GSX

Database Monitoring and Reporting Capabilities of GSX Monitor

Document Information

Document Name: Database Monitoring and Reporting Capabilities of GSX Monitor

Document Version: 1.0

Release Date:

Part Number:

Authors: Eileen Fitzgerald – VP Product Management and Customer Service

Sebastien Giraud – VP Software Development

Legal Statement

Disclaimer

Company Information

GSX Groupware Solutions has its registered office at 36 Boulevard Helvétique, 1207 Genève, Switzerland.

Contents

1 About This Document

This section outlines the purpose and aim of the document, related documents, and any source materials or terminology used.

Please note that this document is regarded as confidential and is for customer use only.

Purpose

The purpose of this document is to provide a detailed overview of the database monitoring and reporting capabilities of ***GSX Monitor*** software.

Related Documents

In addition to this guide, you can also refer to the following documents in the GSX Groupware Solutions documentation set for information:

- *GSX Environmental Health*
- *Alerting Capabilities of GSX Monitor*

Terminology

The following table contains a definition of the terms commonly used in the document:

Term	Definition
Audit Rule	Rules or reports you can run on demand.
Automatic Rule	Rules that can be defined and scheduled to automatically send a report to an Alert Profile.
Server	The physical server (or VMWare slice) that is being monitored.
System	The system that resides on the server. For example, BES, Sametime, or Exchange.
Threshold	A customer defined point that generates an action and/or event when reached.
Alerts	Alarms that are generated when a monitored Key Performance Indicator (KPI) has exceeded a predefined

	threshold.
Delivery Method	The method by which an alert is delivered to one or more predefined recipients. For example, phone, pager, email, or fax.
Reminders	If an alert is generated and the condition generating this alert is not addressed within a predefined time frame, a reminder is sent to the original recipient.
Escalation	If a reminder concerning an alert is sent and the condition generating the alert is still not addressed, an escalation alert is generated. This escalation is delivered to a recipient other than the recipient of the original and reminder alerts, such as a manager.
Severity	Defined severity levels for different alerts. For example, pending mail greater than a predefined threshold may be a severity 3 alert, while a server down may be defined as a greater, severity 1, alert. The ability to associate several different severity levels with every alert enables administrators and IT managers to prioritize their response to alerts.
Profiles	Tailored alert settings that can be applied to the alerts that you want activated. Profile details include, Profile Name, Delivery Mechanism, Target, Severity, Reminder, and Escalation.
Maintenance	The time period where a server can be taken offline for systems maintenance. In some cases the server may be unavailable to the business. GSX Monitor enables you to specify repeat or once off maintenance periods that can be excluded from reporting and alerting if required.

2 Overview

GSX Monitor is the most widely used monitoring tool on the market today and currently safeguards over 5 million email accounts. The software can simultaneously monitor IBM Lotus Domino and Sametime, Microsoft Exchange, Blackberry Enterprise Servers, LDAP and SMTP ports, and URLs.

Alert capability is an integral part of the ***GSX Monitor*** software solution and warns administrators of potential problems before they lead to performance problems or outages. Alerts can be configured so the correct personnel are notified when performance indicators reach defined levels. As a result, remedial action can be taken ***before*** a problem actually occurs. The use of this proactive, automated monitoring can save money for your business, while ensuring a reliable service from your communications infrastructure.

In this increasingly technology driven, fast-paced and demanding business environment it is vital that IT systems function efficiently and do not create a potentially crippling business impact when they are not available.

Many Domino applications start out as a very simple database with a simple function. Applications gradually become more complex with the inclusion of additional functionality and integration with other systems. This increases their importance to the business. These databases support business continuity and in frequent cases, if they are not available, not updated or fail to replicate, the business cannot function and the business loses money.

This document details the importance of monitoring business critical databases from a system and service perspective. It also highlights what is possible with GSX, and provides real life examples of the negative results that occur when your business critical databases are not effectively monitored.

3 The GSX Approach

The GSX team have been developing monitoring, reporting, and alerting solutions for collaboration platforms for over 14 years. We work with global multinational customers and partners to ensure that our products are customer focused and new releases incorporate customers' requirements and suggestions.

GSX Monitor can be installed on any client machine on your network and enables the following:

Service and Server Monitoring

The GSX approach is unique and is tried and tested over the many years that we have been in business. Our competitors have tried to imitate this approach with very limited success.

As GSX software emulates a customer accessing the system we, uniquely, simulate the level of service that your customers are experiencing and provide quantifiable metrics on the level of service and Service Level Agreements (SLAs) that they are experiencing and expecting. For example, a server may be up and running, but if your customer cannot work with their data on the server then your service is unavailable. GSX software removes this risk by providing a real-time view of the health of your entire communications infrastructure.

Non Invasive Installation on Servers

As no installation on your servers is required, GSX software results in a low maintenance and management overhead. You can install the software on a client and monitor hundreds of servers from that one single installation.

Consistent Reporting Across Multiple Platforms

As ***GSX Monitor*** software tracks and gathers information, this information is consolidated into ***GSX Analyzer***. Using the software's powerful and highly customizable report building capabilities, you can generate consistent reports across multiple platforms and/or metrics. This ensures you build the reports that you want to deliver.

4 Why Flexibility is Important

At GSX we provide a reporting solution that is highly customizable to suit your business and provide multiple configuration points on alerts. These include:

- The type of alert
- The threshold level that triggers alert generation
- Who the alert is sent to
- How the alert is delivered
- How often the alert is repeated

Such flexibility is vital as the tools that comprise the collaboration suite frequently consist of email, Blackberry, and online collaboration systems. ***GSX Monitor*** will monitor and report on all of these environments at a highly detailed level. If there is a potential issue it is critical that notification is received rapidly, by the correct personnel. This ensures they can address the issue, perhaps before it is even noticed by the business.

The ability to configure different alerting profiles and apply them to different incident scenarios ensures the right information gets to the right person at the right time. Another factor to consider is, as IT departments grow and develop, responsibility becomes more and more segmented and distributed. Therefore, sending all alerts to everyone in the department, or sending alerts to irrelevant teams may result in them being treated as a nuisance and ignored. This may result in a negative impact on the response time to a relevant alert.

