






















ActiveRoles Direct & ActiveRoles Server Comparison Chart

Feature	Direct	Server	Description	Pain
Roles			Role-based delegation simplifies the assignment of administrative permissions by enabling for the creation of templates comprised of well-defined permission sets based on the functional role of the person who will be granted those permissions.	<ul style="list-style-type: none"> Delegating control in Active Directory is time consuming and error prone Protecting the organization from security vulnerabilities and staying in compliance with regulatory laws and best practice is difficult Organizations are ever-transforming making it extremely difficult and time consuming to assign accurate and consistent entitlements to control and manage AD administrators Native tools, while powerful and flexible, often become taxing in complex dynamic environments and increase the time and potential for errors for administrators to do their jobs Native Security is often not granular enough to maintain a least privilege security model. To allow tasks to be performed, more permissions must be granted than necessary.
Rules (Policies)			<p>Rules are used to both enforce business policy and IT practice.</p> <p>ActiveRoles Server provides:</p> <ul style="list-style-type: none"> Validation and Generation Rules – ensure the validity and integrity of data being added or changed in Active Directory. AutoProvision™ Policies – ensure that entitlements such as exchange mailboxes and home folders are granted to new users. Deprovision Rules – Lockdown unused or obsolete accounts. 	<p>Business Objectives are in Jeopardy</p> <ul style="list-style-type: none"> Business processes are not integrated and data errors are common Directory data becomes unreliable or unusable because there are no controls in place to ensure data integrity. Weak, ineffective or non-existent controls in today's IT environments put compliance in jeopardy <p>Native Tools offer no solution</p> <ul style="list-style-type: none"> No mechanism to ensure administrative security or data integrity No infrastructure to enforce business policies and/or practices No way to control or automate assignment of entitlements such as mailboxes or user home folders Naming conventions are not possible with native tools
User Provisioning			<p>AutoProvision™ rules for Microsoft Exchange mailboxes and user home folder shares enable the administrator to take the guess work out of how to provisioning these critical entitlements.</p> <p>Property generation rules can be used to automatically create unique logon names, UPNs, e-mail alias and other critical account information.</p> <p>Automatic User Provisioning can be achieved when Quick Connect is installed on top of ActiveRoles Server. (See Systems Integration section later in this document)</p>	<ul style="list-style-type: none"> Providing employees secure access to resources is complicated and time consuming, yet critical. Provisioning is not a one-time event. Reprovisioning and deprovisioning continually require expensive administrators' time and attention. Administration or Help Desk users must have expert knowledge about infrastructure to assign entitlements such as selecting the proper Exchange Server for a new user's mailbox or placement into proper security or distribution groups.

<p>Group Provisioning</p>			<p>AutoProvision™ policies assign group membership plus dynamic groups that can dynamically include users in distribution or security groups that grant user s access to resources. With the addition of Quest Vintela Authentication Services to Unix, Linux and Java@ applications.</p> <p>Dynamic Groups use queries to automatically include or exclude user accounts or members of other groups into a dynamic security or distribution group. Dynamic Groups can also be used for advanced membership scenarios such as enforcement of separation of duty. For example the HRAdmins security group may never contain members of the Temporary_Contractors security group. If a temporary contractor account is somehow added to the group, Server will automatically remove them from the group.</p> <p>Family Groups automatically create groups based on defined criteria. These groups are then automatically populated with members that meet defined membership criteria.</p>	<ul style="list-style-type: none"> • Managing and maintaining group membership is a difficult and time consuming task. • When groups are used to grant or deny access to files, folders, and/or applications, mistakenly adding a person to the group turns into security breach. • When groups are used as e-mail distribution lists, mistakenly adding a person to the group can compromise the confidentiality of an e-mail sent to that group.
<p>User Deprovisioning</p>			<p>ActiveRoles Server provides complete Deprovisioning Policy support so that accounts and entitlements can quickly and accurately be locked down when no longer needed. Those accounts can then be scheduled for automatic deletion based on an organizations' obsolete user account retention policy.</p>	<ul style="list-style-type: none"> • The timely lockdown and removal of terminated accounts/users major risk and consequences. (See Appendix 1) • Obsolete accounts represent a security and compliance risk
<p>Views</p>			<p>Views provide the administrator with the ability to create query based lists of Active Directory objects to reduce the amount of time spent performing complex searches. For example the administrator may choose to create a view that displays locked out user accounts.</p> <p>Dynamic Delegation describes the ability of Server to perform role based delegation against a view. When the query that defines the objects that make up the view is updated any objects that are added or removed automatically come into or out of control of the role holder.</p>	<ul style="list-style-type: none"> • Locating Active Directory objects that match specific criteria so they can be managed, can be a time consuming project. • Native delegation over large numbers of directory objects can require the assignment of Access Control Entries beyond the limit of Active Directory (known ACL Bloat).
<p>Administrative Approval</p>			<p>ActiveRoles Server provides approval policies that can be applied such that specific tasks performed against Active Directory by day-to-day administrators or help desk users must have an approval before they are written to the directory.</p>	<ul style="list-style-type: none"> • Native Tools offer no solution • Not all administrators are created equal and some require oversight so that critical mistakes are not made.

