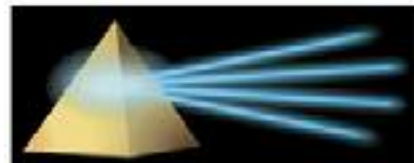


# **Using Virtualization to Leverage your Investment in Active Directory**

**A White Paper by Radiant Logic, Inc**



**RADIANT LOGIC, Inc.**

**1682 Novato Blvd.  
Novato, CA 94947  
415-209-6800**

**[www.radiantlogic.com](http://www.radiantlogic.com)**



## Content

Introduction.....	3
Considerations of deploying Active Directory for new IdM initiatives .....	3
How to successfully deploy AD for new IdM initiatives.....	5
What is a Virtual Directory? .....	6
How virtual directory leverages your AD investment for IDM initiatives.....	8
Summary .....	11

## Introduction

This Paper discusses how virtual directory technology can help solve authentication and security challenges while keeping an existing AD infrastructure.

## Problem statement

AD faces a variety of challenges when deployed at IdM initiatives that are outside of the field AD was originally designed for.

## Current Situation

AD & ADAM can solve some of the problems, but for many IdM initiatives a virtual directory or a complete identity virtualization platform is needed.

## Radiant Logic Solution

RadiantOne™ provides a common virtualization layer that allows you to leverage what you already have in AD without having to stretch AD into areas it wasn't designed for.

- *Consolidating multiple AD Forests and Domains*
- *Schema extensions to Active Directory*
- *Delegated Authentication to Active Directory*



## Introduction

Microsoft Active Directory is an established NOS directory technology and most enterprises have made significant investments in their AD infrastructure. Many of these enterprises are now looking to further improve the user experience, reduce redundancy, and increase simplicity of directory management, by re-using the information currently stored in AD for new initiatives and applications.

In this paper, we will first discuss the challenges that can be encountered when deploying AD outside of the field it was originally designed for, before taking a closer look at how to leverage an existing AD infrastructure for new IdM initiatives. Finally, we will describe how to integrate identity information into a single virtual repository without disrupting the AD environment.

## Considerations of deploying Active Directory for new IdM initiatives

With significant user and group information stored in Active Directory, more and more identity and security initiatives can benefit from this information. Some examples of this increased demand for re-usability are:

- *Users who want to (re)-use their credentials for all their applications within the enterprise*
- *Security teams that want to take advantage of the group definitions that exist in AD*
- *Portal initiatives that require adding an organization's internal users (stored in AD) to the external directory of business partners and customers.*

In many cases, Active Directory Administrators are being asked to better leverage existing resources and make Active Directory an even more important aspect of an enterprise's identity infrastructure. But as with any component that is developed with a specific purpose in mind, questions about AD's ability to meet enterprise requirements remain.

- *How far can AD be used in an enterprise architecture?*
- *What are the risks associated with extending the use of AD beyond its original design?*
- *Where are the scalability and performance limits of AD?*

AD, like any stable information service, does have its own unique strengths and limitations. To better understand those limitations, let's take the scenarios described above and examine them more closely.



### **1. AD Design and Function**

First and foremost, Active Directory is a NOS-based system, and extending its use beyond this design can have serious consequences upon its core functionality. The loss of any functionality for even a few moments within your network could have significant ramifications to your business. In addition, issues of data ownership arise, as well as the fact that certain requirements are better served through the functionality of an RDBMS.

### **2. Active Directory In Application Mode (ADAM)**

Modification of AD profiles for application specific entitlements (and additional extended profiles) is not recommended due to performance, scalability, and stability issues but the need for this functionality can not be ignored.

To address some of these needs, Microsoft introduced ADAM (Active Directory Application Mode), allowing for additional attributes to extend existing AD entries.

ADAM runs as a non-operating-system service, and, as such, it does not require deployment on a domain controller, multiple instances of ADAM can run concurrently on a single server, and each instance can be configured independently.

This is a huge step forward in the use of AD identity data across the enterprise and ADAM certainly can be deployed to address some of the schema extension requirements of internal applications. But restrictions on schema construction, performance levels, the ability to scale the solution (limited due to replication issues), limited LDAP compliance, and accessibility issues still persist.

