Quest ActiveRoles Server

What's New

Version 6.0

QUEST SOFTWARE®

Quest ActiveRoles Server – What's New
Updated – September 14, 2006
Software version – 6.0

CONTENTS

ABOUT QUEST SOFTWARE, INC.

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

E-mail:	info@quest.com
Mail:	Quest Software, Inc. World Headquarters 5 Polaris Way Aliso Viejo, CA 92656 USA
Web site:	www.quest.com

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 support.quest.com

From SupportLink, you can do the following:

- Quickly find thousands of solutions (Knowledgebase articles and documents).
- Download patches and upgrades.
- Seek help from a Support engineer.
- Log and update your 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: support.quest.com/pdfs/Global Support Guide.pdf

WHAT'S NEW IN ACTIVEROLES SERVER 6.0

This new release of ActiveRoles Server considerably enhances and extends the capabilities of the product, which now include extended provisioning and deprovisioning capabilities, approval workflow for administrative operations, automated creation and population of groups and distribution lists, and re-designed Web client. The major new features of ActiveRoles Server 6.0 are as follows:

- **AutoProvision Policies.** Existing policies enhanced and new policies added, to automate provisioning tasks, including population and validation of directory data, creation of resources such as home folders and mailboxes, and provision of user access to resources.
- **Deprovision Policies.** The deprovision function along with new policies added, to automate user management tasks such as removal of user accounts, mailboxes and home folders, and updating security and distribution lists in order to revoke user access to resources.
- **Group Family.** By providing a new, rule-based mechanism for creating and populating collections of security and distribution groups, ActiveRoles Server automates, secures, and ensures accuracy of group membership lists, eliminating error-prone manual tasks.
- **Approval Workflow.** Complements automated rules, to make provisioning and deprovisioning decisions based on human input. Adds to process automation the ability to accept or deny operation requests and to monitor the execution of requests.
- **Web Interface Re-designed.** The Web Interface now has a brand-new, fresh look and feel, and is easier to navigate and customize.
- **Support for Microsoft SQL Server 2005.** ActiveRoles Server takes advantage of high availability, increased performance, improved security, and other mission-critical capabilities enabled by this new technology from Microsoft.
- **Improved Scalability.** Multiple Administration Services with the same configuration are easier to deploy, the use of the SQL Server replication function no longer required to synchronize configurations.
- **Support for Exchange Resource Forest.** Automates the provisioning and synchronization processes involved with the resource forest model—a deployment scenario where a single Exchange organization serves multiple forests.
- **Roles for AD Service Management.** Microsoft-recommended roles for delegating Active Directory service management can now be implemented by using built-in permission templates.

The following sections elaborate on each of these new features.

For information about other new features and improvements, and how to start working with new features, refer to *Feature Guide for ActiveRoles Server 6.0*.

AutoProvision Policies

Existing policies have been enhanced and new policies have been added to the AutoProvision category allowing a wide variety of provisioning rules to be implemented, including population and validation of directory data, creation of resources such as home folders and mailboxes, and provision of user access to resources.

To automate provisioning tasks, ActiveRoles Server now allows configuration and application of polices summarized in the following sections.

User Logon Name Generation (New)

These policies automate the generation and assignment of the user logon name (pre-Windows 2000) upon creation or modification of user accounts, with flexible options to ensure uniqueness of the generated name. A policy can be configured to:

- Add a uniqueness number to the generated logon name
- Apply multiple rules to generate a logon name
- Allow a logon name to be specified manually during the user creation process

Multiple rules can be defined so that the policy applies them successively, attempting to generate a unique name in the event of a naming conflict. A rule can also be configured to include an incremental numeric value to ensure uniqueness of the generated name. There is also the option to allow generated names to be modified by operators who create or update user accounts.

E-mail Alias Generation (New)

These policies automate the generation and assignment of the e-mail alias upon creation or modification of user accounts, to provision user mailboxes on Microsoft Exchange Server. A policy can be configured to generate the alias based on:

- Pre-selected user properties, such as the first and last names
- Custom selection of properties, not limited to user properties

Pre-defined rules can be used to generate the e-mail alias, or custom rules can be configured. Custom rules allow the addition of an incremental numeric value, to ensure uniqueness of the alias. It is also possible to specify whether

the alias can be modified by the operator who creates or updates the user account.

