Virtual Directories Enhance Identity and Access Management Solutions

John Enck

Virtual-directory technology has overcome some of its past market and network limitations, and has caught the attention of major identity and access management vendors. By year-end 2009, it will be used by the majority of organizations implementing IAM solutions.
WHAT YOU NEED TO KNOW

Consider adopting virtual-directory products to address the two stronghold use models described in this research. Evaluate products from the independent vendors in the market; however, understand where virtual-directory capabilities fit into the technology road maps of your strategic suppliers of directory and identity and access management products.

STRATEGIC PLANNING ASSUMPTION(S)

By year-end 2009, 80 percent of organizations deploying IAM solutions will use virtual-directory technology as part of the IAM infrastructure (0.7 probability).

By year-end 2007, Microsoft will introduce virtual-directory technology to Active Directory (0.7 probability).

ANALYSIS

The Evolution of Virtual-Directory Technology

When virtual-directory technology was introduced at the turn of the millennium, its primary purpose was to provide a Lightweight Directory Access Protocol (LDAP) interface to traditional data stores (for example, databases, flat files and non-LDAP directories). However, the real power in virtual-directory technology was that it could aggregate data stores into a unified LDAP view. For example, multiple databases containing different sets of users could be combined into a single, virtual LDAP directory.

Although this approach clearly provided value, there weren't many market opportunities for virtual directories, and the vendors providing these products saw limited growth. One of the biggest limitations of virtual-directory technology was that the early generations of the technology were network-dependent. The data driving the composite view was obtained in real time over live network links. Thus, if a network link went down, a section of the virtual directory was no longer available.

Dependence on network links constrained the use of virtual-directory products. For example, virtual-directory technology would have theoretically been an ideal solution for aggregating multiple repositories into a single authentication directory for extranet use, but any instability in the network would have hampered this function. As a result, virtual-directory products were deployed in environments where the directory function was not mission-critical or where network links were absolutely reliable.

Virtual-directory vendors continued to enhance their products to address this limitation. They added caching and synchronization capabilities that enabled virtual-directory implementation to function through the loss of network links. From Gartner’s perspective, the virtual-directory vendors began to introduce metadirectory capabilities into their products (for example, maintaining a formal, aggregate store and providing synchronization between the underlying repositories).

In addition to addressing network limitations, virtual-directory vendors increased the number and types of repositories they supported. With today's breed of virtual-directory products, nearly any data store can be accommodated. Thus, multiple Active Directory forests can be turned into a single, virtual Active Directory forest, or LDAP directories from different vendors can be combined with multiple databases from different vendors into a single virtual directory.
**Virtual-Directory Use Models**

On the surface, it appears that virtual-directory technology would have broad application; however, virtual-directory products have had limited traction in the market. There are only hundreds of virtual-directory implementations in production, as opposed to tens of thousands of metadirectory implementations.

Virtual-directory implementations lag behind metadirectories because many organizations aren't keen to expose live directories through a virtual model. They prefer to have a tiered repository model for security and stability reasons. For example, a virtual directory would enable two internal Active Directory forests to be exposed as a single, external forest for extranet use. However, organizations might not be willing to do this because of 1) potential exposure to security penetrations through the virtual layer into the physical directories and 2) the performance impact on the physical directories when the virtual layer competes for access with native, internal directory use.

Virtual-directory technology has, however, found two strongholds where the benefits of virtualization clearly outweigh the limitations:

- For highly distributed organizations where business units maintain their own identity repositories separately but the organization wants a view of the aggregated identities. In this case, virtual directories permit the aggregate view without forcing synchronization at the business-unit level. For example, multiple, independent business units could participate in a virtual directory to create an organization-level "White Pages" directory view.

- For larger identity and access management (IAM) solutions. In this case, virtual-directory technology solves a difficult problem for traditional IAM vendors. Without virtual-directory technology, vendors must write connectors in their software to interface with the directories, databases and repositories that store user information. However, with virtual-directory technology, the IAM layer only needs to interface with the virtual directory layer, which handles all of the underlying connections to the repositories.

Many IAM vendors are interested in partnering with virtual-directory vendors. By year-end 2009, 80 percent of organizations deploying IAM solutions will use virtual-directory technology as part of the IAM infrastructure (0.7 probability).

**Market Challenges**

Virtual-directory technology was pioneered by small, independent vendors. MaXware and Radiant Logic were among the first companies to offer this technology, and OctetString recently joined the field. These three companies have been jockeying to sell their products directly to end users and competing to form meaningful partnerships with IAM vendors.

The benefits of virtual-directory technology have captured the attention of some larger IAM vendors. Computer Associates International, IBM, Novell, and Sun Microsystems have added, or are in the process of adding, virtual-directory technology to their product offerings. Microsoft is the only major directory and IAM vendor without virtual-directory capabilities on the road map; however, we believe this will change. By year-end 2007, Microsoft will introduce virtual-directory technology to Active Directory (0.7 probability).

The adoption of virtual-directory technology by the major IAM vendors clearly signals that virtual-directory technology is emerging from the shadows. This is good news for organizations looking to deploy complex IAM solutions. However, this represents a significant challenge to independent vendors that must introduce new features and capabilities in advance of their larger competitors or run the risk of extinction or acquisition.
Organizations considering implementing a virtual directory to aggregate a view of a distributed organization should consider a direct engagement with a virtual-directory product vendor. Organizations looking to use virtual-directory technology in conjunction with a broader IAM solution should look to the primary IAM vendor as the provider of virtual-directory technology (directly or through a partnership).

**Key Issues**

How will identity and access management evolve as an enterprise infrastructure?