Quest® Reporter

User Guide

Version 5.5

QUEST SOFTWARE®

If you have any questions regarding your potential use of this material, please contact:

Quest Software World Headquarters
LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
email: legal@quest.com
U.S. and Canada: 949.754.8000

Please refer to our Web site for regional and international office information.

TRADEMARKS

Quest Reporter User Guide
Updated - September 2006
Software Version - 5.5

CONTENTS

Chapter 3

Chapter 4

Chapter 5

About This Guide

Overview

This document has been prepared to assist you in becoming familiar with Quest® Reporter, an integral component of Quest Windows Management Suite. The User Guide contains the information required to install and use Quest Reporter. It is intended for network administrators, consultants, analysts, and any other IT professionals using the product.

Conventions

In order to help you get the most out of this guide, we have used specific formatting conventions. These conventions apply to procedures, icons, keystrokes and cross-references.

ELEMENT	CONVENTION
Select	This word refers to actions such as choosing or highlighting various interface elements, such as files and radio buttons.
Bolded text	Interface elements that appear in Quest Software products, such as menus and commands.
Italic text	Used for comments.
Bold Italic text	Used for emphasis.
Blue text	Indicates a cross-reference. When viewed in Adobe® Reader®, this format can be used as a hyperlink.
📌	Used to highlight additional information pertinent to the process being described.
💡	Used to provide Best Practice information. A best practice details the recommended course of action for the best result.
⚠	Used to highlight processes that should be performed with care.
+	A plus sign between two keystrokes means that you must press them at the same time.
|	A pipe sign between elements means that you must select the elements in that particular sequence.

About Quest Windows Management

Quest Software, Inc. delivers innovative products that help organizations get more performance and productivity from their applications, databases, and Windows infrastructure. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 18,000 customers worldwide meet higher expectations for enterprise IT. Quest's Windows Management solutions simplify, automate and secure Active Directory, Exchange and Windows, as well as integrate Unix and Linux into the managed environment. Quest Software can be found in offices around the globe and at www.quest.com.

Contacting Quest Software

Phone	949.754.8000 (United States and Canada)
Email	info@quest.com
Mail	Quest Software, Inc. World Headquarters 5 Polaris Way Aliso Viejo, CA 92656 USA
Web site	www.quest.com

Please refer to our Web site for regional and international office information.

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract. Quest Support provides around the clock coverage with SupportLink, our web self-service. Visit SupportLink at http://support.quest.com.

From SupportLink, you can do the following:

- Quickly find thousands of solutions (Knowledgebase articles/documents).
- Download patches and upgrades.
- Seek help from a Support engineer.
- Log and update you case, and check its status.

View the Global Support Guide for a detailed explanation of support programs, online services, contact information, and policy and procedures. The Guide is available at http://support.quest.com/pdfs/Global Support Guide.pdf.

1

Introducing Quest Reporter

- Overview
- Quest Reporter Components
- Managing Your Network with Quest Reporter
- Quest Reporter Features

Overview

Quest Reporter is an invaluable tool for network administrators, security administrators, IT auditors, and other users in an enterprise network. It provides the ability to analyze the network, document the configuration, and make decisions based on the current state of the network.

Quest Reporter helps you administer your network by generating comprehensive enterprise-wide reports, from both real-time and stored data. Report templates can be run and exported on a scheduled basis, offering unprecedented flexibility. The intuitive interface allows users to retrieve necessary data quickly. For organizations with advanced needs, there are multiple formats for exporting data to custom applications.

Getting the Most from Quest Reporter

Day-to-Day Security and Standards Enforcement

Many organizations have policies and standards prescribing how their IT environments are managed. These policies cover such areas as user creation and deletion, and group population. Network and security administrators need to know that policies are being followed and standards are being applied correctly on a daily basis. In large environments, this can be time consuming as there may be thousands of users, groups, and computers to keep track of. To prevent security breaches, you can audit your environment frequently using Quest Reporter.

Preparation for Audit

The process of preparing for comprehensive IT security audits can be tedious and frustrating. You need tools to demonstrate that the environment is secure and being managed according to the organizational policies. Quest Reporter provides the information needed to prepare for a security audit.

Reporter provides report packs that will help you to ensure HIPPA (The American Health Insurance Portability and Accountability Act of 1996) and SOX (Sarbanes-Oxley) standards are adhered to.

Preparation for Change

Change in large IT environments must be accomplished quickly and securely, using minimal resources and without any loss of productivity. Quest Reporter provides the information needed to plan smooth transitions, ensuring that nothing is overlooked.

Quest Reporter Components

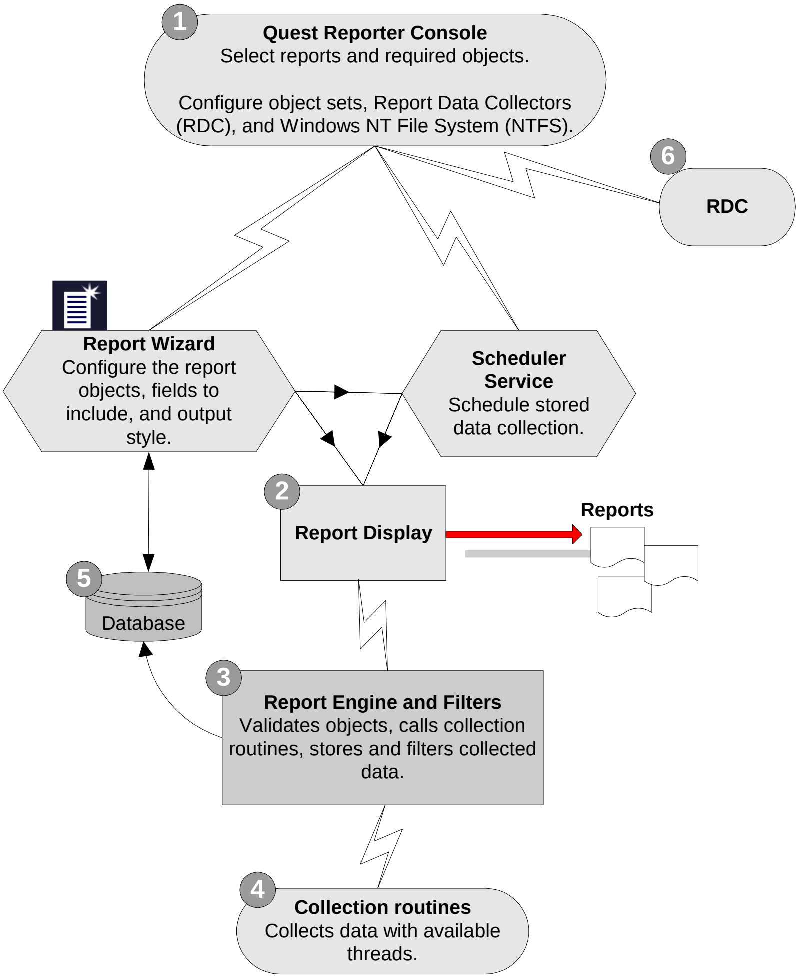

1
Quest Reporter Console
Select reports and required objects.
Configure object sets, Report Data Collectors (RDC), and Windows NT File System (NTFS).
6
RDC
Report Wizard
Configure the report objects, fields to include, and output style.
Scheduler Service
Schedule stored data collection.
2
Report Display
Reports
5
Database
3
Report Engine and Filters
Validates objects, calls collection routines, stores and filters collected data.
4
Collection routines
Collects data with available threads.

Figure 1: Quest Reporter components

① The console displays network information. Use the console to select reports, and configure the report data collectors (RDCs) and object sets.

② The report display component formats the information collected and exports the information into HTML and other formats such as Adobe PDF and CSV (Comma Separated Values).

③ The report engine coordinates all of Quest Reporter’s interaction with its database. It manages the information going to and coming from the collection routines as well as the generation of temporary views containing the actual report data. The report engine stores the data for the reports. Once the data is collected, the report engine invokes the report viewer to display the report.

④ The collection routines are an extensible set of components that Quest Reporter uses to enumerate information about network objects and their attributes.

⑤ The database is configured the first time you run Quest Reporter. Use the Database Setup Wizard to select the target database and to change the data source at a later time.

⑥ The RDC schedules data collection and tracks changes. It stores and timestamps this information, which is then used to create the reports. The RDC is a special packaging of the collection routines and report engine. It is designed to facilitate network object data collection from remote locations in highly distributed environments. Deploying an RDC prevents the need for the RDC installed on the main console to enumerate information across potentially busy or slow WANs (Wide Area Networks).

For more information on RDC deployment, see “Deployment Considerations” on page 18.

Quest Reporter for Novell

Quest Reporter for Novell is an add-on pack for Quest Reporter that offers administrators the ability to collect and report on Novell networks. The report templates are designed to help organizations plan for their pending migration from Novell to AD. Reports range from User and Group data to permissions. With Quest Reporter for Novell, you can also easily perform key critical tasks against objects in the NDS/eDirectory environment using action-enabled reporting.

You can download Quest Reporter for Novell from the Quest Reporter page of the Quest Software web site (http://www.quest.com).

Please refer to the Quest Reporter for Novell User Guide for information on how to install the add-on pack and how to run report templates. You can access the Quest Reporter for Novell User Guide from the Documentation tab of the installation program. You can access the installation program by double-clicking **Autorun.exe** after you have extracted the zipped files.

Managing Your Network with Quest Reporter

Quest Reporter provides a streamlined approach to report generation. Many operations that have traditionally required personal visits to individual computers can now be accomplished locally from your computer.

Quest Reporter helps you maintain and manage enterprise directories through security, standards conformance, and general administration reports.

You can use Quest Reporter to perform the following tasks:

- Create reports by selecting objects and containers from Active Directory, Windows NT, and Windows NTFS
- Access report templates grouped to match directory object classes such as users, groups, domains, computers, and Access Control Lists (ACLs)
- Modify predefined report templates to suit your own requirements
- Schedule reports to run automatically and save the results to a location of your choice
- Gather information by installing RDCs in remote offices
- Schedule collections to generate stored data reports later
- Access NTFS report templates to audit users and groups contained in ACLs, ensuring compliance with your company's standards for protecting sensitive data
- Create reports faster with reusable, user-defined selections of network objects (object sets) from one or more domains
- Create a category of favorites to access on a regular basis and share your list of favorites with other users

Quest Reporter Features

Quest Reporter is more than just a reporting tool. It is a sophisticated, extensible data collector with the ability to present collected information in a number of different formats.

Report Generation

You can run reports in the following ways:

- Selecting objects through the following nodes in the console: Windows NT, Active Directory, IP Subnet, or Object Set
- Running a report template from the Reports or Favorites nodes
- Generating a report using a scheduled favorite

Modes of Reporting

Using Quest Reporter, you can generate reports based on stored or live data.

Live Data Reports

A live data report collects information from the network at the time of running the report template. Select a live report template to collect information for the report immediately. A live data report gathers the latest network information.

For more information on how to generate live reports, see “Generating a Report” on page 35.

Action-Enabled Reports

Action-enabled reporting is a subcategory of live data report templates that allows you to update network information within a report. You no longer have to read from the report output as you make changes within another management tool. Make the changes in the report, and if you have the appropriate rights, the information on the network will be updated immediately.

For information on how to generate action-enabled reports, see “Generating a Report and Changing Network Data” on page 58.

Stored Data Reports

Stored data reports are reports that are generated from previously collected data in the database. The data may have been collected by an earlier live report or from a scheduled collection. An advantage of stored data reports is that they take a fraction of the time to generate compared to live reports.

For information on how to generate stored data reports and configure and schedule data collection, see “Creating Custom Report Templates” on page 53.

Object Sets

An object set is a defined logical container that allows you to group objects in a convenient manner. An object set can contain specific objects, containers (Organizational Units and groups), or entire domains. An object set can cross domains.

For example, you may want to run certain reports on users in the Finance department on a recurring basis but the users exist in multiple places throughout your directory. Instead of searching through your directory to find the users each time you run the report you can create an object set and then add the users to the object set. The next time you run the report, you can select the object set rather than each user in the Finance department.

Favorites

A favorite is a special type of report template that provides a method of persisting or saving all report properties so that the next time the report runs, there is no user intervention. You can schedule a favorite to run at any time.

The report attributes that are saved in a favorite include the following report properties: Objects, Filter, Output, Collection, Attributes, Grouping, and General.

Filtering

Using a filter, you can narrow the focus of report results by setting certain criteria on the resultant set of objects.

You can build the filters using the available attributes for each report type, select a condition (for example, Equals, Is Greater Than), and enter a value for the filter.

Linking Attributes Between Categories

Attribute linking allows you to select additional attributes of an object that are not the primary focus of the report. This allows you to customize the distinguishing attributes of an object that make sense.

This provides a means of associating object types and attributes and providing more meaningful information in your report.

Multi Forest Reporting

A single forest deployment is characterized by all of an organization’s network objects being contained within one forest and a group of domains, whereas a multiforest deployment separates an organization’s network into various forests and their respective domains. The multiforest deployment is by far the more secure deployment; however, it can be complex to administer.

Quest Reporter supports multiforest deployments. Domains in multiple forests are displayed as individual fully-functional nodes that allow you to connect to and run a single report template on object types from different forests.

2

Deploying Quest Reporter

- Deployment Overview
- Data Transport Modes
- Deployment Considerations
- Setting up a Database
- Deployment Considerations for Scheduled Collections

Deployment Overview

This chapter provides information on the following:

- Data transport modes
- Database setup
- Deployment scenarios
- Scheduled collections deployment and scenarios

Data Transport Modes

Quest Reporter provides you with two different types of data transport modes. The collection modes are configured per Reporter Data Collector (RDC). During installation, you can specify installation of one or both.

- Direct data transport

  This mode collects the data and stores it directly to the database.

  Direct data transport is available with live collections and scheduled collections.

- Compressed data transport

  This mode collects and compresses the data on the RDC host. The compressed data pack is then streamed to the Console host, decompressed and uploaded to the database. This mode minimizes bandwidth consumption, as the data being transferred back to the main console is compressed, and thus improves the delivery speed over WANs.

  With the exception of remote permission-based scheduled collections, Compressed data transport mode is available for all remote scheduled collections. Permissions-based collections such as Active Directory and NTFS currently leverage direct mode only.

  If you use the compressed data transport mode then Microsoft Message Queuing (MSMQ) must be installed on the Console host and RDC host. Reporter automates the installation of MSMQ 2.0 or later. If MSMQ is not detected, Reporter performs a silent install of MSMQ in workgroup mode (using independent client setup).

If you choose not to install the compressed data transport during installation, you can always change the transport mode later using the Quest Reporter Configuration utility. For more information, see “Installing Compressed Data Transport Mode” on page 100.

Using Compressed Data Transport Mode

If you choose to use the compressed data transport mode, you can take advantage of the following features:

- Bandwidth on the network. The compressed packets of information will speed the delivery of the data over WANs.
- Improved reliability in case of network connectivity issues.

Permissions-based collections for NTFS and AD object classes and attributes are not supported in compressed data transport mode; they leverage direct mode only.

Figure 2 is a high-level illustration on how the compressed data transport works. The RDC host and Console host can be in the same LAN or they can be across a WAN.

The Microsoft® SQL Server™ database can be installed on the same computer as the Console host or it can be installed on another computer in the domain.

The RDC computer hosts the RDC process and two services. The Console computer hosts two services as shown:

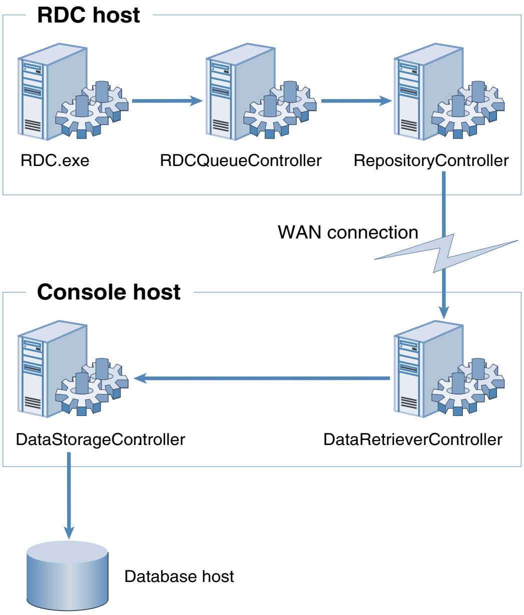


Figure 2: Compressed data transport mode

The following table provides descriptions of the Reporter services:

SERVICE	DESCRIPTION
RDCQueueController	Allows collected data to flow to a repository. Deployed to the RDC host.
RepositoryController	Provides notifications about the repository. Deployed to the RDC host.
DataRetrieverController	Allows data to flow from the RDC host to the Console host. Deployed to the Console host.
DataStorageController	Allows data to flow to the database. Deployed to the Console host.

For more information on the services, see “Managing the Services” on page 101.

Deployment Scenarios

Deployment Considerations

Quest Reporter is a database-driven application. For successful deployment, consider the following:

- Will Quest Reporter be used as a single console application, or will it be distributed to a team of users?
- Will information sharing be required?
- Have SQL Servers been deployed on the network?
- Do the SQL Servers meet the minimum SQL Server standards, and is there sufficient disk space for all collected information?
- Do you want to save collected data and track changes over time?

Depending on your requirements, it might be sufficient to use Microsoft® SQL Server™ Desktop Engine (MSDE 2000) to store the collected information. However, if you intend to conduct large network interrogations and share collected information with other administrators, Microsoft® SQL Server™ 2000 or 2005 is recommended.

Consider how you intend to use the collected data. If you plan to do database mining on your own, SQL Server 2000 or 2005 is recommended. Either of these supplies you with the tools required to view database information and build powerful queries.

Single Computer Deployment

In a single computer deployment, Quest Reporter and the database server are installed on the same computer.

The desktop edition of SQL Server 2000, MSDE, is typically installed.

Limitations

Quest Reporter has the following limitations in single computer deployments:

- Collections across a WAN are inefficient
- The workload cannot be shared across computers

There are no management tools (SQL Enterprise Manager) with MSDE. Managing the database permissions can be cumbersome. Management tools are available if there is a full copy of SQL Server installed on the network.

MSDE is not optimized for multiuser applications and has a 2 Gigabyte (GB) database size limit.

Recommended Hardware

- 1 GHz Pentium® 4 processor or better
- 512 MB RAM (1 GB recommended)

MSDE and Quest Reporter are both processor and memory intensive—they will compete for computer resources.

Enterprise Deployment

In a typical enterprise deployment, Quest Reporter is installed on one of the following: Windows 2000 Professional, Windows XP, or Windows 2003.

You may want to run the Quest Reporter console in a Terminal Services window.

Quest Reporter has been tested to run on Microsoft Windows Terminal Services in Application Mode. For more information about deploying applications under Terminal Services, please see the relevant Microsoft documentation.

The Quest Reporter database is usually hosted on a preexisting Microsoft SQL Server 2000 or 2005 database server.

Non-Microsoft database servers are not supported.

SQL Server Enterprise Manager is required to manage the customized SQL Server roles that ship with Quest Reporter.

Recommended Hardware

The following hardware requirements apply to workstation installations:

- 1 GHz Pentium® 4 multiprocessor or better
- 1 GB RAM (2 GB recommended)

Setting up a Database

The Database Setup Wizard guides you through the process of selecting and (if required) creating the database used by Quest Reporter.