Exchange Mailbox AutoProvisioning (New)

These policies automate the selection of a mailbox store upon creation of user accounts, to provision user mailboxes on Microsoft Exchange Server. A policy can be configured to:

- Determine a single store, or a set of stores, in which creation of mailboxes is allowed
- Apply a rule to distribute mailboxes among multiple stores

It is possible to specify the Exchange servers and mailbox stores where mailbox creation is allowed, and define rules to distribute mailboxes among multiple stores either by using the round-robin method or by automatically selecting a store with the least number of mailboxes.

Group Membership AutoProvisioning (Inherited)

These policies replace those of the **'Member Of' Rules** category, available with earlier versions of ActiveRoles Server. By automating maintenance of group memberships, these policies ensure that directory objects, such as user accounts, belong to appropriate groups. A policy can be configured to:

- Add directory objects to certain groups
- Remove directory objects from certain groups

It is possible to define a list of groups and conditions so that a user account is automatically added to, or removed from, those groups depending on whether the properties of the user account meet the policy conditions. ActiveRoles Server automatically checks users against conditions, and adds or removes users from the specified groups based on the check results. These policies can also be applied to directory objects other than user accounts.

Home Folder AutoProvisioning (Inherited)

These policies replace those of the **User Home Folders and Home Shares** category, available with earlier versions of ActiveRoles Server. The policies of this category automate provisioning actions needed to assign home folders and home shares to user accounts. A policy can be configured to:

- Create home folders for newly created user accounts
- Rename home folders upon renaming of user accounts

It is possible to specify a server on which to create home folders and shares, set up naming conventions for home folders and shares, and define the user

access rights to the newly created home folders and shares. Deprovisioning functions, such as deletion of home folders, are now moved to the new policy category, **Home Folder Deprovisioning**.

Property Generation and Validation (Inherited)

These policies replace those of the **Property Validation and Generation** category, available with earlier versions of ActiveRoles Server. The policies of this category are used to generate default property values when creating new directory objects, such as users or groups, and check whether property values conform to corporate standards when creating or modifying directory objects. A policy can be configured to:

- Populate directory with default data
- Perform data validity check upon directory updates

The policy configuration specifies how to generate directory data by default and what validation criteria must be applied to ensure compliance of directory data with standards in place. For any object property, it is possible to specify criteria that the property values must meet, and define rules on what value must be assigned to the property by default. For example, a policy can be configured to check formatting of telephone numbers in the directory.

Script Execution (Inherited)

The **Script Execution** policy category is now split between the AutoProvision and Deprovision branches. These policies can be used to run supplementary scripts upon requests to perform provisioning operations, such as the creation or updating of user accounts. Scripts can be used to:

- Trigger additional actions to automate user provisioning
- Regulate data format and requirements
- Combine individual administrative tasks into a batch

A script can be associated with a provision operation so that the policy runs it when the operation is requested or after the operation is completed.

Deprovision Policies

ActiveRoles Server now provides the ability to *deprovision* rather than delete or only disable user accounts. Deprovision refers to a set of actions being performed in order to revoke user access to resources. The deprovision command on user objects triggers deprovision policies. ActiveRoles Server comes with a default policy to automate some commonly-used deprovisioning tasks, and allows the deprovision policies to be adjusted as needed.

The ActiveRoles Server user interfaces, both MMC and Web, provide the **Deprovision** command on user accounts. This command originates a request to deprovision the selected users. When processing the request, ActiveRoles Server performs all operations prescribed by the deprovision policies.

To tailor the deprovision process, ActiveRoles Server allows configuration and application of polices summarized in the following sections.

User Account Deprovisioning (New)

These policies automate the following deprovisioning-related tasks on user accounts:

- Disable the user account
- Set the user's password and logon names to random values
- Rename the user account
- Modify other properties of the user account

A policy of this category specifies how to modify the user's account in Active Directory upon a request to deprovision a user so that once the deprovision operation is completed, the deprovisioned user cannot log on to the network.

