Monitoring Novell eDirectory

eG Enterprise v6

Restricted Rights Legend

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

Trademarks

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

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

Copyright

Table of Contents

Table of Figures

Chapter 1

Monitoring Novell eDirectory

Novell eDirectory centrally manages access to resources on multiple servers and computers within a given network.

In simplest terms, eDirectory is a hierarchical, object oriented database that represents all the assets in an organisation in a logical tree. Assets can include people, positions, servers, workstations, applications, printers, services, groups, etc.

Inconsistencies in the performance of this central resource-repository could put critical resources out of a normal user's reach. Continued disturbances will hence severely affect organizational productivity. The need therefore is for a monitoring solution that can perform 24 x 7 monitoring of eDirectory and informs administrators of issues, well before any visible damage occurs.

The eG Enterprise suite with its proactive problem alerting capability is ideal for this purpose. The eG agent serves as a data collector that periodically extracts critical performance statistics from the eDirectory server. The suite then compares these values with manually/automatically set performance baselines, and thus instantaneously detects probable deviations - details pertaining to the probable issues are then quickly provided to administrators, who initiate the corrective measures, without any delay.

The metrics so extracted by the eG agent enables the administrators to find accurate answers to the following performance queries:

Cache Monitoring	➢ Are the block and entry caches of the eDirectory server sufficiently sized? ➢ Are cache hits optimal? ➢ Are there too many direct disk accesses?
Access Monitoring	➢ What are the number and type of requests that are handled by the eDirectory server? ➢ Is the error rate very high? ➢ Are too many requests chained? ➢ Is the load on the server manageable?

To capture and present these metrics in the monitoring console in a user-friendly format, eG Enterprise provides, not one, but two eDirectory monitoring models – the *EDirectory (Netware)* model to monitor eDirectory on the Netware operating system, and the *EDirectory (Win/Unix)* model for monitoring the eDirectory on Windows and Unix operating systems. Figure 1.1 depicts the *Edirectory (Netware)* monitoring model.

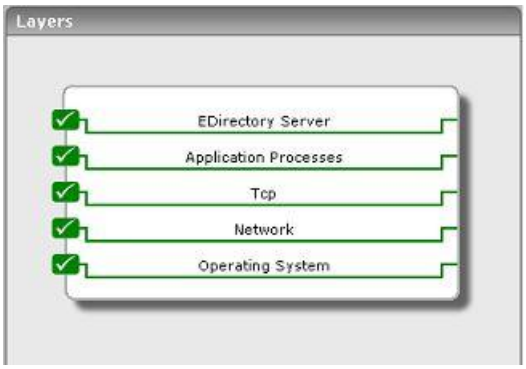

Figure 1.1: The layer model of an eDirectory server

Though both the *EDirectory (Netware)* and *EDirectory (Win/Unix)* models share the same set of layers, the difference lies in the tests mapped to the operating system-specific layers – in other words, the bottom 4 layers of Figure 1.1. To know the details of tests mapped to these 4 layers on Windows/Unix environments, refer to the *Monitoring Unix and Windows Servers* document. Similarly, to know which tests are associated with these 4 layers on Netware, refer to Chapter 4 in the *Monitoring Applications that Support the Host Resources MIB* document. This document however, will discuss the details of tests mapped to and metrics reported by the topmost layer of Figure 1.1.

These tests, when executed, extract the performance statistics from the SNMP MIB of eDirectory. For the tests to communicate with eDirectory's SNMP MIB, you need to ensure the following:

- The SNMP service of the operating system should be installed and started
- The operating system's service pack should be reapplied after installing eDirectory
- The SNMP service of eDirectory should be started

In a Windows installation of eDirectory, follow the steps below to install and start the Windows SNMP service:

1. Go to the **Control Panel** using the menu sequence: Start -> Settings -> Control Panel.
2. Double-click on the **Add/Remove Programs** option within.
3. Figure 1.2 will then appear. Double-click on the **Add/Remove Windows Components** button in the left panel of Figure 1.2.

