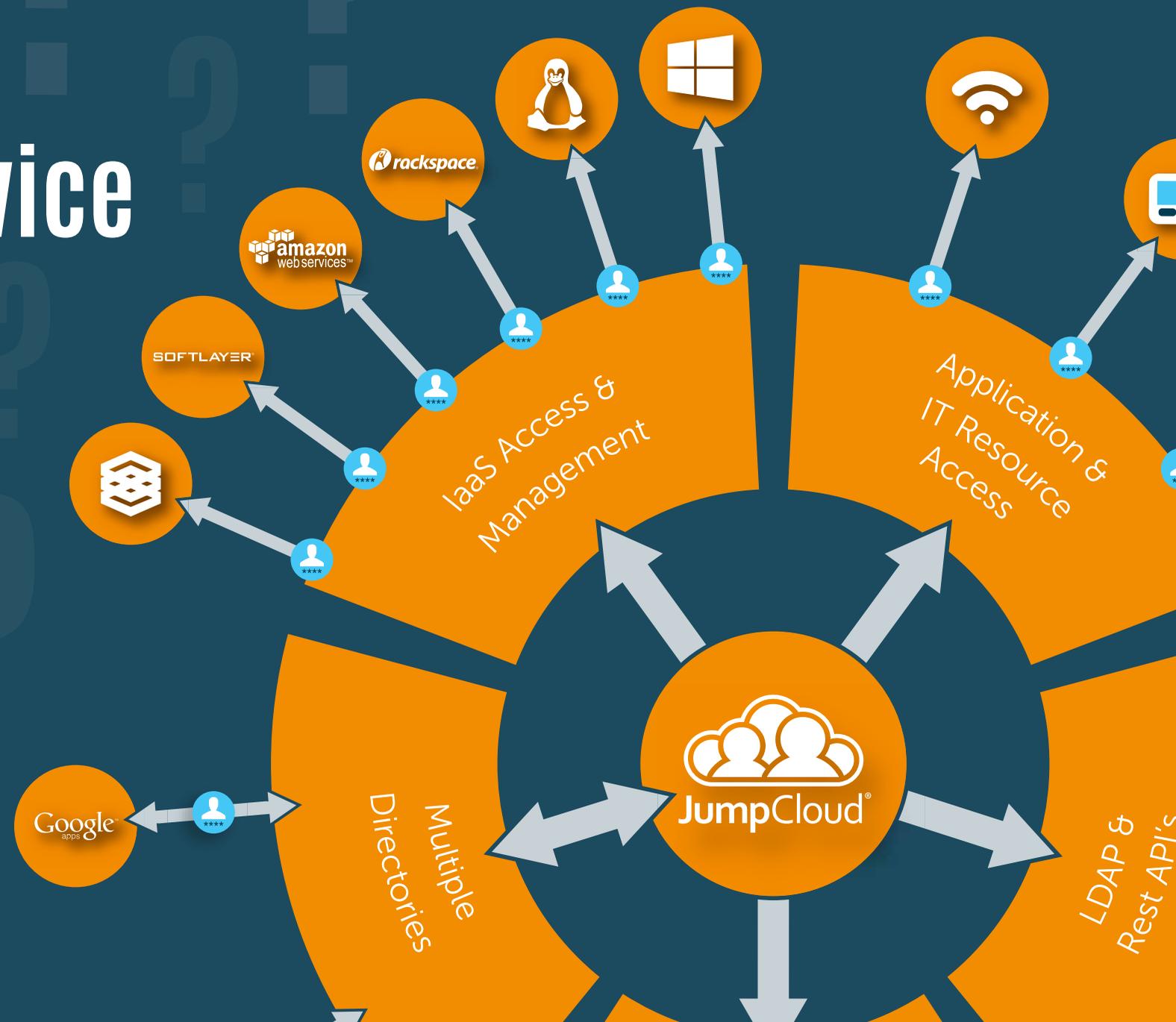


No User Directory? No Problem. Directory-as-a-Service



What is a User Directory?

Many organizations have opted to forgo paying for directory services. While many of these organizations are in the small to medium size category, others are on the larger side. In this paper, we explore reasons why organizations don't implement directory services, the drawbacks and consequences of not having one, and how organizations can easily implement directory services.