If your identity integration needs are exclusive within Microsoft branded bundles, ADAM addresses the limitations of AD perfectly and if configured properly will meet the needs of application entitlements and profiles.

### **3. Limited LDAP v3 compliance**

There are additional constraints which limit AD and ADAM's ability to provide robust LDAP services. This can be a serious consideration since, for instance, your portal project may require a single LDAP directory while your existing AD infrastructure is comprised of multiple AD domains and forests. On one hand, it would make sense to try and consolidate everything into a single Active Directory instance, but the reality is that there are historical and logistical reasons for having multiple forests and domains. Furthermore, consolidating into a single AD instance would still not address LDAP compliancy and performance issues.

LDAP is the preferred protocol around which directory services and most identity driven applications are designed to integrate with out-of-the-box, and LDAP v3 compliance should not be ignored if you want to avoid potential initiative deployment road-blocks. The addition of LDAP functionality by Microsoft in Windows NT 2000 is a clear indicator that LDAP is needed and confirmation of its wide spread adoption as the industry standard.



Obstacles in using AD and/or ADAM in various LDAP enabled projects, requiring high-availability, scalability and complete LDAP v3 compliance are (but not limited to) areas of:

- Schema
  - Attribute character length
  - Attribute Value Limits (1500) (i.e. group definitions)
  - Relative Distinguished Naming contexts
  - Schema structure in the use of OU (organizational unit)
  - Entry provisioning and reloading of directory data (LDIF use)
  - Objectclass and Attribute Definitions not RFC 4524, 2256 compliant
- Data Access
  - Anonymous binding not permitted
  - Access Controls – no extensible ACL framework
  - No support for regular expression attribute matching (search)
- Replication
  - Multi-master / scheduling parameters only
  - Scalability and planning (since replication must be established during installation only)
  - No multi-valued attribute conflict resolution, and no notification to the application
- Management
  - Port 135 requirement, security issues
  - LDAP operation logs not complete, compliance issues
  - No LDAP-based querying of operational statistics, monitoring issues
  - Operational attribute functionality (RFC 3673, 4512), compliance, policy and operational issues
  - Global *timelimit/sizelimit* settings and no support for user/group limits, possible “self-inflicted denial of service”, stability issues
- Performance
  - Indexing options
  - Caching options

After discussing the challenges that can be encountered when deploying AD outside of the field (and environment) it was originally designed for, let us take a look at how to leverage our existing AD infrastructure to fit the new IdM requirements.

## **How to successfully deploy AD for new IdM initiatives**

We have established the value of using Active Directory identity profiles. We also discussed the limitations of using AD and how ADAM helps address most of those issues. Now, let's look at some of the many additional use cases where AD and ADAM can benefit from virtualization.



Some of these use cases are:

- *Deployments requiring AD interoperability with other data repositories*
- *Multiple applications and services leveraging AD user credentials to provide; password synchronization, enforce business logic, managing large groups (greater than 1500 members), and authorization rights, all within traditional LDAP enabled applications.*
- *The need to search across multiple domain controllers and forests quickly and efficiently without establishing trust. (establishing trust enables unlimited search access across all domains and forests, this may create an unacceptable security risk and/or multiple compliance violations) .*
- *The creation of a unified view of fragmented identities across the enterprise. Identity profiles from AD and other data repositories need to be integrated to provide a complete view of users, without modification to AD schema or structure.*
- *The use of AD credentials on non-windows based platforms (operating systems)*

How can you overcome these and other limitations of AD and ADAM, while still leveraging your organization's existing Active Directory infrastructure?

It can be achieved by deploying a virtual directory solution. A virtual directory allows you to access the identity information stored in AD, integrate it with other data repositories, impose business logic, aggregate and manage large groups, and enable enterprise search, on a platform that is environment neutral.

## **What is a Virtual Directory?**

A virtual directory functions as an abstraction layer between applications and data repositories. By virtualizing the data sources, the virtual directory can present identity data in a multitude of views, allowing you to optimize identity data schemas to specific application clients. The identity information is accessed by the client via LDAP (or other industry standards).

