Whitepaper

September 2022

Okta's High Availability Architecture

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871

okta

Contents

Introduction

Nothing is more critical than trust when you've decided to adopt cloud services supporting mission-critical systems and capabilities. You need to trust that the cloud vendor is available, scalable, resilient, reliable, and as committed to security and compliance as you are.

This is especially true when it comes to identity and access management (IAM). Your IAM infrastructure essentially serves as the central point through which your team monitors and secures access to all your applications.

The stakes are high, and hosting core IAM infrastructure on a cloud platform can sometimes feel like a leap of faith, especially for organizations that are accustomed to managing their own proprietary identity infrastructure. If on-premises software or servers experience downtime or an outage, IT admins can take immediate action to solve the problem internally—a scenario not always possible when relying on external third parties.

Furthermore, organizations in highly regulated industries are often cautious when considering cloud infrastructure, as they may be required to report to regulators any situation where the security and privacy of data is compromised, or when critical information systems are rendered inaccessible. In such cases, it's only natural for organizations to want to maintain full control over their IT functions.

> "Therefore, the question you should be asking isn't whether you should work with a cloud vendor to supply your IAM capabilities; the question is which vendor you should work with."

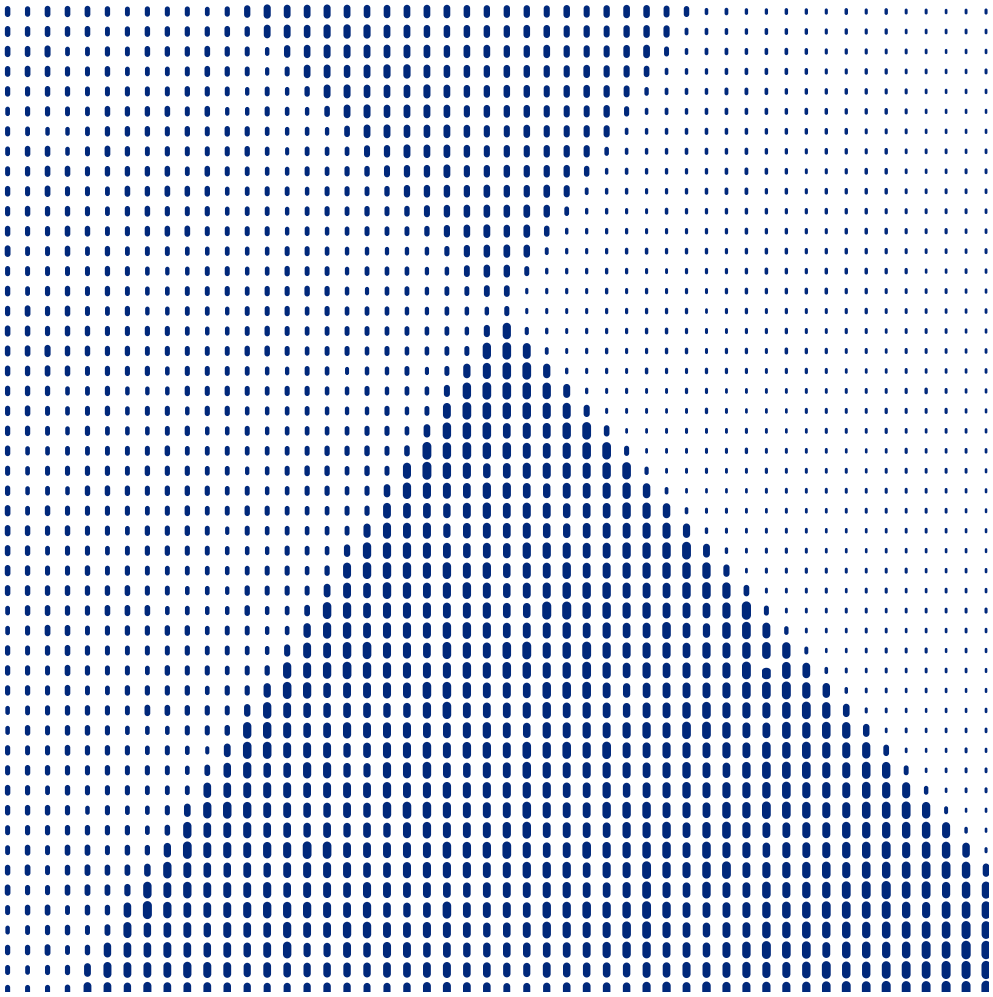
However, the benefits of outsourcing IT infrastructure to cloud partners have been proven repeatedly. It doesn't just significantly reduce the total cost of operations and ownership, it also provides superior security compared to legacy, on-prem platforms.

