

Do you want to add this task now? (y/n): y
```

5. Once the LNSNMP agent installation completes, the following message will appear:

```
Domino Management Agent successfully installed.
Please reboot the system for the changes to take effect.

D:\Lotus\Domino\w32intel>

After Rebooting start the LNSNMP Service first
And then start the Domino Server.
```

2.5.3 Configuring the LNSNMP Agent

Prior to configuring the LNSNMP agent, ensure the following:

- Before using the Domino SNMP Agent, make sure TCP/IP and SNMP are properly installed and configured on the server. Also, make sure that the Domino executable and the Domino data directories are in your search path.

- If you need to add the Windows SNMP Service to your system, be prepared to reinstall any Windows service packs immediately after adding the Windows SNMP Service.
- The Windows SNMP Service is configured by double-clicking the Network icon in the Control Panel, then selecting the Services tab, then selecting SNMP Service, and then clicking the Properties button. You will want to configure appropriate trap destinations and community names for your remote management infrastructure.
- The Domino SNMP Agent is configured as a Windows Service and is set up to run automatically. This means that once the Domino SNMP Agent is configured, it is virtually always running, even when Domino is not. If you later upgrade Domino you should stop the LNSNMP and Windows SNMP Services before beginning the upgrade process.

To configure the LNSNMP agent, do the following:

1. Stop the LNSNMP and SNMP services. Enter these commands:

   net stop lnsnmp

   net stop snmp

2. Configure the Lotus Domino SNMP Agent as a service. Enter this command: **lnsnmp -Sc**
3. Start the SNMP and LNSNMP services. Enter these commands:

   net start snmp

   net start lnsnmp

After configuring the LNSNMP agent, start the Domino server add-in tasks such as the QuerySet, Event Interceptor, and Statistic Collector tasks, using the procedure discussed in Section **2.3.2**.

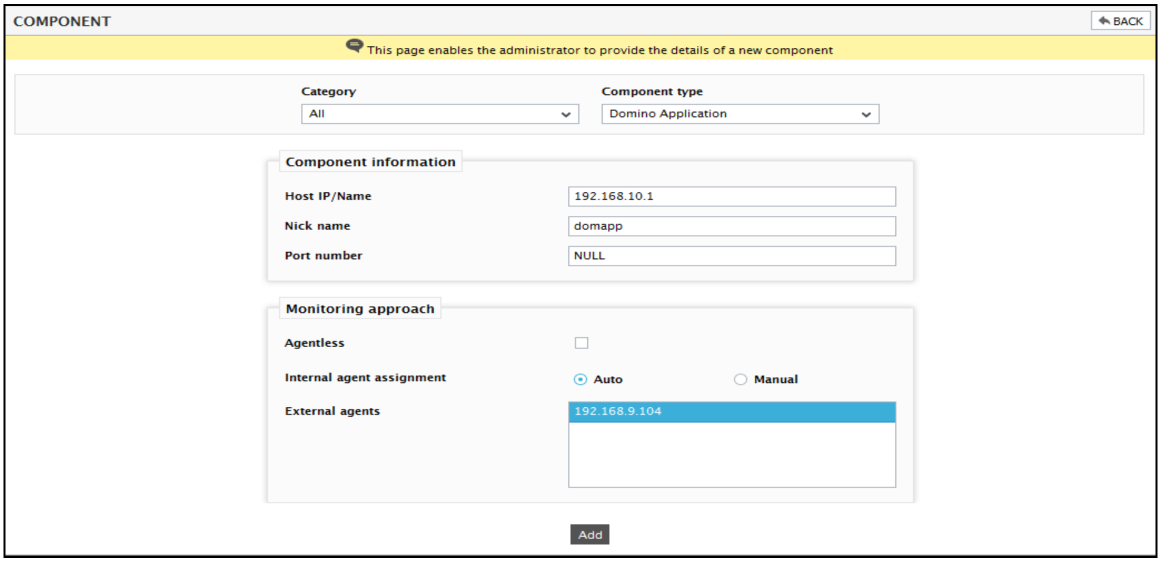
2.6 Managing the Domino Application Server

The eG Enterprise cannot automatically discover the Domino Application Server. This implies that you need to manually add the Domino Application Server component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To add a Docker component, do the following:

1. Log into the eG administrative interface.

2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.

3. In the **COMPONENT** page that appears next, select Domino Application as the **Component type**. Then, click the **Add New Component** button. This will invoke 2.6.



