Quest® Active Administrator® 8.1

Web Console User Guide

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT NOTE, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Active Administrator Web Console User Guide
Updated - February 2017
Software Version - 8.1

Contents

1

Active Administrator Web Console Overview

About the Web Console

Active Administrator® Web Console extends the functionality of the built-in Windows® management tools for Active Directory® by allowing administrators to view and manage security in a much more extensible interface. You can open Active Administrator Web Console on a variety of devices in the following browsers:

- Microsoft® Internet Explorer 11
- Google Chrome™ 47
- Mozilla® Firefox® 44

The Active Directory Health dashboard is where you can monitor the overall health of your organization. From the dashboard, you can view Alerts, set up Notifications, run Health checks, and generate Reports. The Active Directory Topology viewer lets you monitor alerts while viewing a customizable topology diagram of your organization.

To keep you apprised of activity in Active Administrator Web Console, toast notifications appear in the lower corner of the display to inform you of success (green), information (blue), warnings (gold), and critical situations (red). You can close the toast or let them fade on their own.

Topics:

Configuring the web server

By default, the port used by the web server is 8080. You can change the port used by the web server and the logging settings.

By default, HTTP logging is enabled, and 7 days of logs are saved. A new log file is created each day and the logs are stored in the server logging directory in the WebLogs folder.

IMPORTANT: It is recommended that you only use the Web Console internal to the network. If you want to use the Web Console externally, use HyperText Transfer Protocol Secure (HTTPS) by enabling Secure Sockets Layer (SSL). You need to select a certificate, which must be installed in the Personal or My store on the local computer. The default port is 9443.

To configure the web server

1. From the **Start** menu, open AA **Server Manager**.
2. Click **Configure**.
3. Enter the port number, if desired. The default port is 8080.
4. HTTP logging is enabled by default. To disable logging, clear the check box.
5. Change the number of days HTTP log files are retained, if desired. The default is 7 days.
6. To enable SSL, select the check box, and browse for a certificate. The default port is 9443.

   NOTE: The certificate must be installed in the Personal or My store on the local computer.

7. Use the buttons to view information about the SSL binding and the selected certificate.

   Table 1. Web Server Configuration options

Option	Description
View HTTP Binding	Opens the **SSL Certificate Binding** window.
View Certificate	Opens the **Certificate** dialog where you can view details about the certificate and the certificate path.
Clear Certificate	Clears the certificate from the **Certificate** box.

8. Click **Apply** or **OK**.

   NOTE: When you click **OK**, the ports are checked to see if they are in use. For example, if the server is running a web server such as IIS, and you enter server port 80, you will receive an error because IIS is already using port 80.

Opening Active Administrator in a web browser

1. Open a web browser. Supported browsers include:
   - Microsoft® Internet Explorer 11
   - Google Chrome™ 47
   - Mozilla® Firefox® 44
2. In the address box, enter the fully qualified domain name of the computer on which Active Administrator® is installed, followed by a colon and the port used by the web service.

   For example, if the domain name is **contoso.com**, and the name of the computer running Active Administrator is **AA-server**, you would enter **http://aa-server.contoso.com:8080**.

3 Enter the username and password of an account with administrative rights on the domain where Active Administrator is installed.

4 Click **Log in**.

The Active Administrator dashboard opens. See Using the Active Administrator dashboard.

Using the Active Administrator dashboard

The Active Administrator® dashboard displays panels that provide you an overview of various components of Active Administrator. Each panel is configurable. You can choose to disable a panel, which removes it from the display. Within each panel, you can choose to hide or show various data elements. All panels are enabled by default and all elements within each panel are selected by default. Each user can configure the dashboard to suit their needs. The settings are stored with the user profile.

Topics:

- Displaying the dashboard
- Arranging the dashboard panels
- Setting refresh and rotation
- Configuring dashboard panels

Displaying the dashboard

The dashboard displays when you first open Active Administrator® in a web browser. To return to the dashboard, click **Active Administrator** in the page header.

You can set the panels to cycle through automatically, which can be helpful when viewing the dashboard on a hand-held device. This feature is off by default. When you turn on the feature, you can click ❚❚ to pause the cycle to focus on a panel for more consideration. When you are done, click ▶ to restart.

To set the panels to cycle

1 Click ⚙.

2 Select **Cycle dashboard panels**.

3 Set the cycle rate. The default is 10 seconds.

4 Click **Save**.

Arranging the dashboard panels

By default, all panels are enabled. You can disable a panel to remove it from the display. You also can change the order of the panel display.

To disable panels

1 Click ⚙.

2 Locate the panel, and clear the **Enabled** check box.

3 Click **Save**.

To arrange the panels

1 Click .

2 In the **Order** area, select a panel.

3 Click **Move Up** or **Move Down** to change the order.

4 Click **Save**.

Setting refresh and rotation

Each dashboard pane has a refresh rate that you can set. You can manually refresh a panel by clicking .

Some panels display a number of items that rotate in the display based on the number of items you select to display and the rotation rate. For example, if you select to display 10 Active Directory Health alerts in Dashboard Settings, the alerts display 10 at a time in the dashboard panel and rotate to the next time based on the rotation time you set.

To set the rates, click and set the rotation and refresh rates. The footer for each panel displays the rotation and refresh rates and includes a sliding scale that you can use to adjust the rates.

Configuring dashboard panels

In addition to showing or hiding panels on the dashboard, you also can show or hide components within each dashboard panel. You also can set the rotation and refresh rates for each panel. See Setting refresh and rotation. The settings are saved for each user in their user profile, so each user can create a dashboard specifically to meet their needs.

To configure the dashboard panels

1 Click .

2 Select to show or hide elements in a panel; set refresh and rotation rates; add or remove forests, domains, and domain controllers.

Table 2. Dashboard panels

Dashboard panel	Description
Active Directory Health	Displays an overview of active alerts. The specified number of active alerts display in a scrollable list that rotates at the specified rate. **Show or hide:** • active alert count • active alert summary • active alerts **Rotation:** • Enter number of active alerts to display in rotation.
Active Template Delegation	**Show or hide:** • broken delegation count • delegation status • active template summary
Active Directory Health Check	**Show or hide:** • running health checks • recently completed reports

Table 2. Dashboard panels

Dashboard panel	Description
Forests and Domains	A panel displays for each forest. Each domain in the forest displays on rotation. ***To add a forest*** 1 Click **Add**. 2 Type the name of the forest. 3 Click **Add**. 4 Click **Close**. ***To remove forests*** 1 Select the forests to remove. 2 Click **Remove**.
Active Directory Account Management	Displays locked out accounts for each domain on rotation. Displays number of inactive and expired accounts. Indicates number of times change password reminder has run. **Show or hide:** • Locked out account details • Inactive accounts. • Change password reminder • Account expiration
Certificates	Displays four servers on rotation.
Azure Active Directory Domains	Displays four Azure® Active Directory® domains on rotation.
Domain Controllers	Displays each selected domain controller on rotation. ***To add a domain controller*** 1 Click **Add**. 2 Type the name of the domain controller. 3 Click **Add**. 4 Click **Close**. ***To remove domain controllers*** 1 Select the domain controllers to remove. 2 Click **Remove**. **NOTE:** You can run the Domain Controllers report to get a list of the domain controller names in a given domain. See Active Directory Health reports.

3 Click **Save**.

2

Active Directory Health

About Active Directory Health

Active Directory Health displays read-only real-time data about forests, sites, domains and domain controllers so you can monitor the health of your organization.

IMPORTANT: The Active Directory Health license is required.

NOTE: The Directory Analyzer agent must be monitoring at least one domain controller. See **Managing monitored domain controllers** and **Installing Directory Analyzer agents** in the *Quest*® Active Administrator® *User Guide*.

Using the Active Directory Health landing page

Once you have installed at least one Directory Analyzer agent, the **Active Directory Health** landing page displays summary information for forests, domains, sites, domain controllers, and alerts. Tiles display summary information for each domain that is configured in Active Administrator®.

To access the Active Directory Health landing page

1. Open Active Administrator in a web browser. See Opening Active Administrator in a web browser.
2. Select **Monitor | Active Directory Health**.
3. Open the **Summary** tab, if necessary.

   The landing page is divided into three sections.

Summary area

The **Summary** area displays a summary of the forests, domains, sites, and domain controllers.

Table 1. Summary area

Object	Description
Forest	Number of forests being monitored.
Domains	Number of domains in the forest, including domains not being monitored.
Domain controllers	Number of domain controllers in the forest, including domain controllers not being monitored.
Agents	Number of installed agents.
Monitored DCs	Number of monitored domain controllers.
Global catalog servers	Number of global catalog servers in all domains.
RODCs	Number of read-only domain controllers (RODCs) in all domains.
Sites	Number of sites in all forests.
Bridgehead servers	Number of bridgehead servers in all sites.
Unmonitored DCs	Number of unmonitored domain controllers.
All agents running All schema versions consistent All schema masters consistent All naming masters consistent All PDC masters consistent All infrastructure masters consistent All RID masters consistent All functional levels consistent	Indicates the status of the object in all forests and domains. If one object has a problem, the status becomes No.

Alerts Summary

The **Alerts Summary** area indicates the total number of critical and warning alerts for the forest. The chart shows alert history over the past 12 hours. If you pause the cursor over the graph, you can view the number of critical, and warning alerts that were triggered or created during the hour, and the number of active alerts that occurred during the hour.

Summary of Domains

The **Summary of Domains** area displays details for each domain being monitored by Active Administrator. The tile for each domain indicates the total number of critical and warning alerts; the total number of domain controllers, global catalog servers, and read-only domain controllers; and the functional level of the domain.

Table 2. Summary of Domains area

Object	Description
Domain controllers	Number of domain controllers in the forest, including domain controllers not being monitored.
Global catalog servers	Number of monitored global catalog servers in all domains.
RODCs	Number of monitored read-only domain controllers (RODCs) in all domains.
Functional level	The Active Directory® domain functional level.

Analyzing health of a domain controller

You can view information on all monitored domain controllers or a selected monitored domain controller.

To analyze health on a selected domain controller

1. Open Active Administrator® in a web browser. See Opening Active Administrator in a web browser.
2. Select **Monitor | Active Directory Health**.
3. Open the **Analyzer** tab.
4. Select the domain controller from the **Monitored Object** list.

   NOTE: A message displays if there is no data to display. There may be a pending workload evaluation or the system is waiting on data from the Directory Analyzer agent. Check to see if the Directory Analyzer agent is running. See **Managing Directory Analyzer agents** in the *Quest® Active Administrator® User Guide*.

   If there is no data because the domain controller is not being monitored, you need to install the agent. See **Installing Directory Analyzer agents** in the *Quest® Active Administrator® User Guide*.

   Data collectors provide the input to the various tabs. Some data collectors can be enabled or disabled. See **Managing data collectors** in the *Quest® Active Administrator® User Guide*.

   If you do not see the corresponding data, make sure the data collector is enabled and the necessary permissions are set. To check the required minimum permissions, see the **Alerts Appendix** in the *Quest® Active Administrator® User Guide*.

   The remaining data collectors used to provide information to the tabs are not available for management and are provided to Active Administrator through Windows Management Instrumentation (WMI).

   The **Domain Controller** window has a summary area and seven tabs: Performance Overview tab, Services tab, Server tab, Active Directory tab, Domain Controller Alerts tab, Installed Applications tab, and Updates tab. The number on the tab indicates the number of items on each tab.

Domain Controller summary

The **Domain Controller** summary area displays the name of the domain controller, the number of active alerts for the domain controller, and general information about the domain controller.

Table 3. Domain Controller general information

Field	Description
Domain	Name of the domain in which the domain controller resides
Site	Name of the site in which the domain controller resides
Forest	Name of the forest in which the domain resides
OS version	Version of the operating system
System up time	Duration of time the domain controller has been running
Read only DC	Indicates if the domain controller is a read-only domain controller (RODC)
Global catalog	Indicates if the domain controller is a global catalog server
Monitored by	Name of the computer on which the agent is installed that is monitoring the selected domain controller.
Last updated	Date and time the domain controller was last updated

Performance Overview tab

The **Performance Overview** tab displays the data collected in the indicated time frame for the selected monitored domain controller via the enabled Performance Counters data collectors.

- To view more detail, click **Show Trends**.
- To hide the detail, click **Hide Trends**.
- To refresh the display, click **Refresh**.

Services tab

The **Services** tab displays the status of Windows® services via the enabled Windows Services data collectors. If a service is running, but has stopped at a point in time, that stoppage is indicated with red.

Server tab

Displays information about the logical disks on the domain controller and the network adapter via the following General data collectors:

- Domain controller time synchronization
- Logic disk details

Active Directory tab

Displays Active Directory® database and SYSVOL disk usage and LDAP response time via the following data collectors:

- Validation data collectors
- General data collectors:
  - Active Directory database details
  - Domain controller relative identifier (RID)
  - LDAP response time
  - SysVol details

Domain Controller Alerts tab

The number on the tab indicates the number of current alerts on the domain controller. The **Domain Controller Alerts** tab displays the current alerts for the domain controller. A count of the current alerts, critical and warnings, displays. For each active alert, the severity, alert name, time the alert triggered, the object name, and the description display.

- To sort the list, click on the column heading you want to sort.
- To refresh the list, click **Refresh**.

Alerts are enabled by default and correspond to data controllers. Both alerts and data collectors can be enabled and disabled. See **Setting alerts** and **Setting data collectors** in the *Quest*® Active Administrator® *User Guide*.

Installed Applications tab

The **Installed Applications** tab has three tabs with numbers that indicate the number of installed, added, or removed applications on the selected monitored domain controller.

- To sort the list, click on the column heading you want to sort.
- To refresh the list, click **Refresh**.

Updates tab

Displays installed updates on the selected monitored domain controller. Updates installed or removed in the last 24 hours are listed in a separate pane.

- To sort the list, click on the column heading you want to sort.
- To refresh the list, click **Refresh**.

Analyzing health of a domain

To analyze health on a selected domain

1. Open Active Administrator® in a web browser. See Opening Active Administrator in a web browser.
2. Select **Monitor | Active Directory Health**.
3. Open the **Analyzer** tab.
4. Select the domain from the **Monitored Object** list.

Domain Summary

The **Domain** summary area displays the name of the domain, the number of active alerts for the domain, and general information about the domain.

Table 4. Domain general information

Item	Description
Domain	Name of the selected domain.
Domain controllers	Number of domain controllers.
GC servers	Number of global catalog (GC) servers
RODC servers	Number of read-only domain controllers (RODCs)
Functional level	Functional level of the forest, domain, or site
PDC owner	Owner of the primary domain controller (PDC) Flexible Single Master Operation (FSMO) role
RID master	Owner of the relative identifier (RID) FSMO role
Infrastructure master	Owner of the infrastructure FSMO role
Operations master consistent	Indicates if all the domain controllers report the same operation masters
Functional level consistent	Indicates if all the domain controllers report the same functional level

Monitored Domain Controllers

Lists all the domain controllers in the selected domain, the domain and site in which the domain controller resides, and the number of alerts for each domain controller.

- To filter the list of domain controllers, type in the **Filter domain controllers** box. The list filters as you type.
- To refresh the tree, click **Refresh**.

Replication Latency tab

The number on the tab indicates the number of replication. The Replication Latency tab lists the replication latency times for a domain controller and its replication partners.

- To filter the list, type in the **Filter domain controllers** box. The list filters as you type.
- To sort the list, click on the column heading you want to sort.

- To refresh the list, click **Refresh**.

GC Replication Latency tab

The number on the tab indicates the number of GC replications. The **GC Replication Latency** tab lists the replication latency times for the domain controllers and servers hosting the global catalog.

- To filter the list, type in the **Filter domain controllers** box. The list filters as you type.
- To sort the list, click on the column heading you want to sort.
- To refresh the list, click **Refresh**.

Domain Alerts tab

The number on the tab indicates the number of current alerts on the domain. The **Domain Alerts** tab displays the current alerts for the domain. A count of the current alerts, critical and warnings, displays. For each active alert, the severity, alert name, time the alert triggered, the object name, and the description display.

- To sort the list, click on the column heading you want to sort.
- To refresh the list, click **Refresh**.

Analyzing health of a site

To analyze health on a selected site

1. Open Active Administrator® in a web browser. See Opening Active Administrator in a web browser.
2. Select **Monitor | Active Directory Health**.
3. Open the **Analyzer** tab.
4. Select the site from the **Monitored Object** list.

   The **Site** window has a summary area and three tabs: Servers tab, Site Links tab, and Site Alerts tab. The number on the tab indicates the number of items on each tab.

Site summary

The **Site** summary area displays the name of the site, the number of active alerts for the site, and general information about the site.

Table 5. Site summary area

Item	Description
Group caching enabled	Indicates if group caching is enabled or disabled.
Intersite topology generation	Indicates if intersite topology generation is enabled or disabled.
Intrasite topology generation	Indicates if intrasite topology generation is enabled or disabled.
Intersite topology generator	Name of the intersite topology generator.

Servers tab

The number on the tab indicates the total number of managed servers in the site. The **Servers** tab lists the monitored domain controllers in the selected site and indicates if the domain controller is:

- a global catalog (GC}
- a read-only domain controller (RODC)
- a bridgehead server
- a primary domain controller (PDC)

- an infrastructure master
- a relative identifier (RID) master
- Schema master
- Naming master

You can filter the list of domain controllers and sort the list.

- To filter the list, type in the **Filter servers** box. The list filters as you type.
- To sort the list, click on the column heading you want to sort.
- To refresh the list, click **Refresh**.

Site Links tab

The number on the tab indicates the total number of links in the site. The **Site Links** tab lists the site link name, the site to which the selected site is linked, the relative cost of using the link, as defined by the administrator.