Therefore, the question you should be asking isn't whether you should work with a cloud vendor to supply your IAM capabilities; the question is which vendor you should work with. Who can you trust to deliver constant uptime, with scalability and flexibility, and the security and protection your users deserve?

The Okta Identity Cloud was designed to be trustworthy. We've built the software, operationalized the processes, and hired the talent it takes to offer customers a suite of best-in-class solutions that adhere to the highest standards. Okta is:

- Built for web scale: the service scales up and down seamlessly according to your needs;
- Always available: the service is architected for zero downtime. No maintenance windows required;
- Secure: the service is more heavily audited than anything that can be built and maintained in-house; and
- Constantly evolving: the service enables new capabilities and rapid innovation, and insulates your organization from the constantly changing IT landscape.

This technical whitepaper offers a comprehensive overview of the software and operational architecture that enables Okta to run a scalable, highly available, on-demand IAM service with 99.99% uptime.



Protection Throughout the Stack

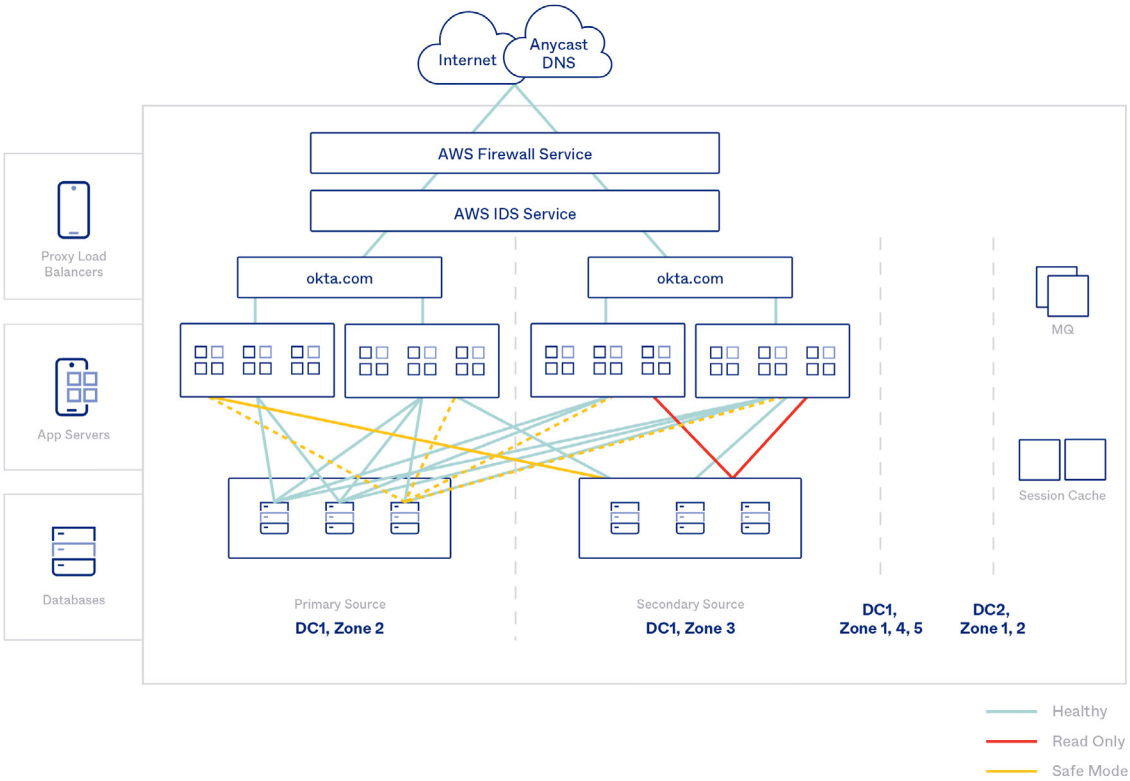
A highly available service begins with incorporating redundancy at every step.

Resilient architecture

One of the most critical aspects of Okta's architecture is that it is completely multi-tenant. With this design, customers share the same underlying environment. This creates an economy of scale, allowing Okta to make the infrastructure extremely robust in terms of redundancy, monitoring, and processes.

