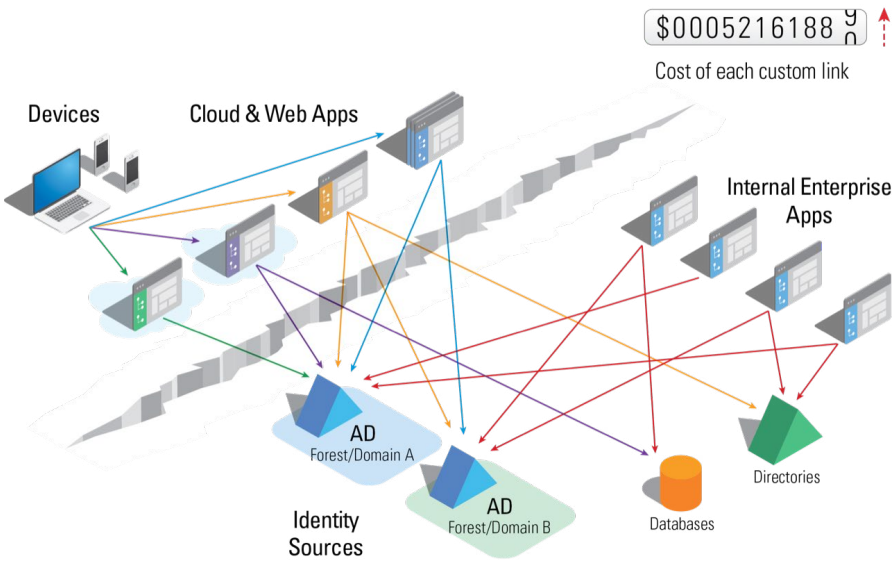
gamechanger Game Changing Technology for Unified Identity in the Cloud

Supporting and Simplifying Secure Cloud Access and Provisioning with a Federated Identity and Directory Service

A federated identity and directory service based on virtualization *integrates and normalizes all identity data into one unified identity service accessible through different protocols (LDAP, REST, SQL). The result is an identity "hub and spokes" architecture that delivers a unified view of identity for securing and simplifying access to cloud applications and web services, along with the ability to synchronize with Azure AD and/or other identity/directory hosts on AWS.*

Large enterprises face many challenges in Identity and Access Management to create the conditions necessary for secure and seamless access (and progressive migration) to the cloud. This is because over time, most large enterprises and organizations end up with an identity infrastructure that can contain multiple AD domains and even multiple forests, along with other non-Microsoft sources of identity data (other LDAP directories, SQL databases, APIs).



A fragmented, distributed identity system is a major challenge facing enterprises today.

Complications can arise with the distributed nature of the business (for example retailers or organizations with multiple regional points of distribution), or when mergers and acquisitions and seasonal fluctuations in staffing require adding new populations or reorganizing existing ones. This identity management process is complex, can be costly and time-consuming, and can require extensive customization. Combine that with the increasing adoption of the cloud for both popular applications such as Office 365, and for computation and data storage, and the need for a unified approach for access and identity becomes even greater.

Companies are moving toward a consolidated identity and directory model to achieve the goals of:

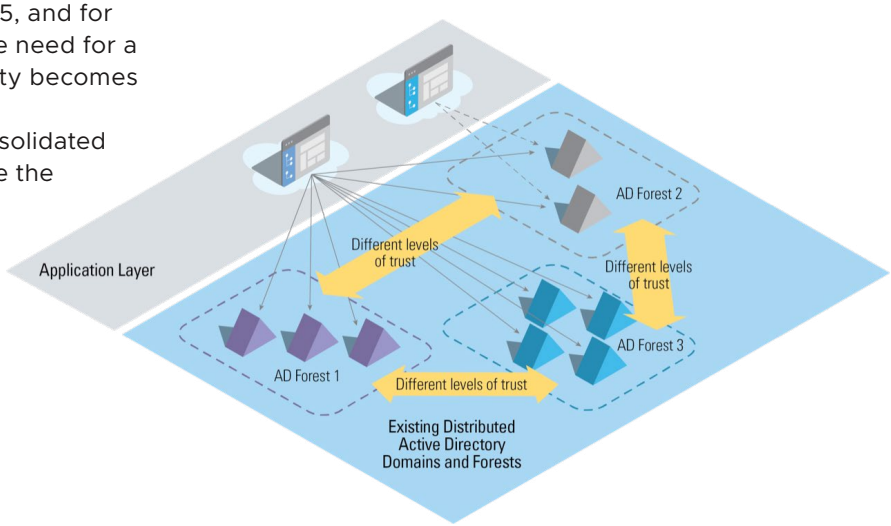
- improved security
- simplified management
- cost reduction (avoiding high maintenance/support/licenses)
- regulatory compliance
- migration to the cloud