With ***GSX Monitor*** you can target your alerts to ensure that they are delivered only to relevant personnel. Ideally, you should set alerts to give warnings of threats to your service and ensure they get the response that they deserve by tailoring and configuring them to meet your business service expectations and organizational support structure.

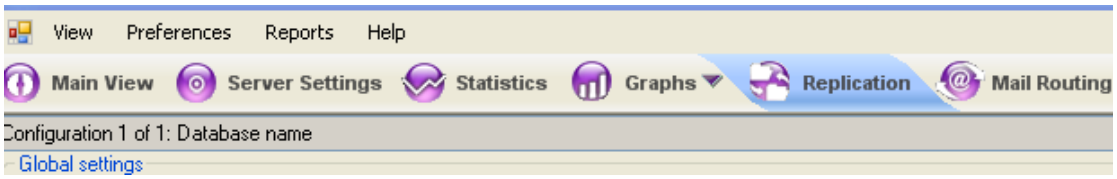
Important: Set your alerts at a threshold that indicates they are alerts and not just information. This ensures alerts generated in your environment are treated with the urgency that they merit.

5 Configuration of Database Management Options

In this section we will discuss the various database management options available for configuration in ***GSX Monitor***.

Replication Tab

Under the **Replication** tab there are various options available to ensure critical data is replicated within the organization.

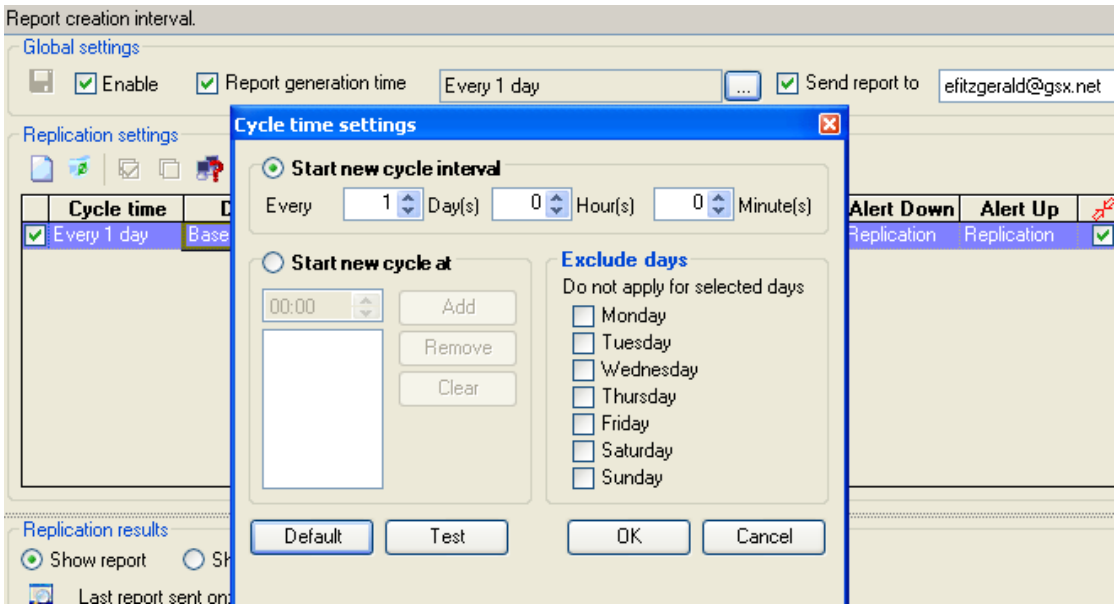


If data is not updated in a timely manner this can have a very costly impact on your business.

> **Real Life Example:** An example of this is a situation where engineering specifications were stored in and shared via Notes databases. Specifications were updated to resolve an issue but had not replicated in a timely manner to the assembly line in a separate continent. The entire production line was down and unable to work until they received the updated specifications.

The **Replication** tab enables you to do the following:

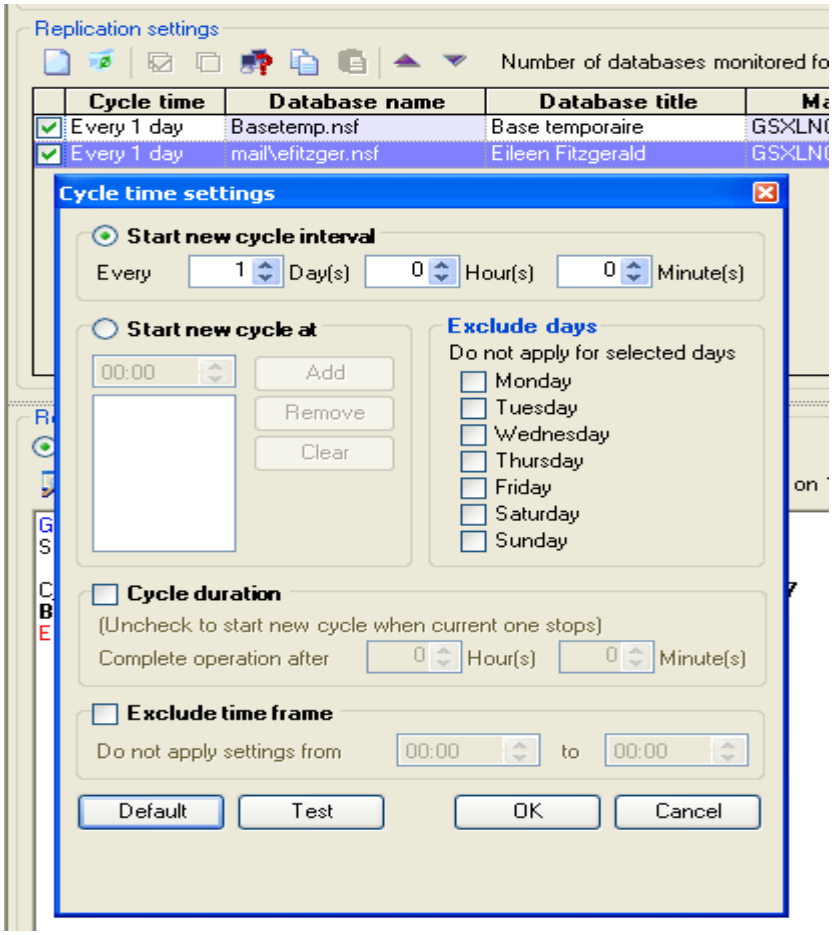
- Select a report to be generated on an, hourly, daily, or weekly basis and emailed to individuals or a distribution list.



