

**Product Report: Quest ActiveRoles Server**

## **Quest ActiveRoles Server**

### **Product Report**

© Kuppinger Cole + Partner, Digital ID Analysis + Evaluation, 2009-07-09

**Author: Martin Kuppinger**

### **Executive Summary**

---

Quest's ActiveRoles Server belongs to the category of *Enterprise Provisioning* products, but it is not a typical standard-issue provisioning solution. Instead, it is a tool for role-based administration of both Active Directory and a growing number of other system environments.

As is to be expected, its greatest strengths are in management of Active Directory environments, where its functionality extends significantly beyond just simple provisioning. On the other hand, Quest has been systematically augmenting and improving the product's existing provisioning functions over the years and through various releases cycles. The result is a powerful solution for Identity & Access Management (IAM) that extends far beyond Active Directory. It can be best applied in environments where Active Directory is employed or in which Active Directory plays a major role. It fully addresses the special requirements of typical Active Directory environments, as well as cases where an insufficient degree of integration in traditional provisioning solutions may prove a limiting factor in handling Windows-specific functions.

Quest ActiveRoles Server is one of the most interesting offerings in today's provisioning market because it takes a very different approach than other products. It integrates closely with Active Directory and therefore provides outstanding management capabilities in conjunction with Windows servers. However, certain restrictions remain due to the limited number and functionality of connectors, as well as the lack of workflows.

We recommend including Quest ActiveRoles Server in any list of evaluation candidates for environments in which Active Directory is crucial and where the existing IT infrastructure is relatively homogeneous. The same goes for environments where conventional provisioning products are unable to deliver the desired administration functions for Active Directory and Windows servers.

**Product Report: Quest ActiveRoles Server****Analysis overview**

---

➤ Very close integration with Active Directory	➔ Limited number of connectors for other than standard systems
➤ Supports Windows-specific management functions	➤ Poor SAP connection
➤ Good integration interfaces	➔ Administration via MMC console needs improvement
➤ Comparatively lean product with potentially low project overhead	➔ Does not support complex application and approval procedures (planned)
➤ Modular concept allows phased adoption and upgrading	➔ Does not support password synchronization (planned), but provides various tools for single sign-on and other functions within the portfolio
➤ Simple-to-use interface and scripting functions	➤ The encryption key for sensitive information is stored in a file on the hard disk, thus offering intruders a single point of attack
➤ Built-in support for auditing, reporting and attestation	➤ No signed audit logs
➤ Optimized for Microsoft infrastructure (.NET Framework, SQL Server, etc.)	
➤ Excellent self-service interfaces	

**Product Category**

---

Quest ActiveRoles Server belongs to the Enterprise Provisioning product category. These are systems that can automatically handle user and permission allocation in connected systems, often using application and approval workflows.

Essential functions of such systems include the provisioning itself, usually with the help of connectors, also basic self-service and password management, as well as auditing and role-based change management. Delegated administration is also an important feature.

Unlike most established Enterprise Provisioning products, Quest ActiveRoles Server traces its origin to administration tools developed specifically for Active Directory environments. They fit easily into Active Directory infrastructures, but can also administer identities and rights within other systems. It makes sense therefore to rank it among Enterprise Provisioning products and not to regard it simply as an administration tool for Active Directory. It must be noted, however, that the emphasis differs from similar products in this category. Due to its antecedents as an Active Directory admin tool it is especially useful for small and medium companies where a Microsoft infrastructure is in place since it is potentially easier to implement there than most conventional provisioning products. The large number of customers (Quest talks of more than 2,000 installations, far more than most competitors) is a result of this fact.

**Product Report: Quest ActiveRoles Server****Product Description**

---

As already indicated, Quest ActiveRoles Server is unlike most typical provisioning products in that it provides basic functionality for role-based administration of Active Directory environments, as well as a growing number of others.

The strength of the products lies, as is to be expected, in the management of Active Directory environments where it outperforms most conventional provisioning tools. On the other hand, Quest has been busy over the past few years improving the product's provisioning functionality from one release to the next. It can now be considered a powerful solution for most tasks within the area of Identity & Access Management (IAM) and not just for Active Directory environments.

It performs best in environments in which Active Directory is either the only system in use or where it at least plays a major role. Quest ActiveRoles Server was initially intended for delegated administration of Active Directory by providing automated control and maintenance based on roles and rules. These include for instance setting up Exchange mailboxes and user directories which are typical use cases within Active Directory environments, and it is here that conventional provisioning solutions often run into problems with Windows infrastructures.

The product is based on client/server architecture with centralized services and decentralized administration components. Administration information is stored in a central database running on Microsoft SQL server. Sensitive information is stored in encrypted form. However, the encryption key is stored in a file located on the hard disk and is secured only with a password. It therefore represents a potential risk, but since ideally the server itself, and not just the ActiveRoles Server, should be secured, the potential threat appears small.