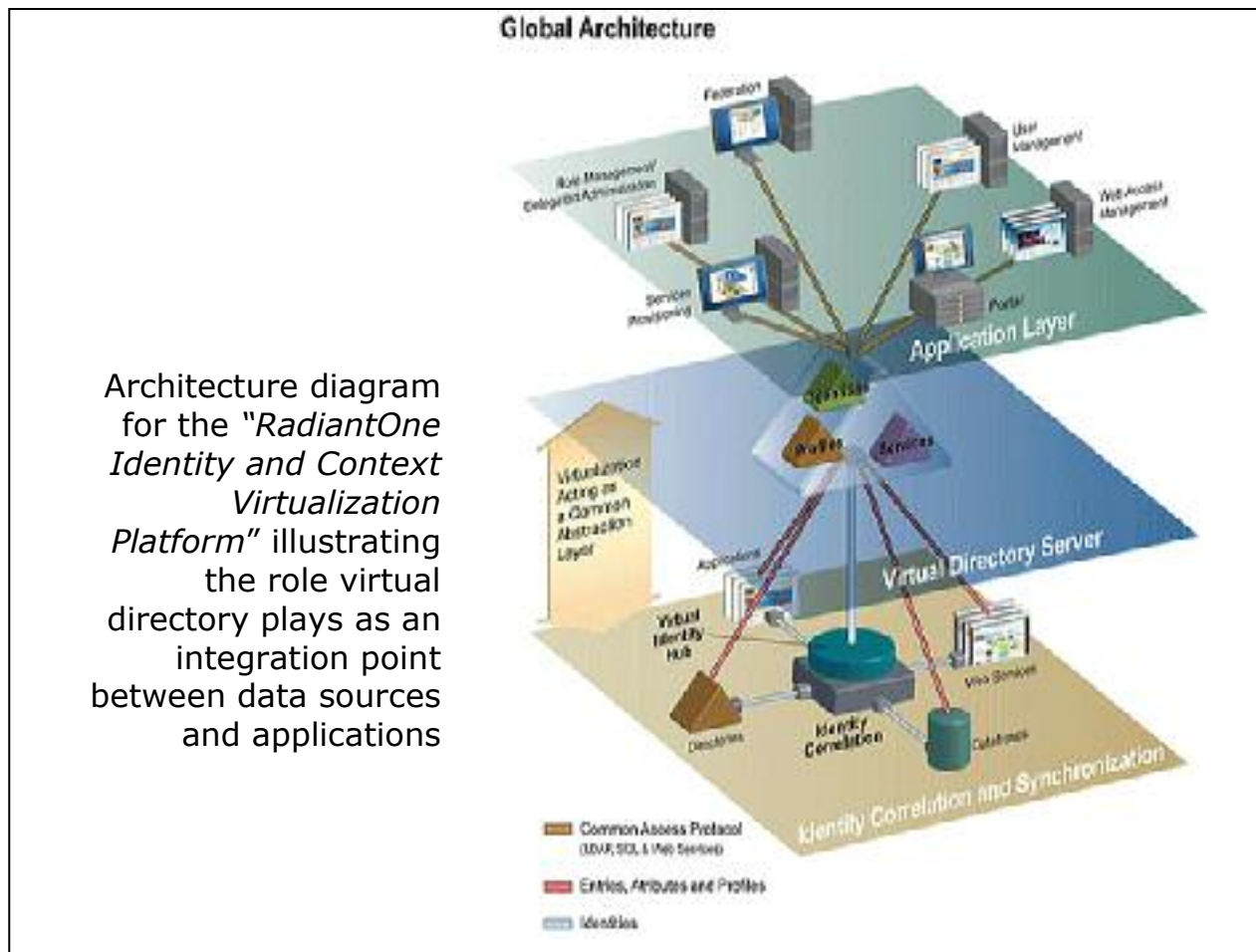
By virtualizing data sources into a common namespace and supporting multiple views of identity data, the virtual directory becomes more than a "one-size-fits-all" solution. VDS leverages an organization's existing infrastructure and radically simplifies the deployment of any identity management initiative without disrupting your organization's current applications and/or services.