- Set up replication monitors to ensure successful replication of your targeted database.

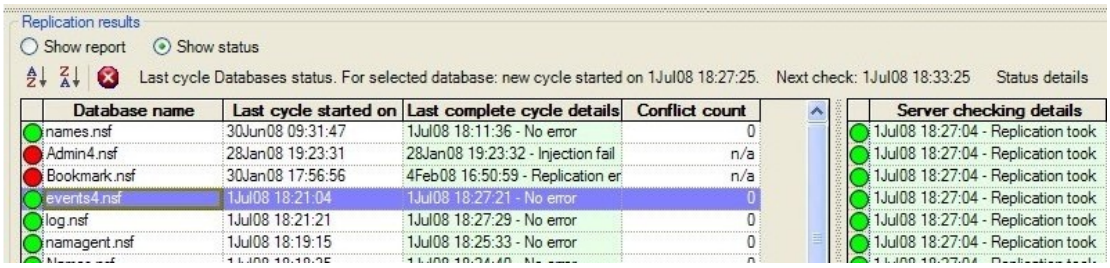
With ***GSX Monitor*** you can configure and monitor up to 200 databases and set alerts to automatically notify you if errors are detected. This is defined by configuring the following parameters:

- **Cycle Times** – The duration of time before replication is considered in error and an alert is generated.



- To include information on replication conflicts, click  .
- To include information on document count, click  .
- To include information on document information, click 
  Replication errors are always reported, however selecting this option adds all replication information, even when replication is successful. This results in larger replication reports.

Example of a replication report:



Name and Address Book (Names.nsf - ID=8525634A:006F7DAA) - OK=42 KO=0 Other=1 Excluded Server(s)=2
Maximum Replication Time: 67 minutes Average Replication Time: 23 minutes
Replication completed successfully on 42 server(s). 1 server(s) could be accessed. 2 excluded server(s).
ALBR0000 - Brisbane User server: NT - Available after 54 mns (13:54). Server is 0 mns ahead. Time zone= -1 (23322 Docs)

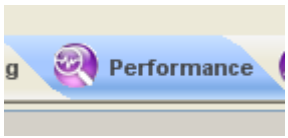
The following is a description of the various outputs of the replication report:

- **Name and Address Book (Names.nsf - ID=8525634A:006F7DAA)** - the database title, filename, and Replica ID.
- **OK=42 KO=0 Other=1 Excluded server(s)=2**
  - OK=n - the number of servers that successfully received a document change.
  - KO=n - the number of servers that did not receive a document change.
  - Other=n - the number of servers that could not be checked due to an access problem, therefore, have some kind of replication error.
  - Excluded server(s) =n - the number of servers for which replication monitoring of that particular database is skipped.
- **Maximum Replication Time** - the maximum time it took for a document change to replicate from the master server to another server during the cycle.
- **Average Replication Time** - the average time it took for document changes to replicate from the master server to all other servers during the cycle.
- **Replication completed successfully on 42 server(s). 1 server(s) could be accessed. 2 excluded server(s)** - more detailed information on replication errors.
- **ALBR0000 - Brisbane User server: NT** - the alias of a server checked for replication.
- **Available after 54 mns (13:54)** - this output indicates that if a change is made to the database Names.nsf on the master server, then the change became available on server ALBR0000 54 minutes later, at 13:54 local time. This is not the replication time between the 2 servers; it is the time users had to wait for the change to become available on their server.
- **Server is 0 mns ahead** - the time difference between the master server and the server being checked. The master server time is the reference time and time zone.
- **Time zone=-1 -** time zone in which the server being monitored resides.
- **(23322 Docs)** - the number of documents found in the monitored database.

6 Response Time and Database Availability

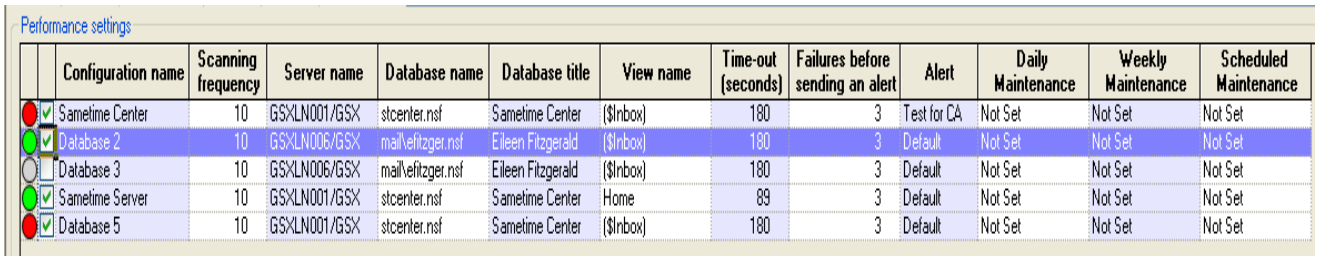
The ability to monitor the availability of individual databases highlights yet again the importance of flexibility in your monitoring environment. Simply monitoring the availability of the server is not sufficient to ensure that the service, such as the business functionality that the database provides, is being delivered to your customers.

What if a view is corrupted and users cannot access the database? Will this be highlighted by Server Monitoring? By having focused alerts on specific business critical databases you can ensure that you have a proactive alerting system in place. Know that there is an issue with your environment before your customer informs you.



