Monitoring Active Directory

eG Innovations Product Documentation

www.eginnovations.com

eG
Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

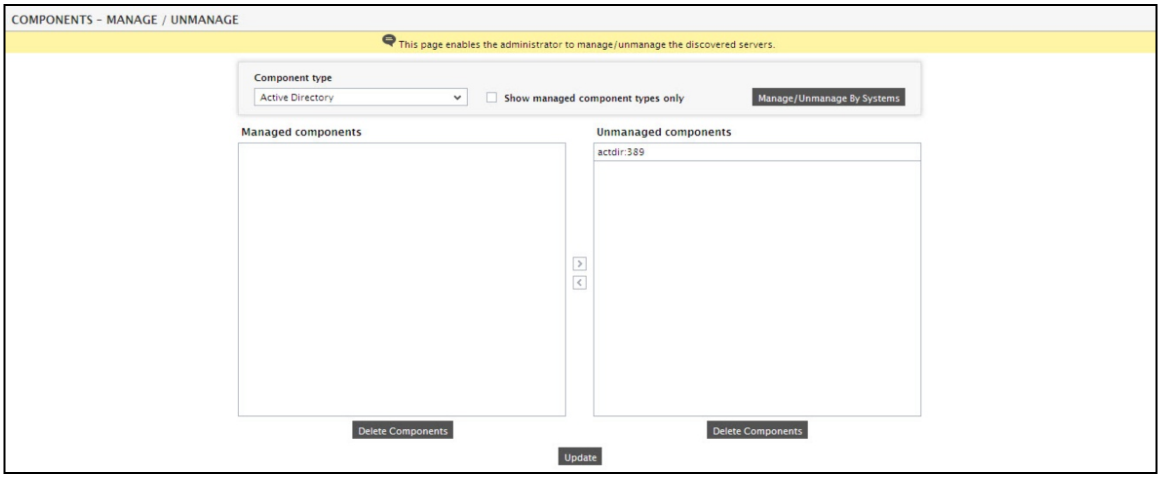
A directory service consists of both a directory storage system called the “directory store” and a mechanism that is used to locate and retrieve information from the system. The primary functions of the directory service are managed by the Directory System Agent (DSA), which is a process that runs on each domain controller (abbreviated as DC). Active Directory is the directory service that is included with Microsoft Windows. It stores objects that provide information about the real entities that exist in an organization’s network like printers, applications, databases, users etc. Active Directory is a part of the domain controller. It is associated with one or more domains. It stores information about users, specific groups of users like the Administrator, computers, applications, services, files, and distribution lists etc. Active Directory then makes this information available to the users and applications throughout the organization.

Active Directory is an important component of the Windows environment. Like any other Windows applications, its performance can affect the rest of the target environment. Active Directory consumes resources and the administrator needs to be aware of how much of the system's resources are being consumed over a long term. This helps the administrators to plan for future upgrades. Gathering performance data gives the administrators a good way to see the effects of any optimization efforts that he/she might attempt, and provides a great way for diagnosing problems when they occur. Most of the Windows servers and components are dependent on Active Directory either directly or indirectly. So monitoring the Active Directory server’s performance regularly is necessary to make sure that the target environment is meeting your business and networking goals. This is where the eG Enterprise helps administrators.

Chapter 2: Managing the Active Directory server

An Active Directory server is an integral part of a Windows 2000 server installation.

1. If an Active Directory server is automatically discovered by the eG Manager, it can be managed by the **COMPONENTS - MANAGE/UNMANAGE** page that appears when the Infrastructure -> Components -> Manage/Unmanage menu sequence is used. The screens below will guide you through this process. If an Active Directory server is not discovered automatically, then the **COMPONENTS** page can be used to manually add an Active Directory server for monitoring. In such a case, the manual management procedure can be dispensed with, as the eG Enterprise system automatically manages added components.



COMPONENTS - MANAGE / UNMANAGE

This page enables the administrator to manage/unmanage the discovered servers.

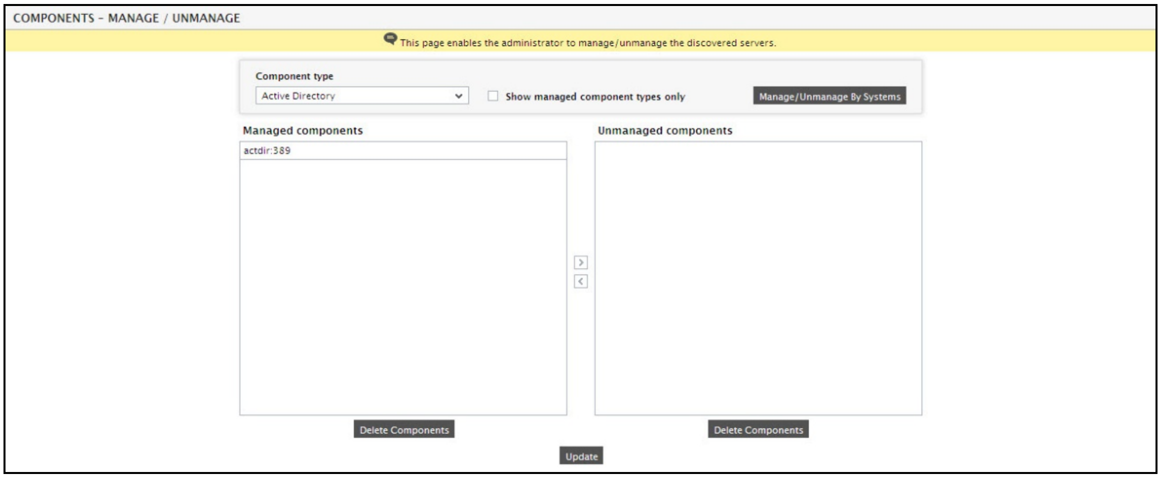
Component type: Active Directory

□ Show managed component types only

Managed components

Unmanaged components: actdir:389

Figure 2.1: Viewing the list of unmanaged Active Directory servers



COMPONENTS - MANAGE / UNMANAGE

This page enables the administrator to manage/unmanage the discovered servers.

Component type: Active Directory

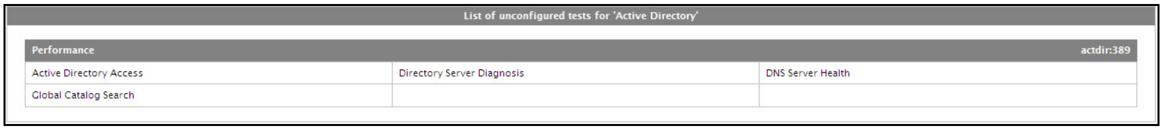
□ Show managed component types only

Managed components: actdir:389

Unmanaged components:

Figure 2.2: Managing the Active Directory server

2. Try to signout of the eG administrative interface. Figure 2.3 will appear prompting you to configure a list of tests.



List of unconfigured tests for 'Active Directory'

Performance		actdir:389
Active Directory Access	Directory Server Diagnosis	DNS Server Health
Global Catalog Search		

Figure 2.3: List of unconfigured tests for the Active Directory server

3. Click on the **Active Directory Access** test to configure it. This monitors the availability and response time from clients of the Active Directory server. To know how to configure the test, the **Monitoring Active Directory Servers** chapter.

4. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring Active Directory Servers

The eG Enterprise suite provides extensive monitoring support to the Active Directory (AD) server operating on Windows 2000, 2003, and 2008/2012. The specialized monitoring model that the eG Enterprise offers (see Figure 3.1) periodically executes a number of tests on the AD server to extract a wide gamut of metrics indicating the availability, responsiveness, and overall health of the AD server and its underlying operating system. Using this model, Active Directory servers can be monitored in an agent-based or an agentless manner.

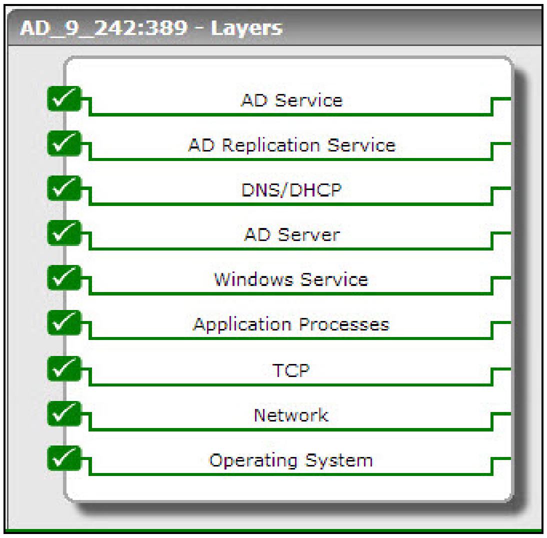


Figure 3.1: Layer model for Active Directory

Using these metrics, an administrator can find quick answers to the following performance queries:

- Is the AD server available?
- How quickly is the server responding to user requests?
- Are there adequate work items to service blocking requests, or are too many requests getting rejected?
- Have any internal server errors been reported recently?
- Have too many login attempts failed?
- Did session timeouts occur too frequently?
- Is the schema cache effectively utilized, or is disk read/write activity high?

- Is the server currently overloaded? Are sufficient domain controllers available in the environment to handle the load?
- Are all changes to the AD server getting replicated across and within sites?
- How many directory synchronizations are in queue? Is the number high enough to force a replication?

The last 5 layers of Figure 3.1 have been discussed in the *Monitoring Unix and Windows Servers* document, and will hence not be discussed again. However, for the Active Directory server alone, the **Operating System** layer is mapped to an additional **Net Logon** test. The section that follows will discuss this test in detail. All other sections in this chapter will focus only on the top 3 layers of Figure 3.1.

3.1 The Operating System Layer

The **Operating System** layer of a monitored Active Directory server typically runs all the tests that are mapped to the same layer for a Windows server or a Windows Generic server. The only difference however is that for the Active Directory server, an additional **Net Logon** test is mapped to this layer. This section provides details of the Net Logon test.

3.1.1 Net Logon Test

The Netlogon service is responsible for communication between systems in response to a logon request, a domain synchronization request, and a request to promote a Backup Domain Controller (BDC) to a Primary Domain Controller (PDC). The Netlogon service performs several tasks when servicing network logon requests. They are as follows:

- Selects the target domain for logon authentication
- Identifies a domain controller in the target domain to perform authentication
- Creates a secure channel for communication between Netlogon services on the originating and target systems
- Passes an authentication request to the appropriate domain controller
- Returns authentication results to Netlogon on the originating system

Delays in the Netlogon authentication process can often scar a user’s overall experience with not just the domain controller, but also with the application that requests for the authentication. In order to avoid undue authentication delays, you can use the **Net Logon** test. This test monitors the Netlogon authentication feature, proactively detects potential authentication bottlenecks, and promptly alerts administrators to what is causing the bottleneck, so that remedial actions can be initiated in good time.

Target of the test : An Active Directory server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory server being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The host for which this test is to be configured.
Port	Refers to the port used by the Windows server.

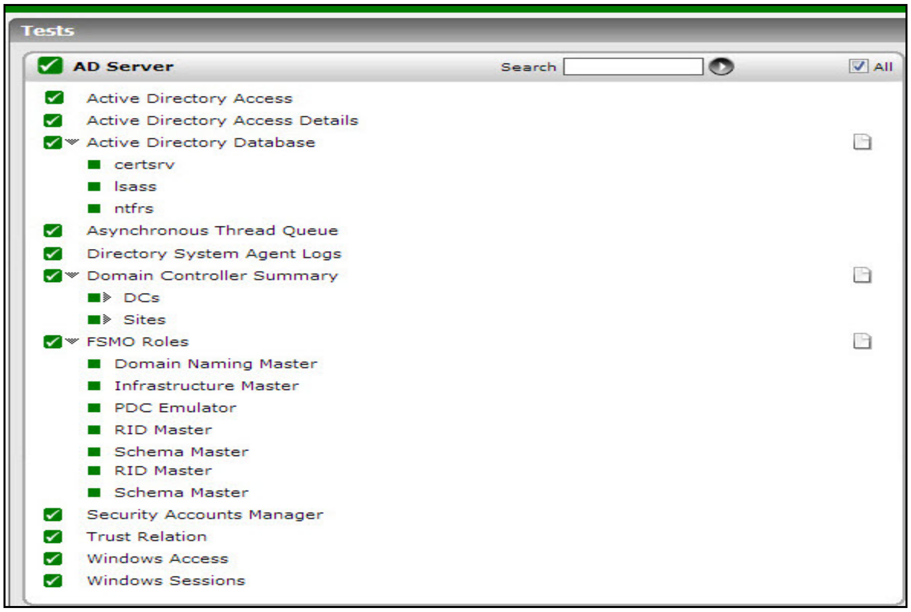
Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Semaphore waiters	Indicates the number of threads currently waiting to acquire the semaphore.	Number	A consistent increase in the value of this measure is a cause forconcern, as it indicates that the count of ‘busy’ semaphores is steadily increasing. This in turn could cause many threads/logon requests to be enqueued, due to the lack of adequate semaphores. Consequently, authentication will be delayed.
Semaphore acquires	Indicates the number of times the semaphore has been acquired over this secure channel during the last measure period.	Number	
Semaphore holders	Indicates the number of threads currently holding the semaphore.	Number	This is a good indicator of the current authentication workload over the secure channel. If the value of this measure is equal to the MaxConcurrentApi registry setting

Measurement	Description	Measurement Unit	Interpretation
			or is fast approaching that value, it indicates that the server is getting overloaded. Authentication delays and timeouts may occur as a result. The typical way to resolve the problem is to raise the maximum allowed worker threads that service that authentication. You can do this by altering the MaxConcurrentApi registry value and then restarting the Net Logon service on the servers.
Semaphore timeouts	Indicates the number of times a thread has timed out waiting for the semaphore over the secure communication channel during the last measure period.	Number	Ideally, this measure has to be 0. A non-zero value for the measure indicates that one/more authentication threads have hit the time-out for the waiting and the logon was denied. This is a sign of a very bad user experience, and typically occurs when the secure channel is overloaded, hung or broken. The typical way to resolve the overload problem is to raise the maximum allowed worker threads that service that authentication. You can do this by altering the MaxConcurrentApi registry value and then restarting the Net Logon service on the servers.

3.2 The AD Server Layer

This layer verifies the availability and responsiveness of the Active Directory (AD) service from an external location. This layer also monitors the user accesses to the AD server and reports how well the server handles access requests. In the process, the layer also reports useful session-related metrics pertaining to the user sessions on the AD server. Besides, the layer also reports the overall health of the AD database (see Figure 3.2).



Tests

☑ AD Server   Search   ☑ All

- ☑ Active Directory Access
- ☑ Active Directory Access Details
- ☑ Active Directory Database
  - 🟩 certsrv
  - 🟩 lsass
  - 🟩 ntfrs
- ☑ Asynchronous Thread Queue
- ☑ Directory System Agent Logs
- ☑ Domain Controller Summary
  - 🟩 DCs
  - 🟩 Sites
- ☑ FSMO Roles
  - 🟩 Domain Naming Master
  - 🟩 Infrastructure Master
  - 🟩 PDC Emulator
  - 🟩 RID Master
  - 🟩 Schema Master
  - 🟩 RID Master
  - 🟩 Schema Master
- ☑ Security Accounts Manager
- ☑ Trust Relation
- ☑ Windows Access
- ☑ Windows Sessions

Figure 3.2: The tests associated with the AD Server layer

3.2.1 Asynchronous Thread Queue Test

LSASS (Local Security Authority Subsystem Service) – the Windows process that is responsible for enforcing the security policy on the system - adopted its threading library from IIS to handle Windows socket communication, and uses the asynchronous thread queue to handle requests from Kerberos and LDAP.

Monitoring the asynchronous thread queue (ATQ) on an AD server will provide useful pointers to the request processing ability of the server. This test monitors the ATQ, reports the number and nature of requests queued in the ATQ, captures a steady growth (if any) in the length of the queue over time, and thus reveals potential processing bottlenecks on the AD server.

Note:

This test applies only to Active Directory Servers installed on Windows 2008.

Target of the test : An Active Directory server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory server being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
ATQ estimated queue delay	Indicates how long the request has to wait in the queue.	Secs	This is the estimated time the next request will spend in the queue prior to being serviced by the directory service.
ATQ outstanding queued requests	Indicate the number of requests currently in the queue.	Number	A high level of queuing indicates that requests are arriving at the domain controller faster than they can be processed. This can also lead to a high latency in responding to requests.
ATQ request latency	Indicates the time it takes to process an enqueued request.	Secs	Since the type of requests can differ, the value of this measure is typically not significant, as its an average value. An expensive LDAP query that takes minutes to execute can be masked by hundreds of fast LDAP queries or KDC requests. The main use of this measure therefore is to monitor the wait time in queue. Any non-zero value indicates that DC has run out of threads.
ATQ threads ldap	Indicates the number of threads used by the LDAP server as determined by LDAP policy.	Number	This measure indicates the number of threads currently servicing LDAP requests. If the value of this measure is unusually high, then look for the following: • Expensive or Inefficient LDAP

Measurement	Description	Measurement Unit	Interpretation
			queries • Excessive numbers of LDAP queries • An Insufficient number of DCs to service the workload (or existing DCs are undersized) • Memory, CPU or disk bottlenecks on the DC Large values for this measure are common but the thread count should remain less than the the value of the ATQ threads total measure. Also, note that this measure could also report abnormally high values for reasons that are initially triggered by LDAP but are ultimately affected by external reasons. Such reasons are as follows: • If the IP address of LDAP pings from clients does not map to an AD site: In this case, the LDAP server performs an exhaustive address lookup to discover additional client IP addresses so that it may find a site to map to the client. • If the DC supports LDAP over SSL / TLS: In this case, a user sends a certificate on a session. The server needs to check for certificate revocation which may take some time. This becomes problematic if

Measurement	Description	Measurement Unit	Interpretation
			network communication is restricted and the DC cannot reach the Certificate Distribution Point (CDP) for a certificate.
ATQ thread others	Indicates the number of threads used by other component, in this case KDC.	Number	You can also have external dependencies generating requests that hit the Kerberos Key Distribution Center (KDC). One common operation is getting the list of global and universal groups from a DC that is not a Global Catalog (GC). A 2nd external and potentially intermittent root cause occurs when the Kerberos Forest Search Order (KFSO) feature has been enabled on Windows Server 2008 R2 and later KDCs to search trusted forests for SPNs that cannot be located in the local forest. The worst case scenario occurs when the KDC searches both local and trusted forests for an SPN that can't be found either because the SPN does not exist or because the search focused on an incorrect SPN. Memory dumps from in-state KDCs will reveal a number of threads working on Kerberos Service Ticket Requests along with pending RPC calls to remote domain controllers.
ATQ threads total	Indicates the total number of threads that are currently allocated.	Number	This measure tracks the total number of threads from the ATQ threads Idap and ATQ threads other measures. The maximum number of threads that a given DC can apply to incoming workloads can be found my multiplying the product of MaxPoolThreads times the number of logical CPU cores.

Measurement	Description	Measurement Unit	Interpretation
			MaxPoolThreads defaults to a value of 4 in LDAP Policy and should not be modified without understanding the implications. Compare the value of this measure with the value of the ATQ threads ldap and ATQ threads other measures. If the ATQ threads ldap measure equals this measure in value then it implies that all of the LDAP listen threads are stuck processing LDAP requests currently. If the ATQ threads other measure equals this measure in value, then it means that all of the LDAP listen threads are busy responding to Kerberos related traffic. Similarly, note how close the current value for this measure is to the max value recorded in the trace and whether both values are using the maximum number of threads supported by the DC being monitored. If so, it's a sure sign of a potential overload.

3.2.2 ADAM Access Details Test

This test measures the load on the AD server in terms of the level of read-write activity on the server and the count of search operations performed by the server. In the process, the test reveals the following:

- Which AD services initiated the read-write operations? Which of these services generated the maximum I/O load on the server - is it the LSA? the NSPI? the NTDS? SAM? or the replication service? - this information is useful when administrators are faced with an AD overload, as it accurately points them to the probable sources of the load;
- Which AD service performed the maximum searches on the server? - in the event of an overload, this metric will help you identify that service which could be contributing to the

overload;

- Is the server sized with adequate threads to handle the I/O load?

Note:

This test applies only to Active Directory Servers installed on Windows 2008.

Target of the test : An Active Directory server

Agent deploying the test : An internal agent

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

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Schema cache hit ratio	Indicates the percentage of object name lookups serviced by the Schema Cache.	Percent	All changes made to Active Directory are validated first against the schema. For performance reasons, this validation takes place against a version of the schema that is held in memory on the domain controllers. This "in-memory version," called the schema cache, is updated automatically after the on-disk version has been updated. The schema cache provides mapping between attribute identifiers such as a database column identifier or a MAPI identifier and the in-memory structures that describe those attributes. The schema cache also provides lookups for class

Measurement	Description	Measurement Unit	Interpretation
			identifiers to get in-memory structures describing those classes. A low value of this measure indicates that the Directory Service needs high disk read/write activity to perform its job. This results in poor response time of the components available in the Active Directory.
Notify queue size	Indicates the number of pending update notification requests that have been queued and not transmitted.	Number	When any change in the Active Directory occurs, the originating domain controller sends an update notification requests to the other domain controllers. A high value of this measure indicates that the Active Directory is changing frequently but the update notification requests have not been transmitted to the other domain controllers. This results in a loss of data integrity in the directory store. This problem can be corrected by forcing the replication.
Current threads in use	Indicates the current number of threads in use by the directory service (which is different from the number of threads in the directory service process).	Number	This is the number of threads currently servicing client API calls; it can be used to indicate whether additional processors should be used. A fluctuating value for this measure indicates a change in the load. A low value could point to network problems that are preventing client requests from succeeding.
Server binds	Indicates the number of domain controller–to–domain controller binds per second that are serviced by this domain controller.	Binds/Sec	
Directory reads	Indicates the rate of	Reads/Sec	These measures serve as effective

Measurement	Description	Measurement Unit	Interpretation
	directory reads.		indicators of the ability of the AD server to process read, write, and search requests.
Directory writes	Indicates the rate of directory writes.	Writes/Sec	
Directory searches	Indicates the number of directory searches per second.	Searches/Sec	
DS reads from DRA	Indicates the percentage of reads on the directory by replication.	Percent	If the AD server is experiencing abnormally high read activity, then, you can compare the value of this measure with the values reported by the DS reads from KCC, DS reads from LSA, DS reads from NSPI, DS reads from NTDS, and DS reads from SAM measures to know which AD service is performing the maximum reads on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS reads from KCC	Indicates the percentage of reads performed by the Knowledge Consistency Checker on the directory.	Percent	The Knowledge Consistency Checker (KCC) generates the replication topology by specifying what domain controllers will replicate to which other domain controllers in the site. The KCC maintains a list of connections, called a replication topology, to other domain controllers in the site. The KCC ensures that changes to any object are replicated to all site domain controllers and updates go through no more than three connections. If the AD server is experiencing abnormally high read activity, then, you can compare the value of this measure with the values reported by the DS reads from DRA, DS reads from LSA, DS reads from NSPI, DS

Measurement	Description	Measurement Unit	Interpretation
			reads from NTDS, and DS reads from SAM measures to know which AD service is performing the maximum reads on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS reads from LSA	Indicates the percentage of reads performed by the Local Security Authority on the directory.	Percent	The Local Security Authority (LSA) is the security subsystem responsible for all interactive user authentication and authorization services on a local computer. The LSA is also used to process authentication requests made through the Kerberos V5 protocol or NTLM protocol in Active Directory. If the AD server is experiencing abnormally high read activity, then, you can compare the value of this measure with the values reported by the DS reads from DRA, DS reads from KCC, DS reads from NSPI, DS reads from NTDS, and DS reads from SAM measures to know which AD service is performing the maximum reads on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS?
DS reads from NSPI	Indicates the percentage of reads performed by the Name Service Provider Interface (NSPI) on the directory.	Percent	The Name Service Provider Interface (NSPI) is the protocol by which Messaging API (MAPI) clients access the AD DS. Exchange Address Book clients use the client MAPI provider Emsabp32.dll to look up e-mail addresses in the global catalog. The client-side MAPI provider communicates with the server through the proprietary Name Service Provider Interface (NSPI) RPC

Measurement	Description	Measurement Unit	Interpretation
			interface. If the AD server is experiencing abnormally high read activity, then, you can compare the value of this measure with the values reported by the DS reads from KCC, DS reads from LSA, DS reads from DRA, DS reads from NTDS, and DS reads from SAM measures to know which AD service is performing the maximum reads on the AD server - is it the replication service? the LSA? the KCC? or the NSPI?
DS reads from NTDS	Indicates the percentage of reads performed by the name service directory APIs on the directory.	Percent	If the AD server is experiencing abnormally high read activity, then, you can compare the value of this measure with the values reported by the DS reads from KCC, DS reads from LSA, and DS reads from DRA, DS reads from NSPI, and DS reads from SAM measures to know which AD service is performing the maximum reads on the AD server - is it the replication service? the LSA? the KCC? the NSPI? or the SAM?
DS reads from SAM	Indicates the percentage of reads performed by the Security Account Manager (SAM) on the directory.	Percent	The Security Accounts Manager (SAM) is used for verifying passwords and for checking passwords against any existing password policies that are in effect on a domain controller. If the AD server is experiencing abnormally high read activity, then, you can compare the value of this measure with the values reported by the DS reads from KCC, DS reads from LSA, and DS reads from DRA, DS reads from NSPI, and DS reads from NTDS measures to know which

Measurement	Description	Measurement Unit	Interpretation
			AD service is performing the maximum reads on the AD server - is it the replication service? the LSA? the KCC? the NSPI? or the NTDS?
DS writes from DRA	Indicates the percentage of writes on the AD server by replication.	Percent	If the AD server is experiencing abnormally high write activity, then, you can compare the value of this measure with the values reported by the DS writes from KCC, DS writes from LSA, DS writes from NSPI, DS writes from NTDS, and DS writes from SAM measures to know which AD service is performing the maximum writes on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS writes from KCC	Indicates the percentage of writes performed by the Knowledge Consistency Checker on the directory.	Percent	If the AD server is experiencing abnormally high write activity, then, you can compare the value of this measure with the values reported by the DS writes from DRA, DS writes from LSA, DS writes from NSPI, DS writes from NTDS, and DS writes from SAM measures to know which AD service is performing the maximum writes on the AD server - is it the replication service? the KCC? the LSA? the NSPI? the NTDS? or the SAM?
DS writes from LSA	Indicates the percentage of writes performed by the Local Security Authority on the directory.	Percent	If the AD server is experiencing abnormally high write activity, then, you can compare the value of this measure with the values reported by the DS writes from DRA, DS writes from KCC, DS writes from NSPI, DS writes from NTDS, and DS writes from SAM measures to know which AD

Measurement	Description	Measurement Unit	Interpretation
			service is performing the maximum writes on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS writes from NSPI	Indicates the percentage of writes performed by the Name Service Provider Interface (NSPI) on the directory.	Percent	If the AD server is experiencing abnormally high write activity, then, you can compare the value of this measure with the values reported by the DS writes from DRA, DS writes from KCC, DS writes from LSA, DS writes from NTDS, and DS writes from SAM measures to know which AD service is performing the maximum writes on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS writes from NTDS	Indicates the percentage of writes performed by the name service directory APIs on the directory.	Percent	If the AD server is experiencing abnormally high write activity, then, you can compare the value of this measure with the values reported by the DS writes from DRA, DS writes from KCC, DS writes from LSA, DS writes from NSPI, and DS writes from SAM measures to know which AD service is performing the maximum writes on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS writes from SAM	Indicates the percentage of writes performed by the Security Accounts Manager (SAM) on the directory.	Percent	If the AD server is experiencing abnormally high write activity, then, you can compare the value of this measure with the values reported by the DS writes from DRA, DS writes from KCC, DS writes from LSA, DS writes from NSPI, and DS writes from

Measurement	Description	Measurement Unit	Interpretation
			NTDS measures to know which AD service is performing the maximum writes on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS searches from DRA	Indicates the percentage of searches performed by the replication service on the AD server.	Percent	If the AD server is processing an abnormally large number of search requests, then, you can compare the value of this measure with the values reported by the DS searches from KCC, DS searches from LSA, DS searches from NSPI, DS searches from NTDS, and DS searches from SAM measures to know which AD service is performing the maximum number of searches on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS searches from KCC	Indicates the percentage of searches performed by the Knowledge Consistency Checker on the directory.	Percent	If the AD server is processing an abnormally large number of search requests, then, you can compare the value of this measure with the values reported by the DS searches from DRA, DS searches from LSA, DS searches from NSPI, DS searches from NTDS, and DS searches from SAM measures to know which AD service is performing the maximum number of searches on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS searches from LSA	Indicates the percentage of searches performed by the Local Security Authority on the directory.	Percent	If the AD server is processing an abnormally large number of search requests, then, you can compare the value of this measure with the values

Measurement	Description	Measurement Unit	Interpretation
			reported by the DS searches from DRA, DS searches from KCC, DS searches from NSPI, DS searches from NTDS, and DS searches from SAM measures to know which AD service is performing the maximum number of searches on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS searches from NSPI	Indicates the percentage of searches performed by the Name Service Provider Interface (NSPI) on the directory.	Percent	If the AD server is processing an abnormally large number of search requests, then, you can compare the value of this measure with the values reported by the DS searches from DRA, DS searches from KCC, DS searches from LSA, DS searches from NTDS, and DS searches from SAM measures to know which AD service is performing the maximum number of searches on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS searches from NTDS	Indicates the percentage of searches performed by the name service directory APIs on the directory.	Percent	If the AD server is processing an abnormally large number of search requests, then, you can compare the value of this measure with the values reported by the DS searches from DRA, DS searches from KCC, DS searches from LSA, DS searches from NSPI, and DS searches from SAM measures to know which AD service is performing the maximum number of searches on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?

Measurement	Description	Measurement Unit	Interpretation
DS searches from SAM	Indicates the percentage of searches performed by the Security Accounts Manager (SAM) on the directory.	Percent	If the AD server is processing an abnormally large number of search requests, then, you can compare the value of this measure with the values reported by the DS searches from DSA, DS searches from KCC, DS searches from LSA, DS searches from NSPI, and DS searches from NTDS measures to know which AD service is performing the maximum number of searches on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?

3.2.3 ADAM Database Test

This test reports critical statistics pertaining to the usage of the database caches, and the overall health of the AD database.

Target of the test : An Active Directory server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory server being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The host for which this test is to be configured.
Port	Refers to the port used by the Windows server.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Database cache hits	Indicates the percentage of page requests of the database file that were occupied in a cache before responding to the request.	Percent	Ideally, the value of this measure should be moderate. A high value of this measure indicates the high utilization of physical memory. In such a case, you can add the required memory to the database.
Database table cache hits	Indicates the percentage of database tables that were opened using cached schema information.	Percent	Ideally, the value of this measure should be high.
Log records waiting	Indicates the rate of log record stalls, per second.	Records/Sec	
Log threads waiting	Indicates the current number of threads waiting for data to be written to the log so that database updation will be executed.	Number	

3.2.4 Active Directory Access Test

This test monitors the availability and response time from clients of an Active Directory server from an external perspective.

Target of the test : An Active Directory or Domain Controller

Agent deploying the test : An external agent

Outputs of the test : One set of results for every Active Directory server being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port

Parameters	Description
	number is *389*.
Domain	The default value of this parameter will be *none*. In Windows 2003 environments however, the ADServerTest will function effectively only if a "fully qualified domain name" is provided in the this text box.
User	Provide the name of a domain user in this text box. This can be *none* for Windows 2000 environments.
Password	Provide the password for the domain user specified above, in this text box. This can be *none* for Windows 2000 environments.
Confirm Password	Confirm the Password by retyping it here.
ConnectTimeOut	By default, this is set to 30 seconds. This implies that by default, the test will wait for 30 seconds to establish a connection with the target Active Directory server. If a connection is established within the default 30 second period, then the test will report that the server is available; if the test is unable to connect to the server within the default period, then it will report that the server is unavailable. If it generally takes a longer time for clients to connect to the AD server in your environment, then, you may want to change the ConnectTimeOut period so that, the test does not time out before the connection is established, and consequently present an "untrue" picture of the availability of the server.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Active directory availability	Indicates the availability of the server.	Percent	The availability is 100% when the server is responding to a request and 0% when it is not. Availability problems may be caused by a misconfiguration / malfunctioning of the server, or if the server has not been started.
Active directory response time	Indicates the time taken by the server to respond to a user query	Secs	A sudden increase in response time is indicative of a bottleneck at the server.

3.2.5 Windows Access Test

This test monitors the accesses to an AD server.

Target of the test : An Active Directory server or a Domain Controller

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory server or a Domain Controller that is being monitored .

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The host for which this test is to be configured.
Port	Refers to the port used by the Windows server.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Blocking request rejects	The number of times in the last measurement period that the server has rejected blocking requests due to insufficient count of free work items	Reqs/sec	If the number of blocking request rejects is high, you may need to adjust the MaxWorkItem or MinFreeWorkItems server parameters
Permission errors	The number of times opens on behalf of clients have failed with *STATUS_ACCESS_ DENIED* in the last measurement period	Number	Permission errors can occur if any client/user is randomly attempting to access files, looking for files that may not have been properly protected.
File access denied errors	The number of times accesses to files opened successfully were denied in the last measurement period	Number	This number indicates attempts to access files without proper access authorization.
Internal server errors	This value indicates the number of times an internal server error was detected in the last	Number	Unexpected errors usually indicate a problem with the server.

Measurement	Description	Measurement Unit	Interpretation
	measurement period.		
Data received	The rate at which the server has received data from the network	Kbytes/sec	This metric indicates how busy the server is.
Data transmitted	The rate at which the server has sent data over the network	Kbytes/sec	This metric indicates how busy the server is.
Resource shortage errors	The number of times *STATUS_DATA_NOT_ ACCEPTED* was returned to clients in the last measurement period	Number	A resource shortage event occurs when no work item is available or can be allocated to service the incoming request. If many repeated resource shortage events occur, the InitWorkItems or MaxWorkItems server parameters might need to be adjusted.
Avg response time	Average time taken by the server to respond to client requests	Secs	This is a critical measure of server health.

3.2.6 Windows Sessions Test

This test reports various session-related statistics for an AD server.

Target of the test : An Active Directory server or a Windows Domain Controller

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory server or a Windows Domain Controller that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The host for which this test is to be configured.
Port	Refers to the port used by the Windows server.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Logons	Rate of logons to the server	Reqs/sec	This measure reports the rate of all interactive, network, and service logons to a windows server. The measure includes both successful and failed logons.
Logon errors	Number of logons in the last measurement period that had errors	Number	This measure reports the number of failed logon attempts to the server during the last measurement period. The number of failures can indicate whether password-guessing programs are being used to get into the server.
Current sessions	The number of sessions currently active in a server	Number	This measure is one of the indicators of current server activity.
Sessions with errors	The number of sessions in the last measurement period that were closed to unexpected error conditions	Number	Sessions can be closed with errors if the session duration reaches the autodisconnect timeout.
Sessions forced off	The number of sessions in the last measurement period that have been forced to logoff	Number	This value indicates how many sessions were forced to logoff due to logon time constraints.
Sessions logged off	The number of sessions in the last measurement period that were terminated normally	Number	Compare the number of sessions logged off to the number of sessions forced off, sessions with errors, or those that timed out. Typically, the percentage of abnormally terminated sessions should be low.
Sessions timed out	The number of sessions that have been closed in the last measurement period due to their idle time exceeding the AutoDisconnect parameter for the server	Number	The number of session timed out gives an indication of whether the AutoDisconnect setting is helping to conserve server resources

3.2.7 FSMO Roles Test

FSMO stands for Flexible Single Master Operations, and FSMO roles (also known as operations master roles) help you prevent conflicts in your Active Directory.

For most Active Directory objects, the task of updating can be performed by any Domain Controller except those Domain Controllers that are read-only. Updates such as computer object properties, renamed organizational units, and user account password resets can be handled by any writable domain controller.

After an object is changed on one domain controller, those changes are propagated to the other domain controllers through replication. During replication all of the Domain Controllers share their updates. So a user that has their password reset in one part of the domain may have to wait until those changes are replicated to the Domain Controller that they are signing in from.

This model works very well for most objects. In the case of any conflicts, such as a user's password being reset by both the central helpdesk as well as an administrator working at the user's site, then conflicts are resolved by whichever made the last change. However, there are some changes that are too important, and are not well suited to this model.

There are 5 specific types of updates to Active Directory that are very specific, and conflicts should be avoided. To help alleviate any potential conflicts, those updates are all performed on a single Domain Controller. And though each type of update must be performed on a single Domain Controller, they do not all have to be handled by the same Domain Controller.

These types of updates are handled by Domain Controllers Flexible Single Master Operations roles, or FSMO roles. Each of the five roles is assigned to only one domain controller.

There are five FSMO roles in every Active Directory forest. They are:

- Schema Master
- Domain Naming Master
- Infrastructure Master
- Relative ID (RID) Master
- Primary Domain Controller (PDC) Emulator

Among these five FSMO roles, the following three FSMO roles are needed only once in every domain in the forest:

- Infrastructure Master
- Relative ID (RID) Master
- Primary Domain Controller (PDC) Emulator

If a domain controller configured with a specific FSMO role is suddenly rendered unavailable or is unreachable, then that particular function cannot be performed. This in turn implies that the types of updates that will otherwise be handled by that domain controller can no longer be processed, thus creating a climate of conflict in the AD environment. With the held of the **FSMO Roles** test however, you can rapidly detect the unavailability of an FSMO domain controller over the network, isolate potential network connectivity issues and latencies, and spot real/probable delays in LDAP binding, so that such issues can be promptly remedied and conflicts prevented.

Target of the test : An Active Directory server or a Windows Domain Controller

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each FSMO role

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The host for which this test is to be configured.
Port	Refers to the port used by the Windows server.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
LDAP bind time	Indicates the time taken for the last successful LDAP bind.	Secs	In Active Directory Domain Services, the act of associating a programmatic object with a specific Active Directory Domain Services object is known as binding. When a programmatic object, such as an IADs (Interface Adapter Device) or DirectoryEntry object, is associated with a specific directory object, the programmatic object is considered to be bound to the directory

Measurement	Description	Measurement Unit	Interpretation
			object. The method for programmatically binding to an Active Directory object will depend on the programming technology that is used. All bind functions and methods require a binding string. The form of the binding string depends on the provider. Active Directory Domain Services are supported by two providers, LDAP and WinNT. Beginning with Windows 2000, the LDAP provider is used to access Active Directory Domain Services. The LDAP binding string can take one of the following forms: *“LDAP://<host name>/<object name>” “GC://<host name>/<object name>”* Ideally, the value of this measure should be low. A high value for this measure could be a possible indication of network-related problems or of the hardware that needs to be upgraded immediately. This measure will not be reported if the value of the Availability measure is 0.
Avg network delay	Indicates the average delay between transmission of packet to a target and receipt of the response to the packet at the source.	Secs	An increase in network latency could result from misconfiguration of the router(s) along the path, network congestion, retransmissions at the network, etc. The detailed diagnosis capability, if enabled, lists the hop-by-hop connectivity and delay. This measure will not be reported if the value of the Availability measure is 0.

Measurement	Description	Measurement Unit	Interpretation
Minimum network delay	Indicates the minimum time between transmission of a packet and receipt of the response back.	Secs	A significant increase in the minimum round-trip time is often a sure sign of network congestion. This measure will not be reported if the value of the Availability measure is 0.
Packet loss	Indicates the percentage of packets lost during transmission from source to target and back.	Percent	Packet loss is often caused by network buffer overflows at a network router or by packet corruptions over the network. The detailed diagnosis for this measure provides a listing of routers that are on the path from the external agent to target server, and the delays on each hop. This information can be used to diagnose the hop(s) that could be causing excessive packet loss/delays. This measure will not be reported if the value of the Availability measure is 0.
Availability	Indicates whether/not this FSMO role is available over the network.	Percent	A value of 100 indicates that the FSMO role is available. The value 0 indicates that the FSMO role is not available. Typically, the value 100 corresponds to a Pkt_loss_pct of 0. If the FSMO role is not available over the network i.e., if this measure reports a value 0, all other measures applicable for this test will not be reported.

3.2.8 Directory System Agent Logs Test

This test monitors the Active Directory database files and log files for file size, and also monitors free disk space on the hosting volumes.

Target of the test : An Active Directory server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory server that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The host for which this test is to be configured.
Port	Refers to the port used by the Windows server.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Directory system agent DB size	Indicates the size of the database files on the AD server.	MB	
System volume size	Indicates the size of the *SYSVOL* folder - *SYSVOL* is the shared directory on domain controllers that contains Group Policy and logon script information.	MB	
Directory system agent log file size	Indicates the size of the log files on the AD server.	MB	
Directory system agent free log space	Indicates the amount of free space on the volume hosting log files.	MB	Ideally, this value should be high.
Directory system agent free DB space	Indicates the amount of free space on the volume hosting database files.	MB	Ideally, this value should be high. If the free space for database files is very low, then the AD server might be rendered unable to update objects.
System volume share availability	Indicates whether the *SYSVOL* folder is available or not.	Percent	If the value of this measure is 100, it indicates the SYSVOL folder is available. The value 0 on the other hand, indicates that the folder is not available.

3.2.9 Domain Controller Summary

Use this test to know the number and names of all domain controllers that manage the servers and users in the domains of interest to you.

Note:

This test runs only on Active Directory servers operating on Windows 2008.

Target of the test : An Active Directory server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every domain name configured against DNS Name

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The host for which this test is to be configured.
Port	Refers to the port used by the Active Directory server.
DNS Name	Provide a comma-separated list of the fully qualified domain names of all the domains that you want the test to scan for domain controllers. For instance, your specification can be, *chn.eginnovations.com,mas.eginnovations.com*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Domain Controllers	Indicates the number of domain controllers in this domain.	Number	The detailed diagnosis of this measure lists the names of all domain controllers in a chosen domain.

3.2.10 Security Accounts Manager Test

Every Windows computer has a local Security Accounts Manager (SAM). The SAM is responsible for a few functions. First, it is responsible for storing the local users and groups for that computer. Second, the local SAM is responsible for authenticating logons. When a computer is not joined to a domain, the only option is to use the local SAM to perform the authentication.

If too many computer/user creations in SAM fail or if SAM takes too long to enumerate, evaluate, and authenticate users/user groups, the user experience with the computer is bound to be impacted adversely. By periodically monitoring the operations of SAM, administrators can proactively detect potential problem conditions and plug the holes, so that the user experience remains unaffected. The **Security Accounts Manager** test does just that. At configured intervals, this test checks how well SAM performs its core functions, and promptly reports real/probable failures and latencies to the administrator.

Note:

This test applies only to Active Directory Servers installed on Windows 2008 and above.

Target of the test : An Active Directory server or a Windows Domain Controller

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory server that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Machine creation attempts	Indicates the number of attempts per second to create computer accounts.	Number	
User creation attempts	Indicates the number of attempts per second to create user accounts.	Number	
Successful user creations	Indicates the number of user accounts successfully created per	Number	Ideally, the value of this measure should be equal to the value of the User creation attempts measure. A

Measurement	Description	Measurement Unit	Interpretation
	second.		low value is a cause for concern, as it indicates that many user creation attempts are failing; the reasons for the same have to be ascertained and addressed soon.
Successful computer creations	Indicates the number of computers successfully created per second.	Number	Ideally, the value of this measure should be equal to the value of the Machine creation attempts measure. A low value is a cause for concern, as it indicates that many machine creation attempts are failing; the reasons for the same have to be ascertained and addressed soon.
GC evaluations	Indicates the number of SAM global catalog evaluations per second.	Number	
Enumerations	Indicates the number of net user, net group, and net local function enumerations per second.	Connections/Sec	
Display information queries	Indicates the number of queries per second to obtain display information.	Connections/Sec	
Account group evaluation latency	Indicates the time taken by SAM to evaluate an account group.	Secs	This indicates the mean latency of the last 100 account and universal group evaluations performed for authentication. A high value could indicate a bottleneck.
Resource group evaluation latency	Indicates the time taken by SAM to evaluate a resource group.	Secs	This indicates the mean latency of the last 100 resource group evaluations performed for authentication. A high value could indicate a bottleneck.

3.2.11 Trust Relation Test

Trusts are relationships that are established between domains or forests that enable users in one domain or forest to be authenticated by a domain controller in another domain or forest. Trusts allow users in one domain or forest to access resources in a different domain or forest.

This test automatically discovers the trust relationship that the configured domain shares with other domains, and brings to light problems (if any).

Note:

This test will not work on an Active Directory server running on Windows 2000.

Target of the test : An Active Directory server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory server that is being monitored

Configurable parameters for the test

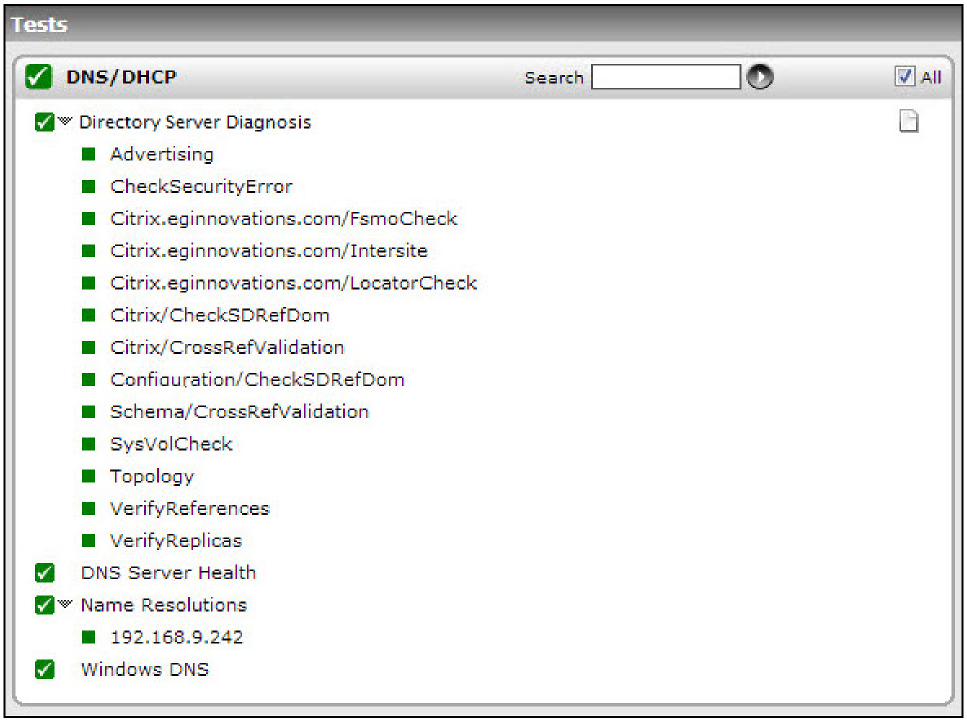
Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The host for which this test is to be configured.
Port	Refers to the port used by the Windows server.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Trust errors	Indicates the number of errors in the trust relationship between the configured domain and other domains.	Number	Ideally, this value should be 0. In the event of the occurrence of one/more errors, you can use the detailed diagnosis capability of this measure to view elaborate error descriptions, and accordingly investigate the problem further.

3.3 The DNS/DHCP Layer

The tests mapped to this layer perform periodic health checks on the DNS and DHCP services that AD relies on.



Tests

☑ DNS/DHCP Search ☑ All

- ☑ Directory Server Diagnosis
  - Advertising
  - CheckSecurityError
  - Citrix.eginnovations.com/FsmoCheck
  - Citrix.eginnovations.com/Intersite
  - Citrix.eginnovations.com/LocatorCheck
  - Citrix/CheckSDRefDom
  - Citrix/CrossRefValidation
  - Configuration/CheckSDRefDom
  - Schema/CrossRefValidation
  - SysVolCheck
  - Topology
  - VerifyReferences
  - VerifyReplicas
- ☑ DNS Server Health
- ☑ Name Resolutions
  - 192.168.9.242
- ☑ Windows DNS

Figure 3.3: The tests mapped to the DNS/DHCP layer

3.3.1 Directory Server Diagnostics Test

Domain controllers are the backbone of a Windows network. If your domain controllers are not working then the Active Directory does not work either. If the Active Directory does not work, then users cannot log on, group policies cannot be enforced, and a whole slew of other features become unavailable. To enable administrators to quickly detect and troubleshoot issues with the domain controller before they affect the operations of the AD server, Windows ships with a specialized tool called the *Domain Controller Diagnostic* (DCDIAG) Utility. dcdiag is a command- line tool that encapsulates detailed knowledge of how to identify abnormal behavior in the system. The tool analyzes the state of one or all domain controllers in a forest and reports any problems to assist in troubleshooting. It consists of a framework for executing tests and a series of tests to verify different functional areas of the system - eg., replication errors, domain controller connectivity, permissions, proper roles, etc.

Using the **Directory Server Diagnostics** test, the eG Enterprise Suite leverages the dcdiag utility's ability to report on a wide variety of health parameters related to the domain controller. This ensures that even the smallest of aberrations in the performance of the domain controller is captured and promptly brought to the attention of the administrators. The **Directory Server Diagnostics** test executes the DCDIAG command at configured intervals, and based on the output of the command, discovers the *DCDIAG* health checks that were performed, and the current status of each check - whether it reported a success or an error. In case the check resulted in an error/failure, you can use the detailed diagnosis of the test to understand the reason for the same, so that troubleshooting is easier!

Note:

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

Target of the test : An Active Directory or Domain Controller on Windows 2003 or above

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every *DCDIAG* health check that was performed

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.

Parameters	Description
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.
Domain, Username, Password, and Confirm password	In order to execute the DCDIAG command, the eG agent has to be configured with a domain administrator's privileges. Therefore, specify the domain name and login credentials of the domain administrator in the Domain, Username and Password text boxes. Confirm the password you provide by retyping it in the confirm password text box.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Status</td><td>Indicates the status of this <i>DCDIAG</i> health check.</td><td></td><td>If the health check returns a positive result, the value of this measure will be Pass. If not, the value of this measure will be Fail. The numeric values that correspond to these measure values have been discussed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Pass</td><td>1</td></tr>
<tr><td>Fail</td><td>0</td></tr>
</table>
</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			Note: By default, the measure reports the **Measure Values** listed in the table above to indicate the status of a DCDIAG health check. However, in the graph of this measure, the same will be represented using the numeric equivalents only. If the measure reports the value Fail, you can use the detailed diagnosis of this measure to know the reason for the failure and the domain controller where the failure occurred. This eases the pain involved in troubleshooting problem conditions.

3.3.2 DNS Server Health Test

If the DNS component of the AD server is unable to provide domain name resolution services, then users may be denied access to their mission-critical servers managed by the AD server. Under such circumstances, you may want to quickly check what is stalling the operations of DNS, so that the source of the issue can be isolated and eliminated.

DCDIAG is a command-line tool that encapsulates detailed knowledge of how to identify abnormal behavior in the system. The tool analyzes the state of one or all domain controllers in a forest and reports any problems to assist in troubleshooting. It consists of a framework for executing tests and a series of tests to verify different functional areas of the system.

DCDIAG also performs seven DNS-centric health checks to report on the overall DNS health of the domain controllers. To know the current status of each of these seven health checks, use the **DNS Server Health** test. The periodic health reports provided by the DNS Server Health test will enable administrators to proactively isolate potential DNS- related issues with their domain controllers, determine the reason for these issues, and work towards preventing them.

Target of the test : An Active Directory or Domain Controller on Windows 2008

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.
Use DNSBasic	In some environments, when the DCDIAG command is executed on the domain controllers, if the **Forwarder** test failed due to the Forwarder not configured in the tartget environment or if the Forwarder is not working properly, then, this test may not report metrics. In such cases, set the Use DNSBasic flag to **Yes**. By default, this flag is set to **No**.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Authentication	This test is run by default and checks the following: • Are domain controllers registered in DNS? • Can they be pinged? • Do they have Lightweight		The values that this measure reports and their corresponding numeric values have been discussed in the table below:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td>Directory Access Protocol/Remote Procedure Call (LDAP/RPC)?
This measure reports the current status of the Authentication or Connectivity test.</td><td></td><td><table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Pass</td><td>1</td></tr><tr><td>Fail</td><td>0</td></tr><tr><td>Warning</td><td>2</td></tr></table>
<b>Note:</b>
By default, the measure reports the <b>Measure Value</b>s listed in the table above to indicate the status of a DCDIAG health check. However, in the graph of this measure, the same will be represented using the numeric equivalents only.
If the measure reports the value Fail or Warning, you can use the detailed diagnosis of this measure to know the reason for the failure/warning. This eases the pain involved in troubleshooting problem conditions.</td></tr>
<tr><td>Basic</td><td>The basic DNS test confirms the following:
a. Whether the DNS client, Netlogon, KDC, and DNS Server services are running and available on domain controllers tested by dcdiag
b. Whether the DNS servers on all adapters are reachable.
c. Whether A record of</td><td></td><td>The values that this measure reports and their corresponding numeric values have been discussed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Pass</td><td>1</td></tr><tr><td>Fail</td><td>0</td></tr><tr><td>Warning</td><td>2</td></tr></table>
<b>Note:</b>
By default, the measure reports the <b>Measure Value</b>s listed in the table above to indicate the status of a DCDIAG health check. However, in</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td>each domain controller is registered on at least one of the DNS servers configured on the client.
d. If a domain controller is running the DNS Server service, whether the Active Directory domain zone and SOA record for the Active Directory domain zone are present.
e. Whether the root (.) zone is present.

This measure reports the current status of the Basic test.</td><td></td><td>the graph of this measure, the same will be represented using the numeric equivalents only.

If the measure reports the value Fail or Warning, you can use the detailed diagnosis of this measure to know the reason for the failure/warning. This eases the pain involved in troubleshooting problem conditions.</td></tr>
<tr><td>Forwarders</td><td>The forwarder test determines whether recursion is enabled. If forwarders or root hints are configured, the forwarder test confirms that all forwarders or root hints on the DNS server are functioning, and also confirms that the _ldap._ tcp.<Forest root domain> DC Locator record is resolved.

This measure reports the current status of the</td><td></td><td>The values that this measure reports and their corresponding numeric values have been discussed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Pass</td><td>1</td></tr><tr><td>Fail</td><td>0</td></tr><tr><td>Warning</td><td>2</td></tr></table>
<b>Note:</b>

By default, the measure reports the <b>Measure Value</b>s listed in the table above to indicate the status of a</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td>Forwarder test.</td><td></td><td>DCDIAG health check. However, in the graph of this measure, the same will be represented using the numeric equivalents only.
If the measure reports the value Fail or Warning, you can use the detailed diagnosis of this measure to know the reason for the failure/warning. This eases the pain involved in troubleshooting problem conditions.</td></tr>
<tr><td>Delegations</td><td>The delegation test confirms that the delegated name server is a functioning DNS Server. The delegation test checks for broken delegations by ensuring that all NS records in the Active Directory domain zone in which the target domain controller resides have corresponding glue A records.
This measure reports the current status of the Delegation test.</td><td></td><td>The values that this measure reports and their corresponding numeric values have been discussed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Pass</td><td>1</td></tr>
<tr><td>Fail</td><td>0</td></tr>
<tr><td>Warning</td><td>2</td></tr>
</table>
<b>Note:</b>
By default, the measure reports the <b>Measure Value</b>s listed in the table above to indicate the status of a DCDIAG health check. However, in the graph of this measure, the same will be represented using the numeric equivalents only.
If the measure reports the value Fail or Warning, you can use the detailed diagnosis of this measure to know the reason for the failure/warning. This eases the pain involved in troubleshooting problem conditions.</td></tr>
<tr><td>Dynamic update</td><td>The dynamic update test</td><td></td><td>The values that this measure reports and their corresponding numeric</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td>confirms that the Active Directory domain zone is configured for secure dynamic update and performs registration of a test record (_dcdiag_test_ record).
This measure reports the current status of the Dynamic Update test.</td><td></td><td>values have been discussed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Pass</td><td>1</td></tr>
<tr><td>Fail</td><td>0</td></tr>
<tr><td>Warning</td><td>2</td></tr>
</table>
<b>Note:</b>
By default, the measure reports the <b>Measure Value</b>s listed in the table above to indicate the status of a DCDIAG health check. However, in the graph of this measure, the same will be represented using the numeric equivalents only.
If the measure reports the value Fail or Warning, you can use the detailed diagnosis of this measure to know the reason for the failure/warning. This eases the pain involved in troubleshooting problem conditions.</td></tr>
<tr><td>Record registration</td><td>The record registration test verifies the registration of all essential DC Locator records on all DNS Servers configured on each adapter of the domain controllers.
This measure reports the current status of the Record Registration test.</td><td></td><td>The values that this measure reports and their corresponding numeric values have been discussed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Pass</td><td>1</td></tr>
<tr><td>Fail</td><td>0</td></tr>
<tr><td>Warning</td><td>2</td></tr>
</table>
<b>Note:</b>
By default, the measure reports the</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><b>Measure Value</b>s listed in the table above to indicate the status of a DCDIAG health check. However, in the graph of this measure, the same will be represented using the numeric equivalents only.
If the measure reports the value Fail or Warning, you can use the detailed diagnosis of this measure to know the reason for the failure/warning. This eases the pain involved in troubleshooting problem conditions.</td></tr>
<tr><td>Resolve external name</td><td>The external name resolution test verifies basic resolution of external DNS from a given client, using a sample Internet name (www.microsoft.com), or user-provided Internet name.
This measure reports the current status of the External name resolution test.</td><td></td><td>The values that this measure reports and their corresponding numeric values have been discussed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Pass</td><td>1</td></tr><tr><td>Fail</td><td>0</td></tr><tr><td>Warning</td><td>2</td></tr></table>
<b>Note:</b>
By default, the measure reports the <b>Measure Value</b>s listed in the table above to indicate the status of a DCDIAG health check. However, in the graph of this measure, the same will be represented using the numeric equivalents only.
If the measure reports the value Fail or Warning, you can use the detailed diagnosis of this measure to know the reason for the failure/warning. This eases the pain involved in troubleshooting problem conditions.</td></tr>
</table>

3.3.3 Name Resolutions Test

Active Directory uses DNS as its domain controller location mechanism and leverages the namespace design of DNS in the design of Active Directory domain names. As a result, DNS is positioned within the discoverability and logical structure components of Active Directory technology components. If a user complaints of being unable to access an AD domain, then administrators should first check whether the DNS component of AD is available and is able to resolve the IP address of the domain to its corresponding domain name and vice-versa. This is where, the **Name Resolutions** test will be useful!

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

Target of the test : An Active Directory or Domain Controller on Windows 2008

Agent deploying the test : An external agent

Outputs of the test : One set of results per Target configured

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port on which the specified host is listening.
Targets	The IP address or host name to be resolved during the test. Multiple targets can be specified as a comma-separated list.
Recursive	DNS supports two types of queries. For a non-recursive query, DNS attempts to respond to the request based on its local cache only. For a recursive query, a DNS server may use other DNS servers to respond to a request. The Recursive flag can be used to determine the type of queries to be issued to DNS.
DNS Port	Specify the port at which the DNS server listens.

Measurements made by the test

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

3.3.4 Windows DNS Test

This test measures the workload and processing ability of the DNS component of the AD server.

Target of the test : An Active Directory or Domain Controller on Windows 2008

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The host for which the test is to be configured.
Port	Refers to the port used by the Windows server.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total queries	The rate of queries received by DNS.	Reqs/sec	Indicates the workload of the DNS component of the AD server.

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

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

3.4 The AD Replication Service Layer

The tests mapped to this layer report on the health of the AD replication service.

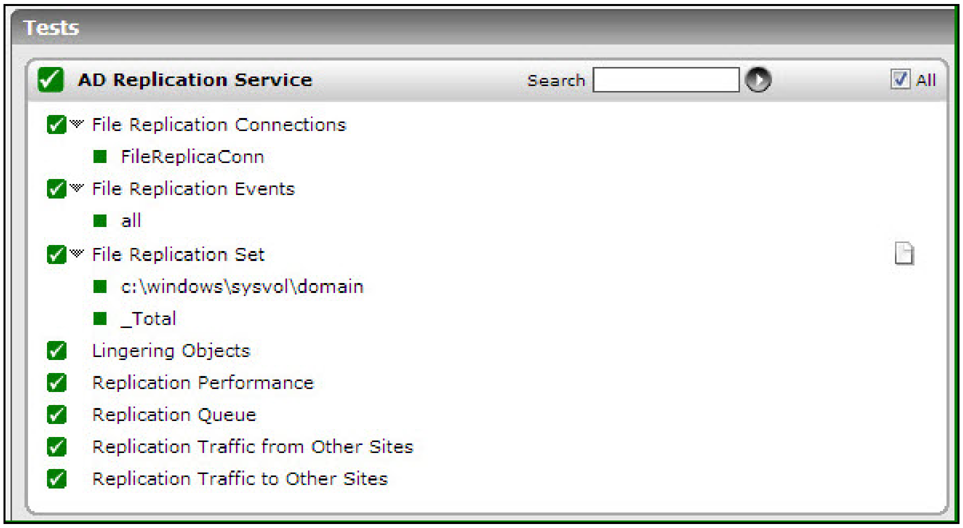


Figure 3.4: The tests mapped to the AD Replication Service layer

3.4.1 File Replication Connections Test

This test reports metrics related to the file replication connections to Distributed File System roots (DFS) in an Active Directory.

Target of the test : An Active Directory server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory server being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Authentications	Indicates the number of successful authentications that were performed.	Number	
Bindings	Indicates the number of successful RPC bindings that were completed.	Number	
Joins	Indicates the number of joins.	Number	After FRS discovers a connection from Active Directory, FRS establishes a connection session with the remote connection partner based on the information provided by the connection object. The connection is called "joined" when a connection session is successfully established.
Unjoins	Indicates the number of unjoins.	Number	
Local change orders sent	Indicates the number of local change orders that were sent.	Number	A change order is a message that contains information about a file or folder that has changed on a replica. A local change order is a change order that is created because of a change to a file or folder on the local server. The local server becomes the originator of the change order and constructs a staging file – this file is nothing but a

Measurement	Description	Measurement Unit	Interpretation
			backup of the changed file or folder.
Packets	Indicates the packets that were sent.	Number	
Remote change orders sent	Indicates the number of remote change orders that were sent.	Number	A remote change order refers to a change order received from an inbound (or upstream) partner that originated elsewhere in the replica set.
Remote change orders received	Indicates the number of remote change orders that were received.	Number	

3.4.2 File Replication Events Test

This test reports statistical information about the File Replication Service events recorded in the File Replication Service event log. This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick the Active Directory as the **Component type**, set *Performance* as the **Test type**, choose the test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the test : An Active Directory server

Agent deploying the test : An internal agent

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

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The host for which the test is to be configured.
Port	Refers to the port used by the EventLog Service. Here it is null.
Policy Based Filter	Using this page, administrators can configure the event sources, event IDs, and event descriptions to be monitored by this test. In order to enable administrators to easily and accurately provide this specification, this page provides the following options: • Manually specify the event sources, IDs, and descriptions in the Filter text area, or,

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

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

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

Measurements made by the test

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

Measurement	Description	Measurement Unit	Interpretation
			like loss of functionality or data. The detailed diagnosis capability, if enabled, lists the description of specific events. Please check the Application Logs in the Event Log Viewer for more details.
File replication information count	This refers to the number of File Replication Service information events generated when the test was last executed.	Number	A change in the value of this measure may indicate infrequent but successful operations performed by the File Replication Service. The detailed diagnosis capability, if enabled, lists the description of specific events.
File replication warnings	This refers to the number of warnings that were generated when the test was last executed.	Number	A high value of this measure indicates problems that may not have an immediate impact, but may cause future problems in the File Replication Service. The detailed diagnosis capability, if enabled, lists the description of specific events.
File replication critical errors	Indicates the number of critical events that were generated when the test was last executed.	Number	**This measure is applicable only for Windows 2008/Windows Vista/Windows 7 systems.** A high value of this measure indicates that too many events have occurred, which the File Replication Service cannot automatically recover from. The detailed diagnosis capability, if enabled, provides the description of specific events.
File replication verbose count	Indicates the number of verbose events that were generated when the test was last executed.	Number	**This measure is applicable only for Windows 2008/Windows Vista/Windows 7 systems.**

Measurement	Description	Measurement Unit	Interpretation
			Verbose logging provides more details in the log entry, which will enable you to troubleshoot issues better. The detailed diagnosis of this measure describes all the verbose events that were generated during the last measurement period.

3.4.3 File Replication Set Test

In the FRS, the replication of files and directories is according to a predefined topology and schedule on a specific folder. The topology and schedule are collectively called a replica set. A replica set contains a set of replicas, one for each machine that participates in replication.

This test reports statistics related to the health of the replication service provided by every replication set on an AD server.

Target of the test : An Active Directory server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every replication set on the Active Directory being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Change orders	Indicates the number of	Number	A change order is a message that

Measurement	Description	Measurement Unit	Interpretation
received	change orders that were currently received by this replica set.		contains information about a file or folder that has changed on a replica. These measures therefore serve as good indicators of the workload on the replica set.
Change orders sent	Indicates the number of change orders that were currently sent by this replica set by this replica set.	Number	
Files installed	Indicates the number of file installations.	Number	Installation is the process by which FRS applies a change order to the local file system to restore the file or folder as it is in the upstream partner. If the change order is for a deletion, the file or folder in the local file system is deleted (staging file is not needed). If the change order is for a renaming, the file or folder in the local file system is renamed (staging file is needed). If the change order is for a copying or creation, the file or folder is copied or created (staging file is needed). Installing a file or folder may fail if the file or folder is already opened by another process. If the installation failed, FRS retries installing the file or folder at a later time.
Packets received	Indicates the number of packets received currently.	Number	In an idle state, there should be no packets received unless a computer is having trouble joining with other computers in the replica set.
Packets sent	Indicates the number of packets sent currently.	Number	
USN records accepted	Indicates the number of USN records that were currently accepted.	Number	Active Directory replication does not primarily depend on time to determine what changes need to be propagated. Instead it uses update sequence numbers (USNs) that are assigned by

Measurement	Description	Measurement Unit	Interpretation
			a counter that is local to each domain controller. Because these USN counters are local, it is easy to ensure that they are reliable and never run backward (that is, they cannot decrease in value). Domain controllers use USNs to simplify recovery after a failure. When a domain controller is restored following a failure, it queries its replication partners for changes with USNs greater than the USN of the last change it received from each partner.
Staging space free	Indicates the staging space that is currently free.	KB	The Staging Directory is an area where modified files are stored temporarily either before being propagated to other replication partners or after being received from other replication partners. FRS encapsulates the data and attributes associated with a replicated file or directory object in a staging file. FRS needs adequate disk space for the staging area on both upstream and downstream machines in order to replicate files. Typically, if the Staging space free measure reports the value 0, or is found to be dangerously close to 0, it indicates that the staging directory is full. If the staging area is full, the FRS will stop functioning, and will resume only if disk space for the staging area becomes available or if the disk space limit for the staging area is increased. The staging area could get filled up owing to the following reasons: One or more downstream partners are

Measurement	Description	Measurement Unit	Interpretation
			not accepting changes. This could be a temporary condition due to the schedule being turned off and FRS waiting for it to open, or a permanent state because the service is turned off, or the downstream partner is in an error state. The rate of change in files exceeds the rate at which FRS can process them. A parent directory for files that have a large number of changes is failing to replicate, and so, all changes to subdirectories are blocked.
Staging space in use	Indicates the staging space that is currently in use.	KB	

3.4.4 Replication Performance Test

Replication is the process by which the changes that are made on one domain controller are synchronized with all other domain controllers in the domain that store copies of the same information or replica.

Monitoring the replication operations on an AD server will shed light on the load generated by such operations and helps measure the ability of the AD server to process this load. The **Replication Performance** test does just that. In the process, the test points you to replication-related activities that could be contributing to processing delays (if any) and why. In addition, the test also promptly reports replication errors such as synchronization failures, and compels administrators to do what is necessary to ensure that no non-sync exists in the data that is replicated across the domain controllers in a forest.

Note:

This test applies only to Active Directory Servers installed on Windows 2008 or above.

Target of the test : An Active Directory or Domain Controller on Windows 2008 or above

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory server that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
DRA inbound full sync objects remaining	Indicates the number of object updates received in the current directory replication update packet that have not yet been applied to the local server..	Number	
DRA inbound object updates remaining	Indicates the number of object updates received in the current directory replication update packet that have not yet been applied to the local server.	Number	The value of this measure should be low, with a higher value indicating that the hardware is incapable of adequately servicing replication (warranting a server upgrade).
Pending replication operations	Indicates the total number of replication operations on the directory that are queued for this server but not yet performed.	Number	A steady increase in the value of this measure could indicate a processing bottleneck.
Pending replication synchronizations	Indicates the number of directory synchronizations that are queued for this server but not yet processed.	Number	An unusually high value for a long duration may signify that the replication process is not being carried out at the desired rate. Forcing the replication activity may solve this problem.
Sync failures on schema mismatch	Indicates the number of synchronization requests made to neighbours that	Number	Ideally, the value of this measure should be 0.

Measurement	Description	Measurement Unit	Interpretation
	failed because their schema are not synchronized.		
Sync requests made	Indicates the number of synchronization requests made to neighbors.	Number	
Sync requests successful	Indicates the number of synchronization requests made to neighbors that were successfully returned.	Number	Ideally, the value of the Sync requests made measure should be equal to the value of the Sync requests successful measure - meaning, all sync request made should be successful, as one/more sync failures are a cause for concern.
DRA inbound objects applied rate	Indicates the rate at which replication updates received from replication partners are applied by the local directory service. This counter excludes changes that are received but not applied (because, for example, the change has already been made). This indicates how much replication update activity is occurring on the server as a result of changes generated on other servers.	AppId/Sec	A low value may indicate one of the following • less changes to the objects in the other domains • this domain controller is not applying the changes to the objects at the desired rate. If the object changes are not applied at the desired rate, it may result in a loss of data integrity in the Active Directory. Forcing the replication activity may solve this problem.
DRA inbound properties applied rate	Indicates the number of properties that are updated due to the incoming property's winning the reconciliation logic that determines the final value to be replicated.	AppId/Sec	A low value may indicate one of the following less changes to the object properties in the other domains this domain controller is not applying the change to the object properties at the desired rate. If the object properties are not applied

Measurement	Description	Measurement Unit	Interpretation
			at the desired rate, it may result in a loss of data integrity in the Active Directory. Forcing the replication activity may solve this problem.
DRA inbound objects filtered rate	Indicates the number of objects received from inbound replication partners that contained no updates that needed to be applied.	Filtrd/Sec	A high value for this measure indicates that the objects are all static. This problem can be solved by increasing the replication frequency.
DRA inbound properties filtered rate	Indicates the number of property changes (per second) already seen that were received during the replication.	Filtrd/Sec	A high value for this measure indicates that the properties are all static. This problem can be solved by increasing the replication frequency in the replicated domain.
DRA inbound bytes total	Indicates the rate at which bytes were replicated in.	Total/Sec	This counter is the sum of the number of uncompressed bytes (never compressed) and the number of compressed bytes (after compression) per second.
DRA outbound properties	Indicates the number of properties sent per second.	Properties/Sec	This counter tells you whether a source server is returning objects or not. Sometimes, the server might stop working correctly and not return objects quickly or at all.
DRA outbound objects filtered rate	Indicates the number of objects per second that were determined by outbound replication to have no updates that the outbound partner did not already have.	Filtrd/Sec	A high value for this measure indicates that the objects are all static. This problem can be solved by increasing the replication frequency in the target domain.
DRA outbound bytes total	Indicates the rate at which bytes were replicated out.	Total/Sec	This counter is the sum of the number of uncompressed bytes (never compressed) per second and the number of compressed bytes (after compression) per second.

3.4.5 Active Directory DFS Replication Backlog Test

DFS Replication is an efficient, multiple-master replication engine that you can use to keep folders synchronized between servers across limited bandwidth network connections.

To use DFS Replication, you must create replication groups and add replicated folders to the groups. Replication groups, replicated folders, and members are illustrated in the following figure.

