Datasheet

May 2021

Advanced Server Access

A zero trust approach to securing access to protected resources in the Cloud

At any scale, controlling access to servers is a challenge for IT and security teams. It's a delicate balance: DevOps and IT need fast, flexible access to compute resources to do their jobs, but without putting the enterprise at risk. Static credentials are inherently risky, consistently targeted by attackers hoping to gain unauthorized access to enterprise assets.

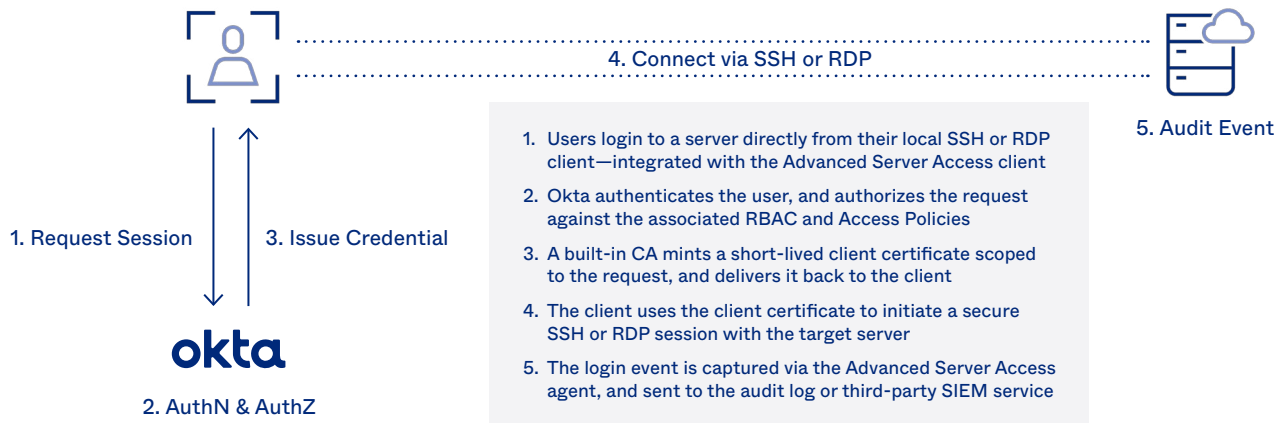
Historically, the problem has been that the credentials themselves hold the privileges, with no way to consider the context of the user or the device. Now, Okta Advanced Server Access provides that critical context, centralizes control, and seamlessly secures your infrastructure—in the cloud or on premises—with a Zero Trust architecture capable of making smart, informed access decisions in real time.

Provide secure access to cloud resources, and simplify access management

Managing secure access to ephemeral server instances in the cloud with static credentials poses a significant challenge. Legacy server protection solutions or homegrown solutions your organization may have built to address the problem can have limitations, including security gaps, a burdensome user experience, and the ongoing costs of keeping a DIY solution current.

Okta Advanced Server Access takes a modern approach to server access by eliminating the need for static keys, and introducing cloud-first, zero-trust access management for AWS EC2 instances. Authorized parties receive dynamic single-use access to exactly the servers they're authorized for at this moment in time, significantly minimizing the attack surface. And IT gets new tools to centralize access management and set policies informed by user, device, and session context, and simplified lifecycle management tools for automating provisioning and deprovisioning users and groups to server instances.

How Okta Advanced Server Access Works



1. Users login to a server directly from their local SSH or RDP client—integrated with the Advanced Server Access client
2. Okta authenticates the user, and authorizes the request against the associated RBAC and Access Policies
3. A built-in CA mints a short-lived client certificate scoped to the request, and delivers it back to the client
4. The client uses the client certificate to initiate a secure SSH or RDP session with the target server
5. The login event is captured via the Advanced Server Access agent, and sent to the audit log or third-party SIEM service

Together, Okta Advanced Server Access + AWS let you:

- Protect cloud infrastructure from credential-based threats
- Replace risky static credentials and keys with dynamic, single-use ephemeral client certificates
- Dramatically simplify account lifecycle management, including user provisioning and deprovisioning to compute resources
- Deliver seamless Single Sign-On (SSO) and Multi-Factor Authentication (MFA) to your SSH and RDP workflows, inline to the protocols
- Get fine-grained contextual controls to guide informed access decisions
- Quickly update cloud-access security to meet compliance requirements like SOC2 or PSI
- Easily enroll servers into configuration management solutions like Terraform, Puppet, or Chef
- Capture login events for auditing

Additional features of Okta Advanced Server Access + AWS

Agent enrollment

VPC jumping

Auto-scaling groups

Meta-data integration

Bastion architecture

AWS account mapping

How Okta Advanced Server Access + AWS work together to secure and manage cloud server access

Okta Advanced Server Access lets you install a lightweight agent on servers to configure them for client certificate authentication, and to capture login events for audit trails. Centralized access controls across AWS cloud instances let your teams make granular, contextual access decisions that consider device, session context, and dynamic user information.

After the agent is installed and users log into a server directory with their local SSH or RDP tools, Okta authenticates them according to role-based access policies. A short-lived, single-use, narrowly-scoped certificate is minted and returned to the client, which initiates secure access. Local server user and group accounts, once authorized, can enjoy streamlined access to AWS servers for their workflows. Extending the benefits of Okta Identity to AWS server access reduces the risk of credential harvesting and other security threats, and seamlessly extends the Okta benefits you know and love to your cloud infrastructure.

Similarly, Advanced Server Access working in the AWS environment extends Okta's familiar lifecycle management tools to compute resources in the cloud.

Provision users and groups into servers as easily as you provision users and groups into applications, disable the cloud server access of departing users automatically, and apply protective MFA wherever it's needed or desired.

Teams can access these tools in multiple ways: via a webpanel, at the command-line level, or, at sufficient scale, via an API-driven setup. (In testing environments, for example, API automation can allow multiple engineers or development groups to stand up separate cloud resources and configurations to work on individual features on an as-needed basis).

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 7,000 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. More than 10,000 organizations, including JetBlue, Nordstrom, Slack, T-Mobile, Takeda, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers.