Centrify Multi-Directory Brokering

Many organizations are embarking on cloud migration projects that require new Windows and Linux instances in one or multiple Infrastructure-as-a-Service (IaaS) platforms. A big concern for them is how to leverage their existing on-premises or cloud-based Identity and Access Management (IAM) infrastructure to enable administrators, developers, and operations teams to access those systems securely, without massive incremental cost, effort, and complexity.

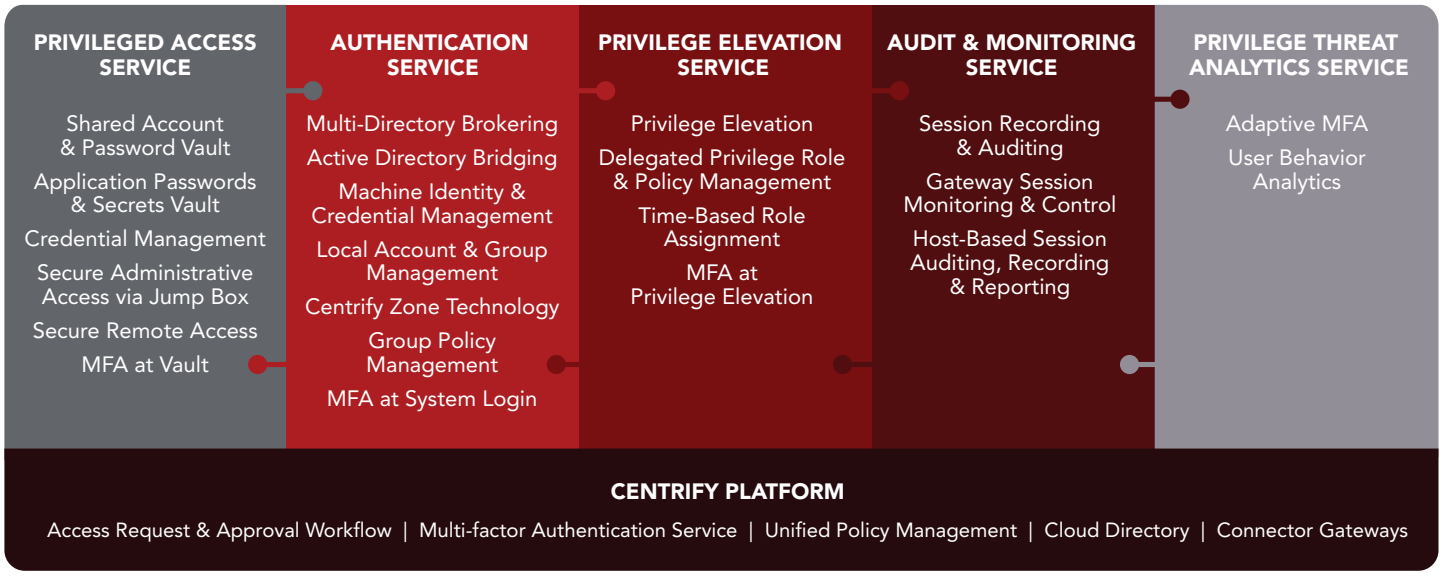
In general, these organizations are faced with having to replicate much of their IAM infrastructure and introduce complex Active Directory trust models to ensure the hybrid IT infrastructure is unified and harmonized and complies with internal and industry regulations for security and privacy.

This solutions brief introduces **Multi-Directory Brokering**, designed to overcome these challenges. It is a capability of the **Centrify Authentication Service**, part of the broader suite of Privileged Access Management (PAM) solutions that is covered under **Centrify Identity-Centric Privileged Access Management (PAM)**.

From its humble roots as the Active Directory Bridging product that Centrify was founded on, Centrify Authentication Service has grown into a rich framework extending PAM to address modern hybrid cloud use cases.

Although we'll use Amazon® Web Services (AWS) in our discussion, the challenge and solutions apply equally to other IaaS providers such as Microsoft® Azure and Google® Cloud.

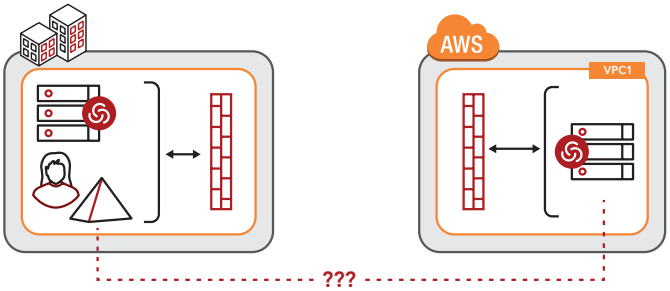
Centrify's Identity-Centric PAM Platform: Modern. Agile. Hyper-Scalable Modular.



