



**NETPRO®**

**The  
Directory  
Experts**

# **DirectoryAnalyzer™**

**For Microsoft® Active Directory™**

## **White Paper**

**Printed: October 2000**

**Copyright Notice**

© NetPro Computing, Inc., 2000

All rights reserved. No part of this White Paper may be reproduced in any form or by any means without the express written permission of NetPro Computing, Inc.

**Limited Liability**

THIS DOCUMENT MAY CONTAIN TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. ANY DOCUMENTATION WITH RESPECT TO NETPRO COMPUTING, INC. SOFTWARE PRODUCTS IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY AND DOES NOT EXTEND OR MODIFY THE LIMITED WARRANTY EXTENDED TO THE LICENSEE OF NETPRO COMPUTING, INC. SOFTWARE PRODUCTS.

**Trademark Acknowledgments**

Microsoft, Microsoft Active Directory, Microsoft SQL Server, Microsoft Small Business and SQL Server Enterprise Edition, ActiveX, Windows, Windows NT and Windows 2000 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NetPro Computing, NetPro, and DirectoryAnalyzer are registered trademarks and the NetPro Computing Logo is a trademark of NetPro Computing, Inc.

All other brand and product names are trademarks or registered trademarks of their respective companies.

**Printed in the United States of America.**

# Contents

- Introduction** **1**
  - Welcome..... 1
  
- What is Active Directory?** **2**
  - Overview..... 2
  - A Unified Directory..... 3
  - A Single Point of Administration ..... 3
  - Scalability ..... 4
  - Operating System Integration ..... 4
  - Summary of Features and Benefits..... 5
  
- What Components Comprise Active Directory’s Infrastructure?** **6**
  - Overview..... 6
  - Replication..... 6
  - Operations Masters..... 6
  - DNS..... 7
  - Domain Controllers ..... 7
  - Global Catalogs..... 8
  - Domains..... 8
  - Sites ..... 8
  
- Why Monitor the Active Directory Infrastructure?** **9**
  - Overview..... 9
  
- DirectoryAnalyzer Features** **11**
  - What is DirectoryAnalyzer?..... 11
  - Proactive Monitoring..... 11
    - Replication ..... 11
    - Active Directory-Related DNS..... 12
    - Operations Masters ..... 12
    - Domain Controllers ..... 12
    - Global Catalogs ..... 12
    - Domains ..... 13
    - Sites ..... 13
  - Alerting & Notification..... 14
  - Knowledge Base..... 16
  - Alert History Reporting ..... 17
  - Troubleshooting ..... 18
  - Directory Browsing ..... 19

<b>DirectoryAnalyzer Benefits</b>	<b>20</b>
Overview.....	20
Ensures the Health of the Directory.....	20
Delivers Early Warning of Directory Errors .....	20
Context-Sensitive Knowledge Base Provides Error Resolution .....	21
Troubleshoot Domains, DCs and Sites .....	21
Centralizes Access to Directory Information .....	21
<b>Architecture</b>	<b>22</b>
Goals.....	22
Directory Independence .....	22
Minimal Network Traffic .....	22
Scalability.....	22
Building Blocks.....	23
DC Agent .....	24
Site Agent.....	25
Enterprise Agent.....	25
Client .....	25
Agent Communications .....	26
Fault Tolerance .....	26
<b>DirectoryAnalyzer Client</b>	<b>28</b>
Overview.....	28
View Status .....	29
Current Alerts.....	29
Browse Directory .....	30
Troubleshooting .....	31
DC Connectivity Test .....	31
Domain Connectivity Test.....	32
Site Connectivity Test.....	32
Alert History Reports.....	33
Configuration .....	34
<b>For More Information</b>	<b>35</b>
Contact NetPro.....	35
<b>Glossary of Terms</b>	<b>36</b>

# Introduction

---

## Welcome

The release of Microsoft Windows 2000 Server, and the directory service at its core, Active Directory, is having a tremendous impact on enterprise networks. As Windows 2000 with Active Directory penetrates the enterprise, it is increasingly important to ensure that the directory is healthy and trouble-free. Because the directory is the heart of a network, directory problems can result in unplanned service disruptions and business-crippling network downtime. For this reason, it is vital to assure optimal directory availability and performance.

NetPro's DirectoryAnalyzer is the first solution that proactively monitors and troubleshoots the infrastructure of Active Directory, including such vital components and background processes as replication, Active Directory-related DNS functions, operations masters, domain controllers, global catalogs, domains and sites. This paper provides a brief overview of the Active Directory infrastructure and detailed explanations of the capabilities and architectural elements of DirectoryAnalyzer.

# What is Active Directory?

---

## Overview

---

**Note:** This section has been taken directly from Microsoft's white paper, "*Microsoft Windows Active Directory: An Introduction to the Next Generation Directory Services.*"

---

Active Directory is a directory service that is completely integrated with Windows 2000 Server and offers the hierarchical view, extensibility, scalability, and distributed security required by all business customers. For the first time, network administrators, developers, and users gain access to a directory service that:

- Is seamlessly integrated with both Internet and Intranet environments.
- Provides simple, intuitive naming for the objects it contains.
- Scales from a small business to the largest enterprise.
- Provides simple, powerful, open application programming interfaces.

Active Directory is a critical part of the distributed system. It allows administrators and users to use the directory service as a source of information, as well as an administrative service.

---

## A Unified Directory

Active Directory integrates the Internet concept of a *name space* with the operating system's directory services, thus allowing enterprises to unify and manage the multiple name spaces that now exist in the heterogeneous software and hardware environments of corporate networks. It uses the lightweight directory access protocol (LDAP) as its core protocol and can work across operating system boundaries, integrating multiple name spaces. It can subsume and manage application-specific directories, as well as other NOS-based directories, to provide a general-purpose directory that can reduce the administrative burden and costs associated with maintaining multiple name spaces.

Active Directory is not an X.500 directory. Instead, it uses LDAP as the access protocol and supports the X.500 information model without requiring systems to host the entire X.500 overhead. The result is the high level of interoperability required for administering real-world, heterogeneous networks.

---

## A Single Point of Administration

Active Directory allows a single point of administration for all published resources, which can include files, peripheral devices, host connections, databases, Web access, users, other arbitrary objects, services, and so forth. It uses the Internet Directory Name Space (DNS) as its locator service, organizes objects in domains into a hierarchy of organizational units (OUs), and allows multiple domains to be connected into a tree structure. Administration is further simplified because there is no notion of a primary domain controller (PDC) or backup domain controller (BDC). Active Directory uses domain controllers (DCs) only, and all DCs are peers. An administrator can make changes to any DC, and the updates will be replicated on all other DCs.

---

## Scalability

The Microsoft Exchange 4.0 directory structure and storage engine provide the foundation for Active Directory. The Microsoft Exchange storage engine provides multiple indexes for fast retrieval and an efficient mechanism for storing sparse objects. That is, objects that support many different properties but do not always have values for all of them. From this foundation, Microsoft has developed general-purpose directory services that scale from a small installation with a few hundred to a few thousand objects, to a very large installation with millions of objects.

Active Directory supports multiple stores and can hold more than 1 million objects per store, thus offering unparalleled scalability while maintaining a simple hierarchical structure and ease of administration. When combined with the Microsoft Distributed File System, Active Directory will bring networks even closer to the goal of a single global name space.

---

## Operating System Integration

Active Directory is seamlessly integrated with Windows 2000 Server, which is the only operating system that offers traditional file and print, applications, communications, and Internet/intranet support built into the base product. Windows 2000 Server is the best file and print server for all of a business' information and resource sharing needs, outperforming all other operating systems available today. It is also the best applications server available, offering the best scalability/price ratio in the industry. Additionally, Windows 2000 Server is an excellent communications platform, offering such features as Remote Access Services, TAPI, and PPTP.

---

## Summary of Features and Benefits

Active Directory includes the following features and benefits:

- Support for open standards to facilitate cross-platform directory services, including support for the Domain Name System (DNS) and support for standard protocols, such as LDAP.
- Support for standard name formats to ensure ease of migration and ease of use.
- A rich set of APIs, which are easy to use for both the scripter and C/C++ programmer.
- Simple, intuitive administration through a simple hierarchical domain structure and the use of drag-and-drop administration.
- Directory object extensibility via an extensible schema.
- Fast lookup via the global catalog.
- Speedy, convenient updates through multi-master replication.
- Backward compatibility with previous versions of the Windows NT operating system.
- Interoperability with NetWare environments.

