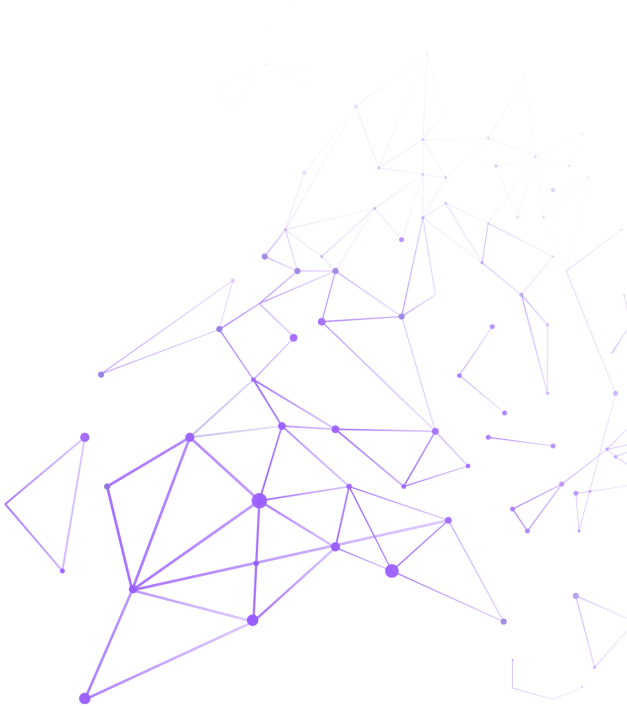
Teleport



Root Cause Analysis

2025-10-20: US East Region Connectivity

Teleport

Summary

On October 20, 2025, between 06:48 and 22:07 UTC, some Teleport Cloud customers experienced issues connecting to their cluster. These issues were triggered by an AWS outage impacting the US East region (N. Virginia: us-east-1). The severity of the impact was dependent on the type of Teleport Cloud deployment and where users or agents were located.

- Customers with single-region auth service deployments in the US East region were unable to connect to their cluster
- Customers with multi-region auth service deployments in the US East region experienced intermittent connectivity issues
- Users and agents located near the US East region experienced intermittent connectivity issues

Impact

Teleport Cloud services were impacted during two related but distinct periods.

The first period occurred between 06:48 and 09:23 UTC. Customers with a single-region auth service deployment located in the US East region were not able to access their Teleport cluster. Existing sessions were unaffected but all workflows requiring the auth service, such as certificate issuance, were unavailable. The root cause was failed connections to DynamoDB by auth services in the US East region, which was reported by AWS as a DynamoDB outage resulting from a race condition updating DNS. Workflows requiring the auth service recovered once AWS updated their DynamoDB DNS endpoint configuration.

Users and agents located near the US East region experienced intermittent connection failures if their Teleport Cloud deployment includes an auth service located in the US East region. This includes both single and multi-region auth service deployments. The root cause was a cascading failure within AWS impacting the AWS Security Token Service (STS), which is used by Teleport Cloud to access multiple AWS services. This includes the AWS Key Management Service (KMS), which is required to issue certificates during the user login workflow. The STS issue also prevented US East auth services for multi-region auth service deployments from writing audit log events.

The second period occurred between 12:30 and 21:09 UTC. All connectivity to Teleport Cloud deployments in the US East region were impacted by intermittent connectivity issues. The root cause was a cascading failure within AWS impacting AWS Network Load Balancers (NLB) used by all Teleport Cloud deployments.

Between 12:30 and 15:52 UTC, less than 5% of all connections to the US East region experienced issues connecting to US East load balancers. By 15:52, connectivity degraded, triggering health check failures and automatic DNS failover, which routed new connections to the next closest region (US West or EU Central). New connections began routing to the next closest region within 5 minutes. It took another 35 minutes for external DNS propagation to impact the majority of all connections.

DNS recovery was triggered once US East load balancers were restored at 21:02, routing all new connections through the US East region once again.

Operations

At 06:58 UTC, Teleport Cloud operations responded to alerts triggered by backend write failures in the US East region. After identifying the issue reported by AWS, the team attempted to update the Teleport Cloud status page (status.teleport.sh) but failed due to a related outage by a third party service provider. The operations team then prepared an email status update which was sent to all customer security contacts by 08:51. The team updated the status page retroactively once it became available at 10:00.

At 15:27 UTC, Teleport Cloud operations responded to health check alerts. The status page was updated at 15:59 after the team observed connections routing away from US East due to DNS failover. The team continued to monitor connectivity and respond to customer requests throughout the day; and by 21:07, connections were observed routing back to US East as a result of DNS recovery. The team continued to monitor, keeping the incident open until AWS reported load balancers in US East had fully recovered. The status page incident was resolved at 22:56.

Background

All Teleport Cloud deployments are highly available. Proxy services, which handle connectivity between users and resources, are deployed globally to six AWS regions, and each region has two services running in distinct availability zones. This configuration allows proxy services to failover between availability zones and regions when a service is unhealthy or due to a network partition.

Auth services, which handle authentication, certificate issuance, and audit event workflows, support two different deployment models. The single-region deployment model consists of two auth services deployed to two distinct availability zones running in a single region. The multi-region deployment model consists of at least four auth services deployed to four availability zones across two regions. In either model, if a single auth service is unavailable, the Teleport cluster will continue to function by routing connectivity to a healthy auth service.

Teleport Cloud includes additional redundancy beyond Teleport Proxy and Auth Service high availability. All connections flow through AWS network load balancers to an internal ingress service, both of which are deployed with redundancy. Teleport Cloud is also configured with per-cluster health checks and DNS latency records. Health checks verify connectivity and latency globally. DNS latency records measure per-cluster response time regionally and automatically detects connectivity issues such as unhealthy load balancers.

DNS failover was initiated during the second period of this incident when load balancers in US East became unavailable. This type of failover - impacting all edge network load balancers in a region - is the last resort for Teleport Cloud resilience. All other forms of redundancy such as auth and proxy services failover quickly. DNS failover takes more time due to propagation delay. Failover with DNS is a byproduct of using network load balancers. Teleport Cloud's architecture utilizes network load balancers to ensure long-lived connection stability because alternatives such as anycast do not provide the same long-lived connection stability guarantees.

Teleport

Actions

The following action items are being tracked by Teleport.

Multi-Region Failover Support for KMS

Status: In-Progress
ETA: 2-3 months

Users of multi-region auth service deployments should be able to login when STS is not available in a single region. This work was already planned to begin in November.

Audit Event Delivery Resilience

Status: Pending
ETA: 6 months

Audit events should not be dropped when the STS service is unavailable.

KMS Alerting

Status: In-Progress
ETA: 1 month

Enhance ability to detect issues accessing KMS by creating new alerts tracking existing metrics.

Email Communication Enhancements

Status: Pending
ETA: 3 months

Reduce the time to send email communications when the status page is unavailable by updating email service distribution lists automatically and updating the runbook.

Links

Teleport Cloud Status: Period 1 | Period 2
Teleport Enterprise Cloud Architecture
AWS RCA