To identify what database Reporter is currently accessing, right-click the Reports subnode and select **Properties**.

You can use one of the following security credentials when setting up the database:

- The user is a member of the Administrators group on the workstation and is added to SQL Server with permissions to create a database.
- The user is a member of any group on the workstation and is added to SQL Server with permissions to create a database.
- The user connects using SQL Server authentication with an account that has permissions to create a database.

Quest Reporter uses one database for live and stored data collections.

Quest Software recommends that you create a new database if you are installing Quest Reporter for the first time.

To create a database

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Quest Reporter Database Setup**.

   If you restart your computer, with SQL Server installed, the Database Setup Wizard does not initially list your computer as a database *option. There is a delay before SQL Server is recognized by the Browser Service. Type the name of the computer in the Computer box to avoid a time lapse.*

You can change the database after the initial installation of Quest Reporter. Run DBSetup.exe located in the following directory: Program Files\Common Files\Quest Shared\Quest Management Suite.

2. Click **Next**.
3. Select the domain and computer where you want to create the database.
4. Select the authentication method to grant database access.

   NT authentication requires a valid Windows NT user name and password.

   SQL Server authentication requires a valid SQL Server log on name and password.
5. Click **Next**.
6. Enter a name for the database or select an existing database on the server, then click **Next**.
7. Click **Next**.
8. Review the summary information, then click **Finish**.

SQL Server Roles

Depending on your corporate security policies, you may want to restrict access to the Quest Reporter database.

As Quest Reporter uses a Microsoft SQL Server database, you must use the security mechanisms provided by SQL Server. Permissions on SQL Server databases are managed through “roles”. To grant someone the rights associated with a particular role, you must add that user account to the role. For more information on managing roles in SQL Server, see the Microsoft SQL Server Enterprise Manager Help.

To take advantage of the predefined SQL Server roles created by Quest Reporter, you must first determine the reporting responsibilities of your administrators and end users. Depending on the rights you want to grant, add these users to one or more of the roles.

Quest Reporter includes the following customized SQL Server roles, each providing a different level of access to the database:

ROLE	DESCRIPTION
Reporter Admin	Members have full access to the Quest Reporter database.
Stored Report Generator	Members can run report templates against stored data only. **Note:** Unless the default Report Wizard collection type is changed using the Configuration Utility, it may appear that members in this role can run a live report template. However, no data is stored to the database and any resulting report is based on the existing contents of the database.
Live Report Generator	Members can run report templates against live or stored data.
Reporter Data Collector	Members can only set up stored data collections. **Best Practice:** Create a dedicated user account for scheduled collections and add the user account to this role. **Note:** This role is not intended for regular interactive users of Quest Reporter.
Report Creator	Members can create, modify, and delete report templates. Members can duplicate report templates, add and remove fields, and change groupings. If you select this role, then you must also select either the Live Report Generator role or the Stored Report Generator role. If you add an account to only this role, then the account will not have sufficient database permissions to run Quest Reporter.
Object Set Creator	Privileges to create, modify, and delete object sets. If you select this role, then you must also select either the Live Report Generator role or the Stored Report Generator role. If you add an account to only this role, then the account will not have sufficient database permissions to run Quest Reporter.

Deployment Considerations for Scheduled Collections

When you install Quest Reporter, you must select a database where all data will be stored. When a scheduled collection is created, it associates the data collection with the database. The database association is maintained by the scheduled collection and not the Report Data Collector (RDC). An RDC host may be used by different installations of Quest Reporter that may point to separate databases and possibly different SQL Servers.

If you are running collections over a Wide Area Network (WAN), you may consider deploying several RDCs throughout your network. This decreases network traffic during data collection, and will help collect data in parallel. Then each RDC stores data back to a central database from which you can later run your reports.

Logon Credentials

When setting up scheduled collections, you need to provide accounts that can

- Access the database and save the data to the database

  You can use either Windows NT or SQL Server logon credentials.

- Run the scheduled collection on the selected computer

  You can only use Windows NT logon credentials.

As a database administrator, you may want minimal access to the database. If so, select the SQL Server authentication to log on to the database.

Using the same SQL Server account but different Windows NT accounts for each scheduled collection provides flexibility in collecting data from different (possibly untrusted) domains while limiting the number of accounts that access the database.

Distributed Scheduled Collections

Recommendations for scheduled collections are as follows:

- Place RDCs close to the data source.

  For example, install RDCs in remote offices to collect information from the computers in these offices.

- Create object sets to divide the collections among several RDCs in domains with large numbers of users, groups, or computers.

  For example, create object sets called “Users A-M” and “Users N-Z”. Each RDC can use its local domain controller (DC) as its data source. This practice prevents a single DC from being overloaded with requests for information from multiple RDCs.

Ordinarily, RDCs should not be installed on DCs - there is no reason to do so, even when collecting domain (user or group) information.

- Create scheduled collections to collect different types of information, such as user and group data.

  This helps you organize collections and track progress of the collection.

- If multiple RDCs are deployed, configure each to store its data into a central SQL Server database or repository. This consolidates the data and prevents data source switching when generating reports.

The flexibility of the RDCs results in an infinite number of combinations for deployment. Determine the appropriate conditions for the environment. When deciding how to deploy RDCs, ask yourself the following questions:

- Where are my domains located?
- What is the bandwidth between remote offices?
- Where are my resource domains, and what types of network objects do they contain?
- Where is my database located in relation to my domains?

Scheduled Collection Scenarios

A scheduled collection can be set up on any enterprise computer to collect network information. This collection process can be extended as the enterprise grows.

The following general scenarios are illustrated in this section:

- Small enterprise
- Medium enterprise
- Large enterprise

Small Enterprise Deployment Scenario

A small enterprise may contain approximately 20,000 computers and accounts. The RDC, installed when Quest Reporter is installed, can collect all data.

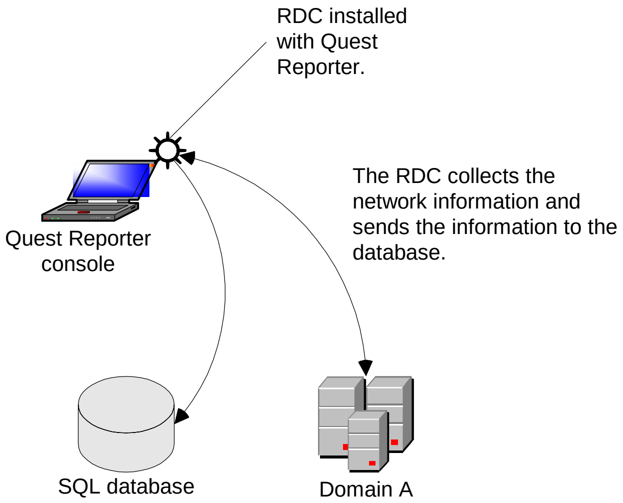

RDC installed with Quest Reporter.
Quest Reporter console
The RDC collects the network information and sends the information to the database.
SQL database
Domain A

Figure 3: RDC deployment for small enterprises

Medium Enterprise Deployment

In a medium enterprise, several RDCs can be deployed. Deploying multiple RDCs has the following advantages:

- Increases the speed of data collection
- Reduces the redundancy of RDCs collecting the same data
- Provides a means of organizing the data collection process

When there are multiple RDCs, divide the tasks among the RDCs. For example, the scheduled collections can be based on domain, geographical separation, or object types (computers, user accounts, printers).

A medium enterprise may contain 20,000–50,000 computers and accounts and four domains.

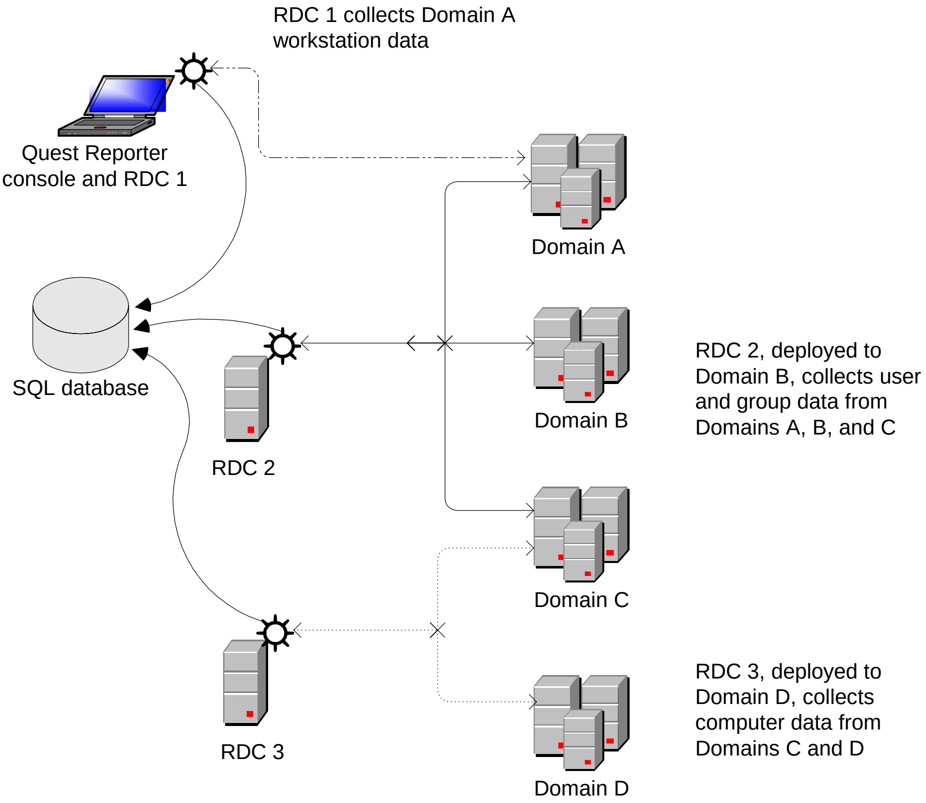

RDC 1 collects Domain A workstation data
Quest Reporter console and RDC 1
SQL database
RDC 2
RDC 3
Domain A
Domain B
Domain C
Domain D
RDC 2, deployed to Domain B, collects user and group data from Domains A, B, and C
RDC 3, deployed to Domain D, collects computer data from Domains C and D

Figure 4: RDC deployment for medium enterprises

As shown in Figure 4 on page 26, the RDCs send the collected information to the SQL Server database.

Large Enterprise Deployment

In large enterprises, multiple RDCs can be deployed per domain. Each RDC can then collect selected data.

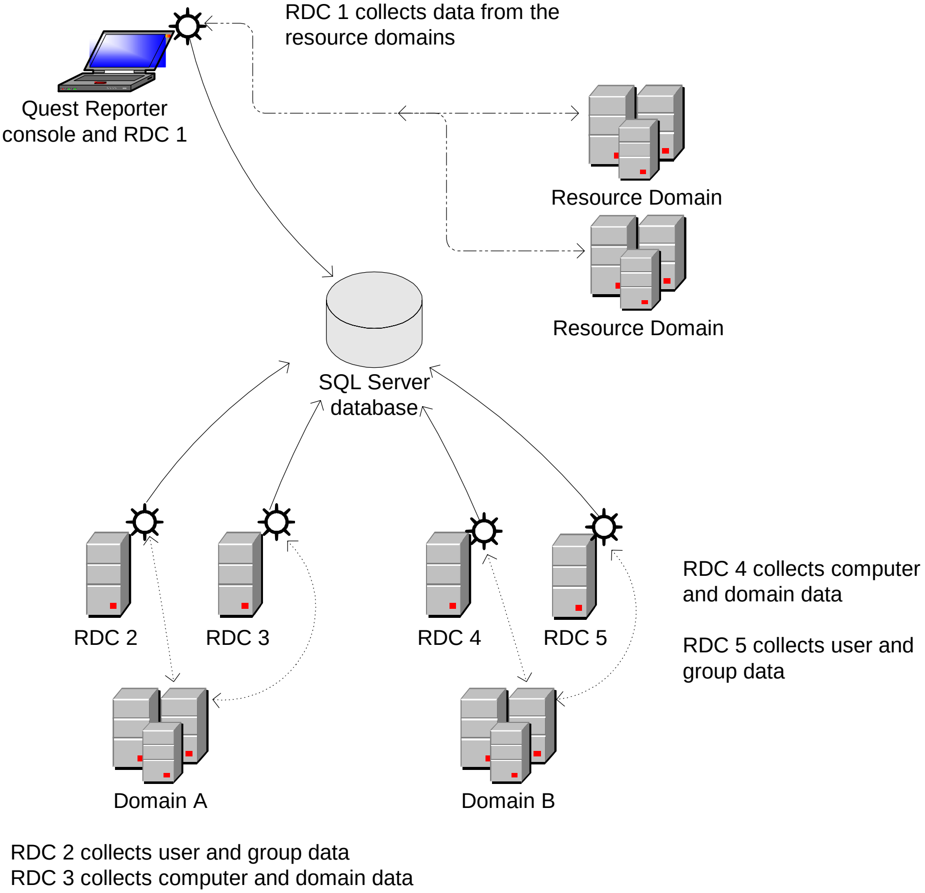


Figure 5: RDC deployment for large enterprises

3

Getting Started with Quest Reporter

- Getting Information About Your Enterprise
- Setting up the Console
- Generating a Report
- Reviewing the Status of Collections

Getting Information About Your Enterprise

Quest Reporter ships with many predefined report templates that collect different types of network information. Quest Reporter can collect information from the following sources:

- Windows NT Security Accounts Manager (SAM)
- Active Directory
- Active Directory security (ACLs)
- Windows NTFS (folders, space used)
- Windows NTFS security (ACLs)
- Server and workstation configuration

Report Template Categories

The predefined report templates are organized by the following categories:

- Computers
- Groups
- Permissions
- SOX Compliance
- Users
- Domains
- HIPAA Security Standards Compliance
- Security Auditing
- Summary
- VAS Reporting

Setting up the Console

This chapter assumes the following:

- Quest Reporter has been installed on a computer.
- A Microsoft® SQL Server™ 2000 or 2005 database has been set up using the Database Setup Wizard.

Before you begin generating reports, you must add the objects that you want to gather data from.

Every organization’s network is different. Some networks are large and contain many domains, while others may have only one. Quest Reporter allows you to set up the console, so you can view only those parts of your network on which you want to report. After you add a domain or IP subnet to the console, you can expand it and set options to retrieve data and generate reports.

You can also display network objects by creating an object set. For more information on object sets, see “Creating Object Sets” on page 64.

Working in the Console

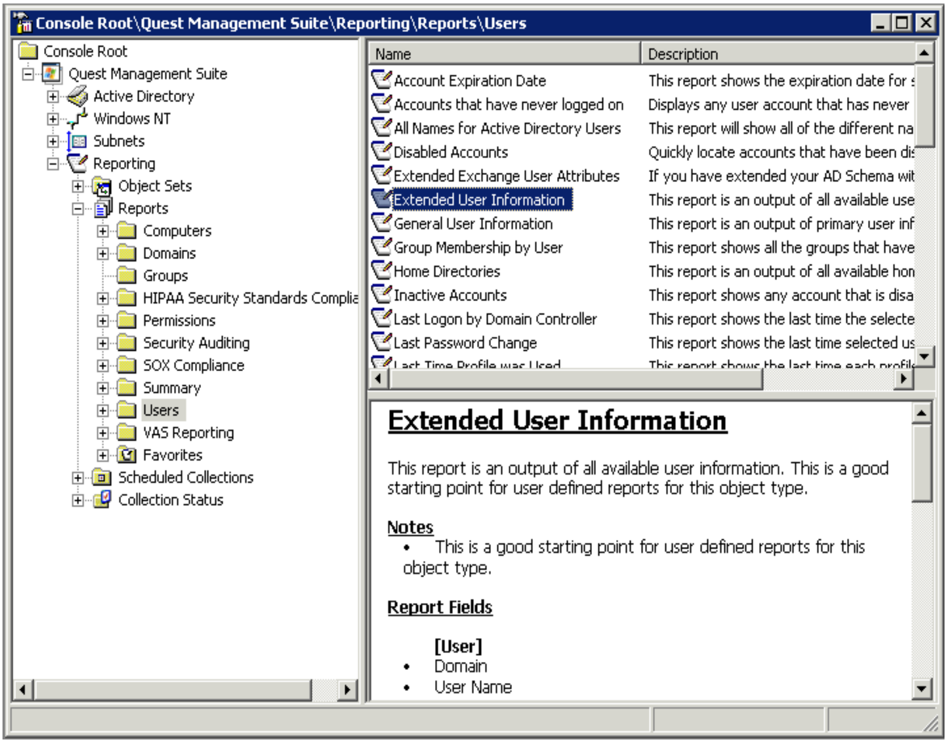
Quest Reporter runs in the Quest Management Suite console. The console design is based on the Microsoft Management Console (MMC). You can customize the view by hiding or showing various components of the console such as menus, toolbars, tabs and the console tree.

To customize the view

1. Click and select **Customize View**.
2. Modify the current view by selecting or clearing the appropriate check boxes.

Quest Reporter uses the right-click menus typical in the MMC application design. The Quest Reporter right-click menus also include standard MMC menu items.

In the Reporter console, the left pane contains a treeview that includes the domains and subnets you have added, along with the Reporting node. The Reporting node contains the following subnodes: Object Sets, Reports, Scheduled Collections, and Collection Status. When you select one of these subnodes, information about its contents is displayed in the panes to the right.



Name	Description
Account Expiration Date	This report shows the expiration date for s
Accounts that have never logged on	Displays any user account that has never
All Names for Active Directory Users	This report will show all of the different na
Disabled Accounts	Quickly locate accounts that have been dis
Extended Exchange User Attributes	If you have extended your AD Schema wit
Extended User Information	This report is an output of all available use
General User Information	This report is an output of primary user inf
Group Membership by User	This report shows all the groups that have
Home Directories	This report is an output of all available hon
Inactive Accounts	This report shows any account that is disa
Last Logon by Domain Controller	This report shows the last time the selecte
Last Password Change	This report shows the last time selected us

Extended User Information

This report is an output of all available user information. This is a good starting point for user defined reports for this object type.

Notes

- This is a good starting point for user defined reports for this object type.

Report Fields

[User]
- Domain
- User Name

Figure 6: Quest Management Suite console with Quest Reporter installed

When you select a report template in the upper-right pane, a report information page is displayed in the lower pane that includes the following information about the report template. Not all of the report templates display all of the items.

ITEM	DESCRIPTION
Report Fields	Shows a list of fields that can be generated in the report.
Notes	Provides recommendations on when to use the report template.
Applied Filters	Shows any filters that will be applied to the report template. When you change the filtering, the report information page is updated.
Suggested Filters	Provides a list of links that you can select to apply filters to the report template.
Grouping	Shows the default grouping for the report template. When you change the grouping, the report information page is updated.

ITEM	DESCRIPTION
Related Reports	Provides a list of links to related report templates.

Adding Domains

You can add either a Windows NT 4.0 domain or Active Directory domain to the console.

You can add any trusted Active Directory domains to the console by their down-level (NetBIOS) names.

To add a domain

1. Right-click **Windows NT | Connect to**.

   – OR –

   Right-click **Active Directory | Connect to**.
2. Enter a domain name or the DNS name of the domain controller.

   – OR –

   Click **Browse** and select a domain from the list of all available domains.