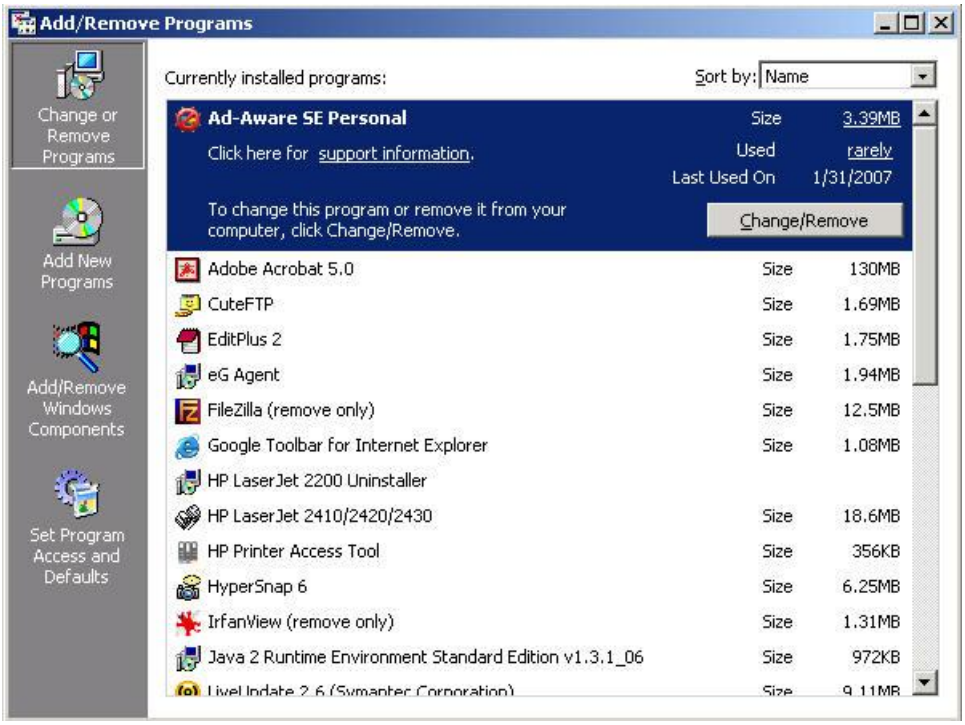

Figure 1.2: The Add/Remove Programs window

4. Doing so invokes Figure 1.3 that lists the components that can be added or removed. Next, click on the **Management and Monitoring Tools** option from the **Components** list.

Figure 1.3: Components that can be added/removed

5. Figure 1.4 that appears next reveals the management tools that can be / have already been installed on the Windows operating environment. To install the SNMP service, select the check box

preceding the **Simple Network Management Protocol** option in Figure 1.4, and click the **OK** button therein.