**Connectors**

---

The ability to connect to a variety of systems is crucial for any provisioning solution. Quest ActiveRoles Server supports Active Directory and AD LDS (Active Directory Lightweight Directory Services, formerly ADAM) so it can link seamlessly with Microsoft Exchange Server. There is also an add-on edition for more complex installation scenarios.

Other systems can be added through ActiveRoles Quick Connect, a solution that allows synchronization of identity data and provides access control information such as groups and roles, as well as the ability to map objects between Active Directory and the other connected systems. In this case, Active Directory serves as the lead system due to the fact that ActiveRoles Server primarily acts there.

ActiveRoles Quick Connect is available in different flavors. The basic version supports most standard systems such as Novell eDirectory, various database formats and data format conversion, as well as additional Active Directory and AD LDS installations. This means that most HR systems and other essential business processes can link up with ActiveRoles quickly and easily. Other editions include Lotus Notes/Domino and IBM RACF connectors.

**Product Report: Quest ActiveRoles Server**

This is probably enough connectivity for most. The current list of connectors does seem short compared to the offerings of other vendors, but it covers most popular systems. There is also a mainframe connector available. A weak point appears to be SAP integration which is important for many companies, especially small and medium businesses typically running Active Directory and SAP as their central IT components.

On the other hand, connecting an ActiveRoles infrastructure with SAP can be relatively simple with the help of SAP's increasingly popular NetWeaver Identity Management. While NetWeaver is mostly used to manage SAP infrastructures, it also offers a robust and highly integrated management capability for most other IT systems at very reasonable cost.

Quest has announced plans to substantially expand the functionality of ActiveRoles Quick Connect in 2009, a fact that will contribute to positioning ActiveRoles as a comprehensive provisioning solution.

The product already offers a number of benefits within the Active Directory space, including temporary group membership as well as the ability to undo the erroneous de-provisioning of a user – something that experience shows can be extremely tricky with Active Directory.

**Workflows**

---

While automating administrative tasks in the area of identities and access rights in connected systems remains a core component of any provisioning solution, the ability to handle applications and approvals for new users and rights is also very important.

Right now, this must be considered a weak spot in Quest ActiveRoles Server which is unable to handle applications, and which only provides simple, one-step approvals due to the lack of complex workflows. However, Quest has already announced plans to add these capabilities before the end of 2009.

Besides, most critical tasks within an administration-oriented IAM installation can be implemented already today using rules, regulations and roles, as well as simple approval models. Applications can also be submitted through the self-service interface which will be described in more detail below.

Finally, thanks to its open design, Quest ActiveRoles Server can integrate quickly and easily with existing application systems and other business processes within the company by using VBScript.

**Password Management**

---

Quest plans to substantially enhance ActiveRoles Quick Connect by the end of this year by adding the ability to propagate passwords to other platforms. Quest already offers a number of products which offer Single Sign-on and other capabilities required for efficient authentication. These can be used in conjunction with the Quest ActiveRoles Server.

**Product Report: Quest ActiveRoles Server****Self-services**

---

Quest ActiveRoles Server was originally intended as an administration tool. Since provisioning and administration processes usually require some kind of self-service capability, this was added as an option.

Quest ActiveRoles Self-Service Manager allows users to generate requests. That way they can ask for resources such as data, approvals, Exchange mailing lists or applications. The owner of the resource can approve, administer, and monitor access and thus make certain that access is given on a need-only basis.

The self-service module again demonstrates the close connection between Quest ActiveRoles Server and Active Directory because it enables sharing of resources in Windows server environments. This means that management need not restrict itself to providing abstract assignment of users to certain groups or roles.

**Delegated administration**

---

ActiveRoles Server was originally built to Delegate administrative tasks within Active Directory environments and other connected systems and directories. This soon becomes apparent in everyday deployment.

The aim was to allow controlled, replicable and rule-based administration of Active Directory (and other systems) through a given set of permissions. This can be achieved by setting up appropriate roles and rules. The role defines who is allowed to alter what kind of information. Rules control individual values. That way, it becomes easy for instance to stipulate uniform syntax for e-mail addresses, required fields or standard formats such as telephone numbers. The rules are easy to configure, at most requiring a little VBScripting. As a result, customization is generally much easier than with comparable products.

These functions are simplified with the help of approval processes and dynamic views of queries.

**Architecture and interfaces**

---

In terms of architecture and interfaces Quest closely followed Microsoft's lead in standards and concept development. The products works with Windows servers, draws on Microsoft .NET Framework 3.5, and uses Microsoft SQL Server as its database. Web interfaces are based on Microsoft IIS and ASP.NET. The administrative interfaces running on Windows are built on MMC interfaces (Microsoft Management Console). Expansion and integration make use of Web Services and VBScript. However, greater emphasis on task orientation in the MMC console would be an improvement.

Quest offers an ActiveRoles Management Shell for Active Directory as an add-on in order to allow its customers to use the basic functions of Microsoft PowerShell. Additional expansions are in the pipeline, for instance the ability to do scripting in ActiveRoles Server through PowerShell.