Availability

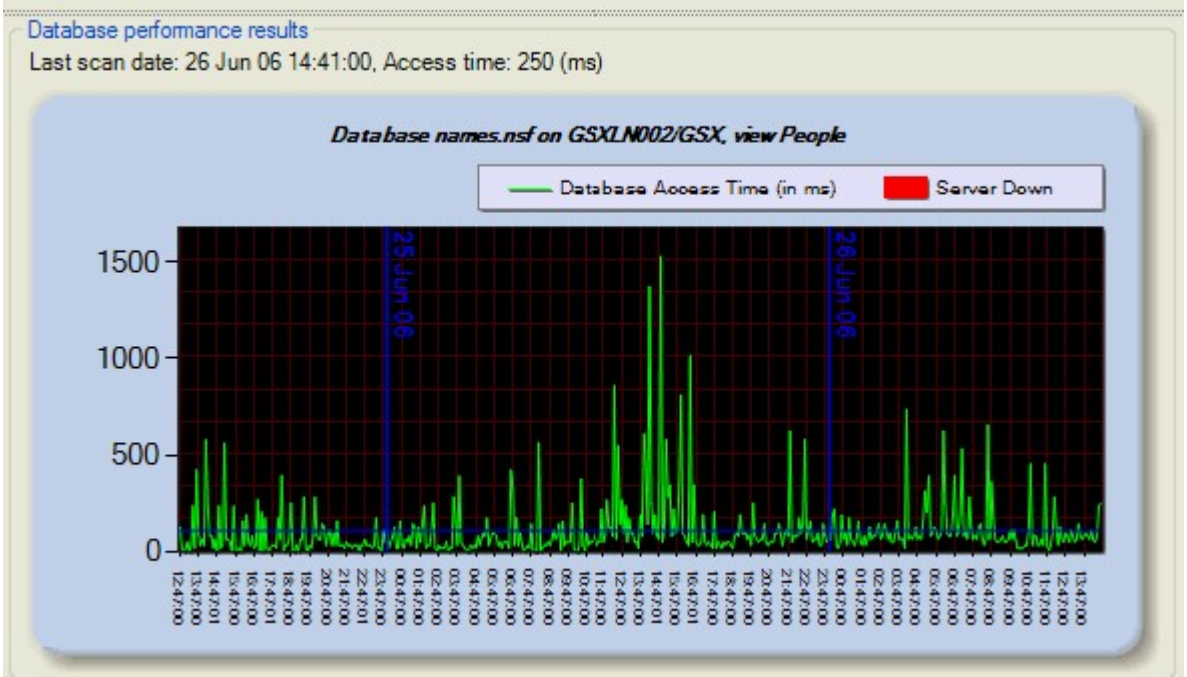
Under the **Performance** tab you can configure business critical databases to be monitored on a regular basis for availability and performance. You can configure ***GSX Monitor*** to repeatedly test open a database on a specific view. If the view fails to open in a predefined number of seconds, for a predefined number of repeat attempts, then an alert is generated.


Performance settings

Configuration name	Scanning frequency	Server name	Database name	Database title	View name	Time-out (seconds)	Failures before sending an alert	Alert	Daily Maintenance	Weekly Maintenance	Scheduled Maintenance
Sametime Center	10	GSXLN001/GSX	stcenter.nsf	Sametime Center	($Inbox)	180	3	Test for CA	Not Set	Not Set	Not Set
Database 2	10	GSXLN006/GSX	mail\efitzger.nsf	Eileen Fitzgerald	($Inbox)	180	3	Default	Not Set	Not Set	Not Set
Database 3	10	GSXLN006/GSX	mail\efitzger.nsf	Eileen Fitzgerald	($Inbox)	180	3	Default	Not Set	Not Set	Not Set
Sametime Server	10	GSXLN001/GSX	stcenter.nsf	Sametime Center	Home	89	3	Default	Not Set	Not Set	Not Set
Database 5	10	GSXLN001/GSX	stcenter.nsf	Sametime Center	($Inbox)	180	3	Default	Not Set	Not Set	Not Set

Performance

While it is important to monitor availability, knowing the average response time of a number of databases on your servers can be critical for various other reasons.



- **Troubleshooting**
  Troubleshooting is a vital part of performance management. If you are monitoring the response time of multiple databases on the same server and a user complains about response times on one of the databases, where does the fault lie and where do you start troubleshooting on the server or the database? Where you start your trouble shooting has a major impact on time to resolution and radically reduces the time required to identify the issues, assign resources, and get the business back up and running. As you are monitoring multiple databases on the one server you now have a very advantageous starting point to identify where your problem lies:
  - If all five databases being monitored are showing a performance decrease then it is an issue at server level.
  - If only one of the databases is showing a performance issue, then it is an issue with the database.
- **Change Management**

  When making changes to databases, for example version, bug, or upgrades, it is vital to identify the success or failure of the changes that are implemented. Two key metrics that can be used to judge the success or failure of the implementation are the average availability percentage

and the response times. If either of these key metrics decline after a change to a database then you cannot classify the change as a success.

- **SLA**
  For databases that are critical to the business there may be a formal Service Level Agreement that defines the expected quality of service delivery in quantifiable metrics. Formal and regular reporting is expected with these SLA's. Frequently, customers who outsource their IT collaborative management put in place SLAs on the key business points, and both customers and providers need to have a structured, quantifiable method of measuring service.

7 Detailed Database Monitoring

The **DB Monitoring** tab in ***GSX Monitor*** enables you to configure detailed databases rules.

Rules are reports which are scheduled to run automatically at specified intervals or triggered manually. Optionally, you can associate an alert profile with a rule, so that an alert is sent when a parameter exceeds a specified threshold. Database Monitoring rules are grouped into four categories:

- ACL Monitoring
- Size & Quota Monitoring
- Agent Monitoring
- Database Usage

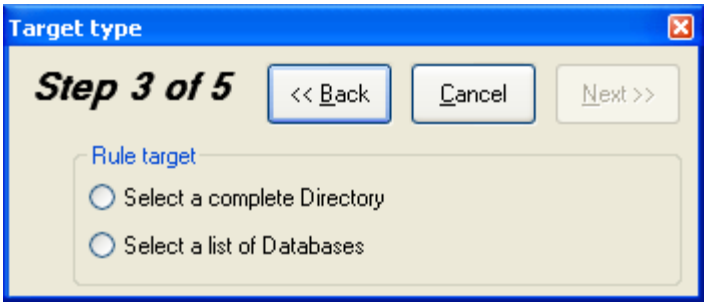
You can set the scanning mode for each rule to be **Audit** or **Automatic**:

- **Audit** rules are triggered manually and are intended for reports you want to run on demand.
- **Automatic** rules are executed automatically based on the scanning interval you specify.