<p>Web and MMC Interface</p>	 	<p>The MMC (Microsoft Management Console) is a standard component that ships with all version of Windows Server. The MMC console not only provides a consistent way of accessing applications, it also often has performance benefits over web based counter parts.</p> <p>Web-Based interfaces for the Management for Active Directory not only provide a way for administrators to manage Active Directory remotely but eliminate the need to distribute an MMC console.</p> <ul style="list-style-type: none"> • Both ActiveRoles Server and Direct support use of MMC and/or Web-based interfaces. • ActiveRoles Server offers 3 separate audience-specific web interfaces, each tailored to a specific set of tasks. The Administrator, Help Desk and the Self-Service web interfaces are all designed with a specific group of users in mind. • ActiveRoles Server adds point and click customization of its web interfaces so you can add any attributes to any form. 	<ul style="list-style-type: none"> • Native Tools offer only an MMC interface • Often administrative tasks need to be perform remotely • MMC interface is inflexible and all encompassing, not very user specific
<p>Point and Click Customization of the Web Interface</p>		<p>ActiveRoles Server provides point and click customization for its web site. This allows attributes to quickly be added or removed to the interface without modify HTML code.</p>	<ul style="list-style-type: none"> • Native Tools offer no such feature.
<p>Exchange support</p>	 	<p>The native utility for managing users that ships with Active Directory is extended when Microsoft Exchange is installed. The changes to this utility are to allow for the configuration of AD data that allows users and groups to be mailbox enabled.</p> <ul style="list-style-type: none"> • ActiveRoles Server adds to this capability by adding AutoProvision rules (automation) for Microsoft Exchange that per-determine the Exchange Server and Store a mailbox will be provisioned to during the user creation process. 	<ul style="list-style-type: none"> • Determining a mailbox location and store for users can be tedious, time consuming, and require senior (and expensive) administrative assistance.
<p>Centralized Reporting</p>		<p>Centralized reporting provides a single set of reports showing your, role definitions and where they are delegated, rule definitions and where they are enforced, objects that don't comply with current rules, activity of administrators and objects under control by administrator for the entire enterprise - regardless of domain, forest or other boundary.</p> <p>Some management systems claim to have centralized reporting but require the administration be done in a single centralized site.</p> <p>When issues arise, real-time on-line reporting allows the key administrators to see who changed an object, what they changed and when.</p>	<ul style="list-style-type: none"> • Documented procedures on how an organization manages users and their access is often lacking for audits • Auditing and tracking of user and administrator activity to ensure compliance with external regulations and internal policies is often difficult to compile and incomplete.

