Benefits of SaaS-Based LDAP

A guide for how modern IT/ops teams minimize LDAP hassles

JumpCloud™

How Did We Get Here?

The move to cloud infrastructure creates a host of problems for traditional user management

A significant issue for modern organizations is the management of internal user identities. These identities are important for tasks such as providing access to the internal network and applications, third party and Web-based applications, and server infrastructure whether hosted on-premise or in the cloud.

This issue is growing more complex by the day. With the introduction of Google Apps, SaaS-based applications, and cloud-based infrastructure, IT administrators have interesting challenges that they need to meet — not to mention the proliferation of devices including desktops, laptops, tablets, and mobile devices.

Specifically, the problems that IT admins need to solve with their user directory structure include:

Device support
No longer is a Microsoft Windows desktop the standard device for an employee. In today's "BYOD" (Bring Your Own Device) culture, every employee has a laptop, tablet, or mobile device — and they want each one to connect to their corporate identity.

Synchronization of user identities across services
Users no longer accept that they need different logins for each of their corporate services. IT admins need to figure out a way for their users to leverage their corporate identity across services — whether third party or internal. But with such a wide range of various "types" of services, protocols, and security challenges, that's no easy feat.

Security
The number one IT security risk to an organization is the compromise of one of their employee's credentials, and the scope of that risk has never been greater. IT admins need to ensure that employees have immediate access to cloud applications, internal services, and cloud-based server infrastructure, while keeping hackers out. How do you ensure that all of that is secure and know when a user's identity has been compromised? This is a critical issue for every IT admin, one that keeps many of them tossing and turning at night.

Management

IT admins have less time than ever and more responsibility. IT is critical to making any enterprise work these days. Businesses rely on email, applications, cloud-based infrastructure, and a multitude of devices to get their jobs done. What's the one central, common requirement for all of those services? A secure, robust user store.

The Problem With Traditional LDAP Solutions

Why LDAP breaks down:

Cloud versus on-premise

Organizations are moving more of their infrastructure to the cloud. A modern organization's infrastructure now really only consists of laptops, mobile devices, and WiFi. There is little reason for organizations to put hardware infrastructure within their four walls. They can leverage cloud-based, SaaS services for everything from their document and file storage to CRM. So in this scenario with no servers in the building, where does the user directory live?

Google Apps/Gmail

The hosted Google Apps suite is a major change that Google has been driving for the last several years. As a result, Gmail services – including app-based tools like Google Documents and Presentations – are winning in the marketplace. While the shift has arguably increased some enterprise productivity, it causes significant issues with source of identity (e.g., does AD or LDAP sync with your Google Apps infrastructure or is Google Apps authentication the authoritative source?). If Google Apps is the source of user truth, then how does that hook to your backend IaaS and cloud-based server infrastructure? How do you manage devices?

Resources

Both AD and LDAP require significant time and resources. Most businesses have dedicated IT personnel focused on managing these solutions. Their tasks include ensuring that the directory is in sync and updated with a current roster of employees. They also need to ensure that this core user directory is connecting to all of the different Web-based SaaS-services that the business needs. Further, on the infrastructure side IT admins need to determine how this directory talks to the cloud-based server infrastructure required by developers and operations running the backend applications that the business requires.

The problem is that all of these tasks consume significant time. There are ad hoc password resets, rotation of passwords/keys, and security tasks. And, IT admins know that a user management directory is a 100% uptime service. Any outage means that users aren't connecting to their services and that means loss of productivity and disgruntled employees. Managing an on-premise user directory is painful to say the least.

A Modern Operations Approach - Hosted LDAP

Modern IT organizations know the limitations of LDAP and don't accept the flaws

The most innovative organizations on the planet are aggressively leveraging cloud-based services for everything. They can do this because SaaS-based cloud services provide tremendous benefits and leverage and enable businesses to focus all their energy toward their business goals, not managing and bearing the expense of infrastructure.

Hosted user management solutions such as hosted LDAP are no different.

The benefits of an LDAP-as-a-Service implementation include:

Always-on capabilities
SaaS-based services are available from anywhere at all times and are the underlying core responsibility of the provider. Robust SaaS solutions build in uptime and availability SLAs as a primary part of their business models, mainly so you don't have to. As discussed, a critical requirement for your user directory store is 100% availability. Hosted LDAP services give you that at a much lower cost. You don't need to invest in the infrastructure, code to make it highly available, or the time and effort to manage it.

Standard APIs

Hosted LDAP services know that they are the central source of truth for user credentials. As a result, they will have a variety of ways that those user identities can be consumed for internal and external services. Obviously, the core of a cloud-based LDAP solution is authentication via the LDAP protocol. Additionally, modern hosted LDAP solutions can integrate with Web-federation protocols such as OAuth or SAML. Hosted LDAP solutions can support applications and a variety of devices as well: Windows, Mac OS, Linux, and others. LDAP is a standard protocol that most devices and services will support, and is widely understood by the IT community. For cloud servers, a directory-as-a-service solution can enable access to Windows- and Linux-based servers through native protocols such as Remote Desktop Protocol (RDP) or SSH.

Security

Perhaps one of the most critical reasons modern organizations are moving to hosted LDAP solutions is security. Securing a directory store is one of the most important tasks for an IT admin. How can IT admins easily enforce users to use SSH keys or rotate their passwords or easily review who has accessed their core systems? A single set of user credentials for access to an organization's IT resources is much easier for the employees, but also creates a significant point of risk. Keeping one, central, source of truth and letting that propagate properly is critical to keeping your identities secure.

The smartest modern organizations are leveraging services that reduce their costs, increase their security, and let their best and brightest work on their core business needs. User management is an extremely critical part of the IT infrastructure but generally not a core activity to a company's business, so it's an excellent candidate to leverage as a service.

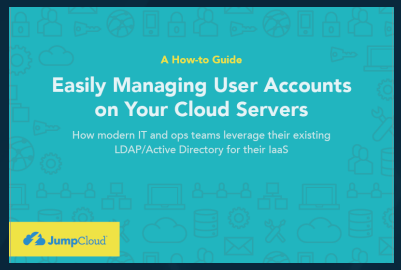
Looking for more Information?

Find out more about what JumpCloud's Directory-as-a-Service can do for your company.

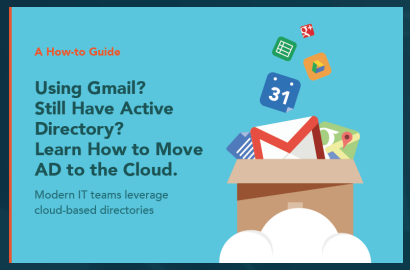
Contact us

For additional reading, blog updates, and the latest news please visit our **blog**.

Read more about DaaS



Easily Managing User Accounts on Cloud Servers
Download the Guide



Using Gmail? Still Have Active Directory? Learn How to Move AD to the Cloud.
Download the Guide

About JumpCloud:
JumpCloud®, the first Directory-as-a-Service (DaaS), is Active Directory® and LDAP reimagined. JumpCloud securely connects and manages employees and their devices and IT applications. Try JumpCloud's cloud-based directory free at jumpcloud.com.