A policy can also be configured to update any user properties, such as those that regulate users' membership in ActiveRoles Server's Managed Units and Dynamic Groups. In this way, the policy can automate the addition or removal of deprovisioned users from Dynamic Groups and Managed Units.

Group Membership Removal (New)

These policies automate the removal of deprovisioned users from groups. A policy can be configured to remove user accounts from all groups with optional exceptions. Individual policy rules can be applied to security groups and to mail-enabled groups of both the security and distribution type.

Policies of this category determine what changes are to be made to group memberships of deprovisioned users. By removing users from security groups, the policy revokes user access to resources. By removing users from mail-enabled groups, the policy prevents erroneous situations where e-mail is sent to deprovisioned mailboxes.

User Account Relocation (New)

These policies are used to automatically move deprovisioned user accounts to specified organizational units. This operation removes such accounts from the control of the administrators responsible for management of the organizational units in which those accounts originally reside

A policy can also be configured not to move user accounts. When applied at a certain level of the directory hierarchy, such a policy overrides any other policy of this category applied at a higher level of the directory hierarchy, causing the deprovisioned users not to be moved from the organizational units below the point at which the policy is applied.

Exchange Mailbox Deprovisioning (New)

These policies are used to deprovision Microsoft Exchange resources for the deprovisioned users. A policy can be configured to:

- Hide the mailbox from the global address list (GAL)
- Prevent non-delivery reports (NDR) from being sent
- Grant designated persons read access to deprovisioned mailboxes
- Redirect e-mail addressed to deprovisioned users

The policy specifies how to modify the user's account and mailbox upon a request to deprovision a user, in order to reduce the volume of e-mail sent to the mailbox of the deprovisioned user, and to authorize designated persons to monitor such e-mail.

Home Folder Deprovisioning (New)

These policies automate the following tasks on deprovisioning home folders for deprovisioned users:

- Revoke access to home folders from deprovisioned user accounts
- Grant designated persons read access to deprovisioned home folders
- Change ownership on deprovisioned home folders
- Delete deprovisioned home folders

The policy specifies how to modify security on the user's home folder upon a request to deprovision a user, and whether to delete home folders upon user account deletion, in order to prevent deprovisioned users from accessing their home folders, and to authorize designated persons to access deprovisioned home folders.

User Account Permanent Deletion (New)

These policies automate the deletion of deprovisioned user accounts. Once deprovisioned, a user account is retained for a specified amount of time before it is permanently deleted. A policy can also be configured not to delete user accounts.

A policy configured to delete user accounts specifies the number of days to retain deprovisioned user accounts. With such a policy, ActiveRoles Server

permanently deletes a user account after the specified number of days has passed since the account was deprovisioned.

A policy configured not to delete user accounts behaves as follows. When applied at a certain level of the directory hierarchy, it overrides any other policy of this category applied at a higher level of the directory hierarchy.

Notification Distribution (New)

These policies are intended to automatically send out e-mail notifications upon the deprovisioning of users. The primary purpose of such a policy is to notify designated persons about a request to deprovision a given user, so as to take additional deprovisioning-related actions on that user if necessary. The policy specifies the notification recipients and message, and determines the outgoing mail server (SMTP). The subject and the body of the message may include auto-text fields to provide information about the user being deprovisioned, to make the message more meaningful to the recipients.

A notification message cannot be considered as an indication of success or failure of the deprovision operation. It only indicates that the deprovisioning of a user has been requested. To inform of deprovisioning results, policies of the Report Distribution category can be used.

Report Distribution (New)

These policies are used to automatically send out reports on deprovisioning results upon completion of user deprovision operations. The primary purpose of such a policy is to inform designated persons about problems, if any encountered, when processing deprovisioning requests. The report includes a list of actions taken during the deprovisioning of the user. For each action, the report informs of whether the action is completed successfully, and provides information about the action results.

The policy specifies the report recipients, the subject of the report message, and whether to suppress issuing reports in case of no errors. Similar to the notification messages, the message subject can be configured to include auto-text fields. Report messages are delivered via e-mail by using SMTP transport.