COMPONENT

This page enables the administrator to provide the details of a new component

Category: All

Component type: Domino Application

Component information

Host IP/Name: 192.168.10.1

Nick name: domapp

Port number: NULL

Monitoring approach

Agentless: □

Internal agent assignment: ● Auto ○ Manual

External agents: 192.168.9.104

Figure 2.6: Adding a Domino Application server

4. Specify **Host IP/Name** and **Nick name** of the Domain Application server component (see Figure 2.6). The **Port number** will be set as *NULL* by default. If the server is listening on ay specific port, then enter that specific port number here.

5. Then, click on the **Add** button to add the server for monitoring.

6. Next, sign out of the eG administrative interface.

3

Chapter 3: Monitoring Domino Application Servers

eG Enterprise has developed an exclusive *Domino application* monitoring model (see Figure 3.1) for the Domino application server, which employs an eG agent to continuously monitor the performance of the server. This eG agent executes tests which communicate with the Domino SNMP agent to collect key metrics relating to server performance. To facilitate this communication, SNMP should be enabled on the application server.

Once the Domino SNMP agent is completely configured, the tests executed by the eG agent (which is monitoring the Domino server's performance), polls the SNMP agent at frequent intervals for performance data. The SNMP agent then retrieves the desired performance statistics from the SNMP MIB of the Domino server and forwards the same to the eG agent.

Using these statistics, administrators can easily and accurately answer the following performance queries:

- Has the Domino server's capacity been fully utilized? If not, what percentage of its capacity is still available for request processing?
- Are sufficient threads available for handling requests to the Domino server?
- Are there too many concurrent connection requests to the server?
- Has enough memory been allocated to the Domino processes and shared memory segments?
- Are the NSF buffer pools and buffer control pools adequately sized on the Domino database?
- Are hits to the database cache optimal, or does the cache require any resizing?
- How many databases are currently awaiting replication and for how long have they been waiting? Were too many databases in the queue for too long? If so, can additional replicators be configured to share the load?
- Has the cluster replicator successfully handled all replication requests to it, or have too many requests failed?
- What is the current load on the web server component of the application server? Is it too heavy?
- Is the idle session count kept at a minimum?

The tests that reveal the above are mapped to the various layers of the monitoring model of Figure 3.1.

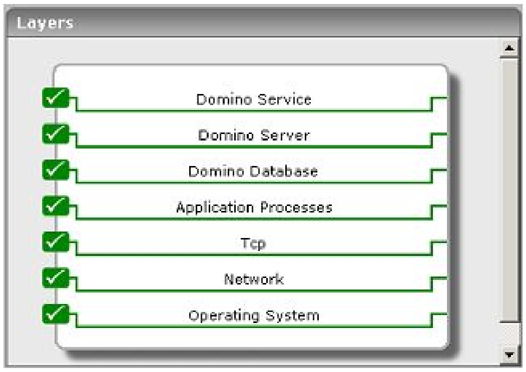


Figure 3.1: Figure 16.6: Layer model of the Domino application server

The section that follows discusses the first layer of Figure 3.1 and the tests that are mapped to it. While the next 2 layers have been dealt with extensively in the *Monitoring Mail Servers* document, the remaining layers have been elaborately discussed in the *Monitoring Unix and Windows Servers* document.

3.1 The Domino Service Layer

The critical services provided by the Domino server are monitored by the tests associated with the **Domino Service** layer. These include:

- Servicing the web requests to its web server component
- Servicing the database replication requests to servers in a cluster

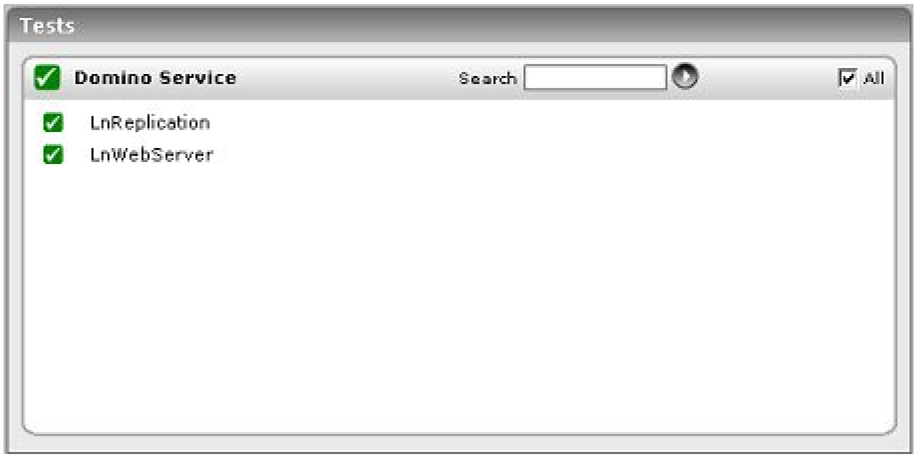


Figure 3.2: The tests associated with the Domino Service Layer

3.1.1 Lotus Notes Web Server Test

This test reports the web server statistics of a Lotus Domino server.