FEDERATING ACCESS IS ONLY PART OF THE EQUATION

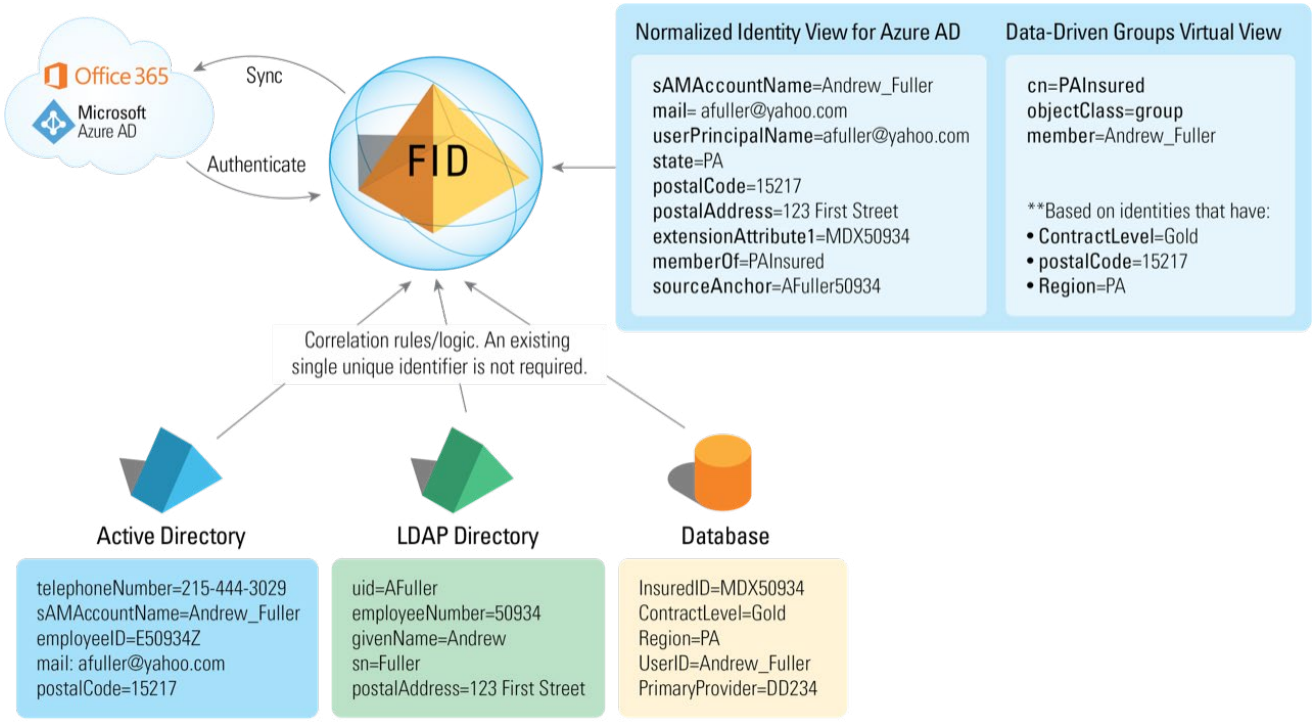
To simplify access to the cloud, many organizations turn to federated single sign-on offerings (such as ADFS, Okta, Ping, etc.), but these solutions only address the access side of the equation. Popular Identity Providers (IdPs) aren't designed to sort through issues with your data, such as overlapping users spread across multiple heterogeneous sources. Most large organizations have identity data stored in a number of places, from Active Directory domains, to Oracle/SUN directories, to SQL databases.