# What Components Comprise Active Directory's Infrastructure?

---

## Overview

Active Directory is made up of many infrastructure components and processes, including replication, operations masters, DNS, domain controllers, global catalogs, domains, sites, etc. All of these components are important to the operation of Active Directory. Following is a brief overview of each of the important aspects of the Active Directory infrastructure and their impact on directory performance and reliability.

---

## Replication

Replication is the process whereby changes that are made to objects and attributes on one domain controller are copied to other domain controllers. Replication provides the mechanism whereby a directory database can be distributed across many servers, allowing for fault tolerance and load balancing on these servers, called domain controllers. In Active Directory, each domain controller regularly analyzes its placement in the Active Directory deployment and determines the optimal replication topology through a process called the Knowledge Consistency Checker (KCC). Creation of a proper and consistent replication topology is critical to making sure that updates to Active Directory objects and attributes are copied to other domain controllers.

---

## Operations Masters

Active Directory performs multi-master replication, as opposed to the master-slave replication processes that occurred in NT 3.51/4. However, certain infrastructure changes are not suited for a multi-master environment. Therefore, for a particular single-master function, only one domain controller, the 'operations master', manages that infrastructure operation. Active Directory contains five operations masters, two for the entire enterprise and three for each domain in the enterprise.

### Enterprise Operations Masters

**Schema Master** – The Schema Master is a single domain controller that is responsible for schema management for the entire forest, including schema extensions and modifications. If any schema management needs to occur, this domain controller is responsible for performing the action and then propagating changes to other domain controllers. There can be only one Schema Master in the entire forest.

**Domain Naming Master** – The Domain Naming Master is a single domain controller that is responsible for adding and removing domains in the forest. Whenever a new domain is created or a domain is deleted, this domain controller is responsible for verifying that it is okay to perform this operation. There can be only one Domain Naming Master in the entire forest.

### **Domain Operations Masters**

**RID Master** – The RID Master allocates blocks of RIDs\* to other domain controllers in it's domain. There can only be one RID Master per domain.

\*Whenever a domain controller creates a user, group, or computer object, it assigns the object a unique security ID. The security ID consists of a domain security ID (that is the same for all security IDs created in the domain), and a relative ID that is unique for each security ID created in the domain.

**PDC Emulator** – The PDC emulator acts as the primary domain controller for downlevel (NT 4 and prior) BDCs, as well as for computers operating without Windows 2000 client software running on them. The PDC emulator is responsible for processing password changes from these clients and replicating updates to BDCs. Even when there are no more downlevel clients or BDCs and Active Directory is operating in native mode, the PDC emulator still preferentially receives password updates, and certain operations like Group Policy editing key on the PDC emulator. There can be only one PDC emulator per domain.

**Infrastructure Master** – The Infrastructure Master is responsible for updating group-to-user references whenever members of groups are changed or renamed. There can be only one Infrastructure Master per domain.

---

## **DNS**

Active Directory uses the Domain Naming System, the Internet standard for name resolution, as its location service. In order for Active Directory to function correctly, a number of Active Directory-related DNS records must exist in the appropriate DNS zone files. The majority of these records are of the type SRV (Service Location) and identify which domain controllers provide the various services within Active Directory. Windows 2000 clients and other Active Directory-enabled applications query these SRV records to find the IP addresses of various Active Directory services being hosted on different domain controllers (global catalog service, LDAP service, Kerberos service, etc.).

---

## **Domain Controllers**

Domain Controllers are the Windows 2000 servers that have been configured to provide Active Directory services to network users and computers. Domain Controllers manage and store domain-wide information. They also manage user-to-domain interactions, including user logon, authentication to the directory and searches through the directory. Since Domain Controllers store the domain information, they also oversee the replication to other domain controllers.

---

## Global Catalogs

Global Catalogs are specialized Domain Controllers that contain a partial copy of every object in the forest. The global catalog performs two key roles in Active Directory: logon and querying. First, a Global Catalog must be available for every directory logon by a client. Otherwise, the user will not be able to log on. Second, global catalogs streamline forest-wide searches of often-used data (such as email addresses), eliminating the need to perform separate searches at each domain individually.

---

## Domains

Domains (also known as naming contexts or NCs) are the formal security and replication boundaries in Active Directory. They exist as a domain database on each Domain Controller that participates in that particular domain. They store all of the important information for that domain, including users, computers, printers, applications, etc. Domains are used to accomplish a number of management goals, including security management, replication control, etc. In addition to hosting a domain NC, every Domain Controller also hosts two other NCs, the Configuration NC and the Schema NC. The Configuration NC hosts information about the structure of the forest, such as the domain structure and hierarchy and the replication topology. The Schema NC hosts information about the definition of every object and attribute that can exist in Active Directory and their relationships.

---

## Sites

Sites in Active Directory allow the physical network to be mapped to Active Directory, as defined by IP subnet information. Active Directory sites exist for two reasons:

- 1) To service directory clients.
- 2) To control the replication process.

When a client requests a service from a domain controller, it directs the request to a domain controller in the same site, if there is one available. Without sites to guide directory client requests, it is possible that a user could try to access resources from a domain controller that is across the WAN rather than one that exists on the local network segment. In order to manage network traffic across WAN links, sites control the replication process both within sites and between sites.

# Why Monitor the Active Directory Infrastructure?

---

## Overview

Active Directory is the repository for information regarding all types and levels of Windows 2000 network information. Active Directory stores information on everything from server information (file shares, printers, etc.), to network devices (hubs, routers, switches, firewalls, etc.) and applications.

Each of Active Directory's infrastructure components plays an important role in fulfilling the goals of the directory. As the Active Directory environment grows larger and more distributed, it becomes more difficult to keep track of all the various components as a means for ensuring that they are functioning properly. For example, if any one of the components is not functioning as it should, there is high risk that other components could be impacted. This could cause problems for parts, or all, of the Active Directory environment. In order to ensure the directory's health and performance, it is critical to proactively monitor its core infrastructure components and background processes.

Following is an example of a simple Active Directory deployment and the number of components that need to be monitored.

### **Sample Active Directory enterprise:**

- 3 domains
- 10 sites across a wide geographic area
- 3 domain controllers (DCs) per site (1 GC, 1 DC/DNS and 1 DC)

### **Results**

- 20 domain controllers
- 10 global catalogs
- 10 DNS servers
- 10 sites
- 11 operations masters (2 enterprise and 3 for each of 3 domains)

In this sample environment alone there are more than 60 different components and processes to monitor. And, it's important to note that this

does not include the replication that occurs between all of the domain controllers and zone transfers between DNS servers (Exception: If they are Active Directory-integrated DNS zones, the DNS zones would replicate via standard Active Directory replication methods). Monitoring all of these elements manually is a time-consuming task. DirectoryAnalyzer eliminates the need to perform these tasks by automating the monitoring process, allowing administrators to focus on more strategic directory initiatives.

# DirectoryAnalyzer Features

---

## What is DirectoryAnalyzer?

DirectoryAnalyzer monitors the infrastructure of Active Directory, including replication, DNS, operations masters, domain controllers, global catalogs, domains, and sites for key conditions that are vital to the health of Active Directory. DirectoryAnalyzer continuously analyzes all aspects of the Active Directory infrastructure and alerts on the issues that it detects. Once a problem has been detected, DirectoryAnalyzer provides multiple notification mechanisms to indicate that an alert has occurred, and it helps resolve directory issues through an online knowledge base. Additionally, DirectoryAnalyzer provides directory troubleshooting capabilities, as well as the ability to browse the entire Active Directory infrastructure and associated information from a central location, including keeping records of each alert for compiling reports of Active Directory health over time. A thorough review of key DirectoryAnalyzer features follows.

---

## Proactive Monitoring

DirectoryAnalyzer is a constant watchdog for your Active Directory installation. It monitors all of Active Directory's critical infrastructure components on an ongoing basis to ensure that the directory is functioning properly. These components include replication, Active Directory-related DNS, operations masters, domain controllers, global catalogs, domains and sites.

### Replication

If changes to Active Directory are not being propagated to other domain controllers in the domain, then sooner or later a user may not get the resources they need or they may get access to resources that they shouldn't have. DirectoryAnalyzer ensures the health and performance of Active Directory replication processes, including:

- Replication latency issues
- Replication topology problems
- Replication errors and failures
- Replication partner problems
- Replication cycle slowness
- Replication conflict concerns

## Active Directory-Related DNS

If something has gone wrong with DNS, then Active Directory can be brought to a standstill, since Active Directory completely relies on DNS for its location service. DirectoryAnalyzer provides important monitoring capabilities for DNS as it relates to Active Directory, including:

- DNS server/service status
- Status of domain controller SRV records
- DNS response time
- DNS zone conflict problems

## Operations Masters

If the appropriate Operations Masters are not consistent and available when certain infrastructure operations need to occur, quirky problems can occur with Active Directory. DirectoryAnalyzer provides important monitoring capabilities for Operations Masters, including:

- Operations Master consistency
- Operations Master availability
- Operations Master placement

## Domain Controllers

If domain controllers are not functioning properly, it is virtually guaranteed that Active Directory will experience problems. Thus, it is critical to track the performance and availability of domain controllers. DirectoryAnalyzer provides around-the-clock monitoring of the critical aspects of each domain controller in the Active Directory infrastructure, including:

- CPU loads
- LDAP loads
- LDAP response rates
- Trust relationships
- GPO inconsistencies

## Global Catalogs

If a global catalog is not available when a user tries to log on, the user will not be able to log on. This critical piece of Active Directory can cause major headaches for administrators. DirectoryAnalyzer automates important monitoring capabilities for global catalogs, including:

- Global Catalog response time
- Global Catalog load
- Global Catalog replication latency concerns

## **Domains**

DirectoryAnalyzer monitors all of the important attributes of each domain within Active Directory, including:

- Domain replication latency
- Domain replication topology
- Consistency of DNS records with Active Directory domains
- Status of each DC in the domain

## **Sites**

Because sites determine client access and define the replication topology for Active Directory, it is important that sites function properly at all times.

DirectoryAnalyzer monitors such important site attributes as:

- Inter-site and intra-site replication topology generation
- Global catalog status
- Number of global catalogs in the site
- Status of each DC within the site
- Status of each DNS server within the site

---

## Alerting & Notification

Continuous monitoring of Active Directory's key infrastructure components is just one piece of DirectoryAnalyzer. Alerting and notification is another fundamental piece. DirectoryAnalyzer's alerting feature ensures that administrators receive immediate notification of the problems detected during the continuous monitoring process. DirectoryAnalyzer provides two levels of alerting:

- **Warning Alert** - Indicates that a designated warning threshold has been violated and the problem may lead to an error condition if not addressed promptly.
- **Critical Alert** – Indicates that a designated error condition has occurred.

In addition to two levels of alerting, DirectoryAnalyzer provides customizable “set duration” and “clear duration” parameters. So, not only does an alert threshold have to be crossed to constitute an alert condition, but also a specified amount of time must pass before an alert condition is considered a true alert. Conversely, a predetermined amount of time must pass before an alert can clear. Each and every Active Directory implementation is unique, so it's critical that these parameters be customizable for each individual environment. The combination of multiple alert levels and set and clear duration parameters enables significant customization of the Active Directory-monitoring environment. Once a warning or critical alert has occurred, DirectoryAnalyzer notifies administrators through a number of methods:

- **DirectoryAnalyzer Client** – The DirectoryAnalyzer Client provides on-screen alerts when a monitored attribute has exceeded either a warning or critical threshold and its accompanying set duration. The DirectoryAnalyzer client “View Status” function displays the current alerts, which can be sorted by severity, time and type of occurrence.

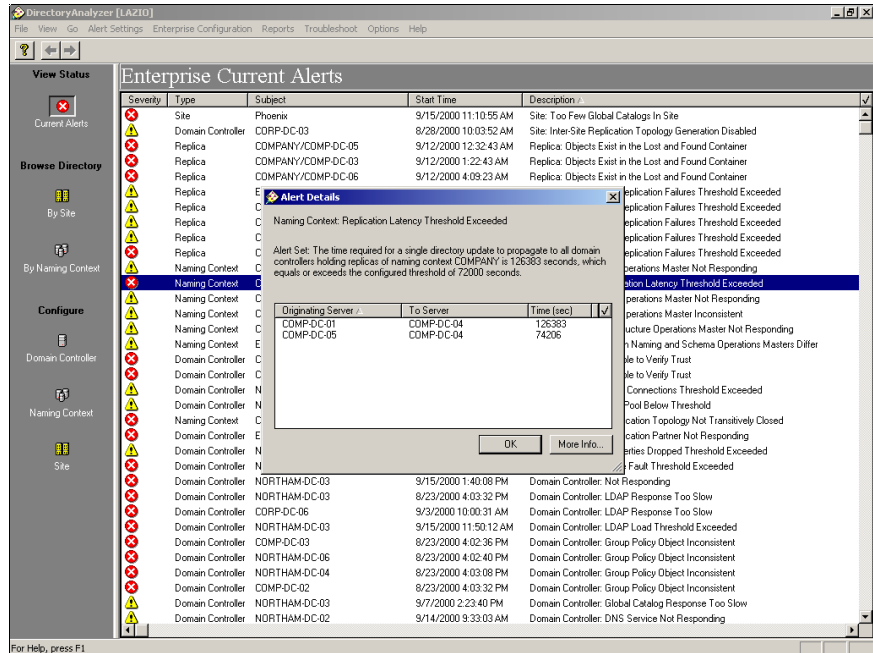


Figure 1 - DirectoryAnalyzer Current Alerts screen displays all alert conditions that exist in a forest and provides access to a comprehensive knowledge base

- **SNMP** – DirectoryAnalyzer integrates with the Windows 2000 SNMP service to provide SNMP notification of problems to a number of enterprise management consoles.
- **Event Log** – DirectoryAnalyzer integrates with the Enterprise Agent’s NT Event Log to record the various alerts that DirectoryAnalyzer detects.

# Knowledge Base

Identifying problems and providing notification that the problem has occurred are important benefits. DirectoryAnalyzer does exactly that. But that's only the first step. Once a problem has been uncovered, it must be solved. DirectoryAnalyzer helps to solve Active Directory infrastructure problems through its comprehensive knowledge base. When an alert occurs or when troubleshooting turns up a problem, the administrator accesses the knowledge base in DirectoryAnalyzer for answers. It explains what the problem is, it provides likely explanations of the problem's cause, and it recommends steps for repairing the problem.

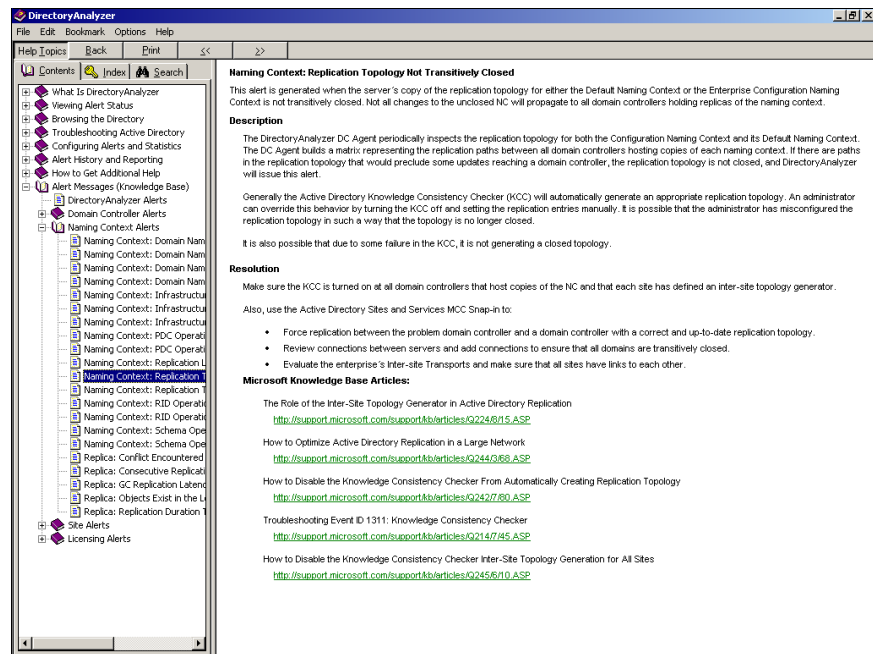


Figure 2 - DirectoryAnalyzer knowledge base entry

# Alert History Reporting

DirectoryAnalyzer's ability to detect, notify and assist in the resolution of Active Directory problems provides invaluable information to administrators. At the same time, Active Directory administrators need a way to be able to trend the occurrence of these directory problems over time. By providing an alert history database and reporting capability, DirectoryAnalyzer can deliver this alert trending capability so that administrators better understand where the key problem points in the directory have been from a historical standpoint. DirectoryAnalyzer's alert history reporting capabilities allow administrators to run reports on current alerts and/or past alerts, selectable by domain, domain controller, site, etc. These reports can be printed or saved to a number of file formats or delivered via MAPI client or to an Exchange folder.

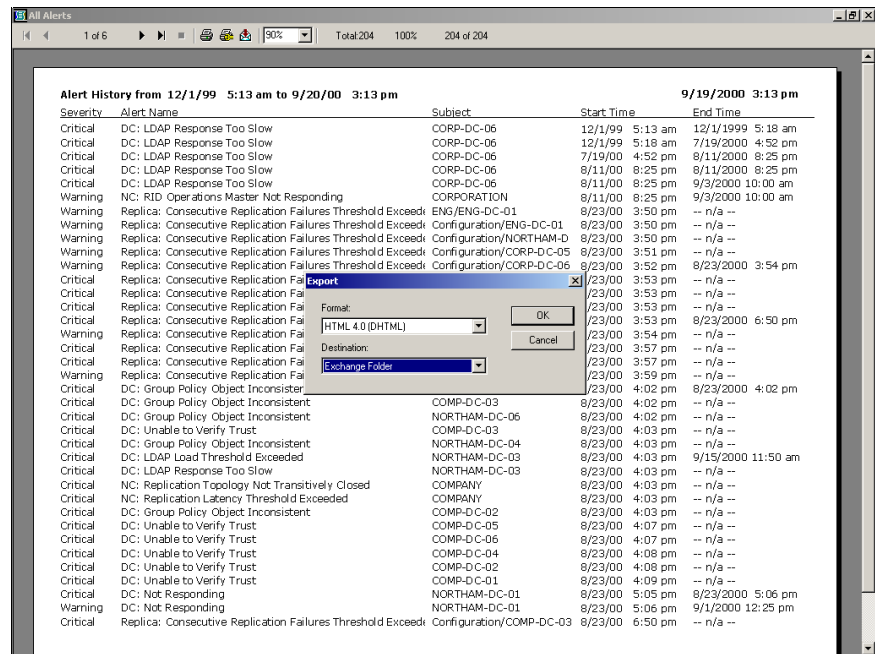


Figure 3 - Alert history reporting interface

# Troubleshooting

In addition to proactive monitoring and alerting, DirectoryAnalyzer provides a variety of interactive tools designed to help administrators quickly determine what problems exist in the directory, without physically leaving the DirectoryAnalyzer Client. These interactive tools include:

- **DC Connectivity Tests** – A sequence of tests to evaluate the current state of connectivity between various Domain Controllers in the forest.
- **Domain Connectivity Tests** – A sequence of tests to assess the status of connectivity between Domain Controllers either in the same or different domains in the forest.
- **Site Connectivity Tests** – A sequence of tests to analyze the state of connectivity between Domain Controllers in various sites throughout the world.

The details of each of these tests are discussed further in the “DirectoryAnalyzer Client” section.

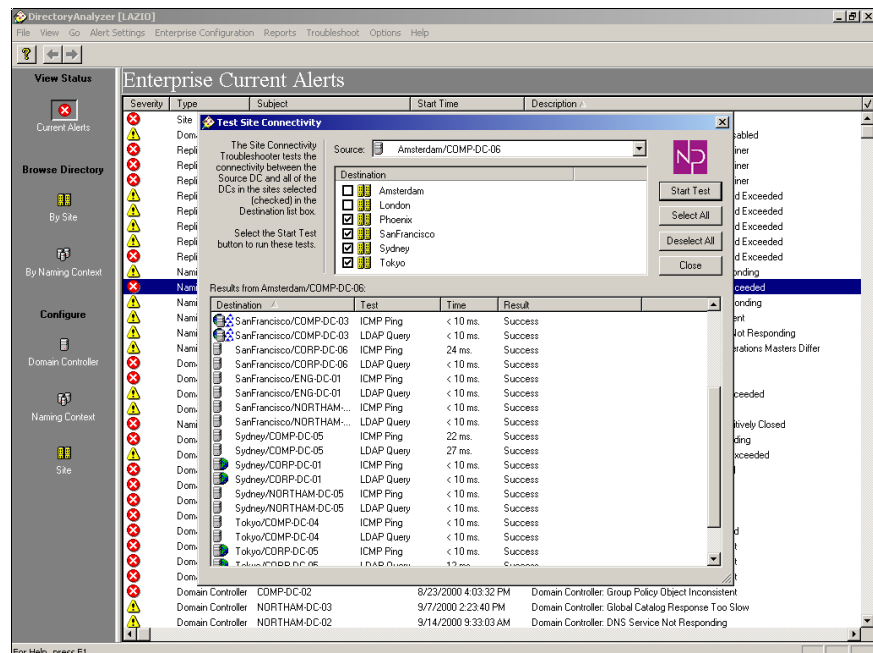


Figure 4 - DirectoryAnalyzer interactive troubleshooting capabilities

# Directory Browsing

Microsoft's Active Directory management tools are excellent for day-to-day administration of the directory. For example, when an administrator needs to add a new user, the Active Directory Users and Computers snap-in is the ideal solution. When it's time to create a new site, the Active Directory Sites and Services Manager snap-in is the appropriate tool. Likewise, if schema operations are required, the Schema Manager is the right snap-in. But Microsoft does not offer a tool that provides a consolidated view of the entire directory infrastructure, including detailed information about each critical component, from domains to sites to DCs to DNS servers. DirectoryAnalyzer is the only tool that manages Active Directory's infrastructure as a single entity across local and wide area links, providing a complete picture of the Active Directory environment from one location. The details of Directory Browsing are discussed further in the "DirectoryAnalyzer Client" section.

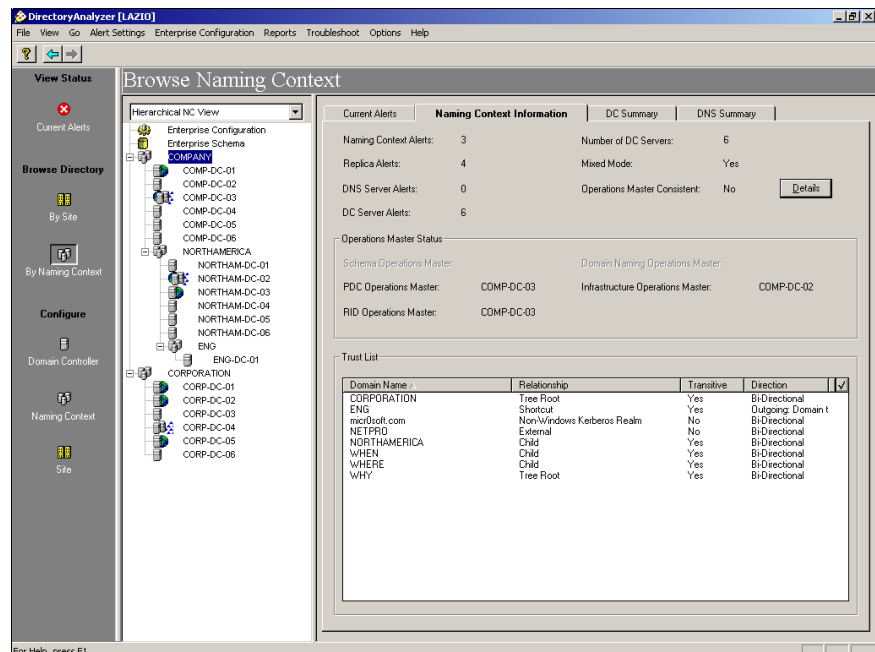


Figure 5 - DirectoryAnalyzer's Browse by Naming Context view

# DirectoryAnalyzer Benefits

---

## Overview

DirectoryAnalyzer proactively monitors and troubleshoots Active Directory so that administrators can deploy and manage Windows 2000 with confidence. This section discusses some of the many benefits that DirectoryAnalyzer provides to Active Directory administrators.

---

## Ensures the Health of the Directory

From replication latency and replication topology problems to high LDAP loads and DNS inconsistencies, DirectoryAnalyzer alerts administrators immediately to the problems they need to know about. Take DNS, for instance. As the name location service for Active Directory, DNS uses unique service location resource (SRV) records to articulate Active Directory service information. If SRV records are inaccurate or missing, DNS will point clients to the wrong location for a given resource. And that's only one example. Replication also poses potential problems. If the directory isn't replicating properly, new or updated group policies won't replicate to the domain controllers and users won't have access to new network resources and applications. DirectoryAnalyzer's proactive monitoring and alerting capabilities ensure the health of the directory and provide vital peace of mind to Active Directory administrators.