The **Schedule** column indicates how the inter-site link is connected.

- **Always** indicates the link is connected all of the time as a schedule is not assigned.
- **Scheduled** indicates the link is connected occasionally on a schedule.
- **Disabled** indicates the link is never connected. A schedule is assigned to the connection, but there is no scheduled time when the link is connected.

You can filter the list of domain controllers and sort the list.

- To filter the list, type in the **Filter domain controllers** box. The list filters as you type.
- To sort the list, click on the column heading you want to sort.
- To refresh the list, click **Refresh**.

Site Alerts tab

The number on the tab indicates the number of current alerts on the site. The **Site Alerts** tab displays the current alerts for the site. A count of the current alerts, critical and warnings, displays. For each active alert, the severity, alert name, time the alert triggered, the object name, and the description display.

- To sort the list, click on the column heading you want to sort.
- To refresh the list, click **Refresh**.

Analyzing the health of a forest

To analyze health of the forest

1. Open Active Administrator® in a web browser. See Opening Active Administrator in a web browser.
2. Select **Monitor | Active Directory Health**.
3. Open the **Analyzer** tab.
4. Select the forest from the **Monitored Object** list.

   The **Forest** window has a summary area and two tabs: Monitored Domains tab and Forest Alerts tab. The number on the tab indicates the number of items on each tab.

Forest summary

The **Forest** summary area displays the name of the forest, the number of active alerts for the forest, and general information about the forest.

Table 6. Forest summary area

Item	Description
Forest	Name of the forest
Domains	Number of domains.
Domain controllers	Number of domain controllers.
Sites	Number of sites.
Empty sites	Number of empty sites.
GC servers	Number of global catalog (GC) servers.
RODC servers	Number of read-only domain controllers (RODCs).
Application partitions	Number of application partitions.
Bridgehead servers	Number of bridgehead servers.
Functional level	Functional level of the site.
Domain naming master	Name of the domain controller with the domain naming master role.
Schema master	Name of the domain controller with the schema master role.
Operations master consistent	Indicates if all the domain controllers report the same operation masters.
Schema master consistent	Indicates if all the domain controllers report the same operation masters.
Functional level consistent	Indicates if all the domain controllers report the same functional level.

Monitored Domains tab

The **Monitored Domains** tab lists all the monitored domains and indicates the number of critical alerts and warnings for each domain. A vertical bar next to each domain indicates its status. A red bar indicates the domain has alerts.

- To filter the list of domains, type in the **Filter domains** box. The list filters as you type.
- To sort the list, click on the column heading you want to sort.
- To refresh the list, click **Refresh**.

Forest Alerts tab

The **Forest Alerts** tab lists the active alerts for the forest. A count of the current alerts, critical and warnings, displays. For each active alert, the severity, alert name, time the alert triggered, the object name, and the description display.

- To sort the list, click on the column heading you want to sort.
- To refresh the list, click **Refresh**.

3

Alerts

Viewing alerts

Directory Analyzer alerts have two levels of severity: warning and critical. As a situation escalates, a warning alert is generated, indicating that a lower priority threshold has been violated. As the severity of the error increases, a critical alert is generated, indicating that the higher priority threshold has been exceeded. A number of attributes can be customized for each of these levels, including the threshold value, duration before an alert occurs and duration before an alert clears. See the *Active Directory Health* chapter in the *Quest® Active Administrator® User Guide*.

You can view alerts in two formats: grid view or table view. Grid view provides several details in a quick view. Table view lets you see several alerts at a time and you can select to view the details of a selected alert. Alerts update every minute, but you can manually refresh the display.

Current alerts display in grid view by default. Critical alerts are indicated in red and appear at the top of the list. Warning alerts are indicated in yellow and appear after the critical alerts. As alerts are cleared, they disappear from the list. You can view the cleared alert on the **Alert History** tab. See Viewing alert history.

For alerts you want to monitor more closely, you can pin them to the top of the list. You also can see which alerts are causing the most issues in the **Linked Alerts** area.

To view alerts

1. Select **Monitor | Active Directory Health**.
2. Open the **Active Alerts** tab.
   - The first 50 alerts display. To load the next batch of alerts, click **Next 50**.
   - To filter the list of alerts, start typing in the **Filter alerts** box. The list of alerts changes as you type.
   - To switch to table view, click  . To sort the alerts in table view, click the column heading.
   - To switch back to grid view, click  . To sort the alerts in grid view, click the icon to sort the alert names in ascending or descending alphabetical order.
   - To manually refresh the alerts, click **Refresh**.

Pinned alerts

If there are alerts you want to pull to the top of the list to monitor more closely, you can add them to the **Pinned Alerts** area. If the alert clears, it will disappear from the list.

To pin an alert

- Display the alerts in grid view, and click the pin in the alert heading.

  The alert moves to the **Pinned Alerts** area and remains there until you click the **X** in the alert heading. If you switch to table view, the pinned alerts remain in grid view.

Linked alerts

The area on the left of the display show a summary of the alerts to help you determine which alerts are causing the most issues. You can collapse or expand the list to fit your needs. To quickly see details on the alert, start typing the alert name in the **Filter alerts** box.

- The **Linked Alerts to Active Directory Objects** list displays a summary of the alerts for each of the types of Active Directory® objects. The number next to the alert indicates the number of occurrences of the alert for all objects. The percentage indicates the percentage of the total number of alerts for all objects.
- The **Linked Domain Controllers to Alerts**, **Linked Domains to Alerts**, **Linked Forests to Alerts**, and **Linked Sites to Alerts** display each Active Directory object with the alerts. The number next to the object indicates the number of alerts for that object. The percentage indicates the percentage of the total number of alerts for the object.

Viewing alert details

In grid view, a lot of details are visible at a glance, but if you prefer to work in table view, you can still see these details quickly.

To view alert details

- In grid view, double-click the alert heading, or click **View Details**.

  OR

  In table view, click the alert name.

  - The **General** tab displays much of the same information that you see in grid view. The list of Observed Values shows the number of times the alert was triggered.
  - The **Details** tab provides more information to help you troubleshoot the problem.
  - The **Notifications** tab displays the notifications sent for the alert.

Viewing alert history

Once an alert is cleared, it no longer appears on the **Active Alerts** tab. If you want to examine the progress of the alert, check the **Alert History** tab. You can see the most recent alert activity, and filter the list to closely examine specific alerts.

To view alert history

1. Select **Monitor | Active Directory Health**.
2. Open the **Alerts History** tab.

Alert History displays the newest current and cleared alerts in grid view. The alerts display in chronological order. Critical alerts are indicated in red. Warning alerts are indicated in yellow. Cleared alerts are indicated in pale gray.

- By default, the Alert History displays alerts from the live Active Administrator® database. To view alerts from the Active Administrator archive database, choose **Archive** as the source of the Alert History.
- To load another batch of alerts, click **More**.
- By default, the Alert History is filtered by date range for the current day.
  - To change the filter, click **Filter**. You can display all alerts, all alerts for a specific date, date range, domain, or domain controller.
  - To filter the list of alert history, start typing in the **Filter alerts** box. The list of alerts changes as you type.
- To switch to table view, click  . To sort the alerts history in table view, click the column heading.
- To switch to grid view, click  . To sort the alert history in grid view, click the icon to sort the alert names in ascending or descending alphabetical order.
- To manually refresh the alert history, click **Refresh**.

To view alert history details

- In grid view, click **View Details**.

  OR

  In table view, click the alert name.

  - The **General** tab displays much of the same information that you see in grid view. The list of Observed Values shows the number of times the alert was triggered.
  - The **Observed Values** tab displays the time the alert was triggered, the observed value, and the severity of the alert.
  - The **Details** tab provides more information to help you troubleshoot the problem.
  - The **Notifications** tab displays the notifications sent for the alert.

Generating an alert history report

You can generate a report of the alert history for specified dates and selected alerts.

NOTE: You also can access this report from **Report | Active Directory Health | Health Alerts**. See Active Directory Health reports.

To generate an alert history report

1. Select **Monitor | Active Directory Health**.
2. Open the **Alerts History** tab.
3. Click **Report**.
4. By default, all dates are included. You can select a specific date or date range.
5. By default all alerts are included. To filter the report, select **Filter by Alerts**, and select only those alerts to include in the report. Use **Clear All** or **Select All** to help you make the selection.
6. Click **Run**.

   The **Reports** tab displays the report based on the parameters you entered.

   - If the report generation is taking too much time, you can click **Cancel**.

- To collapse report sections, click on the section heading.
- The report remains open in the **Reports** tab until you run another report of this type. To redisplay the report with fresh data, click **Refresh**.
- To print the report, click **Print**.
- To return to the **Alert History** tab, click **Directory Health**.
- To go to the Active Directory Reports list, click **back to Reports**. See Active Directory Health reports.

Muting alerts

If you know about an upcoming maintenance to the system or some other event that may cause a lot of unnecessary alerts, you can mute the collection of alerts. During the mute period, no alerts are collected into the Active Administrator® database and no alert notifications are sent.

A banner displays on every analyzer page to indicate what object is muted, the time it was muted, and by whom it was muted. If more than one object is muted, only the number of muted objects displays. The banner updates every 15 seconds. The mute automatically clears after 1 hour.

You can mute all alerts or just alerts for a specific forest, domain, domain controller, or site. The Mute option displays on each window in the Directory Analyzer. If you are viewing health for a specific object, the Mute option will mute the alerts for that object. For example, if you are viewing a specific site and you click **Mute**, only the site alerts for that site are muted. If you wanted to mute all the alerts for a site, you could mute all or mute the forest and include domain controllers and sites. Table 1 shows how alerts are muted to help you select the appropriate mute type.

Table 1. Muting alerts

Mute type	Forest alerts	Domain alerts	DC alerts	Site alerts
All	Muted	Muted	Muted	Muted
Forest	Muted	Alerts sent	Alerts sent	Alerts sent
Forest + domain controllers + sites **NOTE:** Applies to only one forest.	Muted	Muted	Muted	Muted
Domain	Alerts sent	Muted	Alerts sent	Alerts sent
Domain + domain controllers	Alerts sent	Muted	Muted	Alerts sent
Domain controller	Alerts sent	Alerts sent	Muted	Alerts sent
Site	Alerts sent	Alerts sent	Alerts sent	Muted

To mute alerts

1. Select **Monitor | Active Directory Health**.
2. Open the **Analyzer** tab.
3. Select an object. See Table 1 to see what alerts are muted for each object.
4. Click **Mute**.
   - To mute the entire system, including all forests, domains, sites, and domain controllers, click **Mute All**.
   - To mute the selected object only, click **Mute**.
     - When muting a forest, you can also choose to include the sites, domains, and domain controllers.
     - When muting a domain, you can also choose to include domain controllers.
5. Click **Yes** to confirm the mute.

A banner displays on every analyzer page to indicate what object is muted, the time it was muted, and by whom it was muted. If more than one object is muted, only the number of muted objects displays. The banner updates every 15 seconds. The mute automatically clears after 1 hour.

- To clear all mutes, click **Clear All**.

Clearing mutes

A banner displays on every Active Directory Health page to indicate what object is muted, the time it was muted, and by whom it was muted. If more than one object is muted, only the number of muted objects displays. The banner updates every 15 seconds. A mute automatically clears after 1 hour. You can quickly clear all mutes from the banner. You also can clear just a selected mute.

To clear all mutes

1. Select **Monitor | Active Directory Health**.
2. Click **Clear All** in the banner.

To clear a selected mute

1. Select **Monitor | Active Directory Health**.
2. Open the **Analyzer** tab.
3. Select an object.
4. Click **Mute**.
    - To clear all mutes, click **Clear All**.
    - To clear the selected object only, click **Clear Mute**.

Viewing mute history

A history of mutes is kept so you can see the object that was muted, who set the mute and at what time, and who cleared the mute and at what time.

To view mute history

1. Select **Monitor | Active Directory Health**.
2. Open the **Analyzer** tab.
3. Click **Mute History**.

4

Notifications

About alert notifications

Directory Analyzer generates alerts when problems with Active Directory® are detected. You can create notifications to send to specified email recipients. A wizard helps you create multiple types of notifications to address varied audiences and their specific needs. For more information on the types of alerts you can include in the notifications, see the **Alerts Appendix** in the *Quest® Active Administrator® User Guide*.

For example, you might send only site alerts on a selected site to a certain user. You would exclude all forests, all domains, and all domain controllers from the notification. On the **Site Selection** page, you would choose the selected site.

Assign names and add descriptions to your alert notifications so you can easily manage the list. You can edit and remove alert notifications as your needs change. You also can limit the number of alert notifications sent within a specified time period.

Once you create alert notifications, you can see who alerts were sent to and when by displaying the details of an alert. See Viewing alert details.

IMPORTANT: To view, add, and edit alert notifications, the user must have:

- the Directory Analyzer Notification Management permission (See *Defining role based access* in the *Quest® Active Administrator® User Guide*);
- the Directory Analyzer Alert Management permission (See *Defining role based access* in the *Quest® Active Administrator® User Guide*); and
- membership in the Administrators group on the computer where Active Administrator Foundation Service (AFS) is installed.

Viewing alert notifications

You can view alert notifications in two formats: grid view or table view. Grid view provides several details in a quick view. Table view lets you see several notifications at a time. Notifications display in grid view by default.

To view alerts

1. Open Active Administrator® in a web browser. See Opening Active Administrator in a web browser.
2. Select **Monitor | Active Directory Health**.
3. Click **Notifications**.

- To filter the list of notifications, start typing in the **Filter notifications** box. The list of alerts changes as you type.
- To switch to table view, click  . To sort the notifications in table view, click the column heading.
- To switch back to grid view, click  . To sort the notifications in grid view, click the icon to sort the alert names in ascending or descending alphabetical order.
- To manually refresh the notifications, click **Refresh**.
- To edit a notification, click **Edit**. See Creating alert notifications.
- To disable a notification, click **Disable**. To enable the notification again, click **Enable**. You also can disable/enable a notification in the create notification wizard. See Creating alert notifications.
- To delete a notification, click **Delete**.

Creating alert notifications

NOTE: To create an alert notification successfully, you must:

- Add at least one email address.
- Select at least one Active Directory® object (forest, domain, domain controller, or site).
- Select alerts to match the selected Active Directory object.

  For example, if you select only domain alerts, and select only domain controllers, you receive a warning.

To create an alert notification

1. Open Active Administrator® in a web browser. See Opening Active Administrator in a web browser.
2. Select **Monitor | Active Directory Health**.
3. Click **Notifications**.
4. Click **Add Notification**.
5. Type a name and description for the alert notification.
6. By default, the notification is enabled, and all alert states are selected. Make the selections for the notification.
7. Click **Next**.
8. By default, all alerts are included in the notification. If you want to send notifications for selected alerts, clear the check box, and select the alerts to include. For more information on the alerts, see the *Alerts Appendix* in the *Quest*® Active Administrator® *User Guide*.
   - To filter the list of alerts, start typing in the **Filter Alerts** box. The list filters as you type.
   - To sort the list of alerts, click in the column headings.
9. Click **Next**.

   By default all forests are included in the notification. You can choose to exclude all forests or include only selected forests.
   - To filter the list, start typing in the **Filter by forest name** box. The list filters as you type.

   NOTE: If you select a forest, only forest alerts are included in the notification. The domains, domain controllers, and sites associated with the forest are not automatically included in the notification. You must select domains, domain controllers, and sites separately.

   If you select a forest, you must select at least one forest alert. If you receive a warning, go back and select a forest alert.

10 Click **Next**.

11 By default all domains are included in the notification. You can choose to exclude all domains or include only selected domains.

To filter the list, start typing in the **Filter by domain name** box. The list filters as you type.

> **NOTE:** If you select a domain, only domain alerts are included in the notification. The domain controllers and sites associated with the domain are not automatically included in the notification. You must select domain controllers and sites separately.
>
> If you select a domain, you must select at least one domain alert. If you receive a warning, go back and select a domain alert.

12 Click **Next**.

13 By default all domain controllers are included in the notification. You can choose to exclude all domain controllers or include only selected domain controllers.

To filter the list, start typing in the **Filter by domain controller name** box. The list filters as you type. You also can click the header to sort the list in ascending or descending order.

> **NOTE:** If you select a domain controller, you must select at least one domain controller alert. If you receive a warning, go back and select a domain controller alert.

14 Click **Next**.

15 By default all sites are included in the notification. You can choose to exclude all sites or include only selected sites.

To filter the list, start typing in the **Filter by site name** box. The list filters as you type.

> **NOTE:** If you select a site, only site alerts are included in the notification. The domain controllers associated with the site are not automatically included in the notification. You must select domain controllers separately.
>
> If you select a site, you must select at least one site alert. If you receive a warning, go back and select a site alert.

16 Click **Next**.

17 Add, edit, or remove email addresses of the recipients of the notification.

18 Click **Next**.

19 Review the selections, and click **Finish**.

20 Click **Finish**. See Viewing alert notifications.

Limiting notifications

To prevent being overwhelmed with notifications, you set up the notification limiter to govern the number of notifications sent within a specified time period. For example, you set the notification limit to 100 notifications within 20 minutes with a 10 minute reset time, which is the default. Once 100 notifications are sent within the 20 minute time period, notifications are suspended for 10 minutes, which is the reset time.

The **Notification Limiter** dialog indicates if notifications are being sent or suspended and the countdown for the reset. Once the **Current Count** reaches the limit, the **Reset Duration** starts to increment. The **Missed Notification** indicates the number of notifications that were not sent. Click **Refresh** to renew the display information.Once the **Reset Duration** reaches the limit, all counts return to zero. You can manually reset the counter when notifications are suspended by clicking **Reset**.