In addition, organizations will have to reconcile the requirements of maintaining the on-premises system while integrating with and extending to the cloud-based environment. And for large enterprises with extensive investment in on-premises identity and a multitude of user populations and applications, this task will take a while. Before they can move to the cloud, enterprises will likely be in a transition "hybrid" state that involves managing access to both on-premises and cloud-based applications.

Reducing the complexity of the directory environment by consolidating AD forests and



The AD world for many large and medium enterprises is a fragmented one of forests and domains.



RadiantOne federated identity and directory service provides a reference list to sync to Office 365.

domains can increase efficiency, reduce the cost of administration, and reduce the number of servers needed as well as the associated data center capacity. Microsoft's recommended approach for moving to the cloud is to consolidate AD domains/forests, but AD consolidation using existing tools is a complicated process that does not yield complete identity data integration.

ADDRESSING THE CHALLENGES IN THE CURRENT DEPLOYMENT OF AD

Setting aside the cloud issues for a moment, today's enterprises have already stretched the use of AD beyond the traditional LAN-based deployments for which it was designed. This growth of domains and forests has left many companies with complex thickets of on-premises identity sources that are difficult to maintain or evolve.

For many internal applications, AD should be the authoritative source of all employee data, that single unified list that drives security and access. Unfortunately, achieving this global view of identity is difficult due to fragmentation across multiple domains and forests—and configuring internal applications to chase those different directories is a huge challenge.

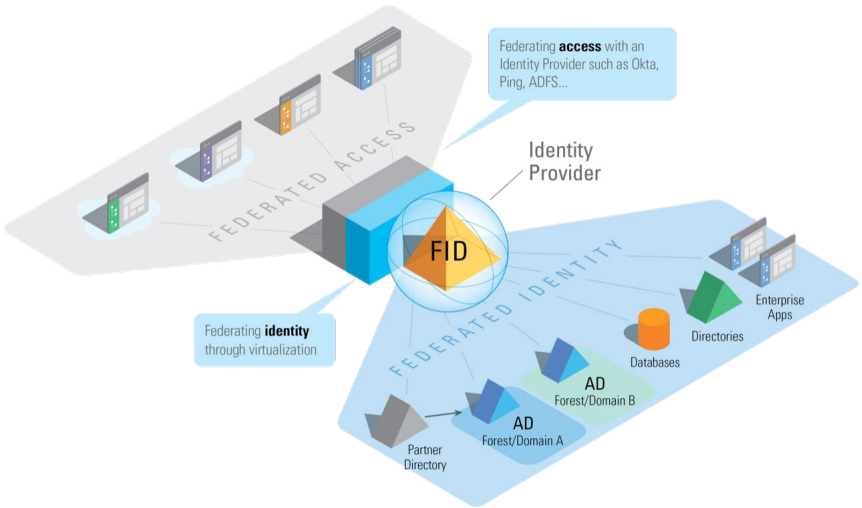
CONSOLIDATING YOUR IDENTITY TO REACH THE CLOUD

Large enterprises deal with many issues when trying to consolidate AD into a single domain, such as rationalizing duplicate accounts and group names, dealing with untrusted AD forests after M&As, and integrating Azure AD Connect across multiple forests. You could use Identity Manager to flatten the existing list of entries, but the need for complex sync logic and connections grows with the number of domains. This is not a comprehensive or scalable solution to the identity integration challenge.

And because Azure AD requires a flat list of users without duplicates, so many companies attempt complex workarounds to create this global list. AD is also only one front in the identity infrastructure, which includes legacy LDAP apps, or attributes/groups information in SQL or APIs. You need a layer that can rationalize and consolidate all your sources of identity—not just AD.