---

## Delivers Early Warning of Directory Errors

DirectoryAnalyzer monitors and alerts on all conditions critical to Active Directory. It dispatches the alerts at the first sign of trouble via SNMP traps, to the NT Event Log and the DirectoryAnalyzer Client. With DirectoryAnalyzer, administrators can set alert thresholds to meet the needs of their own environments. And DirectoryAnalyzer enables administrators to define two levels of alerts for each condition— warning and critical. DirectoryAnalyzer provides early warning that an error condition has occurred and may be escalating. It also tells the administrator the exact location of the problem for fast, efficient resolution.

---

## **Context-Sensitive Knowledge Base Provides Error Resolution**

DirectoryAnalyzer proactively notifies administrators of directory trouble – and it goes a step further. DirectoryAnalyzer’s comprehensive knowledge base provides context-sensitive solutions to Active Directory problems. To obtain answers to tough directory questions, administrators simply drill down on a given alert to access expert advice from the knowledge base. The product provides practical advice for both Active Directory experts and novices.

---

## **Troubleshoot Domains, DCs and Sites**

DirectoryAnalyzer helps to research specific issues with timesaving troubleshooting tests that quickly perform in-depth diagnostic tests. Administrators can test connectivity to Domain Controllers, domains and sites, and quickly measure everything from IP ping-time results and server status details to LDAP query time on all of the domain controllers. To conduct similar tests manually, troubleshooting from many locations across the network would be required. DirectoryAnalyzer troubleshoots problems in minutes that would take hours to troubleshoot manually.

---

## **Centralizes Access to Directory Information**

DirectoryAnalyzer displays a comprehensive, enterprise-level view of the Active Directory infrastructure, identifying relationships and disclosing detailed information about each component. When an administrator chooses “Browse Directory by Naming Context,” for example, they will see details on the Operations Master Roles, including the status of each and their consistency across all servers from any DirectoryAnalyzer client in the network. Or, when they select “Browse Directory by Site,” everything from current alerts to inter-site connection and replication status is displayed. DirectoryAnalyzer provides a view of Active Directory that is unavailable from any other solution, allowing administrators to browse the entire directory from a single location.

# Architecture

---

## Goals

DirectoryAnalyzer was designed to provide a reliable, manageable, secure, and scalable solution for monitoring Active Directory. DirectoryAnalyzer was developed with three key architectural goals in mind:

### **Directory Independence**

DirectoryAnalyzer enables administrators to diagnose problems with Active Directory. DirectoryAnalyzer must work even if Active Directory has problems. For this reason, DirectoryAnalyzer does not use Active Directory to store configuration information or to locate DirectoryAnalyzer services.

### **Minimal Network Traffic**

To avoid adversely affecting the performance of the network, the DirectoryAnalyzer architecture provides for minimal communication, particularly over WAN links.

### **Scalability**

DirectoryAnalyzer monitors both small Active Directory installations with only a few DCs, and large enterprise customers with hundreds or thousands of servers distributed over many sites. To support all of these systems, the DirectoryAnalyzer architecture limits the amount of CPU, memory, and network bandwidth it uses to support networks of various sizes. And DirectoryAnalyzer easily accommodates large networks, which are inherently unreliable, with servers and network links going up and down.

## Building Blocks

The DirectoryAnalyzer architecture is comprised of four components: Enterprise Agent, Site Agent, Domain Controller Agent (DC Agent), and Client. DirectoryAnalyzer is designed to minimize network communication traffic between components of the DirectoryAnalyzer system.

- **DC Agent** – NT service that resides on each DC in Active Directory. The DC Agent is charged with monitoring the local DC for alert conditions and passing them on to the Site Agent.
- **Site Agent** – NT service that resides on a one DC in each Active Directory site. It is responsible for monitoring site-level conditions and collecting alert conditions and information from DC Agents to pass on to the Enterprise Agent.
- **Enterprise Agent** – NT service that resides on a member server in the enterprise. It is responsible for monitoring domain/tree/forest-wide conditions and collecting alert conditions and information from Site Agents in order to generate notifications to administrators and display status to the client.
- **Client** – 32-bit user interface for managing all aspects of the DirectoryAnalyzer environment.

The following diagram depicts how these components fit together to accomplish the task of monitoring Active Directory:

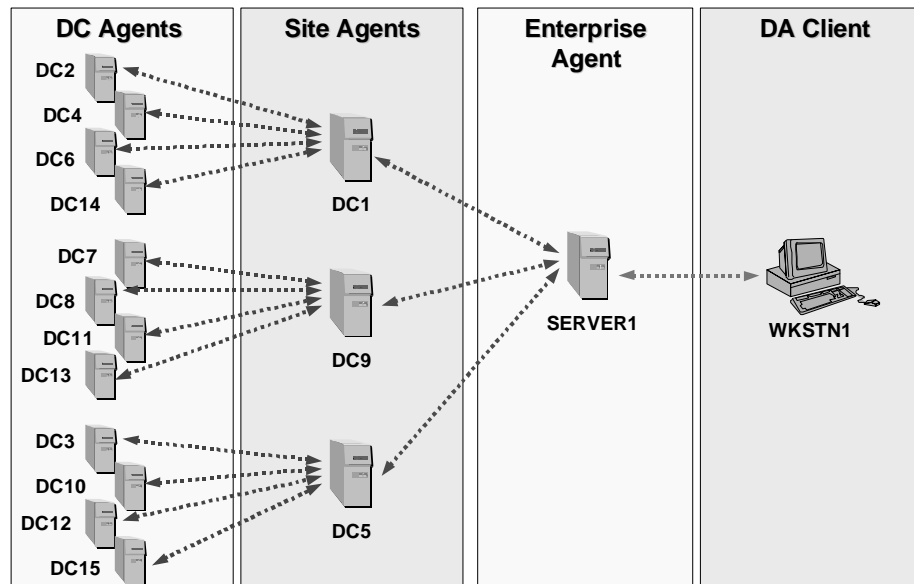


Figure 6 - DirectoryAnalyzer agent architecture

1. The DC Agent detects a threshold violation on the local DC.
2. The alert is passed on to that DC's Site Agent.
3. The Site Agent aggregates alerts from all DC Agents that are in its site.
4. The Site Agent passes the alerts on to the Enterprise Agent.
5. The Enterprise Agent sends out notifications to appropriate administrators based on notification configuration.
6. The Enterprise Agent presents a visual representation of the alerts to the administrator via the DirectoryAnalyzer Client.

The above description represents the general flow of alert communications throughout DirectoryAnalyzer. The path that is followed to generate an alert is the same path that is used to clear an alert when the threshold is no longer being violated. This is a simple example. However, even in complex environments with many sites and levels of administration, the flow of communication works the same way.

## DC Agent

The DC Agent is an NT service that resides on each Windows 2000 Domain Controller and is responsible for monitoring the activity of a single domain controller. The DC Agent builds a partial model of Active Directory relevant to the domain controller on which the DC Agent resides. It then monitors for local Active Directory issues and generates alerts when conditions warrant attention. The DC Agent is configured by its Site Agent, and communicates only with the Site Agent as a general rule. The DC Agent:

- Monitors server performance counters, event log, registry, and service status
- Monitors configuration and performance of the local copy of the directory and associated services
- Performs local processing of server data to minimize network traffic
- Detects alert conditions and other significant events on the local Domain Controller

## Site Agent

The Site Agent is an NT service that resides on a single Windows 2000 domain controller within the Active Directory site for which it is responsible. The Site Agent builds a partial model of Active Directory relevant to its site and then analyzes that model to detect and alert on site-level Active Directory issues. It communicates with the DC Agents in its site and configures those DC Agents, which monitor the other domain controllers in its site. The Site Agent passes its model information, as well as relevant changes, events and alerts to requesting Enterprise Agents. The Site Agent also:

- Configures local DC Agents
- Aggregates data from local DC Agents
- Detects site-specific alert conditions, e.g., too few Global Catalogs in the site
- Builds a partial model of Active Directory relevant to the site

## Enterprise Agent

The Enterprise Agent is an NT service that runs on a Windows 2000 member server or workstation in the enterprise. Based on model information that is received from each of the Site Agents, it builds an enterprise-level model of Active Directory. The Enterprise Agent also:

- Detects domain/tree/forest-wide alert conditions, e.g., domain replication latency too high
- Communicates with Site Agents to build an enterprise model
- Generates SNMP traps and NT Event Log entries for alerts detected in the DirectoryAnalyzer system
- Services DirectoryAnalyzer Client requests
- Maintains DirectoryAnalyzer configuration and threshold settings

DirectoryAnalyzer's architecture allows for multiple redundant Enterprise Agents as an administrative option for fault tolerance. For more information on fault tolerance, go to the section entitled "**Fault Tolerance.**"

## Client

The DirectoryAnalyzer Client is a Win32 application that provides a task-oriented user interface to manage the DirectoryAnalyzer environment. The client communicates with the Enterprise Agent.

