Top 10 Reasons for The Virtual Identity Server

The .NET Virtual Directory

Introduction

LDAP Virtual Directories, such as Optimal IdM's Virtual Identity Server (VIS), are not a brand new technology. Instead, they have been around for many years. They have quietly solved business issues without much fanfare or publicity. Only recently, has the topic of LDAP Virtual Directories hit the mainstream.

In fact, just a few years ago, it was nearly impossible to find Virtual Directory sessions at industry conferences, while this years Directory Experts Conference and Digital ID World conference had several sessions on the topic. This is good news for CIO's, IT managers and companies in general as the benefits and use cases of Virtual Directories become better known.

The key to a successful, wide scale adoption of any technology is education. This is taking place as people are learning how companies large and small are using Virtual Directory technology such as Optimal IdM's Virtual Identity Server to:

- Simplify their IT infrastructure
- Better manage the environment
- Reduce IT Costs and total cost of ownership (TCO)
- Enhance compliance & reporting capabilities

When do I need a Virtual Directory? And...When should I use it?

These apparently benign questions have sparked many blogging wars over whether synchronization or Virtual Directories should reign supreme. The simple fact is that organizations usually need both technologies. Each of these technologies is a tool, serving a given purpose and the key is knowing when to use which technology. This whitepaper will outline some of the reasons and use cases (in no particular order) where a Virtual Directory is needed and is the best choice.

Reason 1—Mergers & Acquisitions

Immediately following a merger or acquisition, executives want a single merged entity. Waiting for network changes, system consolidations and new corporate standards is simply not an option. Unifying these separate data stores needs to be done immediately and without delay.

A Virtual Directory can immediately provide a quick and easy way to deploy the applications to users in multiple repositories without making any application code changes or altering the data in those repositories.

On multiple occasions and in under two hours, the Virtual Identity Server has been installed and configured providing a single unified view of two merged companies, achieving an instant and immediate payback.

Reason 2—Multiple Identity Repositories

Users and user identity data are not contained in one large centralized ***Enterprise Directory***. Instead, this information is scattered throughout the enterprise. Directories should be consolidated whenever possible, but the reality is that user data is separated for many reasons such as:

- A desire to have separate security and control
- Some applications require separate physical stores
- Legal or application constraints
- Data must be in a different format (i.e. database)

A virtual directory can easily join, merge and view this data from multiple siloed data repositories into joined enterprise views with ***real-time, live connections*** to the backend data sources. Applications can then leverage these joined views to make business decisions.

Reason 3—Rapidly Deploy Applications

Having one large Enterprise Directory is simply not feasible on a grand scale. In fact, in the late 1990's Microsoft's vision was for organizations to have one centralized Enterprise Active Directory. While Active Directory is the worldwide standard, it is not deployed as a single Enterprise Directory for most organizations.

An Enterprise Directory forces everyone to agree on fundamental/structural items such as the namespace, schema, tree structure, and data ownership. This becomes increasingly difficult as the number of applications and uses increases.

VIS, however, can easily provide multiple views of data, on an application by application basis, dynamically and virtually. Data and key elements such as namespace, tree structure and schema can be transformed at runtime and be different for each and every application, without making an unnecessary copy of existing data. **This simplifies complexity and reduces costs.**

Reason 4 — Data Latency

A Virtual Directory provides real-time access to data in multiple data stores (LDAP, SQL, etc.). Synchronization, on the other hand, takes processing time and therefore introduces latency, with the data becoming "stale" between synchronization runs.

Most organizations run data synchronization once or twice a day to synchronize data sources, which is sufficient to handle provisioning and de-provisioning of accounts. However, many requirements dictate that certain applications or reporting be based on real-time information, where there can be no latency time. A Virtual Directory, such as the Virtual Identity Server can join and merge views of data directly at the source in real-time.

http://www.optimalidm.com/vis/

Optimal IdM

Top 10 Reasons for The Virtual Identity Server

The .NET Virtual Directory

Reason 5—Protect and Secure Active Directory (AD) with an LDAP Firewall

In the same way that an ISA/IAG server secures and protects an IIS web server, the Virtual Identity Server, proxies data to and from your Active Directory further protecting your network.

Applications no longer connect directly to Active Directory, issuing bad LDAP queries impacting network performance or even worse taking down Active Directory.

Applications connect to the Virtual Directory, which in turn connects to and queries the AD server. Applications can now be limited on not only what queries are executed, but also what parts of the directory they can view. The result is a increased control, security and a more protected Active Directory environment.

All data and activity through the Virtual Identity Server is optionally logged to a Microsoft SQL Server database. Out of the box reports, allow administrators to see and monitor activity in their environment in real-time, such as number of successful/failed authentications, and LDAP searches against their Active Directory.

Reason 6—Increase performance of Active Directory and your applications

The Virtual Identity Server from Optimal IdM can actually increase performance in both your Active Directory as well as your LDAP applications.

Application Performance Enhanced
In one customers live performance test, all 4 processors of an ADAM server were pegged at 100% usage when an application was connecting directly to ADAM. Connecting the application to the Virtual Identity Server, which in turn connected to ADAM resulted in all 4 processors never exceeding 40% usage.

This is accomplished by the enhanced multi-threading and optimized searches that are performed by the Virtual Identity Server.

Active Directory Performance Enhanced
If applications or users frequently search on the same data and this data does not change frequently, it can be optionally cached at the Virtual Identity Server layer. This results in fewer searches being forwarded to the Active Directory server and results in increased performance of the AD server.

In addition, VIS adds powerful performance enhancing features such as **data paging** (handling large data sets) and **connection pooling** to any application connecting to VIS without any application code changes.

Reason 7 — Data Leakage Prevention

A key concept that has been prophesied lately has been one of data minimization and data leakage. Prevention. This refers to only providing the information that an application requires. For example, if an application only needs to authenticate a user and obtain their job code, then this is the only information that should be returned.

VIS can easily enforce this business rule by restricting the data returned to an application without changing the source code of the application. This reduces the possibility of data leakage by minimizing the amount of data that is spread throughout the environment. Rather than replicating all data everywhere in the event it is needed, data is retrieved as needed, on a case by case basis. This **reduces security risks** by moving less authorization data around the enterprise.

Reason 8 —Single Point of Administration

A Virtual Directory creates joined real-time views of multiple siloed data repositories. The Virtual Identity Server from Optimal IdM, with its Windows and .NET web applications, allows you to **manage and report on your entire enterprise from a single point of administration.**

Reason 9 — Eliminating AD Schema Changes

Many third party applications require Active Directory Schema changes. This is not a technical difficulty, but one that usually requires a large amount of bureaucracy and processes for organizations. Often, there is a schema management board, reviewing and approving proposed AD schema changes.

The Virtual Identity Server provides the ability to apply these Active Directory schema changes at the virtual layer and seamlessly apply the data changes on-the-fly at run-time with no application code changes.

Reason 10 —Real-time Enterprise Compliance & Reporting

Real-time views of data are a necessary component of compliance initiatives, as well as monitoring and reporting. A Virtual Directory provides these real-time views of multiple siloed data sources such as directories, databases or any connected data store. Software such as Optimal IdM's VIS for Automated Compliance Management utilizes a Virtual Directory to apply real-time compliance automation for an enterprise. Actions or alerts can be triggered to automatically occur as data changes within the enterprise. This provides greater information and security and information, while leveraging the existing infrastructure, to reduce costs and lower TCO.

Contact Sales@optimalidm.com to learn 5 more reasons!

http://www.optimalidm.com/vis/

Optimal IdM