Target of the test : A Domino application server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for the Domino application server that is 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 at which the host listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned UserName. This parameter once again appears only if the SNMPversion selected is **v3**.

Parameter	Description
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Request rate	Indicates the number of requests handled by the web server during the last measurement period.	Reqs/Sec	A high value is indicative of heavy work load on the server.
HTTP connections	Indicates the number of HTTP connections accepted during the last measurement period.	Conns/Sec	
Current connections	Indicates the number of current HTTP connections.	Number	
Data received rate	Indicates the amount of data received by the web server during the last measurement period.	Kbytes/Sec	
Data sent rate	Indicates the amount of data sent by the web server during the last measurement period.	Kbytes/Sec	
Http workers	Indicates the number of HTTP worker processes currently servicing web server requests.	Number	
Idle session timeouts	Indicates the number of idle sessions timed out during the last measurement period.	Number	Idle sessions might waste server resources. If the load on a server is very high and idle sessions are also quiet a few, you may want to reduce the idle session timeout value so that idle sessions get timed out more often. This way the strain on the server is greatly reduced, and server resources are preserved.

3.1.2 Lotus Notes Replication Test

A Domino cluster is a group of two or more servers that provides users with constant access to data, balances the workload between servers, improves server performance, and maintains performance when you increase the size of your enterprise. The servers in a cluster contain replicas of databases that you want to be readily available to users at all times. If a user tries to access a database on a cluster server that is not available, Domino opens a replica of that database on a different cluster server, if a replica is available. Domino continuously synchronizes databases so that whichever replica a user opens, the information is always the same.

There is a special component on the servers in a cluster, called "Cluster Replicator" that is responsible for replication being performed between the databases. When a cluster replicator learns of a change to a database, it immediately pushes that change to all other replicas in the cluster. All replication events are stored in memory, and if a destination server is not available, the "Cluster Replicator" continues to store these events in memory until the destination server becomes available.

By default, every server in a cluster consists of a single cluster replicator. However, in order to augment the performance of the Domino cluster, multiple replicators can be configured on a server. The decision to introduce more replicators on a cluster server can be taken only after understanding and analyzing how well the default replicator on the server handles the replication requests to it. This test periodically monitors a cluster server's replicator- related activities and reveals critical performance statistics based on which administrators can decide whether/not to add more replicators to it.

Target of the test : A Domino application server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for the Domino application server that is 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 at which the host listens. By default, this will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.

Parameter	Description
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned UserName. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by

Parameter	Description
	default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Successful replications	Indicates the rate of successful replications during the last measurement period.	Replications/Sec	
Replication failures	Indicates the rate of failed replications during the last measurement period.	Replications/Sec	
Replication docs added	Indicates the rate at which replication docs were added during the last measurement period.	Docs/Sec	

Measurement	Description	Measurement Unit	Interpretation
Replication docs deleted	Indicates the rate at which replication docs were deleted during the last measurement period.	Docs/Sec	
Replication docs updated	Indicates the rate at which replication docs were updated during the last measurement period.	Docs/Sec	
Avg work queue length	Indicates the average work queue length since server startup.	Number	
Current work queue length	Indicates the current number of databases awaiting replication by the cluster replicator.	Number	If the value of this measure increases consistently, it could indicate a replication backlog - in other words, too many databases could be waiting to be replicated. In such a case, consider configuring more replicators on the server so that replication workload is shared and pending replication requests are cleared in a timely manner. Steady spikes in this measure could also indicate insufficient network bandwidth to process the transactions. If this is the case, you should consider setting up a private LAN for your cluster.
Avg work queue wait time	Indicates the average amount of time in seconds that a database spent on the work queue.	Secs	Since the cluster replicator checks its queue every 15 seconds, this number should be under 15 during periods of light load. If this number is frequently higher than 30, you should consider adding one or more cluster replicators.
Data received rate	Indicates the rate at which data was received by the replicator during the last measurement period.	KBytes/Sec	

Measurement	Description	Measurement Unit	Interpretation
Data sent rate	Indicates the rate at which data was sent by the replicator during the last measurement period.	KBytes/Sec	

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.