---

## Agent Communications

The general rules for DirectoryAnalyzer communication are as follows:

- The DirectoryAnalyzer Client only communicates with the Enterprise Agent.
- The Enterprise Agent communicates with all Site Agents for which it is responsible, in order to build a model of Active Directory and receive alert information.
- The Site Agent communicates with all DC Agents for which it is responsible, in order to configure them, build a partial model of the Active Directory, and receive alert information.
- The DC Agent is responsible for a single, specific domain controller and communicates only with the Site Agent to provide alert status information.

DirectoryAnalyzer uses an event-driven communication methodology, which means that agents do not poll each other to find out new information. Instead, DirectoryAnalyzer uses a publish/subscribe model for communicating events back and forth. And there are multiple communications channels. The net result is that DirectoryAnalyzer is very efficient in its use of network resources to communicate between agents.

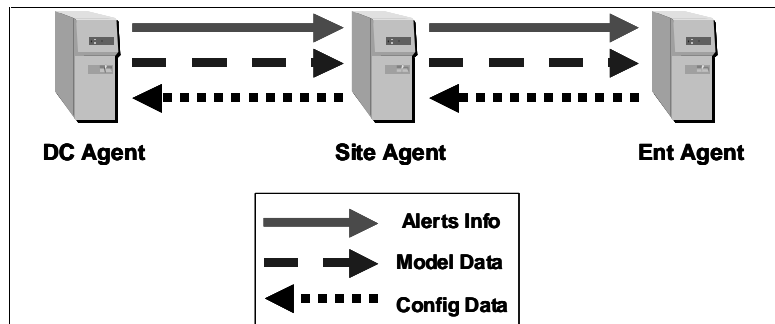


Figure 7 - Flow of DirectoryAnalyzer agent communications

Finally, DirectoryAnalyzer agents communicate via TCP over an IANA-assigned, static IP port number so that there is no guesswork in opening up ports for internally firewalled organizations.

---

## Fault Tolerance

The DirectoryAnalyzer architecture provides a fault-tolerant environment for monitoring Active Directory. Since DirectoryAnalyzer's role is to make sure that Active Directory is performing correctly, it is critical that DirectoryAnalyzer detect agent communication problems and not have a

single point of failure. To realize this, DirectoryAnalyzer implements two fault-tolerance measures:

1. **Agent communications problem detection** – On a regular basis the various DirectoryAnalyzer agents verify that they can still communicate with subordinate agents. If they can't, an alert is escalated through the system. For example, if a DC Agent is too slow to respond to a request from a Site Agent, an alert is generated indicating that the DC Agent is not responding. The same applies to Site Agent – Enterprise Agent communications.

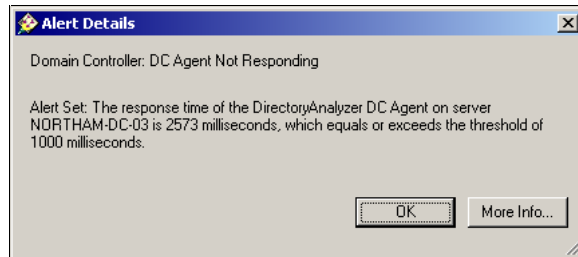


Figure 8 - DirectoryAnalyzer can detect problems with its own agents

2. **Enterprise Agent redundancy** – The Enterprise Agent is a key piece to the DirectoryAnalyzer puzzle. If there is only one Enterprise Agent implemented in an environment and that Enterprise Agent fails for any reason, the environment will be oblivious to directory problems that might be happening. To avoid this situation, DirectoryAnalyzer allows for redundant Enterprise Agents to operate simultaneously. With this type of implementation, even if one Enterprise Agent fails, others will continue to receive alert information and provide notifications to administrators. Enterprise Agent redundancy is implemented “fully meshed” -- all Site Agents communicate with all Enterprise Agents. This means that there is no opportunity for alert information to slip through the cracks. The following diagram displays the redundancy architecture for Enterprise Agents.

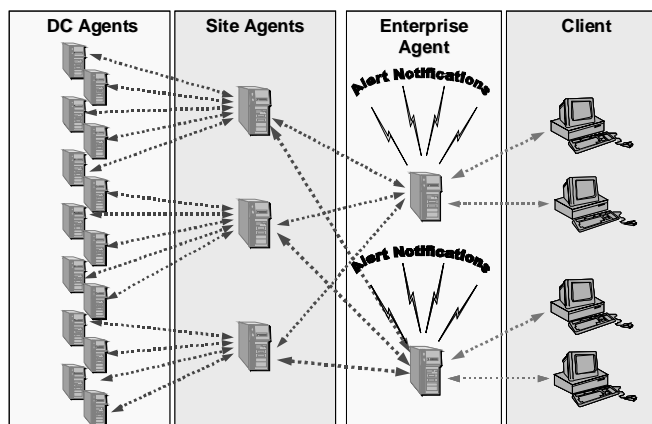


Figure 9 – DirectoryAnalyzer provides Enterprise Agent redundancy capabilities

# DirectoryAnalyzer Client

---

## Overview

The DirectoryAnalyzer client runs on NT 4 or Windows 2000 and provides the primary interface to all aspects of DirectoryAnalyzer. The DirectoryAnalyzer client user interface enables the administrator to:

- View current enterprise alerts
- Obtain knowledge base information
- Browse the directory structure
- View detailed domain, site, domain controller and DNS information
- Troubleshoot the directory infrastructure
- Configure alert thresholds and set/clear durations
- Configure alert notification methods

The DirectoryAnalyzer client accomplishes five primary tasks:

- **View Status** – Display current alerts and access knowledge base information to assist in resolving directory problems
- **Browse directory** – Navigate the directory hierarchy by domain or by site and obtain vital information about the status of all critical directory components
- **Troubleshoot** – Perform interactive troubleshooting tests to determine status of directory connectivity
- **Report** – Specify and deliver alert history trending and analysis reports
- **Configure** – Set thresholds and set/clear durations for domain controllers, domains and sites

Following is a detailed description of each of the client tasks.

# View Status

View Status is the default screen displayed when the DirectoryAnalyzer client is launched. View Status provides the opportunity to view current alerts within the enterprise monitored by DirectoryAnalyzer.

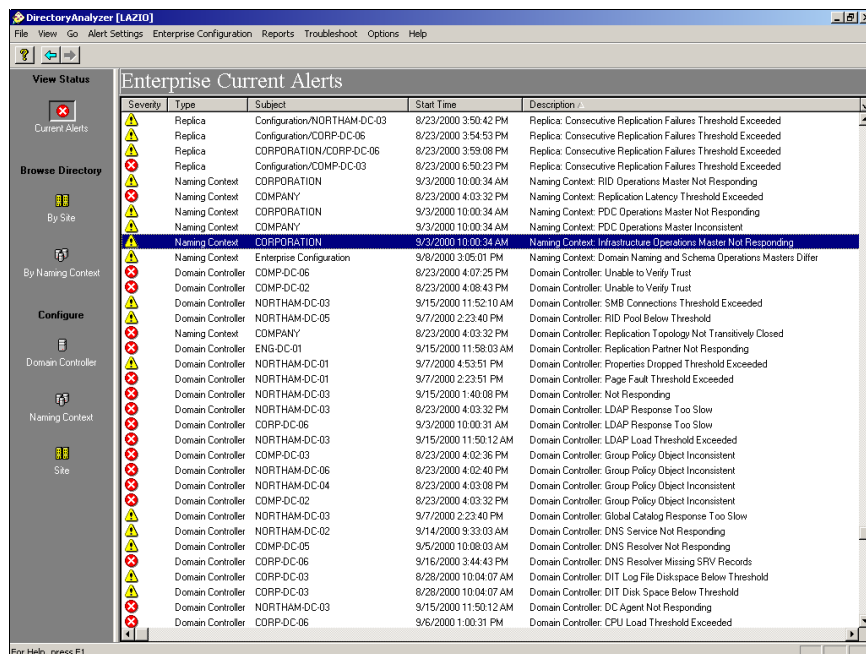


Figure 10 - DirectoryAnalyzer Enterprise Current Alerts screen

## Current Alerts

This screen displays all alerts that currently exist anywhere within the administrator's view of Active Directory. Following is a list of the information provided for each alert:

- **Alert Status** – This can be warning or critical.
- **Type** – The type of alerted object, such as a naming context, domain controller, etc.
- **Subject** – The subject of the alerted object, such as the name of the domain controller or site that generated the alert.
- **Start Time** – When the alert threshold was exceeded.
- **Description** – Description of the actual alert.