Example Use Case

Let's assume you're starting a small proof of concept by standing up a few Windows and Linux Elastic Compute Cloud (EC2) instances in AWS. Developers work on these systems directly, as does the operations team and the system administrators. They all use local accounts to log in since that's quick and easy for a proof of concept.

Fast forward — the proof of concept is a success and now this environment needs to be secured and scaled for production. IT security dictates that these systems must now be brought under Centrify management just like their on-premises production servers. This means deleting or disabling all the local accounts and joining the servers to Active Directory. Users will then log in with their



individual low-privilege corporate Active Directory account and use Centrify privilege elevation to run administrative tasks only when required, in a time-boxed fashion.

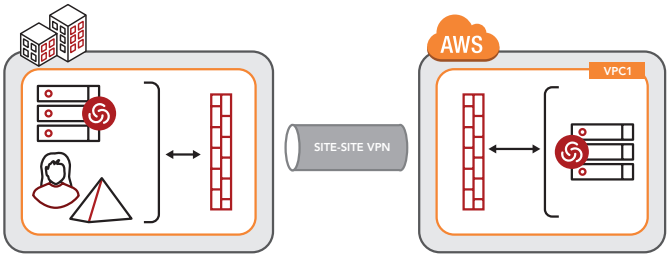
Centrifying the servers is trivial. Possibly your biggest challenge is joining the servers to the corporate Active Directory forest, on-premises.

Solution

You have several options. Let's briefly summarize the main ones.

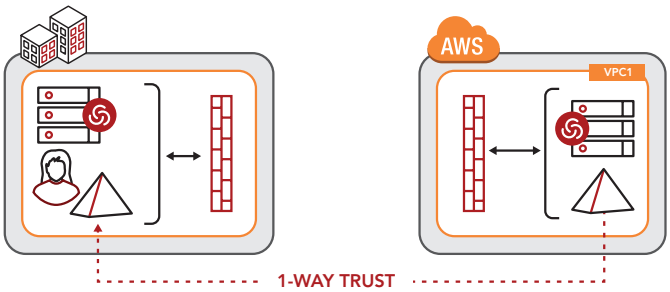
VPN Connection

Multiple options exist for the various IaaS providers. For example, Amazon provides Amazon Direct Connect and Amazon Hardware VPN. As dedicated site-to-site solutions, they can get expensive and they may not be available in every geography. A security disadvantage is having to open all Active Directory ports, which increases the attack surface as an AWS EC2 instance in the VPC can now communicate openly with the corporate Active Directory.



Extend On-Premises Active Directory to the Cloud

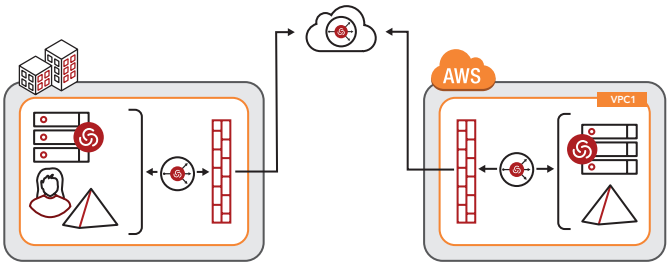
Alternatively, various Active Directory configurations are possible that involve replicating the corporate forest or creating a new forest in AWS, each with varying pros and cons.



A best practice would be to establish a new Active Directory resource forest in AWS with a one-way trust back to the corporate forest. That adds quite a bit of complexity and additional infrastructure, cost, and maintenance; not to mention extra firewall ports that increase the attack surface.

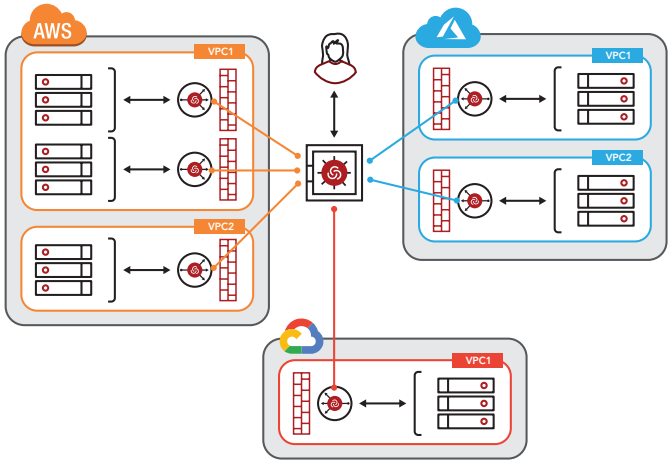
Centrify Client for Linux and Centrify Client for Windows

Centrify has added a modern Brokered Authentication Service to satisfy this hybrid IT use case, focusing on speed, agility, low cost, strong security, and integration with existing on-premises infrastructure and PAM security controls. It involves Centrify Client, Centrify Platform, and Centrify Gateway Connector.