> **NOTE:** The notification limit applies collectively to all email notifications sent from Directory Analyzer. Any email notification from Active Administrator Health, including Directory Analyzer agent notifications, increases the notification count in the notification limiter count by 1.

To limit notifications

1 Open Active Administrator® in a web browser. See Opening Active Administrator in a web browser.

2 Select **Monitor | Active Directory Health**.

3 Click **Notifications**.

4 Click **Limiter**.

5 By default, the notification limiter feature is enabled. If you want unlimited notifications sent, clear the **Enabled** check box.

6 By default, an email is sent to the administrator when the limit is reached. To suppress the email, clear the check box.

7 Set the number of notifications to send within a specified time period. Once the limit is met, notifications are suspended until the reset time period is met.

8 Set the reset time period, which is the period of time to wait after the limit is met before automatically resetting the count.

- To renew the counter display, click **Refresh**.
- To reset the counters manually, click **Reset**.

  NOTE: Notifications must be in the Suspended state to reset the counters manually.

9 Click **OK**.

5

Active Directory Health Check

Using the Health Check landing page

To use the Health Check landing page

1. Open Active Administrator® in a web browser. See Opening Active Administrator in a web browser.
2. Select **Monitor | Active Directory Health Check**.

   The landing page is divided into four sections.

   - **Most Recently Completed Reports** lists reports initiated within the last 24 hours.
   - **Active Directory Health Check Report History** lists all reports.
   - **Running Health Checks** lists reports that are in process.
   - **Waiting Health Checks** lists reports that are scheduled but have not started.

Creating a Health Check

A Health Check is a customizable report on forests, domains, sites, and domain controllers. You can choose to take a snapshot of a moment in time or capture a trend over a specified period of time. There are many different tests from which you can choose. See Health check tests. There are also settings to help you customize the Health Check tests. See Setting options for Health Check tests.

Since you cannot rerun a Health Check, you have the option to save the Active Directory® objects, tests, and test settings you choose as a template. When you create a new Health Check, you can choose to use that template to populate the wizard. The only changes that are not saved are those on the **Health Check Options** page. You can make changes to the settings and save those as a new template or update the selected template.

NOTE: There are numerous choices to make in the Health Check Wizard.

- Use **Clear All** or **Select All** to help make selections.
- To filter lists, start typing in the **Filter** box.
- To sort lists, click in a column heading.

To create a new Health Check

1. Select **Monitor | Active Directory Health Check**.
2. Click **New Heath Check**.
3. Type a name for the Health Check.

4 Type a forest name, or click and select a previously discovered forest.

5 By default, the default credentials are used. If you want to change the account, clear the check box, and type the user name and password.

6 Click **Next**.

7 Select the forest tests to run. By default, all forest tests are selected. See Forest tests.

8 Configure the **Operator** and **Threshold** for the selected tests.

9 Click **Next**.

10 Select the domains to check.

11 Click **Next**.

12 Select the domain tests to run. By default, all domain tests are selected. See Domain tests.

13 Configure the **Operator** and **Threshold** for the selected tests.

14 Click **Next**.

15 Select the domain controllers to check.

16 Click **Next**.

17 Select the domain controller tests to run. By default, all domain controller tests are selected.

There are three tabs of domain controller tests: **General**, **Performance Counters**, and **Windows Services**. See Domain controller tests.

18 Configure the **Operator** and **Threshold** for the selected tests.

19 Click **Next**.

20 Select the sites to check.

21 Select the site tests to run. By default, all domain tests are selected. See Site tests.

22 Configure the **Operator** and **Threshold** for the selected tests.

23 Click **Next**.

24 Select the type of Active Directory Health Check you want to run.

- **Trending** collects data points for each selected test over the number of specified hours.
- **Snapshot** collects a single data point for each selected test.

25 Select when to run the Health Check. You can run it now or schedule the Health Check to run at a specified time.

26 Click **Next**.

27 If you want to save your choices of Active Directory objects, tests, and test settings, click Save as template and type a name for the template.

NOTE: You cannot rerun a completed Health Check. If you want to repeat a Health Check, save your selections as a template. The next time you create a new Health Check, you can choose the saved template. The settings display in the wizard.

- The only settings that are not saved are those on the **Health Check Options** page. You must make those selections again.
- You can make changes to the settings and save those as another template or write over the current selected template.
- To delete templates, see Setting options for Health Check tests.

28 Click **Next**.

29 Review the summary.

30 Click **Finish**.

While the Health Check is running, you can show or hide the log, show or hide a list of errors, or stop the Health Check.

By default, only the last 1000 entries display in the lists of log and error entries. If you want to see all the entries, click **View All**. To sort the list, click in the column heading. Once the report is completed, the complete list of log entries and errors display in the report.

Table 1. Active Directory Health Check Report options

Option	Description
Show/Hide Log	Show or hide entries to the log.
Show/Hide Errors	Show or hide errors.
Stop Now	Stop the test and present the results collected before the stop was initiated. The status of the test indicates Stopped.
Cancel	Cancel the test. No results are presented. The status of the test indicated Canceled.

Once the Health Check is complete, the report displays. Use the tool bar to manage the report.

Table 2. Active Directory Health Check Report tool bar

Option	Description
Report link	Copy the URL of the report to paste into a document or email.
Print	Print the report.
Expand all	Expand all the sections in the report. You also can click a header to expand a specific section.
Collapse all	Collapse all the sections in the report.
Back to Health Check	Return to the Active Directory Health Check main page.

The report displays below the **Most Recently Completed Reports** heading for 24 hours. The Health Check displays below the **Active Directory Health Check Report History** heading until you delete it.

- To view a Health Check result, click the test name.
- To delete a Health Check, click  .

Setting options for Health Check tests

On the **Active Directory Health Check** landing page (see Using the Health Check landing page), each test has a grade to indicate the level of success. You can customize the grading scale to fit your specifications. You also can turn off FSMO role validation for those tests that check FSMO roles and delete heath check templates.

To set options for Health Check tests

1. Select **Monitor | Active Directory Health Check**.
2. Click **Health Check Settings**.
3. For the grading scale, type the value to represent the percentage of success for each category.

   The default values are Excellent (89%), Good (79%), Fair (69%), and Caution (59%).
4. For FSMO placement tests, select the FSMO roles to validate.

   By default, all roles are selected. FSMO roles are validated based on Microsoft recommendations.
5. To delete selected Health Check templates, click **Delete Selected**, and then click **Yes**.

   When creating a Health Check, you can save your choices of Active Directory® objects, tests, and test settings as a template. See Creating a Health Check.

6 Click **Save**.

- To return values to the default, click **Defaults**.
- To exit without saving your selections, click **Cancel**.

Health check tests

Forest tests

Forest details

Information only.

Table 3. Forest details

Field	Description
Forest	Name of the forest.
Domains	Number of domains.
Domain controllers	Number of domain controllers.
Sites	Number of sites.
Empty sites	Number of empty sites.
GC servers	Number of global catalog (GC) servers.
RODC servers	Number of read-only domain controllers (RODCs).
Application partitions	Number of application partitions.
Bridgehead servers	Number of bridgehead servers.
Functional level	Functional level of the site.
Domain naming master	Name of the domain controller with the domain naming master role.
Schema master	Name of the domain controller with the schema master role.
Operations master consistent	Indicates if all the domain controllers report the same operation masters.
Schema master consistent	Indicates if all the domain controllers report the same schema masters.
Functional level consistent	Indicates if all the domain controllers report the same functional level.

Naming operations master inconsistent

Indicates that the naming operations master is not consistent among all domain controllers in the forest.

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege in all domains in the forest.

Description

The domain naming operations master is contained in the fSMORoleOwner property of the CN=Partitions,CN=Configuration,DC=<root domain> container. Because the partitions container is part of the configuration naming context, every domain controller in the forest has a copy of the domain naming operations master. The domain naming operations master determines what domain controller in the forest can initiate a domain renaming operation. If the domain naming operations master is inconsistent, it is possible to issue a domain renaming operation simultaneously at two different domain controllers, with potentially disastrous consequences.

The domain naming operations master can become inconsistent because an administrator used NTDSUTIL.EXE to move the operations master when there was incomplete connectivity to all domain controllers. It can also occur because of replication errors.

Resolution

- Make sure that no one attempts to rename a domain.
- Wait to see if the error clears. If an administrator has moved an operations master to another domain controller, replication to all domain controllers in the forest can take a long time.
- If the situation does not clear, contact your Microsoft® Windows® support representative.

Related article

- How to Find Servers That Hold Flexible Single Master Operations Roles

Naming operations master is not a global catalog server

Indicates that a server possessing the domain naming operations master does not host a global catalog (GC).

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege in the domain where the schema and naming masters reside.

Description

The domain naming operations master must be a global catalog server because the domain naming operations master is responsible for creating objects that represent new domains. In order to do this, the domain naming operations master must be able to make sure that no other object — whether it is a domain object or not — has the same name as the new domain object. The domain naming operations master always runs a global catalog, which contains a partial replica of every object, to allow the domain naming operations master to quickly check for a duplicate object name prior to creating a new domain object.

Resolution

- Enable a global catalog on the domain naming operations master.

Naming operations master not responding

Indicates if the naming operations master is not responding within the configured threshold.

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege is required.

Description

- The domain controller does not exist, is not running, or lost connectivity to the network
- The DNS records for the domain controller are incorrect; e.g., the IP address for the domain controller is not what is published in DNS.
- Active Directory® on the domain controller has failed, or is overloaded and taking too long to respond.

Resolution

- Ping the domain controller to see if there is connectivity. If there is not, fix that problem. The problem may be that DNS has the incorrect address or the IP stack for the domain controller is misconfigured.
- If the domain controller does not exist, run NTDSUTIL and select the **metadata cleanup** option to clean up the erroneous objects in the directory.
- Check the LDAP response time for the domain controller. If it is too high, you may need to add another domain controller for the same domain in the same site.

Schema operations master inconsistent

Indicates that the schema operations master is not consistent among all domain controllers in the forest.

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege is required.

Description

The schema operations master object (CN=&ldots;) contains an attribute called fSMORoleOwner, which contains the distinguished name of the domain controller that is allowed to originate changes to the Active Directory® schema. When an administrator attempts to modify the Active Directory schema, the directory system agent (DSA) makes sure that the fSMORoleOwner property refers to the server on which the administrator is making the change. If it does not refer to that server, the DSA will not modify the schema. The schema operations master ensures that the schema cannot become inconsistent because of conflicting changes issued from different domain controllers.

If the schema operations master is inconsistent, meaning the domain controllers have differing values for the fSMORoleOwner attribute, it is possible for administrators (or others) to issue conflicting updates to the schema, potentially causing sufficient damage to Active Directory that replication will fail. It is important to not attempt to modify the Active Directory schema when the schema operations master is inconsistent.

The schema operations master can become inconsistent due to replication failures or due to an administrator using NTDSUTIL.EXE to force the operations master to another domain controller. This can also be transient if the replication latency for the schema naming context is fairly large.

Resolution

- Make sure that no one attempts to modify the Active Directory schema while the schema operations master is inconsistent.
- Normally, the Active Directory replication process will correct this error, so the next step is to wait awhile to see if the error clears by itself. The amount of time you should wait depends on the replication latency for the schema naming context.
- If the error does not clear itself in a reasonable amount of time, contact your Microsoft® Windows® support representative.

Related article

- How to Find Servers That Hold Flexible Single Master Operations Roles

Schema operations master not responding

Indicates that the schema operations master is not responding within the configured threshold.

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege is required.

Description

- The domain controller does not exist, is not running, or lost connectivity to the network
- The DNS records for the domain controller are incorrect; e.g., the IP address for the domain controller is not what is published in DNS.
- Active Directory® on the domain controller has failed, or is overloaded and taking too long to respond.

Resolution

- Ping the domain controller to see if there is connectivity. If there is not, fix that problem. The problem may be that DNS has the incorrect address or the IP stack for the domain controller is misconfigured.
- If the domain controller does not exist, run NTDSUTIL and select the **metadata cleanup** option to clean up the erroneous objects in the directory.
- Check the LDAP response time for the domain controller. If it is too high, you may need to add another domain controller for the same domain in the same site.

Schema version inconsistent

Indicates that the schema version is not consistent across all domain controllers in the forest.

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege is required.

Resolution

- Wait for a while to see if the error clears itself. An inconsistent schema version error can be transitory in nature.

- If you have waited long enough for replication to have occurred to all domain controllers, contact your Microsoft® Windows® support representative.

Domain tests

Conflict encountered during replication

Indicates that conflicting objects were encountered during replication and reported by Active Directory®.

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege is required.

Description

Conflicts arise when two objects are created independently at separate locations in the domain. When a conflict is detected during replication, Active Directory creates a conflict entry appending the following to the domain name of the object:

CNF:<GUID-of-authoritative-object>

Resolution

- If the conflict object contains useful information, move that information into a different directory object, and then delete the object.
- If the conflict object does not contain useful information, delete the object.

DC replication latency

Indicates that replication changes from one domain controller to all other domain controllers in the naming context exceeds the configured threshold.

Requirement

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privileges with rights to list contents, create objects, read and write properties under the AATemp organizational unit in the domain root.

Description

High replication latency values mean that changes you make in the directory are taking too long to replicate to all of the other domain controllers, which can cause operational difficulties. For example, a user cannot use a new password if the password has not replicated to their domain controller. High replication latency values can also cause directory problems. If you make a change to the Configuration naming context by adding a new site or a new domain controller, the replication process will not work correctly until all domain controllers have a copy of the new site or new domain controller.

High latency times are usually due to poor network connectivity, non-functional domain controllers, or incorrect replication schedules.

Resolution

Make sure that the replication latency is actually too high. In a site with fewer than five domain controllers, the intra-site replication latency should be around five minutes. As you add domain controllers in a site, the intra-site replication latency should go up to about 20-30 minutes, and then stabilize. Inter-site replication latency depends entirely on the link schedules between the sites.

If the latency truly is too high, make sure there are no domain controllers that are down. If a single domain controller acts as a bridgehead between sites, and it goes down, replication will never actually occur.

DNS domain missing SRV records

Indicates one or more requisite Domain Name System (DNS) service locator (SRV) entries are not defined.

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege is required.

Description

Service Records or SRV records are registered specifically for domain controllers when a member server is promoted to a domain controller. The Netlogon service on the domain controller is responsible for registering SRV records. Because Active Directory® depends on DNS, if SRV records of domain controllers are missing from the DNS Zone of the domain, critical failures of Active Directory services can occur.

Resolution

The following methods can be used to re-register SRV records of a domain controller in the domain DNS zone:

- Restart the Netlogon service on domain controller.
- Run DcDiag /fix.
- Run NetDiag /fix.
- Re-register from Netlogon.dns file in \Windows or Winnt\System32\Config directory.

Related article

- SRV Records Missing After Implementing Active Directory and Domain Name System

Domain details

Information only.

Table 4. Domain details

Field	Description
Domain	Name of the selected domain.
Domain controllers	Number of domain controllers.
GC servers	Number of global catalog (GC) servers
RODC servers	Number of read-only domain controllers (RODCs)
Functional level	Functional level of the forest, domain, or site
PDC owner	Owner of the primary domain controller (PDC) Flexible Single Master Operation (FSMO) role
RID master	Owner of the relative identifier (RID) FSMO role
Infrastructure master	Owner of the infrastructure FSMO role
Operations master consistent	Indicates if all the domain controllers report the same operation masters
Functional level consistent	Indicates if all the domain controllers report the same functional level

FSMO placement

Indicates that Active Directory® Flexible Single-Master (FSMO) roles are not configured according to Microsoft® recommendations.

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege is required.

Description

The Active Directory Installation Wizard performs the initial placement of roles on domain controllers and is often correct for directories that have just a few domain controllers. A directory that has many domain controllers may require manual intervention to optimize placement.

Resolution

- Place the schema master on the PDC of the forest root domain.
- Place the domain naming master on the forest root PDC.
- Place the RID master on the domain PDC in the same domain.
- Legacy guidance suggests placing the infrastructure master on a non-global catalog server.

Related article

- FSMO placement and optimization on Active Directory domain controllers

GC replication latency

Indicates that the replication latency of the server that hosts a replica of the global catalog equals or exceeds the configured threshold.

Requirement

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privileges with rights to list contents, create objects, read and write properties under the AATemp organizational unit in the domain root.

Resolution

- Check connectivity between both the domain controller and the replication partner in question.
- Check to see that the link is reasonably clear, especially during replication.
- Check the replication schedule for the connection.
- Make sure that each partner has adequate CPU and memory resources to ensure timely servicing of replication requests.
- Make sure that the link between partners is adequate for the amount of traffic carried during replication.

Infrastructure master host GC

Indicates that the infrastructure operations master hosts a global catalog server.

Requirement

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege is required.

Description

The infrastructure operations master updates references from objects in other domains by comparing local data to data from a global catalog, which is always up to date. If discrepancies are found, the infrastructure operations master updates the local object data from the global catalog, and then replicates the updated object data to all other domain controllers in the domain. If a global catalog exists on the same domain controller as the infrastructure operations master, the infrastructure operations master will never find data that is out of date.

Resolution

Remove the global catalog from the infrastructure operations master domain controller.

Infrastructure master not responding

Indicates that the infrastructure operations master is not responding within the configured threshold.

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege is required.

Description

This error can occur if any of the following occurs:

- The indicated server domain controller does not exist.
- The domain controller no longer has connectivity to the network and to the Directory Analyzer agent.
- The DNS records for the domain controller are incorrect; e.g., the IP address for the domain controller is not what is published in DNS as viewed by the Directory Analyzer agent.

- Active Directory® on the domain controller has failed in some way.
- Active Directory on the domain controller is overloaded and is taking too long to respond.
- The domain controller is not running.