But first, stepping back. What is a directory service? A directory service connects users and employees with the IT resources they need to do their jobs, including devices, applications, and Web services. Historically, the leading directory services solutions have included Microsoft Active Directory (AD) and OpenLDAP. The directory authenticates, authorizes, and in the case of AD, manages users with their devices and applications. More specifically, a directory confirms a user is who they say they are (authenticates), controls the level of access that person should have (authorizes), and then manages their devices. Directory services control who should have access to what resources enabling the users to do their jobs.

Why Some Organizations Don't Have a Directory

In most organizations, directory services are at the center of the network, perhaps as critical to the business's overall success as the underlying network infrastructure itself.

The question, then, is **why would any organization forgo implementing this critical piece of infrastructure?**

In reality, there are multiple ways that connecting users to IT resources can be accomplished, and companies have found work-around procedures that do parts of the directory service role. For instance, companies can use an extra piece of software to help automate the process, or they can even manage the process manually.

In talking with thousands of organizations all across the globe, there are a wide variety of reasons why IT admins don't have directory services. These include:



“The organization is too small.” Some organizations feel they're too small to deal with the overhead of implementing a directory. For these companies, manual management of access control seems easier. It's less time consuming, cheaper, and offers direct control. Most of these IT admins manage the connections in their head because there are just a few users. As an organization grows—even over five users—remembering who has access to what IT resources becomes increasingly difficult as the company scales.

Why Some Organizations Don't Have a Directory



“No on-premise infrastructure.” Other organizations don't have a directory simply because they have no on-premise infrastructure. These companies are “born in the cloud” or are “all cloud.” They lack the infrastructure to have servers on-premise or the ability to manage directories. Some companies may utilize outsourced IT management firms. Directory services historically have been placed on-premise and without the ability to host and manage the servers and software, an organization bypasses this critical capability.



“Too complicated to implement.” Directory services are complex and complicated. Virtually every IT resource—devices, cloud infrastructure, internal applications, and Web-based applications—needs to be connected to a directory. While some of these connections are straightforward, others are not. There are complications around OS platforms, protocol support, networking, and security. OpenLDAP, the leading open source LDAP implementation, for instance, requires significant technical knowledge to manage and maintain it. While AD is a bit easier to install, configuring and managing all of the different pieces of functionality is a full-time IT role. For many organizations, the level of effort doesn't match up with the perceived benefits.

Why Some Organizations Don't Have a Directory



“Can’t support modern IT infrastructure.” Many IT organizations have changed their infrastructure in recent years. No longer are they 100% Microsoft based. More and more they are becoming Mac based, or mobile based. Additionally, with the advent of the cloud, more IT infrastructure is living off-premise. SaaS-based applications run more applications that organizations rely upon. These can include Google Apps, Salesforce, Box, and many others. On the other side, IT is leveraging Infrastructure-as-a-Service or cloud server infrastructure. Both of these uses of cloud IT infrastructure, unfortunately, are problematic for directory services. Further, as Macs and Linux devices are more prevalent, directories such as AD and LDAP struggle to connect and manage them.



“Too expensive to run.” As critical as directory services are to an organization, the cost to run the directory often outstrips an organization’s ability to pay for it. Of course there are hardware and software costs, but the real hidden cost of directory services is in the on-going management. Users come and go. Devices are added and decommissioned. Applications are added into the mix. All of this requires IT admins to be engaged with their directory to update the connections. Further, a directory needs to be up 100% of the time and as a result it takes infrastructure and management. Current directories take time and money to run which is an impediment to a large number of organizations.

How Organizations Operate without a Directory

After understanding why organizations don't leverage a central user directory, the question becomes, "How is this task accomplished, then?" IT admins are creative in solving the problem.



Manual management. Perhaps the most common alternative to a user directory is manual user management. IT admins hand-provision users on devices and applications. When users leave, they manually delete them from IT resources. Admins often will create spreadsheets to manage the details of user access or some will script the process of provisioning and deprovisioning users to create some automation. With a limited number of users, platforms, and applications, manual management is a reasonable approach to controlling access. Business continuity and security, of course, can be compromised in this scenario. There are often only a few IT admins at an organization, and the job can become bigger than they can manage. Further, security takes a back seat as admins in this scenario struggle to find the time to apply best practices.



Configuration Management Tools. For organizations that have grown up in the cloud, or who have embraced DevOps, tools like Puppet, Chef, Salt, or Ansible (among many others) offer a centralized management tool that can provide user management on servers in organizations of up to about 30 people. These tools allow IT admins to provision users, primarily on production systems (as they are not often used in development, test, or desktop environments), via a central set of scripts. The downside to these tools is that they achieve this through the use of scripting, and each change requires a code change. Further, these scripts become very complex when exceptions are needed.