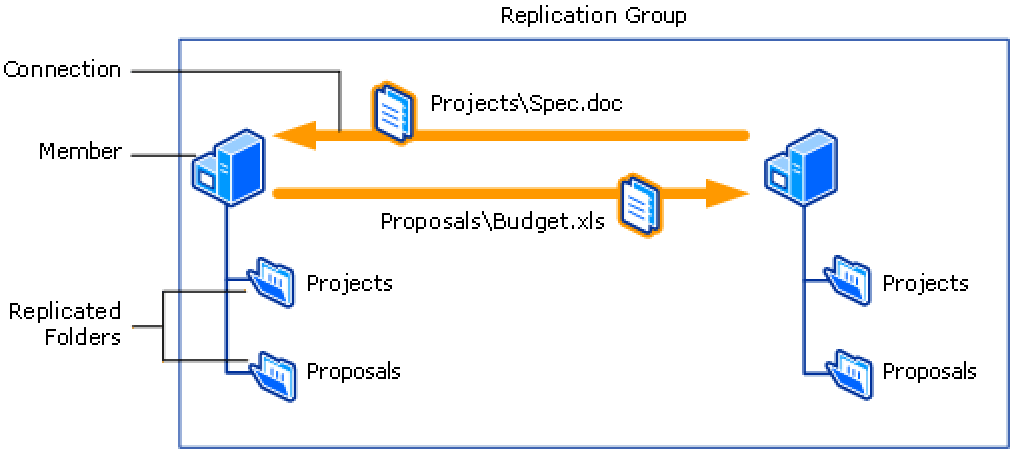


Figure 3.5: How does replication work?

A replication group is a set of servers, known as members , which participates in the replication of one or more replicated folders. A replicated folder is a folder that stays synchronized on each member.

The Replicated folders should be in sync at all times to ward off any data loss that may occur in the event of a disaster! This is why, it is imperative that administrators keep an eye on the replication process and make sure that there is no replication backlog - i.e., pending file updates between the replication folders - at any given point in time. The Active Directory DFS Replication Backlog test eases the pain of administrators in this regard!

This test automatically discovers the replication groups configured on a target AD server and the replication folders within each group. For every replication folder, the test then reports the number of pending file updates. This way, the test proactively alerts administrators to a sudden/steady rise in the count of backlogged updates, and thus points them to replication issues that need to be addressed immediately.

The test also supports a Summary descriptor. Check the metrics reported for the Summary descriptor to know the total number of replication groups, folders and servers participating in the replication, and the folders with backlogs. Detailed diagnostics reveal the names of the groups and folders.

Target of the test : An Active Directory or Domain Controller

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every replication folder in every replication group of the target Active Directory server

First level descriptor: Replication group

Second level descriptor: Replication folder

Metrics are also reported for a Summary descriptor

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying none against DD frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed

Parameters	Description
	diagnosis measures should not be 0.

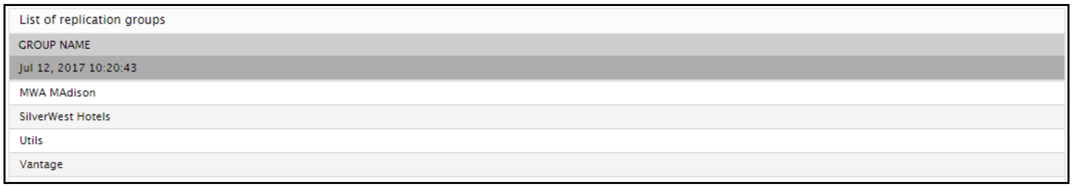
Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total backlogs	Indicates the total number of pending file updates for this replication folder.	Number	**This measure is not reported for the Summary descriptor.** A consistent rise in the value of this measure is a cause for concern, as it indicates that changes are not being replicated as far as they are being made. If the situation persists, then the replicated folders will stay out-of-sync, making complete data recovery impossible when disaster strikes. To avoid it, as soon as this measure starts exhibiting disturbing trends, administrators should quickly figure out why replication is slow and fix the hole. Some of the common causes for a replication slowdown are: • Missing Windows network connectivity-related hot fixes • Missing DFSR Service's latest binary • Out-of-date network card and storage drivers • DFSR staging directory could be too small for the amount of data being modified • Bandwidth throttling or schedule windows could be

Measurement	Description	Measurement Unit	Interpretation
			too aggressive; • Large amounts of sharing violations • RDC could have been disabled over a WAN link • Incompatible anti- Virus software or other file system filter drivers • File Server Resource Manager (FSRM) could have been configured with quotas/screens that block replication; • Un-staged or improperly pre-staged data leading to slow initial replication You can use the detailed diagnosis of this measure to know which server the updates were sent from and which server received it. In the event of slowness in replication, the detailed diagnostics will reveal to you which two servers participated in the slow replication.
Replication groups	Indicates the number of replication groups configured on this AD server.	Number	**This measure is reported only for the Summary descriptor.** Use the detailed diagnosis of this measure to know the names of the replication groups.
Replication folders	Indicates the number of replication folders configured on this AD server.	Number	**This measure is reported only for the Summary descriptor.** Use the detailed diagnosis of this measure to know which are the

Measurement	Description	Measurement Unit	Interpretation
			replication folders.
Sending and receiving member servers	Indicates the total number of servers participating in the replication.	Number	**This measure is reported only for the Summary descriptor.** Use the detailed diagnosis of this measure to know which servers are participating in the replication.
Replication folders with backlog	Indicates the number of replication folders with backlogged updates.	Number	**This measure is reported only for the Summary descriptor.** Ideally, the value of this measure should be 0. If the measure reports a non-zero value, then use the detailed diagnosis of this measure to know which are the replication folders with backlogged updates.

The detailed diagnosis of the Replication groups measure lists the replication groups configured on the monitored AD server.

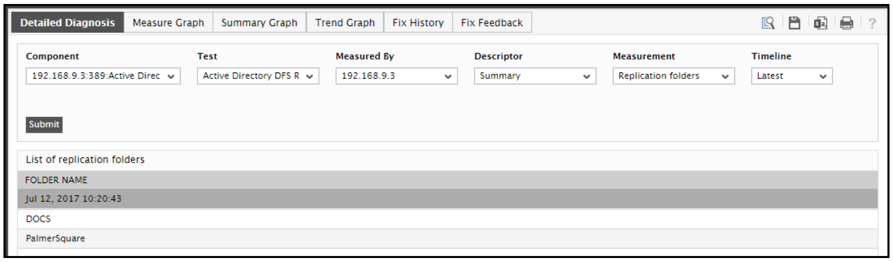


List of replication groups

GROUP NAME
Jul 12, 2017 10:20:43
MWA MAdison
SilverWest Hotels
Utils
Vantage

Figure 3.6: Detailed diagnosis of the Replication groups measure

The detailed diagnosis of the Replication folders measure lists all the replication folders on the member servers.



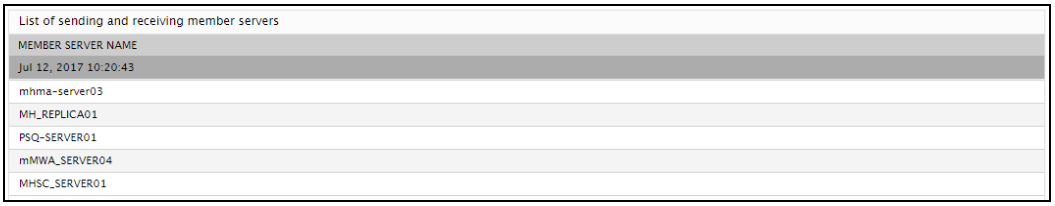
Component: 192.168.9.3:389:Active Direc
Test: Active Directory DFS R
Measured By: 192.168.9.3
Descriptor: Summary
Measurement: Replication folders
Timeline: Latest

List of replication folders

FOLDER NAME
Jul 12, 2017 10:20:43
DOCS
PalmerSquare

Figure 3.7: The detailed diagnosis of the Replication folders measure

The detailed diagnosis of the Sending and receiving member servers measure lists the servers that are participating in the replication.

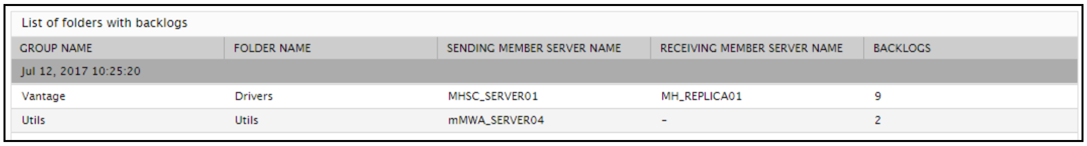


List of sending and receiving member servers

MEMBER SERVER NAME
Jul 12, 2017 10:20:43
mhma-server03
MH_REPLICA01
PSQ-SERVER01
mMWA_SERVER04
MHSC_SERVER01

Figure 3.8: Detailed diagnosis of the Sending and receiving member servers measure

To know which replication folders on which member servers had backlogged updates, use the detailed diagnosis of the Replication folders with backlog measure. The sending and receiving member servers, the replication folder on those servers, and the count of backlogged updates on that folder are displayed as part of detailed diagnostics.

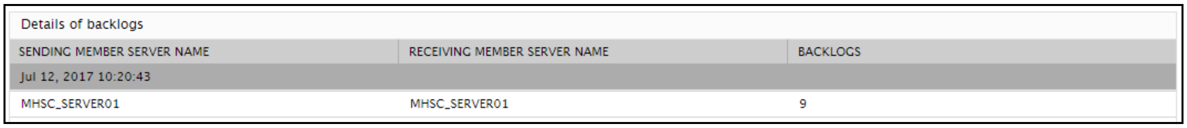


List of folders with backlogs

GROUP NAME	FOLDER NAME	SENDING MEMBER SERVER NAME	RECEIVING MEMBER SERVER NAME	BACKLOGS
Jul 12, 2017 10:25:20				
Vantage	Drivers	MHSC_SERVER01	MH_REPLICA01	9
Utils	Utils	mMWA_SERVER04	-	2

Figure 3.9: Detailed diagnosis of the Replication folders with backlogs measure

With the help of the detailed diagnosis of the Total replication backlogs measure, you can quickly identify the member servers on which the backlogs were detected, and which of these servers are the receiving and sending servers of the replication. This eases troubleshooting, as it reveals between which two servers replication was slow.



Details of backlogs

SENDING MEMBER SERVER NAME	RECEIVING MEMBER SERVER NAME	BACKLOGS
Jul 12, 2017 10:20:43		
MHSC_SERVER01	MHSC_SERVER01	9

Figure 3.10: Detailed diagnosis of the Total replication backlogs measures

3.4.6 Replication Traffic from Other Sites Test

Used in the Active Directory to express proximity of network connection, a site is defined as an IP subnetwork. A site consists of one or more subnets (unique network segments). Client machines use site information to find nearby DCs for logon operations. The Active Directory uses site information to help users find the closest machine that offers a needed network or a third-party service.

The Active Directory provides two methods of replication within the Active Directory environment: intrasite replication and intersite replication. Intrasite replication is replication within an Active Directory site. It is based assumption that the IP subnets within a site are well connected and that bandwidth is considered freely available and inexpensive. Because of this assumption, data is sent without compression.

Inter-site replication is replication between Active Directory sites. It is based on the assumption that the WAN is connected by slower links, so it is designed to minimize traffic rather than CPU cycles. Before being sent out, data is compressed to about 10% to 15% of original volume.

By monitoring the replication data flowing into each site, the Replication Traffic from Other Sites test helps determine the nature of the inbound traffic handled by every site - whether inter-site or intrasite, and reveals what type of inbound traffic is high on a site. Using this information, administrators can determine whether or not the replication data has been compressed enough to optimize bandwidth usage, and accordingly decide if more data compression is required at the source.

Note:

This test applies only to Active Directory Servers installed on Windows 2008 or above.

Target of the test : An Active Directory or Domain Controller on Windows 2008 or above

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
DRA inbound before bytes compression	Indicates the original size of inbound compressed replication data (kilobytes per second before compression, from DSAs	KB/Sec	

Measurement	Description	Measurement Unit	Interpretation
	in other sites).		
DRA inbound after bytes compression	Indicates the compressed size of inbound replication data (kilobytes per second received after compression, before DSAs in other sites).	KB/Sec	To save bandwidth on the network connection, the bridgehead servers in each site compress the traffic at the expense of additional CPU usage. A high value for this measure indicates that the bridgehead server is receiving high inter-site inbound replication traffic. Replication traffic is compressed down to about 40 percent when replication traffic is more than 32 KB in size.
DRA inbound bytes not compression	Indicates the number of incoming bytes replicated per second that were not compressed at the source (that is, from DSAs in the same site).	KB/Sec	A high value for this measure indicates that the intra-site replication traffic is high. Compressing the replication data adds an additional load on the domain controller server. Uncompressed replication traffic preserves server performance at the expense of network utilization.

3.4.7 Replication Traffic to Other Sites Test

Used in the Active Directory to express proximity of network connection, a site is defined as an IP subnetwork. A site consists of one or more subnets (unique network segments). Client machines use site information to find nearby DCs for logon operations. The Active Directory uses site information to help users find the closest machine that offers a needed network or a third-party service.

The Active Directory provides two methods of replication within the Active Directory environment: intrasite replication and intersite replication. Intrasite replication is replication within an Active Directory site. It is based assumption that the IP subnets within a site are well connected and that bandwidth is considered freely available and inexpensive. Because of this assumption, data is sent without compression.

Inter-site replication is replication between Active Directory sites. It is based on the assumption that the WAN is connected by slower links, so it is designed to minimize traffic rather than CPU cycles. Before being sent out, data is compressed to about 10% to 15% of original volume.

By monitoring the replication data flowing from each site, the Replication Traffic to Other Sites test helps determine the nature of the outbound traffic handled by every site - whether inter- site or intrasite, and reveals what type of outbound traffic is high on a site. Using this information, administrators can determine whether or not the replication data has been compressed enough to optimize bandwidth usage, and accordingly decide if more data is to be compressed by the bridgehead server on each site.

Note:

This test applies only to Active Directory Servers installed on Windows 2008 or above.

Target of the test : An Active Directory or Domain Controller on Windows 2008 or above

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
DRA outbound before bytes compression	Indicates the original size of outbound compressed replication data (kilobytes per second before compression, to DSAs in other sites).	KB/Sec	
DRA outbound after bytes compression	Indicates the compressed	KB/Sec	To save bandwidth on the network

Measurement	Description	Measurement Unit	Interpretation
	size of outbound replication data (kilobytes per second sent after compression to DSAs in other sites).		connection, the bridgehead servers in each site compress the traffic at the expense of additional CPU usage. A high value for this measure indicates that the bridgehead server is sending large high inter-site inbound replication traffic. Replication traffic is compressed down to about 40 percent when replication traffic is more than 32 KB in size.
DRA outbound bytes not compression	Indicates the number of outgoing bytes replicated per second that were not compressed at the source (that is, to DSAs in the same site).	KB/Sec	A high value for this measure indicates that the intra-site replication traffic is high. Compressing the replication data adds an additional load on the domain controller server. Uncompressed replication traffic preserves server performance at the expense of network utilization.

3.4.8 Replication Queue Test

As the domain controller formulates change requests, either by a schedule being reached or from a notification, it adds a work item for each request to the end of the queue of pending synchronization requests. Each pending synchronization request represents one <source domain controller, directory partition> pair, such as “synchronize the schema directory partition from DC1,” or “delete the ApplicationX directory partition.”

When a work item has been received into the queue, the domain controller processes the item (begins synchronizing from that source) as soon as the item reaches the front of the queue, and continues until either the destination is fully synchronized with the source domain controller, an error occurs, or the synchronization is pre-empted by a higher-priority operation.

A long replication queue is often an indication that synchronization requests are not swiftly processed by the AD server. If the reasons for the abnormal queue length are not determined quickly and addressed promptly, replication of some changes may be stalled indefinitely causing the source and destination domain controllers to remain ‘out-of-sync’ for long durations; this in turn may result in users having to work with obsolete data! To prevent such an eventuality, you can use this test to continuously track the replication queue length, so that you can be alerted as soon as the number of work items in the queue crosses an acceptable limit. You can also use the detailed diagnostics of this test to know what type of synchronization requests are in queue, so that you can figure out why the requests are taking too long to be processed.

Target of the test : An Active Directory or Domain Controller

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Replication queue size	Indicates the number of synchronization requests	Number	A high value for this measure is a cause for concern, as it indicates that

Measurement	Description	Measurement Unit	Interpretation
	that are currently in the replication queue, awaiting processing.		too many synchronization requests are pending processing. This could be due to a severe processing bottleneck on the AD server. Very short replication schedules and large synchronization requests that require a lot of processing time are also factors that can increase the replication queue length. You can use the detailed diagnosis of this measure to know which requests are yet to be processed, so that you can figure out why there is a delay (if any) in processing.

3.4.9 Lingering Objects Test

When restoring a backup file, Active Directory generally requires that the backup file be no more than 180 days old. If you attempt to restore a backup that has expired, you may encounter problems due to “lingering objects”.

A lingering object is a deleted AD object that re-appears (“lingers”) on the restored domain controller (DC) in its local copy of Active Directory. This can happen if, after the backup was made, the object was deleted on another DC more than than 180 days ago.

When a DC deletes an object it replaces the object with a tombstone object. The tombstone object is a placeholder that represents the deleted object. When replication occurs, the tombstone object is transmitted to the other DCs, which causes them to delete the AD object as well.

Tombstone objects are kept for 180 days, after which they are garbage-collected and removed.

If a DC is restored from a backup that contains an object deleted elsewhere, the object will re-appear on the restored DC. Because the tombstone object on the other DCs has been removed, the restored DC will not receive the tombstone object (via replication), and so it will never be notified of the deletion. The deleted object will “linger” in the restored local copy of Active Directory.

Such lingering objects tend to create problems during replication. For instance, if the source domain controller has outdated objects that have been out of replication for more than one tombstone lifetime a failure event will be logged in the Windows event log at the time of replicating from the source. You will have to promptly capture such events, identify the lingering objects, and delete them to ensure that replication resumes. In order to achieve this, you can use the **Lingering Objects** test. This test scans the event logs for replication events related to lingering objects, and promptly alerts you upon the occurrence of such events. Using the detailed diagnosis of the test, you can easily determine the location of the lingering objects, so that you can immediately proceed to remove them. This way, the test ensures that the replication engine operates without a glitch.

Note:

This test works only on Active Directory servers that operate on Windows 2008 or above.

Target of the test : An Active Directory or Domain Controller on Windows 2008 or above

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory server that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Lingering messages	Indicates the number of messages that are currently logged in the event log, which contains references to lingering objects.	Number	This measure typically captures and reports the number of events with event IDs 1388 and 1988 in the event log. Event ID 1388 indicates that a destination domain controller that does not have strict replication consistency enabled received a request to update an object that does not reside in the local copy of the Active Directory database. In response, the destination domain controller requested the full object from the source replication partner. In this way, a lingering object was replicated to the destination domain controller. Therefore, the lingering object was reintroduced into the directory. Event ID 1988 indicates that a destination domain controller that has strict replication consistency enabled has received a request to update an object that does not exist in its local copy of the Active Directory database. In response, the destination domain controller blocked replication of the directory partition containing that object from that source domain controller. The detailed diagnosis of this test provides the complete description of the events with IDs 1388 and/or 1988 that are logged in the event log. The source domain controller and the lingering objects can be inferred from the event description. Using this information, you can run the repadmin command on the source domain controller to delete the lingering objects.

3.4.10 Replication Status Test

This test summarizes the replication state and relative health of an Active Directory forest by inventorying and contacting every domain controller in the forest, and collecting and reporting information such as replication deltas and replication failures. You can thus accurately identify the domain controllers that are prone to frequent failures.

Target of the test : An Active Directory or Domain Controller

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every domain controller in an Active Directory forest being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total replication links	Indicates the number of	Number	A replica link exists for each naming

Measurement	Description	Measurement Unit	Interpretation
	replica links for this domain controller.		context on a domain controller. This measure is the sum total of such replica links per domain controller. Please note that this is not the connection objects or replication partners per domain controller. You can use the detailed diagnosis of this measure to view the complete details of the replica links - this includes the source and destination sites, the source and destination domain controllers, the transport type, the number of link failures (if any), and details of the failures such as when the failure occurred and the failure status.
Replication links failure	Indicates the total number of replica links on this domain controller that are failing to replicate for one reason or the other. This will never be greater than the Total field.	Number	Ideally, the value of this measure should be 0.
Percent of replication links failure	Indicates the percentage of failures in relation to the total replica links on this domain controller.	Percent	A low value is desired for this measure. A value close to 100% is a cause for concern, as it indicates that almost all replica links are failing.
Longest replication gap	Denotes the longest replication gap amongst all replication links on this domain controller.	Secs	Ideally, this value should be less than 1 hour.

3.4.11 Inter-Site Replication Test

Inter-site replication is based on the assumption that the WAN is connected by slower links or site links. It is designed to minimize traffic rather than CPU cycles. In inter-site replication, data is compressed and then sent out.

Bridgehead servers perform directory replication between sites. Only two designated domain controllers talk to each other. These domain controllers are called “Bridgehead servers”.

After updates are replicated from one site to the bridgehead server in the other site, the updates are then replicated to other domain controllers within the site through intra-site replication process.

Note:

This test applies only to Active Directory Servers installed on Windows 2003.

Target of the test : An Active Directory or Domain Controller on Windows 2003

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory server being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
In rate	This measure indicates the number of inbound kilobytes replicated between sites per second.	KB/Sec	A high value for this measure indicates that the bridgehead server is receiving high inter-site inbound replication traffic.
Out rate	This measure indicates the number of outbound kilobytes replicated between sites per second.	KB/Sec	A high value indicates that bridgehead server is sending high inter-site outbound replication traffic.

3.4.12 Intra-Site Replication Test

Intra-site replication means replication happening between domain controllers in the same site. Intra-site replication attempts to complete in the fewest CPU cycles possible. Intra-site replication avoids unnecessary network traffic by introducing a change notification mechanism that replaces the usual polling of replication partners for updates. When a change is performed in its database, a domain controller waits for a configurable interval (default 5 minutes) and accepts more changes during this time. Then it sends a notification to its replication partners, which will pull the changes from the source. If no changes are performed for a configurable period (default 6 hours) the domain controller initiates a replication sequence anyway, just to make sure that it did not miss anything.

Note:

This test applies only to Active Directory Servers installed on Windows 2003.

Target of the test : An Active Directory or Domain Controller on Windows 2003

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory server being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
In rate	This measure indicates the number of inbound kilobytes replicated within the site per second.	KB/Sec	A high value for this measure indicates that the intra-site replication traffic is high.
Out rate	This measure indicates the number of outbound kilobytes replicated within the site per second.	KB/Sec	A high value for this measure indicates that the intra-site outbound replication traffic is high.

3.4.13 Replication Test

As the number of domain controllers increase, the replication process consumes more network bandwidth. So, replication process should be monitored within the target environment.

Note:

This test applies only to Active Directory Servers installed on Windows 2003.

Target of the test : An Active Directory or Domain Controller on Windows 2003

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory server being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
DRA inbound objects applied rate	This measure shows the number of replication updates applied per second that are occurring on this domain controller as a result of changes generated on other domain controllers.	ApplId/Sec	A low value may indicate one of the following a. less changes to the objects in the other domains b. this domain controller is not applying the changes to the objects at the desired rate. If the object changes are not applied at the desired rate, it may result in a loss of data integrity in the Active Directory.

Measurement	Description	Measurement Unit	Interpretation
			Forcing the replication activity may solve this problem.
DRA inbound properties applied rate	This measure indicates the number of changes applied to object properties per second through inbound replication as a result of reconciliation logic. This logic is used to determine the final value to be replicated to the property.	Appld/Sec	A low value may indicate one of the following a. less changes to the object properties in the other domains b. this domain controller is not applying the change to the object properties at the desired rate. If the object properties are not applied at the desired rate, it may result in a loss of data integrity in the Active Directory. Forcing the replication activity may solve this problem.
DRA inbound objects filtered rate	This measure indicates the number of inbound replication objects received per second from the replication partners that contained no updates that needed to be applied.	Filtrd/Sec	A high value for this measure indicates that the objects are all static. Increasing the replication frequency may solve this problem.
DRA inbound properties filtered rate	This measure indicates the number of inbound replication properties received per second from the replication partners that did not contain any updates to be applied.	Filtrd/Sec	A high value for this measure indicates that the properties are all static. Increasing the replication frequency in the replicated domain may solve this problem.
DRA outbound objects filtered rate	This measure indicates the number of outbound replication objects that have not yet been received by the outbound replication partner per second.	kerFiltrd/Sec	A high value for this measure indicates that the objects are all static. Increasing the replication frequency in the target domain may solve this

Measurement	Description	Measurement Unit	Interpretation
			problem.
Pending replication synchronizations	This measure indicates the number of directory synchronizations that are queued per second for this domain controller but not yet processed.	Number	An unusually high value for a long duration may signify that the replication process is not being carried out at the desired rate. Forcing the replication activity may solve this problem.