Each Okta environment is called a cell. Okta cells contain all of the infrastructure required to operate an instance of Okta. More information about cells can be found in the An Insider Look: How Okta Builds and Runs Scalable Infrastructure whitepaper. Because each cell can operate independently, they form the basis of our availability strategy by helping to limit the number of customers impacted by an outage.

Within each cell, the system consists of a front-end tier containing proxy load balancers and firewall services, an application tier where our software runs, and a set of functionally optimized database services. Everything is hosted in Amazon Web Services (AWS) across multiple availability zones and geographically separated regions. The service is designed for high scale, high throughput, and high availability.



Stateless

Except for databases, all components are functionally stateless. As a result, above the database tier, any server in the stack can handle any request.

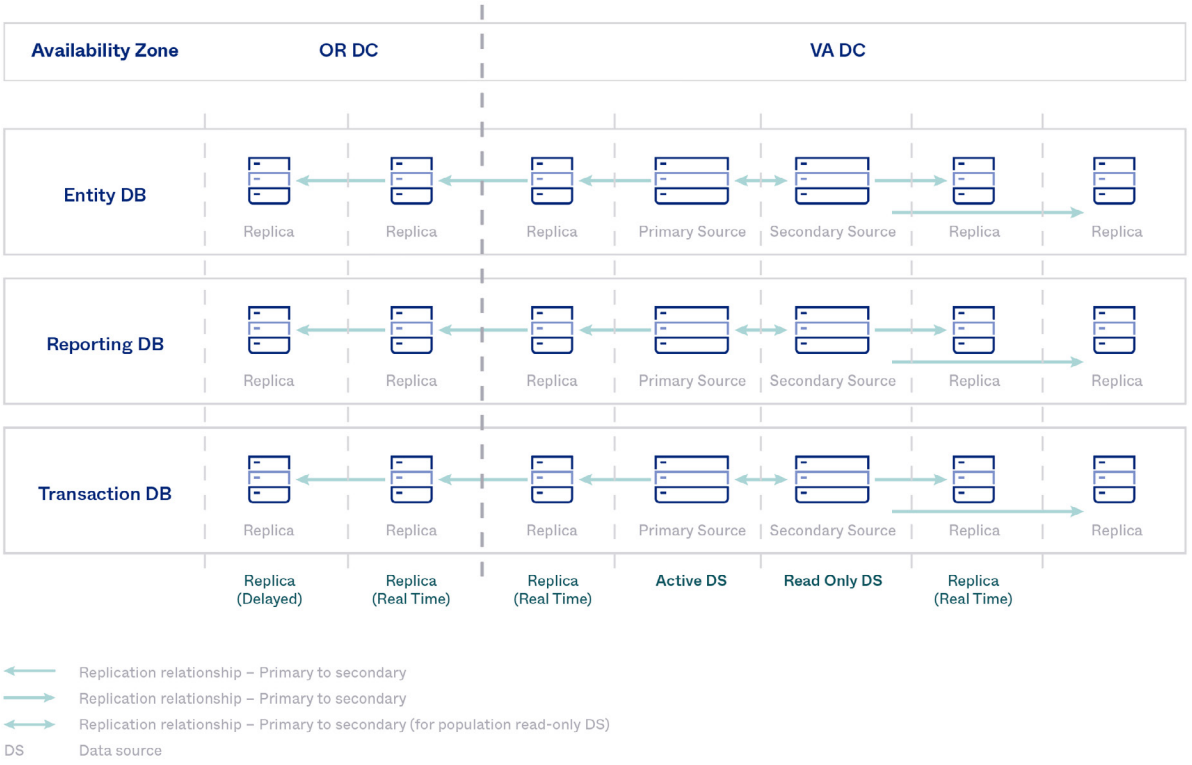
That means that all of the components of our system can be scaled up at will simply by spinning up new services in AWS. This allows Okta to automatically adjust to changes in demand and route around failed services to other active systems.

Requests are queued and processed by available application servers so that application server failures are transparent to users. If an application server fails, the authentication is automatically forwarded to a functioning server and retried.

Functionally optimized databases

While it is possible to add and remove stateless components above the data tier at any time, that is not true for the database layer. Database services must not only retain state, but also manage transactions to ensure that customer data is maintained and not corrupted in the case of an outage.

We run a highly available configuration with read replicas so there is no single point of failure. If one primary database goes down, the other is promoted. Replicas are live across multiple availability zones in two distinct AWS regions, including a time-delayed replica, allowing Okta to quickly restore in the case of data corruption.