   – OR –

   For Active Directory only, select one of the following container types from the list: Domain, Schema, Configuration, or Sites.
3. Click **OK**.

Adding IP Subnets

Reporting by IP subnet is required when you want to base reports on the physical layout of the network.

An IP subnet references objects by IP address rather than by name. An IP subnet is a convenient way of labeling and organizing your network topology for reporting.

For example, an organization might have one office in New York and another in Seattle with computers from both sites located in the same domain (North America) and connected through a WAN. All computers are in the same domain, but their IP addresses are different as they are in different subnets.

Using Quest Reporter, an administrator in New York can add the New York and Seattle subnets, allowing the administrator to report on only the computers in the relevant subnets. By adding the IP subnets, the administrator can generate reports against local computers for faster collection.

The IP subnet number is verified. If the subnet does not exist within the company, reports are not generated against the IP subnet number.

To add an IP subnet

1. Right-click **Subnets | New | Subnet**.
2. Click **Next**.
3. Enter a name and description for the IP subnet, then click **Next**.
4. Enter an IP address and subnet mask.

   The subnet mask allows Quest Reporter to determine how many possible IP addresses are available within an IP subnet. The subnet mask is a 32-bit number that distinguishes the network and computer section of an IP address and determines if the host is local or remote.

   For example, the subnet mask may be 255.255.255.0 and the IP Subnet 10.0.0.0. This means that valid IP addresses for that subnet are 10.0.0.1 to 10.0.0.254. Only 254 computers can be connected to that subnet at one time.
5. Click **Next**.
6. Click **Add** to enter a range of IP addresses to exclude from this IP subnet then click **OK**.

   Excluding ranges allows you to block out a portion of the IP subnet range. For example, if a range (10.0.0.20—10.0.0.30) is reserved for dial-up connections, you might want to exclude this block, as any reporting, collecting, or querying to these computers might be slow.

7. Click **Next**.
8. Click **Finish**.

   Any IP subnets and computers in that subnet are displayed under the IP Subnet node.

Generating a Report

You can generate reports in the following ways:

- Selecting objects through the following nodes in the Quest Reporter console: Windows NT, Active Directory, IP Subnet, or Object Set
- Running a report template through predefined report categories
- Creating and running a favorite

Administrative rights or registry access are required on all computers where you want to run report templates. Otherwise, reports can be generated but not all information may be collected.

Enumerating Object Types

When you are selecting objects to report on, you can set the following levels of recursion for an Organizational Unit container:

- The parent OU container only
- The first child level OU
- All OU levels within the OU container

To generate a report

1. Double-click a report template.

   – OR –

   Right-click a report template and select **Run Report**.

   The Objects, Collection, and Output tabs are displayed by default. You can configure the tabs that will be displayed. For more information, see “Configuring the Tabs in the Report Dialog Box” on page 109.

You can also expand Windows NT or Active Directory, right-click the objects that you want to report on, and select **Reporting | Run Report**.

2. Click the **Objects** tab and select the objects to report on.

   *Use **Query** to set search parameters for the objects you are reporting on. Quest Reporter finds the most current information at the time the report is generated. For more information on using queries, see "To create an object set" on page 65.*

3. To select the level of recursion for an OU container, right-click the container, then select **Options**.
4. Select the level of recursion, then click **OK**.
5. Click the **Collection** tab and proceed as follows:

OPTION	EXPLANATION
Live collection	Select this if you want to collect current data from your environment for reporting. The amount of data being collected can impact the amount of time required to produce report results. This is the default option for source content.
Stored data	Select this if you want to report using data previously collected and stored in the Reporter database. This method of reporting can significantly improve report performance as no live collection is taking place. Also, using stored data does not adversely impact your network.
Change History	Select this if you want to compare stored data with the most recent data. You can track changes on information that is already in the database with information retrieved during a live collection. You can also use the Change History option with stored data only. As no live collection takes place, performance is significantly improved. If you select Change History, you need to enter the date range information.
From To	In this date range option, the date range is based on a set window of time that you specify. **Note:** Midnight is used as a starting and ending point for the dates you select. That is, if the date range is Start Date = 07/22/2006 and End Date = 07/24/2006, this is interpreted as July 22 starting at 00:00 GMT time and ending July 23 at 23:59 GMT time. The report only displays changes that occurred within this time frame. Changes that actually occurred on July 24 are not included. This is an important distinction to keep in mind when you specify a range.

OPTION	EXPLANATION
Or	In this option, the date range is based on a sliding window of time. The sliding window of time provides more current history reporting on the objects. When you specify a number of days, weeks, or months, this value is applied based on the current date and time when the report template is run. For example, if you specify five days and run the report template today at 18:00 hours, the report content is based on data in the Reporter database that was collected over the last five days. The time frame for the data in question would start from today at 18:00 hours and go back to five days ago at 18:00 hours.
Use linked data from the database	Select this option if you do not want to do a fresh collection on linked objects. There may be instances when a fresh linked collection is not necessary. For example, if you do a collection on groups and link in users, you may not want to collect linked users if you have just done a collection on all the Domain users.

6. Click the **Output** tab and proceed as follows:

OPTION	EXPLANATION
Screen	Select this option if you want the report results to be displayed once the report has been generated. This is the default output option.
File	Select this option if you want to save the report results to a file. If you select File, select a file type, browse to the folder where you want to save the report, and enter a file name for the report.
Append datestamp to file name	Select this option if you want to add the date to the end of the file name.
One file per page of report	Select this option if you selected HTML as the file type and you want one HTML file generated for each page of the report.

OPTION	EXPLANATION
Layout	Click this button to select the style and orientation of the printed report.

7. Click **OK**.

   These values are not saved; you must set them every time you want to run a predefined report template. If you want to save the settings, you can save the report template as a favorite. For more information, see "Using Favorites for Frequent Reporting" on page 75.

When a report is generated, a log file is created that lists all the actions which occurred during report generation. Other information, such as the version of Reporter, the user who generated the report, and the computer where the report was generated, is also included at the beginning of the log. The default folder path where these log files are located is C:\ReporterLogs. For information about changing the default path, see "Configuring Log Settings" on page 114.

For information on using more advanced report features and managing report properties, see "Managing Report Template Properties" on page 39.

Reviewing the Status of Collections

When you run scheduled collections or live reports, you can track the status of the report collection. The information is saved in a status file. For more information about collection status files, see "Setting Collection Status Features" on page 121.

To review the collection status for a report

1. Expand **Reporting | Collection Status**.

   The computers shown are the local computer and computers where RDCs reside.

2. Select a computer to display the scheduled collections or live reports in the upper-right pane.
3. Select the name of the job to display the following information about the collection: status, number of objects queried, collection details, and location of log file.

   The collection details include whether the query was successful and if there were any errors encountered during the collection.

4

Managing Report Template Properties

- Using Different Collection Modes
- Applying Filters to Attributes
- Linking Attributes
- Grouping and Sorting Attributes
- Viewing and Saving Reports
- Creating Custom Report Templates
- Importing and Exporting Report Templates

Using Different Collection Modes

A report can be generated against live network data or data already gathered and stored in the database.

Live Data Collections

Live reports retrieve information about the current state of your network environment (based on the selected attributes).

Live reports may take longer to generate than reports based on stored data. A live report template must first enumerate data for the report content from the network (for example, from the Active Directory) and store it in the database. The speed of this process depends on network traffic and other conditions present at the time the report is generated.

Stored Data Collections

The content of stored data reports is based on data previously gathered and stored to the database through either a scheduled collection or using a live report template.

A stored data report is generated quickly because the content is extracted from the database as fast as the SQL Server can provide it.

Though the information in stored data reports is not live data, Quest Reporter’s flexible scheduled collection capabilities will prevent stored information from getting “stale”.

For information on scheduled data collection and report data collectors (RDCs), see “Setting up Scheduled Collections” on page 81.

Linked Attributes and Stored Data

If you are reporting on stored data and want to include information for linked attributes, you need to incorporate this into your scheduled collection. You should include all the primary attributes you intend to report on. If any of the primary attributes are linkable, you must include at least one of the linked-in attributes to insure all the appropriate information is collected for stored data reporting.

The following table shows dependencies based on the following object categories:

FOR	ATTRIBUTES REQUIRED FOR RE-LINKING
NDS Objects	Collect "Tree" and "Distinguished Name" of the linked object.
AD Objects	Collect "Distinguished Name" of the linked object. **Note:** If you are reporting on a SID relation, you need to collect a "SID" and a "Domain" attribute for the linked object.
NT Object	Collect "Account Name" of the linked object.

To change the collection mode

1. Right-click a report template, then select **Run Report**.
2. Click the **Collection** tab and select one of the following collection modes:

OPTION	EXPLANATION
Live collection	Select this if you want to collect current data from your environment for reporting. The amount of data being collected can impact the amount of time required to produce report results. This is the default option for source content.
Stored data	Select this if you want to report using data previously collected and stored in the Reporter database. This method of reporting can significantly improve report performance as no live collection is taking place. Also, using stored data does not adversely impact your network.

3. Select the **Change History** check box if you want to report on any changes that may have occurred on objects since the last data

collection. You will need to select one of the following date range types:

OPTION	EXPLANATION
From To	In this date range option, the date range is based on a set window of time that you specify. **Note:** Midnight is used as a starting and ending point for the dates you select. That is, if the date range is Start Date = 07/22/2006 and End Date = 07/24/2006, this is interpreted as July 22 starting at 00:00 GMT time and ending July 23 at 23:59 GMT time. The report only displays changes that occurred within this time frame. Changes that actually occurred on July 24 are not included. This is an important distinction to keep in mind when you specify a range.
Or	In this option, the date range is based on a sliding window of time. The sliding window of time provides more current history reporting on the objects. When you specify a number of days, weeks, or months, this value is applied based on the current date and time when the report template is run. For example, if you specify five days and run the report template today at 18:00 hours, the report content is based on data in the Reporter database that was collected over the last five days. The time frame for the data in question would start from today at 18:00 hours and go back to five days ago at 18:00 hours.

4. If you do not want to do a fresh collection on linked objects, select the **Do not do linked collection (gather linked data from database)** check box.

   There may be instances when doing a linked collection is not necessary. For example, if you do a collection on groups and link in users, you may not want to collect linked users if you have just done a collection on all the Domain users.

5. Click **OK**.

Applying Filters to Attributes

With Quest Reporter, you can configure filter expressions by

- Building a group of filter expressions
- Selecting a criteria value from a list

  The values that are available are stored in the database and gathered from data previously collected.

In Novell networks, there are two special objects that can be assigned as trustees for files and folders: [Root] and [Public]. [Root] has a object type of "Top". However, [Public] object type is undefined. In order to support the use of [Public] as a filter on NWFS reports, an object type called "Built-in" has been added for [Public].

Grouping Filter Expressions

This section provides sample scenarios for using a group of filter expressions.

Example 1

You may want to generate a User Attributes report that displays all Sales Managers and Marketing Coordinators.

{Department = “Sales” AND Title = “Manager”}
OR
{Department = “Marketing” AND Title = “Coordinator”}

Example 2

You may want to generate a Computer report. You can use the following combination of expressions:

{Computer Role contains Terminal Server}
AND
{Description is null}
OR
{Build Number equals 2195}

To group filters

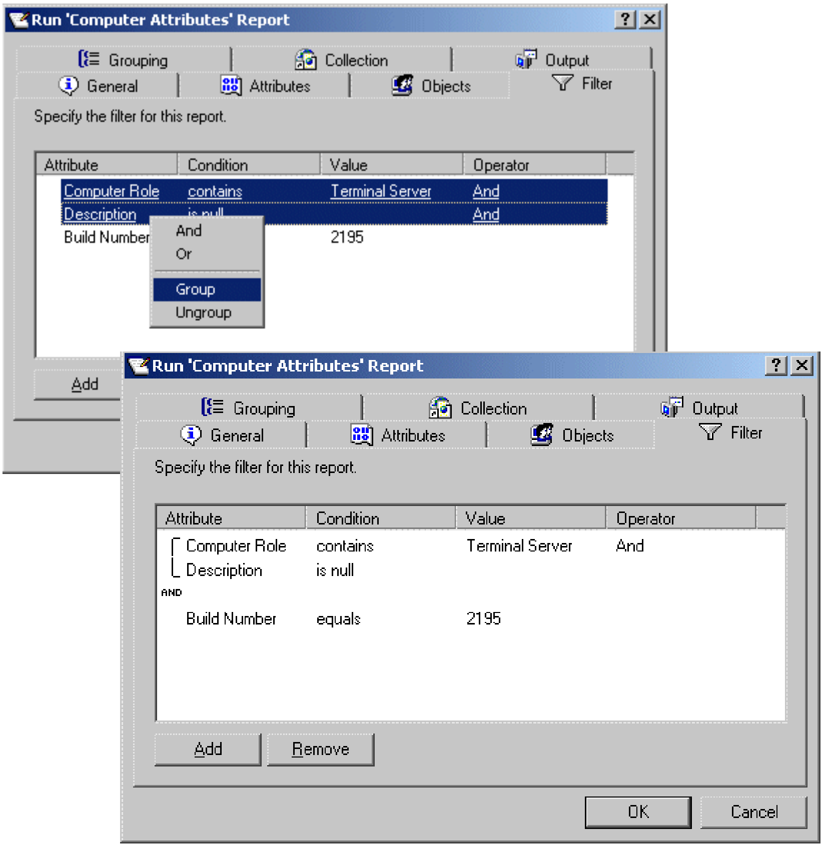
1. Select the report template that you want to run.

   This procedure uses the Computer Attributes report template as an example.

2. Click the **Filter** tab.
3. Enter the information as shown in Example 2.
4. SHIFT+SELECT the first two attributes, then right-click and select **Group**.

   In the following example, there are two conditions that are evaluated against each computer in the report. The Computer Role and Description values, and the values for the Build Number.

   The report results will display all computers with Computer Roles that contain Terminal Server with no description, or computers with the Build Number 2195.



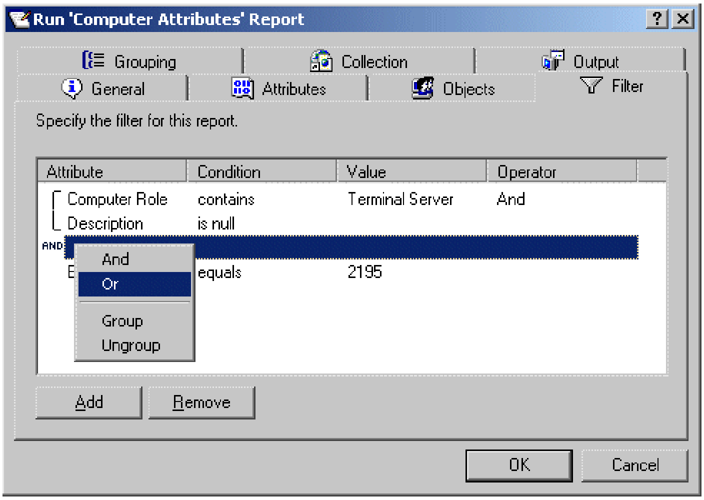
Specify the filter for this report.

Attribute	Condition	Value	Operator
Computer Role	contains	Terminal Server	And
Description	is null		And
Build Number		2195	

Specify the filter for this report.

Attribute	Condition	Value	Operator
⎡ Computer Role	contains	Terminal Server	And
⎣ Description	is null		
AND			
Build Number	equals	2195	

5. Right-click the **And** operator, then select **Or**.



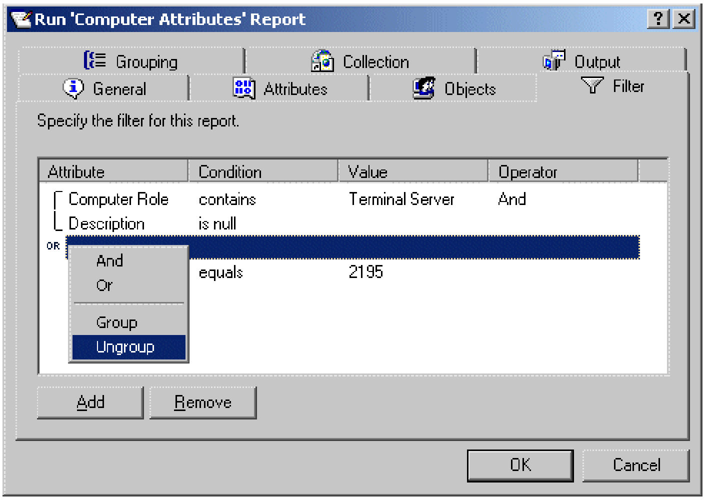
Specify the filter for this report.

Attribute	Condition	Value	Operator
Computer Role	contains	Terminal Server	And
Description	is null		
E	equals	2195	

6. Click **OK** or select another tab to change other settings.

To ungroup filters

1. Select the report template where the filters are set.
2. Click the **Filter** tab.
3. Right-click the **Or** operator and select **Ungroup**:



Specify the filter for this report.

Attribute	Condition	Value	Operator
Computer Role	contains	Terminal Server	And
Description	is null		
	equals	2195	

4. Click **OK** or select another tab to change other settings.

Using Special Characters in a Filter

When setting up a filter, you can enter the following special characters in the Value column:

CHARACTERS	DESCRIPTION
_ (underscore)	Returns any single character.
[]	Returns any single character within the specified range. For example, [a–f]. – OR – Returns any single character within the set range. For example, [abcdef].
[^]	Returns any single character not within the specified range. For example, [^a–f]. – OR – Returns any single character not within the set range. For example, [^abcdef].
%	Returns any string of zero or more characters. For example, 51 % Street returns all street names that begin with the number 51.

You can only use the special characters with the following conditions: contains, does not contain, begins with, does not begin with, ends with, and does not end with.

For more information about special characters, see “Basic Regular Expression Syntax” on page 125.

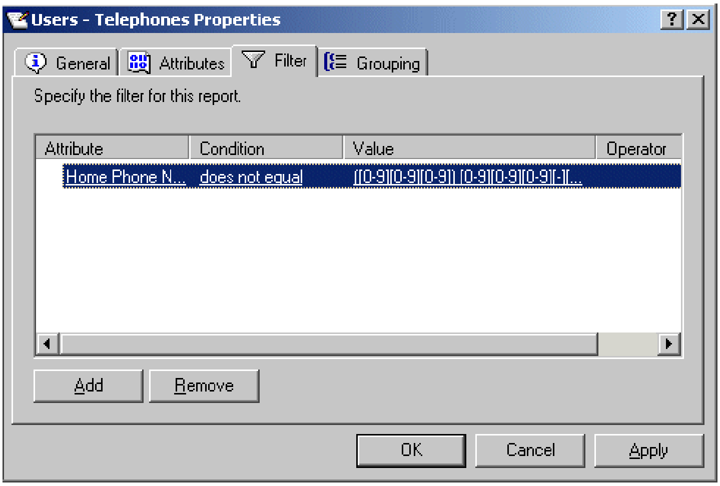
Keep in mind the following when using these conditions:

CONDITION	DESCRIPTION
ends with	Automatically adds the % character to the beginning of the filter value.
begins with	Automatically adds a % character to the end of the filter value.
contains	Automatically adds a % character to the beginning and the end of the filter value.

If you want to filter on a special character, use brackets around the character. For example, [%], [_], [[].