How Organizations Operate without a Directory

By the time an organization reaches 30 users, these exceptions become common, as do third-party audits, which require fine-grained access control. Configuration management tools do not handle these types of requirements well. In addition, configuration management tools do not satisfy the user management needs of IT for their desktops, laptops, and applications.



Google Apps Directory. Google's corporate Gmail solution has become a standard for small to medium-sized enterprises. With email a primary business application, organizations place their users in the Google Apps Directory. The users then have access to a number of Google services and they can also use their Google credentials with other Web-based applications and services. The Google Apps Directory, however, does not extend to devices such as a user's desktop or laptop. Further, an organization's server infrastructure – whether on-premise or in the cloud needs to be managed in a different way outside of Google Apps Directory. For organizations that don't need a significant amount of IT infrastructure, Google's directory could be an excellent option. However, for those companies that need more than just email and Google services, Google Apps Directory will not be sufficient.

Directory-as-a-Service, the Solution for No Directory Situations

“Innovative organizations don’t settle for these issues with directory services. IT admins at these companies” “know that a central user directory is absolutely imperative. It’s arguably the most critical piece of infrastructure within an IT organization. Manually managing users, trying to script the process, or leveraging Google Apps Directory is not good enough. SSO solutions, while valuable, don’t give IT admins the level of control that they desire. As a result, while most organizations go without a central directory, these innovative companies opt for a modern solution to directory services—Directory-as-a-Service, or DaaS.”

“DaaS eliminates many of the roadblocks that organizations face with a directory. As a hosted directory service,” “there is no infrastructure for IT admins to implement or manage. That means that things like backups, upgrades, security, networking, and maintenance are all handled for you. As a result, a hosted central user directory takes less time and expertise, making it ideal for small to medium sized enterprises.”

“Perhaps the most critical aspect of DaaS is the ability for it to function as the central directory for virtually all IT” “resources including devices, applications, and cloud/Web infrastructure. DaaS leverages multiple authentication protocols including a device’s native authentication, LDAP, and SAML. This enables the” “SaaS-based central directory to control desktops, laptops, and servers whether on-premises or in the cloud. Further, LDAP and SAML authentication enables the DaaS solution to control access over applications both” “internal and Web-based. A DaaS solution supports the modern IT infrastructure that companies are moving to.”

Directory-as-a-Service, the Solution for No Directory Situations

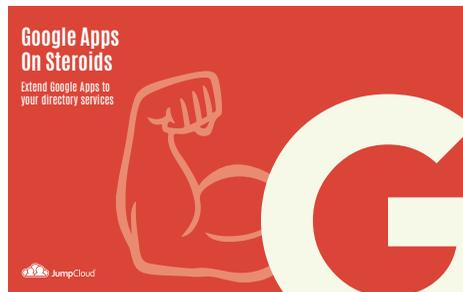
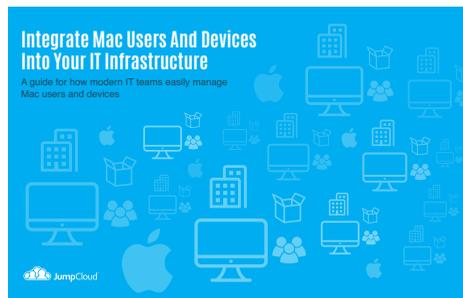
Another critical aspect of DaaS solutions are that they are cost-effective. Because of their SaaS-based approach, organizations only pay for what they use, so the solution becomes scalable. Further, there are no separate hardware, software, and implementation costs. A simple, monthly subscription model covers what organizations need for their directory services.

For organizations that don't have a formal user directory solution, DaaS is an ideal approach.

For more information on DaaS, contact [JumpCloud](#) or give DaaS a try. 10 users are free forever.

Looking for more information?

Click these guides to learn more about DaaS:



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

About JumpCloud:

JumpCloud®, the first Directory-as-a-Service® (DaaS), is Active Directory® and LDAP reimaged. JumpCloud securely manages and connects employee identities to IT resources including devices, applications, and networks. Try JumpCloud's cloud-based directory free at JumpCloud.com or **contact us at 720.240.5001**.

[Contact us](#)

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

Or follow us:

