JumpCloud™

Directory-as-a-Service Primer (DaaS)

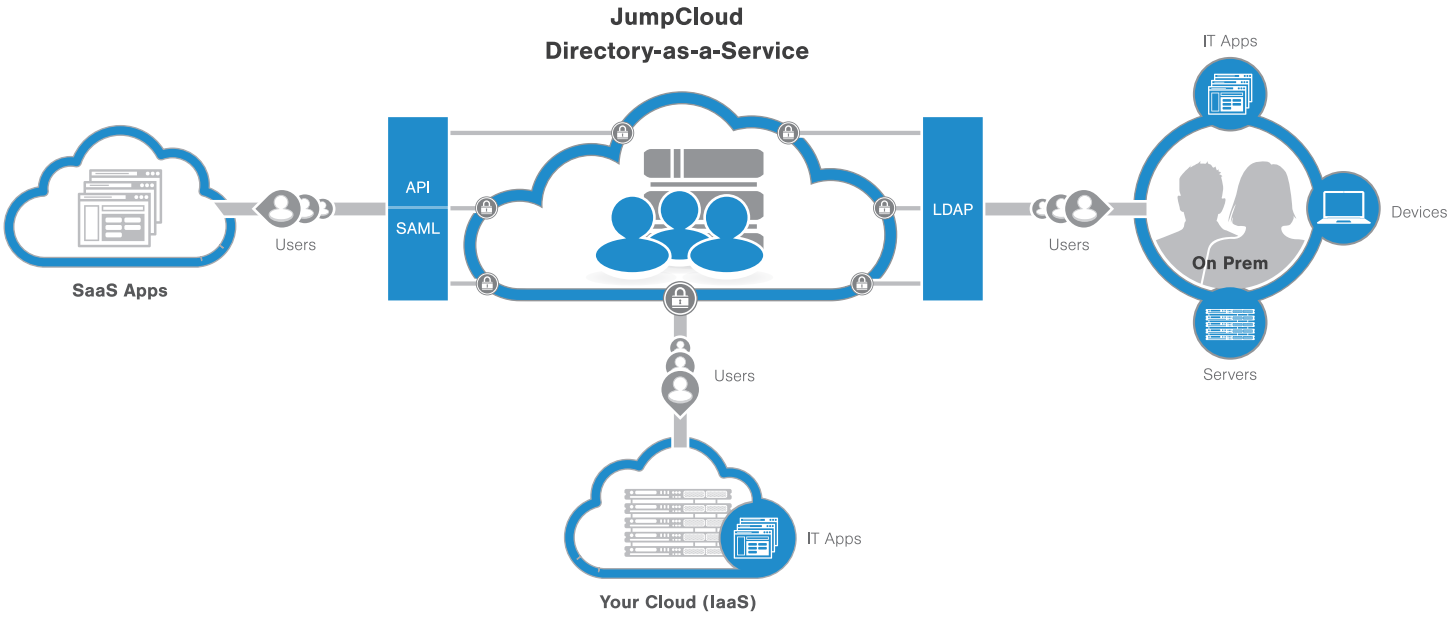
Directory-as-a-Service — or DaaS

is the modern adaptation of traditional Microsoft Active Directory (AD) and Lightweight Directory Access Protocol (LDAP). It is a cloud-based service optimized to authenticate, authorize and manage user access to IT resources across any device type, on any operating system, with any IT or Web-based applications located on-premise or in the cloud.

As a simplified, yet more powerful and economical approach to a user directory, DaaS changes the game for IT admins. Organizations are struggling with the costs and management overhead of maintaining on-premise AD or LDAP in the face of increased IT complexity. These legacy solutions are losing out to new cloud-based alternatives that are streamlined, secure, and easy-to-use. DaaS solutions support all major OS platforms and are designed to control and manage user access to both internal and external IT resources such as servers and applications. In short, a cloud-based directory makes it easier for admins to connect their employees to the IT resources they need, wherever it exists.

Why DaaS?