Resolution

- Ping the domain controller from the Directory Analyzer agent to see if there is connectivity. If there is not, fix that problem. The problem may be that DNS has the incorrect address or that the IP stack for the domain controller or the Directory Analyzer agent is misconfigured.
- Make sure the domain controller is running. If the domain controller is not running, start it.
- Make sure the indicated domain controller actually exists. If it does not exist, run NTDSUTIL and select the **metadata cleanup** option to clean up the erroneous objects in the directory.
- Check the LDAP response time for the domain controller on the **Active Directory** tab in Directory Analyzer. If it is too high, you may need to add another domain controller for the same domain in the same site.

Infrastructure operations master inconsistent

Indicates that the infrastructure operations master is not consistent among all domain controllers in the domain.

Requirement

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege is required.

Description

The infrastructure operations master is contained in the fSMORoleOwner property of the infrastructure object contained by each domain object. Every domain controller in the domain has a copy of the infrastructure operations master.

Active Directory® objects can contain links to other objects in the directory. Active Directory keeps these links up-to-date even if the linked-to object is moved to another container or is renamed. This update cannot happen if the linked-to object is in another domain.

If the infrastructure operations master is inconsistent, it is possible that two copies will run simultaneously on two different domain controllers, with potentially disastrous consequences.

The Infrastructure operations master can become inconsistent because an administrator used NTDSUTIL.EXE to move the Operations Master when there was incomplete connectivity to all domain controllers in the domain. It can also occur because of replication errors.

Resolution

Wait to see if the error clears itself. If an administrator has moved an operations master to another domain controller, replication to all domain controllers in the domain can take some time.

If you have waited long enough for replication to have occurred to all domain controllers in the domain, contact your Microsoft Windows support representative.

Related article

- How to Find Servers That Hold Flexible Single Master Operations Roles

Objects exist in the Lost and Found

Generated when Directory Analyzer discovers objects in the Lost And Found container of a naming context.

Requirement

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege is required.

Description

During the replication process, Active Directory® may encounter orphaned objects, which are objects that have no parent container. For example, a user deletes container X on domain controller A, and another user modifies object Y contained in container X on domain controller B. During replication, domain controller A will receive an update operation for an object that has no container because container X was deleted. In this case, the directory system agent (DSA) on domain controller A puts the object in the Lost And Found container.

The DSA will place objects in the Lost And Found container as part of its normal operation. However, several Lost And Found objects may indicate a replication problem, or at least the deletion of a container that should not have been deleted.

Resolution

Inspect the objects in the Lost And Found container of the replica using an appropriate utility. Move the objects to an appropriate container or delete them from the Lost And Found container.

PDC master not responding

Indicates that the PDC (primary domain controller) operations master is not responding within the configured threshold.

Requirement

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege is required.

Description

This error can occur if any of the following occurs:

- The indicated domain controller does not exist.
- The domain controller no longer has connectivity to the network.
- The DNS records for the domain controller are incorrect; e.g., the IP address for the domain controller is not what is published in DNS.
- Active Directory® on the domain controller has failed in some way.
- Active Directory on the domain controller is overloaded and is taking too long to respond.
- The domain controller is not running.

Resolution

- Ping the domain controller from the Directory Analyzer to see if there is connectivity. If there is not, fix that problem.
- Make sure the domain controller is running. If the domain controller is not running, start it.
- Make sure the indicated domain controller actually exists. If it does not exist, run NTDSUTIL and select the metadata cleanup option to clean up the erroneous objects in the directory.
- Check the LDAP response time for the domain controller. If it is too high, you may need to add another domain controller for the same domain in the same site.

RID master not responding

Indicates that the relative identifier (RID) operations master is not responding within the configured threshold.

Requirement

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege is required.

Description

This error can occur if any of the following occurs:

- The indicated server is not actually a domain controller.
- The domain controller no longer has connectivity to the network.
- The DNS records for the domain controller are incorrect; e.g., the IP address for the domain controller is not what is published in DNS.
- Active Directory® on the domain controller has failed in some way.
- Active Directory on the domain controller is overloaded and is taking too long to respond.
- The domain controller is not running.

Resolution

- Ping the domain controller from the Directory Analyzer agent to see if there is connectivity. If there is not, fix that problem. The problem may be that DNS has the incorrect address or that the IP stack for the domain controller or the Directory Analyzer agent is misconfigured.
- Make sure the domain controller is running. If the domain controller is not running, start it.
- Make sure the indicated domain controller actually exists. If it does not exist, run NTDSUTIL and select the **metadata cleanup** option to clean up the erroneous objects in the directory.
- Check the LDAP response time for the domain controller. If it is too high, you may need to add another domain controller for the same domain in the same site.

RID operations master inconsistent

Indicates that the relative identifier (RID) operations master is not consistent among all domain controllers in the domain.

Requirement

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege is required.

Description

The domain RID operations master is contained in the fSMORoleOwner property of the RID Manager object in the CN=System,DC=<domain> container. Every domain controller in the domain has a copy of the domain RID operations master. The RID operations master allocates sequences of RIDs to each of the various domain controllers in its domain. At any time, there can be only one domain controller acting as the RID master in each domain in the forest.

Whenever a domain controller creates a user, group, or computer object, the domain controller assigns the object a unique security ID (SID). The SID consists of a domain SID, which is the same for all SIDs created in the domain, and a RID, which is unique for each SID created in the domain. If the domain RID operations master is

inconsistent, it is possible that two different domain controllers will assign overlapping RID ranges to other domain controllers in the domain, with potentially disastrous consequences.

The domain RID operations master can become inconsistent due to replication errors or if an administrator used NTDSUTIL.EXE to move the operations master when there was incomplete connectivity to all domain controllers in the domain.

Resolution

Wait to see if the error clears. If an administrator has moved an operations master to another domain controller, replication to all domain controllers in the domain can take some time.

If the error does not clear, contact your Microsoft® Windows® support representative.

Related article

- How to Find Servers That Hold Flexible Single Master Operations Roles

Root PDC time source missing

Indicates the PDC Role Owner of the root domain in the forest is not configured to use an external time source. All domain controllers in the forest synchronize their time by the clock of the PDC Role Owner.

Requirement

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege is required and the target server must have WMI remote access enabled. The user must be a member of the Distributed COM Users group.

Description

Since Active Directory®, by default, sets all the clocks on all of the domain controllers in the forest from the PDC Role Owner of the root domain, it is recommended that the domain controller be configured to synchronize its time with an external time source.

Resolution

Use the w32time command at an elevated PowerShell® session to configure the PDC Role Owner to use an external time source.

```
w32tm /config /manualpeerlist:TimeSource /syncfromflags:MANUAL
```

Where TimeSource is one or more NTP servers noted by DNS or IP address. When TimeSource is a list of time servers the list must be enclosed in double quotes and each entry must be separated by at least one space. Some examples are listed below:

```
w32tm /config /manualpeerlist:pool.ntp.org /syncfromflags:MANUAL
w32tm /config /manualpeerlist:”1.pool.ntp.org 2.pool.ntp.org“ /syncfromflags:MANUAL
```

Domain controller tests

Domain controller tests are divided into four categories that are organized on four tabs. You can select tests from all four tabs to run together.

General tests

- Consecutive replication failures threshold exceeded
- DFSRS conflict area disk space

- DFSRS conflict files generated
- DFSRS RDC is not enabled
- DFSRS sharing violation
- DFSRS staged file age
- DFSRS staging area disk space
- Domain controller relative identifier (RID)
- Domain controller responsive
- Domain controller time synchronization
- Group policy object inconsistent
- Installed applications
- Installed updates
- Invalid primary DNS domain controller IP address
- Invalid secondary DNS domain controller IP address
- LDAP response time
- Logic disk details
- Memory details
- Missing domain controller SRV DNS record
- NetLogon folder shared
- Network adapter information
- Operating system details
- Primary DNS resolver not responding
- Secondary DNS resolver not responding
- SysVol details
- SysVol folder shared

Performance counters

- Cache copy read hits
- CPU processor time
- DFSRS % processor time
- DFSRS private bytes
- DFSRS USN records accepted
- DFSRS working set
- File replication (NTFRS) staging space free in kilobytes
- LSASS % processor time
- LSASS private bytes
- LSASS working set
- Memory page faults a second
- NTDS DRA inbound properties filtered a second
- NTDS LDAP searches a second
- NTDS LDAP writes a second

- NTFRS % processor time
- NTFRS process private bytes
- NTFRS working set
- Server sessions

Windows services

- Active Directory Domain Service
- DFS namespace service
- DFS replication service
- File replication service
- Kerberos Key Distribution Center service
- NetLogon Windows service
- Windows Time service

Replication latency

- DC replication latency
- GC replication latency

Active Directory Domain Service

Indicates if the Active Directory® Domain Service is running on the domain controller.

Category

- Windows Services

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions:** When monitored locally or remotely, domain administrator privilege is required.

Description

The most typical cause of this situation is when a server administrator shuts down the Distributed File System (DFS) service and forgets to restart it.

Resolution

Use the Services MCC snap-in or another SCP application to restart Active Directory Domain Services.

Cache copy read hits

Indicates the performance of the server may be degraded because of too few cache read hits.

Category

- Performance counters

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions:** When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs User group.

Description

Tests the cache copy read hits data collector on the domain controller to see if the value of the data collector drops below the configured threshold for a period exceeding the configured duration.

Resolution

- Reduced cache hits are due to excessive disk I/O or insufficient memory, or both. When the cache hit percentage drops, the system spends more time waiting for disk accesses to complete, and overall system throughput suffers enormously.
- If possible, try to reduce the number of applications running on the server that is generating disk I/O. If you are running several batch jobs on the server, running them one after the other, rather than all at the same time, may actually be faster.
- You can also try to reduce the number of users accessing the server by moving heavily-used files to other, less-loaded servers.

Consecutive replication failures threshold exceeded

Indicates that the number of consecutive replication failures equals or exceeds the configured threshold.

Category

- General

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions:** When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Resolution

- Check connectivity between the domain controller and the replication partner in question. Check to see that the link is reasonably clear, especially during replication (check the replication schedule for the connection).
- Make sure that each partner has adequate CPU and memory resources to ensure timely servicing of replication requests.
- Make sure that the link between partners is adequate for the amount of traffic carried during replication. For example, if thousands of objects are being replicated over a slower connection link, the link should be upgraded, or the replication topology reconsidered.

CPU processor time

Indicates that the CPU for the domain controller is too busy, which may indicate a problem with directory service or it can indicate that a problem may occur because the domain controller cannot respond to requests quickly enough.

Category

- Performance counters

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

Tests the Processor\% Processor Time performance counter on the domain controller to see if the value of the performance counter goes above the configured threshold for a period exceeding the configured duration.

Increased CPU load is a result of running too many applications on the server, or running applications that require too much CPU time.

It is also possible that the CPU load has increased due to some pathological condition in a particular application. For instance, Active Directory® itself requires substantial CPU resources when it is processing inherited Access Control Lists (ACLs). Active Directory can also require a lot of CPU resources when it processes complex, non-indexed directory searches.

Resolution

First, try to determine if the increased CPU load is due to a particular program, or if it is due to running too many programs. Use a utility like Task Manager to inspect the CPU usage of all processes on the system. If there are several processes getting more than 10% of the CPU, then the problem is most likely due to running too many programs on the server. If possible, stop some of the programs.

If one process is using all of the CPU for an extended period of time, it may be due to a bug in the software, or it may be that the program just requires too much CPU. If possible, stop the program and run it on a different machine.

DC replication latency

Indicates that replication changes from one domain controller to all other domain controllers in the naming context exceeds the configured threshold.

NOTE: The replication latency tests create or modify objects in Active Directory, and then check for those changes on each selected domain controller. The length of time for the tests to complete is dependent on the number of domains and domain controllers you select.

Category

- Replication Latency

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privileges with rights to list contents, create objects, read and write properties under the AATemp organizational unit in the domain root.

Description

This test checks latency between each domain controller in the domain by creating an object on a domain controller and then checking every other domain controller for the change. Once the change is noticed, the time difference is recorded.

NOTE: On service startup there is a 5 minute delay before Active Administrator Data Service (ADS) starts checking replication, and then every hour after that. If the latency container does not exist, it is created and there is a 10 minute delay. The latency containers are located at AATemp\Latency under the domain.

There is a timeout for the test. The timeout is the alert value plus three minutes. If the alert is set to 20 minutes and the test is still running at 23 minutes it will terminate.

High replication latency values mean that changes you make in the directory are taking too long to replicate to all of the other domain controllers, which can cause operational difficulties. For example, a user cannot use a new password if the password has not replicated to their domain controller. High replication latency values can also cause directory problems. If you make a change to the Configuration naming context by adding a new site or a new domain controller, the replication process will not work correctly until all domain controllers have a copy of the new site or new domain controller.

High latency times are usually due to poor network connectivity, non-functional domain controllers, or incorrect replication schedules.

NOTE: This test only measures replication latency to another domain controller if replication actually occurs on that domain controller. If the domain controller is down or disconnected, this test will not measure the latency to that domain controller.

Resolution

Make sure that the replication latency is actually too high. In a site with fewer than five domain controllers, the intra-site replication latency should be around five minutes. As you add domain controllers in a site, the intra-site replication latency should go up to about 20-30 minutes, and then stabilize. Inter-site replication latency depends entirely on the link schedules between the sites.

If the latency truly is too high, make sure there are no domain controllers that are down. If a single domain controller acts as a bridgehead between sites, and it goes down, replication will never actually occur.

DFS namespace service

Indicates the Distributed File System (DFS) namespace service is stopped.

Category

- Windows Services

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally, only domain user privilege is required. When monitored remotely, domain administrator privilege is required.

Description

This test checks if the DFS Namespace service is running.

Resolution

Use the Services MCC snap-in or another SCP application to restart the DFS Namespace service.

DFS replication service

Indicates that a server hosting Distributed File System (DFS) is running, but the DFS Replication (DFSR) service is not. A DFSR service not running can affect group policies.

Category

- Windows Services

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally, only domain user privilege is required. When monitored remotely, domain administer privilege is required.

Description

This test queries the Service Control Manager (SCM) to determine if the DFS Replication service is up and running.

DFS Namespaces and DFS Replication offer simplified but highly-available access to files, load sharing, and WAN-friendly replication. DFS in Windows Server 2008 is implemented as a role service of the File Services role.

The most typical cause of this alert is when a server administrator shuts down the DFS service and forgets to restart it.

Resolution

- Check the status of the service by running the Services MMC snap-in. Select the Server DNS (not DNS Client) entry. If the status is stopped, then the service is actually down.
- If the DFS service is stopped, use the Services MCC snap-in or another SCP application to restart the DFS Service. Check the Event Logs and fix any problems indicated by the logs.

DFSRS % processor time

Indicates that the CPU for the Distributed File System Replication (DFSR) service is too busy.

Category

- Performance Counters

Data collector

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

Tests the CPU utilization by the DFSR service to see if the utilization is above the configured threshold.

Resolution

Wait for a while to see if the error clears itself. For example, a high CPU utilization that occurs during an initial replication is transitory in nature.

Review the system configuration and tune the environment to optimize DFSRS performance as described in these references:

- Common DFSR Configuration Mistakes and Oversights

- Tuning replication performance in DFSR (especially on Win2008 R2)

DFSRS conflict area disk space

Detects that the amount of disk space allocated for conflict files during replication is less than or equal to the specified threshold.

Category

- General

Requirement

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

If the ConflictandDeleted folder runs out of space, DFS Replication removes older conflicting or deleted files to free up disk space, which might temporarily decrease replication performance.

If a staging folder quota is configured to be too small, DFS Replication might consume additional CPU and disk resources to regenerate the staged files. Replication might also slow down because the lack of staging space can limit the number of concurrent transfers with partners. Increasing the size of the staging folder and the ConflictandDeleted folder can increase replication performance and the number of recoverable conflicting and deleted files.

Resolution

Delete files from the ConflictandDeleted folder, or increase the quota of the ConflictandDeleted folder for the appropriate replicated folder(s).

Related article

Edit the Quota Size of the Staging Folder and Conflict and Deleted Folder

DFSRS conflict files generated

Indicates that there are conflicted files in ConflictAndDeleted folder assigned to the replicated folder.

Category

- General

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

This test enables administrators to keep track of the number of replication conflicts generated for replicated folders on the monitored computer. Monitoring the space utilization of the Conflict and Deleted area helps ensure that there is enough space to store replication conflicts and files deleted from replicated folders on the monitored computer. You can view a log of conflict files and their original file names by viewing the ConflictandDeletedManifest.xml file in the DfsrPrivate folder.

Frequent conflicts indicate that files in a replicated folder are frequently being modified on multiple servers in a short period.

Resolution

In general, resolution of this condition involves deciding whether a conflict object contains useful information, moving that information into a different directory object, and then deleting the object.

DFSRS private bytes

Indicates that the virtual memory allocated to the Distributed File System Replication (DFSR) service is too high.

Category

- Performance Counters

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

Tests the **DFSRS private bytes** performance counter on the domain controller for the DFSR service to see if the value in the performance counter goes above the configured threshold for a period exceeding the configured duration.

Resolution

Review the system configuration and tune the environment to optimize DFSRS performance as described in these references:

- Common DFSR Configuration Mistakes and Oversights
- Tuning replication performance in DFSR (especially on Win2008 R2)

DFSRS RDC is not enabled

Indicates that any of Distributed File System Replication (DFSR) connections have the Remote Differential Compression (RDC) option disabled.

Category

- General

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

Remote Differential Compression (RDC) only updates changes to files, which is useful when replicating across a wide area network.

Resolution

Enable Remote Differential Compression.