Script Execution (Inherited)

The **Script Execution** policy category is now split between the AutoProvision and Deprovision branches. These policies can be used to run supplementary scripts upon requests to deprovision users. Scripting allows custom actions to be included in the user deprovision process. A script can be associated with a deprovision operation so that the policy runs it when the operation is requested or after the operation is completed.

Default Deprovision Options

There is a built-in Policy Object that specifies the operations to perform when deprovisioning a user. It determines the default effect of the **Deprovision** command on user accounts, which can be altered by adjusting and applying additional policies of the Deprovision category. It is possible to modify the built-in Policy Object, as well as to create and configure additional Policy Objects to define deprovision policies.

Delegation of Deprovision Tasks

The deprovision tasks can be delegated to any group or user. A dedicated Access Template is provided for that purpose so the administrator can easily delegate the use of the **Deprovision** command on user accounts. The delegation of the deprovision task only permits the delegates to start the deprovision process, and does not give them any additional rights, such as the ability to create, modify, or delete user accounts.

Report on Deprovision Results

Once a user is deprovisioned, ActiveRoles Server generates a report to inform of the results of the user deprovision operation. The report is displayed upon completion of the deprovision operation, and can also be accessed by using a special command on the deprovisioned user account. In addition, a policy can be configured to send the report via e-mail.

The report includes a list of actions taken during the deprovisioning of the user. For each action, the report informs of success or failure of the action. In the event of a failure, the report gives a description of the error situation.

Group Family to AutoProvision Groups

ActiveRoles Server provides for a new category of rule-based policies for group auto-provision. Each policy of that category, referred to as *Group Family*, acts as a control mechanism for creating and populating groups. These new policies address significant challenges inherent in administering group membership by automating group membership maintenance based on user information stored in the directory.

Group Family automatically creates groups and maintains group membership lists in compliance with configurable rules, allowing group membership to be defined as a function of object properties in the directory. Group Family also allows for creation of new groups based on new values encountered in object properties.

For instance, in order to manage groups by geographical location, Group Family can be configured to create and maintain groups for every value found

in the "City" property of user objects. Group Family discovers all values of that property in the directory and generates a group for each, populating the group with the users that have the same value of the "City" property. If a new value is assigned to the "City" property for some users, Group Family automatically creates a new group for those users. If a user has the value of the "City" property changed, Group Family modifies the group membership for that user accordingly.

The configuration of Group Family does not have to be limited to a single property of objects. Rather, it can combine as many properties as needed. For example, Group Family can be set up to look at both the "Department" and "City" properties. As a result, Group Family creates and maintains a separate group for each department in each geographical location.

Design Overview

The key design elements of Group Family are as follows:

- **Scoping by object location.** This determines the directory containers that hold the objects to be managed by Group Family. The scope of Group Family can be limited to certain containers, thereby causing it to affect only the objects in those containers.
- **Scoping by object type and property.** This determines the type of objects, such as User or Computer, to be managed by Group Family. Thus, the scope of Group Family can be limited to a set of objects of a certain type. The scope can be further refined by applying a filter in order for Group Family to manage only those objects that meet certain property-related conditions.
- **Grouping by object property.** Group Family breaks up the set of managed objects (scope) into *groupings*, each of which is comprised of the objects with the same combination of values of the specified properties (referred to as *group-by properties*). For example, with Department specified as a group-by property for user objects, each grouping only includes the users from a certain department.
- **Creating or capturing groups.** For each grouping, Group Family normally creates a new group to associate (link) with the grouping, and ensures the members of the grouping are the only members of that group. When creating groups to accommodate groupings, Group Family uses group naming rules based on the values of the group-by properties. Another option is to manually link existing groups with groupings; this operation is referred to as *capturing groups*.
- **Maintaining group membership lists based on groupings.** During each subsequent run of Group Family, the groupings are re-calculated, and their associated groups are updated to reflect the changes in the groupings. This process ensures that the group associated with a given grouping holds exactly the same objects as the grouping. If a new grouping found, Group Family creates a group,

links the group to the new grouping, and populates the group membership list with the objects held in that grouping.