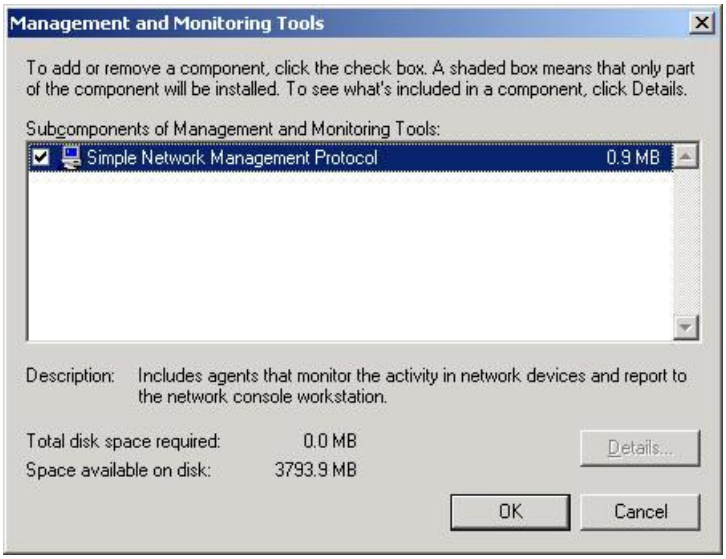

Figure 1.4: Selecting SNMP for installation

6. You will return to Figure 1.3. To proceed with the SNMP installation, click on the **Next** button in Figure 1.3.
7. Once installation ends, start the SNMP service. To do so, first, follow the menu sequence, Start -> Run, and type **services.msc** in the **Run** text box. The **Services** window then appears. To start the SNMP service, select the **SNMP Service** from the Services list, right-click on it, and select **Start** from its shortcut menu.

Next, make sure that the eDirectory's SNMP service is started. The SNMP service for eDirectory is installed when eDirectory is installed. To start the service on a Windows installation of eDirectory, do the following:

1. Open the **Control Panel** and double-click on the **Novell eDirectory Services** option within (see Figure 1.5).

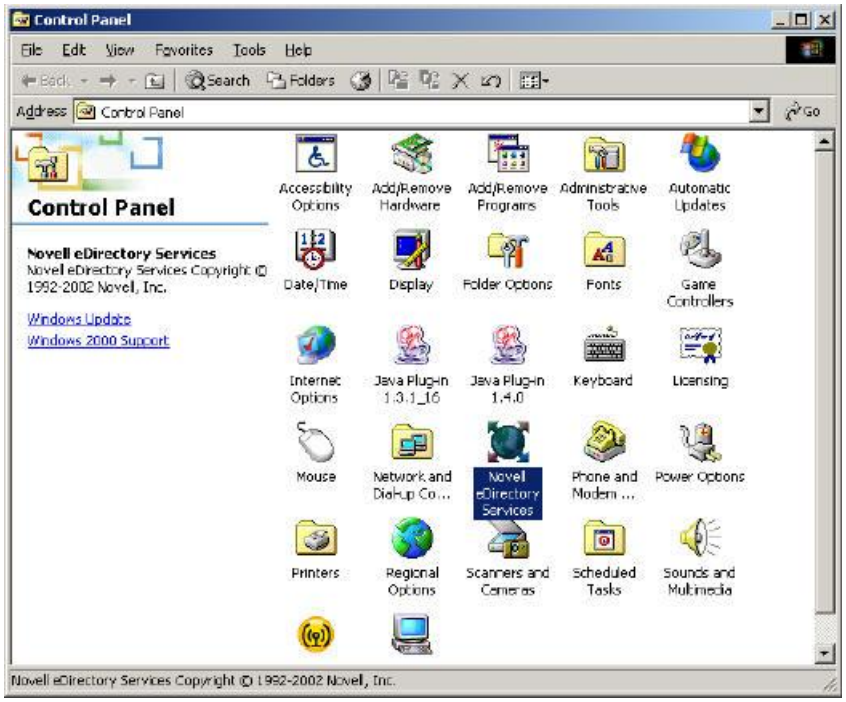

Figure 1.5: Selecting the Novell eDirectory Services

2. From the list of services that is displayed (see Figure 1.6), select the **ndssnmp.dlm** service and click on the **Start** button therein to start it.