CREATING A CONSOLIDATED VIEW BY FEDERATING IDENTITY— NOT JUST CENTRALIZING IT

The best way to create this global list—and streamline your infrastructure, feed ADFS, and



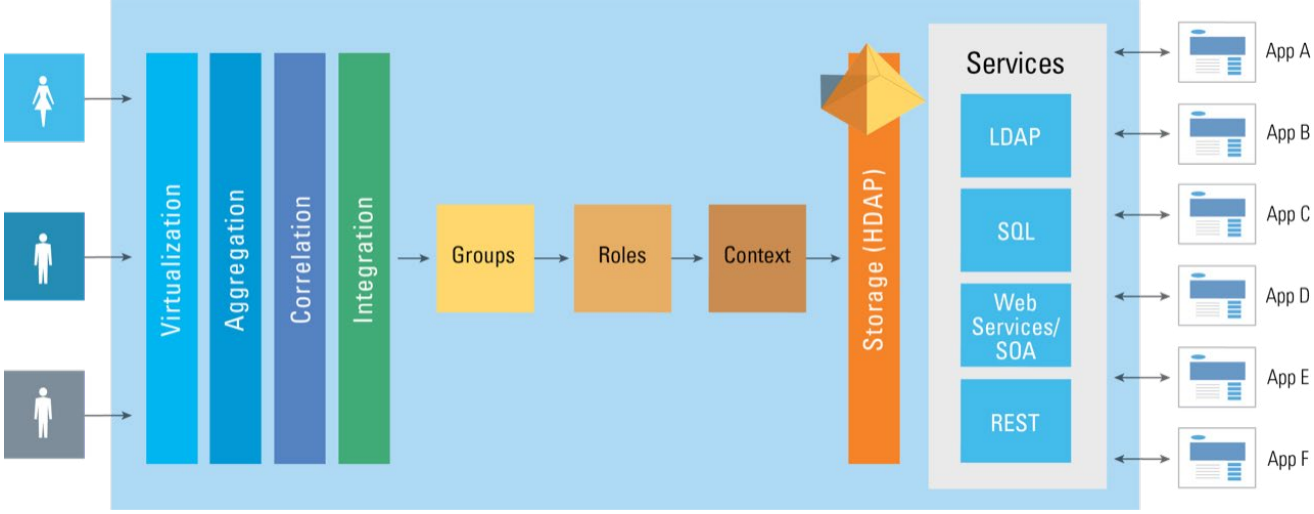
A better approach for federation and access: A consolidated, federated view(s) of identity based on virtualization.

provision SaaS apps—is to use a federated identity and directory service, such as RadiantOne FID from Radiant Logic. A federated identity and directory service uses the power of virtualization to create a global list of users where every user is represented once, as well as complete global profiles drawn from all your identity sources, from AD to LDAP, SQL, and web services.

A federated identity and directory service has two parts: a virtualization layer and a directory service. The virtualization layer integrates identity data for each user from all the disparate data sources into a complete authoritative source, enabling a global view of identities that can be modeled to meet the needs of any application at will. The virtualization layer makes it easy to inventory and intercept existing client application requests, and "reverse engineer" the views that will be required to meet the needs of those existing applications.

The storage layer, HDAP, is a highly-available version of LDAP that offers better performance and increased scalability. These two layers together make a complete identity service that enables you to:

- Get the right list of identities and groups into Office 365 and all your other apps, no matter where they're hosted.
- Authenticate users to the correct authoritative identity data store and authorize access using attributes drawn from your AD infrastructure and beyond.
- Create a reference image for quickly provisioning SaaS apps, then feed ADFS exactly the information it needs to authenticate and authorize users in the cloud.
- Add flexibility to your identity infrastructure and save time and money onboarding new apps, integrating M&As, and accessing the cloud.



Acting as an abstraction layer between applications and the underlying identity silos, virtualization isolates applications from the complexity of back-ends.