DFSRS sharing violation

Indicates that a sharing violation exists for a period greater than or equal to the specified threshold.

Category

- General

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

The Directory Analyzer agent monitors the DFRS debug log for reports of sharing violations. If the sharing violation exists for a period exceeding the configured duration, the agent sets this alert condition.

One possibility for the sharing violation is that other sources may have opened the file to be replicated on the target machine.

Another possibility for a sharing violation is that other sources have open handles to the file to be replicated. Typically, programs that can instigate sharing violations are:

- Antivirus programs
- Disk optimization tools
- File system policies that repeatedly apply access control list (ACL) changes
- A user profile or personal data that is constantly in use that is placed on the replica set
- Any other type of data that is held open for long periods by an end user, a program, or a process

Resolution

- Rename the locked file.
- Identify the locked files and release the handles.

Related article

FRS Encounters "ERROR_SHARING_VIOLATION" Errors When It Tries to Replicate Data That Is Still in Use

DFSRS staged file age

Indicates that the age of files in the Distributed File System Replication (DFSR) staging folder is greater than or equal to the specified threshold.

Category

- General

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016

- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

This situation could be caused by the following factors:

- The replication schedule is too short to allow all data to replicate to other members.
- Network bandwidth is affecting the speed at which files replicate, causing a delay.
- A downstream partner is unavailable due to network problems or other issues.
- Possibly caused by a nonauthoritative restore (also called D2) on a downstream partner.

Resolution

If a D2 was not performed on a downstream partner, look for failure indicators at either the upstream or downstream partners. If you cannot find failure indicators, re-examine the schedule and network bandwidth on this connection to ensure that enough replication time is scheduled to allow the data to replicate.

DFSRS staging area disk space

Indicates that the amount of disk space allocated for staging files during replication is less than or equal to the specified threshold.

Category

- General

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

If the File Replication Service (FRS) runs out of staging disk space, replication will stop. The size of the contents of the staging areas for all active replication sets are subtracted from the user controlled size.

A low disk space condition can be due to many different things. Some possibilities are: the size of the data to be replicated is larger than the staging area, there are too many replica sets active at once, or there are files destined for one or more out-bound partners that have not been connected for a while.

Resolution

- Increase the amount of space allowed for file staging.
- Check replication schedules and connectivity between partners.

Related article

Edit the Quota Size of the Staging Folder and Conflict and Deleted Folder

DFSRS USN records accepted

Detects that there is heavy file replication traffic.

Category:

- Performance counters

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

Tests the **DFSR USN records accepted** performance counter on a domain controller to see if the value of this performance counter goes above the configured threshold for a period exceeding the configured duration.

Replication is triggered by entries to the NTFS update sequence number (USN) change journal. A high value on this counter, such as one every five seconds, indicates heavy replication traffic and may result in replication latency.

Resolution

None.

DFSRS working set

Indicates that the working set allocated to the DFS Replication service is too high.

Category

- Performance Counters

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

Tests the **DFSRS working set** performance counter on the domain controller for the DFSR service to see if the value in the performance counter goes above the configured threshold for a period exceeding the configured duration.

Resolution

Review the system configuration and tune the environment to optimize DFSRS performance as described in these references:

- Common DFSR Configuration Mistakes and Oversights
- Tuning replication performance in DFSR (especially on Win2008 R2)

Domain controller relative identifier (RID)

Indicates that the available pool of relative identifiers (RIDs) on the selected domain controller is less than or equal to the configured threshold.

Category

- General

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required.

Description

Tests the RID pool assigned to the domain controller to see if the number of RIDs available to the server goes below the threshold.

All security principals in the Windows® NT Security Architecture are assigned a unique security ID (SID). The SID is made up of a domain identifier and a RID. RIDs are sequential numbers issued by the domain each time a new security principal (for instance a user object) is created in that domain.

Because each domain controller can create security principals, Active Directory® breaks the available range of RIDs into allocation pools that it assigns to each domain controller. Active Directory assigns one domain controller in each domain to be responsible for allocating RID pools to all of the other domain controllers in the domain; this is the RID Operations Master. When a domain controller uses up its allocation, it requests a new range from the RID Operations Master.

If a domain controller has a problem contacting the RID Operations Master, the domain controller can actually use up its entire allocation of RIDs, and be unable to create new security principals, which can result in failures when adding new users, services, and domain controllers to the domain.

Resolution

Contact your Microsoft® Windows® support representative.

Domain controller responsive

Indicates if the domain controller is responsive.

Category

- General

Requirement

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege required.

Description

If Active Administrator® Data Service (ADS) can connect to TCP port 135, the domain controller is reponsive.

If the domain controller is unresponsive, one or more of the following may be the reason:

- The indicated server is not actually a domain controller.
- The domain controller no longer has connectivity to the network.
- The DNS records for the domain controller are incorrect.
- Active Directory® on the domain controller has failed in some way.
- Active Directory on the domain controller is overloaded and is taking too long to respond.
- The domain controller is not running.

Resolution

- Make sure the indicated server is actually a domain controller. If it is not, run NTDSUTIL and select the metadata cleanup option to clean up the erroneous objects in the directory.
- Make sure the domain controller is running. If the domain controller is not running, start it.
- Ping the domain controller to see if there is connectivity. If there is not, fix that problem. The problem may be that DNS has the incorrect address or that the IP stack for the domain controller is misconfigured.
- Check the LDAP response time for the domain controller. If it is too high, you may need to add another domain controller for the same domain in the same site.

If the domain controller is also a global catalog, you may need to add another global catalog to the site.

Domain controller time synchronization

Indicates that the time of the target domain controller differs from one of its reference sources by more than the configured threshold (in seconds).

Category

- General

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

The Windows® Time (W32Time) service on a domain controller is responsible for maintaining the accuracy of the clock with respect to the time sources. Active Directory® defines rules for time sources as follows:

- A domain controller in a domain will synchronize its clock to the domain controller in the domain that is the PDC Role Owner for its domain, unless the domain controller in question is the PDC Role Owner.
- If the domain controller is the PDC Role Owner, it will synchronize its clock with the PDC Role Owner of its parent domain, unless the domain controller is in the root domain.
- If the domain controller is in the root domain and it is the PDC Role Owner for that domain, it must be configured to synchronize its clock to an external time source.

A special case exists for the PDC Role Owner in domains that are at the root of the forest but are not the root domain (the root domain being defined as the first domain ever created in the forest). These domain controllers synchronize themselves to the PDC Role Owner in the root domain.

Any domain controller can have these settings overridden by configuring the domain controller to synchronize with an external time source using the Net Time command. If the domain controllers are so configured, then the DirectoryAnalyzer agent will check the time against the configured external time source(s).

Resolution

- Ensure that the W32Time service is running on the domain controller that has this alert.
- Check the event log on the domain controller to determine ensure that the W32Time service is not reporting errors.
- Since the domain controller must have connectivity to its time source in order to synchronize its clock, use Directory Analyzer to determine if other connectivity related alerts may be occurring.

File replication service

Indicates if the File Replication Service (Ntfrs.exe) is running on the domain controller.

Category

- Windows Services

Requirements

- **Supported on:** Windows Server® 2008
- **Required permissions**: When monitored locally, only domain user privilege is required. When monitored remotely, domain administrator privilege is required.

Resolution

Use the Services MCC snap-in or another SCP application to restart File Replication Service.

File replication (NTFRS) staging space free in kilobytes

Indicates that the amount of disk space allocated for staging files during replication is less than or equal to the specified threshold.

Category:

- Performance Counters

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

Tests the **FileReplicaSet\KB of Staging Space Free** performance counter on the domain controller to see if the value of the performance counter drops below the configured threshold for a period exceeding the configured duration.

If the File Replication Service (FRS) runs out of staging disk space, replication will stop. The size of the contents of the staging areas for all active replication sets are subtracted from the user controlled size.

A low disk space condition can be due to many different things. Some possibilities are:

- The size of the data to be replicated is larger than the staging area
- There are too many replica sets active at once
- There are files destined for one or more out-bound partners that have not been connected for a while

Resolution

One possible solution is to increase the amount of space allowed for file staging.

1. Determine that the number and size of the files that need replicating will fit in the amount of space allocated. The staging areas can be found by searching the registry.

   The **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NtFrs\Parameters\ReplicaSet** registry key contains one or more sub-keys using a GUID as the key name for each active replica set. Each replica set contains both a **Replica Set Root** and **Replica Set Stage** value.

   - The **Replica Set Root** value describes the file system folder that will be replicated.

- The **Replica Set Stage** value describes the folder that is used for the staging area. The staging areas can be inspected to determine which one(s) are consuming disk space.

2 Check the amount of space allocated by viewing the **Staging Space Limit in KB** value under the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NtFrs registry key**. This value defines the maximum amount of disk space that can be consumed by all staging areas at any one time.

3 If you determine that the staging areas need more disk space, increase the value of the **Staging Space Limit in KB**.

If the problem cannot be resolved by adjusting the amount of space needed and allowed, turn your attention towards replication schedules and the connectivity between computers. The SYSVOL share is replicated between all domain controllers in the same domain. Other replication partners can be found using the Distributed File System (DFS) console.

1 Check that the server has good connectivity with each of its replication partners. Ping the replication partners from the domain controller that issued this alert to determine if there is connectivity. The problem may be that DNS has the incorrect address or that the IP stack for the domain controller or the Directory Analyzer agent is misconfigured.

2 Use the Active Directory® Sites and Services snap-in to confirm that replication schedules allow replication partners to communicate.

GC replication latency

Indicates that the replication latency of the server that hosts a replica of the global catalog equals or exceeds the configured threshold.

NOTE: The replication latency tests create or modify objects in Active Directory®, and then check for those changes on each selected domain controller. The length of time for the tests to complete is dependent on the number of domains and domain controllers you select.

Category

- Replication Latency

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privileges with rights to list contents, create objects, read and write properties under the AATemp organizational unit in the domain root.

Description

The elapsed time between changing a distinct object on each domain controller and the time the change appears in every copy of the global catalog. This test applies to all domain controllers that host a replica of the Global Catalog.

Resolution

- Check connectivity between both the domain controller and the replication partner in question.
- Check to see that the link is reasonably clear, especially during replication.
- Check the replication schedule for the connection.
- Make sure that each partner has adequate CPU and memory resources to ensure timely servicing of replication requests.
- Make sure that the link between partners is adequate for the amount of traffic carried during replication.

Group policy object inconsistent

Indicates the Group Policy object (GPO) for a given policy has fallen out of sync with the representation stored on the local SYSVOL share.

Category

- General

Requirements

- **Supported on:** Windows Server® 2008, Window Server 2008 R2, Windows Server 2012, Window Server 2012 R2
- **Permission requirements:** When monitored locally and remotely, only domain user privilege is required.

Description

This situation typically arises from high replication latency or duplicated NTDS Connection Objects.

Resolution

A Group Policy Object on <*server-name*> is represented inconsistently between the local directory and the local file system. This problem can be remedied by forcing NTFRS and Active Directory® to refresh.

Related article

NTFRS Event ID 13557 Is Recorded When Duplicate NTDS Connection Objects Exist

Installed applications

Information only. Lists the application name, version number, vendor name, and description of the application.

Category

- General

Installed updates

Information only. Lists the update name, type of update, URL, who installed the update, and on what date it was installed.

Category

- General

Invalid primary DNS domain controller IP address

Indicates that the primary DNS service is reporting one or more invalid IP addresses for domain controllers in the domain in which the DNS server is located. An invalid IP address can cause the domain controller to be unreachable by some or all clients.

Category

- General

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016

- **Required permissions**: When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

This test queries DNS for the Service Locator (SRV) records and compares the results to the IP address reported by the Directory Analyzer agent hosted on the domain controller. The results indicate if the address retrieved in the DNS query is malformed, does not exist, or does not match the address reported by the agent.

The results are accompanied by a list of aberrant DNS SRV entries. Each entry consists of an IP address and a DNS name delimited by a single space. For example:

```
194.165.85.104 mothra.destroy.all.monsters.com
194.165.85.99 gammra.destroy.all.monsters.com
```

This situation may also occur if a domain controller is configured to obtain its IP address dynamically (via DHCP). Note that it is strongly recommended that the IP addresses of all domain controllers be statically assigned.

Resolution

Reconcile the DNS SRV entries with the IP address reported by the network adapter (or by DHCP, if applicable). The SRV entries appear under **_ldap._tcp.dc._msdcs.<zone-name>** in the DNS Management Console.

Invalid secondary DNS domain controller IP address

Indicates that the secondary DNS service is reporting one or more invalid IP addresses for domain controllers in the domain in which the DNS server is located. An invalid IP address can cause the domain controller to be unreachable by some or all clients.

Category

- General

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

This test queries DNS for the Service Locator (SRV) records and compares the results to the IP address reported by the Directory Analyzer agent hosted on the domain controller. This test indicates if the address retrieved in the DNS query is malformed, does not exist, or does not match the address reported by the agent.

This test is accompanied by a list of aberrant DNS SRV entries. Each entry consists of an IP address and a DNS name delimited by a single space. For example:

```
194.165.85.104 mothra.destroy.all.monsters.com
194.165.85.99 gammra.destroy.all.monsters.com
```

This situation may also occur if a domain controller is configured to obtain its IP address dynamically (via DHCP). Note that it is strongly recommended that the IP addresses of all domain controllers be statically assigned.

Resolution

Reconcile the DNS SRV entries with the IP address reported by the network adapter (or by DHCP, if applicable). The SRV entries appear under **_ldap._tcp.dc._msdcs.<zone-name>** in the DNS Management Console.

Kerberos Key Distribution Center service

Indicates the Kerberos Key Distribution Center (KDC) service is not currently running on the domain controller.

Category

- Windows Services

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally, only domain user privilege is required. When monitored remotely, domain administrator privilege is required.

Description

This test checks if KDC service is running.

Resolution

Use the Services MCC snap-in or another SCP application to restart the KDC service.

LDAP response time

Indicates that the response time of the domain controller to a Lightweight Directory Access Protocol (LDAP) request equals or exceeds the configured threshold.

Category

- General

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required.

Description

Active Directory® clients use LDAP to communicate with the Directory Service Agent (DSA). A high response time value indicates that the domain controller is not satisfying directory requests quickly, which can result in poor client response times and, if bad enough, login and authentication failures.

Anything that could cause a reduction in overall system performance can increase LDAP response time. For instance, running too many processes, or running processes that use too much memory or CPU can reduce system performance and increase LDAP response times.

A poorly configured server can also increase LDAP response times. For instance, if the paging file is not large enough or if the disks are badly fragmented, poor disk performance can increase LDAP response time.

In some cases faulty hardware can also cause an increase in LDAP response time. For instance, a marginal Network Interface Card (NIC) can reduce network performance on the server, and a failing disk can make directory queries take a long time.

It is possible that the DSA on the domain controller is overloaded by incoming directory requests, by excessive Access Control List (ACL) propagation, or by too many complex directory queries.

Resolution

- Determine if anything is degrading overall system performance, or if just Active Directory performance is poor.

- Check the LDAP load on the server. If this is high, try to identify the traffic that is causing the LDAP load on the server.
- Determine what processes are using the most CPU and generating the most disk I/O.
    - If a single process is generating most of the load, see if that process can be run on a different server.
    - If there are many processes using a significant amount of system resources, try to remove several of them.
    - If Local Security Authority Subsystem Service (LSASS) is using more than its share of server resources, then something is overloading the DSA.

Logic disk details

Information only. Lists the disk name, total disk size, amount of free space, percentage of used space, and whether or not the disk is compressed.

Category

- General

LSASS % processor time

Indicates that the CPU for the Local Security Authority Service (LSASS) service on the domain controller is too busy, which can indicate a problem with directory service.

Category

- Performance counters

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

Tests the Process(lsass)\% Processor Time performance counter on the domain controller for the LSASS service to see if the value of the performance counter goes above the configured threshold for a period exceeding the configured duration.

Resolution

Please refer to the documents listed below for resolutions when Lsass.exe causes high CPU usage.

Related articles

- Troubleshooting High CPU Usage on a PDC Emulator

LSASS private bytes

Indicates that the virtual memory used for Local Security Authority Service (LSASS) on the domain controller is above the preset threshold.

The amount of memory used for LSASS varies depending on the load of the computer. As the number of running threads increases, so does the number of memory stacks. Lsass.exe usually uses 100 MB to 300 MB of memory.

Lsass.exe uses the same amount of memory no matter how much RAM is installed in the computer. However, when a larger amount of RAM is installed, Lsass.exe can use more RAM and less virtual memory.

Category

- Performance Counters

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

Tests the Process(lsass)\Virtual Memory performance counter on the domain controller for the lsass service to see if the value in the performance counter goes above the configured threshold for a period exceeding the configured duration.

This situation can occur when event tracing for Security Accounts Manager (SAM) events is enabled. When event tracing for SAM events is enabled, the remote procedure call (RPC) binding is not released. Therefore, a memory leak occurs in the Lsass.exe process.

Resolution

Please refer to the Microsoft knowledge base articles listed below.

Related articles

- A Memory Leak Occurs in the LSASS Process

LSASS working set

Indicates that the working set memory used for Local Security Authority Service (LSASS) on the domain controller is above the preset threshold.

The amount of memory used for Lsass varies depending on the computer's load. As the number of running threads increases, so does the number of memory stacks. Lsass.exe usually uses 100 MB to 300 MB of memory. Lsass.exe uses the same amount of memory no matter how much RAM is installed in the computer. However, when a larger amount of RAM is installed, Lsass.exe can use more RAM and less virtual memory.

Category

- Performance Counters

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be part of the Performance Logs user group.

Description

Tests the Process(lsass)\Working Set performance counter (corresponding to Mem Usage from Task Manager) on the domain controller for Lsass to see if the value in the performance counter goes above the configured threshold for a period exceeding the configured duration.