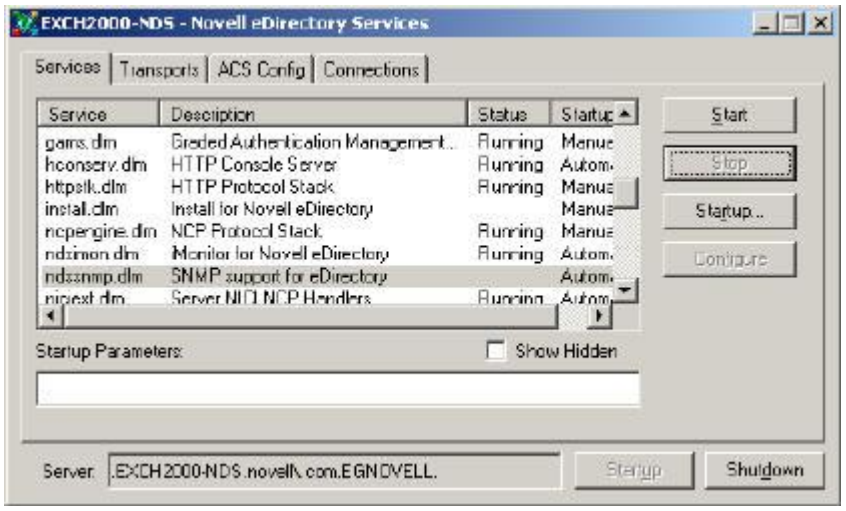

Figure 1.6: Starting the eDirectory SNMP service

3. Figure 1.7 will then appear prompting you to provide authentication to start the SNMP service.

Figure 1.7: Authentication for starting the SNMP service

4. Provide an administrator's **User Name** and **Password** in Figure 1.7. You can also save the password so that the password prompt does not reappear every time you attempt to restart the service. To ensure this, simply, select the **Remember Password** check box in Figure 1.7. Finally, click the **OK** button therein to start the SNMP service.

Once the SNMP agent (i.e., the operating system's SNMP service) and sub-agent (i.e., eDirectory's SNMP service) are up and running, the eG agent communicates with the agent and sub-agent to collect the required metrics from within eDirectory's SNMP MIB.

1.1 The EDirectory Server Layer

The tests associated with this layer (see Figure 1.8) enable extensive monitoring of the following:

- The extent of utilization of the caches associated with every eDirectory database
- The efficiency of every application protocol interface of the eDirectory server

Figure 1.8: The tests associated with the EDirectory Server layer

1.1.1 EDirDbCache Test

The most significant setting that affects eDirectory performance is the cache. With eDirectory 8.5 or later, you can specify a block cache limit and an entry cache limit. The block cache caches only physical blocks from the database. The entry cache caches logical entries from the database. The caching of entries reduces the processing time required to instantiate entries in memory from the block cache.

The EDirDbCache test monitors the block and entry caches of every eDirectory database, and reports whether they are efficiently utilized or not.

Purpose	Monitors the block and entry caches of eDirectory
Target of the test	The eDirectory server
Agent deploying the test	An internal agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **host** - Host name of the server for which the test is to be configured 3. **snmpport** - The port number through which the server exposes its SNMP MIB. The default value is 161. 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **snmpversion** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the target server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 6. **username** – This parameter appears only when **v3** is selected as the **snmpversion**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **username** parameter. 7. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **confirm password** – Confirm the **authpass** by retyping it here. 9. **authtype** – This parameter too appears only if **v3** is selected as the **snmpversion**. From the **authtype** list box, choose the authentication algorithm using which SNMP v3 converts the specified **username** and **password** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 10. **encryptflag** – This flag appears only when **v3** is selected as the **snmpversion**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **encryptflag** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **encrypttype** – If the **encryptflag** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **encrypttype** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 12. **encryptpassword** – Specify the encryption password here. 13. **confirm password** – Confirm the encryption password by retyping it here.

	14. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for every eDirectory database being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	EDirectory database size: Indicates the current size of the eDirectory database.	KB	
	Database block size: Indicates the current block size of the eDirectory database.	KB	
	Database entry current size: Indicates the current entry cache size.	KB	With an entry cache and a block cache, the total available memory for caching should be shared between the two caches. If the server you are installing eDirectory on does not have a replica,