No single points of failure

Subprocessor failover

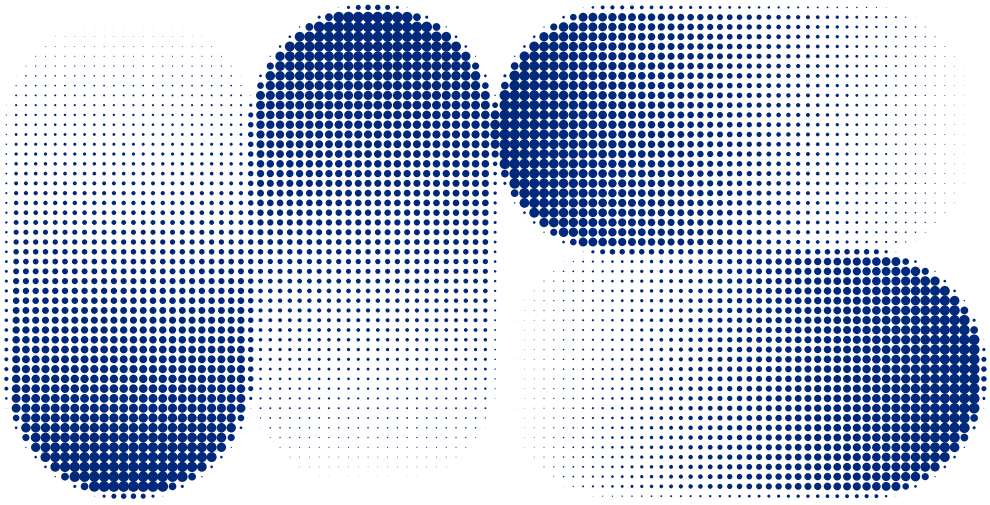
We're not perfect. In 2016, Okta suffered an outage due to a vendor who fell victim to one of the largest distributed denial-of-service attacks in history. Okta's customer support team scrambled to help our customers restore service, and afterwards, a full root cause analysis (RCA) was performed to identify any other single points of failure that may exist in the service. As a result, Okta identified and implemented backup vendors for our subprocessors that help us serve our customers' critical identities. From SMS and voice authentication to round-the-clock customer support, Okta is ready to react. As part of the vendor risk-assessment program, Okta also assesses subprocessors for disaster recovery readiness.

Employee failover

Recovery of the service also requires contributions from Okta team members who are able to support it. Okta's disaster recovery and business continuity plans therefore include provisions to ensure that, in the case of a regional disaster, employees are geographically distributed. Each team also maintains multiple methods of communication, so in the event of concurrent loss of production and corporate services, engineering teams are able to communicate and focus on restoring the service.

Data backup

Replication across multiple availability zones and regions ensures that Okta is able to function as a highly available service, but it does not provide adequate protection in the event of a catastrophic failure of AWS infrastructure or data corruption. Therefore, Okta also takes frequent database snapshots and stores them in a read-only, protected account. These encrypted, protected backups serve as a failsafe that enables Okta to restore the service across fresh infrastructure as needed.



Identity that's always on

No maintenance windows

Traditionally, the ability to provide a highly available service is in direct conflict with delivering continuous innovation to that service. At Okta, we knew we couldn't make that compromise. By combining a canary-based deployment architecture with an automated testing and deployment process, we can deliver continuous innovation with no planned downtime or maintenance windows required.

Any development committed to our mainline code kicks off with a new build and a series of unit, functional, and security tests. Once the fully automated process completes and ensures that the code has passed our rigorous testing, the software is ready to be deployed.

The operations team then deploys the fully tested code to our customer-facing environments. Product updates are first published into the preview environment to allow customers to perform their own acceptance testing. After one week, the changes are published to production. Throughout this rolling deployment process, we ensure upgraded app servers only talk to upgraded versions of the data backup, avoiding the risk of data corruption.

Proactive monitoring

"The first layer of defense against the unexpected is robust instrumentation and monitoring for all components of the system. We split this into two categories: external monitors and internal monitors."

Disasters are never caused by one single event; they typically come about through a chain of events that must all happen together. Identifying and stopping this chain early is key to a successful high-availability program, and that's why Okta invests heavily in proactive monitoring of the service.

The first layer of defense against the unexpected is robust instrumentation and monitoring for all components of the system. We split this into two categories: external monitors and internal monitors.