Now you can:

- **Create customized views of Identity Data** can be created without disrupting existing integration points that are completely different from the underlying source.
- **Aggregate or Integrate Identity Data** from multiple data sources based on your current requirements and security concerns, including selected domain controllers, forests, or even branches within your existing AD infrastructure.
- **Access identity data a fully LDAP v3 compliant directory service.** Other Industry Standard Access Protocols can also be used to access the VDS such as HTTP, SOAP, DSML, XML, SPML, SAML, SQL.
- **Have guaranteed high availability and high speed** through the high performance, scalable, and fault resistant LDAP v3 directory service.

The virtual directory enables an identity infrastructure that will meet the ever changing requirements of an organization. Whether it is for internal or external users, the virtual directory is a single access point for IdM applications and service platforms.





## How virtual directory leverages your AD investment for IDM initiatives

The problems faced with identity integration are definitely numerous and diverse, but even greater are the rewards of creating an identity integration layer, a flexible identity infrastructure such as a virtual directory solution offers.

Virtual directory integrates extremely well with AD, offering performance, scalability, extendibility, and flexibility that is simply not possible using AD or ADAM alone. If your IdM needs will ever extend past Microsoft-based applications, and you still want to take advantage of the users, group definitions, and other valuable information within Active Directory, a Virtual Directory Server is a must.

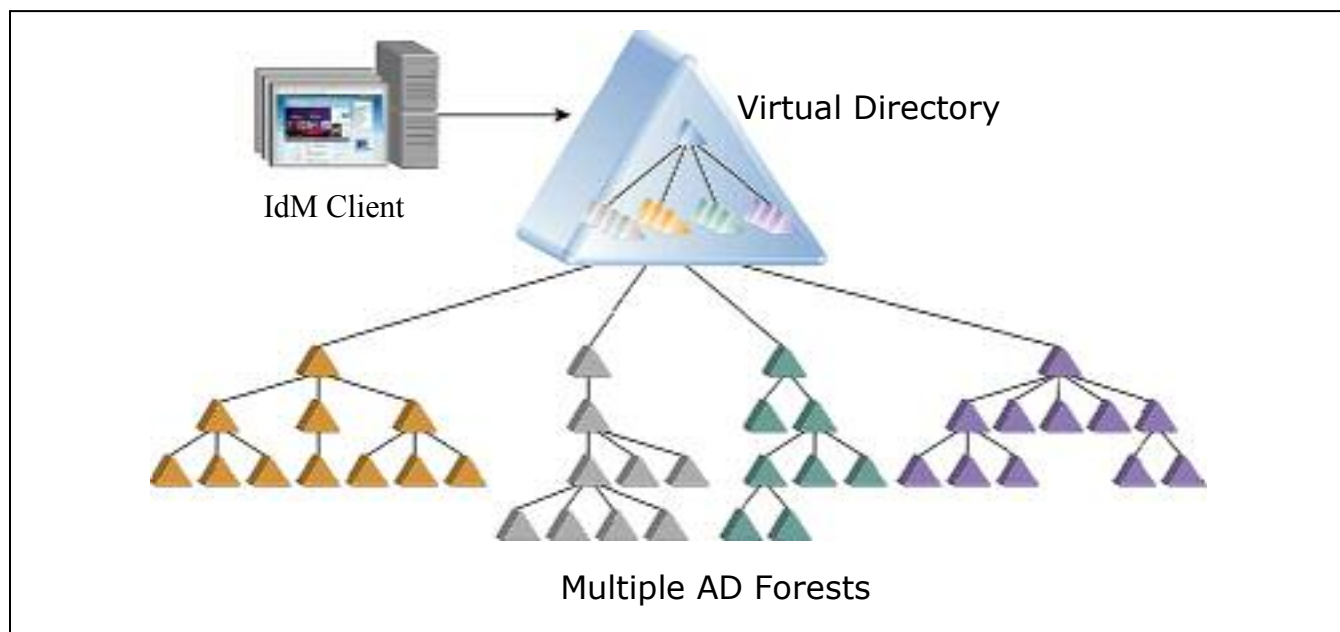
Let's look at some practical use-cases of how a virtual directory solution can take advantage of the great resources in Active Directory, without risk to its existing integration and structure.