This combination obviates the need for your EC2 instances to join directly to Active Directory for user authentication. Even Windows EC2 instances don't have to be domain-joined. Instead, the EC2 instances join to the Centrify Platform.

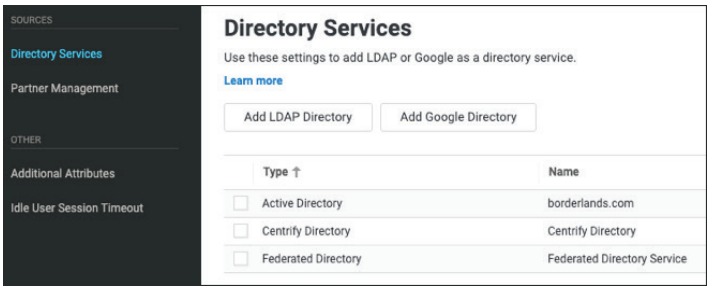
The Centrify Platform has a modern brokered authentication capability that allows it to authenticate users against your corporate directory. With this configuration, users can now log into Windows or Linux EC2 instances using their corporate account without the instances needing direct visibility to the corporate directory. This method is not only quick and easy, but more secure than the alternatives. Since the Centrify Gateway Connector maintains a persistent outbound connection to the Centrify Platform, there's no need to poke additional holes in your firewall.



This solution was also designed to scale in support of modern hybrid use cases. If your applications and services are distributed — across multiple VPCs/VNets or even across multiple IaaS platforms,

traditional password vaults would need to be replicated along with all the supporting infrastructure necessary to synchronize across the systems. Due to its modern hub-and-spoke design, however, and since the Centrify Platform is a true SaaS service, it is accessible from any DMZ, any VPC/VNet, any IaaS provider.

One final benefit — if you happen to maintain administrator accounts in multiple enterprise directories — for example, internal IT in Active Directory and outsourced or third-party identities in LDAP, the Centrify Authentication Service has you covered since it can validate user credentials against Active Directory, LDAP, Google Cloud Platform Directory, or Centrify's own Cloud Directory.

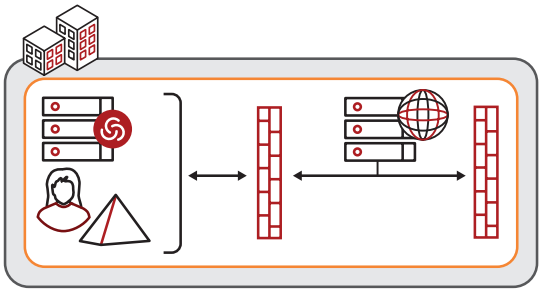


The net-net is that you can avoid the use of local accounts and enable users — administrators, operations team, developers — to log into IaaS instances using their corporate identities without IT having to replicate enterprise directory infrastructure and without these instances needing to join to the corporate directory. Even the Windows instances can be standalone.

Bonus — DMZ Use Cases

Many customers stand up Windows or Linux boxes on-premises in their DMZ for applications such as Web servers. They don't want the inherent risk of extending Active Directory into the DMZ to enable Active Directory-based login, so they use local accounts for user login. Sound familiar?

The solution described above for the cloud-based use case works identically for this use case as well. The servers in the DMZ don't need to join to Active Directory. They instead join to the Centrify Cloud Service, which in turn securely bridges to Active Directory inside the corporate network or the other directories mentioned earlier.



So, this is a prime example of Centrify evolving to solve modern hybrid use cases that legacy PAM solutions are simply not designed to accommodate, but in the process, satisfying an existing security challenge that plagues many customers today.

US Headquarters +1 (669) 444 5200
EMEA +44 (0) 1344 317950
Asia Pacific +61 1300 795 789
Brazil +55 11 3958 4876
Latin America +1 305 900 5354

sales@centrify.com

www.centrify.com