<p>Development Environment</p>			<p>ADSI Scripts provide powerful features that can be used to automate many day-to-day operational tasks in Active Directory.</p> <ul style="list-style-type: none"> ActiveRoles Server provides for the creation of script libraries for storing and executing ADSI scripts against the custom ARS_ADSI provider. By providing a custom ADSI provider the scripts can make use of features that do not exist in Active Directory and yet are subject to the same Roles and Rules implemented to control day-to-day administration. ActiveRoles Direct provides a place to store and execute native ADSI scripts. 	<ul style="list-style-type: none"> Scripts are often used in an attempt to automate a specific task or process. Unfortunately, native scripting is not constrained by Roles and Rules so a simple typing error can have drastic consequences in a production environment. Native tools provide little in the way of help in organizing and maintaining scripts so the chance that the wrong script will be used is increased. Native tools provide no mechanism for tying the native user interface to a script so scripts must be run in one-off scenarios Native tools provide no way of distributing scripts between locations.
<p>Systems Integration</p>				
<p>Automatic User and Group Provisioning from HR Data</p>			<p>When Quick Connect is installed on top of ActiveRoles Server, automatic deprovisioning based on authoritative HR or ERP data is achieved. Many legal and regulatory compliance initiatives require that when a user retires or is terminated their Active Directory account is automatically disabled to prevent on-going network access.</p> <p>Scheduled Import Wizard allows for a scheduled one-way import of HR or ERP data into Active Directory through ActiveRoles Server.</p>	<ul style="list-style-type: none"> Regulatory requirements are at the forefront of IT initiatives and managing identities has become a key factor in compliance Duplicate data entry into Active Directory and HR and ERP systems is time-consuming and error-prone.
<p>Unix/Linux/Mac Users and Groups</p>			<p>ActiveRoles Server extends management control to Unix, Linux, Java and Mac identities, including users, groups and computers, when it is combined with Quest's Vintela Authentication Services. Decrease your administrative costs and better leverage ActiveRoles Server by utilizing this unique technology.</p>	<ul style="list-style-type: none"> Managing Active Directory identities is difficult enough, but add to that Unix, Linux, and Mac identities and the administrative workload, security breaches, and potential for errors only gets worse
<p>SPML Support</p>			<p>The SPML Provider provides enterprise architects and administrators with the flexibility needed to use ActiveRoles Server to perform user management and user provisioning in heterogeneous environments. Because the SPML Provider uses open standards such as HTTP, XML, and SOAP, a greater level of interoperability with ActiveRoles Server and/or Active Directory is possible.</p> <p>Download this "How to" paper to see how the SPML 2.0 Provider was used to integrate Quest ActiveRoles Server and IBM's Tivoli Identity Manager - Link</p>	<ul style="list-style-type: none"> Integration in heterogeneous environments is complex, difficult to maintain, and once built is often not flexible.

<p>Cross Platform Provisioning with ILM/MIIS</p>			<p>Quick Connect for ActiveRoles Server integrates ActiveRoles Server with Identity Lifecycle Manager (ILM) formerly known as Microsoft Identity Integration Server (MIIS).</p> <p>Simplify MIIS deployment: Integration with Microsoft Identity Integration Server (MIIS) provides a two-way synchronization including but not limited to provisioning of user accounts and groups in ADAM, SunOne®, Lotus Notes® and Microsoft SQL Server®.</p> <p>Self Service Interfaces: Point and click customization of the Web Interface provides custom forms for managing Active Directory objects or Virtual Attributes allowing the system to be tailored to the organizations needs.</p>	<p>Given the complexity of today's Information Systems, managing user and group identities has become time-consuming error-prone</p> <p>Cost and Complexity of Identity Management continues to be a barrier</p> <ul style="list-style-type: none"> • IT processes are complex, and managing identities has become time-consuming, but businesses struggle to afford multi-year, multi-million dollar projects to gain control of Identity management. • Multiple infrastructure solutions, for multiple platforms, multiply costs!
---	--	---	---	---

Appendix

1. Potential consequences and risks of not timely ceasing access and accounts of terminated users

- ✓ For several days, a \$1 billion per year computer monitor manufacturer's Taiwan office was **unable to access critical files** that were **deleted by a former network administrator** that had been terminated 2 weeks earlier.
- ✓ A former AS/400 programmer caused **\$80,000 in damage** to his former employer after breaking in from a remote location.
- ✓ After being terminated, a former administrator to a transportation services company **deleted the company's customer database and changed system passwords**.
- ✓ After being fired, a former employee accessed his company's servers, **deleted 675 files, changed access control levels, altered billing records, and sent email with false statements** about the company to hundreds of its customers.