For each alert that occurs, DirectoryAnalyzer provides access to a context-sensitive knowledge base containing helpful information about the nature of the problem and recommendations for how to resolve it.

# Browse Directory

Browse Directory provides a means for the administrator to navigate Active Directory and obtain information about the different components of the environment. The administrator can choose to view Active Directory either from a site view or a domain view.

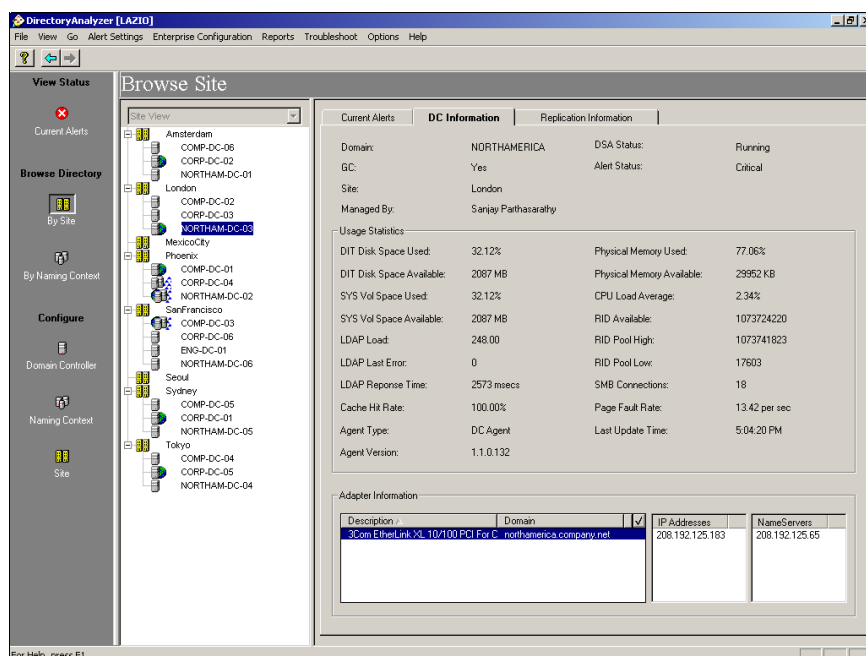


Figure 11 - DirectoryAnalyzer provides detailed information on critical Active Directory components

The following list details the types of information that can be displayed:

- **Naming Context Information** – Provides information specific to the selected naming context (e.g. domain operations master status and consistency, domain trust list, etc.).
- **DC Information** – Displays information specific to the selected Domain Controller (e.g. domain that it maintains; site that it's a member of; whether or not a copy of the global catalog is stored on this domain controller; who its replication partners are; and additional information about the current operational status of the DC.)
- **DNS Information** – Supplies information specific to the selected DNS server (e.g. server status, zones the server is authoritative for, whether or not they are primary, primary DNS or secondary, etc.)
- **Site Information** – Provides information specific to the selected site (e.g. list of domain controllers, DNS servers and global catalogs in the site, inter-site connections list, etc.)

# Troubleshooting

DirectoryAnalyzer provides specific, timesaving troubleshooting tests, including: DC, domain and site connectivity tests. Due to the advanced, distributed design of the DirectoryAnalyzer architecture, these troubleshooting tests do not take up critical bandwidth across WAN links. Some of the tools DirectoryAnalyzer provides are:

## DC Connectivity Test

DC connectivity tests afford an in-depth look at potential connectivity problems between selected domain controllers. DirectoryAnalyzer allows an administrator to run a variety of interactive tests for the selected domain controllers to determine important information, such as:

- IP ping response times
- DNS query response time
- LDAP query response time

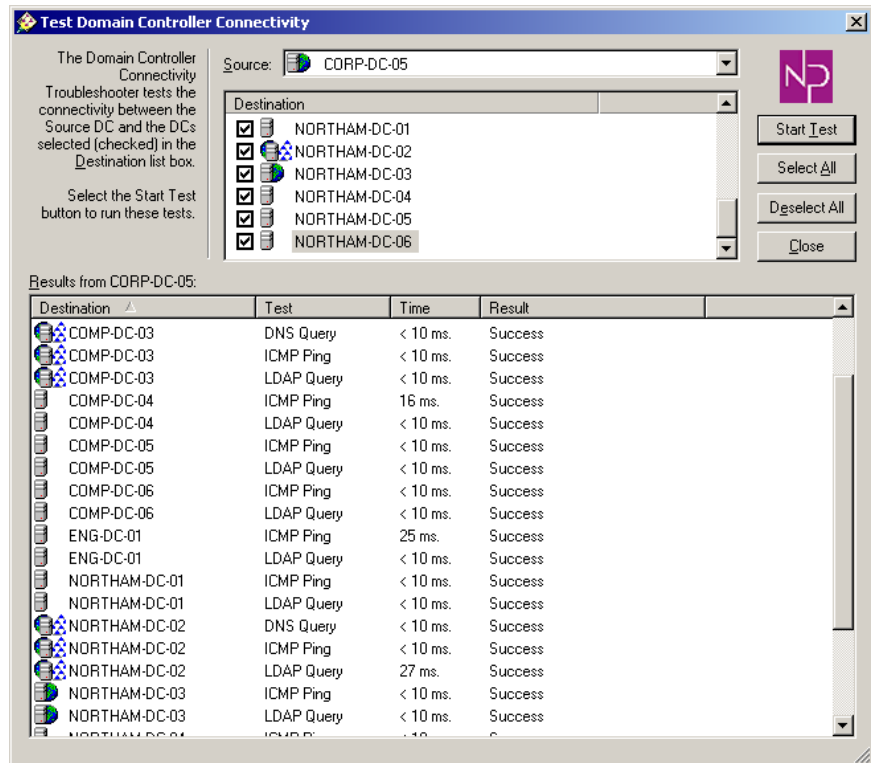


Figure 12 - DC connectivity tests can tell how well domain controllers are communicating

## Domain Connectivity Test

Domain connectivity tests provide administrators the means to run interactive tests against domains or sub-domains within Active Directory. Some of the important tests that DirectoryAnalyzer runs include:

- IP connectivity to each Domain Controller in the domain
- IP connectivity to each DNS server that is authoritative for the domain
- LDAP query response time for each Domain Controller in the domain
- DNS query response time for each DNS server that is authoritative for the domain

## Site Connectivity Test

Site connectivity tests determine what response times are between domain controllers in various sites. Site connectivity tests include the following:

- IP ping response times
- DNS query response times
- LDAP query response times

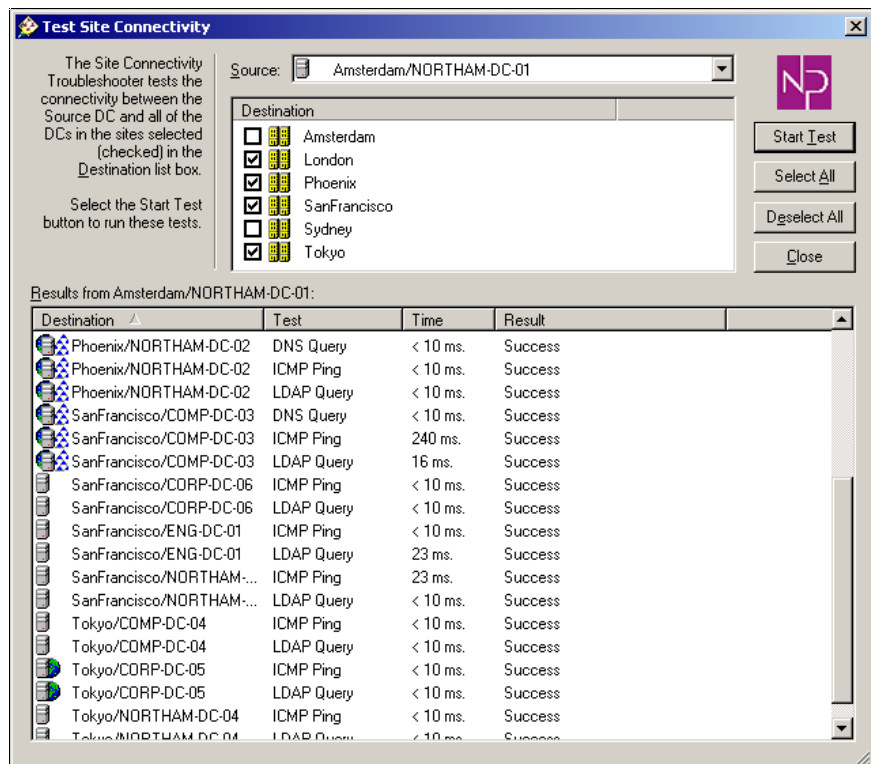


Figure 13 - Site connectivity tests provide interactive feedback on response times to various tests between sites

# Alert History Reports

DirectoryAnalyzer logs all alert activity, such as alert generation, alert escalation and alert clearing, in an alert history database that is stored on the Enterprise Agent. The purpose of this database is to provide administrators with the opportunity to trend and analyze their Active Directory alerts over time. With this capability, potential trouble spots can be identified early and action may be taken to remedy the problem before a crisis occurs. Through the DirectoryAnalyzer Client, administrators can specify the reports to be generated and can then save them to various file formats and/or deliver them to various locations via MAPI mail or Exchange Folders.