- **Adjusting properties of generated groups.** When Group Family creates a new group to accommodate a given grouping, the name and other properties of the new group are adjusted in compliance with the rules defined in the Group Family configuration. These rules are also used to determine the container where to create new groups, the group type and scope settings, and Exchange-related settings such as whether to mail-enable the generated groups.
- **Running on a scheduled basis.** Group Family is a state-based policy by nature. During each run, it analyses the state of directory data, and performs certain provisioning actions based on the results of that analysis. Group Family can be scheduled to run at regular intervals, ensuring that all the groups are in place and the group membership lists are current and correct. In addition, Group Family can be run manually at any time.
- **Action summary log.** ActiveRoles Server provides a log containing information about the last run of Group Family. The log includes descriptions of the error situations, if any occurred during the run, and summarizes the quantitative results of the run, such as the number of updated groups, the number of created groups, and the number of objects that have group memberships changed.

By combining these design elements, Group Family provides a powerful and flexible solution for group auto-provision.

Approval Workflow

ActiveRoles Server now adds approval workflow capabilities to its Rules &Roles engine. By providing rule-based, customizable approval routing, ActiveRoles Server decreases errors and inconsistencies in the processes of directory data management, including provisioning and deprovisioning. Robust approval procedures allow a workflow process to be established, consistent with business requirements, putting in place efficient responsibility chains to complement the automated management of directory data.

Approval workflow complements the automated policies, to make provisioning and deprovisioning decisions based on human input. While automated policies require no manual intervention, approval-based fulfillment of administrative operations adds to process automation the ability to manually accept or deny operation requests, and to monitor the execution of request-processing tasks to ensure they are responded in a timely fashion.

Approval workflow can serve a wide range of requests, which are user actions intended to perform administrative operations via the ActiveRoles Server Web Interface. Examples of such operations include (but not limited to) the creation and modification of user accounts.

When a requested operation requires permission from certain individuals in an organization, a workflow starts to coordinate the approval process. The system only performs the requested operation after approval is given by an authorized person.

To configure approval workflow, the administrator creates approval rules by using the ActiveRoles Server console. Approval rules are used to specify the operations that are subject to approval and persons who are authorized to approve or deny operation requests.

Design Overview

The approval workflow-based provisioning system included with ActiveRoles Server provides:

- A point-and-click interface to configure approval rules, available from the ActiveRoles Server console. The approval rules are stored and put into action by the ActiveRoles Server Administration Service.
- The directory management section of the Web Interface for submitting operation requests to approval. For example, approval rules could be configured so that the creation of a user account via the Web Interface starts the approval workflow instead of immediately executing the user creation operation.
- The approval-related section of the Web Interface to manage operation requests. This section provides a "to-do" list of the approval tasks a designated user has to carry out, allowing the user to perform tasks such as approving or rejecting operation requests.

It is approval rules that govern approval workflow. These rules are created and administered via the ActiveRoles Server console, and include the following configurable elements:

- **Approval Conditions.** These are the conditions that must be met in order for approval workflow to start. The configurable settings are as follows.
    - The operation that is subject to approval, along with the category of objects on which to keep track of the operation.
    - The users or groups whose operation is subject to approval (operation requestors, referred to as Initiators), along with the containers in which to keep track of the operation.
- **Approvers.** These are the users or groups that are authorized to perform approval tasks. The configurable settings determine who is authorized to perform approval tasks, such as approve or deny operation requests.
- **Notification.** This is used to subscribe recipients to the notifications of approval-related events, configure notification e-mails, and set up e-mail transport.

Approval workflow provides e-mail notifications to workflow users in association with various events, such as the creation of approval tasks upon operation requests. Thus, approvers can be notified of the requests awaiting their approval via e-mails including hypertext links to the approval-related section in the Web Interface.

The notification-related settings are as follows.

- Options that determine the events to notify of. This could be the creation or completion of approval tasks, as well as the completion of the operations that were approved.
- Options that determine the notification recipients. This could be the operation requestor (Initiator), the user or group that is in charge of approval (Approver), or a specified e-mail address.
- Options that determine the contents of the notification message. A message may include fields that represent data being calculated in the run time of the approval process. Hypertext links can also be added to notification messages.
- Options that determine the outgoing mail server for notification e-mails. SMTP transport is utilized to send e-mail notifications.