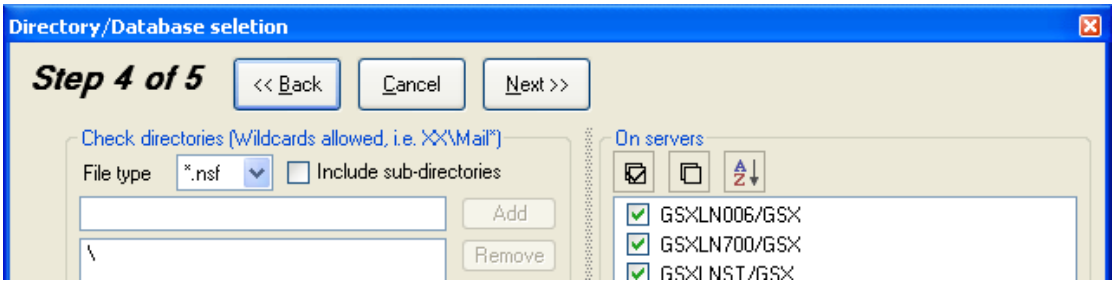
Note: Rules in the Database Usage category cannot be configured as **Automatic** as this feature uses a lot of resources on the server and slows down the performance of ***GSX Monitor***.

Click the new rule icon to create and configure a new rule. A setup wizard will appear with a series of dialog boxes to guide you through the five configuration steps:

- **Step 1** - Select the rule category (ACL Monitoring, Database Size, Agent Monitoring or Database Usage)
- **Step 2 -** Select a specific type of rule and enter the parameters required for that rule.
- **Step 3** - Choose whether you want to select a complete directory or a list of specific databases.

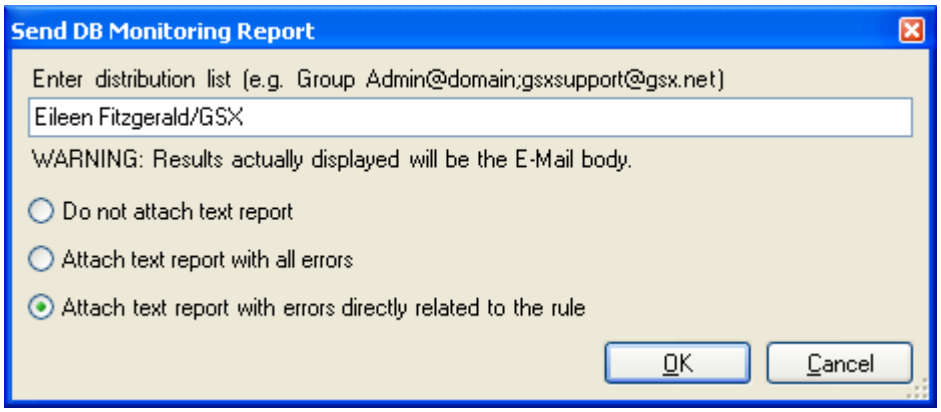


- **Step 4** - Select the databases and/or directories. All rules are applied to run on selected servers as defined in the **Server Settings** folder. The target databases are selected by their file name or their directory name from a list on the server as shown below.



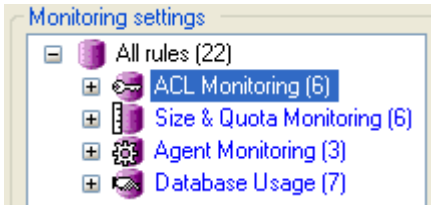
- **Step 5**: Configure the alias, alert, and scanning frequency.

An additional report can be run and sent at any time, using the **Send Report** option shown below:

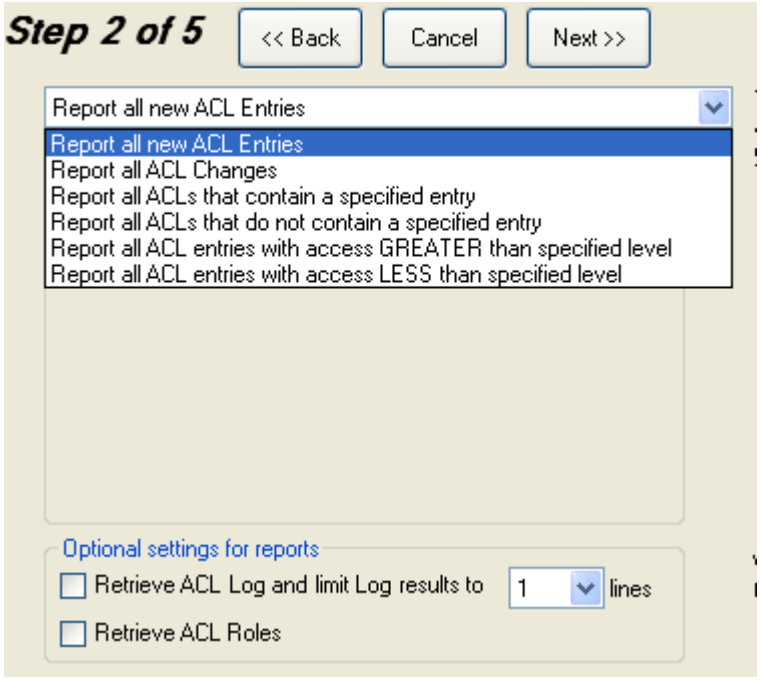


ACL Monitoring

Under **ACL Monitoring**, in the **DB Monitoring** folder, you can configure reports that enable you to monitor changes to ACL entries.



In today's security and compliance focused IT environment, it is critical to have security controls in place and to monitor those controls closely to ensure they are working as expected. ACL access is the key Domino security control and ACL Monitoring rules can be used to verify whether the controls in place are working effectively.