DaaS is the secure connection and management of employees and IT resources through a single, unified cloud-based user directory. It is the single point of authority and authentication for a business's many employees and access rules. Additionally, it's a central source of truth regarding employees and system users for other complementary solutions such as single sign-on (SSO) technologies.



The Benefits of DaaS

IT admins are underwater with a crushing load of tasks. Meanwhile, cloud-based solutions have become a new staple for IT admins. Cloud-based software off-loads the setup and on-going operations of core IT services to experts. For example, a common cloud-based business solution is Gmail, having supplanted many legacy email systems installed and managed historically on-premises. A SaaS-based directory is an analog to this. By using a cloud-based approach for a user directory, IT admins outsource the setup, configuration, and on-going maintenance of their central user directory. In return, they reclaim precious time, increase security, and gain valuable control and visibility over their IT environment.

How DaaS Works

DaaS is a critical IT service for authenticating, authorizing, and managing users, devices, and applications. A brief description of each function is described below.

Authentication

JumpCloud can act as your directory of record or an extension of your existing directory. Requests to authenticate users are sent to JumpCloud via LDAP protocol or our REST API. The JumpCloud agent can also be deployed on your Windows, Mac, and Linux devices for task and policy management, survivability and security auditing.

Authorization

JumpCloud is your authorization solution, ensuring that the right users have the right access to your IT resources. JumpCloud can manage group membership and sudo access. It can also execute a command when users are added to or removed from any device.

Management

A critical part of a DaaS solution is the ability to manage Windows, Mac, and Linux devices at scale. DaaS simplifies task execution on devices including globally updating policy settings, modifying registry settings, applying patches, and changing system configurations. It ensures consistency across your environment, by allowing you to group like objects and apply the same policies and configurations across them.

Why DaaS is Needed Now

For companies that are leveraging the cloud, have Macs, are on Gmail, or all of the above, a modern solution to the directory is desperately needed to centrally manage and control user access. As most IT admins know, it's hard to patch directory solutions together to accommodate the changing IT landscape. Specifically, while moving to the cloud solves many problems, it also creates others. For example, cloud servers hosted at AWS or Digital Ocean are currently "out-of-purview" for most on-premise hosted directory solutions. As a result, end user cloud apps such as Salesforce and Dropbox are managed by single sign-on vendors which require integration back to the core user store.

Macs are the fastest growing end-user compute device, and they're causing tremendous problems and pain for IT administrators. For most organizations, Macs are not managed devices. That means IT has little control over access and even less over the device's security posture. As more device types appear including phones and tablets, the IT organization is blind to them. These devices will invariably have core digital assets, but will not be managed. That's a recipe for disaster and one that needs to be solved quickly.

The move to Google's enterprise email and productivity services, Google Apps and Gmail, is bifurcating the once dominant Active Directory/Exchange tandem. The challenge is that as organizations move email to Google, they are still stuck with an on-premise directory — an anchor preventing their full move to cloud services. Google's user store is not meant to be a complete directory with full authentication, authorization, and management services. It was largely meant as a contacts list and control point for Google services.

Additionally, single sign-on solutions are very popular today with investors, but unfortunately do not solve core internal IT problems. IT admins know that even with SSO solutions for their Web apps, they still need to manage their desktops, servers, and internal Web apps, not to mention their cloud servers. And, the way that they do that today is through a core user directory and management tools.

These challenges are driving the innovation of DaaS. With decades of history and little innovation, solutions such as AD and LDAP have set a foundation for what will be needed in the cloud era, but unfortunately they have not made the jump. This next generation directory will stand on the shoulders of these giants, but will carve a new path for smart, modern organizations.

Who Should Use DaaS?

Modern organizations that already leverage the cloud are ideal candidates for DaaS. IT admins at these companies know first-hand the challenges of managing access to cloud servers and infrastructure. Further, many of these companies are leveraging Google Apps and Macs, so they know all too well the pain of user and device management.

The cloud era is an opportunity, but also a significant risk for organizations. A modern directory delivered as a SaaS-based service capitalizes on the opportunity while decreasing risk for organizations.

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