Toward a Federated Identity Service Based on Virtualization

A Buyer's Guide to Identity Integration Solutions, from Meta and Virtual Directories to a Federated Identity Service Based on Virtualization
# Table of Contents

**INTRODUCTION** .......................................................................................................................... 3  
  Today's IAM: The New Urgency for a More Agile Identity ................................................................. 3

**THE RISE OF FEDERATION STANDARDS: SOLVING THE ISSUE OF ACCESS** .............................................. 4  
  An Excellent Solution to the Access Problem .................................................................................... 4
  …That Doesn’t Solve the Underlying Identity Integration Issues .......................................................... 5
  An Identity Hub to Support the IdP: Why You Need a Federated Identity Service .............................. 5
  Implementing the Enterprise Identity Provider ................................................................................... 6
  The Need to Consolidate and Rationalize Identity and Profiles Across Silos ...................................... 6
  Cracking the Code of Identity Integration: A Quick Review of Challenges and Solutions .................. 6

**BEYOND META AND VIRTUAL: A FEDERATED IDENTITY SYSTEM BASED ON VIRTUALIZATION** ......................... 7  
  Federating Identity: A Proven Pattern for Integration ........................................................................ 7
  Protect Your Investments and Future-Proof Your Infrastructure with RadiantOne ............................. 8
  Key Components of a Federated Identity Service ............................................................................. 9

**USE CASES FOR THE RADIANTONE FEDERATED IDENTITY SYSTEM** ................................................................... 10
Introduction

The world of identity and access management is expanding in all dimensions, with more users, more applications, more devices, and more diversity—and these multi-faceted demands are stretching the current landscape of IAM for most organizations and enterprises.

The adoption of federation standards, such as SAML 2.0, OpenID Connect, and OAuth 2.0, promises a new way to combat rising complexity. However, the successful adoption of these technologies also requires a rationalization and consolidation of the identity infrastructure, which, for most sizable enterprises, is highly fragmented across multiple identity silos. While federation standards can bring secure and orderly access to the doors of the enterprise, organizations will still need a way to unlock those doors into their complex and often messy identity infrastructures.

To ensure security these days, the entire diverse and distributed enterprise identity infrastructure must become one secure global service. A federated identity service based on virtualization is the answer for protecting today's increasingly federated environments—and evolving them to meet future demands and opportunities. In this paper, we'll look at how such a service helps you manage all this complexity and see how other solutions stack up.

Today's IAM: The New Urgency for a More Agile Identity

With new applications on the web and in the cloud to enable, your security is stretching far beyond the borders of your enterprise. At the same time, new user populations are accessing these applications, from employees to contractors, customers, partners, and more. And the types of devices used to access these apps are exploding as well, with users tapping in from anywhere in the world, using mobile devices both corporate and personal. The days when your largest concern was employees accessing internal resources from their desks using their company computers are over.

All this points to one massive access and identity integration problem with multifaceted dimensions within an increasingly far-flung, heterogeneous environment. If you dive into the details of most web, portal, and cloud access deployments, you see a pattern of complex, hard-coded point-to-point connections that are expensive to deploy, inflexible to maintain, and difficult to evolve.
Today’s identity infrastructures face the traditional challenge of multiple links to multiple sources and targets. This creates an unmanageable “n-squared” problem, where there are too many custom links, each one extremely expensive to manage.

The Rise of Federation Standards: Solving the Issue of Access

The good news is that as identity environments become more complex, we have also seen the adoption of Federation standards, such as SAML 2.0, OpenID Connect, and OAuth 2.0, designed to better manage security and address complexity. In this architecture, the application can focus on delivering its core services, while delegating authentication and attribute management to a third party. Essentially, federation architecture divides application security into two roles:

- **The service provider** (SP), which provides the functionality of the application, on the web, internet, or cloud. The SP controls the access to the resource, but delegates authentication, groups, and attribute management to a trusted external identity source, namely…

- **The identity provider** (IdP), which manages its own identities and profiles, providing them with access to the universe of new applications.

The end goal is to increase security, flexibility, and end user experience with seamless SSO—let’s look at how that’s working in practice.

An Excellent Solution to the Access Problem…

The promise of federation is to separate out the identity management tasks—the job of the IdP—from the application, the SP. First, let’s consider the SP at work. On the first request from a user to access a protected page or service, the service provider delegates the request for authentication and any additional attributes required by that application logic to an agreed-upon identity provider. So far, so good.

Now imagine that we have n different service providers, all routing access requests for authentication and attributes to a common identity provider. This action is how SSO is delivered via federation, and it’s a key value for a federation of applications. And the beauty of this mechanism is that it’s well-supported by industry standards and many excellent SPs or companies.