With these key design elements, approval workflow provides a robust, yet flexible solution for organizations to establish approval processes complementing the automated provisioning and deprovisioning policies.

Web Interface Re-designed

The ActiveRoles Server Web Interface is a highly customizable, easy-to-use Web-based application that provides administrative coverage for all aspects of Active Directory data management. With the new version, the Web Interface has been re-designed for greater clarity and ease of use, to ensure consistent look and feel, and to improve user experience by adding new navigation options, optimizing search pages and enhancing the point-and-click interface for customization-related tasks. Also, steps have been taken to decrease response time and improve performance of the Web Interface by leveraging new technologies from Microsoft, such as ASP.NET.

The new Web Interface retains and improves upon all the enterprise-class features of its predecessor, including individually customizable Web Interface sites, user permission-based view of the Web Interface pages, and support for self-administration. It combines an attractive design with superior flexibility and many advanced features. The result is a solution that can be tailored for any category of administrative personnel, whether day-to-day administrators, business data owners, help desk operators, or even regular end-users.

The Web Interface is now easier to navigate by using a tree view. Intended for locating directory data, this additional view allows for navigation through

hierarchical structures of data containers, making the location of the data easily discoverable.

Search pages provide an alternative way for locating data. In the new version, the search pages have been optimized to be more intuitive to users. These search pages, in advanced and basic modes, allow users to build very specific searches that produce concentrated and precise lists of search results.

The Web Interface allows for much more customization than other methods of access, such as the ActiveRoles Server console. To improve the administrator experience with customizing the Web Interface, the customization-related sections have been redesigned, and enhanced with a form editor. The editor displays all pages (tabs) a given form consists of, along with the interface elements (entries) disposed on each tab, and provides the administrator with a central place to add, remove, or modify tabs and entries, as well as to change the order of tabs and entries on the form.

Support for Microsoft SQL Server 2005

ActiveRoles Server now supports Microsoft SQL Server 2005, to take advantage of high availability, increased performance, improved security, and other mission-critical capabilities enabled by this new technology from Microsoft. SQL Server 2000 is also supported, which gives organizations the flexibility to maintain repository of ActiveRoles Server configuration data using the database platform of their choice.

By choosing SQL Server 2005 as the database platform for ActiveRoles Server, you gain the following benefits:

- **High availability.** New SQL Server features, such as database mirroring, help ensure uninterrupted operation of the core ActiveRoles Server components that are heavily dependent on availability of SQL Server.
- **Increased performance.** Microsoft announced a series of audited TPC (Transaction Processing Performance Council) benchmark results that show SQL Server 2005 is up to 150 percent faster than SQL Server 2000 in some scenarios. Faster access to the configuration storage considerably improves responsiveness of ActiveRoles Server.
- **Improved security.** Security enhancements in SQL Server 2005, such as native encryption of data at all levels of access, helps ensure that sensitive configuration data of ActiveRoles Server, including administrative right assignments, is not compromised.

Any edition of SQL Server 2005 can be used to host the configuration database of ActiveRoles Server. The product comes with Microsoft SQL Server 2005 Express Edition included in the distribution package.

Improved Scalability

Administration Service is now easier to scale since the use of the SQL Server replication function is no longer required to synchronize configuration data. Multiple Administration Services can now be installed with the option to share the same configuration database on a dedicated SQL Server.

Administration Service relies on SQL Server to store configuration data such as administrative right assignments, rule-based policy definitions, administrative view settings, and many other parameters that determine the ActiveRoles Server work environment. Multiple Administration Services, normally being deployed for the purpose of load distribution and fault tolerance, should have configuration data synchronized so that switching from one Administration Service to another does not result in changing the work environment.

ActiveRoles Server now provides for two deployment models allowing you to achieve synchronization of configuration data between Administration Services:

- One Service - One Database
- Multiple Services - One Database

By combining these two models, you can gain advantages from both.