For external monitoring, Okta uses multiple services with globally distributed test agents to constantly monitor our application. This provides us with a constant feed of real data on how our service is operating. Because we are fully multi-tenant, the data is real and applicable to all of our customers.

We also use internal monitors to show us when things are having problems, but more importantly, we use them to show us what systems are having problems. They are more sensitive than the external monitors, so they frequently warn of problems before they affect site performance or availability. Okta uses internal monitors on all subsystems and software components for maximum visibility.

Rapid disaster recovery

As the market leader in IAM, Okta is used to control access to all types of mission-critical data for our customers, and this data must be available all the time. Okta's architecture is therefore designed to be highly resilient and always available. But even the best systems can fall to unforeseen events. In these cases, Okta provides a one-hour recovery time objective (RTO) for authentications and a 24-hour RTO for full restoration of the service, which exceeds the availability of many other cloud services. This way, as we deal with an incident, you don't have to worry about data loss.

Backing up your data is only half of the battle, and the middle of a disaster is not the right time to test whether you can successfully restore your service. That's why Okta performs disaster recovery testing at least quarterly. These tests ensure that when the team is required to respond to an emergency, they will have honed the required skills and the data will be ready.

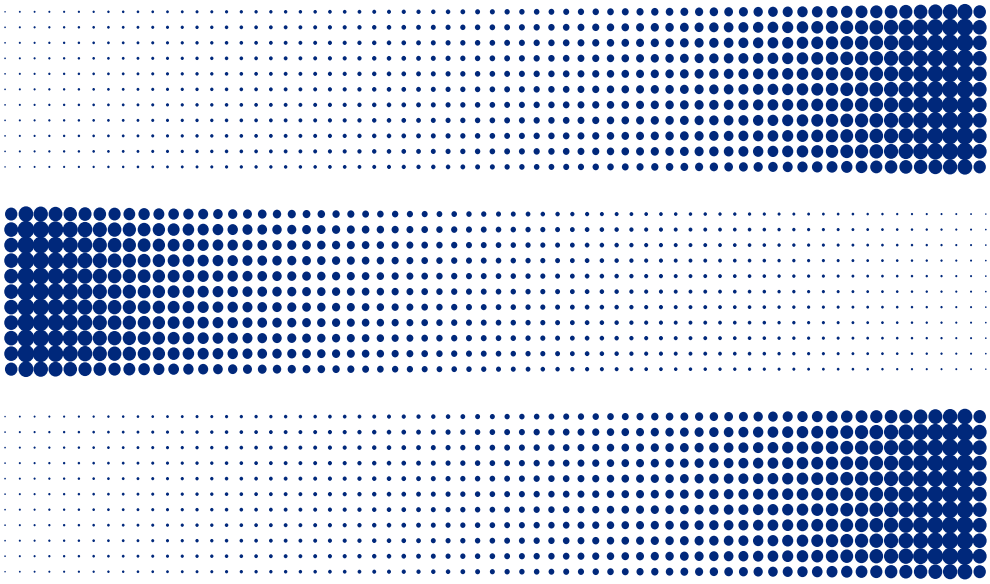
Disaster recovery is a core control of compliance programs like PCI, SOC2, and ISO 27001, each of which require evidence of regular testing for in-scope systems. To help our customers demonstrate their ability to meet these requirements, Okta publishes attestations for each of our tests through a self-service documentation portal. These attestations include when the test was performed, its duration, the result, and any actions Okta is required to take to ensure your data is ready when you need it.

In addition, Okta publishes statistics on status.okta.com, which includes not only the current status, but the history of any outages and performance issues that affect the service, whether or not they were caused by Okta. We also provide detailed information about the issue and what Okta is doing to prevent it from happening again.

Conclusion

At Okta, we understand that when your identity system goes down, business stops. That's why we've designed our system to be resilient to the known and the unknown, and we stand behind that statement with industry-leading service level agreements and transparency. Across the entire system lifecycle, from design to deployment, maintenance and disposition, Okta is built to be always on.

Want to learn more? We'd love to hear from you, please email us at: info@okta.com



About Okta

Okta is the leading independent identity provider. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With more than 7,000 pre-built integrations to applications and infrastructure providers, Okta provides simple and secure access to people and organizations everywhere, giving them the confidence to reach their full potential. More than 14,000 organizations, including JetBlue, Nordstrom, Siemens, Slack, Takeda, Teach for America, and Twilio, trust Okta to help protect the identities of their workforces and customers. For more information, go to **okta.com**.