The various ACL Monitoring rules available in ***GSX Monitor*** described in the sections below:

Report on all new ACL Entries

This rule reports on all new ACL entries on selected databases or directories since the last scan. This means a new ACL entry is reported only once. This report can be defined as either **Automatic** or **Audit** to facilitate scheduled or immediate scanning if a security breach is suspected. In today's security and compliance focused IT environment, not only is it critical to prove that controls are in place, it is critical to be able to prove that the effectiveness of these controls is monitored.

Report on all ACL Changes

This rule reports on all ACL changes since the last scan. This includes additions, deletions, and modifications, even for roles if that option is selected.

Report all ACL's that contain a specified entry

This rule searches all databases for a specific ACL entry, for example, anonymous, or if there is a security issue for a specific group or person. This rule can be run in **Audit** or **Automatic** mode and can also trigger an alert when running in **Automatic** mode.

Report all ACL's that do not contain a specified entry

This rule searches all databases and reports on the absence of a specific ACL entry. For example, LocalDomainServers which has to be present for replication purposes. This rule can be run in **Audit** or **Automatic** mode, and alerts can be set on the automatic rule to trigger when the condition is met.

Report all ACL's with access GREATER than the specified level

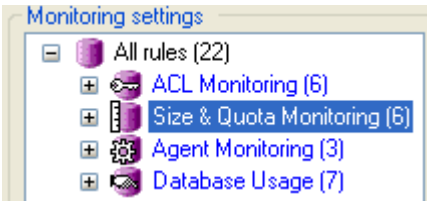
This rule returns a list of all of the databases on a specified server or directory where the level of access is greater than the threshold level. For example, indicating who has manager access, which is greater than designer access, to databases on the hub server. This report can be run in both **Automatic** and **Audit** mode with the option to set alerts on the automatic report.

Report all ACL's with access LESS than the specified level

This rule returns a list of all of the databases on a specified server or directory where the level of access is less than the threshold level. For example, indicating who has author access, which is less than editor access, to databases in the Sales folder. This report can be run n both **Automatic** and **Audit** mode with the option to set alerts on the automatic report.

Size & Quota Monitoring

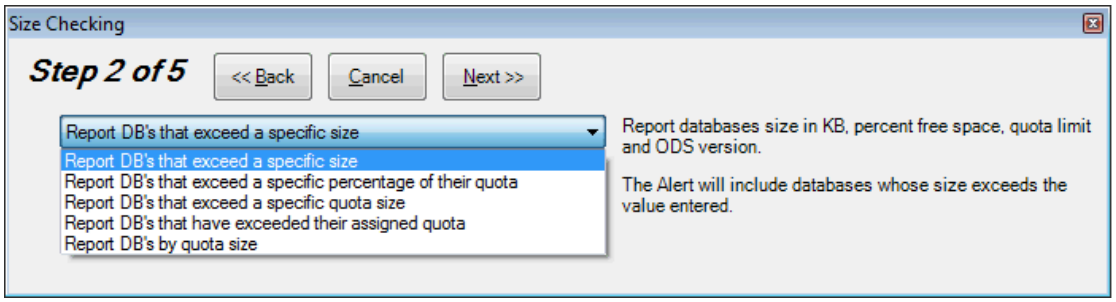
Size and Quota Monitoring rules for databases were introduced to assist administrators in managing the storage requirements of their Domino Servers and ensuring storage is used efficiently.



It is often said that disk space is cheap, but the overheads associated with inefficient disk space usage are far from cheap, and can be a significant but hidden cost. When purchasing or allocating additional disk space, the following cost and management overheads must also be taken into account:

- Cost of backups, including the additional time and storage requirements for backups
- Antivirus
- Management such as operations and applications
- Performance - the larger the system, the higher the risk of poor performance
- Associated indexes such as CPU and storage
- Impact on resources of larger databases such as CPU and Memory
- WAN implications especially with Domino databases such as replication overheads

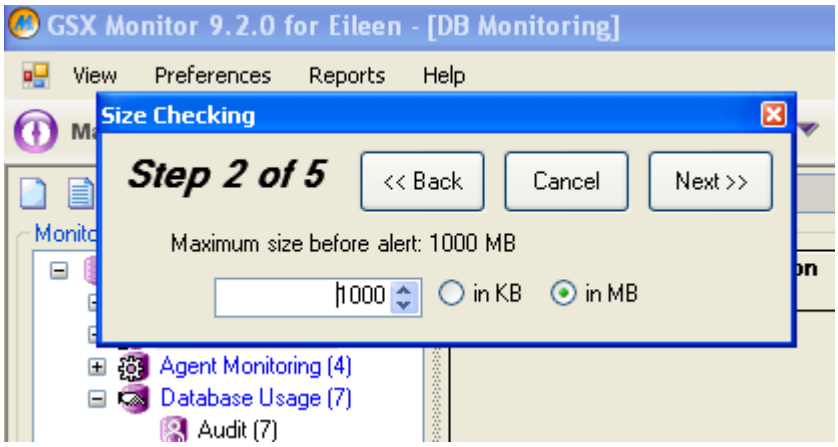
While the cost of adding additional disk space may not be high, when you factor in the ancillary costs associated with inefficient disk management, it can radically increase.



The various Size & Quota Monitoring rules available in ***GSX Monitor*** are described in the sections below:

Report DB's that exceed a specific size

This rule monitors a directory or a database and triggers an alert when the size exceeds a specified value. It can be configured as **Audit** or **Automatic**.



Report DB's that exceed a specific percentage of their quota

This rule reports on the number of databases that have exceeded a certain percentage of their quota. For example, you can run a report identifying the number of users that have exceeded 90% of their quota. These users may shortly have issues or receive warnings, so it is an ideal time for administrators to intervene and send them information on how to reduce their mail file size. Proactively offering this information to customers can greatly improve the impression of IT service delivery and reduce calls to the help desk.

Reports DB's that exceed a specific quota size

This rule reports on mail files that exceed a certain size. This helps administrators to understand the utilization of resources in the mail environment and identify resource intensive users.