Federation cuts through the confusion of multiple applications making access requests to multiple identity sources—and it separates the ownership of the service from management of the identity. So it should be no surprise that amid the barrage of new apps, new populations, and new devices, the whole IT world is heading toward a large-scale adoption of federation.
…That Doesn’t Solve the Underlying Identity Integration Issues

However, as implementations are spreading, we’re seeing another part of the architecture becoming a serious impediment to success. While solving the issue of having to federate access, the federation architecture is putting new pressure on organizations and enterprises that now need to assume the role of identity provider. For most sizable current deployments, this means dealing with a large number of heterogeneous and distributed identity silos—AD & LDAP directories, databases, APIs—each with its own authentication method and specific identity representation.

In order to present a global view of identity and attributes to the federation access layer, they must broker authentication and identity attributes from across their multiple internal identity systems. And that’s no mean feat, given all the complexity within the infrastructure.

Multiply this by all the applications you need to support, and you’ll begin to see the difficulty that companies face today. For every application, the IdP must find the user profile in your diverse infrastructure, authenticate them, and gather relevant attributes—then package this information in the specific format required by that application, because even though tokens might be expressed using the same standard, each application expects its own flavor of SAML or OAuth.

An Identity Hub to Support the IdP: Why You Need a Federated Identity Service

Just as planes don’t fly from every location to every other location, you shouldn’t have to route every authentication and access request through all your backend stores. No distributed, heterogeneous system can integrate identities on the fly like that. After all, there’s a reason that federation standards focus the authentication requests to one or a limited number of IDPs—because hubs make routing easier and more efficient.

Airlines have established hub cities to route flyers more efficiently, and your identity infrastructure needs the same smart structure to better fulfill its role as IdP. But establishing a hub means more than responding to SP requests and providing a secure token service, it requires that you have a global view of your identity that’s fully rationalized across all sources—an agile and responsive identity that can be accessed, remapped, and adapted quickly.

In short, that means a layer of identity integration.
Implementing the Enterprise Identity Provider

Although it’s grown more complex, this problem of identity integration is not new. As soon as you have multiple applications, where you need to grant access to resources based on the identity or roles of a person, program, or agent—you need a way to provide a list of those identities, along with their credentials and attributes, to support authentication and authorization.

Initially, most applications internalized identity information, managing this list on their own. But while different applications exist to serve different needs, the population of users is generally common—or shared across many common sub-groups—between applications. As applications multiplied, so grew the need to externalize these identities and attributes outside of the specific scope of a given application. It became clear that identity should be managed as a common shared service, and the idea of the common repository, a directory, along with the related services to keep such a system up-to-date, was born.

The Need to Consolidate and Rationalize Identity and Profiles Across Silos

The specialization that makes an application efficient and useful also tends to create an information silo. When a given application manages its own list of identities, it will generally enrich this identity profile with attributes that are characteristic of that application. So an HR application will enrich a generic employee profile with attributes that are specific to the HR realm, while a sales automation tool will enrich a customer profile with information collected during the sales process. Of course, some of those aspects will be useful only to each application, while others are critical to share across the organization.

As applications multiply, relevant identity information spreads everywhere. But because some of that information is shared, the requirement of synchronizing these different identity images managed by given applications gave rise to multiple “synchronization” processes. So even if externalizing identity from an application into a directory is a step in the right direction, without support for additional services, this approach only adds to the problem, instead of solving it.

As we saw in the \( n \)-squared diagram on page 4, in a system already saddled with multiple point-to-point-links (many painstakingly hard-coded and difficult to evolve), we are only compounding the complexity with new nodes and new links. Point-to-point integration, where the identity information is consolidated into a single store, is fine in small doses, but doesn’t scale well as you add more sources.

Cracking the Code of Identity Integration: A Quick Review of Challenges and Solutions

In light of these issues, one potential solution is to create a central repository that acts as an identity hub. This idea evolved into the enterprise directory, which gave us a centralized view of identity, but also proved to be inflexible. It was theorized that such a collection of information about identity would act as an “omniscient” process—an “application of all applications.” In reality, however, the sort of generic information that could be collected and managed centrally amounted to a very bland profile and negated the value and contributions of specialized applications. After all, they may be silos, but they’re full of rich and relevant attributes.

The metadirectory was designed to address this inflexibility, creating an abstract integration and synchronization layer to aggregate all the identity directories. Metadirectories were a big step forward, faster and much easier to update than the traditional enterprise directory. But they weren’t quite “meta” enough to solve the ongoing issue of identity integration. Metadirectories were complicated to deploy, support, and upgrade, because the amount of abstraction was not enough to automate processes, turning identity architects into programmers instead of power users. Without a clear data model, or the tools to reverse-engineer the data models behind existing sources, the system cannot abstract away the complexity of the synchronization process and still requires too much scripting or lightweight programming.