3.4.14 AD Replications Test

Replication is the process by which the changes that are made on one domain controller are synchronized with all other domain controllers in the domain that store copies of the same information or replica. Given the various types of information that Active Directory can store, changes to Active Directory can swiftly accumulate across multiple domain controllers in a large organization. It is therefore necessary for Windows to frequently synchronize the domain controllers through the replication process. If replication fails, it causes Active Directory objects that represent the replication topology, replication schedule, domain controllers, users, computers, passwords, security groups, group memberships, and Group Policy to be inconsistent between domain controllers. Directory inconsistency causes either operational failures or inconsistent results, depending on the domain controller that is contacted for the operation at hand.

To avoid such inconsistencies, its best to capture failures promptly, isolate the source of failures, and fix them, The **AD Replications** test aids in this regard. This test closely monitors the replication activities on the domain controller and promptly reports replication failures, so that administrators can investigate such failures, discover the reasons for the same, fix them, and restore normalcy.

Target of the test : An Active Directory or Domain Controller on Windows

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory server being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.

Parameters	Description
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Replication failures	Indicates the number of replication failures in the target domain controller.	Number	Ideally, the value of this measure should be low.
Total replications	Indicates the number of replication successes in the target domain controller.	Number	
Percent replication failures	Indicates the percentage of replication failures in the target domain controller.	Percent	Ideally, the value of this measure should be low. A high value is indicative of too many replication failures. Active Directory replication problems can have several different sources. For example, Domain Name System (DNS) problems, networking issues, or security problems can all cause Active Directory replication to fail. • Network connectivity: The network connection might be unavailable or network settings are not configured properly. • Name resolution: DNS misconfigurations are a common cause for replication failures. • Authentication and authorization: Authentication and authorization problems cause "Access denied"

Measurement	Description	Measurement Unit	Interpretation
			errors when a domain controller tries to connect to its replication partner. - Directory database (store): The directory database might not be able to process transactions fast enough to keep up with replication timeouts. - Replication engine: If intersite replication schedules are too short, replication queues might be too large to process in the time that is required by the outbound replication schedule. In this case, replication of some changes can be stalled indefinitely — potentially, long enough to exceed the tombstone lifetime. - Replication topology: Domain controllers must have intersite links in Active Directory that map to real wide area network (WAN) or virtual private network (VPN) connections. If you create objects in Active Directory for the replication topology that are not supported by the actual site topology of your network, replication that requires the misconfigured topology fails.

3.4.15 Distributed File System Events Test

If you are suspecting that the DFS replication between members is failing, then use the DFS Replication log to confirm your suspicions or to negate them. This event log records events for the Distributed File System Replication services, such as when the DFS replication service started, and also captures service failures (if any). This way, the DFS Replication log serves as a rich source of information that is most useful when troubleshooting issues related to replication. By monitoring this event log, the **Distributed File System Events** test promptly alerts administrators to current replication problems and even warns them of probable replication failures.

Target of the test : An Active Directory server

Agent deploying the test : An internal agent

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

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The host for which the test is to be configured.
Port	Refers to the port used by the EventLog Service. Here it is *null*.
Policy Based Filter	Using this page, administrators can configure the event sources, event IDs, and event descriptions to be monitored by this test. In order to enable administrators to easily and accurately provide this specification, this page provides the following options: • Manually specify the event sources, IDs, and descriptions in the Filter text area, or, • Select a specification from the predefined filter policies listed in the Filter box For explicit, manual specification of the filter conditions, select the **No** option against the Policy Based Filter field. This is the default selection. To choose from the list of pre-configured filter policies, or to create a new filter policy and then associate the same with the test, select the **Yes** option against this field.
Filter	If the Policy Based Filter flag is set to **No**, then a Filter text area will appear, wherein you will have to specify the event sources, event IDs, and event descriptions to be monitored. This specification should be of the following format: *{Displayname}:{event_sources_to_be_included}:{event_sources_to_be_excluded}:{event_IDs_to_be_included}:{event_IDs_to_be_excluded}:{event_descriptions_to_be_included}:{event_descriptions_to_be_excluded}*. For example, assume that

Parameters	Description
	the Filter text area takes the value, *OS_events:all:Browse,Print:all:none:all:none*. Here: • OS_events is the display name that will appear as a descriptor of the test in the monitor UI; • all indicates that all the event sources need to be considered while monitoring. To monitor specific event sources, provide the source names as a comma-separated list. To ensure that none of the event sources are monitored, specify *none*. • Next, to ensure that specific event sources are excluded from monitoring, provide a comma-separated list of source names. Accordingly, in our example, Browse and Print have been excluded from monitoring. Alternatively, you can use all to indicate that all the event sources have to be excluded from monitoring, or none to denote that none of the event sources need be excluded. • In the same manner, you can provide a comma-separated list of event IDs that require monitoring. The all in our example represents that all the event IDs need to be considered while monitoring. • Similarly, the none (following all in our example) is indicative of the fact that none of the event IDs need to be excluded from monitoring. On the other hand, if you want to instruct the eG Enterprise system to ignore a few event IDs during monitoring, then provide the IDs as a comma-separated list. Likewise, specifying all makes sure that all the event IDs are excluded from monitoring. • The all which follows implies that all events, regardless of description, need to be included for monitoring. To exclude all events, use none. On the other hand, if you provide a comma-separated list of event descriptions, then the events with the specified descriptions will alone be monitored. Event descriptions can be of any of the following forms - desc*, or desc, or *desc*,or desc*, or desc1*desc2, etc. desc here refers to any string that forms part of the description. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters. • In the same way, you can also provide a comma-separated list of event descriptions to be excluded from monitoring. Here again, the specification can be of any of the

Parameters	Description
	following forms: desc*, or desc, or *desc*,or desc*, or desc1*desc2, etc. desc here refers to any string that forms part of the description. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters. In our example however, none is specified, indicating that no event descriptions are to be excluded from monitoring. If you use all instead, it would mean that all event descriptions are to be excluded from monitoring. **Note:** The event sources and event IDs specified here should be exactly the same as that which appears in the Event Viewer window. On the other hand, if the Policy Based Filter flag is set to **Yes**, then a Filter list box will appear, displaying the filter policies that pre-exist in the eG Enterprise system. A filter policy typically comprises of a specific set of event sources, event IDs, and event descriptions to be monitored. This specification is built into the policy in the following format: *{Policyname}:{event_sources_to_be_included}:{event_sources_to_be_excluded}:{event_IDs_to_be_included}:{event_IDs_to_be_excluded}:{event_descriptions_to_be_included}:{event_descriptions_to_be_excluded}* To monitor a specific combination of event sources, event IDs, and event descriptions, you can choose the corresponding filter policy from the Filter list box. Multiple filter policies can be so selected. Alternatively, you can modify any of the existing policies to suit your needs, or create a new filter policy. To facilitate this, a **Click here** link appears just above the test configuration section, once the **Yes** option is chosen against Policy Based Filter. Clicking on the **Click here** link leads you to a page where you can modify the existing policies or create a new one. The changed policy or the new policy can then be associated with the test by selecting the policy name from the Filter list box in this page.
UseWMI	The eG agent can either use **WMI** to extract event log statistics or directly parse the event logs using event log APIs. If this flag is **Yes**, then **WMI** is used. If not, the event log APIs are used. This option is provided because on some Windows 2000 systems (especially ones with service pack 3 or lower), the use of WMI access to event logs can cause the CPU usage of the WinMgmt process to shoot up. On such systems, set this parameter value to **No**.
Stateless Alerts	Typically, the eG manager generates email alerts only when the state of a specific measurement changes. A state change typically occurs only when the threshold of a measure is violated a configured number of times within a specified time window.

Parameters	Description
	While this ensured that the eG manager raised alarms only when the problem was severe enough, in some cases, it may cause one/more problems to go unnoticed, just because they did not result in a state change. For example, take the case of the **EventLog** test. When this test captures an error event for the very first time, the eG manager will send out a critical email alert with the details of the error event to configured recipients. Now, the next time the test runs, if a different error event is captured, the eG manager will keep the state of the measure as critical, but will not send out the details of this error event to the user; thus, the second issue will remain hidden from the user. To make sure that administrators do not miss/overlook critical issues, the eG Enterprise monitoring solution provides the stateless alerting capability. To enable this capability for this test, set the stateless alerts flag to **Yes**. This will ensure that email alerts are generated for this test, regardless of whether or not the state of the measures reported by this test changes.
Events During Restart	By default, this flag is set to **Yes**. This ensures that whenever the agent is stopped and later started, the events that might have occurred during the period of non-availability of the agent are included in the number of events reported by the agent. Setting the flag to **No** ensures that the agent, when restarted, ignores the events that occurred during the time it was not available.
DDforInformation	eG Enterprise also provides you with options to restrict the amount of storage required for event log tests. Towards this end, the DDforInformation and DDforWarning flags have been made available in this page. By default, both these flags are set to **Yes**, indicating that by default, the test generates detailed diagnostic measures for information events and warning events. If you do not want the test to generate and store detailed measures for information events, set this flag to **No**.
DDforWarning	To ensure that the test does not generate and store detailed measures for warning events, set the DDforWarning flag to **No**.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option.

Parameters	Description
	The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

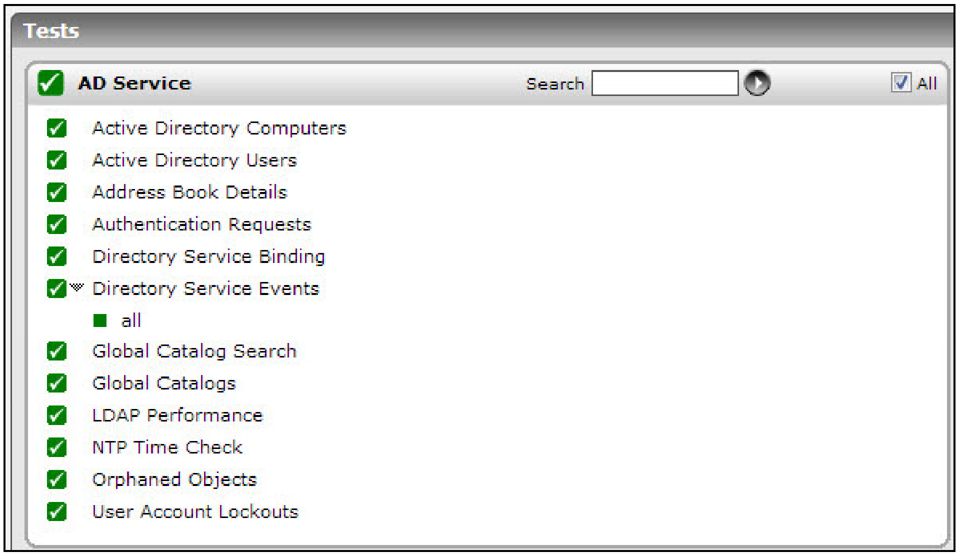
Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Distributed file system information messages	This refers to the number of information events that were captured by the DFS Replication log during the test's last execution.	Number	A change in value of this measure may indicate infrequent but successful replications. Please check the DFS Replication log in the Event Log Viewer for more details.
Distributed file system warnings	This refers to the number of warning events captured by the DFS Replication log during the test's last execution.	Number	A high value of this measure indicates problems that may not have an immediate impact, but may cause future problems. Please check the DFS Replication log in the Event Log Viewer for more details.
Distributed file system errors	This refers to the number of error events captured by the DFS Replication log during the test's last execution.	Number	A very low value (zero) is desired for this measure, as it indicates good health. An increasing trend or a high value indicates the existence of problems. Please check the DFS Replication log in the Event Log Viewer for more details.
Distributed file system critical errors	Indicates the number of critical events that were generated when the test was last executed.	Number	A critical event is one that the replication service cannot automatically recover from. This measure is applicable only for

Measurement	Description	Measurement Unit	Interpretation
			Windows 2008/Windows Vista/Windows 7 systems. A very low value (zero) indicates that the service is in a healthy state and is running smoothly without any potential problems. An increasing trend or high value indicates the existence of fatal/irrepairable problems. The detailed diagnosis of this measure describes all the critical events captured by the DFS Replication log during the last measurement period. Please check the DFS Replication log in the Event Log Viewer for more details.
Distributed file system verbose messages	Indicates the number of verbose events that were generated when the test was last executed.	Number	Verbose logging provides more details in the log entry, which will enable you to troubleshoot issues better. This measure is applicable only for Windows 2008/Windows Vista/Windows 7 systems. The detailed diagnosis of this measure describes all the verbose events that were captured by the DFS Replication log during the last measurement period. Please check the DFS Replication log in the Event Log Viewer for more details.

3.5 The AD Service Layer

This layer tracks the health of the Active Directory in a Windows environment using the ActiveDirectory test shown in Figure 3.11.



Tests

☑ AD Service   Search ☑ All

- ☑ Active Directory Computers
- ☑ Active Directory Users
- ☑ Address Book Details
- ☑ Authentication Requests
- ☑ Directory Service Binding
- ☑ Directory Service Events
  - 🟩 all
- ☑ Global Catalog Search
- ☑ Global Catalogs
- ☑ LDAP Performance
- ☑ NTP Time Check
- ☑ Orphaned Objects
- ☑ User Account Lockouts

Figure 3.11: Tests mapping to the DC Service layer

3.5.1 Orphaned Objects Test

On a domain controller, the Lost and Found container contains Active Directory objects that have been orphaned. An object is orphaned when the object is created on one domain controller and the container in which the object is placed is deleted from the directory on another domain controller before the object has a chance to replicate. An orphaned object is automatically placed in the Lost and Found container where it can be found by an administrator, who must determine whether to move or delete the object.

This test periodically reports the number of orphaned objects on a domain controller.

Target of the test : An Active Directory or Domain Controller

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

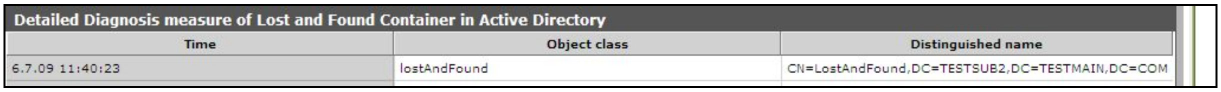
Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.

Parameters	Description
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Orphaned objects	Indicates the number of objects in the Lost and Found container.	Number	If the value of this measure is greater than 0, it indicates the existence of orphaned objects. In such a case, you can use the detailed diagnosis capability of this measure to view the complete details of the objects, and accordingly decide whether to move the object or delete it.

The detailed diagnosis of the *Orphaned objects* measure, if enabled, provides the complete details of the orphaned objects, which includes the named of the Object class and Distinguished name.



Detailed Diagnosis measure of Lost and Found Container in Active Directory

Time	Object class	Distinguished name
6.7.09 11:40:23	lostAndFound	CN=LostAndFound,DC=TESTSUB2,DC=TESTMAIN,DC=COM

Figure 3.12: The details of orphaned objects

3.5.2 Active Directory Status Test

This test tracks the performance of Active Directory existing in a Windows 2000 environment. Before getting into the details of this test, it is essential for the users to know that there are two choices for network authentication in a Windows 2000 environment. They are

- Kerberos Version 5.0: This protocol is the default network authentication protocol for Windows 2000 servers.
- Windows NT LAN Manager (NTLM): The NTLM protocol was the default network authentication protocol for Windows NT 4.0 operating system. NTLM is also used to authenticate logons to standalone computers with Windows 2000.

When a user first authenticates to Kerberos, he/she talks to the Authentication Service (AS) on the Kerberos Key Distribution Center (KDC) to get a Ticket Granting Ticket (TGT). This ticket is encrypted with the user's password. When the user wants to talk to a Kerberized service, he/she uses the Ticket Granting Ticket (TGT) to talk to the Ticket Granting Service (TGS), which also runs on the KDC. The Ticket Granting Service then verifies the user's identity using the TGT and issues a ticket for the desired service. The reason the Ticket Granting Ticket exists is that a user doesn't have to enter their password every time they wish to connect to a Kerberized service.

Target of the test : An Active Directory or Domain Controller

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Schema cache hit ratio	This measure shows the percentage of object name lookups available in the Schema Cache. This cache is present in the Domain Controller. All changes made to the	Percent	A low value of this measure indicates that the Directory Service needs high disk read/write activity to perform its job. This results in poor response time of the components available in the Active Directory.

Measurement	Description	Measurement Unit	Interpretation
	Active Directory are first validated against this schema cache.		
Notify queue size	When any change in the Active Directory occurs, the originating domain controller sends an update notification requests to the other domain controllers. This measure shows the number of pending update notification requests that have been queued and not transmitted.	Number	A high value of this measure indicates that the Active Directory is changing frequently but the update notification requests have not been transmitted to the other domain controllers. This results in a loss of data integrity in the directory store. This problem can be corrected by forcing the replication process.
Current threads	This measure shows the number of threads that are currently servicing the API calls by the users.	Number	A fluctuating value for this measure indicates a change in the load.
Directory writes	This measure shows the number of successful write operations made by the directory service per second.	Writes/Sec	A high value for this measure indicates that the directory service has made write operations in the Active Directory. This results in the fragmentation of the Active Directory. This problem can be corrected by forcing the replication process.
Kerberos requests	This measure shows the number of times per second that the user uses the user credentials to authenticate himself or herself with the domain controller that is being monitored.	Reqs/Sec	A high value for this measure indicates that the user requested some network resource, which requires authentication. Installing one or more Active Directory in the target environment can solve this problem
NTLM requests	This measure shows the number of times per second that the user uses the user credentials to	Reqs/Sec	A high value for this measure indicates that the user requested some network resource, which basically belongs to the Windows NT network. Accessing

Measurement	Description	Measurement Unit	Interpretation
	authenticate himself or herself with the domain controller, which is having the PDC emulator operation role.		this kind of resource needs authentication, which is serviced by the domain controller, who is having the PDC emulator operation role. Installing one or more domain controllers with PDC emulator operation role in the target environment can solve this problem.
Ticket requests	This measure indicates the number of requests made by the Ticket Granting Service per second.	Reqs/Sec	A high value for this measure indicates that the user requested some network resources, which needs authentication. Installing one or more domain controllers in the target environment can solve this problem.
Authentication requests	This measure indicates the number of requests made by the Authentication Server (to obtain the TGT) per second.	Reqs/Sec	A high value for this measure indicates that the user requested some network resources, which needs authentication. Installing one or more domain controllers in the target environment can solve this problem.
Ldap sessions	This measure indicates the number of Ldap clients currently connected to the Active Directory.	Number	This measure is just an indicator of the number of Ldap clients connected to the Active Directory. A high or low value for this measure does not always denote an error situation.

3.5.3 Directory Service Events Test

This test reports statistical information about the Directory Service events recorded in the event log. This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick the *Active Directory* as the desired **Component type**, set *Performance* as the **Test type**, choose the test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the test : An Active Directory server

Agent deploying the test : An internal agent

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

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The host for which the test is to be configured.
Port	Refers to the port used by the EventLog Service. Here it is *null*.
Log Type	Refers to the type of event logs to be monitored. The default value is application.
Policy Based Filter	Using this page, administrators can configure the event sources, event IDs, and event descriptions to be monitored by this test. In order to enable administrators to easily and accurately provide this specification, this page provides the following options: • Manually specify the event sources, IDs, and descriptions in the Filter text area, or, • Select a specification from the predefined filter policies listed in the Filter box For explicit, manual specification of the filter conditions, select the No option against the Policy Based Filter field. This is the default selection. To choose from the list of pre-configured filter policies, or to create a new filter policy and then associate the same with the test, select the Yes option against this field.
Filter	If the Policy Based Filter flag is set to No, then a Filter text area will appear, wherein you will have to specify the event sources, event IDs, and event descriptions to be monitored. This specification should be of the following format: *{Displayname}:{event_sources_to_be_included}:{event_sources_to_be_excluded}:{event_IDs_to_be_included}:{event_IDs_to_be_excluded}:{event_descriptions_to_be_included}:{event_descriptions_to_be_excluded}*. For example, assume that the Filter text area takes the value, *OS_events:all:Browse,Print:all:none:all:none*. Here: • OS_events is the display name that will appear as a descriptor of the test in the monitor UI; • all indicates that all the event sources need to be considered while monitoring. To monitor specific event sources, provide the source names as a comma-separated list. To ensure that none of the event sources are monitored, specify none.

Parameters	Description
	• Next, to ensure that specific event sources are excluded from monitoring, provide a comma-separated list of source names. Accordingly, in our example, Browse and Print have been excluded from monitoring. Alternatively, you can use all to indicate that all the event sources have to be excluded from monitoring, or none to denote that none of the event sources need be excluded. • In the same manner, you can provide a comma-separated list of event IDs that require monitoring. The all in our example represents that all the event IDs need to be considered while monitoring. • Similarly, the none (following all in our example) is indicative of the fact that none of the event IDs need to be excluded from monitoring. On the other hand, if you want to instruct the eG Enterprise system to ignore a few event IDs during monitoring, then provide the IDs as a comma-separated list. Likewise, specifying all makes sure that all the event IDs are excluded from monitoring. • The all which follows implies that all events, regardless of description, need to be included for monitoring. To exclude all events, use none. On the other hand, if you provide a comma-separated list of event descriptions, then the events with the specified descriptions will alone be monitored. Event descriptions can be of any of the following forms - desc*, or desc, or *desc*,or desc*, or desc1*desc2, etc. desc here refers to any string that forms part of the description. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters. • In the same way, you can also provide a comma-separated list of event descriptions to be excluded from monitoring. Here again, the specification can be of any of the following forms: desc*, or desc, or *desc*,or desc*, or desc1*desc2, etc. desc here refers to any string that forms part of the description. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters. In our example however, none is specified, indicating that no event descriptions are to be excluded from monitoring. If you use all instead, it would mean that all event descriptions are to be excluded from monitoring. **Note:**

Parameters	Description
	The event sources and event IDs specified here should be exactly the same as that which appears in the Event Viewer window. On the other hand, if the Policy Based Filter flag is set to **Yes**, then a Filter list box will appear, displaying the filter policies that pre-exist in the eG Enterprise system. A filter policy typically comprises of a specific set of event sources, event IDs, and event descriptions to be monitored. This specification is built into the policy in the following format: *{Policyname}:{event_sources_to_be_included}:{event_sources_to_be_excluded}:{event_IDs_to_be_included}:{event_IDs_to_be_excluded}:{event_descriptions_to_be_included}:{event_descriptions_to_be_excluded}* To monitor a specific combination of event sources, event IDs, and event descriptions, you can choose the corresponding filter policy from the Filter list box. Multiple filter policies can be so selected. Alternatively, you can modify any of the existing policies to suit your needs, or create a new filter policy. To facilitate this, a **Click here** link appears just above the test configuration section, once the **Yes** option is chosen against Policy Based Filter. Clicking on the **Click here** link leads you to a page where you can modify the existing policies or create a new one. The changed policy or the new policy can then be associated with the test by selecting the policy name from the Filter list box in this page.
UseWMI	The eG agent can either use **WMI** to extract event log statistics or directly parse the event logs using event log APIs. If this flag is **Yes**, then **WMI** is used. If not, the event log APIs are used. This option is provided because on some Windows 2000 systems (especially ones with service pack 3 or lower), the use of WMI access to event logs can cause the CPU usage of the WinMgmt process to shoot up. On such systems, set this parameter value to **No**.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be

Parameters	Description
	available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Directory service errors	This refers to the number of Directory Service events that were generated.	Number	A very low value (zero) indicates that the Directory Service is in a healthy state without any potential problems. An increasing trend or high value indicates the existence of problems like loss of functionality or data. The detailed diagnosis capability, if enabled, lists the description of specific events. Please check the Application Logs in the Event Log Viewer for more details.
Directory service information count	This refers to the number of Directory Service Service information events generated when the test was last executed.	Number	A change in the value of this measure may indicate infrequent but successful operations performed by the Directory Service. The detailed diagnosis capability, if enabled, lists the description of specific events.
Directory service warnings	This refers to the number of warnings that were generated when the test was last executed.	Number	A high value of this measure indicates problems that may not have an immediate impact, but may cause future problems in the Directory Service. The detailed diagnosis capability, if enabled, lists the description of specific events.