Report DB's that have exceeded their assigned quota

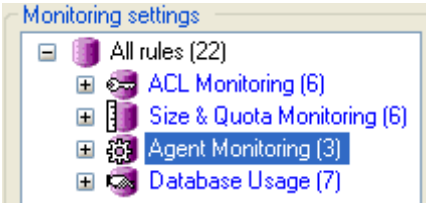
Domino uses a rule that prevents the delivery of mail to accounts that have reached their quota. Although this rule is effective, it is difficult to implement in practice because most IT Managers will not actually refuse to deliver email to a mailbox. While a user will be warned that they are about to reach their quota, once they exceed their quota, they will no longer be warned. Administrators can use the **Report DB's that have exceeded their assigned quota** rule to report on users that have exceeded their quota and are currently running over the quota allocated to them.

Report DBs by quota size

In many organizations, the mail quota assigned to users may depend on their role in the organization. For example, Marketing users may require a higher quota than Facilities, because Marketing may share more files. Administrators can use this rule to compile a list of databases that are set a certain quota. This report can be of great benefit when policies change or when performing a review of the allocation of quotas across departments, customers or the entire company.

Agent Monitoring

All databases have agents running on them to process data. Ensuring that an agent runs successfully can have a critical business impact.



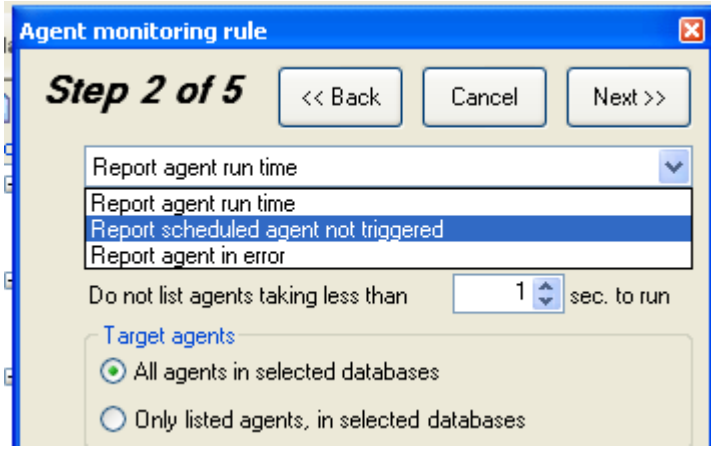
Real Life Example: An example of the importance of the good work practices of an agent is in a credit application business. During the day, credit applications are submitted from various regional offices. These applications are processed in a central approval database; those above a certain limit may be subjected to an additional approval cycle while some may be pre approved. All these decisions are made by a central processing agent.

If this agent fails in this job, then all credit processing stops, therefore the business stops, internationally. This is a real situation where successful day to day operations, with a turnover of approximately 1 Million Euro a day, depends on a single agent in a single database. Due to the potential impact of agent failure on the business, it is vital that this particular agent is monitored.

You can use Agent Monitoring rules to monitor the following:

- A specific agent
- All agents in a specific database
- All agents in all databases under a specific directory

You can also set these rules to run in **Audit** or **Automatic** mode and set alerts.



The various Agent Monitoring rules available in ***GSX Monitor*** are described in the sections below:

Report agent run time

It is very important to understand the average running time of agents for the following reasons:

- The work the agent performs may be time critical. For example, the rules may need to run outside of business hours and ensure that data is processed by the start of the following business day.
- If your agents are taking longer and longer to run it may indicate that additional resources are required.
- For change management purposes, if a code change has occurred and the average run time has significantly increased, there may be issues with the efficiency of the code or the benefits achieved by the code change.

Report scheduled agent not triggered

This rule specifically monitors agents to ensure that they have actually triggered.

Frequently it is the developers or database managers who receive these alerts and reports. With a business application it is even more important to proactively manage incidents relating to the application. The failure of one agent to process data can result in other individuals unable to perform their job function. Advance warning of issues with an application and the ability to resolve issues, before your customers even realize that there is an issue, is critical in the delivery of a high quality service to your customers.

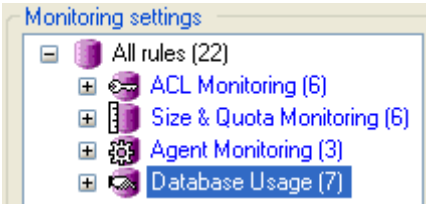
Report agent in error

This rule identifies agents that run to completion but report an error during their processing. This error may or may not impact on the results of the agent, but it is important to be notified if an error is detected such as corrupt data, access issues, missing data, or incorrect values.

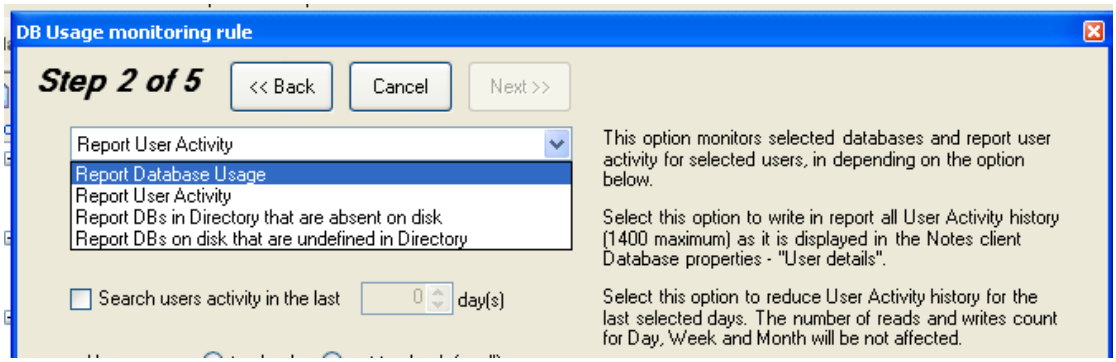
This rule retrieves information from a scan of the Log.nsf file. This can potentially take a long time and be resource intensive, depending on the size of the log and number of agents. It is important to be aware of resource requirements when configuring automatic rules. It is better to configure Automatic rules to run outside of business hours.

Database Usage

Database Usage rules enable you to monitor your Domino databases and evaluate their volume and type of user activity.



In a Domino environment, there can be thousands of Domino databases. It is important to know and understand the usage patterns on these databases, identify the databases that are used the most frequently as well as those that are not being used and could potentially be retired. In this section the various options for monitoring your Domino databases and compiling reports to evaluate their volume and type of user activity are discussed.