In an effort to avoid the synchronization issues of the metadirectory, Radiant Logic invented the virtual directory. While this agile abstraction layer was easier to use and deploy, it also requires multiple hits on the underlying identity stores, making it only as fast as its slowest source. With the virtual directory, you trade the performance of the metadirectory for the flexibility and simplicity of virtualization. But while this simplicity enables the deployment of more use cases and adds value to your identity, these performance issues mean the virtual directory alone can never be a strategic piece of your identity infrastructure.
Beyond Meta and Virtual: A Federated Identity System Based on Virtualization

What you need is a way to combine the best of meta and virtual directories, for a 360-degree view of identity. Such a solution:

▲ Integrates and federates your identity sources into a common hub.
▲ Brokers authentication for your portal, federations, and applications.
▲ Delivers attributes and rich profiles for smarter security policies.
▲ Migrates and modernizes your aging directory infrastructure.

So how does such a system work? First, we must federate identity in order to integrate it.

Federating Identity: A Proven Pattern for Integration

We have seen that the main challenge is to integrate identity and deliver it as a global/shared service that many applications can use for their authentication and authorization needs. We know that centralizing data into an authoritative store makes for an inflexible and difficult to evolve identity infrastructure. And we know that while the partially-abstracted directory service supported by metadirectories offers good performance and synchronization, it’s still too complex to deploy, too inflexible to update, and too centralized in its synchronization of credentials.

But by applying a pattern—federation—that has shown success across two different domains that are relevant to identity and data management, we are building on more solid ground.

In the domain of security, we’ve already seen that by funneling authentication requests for multiple service providers through standards such as SAML 2.0 and OpenID Connect, we can “federate access” around identity providers. Notice here that the redirection of the calls and the support of an identity provider are greatly simplified by the adoption of a common authentication method—standards-based tokens.

And in the world of the data management and distributed databases, a federated database—which is often deployed as a hub and leverages “data virtualization”—pulls images and rationalizes them from across distributed sources, each of them staying authoritative for some specialized aspects of the data but contributing to the global system.

Sounds familiar, right? In fact, this looks a lot like the way our federated identity system works:
So the pattern for identity integration is to use a federated architecture where identity is federated from across diverse data stores, each with its own way of describing identity. This is accomplished through advanced identity virtualization. As the world of identity has grown increasingly complex, we’ve been evolving the virtual directory to meet new requirements. The process of virtualization has taught us how to translate diverse protocols, creating a smart abstraction layer that acts as a *lingua franca*, a way to represent very different identity systems in a unified world. This common representation or “data model”—allows us to automate the synchronization process, delivering the best of a “meta-virtual” directory: a federated system that is always in sync—automatically.

**Protect Your Investments and Future-Proof Your Infrastructure with RadiantOne**

Based on sophisticated virtualization, RadiantOne federates, transforms, and rationalizes identity from diverse sources across the enterprise. The end result is an **identity hub acting as an authoritative source for all user identities**, along with attribute-rich profiles for **every user** drawn from multiple application silos. This information is delivered through customized views, designed to meet the needs of applications, whether they’re in the enterprise, on the web, or in the cloud. These views are stored in **HDAP**, a highly available, highly scalable LDAP directory based on big data technology, and kept in sync with the local identity sources.

RadiantOne complements existing identity infrastructure investments and provides a flexible solution for the rationalization and integration of identities across existing silos, as well as newly merged or acquired organizations. Instead of blindly synchronizing identities and attributes across all of the different systems in a never-ending process of point-to-point synchronizations, the federated identity service provides multiple views of the identity information stored across these systems, in exactly the format and protocol that each specific application can easily consume—without any customization or changes.

While RadiantOne is useful at any point in the project lifecycle, it’s particularly helpful to **implement this data integration and synchronization layer first**, unifying the fragmented infrastructure and creating the unique user profiles that drive IAM projects. Having **RadiantOne in your environment speeds future deployments and ensures success across many essential initiatives**, including WAM/portal, cloud, federation, ABAC, mergers and acquisitions, and directory migration and modernization.
The advantages of a federated identity service include:

- **Quick deployments**: Configure, don’t hard-code—RadiantOne makes it easy to deploy even the most complex applications, delivering identity data from multiple sources, without costly customization or complex synchronization.

- **Global view**: Get a single, rationalized view of your identity without violating internal or external regulations governing identity data—or needlessly centralizing that data.

- **Seamless evolution**: Expand your portal security to keep up with new demands, while leveraging existing investments and taking advantage of high-availability for authoritative data stores.

- **Richer data**: Give your applications the exact views of identity they need, without slowing your system or having to develop a master enterprise schema.