Measurement	Description	Measurement Unit	Interpretation
Directory service critical errors	Indicates the number of critical events that were generated when the test was last executed.	Number	**This measure is applicable only for Windows 2008/Windows Vista/Windows 7 systems.** A high value of this measure indicates that too many errors have occurred, which the Directory Service cannot automatically recover from. The detailed diagnosis capability, if enabled, provides the description of specific events.
Directory service verbose count	Indicates the number of verbose events that were generated when the test was last executed.	Number	**This measure is applicable only for Windows 2008/Windows Vista/Windows 7 systems.** Verbose logging provides more details in the log entry, which will enable you to troubleshoot issues better. The detailed diagnosis of this measure describes all the verbose events that were generated during the last measurement period.

3.5.4 User Account Lockouts Test

Account lockout is a feature of password security that disables a user account when a certain number of failed logons occur due to wrong passwords within a certain interval of time. The purpose behind account lockout is to prevent attackers from brute-force attempts to guess a user's password.

Other ways accounts can get locked out include:

- Applications using cached credentials that are stale.
- Stale service account passwords cached by the Service Control Manager (SCM).
- Stale logon credentials cached by Stored User Names and Passwords in Control Panel.
- Scheduled tasks and persistent drive mappings that have stale credentials.
- Disconnected Terminal Service sessions that use stale credentials.

- Failure of Active Directory replication between domain controllers.
- Users logging into two or more computers at once and changing their password on one of them.

Any one of the above situations can trigger an account lockout condition, and the results can include applications behaving unpredictably and services inexplicably failing.

This is why, whenever a user complaints of inability to login to his/her desktop, help desk should be able to instantly figure out whether that user's account has been locked out, and if so, why. The **User Account Lockouts** test provides answers to these questions. This test, at configured intervals, reports the count of locked user accounts and names the users who have been affected by this anomaly.

Target of the test : An Active Directory or Domain Controller

Agent deploying the test : An internal agent; this test cannot be run in an 'agentless' manner

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Account lockout events</td><td>Indicates the number of account lockouts that occurred during the last measurement period.</td><td>Number</td><td>A very high value for this measure could indicate a malicious attack, and may require further investigation.
If the high lockout rate is not due to any such attacks, then it is recommended that you alter the lockout policy in your environment to minimize the count and consequently, the impact of account lockouts. Microsoft recommends the following policies for high, medium, and low security environments:
<table>
<tr><th>Security Level</th><th>Lockout Policy</th></tr>
<tr><td>Low</td><td>Account Lockout Duration =Not Defined
Account Lockout Threshold = 0 (No lockout)
Reset account lockout counter after = Not Defined</td></tr>
<tr><td>Medium</td><td>Account Lockout Duration =30 minutes
Account Lockout Threshold = 10 invalid logon attempts
Reset account lockout counter after</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><th>Security Level</th><th>Lockout Policy</th></tr><tr><td></td><td>= 30 minutes</td></tr><tr><td>High</td><td>Account lockout duration = 0 (an administrator must unlock the account)
Account lockout threshold = 10 invalid logon attempts
Reset account lockout counter after = 30 minutes</td></tr></table></td></tr>
<tr><td>Unique users locked out</td><td>Indicates the number of distinct users who were locked out during the last measurement period.</td><td>Number</td><td>Use the detailed diagnosis of this measure to view the names of these users.</td></tr>
<tr><td>Users currently locked out</td><td>Indicates the number of users who are currently locked out.</td><td>Number</td><td>Use the detailed diagnosis of this measure to know which users are currently locked out.</td></tr>
</table>

3.5.5 Active Directory Lost and Found Test

On a domain controller, the Lost and Found container contains Active Directory objects that have been orphaned. An object is orphaned when the object is created on one domain controller and the container in which the object is placed is deleted from the directory on another domain controller before the object has a chance to replicate. An orphaned object is automatically placed in the Lost and Found container where it can be found by an administrator.

This test reports the number of orphaned objects currently in the Lost and Found container, provides the details of these objects, so that administrators can determine which objects to move and which ones to delete.

Note:

This test applies only to Active Directory Servers installed on Windows 2008.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick the *Active Directory* as the desired **Component type**, set *Performance* as the **Test type**, choose the test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the test : An Active Directory or Domain Controller on Windows 2008

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is *389*.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Lost and Found objects	Indicates the number of objects currently available	Number	A non-zero value indicates the existence of orphaned objects. Use

Measurement	Description	Measurement Unit	Interpretation
	in the Lost and Found container.		the detailed diagnosis of this measure to know which objects to move and which ones to delete.

3.5.6 Global Catalog Search Test

The global catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain in a multidomain Active Directory Domain Services (AD DS) forest. The global catalog is stored on domain controllers that have been designated as global catalog servers and is distributed through multimaster replication.

The Global Catalog enables searching for Active Directory objects in any domain in the forest without the need for subordinate referrals, and users can find objects of interest quickly without having to know what domain holds the object. The global catalog makes the directory structure within a forest transparent to users who perform a search. For example, if you search for all printers in a forest, a global catalog server processes the query in the global catalog and then returns the results. Without a global catalog server, this query would require a search of every domain in the forest.

This test reveals whether the server being monitored is a global catalog server or not. If it is, then the test attempts to search the global catalog server for a configured user and reports whether that user was found or not. The test also reports the time taken to search for that user. This information helps administrators assess how efficient the global catalog is in minimizing the time taken to locate a user across domains.

Note:

This test applies only to Active Directory Servers installed on Windows 2008.

Target of the test : An Active Directory or Domain Controller on Windows 2008

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.

Parameters	Description
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is *389*.
Username	Specify the name of the user who has to be searched in the global catalog.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Is it a global catalog server?	Indicates whether the monitored server is a global catalog server or not.	Boolean	This measure reports the value *True* if the AD server being monitored is a global catalog server, and the value *False* if it is not. If this measure reports the value *False*, the remaining measures of the test will not report any values.
Was user found?	Indicates whether the configured Username was found or not in the global catalog server.	Boolean	This measure reports the value *True* if the configured Username was found in the global catalog server and the value *False* if the user name was not found.
Catalog search time	Indicates the time taken by the global catalog server to search and find the configured Username.	Secs	A high value for this measure would warrant an investigation.

3.5.7 Address Book Details Test

The Address Book is a client for the Active Directory database. It performs lookups and search operations on the Active Directory database to look for details such as account email ID, and so forth. Using the **Address Book Details** test, you can determine the number of Address Book clients currently connected to the AD database and the rate at which search operations are performed by each AD server. In the event that the AD database gets inundated with search queries, you can use this test to figure out whether or not the Address Book clients are contributing to the query load.

Note:

This test applies only to Active Directory Servers installed on Windows 2008.

Target of the test : An Active Directory or Domain Controller on Windows 2008

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is *389*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Client sessions	Indicates the number of client sessions that are currently connected to the AD database.	Number	A high value is indicative of heavy load. A consistent increase in the value of this measure could indicate a potential overload condition.
Search operations	Indicate the rate at which the key search operations are performed on the AD database.	Searches/Sec	If the value of this measure decreases while the number of Client sessions keeps increasing, it indicates that search queries are not been processed as quickly; this in turn is indicative of a processing bottleneck, which can consequently choke the AD server database.

3.5.8 ADAM LDAP Performance Test

The Lightweight Directory Access Protocol (LDAP) is a directory service protocol that runs on a layer above the TCP/IP stack. It provides a mechanism used to connect to, search, and modify Internet directories. The LDAP directory service is based on a client-server model. The function of LDAP is to enable access to an existing directory. LDAP is one of the protocols used to query and modify items on the Active Directory server.

To monitor the interactions between clients and the AD server over LDAP, and to promptly capture slowdowns in LDAP searches and binds, use the **ADAM LDAP Performance** test.

Note:

This test applies only to Active Directory Servers installed on Windows 2008.

Target of the test : An Active Directory or Domain Controller on Windows 2008

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is *389*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Ldap searches	Indicates the rate at which LDAP clients perform search operations.	Searches/Sec	This counter should show activity over time. If it does not, network problems are probably hindering the processing of client requests.
Ldap writes	Indicates the rate at which clients perform write operations on the AD server.	Writes/Sec	
Ldap active threads	Indicates the current number of threads in use by the LDAP subsystem of the local directory service.	Number	A high number indicates a high level of LDAP activity on the directory service.
Ldap bind time	Indicates the time, in milliseconds, taken for	Secs	In Active Directory Domain Services, the act of associating a programmatic object

Measurement	Description	Measurement Unit	Interpretation
	the last successful LDAP bind.		with a specific Active Directory Domain Services object is known as binding. When a programmatic object, such as an IADs or DirectoryEntry object, is associated with a specific directory object, the programmatic object is considered to be bound to the directory object. This measure should be as low as possible. If it is not, hardware or network-related problems are indicated.
Ldap sessions	Indicates the number of currently connected LDAP client sessions.	Number	This measure is just an indicator of the number of Ldap clients connected to the Active Directory. A high or low value for this measure does not always denote an error situation.
Ldap closed connections	Indicates the LDAP connections that have been closed in the last second.	Connections/Sec	
Ldap new connections	Indicates the number of new LDAP connections that have arrived in the last second.	Connections/Sec	
Ldap new ssl connections	Indicates the number of new SSL or TLS connections that arrived in the last second.	Connections/Sec	
Ldap successful binds	Indicates the number of successful LDAP binds per second.	Binds/Sec	In Active Directory Domain Services, the act of associating a programmatic object with a specific Active Directory Domain Services object is known as binding. When a programmatic object, such as an IADs or DirectoryEntry object, is associated with a specific directory object, the programmatic object is considered to be bound to the directory

Measurement	Description	Measurement Unit	Interpretation
			object. A high value is desired for this measure. A very low value could indicate network problems.

3.5.9 Authentication Performance Test

Authentication of domain user logins is a core function of an Active Directory server. The default authentication protocol used by the AD server is **Kerberos**. Kerberos authentication is based on specially formatted data packets known as tickets. In Kerberos, these tickets pass through the network instead of passwords. Transmitting tickets instead of passwords makes the authentication process more resistant to attackers who can intercept the network traffic.

In a Kerberos environment, the authentication process begins at logon. The following steps describe the Kerberos authentication process:

a. When a user enters a user name and password, the computer sends the user name to the KDC (Key Distribution Center). The Key Distribution Center (KDC) maintains a database of account information for all security principals in the domain. The KDC stores a cryptographic key known only to the security principal and the KDC. This key is used in exchanges between the security principal and the KDC and is known as a long term key. The long term key is derived from a user's logon password.

b. Upon the receipt of a user name, the KDC looks up the user's master key (KA), which is based on the user's password. The KDC then creates two items: a session key (SA) to share with the user and a Ticket-Granting Ticket (TGT). The TGT includes a second copy of the SA, the user name, and an expiration time. The KDC encrypts this ticket by using its own master key (KKDC), which only the KDC knows.

c. The client computer receives the information from the KDC and runs the user's password through a one-way hashing function, which converts the password into the user's KA (i.e., master key). The client computer now has a session key and a TGT so that it can securely communicate with the KDC. The client is now authenticated to the domain and is ready to access other resources in the domain by using the Kerberos protocol.

d. When a Kerberos client needs to access resources on a server that is a member of the same domain, it contacts the KDC. The client will present its TGT and a timestamp encrypted with the session key that is already shared with the KDC. The KDC decrypts the TGT using its KKDC.

The TGT contains the user name and a copy of the SA. The KDC uses the SA to decrypt the timestamp. The KDC can confirm that this request actually comes from the user because only the user can use the SA.

e. Next, the KDC creates a pair of tickets, one for the client and one for the server on which the client needs to access resources. Each ticket contains the name of the user requesting the service, the recipient of the request, a timestamp that declares when the ticket was created, and a time duration that says how long the tickets are valid. Both tickets also contain a new key (KAB) that will be shared between the client and the server so they can securely communicate.

f. The KDC takes the server's ticket and encrypts it using the server master key (KB). Then the KDC nests the server's ticket inside the client's ticket, which also contains the KAB. The KDC encrypts the whole thing using the session key that it shares with the user from the logon process. The KDC then sends all the information to the user.

g. When the user receives the ticket, the user decrypts it using the SA. This exposes the KAB to the client and also exposes the server's ticket. The user cannot read the server's ticket. The user will encrypt the timestamp by using the KAB and send the timestamp and the server's ticket to the server on which the client wants to access resources. When it receives these two items, the server first decrypts its own ticket by using its KB. This permits access to the KAB, which can then decrypt the timestamp from the client.

In situations where a domain controller is not available or is unreachable, **NTLM** (the NT LAN Manager) is used as the authentication protocol. For example, **NTLM** would be used if a client is not Kerberos capable, the server is not joined to a domain, or the user is remotely authenticating over the web.

In some other environments, **Digest** authentication is supported. Digest authentication offers the same functionality as Basic authentication; however, Digest authentication provides a security improvement because a user's credentials are not sent across the network in plaintext. Digest authentication sends credentials across the network as a Message Digest 5 (MD5) hash, which is also known as the MD5 message digest, in which the credentials cannot be deciphered from the hash.

Regardless of the protocol/authentication mode used, the quality of a user's experience with the AD server largely relies on how fast his/her login is authenticated by the AD server. The slightest of delays will hence not be tolerated! Administrators therefore need to keep their eyes open at all times for authentication-related latencies, isolate their source, and fix the problems, so that users are able to login to their systems quickly. The **Authentication Performance** test helps administrators in this regard.

This test reports the rate at which Kerberos, NTLM, and Digest authentication requests are serviced by the AD server and thus promptly reveals delays in authentication (if any). Where latencies are noticed in Kerberos requests, the test goes one step further and indicates the probable source of the latencies - could it be because the KDC took too long to grant TGTs to the clients? or is it because the KDC took too long to process the TGTs and grant the clients access to authorized resources?

Note:

This test applies only to Active Directory Servers installed on Windows 2008.

Target of the test : An Active Directory or Domain Controller on Windows 2008

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is *389*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Kerberos requests	Indicates the number of times per second that clients use a ticket to authenticate to the domain controller.	Reqs/Sec	A low value indicates a bottleneck when processing Kerberos requests.
Digest requests	Indicates the rate at which requests from a potential user were received by a network server and then sent to a domain controller.	Reqs/Sec	A low value indicates a bottleneck when processing Digest requests.

Measurement	Description	Measurement Unit	Interpretation
NTLM requests	Indicates the rate at which NTLM authentication requests were serviced by the domain controller.	Reqs/Sec	A low value indicates a bottleneck when processing NTLM requests. A high value for this measure indicates that the user requested some network resource, which basically belongs to the Windows NT network. Accessing this kind of resource needs authentication, which is serviced by the domain controller, who is having the PDC emulator operation role. Installing the domain controller with PDC emulator operation role in the target environment can solve this problem.
Authentication requests	Indicates the number of Authentication Server (AS) requests serviced by the Kerberos Key Distribution Center (KDC) per second.	Reqs/Sec	AS requests are used by the client to obtain a ticket-granting ticket. If the AD server appears to be taking too long to process Kerberos requests - i.e., if the value of the Kerberos requests measure is too high - then you can compare the value of this measure with that of the Ticket requests measure to know where the request spent too much time - when granting TGTs to clients? or when processing the TGTs to allow users access to a resource?
Ticket requests	Indicates the number of Ticket Granting Server (TGS) requests serviced by the KDC per second.	Reqs/Sec	TGS requests are used by the client to obtain a ticket to a resource. If the AD server appears to be

Measurement	Description	Measurement Unit	Interpretation
			taking too long to process Kerberos requests - i.e., if the value of the Kerberos requests measure is too high - then you can compare the value of this measure with that of the Authentication requests measure to know where the request spent too much time - when granting TGTs to clients? or when processing the TGTs to allow users access to a resource?

3.5.10 ADAM Binding Test

In Active Directory Domain Services, the act of associating a programmatic object with a specific Active Directory Domain Services object is known as binding. When a programmatic object, such as an IADs or DirectoryEntry object, is associated with a specific directory object, the programmatic object is considered to be bound to the directory object.

This test reports the type of binds that exist in an AD environment, and for each bind type, reports how fast the AD server bound the programmatic objects to the directory object.

Note:

This test applies only to Active Directory Servers installed on Windows 2008.

Target of the test : An Active Directory or Domain Controller on Windows 2008

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.

Parameters	Description
Port	The port number through which the Active Directory communicates. The default port number is *389*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Ntlm binds	Indicates the rate at which programmatic and directory objects were bound to one another using NTLM binds.	Binds/Sec	
Simple binds	Indicates the rate at which programmatic and directory objects were bound to one another using Simple binds.	Binds/Sec	In a simple bind, the client either binds anonymously, that is, with an empty bind Distinguished Name, or by providing a Distinguished Name and a password.
External binds	Indicates the rate at which programmatic and directory objects were bound to one another using External binds.	Binds/Sec	
Fast binds	Indicates the rate at which programmatic and directory objects were bound to one another using Fast binds.	Binds/Sec	Fast bind mode allows a client to use the LDAP bind request to simply validate credentials and authenticate the client without the overhead of establishing the authorization information.
Negotiated binds	Indicates the rate at which programmatic and directory objects were bound to one another using Negotiated binds.	Binds/Sec	

3.5.11 Global Catalogs Test

The global catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain in a multidomain active directory domain services (AD DS) forest.

The global catalog is stored on domain controllers that have been designated as global catalog servers and is distributed through multimaster replication.

The global catalog enables searching for active directory objects in any domain in the forest without the need for subordinate referrals, and users can find objects of interest quickly without having to know what domain holds the object. The global catalog makes the directory structure within a forest transparent to users who perform a search. For example, if you search for all printers in a forest, a global catalog server processes the query in the global catalog and then returns the results. Without a global catalog server, this query would require a search of every domain in the forest.

This test monitors the global catalogs in the target domain controller and reports the number of catalogs that are currently available and unavailable. This way, the test enables administrators to determine whether/not adequate global catalogs are available in the domain controller to handle the request load.

Target of the test : An Active Directory or Domain Controller on Windows

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is *389*.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total global catalogs	Indicates the total number of global catalogs on the domain controller being monitored.	Number	
Available global catalogs	Indicates the number of global catalogs that are currently available on the domain controller.	Number	
Unavailable global catalogs	Indicates the number of global catalogs that are currently unavailable on the domain controller.	Number	If the value of this measure is equal to the value of the Total global gatalogs measure or is higher than that of the Available global catalogs measure, it indicates that enough global catalogs may not be available on the domain controller to process user logon requests and search requests. As a result, requests may fail.
Percent unavailable global catalogs	Indicates percentage of global catalogs that are currently unavailable.	Percent	A high value indicates that too many global catalogs are unavailable for request processing. This in turn can cause many user logon and search requests to the domain controller to fail. Ideally therefore, the value of this measure should be very low.

3.5.12 Active Directory Users Test

This test reports the status of user accounts configured in the Active Directory server and thus, quickly points you to ‘unused’ accounts that can be deleted to make room for those that are actively used.

Target of the test : An Active Directory or Domain Controller on Windows

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is *389*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Never logged on users	Indicates the indicates the number of AD users who have never logged on to the network.	Number	A healthy AD server is one that has no or very few ‘unused’ user accounts. A high value is therefore not desired for this measure. To know who these users are, use the detailed diagnosis of this measure.
Inactive users	Indicates the number of users who are currently inactive in the AD server.	Number	To identify the inactive users, use the detailed diagnosis of this measure. The detailed diagnosis displays the Distinguished Name of the user, the date/time he/she logged in last, and the date/time at which the user account was created. This will help you in figuring out how long that user has been inactive. If you think that the user will never again become active, you can proceed to delete that user account.
Disabled users	Indicates the number of user accounts that are currently disabled on the AD server.	Number	To identify the disabled users, use the detailed diagnosis of this measure. The detailed diagnosis displays the Distinguished Name of the user and the date/time at which the user account was created. This will help you in figuring out how long each user account has remained disabled. If you think that the user will never again

Measurement	Description	Measurement Unit	Interpretation
			become active, you can proceed to delete that user account.
Total users	Indicates the total number of users managed by the AD server.	Number	

3.5.13 Account Management Events Test

The addition of new users/computers/groups to an Active Directory domain, changes to existing user/computer/group accounts, and deletion of accounts are important to verify that they were performed only by authorized personnel and with no malicious intent. To track such operations, “Audit account management events” provides specific event IDs. Using the **Account Management Events** test, you can continuously track events with the event IDs grouped under Audit account management events, and be proactively alerted to the sudden addition/modificiation/deletion of users/groups/computers in the Active Directory. You can also use the detailed diagnosis of the test to know which user performed the addition/modification/deletion and when.

Target of the test : An Active Directory server

Agent deploying the test : An internal agent

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

Configurable parameters for the test

Parameters	Description
Test Period	This indicates how often should the test be executed.
Host	The host for which the test is to be configured.
Port	Refers to the port used by the EventLog Service. Here it is *null*.
SuccesseventsinDD	By default, this parameter displays *none*, indicating that by default none of the successful log audits will be reflected in the detailed diagnosis. If you set this parameter to, say *10*, then the test will display only the 10 most recent successful log audits in the detailed diagnosis page. Setting this parameter to all, on the other hand will make sure that all successful log audits are listed in the detailed diagnosis.
FailureeventsinDD	By default, this parameter displays all, indicating that by default *all* the failed log audits will be reflected in the detailed diagnosis. If you set this parameter to, say *10*, then the

Parameters	Description
	test will display only the 10 most recent log audits that failed, in the detailed diagnosis page. Setting this parameter to none, on the other hand will make sure that none of the failed log audits are listed in the detailed diagnosis.
Policy Based Filter	Using this page, administrators can configure the event sources, event IDs, and event descriptions to be monitored by this test. In order to enable administrators to easily and accurately provide this specification, this page provides the following options: • Manually specify the event sources, IDs, and descriptions in the Filter text area, or, • Select a specification from the predefined filter policies listed in the Filter box For explicit, manual specification of the filter conditions, select the No option against the Policy Based Filter field. This is the default selection. To choose from the list of pre-configured filter policies, or to create a new filter policy and then associate the same with the test, select the **Yes** option against this field.
Filter	If the Policy Based Filter flag is set to No, then a Filter text area will appear, wherein you will have to specify the event sources, event IDs, and event descriptions to be monitored. This specification should be of the following format: *{Displayname}:{event_sources_to_be_included}:{event_sources_to_be_excluded}:{event_IDs_to_be_included}:{event_IDs_to_be_excluded}:{event_descriptions_to_be_included}:{event_descriptions_to_be_excluded}*. For example, assume that the Filter text area takes the value, *OS_events:all:Browse,Print:all:none:all:none*. Here: • OS_events is the display name that will appear as a descriptor of the test in the monitor UI; • all indicates that all the event sources need to be considered while monitoring. To monitor specific event sources, provide the source names as a comma-separated list. To ensure that none of the event sources are monitored, specify none. • Next, to ensure that specific event sources are excluded from monitoring, provide a comma-separated list of source names. Accordingly, in our example, Browse and Print have been excluded from monitoring. Alternatively, you can use all to indicate that all the event sources have to be excluded from monitoring, or none to denote that none of the event sources need be excluded. • In the same manner, you can provide a comma-separated list of event IDs that require monitoring. The all in our example represents that all the event IDs need to

Parameters	Description
	be considered while monitoring. • Similarly, the none (following all in our example) is indicative of the fact that none of the event IDs need to be excluded from monitoring. On the other hand, if you want to instruct the eG Enterprise system to ignore a few event IDs during monitoring, then provide the IDs as a comma-separated list. Likewise, specifying all makes sure that all the event IDs are excluded from monitoring. • The all which follows implies that all events, regardless of description, need to be included for monitoring. To exclude all events, use none. On the other hand, if you provide a comma-separated list of event descriptions, then the events with the specified descriptions will alone be monitored. Event descriptions can be of any of the following forms - desc*, or desc, or *desc*,or desc*, or desc1*desc2, etc. desc here refers to any string that forms part of the description. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters. • In the same way, you can also provide a comma-separated list of event descriptions to be excluded from monitoring. Here again, the specification can be of any of the following forms: desc*, or desc, or *desc*,or desc*, or desc1*desc2, etc. desc here refers to any string that forms part of the description. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters. In our example however, none is specified, indicating that no event descriptions are to be excluded from monitoring. If you use all instead, it would mean that all event descriptions are to be excluded from monitoring. **Note:** The event sources and event IDs specified here should be exactly the same as that which appears in the Event Viewer window. On the other hand, if the Policy Based Filter flag is set to **Yes**, then a Filter list box will appear, displaying the filter policies that pre-exist in the eG Enterprise system. A filter policy typically comprises of a specific set of event sources, event IDs, and event descriptions to be monitored. This specification is built into the policy in the following format: *{Policyname}:{event_sources_to_be_included}:{event_sources_to_be_excluded}:{event_IDs_to_be_included}:{event_IDs_to_be_excluded}:{event_*

Parameters	Description
	descriptions_to_be_included}:{event_descriptions_to_be_excluded} To monitor a specific combination of event sources, event IDs, and event descriptions, you can choose the corresponding filter policy from the Filter list box. Multiple filter policies can be so selected. Alternatively, you can modify any of the existing policies to suit your needs, or create a new filter policy. To facilitate this, a **Click here** link appears just above the test configuration section, once the **Yes** option is chosen against the Policy Based Filter. Clicking on the **Click here** link leads you to a page where you can modify the existing policies or create a new one. The changed policy or the new policy can then be associated with the test by selecting the policy name from the Filter list box in this page.
Events During Restart	By default, this flag is set to **Yes**. This ensures that whenever the agent is stopped and later started, the events that might have occurred during the period of non-availability of the agent are included in the number of events reported by the agent. Setting the flag to **No** ensures that the agent, when restarted, ignores the events that occurred during the time it was not available.
Stateless Alerts	Typically, the eG manager generates email alerts only when the state of a specific measurement changes. A state change typically occurs only when the threshold of a measure is violated a configured number of times within a specified time window. While this ensured that the eG manager raised alarms only when the problem was severe enough, in some cases, it may cause one/more problems to go unnoticed, just because they did not result in a state change. For example, take the case of the **EventLog** test. When this test captures an error event for the very first time, the eG manager will send out a critical email alert with the details of the error event to configured recipients. Now, the next time the test runs, if a different error event is captured, the eG manager will keep the state of the measure as critical, but will not send out the details of this error event to the user; thus, the second issue will remain hidden from the user. To make sure that administrators do not miss/overlook critical issues, the eG Enterprise monitoring solution provides the stateless alerting capability. To enable this capability for this test, set the stateless alerts flag to **Yes**. This will ensure that email alerts are generated for this test, regardless of whether or not the state of the measures reported by this test changes.
UseWMI	The eG agent can either use **WMI** to extract event log statistics or directly parse the event logs using event log APIs. If this flag is **Yes**, then **WMI** is used. If not, the event log APIs are used. This option is provided because on some Windows 2000 systems (especially ones with service pack 3 or lower), the use of WMI access to event logs can cause the CPU usage of the WinMgmt process to shoot up. On such systems, set this parameter value to **No**.