It is also possible that the number of bytes allocated to the working set has increased to some pathological condition in a particular application.

Resolution

Please refer to the Microsoft knowledge base articles listed below.

Related articles

- A Memory Leak Occurs in the LSASS Process

Memory details

Information only. Indicates total, free, and used physical and virtual memory.

Category

- General

Memory page faults a second

Indicates that the performance of the server may be degraded because of too many page faults.

Category

- Performance Counters

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

Tests the Page Faults/sec performance counter on the domain controller to see if the number exceeds the configured threshold.

A page fault occurs whenever the Windows® 2000 operating system tries to access a virtual memory page that is not currently in memory or is in the incorrect place in memory. The process requesting the page must wait while the operating system makes room for the requested page in memory and reads it from disk or relocates it, which may cause a significant delay for the faulting process. If many processes are causing page faults, a condition known as thrashing can occur. If this happens, the performance of the server goes to zero as the operating system spends most of its time managing memory and very little running applications.

A continuously high page fault rate is an indication that the server is running too many processes with insufficient real memory. If left unattended, Active Directory® performance will suffer greatly, and eventually the directory system agent (DSA) will be unable to service requests, which can result in failed logins and authentications, as well as the inability of some applications and services to run at all.

Resolution

First, determine if the page fault rate is too high or if the threshold is set too low. Assess the overall performance of the server while the page fault rate is high. If the performance seems adequate, increase the threshold; if the performance seems poor, try to reduce the page fault rate.

To reduce the page fault rate on the server, determine if the page faults are due to a single process or a combination of several processes.

1. Run the Windows NT Task Manager and open the **Processes** tab.
2. Select **View | Select Columns**.
3. Select **Memory Delta** and **Page Fault Delta**, if necessary.

4 Observe the numbers to determine if there is one process generating page faults, or if there are several.

If there is only one process, run that program on another server or at a different time when the server is not as loaded.

If there are several processes that are generating high page fault rates, you will either have to run some of them on another server, or you will have to add more RAM to the server.

Missing domain controller SRV DNS record

Indicates one or more requisite Domain Name System (DNS) Service Locator (SRV) entries are not defined. DNS SRV entries are vital to the proper functioning of Active Directory®.

Category

- General

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

This test queries the DNS service for the SRV entries required for each zone hosted on the server. Note that this applies exclusively to zones designated as primary. This test does not evaluate SRV entries for accuracy - only that the entries are, in fact, present.

This test confirms the existence of the following SRV entries for each zone hosted on the server:

```
_ldap._tcp.<zone-name>
_ldap._tcp.dc._msdcs.<zone-name>
_ldap._tcp.pdc._msdcs.<zone-name>
_kerberos._tcp.<zone-name>
_kerberos._udp.<zone-name>
_kerberos._tcp.dc._msdcs.<zone-name>
_kpasswd._tcp.<zone-name>
_kpasswd._udp.<zone-name>
```

This test is accompanied by a list of the missing SRV entries.

Whenever a domain controller is promoted, the Microsoft NetLogon process registers the applicable SRV entries with the primary DNS server of the affected domain. As SRV entries are used to identify the constituent domain controllers, the Primary Domain Controller(PDC), and the owner of the global catalog of each zone, the absence of an SRV entry can have serious consequences for Active Directory.

The presence of all requisite SRV locator entries is evaluated for top-level zones exclusively. However, SRV locator entries of sub-zones that host at least one domain controller (with a Directory Analyzer agent) are evaluated.

Cause

Typically, missing SRV entries indicate that Dynamic DNS has been disabled for one or more DNS zones. Active Directory relies on Dynamic DNS to update all affected entries when network resources are altered or relocated. Other possible causes include DCPROMO failure, and erroneous manual configuration of SRV entries.

NOTE: Dynamic DNS can be disabled explicitly via Windows Registry settings.

Resolution

Confirm that Dynamic DNS is enabled on all applicable zones. Either add the SRV entries manually in the DNS Management Console or cause the entries to be refreshed (for example, by demoting and subsequently promoting the effected domain controllers).

NetLogon folder shared

Indicates if the NETLOGON folder is shared. File Replication Service requires this folder to be shared on domain controllers for replication to work correctly.

Category

- General

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

Logon scripts for a domain controller are found under the NETLOGON admin share for Windows® NT, whereas they are found under the SYSVOL share for Windows 2000, which can cause some confusion for Windows NT administrators not familiar with the name change. On Windows NT domain controllers, the **%SystemRoot%\System32\Repl\Import\Scripts** folder is shared as NETLOGON. Dcpromo modifies the registry value that defines the path to the NETLOGON share as part of the upgrade to **%SystemRoot%\Sysvol\Sysvol\domain_name\Scripts**.

The default folder structure for W2K is:

```
%SystemRoot%\Sysvol\Sysvol\domain_name\Policies
%SystemRoot%\Sysvol\Sysvol\domain_name\Scripts
```

Any changes to the **%systemroot%\SYSVOL** folder on any domain controller are replicated to the other domain controllers in the domain. Replication is RPC based.

You can use NETLOGON and SYSVOL to distinguish between a domain controller and a member server. If both the NETLOGON and SYSVOL shares exist on a W2K server, it is a domain controller. When dcpromo demotes a domain controller to a member server, the NETLOGON share is removed, so the presence of only SYSVOL indicates a member server.

Resolution

All potential source domain controllers in the domain should themselves have shared the NETLOGON and SYSVOL shares and applied default domain and domain controllers policy.

SYSVOL directory structure:

```
Domain
   DO NOT REMOVE NtFrs PreInstall Directory
   Policies
      {GUID}
            Adm
            Machine
            User
      {GUID}
            Adm
            Machine
            User
```

```
   {etc.,}
Scripts
Staging
Staging Areas
   MyDomainName.com
Scripts
Sysvol( sysvol share )
   MyDomainName.com
         DO NOT REMOVE NtFrs PreInstall Directory
         Policies
               {GUID}
                     Adm
                     Machine
                     User
               {GUID}
                     Adm
                     Machine
                     User
               {etc.,}
         Scripts(NETLOGON share)
```

To set the Netlogon path

1. Click **Start**, Click **Run**, type **regedit**, and press **ENTER**.
2. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters**.
3. Right-click **NetLogon**, and select **Modify**.
4. In the **Value data** box, enter the new path, including the drive letter, and click **OK**.
5. Close the Registry Editor.

To share folders with other users on your network

1. Open **My Documents** in Windows Explorer.
2. Click **Start**, point to **All Programs**, point to **Accessories**, and click **Windows Explorer**.
3. Navigate to the NETLOGON folder.
4. Click **Share this folder in File and Folder Tasks**.
5. In the **Properties** dialog box, select **Share this folder to share the folder with other users on your network**.

Related articles

- Check the Status of the SYSVOL and Netlogon Shares

NetLogon Windows service

Indicates if the NetLogon service is running on the domain controller.

Category

- Windows Services

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally, only domain user privilege is required. When monitored remotely, domain administrator privilege is required.

Resolution

Use the Services MCC snap-in or another SCP application to restart the Net Logon service.

Network adapter information

Information only. Displays the network adapter name. Indicates if DHCP is enabled, and if enabled, displays the time stamp for when the lease was obtained and when it expires, and the name of the DHCP server. Displays the domain name, DNS host name, MAC address, IP address, Subnet mask, Gateway IP address, DNS servers IP addresses, and primary and secondary WINS server IP addresses, if enabled.

Category

- General

NTDS DRA inbound properties filtered a second

Indicates directory property updates were dropped during replication.

Category

- Performance Counters

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

Tests the **NTDS\DRA Inbound Properties Filtered\second** performance counter on the domain controller to see if the value of the performance counter goes above the configured threshold for a period exceeding the configured duration.

During the replication process, Directory Service Agent (DSA) checks each incoming attribute and determines if it was modified subsequent to the version the DSA already has. If the incoming version is later than what the DSA has, the DSA will store the attribute in the directory. If the attribute is the same version or earlier than what the DSA already has, the DSA will drop the attribute, ignoring it for the purposes of replication. This is called a dropped property.

An occasional dropped property is not cause for concern, but a consistent rate of dropped properties may indicate a problem with the replication topology or with the behavior of the domain controllers. A domain controller that is consistently dropping properties during replication is wasting network bandwidth and processing time checking replicated properties that it cannot use.

Resolution

- Wait for several replication cycles to see if the problem clears up by itself.
- If the alert persists, check that the server has good connectivity with each of its replication partners.

If the alert does not clear by itself in a reasonable amount of time, contact your Microsoft® Windows® support representative.

NTDS LDAP searches a second

Indicates that the response time of the servers that host the replica of the Global Catalog (GC) equals or exceeds the configured threshold value.

Category

- Performance Counters

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

This test issues a query against a well-known object in the GC and records the time that it takes to receive a response.

Failures occur if any of the following occurs:

- The indicated domain controller does not exist.
- The server might not host the replica of the Global Catalog.
- The domain controller no longer has connectivity to the network.
- The DNS records for the domain controller are incorrect; e.g., the IP address for the domain controller is not what is published in DNS as viewed by the Directory Analyzer agent.
- Active Directory® on the domain controller has failed in some way.
- Active Directory on the domain controller is overloaded and is taking too long to respond.
- The domain controller is not running.

Resolution

- Make sure the indicated domain controller actually exists. If it is not, run NTDSUTIL and select the metadata cleanup option to clean up the erroneous objects in the directory.
- Make sure the domain controller is running. If the domain controller is not running, start it.
- Make sure the domain controller hosts a replica of the Global Catalog.
- Ping the domain controller to see if there is connectivity. If there is not, fix that problem. The problem may be that DNS has the incorrect address or that the IP stack for the domain controller or the Directory Analyzer agent is misconfigured.
- Check the LDAP response time for the domain controller on the Directory Analyzer Summary tab for the domain controller. If the LDAP response time is too high, you may need to add another domain controller for the same domain in the same site.
- If this is the only server that hosts a replica of global catalog, you may need to add another global catalog to the site.

NTDS LDAP writes a second

Indicates that the amount of Lightweight Directory Access Protocol (LDAP) traffic serviced by the domain controller equals or exceeds the configured threshold.

Category

- Performance Counters

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016

- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

Tests the **NTDS LDAP writes a second** performance counter on the domain controller to see if the value goes above the configured threshold for a period exceeding the configured duration.

Active Directory® clients use LDAP to communicate with the Directory Service Agent (DSA). A high LDAP load indicates that a lot of clients are making many requests of the DSA. Increased LDAP load can reduce the throughput of the DSA, and can cause important directory transactions, such as login and authentication, to fail.

Resolution

Identify the source of the LDAP traffic by using a network traffic analyzer. Note that a traffic analyzer will not detect the traffic generated by a process running on the domain controller itself.

- If the majority of LDAP traffic is due to a single process, terminate that process or redirect it to another less loaded server.

If the traffic is due to many different workstations, the problem may be that there are not enough functioning domain controllers or global catalogs in the site.

NTFRS % processor time

Indicates that the CPU for the NTFRS service on the domain controller is too busy, which can indicate a problem with Windows File Replication Service (FRS).

Category

- Performance counters

Requirements

- **Supported on:** Windows Server® 2008
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

Tests the Process(ntfrs)\% Processor Time performance counter on the domain controller for the ntfrs service to see if the value of the performance counter goes above the configured threshold for a period exceeding the configuration duration.

Excessive CPU usage by FRS can be caused by an application that is unnecessarily changing all or most of the files in a replica set on a regular basis. For example, an antivirus software package might be rewriting the ACL on many files, causing FRS to replicate these files unnecessarily.

Resolution

You can use one of the following methods to identify excessive replication generators:

- Selectively turn off common causes such as antivirus software, defragmentation tools, and file system policy, and determine if this activity declines.
- Inspect the NTFRSUTL OUTLOG report to see which files are being replicated.
- Inspect the USN journal tracking records in the FRS debug logs on computers running Windows SP2 or later with the following command: Findstr /I ":U:" %systemroot%\debug\ntfrs_00*.log

Related articles

- Antivirus programs may modify security descriptors and cause excessive replication of FRS data in SYSVOL and DFS

- The Effects of Setting the File System Policy on a Disk Drive or Folder Replicated by the File Replication Service
- Possible Causes of a Full File Replication Service Staging Area

NTFRS process private bytes

Indicates that the virtual memory used for the NTFRS service on the domain controller is above the preset threshold, which can indicate a problem with Windows File Replication Service (FRS).

The FRS (NTFRS.exe) is a multi-threaded, multi-master replication engine that replaces the LMREPL (LAN Manager Replication) service in Microsoft Window NT versions 3.x and 4.0. Windows 2008 domain controllers and servers use FRS to replicate system policies and login scripts for Windows 2008, Windows Vista, and down-level clients.

Category

- Performance Counters

Requirements

- **Supported on:** Windows Server® 2008
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

Tests the Process(NTFRS)\Virtual Memory performance counter on the domain controller for the NTFRS service to see if the value in the performance counter goes above the configured threshold for a period exceeding the configured duration.

Resolution

Please refer the Microsoft® knowledge base article listed below.

Related articles

- Troubleshooting File Replication Service

NTFRS working set

Indicates that the working set memory used for the NTFRS service on the domain controller is above the preset threshold, which can indicate a problem with Windows® File Replication Service (FRS).

The FRS (NTFRS.exe) is a multi-threaded, multi-master replication engine that replaces the LMREPL (LAN Manager Replication) service in Microsoft® Windows® NT versions 3.x and 4.0. Windows Server® 2008 domain controllers and servers use FRS to replicate system policies and login scripts for Windows Server 2008, Windows Vista, and down-level clients.

Category

- Performance Counters

Requirements

- **Supported on:** Windows Server® 2008
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

Tests the Process(NTFRS)\Working Set performance counter on the domain controller for the NTFRS service to see if the value in the performance counter goes above the configured threshold for a period exceeding the configured duration.

It is also possible that the number of bytes allocated to the working set has increased due to some pathological condition in a particular application.

Resolution

Please refer the Microsoft® knowledge base articles listed below.

Related articles

- Troubleshooting File Replication Service

Operating system details

Information only. For each selected domain controller, displays the names of the forest, domain, and site; the operating system, version number, installed service pack, and installation date; if the domain controller is a global catalog server or a read-only domain controller; the system time, time stamp for the last boot, and how long the system has been up; the system drive, system directory, Windows directory, boot device, system device, and amount of system memory.

Category

- General

Primary DNS resolver not responding

Indicates one or more of the configured primary DNS resolver for a domain controller is not responding.

Category

- General

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

The test for responsiveness is done by timing the lookup of critical DNS service records from each resolver.

Resolution

Check to make sure that the identified resolver is actually available and responsive.

Secondary DNS resolver not responding

Indicates one or more of the configured secondary DNS resolver for a domain controller is not responding.

Category

- General

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

The test for responsiveness is done by timing the lookup of critical DNS service records from each resolver.

Resolution

Check to make sure that the identified resolver is actually available and responsive.

Server sessions

Indicates the number of Server Message Block (SMB) connections in use on the domain controller equals or exceeds the configured threshold.

Category

- Performance Counters

Requirements

- **Name: Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

Tests the Server\Server Sessions performance counter on the domain controller to see if the value of the performance counter goes above the configured threshold for a period exceeding the configured duration.

System Message Block (SMB) is the protocol Windows 2000 uses for file and print access. Whenever a client workstation accesses files or directories on a server, or whenever the workstation prints a document to a network printer, the client uses an SMB connection.

The number of SMB connections in use on a server is a rough indication of the number of client workstations that are accessing the servers. An unusually high number of SMB connections indicates a large number of clients accessing the server.

A large number of SMB connections will use some amount of memory on the server, though this is generally not a big problem. However, the inordinate number of clients accessing the server can have a negative effect on overall server performance and consequently a negative effect on directory performance as well.

Resolution

Determine if the increased number of SMB connections is degrading the overall performance of the server. If the performance is being affected, run other tests, including LDAP response time, CPU processor time, Cache copy read hits, and Memory page faults a second.

- If these other tests are within limits, the increased number of SMB connections is not adversely affecting the performance of the domain controller.
- If these other tests are outside the limits, the performance of the DSA is being adversely affected, and you should try to reduce the number of clients connected to the domain controller.

SysVol details

Information only. Displays the device total size, amount of free space, and percent used; the size of SysVol and the percent of device used; and the path to SysVol.

Category

- General

SysVol folder shared

Indicates if the SYSVOL folder is shared. File Replication Service requires this folder to be shared on domain controllers for replication to work correctly.

Category

- General

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

The Sysvol folder is shared on an NTFS volume on all the domain controllers in a particular domain and is used to deliver the policy and logon scripts to domain members. By default Sysvol includes two shared folders, where the scripts folder is shared with the name NETLOGON:

- %SystemRoot%\Sysvol\Sysvol\domain_name\Policies
- %SystemRoot%\Sysvol\Sysvol\domain_name\Scripts

The file replication service (FRS) replicates these folders among all domain controllers in the domain. If this folder is not shared, the FRS cannot replicate it.

The test checks the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\Shares\SYSVOL** registry key. If the key is not present, the SYSVOL folder is not shared and cannot be replicated.

Resolution

SYSVOL directory structure:

Domain

```
DO NOT REMOVE NtFrs PreInstall Directory
Policies
        {GUID}
             Adm
             Machine
             User
        {GUID}
             Adm
             Machine
             User
        {etc.,}
Scripts
Staging
Staging Areas
        MyDomainName.com
```

Scripts

```
Sysvol( sysvol share )
      MyDomainName.com
            DO NOT REMOVE NtFrs PreInstall Directory
            Policies
                  {GUID}
                        Adm
                        Machine
                        User
                  {GUID}
                        Adm
                        Machine
                        User
                  {etc.,}
      Scripts(NETLOGON share)
```

To set the SYSVOL path

1. Click **Start**, click **Run**, type **regedit** and press **Enter**.
2. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters**.
3. Right-click **SYSVOL**, and select **Modify**.
4. In the **Value data** box, enter the new path, including the drive letter, and click **OK**.
5. Close the Registry Editor.