Example 1

To find a user's Home Telephone Number that is not in the format: (###) ###-####, apply a filter on Home Telephone Number where it does not equal: "([0-9][0-9][0-9]) [0-9][0-9][0-9][-][0-9][0-9][0-9][0-9]" as shown:

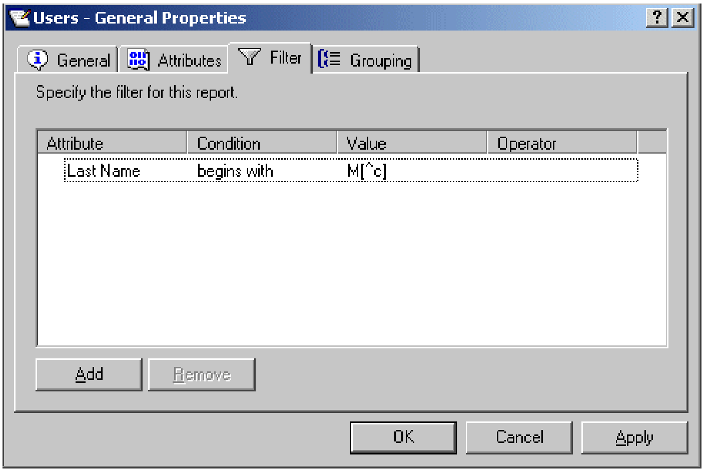


Specify the filter for this report.

Attribute	Condition	Value	Operator
Home Phone N...	does not equal	([0-9][0-9][0-9]) [0-9][0-9][0-9][-][...	

Example 2

To find all last names that begin with M and do not have c as the second letter, apply a filter on Last Name as shown: M[^c].



Specify the filter for this report.

Attribute	Condition	Value	Operator
Last Name	begins with	M[^c]	

Using the List Does Contain Partial Match Filter

The List Does Contain Partial Match filter complements the Contains filter. The List Does Contain Partial Match filter treats a multi-value attribute as a single entity—filtering applies to the entire attribute. This is different from the Contains filter which treats each value of a multi-value attribute as a separate entity.

Filter Functionality

The List Does Contain Partial Match filter returns all instances of the string value entered, even if that string occurs as part of a larger string. For example, if you enter "100" the filter returns all instances of that string and also instances that contain that string, that is, "100", "1000", "10001", "10010", "33100", and so forth.

This is also true for the List Does Not Contain Partial Match filter. All instances of the string value entered and instances containing that value will be excluded.

Supported Attributes

The List Does Contain Partial Match and the List Does Not Contain Partial Match filters are available with the following multi-valued attributes:

- Boot Entries
- Installed Software
- Role
- Trusted Domains
- Members
- Restricted To
- Global Catalogs
- GC Replicated Attributes
- Telex Number
- Other Pager
- Hot Fixes
- NIC Bindings
- Password Filters DLLs
- Trusting Domains
- Group Membership
- Protocols
- Post Office Box
- URL
- Other Telephone
- Other Mobile
- Other Mailbox
- Other IP Phone
- Other Home Phone
- Other Fax Number
- International ISD Number
- Direct Reports
- SID History
- Proxy Addresses
- Member Of
- Nested Groups

Multi-valued attributes of child object types are not supported with the List Does Contain Partial Match or the List Does Not Contain Partial Match filter.

To apply filter expressions to attributes

1. Right-click a report template, and select **Properties**.
2. Click the **Filter** tab.
3. Click **Add**.
4. Double-click the **Attributes** link.
5. Select an attribute from the list, then click **OK**.
6. Click the **Condition** link.

   The condition values in the list depend on the attribute that you select. Only parameters that pertain to the selected field appear in the list. Condition values include the following:

   - equals
   - is greater than
   - is less than
   - contains
   - does not equal
   - is greater than or equal to
   - is less than or equal to
   - does not contain

- begins with
- ends with
- is null
- list does contain partial match
- does not begin with
- does not end with
- is not null
- list does not contain partial match

7. Select a condition from the list, then click **OK**.
8. Click the **Value** link.
9. Enter a value.

   – OR –

   Click **Values** and select a value from the list.

If you are applying a filter to a date-related attribute, you can select a value that is a specific date or a date range based on a sliding window of time. The date range can be a number of days, weeks, or months. This value is applied based on the current date and time at the moment the report template is run.

For example, if you specify five days and run the report template today at 18:00 hours, the report content is based on data in the Reporter database that was collected over the last five days. The time frame for the data in question would start from today at 18:00 hours and go back to five days ago at 18:00 hours.

10. Click **Apply**, then continue to add filters as required.

    The filters that are applied to the report template are displayed on the report information page.

11. Click **OK**.

Linking Attributes

Attributes for one object type can be associated with attributes from another object type. The attributes selected as ‘link in’ appear in the report.

The attributes that can be linked in are shown as linkable on the report information page. Some examples of report templates with linkable attributes include: Global Group Membership, Group Membership, and account and owner attributes in the security report templates.

For example, when running the Global Group Membership report template, the members attribute, which displays as the user’s Distinguished Name for Active

Directory, may not be enough information. You can link in other user attributes in addition to or instead of the Distinguished Name, such as the user's Logon Name or Office attribute.

If you want to report on linked attributes in stored data, there are certain attribute dependencies you need to be aware of. For more information on linked attributes in stored data, see "Linked Attributes and Stored Data" on page 40.

To link attributes

1. Right-click a report template, then select **Properties**.
2. Click the **Attributes** tab.

   The <...> indicates that you can link that attribute to other object type attributes.
3. Select the check box for the attribute, then right-click the attribute and select **Link In**.
4. Select the check boxes for the attributes that you want in the report template, then click **OK**.

   The attributes that you selected appear in the Linked in Attributes list.

Grouping and Sorting Attributes

You can group, sort, and select the attributes that you want displayed in the report.

To group the attributes in a predefined report template

1. Right-click a report template then select **Properties**.
2. Click the **Grouping** tab.
3. Drag attributes to the Grouping list.
4. Right-click attributes and choose the sort order.

   The following example shows that the report will be grouped by the Domain attribute. The Account Disabled attribute will not be displayed in the report output.

   *The 👓 icon indicates that the attribute will appear in the report. Right-click the attribute and select **Visible** to remove the check mark and turn this feature off. You can use this feature to avoid repeating the same information throughout a report.*

   For example, if you are generating the Disabled Accounts report, you may not need to repeat in the report that each account is disabled. On the properties dialog box for the Disabled Accounts report *template, click the **Grouping** tab. Right-click the **Account Disabled** attribute and select **Visible**.*

5. Click **OK**.

Viewing and Saving Reports

You can choose to view a report on the screen or save the report to a file.

To save report output to a Microsoft® Excel file, Microsoft Excel 2000 or later must be installed.

Sorting Columns in Delimited Files

You can set the sort order for columns when the report output is in a comma delimited or tab delimited format. You can set the sort order for the following file types: .csv, .tsv, and .xls.

To choose report output options

1. Right-click a report template and select **Run Report**.
2. Click the **Output** tab.
3. Select **Screen** (default) or **File**.
4. Click **Layout** to choose the style and orientation of the report.

   The layout options apply to the following: reports displayed on the screen, .html reports, .pdf reports, and .rtf reports.

5. Enter a file name and description if you select the **File** check box.

   You can save the file to a network location or another user's computer rather than on the local computer. For example, if your manager wants to review a certain report every Monday morning, you can generate the report Sunday night and save the report to your manager's workstation.

6. If you select **File**, the following options are available:

OPTION	DESCRIPTION
File types	Select the file type: .html, .txt, .csv, .tsv, .rtf, .pdf, or .xls. If you select .html as the file type, select the check box if you want one HTML file generated for each page of the report. If you select .csv, .tsv, or .xls, click **Field Order** to set the sort order for the fields. You must set this option every time you run the report template. If there are different attributes in the report, you can only sort the object types for each attribute.
Append datestamp to file name	Select this check box to add the date that the report was generated to the end of the report name.

7. Click **OK**.

Creating Custom Report Templates

You may want to present a specific combination of content in a report that is not available in a predefined report template. Using Quest Reporter, you can create custom report templates and choose any attribute available in the Reporter database.

Custom report templates can be based on either stored or live data.

There are two ways to create custom report templates:

- Duplicate a predefined report template and save it as a custom report template
- Create an original custom report template

To create a custom report template

1. Right-click a report category, then select **New | Report**.
2. Click **Next**.
3. Enter general information about the report template.
   a) Enter a name and description.
   b) Click **Categories** to select a report category.

The new report template is then associated with the category and saved in that Category directory.

4. Click **Next**.
5. Select the type of report template and associated attributes.

   The report types in the list include: Computers, Domains, Groups, HIPAA Security Standards Compliance, Permissions, Security Auditing, SOX Compliance, Summary, Users and VAS Reporting.

6. Click **Next**.
7. Select the filters.

   Use report filters to enforce policies and standards in your organization. Customizing the filters in report templates allows you to see exceptions to your policies.

   a) Click **Add**.
   b) Click the attribute link.
   c) Select an attribute from the list, then click **OK**.
   d) Select a Condition value, then click **OK**.
   e) Click the value link, then select a value.

   For example, a user account can have one of the following values: enabled or disabled.

   f) Click **OK**.
8. Click **Next**.
9. Select the grouping and sorting options.
   a) Drag an attribute to the Grouping box.

   The generated report will be grouped on that attribute. You can select more than one attribute.

   b) To sort the report by attribute, right-click and select either **Sort Ascending** or **Sort Descending**.

   By default, the check mark is displayed next to the Visible feature to indicate that it is enabled.

   c) Right-click an attribute and select **Visible** to clear the check mark if you do not want the attribute displayed in the report.
10. Click **Next**.
11. Click **Finish** after you review the confirmation page.

    The report template is added to the category directory that you selected. To run the report template, see "Generating a Report" on page 35.

To change the properties for a predefined report template

Create a copy of the report template before changing the properties.
The default settings for the original predefined report template remain intact.

1. Right-click a report template and select **Duplicate** to create a copy of the report template.
2. Right-click the duplicate report template and select **Properties**.
3. Change the properties as required, then click **Apply**.

   You can change the following report properties: General, Attributes, Filter, and Grouping.

Importing and Exporting Report Templates

If you are an administrator working in a distributed Quest Reporter environment, you may need to share report templates with your colleagues.

To create and export a report template

1. Right-click a report template, then select **Export**.
2. Click **Next**.
3. Click **Browse** to select the directory where you want to save the report template, then click **Next**.

   The report file name format uses a .qxr extension.
4. Click **Finish**.

To import a report template

1. Right-click a report container, then select **Import**.
2. Click **Next**.
3. Click **Add**.
4. Browse to the directory where the file is located.
5. Select the file then click **Open**.

   Attributes contained in the report template that you are importing may not reside in your database. You cannot continue until the attributes are removed or the report template is removed.

   *To remove invalid attributes, right-click the report template, select **Properties**, then click **Remove**.*

You can add attributes to your database using the configuration utility. For more information, see “Adding Attributes for Customized Report Templates” on page 115.

6. Click **Next**.
7. Select the categories where you want to save the report template, then click **Next**.
8. Review the settings, then click **Finish**.

5

Using Advanced Reporting Features

- Generating a Report and Changing Network Data
- Generating an NTFS Security Report
- Using Object Sets to Organize Network Objects
- Using Favorites for Frequent Reporting

Generating a Report and Changing Network Data

Using Quest Reporter's action-enabled report templates, you can enumerate and display network data, and edit the data displayed on the screen report. You can take immediate corrective action on the objects listed in the report—the changes to the data are applied immediately. This is useful for making mass changes to attributes. For example, if you generate a list of locked user accounts, you can right-click the objects in the report and specify that they be unlocked.

Quest Reporter adheres to Windows security policies. You must be assigned the appropriate administrative rights to change object attributes.

There are predefined action scripts available with Quest Reporter that you can copy and modify, or you can create your own scripts. You can use these action scripts to modify information that would normally be changed using the Active Directory Users and Computers snap-in. Action scripts can be used to change either objects or attributes that appear in the report. For more information, see "Setting Up Scripts to Run on Action-Enabled Reports" on page 117.

Action-enabled reporting should occur regularly in order to maintain tight security controls and minimize operational impact. With it, you not only collect, store, and report on your environment, but you can also run action scripts on the results in a timely manner and on a regular basis.

Create a custom report template that you can use specifically for action-enabled reporting. For more information, see "Creating Custom Report Templates" on page 53.

Working with the Action-Enabled Report Display

You can assess the report information in an action-enabled report using

- The view that is available when the Attributes node is selected in the Action-Enabled Report dialog box.

  In the Attributes node view, you can right-click an object, select Edit, then select an attribute. You can then change the value as required.

  When the Attributes node is selected, only those with an asterix (*) in the column header for the attribute can be changed.

- The view that is available when an individual attribute is selected

If you are viewing attributes that can be changed, there are two columns displayed: <attribute name> (Collected) and <attribute name> (New). If the attribute cannot be changed, the New column is not displayed.

By default, the first attribute displayed below the Attributes node is displayed in the first column in the upper-right pane of the report display. To change the attribute displayed in this column, right-click in the column header and select another attribute.

You cannot use action-enabled reporting to modify primary groups.

To change network information interactively

1. Right-click a report template and select **Run Action Enabled Report**.
2. Select the reporting options.

   For more information on report options, see "Managing Report Template Properties" on page 39.

   After the report is generated, the Action-Enabled Report dialog box opens.
3. Expand the **Attributes** node to browse the attributes.
4. Select an attribute.
5. Right-click in the cell to view the available options for this attribute.
6. Select one of the available options.

   If you select to edit, the input method depends on the data type of the attribute. For example, if you change the expiry date attribute for an account, a Date and Time dialog box opens.
7. Click **Apply** to run the action script or to save any changes.
8. Click **Close**.

While the use of action-enabled reporting immediately changes values for objects and attributes, the changed data is not saved to the database. You must generate the report again to add the changed data to the database.

When a report is generated, a log file is created that lists all the actions which occurred during report generation. Other information, such as the version of Reporter, the user who generated the report, and the computer where the report was generated, is also included at the beginning of the log. The default folder path where these log files are located is C:\ReporterLogs. For information about changing the default path, see "Configuring Log Settings" on page 114.

Generating an NTFS Security Report

Windows NT File System (NTFS) reporting allows you to create reports to address potential security issues. Using the available NTFS security report templates, you can identify user and group access based on the associated Access Control Lists (ACLs). NTFS reporting also allows you to view the permissions assigned to network shares and directories.

You can use NTFS report templates to do the following:

- Enforce permission standards

  Many organizations have standards for data collection permissions. For example, they may define the specific ACEs (Access Control Entries) that should be contained in the ACLs on shares and folders. Ensuring that these policies are followed helps protect data integrity.

- Audit security

  Some organizations (such as financial institutions) have legal obligations concerning data security. They must control and monitor data access. The ability to detect security problems arising from data permissions is paramount. In this situation, NTFS reporting on share and directory permissions is central to daily network administration.

- Prepare for domain consolidation or Windows 2000 migration

  Consolidations and migrations are likely to involve new permissions. This lengthy process requires careful planning to determine the resources to which users have access. NTFS reports expedite this process.

To run an NTFS report template

1. Expand **Reporting | Reports | Permissions**.
2. Select **NFTS**.
3. Right-click an NTFS report template and select **Run Report**.
4. Click the **Objects** tab, then click **Add**.

   The Object Picker dialog box is displayed.
5. Expand **Windows NT | Computers**.

   – OR –

   Expand **Active Directory | Computers**.
6. Select the computer you want to report on and click **Add**.

   – OR –

a) Expand the computer you have selected and navigate to the folders, shares, or logical drives that you want to report on.

b) Select the objects you want and click **Add**.

You can select multiple objects in the upper-right pane to add a group of objects. You also can select a combination of computers, shares, folders, and logical drives.

Instead of selecting objects and creating a static object set, you can create a dynamic object set that uses query searches. For more information, see "To create an object set" on page 65.

7. To include system paths for the selected objects, click **Paths** and proceed as follows:

OPTION	EXPLANATION
Path	Select one of the following: • Common program files • Program files • System drive • Windows directory
Recurse	Select the level of subfolders to report on.
Subfolder Expression Filter	Filter the search using regular expressions. For example, you can enter ^ followed by the text you want to search on. The carrot symbol (^) is a regular expression that is interpreted as "Only look for object types with names that begin with" followed by the text to search for. For example, if you entered ^msadc, the search would return all objects of the type specified whose names begin with "msadc". For more information on regular expressions, see "Appendix B: Regular Expressions" on page 125.

8. Click **OK**.
9. If you are reporting on shares, click **Shares**.
10. Select one of the following share selection options:

OPTION	DESCRIPTION
All Shares	Searches for all shares.

OPTION	DESCRIPTION
Search	Filter the search using regular expressions. For example, you can enter ^ followed by the text you want to search on. The carrot symbol (^) is a regular expression that is interpreted as "Only look for shares that have names that begin with" followed by the text to search for. For example, if you entered ^sales, the search would return all shares whose name begins with "sales". For more information on regular expressions, see "Appendix B: Regular Expressions" on page 125.

Using regular expressions allows you to narrow the focus of the search, making it much more efficient.

11. Select one of the following share and folder reporting options, then click **OK**:

OPTION	DESCRIPTION
Retrieve Share ACL	Reports on permissions applied to the shares. This option is selected by default.
Retrieve Folder ACL	Reports on the folder permissions on each share. You can enter the level of recursion or report on all levels.
Recurse Folders	Determines the level of subfolders to report on. **Note:** This option only becomes available when the "Retrieve Folder ACL" option is selected.
Subfolder Filter	Applies a regular expression filter to the names of the subfolders of the selected path. For more information on regular expressions, see "Appendix B: Regular Expressions" on page 125.

While still in the Object Picker, you can change selected share and folder reporting options for shares you have added. Right-click the share in question and select **Options**.

12. Click **OK** to return to the Run Report dialog box.

13. Click the **Attributes** tab if you want to add, remove, or link the attributes being reported on.

    For more information, see "Linking Attributes" on page 50.

14. Click the **Filter** tab if you want to filter the data being collected.

    For more information, see "Applying Filters to Attributes" on page 43.

15. Click the **Grouping** tab if you to specify a grouping and sorting order for the report.

    For more information, see "Grouping and Sorting Attributes" on page 51.

16. Click the **Collection** tab to select collection options.

    For more information, see "Using Different Collection Modes" on page 40.

17. Click the **Output** tab to select output options.

    For more information, see "Viewing and Saving Reports" on page 52.

18. Click **OK** to generate the report.

Using Object Sets to Organize Network Objects

Object sets are a collection of objects that are of particular interest to a system adminstrator. They are created for data collection and report generation and can be used over and over. Object sets should contain objects of the same category. There are two kinds of object sets:

- Static - contains predefined objects you have selected or imported from a list
- Dynamic - leverages queries for which you have set search parameters

One advantage to using a dynamic object set is the use of queries. Any time any object meeting the search criteria you have specified is added to the network it is automatically added to the data collection.

You can use object sets to target only the network information that you want, as the focus of an object set is only on the objects defined in it. You can also create object sets to be used offline, where the reporting is done using previously collected data stored in the database.

To give you an idea of how beneficial object sets can be, consider the following scenario. Suppose you, as an administrator, are typically responsible for a specific aspect of your organization’s network. For example, Admin 1 is responsible for the Research and Development department in Chicago. This encompasses all users, groups, and computers that are part of this department.