Parameters	Description
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying none against DD frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
User password reset by administrator	Indicates the number of times the user password was changed by the administrator since the last measurement period.	Number	Typically, such an event occurs when the administrator attempts to change some other user's password in response to a 'forgot password' call. You can use the detailed diagnosis of this measure to know which admin user attempted the password change on which computer.
User password reset by users	Indicates the number of times the user password was changed by the users themselves since the last measurement period.	Number	You can use the detailed diagnosis of this measure to know which user attempted the password change on which computer.
User accounts created	Indicates the number of user accounts that have	Number	New user accounts are important to

Measurement	Description	Measurement Unit	Interpretation
	been created since the last measurement period.		audit to verify that they correspond to a legitimate employee, contractor or application. Outside intruders often create new user accounts to facilitate continued access to the penetrated system. Therefore, you need to eye any sudden increase in the value of this measure with suspicion. You can use the detailed diagnosis of this measure to know which user created new users on which computer.
User accounts deleted	Indicates the number of user accounts that have been deleted since the last measurement period.	Number	You can use the detailed diagnosis of this measure to know which user deleted user accounts on which computer.
User account changed	Indicates the number of times the user account has been changed since the last measurement period.	Number	Certain changes to user accounts are important to audit since they can be a tip-off to compromised accounts. For instance, both insider and outsider computer criminals often gain access to a system by socially engineering the help desk to a user's password. Or a previously disabled account being re-enabled may be suspicious depending on the history and type of the account. You can use the detailed diagnosis of this measure to know which user made changes to user accounts on which computer.
Computer accounts created	Indicates the number of times computer accounts have been created since the last measurement period.	Number	You can use the detailed diagnosis of this measure to know which user created computer accounts on which computer.
Computer accounts deleted	Indicates the number of computer accounts that have been deleted since	Number	You can use the detailed diagnosis of this measure to know which user deleted computer accounts on which

Measurement	Description	Measurement Unit	Interpretation
	the last measurement period.		computer.
Computer accounts changed	Indicates the number of times the computer accounts that have been changed since the last measurement period.	Number	You can use the detailed diagnosis of this measure to know which user changed computer accounts on which computer.
User/Computer object disabled	Indicates the number of times the user/computer object was disabled during the last measurement period.	Number	You can use the detailed diagnosis of this measure to know which user disabled user/computer objects on which computer.
User/Computer object enabled	Indicates the number of times the user/computer object was enabled during the last measurement period.	Number	You can use the detailed diagnosis of this measure to know which user enabled user/computer objects on which computer.
User added to security group	Indicates the number of users who were added to the security group during the last measurement period.	Number	Group changes, especially changes to the group's membership, are very useful to track since groups are used to control access to resources, link security policies and control wireless and remote access all over a Windows network. Security groups are the only group type that you can assign permissions and rights. Security groups are referred to as "security enabled" groups in the security log. You can use the detailed diagnosis of this measure to know which user added users to the security group on which computer.
Security groups deleted	Indicates the number of security groups that were deleted during the last measurement period.	Number	You can use the detailed diagnosis of this measure to know which user deleted security groups on which computer.

Measurement	Description	Measurement Unit	Interpretation
Security groups created	Indicates the number of security groups that were created during the last measurement period.	Number	You can use the detailed diagnosis of this measure to know which user created security groups on which computer.
Security groups changed	Indicates the number of security groups that were changed during the last measurement period.	Number	You can use the detailed diagnosis of this measure to know which user changed security groups on which computer.

Once the **STATELESS ALERTING** capability is enabled for a test (as discussed above), you will find that everytime the test reports a problem, the eG manager does the following:

- Closes the alarm that pre-exists for that problem;
- Sends out a normal alert indicating the closure of the old problem;
- Opens a new alarm and assigns a new alarm ID to it;
- Sends out a fresh email alert to the configured users, intimating them of the new issue.

In a redundant manager setup, the secondary manager automatically downloads the updated eg_ specs.ini file from the primary manager, and determines whether the stateless alerting capability has been enabled for any of the tests reporting metrics to it. If so, everytime a threshold violation is detected by such a test, the secondary manager will perform the tasks discussed above for the problem reported by that test. Similarly, the primary manager will check whether the stateless alert flag has been switched on for any of the tests reporting to it, and if so, will automatically perform the above-mentioned tasks whenever those tests report a deviation from the norm.

Note:

The **STATELESS ALERTING** capability is currently available for the following tests alone, by default:

- EventLog test
- ApplicationEventLog test
- SystemEventLog test
- ApplicationEvents test

- SystemEvents test
- SecurityLog test
- Account Management Events test

If need be, you can enable the **STATELESS ALERTING** capability for other tests. To achieve this, follow the steps given below:

- Login to the eG manager host.
- Edit the *eg_specs.ini* file in the <EG_INSTALL_DIR>\manager\config directory.
- Locate the test for which the **Stateless Alarms** flag has to be enabled.
- Insert the entry, **-statelessAlerts yes**, into the test specification as depicted below:

```
EventLogTest::$hostName:$portNo=$hostName, -auto, -host $hostName -port $portNo -
eventhost $hostIp -eventsrc all -excludedSrc none -useWmi yes -statelessAlerts yes -
ddFreq 1:1 -rptName $hostName, 300
```

- Finally, save the file.
- If need be, you can change the status of the **statelessAlerts** flag by reconfiguring the test in the eG administrative interface.

Note:

- Since alerts will be closed after every measurement period, alarm escalation will no longer be relevant for tests that have **statelessAlerts** set to **yes**.
- For tests with **statelessAlerts** set to **yes**, **statelessAlerts** will apply for all measurements of that test (i.e., it will not be possible to only have one of the measurements with stateless alerts and others without).
- If **statelessAlerts** is set to **yes** for a test, an alarm will be opened during one measurement period (if a threshold violation happens) and will be closed prior to the next measurement period. This way, if a threshold violation happens in successive measurement periods, there will be one alarm per measurement period. This will reflect in all the corresponding places in the eG Enterprise system. For example, multiple alerts in successive measurement periods will result in multiple trouble tickets being opened (one for each measurement period). Likewise, the alarm history will also show alarms being opened during a measurement period and closed during the next measurement period.

3.5.14 Active Directory Computers Test

This test takes stock of the total number of computers managed by the AD server and the status of these computers, so that administrators can determine from a single glance which computers are inactive/unused.

Target of the test : An Active Directory or Domain Controller on Windows

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test Period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is *389*.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Never logged on computers	Indicates the number of computers to which no user has ever logged in.	Number	To know which computers are unused, use the detailed diagnosis of this measure. You can consider removing

Measurement	Description	Measurement Unit	Interpretation
			such computers to reduce the workload of the AD server.
Inactive computers	Indicates the number of computers that are currently inactive.	Number	To identify the inactive computers, use the detailed diagnosis of this measure. The detailed diagnosis displays the Distinguished Name of the computer, the age of the computer, and the date/time at which the computer was created. This will help you in figuring out how long that computer has been inactive. If the computer has been inactive for too long, you may think about deleting it from the AD server.
Disabled computers	Indicates the number of computers that are currently disabled on the AD server.	Number	To identify the disabled computers, use the detailed diagnosis of this measure. The detailed diagnosis displays the Distinguished Name of the computer and the date/time at which the computer was created.
Total computers	Indicates the total number of computers managed by the AD server.	Number	Use the detailed diagnosis of this measure to know the Distinguished Names of the computers.

3.5.15 Key Management Events Test

The Key Management Service (KMS) activates computers on a local network, eliminating the need for individual computers to connect to Microsoft. To do this, KMS uses a client–server topology. KMS client computers can locate KMS host computers by using Domain Name System (DNS) or a static configuration. KMS clients contact the KMS host by using remote procedure call (RPC). A KMS host responds to each valid activation request from a KMS client with the count of how many computers have contacted the KMS host for activation. Clients that receive a count below their activation threshold are not activated. If a computer running Windows Server 2008 or Windows Server 2008 R2 receives an activation count that is ≥5, it is activated. If a computer running Windows 7 receives an activation count ≥25, it is activated.

If users to a Windows server are having trouble logging on, administrators may want to check the **Key Management Service** event log to see if it is owing to an issue with KMS. This event log tracks events related to Kerberos key distribution, when a server functions as a key distribution center. To enable administrators to rapidly capture error/warning events captured by this event log and troubleshoot logon issues that occur, administrators can run the **Key Management Events** test. This test monitors the **Key Management Service** event log and reports the count and details of errors and warning events captured by that log.

Target of the test : An Active Directory server

Agent deploying the test : An internal agent

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

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The host for which the test is to be configured.
Port	Refers to the port used by the EventLog Service. Here it is *null*.
Logtype	Refers to the type of event logs to be monitored. By default, this is set to **Key Management Service**.
Policy Based Filter	Using this page, administrators can configure the event sources, event IDs, and event descriptions to be monitored by this test. In order to enable administrators to easily and accurately provide this specification, this page provides the following options: • Manually specify the event sources, IDs, and descriptions in the Filter text area, or, • Select a specification from the predefined filter policies listed in the Filter box For explicit, manual specification of the filter conditions, select the **No** option against the Policy Based Filter field. This is the default selection. To choose from the list of pre-configured filter policies, or to create a new filter policy and then associate the same with the test, select the **Yes** option against this field.
Filter	If the Policy Based Filter flag is set to **No**, then a Filter text area will appear, wherein you will have to specify the event sources, event IDs, and event descriptions to be monitored. This specification should be of the following format: *{Displayname}:{event_sources_to_be_included}:{event_sources_to_be_excluded}:{event_IDs_to_be_included}:{event_IDs_to_be_excluded}:{event_descriptions_to_be_included}:{event_descriptions_to_be_excluded}*. For example, assume that the Filter text area takes the value, *OS_events:all:Browse,Print:all:none:all:none*. Here:

Parameters	Description
	• OS_events is the display name that will appear as a descriptor of the test in the monitor UI; • all indicates that all the event sources need to be considered while monitoring. To monitor specific event sources, provide the source names as a comma-separated list. To ensure that none of the event sources are monitored, specify none. • Next, to ensure that specific event sources are excluded from monitoring, provide a comma-separated list of source names. Accordingly, in our example, Browse and Print have been excluded from monitoring. Alternatively, you can use all to indicate that all the event sources have to be excluded from monitoring, or none to denote that none of the event sources need be excluded. • In the same manner, you can provide a comma-separated list of event IDs that require monitoring. The all in our example represents that all the event IDs need to be considered while monitoring. • Similarly, the none (following all in our example) is indicative of the fact that none of the event IDs need to be excluded from monitoring. On the other hand, if you want to instruct the eG Enterprise system to ignore a few event IDs during monitoring, then provide the IDs as a comma-separated list. Likewise, specifying all makes sure that all the event IDs are excluded from monitoring. • The all which follows implies that all events, regardless of description, need to be included for monitoring. To exclude all events, use none. On the other hand, if you provide a comma-separated list of event descriptions, then the events with the specified descriptions will alone be monitored. Event descriptions can be of any of the following forms - desc*, or desc, or *desc*,or desc*, or desc1*desc2, etc. desc here refers to any string that forms part of the description. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters. • In the same way, you can also provide a comma-separated list of event descriptions to be excluded from monitoring. Here again, the specification can be of any of the following forms: desc*, or desc, or *desc*,or desc*, or desc1*desc2, etc. desc here refers to any string that forms part of the description. A leading '*' signifies any

Parameters	Description
	number of leading characters, while a trailing '*' signifies any number of trailing characters. In our example however, none is specified, indicating that no event descriptions are to be excluded from monitoring. If you use all instead, it would mean that all event descriptions are to be excluded from monitoring. **Note:** The event sources and event IDs specified here should be exactly the same as that which appears in the Event Viewer window. On the other hand, if the Policy Based Filter flag is set to **Yes**, then a Filter list box will appear, displaying the filter policies that pre-exist in the eG Enterprise system. A filter policy typically comprises of a specific set of event sources, event IDs, and event descriptions to be monitored. This specification is built into the policy in the following format: *{Policyname}:{event_sources_to_be_included}:{event_sources_to_be_excluded}:{event_IDs_to_be_included}:{event_IDs_to_be_excluded}:{event_descriptions_to_be_included}:{event_descriptions_to_be_excluded}* To monitor a specific combination of event sources, event IDs, and event descriptions, you can choose the corresponding filter policy from the Filter list box. Multiple filter policies can be so selected. Alternatively, you can modify any of the existing policies to suit your needs, or create a new filter policy. To facilitate this, a **Click here** link appears just above the test configuration section, once the **Yes** option is chosen against the Policy Based Filter. Clicking on the **Click here** link leads you to a page where you can modify the existing policies or create a new one. The changed policy or the new policy can then be associated with the test by selecting the policy name from the Filter list box in this page.
Events During Restart	By default, this flag is set to **Yes**. This ensures that whenever the agent is stopped and later started, the events that might have occurred during the period of non-availability of the agent are included in the number of events reported by the agent. Setting the flag to **No** ensures that the agent, when restarted, ignores the events that occurred during the time it was not available.
Stateless Alerts	Typically, the eG manager generates email alerts only when the state of a specific measurement changes. A state change typically occurs only when the threshold of a measure is violated a configured number of times within a specified time window. While this ensured that the eG manager raised alarms only when the problem was severe enough, in some cases, it may cause one/more problems to go unnoticed, just because they did not result in a state change. For example, take the case of the **EventLog** test. When this test captures an error event for the very first time, the eG

Parameters	Description
	manager will send out a critical email alert with the details of the error event to configured recipients. Now, the next time the test runs, if a different error event is captured, the eG manager will keep the state of the measure as critical, but will not send out the details of this error event to the user; thus, the second issue will remain hidden from the user. To make sure that administrators do not miss/overlook critical issues, the eG Enterprise monitoring solution provides the stateless alerting capability. To enable this capability for this test, set the stateless alerts flag to **Yes**. This will ensure that email alerts are generated for this test, regardless of whether or not the state of the measures reported by this test changes.
UseWMI	The eG agent can either use **WMI** to extract event log statistics or directly parse the event logs using event log APIs. If this flag is **Yes**, then **WMI** is used. If not, the event log APIs are used. This option is provided because on some Windows 2000 systems (especially ones with service pack 3 or lower), the use of WMI access to event logs can cause the CPU usage of the WinMgmt process to shoot up. On such systems, set this parameter value to **No**.
DDforInformation	eG Enterprise also provides you with options to restrict the amount of storage required for event log tests. Towards this end, the DDforInformation and DDforWarning flags have been made available in this page. By default, both these flags are set to **Yes**, indicating that by default, the test generates detailed diagnostic measures for information events and warning events. If you do not want the test to generate and store detailed measures for information events, set this flag to **No**.
DDforWarning	To ensure that the test does not generate and store detailed measures for warning events, set this flag to **No**.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying none against DD frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

Parameters	Description
	- The eG manager license should allow the detailed diagnosis capability - Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Key management event information messages	This refers to the number of information events that were captured by the Key Management Service log during the test's last execution.	Number	A change in value of this measure may indicate infrequent but successful operations. Please check the Key Management Service log in the Event Log Viewer for more details.
Key management event warnings	This refers to the number of warning events captured by the Key Management Service log during the test's last execution.	Number	A high value of this measure indicates problems that may not have an immediate impact, but may cause future problems. Please check the Key Management Service log in the Event Log Viewer for more details.
Key management event errors	This refers to the number of error events captured by the Key Management Service log during the test's last execution.	Number	A very low value (zero) is desired for this measure, as it indicates good health. An increasing trend or a high value indicates the existence of problems. Please check the Key Management Service log in the Event Log Viewer for more details.
Key management event critical errors	Indicates the number of critical events that were generated when the test was last executed.	Number	A critical event is one that the KMS cannot automatically recover from. **This measure is applicable only for Windows 2008/Windows Vista/Windows 7 systems.** A very low value (zero) indicates that

Measurement	Description	Measurement Unit	Interpretation
			the service is in a healthy state and is running smoothly without any potential problems. An increasing trend or high value indicates the existence of fatal/irrepairable problems. The detailed diagnosis of this measure describes all the critical events captured by the Key Management Service log during the last measurement period. Please check the Key Management Service log in the Event Log Viewer for more details.
Key management event verbose messages	Indicates the number of verbose events that were generated when the test was last executed.	Number	Verbose logging provides more details in the log entry, which will enable you to troubleshoot issues better. **This measure is applicable only for Windows 2008/Windows Vista/Windows 7 systems.** The detailed diagnosis of this measure describes all the verbose events that were captured by the Key Management Service log during the last measurement period. Please check the Key Management Service log in the Event Log Viewer for more details.

3.5.16 Active Directory Web Services Test

Active Directory Web Services (ADWS) in Windows Server 2008 R2 is a new Windows service that provides a Web service interface to Active Directory domains, Active Directory Lightweight Directory Services (AD LDS) instances, and Active Directory Database Mounting Tool instances that are running on the same Windows Server 2008 R2 server as ADWS. If the ADWS service on a

Windows Server 2008 R2 server is stopped or disabled, client applications, such as the Active Directory module for Windows PowerShell or the Active Directory Administrative Center will not be able to access or manage any directory service instances that are running on this server.

This is why, it is important that administrators are promptly alerted to critical error events and warning events pertaining to the ADWS. The **Active Directory Web Services** test does just that! This test scans the Active Directory Web Services event log for current and probable problems related to the ADWS, and brings the count and details of such problems to the notice of administrators.

Target of the test : An Active Directory server

Agent deploying the test : An internal agent

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

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The host for which the test is to be configured.
Port	Refers to the port used by the EventLog Service. Here it is *null*.
LogType	Refers to the type of event logs to be monitored. By default, this is set to **Active Directory Web Services**.
Policy Based Filter	Using this page, administrators can configure the event sources, event IDs, and event descriptions to be monitored by this test. In order to enable administrators to easily and accurately provide this specification, this page provides the following options: • Manually specify the event sources, IDs, and descriptions in the Filter text area, or, • Select a specification from the predefined filter policies listed in the Filter box For explicit, manual specification of the filter conditions, select the No option against the Policy Based Filter field. This is the default selection. To choose from the list of pre-configured filter policies, or to create a new filter policy and then associate the same with the test, select the **Yes** option against this field.
Filter	By default, the all filter policy is set for this test. This filter policy is pre-configured to monitor all events in the **Active Directory Web Services** log, regardless of the event source or event ID. If required, you can modify this filter policy definition by clicking the encircled '+' icon alongside the filter text area. Clicking on this icon leads you to a page

Parameters	Description
	where you can modify the all filter policy by specifying a different policy name and/or by by including/excluding specific event sources, event ids, and event descriptions in the **Active Directory Web Services** log. **Note:** The **Event sources** and **Event IDs** specified here should be exactly the same as that which appears in the Event Viewer window.
UseWMI	The eG agent can either use **WMI** to extract event log statistics or directly parse the event logs using event log APIs. If this flag is **Yes**, then **WMI** is used. If not, the event log APIs are used. This option is provided because on some Windows 2000 systems (especially ones with service pack 3 or lower), the use of WMI access to event logs can cause the CPU usage of the WinMgmt process to shoot up. On such systems, set this parameter value to **No**.
DDforInformation	eG Enterprise also provides you with options to restrict the amount of storage required for event log tests. Towards this end, the DDforinformation flag is made available in this page. By default, this flag set to **No**, indicating that by default, the test conserves space in the eG database by not generating and storing detailed measures for information events. If you want to view and analyze information events, then set the DDforinformation flag to **Yes**.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
AD web service information messages	This refers to the number of information events that were captured by the Active Directory Web Services log during the test's last execution.	Number	A change in value of this measure may indicate infrequent but successful operations. Please check the Active Directory Web Services log in the Event Log Viewer for more details.
AD web service warnings	This refers to the number of warning events captured by the Active Directory Web Services log during the test's last execution.	Number	A high value of this measure indicates problems that may not have an immediate impact, but may cause future problems. Please check the Active Directory Web Services log in the Event Log Viewer for more details.
AD web service errors	This refers to the number of error events captured by the Active Directory Web Services log during the test's last execution.	Number	A very low value (zero) is desired for this measure, as it indicates good health. An increasing trend or a high value indicates the existence of problems. Please check the Active Directory Web Services log in the Event Log Viewer for more details.
AD web service critical errors	Indicates the number of critical events that were generated when the test was last executed.	Number	A critical event is one that the ADWS cannot automatically recover from. **This measure is applicable only for Windows 2008/Windows Vista/Windows 7 systems.** A very low value (zero) indicates that the service is in a healthy state and is running smoothly without any potential problems. An increasing trend or high value indicates the existence of fatal/irrepairable problems.

Measurement	Description	Measurement Unit	Interpretation
			The detailed diagnosis of this measure describes all the critical events captured by the Active Directory Web Services log during the last measurement period. Please check the Active Directory Web Services log in the Event Log Viewer for more details.
AD web service verbose messages	Indicates the number of verbose events that were generated when the test was last executed.	Number	Verbose logging provides more details in the log entry, which will enable you to troubleshoot issues better. **This measure is applicable only for Windows 2008/Windows Vista/Windows 7 systems.** The detailed diagnosis of this measure describes all the verbose events that were captured by the Active Directory Web Services log during the last measurement period. Please check the Active Directory Web Services log in the Event Log Viewer for more details.