### Consolidating multiple AD Forests and Domains

A virtual directory can allow you to keep your existing AD forests and domains while still enabling you to logically consolidate them into a single Directory Information Tree (DIT).

Often, it is impractical to establish trust between Active Directory trees, forests, and domain controllers for logistical, compliance, and other possible security concerns. It is also advantageous to be able to access individual branches, trees, forests, or any combination thereof for improved performance and to avoid unnecessary network traffic across multiple forests.

Virtual directory can consolidate Active Directory instances at any level into a common namespace for quick and easy access.



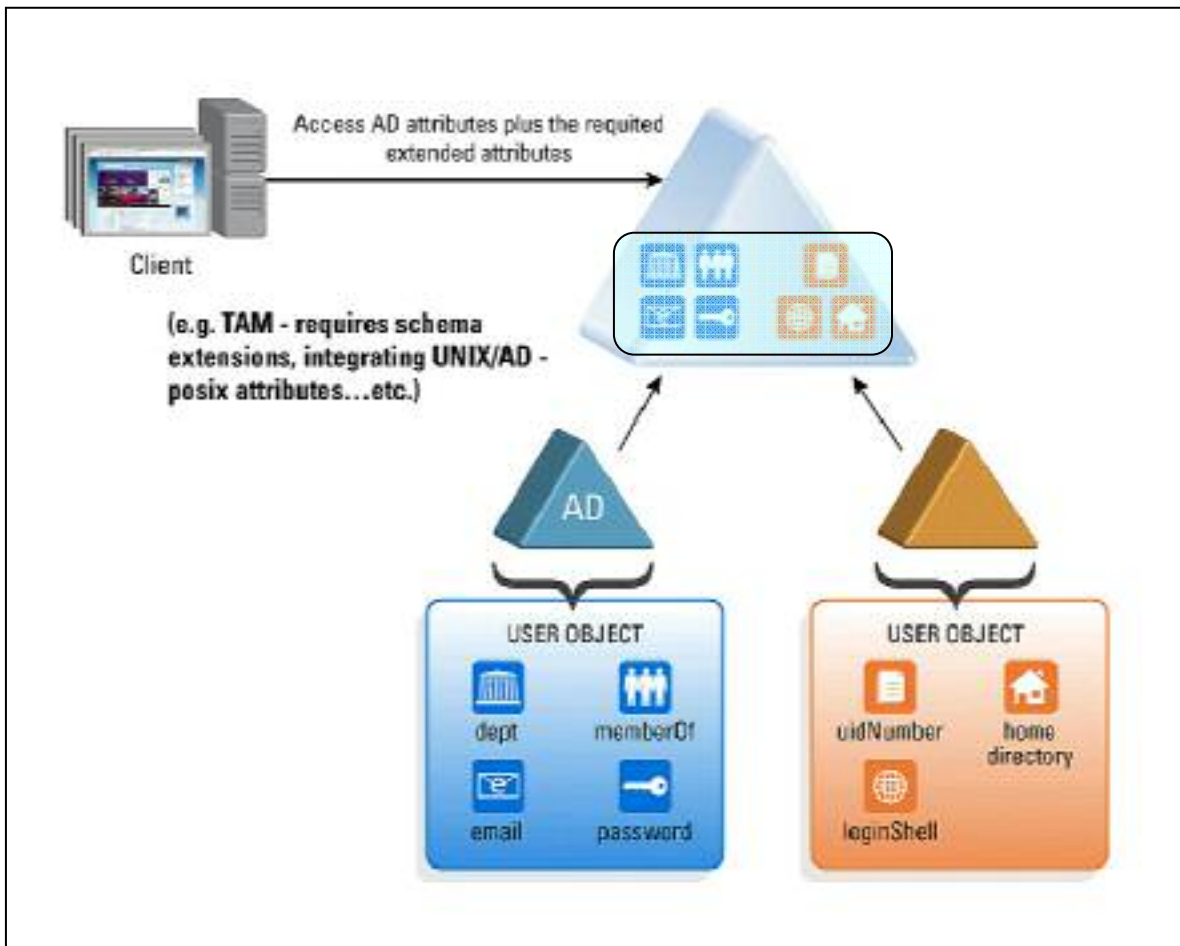
## Extending Active Directory Entries

Virtual directory can provide a unified view, or global profile of users. By keeping application specific objects and attributes in their existing sources, heavy synchronization is avoided and current identity integration points are not disrupted in any way.

Virtual directory can bring together objects, and individual attributes into a single view, from multiple data sources. You can view your AD user profile with information from an HR database, and combined with information from other directories, or web services. Now you can meet the needs of very customized identity views of data that is currently scattered across the enterprise, and make it available in a fully LDAP-compliant directory.

Even if the identities are not currently correlated, virtual directory can still create global profiles, with extended entries from multiple data sources, joined into a single user view. This type of functionality makes identity integration possible for even the largest enterprises.

Being able to extend AD user profiles with multiple non-Microsoft based data repositories allows more flexible and reliable identity information delivery, without disturbing Active Directory's primary function as the NOS directory.