One Service - One Database

This model is supported by all versions of ActiveRoles Server. It involves a set of Administration Services enabling ActiveRoles Server to partition its load, with each Service using a separate database to store configuration data. Since the Service configuration is database dependent, the databases need to be synchronized with each other so that all Services have the same configuration. In this model, databases are synchronized by means of the SQL Server replication function.

This architecture has the advantage of having very simple layout. In addition, having a separate database for each Service improves fault tolerance since a database failure only causes one Service to get unavailable. However, it could be inefficient and costly to set up and maintain a replication environment for numerous copies of the same configuration storage. To address this shortcoming, the new version of ActiveRoles Server allows multiple Services to share one database.

Multiple Services - One Database

This is a new model, available with ActiveRoles Server version 6.0. Unlike the earlier versions requiring each Service to have a dedicated database so that there is one-to-one correspondence between Administration Services and configuration databases, the new version provides the option for a newly

deployed Service to connect to an existing database in use by other Services. With this option, the configuration data is shared by multiple Services rather than duplicated. You create the configuration database only once because any additional Services you install will connect to the same database and use the same configuration data.

As before, a set of Administration Services can be deployed for load distribution, with the difference that all Services share common configuration storage. Given that this model involves only one database, there is no data replication overhead. However, the advantages of centralizing the configuration storage also entail certain limitations.

Since all Services update and retrieve configuration data from the same database, you need to make sure that the database server does not become a bottleneck or a point of failure. With this scenario, a database failure inevitably causes all Administration Services in your environment to fail. The use of SQL Server 2005 might help ensure high availability and performance of the configuration database.

Another way to avoid the risk of unavailability of all Administration Services in the event of a database failure is by combining the two models, which is also possible with the new version of ActiveRoles Server. Several groups of Administration Services can be deployed so that each group shares a separate database, with each database being hosted by an individual server and all databases being synchronized via replication.

Support for Exchange Resource Forest

Deployment of multiple forests introduces the need for inter-forest collaboration solutions, among which the most important is the Exchange 2000 or Exchange 2003 messaging system. With multiple forests, one of the options for integrating Exchange with Active Directory is the *resource forest model*.

The resource forest model, also referred to as *dedicated Exchange forest*, implies a single Exchange organization that serves multiple forests. The Exchange forest (also known as the *resource forest*) is dedicated to running Exchange and hosting mailboxes. User accounts are contained in one or more forests, referred to as the *account forests*, which are separate from the resource forest.

The ability to have user accounts and user mailboxes in separate forests requires that shadow (or proxy) versions of user accounts be created and maintained in the Exchange forest by a directory synchronization process. For example, provisioning a user account in an account forest involves creation of a shadow, mailbox-enabled user account in the Exchange forest. The account properties need to be synchronized between the account forest and the Exchange forest.

To automate the provisioning and synchronization processes involved with the resource forest model, you can use *ActiveRoles Exchange Resource Forest Manager*—an ActiveRoles Server-based solution that includes the following capabilities:

- **Mailbox AutoProvision.** Provision of mailboxes in the Exchange forest upon creation of user accounts in account forests (Provision of mailboxes for existing accounts is also supported.)
- **Synchronization.** Updating directory data in the Exchange forest upon changes to user accounts and distribution lists in account forests
- **Deprovision.** De-provision of mailboxes in the Exchange forest upon deprovision of user accounts in account forests

Roles for AD Service Management

Microsoft-recommended roles for delegating Active Directory service management can now be implemented by using Access Templates available "out of the box." Designed in accordance with Microsoft's white paper "Best Practices for Delegating Active Directory Administration," these roles provide administrative coverage for almost all aspects of AD service management.

These Access Templates require the permissions propagation option. This option ensures the permissions they define are synchronized to the native security of Active Directory, thereby enabling the tasks of AD service management to be performed by using regular administrative tools.

Access Templates can now be used to implement the following roles for delegating Active Directory service management:

- **Forest Configuration Operators.** Forest-wide configuration-related tasks such as adding child domains, managing trust relationships, transferring the forest-wide operations master roles, modifying forest-wide LDAP settings, and raising the forest functional level.
- **Domain Configuration Operators.** Domain-wide configuration-related tasks such as adding domain controllers, transferring the domain-wide operations master roles, and managing the Domain Controllers OU and System container.
- **Service Admin Managers.** Tasks such as managing and modifying memberships in service administrator groups and managing service administrator accounts across the forest.
- **Replication Management Admins.** Tasks that involve setting up and configuring replication topology, such as creating and maintaining sites and subnets, site links, and site link bridges, as well as changing replication configuration as required.