	Database block current size: Indicates the current block cache size.	KB	the default is a hard memory limit of 16 MB, with 8 MB for block cache and 8 MB for entry cache. If the server contains a replica, the default is a dynamically adjusting limit. The dynamically adjusting limit causes eDirectory to periodically adjust its memory consumption in response to the ebb and flow of memory consumption by other processes. You specify the limit as a percentage of available physical memory. Using this percentage, eDirectory recalculates a new memory limit at fixed intervals. The new memory limit is the percentage of physical memory available at the time. Along with the percentage, you can set a maximum and minimum threshold. The threshold is the number of bytes that eDirectory will adjust to. It can be set as either the number of bytes to use or the number of bytes to leave available. The minimum threshold default is 16 MB. The maximum threshold default is 4 GB. With the dynamically adjusting limit, you also specify the interval length. The default interval is 15 seconds. The shorter the interval, the more the memory consumption is based on current conditions.
	Database entry items cached: Indicates the number of entries in the entry cache, currently.	Number	An Entry cache is most useful for operations that browse the eDirectory tree by reading through entries, such as name resolution. A well-sized entry cache thus speeds up the retrieval of entries referenced from an index. Therefore, ideally, the value of this measure should be high.
	Database block items cached: Indicates the number of blocks in the block cache, currently.	Number	A well-sized block cache is most useful for update operations and can speed up index searching. A very low number of blocks in this cache could considerably slow-down key eDirectory operations. Therefore, ideally, this value should be high. The more blocks and entries that can be cached, the better the overall performance will be.

	Database entry cache hits: Indicates the percentage of database hits that were served by the entries in the entry cache.	Percent	Typically, a 1:1 ratio for block cache, and a 1:2 or 1:4 ratio for the entry cache is desired. Anything lesser indicates that the entry and block caches are unable to fulfill most of the requests to the eDirectory server. This happens when an adequate number of blocks/entries is not cached. Badly-sized caches escalate direct disk accesses and processing overheads as well. The ideal is to cache the entire database in both the entry and block caches, although this is not possible for extremely large databases.
	DB block cache hits: Indicates the percentage of database hits that were serviced by the blocks in the block cache.	Percent	

1.1.2 EdirProtocol Test

The EdirProtocol test provides summary statistics on the accesses, operations and errors for each application protocol interface of a directory server.

Purpose	Provides summary statistics on the accesses, operations and errors for each application protocol interface of a directory server
Target of the test	The eDirectory server
Agent deploying the test	An internal agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **host** - Host name of the server for which the test is to be configured 3. **snmpport** - The port number through which the server exposes its SNMP MIB. The default value is 161. 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **snmpversion** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the target server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 6. **username** – This parameter appears only when **v3** is selected as the **snmpversion**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **username** parameter. 7. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **confirm password** – Confirm the **authpass** by retyping it here. 9. **authtype** – This parameter too appears only if **v3** is selected as the **snmpversion**. From the **authtype** list box, choose the authentication algorithm using which SNMP v3 converts the specified **username** and **password** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 10. **encryptflag** – This flag appears only when **v3** is selected as the **snmpversion**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **encryptflag** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **encrypttype** – If the **encryptflag** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **encrypttype** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 12. **encryptpassword** – Specify the encryption password here. 13. **confirm password** – Confirm the encryption password by retyping it here.

	14. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for every application protocol interface of the eDirectory server being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Unauthenticated bind requests received: Indicates the number of unauthenticated/anonymous bind requests received since the last measurement period.	Number	All LDAP clients bind (connect) to Novell eDirectory as one of the following types of users: ➢ [Public] User (Anonymous Bind) ➢ Proxy User (Proxy User Anonymous Bind) ➢ NDS or eDirectory User (NDS User Bind) The type of bind the user authenticates with determines the content that the LDAP client can access. An anonymous bind is a connection that does not contain a username or password. If an LDAP client without a name and password binds to LDAP Services for eDirectory and the service is not configured to use a Proxy User, the user is authenticated to eDirectory as user [Public]. By default, user [Public] is assigned the Browse right to the objects in the eDirectory tree. The default Browse right for user [Public] allows users to browse eDirectory objects, but blocks user access to the majority of object attributes. This measure provides a fair idea of the number of [Public] users who are attempting to connect to Novell eDirectory.
	Bind requests that have been rejected: Indicates the number of bind requests that have been rejected due to inappropriate authentication or invalid credentials, since the last measurement period.	Number	This is a good indicator of the health of the security mechanism. If the value of this measure is unusually high, then you might have to investigate further to determine whether all rejects are genuine.