## Product Report: Quest ActiveRoles Server

The net result is that Quest ActiveRoles Server is extremely easy to integrate with existing Microsoft environments without the need for additional specialized know-how. We consider this ease of integration and the close proximity to Microsoft to be the biggest benefits the product has to offer from a typical customer viewpoint.

This does not mean that introducing Quest ActiveRoles Server can be achieved without some conceptual grunt work. While this may be less than with comparable provisioning products, it remains essential to properly plan the use case as well as the appropriate rules and roles. And creating role models may call for the use of third-party tools since Quest does not currently offer any of their own.

## Additional products

---

Another thing that distinguishes Quest ActiveRoles Server from similar products in the market is its modular structure. Besides the basic product there is a long list of add-ins available:

- ActiveRoles DNS Manager which manages distributed DNS environments integrated with Active Directory
- ActiveRoles Quick Connect which is described above
- ActiveRoles Exchange Forest Resource Manager which helps to manage infrastructures in which Exchange is installed in its own Forest parallel to Active Directory
- ActiveRoles Self-Service Manager
- ActiveRoles Management Shell for Active Directory

Also, there are methods and interfaces available to integrate with other Quest products in areas such as central auditing or operations management.

Since all the products in the ActiveRoles product family share the same architecture they are easy to combine and scale. Customers can start small and build their way up to a comprehensive provisioning infrastructure, starting with management of Active Directory environments.

## Internal security and auditing

---

Quest ActiveRoles Server offers powerful integrated auditing and reporting to monitor and control changes in Active Directory and other systems. However, it lacks the option for signed entries in audit logs demanded by some customers.

Interestingly, in addition to the standard approval functions, the product offers an attestation function which can enforce the regular review of allocations.

With the single exception of the way the encryption key is stored on the hard disk Quest's security concept appears sophisticated and convincing. We were unable to find any other weak points.

**Product Report: Quest ActiveRoles Server****Fields of application**

---

As frequently mentioned, Quest ActiveRoles Server is a provisioning solution that emerged from an administration tool for Active Directory. This determines to some degree the product's possible application scenarios.

While it is ideally suited for pure Active Directory environments, it can also be used to provision other systems. Restrictions apply due to the lack of workflows and the limited number of connectors. Quest has promised to provide these in future releases.

It is also possible to imagine using Quest ActiveRoles Server in combination with other provisioning solutions, as was noted above in the case of SAP NetWeaver Identity Management. Here, Quest ActiveRoles Server would ideally serve as an optimized subordinate interface for Active Directory environments due to its close integration with that system.

From a budget perspective, Quest ActiveRoles Server offers both lower license costs and implementation overhead, neither of which should be neglected. Should the functionality offered by Quest ActiveRoles Server be sufficient for a company's needs it can be a true alternative to other provisioning solutions, especially since SAP integration through SAP NetWeaver Identity Management, as well as other systems, is a viable option.

**Partners**

---

Quest offers both its own Professional Services division and a broad network of partners to assist customers in implementing its products. External service providers range from small local shops to big regional and national system integrators.

**General assessment**

---

Quest ActiveRoles Server is one of the most interesting products currently available in the provisioning solutions market, especially since the vendor has chosen a unique approach to the problem. It can be closely integrated with Active Directory and offers excellent management support for Windows server. Some reservations are due regarding the depth of its basic provisioning functionality, the number of connectors on offer, and the lack of workflows.

Strengths include modular design, easy customization, a wealth of interfaces, and comparatively quick and simple implementation. In contrast to earlier versions, the current edition of the Quest ActiveRoles Server appears notably matured and well on its way to becoming a full-fledged provisioning product with all the bells and whistles, especially if Quest makes good on its promise to close the last remaining gaps by the end 2009.

Quest ActiveRoles Server can already be seen as a viable alternative to classic provisioning products, especially if Active Directory is important for the company. Other potentially interesting scenarios include integration with other provisioning solutions or running Quest ActiveRoles Server as a subsystem within a GRC platform.

**Product Report: Quest ActiveRoles Server**

These promise comparatively straightforward answers to the complex requirements of many IAM and GRC infrastructures, especially since implementation costs compare favorably with other provisioning solutions.

We recommend including Quest ActiveRoles Server in the short list of options wherever Active Directory is a crucial component and within relatively homogenous IT environments. The same goes for environments in which conventional provisioning products have difficulties handling the special requirements of management both Active Directory and Windows servers.

Quoting information and data from Kuppinger Cole + Partner: Individual sentences and sections may be used in internal documents and presentations exclusively for internal communication within the company without the explicit permission of Kuppinger Cole + Partner. Use of large sections or the complete document requires previous written permission from Kuppinger Cole + Partner and may include the payment of royalties. External publication of documents and information by Kuppinger Cole + Partner in advertisements, press reports or other marketing material generally requires previous written permission from Kuppinger Cole + Partner. A draft of the relevant documents should be provided. Kuppinger Cole + Partner reserve the right to refuse external use for any reason. © Kuppinger Cole + Partner 2004-2009. Reproduction forbidden unless authorized. For additional copies, please contact [service@kuppingercole.com](mailto:service@kuppingercole.com)