Monitoring Windows Domain Controller

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Windows Domain Controllers are critical components of IT infrastructures. Users accessing resources in a Windows domain have to first be authenticated by the Domain Controller in order to get access. Any slowdown or failure of the domain controllers can severely impact users. Hence, 24x7 monitoring of domain controllers is critical.

To achieve this, eG Enterprise provides a specialized Domain Controller monitoring model for the Windows domain controller (DC) using which key performance parameters related to the DC can be continuously monitored, and anomalies, instantly detected.

Chapter 2: Monitoring Windows Domain Controllers

Windows Domain Controllers are critical components of IT infrastructures. Users accessing resources in a Windows domain have to first be authenticated by the Domain Controller in order to get access. Any slowdown or failure of the domain controllers can severely impact users. Hence, 24x7 monitoring of domain controllers is critical.

The eG Enterprise suite provides a specialized Domain Controller monitoring model for the Windows domain controller (DC) (see Figure 2.1), using which key performance parameters related to the DC can be continuously monitored, and anomalies, instantly detected.

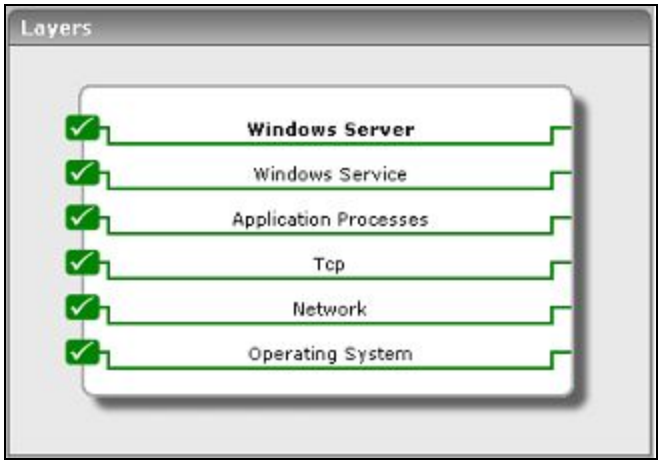

Figure 2.1: Layer model of a Windows Domain Controller

Each of the layers in this specialized model (see Figure 2.1) executes a wide variety of tests on the DC and extracts critical metrics, which help quantify the performance level achieved by the DC, and simplifies problem identification.

The *Monitoring Unix and Windows Servers* document deals extensively with the bottom 5 layers of Figure 2.1. In the section that follows, the **Windows Server** layer will be discussed.

2.1 The Windows Server Layer

Using the tests associated with this layer, administrators can gauge how effectively the DC authenticates login requests it receives.

Figure 2.2: Tests associated with the Windows Server layer

2.1.1 Windows Access Test

This test monitors the accesses to a Windows server.

Target of the test : A Windows Domain Controller

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Windows 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	The port at which the Windows server listens to.

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	Reqs/sec	If the number of blocking request rejects is high, you may need to adjust the MaxWorkItem or MinFreeWorkItems server parameters

Measurement	Description	Measurement Unit	Interpretation
	insufficient count of free work items		
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 measurement period.	Number	Unexpected errors usually indicate a problem with the server.
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	Secs	This is a critical measure of server

Measurement	Description	Measurement Unit	Interpretation
	the server to respond to client requests		health.

2.1.2 Windows Sessions Test

This test reports various session-related statistics for a Windows server.

Target of the test : A Windows Domain Controller

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Windows 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	The port at which the Windows server listens to.

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

Measurement	Description	Measurement Unit	Interpretation
			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

2.1.3 Window Authentication Test

This test emulates a user logging into a Windows domain or local host and reports whether the login succeeded and how long it took.

Target of the test : A Windows Domain Controller

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every user account 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	The port at which the Windows server listens to.
Username and Password	This test emulates a user logging into a domain controller at the system-level. Therefore, specify the credentials of a user with both interactive logon and logon locally privileges against the Username and Password fields
Confirm Password	Confirm the password by retyping it here.
Domain	Specify the name of the domain to which the test will try to login. If the test is to login to a local host, specify '*none*' here. **Note:** If users are spread across multiple domains, then, you can configure this test with multiple domain specifications; in this case, for every domain, a user-password pair might also have to be configured. Sometimes, you might want the test to login as specific users from the same domain, to check how long each user login takes. Both these scenarios require the configuration of multiple domains and/ormultiple user names and passwords. In order to enable users to specify these details with ease, eG Enterprise provides a special page; to access this page, click on the **Click here** hyperlink at the top of the parameters in the test configuration page. To know how to use this page, refer to the *Configuring Multiple Users for the Citrix Authentication Test* section in the *Monitoring Citrix Environments* document.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Authentication status	Indicates whether the login was successful or not	Percent	A value of 100 % indicates that the login has succeeded. The value 0 is indicative of a failed login.

Measurement	Description	Measurement Unit	Interpretation
Authentication time	Indicates the time it took to login	Secs	If this value is very high then it could be owing to a configuration issue (i.e. the domain might not be configured properly) or a slow-down/unavailability of the primary domain server.

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.