Rather than collecting data from the entire domain that contains these objects, it is more efficient to create an object set that contains only this subset of network information.

Information gathered and reports generated against this object set only show information that is relevant to Admin 1.

This section provides information on creating online and offline objects sets, importing objects into an object set, and using object sets for report generation.

Creating Object Sets

Creating an object set allows you to focus on a subset of network objects, which optimizes data collection and returns filtered results for the reports. For example, an object set contains certain computers; when a computer report is generated, only those computers in the object set are reported on.

Object sets can reference any of the following:

- individual objects
- containers such as domains, or Active Directory organizational units (OUs)

  If the content of the containers changes, the objects are updated when the object set is selected for data collection or report generation.
- queries

  With queries, you can use regular expressions to narrow the focus of the search, for example, include all computers that have names starting with "G".

Object sets can contain objects from one or more Windows NT or Active Directory domains or IP subnets.

Use IP subnets to group computers. If you only want to report on a specific group of computers, add the IP subnet to the object set.

After you create an object set, you can configure the RDC to collect data based on this customized collection option. For more information on RDCs, see "Report Data Collectors" on page 83.

To create an object set

1. Right-click **Object Sets | New | Object Set**.
2. Click **Next**.
3. Enter a name and description for the object set, then click **Next**.
4. Click **Add.**

   The Object Picker dialog box is displayed.

   – OR –

   Click **Import** and select the file.

   For information on importing files, see "Importing Users, Groups, and Computers" on page 73.
5. Use one of the following methods to create the type of object set you want:

IF YOU WANT A	**THEN**
Static object set (predefined objects)	1. Expand **Windows NT** or **Active Directory**. 2. Navigate to the object type that you want to report on. 3. Drag one or more objects that appear in the upper-right pane to the lower pane. 4. Click **Add**. 5. Click **OK**.

IF YOU WANT A	THEN
Dynamic object set (uses search queries)	1. Click **Query**. The Find dialog box that displays allows you to define the parameters for your query. 2. Click **Find** and select an object type. 3. Click the **Advanced** tab. 4. Click **Field** and select the field to search on. 5. Click **Condition** and select the condition to apply. 6. Enter a parameter value in the Value box. This value will be used to define the query. For example, if you selected computers as the object type and entered DC1 as the value, the query would select all computers with a name that ended in DC1. 7. Click **Add**. 8. Click **Find Now** to show the query results. 9. Click **OK**. **Note:** You cannot use Query for cross forest searches.

To access an Active Directory member server, you must be a member of the local Administrators group on that computer.

6. If you want to include system paths for computers, click **Paths** and proceed as follows:

OPTION	EXPLANATION
Path	Select one of the following: • Common program files • Program files • System drive • Windows directory
Recurse	Select the level of subfolders to report on.

OPTION	EXPLANATION
Subfolder Expression Filter	Filter the search using regular expressions. For example, you can enter ^ followed by the text you want to search on. The carrot symbol (^) is a regular expression that is interpreted as "Only look for object types with names that begin with" followed by the text to search for. For example, if you entered ^msadc, the search would return all objects of the type specified whose names begin with "msadc". For more information on regular expressions, see "Appendix B: Regular Expressions" on page 125.

7. Click **OK**.
8. If you are reporting on shares, click **Shares** and select one of the following share selection options:

OPTION	DESCRIPTION
All Shares	Searches for all shares.
Search	Filter the search using regular expressions. For example, you can enter ^ followed by the text you want to search on. The carrot symbol (^) is a regular expression that is interpreted as "Only look for shares that have names that begin with" followed by the text to search for. For example, if you entered ^sales, the search would return all shares whose name begins with "sales". For more information on regular expressions, see "Appendix B: Regular Expressions" on page 125.

Using regular expressions allows you to narrow the focus of the search, making it much more efficient in terms of processing and performance.

9. Select from the following recursion options:

OPTION	DESCRIPTION
Retrieve Share ACL	Reports on permissions applied to the shares. This option is selected by default.

OPTION	DESCRIPTION
Retrieve Folder ACL	Reports on the folder permissions on each share. You can enter the level of recursion or report on all levels.
Recurse Folders	Determines the level of subfolders to report on. **Note:** This option only becomes available when the "Retrieve Folder ACL" option is selected.
Subfolder Filter	Applies a regular expression filter to the names of the subfolders of the selected path. For more information on regular expressions, see "Appendix B: Regular Expressions" on page 125.

10. Click **OK**, then click **OK** again to return to the Object Set Wizard.
11. Click **Next**, then click **Next** again.
12. Review the settings, then click **Finish**.

    The object set is displayed in the console. You can now run report templates based on this object set.

Creating Offline Object Sets

As with regular object sets, you can use offline object sets for both data collection and report generation. When online object sets are used, they must access the network to validate the objects. Offline object sets store this validation information in the Reporter database. Therefore, when offline object sets are used, there is no need to access the network for validation as this information is retrieved from the Reporter database.

If you are not connected to the network, your database must be on the same computer as the Reporter console in order to access the stored data.

For speed and bandwidth reasons, especially in larger deployments of Quest Reporter, you may want to generate reports from stored data. Once the data has been collected and stored in the Reporter database, you can generate reports using the stored data and an offline object set, thus eliminating the need to query the network for either object validation or data collection.

When you use offline object sets to report on stored data, the benefits are twofold:

- You can generate reports from a local Reporter database when disconnected from the network.
- Reports are generated much faster as the database is referenced instead of querying the network.

You can synchronize the objects in the offline object set with live network data. During the synchronization, the validation information for those objects is updated with the most recent network information.

To create an offline object set

1. Right-click **Object Sets | New | Object Set**.
2. Click **Next**.
3. Enter a name and description for the object set, then click **Next**.
4. Click **Add.**

   The Object Picker dialog box is displayed.

   – OR –

   Click **Import** and select the file.

   For information on importing files, see "Importing Users, Groups, and Computers" on page 73.
5. Use one of the following methods to create the type of object set you want:

IF YOU WANT A	THEN
Static object set (predefined objects)	1. Expand **Windows NT** or **Active Directory**. 2. Navigate to the object type that you want to report on. 3. Drag one or more objects that appear in the upper-right pane to the lower pane. 4. Click **Add**. 5. Click **OK**.

IF YOU WANT A	THEN
Dynamic object set (uses search queries)	1. Click **Query**. The Find dialog box that displays allows you to define the parameters for your query. 2. Click **Find** and select an object type. 3. Click the **Advanced** tab. 4. Click **Field** and select the field to search on. 5. Click **Condition** and select the condition to apply. 6. Enter a parameter value in the Value box. This value will be used to define the query. For example, if you selected computers as the object type and entered DC1 as the value, the query would select all computers with a name that ended in DC1. 7. Click **Add**. 8. Click **Find Now** to show the query results. 9. Click **OK**. **Note:** You cannot use Query for cross forest searches.

To access an Active Directory member server, you must be a member of the local Administrators group on that computer.

6. If you want to include system paths for computers, click **Paths** and proceed as follows:

OPTION	EXPLANATION
Path	Select one of the following: • Common program files • Program files • System drive • Windows directory
Recurse	Select the level of subfolders to report on.

OPTION	EXPLANATION
Subfolder Expression Filter	Filter the search using regular expressions. For example, you can enter ^ followed by the text you want to search on. The carrot symbol (^) is a regular expression that is interpreted as "Only look for object types with names that begin with" followed by the text to search for. For example, if you entered ^msadc, the search would return all objects of the type specified whose names begin with "msadc". For more information on regular expressions, see "Appendix B: Regular Expressions" on page 125.

7. Click **OK**.
8. If you are reporting on shares, click **Shares** and select one of the following share selection options:

OPTION	DESCRIPTION
All Shares	Searches for all shares.
Search	Filter the search using regular expressions. For example, you can enter ^ followed by the text you want to search on. The carrot symbol (^) is a regular expression that is interpreted as "Only look for shares that have names that begin with" followed by the text to search for. For example, if you entered ^sales, the search would return all shares whose name begins with "sales". For more information on regular expressions, see "Appendix B: Regular Expressions" on page 125.

Using regular expressions allows you to narrow the focus of the search, making it much more efficient in terms of processing and performance.

9. Select from the following recursion options:

OPTION	DESCRIPTION
Retrieve Share ACL	Reports on permissions applied to the shares. This option is selected by default.

OPTION	DESCRIPTION
Retrieve Folder ACL	Reports on the folder permissions on each share. You can enter the level of recursion or report on all levels.
Recurse Folders	Determines the level of subfolders to report on. **Note:** This option only becomes available when the "Retrieve Folder ACL" option is selected.
Subfolder Filter	Applies a regular expression filter to the names of the subfolders of the selected path. For more information on regular expressions, see "Appendix B: Regular Expressions" on page 125.

10. Click **OK**, then click **OK** again to return to the Object Set Wizard.
11. Click **Next**.
12. To create an offline object set, select the **Object Set is an Offline Object Set** check box.
13. Move the object types whose content you want to synchronize in the object set from the Object Types to Collect list to the Available Object Type list.
14. Select the following synchronization options as required:

SELECT...	TO...
Remove existing data before synchronizing	Clear any existing data for the objects in this object set from the database. Synchronization will result in the database being updated with current data for the objects in the object set.
Synchronize contents when finished	Synchronize the data after you complete the wizard. Existing data in the database will be updated to reflect the current status of the objects in the object set. Selecting this option allows you to report on objects that have been deleted from the database.

15. Click **Next** after you select the appropriate synchronization settings.
16. Review the settings, then click **Finish**.

    The object set is displayed in the console. You can now run report templates based on this object set.

Importing Users, Groups, and Computers

You can import users, groups, and computers into an object set.

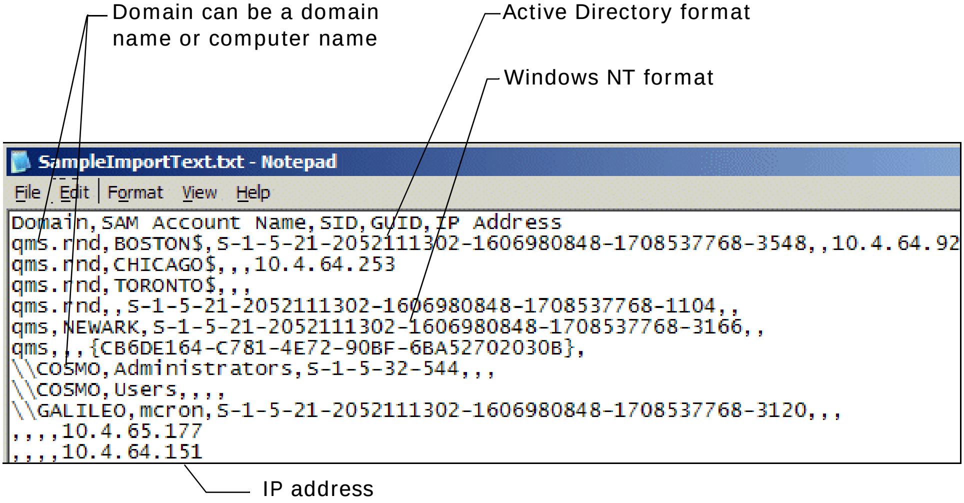
You can generate a report using Quest Reporter (or any other reporting tool), export the report results to a file, then import the information into the object set. The following file formats can be used: csv, .txt, and a comma or tab delimited text file.

There are required attributes that you need in the file to successfully import users, groups, and computers. The column header information must be provided in the text file exactly as shown in the following table. Note that some attribute combinations may take longer to retrieve than others.

OBJECT TYPES	REQUIRED COLUMN HEADERS	RETRIEVAL RATE
Active Directory object types	Domain and SAM Account Name	Slow
	– OR –	
	Domain and GUID	Fast
	– OR –	
	Domain and SID	Slow
Windows NT object types	Domain and SAM Account Name	Slow
	– OR –	
	Domain and SID	Slow
computers by IP	IP Address	Fast

In the example text file shown in Figure 7, Domain and SAM Account Name are required column headers. The data in those two columns will be imported into the object set—any other information in the text file is ignored.

The Domain name format can be provided in either Windows NT format or Active Directory format.


Domain can be a domain name or computer name
Active Directory format
Windows NT format
SampleImportText.txt - Notepad
File
Edit
Format
View
Help
IP address

```
Domain,SAM Account Name,SID,GUID,IP Address
qms.rnd,BOSTON$,S-1-5-21-2052111302-1606980848-1708537768-3548,,10.4.64.92
qms.rnd,CHICAGO$,,,10.4.64.253
qms.rnd,TORONTO$,,,
qms.rnd,,S-1-5-21-2052111302-1606980848-1708537768-1104,,
qms,NEWARK,S-1-5-21-2052111302-1606980848-1708537768-3166,,
qms,,,{CB6DE164-C781-4E72-90BF-6BA52702030B},
\\COSMO,Administrators,S-1-5-32-544,,,
\\COSMO,Users,,,,
\\GALILEO,mcron,S-1-5-21-2052111302-1606980848-1708537768-3120,,,
,,,,10.4.65.177
,,,,10.4.64.151
```

Figure 7: Sample text file information that will be imported into an object set

Using Object Sets to Generate Reports

After you create an object set that meets your requirements, you can generate a report quickly.

If you run a live report template and you select an offline object set to run the report template on, the report information will be gathered from the network and not the database.

To generate a report based on an object set

1. Right-click an object set, then select **Reporting | Run Report**.
2. Select the appropriate report template and click **OK**.

Synchronizing Content for Offline Object Sets

Before you generate a report based on an offline object set, you may want to synchronize the content between the current network data and the data stored about the objects in the object set.

The most efficient way to synchronize content is to set this option during the creation of a scheduled collection, when you are adding object sets. With this method, the process is automatically done each time the scheduled collection is run. For more information, see "To set up a scheduled collection" on page 84.

You can also immediately synchronize an offline object set by right-clicking it in the Reporter console and selecting the Synchronize option.

Synchronizing an offline object set may take some time depending on the number of objects that must be resolved.

Editing Object Set Contents

You can change the following properties in both regular and offline object sets:

- The network objects contained in the object set
- The name and description for the object set

To change the properties of an object set

1. Expand **Reporting | Objects Sets**.
2. Right-click an object set and select **Properties**.
3. Click the **General** tab to change the name or description.
4. Click the **Contents** tab to add or remove objects.

   If you change the contents for an offline object set, the existing data in the database is removed.

5. Click the **Offline Objects** tab to change the offline and synchronization options.
6. Click **OK**.

An object set maintains a separate copy of the objects it contains. If you delete an object through Administrative Tools, a copy of that object still remains in the object set. To remove the object completely, you must also remove it from the object set.

Using Favorites for Frequent Reporting

As an administrator, there may be report templates that you run on a regular basis. Quest Reporter allows you to create and display favorites grouped by organizational folders and subfolders for better organization and easier access.

Rather than having to browse through all the available report templates, you can create favorites that you can quickly use on a frequent basis.

A favorite saves the following report settings:

- Objects
- Filters and groupings
- Output options

Favorites are stored on your local drive in the following location: Program Files\Common Files\Quest Shared\Quest Management Suite\Favorites.

The values that are set in a favorite are created and saved in the report template. Once set, this information is retained for future report generation.

You can share a favorite report template with another user. Send the .inf file and have the user copy it to the Favorites folder (Program Files\Common Files\Quest Shared\Quest Management Suite\Favorites).

Using Windows Explorer, you can organize favorites by adding or deleting folders, moving favorites between folders, moving entire folder hierarchies, renaming folders and reports, sharing favorites with other users, and setting security permissions on favorites directories.

Creating and Modifying Favorites

You can create a favorite in any of the following ways:

- Save the output to screen as a favorite.
- Save a report template as a favorite.
- Copy an existing favorite and rename it.

You can modify a favorite at any time by changing its attributes and filters.

To save a generated report as a favorite

1. Run the report template you want to save as a favorite.
2. In the print preview pane, click **Save**.
3. Select **Favorite** and click **OK**.

To save a report template as a favorite

1. In the treeview of the Reporter console, expand **Reporting | Reports**.

2. Right-click **Favorites | New | Favorite**.
3. Select a report template, then click **Add**.
4. Click **OK**.

   A Properties dialog box opens for the report template you selected. For more information on report properties, see "Using Different Collection Modes" on page 40.

5. Change the report properties if required, then click **OK**.

To copy an existing favorite and rename it

1. In the treeview of the Reporter console, expand **Reporting | Reports**.
2. Right-click **Favorites** and select **Manage** to open Windows Explorer.
3. Right-click the favorite you want to copy and select **Copy**.
4. Right-click in the Explorer window and select **Paste**.
5. Right-click the copy of the report template and select **Rename**.
6. Type in the new report name.
7. Close the Explorer window.

   The new favorite should appear when you select the Favorites node in the Report console. If necessary, press F5 to refresh the view.

To modify a favorite

1. In the treeview of the Reporter console, select **Reporting | Reports | Favorites**.
2. Right-click the report template you want in the upper-right pane and select **Properties**.

   In the Properties dialog box you can change the report template name, description, and grouping, modify the options for attributes, filtering, collection, and output, and add or remove objects.

   The Attribute and Filter tabs allow you to modify favorites by adding or removing attributes, and by filtering data to meet specific criteria.

3. Select the appropriate tab and make the desired modifications.
4. Click **OK** when you have completed your modifications.

Generating Favorite Reports

All the favorites you create are contained in the Favorites folder. You run them in the same way as you would any of the predefined report templates.

To generate a favorite report

1. Expand **Reports | Favorites**.
2. Double-click the favorite you want to run.

   The report is generated in print preview mode with the report options previously specified in place.

3. Click 🖨 to print the report.

   – OR –

   Click **Close**.

There are several other output options with which to run a favorite. For more information, see “Viewing and Saving Reports” on page 52.

Scheduling Favorites

After you create your favorites, you can schedule them to run at regular intervals to give an ongoing status of key network objects.

For example, you can create the following favorites directory structure:

- Monday
- Tuesday
- Wednesday
  - Morning
  - Afternoon
- Thursday
- Friday

Add favorite report templates to these folders that are appropriate to the type of administrative work that must be done on that day. Schedule the favorite to run the night before, so that the reports are generated by the time you get in that day. The output of the favorites will show you areas that must be addressed in the network for that day.

To schedule a favorite

1. Right-click a favorite and select **Schedule**.
2. Enter account and password information, then click **Next**.

The account requires the right, Log on As Batch Job. Each time a job is created, Quest Reporter ensures the right is assigned to the account. If you are an administrator, assign the right if necessary.

3. Select the date and time that you want to run the favorite, then click **Next**.

   If you set the favorite report output type to File, then you can set up email notification. The email addresses receive a confirmation message each time a favorite runs.

   You must configure SMTP settings before you can set the email address here. For more information, see "Setting up a Server for Email Notifications" on page 123.

4. Enter email addresses, then click **Next**.

   You can also enter subject and body information in the email.

5. Review the settings, then click **Finish**.

   The scheduling information for a favorite can be viewed in the lower pane.

6

Setting up Scheduled Collections

- Overview
- Creating a Scheduled Collection
- Changing Settings for Scheduled Collections
- Removing Scheduled Collections and RDCs

Overview

Scheduled collections provide a method for collecting information on your network objects on a recurring basis. As the information is collected, it is stored to the associated database for later use. You can then generate reports from the stored data. Scheduled reporting is a good way to incorporate Quest Reporter into your ongoing Windows network auditing process.