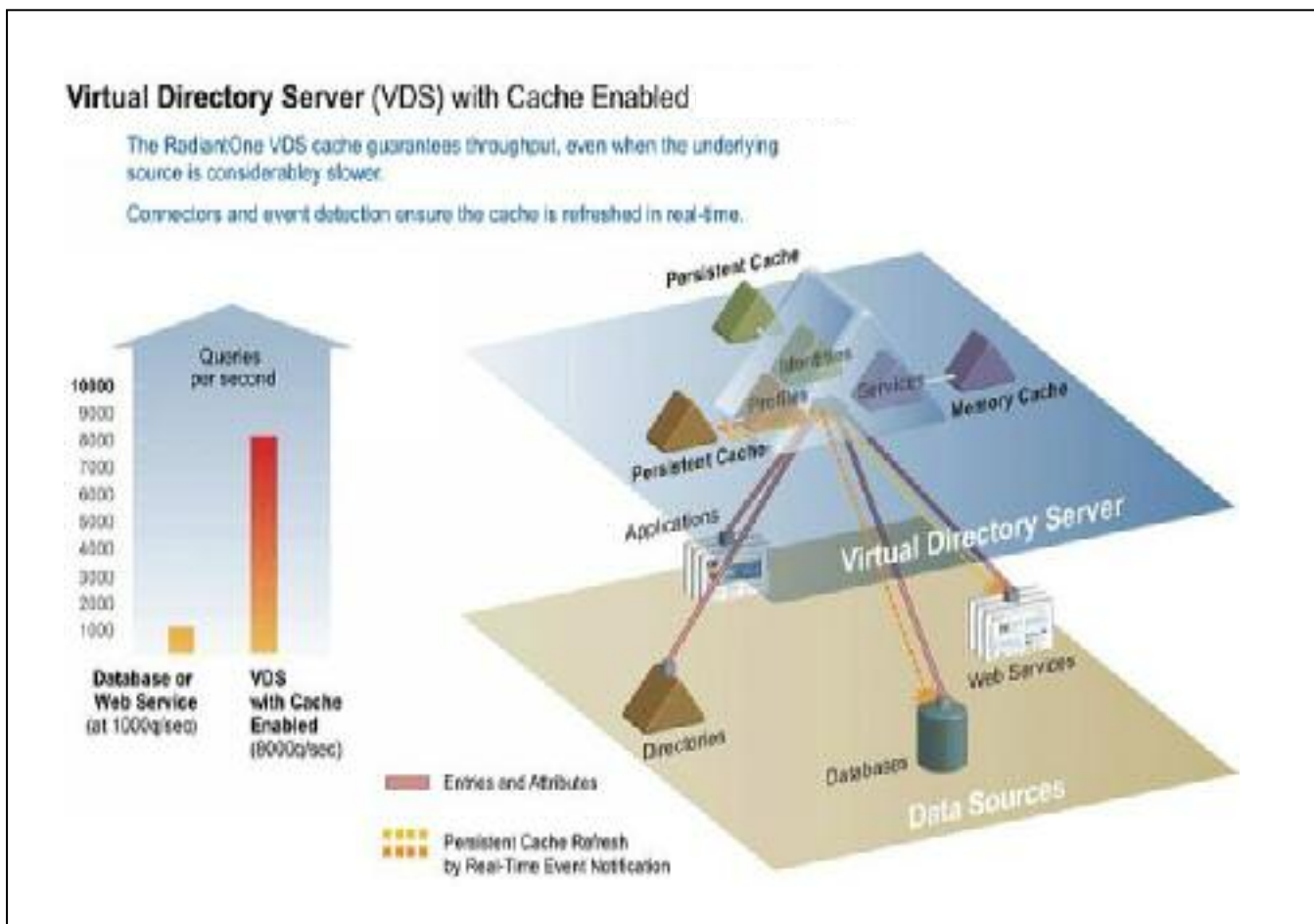


### Improving performance and availability and lowering AD load levels

Let us look at a more specific use case, authentication. We can break down authentication into two steps, the first is a search to find the user (identification) and the second is to verify the credentials.

The IdM application needs to issue a search on the user id across several directories. This search can be costly, and as new IdM initiatives are brought online, the need for a scalable solution is essential. By making use of virtual directory caching technology, search requests can be handled even faster than the underlying system could natively. Only the credentials need to be delegated back to Active Directory for a successful bind request. Network traffic and Active Directory load levels can be significantly lowered, 50% or more in some cases.

Multiple instances of VDS can be introduced with different levels of caching to provide a scalable solution for almost any level.





In the above diagram you can see that the underlying source is a database or web service. The native speed of the underlying source is 1000 queries per second (q/sec). The speed at the VDS level is 8000 q/sec. The underlying source could be even slower, and the speed of the VDS would be unaffected. In the case of Active Directory as the primary source of identity data, only delta updates to the cache and credentials would be consuming the resources of AD.

## Summary

There is no doubt about the viability and longevity of Active Directory in the enterprise. It only makes sense that we begin to examine ways to exploit and extend the use of this valuable resource without disturbing AD's native operations.