3.5.17 Group Policy Updater Test

Computers in a domain should be frequently updated with changes made to group policy settings. If a computer is not updated with changes made to **Computer Configuration Settings** and current **User Configuration Settings** in group policy, it can cause serious security lapses. To avoid this, administrators should manually update the computer and user policy settings on a target host at regular intervals. This is exactly what the **Group Policy Updater** test does.

At configured intervals, this test runs the *Gpudate* command to force a group policy update on the target host. By default, this command attempts to refresh both the **Computer Configuration Settings** and current **User Configuration Settings** on the local computer. Based on the output returned by the command, the test then reports whether/not the command succeeded in updating the target host's policy settings, and if so, whether both computer and user policy settings were updated in the process. This way, the test periodically alerts administrators to the use of obsolete policy settings. You can also use the detailed diagnosis of the test to determine why the update failed. This greatly aids troubleshooting efforts.

Target of the test : An Active Directory or Domain Controller on Windows

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
User policy status	Indicates whether/not the User policy settings were updated.		This measure reports the value Bad if the user policy update failed. The value Good is reported, if user policies were successfully updated. The numeric values that correspond to these measure values are listed below:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Bad</td><td>0</td></tr>
<tr><td>Good</td><td>1</td></tr>
</table>
<p>The detailed diagnosis of this measure will provide you with a status report. If the user policy update fails, you can use this report to figure out why the update failed.</p>
<p><b>Note:</b></p>
<p>By default, the test reports only the <b>Measure Value</b>s listed in the table above to indicate the update status. In the graph of this measure however, the update status is represented using the numeric equivalents only.</p>
</td></tr>
<tr><td>Computer policy status</td><td>Indicates whether/not the Computer policy settings were updated.</td><td></td><td>
<p>This measure reports the value Bad if the computer policy update failed. The value Good is reported, if computer policies were successfully updated.</p>
<p>The numeric values that correspond to these measure values are listed below:</p>
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Bad</td><td>0</td></tr>
<tr><td>Good</td><td>1</td></tr>
</table>
<p>The detailed diagnosis of this measure will provide you with a status report. If the computer policy update fails, you can use this report to figure out why the update failed.</p>
<p><b>Note:</b></p>
<p>By default, the test reports only the</p>
</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			Measure Values listed in the table above to indicate the update status. In the graph of this measure however, the update status is represented using the numeric equivalents only.

3.5.18 DC Locator Status Test

When an application requests access to Active Directory, an Active Directory server (domain controller) is located by a mechanism called the domain controller locator (DC Locator). Locator is an algorithm that runs in the context of the Net Logon service. Locator can find domain controllers by using DNS names (for IP or DNS-compatible computers) or by using Network Basic Input/Output System (NetBIOS) names, or it can be used on a network where IP transport is not available. If the DC Locator process/algorithm is unable to locate the domain controller, dependent applications will be denied access to Active Directory. This can cause application performance to suffer. To avoid this, administrators must periodically check whether/not the DC Locator process is able to locate the Active Directory server. This can be achieved using the **DC Locator Status** test.

Periodically, this test invokes the DC Locator algorithm/process to check whether/not it is able to locate the AD server being monitored. The success/failure of the DC location process is then reported.

Target of the test : An Active Directory

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates whether/not the DC locator process located the Active Directory server.	Percent	This measure reports the value 100 to indicate that DC location is successful. The value 0 is reported if DC location fails.

3.5.19 Group Policy Application Health Test

The application event log may capture several different issues that make up a category of warnings collectively called "1202 events" – i.e., events with the event ID 1202. Events of this category are typically related to group policy propogation. The common error codes under this category are as follows:

- **Error code 0x5 – Access is denied:** This issue occurs because of the locked-down security that was originally set on the FRS through Group Policy. When you attempt to configure the FRS through Group Policy, the policy engine no longer has the permission to set security on the FRS and does not attempt to take ownership of the FRS.
- **Error code 0xd – The data is invalid:** This behavior occurs because three system environment variables (%SYSVOL%, %DSDIT%, and %DSLOG%) are referenced in the Basicdc.inf file, but exist only during the Dcpromo process. These error messages are generated each time the Default Domain Controllers policy is applied.
- **Error code 0x3e5 - Overlapped I/O operation is in progress:** This problem can occur if a third-party, real-time backup product interferes with Active Directory operations.
- **Error code 0x534 - No mapping between account names and security IDs was done:** A program was installed, which creates user accounts and assigns rights to those user accounts. Later, the program was removed, the user accounts deleted, but the rights from policy before the accounts were still there. A user account is added and rights assigned to the account. The account is deleted, but not from security policies. The "0x534" code is the hex for "1332".
- **Error code 0x4b8 - An extended error occurred:** A conflict in Group Policy can cause these events to occur. These error messages can occur if the "Rename Administrator Account" security policy is enabled and then set to an account name that is already in use.

Using the **Group Policy Application Health** test, you can be instantly alerted if any of the aforesaid errors, which are categorized as '1202 events', is captured by the application event log.

Detailed diagnostics provided by the test will enable you to troubleshoot these errors. This way, issues in group policy application/propogation can be quickly captured and efficiently resolved.

Target of the test : An Active Directory

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.
Logtype	Refers to the type of event logs to be monitored. By default, this is set to *Application*.
Policy Based Filter	Using this page, administrators can configure the event sources, event IDs, and event descriptions to be monitored by this test. In order to enable administrators to easily and accurately provide this specification, this page provides the following options: • Manually specify the event sources, IDs, and descriptions in the Filter text area, or, • Select a specification from the predefined filter policies listed in the Filter box For explicit, manual specification of the filter conditions, select the **No** option against the Policy Based Filter field. To choose from the list of pre-configured filter policies, or to create a new filter policy and then associate the same with the test, select the **Yes** option against the Policy Based Filter field. Since this test is pre-configured with a filter policy definition, this flag is set to **Yes** by default.
Filter	For this test, the Filter is set to **all** by default. The **all** filter policy is pre-configured to monitor all event descriptions with the event source *SceCli* and event ID *1202*. Do not disturb this default setting.
UseWMI	The eG agent can either use **WMI** to extract event log statistics or directly parse the event logs using **event log API**s. If the UseWMI flag is **Yes**, then **WMI** is used. If not, the **event log API**s are used. This option is provided because on some Windows NT/2000 systems (especially ones with service pack 3 or lower), the use of WMI access to event logs can cause the CPU usage of the **WinMgmt** process to shoot up. On such systems, set the UseWMI parameter value to **No**. **On the other hand, when monitoring systems that are operating on any other flavor of Windows (say,**

Parameters	Description
	Windows 2003/XP/2008/7/Vista/12), the USEWMI flag should always be set to 'Yes'.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Status</td><td>Indicates whether/not events with ID 1202 occurred.</td><td></td><td>This measure reports the value Bad if the application log captures an 1202 event. On the other hand, the value Good is reported if the 1202 error event is not captured but the application log.
The numeric values that correspond to these measure values are as follows:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Bad</td><td>0</td></tr><tr><td>Good</td><td>1</td></tr></table></td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			Note: By default, the test reports the **Measure Value**s listed in the table above to indicate the status of group policy application. In the graph of this measure however, the same is indicated using the numeric equivalents only. The detailed diagnosis of this measure reports the complete details of the 1202 error events (if any) captured by the application log.

3.5.20 Group Policy Details Test

An active directory may contain organization units, groups, user accounts, group policy objects etc. To centrally manage all the components of the active directory, the directory services use different group policies. Group Policies are applied to users, groups and organizational units. Group Policy uses directory services and security group membership to provide flexibility and support extensive configuration information. Policy settings are specified by an administrator. This is in contrast to profile settings, that are specified by a user. Policy settings are created using the Microsoft Management Console (MMC) snap-in for Group Policy.

From an administrator's point of view, it is essential for the administrator to ensure that the components of the active directory are well-utilized. From time to time, administrators need to take stock on the organizational units, groups, user accounts etc. This will help administrators in identifying the user accounts that were inactive and the organizational units and groups that were empty. This exercise will help administrators in fine-tuning the active directory and retain the most sought organizational units and groups and identify active user accounts. The Group Policy Details test helps administrators in this regard!

This test tracks the number of organization units, groups and group policy objects in the target active directory environment. The organization units and groups that were empty are identified so that administrators can analyze whether/not to retain them. The inactive user accounts too are identified. The group policy objects that were disabled and empty are also quickly identified. By analyzing the measures provided by this test, administrators can scale the logical components such as organizational units, groups etc within the target active directory.

Target of the test : An Active Directory or Domain Controller on Windows

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is *389*.
Inactive Days	By default, the value specified against this parameter is 90 days. This implies that the user accounts in the domain controller or active directory will be considered as *inactive* after a period of 90 days.
Detailed Info	By default, this flag is set to **No**, indicating that by default, the test does not generate detailed measures for the measures, so as to conserve storage space. If you want the test to generate and store detailed measures for information events, set this flag to **Yes**.
Show Organizational Unit DD	By default, this flag is set to **No**. Accordingly, this test, by default, will not report detailed diagnostics for the *Organizational units* and *Empty organizational units* measures. To view the list of Organization units and empty Organizational Units on the domain controller or active directory, set this flag to Yes.
Show Group DD	By default, this flag is set to **No**. Accordingly, this test, by default, will not report detailed diagnostics for the *Groups* and *Empty Groups* measures. To view the list of groups and empty groups in the domain controller or active directory, set this flag to **Yes**.
Group Name	Specify the name of the active directory group for which the test should report metrics. By default, *none* is specified against this parameter indicating that this test will report metrics for all the active directory groups, by default.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option.

Parameters	Description
	The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Organizational units	Indicates the total number of organizational units on the domain controller being monitored.	Number	Organizational Unit (OU) is a container in Active Directory domain that can contain different objects from the same AD domain: other containers, groups, user and computer accounts. Active Directory OU is a simple administrative unit within a domain on which an administrator can link Group Policy objects and assign permissions to another user. The detailed diagnosis of this measure if enabled, lists the organization units, the date on which the OUs were created, the date on which the OUs were modified, the objects associated with the OUs, the flag operation and the version.
Empty organizational units	Indicates the number of organizational units that are empty on the domain controller.	Number	The detailed diagnosis of this measure if enabled, lists the organization units that were empty, the date on which the OUs were created, the date on which the OUs were modified, the objects associated with the OUs, the flag operation and the version.
Groups	Indicates the number of groups on the domain controller being monitored.	Number	The Active Directory groups is a collection of Active Directory objects. The group can include users,

Measurement	Description	Measurement Unit	Interpretation
			computers, other groups and other AD objects. The administrator manages the group as a single object. The detailed diagnosis of this measure if enabled, lists the groups, the date on which the groups were created, the date on which the groups were modified, the objects associated with the groups, flag operation and the version.
Empty groups	Indicates the number of groups that are empty on the domain controller.	Number	The detailed diagnosis of this measure lists the groups that were empty, the date on which the group was created, the date on which the group was modified, the objects within the group, flag operation and version.
Inactive user accounts	Indicates the number of user accounts that are inactive beyond the number of days configured against the Inactive Days parameter.	Number	A high value for this measure indicates that many users are inactive. Administrators can drill down the detailed diagnosis to identify the user accounts that were inactive and remove them as and when, necessary. The detailed diagnosis also lists whether the user account is enabled, whether the password expired for the user account, the last login date of the user, the objects associated with the user, flag operation and version.
Group policy objects	Indicates the number of group policy objects available on the domain controller being monitored.	Number	A Group Policy Object (GPO) is a virtual collection of policy settings. Group Policy settings are contained in a GPO. A GPO can represent policy settings in the file system and in the Active Directory.
Disabled group	Indicates the number of	Number	The detailed diagnosis of this measure

Measurement	Description	Measurement Unit	Interpretation
policy objects	group policy objects that were disabled on the domain controller.		lists the name of the group policy objects that were disabled, the category ID, name of the owner, the date on which the GPOs were modified, the flag operation and version.
Empty group policy objects	Indicates the number of group policy objects that were empty on the domain controller.	Number	The detailed diagnosis of this measure lists the name of the group policy objects that were empty, the name of the owner, the date on which the GPOs were created, the PS object name, the flag operation and version.
Unlinked group policy objects	Indicates the number of group policy objects that were not linked to any site, domain or active directory containers.	Number	The detailed diagnosis of this measure lists the name of the group policy objects that were not linked, the name of the owner, name of the owner, the date on which the GPOs were modified, the flag operation and version.
Inactive group policy objects	Indicates the number of group policy objects that were inactive on the domain controller.	Number	Administrators can drill down the detailed diagnosis to figure out the group policy objects that were inactive.
Group policy objects with no settings enabled	Indicates the number of group policy objects on which policy settings are disabled.	Number	The detailed diagnosis of this measure lists the name of the GPOs on which settings are disabled, the date on which the GPOs were created, the date on which the GPOs were modified, the account name, the PS object name, the flag operation and the version.
Group memberships changed	Indicates the number of group memberships that were changed on the domain controller.	Number	The detailed diagnosis of this measure lists the distinguished name of the group, the created date, the modified date, account name, PS object name, flag operation and version.

3.5.21 Security Group Management Test

Groups are used to collect user accounts, computer accounts, and other groups into manageable units. Working with groups instead of with individual users helps simplify network maintenance and administration.

Group scope normally describes the type of users that should be clubbed together in a way that is easy for their administration. Therefore, groups play an important part in domain. One group can be a member of other group(s), which is known as Group nesting. One or more groups can be members of any group in the entire domain(s) within a forest. The different types of group scopes are as follows:

- **Domain Local Group:** Use this scope to grant permissions to domain resources that are located in the same domain in which the domain local group was created. Domain local groups can exist in all mixed, native, and interim functional level of domains and forests. Domain local group memberships are not limited as users can add members as user accounts and universal and global groups from any domain. Nesting cannot be done in a domain local group. A domain local group will not be a member of another Domain Local or any other groups in the same domain.
- **Global Group:** Users with similar functions can be grouped under global scope and can be given permission to access a resource (like a printer or shared folder and files) available in local or another domain in the same forest. Simply put, global groups can be used to grant permissions to gain access to resources that are located in any domain but in a single forest as their memberships are limited. User accounts and global groups can be added only from the domain in which the global group is created. Nesting is possible in Global groups within other groups as users can add a global group into another global group from any domain.They can be members of a Domain Local group to provide permission to domain specific resources (like printers and published folder). Global groups exist in all mixed, native, and interim functional level of domains and forests.
- **Universal Group Scope:** These groups are precisely used for email distribution and can be granted access to resources in all trusted domains. Universal group memberships are not limited like global groups. All domain user accounts and groups can be a member of a universal group. Universal groups can be nested under a global or Domain Local group in any domain.

Administrators may want to be alerted whenever a group/member is created, modified, or deleted, as such changes may sometimes trigger performance or operational changes. For instance, changes in the membership of Universal groups will impose global catalog replication throughout an entire enterprise. Also, changes in group configuration, if performed carelessly, can pose a serious security threat, as it may allow malicious users access to critical directory resources. This is why, it is important that administrators periodically run the **Security Group Management** test. This test keeps track of changes made to groups and members, and promptly notifies administrators when such changes are made. Moreover, the detailed diagnosis of the test also reveals the details of the changes – for instance, if a global group is created, then detailed metrics provided by the test indicate which group was created and which user created the group. This enables administrators to determine whether/not the change was made by an authorized user.

Target of the test : An Active Directory

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Universal group created	Indicates the number of universal groups created during the last measurement period.	Number	The detailed diagnosis of this measure reveals the universal groups that were newly created and the user who created each group.
Universal group changed	Indicates the number of universal groups that were changed during the last measurement period.	Number	The detailed diagnosis of this measure reveals the universal groups that were changed and the user who made the change.
Universal group deleted	Indicates the number of universal groups that were deleted during the last measurement period.	Number	The detailed diagnosis of this measure reveals the universal groups that were deleted and the user who deleted the group.
Member added to universal group	Indicates the number of members added to universal groups during the last measurement period.	Number	The detailed diagnosis of this measure reveals the universal groups to which members were added and the user who added the members.
Member removed from universal group	Indicates the number of members removed from universal groups during the last measurement period.	Number	The detailed diagnosis of this measure reveals the universal groups from which members were removed and the user who removed the members.
Global group created	Indicates the number of global groups created during the last measurement period.	Number	The detailed diagnosis of this measure reveals the global groups that were newly created and the user who created each group.
Global group changed	Indicates the number of global groups that were changed during the last measurement period.	Number	The detailed diagnosis of this measure reveals the global groups that were changed and the user who made the change.
Global group deleted	Indicates the number of global groups that were deleted during the last measurement period.	Number	The detailed diagnosis of this measure reveals the global groups that were deleted and the user who deleted each group.
Member added to global group	Indicates the number of members added to global groups during the last	Number	The detailed diagnosis of this measure reveals the global groups to which members were added and the user

Measurement	Description	Measurement Unit	Interpretation
	measurement period.		who added the members.
Member removed from global group	Indicates the number of members removed from global groups during the last measurement period.	Number	The detailed diagnosis of this measure reveals the global groups from which members were removed and the user who removed the members.
Local group created	Indicates the number of local groups created during the last measurement period.	Number	The detailed diagnosis of this measure reveals the local groups that were newly created and the user who created each group.
Local group changed	Indicates the number of local groups that were changed during the last measurement period.	Number	The detailed diagnosis of this measure reveals the local groups that were changed and the user who made the change.
Local group deleted	Indicates the number of local groups that were deleted during the last measurement period.	Number	The detailed diagnosis of this measure reveals the local groups that were deleted and the user who deleted each group.
Member added to local group	Indicates the number of members added to local groups during the last measurement period.	Number	The detailed diagnosis of this measure reveals the local groups to which members were added and the user who added the members.
Member removed from local group	Indicates the number of members removed from local groups during the last measurement period.	Number	The detailed diagnosis of this measure reveals the local groups from which members were removed and the user who removed the members.

3.5.22 Software and Service Installation Test

Changes made to the configuration of the Windows system that hosts the Active Directory server – eg., installation of new drivers/software/services, application of Windows updates, etc. – can impact the performance of the server. This in turn can adversely impact the overall health and uptime of mission-critical applications and business services that rely on the Active Directory server. It is hence the responsibility of the AD administrator to keep an eye out for such system-level configuration changes, analyse their impact as and when they occur, and decide whether/not to rollback the changes. The **Software and Service Installation** test helps administrators in this exercise.

This test promptly alerts administrators to crucial configuration changes – eg., loading of new drivers, installation of new Windows services/applications/packages/updates, etc. – on the Active Directory host. Using the detailed diagnostics reported by the test, administrators can also clearly understand the nature of these changes. In the light of the detailed change information provided by this test, administrators can perform effective impact analysis of the change.

Target of the test : An Active Directory

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
New kernel filter driver loaded and registered	Indicates the number of kernel filter drivers that were newly loaded and registered.	Number	The detailed diagnosis of this measure reveals the kernel filter drivers that were loaded and registered and the user responsible for the same.
New Windows services installed	Indicates the number of Windows services that were newly installed.	Number	The detailed diagnosis of this measure reveals the Windows services that were installed recently and the user who installed them.
New MSI files installed	Indicates the number of MSI files that were newly installed.	Number	The detailed diagnosis of this measure reveals the MSI files that were installed recently and the user who installed them.
New applications installed	Indicates the number of applications that were newly installed.	Number	The detailed diagnosis of this measure reveals the applications that were installed recently and the user who installed them.
Updated applications	Indicates the number of applications that were updated during the last measurement period.	Number	The detailed diagnosis of this measure reveals the applications that were updated recently and the user who updated them.
Removed applications	Indicates the number of applications that were removed during the last measurement period.	Number	The detailed diagnosis of this measure reveals the applications that were removed recently and the user who uninstalled them.
Updated packages installed	Indicates the number of updated packages installed during the last measurement period.	Number	The detailed diagnosis of this measure reveals the packages that were installed recently and the user who installed them.
Windows updates installed	Indicates the number of Windows updates that were installed during the last measurement period.	Number	The detailed diagnosis of this measure reveals the Windows updates that were installed recently and the user who installed them.

3.5.23 Windows Firewall Test

If the Windows firewall rules of the Active Directory server are changed – i.e., are added, modified, or removed – it can impact accesses to and from the server. This is why, it is important that such critical changes are tracked and vetted. For this purpose, administrators can take the help of the **Windows Firewall** test. This test brings Windows Firewall configuration changes to the immediate notice of administrators, reports what has changed, and also reveals who made the change. This enables administrators to rapidly isolate unauthorized / unnecessary changes. In addition, the test also captures and reports firewall rules that failed to load the group policy, so that administrators can troubleshoot the failure.

Target of the test : An Active Directory

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability

Parameters	Description
	• Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Firewall rule added	Indicates the number of firewall rules that were added during the last measurement period.	Number	The detailed diagnosis of this measure reveals the firewall rules that were added and the user who added them.
Firewall rule changed	Indicates the number of firewall rules that were changed during the last measurement period.	Number	The detailed diagnosis of this measure reveals the firewall rules that were changed and who changed them.
Firewall rule deleted	Indicates the number of firewall rules that were deleted during the last measurement period.	Number	The detailed diagnosis of this measure reveals the firewall rules that were deleted and the user who deleted them.
Firewall rule failed to load group policy	Indicates the number of firewall rules that failed to load the group policy during the last measurement period.	Number	The detailed diagnosis of this measure reveals the firewall rules that failed to load the group policy.

3.5.24 Event Log Cleared Status Test

Administrators rely on event logs to capture and troubleshoot errors and warning events that occur on an Active Directory server. This is why, if a user inadvertently or wilfully clears an event log, many critical problem conditions may go unnoticed! Under such circumstances, it is only natural that administrators want to find out who cleared the logs, so that that user can be pulled up for questioning. The **Event Log Cleared Status** test helps with this. This test promptly alerts administrators if an application, system, or event log gets cleared. The detailed diagnosis of the test also points administrators to the user who cleared the log, thus assisting investigation.

Target of the test : An Active Directory

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Application/System event log cleared	Indicates the number of times the application and/or system event log was cleared during the last measurement period.	Number	The detailed diagnosis of this measure reveals when and who cleared the application/system event log.
Security event log cleared	Indicates the number of	Number	The detailed diagnosis of this measure

Measurement	Description	Measurement Unit	Interpretation
	times the security event log was cleared during the last measurement period.		reveals when and who cleared the security event log.

3.5.25 Registry Management Test

Typically, changes to the Windows Registry have to be carried out carefully, and on a need-only basis. If such changes are wrongly done, particularly on a mission-critical server such as the Active Directory server, they can adversely impact the availability, operations, and performance of the server. AD administrators therefore need to have their eyes open for registry changes, capture such changes as and when they occur, and find out what changed and who did it. To achieve this, administrators can use the **Registry Management** test.

This test tracks registry changes on the AD server and notifies administrators when such changes are made. The detailed diagnostics of the test additionally describes the registry entry that was changed and the user who made the change. With the help of this information, administrators can figure out whether/not the change was valid and was done by an authorized person.

Target of the test : An Active Directory

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory site that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.

Parameters	Description
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Registry value changed	Indicates the number of times during the last measurement period registry values were changed.	Number	The detailed diagnosis of this measure describes the change and points administrator to the user who made the change.

3.5.26 External Media Detection Test

This test instantly alerts administrators if any external media device, such as a USB mass storage device, is plugged into the AD server host. Detailed diagnostics reported by the test reveal the device and the user using it. This information is very useful in high-security environments, where the use of external media devices is strictly prohibited or is allowed only for authorized personnel.

Target of the test : An Active Directory or Domain Controller

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the Active Directory server being monitored

Configurable parameters for the test

Parameters	Description
Test period	This indicates how often should the test be executed.
Host	The IP address of the machine where the Active Directory is installed.
Port	The port number through which the Active Directory communicates. The default port number is 389.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
New storage mass installation	Indicates the number of times during the last measurement period a USB mass storage device was plugged into the server.	Number	The detailed diagnosis of this measure indicates which storage device was plugged in and by who.

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.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of eG Innovations. eG Innovations 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. The information contained in this document is subject to change without notice.

All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of eG Innovations. All trademarks, marked and not marked, are the property of their respective owners. Specifications subject to change without notice.