- **Automatic updates**: Changes made in authoritative sources are reflected in real-time in the identity hub, thanks to RadiantOne’s smart synchronization.

- **Elastic scalability**: Radically scale your access and throughput, using HDAP, the first highly scalable and secure directory that’s based on big data and search technology.

- **Safer system**: Identity firewalls provides only one opening to the outside world, preventing denial of service attacks on primary data stores and providing further security to sensitive data inside the enterprise.

### Key Components of a Federated Identity Service

<table>
<thead>
<tr>
<th>Categories</th>
<th>Features and Capabilities/Characteristics</th>
<th>Virtual Directories</th>
<th>Metadirectories</th>
<th>FID based on virtualization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metadata, Information Representation, Context, and Semantic</td>
<td>Get complete schema remapping, common data model, and reverse engineering of objects and relationships.</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Perform data mapping and translation for simple objects.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Discover and extract metadata from each source and map this information to a common naming.</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Use simple aggregation to create a complete list of identities where there’s no user overlap.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Integrate identities to build a unique list, correlating identities where user overlap exists, even without an existing global identifier.</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Build trees which expose semantic relationships between identities and their resources.</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Enable keyword search and contextual, semantically expressed data across the identity infrastructure.</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Data Quality, Integration, and Application-Specific Views of Identity</td>
<td>Handle complex joins to create global profiles, for fine-grained authorization and smart IdP.</td>
<td>Partial</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Dynamic groups: Create flexible group definitions and automatically-generated groups based on attributes.</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Create a flexible namespace allowing each application to have its own hierarchy and view of the data.</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Restructure existing LDAP trees as new application views.</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Easily extend views to reach additional backends or modify views to meet new requirements.</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Authentication Proxying and Routing</td>
<td>Proxy/route authentication requests to the appropriate identity source.</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Handle different security protocols and credentials checking mechanisms.</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Synchronization: Information Propagation and Update</td>
<td>Enjoy easy to deploy point-and-click synchronization, with minimal scripting/custom coding.</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Storage, Performance, and High Availability</td>
<td>Persistent cache equipped with real-time synchronization that guarantees data integrity of authoritative sources.</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Full LDAP v3 directory storage, based on big data technology for highest performance, availability, and scalability.</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Use Cases for the RadiantOne Federated Identity System

Drive Your Web Access Management/Portal, Cloud, Federation, M&A, ABAC, and Directory Migration and Modernization Projects with RadiantOne

RadiantOne integrates identity from across heterogeneous sources, providing a rationalized view of all your identity, no matter where or how it’s stored. By federating identity into a common “identity hub,” you can rise above complexity and deliver the very specific views of identity required by any application, whether it’s hosted at your enterprise, on the web, in the cloud—or even accessed via mobile devices. Because these views are data-intensive beyond the narrow scope of the traditional virtual directory, you also need a new way to store this information. Our RadiantOne federated identity system features HDAP, the world’s first high-availability directory built on big data standards. Thanks to its cluster computing architectures, HDAP scales easily to hundreds of millions of users and highly complex queries.

With RadiantOne, you can:

**Authenticate Users:**
- Create a global list of all identities, where every user is represented once and credential checking is delegated back to each authoritative source.
- Broker authentication across diverse internal user stores—including LDAP, AD, SQL, and web services—for any WAM/portal, cloud, or mobile applications.

**Authorize Access:**
- Build a complete global profile for each user that’s referenced locally, with attributes coming from across your heterogeneous infrastructure.
- Build attribute-driven dynamic groups to easily enable a world of new services—and drive attribute-based access control (ABAC) policies.
- Manage context for finer-grained authorization, delivering a coherent view of attributes through advanced virtualization and joins.

**Extend Your Security Infrastructure:**
- Integrate new populations and applications, for a single view of user data. With RadiantOne, integrating data stores from mergers and acquisitions take minutes instead of months.
- Externalize identity out of the data silos, such as databases and directories.
- Expand your portal and WAM solution without the risk, hassle, and expense of complex synchronizations and hard-coded identity integration.
- Project identities safely beyond the firewall, without exposing them to unnecessary risks.

**Modernize Your Directory Infrastructure:**
- Unify user directories across AD and LDAP, resolving disparate user representations, naming conventions, and security means, while delivering a single view of users out of diverse infrastructures and providing a complete profile of every user with all the attributes needed for authorization and policy enforcement.
- Evolve an aging LDAP infrastructure without impacting your existing applications, using RadiantOne as an easily deployed in-place replacement with plug-and-play capability.
- Better leverage Active Directory by consolidating forests and domains, extending AD schemas, delegating authentication to AD, and even enabling Windows Azure Active Directory to extend SSO to Microsoft 365 and other cloud apps using AD credentials.