This chapter provides information on how to schedule collections and how to manage the properties of scheduled collections.

An important part of using scheduled collections is ensuring the correct settings for your database. For more information on database setup and scheduled collections, see “Deployment Considerations for Scheduled Collections” on page 23.

Benefits of Scheduled Collections

Running a scheduled collection and a subsequent report template against the stored data can have several advantages over running the same report template live on the network:

- A report generated against stored data is faster since a live report must gather data, then store it. Therefore, you spend only a fraction of the time waiting for the report results.
- Scheduled collections can be run during periods when the network is not busy. The collection can run faster and not burden the network during regular business hours.
- Scheduled collections can take place closer to the source of information by placing a Report Data Collector (RDC) on a computer in that domain.
- Recurring scheduled collections allow you to track changes to objects over time. Any detected changes to the objects are saved in the database.
- Each scheduled collection can take place in its own security context. This provides flexibility when you need to collect data from multiple locations—it is then not necessary for a single account to have rights in all locations.

For more information on generating reports, see “Managing Report Template Properties” on page 39.

Creating a Scheduled Collection

There are two components required in setting up a scheduled collection:

- The RDC

  The RDC reads in job information, collects the required data, and stores the data to the database.

- The scheduled collections job

  The scheduled collections job contains the settings for a collection and provides the following information: the report types, the network objects to collect data on, and how often to collect data.

Report Data Collectors

The RDC ensures that the scheduled collection runs and that the network objects and information are stored to the database.

RDCs can collect information from domains (Active Directory or Windows NT 4.0) or object sets. If a domain is selected, all objects of the required type for the collection (such as users) are enumerated.

Each time that the RDC gathers information on an object, such as full name, it collects that information on all users in the selected domains. This may be time-consuming depending on the number of users in the selected domain. Use object sets to limit the number of objects from which to collect information or to collect information only on specific objects. For more information, see “Using Object Sets to Organize Network Objects” on page 63.

How Do I Deploy an RDC?

When you are creating a scheduled collection, you select the computer where you want to deploy the RDC. The RDC is then automatically copied to that selected computer.

By default, there is an RDC on the computer where Quest Reporter is installed.

After an RDC is copied to a computer, you can select this RDC when setting up additional scheduled collections. The RDC can be shared by any administrators setting up a scheduled collection. There can be only one RDC on a computer.

To set up a scheduled collection

1. Expand **Reporting**.
2. Right-click **Scheduled Collections | New | Scheduled Collection**.
3. Click **Next**.
4. Select the computer where you want to run the collection.

   The list displays only the computers with RDCs installed.

   – OR –

   Click **Add** to send the scheduled collection to another computer, then select an install location for the RDC.

   If there is an RDC installed on the computer, you cannot change the location. The installation directory box is only available if an RDC is not installed on the computer.
5. Select either **NT Authentication** or **SQL Authentication**.

   If you choose SQL Authentication, enter a SQL user name and password.

   If you choose NT Authentication, the account provides the security credentials for collecting the data and storing the data to your database. The user name and password are entered in step 14.
6. Click **Next**.
7. Select **Direct to Database** and click **Next**.

   – OR –

   Select **Compressed Data** and click **Next**.
8. If you selected Compressed Data, enter the credentials that are required to run the services and click **Next**.

   This account requires the right Log on as a service. This right is assigned automatically to the account if it is not already assigned.
9. Enter a name and description for the collection, then click **Next**.
10. Select the report templates to include, then click **Next**.

There may be instances when doing a linked collection is not necessary. For example, if you do a collection on groups and link in users, you may not want to collect linked users if you have just done a collection on all the Domain users.
If you do not want to do a fresh collection on linked objects, select the **Do not do linked collection (gather linked data from database)** check box.

11. Select the object sets on which the scheduled collection will run and drag them to the lower pane.
12. If you want to ensure the object sets are current, right-click each one and select **Synchronize while reporting**.

This step will configure the offline object set to be synchronized each time a scheduled or live collection occurs. Offline object sets should be synchronized with the environment to ensure the contents are accurate.

13. Click **Next**.
14. Enter a Windows NT account user name and password, then click **Next**.

    The credentials provided here are used to run the report template. This account is also used if you selected NT authentication for the database connections in step 5.

    For more information on logon credentials, see “Logon Credentials” on page 23.

15. Set the scheduling information on when you want the collection to run, then click **Next**.
16. Select the **Send confirmation email after scheduled collection completes** check box, then enter email addresses.

    You can also enter subject and body information in the email. The email addresses receive a confirmation message each time a scheduled collection is completed.

    You must configure SMTP settings before you can set the email address here. For more information, see “Setting up a Server for Email Notifications” on page 123.

17. Click **Next**.
18. Review the settings, then click **Finish**.

    The scheduled collection is created and will run with the selected RDC.

Changing Settings for Scheduled Collections

After you set up a scheduled collection, you can:

- View scheduled collections on an RDC
- Edit scheduled collection properties

To view scheduled collections on an RDC

1. Expand **Reporting | Scheduled Collections**.
2. Select a computer where an RDC is installed.

   The scheduled collections assigned to the RDC are displayed in the upper-right pane.

To edit scheduled collection properties

1. Expand **Reporting | Scheduled Collections**.
2. Select a computer where an RDC is installed.
3. In the upper-right pane, right-click the scheduled collection and select **Properties**.
4. Click the following tabs to change properties:

TAB	DESCRIPTION
General Collection Information	Change the name or description.
Report Selection	Change the report types.
Object Selection	Change the objects on which you collect information.
Computer Selection	Change the authentication method to your database.
Data Transport Mode	Change the transport mode.

5. Click **Apply**.
6. Click **Close**.

Removing Scheduled Collections and RDCs

You can remove scheduled collections and RDCs from the Quest Reporter console.

Scheduled collections displayed on your console may have been created by other administrators.

When you delete scheduled collections or RDCs, they are permanently removed from the system.

Before you delete an RDC, ensure there are no collections running. If collections are running, then certain files will not be deleted.

If you are using Compressed Data Transport mode note the following:

- The services required to use this mode will be deleted.
- Microsoft Message Queuing (MSMQ) queues will not be deleted. You need to manually delete the queues using Microsoft native tools.

To delete a scheduled collection

1. Expand **Reporting | Scheduled Collections**.
2. Select a computer where there is an RDC installed.
3. In the upper-right pane, right-click a scheduled collection and select **Delete**.
4. Click **Yes**.

To remove a RDC

1. Expand **Reporting | Scheduled Collections**.
2. Select an RDC and remove all scheduled collections in the upper-right pane.

   You can only remove an RDC after the scheduled collections are deleted.

3. Right-click an RDC and select **Delete**.
4. Click **Yes**.

   A dialog box might be displayed that indicates that some files were not deleted on a remote RDC computer. You must delete these files manually if you want to deploy an RDC to that computer in the future.

   If you do not delete the files, then any future RDC deployments to that computer will fail.

7

Vintela Authentication Services Reporting

- Overview
- Guidelines for Using VAS Reporting
- VAS Reporting Using Stored Data
- VAS Reporting Using Live Data

Overview

Vintela Authentication Services (VAS), now part of Quest Software, provides organizations with enterprise-wide access, authentication, and authorization for Unix and Linux systems from the identity management infrastructure already in place for Windows Active Directory. With VAS, Unix and Linux systems natively and seamlessly become full members of Active Directory - joined to the Active Directory domain, functionally extending Active Directory's security, compliance, and authentication capabilities to Unix and Linux.

Quest Reporter provides VAS reporting capabilities using VAS Report templates from the following report categories:

- Group Personalities
- UNIX enabled Groups
- UNIX enabled Users
- UNIX Hosts
- Personality Containers
- User Personalities

There is also another report category called Collection templates. You use these templates to collect data that the VAS Report templates require for both stored data reporting and live data reporting.

For stored data reporting, use the Collection templates for scheduled collections. The data is collected and stored in the Reporter database, and you can generate VAS reports without querying your live network again and again. This can significantly improve performance, and is the recommended workflow in large enterprises.

Guidelines for Using VAS Reporting

With VAS reporting, there are two ways to generate reports:

- Using stored data from scheduled collections
- Using live data collection

VAS Reporting Using Stored Data

For optimal performance in a large network environment, the recommended Best Practice is to use the following workflow:

- Create scheduled collections by leveraging the templates found under the Collection Templates node.
- Once the Reporter database has been populated by the scheduled collections, run the VAS Report templates.

  By default, the VAS Report templates are set to run as stored data reports, that is, using data previously collected and stored in the Reporter database.

VAS Reporting Using Live Data

An alternate method of VAS reporting is to run the VAS Report templates using live data. There may be instances where you need to report against live data, for example, to assess the current status of a small scope, or to address an immediate concern.

With this workflow, you would simply run the VAS Report templates as live reports.

If you plan to run VAS Report templates against live data, create favorites. You can access favorites quickly, and easily modify them to suit your purposes. For more information, see "Using Favorites for Frequent Reporting" on page 75.

VAS Reporting Using Stored Data

With VAS reporting using stored data, the data must first be collected by means of the logical relation that Active Directory has with the Unix and Linux systems. Once the data has accumulated in Reporter's SQL Server database, it is then used when running any of the VAS Report templates.

The workflow for this method of VAS reporting can be summarized as follows:

- Collect and store data for VAS reporting

  Create scheduled collections using the Collection templates. For more information, see "Collecting and Storing Data for VAS Reporting" on page 92.

- Create VAS favorites

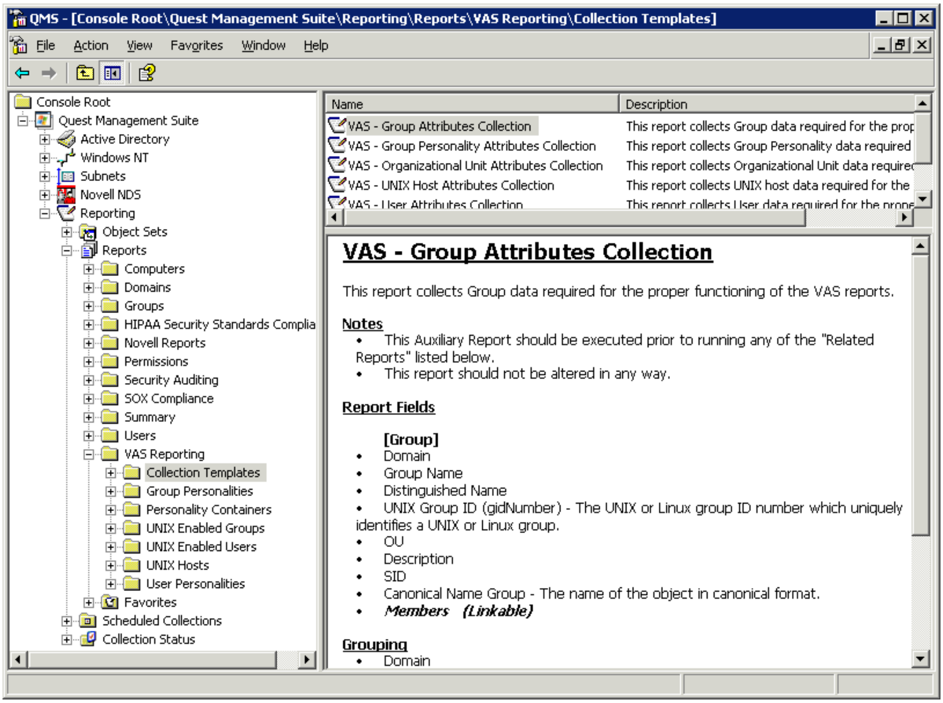
  You can save any of the predefined VAS Report templates as a favorite. For more information on favorites, see “Creating and Modifying Favorites” on page 76.

- Schedule your VAS favorites to generate reports

  For more information on scheduling favorites, see “Scheduling Favorites” on page 78.

Collecting and Storing Data for VAS Reporting

The VAS Reporting node includes the Collection templates, a group of predefined templates that you can use for the scheduled collections.



Name	Description
VAS - Group Attributes Collection	This report collects Group data required for the prop
VAS - Group Personality Attributes Collection	This report collects Group Personality data required
VAS - Organizational Unit Attributes Collection	This report collects Organizational Unit data require
VAS - UNIX Host Attributes Collection	This report collects UNIX host data required for the
VAS - User Attributes Collection	This report collects User data required for the prope

VAS - Group Attributes Collection

This report collects Group data required for the proper functioning of the VAS reports.

Notes
- This Auxiliary Report should be executed prior to running any of the "Related Reports" listed below.
- This report should not be altered in any way.

Report Fields

[Group]
- Domain
- Group Name
- Distinguished Name
- UNIX Group ID (gidNumber) - The UNIX or Linux group ID number which uniquely identifies a UNIX or Linux group.
- OU
- Description
- SID
- Canonical Name Group - The name of the object in canonical format.
- ***Members (Linkable)***

Grouping
- Domain

Unless you need to run the VAS Report templates against live data, you must schedule the Collection templates to run regularly. This will ensure that the database is populated with the information needed for the successful generation of the VAS Reports. In most instances, weekly intervals will suffice. However, it is recommended that you evaluate your organization's particular situation and schedule the Collection templates accordingly.

To set up a scheduled collection

1. Expand **Reporting**.
2. Right-click **Scheduled Collections** and select **New | Scheduled Collection**.
3. Click **Next**.
4. Select the computer where you want to run the collection.

   The list displays only the computers with RDCs installed.

   – OR –

   Click **Add** to send the scheduled collection to another computer, then select an install location for the RDC.

   If there is an RDC installed on the computer, you cannot change the location. The installation directory box is only available if an RDC is not installed on the computer.
5. Select either **NT Authentication** or **SQL Authentication**.

   If you choose NT Authentication, the account provides the security credentials for collecting the data and storing the data to your database. The user name and password are entered in step 15.

   If you choose SQL Authentication, enter a SQL user name and password.
6. Click **Next**.
7. Select **Direct to Database** and click **Next**.

   – OR –

   Select **Compressed Data** and click **Next**.

   For more information on data transport modes, see "Data Transport Modes" on page 16.
8. If you selected Compressed Data, enter the credentials that are required to run the services and click **Next**.

   This account requires the right Log on as a service. This right is assigned automatically to the account if it is not already assigned.
9. Enter a name and description for the collection, then click **Next**.
10. Select **Browse by Report Category** and navigate to the Collection Templates subfolder.

11. Select the Collection templates to include for collection, then click **Next**.

There may be instances when doing a linked collection is not necessary. For example, if you do a collection on groups and decide to also link in users, you may not need to collect linked users if you have just done a collection on all the Domain users.
If you do not want to do a fresh collection on linked objects, select the **Do not do linked collection (gather linked data from database)** check box.

12. Click **Add**.

    The Object Picker dialog box is displayed.

13. Select the object sets or objects on which the scheduled collection will run, drag them to the lower pane, then click **OK**.

User Personality and Group Personality objects cannot be imported into object sets. For more information on using object sets, see “Using Object Sets to Organize Network Objects” on page 63.

14. Click **Next**.
15. Enter a Windows NT account user name and password, then click **Next**.

    The credentials provided here are used to run the report template. This account is also used if you selected NT Authentication for the database connections in step 5.

    For more information on logon credentials, see “Logon Credentials” on page 23.

16. Set the scheduling information on when you want the collection to run, then click **Next**.
17. Select the **Send confirmation email after scheduled collection completes** check box then enter email addresses.

    You can also enter subject and body information in the email. The email addresses receive a confirmation message each time a scheduled collection is completed.

    You must configure SMTP settings before you can set the email addresses. For more information, see “Setting up a Server for Email Notifications” on page 123.

18. Click **Next**.
19. Review the settings, then click **Finish**.

    The scheduled collection is created and will run with the selected RDC.

VAS Reporting Using Live Data

You can also do VAS reporting using live data, in the event that you need to immediately assess a specific need or address an issue.

The workflow for this method of VAS reporting is fairly straightforward; you select the VAS main report template you want and run it.

Collection Template Dependencies

The following VAS reports require certain information from specific Collection templates:

REPORT	COLLECTION TEMPLATE
VAS - User with Personality Information	• VAS - User Attributes Collection • VAS - User Personality Attributes Collection
VAS - Group with Personality Information	• VAS - Group Attributes Collection • VAS - Group Personality Attributes Collection
VAS - UNIX Group ID Conflict Information	• VAS - Group Attributes Collection
VAS - UNIX User ID Conflict Information	• VAS - User Attributes Collection
VAS - UNIX Host Access Summary	• VAS - User Attributes Collection • VAS - User Personality Attributes Collection • VAS - Group Attributes Collection • VAS - Group Personality Attributes Collection • VAS - UNIX Host Attributes Collection • VAS - Organizational Unit Attributes Collection
VAS - Associated Personalities	• VAS - User Personality Attributes Collection • VAS - Group Personality Attributes Collection • VAS - UNIX Host Attributes Collection • VAS - Organizational Unit Attributes Collection
VAS - Associated UNIX Enabled Users and Groups	• VAS - User Attributes Collection • VAS - Group Attributes Collection • VAS - UNIX Host Attributes Collection • VAS - Organizational Unit Attributes Collection

REPORT	COLLECTION TEMPLATE
VAS - Associated UNIX Hosts	• VAS - UNIX Host Attributes Collection • VAS - Organizational Unit Attributes Collection

Before running these report templates against live data, you must run the associated Collection templates to ensure the information contained in these VAS reports is accurate.

To generate a VAS report

1. Double-click one of the VAS Report templates.

   – OR –

   Right-click one of the VAS Report templates and select **Run Report**.

   The Objects, Collection, and Output tabs are displayed by default. You can configure the tabs that will be displayed. For more information, see “Configuring the Tabs in the Report Dialog Box” on page 109.
2. Click the **Objects** tab and select the objects to report on.
3. *Use **Query** to set search parameters for the objects you are reporting on. Quest Reporter finds the most current information at the time the report is generated. For more information on using queries, see “To create an object set” on page 65.*

User Personality and Group Personality objects cannot be imported into object sets. For more information on using object sets, see “Using Object Sets to Organize Network Objects” on page 63.

4. To select the level of recursion for an OU container, right-click the container, then select **Options**.
5. Select the level of recursion, then click **OK**.
6. Click the **Collection** tab and select **Live collection** as the source of content.

7. Select from the following options:

OPTION	EXPLANATION
Change History	Select this if you want to compare stored data with the most recent data. You can track changes on information that is already in the database with information retrieved during a live collection. If you select Change History, you need to enter the date range information.
From To	In this date range option, the date range is based on a set window of time that you specify. **Note:** Midnight is used as a starting and ending point for the dates you select. That is, if the date range is Start Date = 07/22/2006 and End Date = 07/24/2006, this is interpreted as July 22 starting at 00:00 GMT time and ending July 23 at 23:59 GMT time. The report only displays changes that occurred within this time frame. Changes that actually occurred on July 24 are not included. This is an important distinction to keep in mind when you specify a range.
Or	In this option, the date range is based on a sliding window of time. The sliding window of time provides more current history reporting on the objects. When you specify a number of days, weeks, or months, this value is applied based on the current date and time when the report template is run. For example, if you specify five days and run the report template today at 18:00 hours, the report content is based on data in the Reporter database that was collected over the last five days. The time frame for the data in question would start from today at 18:00 hours and go back to five days ago at 18:00 hours.
Use linked data from the database	Select this option if you do not want to do a fresh collection on linked objects. There may be instances when a fresh linked collection is not necessary. For example, if you do a collection on groups and decide to also link in users, you may not need to collect linked users if you have just done a collection on all the Domain users.