> **NOTE:** The path in the registry points to the SYSVOL folder located inside the SYSVOL folder that is under the root. When updating the path in the registry, ensure that it still points to the SYSVOL folder inside the SYSVOL folder that is under the root.

To share folders with other users on your network

1. Open My Documents in Windows® Explorer.
2. Click **Start**, point to **All Programs**, point to **Accessories**, and click **Windows Explorer**.
3. Navigate to the SYSVOL folder.
4. Click **Share this folder in File and Folder Tasks**.
5. In the **Properties** dialog box select **Share this folder to share the folder with other users on your network**.

Related articles

- Troubleshooting Missing SYSVOL and NETLOGON Shares on Windows 2000 Domain Controllers

Windows Time service

Indicates if the Windows® Time (W32Time) service is running on the domain controller.

Category

- Windows Services

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: When monitored locally, only domain user privilege is required. When monitored remotely, domain administrator privilege is required.

Resolution

Use the Services MCC snap-in or another SCP application to restart the W32Time service.

Site tests

- No authority in site to resolve universal group memberships
- Inter-site replication manager
- Inter-site replication topology generation disabled
- Intra-site replication topology generation disabled
- Morphed directories exist in site
- Too few global catalog servers in site
- Site details
- Too few global catalog servers in site

No authority in site to resolve universal group memberships

Indicates if a specified site has no global catalog and if universal group membership caching is disabled. While this is a valid configuration for a site, if the site is connected through a slow link, it can result in poor logon performance.

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege is required.

Resolution

- Configure a domain controller as a global catalog server.
- Enable universal group membership caching.

Related articles

- Configure a domain controller as a global catalog server
- Enable Universal Group Membership Caching in a Site

Inter-site replication manager

Indicates if a domain controller, other than the preferred bridgehead server(s), is actively replicating outside of its current state.

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege is required.

Description

Active Directory® allows administrators to configure preferred bridgehead servers for each site. Sometimes connection objects are created manually to solve a quick problem, but they are never removed. If these manually-created links are actively replicating, undesirable results may occur.

Resolution

It is possible that this is a transient issue caused by Active Directory replication delays associated with updating File Replication service (FRS) configuration objects. If file replication does not take place after an appropriate waiting time, which could be several hours if cross-site Active Directory replication is required, you must manually reset the preferred bridgehead server.

Related articles

- Designate a preferred bridgehead server
- NTFRS Event ID 13557 is Recorded When Duplicate NTDS Connection Objects Exist

Inter-site replication topology generation disabled

Indicates if the inter-site replication topology generation functionality of the Knowledge Consistency Checker (KCC) has been explicitly disabled. While disabling the KCC is a valid administrator action, it can result in poorly-tuned replication topologies.

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege is required.

Resolution

Clear the fifth bit (16) of the **<Root Domain>\Configuration\Sites\<Site name>\NTDS Site Settings\options** value to re-enable inter-site topology generation.

Related articles

- The Role of the Inter-Site Topology Generator in Active Directory Replication
- How to Optimize Active Directory Replication in a Large Network
- How to Disable the Knowledge Consistency Checker From Automatically Creating Replication Topology
- Troubleshooting Event ID 1311: Knowledge Consistency Checker
- How to Disable the Knowledge Consistency Checker Inter-Site Topology Generation for All Sites

Intra-site replication topology generation disabled

Indicates if the intra-site replication topology generation functionality of the Knowledge Consistency Checker (KCC) has been explicitly disabled. While disabling the KCC is a valid administrator action, it can result in poorly-tuned replication topologies.

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege is required.

Resolution

Clear the first bit (1) of the **<Root Domain>\Configuration\Sites\<Site name>\NTDS Site Settings\options** value to re-enable inter-site topology generation.

Related articles

- The Role of the Inter-Site Topology Generator in Active Directory Replication
- How to Optimize Active Directory Replication in a Large Network
- How to Disable the Knowledge Consistency Checker From Automatically Creating Replication Topology
- Troubleshooting Event ID 1311: Knowledge Consistency Checker
- How to Disable the Knowledge Consistency Checker Inter-Site Topology Generation for All Sites

Morphed directories exist in site

Indicates if morphed directories are found in a replica tree.

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege is required.

Description

All files and folders that File Replication Service (FRS) manages are uniquely identified internally by a special file identifier. FRS uses these identifiers as the canonical identifiers of files and folders that are being replicated. If FRS receives a change order to create a folder that already exists, which by definition has a different file identifier than the duplicate folder, FRS protects the conflicting change by leaving the original directory structure intact, and renaming the conflicting directory to a unique name so that underlying files and folders can be preserved. The conflicting folder is given a new name in the following format: **<*FolderName*>_NTFRS_<*GUID*>**, where **<*FolderName*>** is the original name of the folder and <***GUID***> is a unique character string, such as 001a84b2.

Common causes of this condition are:

- A folder is created on multiple machines in the replica set before the folder has been able to replicate. This could be due to the administrator or application duplicating folders of the same name on multiple FRS members.
- You initiated an authoritative restore on one server and did not stop the service on all other members of the re-initialized replica set before restarting FRS after the authoritative restore.
- You initiated an authoritative restore on one server and did not set the D2 registry key for the authoritative restore on all other members of the re-initialized replica set before a server replicated outbound changes to re-initialized members of the replica set.
- You initiated an authoritative restore on one server and manually copied directories with names identical to those being replicated by FRS to computers in the replica set.

Resolution

- Move the morphed directories out of the replica tree and back in. This method works well for small amounts of data on a small number of targets. However, if you miss end-to-end replication of the move-out, this method can cause morphed directories. This method also forces all members to re-replicate data.
- Rename the morphed directories. This method does not require re-replication of data, however, it can cause a denial-of-service condition by giving an invalid path when the originating path is renamed.

Site details

Information only.

Table 5. Site details

Field	Description
Group caching enabled	Indicates if group caching is enabled or disabled.
Intersite topology generation	Indicates if intersite topology generation is enabled or disabled.
Intrasite topology generation	Indicates if intrasite topology generation is enabled or disabled.
Intersite topology generator	Name of the intersite topology generator.
Domain controllers	Number of domain controllers
Site links	Number of site links.

Too few global catalog servers in site

Indicates if the number of global catalog servers in a given site is less than or equal to the configured threshold.

Requirements

- **Supported on:** Windows Server® 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016
- **Required permissions**: Domain user privilege is required.

Description

Each site in an Active Directory® enterprise should have at least one domain controller configured as a global catalog. The workstation login process always attempts to contact a global catalog server, and if none are running at the site where the workstation resides, the workstation will connect to a global catalog server outside of the site, which can cause excess WAN traffic and unnecessary delays in the login process.

Resolution

- Configure a domain controller as a global catalog server.

Related article

- Configure a domain controller as a global catalog server

6

Active Directory Topology

Viewing Active Directory forest topology

For a selected forest, you can view and customize a topology diagram, and quickly see a list of domain controllers with their roles.

To view Active Directory topology

1. Select **Monitor | Active Directory Topology**.
2. Type a forest name, or click in the box to select from a list of previously discovered forests.
3. Every three hours, the Active Administrator® Foundation Service (AFS) server updates the topology data in the cache with the latest data from Active Directory® Service. If you want to update the forest topology data when you run the topology and update the domain controller list, select **Update topology**. Otherwise, if the check box is not selected, the forest topology data is loaded from the cache.

   NOTE: Once you click ▶ to load the forest topology data and update the domain controller list, the check box is hidden from the display. To restore the check box, clear the forest name box.

4. Click ▶ to load the forest topology data.

   NOTE: If you typed a forest name that is not in the list of previously discovered forests or if the **Update topology** check box is selected, a pop-up message displays every 15 seconds while data is being collected by the computer running Active Administrator®. If the forest is large, there may be a delay loading the domain controller list.

5. Select the domain controllers.

   To filter the list, start typing in the **Search domain controllers** box. The list filters as you type. To clear the filter, press **Esc**.

   NOTE: It is recommended that you limit the number of domain controllers in the diagram to 80 or less.

6. Click **Run**.

   The **Topology** tab opens to display an interactive forest topology diagram. The intra-site replication links are shown in blue and the inter-site replication links are shown in gray. You can click and drag the sites and domain controllers to rearrange the diagram. See Customizing the topology layout.

7 Use the tool bars to manipulate the topology diagram. There are two tool bars for the Topology Viewer. One is located at the top of the page and the second is located below the diagram design area

Table 1. Topology tool bar at the top of the page

Option	Description
Print	Print the topology diagram.
Zoom to fit	Zoom the diagram to fit the screen vertically. If the diagram fits the screen vertically, zooms the diagram to fit the screen horizontally.
Auto layout	Switch between the current layout and an optimized layout, which minimizes overlap between the site or domain nodes. **NOTE:** If the layout is already optimized, a message displays.
Reload	Reload the last saved layout.
Save layout	Save the layout for the selected forest topology. See Customizing the topology layout.
Edit layout	Edit the layout for the selected forest topology. See Customizing the topology layout.
Show alert	Show or hide the server and replication alert status. See Viewing alerts.
Help	Displays list of keyboard shortcuts. See Table 3: Keyboard Shortcuts.

Table 2. Topology diagram tool bar under the topology diagram design area

Option	Description
Refresh	Refresh the alerts. If **Alert** is not selected, clicking **Refresh** displays the Alert Summary. See Viewing alerts.
Pause	Pause the alert refresh.
Domain view	Select to view the domain topology.
Site view	Select to view the site topology.
Alert status	If **Alert** is selected, displays the date and time of the last update and the number of alerts that match the topology diagram.

Viewing alerts

Every 300 seconds, the topology diagram is updated to get server alert status from the Active Administrator foundation server (AFS). The node for each domain controller displays in a color to indicate its status.

- Green: no alert is detected
- Red: critical alerts are detected
- Orange: warning alerts are detected
- Grey: domain controller or site is not monitored by a Directory Analyzer agent

When replication latency alerts are detected, the color of the link between domain controller nodes indicates the status.

- Red: critical alerts are detected
- Orange: warning for latency exceed the threshold defined by user in Active Administrator console).

NOTE: Replication latency alerts are turned off by default. You must enable this alert in the Active Administrator console. See the *Quest® Active Administrator® User Guide*.

To view alerts

- Click **Show alerts** in the tool bar.

> **NOTE:** If **Show alerts** is not selected, clicking **Refresh** also displays the list of alerts.

The list of alerts displays below the diagram in the **Alert Summary** area. The alert severity, alert name, source, domain, and the alert start time display.

You can refresh or pause the refresh of the alerts.

> **NOTE:** The alerts that display in the Topology Viewer relate to the displayed diagram and is not a complete list of alerts.

Filtering alerts

To filter the list of alerts

- Click the node or link that indicates alerts are present. If you click a node outlined in red or orange, the alert list filters to match the status of the selected node. If you click a domain controller, only the alerts for that domain controller display.

  -OR-

  Type the domain controller in the **Search alerts** box. Only the alerts for that domain controller display.

Viewing alert details

To view alert details

- Click the alert link in the **Alert** column to view the alert description.
- Click **Alert details** in the **Alert description** box to view details about the alert.

Customizing the topology layout

You can change the forest topology layout by dragging the domain controller and site objects on the topology diagram. If you chose to save the layout, the layout is associated with the forest in the cache and loads the next time you run the topology on that forest. Each user can create their own layout that is associated with their user account.

To customize the forest layout

1. Click **Edit layout** in the tool bar.

   > **NOTE:** While you are editing the diagram, the **Show alerts** check box is cleared and the alerts list is hidden.

2. Click and drag site objects to new locations with the design area, which is delineated by the thin blue line. Within a site diagram, click and drag domain controllers to new locations. The site diagrams automatically resize as you drag the domain controllers around.

   > **NOTE:** If the forest topology diagram exceeds the design area, click **Zoom** to fit the diagram within the design pane.

3. If you are using a keyboard, use the keyboard shortcuts to zoom in and out. If you are using a touch screen, use the pinch gesture to zoom in and out.

   > **NOTE:** Click inside the design pane before applying the zoom controls. If you do not see the blue outline of the design area, the zoom controls apply to the browser window.

Table 3. Keyboard shortcuts

Keyboard shortcut	Description
Ctrl +	Zoom in
Ctrl -	Zoom out
Ctrl + mouse wheel	Zoom diagram in or out
Shift + mouse wheel	Move the diagram horizontally

NOTE: If you previously saved the layout and want to clear the changes you make to the layout, click **Undo Layout** to return the diagram to the last saved layout. If you have not saved the layout and want to return the diagram to the original state, open the **Discover Forest** tab and run the discovery again.

4 Click **Save Layout**.

7

Reports

Running reports

Several reports are available to help you manage your organization. Once you run a new report, the report remains open until you run another report. You can refresh the parameters and run the report again. You also can rerun an existing report from the **History** tab.

To run a report

1. Open Active Administrator® in a web browser. See Opening Active Administrator in a web browser.
2. Click **Report**.
3. Select a report category.
   - Active Directory Health reports
   - Active Directory Infrastructure reports
   - DNS reports
   - Security reports
4. The landing page for the report category displays the available reports.
   - To filter the list of reports, start typing in the **Search report** box. The list of reports changes as you type.
   - To switch to list view, click  . To sort the reports in list view, click the column heading.
   - To switch to grid view, click  . To sort the reports in grid view, click the icon to sort the report names in ascending or descending alphabetical order.
5. Select a report. You can create a new report or run an existing report.

   To run a new report

   a. On the **Parameters** tab, enter the parameters for the report.

   > **NOTE:** Start typing in the **Domain Name** box, and a list of domains will filter and display. Select from the list of domains, and click  to load the list of target domain controllers or click  to add the domain to the list.
   >
   > **NOTE:** Use Ctrl and Shift to select multiple parameters.

   b. Click **Run**.

To run an existing report

a Open the **History** tab.

b Select a report.

The **Reports** tab displays the report.

- If the report generation is taking too much time, you can click **Cancel**.
- The report remains open in the **Reports** tab until you run another report of this type. To redisplay the report with fresh data, click **Refresh**.
- To print the report, click **Print**.
- To return to the list of reports, click **Back to Reports**.

Active Directory Health reports

NOTE: To access and run Active Directory Health reports, you must have a license to the Active Directory Health module.

To access Active Directory Health reports

1 Open Active Administrator® in a web browser. See Opening Active Administrator in a web browser.

2 Select **Reports | Active Directory Health**.

3 Select a report. See Running reports.

Table 1. Active Directory Health reports

Report	Description
Active Directory White Space	Displays white space events (Event ID 1646 – the amount of disk space that can be recovered by offline defragmentation) in the NTDS event log. The results indicate if White Space Logging is enabled, the amount of white space in the database, the size of the Active Directory® database, and the number of events. **NOTE:** You must set the Garbage Collection value in the registry to view Event ID 1646. See https://technet.microsoft.com/en-us/library/cc816652(v=ws.10).aspx. **Minimum required permission:** The Active Administrator Foundation service (AFS) account must have read access to HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics\ registry key on the remote system or the AFS account should be a member of the Server Operators group in Active Directory.
AD Diagnostic Event Logging Levels	Lists values and descriptions for each event log level for the selected domain controller. **Minimum required permission:** The Active Administrator Foundation service (AFS) account must have read access to HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics\ registry key on the remote system or the AFS account should be a member of the Server Operators group in Active Directory.

Table 1. Active Directory Health reports

Report	Description
AD Disk Space	Lists file locations, page file information, Active Directory file location check, file information, disk usage, and SYSVOL information. **Minimum required permission:** The Active Administrator Foundation service (AFS) account must have read access to: • HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters\ registry key on the remote system, • the SYSVOL directory, and • the folder where the Active Directory databases are located.
Application Event Log	Lists events generated by applications for a specified domain controller. You can filter the report by text, event ID, and event type, and specify the number of events and the time period. **Minimum required permission:** The Active Administrator Foundation service (AFS) account must be a member of the Event Log Readers group in Active Directory.
Authentication Methods	Lists RootDSE and Registered Service Principal Name attributes and values resulting from the authentication of the specified domain controller using three methods: negotiate authenticated LDAP, NTLM authenticated LDAP, and un-authenticated LDAP. **Minimum required permission:** Domain User rights.
Bind with RID Master	Lists the relative identifier (RID) master role and the results of the binding (DSBind) with the selected domain controller. **Minimum required permission:** Domain User rights.
Conflicting Objects	Lists the object and the conflicting object including the date and time of creation. **Minimum required permission:** Domain User rights
Connection Object Duplicates	Lists the duplicated connection objects for the selected domain controller. **Minimum required permission:** Domain User rights.
Cross-Domain Linked GPOs	Lists the number and names of GPOs that are linked to a different domain. **Minimum required permission:** Domain User rights.
DC Adapter Information	Displays information from WMI regarding the network adapters present on the specified domain controller(s). **Minimum required permission:** Domain User rights and the Active Administrator Foundation service (AFS) account must have Enable Account and Remote Enable WMI Security permissions for the target servers.
DC Advertising	Lists the services advertised by the domain controller to the Directory Service. **Minimum required permission:** Domain User rights.
DC Connection Objects	Lists the connections objects, with details, from the domain controllers that are used during replication. **Minimum required permission:** Domain User rights.
DC Consistency	Compares domain controller level configurations between two or more domain controllers in a domain. **Minimum required permission:** Domain User rights.