Virtualization extends AD's usefulness in a safe and effective manner. Virtual directory is an excellent tool to bring LDAP compliance, performance and scalability to AD, especially when there is a need to integrate AD and other data sources. Also, through virtual directory, AD has almost unlimited scalability possibilities since replication issues are solved through the LDAP compliance features of the VDS.



## About Radiant Logic, Inc

Radiant Logic, Inc. is the leading provider of virtual directory solutions for identity management and enterprise information integration. The RadiantOne™ Identity and Context Virtualization Platform is being utilized by Fortune 500 corporations to provide virtual access to any applications and data sources for authentication, authorization, profile and personalization data, for portals, and services provisioning for application integration projects.

Radiant Logic's solutions have been used to solve tough identity and data integration problems at companies around the world. Companies and organization such as British Petroleum, Comcast, Discover Financial, Disney, Defense Information Systems Agency, Federal Reserve Bank, Federal Home Loan Bank, Fifth Third Bank, Freddie Mac, Lexmark, Telecom Italia, Symantec, USAF and Time Warner Telecom use the RadiantOne™ solution to speed deployment, solve integration challenges and cut costs for identity management projects.

Partnerships with identity management software vendors- CA and RSA/EMC- along with professional services organizations- Accenture, Booz Allen Hamilton and Deloitte- demonstrate the broad impact of Identity and Context Virtualization on the market.

### Corporate Office

1682 Novato Blvd., Suite 300

Novato, CA. 94947

Phone: 415.209.6800

Fax: 415.892.7085

E-Mail: [info@radiantlogic.com](mailto:info@radiantlogic.com)

© 2008 Radiant Logic, Inc. All rights reserved.