- **Replication Monitoring Operators.** Tasks such as checking replication summary, status and latency information, and inspecting pending operations on domain controllers.
- **DNS Admins.** Tasks involved in managing Active Directory-integrated DNS, such as configuring name resolution settings and configuring domain controllers to host the appropriate DNS zone.

Engineered by Microsoft, these role recommendations take into account well-defined sets of logically related administrative tasks and the security sensitivity and impact of these tasks.

For more information about these new Access Templates, refer to the "Active Directory Service Management" section in the *Access Templates Available out of the Box* document for ActiveRoles Server 6.0.

UPGRADE FROM AN EARLIER VERSION

If an earlier version of the product is already installed, the Setup program first uninstalls all features of the old version, and then installs the features you have selected from the new version.

Setup allows you to import configuration data stored by the previous version. When upgrading the Administration Service, you have the option to copy all data from the old database to the new one. In this way, Setup ensures that the configuration settings, including all permission and policy definitions and assignments, are identical to those used in the earlier installation.

For more information on how to install or upgrade ActiveRoles Server, refer to *Quick Start Guide for ActiveRoles Server*.

Component Compatibility

The user interfaces such as the ActiveRoles Server console or Web Interface of earlier versions are incompatible with the new Administration Service. If you upgrade the Service, you also need to upgrade the user interfaces.

The Administration Service of an earlier version is incompatible with the new version of the user interfaces. To use the new version of the ActiveRoles Server console or Web Interface, you first need to upgrade the Service.

Upgrade Issues

The upgrade process of the Administration Service does not preserve the replication settings. Furthermore, upgrade can only be performed if the Service is not configured for replication. Before upgrading the Service, you should ensure that it is not configured as a Subscriber or Publisher. Replication for the new Administration Service needs to be configured after the upgrade.

When upgrading ActiveRoles Server components to the new version, keep in mind that the components of the earlier version may not work in conjunction with the components you have upgraded. The new Administration Service is only compatible with the ActiveRoles Server console and Web Interface version 6.0. Therefore, you need to upgrade the ActiveRoles Server console and Web Interface that use the Administration Service you have upgraded. Similarly, the new ActiveRoles Server console or Web Interface requires the Administration Service version 6.0, so you need to upgrade the Service once you have upgraded the console or Web Interface.

Impact on Custom Solutions

An upgrade of ActiveRoles Server components also affects custom solutions, if any, that rely on the functions of ActiveRoles Server. Any custom solutions (such as scripts or other modifications) that work fine with the earlier version of ActiveRoles Server may seize to work after the upgrade. Therefore, prior to attempting an upgrade, you should test the existing solutions with the new version of ActiveRoles Server in a lab environment to verify that the solutions continue to work. Should any compatibility issues arise during the test process, you can contact Quest Professional Services for paid assistance with those solutions.

Impact on Dynamic Groups

The new Administration Service uses a new mechanism to handle Dynamic Groups, so you must upgrade your existing Dynamic Groups after upgrading the Service from version 5.x. For that purpose, the script **DGUpgrade6x.vbs** must be executed on the computer running the Service you have upgraded to version 6.0. You can find the **DGUpgrade6x.vbs** file on the ActiveRoles Server CD, in the **Misc** folder. For more information, refer to the *ActiveRoles Server Quick Start Guide*.

Impact on Mailbox Policies

The new Administration Service uses a new mechanism to handle mailbox-related policies, so you must upgrade your existing mailbox-related policies after upgrading the Service from version 5.x. For that purpose, the script **ExchangePolicyUpgrade6x.vbs** must be executed on the computer running the Administration Service you have upgraded to version 6.0. You can find the **ExchangePolicyUpgrade6x.vbs** file on the ActiveRoles Server CD, in the **Misc** folder. For more information, refer to the *ActiveRoles Server Quick Start Guide*.