Table 1. Active Directory Health reports

Report	Description
DC Information	Displays the following information for the specified domain controller(s) as held by the Directory Service: Domain Controller name, NetBIOS Name, Domain Name, Domain Controller GUID, Domain Controller SID, DNS Forest Name, Domain GUID, Domain SID, Site name, Client site name, Address, and Address type, and Domain Controller Roles. **Minimum required permission:** Domain User rights.
DC Operating System Information	Displays information about the operating system installed on the specified domain controller(s). **Minimum required permission:** Domain User rights and the Active Administrator Foundation service (AFS) account must have Enable Account and Remote Enable WMI Security permissions for the target servers.
DC Replica State	Displays the state of the replicas of a domain in relation to the selected domain controllers. **Minimum required permission:** Domain User rights.
DC Roles	Indicates which of the following operations master roles are being performed by the specified domain controller(s): Inter-site Topology Generator, Schema Master, Infrastructure Master, RID Master, Domain Naming Master, PDC Emulator Manager, and Global Catalog Manager. **Minimum required permission:** Domain User rights.
DC RootDSE	Displays the values of the attributes in the RootDSE for the specified domain controller(s). **Minimum required permission:** Domain User rights.
DC Security Configuration	Checks core security configurations on one or more domain controllers and compares them against the Microsoft® Best Practices guidelines. This report highlights any configuration parameters that exceed the recommended guidelines and provides recommendations to correct the issue(s) reported. **Minimum required permission:** Domain user rights, WMI rights, and File System rights.
DC Services	Displays the following information for all services on the specified domain controller(s) as held by the Service Control Manager: Service Name, Display Name, Status, Startup Type, and Log On As. **Minimum required permission:** Domain Administrator rights.
DC Site Coverage	Lists the sites covered by the specified domain controller. The information is derived from the site coverage key. **Minimum required permission:** Domain User rights.
DC Sites	Displays a list of all the domain controllers and the site to which each belongs for the specified domain. **Minimum required permission:** Domain User rights.
DC SPNs	Lists the Service Principal Name (SPN) for all services on the specified domain controller. **Minimum required permission:** Domain User rights.

Table 1. Active Directory Health reports

Report	Description
Directory Health Alerts	Displays a detailed Directory Health alerts report. You can choose the date or date range, and the specific alerts to include. **NOTE:** You can also access this report from **Monitor | Active Directory Health | Alert History | Report**. See Generating an alert history report. **Minimum required permission:** Domain User rights and the Active Administrator Foundation service (AFS) account must be a member of the AA_Admins group either in the domain or on the database server, depending on the configuration selected during setup.
Directory Objects	Displays a count, in both a horizontal bar graph and a table, of the number of specified directory objects in a specified domain over a specified time period. Directory objects include user, group, computer, group policy objects, and organizational units. **Minimum required permission:** Domain User rights and the Active Administrator Foundation service (AFS) account must be a member of the AA_Admins group either in the domain or on the database server, depending on the configuration selected during setup.
Directory Service Event Log	Lists events from the Directory Service Event Log for the specified domain controller. **Minimum required permission:** The Active Administrator Foundation service (AFS) account must be a member of the Event Log Readers group in Active Directory.
Directory Service Parameters	Lists directory service configuration parameters from the registry: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters **Minimum required permission:** The Active Administrator Foundation service (AFS) account must have read access to HKLM\CurrentControlSet\Services\NTDS\Parameters\ registry key on the remote system or the AFS account should be a member of the Server Operators group in Active Directory.
Disk Drives	Displays detailed information about all of the fixed drives in the selected domain controller(s), such as Name, Type (e.g., NTFS, FAT), Capacity, Free Space (amount and percentage), System Volume (yes/no), and whether the drive contains the Active Directory database, SYSVOL, and/or Active Directory Log Files. **Minimum required permission:** The Active Administrator Foundation service (AFS) account must have read access to HKLM\CurrentControlSet\Services\NTDS\Parameters\ registry key on the remote system, or be a member of the Server Operators group in Active Directory.
Distributed File System (DFS) Shares	Lists the Distributed File System (DFS) shares available on a domain controller, including the following information for each DFS share: entry path, volume state and timeout, comments associated with the DFS share, and the DFS storage entry(s) associated with the name including server name, share name, and storage state. **Minimum required permission:** Domain User rights.

Table 1. Active Directory Health reports

Report	Description
Distributed File System Replication	Lists Distributed File System Replication (DFSR) partners, DFSR service information, connection objects, SYSVOL statistics, connectivity tests, and recent event log messages. Optionally, if the DFSR service is not running, you can choose to start the DFSR service on the target domain controller and on its DFSR partners. The default setting is to not start the DFSR service. You also can choose to include details about the files and folders that were moved to the Conflict and Deleted folder due to conflicting updates. **NOTE:** Requesting details about the files and folders may add considerable time to the report generation. **Minimum required permission:** Domain User rights and the Active Administrator Foundation service (AFS) account must have Enable Account and Remote Enable WMI Security permissions for the target servers.
DNS Configuration	Displays DNS configuration information from the specified domain controller. The results include Registry keys and values from HKLM\System\CurrentControlSet\Services\ DNS\Parameters, zones hosted on the specified domain controller, DNS Service Information, and Active Directory DNS Information. **Minimum required permission:** Domain User rights and the Active Administrator Foundation service (AFS) account must have Enable Account and Remote Enable WMI Security permissions for the target servers.
DNS Event Log	Lists events from the DNS Server Event Log for the specified domain controller. **Minimum required permission:** Domain Administrator rights.
DNS Zone Information	Displays zone information for the specified domain controller. The results include the DNS server and forward zone parameters and values. **Minimum required permission:** The Active Administrator Foundation service (AFS) account must have read access rights to all DNS zones on the target DNS servers, and Enable Account and Remote Enable WMI Security permissions for the target servers.
DNS Zones	Lists the zones for the specified domain controller. **Minimum required permission:** The Active Administrator Foundation service (AFS) account must have read access rights to all DNS zones on the target DNS servers and Enable Account and Remote Enable WMI Security permissions for the target servers.
Domain Advertising	Displays the roles being advertised by each domain controller in the specified domain, and verifies that all domain controllers in the domain are properly registered. **Minimum required permission:** Domain User rights.
Domain Configuration	Lists domain role holders, Group Policy objects, protected groups, domain administrators, and trusted domains. **Minimum required permission:** Domain User rights.
Domain Controllers	Lists all domain controllers for the specified domain. Information includes the DNS host name, IP address and the distinguished name for each domain controller in the domain. **Minimum required permission:** Domain User rights.
Domain Controllers without replication links	Lists the domain controllers without replication links. **Minimum required permission:** Domain User rights.

Table 1. Active Directory Health reports

Report	Description
Domain Naming Masters	Lists all the Domain Naming Masters in a given forest and domain. **Minimum required permission:** Domain User rights.
Domain Role Holders	Lists all servers that hold the following operation masters: • PDC Operations Master • RID Operations Master • Infrastructure Operations Master • Schema Operations Master • Domain Naming Operation Master **Minimum required permission:** Domain User rights.
Domains	Lists all the domains in a given forest, along with the number of sites, domain controllers, and directory objects associated with each domain. Click on a number of sites, domain controllers, or directory objects to drill down to a greater level of detail. **Minimum required permission:** Domain User rights.
Drivers List	Lists all the drivers on the specified domain controller. The results include the following properties for each driver: Display Name, Driver Name, State, and Status. **Minimum required permission:** Domain Administrator rights.
Duplicate SIDs	Lists duplicate SIDs for the selected domain controller. **Minimum required permission:** Domain User rights.
Event Log	Lists the events from selected event logs on the selected domain controller. You can filter events based on text, event ID, date, or event status. **Minimum required permission:** The Active Administrator Foundation service (AFS) account must be a member of the Event Log Readers group in Active Directory. **NOTE:** If selecting the DNS Event Log the AFS account must also have Domain Administrator rights.
Event Log Errors	Lists all the Event Log errors on the selected domain controller In the last day, week, and month. **Minimum required permission:** The Active Administrator Foundation service (AFS) account must be a member of the Event Log Readers group in Active Directory. **NOTE:** If selecting the DNS Event Log the AFS account must also have Domain Administrator rights.
Forest Configuration	Displays forest configuration details, such as role holders, partition information, and counts of GPOs and connection objects. **Minimum required permission:** Domain User rights.

Table 1. Active Directory Health reports

Report	Description
Forest Inventory	Displays an inventory of all forests previously discovered by Active Administrator, along with the number of domains, sites and domain controllers associated with each forest. To view forest inventory with greater level of detail, enter the forest name or select the forest name in the **Summary** area, and run the report. **NOTE:** When Active Administrator Foundation Service (AFS) starts, it refreshes the Active Directory forest cache in the Directory Analyzer cache folder. If no forest is found in the cache, AFS automatically discovers the current forest where the Active Administrator server is installed, and adds that forest topology to the cache folder. **NOTE:** By default, AFS refreshes the forest cache every three hours. To change the refresh schedule, edit the **RefreshForestCacheIntervalHours** value in the registry key below and restart the AFS service. To disable the scheduled refresh of the forest cache, set this value to zero. • **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Quest Software\Active Administrator\Settings\AFS** **Minimum required permission:** Domain User rights and the AFS account must have read and write access to the Active Administrator share.
Global Catalogs	Lists all the Global Catalogs in a given forest and domain. **Minimum required permission:** Domain User rights.
GPO Consistency	Performs a Cyclic Redundancy Check (CRC) of the Group Policy Object (GPO) files on two or more selected domain controllers. The results display a list of inconsistent policies found between the specified domain controllers. **Minimum required permission:** Domain User rights.
Ineffective GPO	Lists policies that are not linked, as well as all policies that are linked, but currently in a disabled stated, which renders them ineffective. Information includes the display name of the group policy, its unique ID, and a brief description why it is considered an ineffective link. **Minimum required permission:** Domain User rights.
Infrastructure Masters	Lists all the Infrastructure Masters in a given forest and domain. **Minimum required permission:** Domain User rights.
Installed Updates	Displays the current service pack information for the specified domain controller, including when the service pack was installed and who installed it. **Minimum required permission:** Domain Administrator rights.
Inter-site Topology Generators	Lists all the Inter-site Topology Generators in a given forest. **Minimum required permission:** Domain User rights.
Lost and Found Items	Lists the lost and found items for the specified domain controllers. **Minimum required permission:** Domain User rights.
Naming Context Metadata	Displays the following information for each domain controller in the specified naming context: local USN, originating DSA, originating USN, originating time/date, version, and attribute. **Minimum required permission:** Domain User rights.

Table 1. Active Directory Health reports

Report	Description
Naming Context Topology	Checks that the generated topology is fully connected for all domain controllers, and checks the connection objects and the naming context (NC) header where RepsFrom and RepsTo is saved. The results include the sites in the domains, and domain controller replication topology and intersite replication information. **Minimum required permission:** Domain user rights.
Naming Context Topology Aliveness	Initiates a replication of the selected domain and reports the results of the replication. The results include the following synchronization information: source server, destination server, event, and event description. **Minimum required permission:** Domain User rights.
Naming Context Up-to-Dateness	Displays the Up-to-Dateness vector from the state information of the directory service for the specified domain. **Minimum required permission:** Domain User rights.
Owner Information	Lists the global advertised services known by the specified domain controller. The advertised services are Global Catalog, Time Server, Preferred Time Server, Primary Domain Controller (PDC) emulator, and Key Distribution Center (KDC). The results include the server holding the service, the ping times, and other advertised services held by that server. **Minimum required permission:** Domain User rights.
PDC Emulators	Lists all the PDC (Primary Domain Controller) Emulator Masters in a given forest and domain. **Minimum required permission:** Domain User rights.
Ping Global Catalog	Lists all Global Catalog servers in the specified domain. The results include the total number of GCs in the domain and the ping times for each GC. **Minimum required permission:** Domain User rights.
Remote Access Information	Displays the settings and status of the current active remote access connections for the specified domain controllers. **Minimum required permission:** Domain Administrator rights.
Replication Failures	Lists the results of replication operations for every naming context and every replication partner. **Minimum required permission:** Domain User rights.
Replication Logon Privileges	Checks that logon privileges are appropriate for replication. **Minimum required permission:** Domain User rights.
Replication Partners	Lists information about inbound and outbound replication partners for the selected domain controller. **Minimum required permission:** Domain User rights.
Replication Partner DNS Resolution	Validates that DNS resolution is functioning properly. Displays the domain controller IP address, the DNS server IP address that the domain controller is configured to use, the records queried, and the records returned by DNS, including the IP address and ping response times. **Minimum required permission:** Domain User and WMI rights.
Replication Queue Length	Lists the length of the queues for current and pending replication tasks. **Minimum required permission:** Domain Administrator rights.

Table 1. Active Directory Health reports

Report	Description
RID Information	Lists the following RID (relative ID) information from the registry and Active Directory containers for the selected domain controller: minimum RID, maximum RID, RID threshold, RID block size, RID cache size, cached next RID, role owner (RID Master name), available RID pool for domain, allocation pool, next RID, previous allocation pool, and used pool. **Minimum required permission:** Domain User rights.
RID Masters	Lists all the RID (relative ID) masters in a given forest and domain. **Minimum required permission:** Domain User rights.
RIDs	Verifies the low and high values of RID sets for each domain controller in the specified domain. The results include values and pass/fail. **Minimum required permission:** Domain User rights.
Schema Master	Lists all the schema masters in a given forest and domain. **Minimum required permission:** Domain User rights.
Security Event Log	Lists events from the Security Event Log for the specified domain controller. **Minimum required permission:** The Active Administrator Foundation Service (AFS) account must be a member of the Event Log Readers group in Active Directory.
System Event Log	Lists events from the System Event Log for the specified domain controller. **Minimum required permission:** The Active Administrator Foundation Service (AFS) account must be a member of the Event Log Readers group in Active Directory.
SYSVOL Consistency	Performs a Cyclic Redundancy Check (CRC) of the SYSVOL content on two or more domain controllers. The report groups data based on the Policies (Group Policy Objects) and Scripts directories stored on the SYSVOL. **Minimum required permission:** Domain User, WMI, and File System Access rights.
Time Synchronization	Verifies time synchronization for the specified domain controller and displays the domain controllers that have time differences with their W32Time Parent. Report information is displayed in Coordinated Universal Time (UTC). For the specified domain controller, the results include SNTP Server (yes/no), UTC Time, Local Time, Forest Root Domain (yes/no), PDC (yes/no), and Time Servers. For the Time Server for the specified domain controller, the results include Name, SNTP Server (yes/no), UTC Time, Local Time, and Difference (in seconds between Time Server and specified DC). **NOTE:** If the Time Server is not a domain controller in the forest, the information for the Time Server is limited to Name and SNTP Server (yes). **Minimum required permission:** Domain User and WMI rights.
Unlinked GPO	Lists the GPOs that are not linked at the site, domain, or organizational unit level for a specified domain. This is a forest-wide search, so it detects cross-domain linking of GPOs. **Minimum required permission:** Domain User rights.

Active Directory Infrastructure reports

NOTE: To access and run reports, you must have a license to Active Administrator.

1. Open Active Administrator® in a web browser. See Opening Active Administrator in a web browser.
2. Select **Reports | Active Directory Infrastructure**.

Table 2. Active Directory Infrastructure reports

Report	Description
Forest and Domain Trusts	Lists the domain trusts for the domain where the specified domain controller resides. Information includes the name of the trusted domain, the type of trust, whether the trust is transitive or not, and the direction of the trust.
Forest Assessment	Lists details about forest trusts, Global Catalog servers, sites, and domains for the specified forest.
Global Catalog Server	Lists the global catalog servers in all domains.
Replication Assessment	Lists replication errors and details about domain controller replications for the specified forest.
Site Configuration	Displays site level configurations for one or more sites, including a list of the domain controllers located in the site and the domains within the site, and details on topology generation, universal group caching, and site links.
Site Information	Displays information about associated subnets, schedules, site links, and site link bridges for the specified site. Results include the following for Site Links: Name, Cost, Replication Interval and Transport.
Site Link Information	Displays information about associated sites, replication schedules, costs, intervals, and transports for the specified site. Results include the following details for site links: name, transport, cost, interval, associated sites, and schedule.
Site Messaging	Displays inter-site messaging configuration for the specified site. Results include the following information for each transport and site found: bridgehead server(s) (for specified site), cost, interval, and schedule.
Subnet Report	Displays the details of the subnets within the forest. Results include the forest name, domain root, forest functional level, domain naming master, schema master, and the prefix, site name, and location of all subnets.

DNS reports

NOTE: To access and run reports, you must have a license to Active Administrator.

1. Open Active Administrator® in a web browser. See Opening Active Administrator in a web browser.
2. Select **Reports | DNS**.

Table 3. DNS reports

Report	Description
DNS Domain	Lists the subdomains and resource records for the specified DNS domain on a specified DNS server.
DNS Server	Lists zones and their properties for the specified DNS server.

Security reports

NOTE: To access and run Security reports, you must have a license to Active Administrator.

1 Open Active Administrator® in a web browser. See Opening Active Administrator in a web browser.

2 Select **Reports | Security**.

Table 4. Security reports

Report	Description
All Computers Report	Lists all computers in the specified path.
All Groups Report	Lists all groups in the specified path.
All Organizational Units Report	Lists all organizational units in the specified path.
All Users Report	Lists all users in the specified path.
Object Class Summary	Displays counts for each object class type within a specified path.
Security Delegation Report	Lists all delegated permissions for a specified path.

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit https://www.quest.com/company/contact-us.aspx or call +1-949-754-8000.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.