8. Click the **Output** tab and proceed as follows:

OPTION	EXPLANATION
Screen	Select this option if you want the report results to be displayed once the report has been generated. This is the default output option.
File	Select this option if you want to save the report results to a file. If you select File, select a file type, browse to the folder where you want to save the report, and enter a file name for the report.
Append datestamp to file name	Select this option if you want to add the date to the end of the file name.
One file per page of report	Select this option if you selected HTML as the file type and you want one HTML file generated for each page of the report.
Layout	Click this button to select the style and orientation of the printed report.

9. Click **OK**.

   These values are not saved; you must set them every time you want to run a predefined report template. If you want to save the settings, you can save the report template as a favorite. For more information, see "Using Favorites for Frequent Reporting" on page 75.

For information on using more advanced report features and managing report properties, see "Managing Report Template Properties" on page 39.

8

Working with the Compressed Data Transport Mode

- Overview
- Installing Compressed Data Transport Mode
- Managing the Services
- Managing the Repository
- Managing the MSMQ Queues

Overview

As described earlier in the Deployment section of this guide, the compressed data transport mode can be used rather than the standard direct to database transport mode.

This chapter provides information on the settings that you will work with when configuring compressed data transport mode.

Installing Compressed Data Transport Mode

You may have chosen to only install the direct transport mode when you initially installed Reporter. You can change the mode to compressed at any time using the Configuration utility. To set up the compressed data transport mode you need to:

- Provide an account to run services that are required when you use compressed data transport
- If required, install MSMQ on RDC hosts and on the Console host

If you decide to use compressed data transport mode then queues are created through MSMQ. To view and manage these queues, you can use Microsoft native tools.

If you want to use the compressed data transport mode, then MSMQ must be installed on the RDC host and the Console host.

Installing to a Windows 2000 Computer

Before you start the installation, ensure that the Windows 2000 CD and related Service Pack versions are accessible from a computer—either on CD or through a network path. You need to provide the location of these files during the installation.

To install compressed data transport mode

1. To install on the Console host, select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.

   – OR –

   To install on an RDC host, expand **Scheduled Collections**, right-click an RDC host, then select **Configuration**.
2. Click **Compressed Data Mode**.
3. Click **Install**.
4. Click **Next**.
5. Enter the credentials that will run the services.

   This account requires the right Log on as a service. This right is assigned automatically to the account if it is not already assigned.
6. Click **Next** to start the installation.

   If you are installing on Windows 2000 and MSMQ is not detected, then a dialog box opens that allows you to install it.
7. Enter a valid path for the Windows 2000 installation files, and enter a valid path for the Service Pack files, then click **Next**.
8. Click **Finish**.

Managing the Services

You can use the Configuration utility that ships with Quest Reporter to start or stop the services that run if you are using the compressed data transport mode.

For more information on the services that support the compressed data transport mode, see “Using Compressed Data Transport Mode” on page 17.

If you are changing the location for the services log file, you need to stop the services.

To start or stop the services

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.
2. Click **Compressed Data Mode**.
3. Click **Start** or **Stop**.

Changing the Service Account

To change the account that runs compressed data transport mode services

1. To change the account on the Console host, select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.

   – OR –

   To change the account on an RDC host, expand **Scheduled Collections**, right-click an RDC host, then select **Configuration**.
2. Click **Compressed Data Mode**.

   The RDC host requires either a local system account or a domain account that is a member of the local Administrators group. For the domain account, use the format domain\user name.
3. Enter the account name and password, then click **Change Credentials**.

   The services are automatically restarted.

Managing the Repository

A repository is created on the Console host and RDC host when you use the compressed data transport mode. Using the Configuration utility you can

- Clean the repository
- Copy the repository to a designated location
- Retrieve information about the size and number of files and folders in the repository

It is recommended that there be minimal manual intervention with the repository in production environments.

You should only use this feature in your test environment.

To manage the repository

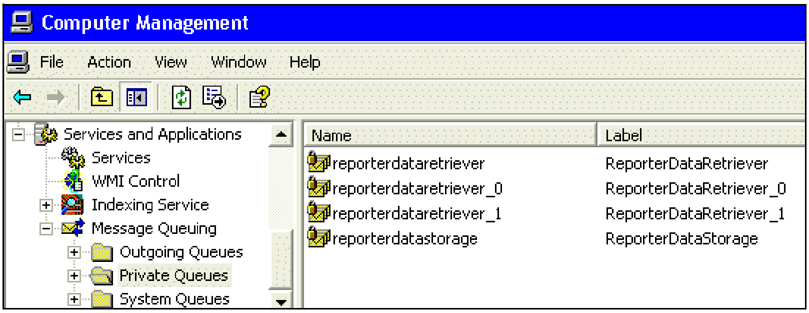
1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.
2. Click the **Repository Configuration** tab.

3. Select from the following options:

OPTION	DESCRIPTION
Purge	Cleans the repository.
Copy to	Copies the repository to the selected location for a backup copy. The original repository remains unchanged.
Get info	Retrieves the repository information including: the size of the repository, and the number of files and folders.

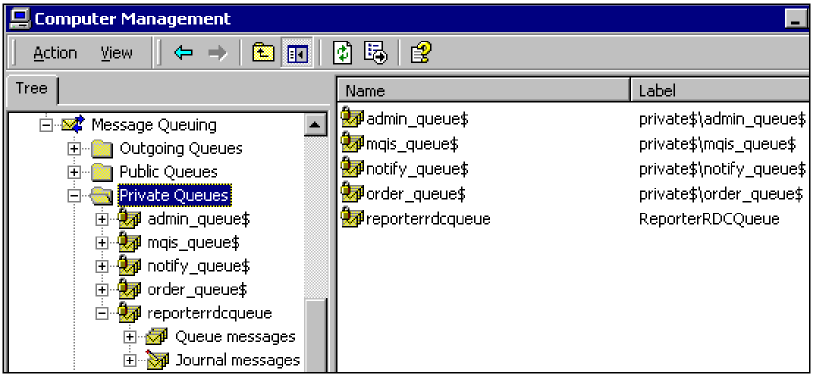
Managing the MSMQ Queues

The compressed data transport mode uses MSMQ. You can use Microsoft native tools to manage the MSMQ queues that are created by Quest Reporter.



Name	Label
reporterdataretriever	ReporterDataRetriever
reporterdataretriever_0	ReporterDataRetriever_0
reporterdataretriever_1	ReporterDataRetriever_1
reporterdatastorage	ReporterDataStorage

Figure 8: Message Queues on the Console Host



Name	Label
admin_queue$	private$\admin_queue$
mqis_queue$	private$\mqis_queue$
notify_queue$	private$\notify_queue$
order_queue$	private$\order_queue$
reporterrdcqueue	ReporterRDCQueue

Figure 9: Message Queues on the RDC Host

9

Database Cleanup Utility

- Overview
- Running Database Cleanup

Overview

The Database Cleanup utility is a wizard-based tool that allows you to remove data from your Reporter database. Depending on your particular usage requirements, you may have data that is no longer relevant. Its important to keep the size of your database in mind especially if you are upgrading your version of Reporter.

To identify what database Reporter is currently accessing, right-click the Reports subnode and select **Properties**.

There are predefined tasks available that are based on the Change History feature. If you are tracking changes in object information, then using the wizard, you can delete the information that is stored in the track changes tables.

Running Database Cleanup

Using the utility, you can

- Create a task that includes the information that you want to remove
- Run the task
- Change the properties for the task including name, activity, and filters

To create and run a task using the Database Cleanup utility

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Database Cleanup**.
2. Right-click on the Database Management dialog box, then select **New | Maintenance Task**.
3. Click **Next**.
4. Type a name and description for the task then click **Next**.

   A list of predefined activities is included with the wizard. For example, you can choose to delete all the change history data associated with computer object reports that you have generated.

5. Select a task from the list then click **Next**.
6. Select the filters then click **Next**.

   Selecting a filter allows you to set the time frame on the data that you want deleted.

7. Click **Finish**.
8. Right-click the task then select **Run**.

You can change the settings for the task at any time. Right-click the task then select ***Properties****.*

Appendix A: Configuration Settings

This appendix provides information on configuration settings for Quest Reporter.

Configuring the Tabs in the Report Dialog Box

By default, the Run Report dialog box displays the following tabs: Objects, Collection, and Output. You can configure the dialog box so that it displays any or all of the following tabs: General, Attributes, Filter, and Grouping.

To configure the tabs in the Report Wizard

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.
2. Click the **Report Wizard** tab.
3. Select the check boxes for the tabs that you want to display.
4. Click **OK**.

   The next time you run a report template, the tabs you have selected appear on the Report Wizard dialog box.

When you review the properties page for a report template, only the following tabs are displayed: General, Attributes, Filter, and Grouping. The tabs on the report properties page are not configurable.

Managing the Data Collection Mode

As described earlier, you can generate content for reports using either live collection or stored data modes of operation. When running a report template, the collection mode is displayed on the Collection tab of the Report Wizard.

There may be cases where one mode or the other is used more frequently. In this case, you can configure a default collection mode.

In other cases, you may want only one option displayed. For example, an administrator who has set up scheduled collections to build up the contents of Quest Reporter's SQL Server database may decide that their users can only run report templates from stored data.

Using the Configure utility you can predefine the following:

- The mode of data collection that is available on the Collection tab
- The default collection mode (if both modes are available)

To restrict users from running live report templates on the network, ensure the following:

- The user is a member in the Stored Report Generator role. For more information, see “SQL Server Roles” on page 21.
- The default collection mode is set to Stored.
- The **Allow Stored** check box is selected and the **Allow Live** check box is cleared.

To set the default collection mode

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.
2. Click the **Report Wizard** tab.
3. In the Content Source area, select the default mode from the list: Live or Stored.

   If you have users assigned to the SQL Server role, Stored Report Generator, select the default collection mode as Stored. This prevents those users from running live data reports.

4. Select one or both of the following check boxes:

OPTION	DESCRIPTION
Allow Live	When selected, allows users logged on to the local computer to run live report templates on the network.

OPTION	DESCRIPTION
Allow Stored	When selected, allows users on the local computer to run report templates on data stored in the Quest Reporter database.

5. Click **OK**.

Selecting Domain Controllers

You can choose the domain controllers (DCs) to collect the information for reports. You can select DCs for both Windows NT and Active Directory.

Windows NT Domain Controllers

On some Windows NT 4.0 networks, collecting Security Accounts Manager (SAM) information from the domain’s Primary Domain Controller (PDC) may not be suited to all situations. For example, if the PDC is situated on the other side of a slow link (WAN or LAN), collecting SAM information can be time-consuming.

In Windows NT 4.0 environments, you can use a local DC as the source for data collection to improve the speed of data collection as well as network browsing.

Active Directory Domain Controllers

The Windows 2000 architecture does not require the Quest Reporter data collection to focus on a local DC, as the operating system takes care of this. When possible, Quest Reporter queries the Global Catalog to obtain basic information to improve performance.

You can preset a DC to use for data collection. When set, the speed of the data collection can increase.

For example, your organization might have offices in New York, Seattle, and Boston, with computers from all sites located in the same domain and connected across a WAN. If a DC is not preset, Active Directory returns the first available DC in your network, regardless of its distance across the WAN or its speed. This can cause delays and reduce the speed of the data collection.

To select a DC

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.
2. Click the **Reporter Collections** tab.
3. Click **Add**.
4. Select a domain from the Domain list.
5. Select a DC from the Domain Controller list.
6. Click **OK**.

Selecting DCs for Last Logon Attribute Queries

You can use this feature to determine the number of DCs that will be queried. This can reduce the time to gather the information. This setting is particularly useful if you are gathering the following Last Logon attribute values:
Last Logon Time and Last Logon Server.

Information for each DC is collected on a thread.

To select a DC

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.
2. Click the **Active Directory Last Logon** tab.
3. Select the number of threads for each DC.
4. Click **Modify** to set the DCs that you want to query.
5. Select the check box if you want to use an Active Directory search.

   This option is recommended if you want to search a large number of objects.

   If you do not select DCs here, then the list of DCs enumerated is the same as the DCs selected on the Reporter Collections tab.

Setting Ping Times

During computer data collection, Quest Reporter pings (TCP/IP) each computer before attempting to connect to it for data collection. Some networks are slower than others, so the acceptable ping return times will vary. To increase the speed of data collection, Quest Reporter does not attempt to collect information from computers that fail to respond within the configured number of ping attempts.

Setting a ping time allows Quest Reporter to take into account possible network latency or computers being inaccessible.

Consider the following when setting ping times:

- Ping automatically times out if the computer does not respond within 30 seconds (30,000 milliseconds). Setting this value higher than 30,000 has no effect.
- When the ping time is set to 0, Quest Reporter tries to connect to computers that are not available. This can increase the collection time.

To set the ping time

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.
2. Click the **Reporter Collections** tab.
3. Enter a ping time.

   This number depends on your network and how many computers you want to risk skipping.
4. Click **OK**.

Setting the Number of Threads

A thread is an operating system object that represents a path of code execution within a particular application. Every 32-bit Windows application has at least one thread, but applications often create other threads to perform other tasks.

With only one thread, a program must stop all execution when waiting for a slow process to finish. Quest Reporter’s multithreaded collection engine manages several simultaneous paths of execution during a data collection. With multiple threads, data collection continues while one thread waits for the results of the slow process.

You can change the thread variable based on the hardware configuration of the computer where Quest Reporter and any Report Data Collectors (RDCs) are installed. The more powerful the computer, the higher you can increase the setting (up to a maximum of eight threads). This means that Quest Reporter collects information on multiple objects or computers simultaneously.

When configuring the number of threads to use for data collection, consider the amount of network bandwidth that data collection might use. If you plan to collect data when the network is busy, you might want to use fewer threads than you might select during a network’s quiet hours.

Setting the number of threads allows Quest Reporter to take into account possible network latency.

To set the number of threads for the collection

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.
2. Click the **Reporter Collections** tab.
3. Select the number of threads to use for data collection.
4. Click **OK**.

Configuring Log Settings

Logging records all actions and errors in Quest Reporter to help you determine their location and probable cause.

You can set logging for the services and collections used with the Compressed Data Transport mode. You do not need to restart the services after you set logging options for them.

Use the Debug check box for services and collections in a test environment only. Selecting the Debug check box for either Services or Collections logging quickly generates extremely large log files (possibly gigabytes).

The information in Quest Reporter's logs is intended for troubleshooting in cooperation with Quest Support. Support might direct you to change the log settings to provide you with more information about a problem. The default settings are acceptable in normal operating conditions.

To configure log settings

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.
2. Click the **Logging Options** tab.
3. Select the check boxes for the types of events that you want to log.

   If you are changing the location for the log files, you need to stop the services first. Click the ***Compressed Data Mode*** *tab and click* ***Stop****.*

4. Enter a location for the log file including the directory path.

By default, the root file name for the service logs includes the name of the service (not ReporterLog_).

If you are setting the log directory to a remote RDC, you must share the target folder in order for the Configure utility to recognize it. Then, when resetting the log directory in the Logging Options tab of the Configure utility, click **Browse** and select **My Network Places** to navigate to the target folder.

5. To set a maximum file size, select the check box and a size.
6. Select whether you want to create a new log file or overwrite the existing log when the maximum file size is reached.
7. Click **OK**.

Adding Attributes for Customized Report Templates

You can add Active Directory attributes and Windows attributes to the Quest Reporter database and then report on these attributes.

The attributes you add are available for all report templates.

Adding Active Directory Attributes

Using the configuration tool, you can

- View Active Directory attributes available for users, groups, and computers
- Add attributes to the database and include them in your report templates

For example, if you extend your Active Directory schema for the user object to store the Social Security Number attribute, you can include this attribute in custom report templates by adding it using the configuration tool.

Quest Reporter does not support the following Active Directory attribute types: ObjectSecurityDescriptor, OID, OctetString, DNWithBinary

To add Active Directory attributes

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.

2. Click the **Extend Reporter Attributes** tab.
3. Click **Add** to select Active Directory attributes.
4. Select an object type from the Type list.
5. Select the check boxes for the attributes that you want to make available in the report templates.
6. Click **OK**.

   The newly added attributes are only available for custom report templates. You need to add them only once to make them available for reporting.

   The attributes cannot be removed after they are added.
7. Click **OK**.

Adding Registry Attributes

Using Quest Reporter you can collect the following Registry information:

- Registry values

  For example, you can browse to HKLM\Software\Microsoft\Windows NT\CurrentVersion and gather the value ProductName.
- List of subkeys

  For example, you can browse to HKLM\Software\Microsoft and gather the list of subkeys under that key.

You can add multi-valued registry attributes. However, there is no data returned when you generate a report template on these attributes.

To add registry attributes

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.
2. Click the **Extend Reporter Attributes** tab.
3. Click **Add** to add registry attributes, then click **Next**.
4. Enter a name and description for the attribute, then click **Next**.
5. Select a collection type from the following:

OPTION	DESCRIPTION
Get a single value from a key	For every computer, a single value for a single key is collected.

OPTION	DESCRIPTION
Get a value from all sibling keys	For a given value, a single value from all sibling subkeys is collected.
Enumerate subkeys	For a given root key, the names of all subkeys are collected.
Enumerate All Values For a Given Key	For a given key, the names and values of each key are collected.

6. Click **Next**.
7. Select the registry entries, then click **Next**.
8. Click **Finish**.

   If you are collecting a Registry value, you can include the selected key only or all the siblings of the selected key.

   You can report on this information by creating a computer-based report template.

Setting Up Scripts to Run on Action-Enabled Reports

Using Quest Reporter, you can run object and attribute action scripts on data collected in action-enabled reports.

Quest Reporter includes a number of predefined action scripts. These scripts are already associated with the seven different categories of object types: users, groups, computers, domains, OUs, User Personalities (VAS), and Group Personalities (VAS). Using the Configure utility, you can add scripts to objects and/or attributes, or copy the predefined scripts and use them as a basis to create your own action scripts.

When using action-enabled scripts, you must consider whether you want to perform the action against the object itself or modify an attribute of that object. Keep in mind the following differences:

- An action-enabled script associated to an object performs an action against the object itself like move, delete, reset password, and so forth.

- An action-enabled script associated to an attribute is specifically targeted against an object's attribute such as modifying the home directory or enabling/disabling the user account.

You cannot use action-enabled reporting to modify primary groups.

Using the Configure utility, you can

- Review the attributes and associated action scripts
- Add, remove, and modify action scripts

To create an action script

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.
2. Click the **Action Enabled** tab.
3. Select an object type from the Category list.
4. Select either **Object Scripts** or **Attribute Scripts**.
5. Right-click in the Script pane and select **Add**.
6. Select from one of the following methods:

TO	DO THIS
Create a new script	1. Select **New Script**. A default script template displays in an editing window. 2. Modify the script content as needed. 3. Click **OK**. **Note:** This new script will be associated with the object type you have selected in step 4.