Following are the various formats that reports can be saved to:

- Excel
- HTML
- DHTML
- RTF

Following are the destinations to which reports can be sent:

- Application
- File
- Exchange Folder
- Microsoft Mail (MAPI)

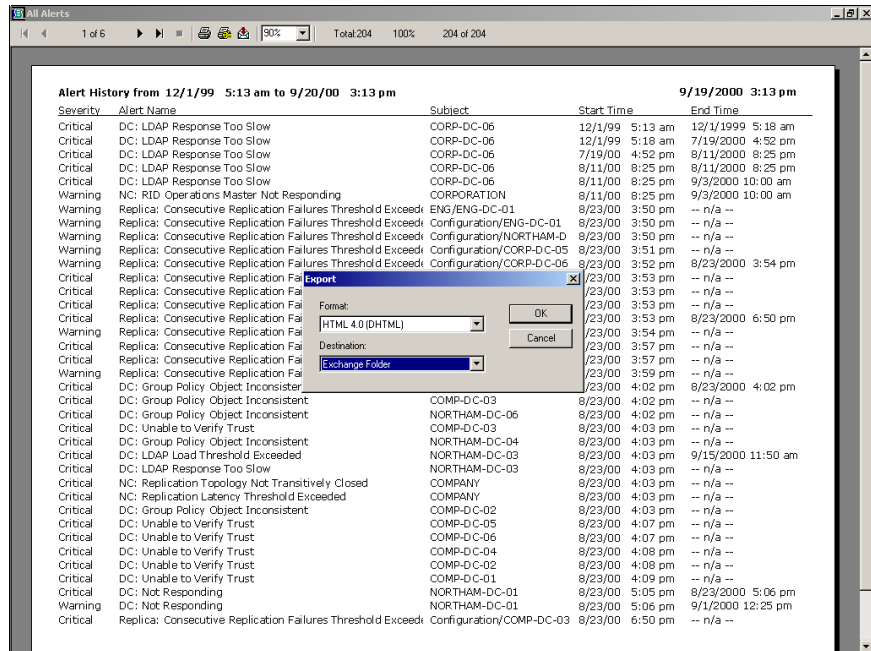


Figure 14 - DirectoryAnalyzer reporting capabilities allow reports to be exported and delivered to many destinations.

# Configuration

The configuration area is where DirectoryAnalyzer alerts can be customized and configured for specific Active Directory environments. The components of DirectoryAnalyzer that can be configured are as follows:

- **Thresholds** – DirectoryAnalyzer alerts have two levels of severity: warning and critical. When a situation escalates, a warning alert will be generated, indicating that a lower-level threshold has been crossed. As the severity of the error condition increases, a critical alert is generated, indicating that the higher-level threshold was crossed. A number of attributes can be customized for each of these levels, including the threshold value, duration before an alert occurs, and the duration before an alert clears.

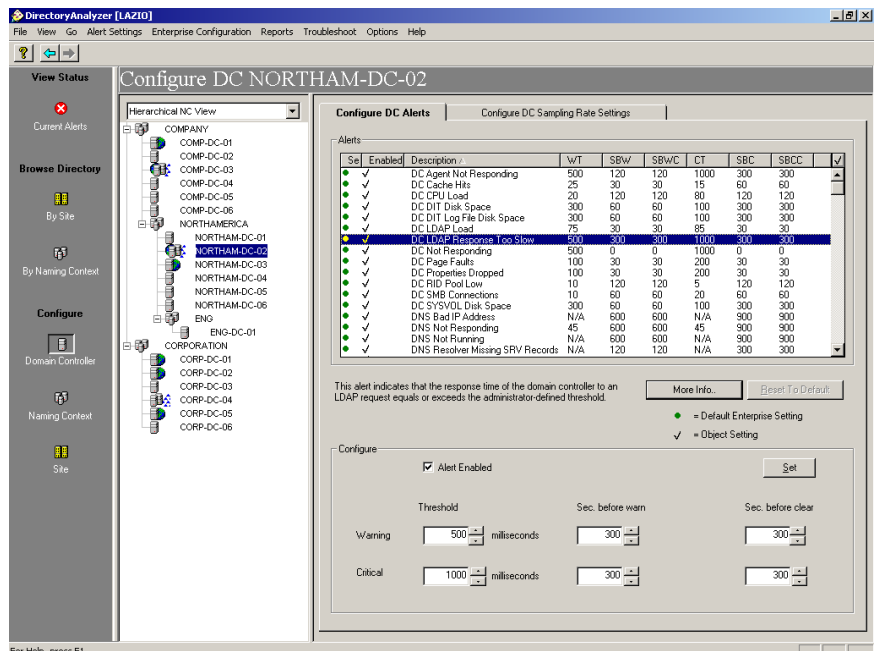


Figure 15 - DirectoryAnalyzer alert conditions can be tailored and customized to any Active Directory environment

- **Sampling Rates** – DC Agents and Site Agents in the DirectoryAnalyzer architecture gather information regularly from the domain controller on which they reside. Allowing the configuration of sampling rates provides an administrator with the ability to tune how often new information is “mined.” If there is a need to use less CPU or transmit data less frequently from a domain controller, tuning the sampling rates can provide that capability. One note of caution, though, the less frequent new information is gathered about the directory’s reliability, the less capable the DirectoryAnalyzer system will be to detect Active Directory problems.

# For More Information

---

## Contact NetPro

For the latest information on DirectoryAnalyzer for Microsoft Active Directory, check out our web site at:

<http://www.netpro.com/DirectoryAnalyzer>

# Glossary of Terms

## **DC Agent**

An NT service that runs on each Domain Controller within Active Directory and does the bulk of the monitoring work. The DC Agent detects alert conditions and passes them on to the Site Agent.

## **DirectoryAnalyzer Client**

The user interface for managing all aspects of DirectoryAnalyzer.

## **DNS**

Domain Naming System – A distributed namespace used on the Internet to resolve computer and service names to IP addresses and vice versa. Active Directory uses DNS for its location service.

## **Domain**

A domain is a partition of the directory namespace that can be replicated to multiple domain controllers. A domain is the security boundary and unit of replication within Active Directory.

## **Domain controller**

A Windows 2000 server that contains a replica of a given Active Directory domain.

## **Enterprise (a.k.a. Forest)**

A collection of one or more domains organized as peers, sharing a common schema, configuration and global catalog.

## **Enterprise Agent**

An NT service that runs on a member server. The Enterprise Agent communicates with Site Agents to build model of the directory. The Enterprise Agent services client requests. It also maintains DirectoryAnalyzer configuration and threshold settings.

## **Global Catalog**

A Domain Controller within Active Directory that contains a partial replica of every name context in the directory. It contains the schema and configuration naming contexts as well.

## **Namespace**

Any bounded area in which a given name can be resolved.

## **Schema**

The formal definition of all object types that can be stored in the directory and their associated attributes.

## **Site**

A location within a network that contains Active Directory servers, as defined by one or more TCP/IP subnets. Sites define the Active Directory replication topology.

## **Site Agent**

The Site Agent manages and configures DC Agents in a particular site and builds a partial model of the directory. The Site Agent passes its model, as well as relevant changes, events and alerts to requesting Enterprise Agents.

## **Tree**

A hierarchical structure of domains that form a contiguous namespace.