The various Database Usage rules available in ***GSX Monitor*** are described in the sections below:

Report Database Usage

Database usage monitoring compiles a report based on the content of the database properties. It reports on the database size, last usage, and the volume of reads and writes in the past month, week, and day.

The database usage rule can be run in **Audit** mode and reports on a specific database or all databases under a specified directory.

This report is very important in meeting the following customer requirements:

- Identifying databases not in use.
- Identifying the databases that are heavily in use.
- Identifying the type of usage. For example, reads or writes and is the data being modified or used as reference.
- Improving efficiencies in your infrastructure and building your collaborative infrastructure to suit how the business is using the collaborative tools.

Report User Activity

This rule reports on who is using your databases and how are they using them.

Use this rule to report on the activities of the following:

- All users
- A specific user
- Multiple users

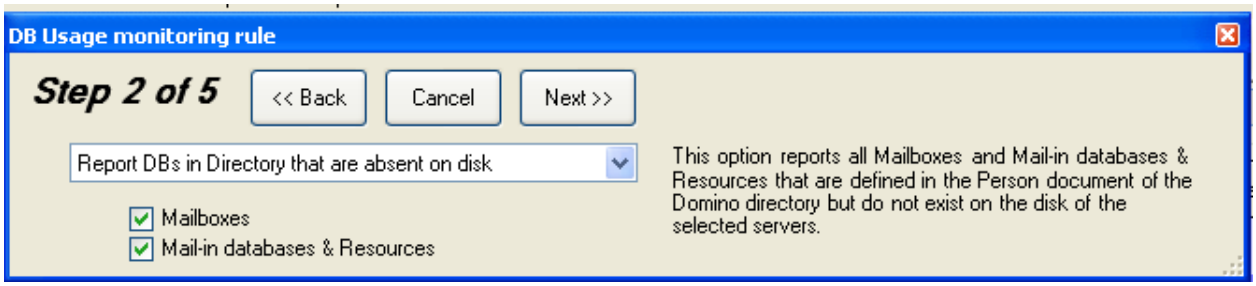
You can apply this rule to one or multiple databases over a specified number of days for as long as the data is in the database properties of the database. The resulting report will provide you with information per database on user reads and writes to the database per month, week, and day.

For security purposes, or to provide information on individual usage trends, this report can be invaluable and save many hours of manually scanning individual databases. This report can be run in **Audit** mode against a specific database or multiple databases contained under a specific directory.

Report DBs in Directory that are absent on disk

Collaborative infrastructures change on a regular basis to meet the business requirements. During times when the physical infrastructure is changing, the physical attributes may not match what is configured in the Domino Directory. Administrators may test configurations and make configuration changes which result in a mismatch of profile documents and corresponding databases.

This rule is configured to ensure that all Mail, resources and mail-in databases have a correctly configured database associated with them.



This rule enables you to configure an address book to check for profiles and then select a specific server or servers to check that the profiles configured for that server actually have corresponding databases on the server. A report is returned highlighting the configurations that do not have a corresponding database.

Report DBs on disk that are undefined in Directory

This rule reports on orphaned database where the profile document has been removed, or never existed in the first place, and there is no corresponding database. It performs a search and compares databases in the mail and mail folders, checking there are matching account or profile documents. In a busy environment, for security purposes, the account may need to be removed immediately, but the database may need to be retained for a period of time to ensure that all of the data has been mined before it is deleted. This ensures it is not forgotten and left to use up valuable disk space and resources. Running a periodic check on these databases can help ensure that these orphaned databases are identified and tidied up.

8 Summary

Frequently, when we look at the components of a collaborative environment, we can overlook the importance of the functions of a Domino database. The service that you deliver to your customers is the service that the business depends on. You need to focus on that service and the specifications of that service that define quality for your customers.

It is not enough to ensure that the server that hosts the Domino database is running; you need to monitor and manage all components of your service. For Domino database management, delivering a quality service can involve ensuring that your databases replicate on time, your response time is within agreed metrics, agents run on time, and your access controls levels are secure and monitored. With so many different aspects to monitor and report on, accuracy and efficient monitoring and reporting requires that the process be consolidated and automated.

9 About GSX Groupware Solutions

Thank you for your interest in GSX Groupware Solutions. GSX is the leading provider of monitoring solutions for messaging and communication environments with more than 500 clients worldwide, including 30% of Fortune 100 companies.

Our clients rely on GSX solutions to monitor their communications infrastructure, and ensure reliable and continuous services. The GSX solution is the only tool available that enables you to monitor, and proactively manage all of your messaging environments through one effective interface.

With a proven track record, GSX solutions offer the most reliable and effective monitoring solution available today. Our strategic partners include IBM, Blackberry Alliance, Microsoft, Double Take Software, Bluewave, Lotus Notes User Group, BMC, and AT&T.

For More Information:

For more information, visit www.gsx.com, where our resource center contains FAQs, Case Studies, Podcasts, White Papers and Webinars. You can also download a fully functional, 30 day evaluation copy of ***GSX Monitor***, ***GSX Server Guard***, and ***GSX ID Manager***.

10 Contact Us

By Email:

Technical Support:	*support@gsx.com*
Sales and Licensing Information:	*sales@gsx.com*
Marketing, business development or partnerships:	*feedback@gsx.com*
Careers and other information:	*gsx@gsx.com*

By Phone or Mail:

HEAD OFFICE:

GSX Groupware Solutions Headquarters
36 Boulevard Helvétique
1207 Genève
Switzerland
Tel: + 41 22 735 82 40
Fax: +41 22 735 82 45

NORTH AMERICA:

GSX Groupware Solutions
240 Redtail Road, Suite 14
Orchard Park, NY 14127
Office: +1 310 765 4139
Toll Free: +1 877 894 0961
Fax: +1 781 670 9122

EUROPE:

GSX Groupware Solutions SARL
"Le Marina 7"
1545 route nationale 7
06270 Villeneuve-Loubet
France
Tel: +33 4 93 81 17 98
Fax: +33 4 93 53 92 33