	Read requests received: Indicates the number of read requests received by the eDirectory server since the last measurement period.	Number	
	Add-entry requests received: Indicates the number of addEntry requests received by the eDirectory server since the last measurement period.	Number	addEntry requests attempt to create a new object - for example, adding a user object using ConsoleOne.
	Remove-entry requests received: Indicates the number of removeEntry requests received by the eDirectory server since the last measurement period.	Number	A removeEntry request attempts to remove an entry from the eDirectory server - for example, deleting a user using ConsoleOne.
	Modify-entry requests received: Indicates the number of modifyEntry requests received by the eDirectory server since the last measurement period.	Number	A non-zero value for this measure indicates the number of requests received for modifying one/more eDirectory entries - for example, modifying the attributes of any user using ConsoleOne.
	Search requests received: Indicates the number of search requests received since the last measurement period - this includes baseObject searches, oneLevel searches, and whole subtree searches.	Number	

	Operations forwarded by this eDirectory server: Indicates the number of operations forwarded by this eDirectory server to other eDirectory servers since the last measurement period.	Number	An LDAP client issues a request to an LDAP server, but the server cannot find the target entry of the operation locally. Using the knowledge references that it has about partitions and other servers in the eDirectory tree, the LDAP server identifies another LDAP server that knows more about the DN. The first LDAP server then contacts the identified (second) LDAP server. If necessary, this process continues until the first server contacts a server that holds a replica of the entry. eDirectory then handles all the details to complete the operation. Unaware of the server-to-server operations, the client assumes that the first server completed the request. This process is called **chaining**. While chaining has a fair share of advantages, a high value of this measure could also mean: ➢ One/more clients might have to wait for feedback while the server chains to resolve the same ➢ If the operation requires the LDAP server to send many entries across a WAN link, the operation might be very time consuming. ➢ If several servers are equally capable of progressing the operation, different servers might process two requests to operate on the same entry.
	Requests that could not serviced because of errors: Indicates the number of requests that could not be serviced due to errors other than security errors, and referrals since the last measurement period.	Number	A partially serviced operation will not be counted as an error. The errors include naming-related, update-related, attribute related, and service-related errors. Ideally, the value of this measure should be 0.

	Replication updates in: Indicates the number of replication updates fetched or received from eDirectory servers since the last measurement period.	Number	The Novell Import Conversion Export utility uses the LDAP Bulk Update/Replication Protocol (LBURP) to send asynchronous requests to an LDAP server. This guarantees that the requests are processed in the order specified by the protocol and not in an arbitrary order influenced by multiprocessor interactions or the operating system's scheduler. LBURP also lets the Novell Import Conversion Export utility send several update operations in a single request and receive the response for all of those update operations in a single response. This adds to the network efficiency of the protocol. The LBURP processor in eDirectory also commits update operations to the database in groups to gain further efficiency in processing the update operations. LBURP can greatly improve the efficiency of your LDIF imports over a traditional synchronous approach.
	Replication_ updates out: Indicates the number of replication updates sent to or taken by eDirectory servers since the last measurement period.	Number	
	Incoming traffic: Indicates the incoming traffic on the interface. This will include requests from DUAs as well as responses from other eDirectory servers.	KB	This is a good indicator of the level of activity on the eDirectory server.
	Outgoing traffic: Indicates the outgoing traffic on the interface. This will include responses to DUAs and eDirectory servers as well as requests to other eDirectory servers.	KB	

Chapter 2

Conclusion

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

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