BUILDING A VIRTUALIZED IDENTITY HUB

At its foundational level, a federated identity and directory service is designed to address the challenges of authentication and authorization in on-prem, hybrid, and cloud-based environments. It can:

1. Inventory data sources: Discover and extract the metadata from each source and map this information to a common naming. Model-driven virtualization is what enables the service to integrate identity and create multiple views of your infrastructure.

2. Integrate identity to create a global list of users: The service creates a global unique reference list, where each user from across the identity infrastructure is represented once and only once, using aggregation, simple correlation, or even advanced correlation logic.

3. Manage diverse credentials checking mechanisms: The service stores this global unique reference list, allowing fast lookups to identify users and retrieve groups and profile information, while still delegating credentials checking to the authoritative backend data sources when needed.

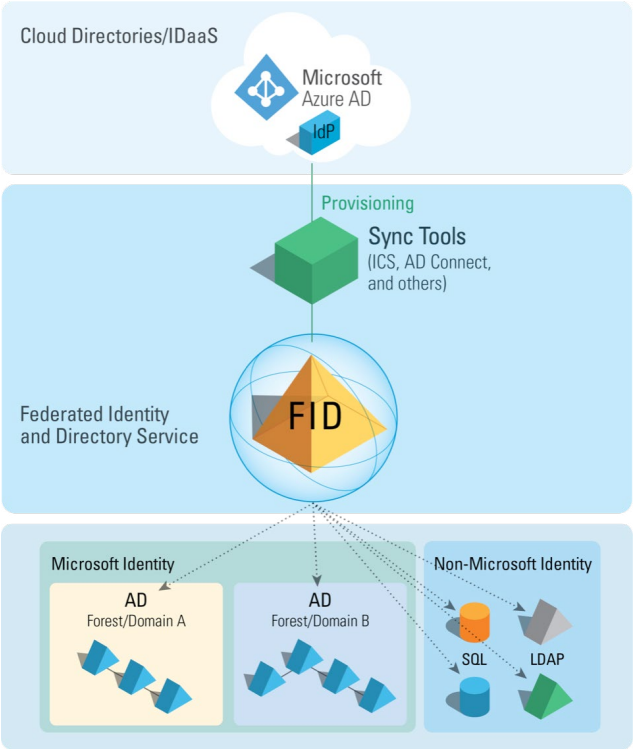
4. Build global profiles: Manage complex joins across diverse data sources— including AD, LDAP, SQL, and web services—for complete user profiles that applications can use for authorization. These profiles can form the reference image to be provisioned and synced to cloud applications.

5. Create flexible group definitions: Often, applications use groups to authorize access—but most groups are managed manually, leading to management headaches and security risks. The service builds dynamic, attributes-based groups to enable much more flexible authorization at the identity layer.

6. Create custom-tailored virtual views: Build a flexible namespace to give each application the precise data it needs—in exactly the format it requires. It's easy to extend views to additional backends for faster application onboarding, or change views to meet new requirements.

7. Cache data for speed and scalability: The materialized view from across all your domains and forests—along with every other attribute source—can be stored as a Big Data-driven LDAP directory, allowing you to scale to hundreds of millions of users without sacrificing performance. This store can be cached on-premises or synced directly to Azure AD.

8. Provision to the cloud: With this infinitely-customizable reference image, it's easy to provision cloud applications such as Office 365 with the appropriate user information—and keep this data in sync with authoritative data stores on-premises.



RadiantOne creates an integrated, rationalized identity source, which can then be used to facilitate cloud access and as a global reference to provision Azure AD and cloud applications using sync tools such as AD Connect.

9. Feed your IdP: This reference image can also be used to provide IdPs such as ADFS with the customized identity information they require to facilitate authentication and authorization for SaaS apps.

A federated identity and directory service such as RadiantOne FID works within your existing infrastructure to integrate all identity data into one unified identity data store, including consolidating multiple AD domains and forests. You can get all the benefits of AD consolidation for your existing LDAP applications, plus a unified view of identity for cloud applications and web services that such a service can then synchronize with Azure AD and/or host on AWS.

For more information: https://www.radiantlogic.com/

RADIANT LOGIC™