TO	DO THIS
Use an existing script as the basis for a new script	1. Select **Pre-existing Script**. 2. Select a script from the list that appears. 3. Right-click the script you added and select **Modify**. 4. Select all of the script and press **CTRL+C** to copy. 5. Click **Cancel** to close the editing window. 6. Right-click in the Scripts window and select **Add | New Script**. 7. Select all of the script in the editing window and press **CTRL+V** to replace it with the script you copied. 8. Locate the line that starts with "displayname" and replace "displayname" with the script name you want. 9. Change the script as required. 10.Click **OK.**

7. Click **OK** to exit the Configure utility.

   – OR –

   Click **Apply** to save the new script and continue.

To modify an action script

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.
2. Click the **Action Enabled** tab.
3. Select an object type from the Category list.
4. Select either **Object Scripts** or **Attribute Scripts**.
5. Select a script from the list.
6. Right-click the script in the Script pane and select **Modify**.
7. Change the script as required and click **OK**.

If you modify a script that is associated with more than one attribute/object (for example, AD MultiPurpose), the changes you make appear in all instances of that script. It is recommended that you create a copy of the script which you can then modify.

To remove an action script

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.
2. Click the **Action Enabled** tab.

3. Select an object type from the Category list.
4. Select either **Object Scripts** or **Attribute Scripts**.
5. Select a script from the list.
6. Right-click **Remove** and select one of the following:

OPTION	DESCRIPTION
Remove From This Attribute	The script no longer runs against the selected attribute.
Remove From All Attributes and Delete	The script no longer runs against any of the attributes with which it is associated, and is deleted from the scripts directory.

7. Click **OK**.

Selecting Report Logos

You can change the default report logos for the cover page and also add a logo to subsequent report pages.

To change the logo

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.
2. Click the **Report Logos** tab.
3. In the Cover Page area, type in the file name and path of the graphic you want to use.

   – OR –

   Click **Change** to find the graphic.
4. In the Page Header area, type in the file name and path of the graphic you want to use.

   – OR –

   Click **Change** to find the graphic.

To fit properly in the logo frame, the image size of the graphic should be approximately 224px wide x 50px high, or 0.52 inches high x 2.33 inches wide.

5. Click **OK**.
6. Click **OK** to close the Configure utility.

Setting Collection Status Features

When you run scheduled collections or live report templates, you can track the status of the report collection. The information is saved in a status file. The status file provides the following information on the collection status for every computer:

- Success
- Success with errors
- Failures

Using the Configure utility, you can:

- Set the directory path for the status file.

  Use this feature if you want all status files from all computers to reside in a central location.

- Set the maximum number of lines to display from the status file.

  Depending on your network reports, the status file can be large. Use this feature to avoid displaying all the information in the listview.

To set the options for the collection status file

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.
2. Click the **Status** tab.
3. Type the directory location.

   – OR –

   Click **Browse** to search for the directory.
4. Set the number of lines you want to display in the listview.
5. Click **OK**.

Deploying Collectors for NULL Password Report Templates

Identifying accounts with blank passwords is an important way to keep your Windows network secure.

Quest Reporter provides two report templates for identifying such accounts:

- Users with NULL Passwords

  The data collection process attempts to log on to the network with each user account using a blank password. In some environments, this could have unintended consequences such as account lockouts.

- Users with NULL Passwords (Agent)

  The data collection uses an agent installed on the DC to search for accounts with blank passwords. The agent need only be installed on one DC per accounts domain in your environment. The data collector queries the security services located on the DC.

You can deploy collectors to Windows 2000 DCs or later.

Rights Required to Run the Agent-Based Report Template

The account that runs the data collection must be a member of the Administrators group on the DC.

To deploy an agent

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.
2. Click the **Null Password Collector** tab.
3. Click **Add**.
4. Select the domain and the DC where you want to deploy the collector.

   The deployment copies several files to the DC and registers a new DLL.

5. Click **Deploy**.

Once the deployment is complete, you can run the "Users with NULL Passwords (Agent)" report template in live collection mode or include the report template as part of a scheduled collection.

For more information, see “Generating a Report” on page 35 or “Creating a Scheduled Collection” on page 83.

Setting up a Server for Email Notifications

When you are setting up a scheduled collection, you can choose to send email notifications to indicate that scheduled collections have run successfully.

You first need to set up your SMTP server using the Configure utility.

To set up SMTP

1. Select **Start | Programs | Quest Software | Quest Management Suite | Reporter | Configure**.
2. Click **SMTP**.
3. Enter the SMTP server name and port number.

   The default port number is 25.
4. Enter the email address that will be used to act as the sender.
5. Enter the logon authentication to the email server.
6. If you want to test your settings, enter a recipient email address, then click **Test**.

   Optionally, you can enter the following information to test your email settings: subject and body information, and attachments.
7. Click **OK**.

   For more information about creating a scheduled collection, see “To set up a scheduled collection” on page 84.

Appendix B: Regular Expressions

This appendix provides information on regular expressions that you can use to set search parameters when running NTFS report templates.

Basic Regular Expression Syntax

A regular expression consists of a specified set of strings that are used for matching criteria during searches.

Regular expressions can contain both special and ordinary characters. Most ordinary characters, like "A", "a", or "0", are the simplest regular expressions; they match themselves. You can concatenate ordinary characters, so last matches the string 'last'.

The following table provides a list of regular expressions:

OPERATOR	DESCRIPTION
.	Use as a placeholder for any character. Examples: "use." matches "user", "used", "uses"
*	Zero or more instances of the previous character exist in sequence. Examples: "do.*" matches "dog", "done" since "d-o- followed by zero or more of any character". "to*" matches "to" and "too" since "t-o- followed by zero or more o’s". "fre*.." matches "frat", "free", "from" since "f-r- followed by zero or more e’s followed by any two characters".
+	One or more of the previous characters. At least one of the previous characters must be in sequence. Similar to * but more strict. Examples: "fre+.." matches "freeze", "fresh" since "f-r- followed by one or more e’s followed by any two characters".

OPERATOR	DESCRIPTION
?	Zero or one of the previous characters but not more than one. This is stricter than either (*) or (+). Examples: "ton?e" matches "toe" and "tone" since "t-o- followed by zero or one n followed by e".
?!	Negative look-ahead operator. Use as part of a construct, typically with positive look ahead. Example: "(?!dmin\$)" searches forward from current position in the sequence of characters to match "dmin$"; if found, this is a negative match and "dmin$" is exempted as a match.
?<!	Negative look-behind operator. Use as part of a construct, typically with negative look behind. Example: "(?<!c)" searches backward from current position in the sequence of characters to match "c"; if found, this is a negative match and "c" is exempted as a match.
()	Group expressions. Use to logically combine two or more patterns. Example: (cat|dog) matches "cat" and "dog".
[]	Use as a placeholder for a single character which matches any of a set of characters. Examples: "ta[pb]" matches "tap" and "tab" since "t-a- followed by one character from the set of pb". "r[aeiou]t" matches "rat", "ret", "rot", "rut" since "r- followed by one character from the set of vowels followed by t". "r[aeiou]+t" matches "rat" (plus all of the above), "riot", "root" since "r- followed by one or more vowels followed by t".

OPERATOR	DESCRIPTION
[^]	Any character not in the set. This regular expression negates the set—the character must match any character not within the set. This is a useful way of specifying a large set of characters, for instance, consonants are "not vowels". Examples: "t[^aeiou]+.*s" matches "thanks", "this" since "t- followed by one or more of any character which is not a vowel followed by zero or more of any character followed by an s".
^	Beginning of data string.
$	End of data string.
\	Escape special characters. Use to match regular expressions like * or ?. Examples: "John\.Smith" matches "John.Smith" since "John" followed by a period followed by "Smith".

To show the use of expressions, consider a couple of real-world scenarios.

Example 1 - Specific Search with Inclusions and Single Exclusion

In this example, the administrator wanted to include shares that started with A through F including lowercase characters while excluding the admin$ share from the search.

The syntax for this set of expressions is as follows:

```
^[a-fA-F](?!dmin\$)[ \w\$]*
```

The first expression in this set, "^[a-fA-F]", starts the search at the beginning of the data string and searches for shares that start with "a", "b", "c", "d", "e", "f", "A", "B", "C", "D", "E", or "F". The next expression, "(?!dmin\$)", looks for the admin share to be excluded since the "!" character represents a negative match. The final expression, "[\w\$]*", continues the entire process until the end of line is reached, or the end of the string is reached, or a white space or word is encountered.

The syntax details are as follows:

EXPRESSION	DESCRIPTION
^[a-fA-F]	Look for any character in the set a-f or A-F

EXPRESSION	DESCRIPTION
(?!dmin\$)	Positive look ahead and match "dmin$"; if found, negative match
[\w\$]*	Zero or more matches until end of line, or $, or white space, or words

Example 2 - Specific Search with Inclusions and Multiple Exclusions

This example is very similar to the first example, but includes an additional exclusion. In this example, the administrator wanted to include shares that started with A through F including lowercase characters while excluding the admin$ and C$ share from the search.

The syntax for this set of expressions is:

```
^[a-fA-F](?!dmin\$)(?<!c)[ \w\$]*
```

The first expression in this set, "^[a-fA-F]", starts the search at the beginning of the data string and searches for shares that start with "a", "b", "c", "d", "e", "f", "A", "B", "C", "D", "E", or "F". The next expression, "(?!dmin\$)", looks for the admin share to be excluded since the"!" character represents a negative match. The third expression, "(?<!c)", searches backward from the current location in the string for any share starting with "c" and excludes it. The final expression, "[\w\$]*", continues the entire process until the end of line is reached, or the end of the string is reached, or a white space or word is encountered.

The syntax details are as follows:

EXPRESSION	DESCRIPTION
^[a-fA-F]	Look for any character in the set a-f or A-F
(?!dmin\$)	Positive look ahead and match "dmin$"; if found, negative match
(?<!c)	Negative look behind and match "c"; if found, negative match
[\w\$]*	Zero or more matches until end of line, or $, or white space, or words

This example uses specific exclusion, in that within the matches found, it then checks for and excludes shares starting with "c". Additional exemptions must each be specified with their own expression, for example, adding "(?<!B)" to this set of expressions would also exclude any share starting with B.

Glossary

A

ACE

Access Control Entry

An object such as a user or group that is present on an Access Control List.

ACL

Access Control List

A table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file.

Active Directory

The Windows 2000/2003 directory service.

Administrative rights

The rights granted to a member of the Administrators local group. This member can perform such actions as creating user accounts, creating groups, and adding group members.

Authentication

The process required to log on locally to a computer. Authentication requires a valid user name and password that exists in the local accounts database. An access token is created if the information provided matches the account in the database.

B

BDC

Backup Domain Controller

A Windows NT server that receives a copy of the domain’s directory database.

C

Child object

An object that is the immediate subordinate of another object in a hierarchy. A child object can have only one immediate superior or parent object.

Compressed Data Transport mode

One of two types of data storage modes used by Quest Reporter. This mode collects and compresses the data on the Reporter Data Collector (RDC) host. The compressed data pack is then streamed to the Console host, decompressed and uploaded to the database. Compressed data transport is available only with remote scheduled collections and is only leveraged during computer based collections. See also Direct Data Transport mode.

Connected domains

Domains managed by Reporter and instantiated within the Reporter user interface.

Container object

An object that can logically contain other objects. For example, a folder is a container object.

D

Data Collection

The phase of the reporting process where data is gathered from the network.

Data Storage

The phase during which collected data is stored in the database. Two modes of data storage are available: direct and compressed.

DC

Domain Controller

A server that authenticates domain logon passwords and maintains security policy and the security accounts master database for a domain.

Direct Data Transport mode

One of two types of data storage modes used by Quest Reporter. In this mode, collected data is stored directly to the database. See also Compressed Data Transport mode.

DN

Distinguished name

The fully qualified name of an object in a hierarchical system. Distinguished names are used for all Active Directory objects and in the Domain Name System (DNS). No two objects in these systems should have the same distinguished name.

DNS

Domain Name System

A hierarchical naming system used for locating domain names on the Internet and private TCP/IP networks.

Domain

In relation to a Microsoft network, a logical collection of resources consisting of computers, printers, computer accounts, user accounts, and other related objects. The domain also has a system of logon authentication of user accounts, and computer accounts.

Domain Component

A domain component is used in distinguished names (DNs) to indicate an identifier for a part of an object's network domain. For example, /O=Internet/DC=COM/DC=Fabrikam/CN=Users/CN=Jeff Smith contains the domain components COM and Fabrikam.

Domain Local Group

A domain local group can be used on access-control lists (ACLs) only in its own domain. A domain local group can contain users and global groups from any domain in the forest, universal groups, and other domain local groups in its own domain.

Domain Naming Master

The domain controller that has the domain naming master role is the only domain controller that can add new domains to the forest, remove existing domains from the forest, and add or remove cross-reference objects to external directories.

F

Favorite

A user-configured, ready-to-run version of a report template which already includes scope (selected objects) and output options for the report. Because they already contain the scope and output options, favorites require no user input and can be executed interactively or by the task scheduler.

File system

The file system data source is used to extract configuration information from remote server file systems. When defining data items, the Quest Reporter administrator must identify the file, and the polling characteristics that include: Size, Version, Presence, Access Date, Create Date, or Modify Date.

Forest

One or more domain trees that do not form a contiguous namespace, but share a common schema, configuration, and global catalog.

G

Global Group

A global group can appear on access control lists (ACLs) anywhere in the forest. A global group can contain users and other global groups from its own domain.

GUID

Global Unique Identifier

An unchangeable 128-bit number that uniquely identifies an object. It works in conjunction with SIDs to identify Active Directory objects.

L

LAN

Local Area Network

A group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area.

LDAP

Lightweight Directory Access Protocol

A protocol used for querying and modifying information stored within directory services. The Active Directory can be queried and modified through the use of LDAP-compatible tools.

Live report

A reporting process during which content for the desired report is collected from the original source (for example, Active Directory or NTFS permissions) when the report template is launched. The user generating the report must have appropriate rights on the original source to run a report template in this fashion. By contrast, see Stored data report.

Load Balancing

The fine-tuning of a computer system, network or disk subsystem in order to more evenly distribute the data or processing across available resources.

Local Group

An entity that provides access to resources and rights to perform system tasks. A local group remains strictly local to the computer where it is created and does not appear in the directory.

M

Member Server

A computer that runs Windows 2000 Server but is not a domain controller of a Windows 2000 domain. Member servers participate in a domain, but do not store a copy of the directory database.

Mixed Mode

Windows 2000 domains are installed in mixed mode, by default. In mixed mode, the domain may have Windows NT 4.0 backup DCs present. Nested groups are not supported in mixed mode.

MSDE 2000

Microsoft SQL Server 2000 Desktop Engine

MSMQ

Microsoft Message Queuing

N

Naming Context

A naming context (also called a directory partition) is a contiguous Active Directory subtree that is replicated on one or more Windows 2000 DCs in a forest.

Native Mode

A Windows 2000 domain is in native mode when all DCs in the domain have been upgraded to Windows 2000 and an administrator has enabled native mode operation.

NIC

Network Interface Card

A network adapter that plugs into both the client and server and controls the exchange of data between them. The NIC object represents a grouping of information related to network interface cards. This grouping allows one server to have one or more network interface cards.

Node

In a network, a node is a connection point, either a redistribution point or an end point for data transmissions.

Notification

Email notification can be enabled or disabled for data collection activities. When notification is enabled, an email is sent once the data collection is complete.

NTFS

Windows NT File System

The system that the Windows NT operating system uses for storing and retrieving files on a hard disk.

O

Object

A Windows NT entity. Examples include users, groups, and computers. Access rights to objects include create, read, edit, and delete.

Object Category

Different category types representing different object types such as users, groups, computers, NTFS, domains, and so on.

Object Class

Within Reporter, object classes represent the different object types for which Reporter collects data, such as users, groups, computers, NTFS, domains, and so on. Each report template defined in Reporter is associated with one and only one object class.

Object Set

A collection of objects that can be reused for purposes of data collection and report generation.

Offline Object Set

An object set that has been configured for offline purposes. The objects are enumerated and the necessary information is stored in the database. Report generation against stored data is much faster as the database is referenced instead of querying the live network in order to enumerate the appropriate objects. As well, this allows the generation of stored reports when disconnected from the network.

OU

Organizational Unit

A container object used to organize the Active Directory objects logically within a domain.

P

Parent Domain

For DNS and Active Directory, domains that are located in the namespace tree directly above other derivative domain names (child domains).

Parent Object

The object that is the immediate superior of another object in a hierarchy. A parent object can have multiple subordinate or child objects.

PDC

Primary Domain Controller

The first controller created in a domain. It contains the primary storehouse for domain data.

Permission

A rule associated with an object to regulate access to a particular object on the network. For example, a user may have read and write access to a file on the network.

Property

An attribute of a Windows NT network object. Examples include a user's password, groups to which a user belongs, and a group's description.

R

RDC

Report Data Collector

A collection engine component deployed to a workstation in proximity to the DCs, servers, and workstations that you want to collect data from.

Registry

A hierarchical database in Windows NT and Windows 2000 that contains configuration information about applications, users, and devices.

Report template

A predefined template containing an object category and corresponding attributes that is presented in a meaningful fashion. A report template requires a scope in order to be executed. Quest Reporter ships with over 180 unique report templates.

Reporter console

The main installation of Quest Reporter, including the MMC console and all the components necessary for the collecting, storing and scheduling mechanisms. This is the interface where you browse your network, manage object properties, schedule data collections and launch reports.

Reporter Data Collector (RDC)

A group of deployable components that allow execution of scheduled collections on a remote computer.

Report generation

The phase during which a report output is generated.

Root directory

The top-level directory on a computer, a partition, or volume.

S

Scheduled collection

A scheduled process that performs the data collection process by leveraging report templates against the appropriate object scope. This process places the data in the Reporter database for later use, and no report output is generated. See also Stored data report.

Schedule Favorite

A scheduled process that allows the execution of a favorite.

Schema

In Windows 2000, this describes the definition of the Active Directory database, including all classes of objects, their mandatory and optional attributes, and the data types used for storing.

Server

A computer in a network shared by multiple users.

Shares

Folders that can be accessed through the network from a computer.

SID

Security Identifier

In Windows NT and Windows 2000 operating systems, the SID is a unique alphanumeric character string that identifies each security principal (domain, user, group, computer). SIDs are used by the Windows operating system to represent these objects in resource permissions and other applications requiring reliable security authentication.

SMTP

Simple Mail Transfer Protocol

The standard email protocol on the Internet for sending email messages between servers.

Stored data report

A reporting process during which only the scope of the report is effectively enumerated from the network. The content itself is extracted from previously collected information existing in the Reporter database. By contrast, see Live report.

Subnet

A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix.

T

Thread

A unit of execution that shares its memory space with other threads. Threads can be implemented within processes on some systems or may be used in place of processes in others (for instance, in Windows NT).

Tree

A set of Active Directory domains that share a common namespace and are connected by a transitive two-way trust.

W

WAN	Wide Area Network A communications network connecting geographically separated computers, printers, and other devices.
WINS	Windows Internet Name Service A software service that dynamically maps IP addresses to computer names (NetBIOS names). Users can access resources by name instead of using IP addresses that are difficult to recognize and remember.
WMI	Windows Management Instrumentation Microsoft technology used to extend the Desktop Management Task Force Web-Based Enterprise Management initiative by representing physical and logical objects in a consistent and unified manner.

INDEX